Click to verify

When it comes to running a business, especially a small or medium-sized enterprise (SME), technology is often the backbone of your operations. From emails and data storage to specialised software and customer management tools, you rely on your IT infrastructure every single day. But with this reliance comes a critical responsibility: ensuring that your systems are up-to-date and secure. One of the most effective yet often overlooked ways to do this is through patch management. In this blog, we'll break down what patch management is, why it's important, and how it can benefit your business. What Is Patch Management? In simple terms, patch management is the process of regularly updating your software with "patches." These patches are small bits of code that software developers release to fix security vulnerabilities, bugs, or to improve the functionality of their products. Think of it like maintaining your car. You wouldn't skip oil changes or leave a brake issue unattended, would you? Similarly, you shouldn't ignore the need to update your software when developers release patches that fix important issues. Why Does Patch Management Matter? While it may sound like a minor task, patching plays a huge role in protecting your business. Cybercriminals are constantly looking for vulnerabilities in software. If you don't patch these weaknesses, your business could become a target for attacks, data theft, or system failures. Benefits of Patch Management: Enhanced Security: The most crucial benefit of patch management is that it helps keep your systems secure. Most patches are released to address security flaws that hackers could exploit. Without regular patching, your business is more vulnerable to cyberattacks. Better Performance: Patches don't just fix security issues; they can also make your software run better by improving speed, stability, or adding new features. You'll often find your systems running smoother and more efficiently after applying patches. Compliance: Many industries have strict regulations regarding data protection and cybersecurity. By keeping your software updated, you ensure compliance with legal standards, reducing the risk of fines or legal complications. Minimised Downtime: Unpatched systems are more likely to crash or face issues that disrupt your business. Regular patching helps prevent costly downtime, allowing your operations to run smoothly Cost Savings: Handling issues before they become full-blown problems saves you money in the long run. An unpatched vulnerability can lead to a costly breach or system failure, which is far more expensive than staying on top of updates. The Challenges of Patch Management While patch management has many benefits, it's not without its challenges. Here are a few of the common issues businesses face: Time-Consuming: Patching can take time, especially if you have a lot of software across multiple devices. If not managed properly, it can disrupt your daily operations. Compatibility Issues: Occasionally, new patches can cause compatibility issues with existing software, which could lead to new problems instead of solving them. Testing patches before deploying them is crucial. Lack of In-House Expertise: Not all SMEs have dedicated IT teams who can handle patch management. Without expert knowledge, businesses might neglect updates or incorrectly apply patches, leaving them exposed to risks. Frequency of Updates: Software providers release patches frequently, and it can be tough to keep up. Many businesses delay applying updates due to concerns about downtime or disruption, but this creates a window of opportunity for cyberattacks. How a Managed IT Service Can Help The good news is that you don't have to handle patch management on your own. As an IT support provider specialising in helping SMEs, we can take care of the entire process for you. With our services, we: Automate patch management to ensure updates are applied promptly without disrupting your operations. Monitor your systems 24/7 to detect available patches for known issues and ensure that all patches are applied in a timely manner. Provide regular reports so you can see exactly what has been updated and how it benefits your business. By working with us, you'll gain peace of mind knowing that your systems are secure, up to date, and running smoothly, allowing you to focus on what really matters—growing your business. Final Thoughts Patch management is a critical aspect of keeping your business safe and your systems running efficiently. While it can be time-consuming and complex, the risks of ignoring it far outweigh the effort. Whether it's safeguarding your data from cyber threats, ensuring compliance with industry regulations, or simply improving the performance of your software, patch management is essential for any business that relies on technology. If you're struggling to keep up with patch management or just want to ensure your business is fully protected, we're here to help. Reach out to us today at hello@q2q-it.com and let's discuss how we can manage your IT Systems so you don't have to worry about them.

A proper Patch Management process is crucial as it helps prevent data breaches by fixing security vulnerabilities and bugs. It is also the way to make sure all your devices run the latest software versions, which implies having access to updated functions and characteristics. Just so we are all on the same page, Patch Management consists of acquiring, testing, distributing, and installing updates or software patches. It is an essential part of an organization's IT Asset Management (ITAM), and it requires following Patch Management best practices and selecting a top patching software to ensure the task is done effectively and efficiently. In this article, we'll dive into its definition and the instructions needed to implement the whole process. We'll also introduce you to InvGate Asset Management, our solution to complete the entire Patch Management process. Ready? Let's go! What exactly is Patch Management? Patch Management is the process of identifying, acquiring, testing, and installing systems or software updates—or patches—to fix vulnerabilities, improve performance, and ensure compliance. It's a crucial component of maintaining the health and security of an organization's IT infrastructure. In essence, Patch Management is about keeping systems up-to-date. By regularly applying patches, organizations can protect against known vulnerabilities that could be exploited by attackers. This proactive approach helps in reducing the attack surface, ensuring that all systems are fortified against potential threats. Patch Management in IT Asset Management Patch Management is deeply intertwined with IT Asset Management. ITAM involves tracking and managing the lifecycle of IT assets within an organization, from acquisition to disposal. Effective Patch Management ensures that all IT assets, including hardware and software, are up-to-date, secure, and functioning as intended. By integrating Patch Management with ITAM, organizations can gain better visibility into their assets, ensuring that all are accounted for and maintained properly. This approach not only improves security but also optimizes the performance and compliance of IT assets, leading to a more resilient IT environment. Patch Management for security vulnerabilities Patch Management plays a critical role in safeguarding an organization's IT infrastructure against security vulnerabilities. Security patches are specifically designed to address flaws or weaknesses in software that could be exploited by malicious actors. By promptly applying these patches, organizations can protect their systems from a wide range of threats, including malware, ransomware, and unauthorized access. Neglecting to apply security patches can leave systems exposed, creating an entry point for cyberattacks. In today's threat landscape, where attackers constantly search for unpatched vulnerabilities to exploit, a robust Patch Management process is essential. Regularly updating and securing systems not only mitigates risks but also ensures that the organization complies with industry regulations and best practices, thereby reinforcing overall cybersecurity. Step-by-step instructions for implementing a Patch Management process Organizations generally try to maintain software consistency across the different devices connected to the network, and resort to centralized Patch Management rather than letting each computer download its updates. Centralized Patch Management usually implies an ITAM software solution that checks missing patches, downloads, and distributes them to the related equipment according to the Patch Management workflow defined by the company. Here are the necessary steps to illustrate this process, as well as some tips to accomplish them with InvGate Asset Management. 1. Establish device groups by OS and critical status Applications and devices should be categorized according to their risk factor. How critical is that system or device to the organization? What data and processes will be affected? These questions will help determine priorities. Preserving security is crucial. Servers or computers with confidential data should be considered a high priority, and thus should receive patches first. In contrast, less relevant, offline, and rarely used devices should be deemed a low priority. It is crucial to have a multi-staged approach to streamline the patching process. In this sense, the chief information security officer might also want to establish device groups based on their operating system, as this will facilitate the patching process. 2. Inventory all the software in use Organizations should build a complete IT inventory, including all the operating systems and applications, as the first step to assessing what patches have been installed and which ones might be missing. Knowing the current state of patching will help outline the strategy to be carried out. In addition to inventorying assets, patch scanning should be performed to identify outdated or vulnerable software versions that require immediate updates. Patch scanning tools can automatically detect missing patches and highlight critical vulnerabilities, ensuring no risks are overlooked. The inventory can be done manually or automatically through Asset Management software. In this sense, InvGate Asset Management provides you with a quick and easy unified view of your entire asset inventory, including their details and status. Plus, by installing InvGate's Agent on your computers, it will also report all their data to your instance (including all the installed software), notify you when something is wrong, and help streamline patch scanning to uncover potential security gaps. 3. Delineate your Patch Management policy Once priorities have been established based on the critical status of all the devices analyzed, it is time to outline a Patch Management policy that will determine how and when security patches should be deployed. The policy will specify the procedures to be carried out based on the criticality of devices, the mitigation capabilities, and the risk imposed by the type of security vulnerability identified in each case. This is part of the Vulnerability Management organizations should carry out. 4. Find outdated software with InvGate Asset Management Up until now, you have put together an inventory outlined the rules to patching. Now, it's time to take action. A crucial part of the Patch Management process is to effectively monitor your network to spot outdated devices that might pose a risk to the organization. InvGate Asset Management offers two options to do it: Use its searching capabilities to find software that matches a specific manufacturer and version. The ones that match stand as the targets to be patched. Go to the software's profile and check the "Installations by market version" dashboard to spot installations from previous versions. Once you have identified the devices, prioritize the work based on usage or risk. If it's a simple patch method, you can apply the patches to all machines at once. However, keep in mind that outdated software might be in place for a reason – be it because of old operating systems, lack of technical capabilities, or other. Part of the asset manager's job is to determine whether updates are the right move for each scenario. 5. Deploy patches Finally, it's time to perform the patch deployment. Here, InvGate Asset Management also provides you with two alternatives: The first one is manual. Once you identify the device in need of patching, open its profile on InvGate Asset Management and use the remote desktop integration to fix it. The second one is using a software deployment tool to automate and streamline the process across various systems. What are the goals of a Patch Management process? Patch Management aims to keep all the operating systems in your network updated and, therefore, as secure as possible against malware and other vulnerabilities that may result in data losses and significant risks. An effective patching process requires attaining the following goals. 1. Reduce interruptions and rollbacks Careful planning is essential to minimize interruptions and prevent rollbacks during the patch deployment process. A well-executed Patch Management strategy involves scheduling updates during times when devices are not in active use, ensuring that the workflow is not disrupted. This approach not only reduces the likelihood of interruptions but also minimizes the chances of encountering issues that could lead to rollbacks, which can be time-consuming and disruptive to business operations. Moreover, by strategically planning patch deployments, IT teams can test patches in controlled environments before rolling them out to the entire organization. This step helps in identifying potential compatibility issues or conflicts, allowing the team to address them proactively. A robust Patch Management process should also include contingency plans for dealing with unexpected issues, ensuring that rollbacks are a last resort rather than a frequent occurrence. 2. Create predictability and routine around patching Establishing predictability in the Patch Management process is crucial for maintaining a secure and efficient IT environment. By developing a consistent routine, IT teams can ensure that all devices and software are regularly updated with the necessary patches. This routine involves categorizing devices and software based on their criticality and scheduling periodic updates to maintain information security and system integrity. A predictable patching routine also helps in building user trust and reducing resistance to updates. When users are aware of when and how updates will occur, they are less likely to experience disruptions and more likely to support the Patch Management process. Additionally, a well-defined schedule allows IT teams to allocate resources effectively, ensuring that patches are applied promptly and without unnecessary delays. 3. Empower IT with emergency powers (rollback and distribution) when needed While automation is a vital component of an effective Patch Management process, it's equally important to empower the IT team with the ability to intervene manually when necessary. In cases where automated patching fails or unforeseen issues arise, IT professionals should have the authority and tools to perform emergency rollbacks or manually distribute patches. This capability ensures that the organization can quickly respond to critical issues, minimizing downtime and maintaining system security. Implementing a well-designed workflow for these emergency procedures is crucial. Such a workflow should outline the steps to be taken, the roles and responsibilities of team members, and the documentation required for future analysis. By having a clear plan in place, the IT team can respond swiftly and efficiently to emergencies, ensuring that the entire Patch Management process remains smooth and effective even under challenging circumstances. 4. Ensure complete visibility into patch status Maintaining full visibility into the status of patches across all devices and software is a fundamental aspect of effective Patch Management. It's essential to know precisely how and when each system has been updated and to track which patch versions have been applied. This level of visibility allows IT teams to ensure that all systems are secure and up-to-date, reducing the risk of vulnerabilities being exploited. An IT Asset Management (ITAM) tool with IT compliance monitoring capabilities can provide detailed historical reports of applied patches and the current software versions on each device. This data is invaluable for designing comprehensive IT asset reports, tracking potential issues, and proving compliance with internal policies and external regulations. Furthermore, complete visibility enables the IT department to proactively address any emerging problems, ensuring that all assets remain secure and functional. Patch Management tools Selecting the right Patch Management software is a critical part of an effective Patch Management strategy. These solutions should provide comprehensive features that help streamline Patch Management process making it more neat and efficient. Our pick -obviously- is InvGate Asset Management. Let's see why. Although it's not a dedicated Patch Management solution, with InvGate Asset Management, you get access to complete visibility of your IT assets within IT inventory, and you can monitor your network, identifying software that needs patching. This enables IT teams to track, manage, and patch devices across the organization efficiently. Plus, its advanced reporting capabilities and customizable dashboards, ensures that IT teams can asses and continually improve their Patch Management process. The tool also integrates seamlessly with other systems (you can check out the full list here!), making it a versatile solution for comprehensive IT Asset Management. Key takeaways An effective Patch Management process should keep your company network safe against multiple vulnerabilities that have the potential to impact its performance. The easiest way to do it is to add the workflow to your IT Asset Management practice. ITAM is well-known for its ability to contribute to reducing risks, and this is no exception. With such a solution, you'll be able to map your entire IT infrastructure, spot outdated software, and update it. If you want to try out InvGate Asset Management's capabilities related to patching, ask for a 30-day free trial! Frequently Asked Questions What is a Patch Management process? A Patch Management process is a procedure that involves acquiring, testing, deploying, and monitoring updates (patches) to software systems to address security vulnerabilities, improve functionality, and maintain system health. How to audit the Patch Management process? To audit Patch Management, review documentation for update policies, assess patch testing procedures, examine deployment records, validate monitoring practices, and ensure alignment with security standards. What are some common problems with Patch Management? One of the most common difficulties is the lack of visibility into the patches deployed and on what devices. Another problem is that the patch may fail, which opens the system to vulnerabilities and attacks. Manual patching is another common obstacle because it is time-consuming and can lead to errors. Finally, there's the problem of lack of mobile control. It is crucial that organizations implement updates on mobile devices to keep the corporate data secure. What are the three types of Patch Management? The 3 most common types of patches are: Security patches - Involves patching newly discovered security holes in the system. Bug fixes - Involves patching newly discovered security holes in the system. Performance patches - Enhance overall performance by lowering resource requirements, making apps run faster, or getting new functionalities. What are Patch Management procedures? Patch Management procedures involve identifying, acquiring, testing, and installing patches or making code changes to solve security vulnerabilities, fix bugs, or add features to a network's software or operating systems. What is a security risk? A security risk refers to the potential for loss, damage, or disruption to an organization's data, systems, or operations due to vulnerabilities that can be exploited by threats, such as cyberattacks, unauthorized access, or system failures. Managing these risks involves identifying vulnerabilities, implementing safeguards, and regularly updating systems to protect against potential threats.

Cultivating a strong security posture begins with the following patch management best practices. Promptly addressing known vulnerabilities helps organizations reduce the risk of unauthorized access, malicious code execution, and operational disruptions. Let's explore essential network patch management best practices, including establishing a patch management policy, automating deployment, prioritizing urgent vulnerabilities, testing patches thoroughly, maintaining an updated inventory, creating a rollback plan, enforcing least privilege access, monitoring and auditing compliance, and training employees. A patch management policy gives a clear framework for how your organization will manage patches. It promotes consistency and accountability, and standardizes patch assessment and application procedures. It also aids in risk management, regulation compliance, and resource allocation. Furthermore, it facilitates communication and awareness regarding the entire patch management process. Expert tips: Regularly review and update your patch management policy to check if it remains relevant and effective as your organization and technological needs evolve. Engage stakeholders in policy development. Clearly outline the roles and responsibilities of individuals involved in the patch management process. 2. Automate patch deployment Using automated patch management tools for patch deployment supports the consistent and timely application of updates. Automation decreases the likelihood of human error and makes sure that security teams don't miss any high-priority patches, thus improving the overall network security. Patch management software solutions like Acronis offer this feature. Expert tips: Choose a software that fits your organization's needs and scale. There are many reliable patch management solutions that can handle various types and system volumes you need to patch. Integrate patch deployment automation with SIEM systems to improve visibility. Develop and implement a test automation framework for patch deployment. 3. Prioritize critical vulnerabilities By prioritizing the remediation of high-severity vulnerabilities, you ensure proper resource allocation to the most serious network security threats first. This minimizes the window of opportunity for potential attackers to exploit these vulnerabilities. Expert tips: Use a vulnerability scoring system like the common vulnerability scoring system (CVSS) to help prioritize patching based on the severity of vulnerabilities. Form a cross-functional team involving members from IT, security, operations, and business units to collectively assess and prioritize critical vulnerabilities for a thorough understanding of both technical and business considerations. Adopt a risk-based approach to prioritize critical vulnerabilities based on their potential impact on the organization. 4. Test patches thoroughly Rigorously testing patches in a controlled environment is vital before deploying them to production systems. This enables identifying potential conflicts, compatibility issues, or unintended consequences that could disrupt operations. Tools like ManageEngine Patch Manager Plus can help in this regard. Expert tips: Conduct thorough testing in an environment that mirrors your production setup. This provides a realistic simulation of production conditions and helps meet compliance requirements in certain industries. Create detailed test cases and consider variations in operating systems, software configurations, and network environments within your organization. 5. Maintain an updated inventory Keep a comprehensive inventory of all devices and software in your network, such as servers, workstations, and network appliances. Regularly update this inventory to reflect changes in your infrastructure to enhance the accuracy of targeting patches to the appropriate systems. SolarWinds Patch Manager can assist with maintaining an updated inventory. Expert tips: Use automated asset discovery tools to ensure that you don't overlook any devices during patching. These tools can greatly ease the manual effort required for inventory management, enabling IT teams to concentrate on tasks of higher strategic importance. Extend the inventory beyond a simple list of assets by capturing relationships and dependencies between different components. Integrate the inventory system with configuration management tools to maintain consistency and accuracy in asset information. 6. Create a rollback plan A rollback plan is a set of procedures that will support reverting systems to their previous state in case a patch causes unexpected problems or conflicts. It cuts down downtime in the event of patch deployment issues, allowing for a quick recovery. Expert tips: Routinely simulate rollback scenarios to verify the effectiveness of the plan. Conduct mock rollbacks in a controlled environment to uncover potential challenges or gaps in the process so the IT team can optimize the rollback plan for real-world situations. Document detailed rollback procedures to guarantee smooth execution. Define clear communication protocols to follow in the event of a rollback. 7. Enforce least privilege access Limit user and system privileges to the minimum required for normal operation to control the potential impact of security vulnerabilities. Restricting access minimizes the attack surface. By granting only necessary permissions, your organizations can diminish the risk of unauthorized modifications to key systems during the patching process. Expert tips: Implement a regular review process for user and system privileges to ensure they remain at the appropriate level even after job roles and responsibilities change. Employ role-based access control (RBAC) to assign permissions based on job roles, streamline access management, and reduce complexity. Track and audit user activity to detect any unusual or unauthorized access patterns. 8. Monitor and audit patch compliance Continuously monitor your network to maintain patch compliance and frequently audit systems to confirm the application of patches aligns with established policies. This allows you to identify and rectify any deviations, thus maintaining a consistently secure and up-to-date network environment. Expert tips: Use a centralized patch management dashboard to monitor patch compliance and get real-time visibility into your patching status. Segment your network into logical zones and monitor patch compliance within each segment. Set up thresholds for acceptable patch compliance levels and configure alerts for deviations from these thresholds. 9. Train employees on the importance of regular updates Educating employees is crucial to emphasize the significance of regularly updating systems and software. Informed employees are less likely to make errors, contributing to heightened security awareness across your organization. This creates a culture of vigilance and responsibility in relation to software updates. Expert tips: Provide training with real-world examples and scenarios to enhance employee understanding. Using real-world examples and scenarios contextualizes theoretical knowledge, making it more tangible and applicable for employees. Offer periodic refresher courses and updates to reinforce the training content. The goal of network patch management is not just to fix problems but to proactively maintain the health and security of your network and systems. By following the best practices outlined in this article, your organizations can reduce vulnerability to cyberthreats. Regular vulnerability assessments, prioritizing patches based on criticality, thorough testing in controlled environments, and automated deployment processes form the foundation of a robust strategy. In addition, maintaining an updated inventory, a well-defined rollback plan, and enforcing least privilege access contribute to a secure infrastructure. Employee training boosts overall awareness and decreases the risk of human error, while continuous monitoring and audits ensure ongoing compliance. It's worth noting, though, that in order to achieve comprehensive network security, it's imperative to integrate best practices for both networking devices and software applications. This involves adhering to software patch management best practices as well to bolster the security of the entire IT infrastructure. These patch management best practices, coupled with expert tips, can strengthen your organization's defense, creating a resilient and well-protected network.

Establishing a patch management policy is an important part of an effective patch management process. Learn how to create your own policy in our complete guide, complete with free template and examples. Welcome to the ultimate guide on Patch Management Policy. If you're wondering what this is all about, you're in the right place. In today's digital world, keeping software up-to-date is crucial. A Patch Management Policy helps organizations manage updates and fixes for software applications. This guide will walk you through everything you need to know about creating and implementing an effective policy. So, let's dive in and explore the ins and outs of patch management!What is a Patch Management Policy?A Patch Management Policy is a set of guidelines that dictate how an organization manages software updates. These updates, often called patches, fix vulnerabilities, improve functionality, and ensure software runs smoothly. Without a proper policy, organizations risk leaving their systems exposed to security threats and operational inefficiencies.Think of it as a roadmap for keeping your software healthy. It outlines the processes for identifying, acquiring, testing, and installing patches. This ensures that all software components are up-to-date and secure. A well-crafted policy not only protects your systems but also helps maintain compliance with industry standards and regulations.The Role of Automation in Patch ManagementAutomation plays a significant role in patch management. By automating the process, organizations can streamline patch deployment, reduce human error, and save time. Automated tools can scan systems for missing patches, download updates, and apply them without manual intervention. This ensures that patches are applied consistently and promptly, minimizing the risk of vulnerabilities.Challenges in Patch ManagementDespite its importance, patch management can be challenging. One common issue is the sheer volume of patches released by software vendors. Keeping track of these updates and determining their relevance can be overwhelming. Additionally, testing patches before deployment is crucial to avoid compatibility issues, but it can be time-consuming.Another challenge is balancing the need for security with operational requirements. Applying patches can sometimes disrupt business operations, so organizations must carefully plan and schedule updates to minimize downtime.Why is Patch Management Policy Important?Patch Management Policy is vital for several reasons. First and foremost, it helps protect your organization from cyber threats. Cybercriminals often exploit vulnerabilities in outdated software to gain unauthorized access to systems. By regularly applying patches, you can close these security gaps and safeguard your data.Moreover, a robust patch management policy ensures compliance with industry regulations. Many regulatory frameworks, such as GDPR and HIPAA, require organizations to maintain secure systems. Failing to comply can result in hefty fines and damage to your reputation.Enhancing System PerformanceBeyond security, patch management also enhances system performance. Patches often include bug fixes and performance improvements that can make your software run more efficiently. This can lead to increased productivity and a better user experience.Cost SavingsImplementing a patch management policy can also lead to cost savings. By preventing security breaches and system failures, organizations can avoid the financial losses associated with data breaches and downtime. Additionally, automated patch management tools can reduce the need for manual intervention, saving time and resources.Patch Management Policy Key ConsiderationsWhen developing a Patch Management Policy, consider the following key points: Identify critical systems and prioritize patches based on risk. Establish a regular patching schedule to ensure timely updates. Test patches in a controlled environment before deployment. Document all patching activities for compliance and auditing purposes. Communicate with stakeholders about patching plans and potential impacts.6 Steps To Create Your Patch Management PolicyStep #1 - Create Your Version Control and Document Mark UpStart by setting up a version control system for your policy document. This ensures that all changes are tracked and documented. Use clear markup to highlight updates and revisions. This step is crucial for maintaining an organized and up-to-date policy.Step #2 - Write The Document PurposeClearly define the purpose of your Patch Management Policy. Explain why it's necessary and what it aims to achieve. This section should provide a high-level overview of the policy's objectives and its importance to the organization.Step #3 - Write The Scope Of The PolicyOutline the scope of your policy by specifying which systems and applications it covers. Be sure to include any exceptions or special considerations. This helps ensure that everyone understands the policy's reach and applicability.Step #4 - Write the Content For The Required SectionsDevelop detailed content for each section of your policy. This includes procedures for patch identification, testing, deployment, and documentation. Be thorough and clear to avoid confusion and ensure consistent implementation.Step #5 - Seek Management ApprovalOnce your policy is complete, seek approval from management. This step is essential to ensure that the policy aligns with organizational goals and receives the necessary support for implementation. Management buy-in is crucial for the policy's success.Patch Management Policy Frequently Asked QuestionsWhat is the main goal of a Patch Management Policy?The main goal is to ensure that all software applications are up-to-date and secure, protecting the organization from vulnerabilities and improving system performance.How often should patches be applied?Patches should be applied regularly, based on the organization's patching schedule. Critical patches should be prioritized and applied as soon as possible to mitigate security risks.What are the risks of not having a Patch Management Policy?Without a policy, organizations risk exposing their systems to security threats, non-compliance with regulations, and potential operational disruptions due to outdated software.Can patch management be automated?Yes, automation is a key component of effective patch management. Automated tools can streamline the process, reduce human error, and ensure timely patch deployment.What should be included in a Patch Management Policy?A comprehensive policy should include procedures for patch identification, testing, deployment, documentation, and communication with stakeholders.ConclusionCreating a Patch Management Policy is essential for safeguarding your organization's software and data. By following the steps outlined in this guide, you can develop a robust policy that enhances security and compliance. Stay informed and proactive by subscribing to the GRCMana newsletter for more insights and updates on patch management and other critical topics. Delve into the intricacies of maintaining network security and system functionality with our comprehensive guide on Patch Management Policy.Government agencies as well as experts in the wider cybersecurity space have consistently pointed out that unpatched vulnerabilities continue to be a primary attack vector, especially for ransomware attacks. There is also a worrying trend where known vulnerabilities are left unpatched for long, giving criminals ample time to plan and attack. According to the United State's Cybersecurity and Infrastructure Security Agency (CISA), some of the top vulnerabilities exploited in 2021 alone include: In October 2022, Microsoft warned about CVE-2022-41033, a vulnerability affecting Windows COM+ event system service. Apparently this vulnerability was already being exploited by the time Microsoft was notified.There is no shortage of examples of companies of all sizes that have suffered the wrath of unpatched vulnerabilities. In July 2021, Kaseya, the MSP software giant, suffered a ransomware attack that took advantage of zero-day vulnerabilities in the Kaseya VSA on-premises product and paralyzed about 1500 organizations that are cumulatively managed by about 50 MSPs. This came as a warning call for the MSP industry. Many organizations rely on Managed Service Providers these days. It means that the criminals now know they can target the parent vendor in the supply chain and easily get their way to thousands of organizations. But to its credit, Kaseya went ahead and shared details of the attack including the actions they took to minimize harm.These happenings have amplified the importance of patch management, a practice that is so important yet so casually handled. Many organizations approach patch management without a patch management policy, and this is where it's going wrong. To correct this problem, it helps to understand what a patch management policy is and why your organization needs to implement it as soon as possible. Also read: Trends shaping the MSP industry What is patch management policy? A patch management policy is a comprehensive document with a clear set of rules and procedures to actively manage the sourcing, distribution and installation of patches across the entire IT Infrastructure. This policy is critical in ensuring that all patches are installed in a timely manner. The goal is to protect systems from vulnerabilities by installing the latest patches as soon as they become available.Patch management policies can be implemented in a variety of ways, but typically involve some combination of automated patch management tools and manual procedures. Automated tools can be used to scan organization-wide systems for missing patches and to deploy the necessary updates automatically. However, manual procedures are still often necessary to address exceptions or specific system configurations that are impossible to automate.A good patch management policy should serve as a guideline for how often systems need to be patched, how personnel should monitor systems for updates, and so on. For example, depending on your organization's threat profile and budget, you may need to have patching performed weekly or even multiple times per day. For larger organizations, it can also be beneficial to have an automated system in place that downloads updates and applies them across the entire network with minimal effort from personnel. Furthermore, patching should take into account any solutions, operating systems, applications, or plugins that are used within the organization. A strong patch management policy will also include provisions for testing new patches before they are installed. Benefits of a patch management policy The fundamental benefit of a patch management policy is to minimize cyber threat risks and downtime costs. It's an essential part of IT security. Here is a comprehensive breakdown of the top 9 key benefits of a patch management policy:1. Reduced vulnerability This is essentially the main purpose of a patch management policy. A patch management routine that is guided by a robust policy ensures that system loopholes are quickly addressed and patched so that malicious actors cannot take advantage. It eliminates the need for users to individually take care of updates, reducing the system's vulnerability to attack.This ultimately improves performance on a consistent basis and enhances system stability, resulting in fewer technical problems overall and more reliable access to applications and services.2. Prompt risk management Policy-driven, regularly deployed security patches can help protect against new exploits before they have a chance to cause any damage, providing an extra layer of proactive protection against cyber threats. In other words, companies are able to prevent attacks from happening in the first place rather than dealing with their aftermath afterwards — immensely valuable from both a security posture standpoint.The patch management policy ensures regular monitoring of software and hardware for any new network vulnerabilities or weaknesses. If it is determined that certain elements pose a risk or offer limited protection, the organization must then implement necessary fixes or upgrades as soon as possible. By establishing how frequently patches must be implemented and how notifications should be sent, a patch management policy ensures that no relevant change goes unnoticed and complications can be avoided quickly.3. Minimal conflicts Patch management should always be an ongoing task, keeping software and hardware up-to-date with the latest patches. Yet managing these updates can add complexity to the work process and create scheduling conflicts between departments or the key IT staff. Additionally, many organizations struggle with determining who among their staff have access to the patches and when they should be installed – leading to inconsistencies in patching.. To minimize these conflicts and make sure time is not wasted during crisis mode, a patch management policy ensures that the right people are assigned to handle specific patching tasks consistently at scheduled intervals; for example, Operating System updates being overseen by alternating IT staff every month on the first Monday of the month. This helps to anticipate conflicts over how quickly patches need to be deployed in order to resolve a security emergency, instead of having two departments or employees clash over who should handle it first. 4. Compliance Across many industries, patching is one of the compliance requirements that an organization needs to meet. A patch management policy comes in handy to guide the organization to properly patch their systems according to laid down compliance requirements by different industry regulators and government agencies. And since the policy provides clear guidelines for documenting the process, organizations will always have all the necessary documentation to meet their compliance obligations without delays.5. Customer satisfaction A patch management policy contributes to customer satisfaction by ensuring that all devices in a customer's environment are kept up-to-date with the latest patches and security updates. This helps to prevent vulnerabilities from being exploited, and minimizes the risk of data loss or theft.This way, businesses can ensure that their customers enjoy a smooth, trouble-free experience with minimal disruptions.6. Improved reputation A strong patching policy sends a strong message that the organization is very serious about prioritizing safety. This is important because with cyber attacks occurring on an almost daily basis, many customers are now taking extra caution. They are keeping a watchful eye on the organizations they entrust with their finances and data. Since the patch management policy gives a clear blueprint on practices such as timely application of patches, it contributes to building trust between a business and its customers by demonstrating that the company genuinely cares about protecting the users of its systems. The overall public perception raises the reputation of the organization, enabling it to attract more customers while naturally locking in the existing ones. 7. Better accountability A complete patch management policy clarifies who should be responsible for performing which patching tasks and on what schedule, with clear consequences for those who don't follow through. This orderly process helps to provide structure and accountability around patch maintenance. As a result, the importance of proper patching remains on top-of-mind for everyone in the organization.Without a patch management policy in place, it's often up to individual employees to take initiative. While this kind of vigilance is commendable, there's no guarantee that less tech-savvy staff members are aware of the latest vulnerabilities—or even that they have the resources they need to identify and patch them. Over time, this lack of focus on proper patching can build up into a larger security gap that increases risk across the entire organization.A comprehensive policy takes away these worries by establishing clear guidelines on how often patches should occur and assigns responsibility accordingly. This ensures that all systems are updated in a timely manner and reduces the chances of missed vulnerabilities due to negligence or oversight.Also read: The importance of cybersecurity awareness training for employees8. Commitment to SLAs The wrong patch work can mess up your Service-Level Agreements (SLAs). Fortunately, a proper patch management policy can avoid this by ensuring all vulnerabilities are patched the right way before any disaster happens, avoiding any trouble with contract terms. 9. Competitive advantage Investing in a quality patching policy could help differentiate a business from its competitors who have yet to implement one. This is an easy way to keep clear of the competition especially now when competition is fierce and customers have numerous options. Features of a patch management policy: what should it contain? The contents of a patch management policy can vary from organization to organization, largely dictated by factors such as the scope of the IT infrastructure, number of users, customer base, the industry, compliance requirements and so on. But some features are basic and will cut across most policies regardless of the organization size or type. Here are the 10 most basic components that should be included in a patch management policy:1. Patch scheduling The patch management policy should contain a precise schedule for all patching tasks. This should specify how often patches should be checked for and applied. It should also be specific about where manual or automated methods will be used for patch deployment. For example, if operating systems only support manual patch deployment, then personnel might need to be allocated time for performing the necessary tasks. By contrast, automated methods might save time by automatically regulating patch delivery schedules and pushing updates to the network.The schedule component should also specify how often each system or application should be monitored.2. Processes for identifying, evaluating and deploying patches This outlines the procedure which new patches must undergo in order to be accepted into the organization's IT infrastructure, taking into account any associated risks with different patching tasks.3. Testing procedures and environment Pre-testing should always be done on non-production systems so that patches can safely be deployed across all environments. 4. Documented rules and communication protocols Clearly defined rules, roles and responsibilities can help to prevent any issues arising due to lack of communication or inconsistent understanding of processes. 5. Data protection In addition to patching applications and operating systems, policies must also cover processes such as backing up files before applying updates or establishing secure protocols for downloading them. This component drastically strengthens the overall security posture by making sure that only approved devices have access to sensitive data. 6. Asset monitoring This specifies guidelines around the monitoring of all hardware, software, and other devices connected to a network. Having insight into what's connected to your networks can help administrators quickly identify systems that are outdated or require patches and other updates. Automated asset tracking can also save time by automatically alerting administrators whenever a new device is installed or connected to the network. 7. Patch sourcing This initially involves sourcing for new patches released by vendors or security researchers. This ensures that any vulnerabilities discovered in patches are identified early, so they can be applied as soon as possible before they can be exploited by malicious actors. Gathering and cataloging relevant patch details provides necessary visibility into the updated status of all assets in a system. Additionally, keeping a single up-to-date repository of all available patches at the disposal of administrators speeds up decision-making when it comes to assessing newly released patches and responding to them promptly. Without consistent patch information gathering, network operators risk leaving vulnerabilities unpatched for long periods of time — a significant risk point. 8. Roles Depending on the size of the organization, one or more individuals should be named as responsible for implementing patching processes. Not only should they make decisions about which patches should be applied and when they would go out, but they should also make sure that all key staff members in different departments know their roles in managing potentially vulnerable systems. For example, designated personnel may need to monitor server and service events or review system logs to determine if additional remediation steps are needed. Including comprehensive roles and responsibilities within a patch management policy ensures that all those involved have a clear understanding of what it means to keep an eye on patching schedules. Everyone involved in the patching process should internalize their duties, including who is responsible for testing patches, scheduling updates and monitoring system performance. 9. Risk categorization and prioritization It's always important to understand the nature of existing risks in order to accurately determine which areas of the system most require attention, and allocate resources accordingly. The policy should outline rules on which patches should be applied first based on severity rating. This categorization will help prioritize critical updates over minor improvements/fixes. Furthermore, assessing risk levels across potential vulnerabilities can help determine which threats are most urgent and need to be addressed first.10. Maintenance window request and approval The success of a patch management policy depends heavily on having a clear and organized process for requesting, scheduling, and approving maintenance windows. This is especially important for organizations that have strict service-level agreements (SLAs) in place as it eliminates the risk of unplanned downtime. Your patch management policy should therefore include a step-by-step guide for initiating requests for maintenance windows and getting approvals. This should include user roles such as system owner, system operator, network admin, and security admin, who may be involved in different stages of the process. Once the request is made via the ticketing system or email by the user responsible, it should be reviewed by all relevant parties and then approved by someone with administrative permissions. Once approved, each party should confirm their acceptance and schedule any necessary developer or IT team time to complete the patch work. Once approvals are granted, make sure users are aware ahead of time. Update them accordingly, letting them know when there will be planned downtime due to patching. This will help them plan accordingly and minimize disruption of services from their end. Creating a patch management policy: quick steps Take the following steps to formulate and create a strong but easy to use patch management policy:Start by outlining procedures for determining how systems including software and hardware will be identified, categorized and prioritized.Assign patching roles for each of the different categories of systems as outlined in step 1. Clearly define the tools and resources that will be used to identify vulnerabilities and how these tools will be used, by who.Document procedures for patch requests, approvals, plus elaborate rollback guidelines.Formulate a patch lifecycle timeline for each category of patches, outlining the timelines for each patching task across different systems.Outline a monitoring process that thoroughly checks and reports the overall effects of each patch, including the negative effects and the root causes.Develop a post-patch analysis template that generates feedback from users, alongside a clear procedure for incorporating the feedback in future patches. Constantly review the policy document, update it to reflect the current landscape. IF need be, strike out or replace whatever is outdated. Best practices for a sound patch management policy Here are the top 7 best practices that should be part of an effective patch management policy.1. Prioritize patches, always! It's essential to develop a process for prioritizing patches, making sure that the most critical ones are implemented first. Start by categorizing updates into three distinct tiersHigh priority patchesMedium risk patchesLow risk patches Take note that regardless of the tier, all patching must be completed. The fact that a vulnerability is low risk does not mean it'll remain that way forever. Even low risk vulnerabilities can quickly escalate to high risk. So never leave anything to chance. 2. Maintain journalistic records Keep comprehensive records regarding installed versions of programs and any updates applied or rejected. This will not only provide an audit trail but also allow easy tracking of patch deployments should the need arise.The policy should clearly outline and even provide simple templates for documenting all vulnerabilities, including common vulnerabilities. This data can be used to bring out a pattern of vulnerabilities, help to devise better protection and cut costs along the way.3. Automate where you can Automation can help reduce manual labor and free up IT personnel to focus on more crucial tasks. Always make an effort to deploy automated solutions that apply patches as soon as they are released by vendors. 4. Establish clear testing guidelines Whenever new patches are available, test them in a controlled environment before rolling them out across your organization's network. This ensures compatibility with existing applications and systems without creating costly errors or downtime.Left unchecked, some installed patches could potentially have a negative effect on system performance or user experience. 5. Cover the entire infrastructure It's important to have a comprehensive patch management policy that covers all aspects of the organization's IT infrastructure. Don't just limit your policy to operating systems and common internal systems such as CRM, ERP.Even items such as basic connectivity devices and security cameras should be patched or upgraded when due. Essentially, all the hardware and software that makes up your entire IT infrastructure both internally and externally must be accommodated in the patch management policy.6. Don't forget third party vendor patches Unfortunately, some vendors don't always provide sufficient communication of available updates, leaving organizations in the dark regarding necessary patches until they are too late. This is where the patch management policy should play the 'watchdog' role. It should outline procedures for checking with vendors and updating third party systems on a regular basis. 7. Seek professional help For particularly complex patches, it's advisable that the policy outlines how professional help will be sought to ensure successful implementation of sensitive patch management processes. You can seek help from professional firms that offer IT services such as network support. Why patch management policies fail? Even the best systems fail at some point. This is also true for patch management policies. A good number of organizations end up failing to achieve their policy objectives for several reasons.Lack of buy-in from executive leadership. Without executive level participation and support in setting expectations and distributing resources, the policy is unlikely to achieve successful results.Limited testing capabilities. Patches need to be thoroughly tested before they can be deployed in production environments. This is often a challenge due to limited resources, time constraints, and other internal factors.Insufficient automation capabilities. Automation is key for ensuring patches are applied quickly and accurately; however, many organizations lack the necessary tools to automate their patching processes.Inconsistent auditing. Many organizations fail to invest in consistent processes for auditing their patching processes as provided in the policy. Limited talent. Patch management requires significant technical implementation at all levels of the organization's network infrastructure. If there is not enough appropriately trained staff on hand to manage the process, then the policy can flop. A culture of failures. If an organization has had a long history of policies that were sometimes neglected or forgotten about, then employees may not take the patch management policy as seriously as they should. You can overcome these pitfalls by allocating adequate resources and assigning high level responsibilities to key IT staff to consistently ensure that all patching is active, and in accordance with the policy. In other words, even the policy itself needs to be monitored. No patching should be done outside the policy. This way, it's always easy to spot gaps in the policy framework and continuously improve it to a level where it becomes a norm and a crucial part of the organizational culture. Conclusion Failure to have a sound patch management policy can actually dilute your patching activities, even when you think you are doing it well. You can miss crucial patching timelines, forget some or even do a poor job. A patching policy brings everything together, always guiding the patching process so that nothing is missed. And even when things go wrong, the policy steps in as a crucial reference point that guides recovery teams to quickly get operations back on track — instead of fumbling in the dark. A well-defined policy outlines how frequently patches should be applied, as well as how administrators should go about identifying risks that would require a patch approval. By following the protocols outlined in the policy, organizations can ensure that they always remain up to date on all of their patches. Not only does this help you to maintain compliance with regulations, but it also helps you to stay ahead of potential risks that could lead to costly damages. Once again, the patch management policy should be constantly reviewed and updated accordingly to match new trends. In January 2024, the National Vulnerability Database received over 1,830 new CVEs. That added up to the other already registered 234,632. Security Officers in charge of closing vulnerabilities need to focus on what to fix first and patching before hackers exploit them. Let's see how you can set up a smart and fast patch management process. Key takeaways Patch management keeps hackers outside your system by closing known vulnerabilities. The 7 key steps of the patch management process are inventory, assess, prioritize, test, schedule, deploy, and monitor. Automated patch management software improves visibility and control, helps overcome talent shortages, and reduces the attack

surface by patching third-party software. Heimdal Patch & Asset Management unifies patching for Windows, MacOS, and Linux. To make patching an easier task for your security team, set a clear patch management policy. Then create an effective patch management process. Make it clear which member of the IT staff is responsible for which step of the process. Make sure you know what you need to protect before you get to work. The first step of a successful patch management process is a thorough inventory of all potentially exposed assets. The inventory list should include: Laptops, mobiles, printers Routers & servers. IoT devices. On-prem or Cloud databases. Operating systems. Third-party apps, etc. Asset inventory – See all software in the Heimdal Dashboard Internet-facing assets pose the highest risk of becoming a target for hackers. Now it's the moment to create device groups based on operating systems and critical status. All software has flaws. Yes, even MacOS has exploitable vulnerabilities, so you should patch MacOS devices too. Vendors like Microsoft, Apple, Adobe, Atlassian, etc. regularly release patches for known vulnerabilities. Keep an eye on new releases and track the old known vulnerabilities. Search for missing patches. Use vulnerability management tools to detect vulnerabilities in your system. Take your time to prioritize patches. Not all vulnerabilities are equally threatening and not all devices are equally exposed. There are so many known flaws that there's not enough time or workforce to patch everything. You'll have to choose. Here are three elements you should base your choice on: Company specifics and asset inventory. CVSS scores – can't use those alone. According to the National Vulnerability Database dashboard, more than 60% of known vulnerabilities are of high or critical severity. You're looking at more than 75,000 CVEs. EPSS scores – this is an instrument that predicts exploitability. It estimates how likely is it that hackers will use a certain vulnerability against their targets. The EPSS score is not a standalone tool either. Get the patches you need from the vendor. Test them in a controlled environment before going live. Document both the testing process and its results. Check how your devices, software versions, and overall system will react to the updates. Operating system or software updates can make them run slow, block, overlook safety measures, etc. You should always have a backup to revert to in case things go wrong. Testing can seem like a tedious task that slows down the patching process, but it pays off. Here are some of the patch testing benefits. Prevent disruption Testing allows you to catch any issues that could interfere with the company's workflow. Make the adjustments you need to ensure business operations continue to run smoothly. Ensure stability of the IT infrastructure See if the patch conflicts with existing systems or applications. Checking compatibility helps avoid slowdowns or outages in your critical systems. Check quality Patches are bits of software, and no software is flawless. So, before installing patches, test them to see if they resolve the vulnerability without creating new bugs or security holes. Keep workflow smooth by scheduling patch deployment at a convenient time for your organization. Based on the company's specific and day-to-day tasks, assess when the best time is to update software. If your company activates in the educational sector, for example, the best time for patching might be in the evening or during weekends. Take time to observe when the devices in your system are less used. Communicate with the company's employees so they understand why patching is important and should be a priority. If your organization is medium to large, my recommendation is to go for an automated patch management tool. Best patch management solutions come with the possibility to schedule patching at your own pace. Prepare the deployment package that will get the patch from the IT admin to the company's computers. This package is also known as a group policy object and includes: a script, which is a piece of code written by the IT admin. The script tells the device what to do with the patch. Professional, automated patch management tools can also help with this step. In a hybrid work environment, you need to be able to safely apply patches remotely. If you patch manually, you'll need to write scripts for the deployment package every time you patch. Additionally, you'll only be able to patch office-located devices. You'll have to postpone deploying patches on devices that belong to people who work remote or are on leave. This is good news for the hackers since you'll be slower to close a known vulnerability. The last step of the patch management process is to monitor, check the results, and document everything for the record: Were there any patch failures or rollbacks? What caused that? What was the impact of patch failures on the company's operations? Take the necessary steps to remediate the issue and apply patches. Documenting how the patch deployment step succeeded or failed is useful intelligence for future diagnosis. You can also use it in incident response, and compliance reports. Here are some aspects that will give you and your team a hard time if you patch manually. Deciding which patch to test and deploy first can be stressful. Lots of companies use different OSes for different departments. IT teams could work on Linux, Accounts on Windows, and Marketing on MacOS, for example. Moving to a hybrid or remote work environment brings a lack of visibility and control. BYOD work policies also complicate endpoint security. Third-party software includes apps like Adobe, Google Chrome, Zoom, TeamViewer, etc. Each third-party app you install on the company's endpoints expands the overall attack surface. Why? Because all software has vulnerabilities. People in the IT or Security teams are usually highly qualified. Having enough hands on the deck to cover the patching process properly depends on the company's budget and the available workforce. Proper patch management is not enough to keep the IT infrastructure safe. Integrating it with other tools, like Endpoint Detection and Response or DNS security, increases safety and incident response efficiency. That's why the trend in cybersecurity is to use unified platforms, that integrate and automate processes. Heimdal's MXDR suite, for example, comes with integrated vulnerability management, patching included. Patching is a tedious task, if done manually. Additionally, things can easily go wrong if the ones in charge with patching don't follow a clear policy. You might overlook patching legacy software. When in a rush, you might feel tempted to skip testing. Not testing a patch or update before deployment can bring new bugs, impact performance and even data loss. Also, check patch status after deployment. Undetected patch failure leaves the system open to vulnerabilities and security risks. Automating the patch management process solves most of the patching challenges. It makes things happen clear and fast. Heimdal's patch management software helps the IT team keep it all on the green: enjoy total visibility over assets; assess; prioritize; test patches in a safe environment; schedule according to the business's needs; deploy; monitor & report; in a few clicks and remotely. Try it here, for free. The tool solves patching for Windows, MacOS, and Linux. All you need to do is set some operating system specific groups at the beginning and you're good to go. There's no need to spend the budget on various tools to patch a diverse IT infrastructure. As businesses develop, the need for using a variety of apps increases. That grows exposure which can bring more opportunities for hackers, and more work for Security Officers. Patching all critical assets to close high-severity vulnerabilities is possible. Use an automated patch management solution that brings all OSs under the same umbrella. Choose a tool that integrates into a unified security platform so you can view and control all processes from the same dashboard. Automating redundant tasks and increasing visibility over all assets will take pressure off the security team and the budget. Patching software is essential to protect systems from security vulnerabilities and ensure smooth operations. However, managing patches across different software and hardware can be challenging without a clear framework. A patch management policy provides the guidelines necessary to maintain up-to-date systems, minimize downtime, and address potential security risks. This blog will walk you through the key components and steps involved in creating an effective patch management policy for your organization.A patch management policy is a formalized set of guidelines that define how an organization handles the process of identifying, testing, deploying, and monitoring software patches. This policy serves as a blueprint for maintaining the security and functionality of an organization's IT environment by ensuring that patches are applied systematically and regularly. It defines the roles, responsibilities, timelines, and procedures necessary to address vulnerabilities in software systems and applications.A well-defined patch management policy should consist of several key components that ensure comprehensive coverage and effective patch management. These include:Before you can manage patches, it's essential to have an up-to-date inventory of all software and hardware assets within your organization. This includes operating systems, applications, and any other software that may require patches. An accurate asset inventory ensures that no system is overlooked during the patching process.Testing patches before deploying them is critical to prevent unforeseen issues. A policy should outline the procedures for testing patches in a controlled environment before their full deployment. This minimizes the risk of patch-related conflicts or system instability.Not all patches are equally important. Some patches address critical security vulnerabilities, while others may be less urgent. Your policy should include guidelines for assessing the severity of each patch and prioritizing them based on risk. Critical security patches should be deployed immediately, whereas less critical patches can be scheduled for later deployment.A patch management policy should define a schedule for patch deployment, including regular patch cycles (e.g., monthly or quarterly). Timely patching is essential for reducing exposure to potential threats. Scheduling also ensures that patches are applied during off-peak hours to minimize disruption.Documentation is vital for accountability and future reference. Your patch management policy should outline the procedure for keeping detailed records of which patches have been deployed, their status, and any issues encountered during deployment. This ensures that all activities are tracked and can be reviewed as needed.Even with thorough testing, sometimes patches can cause issues or conflicts. A rollback plan should be in place to quickly undo any patch that causes unintended consequences. This ensures business continuity and minimizes downtime.Senior management should review and approve a patch management policy to ensure that it aligns with the organization's security goals and compliance requirements. This formal approval establishes the policy as a crucial part of the organization's cybersecurity strategy.Cyber threats are continually evolving, and so are patching needs. Regular reviews of the patch management policy ensure that it remains effective and relevant. It's important to update the policy as new vulnerabilities emerge and as technology changes.By following the below steps you can create a well-structured and defined patch management policy: Assess your current environmentStart by evaluating your existing IT infrastructure, identifying which systems and software need patch management, and determining your current patching practices.Define roles and responsibilitiesAssign individuals or teams responsible for patch management tasks, including patch identification, testing, deployment, and monitoring. Clear roles ensure accountability and smooth execution.Establish patch management proceduresDevelop detailed procedures for patch identification, testing, prioritization, deployment, and rollback. Ensure these procedures align with industry best practices and your organization's unique needs.Define how often patches will be applied and at what time. Consider scheduling patches during off-peak hours to minimize disruption to users.Implement documentation and trackingEstablish a system for documenting all patching activities. Keep detailed records of the patches applied, their status, and any issues encountered, ensuring compliance with internal and external audit requirements.Regular monitoring is critical to ensure that patches are applied correctly and systems are functioning as expected. Periodically review the policy to adapt to new vulnerabilities, software updates, and organizational needs.A well-structured patch management policy offers numerous benefits for organizations such as: Improved security: Timely patching reduces the risk of cyberattacks exploiting known vulnerabilities.Compliance: Many regulatory frameworks require organizations to maintain up-to-date security patches. A patch management policy helps ensure compliance with these regulations.Operational efficiency: Automated patch management reduces the time and effort required for manual updates, enhancing overall productivity.Minimized downtime: By scheduling patches and testing them beforehand, organizations can prevent unexpected disruptions to operations.Cost savings: Preventing security breaches and system failures through proper patch management can save organizations from costly recovery efforts.Creating a robust patch management policy requires careful consideration of several key factors. By following best practices from the outset, you can ensure a smoother patch management process. Here are some essential best practices to keep in mind when developing an effective patch management policy:Automate patch management: Use automated patching tools to simplify the process, ensure timely updates, and reduce human error.Regularly review and test patches: Continuously monitor security advisories and conduct testing to ensure patches are deployed correctly and do not introduce new issues.Prioritize critical patches: Always address security vulnerabilities with the highest severity first, especially those that are actively being exploited in the wild.Maintain clear communication: Keep stakeholders informed about patching schedules, any expected downtime, and the status of ongoing updates. Clear communication prevents misunderstandings and disruptions.Measure the success of the policy: Finally, assess the effectiveness of your patch management policy by using key metrics to evaluate its performance within your organization. Below are some metrics you can use- Key performance indicators (KPIs) for your patch management programPatch compliance ratePatching schedule Patch solution coverage across devicesPatch management solution coverageEfficiency measuresRead More: What is Windows Patch Management?A strong patch management strategy is key to keeping your organization secure. With Scalefusion UEM, you can easily manage device and server patching, ensuring they're always up to date and protected from vulnerabilities. Scalefusion UEM makes deploying patches, tracking compliance, and monitoring the entire process simple. By using Scalefusion, you reduce the risks of security breaches, improve efficiency, and maintain a secure IT environment with less hassle.Connect with our product experts to learn how Scalefusion UEM can simplify patch management for your organization. Book a demo and start your 14-day free trial today! Cyber threats continue to grow in complexity and frequency, putting immense pressure on IT teams to secure their infrastructure. One critical line of defense is effective patch management, ensuring that systems remain updated and protected against known vulnerabilities. This article helps you understand the intricacies of patch management, focusing on the challenges faced by the tech industry, and the compelling need for a well-structured patch management strategy. Patch management is the proactive process of identifying, deploying, and managing software updates, or patches, to rectify vulnerabilities, enhance performance, and boost security. It is a systematic approach to maintain the health and functionality of the endpoints by regularly applying software updates or patches. These patches are released by Microsoft (for Windows devices) and Apple (for Mac and other Apple devices) to address various issues, including security vulnerabilities, software bugs, and performance enhancements. Managing updates across this spectrum requires a nuanced understanding of the operating system's architecture and the specific challenges posed by various hardware configurations. Explore Hexnode's OS update and patch management Difference between OS Updates and patch updates Clarifying the distinction between operating system updates and patch updates is essential for understanding the scope and impact of different types of software updates. This distinction is essential in prioritizing and streamlining patch management efforts for better system reliability and security. Aspect OS update Patch update Scope Comprehensive – includes new features, enhancements, and architecture changes Specific – targets vulnerabilities, bug fixes, and security improvements Impact Significant impact on user experience Minimal impact, focused improvements Installation time Typically longer, often requires system reboot Generally quicker, may not require reboot Frequency Less frequent More frequent and incremental Purpose Enhances functionality and performance Ensures stability and security The need for Patch Management 1. Device & data security Patch management serves as a defense against security threats, safeguarding sensitive data and strengthening the security posture of managed devices. It ensures that known vulnerabilities are promptly addressed, reducing the attack surface and enhancing overall resilience. 2. Reduced device downtime Swift and automated deployment of patches minimizes device downtime, ensuring seamless operations and productivity. This is especially critical in business-critical environments where even short periods of disruption can have significant financial implications. 3. Compliance Meeting regulatory standards is imperative for organizations. Patch management aids in compliance by keeping systems up-to-date and secure, providing evidence of due diligence in maintaining a secure computing environment. 4. Reduce costs From device lifecycle management to repair expenses, a proactive patch management strategy can yield cost savings. Timely updates reduce the likelihood of security incidents that might result in costly data breaches or system failures. 5. Improved functions Patching not only addresses vulnerabilities but also enhances the overall functionality of the devices. Performance optimizations, feature updates, and bug fixes contribute to a smoother and more efficient user experience. 6. Tech support Efficient patch management simplifies the tech support landscape, reducing the burden on IT teams. With fewer issues stemming from unpatched vulnerabilities, tech support can focus on strategic initiatives and higher-value tasks. To understand the situation better, imagine a finance team rushing to close the fiscal year on 40 Windows systems. The IT admin identifies a critical patch and requests a 3–4-hour downtime. Due to tight deadlines, the team postpones it to next week. A few days later, all 40 systems are hit by ransomware. Sensitive financial data is at risk, and the organization faces chaos as the ransom surpasses the entire year's budget projections. This situation could've been avoided with an efficient patch management strategy—one that includes risk-based prioritization, communication between teams, and the ability to schedule updates during non-peak hours or automate patching with minimal disruption. Proactive planning and the right tools can make the difference between a minor delay and a major disaster. Why a Patch Management Strategy is Needed A well-defined patch management strategy is crucial for maintaining a secure and resilient IT infrastructure. It efficiently coordinates timely updates, addressing new features, performance improvements, and security vulnerabilities. It ensures regular, non-disruptive patching tailored to the systems, preventing clashes with employees' productive hours. Furthermore, a patch management strategy, in adherence to regulatory standards like HIPAA and GDPR, plays a crucial role in ensuring compliance. This compliance not only shields against audits but also fosters trust by consistently improving products and services with secure functionality. Simultaneously, the strategy mitigates risks through methodical testing and deployment of updates, reducing the likelihood of security incidents. Furthermore, it facilitates strategic planning by outlining patching frequency, prioritizing critical updates, and establishing efficient communication protocols, ensuring optimal resource allocation. Watch our on-demand webinar "Exploring Modern Patch Management with Hexnode" to learn: Why patching is now a critical part of cybersecurity strategy How Hexnode automates patch deployment across OS and third-party apps Best practices for building a scalable, secure patching workflow A live walkthrough of Hexnode's Patches & Updates tab Watch the webinar Types of Patches Patch management covers a range of updates, each designed to address different aspects of software performance and security. One of the most critical among them is security patches, which fix known vulnerabilities that could be exploited by attackers. These are often released urgently and prioritized to reduce the risk of breaches. Bug fixes are another essential type, targeting issues that affect functionality or performance without adding new features. In contrast, feature updates or OS upgrades introduce new capabilities, interface changes, and performance improvements, often on a scheduled release cycle. Some updates are more urgent in nature. Hotfixes are released outside regular patch cycles to resolve specific, high-impact issues quickly. While less common today, service packs used to bundle multiple fixes and updates into a single package for easier deployment. Other useful categories include cumulative updates, which consolidate all prior patches, and rollup updates, which target a specific set of issues. Driver and firmware updates improve hardware stability and performance, while third-party patches—from vendors like Zoom or Adobe—are vital for securing the broader software ecosystem. Zero-day patches stand out for their urgency, addressing vulnerabilities already under active exploitation. A clear understanding of different types of patches helps IT teams prioritize updates effectively and maintain a secure, stable IT environment. How to choose the right patch management software Selecting the right patch management solution is more than just ticking boxes – it's about aligning the tool with your organization's unique needs and IT infrastructure. Here are a few key factors to consider when evaluating patch management software: 1. Platform compatibility Ensure the software supports all operating systems and devices in your environment – Windows, macOS, Linux, mobile platforms, and even third-party applications. A cross-platform solution simplifies patch deployment across diverse endpoints. 2. Automation capabilities Look for tools that offer automated patch scanning, scheduling, deployment, and rollback. Automation reduces manual effort, minimizes human error, and ensures timely updates without disrupting productivity. 3. Customization and control The ability to customize patch policies – such as setting approval workflows, defining maintenance windows, and excluding specific updates – is crucial for maintaining operational flexibility. 4. Reporting and compliance Robust reporting features help track patch status, identify vulnerabilities, and demonstrate compliance with industry standards and regulations. Real-time dashboards and audit logs are a big plus. 5. Integration with existing tools Choose a solution that integrates seamlessly with your existing IT management stack – whether it's endpoint management, or SIEM systems. This ensures smoother workflows and better visibility. 6. Scalability and support As your organization grows, your patch management tool should scale with it. Check for vendor support, documentation, and community resources to ensure long-term reliability. Patch Management Lifecycle Effective patch management is more than just deploying updates—it's a structured, continuous process that ensures systems remain secure, stable, and compliant. The lifecycle typically follows a series of stages, each playing a critical role in minimizing risks and maximizing uptime. Steps in Patch Management 1. Patch Identification The process begins by monitoring for new patches released by vendors. This includes OS updates, application fixes, and security advisories. 2. Assessment and Prioritization Each identified patch is evaluated based on severity, relevance, and potential impact. Critical vulnerabilities and high-risk systems are prioritized for faster deployment. 3. Testing in Staging Environment Before rolling out patches across the organization, they're tested in a controlled environment to avoid compatibility issues or disruptions in business-critical applications. 4. Deployment Once tested, patches are deployed to target systems using automation tools or manual processes—depending on urgency and environment complexity. 5. Verification Post-deployment, IT teams verify successful installation and system stability to ensure that updates have not introduced any new issues. 6. Reporting & Audit Logs Detailed logs are maintained to track patching activities, compliance status, and system health—helping with audits, future planning, and continuous improvement. A well-defined patch management lifecycle ensures every update is delivered with precision. This results in minimizing downtime, maximizing compliance, and reinforcing security posture. By treating patching as a continuous process rather than a one-off task, organizations can stay ahead of vulnerabilities while maintaining operational efficiency. Traditional vs Modern Patching Patch management has evolved from rigid, manual processes to more adaptive and user-friendly methods. Traditional patching typically focuses on deploying specific fixes for known bugs or vulnerabilities. It's common in legacy systems like older Windows and macOS applications, where updates are discrete and non-cumulative. The process often involves blocking user access, testing on pilot devices, and then deploying patches in controlled batches. Modern patching, on the other hand, is more streamlined. Updates are cumulative, often combining security fixes with feature enhancements. Found mostly in modern OS ecosystems like Apple's, this approach supports user-defined deadlines and admin-imposed maintenance windows. Tools like Hexnode enable granular control over patch deployment—allowing IT admins to schedule updates intelligently without disrupting end users. The shift toward modern patching reflects a broader focus on flexibility, automation, and end-user experience, something that legacy methods often lacked. Did you know? Why Patch Management is Non-Negotiable In today's threat landscape, patch management isn't just a routine IT task – it's a frontline defense against costly breaches, ransomware, and compliance failures. Yet, many organizations still struggle with delayed patching, manual workflows, and limited visibility. Here are some eye-opening facts that highlight why patching – and automating it – is critical for every organization. Key Stats That Speak Volumes Challenges in the tech industry Patch management doesn't happen in a vacuum. From rapidly evolving threats to the sheer diversity of devices and software, maintaining a secure ecosystem poses significant hurdles. Device diversity: Diverse devices and OSes demand adaptable patching strategies to maintain security. Evolving threat landscape: Rapidly evolving threats require agile patching with continuous monitoring and fast response. Interconnected systems: Interconnected systems demand synchronized patching to avoid cascading security risks. Challenges in Patch Management Despite its importance, patch management comes with a set of challenges. 1. Timely deployment Coordinating and deploying patches in a timely manner can be challenging, especially in large and complex environments. Delays in patch deployment leave systems exposed to potential exploits. 2. Compatibility issues Patches may inadvertently introduce compatibility issues with existing software or configurations. Thorough testing is crucial to identify and address these issues before widespread deployment. 3. User resistance In environments where end-users have control over their devices, resistance to updates can pose challenges. Educating users about the importance of patches and implementing user-friendly update processes are key strategies. 4. Rollback complexities Despite thorough testing, issues may arise post-patch deployment. Having robust rollback plans and mechanisms is essential to mitigate the impact of unforeseen complications. Automating Patch Management Automation in patch management simplifies the entire workflow—from identifying patches to deploying them efficiently. Automation is no longer a luxury—it's essential to keep pace with the scale and complexity of modern IT environments. The need for automation arises from the increasing volume and frequency of patches, the complexity of IT environments, and the imperative to reduce manual intervention. Benefits of automating Efficiency gains: Automated patch deployment reduces the time and effort required for manual intervention, allowing IT teams to focus on more strategic tasks. Consistency: Automation ensures consistency in patch deployment, reducing the likelihood of human errors and ensuring that all devices are consistently updated. Timely updates: Automated tools can schedule updates during non-business hours, ensuring that critical patches are applied promptly without disrupting regular operations. Centralized management: Automation provides centralized control and visibility into the patch status of all devices, simplifying the management and monitoring processes. A Patch Management software automates the entire patching lifecycle, covering identification, deployment, monitoring, and reporting. This boosts efficiency, strengthens security, minimizes manual errors, and enables organizations to adeptly address evolving software vulnerabilities. How Patch Management Works: A Real-World Walkthrough Let's walk through a simple example to understand how patch management works in a real-world scenario. Scenario: A mid-sized enterprise uses Windows and macOS devices across departments, along with third-party applications like Zoom, Adobe Reader, and Chrome. The IT team wants to ensure all systems are up to date and secure. Step-by-step patch management process: Asset discovery: The IT team uses an endpoint management tool to scan and list all devices and installed applications. Patch assessment: The tool identifies missing patches, including a critical security update for Windows and a vulnerability fix for Adobe Reader. Testing: Before deployment, patches are tested on a small group of devices to ensure compatibility and avoid disruptions. Deployment: After successful testing, patches are rolled out in phases – starting with high-risk systems and gradually expanding to the rest. Monitoring and reporting: The team monitors patch status through dashboards and generates compliance reports for auditing purposes. Rollback (if needed): If any issues arise post-deployment, the IT team uses rollback features to revert the patch and troubleshoot. This structured approach helps the organization stay secure, reduce downtime, and maintain compliance – all without overwhelming the IT team. How Hexnode improves patch management Hexnode's patch management capabilities are designed to simplify, automate, and scale the update process across diverse device fleets. Whether you're managing Windows, macOS, or third-party applications, Hexnode offers a unified, policy-driven approach that empowers IT teams with precision, visibility, and control. Core Features of Hexnode Patch Management 1. Unified Patch Management Console Hexnode integrates patching into its Unified Endpoint Management (UEM) platform, allowing IT teams to manage OS and app updates from a single pane of glass. This eliminates the need for separate tools and streamlines workflows. 2. Support for Multiple Platforms Patch management is available for Windows, macOS, and third-party applications. Hexnode also announced extended support for Linux devices, making it a cross-platform solution for modern enterprises. 3. Manual and Automated Deployment Options Admins can choose between: Manual deployment for controlled rollouts and pilot testing. Automated deployment for routine updates, scheduled maintenance, and large-scale rollouts. Patch Management Automation4. Granular Targeting and Filtering Deploy patches based on: OS version Device type User role Network Compliance status Patch severity or classification 5. Maintenance Window Scheduling Updates can be scheduled during off-peak hours or designated maintenance windows to avoid interrupting business operations. 6. Reboot and Rollback Controls Admins can configure reboot behavior, allow user deferrals, and even roll back failed patches on Windows devices to maintain system integrity. 7. Real-Time Monitoring and Reporting Hexnode provides: Dashboards showing patch status, missing updates, and reboot requirements. Automated compliance reports for audits. Alerts for failed deployments or patch exceptions. Routine Task Automation8. End-User Experience Customization Admins can: Notify users of upcoming reboots. Allow postponement of restarts. Customize notification messages and timing. 9. WSUS Integration for Windows Hexnode supports WSUS-specific configurations, enabling organizations to align patching with internal infrastructure and policies. 10. Automation via Hexnode Automate With Hexnode Automate, IT teams can: Create rule-based workflows for patch deployment. Trigger actions based on device compliance, location, or patch criticality. Schedule updates and monitor patch health without manual intervention. A Quick Introduction to Hexnode's Patch Management Feature We've put together a short introductory video that gives you a glimpse into the features and its role within the Hexnode UEM platform. Patch management can be handled through a variety of tools, each suited to different environments, device types, and administrative needs. From native OS utilities to full-scale enterprise platforms, organizations have a range of options to ensure systems remain secure and up to date. Native OS Update Utilities Most operating systems come with built-in patching tools—like Windows Update or macOS Software Update. These are ideal for unmanaged or personal devices but lack the centralized control and visibility required in enterprise environments. WSUS and SCCM Windows Server Update Services (WSUS) and Microsoft System Center Configuration Manager (SCCM) are long-standing tools for managing Windows patches. WSUS allows IT admins to approve and deploy updates within a network, while SCCM offers broader configuration management and deeper integration with Microsoft ecosystems. Simplify patching with Hexnode - automate updates, track compliance, and secure endpoints with zero manual effort. Download the datasheet Linux Package Managers Linux environments typically rely on package managers like APT (for Debian-based systems) or YUM/DNF (for Red Hat-based systems). These tools retrieve patches from official repositories and can be scripted or automated for larger environments. MDM/EMM Platforms Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) solutions extend patching capabilities across diverse endpoints. These platforms integrate update management into broader device policy frameworks, supporting mobile devices, desktops, and more. Cloud-Native Tools In cloud and hybrid environments, tools like AWS Systems Manager Patch Manager automate patch deployment across virtual machines and cloud instances. These are useful for dynamic infrastructures requiring scalable and automated solutions. However, their scope is typically limited to assets hosted within that specific cloud environment, making them less suitable for organizations managing multi-cloud or hybrid setups that require centralized visibility and control. Configuration Management Tools Tools like Ansible, Puppet, and Chef are commonly used in DevOps to automate system configuration, including patch deployment. These solutions offer flexibility and scalability in complex IT ecosystems. However, for organizations with simpler infrastructure or smaller teams, these tools may be overkill, as they require significant setup and expertise, potentially adding unnecessary complexity. Vulnerability Management Integration Many organizations pair patching with vulnerability management tools like Qualys or Tenable. These tools identify security gaps and help prioritize patches based on risk severity. While highly effective in identifying and managing vulnerabilities, these tools may not be suitable for smaller businesses or those without dedicated security teams, as they can be costly and require significant resources to properly integrate and maintain. Unified Endpoint and Patch Management Solutions To simplify patching across operating systems and application types, organizations often adopt unified solutions that combine visibility, automation, and cross-platform support—leading into modern tools like Hexnode. These enable centralized patch management across a wide range of endpoints—mobile devices, desktops, and laptops. These tools integrate update workflows into broader device policies, offering automation, policy-based control, and cross-platform support. Unified solutions help IT teams reduce operational overhead while maintaining security compliance. Platforms like Hexnode bring all these capabilities together under a single pane of glass, streamlining patching in diverse IT environments. Try patch management with Hexnode   WSUS vs. WUfB WSUS (Windows Server Update Services) operates as a localized solution, centrally managing Windows updates within an organization's network. It ensures a structured workflow, enabling administrators to meticulously approve, decline, or prioritize updates before deploying them to devices. This approach suits organizations with strict update management policies, providing a controlled and tailored environment. Conversely, WUfB (Windows Update for Business) adopts a cloud-based strategy, utilizing Microsoft's infrastructure for efficient update distribution. By focusing on automatic updates directly from Microsoft's servers, it minimizes dependency on local servers, offering increased flexibility. WUfB allows individual devices to fetch updates based on configured policies, making it a preferred choice for organizations prioritizing ease of use and leveraging Microsoft's cloud capabilities. The choice between WSUS and WUfB depends on personal preferences, with WSUS offering detailed control, while WUfB provides a more adaptable approach that is easy to use. A comprehensive guide on Windows 11 security Best practices for Patch Management Navigating the complexities of patch management requires a strategic approach. Regular audits: Assess patch status regularly. Evaluate installed patches. Identify missing patches. Ensure the system is up-to-date. Automated patching: Enhance efficiency with automation. Schedule updates during non-business hours. Minimize disruption to normal operations. Rollback plans: Mitigate potential failures during updates. Include backups and system restore points. Document procedures for reverting to a pre-update state. User education: Communicate the importance of patches. Inform users about potential downtime. Provide guidance on necessary actions during updates. Patch testing: Conduct thorough testing in a controlled environment. Identify and address conflicts or issues before network-wide deployment. Leverage expert tools: Consider solutions that combine device management with patching capabilities. Centralized platforms like Hexnode can simplify coordination, especially across diverse devices and operating systems. Patch Management FAQs What is third-party patch management? Third-party patch management refers to the process of identifying, deploying, and managing updates for software applications that are not developed by the operating system vendor. These include widely used tools like Adobe Reader, Google Chrome, Zoom, and others. Since these apps often fall outside of native OS update mechanisms, they can become easy targets for attackers if left unpatched. A robust third-party patching strategy ensures these applications are regularly updated, reducing security risks, and maintaining compliance with industry standards. What is the difference between patch management and vulnerability management? While both aim to reduce security risks, patch management and vulnerability management serve different purposes. Patch management focuses on applying software updates to fix known issues – it's a reactive process triggered by vendor-released patches. Vulnerability management, on the other hand, is a broader, proactive discipline that continuously scans for, assesses, and prioritizes all types of security weaknesses, whether or not a patch exists. In essence, patching is one of the many tools used within a vulnerability management strategy. How often should patches be applied? The frequency of patching depends on the severity of the vulnerability and the criticality of the system. Critical patches should be applied as soon as possible – often within 24 to 72 hours – while less urgent updates can be scheduled during regular maintenance windows. Many organizations follow a monthly patch cycle, supplemented by emergency patching when needed. Can patching break applications or systems? Yes, it's possible. That's why testing patches in a controlled environment before deployment is a best practice. Some patches may introduce compatibility issues or unintended side effects. A rollback plan and phased deployment strategy can help mitigate these risks. Is automation necessary in patch management? While not mandatory, automation significantly enhances the efficiency and reliability of patch management. Automated tools can scan for missing patches, schedule deployments, and generate compliance reports – reducing manual effort and minimizing human error. This is especially valuable in large or distributed environments. All you need to know on patch management with Hexnode—set policies, automate updates, monitor and manage OS and app patches with complete visibility. Wrapping up Effective patch management is essential for maintaining security, stability, and compliance across any IT environment. From understanding the different types of patches to selecting the right tools and aligning them with broader IT operations like configuration or vulnerability management, every step plays a crucial role. While the process can be complex—especially in large or hybrid environments—the right strategy and tools can greatly simplify patch deployment and monitoring. Whether you're relying on native OS tools, configuration managers, or unified solutions, a well-structured patch management plan ensures your systems remain resilient in the face of evolving threats and technology changes. If you're not in the know, software can appear as an optical illusion. When you start up an application, you see a slick logo and an attractive user interface that looks so well put together. Under the surface, though, most applications are more like an assemblage of code blocks that invariably contain functional irregularities and security vulnerabilities. That's why virtually all software makers issue "patches" to fix these problems on a regular basis. Microsoft, for example, has "Patch Tuesdays," when it releases fixes to its system software. Staying on top of patching is an important aspect of maintaining a robust cyber defense. Unpatched operating systems (OSs) and application software expose digital assets to cyber risk. Therefore, it's essential to devise and execute a consistent patch management procedure. The question is, should you handle software patch management by yourself or work with a service provider who offers managed patch management? This article explores the advantages of working with an outside managed services provider (MSP) who can deliver patch management as a service (PMaaS). It discusses how patch management services work, along with some best practices for success. Fact Snippets: Patch Management meaning – Patch management means finding, testing, and implementing software patches to fix security vulnerabilities, bugs, and improve performance. Patch management is used to keep systems secure, stable, and compliant with regulations. Managed Patch Management definition – This is a service where a third-party provider handles the entire patch management process—identifying, testing, and deploying updates—to ensure systems remain up-to-date, with less effort required from the organization. What is Patch Management? Patch management is an IT or cybersecurity process that includes identifying and deploying patches for software, especially operating system (OS) software like Windows and Linux. Patch management services can also include hypervisor and network patching support. A patch comprises code that fixes a problem in the software, such as a vulnerability. The patch is a limited software reinstallation that replaces the bug or vulnerability with fresh, non-vulnerable code. Patches also fix functional issues, like a software bug that causes a program to crash. Software makers create patches when they, or users, notice a security or functional problem in their software. Alternatively, researchers or open-source communities may identify a software vulnerability and report it to Common Vulnerabilities and Exposures (CVE), maintained by the MITRE corporation, which is sponsored by the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). Software vulnerabilities are known by CVE identifiers. For example, CVE-2024-20697 refers to a Windows remote code execution vulnerability that affects Libarchive software. A patch is now available to address this vulnerability. Why Patch Management is Important It's hard to overstate the importance of patch management. Patching is an essential activity for cybersecurity and IT reliability, as unpatched vulnerabilities create risk exposure. To this effect, Ivanti revealed that 52% of IT professional see software vulnerabilities as a critical threat, second highest after ransomware attacks. For this reason, a patch management program ensures that such vulnerabilities will be remediated. A thorough, timely patch management program positively affects the following areas of IT: Security—Vulnerability patch management reduces cyber risk exposure. It makes it less likely that malicious actors will be able to exploit vulnerabilities to breach systems, steal data, or disrupt operations. System Uptime—Unpatched software may crash unexpectedly. Patch management keeps software running and supports high levels of system Uptime. System performance—Patching can positively affect system performance. Software may contain bugs that cause functional problems, such as conflicts between systems. Patches can fix these problems. Regulatory compliance—Many compliance frameworks mandate that software be patched, and audits may seek to confirm the existence of a patch program and check its practices and activities. Feature improvements—Patches sometimes go beyond bugs and vulnerabilities, offering updates to features and functions. 9 In-House Patch Management Challenges Should your organization execute on its patch management strategy? Many IT organizations have patch management teams that use tools like (the now deprecated) Microsoft's Windows Server Update Services (WSUS), which enables admins to manage and distribute Windows updates, or Microsoft Endpoint Configuration Manager (MECM), which handles software and OS deployment and configurations. Or they use third-party patch management like Automox. However, in-house patch management comes with its share of challenges. A lot can go wrong in the process, potentially affecting production systems. Here are nine of the more pressing issues. 1. Volume and Complexity of Patches With a thorough and robust patch management plan, you're going to be handling a high volume of patches, some of which are complex to install. It takes resources to keep track of all the patches submitted by vendors and understand what they do and which systems they affect. 2. Compliance Regulations may mandate patching and reporting on the state of patching. Regulatory audits may check on patch management as part of this process, too. An in-house patch management program has to meet these requirements if the organization wants to maintain compliance. This means specialized reporting and audit tooling, as well as people's time. 3. Prioritizing Patches Based on Risk Not all patches deserve the same priority for deployment. Some are absolutely critical and require immediate attention. Others are relatively insignificant and can effectively be ignored for the long term. The best practice is to prioritize patches by risk. A vulnerability that exposes your organization to serious risk merits the most attention and fastest action. The risk assessment process takes knowledge and time, two areas that may be in short supply with an in-house team. 4. Testing and Compatibility It is highly recommended to test patches before installing them. This is easier said than done, however, because proper testing requires setting up an exact replica of the production environment, which is difficult to install and can be costly. Testing matters, though, due to potential compatibility issues. Patches can "break" systems, especially when your ecosystem has integrations that can be disrupted by changes in OS software. 5. IT Staff Resource Limitations Patch management needs a qualified and, at times, large team of employees. In big enterprises, you may find entire teams dedicated to server patching, Windows patching, Linux patching and so forth, highlighting the importance of this process. Even in these conditions, large teams face resource limitations, struggling to keep up with the pace of patch management. If they are deploying patches manually, the resource constraints will become even more pronounced. Automated patch management tools can help, but it is not always viable. Furthermore, organizations frequently limit the downtime available for patching to be during unsociable hours, for example Sunday 1am through to 4am. With a true 24/7 workforce, this can be handled by those working on shift patterns. Yet for smaller IT teams that will have to rely on on-call staff or overtime outside of normal hours, this can cause dissatisfaction within the team. 6. Downtime Risk Patching takes systems offline, so the patch process will result in some inevitable downtime. Ideally, this won't last long, but even with testing, patches can sometimes cause unexpected outages. This is why many organizations install patches at slow times, like early on Sunday mornings. The process can be risky because there's always the potential for unexpected, disastrous disruption or outages in data centers. 7. Visibility and Control Effective patch management requires complete awareness of endpoints and the state of patching across the IT estate. Without visibility into which endpoints need patches, patching will be incomplete and potentially disruptive. An in-house patch management should have a system in place for visibility and control over patching, which could be a strain on the IT team. 8. Third-Party Applications and IoT Third-party applications, i.e., software that is not OS or firmware, need patching, too. For example, Adobe released patches recently for CVE-2024-30311, a vulnerability that is, according to NIST, "an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory." By exploiting unpatched versions of Adobe Reader, an attacker "could leverage this vulnerability to bypass mitigations such as ASLR (Address Space Layout Randomization)." It can be difficult to keep up with the pace and volume of third-party patches. Cloud patch management is another consideration. This refers to patching cloud-based systems hosted on infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS). This is part of the "shared responsibility model" agreed upon when signing up for IaaS or PaaS. The internet of things (IoT) presents a patching challenge due to the number and variety of devices that may need patches. A factory with sensors and cameras, for example, may contain thousands of devices, each of which has an embedded OS subject to patching. Keeping track of those devices and the states of their patches takes an automated solution. 9. Remote Workforce Devices used by people working remotely also require patching. It can be difficult to track which remote work devices are fully patched, especially if their connections to the network are intermittent. As these nine issues suggest, handling patch management in-house takes a commitment of time, people, and resources that not every organization can afford. Or, if they can afford it, is it the best use of resources? Directing the same people to business-facing IT initiatives may be more strategically advantageous. What is Managed Patch Management? Managed Patch Management is when a third-party organization, usually a Managed Service Provider, carries out patching services. The tasks can vary in scope, but most include the MSP handling patch planning, risk prioritization, testing, and deployment, with a focus on managed OS patching. Managed patching services may also offer remediation, which occurs when a patch itself has a problem that needs to be corrected, and some provide patch governance as well. The net effect is to offer patching as a service or PMaaS, typically through specialized patch management solutions. MSP patch management can appear to automate the patch management procedure as it is taken from the in-house teams. While it also provides the visibility and reporting required for compliance and internal reporting to key stakeholders. Top 5 Benefits of Patch Management as a Service Outsourcing patch management delivers a range of benefits compared to handling the process in-house. Here are five benefits of PMaaS that are worth noting: 1. Better IT Staff Productivity Turning over the labor-intensive patch management process to an MSP frees your team members to do work that benefits the business and can reduce the amount of out-of-hours work required. They become more productive, with the time to execute digital transformation projects and other tasks that benefit customers and employees. 2. Improved Security Posture PMaaS should improve organizational security posture by patching systems for security according to the correct risk prioritization. When you also consider that MSPs often include comprehensive EOC or outsourced NOC services within their offerings, security is monitored continually. Companies will therefore be less exposed to the risks posed by having unpatched vulnerabilities that attackers can exploit. 3. Improved Uptime Thoroughly patched systems and reduced alert fatigue lead into fewer unplanned outages. When using a reputable IT infrastructure Managed Service Provider, a dedicated team will monitor and remediate patching 24/7, significantly reducing the chance that the environment is susceptible to attacks. For this reason, using PMaaS should improve infrastructure Uptime. 4. Complete Regulatory Compliance The MSP will handle the patch management to a standard required by regulations. They will also be able to guide businesses and their IT teams through compliance audits related to patching and report patching status to relevant stakeholders. When you consider that the in-house team would not have to handle this previously time-consuming workload, this is a considerable benefit of utilizing a Managed Service Provider. 5. Greater Control Over Costs Though every company is different, PMaaS will likely cost less than having a team of in-house people handle the process. However, even if the cost is similar or higher, the advantage of PMaaS is having greater control over costs. With fixed vendor budgets, you will know what you're paying for versus in-house costs, which can be variable with overtime and recruiting costs, among other unpredictable cost factors. 6 Managed Patch Management Best Practices The benefits of partnering with an MSP for patch management are clear. However, an optimal course of action should be taken to ensure the patching program is carried out effectively and securely. The following six best practices are to be followed, to realize ideal security and IT outcomes. 1. Establish Clear, Agreed-Upon Patch Management Policies It's helpful to establish clear patch management policies that you and the MSP agree upon before embarking on PMaaS. These policies might cover issues like whether all patches must be tested before deployment, how risk prioritization will work, or even times of day when patching will occur. Policies might also define the time horizon for patching, such as "all critical security patches shall be applied within 30 days of the vendor's release of the patch." Setting a defined framework ensures that patches are applied promptly and appropriately, and no vulnerabilities go unnoticed. 2. Collaborate on Developing a Patch Management Strategy A PMaaS engagement should develop from a patch management strategy. For example, the strategy might be to prioritize OS security patches above all others. Until those patches are applied, no other patches will be deployed. This might be called a "security first" patch management approach. In contrast, you might employ a "performance first" or "Uptime first" strategy. A lot will depend on organizational protocols, and establishing this with the MSP will ensure priorities are met. 3. Follow a Documented Patch Management Process Both the business and the partnered Managed Service Provider must work from a documented patch management process. That way, there will be less room for errors and misunderstandings. A suggested process is as follows: Creating a full and current inventory of production systems—Know what OSs are running, locations, and system owners. Assembling a parallel inventory of patches—With potentially hundreds of patches being downloaded, tested, and deployed at any given time, only an organized inventory and monitoring process can prevent errors and omissions that negatively affect security posture. Standardizing systems and OSs to the same version type whenever possible—This step will simplify and speed up the patching process. Matching vulnerabilities against your inventory—This is the first step in determining the priority of patch installation. Classifying risk and assessing risk levels—Focus on the highest-impact vulnerabilities first. Testing patches—The best approach is to try the patch on a sample of systems in a lab environment. Even if the lab can't reproduce the production systems perfectly, this process will reveal compatibility issues before they can cause problems outside the lab. Applying patches—Automate wherever possible. Automation can make a huge difference in the efficacy and resource efficiency of a patch management program. Toolsets for patch automation often include features for monitoring and reporting, which further improve the program's effectiveness. 4. Track Progress and Report Results Patch management occurs within the context of IT and security organizations, yet stakeholders will want to know how the process is going. Regular auditing and reporting serve this need. They also let the patch management team understand how they're doing. Auditing and reporting are also necessary for proving regulatory compliance. 5. Keep Patch Management Services Centralized Patch management can be overwhelming, so it makes sense to keep the activity contained in a centralized management process, ideally tracked and implemented through automated patch management tools managed by the MSP. This approach reduces the chance of human error and enables efficiency in the process. 6. Create a Culture of Patching Accountability The patch management team and PMaaS vendor should have accountability for their work. This might take the form of reporting to senior managers or establishing targets for patching execution. The main idea is to instill the notion that patching is critical, and that the patch management program takes responsibility for their work. Third-Party Patch Management from Park Place Technologies Planning and installing patching updates to your environment, be it OS, hypervisor or network patching can be time-consuming. Not to mention the distraction caused, meaning other business priorities are dropped, it's easy to see why in-house teams can struggle with patch updates. Take the burden away from your IT team and partner with a reliable patch management service provider in Park Place Technologies for all your patching needs. Via our IT infrastructure managed services, our enterprise operations center supports all major OS and virtual platforms including VMware, Microsoft and Linux – no matter your device, we have you covered. Contact Park Place Technologies today, to learn how our managed patch services can keep your systems protected, enforce Uptime and keep you focused on the most important organizational initiatives. The below graphic shows our patch management process, from proactive monitoring to resolution and continued management. Why do customers choose our vulnerability and patchmanagement solution?Improve your threat prevention capabilities by scanning your endpoints' operating system and third-party applications. Get instant reporting to the console and rapid automatic patching.Prioritise vulnerabilities based on their severity, filter them, and patch critical security issues first. Customisable patching policies give you flexibility and let you control deployment of security patches to endpoints.Timely patching is empowered by ESET PROTECT Platform's protection against ransomware and zero-day threats. Enjoy complete visibility into the security posture of your organisation's endpoints and servers, including asset inventory via the ESET PROTECT console. Common use casesPatching of security holes in operating systems and applications remains critical, but remains one of the most time-consuming tasks in IT. IT teams can get overloaded, meaning they are unable to update inventories and consequently fall behind in patching.The complexity of IT systems is growing, making coordination among cross-functional teams and full security visibility harder. What makes our solution a perfect fit for your needs?Vulnerability & Patch ManagementESET Vulnerability & Patch ManagementProvides an additional layer of security for organisations that need to comply with relevant regulations such as FedRAMP and NIS2. Our solution helps to stop threats from out-of-date operating systems and applications, thanks to:Automated scanningSeverity-based prioritisationFiltering optionsExceptions for vulnerabilitiesList of affected devicesAutomatic and manual patchingCustomisable patching policiesList of available patchesCentral managementExplore ESET Vulnerability & Patch Management featuresAutomated scanningAutomated scanning with instant reporting and centralised management from the ESET PROTECT console. Scans thousands of applications and detects over 35,000 Common Vulnerabilities and Exposures (CVEs).Severity-based prioritisationPrioritise vulnerabilities based on their severity. Our wide range of filtering options enables you to quickly identify and focus on critical security issues.Reports & databasesIdentify the most vulnerable software and devices, get numbers of affected devices, see patch inventory including patch names, KB numbers, CVEs, patch severity and affected applications.Automated and manual patchingChoose from automatic or manual patching. ESET's patch inventory ensures that your endpoints are updated with the latest security patches in a timely manner.Complete visibilityBenefit from the unified view provided by the ESET PROTECT console across Windows, Linux and macOS operating systems. Get complete and up-to-date visibility of your organization's endpoints, subscriptions, and vulnerability and patching status.Platform orchestrationDecrease the complexity of your IT management tasks, maintain up-to-date inventory, and benefit from prevention, detection and response capabilities in order to minimise your exposure to threats.Committed to the highest industry standardsPurchase your vulnerability and patch management solution todayFor other purchase options, contact your ESET representative.Complete, multilayered protection for endpoints, cloud applications and email, the number one threat vector 56789101112131415161718192021222324252627282930313233343536373839404142434445464748495051525354555657585960616263646566676869707172737475767778798081828384858687888990919293949596979899YearFor online purchase, please choose correct number of devicesAll included modules:Management ConsoleModern Endpoint ProtectionServer SecurityMobile Threat DefenceFull Disk EncryptionAdvanced Threat DefenceCloud App ProtectionMail Server SecurityVulnerability & Patch ManagementExtended Detection & ResponseMulti-Factor AuthenticationMDR ServicePremium SupportAll-in-one prevention, detection & response combining enterprise-grade XDR with complete multilayered protection Price available on request Leave us your contact details to receive an offer tailored for your company's needs.All included modules:Management ConsoleModern Endpoint ProtectionServer SecurityMobile Threat DefenceFull Disk EncryptionAdvanced Threat DefenceCloud App ProtectionMail Server SecurityVulnerability & Patch ManagementExtended Detection & ResponseMulti-Factor AuthenticationMDR Ultimate ServicePremium Support UltimateSuperior protection with continuous threat hunting and monitoring via 24/7 managed detection & response service Price available on request Leave us your contact details to receive an offer tailored for your company's needs.All included modules:Management ConsoleModern Endpoint ProtectionServer SecurityMobile Threat DefenceFull Disk EncryptionAdvanced Threat DefenceCloud App ProtectionMail Server SecurityVulnerability & Patch ManagementExtended Detection & ResponseMulti-Factor AuthenticationMDR ServicePremium SupportContinuous protection for your evolving IT environment, with premium cyber risk management and 24/7 ESET expertise on callPrice available on request Leave us your contact details to receive an offer tailored for your company's needs.All included modules:Management ConsoleModern Endpoint ProtectionServer SecurityMobile Threat DefenceFull Disk EncryptionAdvanced Threat DefenceCloud App ProtectionMail Server SecurityVulnerability & Patch ManagementExtended Detection & ResponseMulti-Factor AuthenticationMDR Ultimate ServicePremium Support UltimateCybersecurity Awareness TrainingPrevention-first education to ensure employees are the foundation of an organisation's digital securityIncludes: ESET Cybersecurity Awareness Training56789101112131415161718192021222324252627282930313233343536373839404142434445464748495051525354555657585960616263646566676869707172737475767778798081828384858687888990919293949596979899YearFor online purchase, please choose correct number of devicesEffective training methodsSimulated phishing campaignsSmart management and detailed reportingDeep integration with various systemsCompliance with regulations Protecting your business from known exploits and unauthorized access has become more important than ever. With attacks growing in sophistication and frequency, proactive strategies are essential to protecting digital assets. Patch management stands as one of the first defenses against vulnerabilities, ensuring software and systems remain protected before potential threats become exploitable. In our blog, we will explore the fundamentals of patch management, exploring its types, lifecycle, and benefits. We will also highlight best practices to optimize your patch management strategy. Stay tuned as we uncover the importance of patch management in strengthening your organization's cybersecurity posture and reducing risks effectively. Patch management is the systematic process of applying updates, including software, drivers, and firmware, provided by vendors to address vulnerabilities and enhance the performance of systems and devices. It involves the distribution and application of patches to correct errors or bugs in software, ensuring optimal operating performance and protecting against security threats. Effective patch management is essential for maintaining the integrity and security of systems and reducing the risk of breaches, data leaks, and productivity losses. Patch management is essential to companies for several reasons, some of which are as follows: Enhanced Security: Patch management addresses vulnerabilities in software and applications, reducing the organization's susceptibility to cyberattacks. System Uptime: By keeping software up-to-date, patch management minimizes disruptions and downtime, ensuring continuous system availability and functionality. Compliance: Regulatory bodies often mandate maintaining a certain level of security. Effective patch management helps organizations adhere to these standards, ensuring compliance with laws and regulations. Feature Improvements: Beyond security fixes, patch management includes feature/functionality updates, ensuring systems benefit from the latest enhancements and capabilities. Promotion of Productivity: Well-managed software with up-to-date patches works more efficiently, boosting employee productivity rather than hindering it, contrary to common misconceptions. Cost Reduction: Patch management lowers the cost of device lifecycle management and repair by enabling remote management tools, reducing the need for expensive hardware shipments or service calls. Regulatory Compliance: Patch management aids in meeting laws, regulations, and industry standards such as HIPAA and GDPR, ensuring the protection of sensitive data and regulatory compliance. Patch management and vulnerability management are both essential for keeping a company's IT systems safe and running smoothly. Although people sometimes mix them up, they each have their own jobs and steps to follow. Focus Core FunctionsSimilaritiesDifferencesPatch ManagementAddressing software vulnerabilities through patch deploymentBuild IT inventory, prioritize patches, create patching policies, monitor & test patching systems, deploy patches, verify patch deployment, create patch reports & documentationCategorization, monitoring, verificationPatching policies, analyzing vulnerabilitiesVulnerability ManagementIdentifying, assessing, and prioritizing vulnerabilities across IT infrastructureFind and identify vulnerabilities, analyze vulnerabilities, categorize vulnerabilities, monitor vulnerabilities, remediate vulnerabilities, verify remediationCategorization, monitoring, verificationPatching policies, analyzing vulnerabilities Patch management comes with its fair share of benefits that you can utilize in your company. Here are a few advantages outlined below. An efficient patch management program enables organizations to identify vulnerabilities across their enterprise's systems. By continuously monitoring for available patches and systematically deploying them, companies can pinpoint areas of exposure within their network, reducing the likelihood of successful cyber attacks. Understanding and maintaining an inventory of all assets is crucial for effective cybersecurity. Patch management involves the upkeep of a real-time inventory of assets and systems, providing organizations with a comprehensive view of what needs protection. This ensures that no critical asset is left

vulnerable due to oversight. Regularly patching vulnerabilities helps organizations mitigate risks within their network environment, leading to a more secure infrastructure. By addressing vulnerabilities promptly, companies can reduce the likelihood of cyber attacks and security breaches, safeguarding sensitive data and preserving business continuity. Not all vulnerabilities pose the same level of risk to an organization's critical assets. An effective patch management program prioritizes patches based on their severity and relevance, allowing teams to focus on addressing high-risk vulnerabilities efficiently. This targeted approach minimizes the time and resources spent on patching non-critical issues. Compliance with security standards is essential for avoiding fines and penalties from regulatory agencies. Patch management plays a vital role in maintaining compliance by ensuring that systems are up-to-date with the latest security patches. This helps organizations adhere to regulations such as HIPAA and GDPR, protecting both customer and company data from unauthorized access and exploitation. Patching vulnerabilities with the latest software updates strengthens device and data security, reducing the risk of data breaches. By addressing security weaknesses promptly, organizations can prevent sensitive information from falling into the wrong hands and uphold the confidentiality and integrity of their data. Patch management contributes to a smoother user experience by ensuring that devices run efficiently without interruptions. By addressing performance issues and bugs promptly, organizations can enhance productivity and user satisfaction, allowing employees to focus on their tasks without disruptions caused by software vulnerabilities. The patch management lifecycle is a systematic process designed to ensure that software vulnerabilities are promptly identified, prioritized, addressed, and verified to maintain a secure IT environment. It involves several steps, each with its specific tasks and objectives. The lifecycle begins with the identification of vulnerabilities and available patches. This involves conducting a thorough network inventory to identify all IT assets and monitoring vendor sites for known vulnerabilities and updates. Next, vulnerabilities are prioritized based on factors such as severity, potential impact, and criticality of affected systems. High-risk vulnerabilities are given top priority to minimize the risk of cyberattacks. Patch management policies are established to determine which patches need to be applied, when, and under what conditions. These policies provide guidelines for patch deployment and help ensure consistency and efficiency. Continuous monitoring is crucial to stay informed about new patches and vulnerabilities from vendors. Organizations set up systems to receive notifications about upcoming patches and vulnerability updates. Before deployment, patches are tested in a non-production environment to detect any conflicts or issues. This ensures that patches operate as intended and do not cause disruptions in the IT environment. Any necessary documentation or adjustments are made before deploying patches to ensure all stakeholders are informed and prepared for the changes. Patches are deployed according to the established patch management policies. Automated deployment tools streamline the process and reduce the risk of human error. Pending or failed patches are closely monitored for incompatibility or performance issues. End-users are advised of any issues and upcoming solutions if necessary. Patch compliance reports are generated regularly to provide insight into the organization's IT infrastructure and patching effectiveness. This helps stakeholders make informed decisions and track progress over time. The patch management lifecycle is a continuous process that requires regular review, updating, and repetition of the previous stages. This ensures that information remains up-to-date and accurate, allowing organizations to refine and optimize their patch management processes over time. Effective patch management is crucial for maintaining the security and functionality of your organization's IT infrastructure. To optimize your patching process, implementing best practices is essential. Here are seven key patch management best practices to enhance your cybersecurity posture and streamline your operations: Utilize automated patch deployment tools to efficiently scan for missing patches and install them on endpoints, reducing response time and minimizing manual effort. Adopt a critical-updates-first approach to prioritize and promptly address critical vulnerabilities, ensuring the most urgent patches are applied without delay. Implement scheduled auto-deployments at least twice a week to ensure endpoints receive timely patch updates, allowing for proper testing and approval while maintaining security. Maintain user productivity by offering flexible deployment policies that allow users to postpone updates if necessary, ensuring business-critical tasks remain unaffected. Before deploying patches to endpoints, thoroughly evaluate them in a test environment to identify and mitigate potential conflicts or issues, minimizing disruptions to production systems. Keep detailed records of deployed patches and communicate system changes to stakeholders, facilitating accountability and providing clarity on patching activities. Continuously educate yourself on evolving patch management best practices to adapt and refine your patching strategy, ensuring your organization remains resilient against emerging threats. Patch management is a must-have feature to strengthen cybersecurity defenses, regardless of an organization's size or industry. By promptly addressing vulnerabilities and keeping software up-to-date, businesses can effectively manage risks and protect their assets. Moreover, patch management offers greater control and flexibility to IT departments, empowering them to maintain a secure and resilient infrastructure. As cyber threats continue to evolve, investing in strong patch management practices remains essential for ensuring the smooth operation and protection of businesses today. Skip to content Security patch management is an essential organizational capability. This article explains why before detailing some common methods for undertaking patching. This article by @gilad_maayan explains why patch management is an essential organizational capability & details some common methods for undertaking patching. #patchmanagement #security #infosec Share on X Patch management is the process of deploying and applying software updates, usually to fix software bugs or security issues. Almost any computer system occasionally requires patching—including computer hardware, operating systems, applications, and embedded systems such as network devices. Regularly patching systems can help organizations manage and mitigate risks in an IT environment. When software vulnerabilities are discovered after software or hardware is released, the vendor releases a software patch that can remediate the vulnerability. It's critical to apply these security patches urgently. Otherwise, the system can be openly exploited by attackers. Software patches can also address stability and performance issues that negatively affect a system's users. Patch management is an essential element of an organization's cybersecurity strategy, with unpatched operating systems and applications a leading cause of cybersecurity breaches. To help identify these risks in your environment, you can use application dependency mapping tools to identify the full hierarchy of software packages on servers and endpoints. Patch management is an essential element of an organization's #cybersecurity strategy, with unpatched operating systems and applications a leading cause of cybersecurity breaches – @gilad_maayan #patchmanagement Share on X A fast and efficient security patch management process, complemented by continuous monitoring and detection of vulnerabilities, can help minimize the risk of attacks. In addition to improving the security posture, patching systems can improve their performance and reduce downtime or malfunctions caused by unsupported or outdated software. In many cases, patches include new benefits and features, making end-users happier or helping businesses operate more efficiently. Security patch management also has a compliance angle, with it explicitly required by many regulatory and industry standards. Failure to apply patches to sensitive systems could result in fines or legal penalties. Your #patchmanagement process should ensure that every endpoint that connects to the corporate network, regardless of its location or owner, is appropriately patched – @gilad_maayan Share on X The security patch management process should ensure that every endpoint that connects to the corporate network, regardless of its location or owner, is appropriately patched. There are two main types of patch management systems—those that patch multiple systems and those that can patch only a single system. Those patching a single system perform periodic checks to find available patches and typically install and download new patches automatically. However, maintaining the consistency of software versions in a corporate network requires a centralized patch management approach rather than having each machine download patches independently. A central patch management solution employs a centralized server to perform the following: Checking network infrastructure for missing patches Downloading missing patches Distributing patches to various devices across the network according to specified patch management policies. There are two main types of patch management systems—those that patch multiple systems and those that can patch only a single system. This article by @gilad_maayan explains. #patchmanagement Share on X It allows your organization to benefit from: Automation. The central patch management server automates patch management and extends control over the entire process. It enables organizations to make decisions and changes to the process. For example, if a patch has a problem, the admin can set up the patch management tool to prevent the deployment of the patch. Bandwidth savings. Central patch management helps conserve Internet bandwidth, enabling the server to download each patch only once and then distribute it to every computer that requires it. Managed service provider (MSP) services. In addition to operating patch management in-house, organizations can employ an MSP to perform security patch management with the other network management services they provide to clients. MSP patch management can help minimize in-house administrative work, freeing staff to focus on other aspects. This article by @gilad_maayan share three automated methods for patch management. #patchmanagement #infosec Share on X Dedicated Patch Management Solutions. Automated patch management tools regularly scan and apply patches without human intervention. These tools can identify vulnerabilities as soon as they are made known, ensuring teams can test or fix the issue immediately. The traditional automated patch management system was deployed on-premises to support in-house IT networks. As networks moved to the cloud, using diverse networks of servers from various providers like Amazon Web Service (AWS) and Google Cloud, cloud-native patching automation emerged. Cloud-native patching automation helps organizations manage multiple systems and software regardless of the location. These solutions can apply patches 24/7 to ensure downloads and installations do not disrupt workdays and eliminate human errors from the process. Software Configuration Analysis (SCA). This solution allows developers to safely leverage open-source software packages without exposing their organizations to vulnerabilities, as well as legal and compliance issues. When vulnerabilities are discovered in open-source code, they are often found and patched by community members. However, the burden of updating the component to the new version, or applying the patch, rests with the developer. Once the vulnerability is discovered, it is only a matter of time before a publicly available exploit makes it easy for attackers to exploit the issue. SCA creates a software bill of materials (SBOM) that contains all open-source components used in the application. SBOM lists the package version, known vulnerabilities, and details about the license for each component in use. This provides visibility that helps developers and IT operations staff understand the risks inherent in open source components, update them if possible, and if not, remove them from production applications. Endpoint Security Tools to Automate Security Patch Management. Endpoint security tools have significantly evolved over the past decade. What started as a limited solution that provides antivirus scanning has evolved into advanced platforms that offer multiple defensive measures, including next-generation antivirus (NGAV), endpoint detection and response (EDR), and, more recently, extended detection and response (XDR). Endpoint security tools can help organizations identify endpoints containing vulnerabilities and automatically deploy patches to specific endpoint groups at scheduled times. They also enable teams to set organization-wide policies for endpoint security patch management. Many endpoint security platforms make it possible to deploy patches based on type, severity, or vendor, and schedule deployments based on multiple criteria. It can even be possible to automatically test patches before approving deployment to discover any compatibility or productivity issues. I hope this security patch management article is helpful as you level up your ability to manage patches to reduce security risks. Further Reading What's ITSM? ITIL 4 Service Management What ITSM Pros Need to Know About Network Security ITIL 4 Explained – IT Service Management Practices Beyond ITIL v3 – The ITIL 4 IT Service Management Framework Which IT Service Management Tools? Here's an ITSM Tools List Enterprise Service Management – What is ESM? What ITSM Pros Need to Know About CMDBs How to Define, Measure, and Report IT Service Availability Please use the website search capability to find more helpful security and ITSM articles related to topics such as best practices for managing software, ensuring compliance, endpoint management, attack surface minimization, security breach management, threat landscape analysis, common cyber attacks, security team management, patch management best practices, cyber threats, handling data breaches, managing mobile devices, endpoint security solutions, patching status analysis, endpoint protection platform (EPP) capabilities, EDR solutions, remote working risks, and various security threats. Cybersecurity is a pressing concern for businesses of all sizes. With the ever-increasing sophistication of cyber threats, it is crucial to stay one step ahead in protecting your organization's sensitive data. Enter patch management, a proactive approach to maintaining the security of your IT systems. In this informative article, we will demystify patch management, shed light on its importance, and provide practical insights on how to implement an effective patch management strategy for your business. Patch management refers to the process of regularly updating, and applying patches or fixes to software, applications, and operating systems. These patches are released by software vendors to address security vulnerabilities, bugs, and other issues that may compromise the stability and security of the system. Patch management involves identifying, testing, and deploying these patches across the organization's IT infrastructure to ensure that all systems are up-to-date and protected against potential threats. Patch management is of utmost importance for several reasons: Security Enhancement: Regularly applying patches helps to address known vulnerabilities in software and systems, reducing the risk of unauthorized access, data breaches, and other cyber threats. Protection Against Exploits: Hackers often exploit vulnerabilities in outdated software to gain unauthorized access or control over systems. Patch management ensures that these vulnerabilities are patched, minimizing the risk of exploitation. Stability and Performance: Patches not only address security issues but also improve the stability and performance of software and systems. By keeping software up to date, businesses can ensure optimal functionality and minimize system crashes or performance issues. Compliance Requirements: Many industries have specific compliance regulations that require organizations to maintain up-to-date software and security measures. Patch management helps businesses meet these compliance requirements and avoid potential penalties or legal issues. Cost Savings: Proactive patch management can help prevent costly security incidents and system downtime. By investing in regular patching, businesses can save money in the long run by avoiding the financial repercussions of cyberattacks or system failures. Reputation and Customer Trust: Demonstrating a commitment to security through effective patch management can enhance a business's reputation and build trust with customers. It shows that the organization takes data protection seriously and is proactive in safeguarding sensitive information. Patch management is crucial for maintaining the security, stability, and performance of IT systems. With regular updates and patches, businesses can mitigate security risks, comply with regulations, and protect their valuable assets from potential cyber threats. Patch management involves a systematic process to ensure the effective deployment and management of patches across an organization's IT infrastructure. Here is a step-by-step breakdown of how patch management works: The first step is to identify the patches that are relevant to the organization's software, applications, and operating systems. This can be done by staying updated with vendor notifications, security advisories, and patch management tools. Once patches are identified, they need to be assessed to determine their impact on the organization's systems. This involves evaluating the severity of vulnerabilities addressed by the patches and understanding any potential compatibility issues. Before deploying patches to production systems, it is crucial to test them in a controlled environment. This helps ensure that the patches do not introduce any new issues or conflicts with existing software or configurations. After successfully testing the patches, a deployment plan is created to schedule installing patches. This plan considers factors such as system availability, maintenance windows, and any dependencies between patches, ensuring a seamless and efficient patch installation process. The patches are then deployed to the target systems following the deployment plan. This can be done manually or through automated patch management tools that streamline the process and ensure consistency. Once patches are deployed, it is important to monitor the systems to ensure that the patches have been successfully applied and that the systems are functioning as expected. This may involve conducting post-patch testing and verification. It is essential to maintain accurate documentation of the patches applied, including details such as patch versions, deployment dates, and any associated notes. This documentation helps with auditing, compliance, and future reference. Patch management is an ongoing process. Regularly reviewing and updating patching policies, staying informed about new vulnerabilities, and repeating the patch management cycle ensures that systems remain secure and up to date. By following these steps, organizations can establish an effective patch management process that minimizes security risks, ensures system stability, and helps maintain a strong security posture. Patches are an essential part of patch management, which is the process of updating software to fix vulnerabilities and improve performance. There are three main types of patches commonly used in patch management: Security Patches: These patches are specifically designed to address security vulnerabilities in software. They fix flaws that could be exploited by cybercriminals to gain unauthorized access or launch attacks on your systems. Security patches are crucial for maintaining a strong defense against evolving threats. Feature Patches: Feature patches, also known as functional patches, introduce new features and enhancements to the software. They are typically released to improve the functionality and usability of the application. These patches may include bug fixes, performance improvements, and additional capabilities that enhance the user experience. Critical Patches: Critical patches are high-priority updates that address severe vulnerabilities or issues that could have a significant impact on the stability or security of the software. These patches are essential for preventing potential system failures, ensuring data integrity, and safeguarding your IT infrastructure from potential threats. Each type of patch is intended to address specific aspects of software updates, maintenance, systems management, and security. It is crucial to adopt a comprehensive patch management strategy to promptly identify, test, and apply these patches to your systems. Regularly applying updates to your software with the latest patches helps safeguard your business assets, improve functionality, and minimize the risk of security breaches and disruptions. Patch management can present several challenges that organizations need to address effectively. Some of the key challenges include: Distribution and Distributing Patches: Distributing patches across a large number of systems can be a complex task. Ensuring that patches reach all relevant devices and are installed correctly requires a well-defined distribution strategy and robust patch management tools. Acquiring Patches: Keeping track of the latest patches released by software vendors and acquiring them promptly can be challenging. Organizations need to stay updated with vendor notifications, security advisories, and other reliable sources to ensure they have access to the necessary patches. Code Changes and Compatibility: Patches often involve code changes to address vulnerabilities or bugs. However, these code changes can sometimes introduce compatibility issues with existing software or configurations. Organizations need to carefully test patches to ensure they do not disrupt the functionality of critical systems. Patch Testing: Testing patches before deployment is crucial to ensure they do not cause any unintended consequences or conflicts with other software. However, testing can be time-consuming and resource-intensive, especially when dealing with a large number of systems or complex IT environments. System Downtime: Installing patches may require system restarts or temporary downtime, which can impact business operations. Organizations need to carefully plan patch deployment to minimize disruption and schedule maintenance windows during periods of low activity. Patch Prioritization: With a constant stream of patches being released, organizations need to prioritize which patches to apply first based on their severity and potential impact on the systems. This requires a thorough understanding of the organization's IT infrastructure and the associated risks. Legacy Systems and Third-Party Software: Managing patches for legacy systems or third-party software can be challenging, as these may have different patching processes or limited support. Organizations need to develop strategies to address patch management for these systems effectively. Patch Documentation and Reporting: Maintaining accurate documentation of applied patches and generating comprehensive reports can be time-consuming. However, this documentation is essential for auditing, compliance, and tracking the patch management process. By recognizing and addressing these challenges, organizations can establish robust patch management practices that ensure the timely and effective application of patches, minimizing security risks and maintaining the integrity of their IT systems. In general, it is recommended to perform patch management at least once a month, although more critical patches may require immediate attention. Software vendors often release patches and updates to address newly discovered vulnerabilities and to improve the functionality of their products. By staying up to date with patch management, you can protect your business assets from potential security breaches and ensure that your systems are running optimally. In conclusion, patch management is a critical aspect of maintaining the security and stability of an organization's IT infrastructure. By regularly identifying, testing, and deploying patches, businesses can enhance their security posture, protect against potential vulnerabilities, and ensure optimal system performance. However, patch management does come with its challenges, such as distribution, acquiring patches, code changes, and system downtime. By addressing these challenges through effective planning, testing, and prioritization, organizations can overcome these obstacles and establish a robust patch management process. With a proactive approach to patch management, businesses can safeguard their valuable assets, comply with regulations, and build trust with customers, ultimately bolstering their overall cybersecurity defenses. Your business's protection against cyber threats is our utmost priority at Buzz Cybersecurity. With a comprehensive range of services, including managed IT services, cloud solutions, disaster recovery, and ransomware protection, we offer a complete cybersecurity solution. What makes us stand out is our unwavering dedication to exceeding expectations and providing exceptional cybersecurity solutions. Trusted by businesses in neighboring states, we take pride in delivering unmatched protection. Partner with Buzz Cybersecurity today and ensure the highest level of security for your business. Sources Patch management is the process of identifying, acquiring, testing, and installing software updates, or patches, to a computer system or network. The primary goal of patch management is to address security vulnerabilities, fix bugs, and improve the functionality of software and systems. Effective patch management helps prevent cyberattacks, ensures system stability, and maintains compliance with security standards. Steps in Patch Management 1. Inventory Management: • Identify Assets: Create an inventory of all software and hardware within the organization. • Categorize Systems: Classify systems based on criticality, operating systems, applications, and network devices. 2. Patch Identification: • Monitor Sources: Stay updated with information from software vendors, security bulletins, and industry groups about new patches and vulnerabilities. • Automated Tools: Use patch management tools or services that scan for available patches relevant to your systems. 3. Risk Assessment: • Evaluate Impact: Assess the potential impact of not applying a patch, including the risk of exploitation and the importance of the system. • Prioritize Patches: Rank patches based on severity, with critical security patches given top priority. 4. Patch Testing: • Test Environment: Deploy patches in a controlled, test environment that mimics the production environment to identify any potential issues. • Evaluate: Ensure that the patch does not disrupt system functionality or create new problems. 5. Deployment: • Scheduled Rollout: Plan the deployment of patches during maintenance windows to minimize disruption. • Automated Deployment: Use automated tools to deploy patches across the network efficiently. • Staggered Deployment: Implement patches in phases, starting with less critical systems, to monitor for any adverse effects before wider deployment. 6. Verification: • Post-Deployment Testing: Verify that patches have been applied correctly and systems are functioning as expected. • Compliance Checks: Ensure all systems are up-to-date with the latest patches. 7. Documentation and Reporting: • Maintain Records: Document the patch management process, including inventory changes, patches applied, test results, and any issues encountered. • Reporting: Generate reports to demonstrate compliance and to analyze the effectiveness of the patch management process. 8. Continuous Monitoring and Improvement: • Monitor Systems: Continuously monitor systems for new vulnerabilities and ensure patches are consistently applied. • Review Process: Regularly review and improve the patch management process based on feedback and changing security requirements. Tools for Patch Management Automated Patch Deployment: Use tools to automatically detect and deploy security patches across systems, ensuring timely updates with minimal manual effort. Patch Testing & Rollback: Automate testing of patches before deployment and enable automatic rollback if issues arise, ensuring system stability. Risk-based Patch Prioritization: Automate the prioritization of patches based on the severity of vulnerabilities, addressing critical issues first. Continuous Vulnerability Monitoring: Set up automated tools to continuously scan for missing patches and vulnerabilities, ensuring ongoing security. Automated Reporting & Compliance: Automate patch status reporting to maintain accurate records for compliance and audits, reducing manual tracking. Subscribe to Vendor Security Bulletins: Regularly monitor and subscribe to security alerts and advisories from software and hardware vendors to receive timely updates on patches and vulnerabilities. Follow Cybersecurity News Outlets: Stay updated by following trusted cybersecurity news websites, blogs, and social media channels that report on the latest threats, breaches, and patch releases. Join Security Forums and Communities: Participate in cybersecurity forums and communities (e.g., Reddit, Stack Exchange, or industry-specific groups) where professionals share insights on emerging threats and patch updates. Use Threat Intelligence Feeds: Leverage real-time threat intelligence feeds that provide updates on new vulnerabilities and exploits, helping you stay ahead of potential risks. Set Up Automated Alerts: Configure automated alerts through security tools or threat intelligence platforms to notify you of new patches or vulnerabilities affecting your environment. Schedule Regular Backups: Set up automated, scheduled backups for all critical systems and data, ensuring up-to-date recovery points before patching. Test Backups Regularly: Periodically test backup integrity and recovery procedures to verify that backups can be successfully restored in case of issues post-patching. Backup Critical Data First: Prioritize backing up essential data, configurations, and system settings, especially for servers and databases that are vital for business continuity. Use Versioned Backups: Implement versioning for backups so you can roll back to a previous state if a new patch causes issues. Create Backup Snapshots: For virtualized environments, use snapshots or images of the system state right before applying patches to allow quick rollback if necessary. Store Backups Offsite or in the Cloud: Ensure backups are stored securely offsite or in the cloud to protect against local hardware failures or data corruption during patching. Advance Notice: Provide users with ample notice (at least a few days) before patching begins, outlining the scheduled time, expected duration, and any system downtime. Clear Communication Channels: Use clear and consistent communication channels (email, intranet, or internal messaging platforms) to inform users about patching schedules and updates. Describe Impact: Explain the potential impact on users, such as system slowdowns, service interruptions, or application downtime, and offer alternative solutions if necessary. Offer FAQs and Support: Share a FAQ document addressing common concerns and provide contact details for IT support in case users experience issues post-patch. Regular Updates: Send periodic reminders leading up to the patching date and notify users once patches are successfully applied, including any changes made. User Feedback: Encourage users to report any issues or unusual behavior after patching, providing a channel for quick feedback and resolution. Regular Reviews: Periodically review patch management policies and procedures to adapt to new threats and technologies. Evaluate Current Processes: Regularly assess your patch management processes to identify inefficiencies, gaps, or areas for improvement based on recent experiences or incidents. Stay Aligned with New Threats: Keep track of emerging cybersecurity threats and update patch management policies to address vulnerabilities from new attack vectors or zero-day exploits. Adapt to Technological Changes: Review and update your patch management approach to accommodate new technologies, such as cloud services, IoT devices, or software-defined networks, that may require different patching strategies. Incorporate Feedback: Collect feedback from IT staff, end-users, and security teams to understand pain points and areas for enhancement, and integrate these insights into your policies. Compliance Updates: Ensure your patch management procedures align with evolving industry standards and compliance requirements (e.g., GDPR, HIPAA, PCI-DSS) to avoid potential penalties. Effective patch management is crucial for maintaining the security and stability of an organization's IT infrastructure. By following a structured process and leveraging appropriate tools, organizations can minimize the risk of vulnerabilities and ensure their systems are protected against the latest threats. Patch management refers to the process of systematically discovering, acquiring, testing, and installing updates (patches) to software, particularly apps and operating systems, on enterprise endpoints. In the context of Mac computers, it means keeping macOS and installed applications up-to-date with the latest fixes and improvements released by Apple and third-party software vendors. Effective patch management helps to ensure that systems stay secure, stable, and usable over time. It is one of an IT admin's most critical responsibilities. Types of Software Patching There are three main types of software patches. Security Updates Security updates are patches designed to fix vulnerabilities in software that malicious actors might otherwise exploit. They are typically time-sensitive and protect against potential security breaches, data theft, and system compromises. Feature Updates Feature updates introduce new functionality or enhance existing software features. While not as urgent as security updates, these patches can improve the user experience, productivity, and compatibility with newer technologies. Bug Fixes Bug-fix patches address specific software issues that may cause crashes, errors, or other unexpected and unwanted behavior. These updates improve system stability and reliability, often resolving specific problems reported by users or identified through testing. Why Is Patch Management Important? Patch management is crucial for several reasons: Security: Regularly applying patches helps protect systems from known vulnerabilities, reducing the risk of successful cyber attacks. Stability: Updates often improve system performance and prevent crashes or data loss, which can, in turn, improve your organization's productivity. Compliance: Regulatory requirements in many industries frequently mandate that you have some way of keeping systems up-to-date to maintain data security and privacy. Cost Savings: Proactive patching can reduce IT support costs by preventing problems before they occur. How Does Applying Software Patches Help with Security? Software patches play a vital role in maintaining the security posture of Mac computers: Vulnerability Mitigation: Patches address known security vulnerabilities, closing potential entry points for attackers. Zero-Day Protection: Rapid deployment of patches can protect against newly discovered threats before they can be widely exploited. Malware Prevention: Updated systems are better equipped to resist malware infections and other malicious activities. Data Protection: Security patches often include improvements to encryption and data handling, safeguarding sensitive information. Network Security: Patched systems are less likely to become compromised and used as entry points to the broader network. What Is the Patching Process? The patching process for Mac computers typically involves the following steps: Inventory and assess: Identify all of the Mac devices in your network; catalog the software (and their current versions) that's installed on them; determine which systems need to be updated. Acquire patches: Monitor Apple's software update channels and third-party vendor announcements, and download necessary patches only from trusted sources. Test: Create a test environment that mirrors your production systems, apply patches to your test machines to verify functionality, and check for compatibility issues with critical applications. Schedule: Plan the timing of your patch deployment based on urgency and potential impact, and communicate that calendar to to users and other stakeholders. Deploy: Use your MDM solution or Apple's built-in software update mechanisms to deploy patches; consider staging the rollout incrementally to isolate and minimize potential disruptions. Verify: Confirm that the patches were successfully installed across all of the targeted devices; monitor those devices for any issues or anomalies that crop up after the patch is applied. Report: Generate reports on patch status and compliance; document any issues you encountered and how you resolved them. Review and Optimize: Analyze the patching process to identify ways it could be improved, then adjust your policies and procedures accordingly for the next time. Best Practices for Patch Management To ensure effective patch management for Mac computers, consider the following best practices: Establish a patch management policy: Create a formal policy outlining who's responsible for what and what their patching procedures should be. Automate as much as possible: Utilize MDM solutions and built-in macOS features to automate the discovery of available software updates and their subsequent deployment. Prioritize: Focus on the security patches and updates for your organization's most critical applications first. Maintain a regular schedule: Establish a consistent patching cadence, to make sure that systems are updated regularly. Test thoroughly: Always test software updates in a contained, controlled environment first before deploying them more widely. Monitor and report: Implement systems to track patch compliance and generate reports for auditing purposes. Educate your users: Inform end-users about the importance of updates and how to manage them on their devices. Plan for rollbacks: Have a plan in place for reverting patches if unexpected issues arise after you deploy them. Keep documentation updated: Maintain detailed records of the patches you've deployed, the results of your testing, and how you actually ran the deployment. Stay informed: Regularly review Apple security bulletins and stay current with industry best practices. How MDM Solutions Can Streamline Mac Patch Management Mobile device management (MDM) solutions can play a critical role in simplifying and automating patch management for Mac computers in enterprise environments: Centralized control: MDM platforms provide a single interface to manage updates across all enrolled Mac devices. Automated deployment: Schedule and push updates to multiple devices simultaneously, reducing manual intervention. Granular policies: Create custom policies to deploy updates based on device groups, user roles, or other criteria. Compliance monitoring: Easily track which devices are up-to-date and which require attention. Remote management: Apply patches to off-site devices without requiring physical access. Reporting and analytics: Generate comprehensive reports on patch status, compliance, and deployment success rates. User self-service: Empower users to install approved updates through self-service portals. Bandwidth management: Schedule update downloads to optimize network performance, especially during large deployments. Testing and staging: Facilitate phased rollouts by targeting specific device groups for initial deployment. Patching and updating devices can be a hassle and can cause business disruption. Yet, unpatched vulnerabilities provide attackers with open opportunities to cause great damage — with studies showing unpatched vulnerabilities estimated to contribute to 30-60% of all breaches! A patch management policy formalizes the fundamental IT requirement that all systems and software should be patched and updated in a timely manner with rules that explain the requirements for patching and updates, clear processes that can be followed, reported on, and confirmed, and standards that can be tested and verified. This article can help organizations of all sizes start the process with a fundamental overview and a template: Also read: 11 Key Steps of the Patch Management Process To kick start any patch management policy development, eSecurity Planet has developed a template that can be downloaded and modified. Notes of explanation or how to use the template are enclosed [between brackets] and these sections should be removed from final drafts. Access the Sample Patch Management Policy Template. The sample patching policy contains many sections, but not all sections will be required for all organizations and others might require more details. See Common Patch Management Policy Segments below for more details. How to Create a Patch Management Policy in 4 Steps All security policies share the same four key steps to create a policy, and they are explored in detail in IT Security Policies: Importance, Best Practices, & Top Benefits. For a functional patch management policy, we summarized these steps as: Determine the Patch Management Policy: Identify responsible parties, who or what is covered, basic processes, validation methods, and reports; these often will be based on the current practices. Verify the Patch Management Policy: Formally check to ensure basic policy developed in step 1 satisfies the complete needs of the organization and any compliance requirements. Approve the Patch Management Policy: Draft official language and circulate the policy for approval by affected stakeholders and executives. Review and Modify the Patch Management Policy: Periodically review the policy to ensure it remains updated and continues to satisfy the evolving needs of the organization. Patch Management Policy Development Cycle Although the basics remain the same, patch management is a frequently regulated requirement and organizations will need to apply extra caution in verifying compliance requirements. Any rule that does not meet compliance requirements should be adjusted. For example, a fire department might apply patches quarterly in practice. However, they might find that their state's cybersecurity requirements require monthly patching and will therefore need to change their patching frequency to monthly to comply. Practical limitations also will be very important and the policy team should work with the patching team to test the rules. If the IT team cannot comply with standards and requirements with their current resources, should the organization adjust the rules or the resources? In the fire department example above, perhaps the volunteer fireman who used to apply the patches in their spare time will need to be replaced or assisted by a patch management tool or service that can meet the monthly regulatory requirements. Common Patch Management Policy Sections When writing your patch management policy, consider the required, recommended, and bonus (aka nice-to-have) sections. Required Policy Sections These core sections should be part of every policy related to patch management: Scope: What assets are covered by the policy and how to identify software and devices to be covered. Patch Management Authority: Who is in charge and responsible for the patch management policy and its execution. Patching Priority: How to determine the priority of patches and the basis for that determination based on severity, risk, and other factors. Patch Scheduling: The length of time between the patch release and the organization's installation based upon priority. Patch Management Preparation: Backups and other system preparation that needs to be in place in case a patch fails and systems need to be restored. Manual Patch Management: How to apply patches manually — especially for systems that require downtime for maintenance. Explain the process for scheduling and obtaining approval for business system downtime. How to Handle Exceptions: Some patches will fail, some will cause business disruption, and some will simply not be needed. Explain how to recover systems and track exceptions and the process for mitigations to protect open vulnerabilities. Patch and Update Reporting: How to measure success and compliance with patch management with reports, including how and what to report. Recommended Policy Sections These sections help to flesh out the patch management policy with additional rules to protect the organization and to help prepare the IT department: Asset List: A list of resources or links to asset lists to help define the scope of systems and software tracked for patching and updating. Patch and Update Acquisition: Outline where to obtain valid patches and updates. Patch Testing: Test environments or testing of patches to verify they work and do not affect other business systems. Automated Patching: Organizations often express a preference for automated patching processes to reduce patching delays and burdens for IT teams. Audit Controls and Management: Outline what reports, logs, and information can satisfy internal and external auditors to track patch management success and verify patches have been successfully applied. Enforcement: Penalties to the IT department for failure to execute the patch management process, penalties to employees that interfere with the patch management processes, and how to handle assets that do not comply with the patch management policy. Distribution: Who must or should receive the patch management policy. Policy Version: Tracking versions and approvals of the patch management policy. Bonus / Nice-to-Have Policy Sections These sections do not change the core elements of the patch management policy, but can make the policy more usable or comprehensive: Overview: sets expectations and goals for the policy. Compliance Appendix: Copies or links to relevant compliance frameworks with which the organization must comply. How to Deal With BYOD and personal equipment. Top 5 Patch Management Policy Best Practices All security policies share the same five best practices to create a policy, and they are explored in detail in IT Security Policies: Importance, Best Practices, & Top Benefits. For a functional patch management policy, we summarize these steps as: Focus on What to Do, Not How: By focusing on goals and objectives, a policy can set standards while allowing the patch management team the flexibility to determine the best solution to meet those goals and objectives. Make Policies Practical: The patch management team needs to be able to understand and implement the policy. Right-size Policy Length: Too short and the policy may not have sufficient requirements to be verified; too long and the policies may become over prescriptive or hard to understand. Keep Policies Distinct: Overlapping policies can introduce conflicts or become more difficult to keep current. Make Policies Verifiable: Effective policies require reports that prove the policy is both in place and effective. The eSecurity Planet template seeks to be more comprehensive than some organizations may need, so every organization should review the template and add or remove content to fit their needs. Beyond the standard best practices, patch management benefits from additional considerations. For example, when making patch management policies practical, use existing resources such as the Common Vulnerability Scoring System (CVSS) to determine risk and prioritize patches, but balance those resources with consideration of the organization's specific context. For example, some organizations only patch vulnerabilities with a score of 7 or above. Yet these ratings only show the risk of the vulnerability and must also be combined with the likelihood of exploitation and the value of the asset to the organization. A data exfiltration bug of 8.0 on the marketing web server that only contains publicly released documents shouldn't have higher priority than a 6.5 remote code execution vulnerability on the server with the company's Active Directory (AD) services. The impact to the organization of a fully compromised AD simply would be too great to risk even modest possibilities of exploitation. As a special consideration for patch management, many organizations deploy automated tools. These solutions work well and should be used; however, they tend to focus on certain parts of the IT ecosystem such as operating systems and common software such as Microsoft Office or Adobe Acrobat. Tools often lack comprehensive coverage of third-party applications, firmware, internet-of-things (IoT) devices, networking equipment, backup applications, and more. The policy should not rely upon the tools or a patch management service to determine the asset list for the patching policy. The IT department must ensure that all resources that need patches are tracked and patched, even when applying the patch is difficult or may require manual patching. Top 6 Benefits of an Effective Patch Management Policy Many organizations feel that their undocumented patch management processes will not be improved by taking the time to put them into writing. However, this attitude overlooks six key benefits to any security policy: IT Hardening: The process of creating or reviewing security policies forces the evaluation and potential improvement of security practices. Employment Defense: Compliance with an executive-approved written policy provides coverage for the IT and security team in the event of a breach. Executive and Board Member Peace of Mind: Executive stakeholders can easily understand the organization's security posture from plain-language reports required by effective policies. Litigation Protection: Reports and other evidence showing compliance with policies that encompass reasonable security efforts can provide protection against lawsuits and regulators in the event of a breach. Compliance Easy Button: Policy-required reports will automatically be available for auditors if the policy already encompasses the compliance requirements. Improved Operational Efficiency and Resilience: Effective policies, especially patch management policies, can detect end-of-life assets and ensure the installation of the latest features for ease of use and capabilities. A good patch management policy can provide a helpful checklist to help create an efficient, and reliable patch management process. The reduced cybersecurity risk from the patching and the improved communication from the reports will improve overall business processes and executive confidence. However, patching cannot solve all problems. Patch management does not cover whether or not an organization has the correct software in place for their needs or if the software settings are properly configured. Patch management policies provide a helpful part of an overall cybersecurity program but need to be combined with other critical policies and strategies to ensure a resilient organization. More information on Patch Management and Related Topics: Patch management tools are essential for maintaining the security and efficiency of IT systems in 2025. These tools automate the process of identifying, testing, and deploying software updates and security patches across various operating systems and applications. Top contenders in the market include NinjaOne, Automox, Kaseya VSA, ManageEngine Patch Manager Plus, SolarWinds Patch Manager, and Ivanti Patch Management. These solutions offer features such as automated patch deployment, support for multiple operating systems (Windows, macOS, and Linux), third-party application patching, customizable deployment policies, and detailed reporting capabilities. Many of these tools provide cloud-based solutions, eliminating the need for on-premises infrastructure and allowing for remote management of endpoints. They also offer intuitive interfaces, real-time monitoring, and compliance reporting to ensure systems are up-to-date and secure. Some solutions, like NinjaOne, even include additional features such as remote remediation tools and asset management capabilities. SolarWinds: Robust patch management with automated discovery and deployment capabilities. Kaseya VSA: Integrated patch management and IT automation for streamlined updates. ManageEngine Patch Manager Plus: Comprehensive automated patch management for Windows, Mac, and Linux. Endpoint Central: Unified endpoint management with extensive patching features for multiple platforms. Pulseway: Mobile-first patch management solution for remote IT monitoring and management. ConnectWise: Integrated patch management with IT automation for comprehensive system updates. Acronis: Cyber protection platform with integrated patch management and backup. Datto, Inc.: Comprehensive patch management with backup and disaster recovery integration. Ivanti (formerly Landesk): Advanced patch management with real-time endpoint vulnerability assessment. Jamf: Specialized patch management for Apple devices, ensuring timely updates. VMware: Centralized patch management for virtualized environments and VMware products. GFI LanGuard: Network security scanner with comprehensive patch management. BigFix: Real-time visibility and control over patch deployment across diverse environments. SysAid: Integrated ITSM with automated patch management for improved security. Salt: Scalable configuration management and patching with SaltStack automation. Patch Management ToolsFeaturesStand Alone FeaturePricingFree Trial / Demo1. SolarWindsWatching the networkChecking on performanceWatching over servers and appsKeep track of logsManaging how networks are set upComprehensive patch management with real-time monitoring.Pricing starts at $199 monthly.Yes2. Kaseya VSAManagement of mobile devices (MDM)Management of assetsLooking at reports and dataKeeping track of complianceThe service desk and the ticketsUnified IT management with automated patching.Starts at $1,100 annually.Yes3. ManageEngine Patch Manager PlusTake care of patchesAssessment of vulnerabilityEndpoint safetyPatch release that is automatedUpdates for third-party appsAutomated patching for diverse environments.Starts at $245 annually.Yes4. Endpoint CentralManagement of mobile devices (MDM)Management of security data and events (SIEM)Controlling access to a network (NAC)Running a VPNControl of a remote machineEndpoint management with robust patching capabilities.Starts at $345 annually.Yes5. LandeskSelf-service platform for usersManagement of mobile devices (MDM)Virtualization of applicationsSetting up and deploying an OSScripting from afarIntegrated patch management for enterprise environments.Custom pricing, contact sales.Yes6. JamfApple services can be used togetherEnrolling and setting up a devicedistribution with no touchReset your password yourselfManaging the classroomApple device management with seamless patching.$3.33 per device monthly.Yes7. VMwareInfrastructure that is hyper-convergedAutomating and putting togetherManaging multiple cloudsStorage based on softwareManagement of endpointsVirtual environment patching with automation.Custom pricing, contact sales.Yes8. GFI LanGuardAutomation and making plansManagement of configurationsScanning the databaseSupport for virtual environmentsDashboards that can be changed.Network security scanner with patch management.Starts at $26 per node.Yes9. BigFixAbility to grow and be reliableDashboards that can be changedInformation about threatsManaging the lifecycleHandling the cloud.Scalable patching for large enterprises.Custom pricing, contact sales.Yes10. SysAidManagement of incidents and problemsDealing with changeList of servicesDealing with contractsControlling access and proving who the user isIT service management with integrated patching.Starts at $1,211 annually.Yes11. SaltHow to handle packages and appsSending out filesManagement of secretsAutomation of networksAdding third-party tools to the mix.Configuration management with robust patching.Custom pricing, contact sales.Yes12. PulsewaySupport for many platformsControl of a remote machineSafety and following the rulesControlling access based on rolesDashboards that can be changed.Mobile-first IT management with patching.Starts at $65 monthly.Yes13. ConnectWiseAutomation for professional services (PSA)Management and tracking from afar (RMM)The helpline and the ticketsAutomation of sales and CRMTaking care of projectsIT management with automated patch deployment.Custom pricing, contact sales.Yes14. AcronisStorage in a hybrid cloudReplication of backupControl of versionsKeep data centers safeSupport for multiple platforms.Data protection with integrated patch management.Starts at $59 per device annually.Yes15. Datto, Inc.Backup and rescue from disastersKeeping business goingNetworking in the cloudManagement and tracking from afar (RMM)Share and sync filesMSP-focused patch management and backup solutions.Custom pricing, contact sales.Yes SolarWinds SolarWinds Patch Manager simplifies patch implementation in extensive networks and virtual environments with its versatile and scalable automatic patch management software that interfaces with third-party apps. Patch Manager uses Microsoft WSUS and pre-built and pre-tested packages to distribute patches reliably. It also offers configurable alarms and scheduled patch reports. Wake on LAN improves software scan security by reactivating sleeping devices and turning them off afterward. It monitors and manages third-party software, virtual machines, and Adobe and Java fixes, surpassing WSUS and SCCM. Companies can eliminate software vulnerabilities and manage security with real-time security monitoring and thorough compliance reporting. IT managers must keep up with software patches to keep networks secure and efficient. SolarWinds Patch Management helps. What Is Good?What Could Be Better?SolarWinds products are adaptable because they work with various tools and systems.Navigating the software can be initially challenging, but becomes easier with repeated use.SolarWinds regularly releases updates and patches to improve performance and safety.Dependency on WSUS brings along the associated problems linked to that platform.Many SolarWinds products can monitor cloud resources, making hybrid and multi-cloud systems more accessible to manage.Users can configure alerts and automated replies in SolarWinds to fix issues quickly. Kaseya VSA Kaseya VSA automates and streamlines device and operating system software and security patch deployment. The software automatically discovers and applies missing updates on target devices, supporting many software applications, operating systems (Windows, macOS, Linux), and third-party apps. Patch scanning and inventory detects all patches, checks endpoints for missing updates, and keeps a complete inventory of installed software and patch levels to monitor all managed devices. Kaseya VSA administrators manage patches. They authorize patches before distribution, create patching procedures, and schedule company and customer-specific installs. Prioritizing critical updates for immediate deployment resolves security issues and provides flexible patch deployment options for various scenarios. The program permits automated, manual, and patch deployments during non-business hours to minimize disruption. What is Good?What Could Be Better?Provides a single pane of glass for all systems' update statuses, rollouts, and approvalsThe interface can be a little sluggish at timesEnables more effortless third-party software patchingComplicated and challenging report-building processGather an aggregate of computer information from endpointsVery easy to connect to users remotely to help troubleshoot ManageEngine Patch Manager Plus ManageEngine Patch Manager Plus automates Mac, Linux, and Windows endpoint security and offers patching for 850+ third-party programs. The software is available in on-premise and cloud versions, and a free version is available for small enterprises. Patch Manager Plus offers service pack deployment, third-party patch management, server application, patch reporting, active directory authentication, and more. ManageEngine Patch Manager Plus supports straightforward installation and a simple interface. It streamlines patch compliance. This comprehensive utility makes patching easy, keeping your environment secure and up-to-date. Say goodbye to patch management tool complexity and embrace a streamlined approach that saves time, improves security, and achieves corporate goals. What is Good?What Could Be Better?Comprehensive patch management for various operating systems, applications, and third-party software.It is complex for new users and requires time and training to utilize its functionalities fully.Advanced analytics and audits for effective monitoring and decision-making.Initial setup and configuration efforts to align with specific environments.Customizable deployment policies to align with specific business needs.Centralized patch management for streamlined operations. Endpoint Central Endpoint Central is an automated tool for patch management that supports Windows, Mac, Linux, and third-party applications. Critical features of Endpoint Central include a user-friendly dashboard, an updated vulnerability database, periodic patch scanning, system health policies, automated antivirus updates, the ability to decline patches for specific applications, and the option to disable automatic updates. Endpoint Central uses a central patch repository maintained by Zoho Corp, which is regularly synchronized with the client's server. Scanning for missing patches is done automatically, and system health can be classified based on patch status. The tool simplifies antivirus updates and allows administrators to schedule them to reduce bandwidth consumption. It also enables patch testing and automated approval with configurable installation options. What is Good?What Could Be Better? Seamless integration with Service Desk Plus.Lack of a function to link deployment packages and templates.User-friendly software deployment templates.Negative impact of COVID-19 pandemic on companies and economic balance.Remote troubleshooting and support.Efficient Microsoft Updates management. Landesk Landesk Patch Manager is essential for system security. 39% of firms experience software-related security problems. Application patching is essential, with Oracle Java responsible for 50% of vulnerabilities, Adobe Reader 22%, browsers 13%, and others 15%. 0% of vulnerabilities have patches, and 86% are in third-party apps. According to Gartner, over 90% of security exploits target known vulnerabilities. Patching challenges include overwhelming vulnerabilities, network performance, user complaints, and time limits. LANDESK Manages Patches and Task awareness and coordination. One console for system and security administration. Maintain user experience using existing deployment mechanisms. Automatic patch downloads, more accessible remediation, adjustable settings, self-service patching, and flexible reboots. What is Good?What Could Be Better?Robust patch management capabilitiesDifficulty finding support and documentationEffective patching to enhance system securityUsability concerns with Administrator Console InterfaceUser-friendly self-service software installation via Ivanti PortalPowerful vulnerability management features When finding software patches is no longer necessary, Jamf's patch management system saves time. This blog covers App Lifecycle Management, which helps IT professionals safeguard environments. Patching keeps the software current. However, with increasing threats and the use of many devices, implementation is complex. Some reduce updates or omit patching because legacy methods are tedious, while old methods, like manual patching, continue. Jamf Pro's App Installers protect Mac fleets by simplifying macOS patching. App Lifecycle Management simplifies Patch Policy Workflows and App Installers. Eliminating lengthy reports, scavenger hunts, and eligibility requirements modernizes change management. Jamf's App Lifecycle Management streamlines patch deployment with reporting, notifications, and policies. Best practices include an intuitive user experience, visibility, analysis, and correction. Patching macOS games improves performance and user experience. What is Good?What Could Be Better?Powerful and user-friendly MDM solution with easy app and policy management.A lack of timely fixes for issues and problems was reported.Excellent reporting capabilities for valuable insights and data analysis.Lengthy support resolution times, often citing known issues as the cause.Swift support for new operating systems ensures timely updates.Comprehensive training options for smooth operations and system understanding. VMware Introducing VMware Update Manager. Update Manager automates VMware vSphere patch and version management. Supporting ESXi hosts and virtual machines simplifies host upgrades, third-party software installations, and hardware changes. Update Manager requires VMware vCenter Server access. The server and client components are compatible with the vCenter Server on Windows or the Appliance. Update Manager must be installed on a Windows PC, either with the server or separately, for vCenter Server. One vCenter Server per Update Manager instance. After vSphere 6.5, Update Manager cannot be registered to a vCenter Server Appliance during installation. Update Manager is available in the vSphere Web Client (Flex) and Client (HTML5). Adobe Flash Player is no longer recommended, so use vSphere Client. Since vSphere 6.7 Update 3m, the Update Manager client is available in the vSphere Client regardless of Windows server component installation. What is Good?What Could Be Better?Robust troubleshooting with vRealize for quick issue resolution.Sluggish web-based client performance and usability challenges.Scalability without impacting business applications.Limited knowledge base and documentation.Seamless upgrades with ThinApps for in-house software.Non-disruptive patching during production hours. GFI LanGuard Organizations need a comprehensive patch management solution like GFI LanGuard to maintain system security and stability. It streamlines device and application software updates and patch management, and its automated patch distribution is crucial. Automation saves IT teams time and effort when deploying patches. The solution analyzes the network and installs missing fixes on devices. GFI LanGuard conducts frequent vulnerability evaluations to discover system and application security vulnerabilities. It delivers thorough information and prioritizes vulnerabilities by severity, helping organizations take precautions. In addition to operating systems and standard apps, GFI LanGuard supports third-party software, expediting the patching of critical application vulnerabilities and improving security. GFI LanGuard's post-patch scans verify patch deployment and confirm the correct patch application. The solution can roll back updates to fix problems and preserve system stability. Another critical feature of GFI LanGuard is centralized management. What is Good?What Could Be Better?User-friendly interface and streamlined workflow.Potential information overload, leading to noise in displayed data.Robust reporting capabilities with specialized regulation-specific reports.Challenges with timeouts during extensive updates on remote PCs accessed via VPN.Thorough machine scanning through agent installation for vulnerability detection.Continuous updates for non-Windows applications and proactive update notifications. BigFix Patch IT Operations and Security teams can automate endpoint identification, management, and remediation using IBM® BigFix Patch, independent of the operating system, location, or connectivity. This unified and near-real-time visibility and enforcement helps deploy and manage fixes across remote endpoints. BigFix Patch automates patching for hundreds of thousands of endpoints, regardless of device, location, connectivity, or condition. Flexible, near-real-time monitoring and reporting improve patch compliance visibility. HCL content simplifies patching for almost 100 operating systems and variants on the platform. BigFix Patch reduces vulnerability windows and patch time from weeks to hours, delivering over 98% first-pass success. It integrates across the company and scales easily, managing 300,000 endpoints per management server. What is Good?What Could Be Better?Comprehensive multi-platform support.Configuration and implementation complexities.Robust endpoint security and patching.Delayed communication between workstations and servers.Supportive implementation partner.Valuable patch management and inventory control. SysAid The comprehensive SysAid Patch Management software automates and improves patching. It shows appropriate patches for active IT assets and customizes patch management. It also allows manual patching of individual or multiple assets with progress and outcomes tracking. No credit card is needed to try SysAid's demo. Over 10,000 firms use SysAid's Asset Management, Change Management, and Third-Party Integrations to improve performance and service. SysAid Patch Management solution is fully automated and scalable, with easy setup and high configurability. It works perfectly with SysAid Help Desk and ITSM, available in the cloud and on-premises. Microsoft, Adobe Flash, Mozilla Firefox, Google Chrome, Java, and others are supported. It also works with SysAid Change Management to document and comply with internal and external regulations. SysAid Patch Management uses OEM technology to execute server instructions and interface with the OEM cloud via an agent proxy. What is Good?What Could Be Better?Comprehensive Asset InventoryChallenges in communication and understanding with the companySuperior and easy-to-use ITSM solutionDifficulty in filtering customized fieldsModern interface for end-users and administratorsExcellent sales and technical support Salt Salt Patch Management is a complete software patch manager. It automates patch deployment, centralizes management, and monitors compliance. Custom policies, testing, and rollback provide efficient patch administration. Vulnerability scanner integration prioritizes critical updates. Reporting and audits reveal patch deployment status. Salt Patch Management supports multiple operating systems and is scalable. It improves cybersecurity, risk mitigation, and IT infrastructure stability. SaltStack is an open-source configuration management and automation system that provisioned, changed, and installed software on physical, virtual, and cloud servers. It automates tasks, reduces errors, and enables DevOps. Salt is distinguished by its speed, scalability, and event-driven design. A secure, bidirectional communications network enables agent-based or agentless modes. Salt's reactors, minions, grains, and pillars give system administrators flexibility and abstraction. What is Good?What Could Be Better?SaltStack is very flexible and can manage many systems and devices.SaltStack has so many advanced features that it can be challenging for new users to learn how to use it.It uses the ZeroMQ communication protocol, a fast and effective way to send and receive data.Some features might only be in the Enterprise version, which costs money.YAML can be used to define infrastructure configurations as code.Allows remote commands to be run on multiple systems at the same time. Pulseway Pulseway Patch management is crucial and complicated for IT professionals due to the volume of patches and expanding endpoints. Pulseway's Patch Management simplifies this work and keeps systems and apps updated. Pulseway has 400+ 5-star ratings and sent 750M notifications after managing over 950k systems and 6,000 delighted clients. The mobile-first solution lets technicians do vital IT operations anytime, anyplace. Since 2011, Pulseway has provided a user-friendly, cloud-hosted service via its mobile app. Pulseway began as Mobile PC Monitor, MMSOFT Design Limited's

mobile-first IT management software. Since then, system administrators, IT consultants, and managed service providers have used it over 300,000 times. The app allows remote management on iOS, Android, Windows, and Windows Phone. What is Good?What Could Be Better?Simplifies software and tool deploymentLimited graphical user interface (GUI)Offers scripting capabilities for automationThe learning curve for new usersProvides remote control functionalityCustomizable alerts and monitoring policies ConnectWis With ConnectWise Automate's comprehensive remote monitoring and management solution, IT pros may proactively support customers and networks. Automate's asset identification, endpoint management, patch management, remote monitoring, and IT automation make it an essential tool for IT workers. The documentation collections make automated setup and installation easy. The user-friendly Web Control Center has many functions to improve efficiency and operations. Agent deployment covers agent installation and is one of Automate's best features. This allows effective monitoring of the agent system and other network devices, revealing hardware consumption and system performance. Automate prioritizes patch management, a crucial IT maintenance task. Teams may automate patching across numerous workstations using the platform's patch management, which provides patch approvals, policies, and more. Automate simplifies patch management for Microsoft and third-party software. What is Good?What Could Be Better?ConnectWise Automate helps manage Microsoft updates and allows remote troubleshootingThe fat client is unstable, but they are working on a web client.Provides event monitoring and alerting features.The web client doesn't have all the features of the fat client.Integrates well with ConnectWise Manage for streamlined operations.Handles patching and software version control effectively. Acronis Discover Acronis Advanced Management, a powerful endpoint management solution that automates, intelligently, and integrates with Acronis Cyber Protect Cloud. With machine learning, it elevates monitoring by predicting and preventing system issues. Real-time detection and monitoring of 24 Windows and macOS parameters and profiling-based anomaly identification are easy. Automated remediations and configurable notifications eliminate manual interventions. Allow your team to quickly troubleshoot remotely using Remote Desktop assistance. Despite slow networks, Acronis Advanced Management's increased MacOS and Linux support assures platform compatibility. Instant one-time help and screenshot transmission are now accessible. Provide top-notch endpoint management with Acronis Advanced Management. Use its software inventory reporting, multivendor drive health monitoring, and pre-integrated backup and security. What is Good?What Could Be Better?Acronis offers many different ways to back up, such as full system, file, disk, and cloud backups.Acronis solutions can be pretty pricey, especially if they have a lot of extra features.Acronis has features that protect against ransomware attacks and make it easy to get back data that has been locked.The free version of Acronis isn't as good as the paid versions in some ways.The solution encrypts backed-up data and stores it in a safe place.Acronis has easy-to-use interfaces and set-up procedures. Datto, Inc. Datto, Inc Patch management software is essential as cybercriminals look for application vulnerabilities. A complete patching tool that automates the process can improve efficiency and reduce risks for MSPs, establishing end-user trust. A sophisticated built-in patch management solution in Datto RMM gives MSPs precise insights into potentially at-risk apps and devices. Administrators can use an automated technique to patch several systems simultaneously, saving time. It also automates patching based on policies, reducing manual intervention. Datto RMM's reporting and search tools show implemented patches, missing patches, and failed deployments. MSPs need an effective patch management solution to secure their clients' systems against breaches. Using Datto RMM's built-in patch management software, MSPs may create customized patch scheduling strategies and reduce business disruptions. What is Good?What Could Be Better?Simplified device organization and management.Terrible hardware quality, particularly in routers and devices.Effective patch management tool for Microsoft and third-party applications.Slow and unresponsive web remote interface.Automation features for time-saving operations.Integration with other tools like Autotask and ConnectWise Manage. Datto, Inc. – Trial / Demo Patch Management is the process of becoming aware of, and applying, the latest software updates to your Operating System (OS) and Applications (Apps) across your organisation's devices. Why is Patch Management important? The Operating System (OS) of your device, whether a smartphone, tablet or computer, is instrumental in keeping your device reliable and secure. As with all software, your OS must respond to the latest online threats and adapt to the changing usage patterns of its users, so an OS will routinely be updated several times per year, with a combination of new features and security fixes. Similarly, the apps you use on your device will also receive similar, frequent updates. Commonly, these updates fix unreliable behaviour in the app or respond to security loopholes in the application's code. As implied above, failure to keep the software on your devices updated exposes you to online security threats. This may lead to you becoming the victim of data loss, a customer data breach, ransomware, and financial or identity fraud. Why is Patch Management difficult? For organisations with even a relatively small number of devices, each one will have an OS and the majority will have around 10 to 20 apps in regular use. Even with just 10 devices deployed, that might well be 200 potential update points to manage. If those apps are updated by their developers a modest estimate of 6 times per year, that's as many as 1200 updates that need to be executed in an organisation of just 10 devices. So, volume is a problem. Secondly, awareness and oversight are a problem. Without a tool to report on the software your devices have installed, or a set of policies to define which apps are allowed in your organisation, it is very laborious if not practically impossible to work out which apps need updating and which ones have done so automatically (or not). Finally, since many apps use their own bespoke update mechanism, there is no universal protocol for apps or operating systems to reliably send alerts about failed updates. Computer apps in particular can be installed in many different ways, some of which are better at automatically updating than others. Don't updates happen automatically? Yes and no. On the whole, updates to many apps can and will happen automatically. However, there are numerous exceptions: Some apps require user-interaction to complete; often these get deferred by the user It is often advantageous to defer brand new OS releases until their reliability is proven Some updates need admin privileges, which not all users should be allowed to have Apps may fail to auto-update and require manual intervention to fix Occasionally the auto-update process itself can fail to detect an update that is due Some apps do not have an automatic update mechanism at all For legacy systems, you may want to manually control or block updates to older apps With the number of updates per year typically in the thousands, even for the smallest organisations, it's very likely that on a significant number of occasions, one of the above exceptions will arise. How to deliver reliable Patch Management To get around the lack of a universal protocol for app updates, particularly on computers, we recommend use of an MDM (Mobile Device Management) system for Patch Management. Your devices will routinely check-in with the MDM, which will ask them to report their current list of installed software and the version numbers. For software that is installed and managed using the MDM itself (typically as part of a Zero-Touch Setup environment), in most cases the MDM will automatically update the OS and its applications. Our MDM solution can apply updates not only to App Store apps, but also to a large and growing number of additional third party apps as well. The MDM system hosts the installers and will keep your devices up-to-date whenever a new release becomes available. For software which be directly managed by the MDM but is nonetheless distributed by the MDM, Purple will receive an alert for any new releases. Then, we will update the installer package within your MDM environment so that all devices receive the latest version of that app. To implement Patch Management we will: Agree a major OS version for all your devices Set up an agreed maintenance window once per week when automatic OS updates will be attempted, then communicate this to your end users apps and set up a proactive update notification protocol Bring all device operating systems and apps up to date Agree a frequency of patch management checks The stricter compliance standards will require checks as often as every 2 weeks Perform a manual check and provide a report at the desired frequency Remediate any failed automatic updates Where available, update and deploy the manually-managed installer packages Windows devices are central to many work ecosystems, accounting for a significant portion of computers in use. In fact, there's a good chance (around 72%) that you're reading this on a Windows machine. Businesses benefit from the wide range of Windows devices available, from basic to high-end, to suit their diverse needs. However, ensuring these devices function optimally and remain secure throughout their lifespan is crucial. As such, when the Windows device fleet is large, it becomes increasingly difficult for the IT admins to ensure that enterprise devices remain secure against the latest cybersecurity threats. For instance, let's consider that Alex (for illustration purposes only), an IT administrator, has been tasked with ensuring that all Windows devices within his organization are up-to-date with the latest OS updates. Manually updating the patches on hundreds of devices is next to impossible, and he must carefully select the correct patches for each device. Uninstalling or reverting Windows patches may not always be possible. Unpatched vulnerabilities leave the system open to attacks, allowing hackers to steal corporate data and infect the network with malware. Considering the impacts of unpatched vulnerabilities, leaving the devices unpatched is not an option. Given the situation, Alex would need a centralized system to streamline the Windows patching process, with the following capabilities: 1. Continuously scan the Microsoft Catalog for newly released patches and vulnerabilities. Once identified, add them to the repository for validation and approval.2. Scan devices to identify those eligible for OS updates.3. Approve the patches to eligible devices.4. Provide an overview of the patch status and distribution. Having a robust Windows patch management software is not only critical for maintaining system integrity and security, but it is also a key compliance requirement for Information Security frameworks such as ISO 27001, HIPAA, and PCI DSS, etc. Are you an IT admin like Alex, looking for a seamless patch management solution for managing patches on Windows devices? Then look no further than SureMDM! In this blog, we will explain more about Windows patch management and how SureMDM can ease the IT admin's burden in managing OS updates. Windows patch management is a process of identifying, verifying, and deploying OS updates (patches) for Windows-based devices. These updates address security vulnerabilities, fix bugs, and improve system performance. Patch management goes beyond simply deploying updates. It involves ensuring the installation of the correct version, verifying their status, and confirming the continued smooth operation of patched devices. Well, with SureMDM you do not have to invest in a separate Windows patch management software. In addition to offering a range of features, SureMDM can also act as a Windows patch management solution. SureMDM has now consolidated Windows patch management under a dedicated OS updates section on the SureMDM console to enhance user experience. To make the experience hassle-free, SureMDM continuously identifies new patches and patches that enhance Windows OS performance. The identified Windows patches are then made pre-populated for the admins to deploy. The SureMDM device agent (Nix agent) scans eligible devices for Windows patching, helping the admins to effortlessly identify and deploy eligible updates on the devices. Patches can be downloaded from Microsoft servers or from cache servers or even from peers in the same network or office, if available, to save bandwidth. Admins can gather insights on installed/available patches and the date on which the patches were made available at a device level. SureMDM offers a comprehensive overview section which allows IT admins to gather detailed insights on missing, pending, and installed updates and take actions accordingly. You can get insights like: Patch Status: This chart visually represents the distribution of Windows patches across all devices. With this, you can identify the gap between installed and missing patches at a glance. Patch Distribution: This chart illustrates the distribution of Windows patches across different classifications, such as quality updates, security updates, and feature updates. It provides valuable insights into the types of patches applied and their current statuses (installed or pending) for each category. Patches Pending: See the trend of pending installations over a specified period (default: 30 days) to notice any patterns in the installation process. OS Updates Dashboard with detailed insights on missing, pending, and installed updates With the Overview table, you can view the list of patches (by Microsoft) confirmed as available and deployable by the SureMDM Agent. Discovered Updates table listing Windows patches along with details such as classification, KB article, eligible devices, etc. With the SureMDM Scanned Updates table, you can view the list of available, scanned patches that are yet to be installed. With the Microsoft Catalog Updates table, you can view the list of patches (approved by Microsoft) confirmed as available and deployable by SureMDM. Microsoft Catalog with list of OS updates to be added to the local repository With the Uninstall patch feature, SureMDM can now automatically detect Windows patches that are uninstallable and help you boost productivity by rolling back patches that hamper your application performance or end-users productivity. Uninstalling unstable Windows patches SureMDM lets admins configure compliance policies based on the Windows OS version. These policies can automatically take actions such as applying jobs, blocking devices, or locking them when devices fall out of compliance with the defined rules. This ensures all devices remain compliant with the organization's security standards. Establish a Regular Patch ScheduleSet a consistent patching schedule, such as weekly or monthly, and prioritize urgent patches for quick deployment. Stay updated with Microsoft's release schedule/Patch Tuesday updates to avoid missing critical updates. Test Patches Before DeploymentTest patches on selected devices to ensure compatibility with others. This helps prevent potential disruptions to critical infrastructure. Prioritize Critical PatchesPrioritize patches addressing security issues and critical performance issues, particularly zero-day exploits. Focus on high-risk systems, especially those exposed to the internet. Monitor and Verify Patch InstallationMonitor the installation process from the SureMDM patch management 'All Deployed Updates' dashboard. Verify successful updates and address any failures to ensure complete remediation. To summarize, with the latest enhancements, SureMDM helps IT admins to streamline Windows OS updates, ensuring that devices run on the latest versions. This not only helps identify and mitigate patch vulnerabilities but also strengthens the organization's overall security posture. Along with Windows, SureMDM offers OS update and patch management for iOS and macOS, and Linux devices. What is a Windows patch management software?A Windows patch management software helps organizations streamline the process of identifying, testing, and deploying patches or updates to Windows OS and applications. It ensures systems are secure, up-to-date, and protected from vulnerabilities. How different is Windows Update for an individual device from Patch Management?Windows Update is a feature built into the OS that automatically downloads and installs updates for the Windows operating system, including security patches, drivers, and feature updates.Patch Management is a broader process that involves managing and deploying patches not just for Windows but also for third-party applications, ensuring all systems are secure and up-to-date across an organization. Patch management provides more control and customization over when and how updates are applied. Why is Windows patching needed?Windows patching is essential to ensure system security, fix bugs, improve performance, and address vulnerabilities. Regular patching helps protect devices from cyberattacks, malware, and exploits that target outdated software, ensuring the stability and integrity of the operating system and applications. How often should you perform patch management for Windows devices?Patch management should be performed regularly to maintain system security and stability. Critical security patches should be applied immediately or within 24-48 hours. Non-critical patches and routine updates can be scheduled monthly, typically in line with Microsoft's Patch Tuesday. Additionally, continuous monitoring for new vulnerabilities and patches is recommended to ensure timely updates and minimize security risks. What are the different types of patches supported by Windows patch management solution?SureMDM Windows patch management solution supports different types of patches such as Critical updates, Definition updates, Feature packs, Security updates, Service packs, Update rollups, and Cumulative updates. What are the risks of not updating Windows patches regularly?Skipping Windows patches can leave your system vulnerable to security threats, cause software bugs or crashes, create compatibility issues, and risk data loss or compliance violations. Let us begin with an example that underlines the importance of patch management. Software vulnerabilities are real, irrespective of the business entity. One of the leading healthcare organizations providing data for more than 10 million people had an adverse situation in 2023. Their focus group revealed that while there was a nod to patch management, the prioritization was not taken seriously due to a lack of resources and perceived minimal risks. Therefore, like many other organizations, the healthcare company was attacked by cyber criminals who took advantage of an unlatched weakness, with the organization's network being penetrated by hackers. The consequence was becoming critical; a lot of money was lost on the ransoms, more time was wasted, and penalties from the authorities for disruptions in business operations were imposed. There was negative feedback from the public as individuals lost faith in the company, meaning fewer people visited the health facility. The organization performed a significant transformation of IT security management, focusing on patch management. The importance of patch management can be realized because its global market size has grown to $979 million in 2024. Flaw fixing reduces vulnerabilities that implement security breaches and guarantee operational order. Here, we will look at major points of the patching process, its significance, types of patches, the process, and some of the right methods in the organization. What is Patch Management? Patch management applies vendor-issued updates, known as patches, to software and systems to close security vulnerabilities and optimize performance. It is an essential task for IT professionals to ensure the security and stability of their IT infrastructure. The process typically involves several steps, including asset management, patch monitoring, patch prioritization, patch testing, patch deployment, and patch documentation. Each step is crucial in ensuring the effective management of patches and minimizing the risk of security breaches. Importance of Patch Management With the ever-evolving threat landscape, effective patch management is essential for organizations to protect their valuable data and maintain a secure and stable IT environment. 1. Security Enhancements Security patches, specifically designed to address security vulnerabilities, play a crucial role in protecting systems from potential cyber threats. Hackers can exploit software security vulnerabilities to gain unauthorized access to systems or launch malicious activities. By applying security patches promptly, IT professionals can close these vulnerabilities and minimize the risk of security breaches. Effective patch management ensures that the latest available patches are applied to systems on time, reducing the opportunity for hackers to exploit vulnerabilities and thus enhancing security. By staying updated with security patches, IT professionals can significantly enhance the security posture of their systems and protect valuable data from potential threats. 2. Performance Improvements Patch software improves the performance of software applications and systems and provides security enhancements. Software vendors often release patches that address hybrid or local network performance issues and optimize their products' functionality. By applying these performance patches, IT professionals can ensure that software applications run smoothly and efficiently, enhancing user productivity. Performance patches can address various issues, such as software crashes, slow response times, and memory leaks, which can negatively impact user experience and productivity. 3. Compliance and Regulations It is crucial for security and performance and ensuring compliance with regulations and reporting requirements. Many industries, such as healthcare, finance, and government, have specific regulations that organizations must abide by to protect sensitive data and maintain the integrity of their systems. Compliance and reporting requirements often include regularly patching software applications and operating systems to address security vulnerabilities. By implementing effective new patches, organizations can ensure that they meet these regulatory requirements and demonstrate their commitment to cybersecurity. Effective patch management tool provides organizations with the necessary documentation and evidence to demonstrate compliance during audits and assessments. Read Also: Windows Patch Management: 10 Best Practices You Should Know What are the Types of Patches Patches come in different types, each serving a specific purpose. Understanding the different types of patches can help IT professionals prioritize and apply patches effectively. The main types of patches include: 1. Security Patches Security patches are very crucial. They address security vulnerabilities in software applications and operating systems, playing a vital role in protecting systems from potential cyber threats and minimizing the risk of security breaches. Software vendors release security patches in response to identified security vulnerabilities. can exploit these vulnerabilities to gain unauthorized access to systems or launch malicious activities. By applying security patches promptly, IT professionals can close these vulnerabilities and enhance their systems' overall security posture. 2. Bug Fixes Bug fix patches are another important patch type in the patch management process. These patches address issues related to software bugs and glitches that impact software applications' functionality and user experience. By applying bug-fix patches, IT professionals can ensure that software applications are free from known issues and provide a seamless user experience. Bug fix patches can address various issues, such as crashes, performance issues, compatibility problems, and data corruption. By applying feature update patches, IT professionals can take advantage of the latest advancements in software applications and provide users with an improved user experience. Regularly updating software with feature updates ensures that organizations leverage their software investments' full potential. IT professionals should stay informed about the latest feature update patches released by software vendors and assess their relevance and impact on their systems. 4. Service Packs Service packs are comprehensive updates that include multiple patches, bug fixes, and feature updates for operating systems and software applications. Software vendors release these updates periodically to provide users with a consolidated package of improvements and enhancements. Service packs are particularly important for operating systems as they address various issues, including security vulnerabilities, software bugs, and performance optimizations. They offer a more comprehensive and efficient way to update software than applying individual patches. Patch Management Process The patch management process involves several steps that IT professionals should follow to effectively manage patches and ensure the security and performance of their systems. The main steps of the patch management process include: 1. Inventory Management Real time inventory management provides IT professionals visibility into the systems and applications requiring patching. It allows them to track each system's patch status and identify any missing patches or vulnerabilities. By maintaining an accurate inventory, IT professionals can ensure that all systems are included in the patch management process, minimizing the risk of overlooking critical patches or vulnerable systems. Inventory management also helps identify systems requiring additional attention, such as legacy systems or remote endpoints. 2. Patch Assessment Patch assessment is a critical step in the patch management process. It involves regularly scanning systems in real-time for missing patch updates and assessing each system's vulnerability status. Patch assessments help IT professionals prioritize and plan patch deployment. By identifying systems with missing patches or high vulnerability levels, IT professionals can ensure that critical patches are applied promptly to minimize the window of opportunity for hackers. Vulnerability management is closely tied to patch assessment. By assessing system vulnerabilities through patch assessments, IT professionals can prioritize patch deployment based on the severity and potential impact of the vulnerabilities. 3. Patch Testing During the patch testing phase, IT professionals should create a test environment that closely resembles the production environment. This environment should include representative systems and applications to simulate real-world scenarios accurately. By conducting comprehensive testing, IT professionals can identify potential conflicts or issues arising from the patch deployment. Patch testing should involve different types of testing, including functional testing, compatibility testing, and regression testing. Functional testing ensures the patched software continues functioning without new bugs or errors. Compatibility testing ensures the patch does not conflict with the environment's other software or hardware components. Regression testing helps verify that the patch does not introduce new issues or regressions into the system. 4. Patch Deployment Patch deployment involves the actual installation of patches on the target systems. Effective patch deployment requires careful planning and execution to minimize potential security risks. The deployment process should follow a standardized approach to ensure consistency and efficiency. IT professionals should prioritize patches based on their criticality and potential impact on the system's security. Critical patches that address high-risk vulnerabilities should be deployed soon to minimize the exposure window. Before deploying patches, IT professionals should ensure that they have a backup and recovery plan in place. This plan helps mitigate any potential issues during the deployment process, such as system crashes or data loss. It also allows for quick recovery if the deployment process encounters unexpected problems. Additionally, a reliable internet service provider (ISP) is crucial for maintaining consistent connectivity during the deployment process, especially when pushing updates across distributed networks or remote endpoints. A stable connection minimizes disruptions and ensures patches are applied swiftly and effectively. 5. Monitoring and Reporting Monitoring and reporting are crucial aspects of the patch management process. IT professionals should regularly monitor the patch compliance of their systems to ensure that all patches are applied and systems are up to date. They should also generate custom reports to track patch compliance and identify any vulnerabilities or gaps in the patching process. Generating custom reports is essential for tracking patch compliance and assessing the effectiveness of the patch management process. IT professionals should create reports that provide detailed information on patch status, deployment success rates, and any vulnerabilities or gaps in the patching process. These reports can help identify areas for improvement and prioritize future patch deployments. What are the 6-Step Patch Management Lifecycle? A successful patch management program follows a structured lifecycle that ensures patches are applied consistently, without disrupting business operations. Each step plays a critical role in keeping IT environments secure and fully optimized. 1. Scanning and Identification The process begins with scanning the IT environment to detect outdated software, missing patches, and vulnerable systems. Automated tools can simplify this step by continuously monitoring devices across networks. Without this visibility, organizations risk leaving hidden vulnerabilities unaddressed. 2. Assessment and Prioritization Not all patches carry the same level of urgency—some fix minor bugs, while others close critical security loopholes. During this step, IT teams assess the severity of vulnerabilities and prioritize deployment based on potential business impact. This ensures that resources are directed toward the most pressing risks first. 3. Acquisition and Testing Once patches are identified and prioritized, they must be acquired from trusted vendors or official sources. Before wide deployment, patches are tested in a staging environment to ensure compatibility with existing applications and configurations. This minimizes the risk of introducing new problems into production systems. 4. Deployment After testing, patches are carefully rolled out across the production environment. Many organizations follow a phased rollout strategy to reduce the chance of widespread disruptions. Deployment may be scheduled during maintenance windows to ensure minimal impact on business operations. 5. Verification and Validation Deployment is not the final step, IT teams must verify whether the patch was successfully applied. Validation ensures that systems are functioning correctly after the update, with no unexpected performance issues. This step confirms that the intended security or functionality benefits have been realized. 6. Reporting and Auditing Comprehensive reporting provides insights into which systems have been patched and which remain vulnerable. Audit trails are critical for demonstrating compliance during regulatory reviews or internal governance checks. Detailed documentation also helps organizations refine future patch management strategies. Best Practices for Patch Management 1. Automate the security updates: Use a patch manager tool to automate the process of applying security updates to ensure timely patching across the entire network. 2. Schedule the auto-deployments: Set up a regular schedule for auto-deployments to minimize disruptions and ensure consistent patching. 3. Always implement the 'critical first update' approach: Prioritize critical updates that address high-risk vulnerabilities and apply them to minimize the exposure window. 4. Conduct comprehensive testing: Thoroughly test patches in a representative environment to ensure compatibility and stability before deploying them. 5. Have backup and recovery plans: Establish backup and recovery plans to mitigate potential issues during the patching process and enable quick recovery if problems arise. Automating security updates is a best practice in patch management that helps IT professionals ensure timely and consistent patching across their entire network. Using a patch manager tool, IT professionals can automate the process of applying security updates, minimizing the risk of missing critical patches and reducing manual effort. 1. Schedule the auto deployments Scheduling auto-deployments is a best practice in patch management that helps IT professionals ensure consistent and timely patching across their network. IT professionals can minimize disruptions and ensure that all systems receive the latest patches by setting up a regular schedule for auto-deployments. One common scheduling practice is to deploy patches on a specific day, such as "Patch Tuesday." Patch Tuesday is the second Tuesday of each month when software vendors, including Microsoft, release monthly patches. By scheduling auto-deployments on Patch Tuesday, IT professionals can ensure that their systems receive the latest patches as soon as they are available. Implementing a "critical first update" approach is a best practice in patch management that helps IT professionals prioritize critical updates and minimize the window of exposure to high-risk vulnerabilities. IT professionals can quickly address the most significant security risks and mitigate potential breaches by applying critical updates. IT professionals should prioritize deploying a patch over other non-critical updates when they identify a critical security vulnerability. This approach ensures that the most pressing security threats protect systems before they address less critical updates. 3. Comprehensive Testing Conducting comprehensive testing is a best practice in patch management that helps IT professionals ensure the stability and compatibility of patches before deployment. Comprehensive testing involves thoroughly testing patches in a representative environment to identify potential conflicts or issues arising from the patch deployment. Comprehensive testing should include functional testing, compatibility testing, and regression testing. Functional testing ensures the patched software continues functioning without new bugs or errors. Compatibility testing ensures the patch does not conflict with the environment's other software or hardware components. Regression testing helps verify that the patch does not introduce new issues or regressions into the system. 4. Backup and Recovery Plans Having backup and recovery plans is a best practice in patch management that helps IT professionals mitigate potential issues and ensure business continuity during the patching process. Backup and recovery plans provide a safety net if the patching process encounters unexpected problems, such as system crashes or data loss. A backup and recovery plan includes regular backups of critical systems and data to ensure they can be restored during a patching-related issue. This plan should outline the frequency of backups, the storage location of the backups, and the procedures for restoring systems and data. How do you choose the right patch management service provider for your business? Choosing the right patch management service provider is crucial. Here are some factors to help you make a more informed decision. 1. Comprehensive Coverage for the Entire Network When choosing a patch management service provider, it is essential to ensure comprehensive coverage for your entire network, including physical and virtual environments. Comprehensive coverage ensures that all systems, regardless of location or configuration, are included in the patch management process. Organizations with virtual environments must ensure that the patch management service provider can effectively manage and patch virtual servers and virtual machines. These virtual environments often have unique requirements and configurations that the patch management solution needs to support. 2. Immaculate Automation Capabilities Automation capabilities are a critical factor to consider when choosing a patch management service provider. Look for a service provider that offers robust automation capabilities to streamline the patch management process and ensure timely and consistent patching. It helps reduce the risk of human error and ensures that patches are consistently applied according to the organization's patching policies. It can save time and effort, allowing IT professionals to focus on other critical tasks. 3. Intuitive and Ease of Use Ease of use is important when choosing a patch management service provider. Look for a user-friendly solution with an intuitive configuration manager that simplifies the patch management process. An easy-to-use patch management tool should have a user-friendly interface that allows IT professionals to navigate and operate the system effortlessly. The configuration manager should provide a straightforward and intuitive way to configure and customize the patching process based on the organization's specific needs and requirements. 4. Customization and Flexibility Customization and flexibility are crucial when choosing a patch management service provider. Look for a solution that allows you to customize and adjust the patch management process to align with your organization's specific needs and requirements. Flexibility in the patch management process allows IT professionals to adapt to changing requirements and address specific challenges. The solution should accommodate network configurations, operating systems, and software applications. 5. Security Features Patch management tools offer a range of security features to help IT professionals protect their infrastructure from potential vulnerabilities. These features include: Vulnerability scanning: Vulnerability scanning capabilities are essential to identify security vulnerabilities in the network. This allows IT professionals to prioritize patching based on the most critical vulnerabilities. Endpoint management: It provides endpoint management capabilities to ensure that all devices in the network are protected. This includes managing security updates for operating systems, applications, and hardware drivers on endpoints. 6. Testing Options A Patch management tool provides testing capabilities to validate patches before deployment. It is crucial to test patches thoroughly before deploying them to a production environment to ensure they don't cause issues or compatibility problems. Patch testing involves creating a test environment that closely mirrors the production environment and applying patches. This allows IT professionals to identify conflicts, performance issues, or other problems arising after deployment. Comprehensive testing helps ensure patches are safe to deploy in the production environment. 7. Support and Maintenance For comprehensive reports, ensure the service provider has an up-to-date support and maintenance system against security vulnerabilities. The Service providers must offer various support options, including customer service helplines, online forums, and knowledge bases. These resources help IT professionals troubleshoot issues, get answers to technical questions, and get complete control. Regular maintenance is also essential to keep the solutions running smoothly. What Perks Does Motadata's Patch Management Solution Provide? Motadata's Patch Management tool provides IT professionals with the tools and capabilities to manage patches and protect their infrastructure effectively. Complete patch compliance Our comprehensive Patch Management Software automates the patching process and ensures complete patch compliance. By leveraging comprehensive reporting capabilities, IT professionals can monitor and track the patching process to ensure compliance with industry regulations. Patch compliance is crucial to protect against security vulnerabilities and minimize the risk of potential cyberattacks. Organizations can mitigate the risk of security breaches and protect sensitive data by ensuring that systems are patched and updated. Full Visibility of IT infrastructure Our Patch Management Software provides IT professionals with full real-time visibility of their IT infrastructure. This visibility allows IT professionals to quickly identify any patch-related issues and take immediate action to address them. By having real-time visibility into the IT infrastructure, IT professionals can monitor the patching process and ensure that systems are up to date with the latest security updates. This visibility also enables IT professionals to track the patch status of assets and identify any vulnerabilities that must be addressed. Full visibility of the IT infrastructure is crucial for effective patch management. By leveraging Motadata's solution, IT professionals can ensure their infrastructure is secure and protected against potential vulnerabilities. Reduced Total cost of ownership Our solution helps organizations reduce the total cost of ownership by automating and minimizing the need for manual intervention, resulting in cost savings. Motadata's solution's automation capabilities eliminate the need for manual patch deployment and reduce the risk of human errors. This reduces the overall costs associated with the process and increases its efficiency. The decline in possible cyber attacks Cyber attackers often target unpatched systems and exploit known vulnerabilities. By leveraging Motadata's solution, organizations can effectively manage patches and protect their infrastructure from potential attacks. Vulnerability management is a very critical aspect. Our solution helps organizations prioritize critical vulnerabilities and ensure that patches are deployed promptly. Get a free trial here Path management is a vital step to identifying and securing all coding gaps that could potentially be exploited. In this article, we're going to discuss the best patch management practices, and the risks associated with deploying a poor patch management program. Patching is important for several reasons. Patches are released to fix security vulnerabilities in software and systems. Failure to patch these vulnerabilities leaves the company's systems exposed to potential security breaches, data theft, and other cyberattacks. Patch management helps to minimize these risks by ensuring that all software and systems are up-to-date with the latest security patches. Many regulatory and industry standards require companies to implement patch management as part of their cybersecurity program. Failure to comply with these standards can result in hefty fines and legal consequences. Patches also provide bug fixes and other updates that improve the stability and performance of software and systems. Without patch management, companies risk facing system crashes, downtime, and other issues that can negatively impact their operations. A company's reputation can be severely damaged by a security breach or downtime caused by unpatched vulnerabilities. Customers may lose trust in the company and take their business elsewhere. Patch management helps to prevent such incidents and maintains a positive reputation for the company. Improper patch management practices can expose an organization to a number of significant risks. If software vulnerabilities are left unpatched, cybercriminals can exploit them to gain unauthorized access to an organization's systems and steal sensitive information or cause other forms of damage. Malicious attacks can also result in data loss or corruption, which can have significant financial and reputational consequences for the affected organization. Many industries and government regulations require organizations to maintain a certain level of security, and failure to patch vulnerabilities can result in non-compliance and potential legal action. Patching systems can take time and require temporary shutdowns, which can cause significant downtime and disruptions to business operations. A breach resulting from an unpatched vulnerability can damage an organization's reputation, leading to a loss of customer trust and potential revenue. Addressing security breaches, downtime, and other consequences of improper patch management can result in significant costs for an organization. Overall, organizations that fail to maintain proper patch management practices can experience a range of negative consequences, making it essential to prioritize this aspect of cybersecurity. Before you start caring for vulnerabilities, you should start preparing. This step may seem self-explanatory, but it is often overseen. You should have a crystal-clear idea of what software and hardware your company is using, and know exactly how your environment currently stands. Document your systems and understand which devices, operating systems, and third-party applications are currently being used in your organization. Once you have a firm understanding of what you're dealing with, it will be much easier for you to pay attention to vulnerabilities and discover available patches. Not all assets are created equal. You need to investigate which ones of your systems are non-compliant, and vulnerable and thus need patches faster. It won't help if correct identification and prioritization are not put in place. Patching the wrong system won't take you too far. Setting priorities and identifying goals for patching are crucial steps in the patch management process. It's important to identify the software that has to be patched and establish a plan in order to avoid confusion and enable auditing procedures. Also, make sure to prioritize the patches with high security risks, as they should be applied as soon as possible. A patch management policy outlines the standards and rules for handling vulnerabilities properly. This process includes several steps, such as testing, deploying, and documenting the security patches installed on the endpoints of your company. I have covered patch management policy previously, so I strongly suggest you read this article as well. Before deploying a patch, it is essential to test it in a controlled environment. Testing patches allows businesses to identify any issues that may arise from the patch, such as compatibility issues with other software. Testing should involve a representative sample of the IT infrastructure to ensure that the patch works correctly across all systems. By testing patches before deployment, businesses can avoid potential system failures or security breaches. Keep track of the state and performance of your endpoints pre and post-applying patches. This practice is strongly related to the previous one, because sometimes, patches may actually slow down some processes. This way, if problems begin to occur, it will be easier for you to determine if they can be attributed or not to an applied patch. Bonus tip: make sure you have a rollback plan, so that in case of errors or conflicts, you can restore your software to the previous working version as soon as possible. This should help you reduce downtime. Despite the fact that patching can be done manually, an automated procedure is always faster and more accurate. It will assist in reducing the possibility of human error and malware attacks. By automating the patch management process, your system administrators will save time and be free to work on other security-related responsibilities. Also, you will have complete access to your IT system and be rigorous about monitoring fixes and vulnerabilities. Such a solution is our very own Heimdal® Patch & Asset Management Software, a hyper-automated solution that is guaranteed to keep your business secured in terms of patching, whether we're talking about Windows, Linux, macOS, or third-party application patches. Our solution is fully customizable, meaning that it can be configured to perfectly suit your organization's needs. Heimdal®'s software also works as set-and-forget, and will allow you to patch from anywhere in the world, anytime you want it. Updates are delivered fully repackaged, ad-free, and tested from Heimdal® using encrypted packages inside encrypted HTTPS transfer to your endpoints locally. Using local network P2P between your own machines only, to achieve world-leading bandwidth consumption. Book a demo by using the form below and convince yourself of what our solution has to offer! Patch management is an essential part of any business's network security. By implementing the right patch management practices, organizations can ensure their networks remain secure and compliant with industry standards. From establishing a patching policy to automating processes and keeping up-to-date on patches, there are several strategies that businesses should consider in order to maximize the effectiveness of their patch management program. With the proper knowledge and implementation tactics, companies can create a secure environment for their customers and employees alike. If you liked this article, follow us on LinkedIn, Twitter, Facebook, and Youtube, for more cybersecurity news and topics. 2.3K Cristian Neagu is a seasoned cybersecurity expert, with a deep understanding of the digital threat landscape. Cristian specializes in patch and vulnerability management, areas where he has written extensively for the Heimdal® blog. His writing style resonates with both technical and non-technical readers, proof of his skill in communicating complex cybersecurity norms effectively. Get in touch with Cristian on his LinkedIn or by sending him an email over to cristian@patchmanagement.com Updated on March 17, 2025, by ITarian In today's fast-evolving digital landscape, keeping your IT systems secure and up to date is more critical than ever. One of the most effective ways to protect your organization from cyber threats is through a robust patch management strategy. Failing to apply timely software updates can leave your systems vulnerable to exploits, data breaches, and costly downtime. In fact, according to the Ponemon Institute, 57% of cyberattack victims reported that their breaches could have been prevented with proper patching. If you're an IT administrator or system manager, implementing an effective patch management strategy is a key responsibility. This guide will walk you through the importance of patch management, why it matters, and actionable steps to create a strategy that keeps your organization secure and efficient. Plus, we'll show you how tools like ITarian's patch management solutions can streamline the process. What Is Patch Management and Why Does It Matter? Patch Management is the process of identifying, acquiring, testing, and applying software updates (or "patches") to systems, applications, and devices. These patches fix vulnerabilities, enhance functionality, and improve performance. Without a structured patch management strategy, your organization risks: Cybersecurity Threats: Unpatched systems are prime targets for hackers exploiting known vulnerabilities. Compliance Issues: Many industries require regular patching to meet regulatory standards like GDPR, HIPAA, or PCI-DSS. System Downtime: Unpatched software can lead to crashes or compatibility issues, disrupting operations. Data Loss: Exploited vulnerabilities can result in data breaches, damaging your reputation and finances. With cyber threats on the rise and "patch management" generating over 5,000 monthly searches, it's clear that IT professionals are seeking guidance on this critical task. Let's dive into how you can manage software updates effectively. Step-by-Step Guide to Implementing an Effective Patch Management Strategy Step 1: Assess Your IT Environment Before you can manage patches, you need a clear understanding of your IT environment. Conduct an inventory of all hardware, software, and devices connected to your network. This includes: Servers, workstations, and mobile devices. Operating systems (e.g., Windows, Linux, macOS). Applications and third-party software. Pro Tip: Use an automated IT asset management tool to streamline this process. ITarian's patch management solution, for example, provides real-time visibility into your assets, making it easier to identify what needs patching. Step 2: Establish a Patch Management Policy A formal patch management policy sets the foundation for consistent and timely updates. Your policy should outline: Patch Prioritization: Focus on critical patches that address security vulnerabilities first. Roles and Responsibilities: Define who is responsible for identifying, testing, and deploying patches (e.g., IT team members). Patching Frequency: Set a schedule for routine patching (e.g., monthly) and emergency patching for critical vulnerabilities. Approval Process: Establish a workflow for approving patches before deployment. Having a clear policy ensures accountability and reduces the risk of missed updates. Step 3: Identify and Prioritize Patches Not all patches are created equal. Some address critical security flaws, while others improve performance or add features. To prioritize effectively: Monitor Vendor Announcements: Stay informed about patch releases from software vendors like Microsoft, Adobe, or Oracle. Leverage Vulnerability Databases: Use resources like the National Vulnerability Database (NVD) to assess the severity of vulnerabilities (e.g., CVSS scores). Focus on Critical Systems: Prioritize patches for systems that handle sensitive data or are exposed to the internet. Automated patch management tools, such as ITarian's, can scan your environment, identify missing patches, and rank them based on urgency. Step 4: Test Patches Before Deployment Deploying untested patches can lead to compatibility issues, system crashes, or disrupted workflows. To avoid this: Set Up a Test Environment: Create a sandbox or staging environment that mirrors your production systems. Test Critical Patches: Apply patches to a small group of test devices first. Monitor Performance: Check for bugs, performance issues, or conflicts with existing software. Testing ensures that patches won't negatively impact your operations. Step 5: Deploy Patches Efficiently Once patches are tested and approved, it's time to deploy them across your organization. Follow these best practices: Schedule Deployment: Roll out patches during off-peak hours to minimize disruption. Use Automation: Manual patching is time-consuming and error-prone. ITarian's patch management tools allow you to automate deployment across multiple devices with a few clicks. Segment Rollouts: Deploy patches in phases (e.g., to a small group of users first) to catch any unforeseen issues. Automation not only saves time but also ensures consistency and reduces human error. Step 6: Monitor and Verify Patch Success After deployment, confirm that patches were applied successfully and that systems are running smoothly. This involves: Verification Checks: Use patch management software to verify that updates were installed on all targeted devices. Monitor System Health: Watch for performance issues or unexpected behavior post-deployment. Document Changes: Maintain a log of applied patches, including dates, systems affected, and outcomes. ITarian's reporting features can generate detailed patch compliance reports, helping you stay on top of your strategy. Step 7: Educate Your Team and Stay Proactive Patch management isn't just a technical process—it requires buy-in from your team. Educate employees about: The Importance of Updates: Explain how timely patching protects the organization. Avoiding Delays: Discourage users from postponing updates on their devices. Additionally, stay proactive by subscribing to security alerts, attending industry webinars, and reviewing your patch management strategy regularly. How ITarian's Patch Management Tools Can Help Managing software updates manually can be overwhelming, especially for organizations with large IT environments. That's where ITarian's patch management solutions come in. With ITarian, you can: Automate Patch Discovery: Identify missing patches across all devices in real time. Prioritize Updates: Focus on critical patches based on severity and system importance. Streamline Deployment: Schedule and deploy patches with minimal disruption. Ensure Compliance: Generate reports to demonstrate adherence to regulatory standards. By leveraging ITarian's tools, you can save time, reduce risk, and maintain a secure IT environment. Common Patch Management Challenges and Solutions Even with a solid strategy, challenges can arise. Here's how to address them: Challenge: Limited Resources Solution: Use automation to reduce the workload on your IT team. Challenge: Patch Overload Solution: Prioritize critical patches and stagger deployments. Challenge: Resistance to Updates Solution: Educate users about the risks of delaying patches. Conclusion: Build a Secure Future with Patch Management An effective patch management strategy is a cornerstone of IT security and operational efficiency. By assessing your environment, establishing a policy, prioritizing patches, and leveraging automation, you can protect your organization from cyber threats and ensure compliance with industry standards. Ready to take control of your patch management process? ITarian's patch management solutions make it easy to stay ahead of vulnerabilities and keep your systems secure. Start today by exploring how ITarian can simplify your IT management tasks and safeguard your business. Unpatched software remains one of the leading causes of cyberattacks. According to Verizon's 2025 Data Breach Investigations Report, 22% of vulnerability exploits came from VPN and endpoint devices, and it grew almost eight-fold from the 3% found in last year's report. For MSPs and IT teams, effective Windows patch management, particularly for security updates, is the first line of defense against cyberthreats, compliance violations, and costly downtime. Managing Windows updates across distributed client environments requires automation, visibility, and strategic execution. This blog explores everything you need to know about Windows patch management, including challenges and best practices for selecting the right tools tailored to managed service environments. Key takeaways Windows patch management is essential for protecting systems from known vulnerabilities, improving performance, and ensuring regulatory compliance Challenges include high patch volume, compatibility risks, distributed environments, limited IT resources, and user disruption Best practices include continuous connection to devices, patch testing, deployment policies and automation, compliance monitoring, and rollback plans ConnectWise RMM™ includes a robust Windows patch management solution, offering centralized control and visibility, automated deployment by policy, and expert testing and recommendations for security updates What is Windows patch management? Windows patch management is the process of acquiring, testing, deploying, and verifying updates (patches) for Windows operating systems. These patches can include: Security updates to address known vulnerabilities Feature updates to add new functionality Bug fixes to resolve known issues that impact performance or stability For MSPs and IT departments, patch management involves building a structured, repeatable process that supports multiple environments, users, and compliance frameworks. Why Windows patch management matters Effective Windows patch management is essential to safeguarding digital infrastructure, maintaining operational efficiency, and ensuring compliance across industries. For IT departments and MSPs, staying current with Windows updates is a business-critical responsibility. Delayed or inconsistent patching increases the risk of security breaches, system downtime, and regulatory violations. Patch management plays a strategic role in strengthening cybersecurity posture, supporting business continuity, and delivering reliable IT services. Whether you're overseeing a corporate IT environment or managing clients across multiple industries, a proactive approach to patching ensures your systems remain secure, compliant, and high-performing. Windows patch management matters because it: Microsoft regularly issues patches to fix known vulnerabilities and zero-day threats. Without timely updates, systems become exposed to malware, ransomware, and other cyberattacks. By applying patches promptly, IT teams and MSPs close security gaps before they can be exploited, drastically reducing the attack surface. Ensures regulatory compliance Cybersecurity frameworks such as HIPAA, PCI-DSS, GDPR, and SOC 2 mandate the timely application of security updates. Failing to patch known vulnerabilities can result in audit failures, hefty fines, and reputational damage. Implementing a structured patch management program helps demonstrate due diligence and maintain regulatory alignment. Improves system stability and performance Patches often include performance improvements, bug fixes, and system optimizations. Regularly patching your Windows environment minimizes unexpected crashes, reduces support incidents, and enhances user experience. For MSPs, it also means fewer reactive service calls and stronger client satisfaction. Challenges in managing Windows patches Managing the patching process is rarely straightforward, especially at scale. For IT departments and MSPs, patch management introduces a unique set of logistical, technical, and operational hurdles. The sheer number of systems and business-specific requirements make patching a complex, time-consuming, and potentially disruptive task. Understanding these challenges is critical to building a robust patch management strategy. Below are some of the most common obstacles IT professionals face when managing Windows updates: High patch volume and complexity Microsoft releases patches on a monthly basis (commonly known as Patch Tuesday), along with occasional out-of-band updates for critical vulnerabilities. Each patch may apply to multiple versions of Windows and related applications, creating a complex matrix of potential updates. For MSPs managing multiple clients or IT teams overseeing large environments, this leads to: Constant monitoring of patch releases Overwhelming administrative overhead Increased risk of missing critical updates Not all patches are plug-and-play. Some updates can: Break compatibility with legacy systems Disrupt mission-critical applications Trigger hardware or driver issues This is especially problematic in industries with specialized software or in environments with older hardware that lack vendor support. Without rigorous pre-deployment testing, the risk of unintended consequences is significant. Today's IT environments are no longer centralized. Patching must now account for: Remote workers Branch offices Cloud-based virtual machines Without centralized control and visibility, ensuring that every endpoint is up to date becomes a logistical challenge. This is a major concern for MSPs who must maintain patch compliance across multiple customer environments, some with unique configurations and constraints. Limited time and resources Many IT teams, particularly in small and midsized businesses (SMBs) or lean MSP operations, lack the time, personnel, or budget to manage patching effectively. Tasks such as testing, scheduling, and reporting often fall to the bottom of the priority list amid urgent support tickets and strategic initiatives. As a result: Patches may be delayed or missed Emergency patching becomes more common Security and compliance gaps widen over time Lack of visibility and reporting Without real-time dashboards or automated reporting, teams may not know: Which systems are patched and which are not If patches have failed or been rolled back Whether endpoint devices are even online to receive patches This lack of visibility makes it difficult to enforce compliance policies or demonstrate patch coverage during audits, which can be particularly challenging for MSPs trying to meet SLA expectations. User disruption and resistance End users often resist patches due to concerns about: System restarts Downtime during working hours Application disruptions Poorly timed patches can result in productivity loss, user frustration, or even critical system outages, especially if proper communication and scheduling protocols aren't followed. Emergency patching and zero-day vulnerabilities When zero-day vulnerabilities emerge, IT teams must act fast. These situations require: Immediate testing and validation Rapid deployment to all affected systems Coordination across departments and clients The pressure to balance speed and stability during high-stakes situations can be overwhelming, especially if patching infrastructure is not already automated and centralized. Recognizing and addressing these challenges is essential for creating a resilient patch management process. The goal is to transform patching from a reactive fire drill into a proactive, automated discipline that supports security, uptime, and compliance across every environment you manage. Best practices for effective Windows patch management Managing Windows patches effectively goes beyond simply installing updates when prompted. It requires a structured and strategic approach that ensures consistency, minimizes risk, and supports compliance requirements. Whether you're responsible for a few internal systems or thousands of endpoints across client environments, following best practices can improve your patch success rate, reduce downtime, and enhance overall system security. The below best practices should form the foundation of any successful Windows patch management strategy: Maintain a comprehensive asset inventory Before you can manage patches effectively, you need full visibility and access to all devices and applications under your control. This includes endpoints, such as workstations and servers, and details, such as software versions and device location. A centralized asset inventory helps prioritize which systems need immediate attention and ensures nothing slips through the cracks. Define and enforce a patch management policy A written patch management policy provides structure and accountability. It should clearly outline: Patch frequency and approval workflows Roles and responsibilities for team members Guidelines for testing, deployment, and rollback Compliance tracking and reporting requirements This policy ensures consistency across environments, supports audit readiness, and aligns your team with business and client expectations. Test patches in a staging environment Deploying patches without testing can lead to compatibility issues, application crashes, system instability, or even worse, outages. To mitigate this risk: Set up a test environment that mirrors production or identify a small group of machines to patch first Apply new patches to the test group Monitor for issues before full-scale deployment This is particularly critical for MSPs supporting multiple clients with varied "lines of business software" and dependencies. Automate patch deployment Manual patching is time-consuming and error-prone. Automation improves efficiency and ensures patches are applied consistently across all systems. Look for tools that allow you to: Schedule patch scans and deployments Create patch approval workflows Customize patching notifications Apply different patch policies per client, department, or system type Automation is a game-changer for IT professionals managing hundreds or thousands of endpoints simultaneously. Monitor and report on patch compliance Visibility doesn't stop after a patch is deployed. Ongoing monitoring and reporting help you: Verify successful installations Identify systems that missed updates or failed patch installation Document compliance with internal and external standards Use monitors, dashboards, and reports to keep both internal and external stakeholders informed. Implement a patch rollback plan Despite testing, some patches may introduce unforeseen problems in production. A rollback strategy allows you to: Quickly revert to a known state Minimize system downtime Maintain end user productivity This might involve removing the patch, using system restore points, or redeploying a clean system image. Schedule patch deployments strategically Timing is everything. Schedule deployments during off-hours or maintenance windows based on business needs to align with clients' business hours and risk tolerance. Be sure to include sufficient lead time to notify users and the ability to delay patching (if appropriate) for a short time. Strategic scheduling helps avoid disruptions and builds trust with end-users and clients. Keep stakeholders informed Whether you're an IT department manager or an MSP, transparency builds trust. Ensure that: Users are informed of planned updates and potential downtime Management understands the importance of patch compliance (and the difference between planned and unplanned downtime) Clients receive regular reporting on patch activity and coverage Clear communication reduces frustration and reinforces your value as a proactive IT partner. Following these best practices creates a strong foundation of trust, reliability, and operational excellence in your patch management efforts. It not only empowers MSPs to deliver scalable, high-value services across diverse customer environments but also enables IT teams to stay proactive against emerging cyberthreats in today's ever-evolving digital landscape. For more tips on building an effective patching strategy, download our free Patch Management Best Practices Guide. Top tools for Windows patch management When it comes to managing Windows updates at scale, IT teams and MSPs have two primary paths: native tools provided by Microsoft or purpose-built solutions to expand patching capabilities. See a comparison of the two approaches below and discover why ConnectWise RMM stands out for modern patch management. 1. Microsoft patch management solutions Microsoft offers several native tools for Windows patch management: Traditional tools Microsoft Configuration Manager: Offers broader configuration management, including patching, application deployment, and asset tracking. Formerly called System Center Configuration Manager (SCCM). Windows Server Update Services (WSUS): A free tool that provides centralized control over Windows updates, allowing IT admins to approve or reject patches before deployment. According to Microsoft's website, "WSUS is deprecated and is no longer adding new features. However, it continues to be supported for production deployments and receives security and quality updates as per the product lifecycle." Modern alternatives Windows Update client policies: A free cloud-based service that allows IT teams to manage how and when Windows updates are delivered to endpoints. It enables policy-based control over update installation timing, deferrals, and device groupings without requiring on-premise infrastructure. Formerly called Windows Update for Business (WUFB). Azure Update Manager (AUM): Microsoft's modern cloud-native patching solution for Windows and Linux servers, whether they are in Azure, on-premises, or in other clouds. Windows Autopatch: A managed service designed to automate the deployment of updates for Windows, Microsoft 365® apps, Microsoft Edge, and Teams. These tools are powerful, but IT pros often must account for: Complex setup and steep learning curve High maintenance and infrastructure overhead Limited multi-tenant support Manual workflows that reduce efficiency 2. RMM solutions For MSPs and IT service providers seeking automation, flexibility, and scalability, tools such as ConnectWise RMM offer a more agile, modern alternative. Our award-winning RMM software is built to simplify automated and multi-tenant patch management. It enables you to manage Windows updates across hundreds or thousands of endpoints with minimal effort and maximum control. Key advantages of ConnectWise RMM: Multi-client visibilityManage all customer environments from a single, unified dashboard. Automated patch workflowsSchedule approved updates to deploy automatically and monitor for patch issues, freeing up your team to focus on strategic initiatives. Expert patch review and approvalsThe ConnectWise Network Operations Center (NOC) tests all Windows security updates so your team can deploy the most critical updates with greater peace of mind. Built-in compliance reportingEasily monitor and

quickly generate patch compliance reports to support audits and demonstrate value to clients. Ready to take patch management to the next level? Start a 30-day free trial, or contact us today to see how ConnectWise RMM can transform your patching process. The process of fixing bugs or malfunctions in software is called patch management, and when done right, it can protect you from security threats, glitches and other bumps along the road to product launch. Imagine you're riding a bicycle, and a dreaded pothole suddenly appears to pop your tire. This could ruin your day, but if you're equipped with a repair kit and tire patches, you can be back on the road soon enough. The same concept can apply to software. Just like a popped tire, a hole in your software design can be patched up and put back into action as if nothing ever happened. Patch management is a system by which developers can apply patches or new pieces of code to existing software in order to add new features, fix bugs and cover up holes. "Customers are paying for a product or service that they expect to run well and feel safe while using it. By not patching, an organization is putting its customers at risk of a security breach as well as providing a subpar service," said Aaron Sandeen, co-founder of Albuquerque-based IT security company Cyber Security Works. Good patch management practices keep your software in top shape and protect both you and your customers from potentially serious security threats. Here's a deep dive into how patch management works, and how to do it right. More on Software Engineering Perspectives You Need to Relearn HTML What Is Patch Management? Software is by nature never static. Every software product needs to remain dynamic and agile to stay functional and reliable in a world of constant OS updates. Because of this, there's always a chance for error when new features get released. Developers need to keep track of changes and make bug fixes as soon as they can, and that's where patch management comes into play. "Patch management is the process of receiving, testing and installing patches on existing applications and software." "Patch management includes awareness of software updates, testing of updates and rollout of updates, all typically orchestrated by an organization's IT department," said David Strauss, co-founder and CTO at San Francisco-based WebOps platform Pantheon. "The updates often fix bugs, add features and keep applications in a maintainable state." If you tear a seam in your favorite pair of jeans, you'll typically sew in a patch, so you can continue to wear them without issues. You can think of software patch management in the same vein: once developers uncover holes in their product's design, they can apply "patches" to smooth things over and get their software up and running. "Patch management is the process of receiving, testing and installing patches on existing applications and software," Sandeen said. "Patch management enables security teams to determine which patches are appropriate for their environments and keeps their systems up-to-date with code fixes." Why Patch Management Is Important If you've ever dealt with a software program crash or an endlessly loading screen, you'll know just how annoying software bugs can be from a user standpoint. Patch management helps software developers keep their products in top shape, so they can provide their customers with a seamless, enjoyable user experience. But there are also more serious problems that software patching can help coders mitigate. If developers ignore bugs or malfunctions, their products could become defunct entirely, or worse, expose their companies to external threats. "Failure on a user's part to keep their system up-to-date can allow a hacker to exploit any holes in their system," Sandeen said. "[This can] lead to serious data leaks, loss of privacy and even costly ransom situations." It would be nice if launching a software product was a one-and-done affair. Constant patch management takes time and can feel like a hassle to developers who want to spend time working on new projects. But the security threats that come from not doing patch management aren't hypotheticals, Strauss said. "That's how you end up with things like the Equifax breach from years ago," he said. "California, most of Europe and many other places, have imposed regulations on companies that create additional financial and reputational risks from a data breach. The cost of a breach can be debilitating." The Patch Management Process Doing patch management right begins with finding the right tools for the job. Patch management technologies vary from system to system, but there are baseline tools software developers can keep in their back pockets. "For operating systems and mobile devices, there's usually a management infrastructure like Microsoft InTune or Jamf for approving and monitoring rollouts," Strauss said. "For infrastructure management, there are tools like Chef, Terraform and Config Connector. For code, there's usually a package manager like Composer or npm." Once you've figured out the right tools for the job, you'll need to make sure you've taken inventory of all your company's software products and are getting real-time updates on their functionality, said Jamie Moles, senior technical manager at Seattle-based network security company ExtraHop. "You need to make sure you are monitoring all the software information streams to notify you of new software releases and bug fix releases," said Moles. "When a new release is issued, download, test and deploy at the earliest convenience — especially if the patch is one that fixes security problems in the software." This last step of testing is in some ways the most crucial step in successful patch management. If a patch isn't tested before launching, it can cause issues even bigger than the ones you were trying to fix in the first place, Sandeen said. "Test, test, test!" he said. "Incompatible patches can cause a system crash. To avoid shutting down the organization, patches should first be rolled out in test environments before deployed into production environments." More on Software Developers 4 Ways to Help Software Developers Build Their Skills Patch Management Best Practices When it comes to maintaining high patch management standards, testing is among the most important. But just like software products themselves, testing interfaces also need to be updated and fine tuned over time to avoid obsolescence, Strauss said. "The necessity of testing is probably no surprise, but it's perhaps more important that the testing strategy be sustainable," he said. "I've seen teams implement elaborate test suites, only to have the tests rot because they're too brittle or time-consuming to run." Without a set goal, patch rollouts can be discombobulated. Like with any strategic decisions, they need to be rolled out with intention. Effective patch management requires strong communication channels and a cohesive game plan that entire software teams are on board with. "Patch management should be a mainstream part of the IT business, not an afterthought." "Planning and communication are essential," Sandeen said. "Expectations should be set early on and teams should be held accountable to make sure things get done. Communicating necessary changes to other departments and ensuring they understand the importance of continual patching is a part of the process." It's always possible for patches to fail after their launch, so it's also a best practice to create a system for handling the fallout of an unsuccessful patch. "There should be a disaster recovery process already in place just in case something does go wrong with the patch," Sandeen said. When you launch a new software product, it's great to be optimistic. But while you shouldn't let worries about bugs overshadow the excitement of seeing your work in action, coming up with a plan for patch management before things go wrong is crucial for the overall success of your software. Plan for patches ahead of time — that way, nothing will take you by surprise. "IT and security teams should have well-rehearsed procedures for the emergency deployment of critical patches," Moles said. "Patch management should be a mainstream part of the IT business, not an afterthought." In this guide, you'll find: Key features, benefits, and use cases for patch management How to turn stress into peace with quality patch management Actionable 'how-to' guides on prioritizing vulnerabilities and implementing patch management software Picture this: You're the head of IT at a medium-sized company, tasked with overhauling the cybersecurity approach. First thing's first: Installing patches. Should be fairly simple, right? Then, you run a scan and realize the situation is a little more complex. There are hundreds of patches and updates on the list. Some of these are feature updates for apps nobody uses anymore – barely even worth bothering with. Others are critical security patches that will protect sensitive IT assets and data. The best time to install these was yesterday and the second best time is right now. The hard part is working out which are which. Here's the issue: there are hundreds of patches and you don't know how to prioritize them without going through one-by-one. Worse still, some will cause downtime when installed and others might have unforeseen consequences on other systems, apps, and workflows. So where on earth do you start? Here's everything you need to know about patch management. Patch management: Definitions, benefits, and key details What is patch management? "At the end of the day, the risk that many organizations face in their infrastructure and applications is 'What if there's a security vulnerability exploited before I have time to react?'" Chief Product Officer,Snyk Patch management is the process that IT departments use to identify, prioritize, and install software updates. The goal is to identify and eliminate known software vulnerabilities before hackers can use them to access your network and systems. A software vulnerability is essentially an error or bug in the underlying code of an application that wasn't identified before release. This is common and most applications will have them at some point. Some vulnerabilities allow hackers to access your IT environment and elevate privileges once they've done so. This essentially creates an open door into your IT environment for anybody who knows how to exploit it. When a manufacturer identifies a vulnerability, they will fix the issue and generally release the updated code via a patch or update. Installing these is the best way to ensure hackers can't use vulnerabilities to infiltrate your IT environment. Deep dive: What Is Patch Management? Definition, Process, Benefits, and Best Practices [UPDATED 2025] Patch and vulnerability management are two related concepts. Often, they're used interchangeably, but there is a subtle difference between between the two. A vulnerability is the underlying software issue that needs resolving and a patch or update is released by the software manufacturer to solve the problem. Vulnerabilities that aren't known by the manufacturer are referred to as 'zero day' – and no patches exist for these issues. Vulnerability management is therefore the exercise of understanding what software issues you have, which are the most critical, and what patches are required. Patch management is the more direct exercise of applying the patches. In practice, they form two parts of the same process, and neither is complete without the other. This is why both terms are often used to mean the same thing. Deep dive: Patch Management vs. Vulnerability Management: A Comparison "A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it." - Andrei Hinodache , Cybersecurity Community Leader The key goal of patch management is to eliminate key attack vectors that hackers can use to target and infiltrate your IT systems. But this is not the only reason that patches/updates are released. In fact, there are several types of patch management you need to be aware of: Security patches: These are created to fix known software vulnerabilities, generally by replacing the compromised code. Bug fixes: These are released to eliminate issues with the software's features, performance, stability, or usability. Feature updates: These occur when the software vendor adds new features or functionality to the application. All three patch types are important for different reasons. However, only the first is relevant to security, and is therefore the focus of this article. Deep dive: Main Types of Patch Management: A Decision-Making Guide Why is patch management important for you? ""Patching is tough because it is political just as it is technical. I tend to see two patterns. The first is where an admin takes a heavy-handed approach and forces patches on people no matter what, and literally causes business impact [with] reboots at the worst possible times. The other end of the spectrum is the admin who is afraid to touch anything."" Patch management is important because it helps improve your overall security posture. The more software vulnerabilities you have, the greater the risk of being infiltrated by a hacker. But it's more complex than just that. Installing patches requires IT resource and often creates periods of downtime. Most organizations won't have the time to install every single patch or update. In this context, patch management is as much about identifying and prioritizing the most important patches to install – as it is about actually implementing them. Three crucial best practices for patch management It's easy to think that effective patch management simply involves installing all updates as soon as they're made available. In truth, the situation is more complicated. To be successful, there are several best practices it's important to bear in mind. Here are three of the most important: Prioritize vulnerabilities: Few organizations have the time or resources to install every patch. Instead, it's important to understand and prioritize those which pose the most critical threats to your IT environment. Test patches before deployment: When installed, updates can have unforeseen side effects on existing tools, workflows, and processes. It is therefore important to test patches (ideally in a controlled or sandboxed environment) before they're fully deployed, so potential issues can be identified and mitigated. Automate patches: Automated patches are generally quicker and more effective than relying on your IT team to manually identify and install each update. However, you should try to ensure patches that could cause downtime aren't installed automatically. Get the right software: Not all patch management tools are built the same. It's important to choose a tool that's easy to use, cost effective, and integrates with your other cybersecurity products. At Heimdal, our goal is to create a one-stop-shop for cybersecurity through an easy-to-use and cost-effective solution. Deep dive: Six Patch Management Best Practices Three use cases of patch management: For IT teams, patch management can be a complex business. Getting it right involves a whole range of tasks, processes, and technical requirements. Here are three main ways in which the right tools can help with this: Identifying and prioritizing patches: Patch management tools can both identify unpatched vulnerabilities in your environment and help prioritize those that pose the most critical risk. Installing patches: Tools can also directly install the patches themselves, avoiding your IT team needing to do each one manually. The IT team can then select patches to be installed on a case-by-case basis or create automated rules to do this for them. Compliance reporting: Patch management tools can generally create automated reports to quantify which patches have been installed, when, and what systems are affected. This is a crucial part of IT and risk management compliance. Deep dive: Full gated demo Patch management how-tos: Actionable guides for patch management success How to implement and automate patch management software in your organization Patch management software is one of the best ways to identify, prioritize, and install patches. But to get it right, you need to find the right product for your organization. Here are a few points to bear in mind: Get the right features: The right vulnerability management tools should offer features to scan vulnerabilities in your environment, prioritize them with CSS scores, install patches, create automated policies, and create compliant reports. Assess cost and complexity: Different platforms are built for different organizations. The most expensive on the market also tend to be the most complex, since they're designed to be managed by specialist security teams at large companies. Other tools are aimed more towards SMEs and are generally easier for small and less specialist teams to use. It's important to get the right balance of features, costs, and complexity for your organization. Assess integrations: While vulnerability products are important, they're not the only cybersecurity tool in your arsenal. You may also need PAM software, DNS security, email protection tools, endpoint detection and response, and much more. Ideally, all these tools should be available under a single license to reduce costs, complexity, and integrations. Otherwise, you need a tool that effectively integrates with a range of third-party cybersecurity tools. Deep dive: How to Build a Healthy Patch Management Program Prioritizing vulnerabilities is one of the hardest aspects of patch management. The best place to start is by assessing publicly available CSS scores – a ranking that's given to all known vulnerabilities based on their perceived risk. Anything that hackers can use to gain access or elevate permissions is generally considered the highest risk. But to be truly effective, this needs to be a partly subjective process. These scores can't take into account the specific context of your IT environment, what data you have, what systems are involved, and what the potential consequences of them being breached will be. Therefore, effective vulnerability requires trained professionals combining CSS scores with their own qualitative judgments. Deep dive: How to Prioritize Vulnerabilities Effectively: Vulnerability Prioritization Explained Effective patch management is a multi-stage process. To get it right, there are several steps it's useful to consider before installing your patches: Asset inventory: First, you need to create an inventory of all IT assets, which can be done with an endpoint management tool. This will give you an overview of the sensitive assets that need to be protected. Define team roles: Then, you need to define who will prioritize and manage the patches. If you're using a managed security services provider, this will be outsourced. Otherwise, an internal IT or security specialist will need to be responsible for this. Install patch management software: With an effective patch management platform, you'll have the tools to identify, prioritize, and remediate vulnerabilities. Test your patches: Once you've identified patches to install, you should test them to avoid any unforeseen complications like broken workflows or downtime. Create a patching schedule: Patches often require downtime and sometimes cause unforeseen issues. It's helpful to schedule them for quiet periods (ie at night) to reduce the effect of downtime and outages. Document your patching process: It's important to document what patches are installed for your own future reference and, more crucially, to comply with IT regulations. Deep dive: Patch Management Policy Guide [Free Template Inside] How to manage patch reporting Patch management requires a robust process to document and report on all patches installed. By far the best way to do this is to get the right software. These are built with the most recent compliance requirements in mind, and offer plenty of options to automatically generate compliant reports. Deep dive: Patch Management Template [Free & Downloadable] Patch management software: Benefits, features, and best practices What is patch management software and is it worth the investment? Patch management software is an umbrella term for any type of cybersecurity tool that helps to identify, install, and prioritize patches to install. They also generally feature tools to automate patch installation and generate compliance reports. These tools exist because patch management is near-impossible to do manually. There are simply too many vulnerabilities in the average IT environment for you to effectively identify and prioritize them, without the right tools. The right patch management software, therefore, is invaluable. Deep dive: Patch Management Template [Free & Downloadable] Three key features in advanced patch management solutions When looking for the right patch management software, there are a few features it's important to look out for. Here are three of the most important: Vulnerability scanner: This enables organizations to run a scan on their IT environment and identify any unpatched vulnerabilities. CVV score ranking: These tools can also associate unpatched vulnerabilities with publicly available CVV scores. These help quantify the relative risk of different vulnerabilities – though it can't take into account the specific context of your IT environment. Automated policies: Advanced vulnerability management products allow you to customize policies to automatically install patches, controlling the type of patches that are installed and when. Deep dive: Best Patch Management Software & Tools Deep dive: 8+ Free and Open Source Patch Management Tools for Your Company Should you get an expert to manage your vulnerabilities? Patch management software helps IT teams identify vulnerabilities to install, quantify risk, install patches, and generate compliance reports on their activities. Nonetheless, even with these tools, some IT teams may find they don't have the skills or resources in their teams to effectively manage this whole process. In this case, you may decide to go for a 'managed patch management' option. Most cybersecurity providers will offer managed services alongside product licenses. Alternatively, you could engage a managed security services provider (MSSP), who generally offer vulnerability management among their services. These options give organizations the peace of mind that vulnerabilities are being effectively managed and installed by trained cybersecurity professionals. They are therefore particularly popular among small and medium-sized companies with limited internal IT resource. Deep dive: What Is Patch Management as a Service (PMaaS) & What Can It Do For You? Get Started Stay safe and secure with zero worry. Stop breaches with complete protection. Book a Demo Pricing & Bundles The patch management cycle is a core cybersecurity practice involving the systematic acquisition, testing, and deployment of software patches to fix vulnerabilities, resolve bugs, and enhance performance. Neglecting timely patching exposes businesses to serious threats, from ransomware attacks to regulatory penalties. This guide offers a complete breakdown of the patch management process and highlights why it's non-negotiable for secure and stable IT operations.What Is the Patch Management Cycle and Why It MattersPatch management is the structured process of identifying, testing, and deploying updates for software and systems. These patches resolve security flaws, enhance functionality, and maintain compliance with industry regulations. An effective patch strategy significantly reduces an organisation's attack surface and strengthens its cybersecurity posture.Failing to apply patches promptly can result in:System compromises through known vulnerabilitiesOperational outages due to unresolved software bugsNon-compliance with security standards like PCI DSS, HIPAA, and GDPRStep-by-Step Patch Management Cycle1. Inventory & Asset DiscoveryStart by compiling an accurate inventory of all software, hardware, operating systems, and third-party applications. Visibility is essential for prioritising vulnerabilities and ensuring no system is left unpatched.2. Vulnerability Scanning & Risk AssessmentAutomate vulnerability scanning tools to detect security gaps. Prioritise patches based on severity, exploitability, and the criticality of affected systems.3. Patch Identification & TestingAfter identifying vulnerabilities, locate relevant patches from vendors. Test them in a controlled, non-production environment to ensure compatibility and prevent operational disruptions.4. Patch DeploymentDeploy tested patches using phased rollouts or automated tools. Monitor deployments to ensure success and resolve any implementation issues in real time.5. Monitoring & ReportingVerify patch effectiveness and track unresolved vulnerabilities. Generate regular reports to assess performance, identify trends, and drive process improvements.6. Continuous MaintenanceTreat patch management as a continuous process. Monitor threat intelligence feeds and vendor updates to stay ahead of emerging vulnerabilities.Benefits of a Robust Patch Management CycleCybersecurity Risk ReductionTimely patching blocks threat actors from exploiting known weaknesses, protecting your organisation from data breaches, ransomware, and system compromises.Improved System StabilityPatches often fix bugs that can crash applications or degrade performance. Regular updates enhance user experience and system reliability.Business ContinuityPatching minimises the risk of downtime caused by security incidents or application failures, preserving business operations and service availability.Regulatory ComplianceMost regulatory frameworks demand consistent patch management as a baseline control. A well-documented process helps avoid audits, fines, and reputational damage.ConclusionThe patch management cycle isn't just routine maintenance—it's a frontline defence mechanism against ever-evolving cyber threats. With a proactive, structured approach, organisations can maintain system integrity, minimise risk, and uphold regulatory compliance. Implement a smart patch management lifecycle today and future-proof your infrastructure from known vulnerabilities.Don't let your organisation fall behind. Follow Cyber News Live for the latest updates on cybersecurity trends, data breaches, threat intelligence, and expert insights. Keep your Linux operating system and the software you run on it fully up to date. You don't have to worry about remembering to perform patching if you take on one of these automated systems. Automated patch managers will look after your software and operating systems. However, while there are many packages available to patch Windows, there aren't so many for Linux. Rather than trawling through all of the descriptions of every patch manager of the market to find which will update Linux, take a look at our list of Linux patch managers. We have identified patch management systems that will automatically check for updates and implement patching. You won't want the patch manager to interrupt your users, so we looked for patch management tools that can be set to run on a schedule. Patch managers should be able to run overnight without any manual assistance. Here is our list of the seven best Linux patch management tools: NinjaOne Patch Management - EDITOR'S CHOICE: This service will patch Linux, Windows, and macOS operating systems and also 200 applications. The patcher is part of a cloud-based platform that implements remote monitoring and management services. You can register for a 14-day free trial. ManageEngine Patch Manager Plus - FREE TRIAL: This system will patch Linux, macOS, Windows, and also third-party software packages. Start a 30-day free trial. GFI LanGuard: A package that provides asset inventory creation, vulnerability scanning, and patch management for Linux, Microsoft, and macOS devices. Runs on Windows or Windows Server. SecPod SanerNow Patch Management: This cloud-based system is part of a platform of system security tools, and it will patch Linux, Windows, macOS, and more than 450 third-party tools. Automox: This cloud-based automation platform includes a patch manager for Linux, Windows, and macOS. KACE Systems Management Appliance: An endpoint management service that includes patching for Linux, Windows, and macOS. Runs on a VM, on your cloud account, or can be accessed as a SaaS package. SysWard: This patch management tool specializes in patching Linux and will manage CentOS, Ubuntu, Red Hat, Debian, OpenSUSE, SUSE, Fedora, and Oracle Linux. Available as a SaaS platform or for installation on Linux. You can read more about each of these options in later sections of this report. Best Linux patch management tools Our methodology for selecting a Linux patch management tool We reviewed the market for Linux patch managers and analyzed options based on the following criteria: A discovery routine that maintains hardware and software inventories. Patch availability reports. A scheduler that will queue patches. A maintenance calendar that indicates regular periods when patches can be applied. Unattended execution that includes Wake-on-LAN, reboot, and remote shutdown. A free trial or a demo service to enable an assessment before buying. Value for money from a tool that will repay its price through staff cost savings. With these selection criteria in mind, we compiled a list of automated patch management systems for Linux – some will also patch other operating systems. 1. NinjaOne Patch Management (FREE TRIAL) NinjaOne Patch Management is probably the best option for managed service providers (MSPs) looking for a system to patch the systems of their clients. The patch management is part of the NinjaOne RMM service for MSPs, which provides multi-tenant accounts. The Patch Management service is also available for IT departments to use without the other features in the remote monitoring and management package. Key features: Endpoint discovery: Creates hardware and software inventories. OS patching: Updates Windows, Linux, and macOS. Software patching: Updates more than 200 software systems. Patch activity logs: Identifies which technician paused or deleted a specific patch. Why do we recommend it? NinjaOne Patch Management is a good choice because of its high degree of automation and activity logging. These two features are crucial requirements for businesses that need to account for their actions and also bill for them. This package can patch Windows and macOS as well as Linux. It will also patch more than 200 software packages. The patch manager checks for patches, downloads installers, and schedules installation without manual intervention. Once patches are queued for application, technicians have the option to put one on hold or delete one. All actions are logged for possible investigations. The patch manager will run out of office hours. IT will start up each computer, install patches, and reboot the device where necessary. The system will also shut down each device at the end of the session. Who is it recommended for? This system is ideal for managed service providers as part of the NinjaOne RMM package. It is also a useful tool for IT departments. The system documents all activity, which is ideal for compliance reporting or service level agreement tracking. Patch scheduling: Set up a maintenance calendar Cloud-based system: Technicians access the console through any standard Web browser Multi-tenant accounts: Suitable for managed service providers Task automation: Operates an entire patch cycle without human involvement No on-premises option: Only available as a SaaS package NinjaOne doesn't publish its price list, so you have to contact the Sales Department to get a quote. You can also ask for a 14-day free trial. NinjaOne Patch Management is our top pick for a Linux patch management tool because this cloud-based platform can also patch Windows and macOS, so it provides full coverage for sites no matter what computers are connected to it. The NinjaOne system is a large package of remote monitoring and management tools and it is highly automated. The patch manager is part of a chain of utilities that takes care of software. The NinjaOne service discovers and documents all endpoints and then scans each to create a software inventory. The tool then regularly scans the producers of operating systems and 200 applications to discover patch availability. If a patch is available, the system will copy down the installer and queue it for implementation. You have to give the console a maintenance calendar, so you can be sure that patching won't disrupt the work of your users. The NinjaOne platform also provides constant network monitoring and includes a remote access tool for maintenance tasks and troubleshooting. Get a 14-day free trial: Operating system: Cloud-based 2. ManageEngine Patch Manager Plus - FREE TRIAL ManageEngine Patch Manager Plus provides patching for Windows, macOS, and Linux. The system will also update software packages. This is one of many packages provided by ManageEngine that implements patch management. The provider's parent company, Zoho Corp, maintains the Central Patch Repository on the cloud. Each installation of Patch Manager Plus checks with that platform every day for a patch availability report. This software won't run on Linux but you can patch endpoints across a network from a Windows Server host or from the SaaS option on the cloud. Key features: System discovery: Creates hardware and software inventories. Patching for operating systems: Windows, macOS, and Linux. Software patching: More than 850 third-party systems. A central patch repository: Pre-tested and validated patches. A scheduler: Automated patch rollout. Why do we recommend it? ManageEngine Patch Manager Plus is a standalone system that can provide all of your patching needs with very little human involvement. Once you set up a maintenance schedule, the service will check for patches every day, acquire patch installers, and run them automatically out of office hours. The patch manager scans through the software inventory, looking at the software version number. This identifier signifies the patch level. The tool then accesses the Zoho Central Patch Repository and looks at the current version number for each package. If the repository number is higher, the patch manager copies down the patch installer. Patches are queued for installation, which will happen at the next available maintenance window. While they are in the queue, patches can be put on hold or deleted by the administrator. The patches will run overnight, and the patch manager will start up, reboot, and shutdown each device accordingly during the patch run. Who is it recommended for? This package is designed for in-house use. That is, it isn't a multi-tenanted system for managed service providers. ManageEngine produces an edition for use on LANs and another that is able to patch multiple sites from one console. There is also a free edition for small businesses. Deployment options: Available as a software package for Windows Server or as a SaaS platform Unattended operations: The system will operate without the need for human involvement Remote actions: The tool will install patches on each endpoint in turn, starting it up, rebooting it, and shutting it down Pre-tested patches: The Central Patch Repository tests all patches before making them available Completion status reports: Explains if any patch installation failed The software is not available for Linux: However, it will patch Linux computers ManageEngine Patch Manager Plus is available as a SaaS platform or as a software package for Windows Server. The free edition is limited to managing 20 workstations and five servers. You can get a 30-day free trial of the full edition and if you decide not to buy at the end of that period, your installation will switch over to the Free edition. 3. GFI LanGuard GFI LanGuard discovers and documents endpoints. It then assesses each device for vulnerabilities, which could include an out-of-date operating system or software. The package includes a patch manager that will keep the OS updated and also manage third-party software, such as media players, browsers, and supporting services. This package will patch Windows, Linux, and macOS. Its Linux compatibility extends to RedHat Enterprise Linux, CentOS, Debian, Ubuntu, openSUSE, SUSE Linux Enterprise, and Fedora 19. Key features: Patches many Linux distros: RHEL, CentOS, Debian, Ubuntu, SUSE, and Fedora. Patching is triggered by a vulnerability scanner: The two services are linked. System documentation: Maintains a list of endpoints. Why do we recommend it? GFI LanGuard is particularly good at patching Linux, although it is also able to patch Windows and macOS. This service is compatible with a long list of distros, each of which has its own variation on the standard Linux command set. The package also includes a system discovery service and a vulnerability scanner. The combination of a vulnerability scanner and patch manager is particularly appealing. The discoveries of a vulnerability scanner often lead to a requirement to update operating systems and software. So, this package will just launch the patching process to automatically fix many of the problems discovered by the vulnerability manager. The vulnerability scanner has a list of 60,000 exploits to look for. Who is it recommended for? Although this system will scan and patch Linux, it won't run on that operating system. So, if you only have servers running Linux, you can't use GFI LanGuard. The company doesn't publish a price list, which makes recommending the package to small businesses difficult. There is a multi-tenant version of the package for managed service providers. Pay-per-scan option: Metered service or subscription pricing Option for MSPs: Scan and patch the systems of clients Discovers mobile devices: Identify rogue devices connected to the network Doesn't publish a price list: You have to contact the company for a quote GFI Software doesn't offer a free trial and doesn't publish its prices. If you want to move forward with an investigation into GFI LanGuard you can request a demo. 4. SecPod SanerNow Patch Management SecPod SanerNow is a cloud-based system, so this isn't one of those packages that you need to have Windows in order to host. The system will patch Linux, macOS, and Windows. It will also patch more than 450 third-party software packages. The entire SanerNow system provides preventative security scanning for on-premises assets. Key features: Vulnerability scanning: Checks configurations and software age. Port scanning: Identifies open ports and unusual activity. Automated patching: The vulnerability manager automatically triggers the patch manager. Why do we recommend it? SecPod SanerNow Patch Management forms part of a preventative protection system for on-premises assets. This patching system is hosted in the cloud and it will patch Linux. The tool will also patch Windows and macOS, and it has a list of 450 software systems that it will update. Many vulnerabilities, such as misconfigurations and open ports, require manual action. However, the issue of outdated software can be dealt with by the SanerNow platform automatically without human involvement. The system is also able to update firmware on network devices and other equipment. Who is it recommended for? This package is suitable for any business because it doesn't need to be hosted, so you don't need to worry about whether you have the right operating system to run the package. As with many of the packages on this list, SanerNow doesn't have a published price tag, which makes it difficult to recommend the package to small businesses. A comprehensive approach to vulnerability scanning: Also looks at activity to identify security weaknesses Highly automated: Leave the vulnerability scanning and patching systems running all the time in the background Patches the major Linux distros: RHEL, CentOS, Fedora, Oracle Linux, Amazon Linux, Ubuntu, and Debian No price list: You have to contact the Sales Department As this is a SaaS package, you sign up for the service on the SecPod website to get access to the console. Start off with a 30-day free trial. 5. Automox Automox is an endpoint management platform that provides scripts for maintenance automation, called "worklets." The package also provides a patch manager – this is a full service with its own screens, not a worklet. The patch manager is the core service in all plans, and it is able to patch Linux, macOS, and Windows. Key features: Patches multiple OSs: Linux, macOS, and Windows. Operates from the cloud: Installs an agent on each managed site. Maintenance task automation: Provides a library of 345 scripts. Why do we recommend it? Automox, being a cloud-based system, is suitable for all businesses, no matter what operating systems they run on their sites. You don't have to host the software and the console for the package is accessible through any standard Web browser and higher plans provide maintenance automation scripts. The patch manager is able to run unattended and should be given a schedule so that it will only trigger when endpoints are not in use. The package can wake up, reboot, and shut down computers remotely during the patching process. It is possible to set up endpoint groups so only part of your fleet will be involved in each patch run. This is a good solution for companies with a very large number of endpoints. Who is it recommended for? Although any size or type of business could use the Automox system, its ability to partition a fleet into groups for patching and other maintenance tasks means that this package would be particularly useful for large organizations. Automox is available in three plan levels, and all of them include the patch manager. Patch activity logging: Get a record of software versions before and after the patch run Completion statuses: Patches remain in the queue with an error status if they fail Troubleshooting tools: The worklets library includes utilities for investigating problems on endpoints No price list: Prices start at $2 per device per month The Automox platform is a cloud-based SaaS package with three plan levels. The first of these is called Basic and provides just the parch manager. The two higher plans add on system maintenance automation. You can assess the top plan with all the utilities of the platform with a 15-day free trial. 6. KACE Systems Management Appliance KACE Systems Management Appliance is an IT asset manager that focuses on endpoints and software. The package has a number of deployment options that include a SaaS platform and a virtual appliance. The functions of the package provide endpoint asset management tools, which include software license management and patching. Key features: Patches operating systems: Linux, macOS, and Windows. Software management: Distribution and patching. Deployment options: Load it on your cloud account, run it on a VM, or sign up for the SaaS version. Why do we recommend it? KACE Systems Management Appliance helps you to keep track of your IT assets and it is particularly useful for looking after software. This package will maintain an inventory of all of your installed systems and compare them to your record of purchased licenses. You can use the console to set up software profiles per user role and onboard new devices quickly. The package also keeps track of patch statuses. The software inventory management feature in KACE scans endpoints regularly and records all installed systems. This will raise an alert if a new software package appears that isn't in the approved profile for that device. This mechanism makes system administrators aware if users install their own preferred software on endpoints. Who is it recommended for? This system has lots of deployment options, and it can be run on Linux over a VM. IT can also be installed on a cloud account on platforms such as AWS, Azure, or Google Cloud platform. Therefore, companies that only have Linux computers have plenty of choices on where to host the software. There is also a SaaS option available. Patch activity logging: Get a record of software versions before and after the patch run Completion statuses: Patches remain in the queue with an error status if they fail Troubleshooting tools: The worklets library includes utilities for investigating problems on endpoints No price list: Prices start at $2 per device per month KACE Systems Management appliance has many deployment options, and you can get a good look at the system by accessing a 30-day free trial. 7. SysWard SysWard only patches Linux, and you can run the software on Linux. The package is also available as a SaaS platform. Whether you host it yourself or sign up for the SaaS version, you need to install an agent on each of your Linux computers. The agents are available for CentOS, Ubuntu, Debian, RHEL, Rocky Linux, OpenSUSE, SUSE, Amazon Linux, Fedora, Oracle Linux, Vz Linux, Alma Linux, and Arch Linux. Key features: Specialized patching for Linux: Doesn't patch Windows or macOS. Automatic patch availability scans: Checks the current OS version of each machine. Patching schedule: Set up a maintenance calendar. Why do we recommend it? If you have been annoyed by the long list of tools in this review that run on Windows, you will be glad that we have finally included a patching system that will run on Linux. This package can keep many different distros up to date, and you can have a mix of Linux types on your site. This service will run constantly in the background. After you give the tool a maintenance calendar, you won't need to get involved with patching because the service will spot patch availability, acquire the installer, schedule installation, and roll out patch applications without any human involvement. Who is it recommended for? Any business that has only Linux on site would benefit from this tool. Companies that have a mix of operating systems on their endpoint fleet would be better off with a multi-OS patching system. This tool won't patch Windows or macOS. Can be run on Linux: Operates as a virtual appliance within a VM Patches many Linux distros: RHEL, Ubuntu, SUSE, and Raspbian Manages compressed files: Will open zip, tar, and rpm files No price list: You have to request a quote An agent has to be installed on each endpoint and that program reports back to the system dashboard about the operations of the computer, such as memory and CPU usage. You can sign up for a free trial on the SaaS platform or download the software and use it for free. The free trial lasts for 14 days. The following information is available to any site you visit: BLEEPINGCOMPUTER RECOMMENDS: Using a VPN will hide these details and protect your privacy. We recommend using NordVPN - #1 VPN in our tests. It offers outstanding privacy features and is currently available with three months extra free. "JetPatch provided real WOW factor as it innovated our entire vulnerability and patch remediation process. As a result, we were able to meet required compliance, minimize precious downtime, and significantly reduce our risk exposure" Patch management is the practice of deploying software updates, or "patches", to protect a system or network from vulnerabilities. Patch management plays a crucial role in IT system lifecycle management and vulnerability management. A patch is an update provided by a software vendor to fix a technical issue or remediate a security vulnerability. Patches can also include new features and functionalities for the software. Patches secure, upgrade and optimise software (applications and OS). In this blog, we'll cover everything you need to know about patch management, including best practices and challenges of patch management. There are 3 common types of patches: Security patch. One of the main reasons why you should implement patch management is to secure and protect your organization from data breaches. The majority of cyberattacks happened because of outdated software. Patches are created to cover up newly discovered security holes. Unfortunately, these security holes are discovered after they have been exploited. Bug-fixing patch. These patches fix application errors and bugs. They can have a big impact on your organization. For that reason, efficient patch management, which ensures that your applications are updated with the most recent and bug-free version, can provide immediate value for your company. Performance & feature patch. These patches can make the experience of using the applications better, making them load faster. Also, with these patches, software vendors add new features that make using the applications easier and faster. Patch management is a complex and never-ending process. Here are 8 stages of the patch management cycle from discovering an application update to deployment to all users. o update an application firstly you should detect the new version of the application, download and test it before pushing it to the users. If the update is secure and works, you should create a package with a new version of the app. For Microsoft Intune, you should wrap the file into .intunewin, upload it to Intune and deploy it to the assigned users. As soon as you find out that there is a new update available, you must go through the whole process again. And again. A well-implemented patch management system can offer many benefits to an organization, including: Improved security: Patch management can help to ensure that all devices in an organization are up to date with the latest security patches, which can help to reduce the risk of a security breach.Reduced downtime: By keeping devices up to date with the latest patches, a patch management system can help to minimize the amount of downtime that may be caused by unpatched devices.Increased compliance: Organizations that are compliant with industry regulations may find that a patch management system helps them to stay compliant by ensuring that all devices are kept up to date with the latest patches. Patch management is one of the most important, but challenging aspects of your job. Here are the 3 biggest challenges of patch management. Time-consuming According to the Ivanty report (2021), 71% of IT and security professionals find patching complex and time-consuming. Coming back to patching cycle, you must continually identify and assess vulnerabilities, monitor and test patches, and deploy the patches to their systems. Based on the Ivanty survey results, IT & security professionals spend 53% of their working time each month detecting and prioritizing vulnerabilities and 19% testing patches. The biggest problem here is how to find out if there is an update available. Many people think of something like Patch Tuesday with Microsoft. However, it's not like that in most cases – there is no system. And let's consider this: for example, Chrome releases a full OS update about every four weeks. Minor updates, such as security fixes and software updates, happen every 2–3 weeks. Only for patching Google Chrome, an IT specialist must go through the patch cycle 2-3 times a month. But what about other applications? On average, a company uses 110 applications (Statista, 2021). It's difficult to calculate how much time IT admins should spend on patching all the software to prevent the companies from breaches.Patches can break something 72% of managers are afraid that applying security patches right after release could "break stuff." That's true: there is a risk that some things can go wrong with updating software. This can occasionally happen, even if the vendor extensively tested a patch before a patch was released to the public. Sometimes, the reason for a patch failure is that you install the patch and forget to reboot the system. To address this challenge and not "break everything," you must test the updates first in a test environment and then deploy them. 3. Do I have to patch everything? Implementing an inventory management solution can cause another challenge – only highly prioritized vulnerabilities will be patched. This doesn't solve the problem entirely – your company's endpoints are still at risk, and there is no guarantee that you won't be hacked. Read more about the challenges of patch management: Top 5 challenges of patch management How can you improve your patch management process? Fortunately, there are a number of solutions on the market that can make patch management in your organization effective and address the challenges. Below are some best practices to consider for implementation. Create an inventory list of software used in your organization A list of all software, operating systems and devices the company uses is a vital piece of your patch management process. If you have a clear overview of all your endpoints and software installed, you know what you have to protect. With Windows Autopatch it became easier to patch Microsoft products, but you still must patch third-party apps like 7-zip, Adobe and Chrome yourself. Because if you are not patching, this will create multiple attack vectors into your endpoints. Read more about Windows Autopatch here: Getting started with Windows Autopatch: step-by-step guide 2. Monitor application releases and updates With so many applications installed (and so little time), tracking all software updates is critical. In the case of Microsoft products, it's easy – on Patch Tuesday the second Tuesday of each month, Microsoft releases large patches for Windows OS, Microsoft Office and other Microsoft software. But for third-party apps – not so much. Some software vendors publish updates and send email notifications to administrators. 3. Test patches before deploying them to all users Before deploying a patch, it's important to test it in a testing environment. This allows you to verify that the patch does what it is supposed to do and doesn't break anything else. It also gives you time to fix any problems that may arise before the patch goes live. Read more about patch management best practices: 6 patch management best practices Nowadays, organizations must continuously adapt to changes in order to maintain a competitive edge. This is especially true in the world of information technology, where new vulnerabilities are discovered on a regular basis. In order to protect an organization's IT infrastructure from these vulnerabilities, it is necessary to deploy patches and updates as soon as they are made available. Manual patch management can be a time-consuming and error-prone process. It can also be difficult to track all of the patches that need to be applied to an organization's systems. This is where automated patch management comes in handy. Automated patch management solutions can help organizations keep track of all of the patches that need to be applied, and they can automate the process of deploying patches and updates. That's why Scappman should be a part of patch management in your company. Automatically updating all your applications, you save plenty of time that you can spend on other important tasks. You don't need to track all the updates available, prioritize and test them. Scappman will do this job for you. Want to see, how you can automate the update process of your third-party applications? Jump on the call with Scappman. Patch management is the process of identifying, acquiring, testing, and applying patches (or updates) to software systems and applications in order to address vulnerabilities, fix bugs, and improve functionality. It is a critical part of IT security and maintenance. Technology and digital services are constantly evolving, and regularly need attention to ensure there is no space for vulnerabilities to infiltrate. Programmes often release 'patches' for services to ensure they are combatting security and compliance issues, as well as offering the best possible operation. Despite these patches being regularly available, many businesses don't implement them, which can lead to issues around security, compliance and vendor support. Ultimately, not updating your system could lead to a major security breach. Data could be stolen, systems infiltrated, malware installed, phishing attacks launched; the list is endless - and this doesn't only impact your business. A breach of any kind can have a knock-on effect on others within your supply chain, starting a web of security issues and possible, costly down time. Maintaining Cyber Essentials accreditation requires a business to successfully install patches to remediate any 'critical' or 'high' risk within 14 days. If not, a business risks losing its accredited status, potentially impacting other areas of the business such as health and safety, and finance – and could make it ineligible for certain tenders or frameworks. All of which could lead to a loss of revenue. Ultimately, the end must come some time, and vendors, while generous with their support, will choose to end it after a given period. Approved patches should be installed as soon as they become available to ensure the vendor continues to support you. If a business misses several patches for any reason, over time this could leave them far behind the current service, and a vendor can refuse support until a system is up to date. Costly, time consuming, and ultimately fraught with danger. Managed patching is designed to offer a comprehensive and tailored approach to ensuring business systems are on the latest secure and stable version, firmware or update. The service provides a tailored approach for businesses with patching policies developed, schedules agreed, testing metrics applied, and governance and reporting requirements understood and implemented. Ultimately, this ensures that not only do critical updates get installed annually (or whenever agreed), the smaller patches that can make a huge difference to a firm's security posture and vulnerability management, are also implemented. To find out more about managed patching, contact Daniel Wrend at daniel.wrend@waterstons.com. A few years ago, during a SOC 2 audit for a mid-sized SaaS company, we noticed a gap: their patch management program looked solid on paper, but the execution was flawed. The client had a policy that mentioned monthly updates, a ticketing system for patch deployment, and even a patch management report that was presented quarterly. But as we dug into the evidence, we discovered a critical vulnerability had gone unpatched for over six months. The answer to why this happened was both simple and telling: a single server had been excluded from their patch management system due to a misconfigured asset inventory. That single oversight, and the lack of a clearly defined patch management lifecycle, meant that the organization had no process control patches for systems not enrolled in the primary tool. And this wasn't an isolated case. What is Patch Management? Simply stated, patch management is the process of identifying, acquiring, testing, and deploying updates (patches) to software and systems. But the real world is messy. It's one thing to have a process on paper and another to have it work under pressure when your team is juggling other responsibilities or higher-priority items. In the case of our client, the patching process was partially manual, partly automated, and wholly dependent on one system administrator. When he went on leave, things got missed—highlighting why patch management isn't just a technical task, but an organizational responsibility. Read here to learn more about the potential risks of patch management. Why Is Patch Management Important? Many companies think, "We have antivirus and a firewall, why must we focus on patching?" But in SOC 2 audits, patch management is one of the most common areas where we see breakdowns. Unpatched systems often become the cause of control exceptions. It's not just about missed patches, it's about the control failures that allowed those misses to happen. Why patch management is important goes beyond compliance. Vulnerabilities in unpatched systems are often exploited in ransomware attacks and data breaches. For example, a delay in applying a vendor-issued patch for a database system can expose you to a known SQL injection risk. The Patch Management Life Cycle A functioning patch management lifecycle involves several key patch management steps. Asset Inventory – You can't patch what you don't know exists. Most organizations maintain a very basic asset inventory which usually includes Operating Systems, IP Addresses, location, and sometimes the owner. While this is helpful and better than not having an inventory at all, it does not include enough details to properly understand the organization's threat vectors. A best practice is to expand the inventory list to include at least the OS version, installed applications and their versions, the function of the asset (i.e. Domain controller, web server, database), interfaces/services/protocols, and a criticality score. Vulnerability Identification – Once you know what you have, you need to know what's wrong with it. The best way to know if a vulnerability exists is to employ discovery and scanning capabilities. A proper discovery service uses a combination of active and passive scanning features and the ability to identify physical, virtual, and on and off-premise systems. Patch Acquisition – Getting updates from reputable sources. Patch sources should be consistent, authenticated, and auditable, such as Microsoft, Oracle, SQL, etc. You also should define a reliable system for identifying new vulnerabilities. Waiting for the operating system or application to release a patch is not sufficient. In some cases, a new vulnerability may not have a patch available and the organization must mitigate or remediate the risk by other means. Testing – Critical for production systems. Patches should be tested prior to going live. This step is often missed or skipped. To mitigate these risks, organizations with mature patch management programs maintain a dedicated staging environment that mirrors production as closely as possible. Before a patch is pushed live, it is deployed and monitored in staging. This gives teams a chance to review application functionality, performance, and security logging post-patch. Deployment – Automate where possible, but track exceptions. Most people think this step is what makes up patch management, however, while this step is important, to have a working patch management system, all steps should be followed. Review and Reporting – This is where the gaps often surface during audits. Check and report on the patches. A patch was suspected to be applied, and a ticket says it was, however, there's no follow-up to prove it. Review to make sure that the patch was put into place and is working properly. Documentation – Include evidence in your patch management report for audit purposes. How Often Should Patch Management Be Performed? There's no correct answer but the key is consistency and visibility. At a minimum, organizations should be performing vulnerability scans and applying patches on a defined, recurring schedule, typically monthly for standard updates, and as needed for critical vulnerabilities. But timing is only part of the equation. It is important to develop a patch management policy that includes clearly defined frequency requirements and not just for routine updates, but also for how quickly critical or high-risk vulnerabilities should be addressed. The policy should distinguish between different severity levels, environments (e.g., production vs. development), and system types, and it should specify how emergency patches are handled outside the normal cycle. What Are the Different Types of Patch Management? These are the common types of patch management strategies that organizations commonly implement. Security Patch Management: Focuses on fixing vulnerabilities across systems to prevent exploitation. It's essential for protecting sensitive data and maintaining compliance with security standards like SOC 2. Network Patch Management: Involves updating firmware and software on network devices like routers and firewalls for secure and uninterrupted communication. Centralized Patch Management: Uses a single platform to manage patches across an entire IT environment, improving consistency, oversight, and efficiency. Application Patch Management: Covers updates for commercial and custom apps to fix bugs, improve features, and close security gaps without disrupting operations. OS Patch Management: Keeps operating systems current with the latest fixes and enhancements to maintain stability, security, and compatibility. Software Patch Management: Updates software across devices and departments to minimize risks and improve performance. IT Patch Management: Encompasses the overall patching process across an organization's tech stack, supporting both security and operational continuity. Benefits of Patch Management (When Done Right) The benefits of patch management include more than security. They include operational stability, regulatory compliance, and reduced emergencies. A mature patch management program reduces business disruptions. It means fewer high-severity findings in your audits. For the client with the excluded server, their audit ended with a qualified opinion. But the silver lining? They overhauled their patching process, implemented automation with alerts for out-of-band systems, and now run internal mock audits every quarter. That lesson stuck. Common Issues & Roadblocks with Patch Management Even mature environments hit roadblocks with patch management. Here are a few we often see in SOC 2 reports. Unreviewed Exceptions – Exceptions are written when something can't be patched—but they're rarely revisited. If left unchecked, they become long-term risks with no mitigation. Legacy Software That Won't Go Away – Sometimes old systems can't be patched. When that happens, limit access, segment the network, and increase monitoring. Don't let "we can't patch it" be the end of the conversation. Risk in Silos – Looking at vulnerabilities one at a time misses the big picture. A dozen low-risk findings may add up to a high-risk environment if left unmanaged. Policy Without Accountability – A patch management policy isn't effective unless it's enforced. If no one is tracking compliance or holding teams accountable, the policy is just paper. Building a Robust Patch Management Program That Works Patch management is more than just applying software updates; it's a critical security function that often becomes a source of audit findings when overlooked or inconsistently applied. In this post, we explored the full patch management lifecycle – from asset inventory and vulnerability scanning to testing, deployment, and reporting. Drawing from SOC 2 audit experiences, we highlight common pitfalls such as forgotten exceptions, unsupported legacy systems, and policy enforcement gaps. We also explained how to implement an effective patch management program with the right tools, clear roles, and documented processes. Whether you're preparing for an audit or tightening internal controls, this guide offers practical insights into building a patching process that actually works. Linford & Company provides multiple services like SOC 1 audits, SOC 2 audits, FedRAMP compliance certifications, and HIPAA audits that are designed to assess an organization's security management and regulatory compliance effectiveness. Contact us if you would like to discuss our services further. This article was originally published on 8/7/2019 and was updated on 4/9/2025. Jessica joined Linford & Company, LLP in 2023, bringing more than twelve years of experience specializing in SOC 1 and SOC 2 examinations and related assurance services. Her background includes extensive work in internal controls, SOX compliance, ICFR, third-party assurance, and attestations and examinations performed under PCAOB and AICPA standards. Before joining Linford & Company, Jessica spent twelve years with Deloitte, serving in leadership roles for the last eight. She has led numerous SOC engagements across a variety of industries, helping clients strengthen control environments and meet evolving compliance expectations. Jessica is a Certified Information Systems Auditor (CISA) and holds both a Bachelor of Science in Accounting and a Master of Accounting from Southern Illinois University–Carbondale. Failing to patch software vulnerabilities is one of the leading—and entirely preventable—causes of cyberattacks. In fact, according to research by Sophos, one-third of ransomware attacks start with an unpatched vulnerability. The solution? A robust, proactive patch management policy. A patch management policy outlines structured procedures for identifying, evaluating, testing, and deploying patches across all systems in your IT environment. When done correctly, it ensures patches are applied quickly and efficiently, without sacrificing system stability or business continuity. In this blog, we'll explore everything you need to know about patch management policies: what they are, why they matter, how to implement them, and how managed service providers (MSPs) can leverage them to improve customer outcomes and security posture. Key takeaways A patch management policy provides a structured, proactive approach to identifying, testing, and deploying software patches across an organization's IT systems. It helps reduce security risk, minimize downtime, maintain compliance, and improve overall system performance. Core components include clear objectives, defined roles, patch prioritization, testing protocols, deployment schedules, documentation, and exception handling. Common mistakes to avoid include skipping patch testing, ignoring non-security updates, and inconsistent policy enforcement. With increased scrutiny around cybersecurity, businesses and MSPs must adopt rigorous patch management standards to stay secure and competitive. Patch management software, such as ConnectWise RMM™, enables automated, scalable, and policy-driven patch management for IT teams and service providers. What is a patch management policy? A patch management policy is a proactive, structured framework that defines how an organization identifies, evaluates, tests, and deploys software patches across its IT systems. Its purpose is to reduce security risk, resolve known issues, and enable new features while maintaining operational stability. Instead of mindlessly applying patches as they become available, which can introduce unexpected downtime or compatibility issues, a patch management policy ensures that updates are rolled out in a controlled, risk-aware manner. This includes prioritizing patches based on severity, scheduling deployments at optimal times, and documenting all changes for compliance and auditing purposes. These policies are critical for IT and security teams who manage complex infrastructures with potentially thousands of endpoints. A standardized policy helps automate routine updates, protect systems from known vulnerabilities, and align the organization's IT strategy with best practices in vulnerability management and regulatory compliance. In short, a patch management policy is not just about fixing bugs—it's a strategic tool for improving cybersecurity, performance, and operational resilience. Download our Patch Management Best Practices eBook to take the first step toward a stronger, more innovative patch management program. Why do you need a patch management policy? A clear, well-enforced patch management policy is essential for maintaining strong cybersecurity defenses and operational continuity. Without one, organizations risk exposing critical systems to known vulnerabilities, many of which are actively exploited in ransomware and malware attacks. A structured policy ensures that all patches, whether for security, stability, or functionality, are deployed consistently and efficiently. It helps IT teams: Minimize risk by addressing vulnerabilities before they can be exploited Avoid downtime by scheduling updates during low-impact windows Maintain compliance with data protection and cybersecurity regulations Support system performance by incorporating bug fixes and improvements Patch management policies establish clear roles and responsibilities, ensuring accountability across departments and service providers. They enable faster response times when urgent vulnerabilities arise and reduce the burden of manual patch tracking and documentation. A defined policy provides a scalable foundation for automated patch deployment, continuous monitoring, and real-time reporting. It transforms patching from a reactive chore into a proactive strategy that drives security and business continuity. Components of an effective patch management policy An effective patch management policy provides a repeatable, secure, and transparent framework for keeping systems updated and protected. Whether you're an IT professional managing patches in-house or an MSP managing patches for multiple clients, the following seven components are essential for building a strong, risk-resilient policy: Define what your patch management program is intended to achieve. Common objectives include: Enhancing cybersecurity posture Ensuring regulatory compliance Minimizing system downtime Supporting business continuity and performance Clear goals help determine patch prioritization, scheduling, and reporting strategies. Roles and responsibilities Assign specific roles for team members involved in the patch lifecycle. For example: Patching policy creation and continual improvements Patch policy

compliance monitoring Patch testing and approvals Accountability ensures consistent enforcement and response. Patch priorization criteria Not all patches carry the same level of urgency. Establish guidelines for: Evaluating severity (e.g., security updates and critical patches vs. low-impact updates) Aligning patch urgency with business risk Integrating threat intelligence and vendor advisories Prioritization helps maximize security impact with minimal resource strain. Testing and validation procedures Test patches in a staging environment to verify compatibility and avoid service disruption. Validation steps might include: Manual testing for software conflicts Patch compliance scanning post-installation Pilot rollouts to select systems before wider deployment Thorough testing prevents unintended consequences of patching. A consistent deployment cadence improves reliability and planning. Define: How often patches are applied (e.g., weekly, biweekly, monthly) What days/times patches are scheduled to avoid peak usage Notifications and other communication with end users to boost compliance Emergency protocols for zero-day vulnerabilities This ensures critical patches are applied quickly, while routine updates or security updates are managed predictably. Documentation and reporting Maintain a detailed audit trail that includes: What patches were installed Outcomes (success or failure) Documentation supports compliance audits, performance analysis, and continuous improvement. Not all systems can be patched under standard procedures. Your policy should account for: Business-critical systems that can't experience downtime Legacy software or hardware where patches aren't available or compatible Documented risk acceptance procedures and mitigation strategies (e.g., network segmentation, virtual patching) Having an exception protocol ensures that unpatched systems are identified and monitored. How to implement a patch management policy Once a patch management policy has been defined, it must be carefully rolled out to ensure adoption, effectiveness, and continuous improvement, Follow these six steps for successful implementation: Communicate the policy organization-wide Begin by distributing the policy to all relevant stakeholders. Ensure that individuals are aware of their responsibilities Communicate the importance of patching for security, stability, and compliance Consider conducting training sessions to walk through the policy and tools used This builds buy-in and helps prevent resistance or confusion. Assess and inventory all systems You can't patch what you don't know. Start by: Performing a complete asset discovery of inventory hardware, software, and operating systems Identifying critical systems and classifying assets Mapping systems to owners for accountability This baseline is essential for policy enforcement. Set up patch management tools Choose tools that align with your policy's goals, such as remote monitoring and management software that offers patch automation and scheduling systems. Ensure the tools integrate with your ticketing, reporting, and alert systems. Start with a pilot rollout Implement the policy in a controlled environment: Choose a small, representative subset of systems Monitor results, gather feedback, and refine processes Use this phase to validate testing workflows and exception procedures This reduces the risk of disruption and helps fine-tune the rollout. Scale gradually across the organization With the pilot complete: Expand patching across endpoints managed Use automation to scale processes while maintaining control Monitor success metrics, such as patch compliance and reductions in patching-related tickets generated A phased approach ensures stability and stakeholder confidence. Review and improve regularly Security is dynamic, so your patch policy needs to evolve. Regularly: Reevaluate patch prioritization based on new threats Assess tool performance and process bottlenecks Incorporate feedback from your team and customers Schedule annual or quarterly policy reviews and update documentation as needed. Mistakes to avoid for patch management policies Even with a solid patch management policy in place, missteps in execution can expose your organization to unnecessary risk. Many businesses underestimate the complexity of patching or overlook key details that can compromise their security posture. Below are five common patch management mistakes—and how to avoid them. Ignoring non-security patches It's a mistake to focus only on security updates. While security patches often receive top priority, updates that fix performance bugs or improve functionality can affect system security and stability. For example: Non-security patches may resolve underlying issues that could later become exploitable Performance fixes can reduce crashes and support user productivity Issues with approved software can lead to increased usage of unapproved software Best practice: Evaluate all patches with your end users' context in mind and include them in your regular patching cycle with the correct guardrails to prevent possible issues. Deploying untested patches can lead to software conflicts, broken integrations, or system outages. Common oversights include: Skipping validation in test environments Applying patches across all systems without a pilot group Relying solely on vendor documentation Best practice: Always validate patches in a sandbox, staging, or otherwise controlled environment before full deployment. Establish a testing protocol as part of your patch management policy. Inconsistent policy enforcement A policy is only as effective as its enforcement. Applying patches selectively, allowing end-users to opt out, or significantly delaying patching can introduce dangerous inconsistencies, leading to unpatched systems. Best practice: Enforce your patch policy organization-wide while creating standards by site, patch type, or device, as well as limited, well-documented exceptions. Use centralized tools to monitor and report on compliance. Lack of documentation and audit trails Failing to track patching activities creates gaps in visibility, making it difficult to respond to incidents, demonstrate compliance, or identify missed updates. Best practice: Maintain detailed logs of: Comprehensive documentation is vital for troubleshooting, audits, and continuous improvement. Overreliance on automation without oversight Automation is essential for scalability, but it can't replace human judgment. Deploying patches without proper monitoring can result in critical misconfigurations or unintended consequences. Best practice: Balance automation with manual oversight, especially for high-risk or business-critical systems. Monitor for anomalies post-deployment and perform regular tool audits. Avoiding these mistakes can dramatically improve the effectiveness of your patch management strategy, reduce downtime, and protect your organization from avoidable vulnerabilities. Conclusion In today's high-risk digital environment, patch management isn't just a security best practice—it's a business necessity. As high-profile vulnerabilities such as Log4j, MOVEit, and SolarWinds make headlines, the tech industry faces unprecedented scrutiny. This increased public visibility around cybersecurity is driving more organizations, especially in regulated industries, to adopt stricter, standards-based patch management policies. There's less room for error. Business decision makers, IT professionals, and end users now expect businesses to maintain rigorous, transparent, and proactive software maintenance protocols. Without a clearly defined and consistently enforced patch management policy, organizations risk: Whether you manage an in-house IT team or operate as an MSP for multiple businesses, a formal patch management policy builds trust, reduces risk, and critically improves your security posture across your entire IT ecosystem. ConnectWise RMM helps IT teams automate OS and third-party patch deployment, monitor policy compliance, and use real-time alerting and access to remediate issues quickly. ConnectWise NOC Services™ systematically tests all Windows OS security updates and provides approval recommendations and research to our entire partner base so you can confidently patch the most critical updates. Achieve patching peace of mind and help your team turn complex processes into a scalable workflow. Watch a demo or contact us today to learn more about how we can help! We're sorry, your browser appears to be outdated.To see the content of this webpage correctly, please update to the latest version or install a new browser for free, such as Avast Secure Browser or Google Chrome. One of the most common intrusion methods for hackers is exploiting unpatched software vulnerabilities. Proven, industry-leading patch management that keeps all your Windows systems and third-party apps up-to-date with the latest patches. Distribute thoroughly tested patches to thousands of machines in minutes, with minimal impact on your network. Patching support for Microsoft Windows and hundreds of popular vendors like iTunes®, Oracle® Java, Adobe® Flash® and Reader, and more. Patch all devices — whether they're behind the firewall, on the road, at remote sites, or even asleep. Manage all Microsoft Windows and hundreds of third-party software updates from one online management platform. Achieve compliance, mitigate exploits, close vulnerabilities, and remotely deploy software and Windows updates. Easy-to-use platform for ultimate control Our online management platform gives businesses and IT admins total control over the entire patching process, including patch discovery, distribution of software updates, and reporting. 30-day money-back guarantee Patch Management accelerates the software update process, taking it from months to just minutes. Our team of patch content engineers carefully inspects each patch before it gets released to you, ensuring proper compliance. We apply our years of industry experience and innovation to the test, empowering you to quickly patch and secure your third-party apps. Select the frequency of the patch scan, either daily, weekly, or monthly, and schedule when you would like the scan to take place. All vendors, software applications, and severities will be patched automatically, but you can easily exclude individual ones from application patching if needed. From the dashboard, you can view missing patches, patch names and severity levels, along with release notes, release dates, and more. Keep up with security threats and patches Patch Management and our other solutions are deployed through the Business Hub empowering you to seamlessly manage endpoint security for all your devices from a single platform. 30-day money-back guarantee Purchase Avast Business solutions directly from the site and start protecting your endpoints today. Speak with an expert from Avast for Business. No matter what type of business you have, we have a solution for you. Everything you need to know to use Patch Management like a pro No, you should not disable the Windows Update service, but you do need to adjust the Windows Update settings via the Windows Update Center and/or Group Policy. This is so Patch Management can provide updates.The Windows Update settings should be set to either Manual or Automatic to successfully deploy patches. In addition, the Windows Update setting on each target machine (Control Panel > System and Security > Windows Update > Change settings) should be set to Never check for updates. Deployment of patches will run under the remote machine's Local System account, so make sure this is allowed. You can set up your patch schedule in Device Settings > Policy > Patch Management > Step 2. All devices or groups under the Patch Management policy will follow the schedule you set. Simply go to your Patches page, which will provide detailed information on the severity of missing or installed patches with vendors, and on software applications. You will be able to see how many devices are licensed for patch under the 'Subscriptions' section in the console. This could be due to the following reason(s):The patch is currently being installed on those devices and will sync back with the console after the patch has been successfully installed.The patch could have failed to install and will be scheduled for a reinstall based on your patch deployment schedule.The device is offline. You can modify the patch deployment schedule and exclude vendors and applications by going to Device Settings > Select Policy > Patch Management tab. Yes, you can manually deploy patches to individual devices and groups of devices in one step. Patches will be in one of the following states:Scheduled: Grey Icon - Patch approved and scheduled to be deployed to device/sDeployed: Green Icon - Patch successfully deployed to device/sFailed to deploy: Red Icon - Failed to deploy patch/es to device/sMissing: Yellow Icon - Patch is missing from device/sWaiting to scan: Grey Icon - Waiting to run patch scan on deviceFailed to scan: Red Icon - Failed to run patch scan on device It could take a few seconds or several hours. The time depends on the size of the patch that is being downloaded to the device, the software application it is updating, and the hardware of the device. Yes, the device you have selected as the Master Agent will be used to store the software application patches and will distribute them to devices on the network to save bandwidth. If you do not have a Master Agent selected, devices will download the software application patch directly from the internet (not recommended). Visit our support center for more FAQ's Patch Management 30-day money-back guarantee Environment: _____ Template: _____ {%value%} per device per year","qty":"QTY:","quantityError":"Select {%minQuantity%}-{%maxQuantity%} devices or contact sales.","quantityErrorGeneral":"Please review the quantity field for each product and try again.","readyToCheckout":"I'm ready to check out","removeFromCart":"Remove from cart","removeQuantityFromCart":"Remove {%quantity%} from cart","resultForSelections":"Result for your selection of:","saveAmount":"You save {%value%}","savePercent":"Get {%value%}% off","saveMoreByLengthening":"Save more by lengthening your protection","selectAllThatApply":"Select all that apply","stepBack":"Step back","talkToExpert":"Talk to an expert","total":"Total:","totalPrice":"Total price:","trial":"START 30-DAY FREE TRIAL","vatInfo":"All Prices are without VAT","youMayNeed":"You may need","youWillAlsoNeed":"We also recommend","days":"Days","hrs":"Hrs","min":"Min","sec":"Sec","currentPrice":"Current price","originalPrice":"Original price","belowRenewalQuantity":"You lowered the number of devices below your current plan ({%quantity%}). Please make sure this amount is sufficient for you."} data-locale-settings= { "locale": "en-gb", "ulocale": "/en-gb", "currencySymbol": "£", "decimalSeparator": ".", "priceFormat": "#c#p", "precision": "2", "thousandSeparator": ",", "isSoftline": 0, "installments": 0 } data-src={"i": " , "o": " }> 15 July 2024 System patches might not always take centre stage in cybersecurity discussions, but they play a crucial role in maintaining the integrity of your digital infrastructure. In our interconnected world, understanding the different types of patches and their influence on system security is essential knowledge for business leaders and IT professionals alike.This blog will demystify patches so you can implement a patching strategy that fortifies your systems against the evolving threats of the digital landscape. Before we dissect the different categories of patches, it's vital to understand the overarching importance of patch management.First, a simple question: "What are patches?"Patches are updates software vendors release to fix identified bugs and vulnerabilities or improve their products' functionality. Neglecting to apply these updates can leave your systems open to exploitation by malicious actors. The Critical Nature of Security Patches Starting with the most critical type, security patches are issued in response to vulnerabilities that have been discovered. These patches are not optional; they are necessary to prevent potential breaches. Cyber threats evolve continuously, and new vulnerabilities are a constant security concern. Without timely application of security patches, businesses face the risk of data breaches, systems hijacking, and many other dangers. Feature Patches and Systems Enhancement Feature patches are about more than just security. They introduce new features or enhancements to the software, potentially improving user experience and operational efficiency. However, they also come with their own set of risks. A balance must be struck between the desire for additional features and the need to maintain a secure system. Knowing what feature patches to install and which to ignore is best left to trusted IT professionals. Compatibility Patches for Fluid Operations Compatibility patches ensure your system's software functions smoothly with existing and updated operating environments. Incompatibility can lead to performance issues or system failures, directly impacting your business operations and possibly affecting your security posture. In isolation, each patch mitigates specific risks within the software for which it is designed. Together, the patches create part of a holistic defence strategy that protects the software in question and the entire ecosystem. Neglecting one type of patch affects the whole system's integrity, potentially leading to so-called 'chain reactions' of vulnerabilities. In a Forbes article titled, The Imperative of Patching: A Resolution for Cybersecurity in 2024, author Emil Sayegh said, "Recent cybersecurity events, highlighted by a major breach at ICBC bank, have cast a glaring spotlight on the importance of patching as a vital component of cybersecurity." Sayegh notes, "In an era where digital threats are constantly evolving, patching is not a choice but a necessity." Given that patch management is complex and multifaceted, it's crucial to establish structured processes to handle patches effectively. Proactive patch management is not a one-time event but an ongoing practice requiring strategy, oversight, and adaptability. A systematic approach to patch management involves identifying the patches relevant to your systems and establishing protocols for prompt deployment. This should include prioritising security patches while considering the impact of feature and compatibility updates. Automated patch management tools can significantly streamline the process, ensuring that critical updates are not missed. However, manual oversight should always complement these tools, particularly when assessing the potential impact of updates on system performance or compatibility. Effective patch management also requires continuous monitoring of vendor communications for patch releases. Once patches are identified and deployed, systems should be thoroughly tested to ensure the updates do not introduce new issues or conflicts. Whether you manage patching in-house or outsource it to a Managed Service Provider (MSP) ultimately depends on your organisation's needs and capabilities. While managing patching internally may seem cost-effective, it requires significant resources and dedicated staff to stay on top of updates and potential vulnerabilities. Outsourcing to an MSP can alleviate this burden while providing the cybersecurity expertise needed to leverage Patch Management within the scope of a comprehensive cybersecurity strategy. Awareness and diligence in patch management are integral components of a comprehensive cybersecurity strategy. By understanding the different types of patches and their collective impact on systems security, you can make informed decisions that safeguard your business against cyber threats. Stay abreast of the latest patch releases and prioritise a proactive approach to system maintenance. Remember, in cybersecurity, the strength of your defences is only as good as your weakest link – and an unpatched system is a weak link. Need some help keeping your systems patches up to date? Let us help you protect your data and workflow by providing your business with worry-free Patch Management service. Contact us today so we discuss your next steps. Learn more about our Patch Management service Wed | Feb 7, 2024 | 11:38 AM PSTIT administrators and operations managers are responsible for overseeing much of any given organization's incumbent security practices. Upholding best cyber defense practices and maintaining a robust posture across systems and networks is a constant balancing act, especially given the evolving threat landscape of today. As malicious actors find sophisticated new methods of compromising systems and exploiting valuable data, organizations have to adapt and innovate their defense strategies methodically. This is made more challenging as organizations become increasingly more "remote." Their systems and processes need to be flexible enough to scale while providing short- and long-term worker flexibility. Luckily, new real-time collaboration tools, software, and solutions enter the market to make digital transformation challenges easier to overcome, while positioning organizations on the right path towards achieving their scaling targets. However, maintaining oversight over the workability and value of various systems and tools is no easy feat either. Software, as we know, is increasingly prone to bugs and vulnerabilities, and must be kept in good working order to maintain worker and organizational productivity. This is where the process of security patch management comes into play. Patch management in a modern cyber defense ecosystem Patch management is a vital process that allows IT and operations specialists to identify, prioritize, test, and deploy relevant patches and updates for software, firmware, drivers, and APIs across an organization's entire infrastructure. Whether it's an employee desktop, a dormant endpoint device, or a cloud-based document storage system, they all need to be secured and patched. It doesn't have to be the remit of companies the size of Google, for example; patch management is crucial for organizations of all shapes and sizes. The risks of ignoring patch management can be severe, as unpatched devices are more prone to breaches, while productivity can be impacted, not to mention the potential reputational effects should sensitive or customer data be exploited. What does patch management involve? The process of patch management will vary depending on an organization's incumbent setup and complexity. However, the process can often be broken down into several key steps: Inventory – Discovering all hardware, drivers, and software on networks to know precisely what needs patching Prioritization – Determining the severity of vulnerabilities and risk to categorize patch criticality Testing – Validating patches in a development environment (such as a test server) before deployment Deployment – Installing patches systematically across the organization Verification – Confirming patches have been correctly and successfully installed Reporting – Producing documentation on patching status for compliance Undertaking these steps provides greater visibility into an organization's cyber hygiene and risk exposure, allowing IT teams to methodologically and proactively instigate the correct patches to uphold security. How does patch management fit into cyber defense posture? Patch management, much like other cyber defense strategies such as vulnerability scanning, incident response, risk assessments, or penetration testing (pen-testing), mustn't be viewed as a siloed exercise. It should not operate in isolation; instead, it should link seamlessly with other security disciplines, control processes, and other threat containment and risk mitigation steps. Integrating these cyber disciplines ensures that patch management complements other priorities across an incumbent setup, rather than causing obstructions or conflicts. In systems where real-time collaboration and productivity must be maintained, uptime and availability of critical systems should be a priority. Therefore, aligning patch rollout with vulnerability management, change control, and threat intelligence is a much more efficient and proactive way to ensure that security updates are rolled out promptly and to the highest-priority devices first. In addition, organizational patch management relies heavily on clear top-level policies and standards that rely on systematic alignment. Doing so is often a governance and compliance exercise for organizations, but patch management mustn't be ignored when establishing these policies from the off. Such policies may mandate strict timeframes for rollouts after vendors release core OS updates or application firmware patches, or perhaps dictate specific testing requirements pre-deployment. Policies may also instruct IT teams to follow stringent criteria when determining the validity and sensibility of patches in a staging or development environment before they are rolled out into live systems and networks. Why is effective patch management essential? Patch management is one small piece of the overall cybersecurity puzzle, but there are crucial reasons why getting it right delivers immense value in terms of upholding correct cybersecurity and hygiene. It reduces the attack surface.Without system updates and patches, vulnerabilities can be more easily and actively exploited by cybercriminals. Patching means that these security gaps can be proactively closed. It limits the impact of breaches.If threat actors do infiltrate networks, damage from lateral movement and data exfiltration is constrained when flaws are patched. It optimizes resource usage.IT teams have extensive stacks of hardware and software to maintain. Patch management lets admins prioritize based on severity, to focus on fixing critical issues first. It helps firms achieve compliance standards and regulations.Many organizations must satisfy domestic, federal, or global regulations as far as data protection goes. This includes PCI DSS, HIPAA, NIST, GDPR, and more. It's cost- and time-efficient in the long run.Breaches cost organizations nearly $4.45 million on average globally, according to the IBM Cost of a Data Breach Report 2023. Staying on top of patching significantly reduces financial damage and productivity lost due to outages. Patch management best practices Implementing and upholding patch management policies is a responsibility thrust upon many IT teams, many of whom may be stretched thin. However, it's important to bear a few key tips in mind to cultivate an organization that understands, recognizes, and commits to keeping patch management top of mind when it matters. Patch management is more than simply updating operating systems and core hardware; it refers to every aspect of all computer stacks that belong to and are used by organizations and their users. Automate tasks where possible using enterprise-grade management tools to maintain uptime and speed without hindering worker productivity. Segment environments so that patch tests and analysis can be conducted without directly impacting others. Communicate patch management cycles throughout the organization, allowing users to prepare for rollouts and adjust their workloads accordingly. Conduct soft launches or sandbox testing exercises to evaluate patch effectiveness on a small segment of users before determining its suitability for broader organization-wide deployment. Maintain a culture that embraces transparency and feedback. Ensure that teams know exactly who is responsible for patch management and how to communicate anomalies or suspicious behavior of systems pre- or post-rollout. Regular cycle prevents exploitable gaps Fundamentally, it's important to recognize that patch management offers more long-term value and advantages to organizations than drawbacks. By continually cycling through effective patch and repair regimes, businesses can drastically reduce their threat exposure and chances of succumbing to costly data breaches. With attacks growing in complexity and frequency, patch management is evidently a crucial cyber discipline for businesses looking to remain stable in a volatile and risk-heavy threat landscape. In a digital world where cyber-attacks are multiplying and vulnerabilities are being discovered on a weekly basis, ignoring security updates is like leaving your door wide open in the middle of the night. This is where patch management comes in. This often underestimated process is a cornerstone of enterprise cybersecurity. It enables software vulnerabilities to be quickly corrected, sensitive data to be protected, and a healthy, compliant, high-performance infrastructure to be maintained. But beware: between automation, prioritization, and the tools to choose from, good patch management doesn't just happen. In this article, we decipher together what patch management is, why it's crucial for your IS, and how to implement it efficiently as part of an optimal strategy, step by step. The answers in this article! See all software Computer Security What is patch management?Definition Patch management is a centralized process that involves : identifying computer vulnerabilities, prioritize actions, acquiring or loading corrective updates, testing patches to identify potential problems and check that they correct the flaws for which they were developed, plan patch installation according to the characteristics of the services and functions concerned, deploy patches and functional updates. Note: the patch management process also includes an installation acceptance phase and a documentation phase covering patches, vulnerabilities and test results. This provides an up-to-date history that completes the inventory of the company's IT assets and proves its compliance with cybersecurity regulations in the event of an IT security audit. These documented procedures simplify any backtracking in the event of uncontrolled side-effects of a major update.What are the objectives of patch management, and why is it important?As soon as a vulnerability or bug is detected, software publishers, IT and mobile equipment manufacturers, networkAs soon as a vulnerability or bug is detected, software publishers, computer and mobile equipment manufacturers and network equipment suppliers release minor and major updates to correct security flaws and resolve bugs. Updates are also used to add new functionalities, or even improve system performance. Deploying a patch management policy in your company is important, as it is an effective way of combating cyberthreats targeting system and equipment vulnerabilities. It also ensures the compatibility, stability (risk of breakdowns) and performance of the tools available to the company's players.What is a patch management policy?A patch management policy is a documented process that formally and exhaustively defines the procedures for updating the company's various IT assets. It establishes the roles and responsibilities of the people involved, schedules the various phases, and defines the objectives to be achieved according to the nature of the patches and their criticality. The patch management policy also defines the scope of patch management. To sum up, the patch management policy is essential for guaranteeing the correct installation of patches, system security and performance over time, and limit downtime. It must also include a contingency plan, with the possibility of rolling back the system in the event of a problem. A recent backup or disk image should be available to reinstall the system as it was before the patch was applied.As patch management in the enterprise is often complex, it is possible to use patch management software in stand-alone mode, or as part of a more global IT security policy.Types of patches and their impact on IT infrastructurePatches are an integral part of the lifecycle of a company's hardware and software assets. They ensure that systems remain compliant and usable throughout their lifetime. This means regularly monitoring software publishers and suppliers to ensure that systems are compatible with the equipment on which they are deployed, evolving usage and user expectations, and secure. Patches come in various forms: Security patches, Bug fixes, Functional updates and additions, Performance improvements, Regulatory compliance. The implementation of security patches and the various updates have a decisive impact on the smooth running, reliability and longevity of even the most complex IT infrastructures. A rigorous patch management policy : considerably reduces vulnerabilities to intrusion attempts via obsolete code, installation of malware, ransomware..., optimizes software operation (improved performance, enhanced functionality), and ensures regulatory compliance, particularly in terms of data protection. What are the risks of poor patch management?Poor patch management exposes a company to major risks. If patches and updates are not regularly installed on operating systems, applications, terminals and network equipment, infrastructures can be compromised: Risk of loss of compatibility between the various components of the information system, Risk of cyber-attacks on the IS that could jeopardize the organization and expose its employees, Edge effects impacting at the very least the performance of the IS as a whole, and potentially serving as an entry point for the theft of confidential data or hacking. Automating patch management with patch management software saves considerable time and increases efficiency. By implementing automatic routines for distributing and installing updates and patches, you can : industrialize procedures, avoid human error, and systematically apply the right patch versions to all terminals at the right time. ⚡ The precision and speed with which tasks are carried out means you can be reactive when a flaw is discovered, effectively reducing cybercriminals' window of attack. This automation of patch management procedures also improves compliance thanks to the production of summary reports and traceability of actions. Similarly, patch management automation software reduces the work load on IT teams, who can focus on the analysis phases. A forward-looking calendar can help IT teams in charge of patch management to anticipate the deployment of updates and the application of patches. There are different types of updates, with different planning requirements: Security patches, to be deployed as soon as they are released. Functional updates, to be scheduled on a monthly or quarterly basis. As the frequency of major updates depends on the schedules of hardware, network and telecoms publishers and suppliers, it's important to keep abreast of their news, so as to integrate the provisional release schedules of the various versions. Important: this planning work is complex. It must be regularly updated and communicated to all stakeholders, so that everyone can anticipate any unavailability of IT assets.Documenting and tracking updates is one of the best practices for effective patch management procedures. Documentation is essential for reasons of compliance and traceability of operations linked to the integrity and security of a company's information systems. It also provides the various parties involved with a detailed history of events and installed versions, and ensures accurate tracking of updates, enabling them to revert to a previous, more stable version if necessary.6 steps to an optimal patch management processStep 1: Asset identificationThis initial phase consists of making an inventory of all components, in order to establish a precise mapping of the IS. The aim is to compile an exhaustive, detailed list of all IT assets (date commissioned within the company, systems and applications installed, versions, etc.).Step 2: Vulnerability assessmentThe aim of this stage is to identify and analyze vulnerabilities in the various components of the information system (bugs, security holes, obsolete software, inappropriate configurations). This makes it possible to map vulnerabilities precisely, assess the level of risk for each component and for the IS as a whole, and draw up recommendations in line with current regulations.Step 3: Prioritizing patches according to threatsOnce the vulnerabilities of IT assets have been assessed, it's easy to prioritize the actions to be taken: installation of security patches and updates to reduce the risk of cyber-attack.Step 4: Patch testing and validationThis essential step in the patch management process consists of field-testing the installation and effectiveness of security patches and other updates on a configuration representative of the software and hardware park concerned. This test enables you to: assess patch compatibility, check that installation and implementation do not affect system performance and stability. Validating these tests is essential for launching patches and IT asset updates.Step 5: Patch deploymentPatch deployment can be envisaged in several stages. First of all, the most critical systems are updated, then the entire installed base is gradually rolled out. This must be done quickly to reduce the attack surface. ☝ Until a link in the information system has been patched, the whole system remains vulnerable. The automation of this process, made possible by patch management, speeds up the systematic distribution and installation of patches and updates, according to a secure, documented procedure.Step 6: Monitoring resultsEqually important, results monitoring provides a comprehensive overview of operations. Using key indicators, teams measure in real time the progress of patch and update implementation on the target fleet, analyze failures and rollbacks, and monitor the effectiveness of installed patches. Monitoring must be documented to keep a history of versions and events, validate the effectiveness of the patch management process, and benefit from feedback for the continuous improvement of these cybersecurity procedures.Several patch management solutions are available: Heimdal Patch Management Software. This cybersecurity technology platform automates vulnerability management, with patch deployment on Microsoft and Linux OSs, and on third-party and proprietary software, both on site and remotely. This tool gives you complete visibility and precise control over all your software assets. Patch and Asset Management Learn more about Heimdal Security ManageEngine Patch Manager Plus. This patch management platform, available as a cloud or on-premise service, offers automated patch deployment on servers and workstations running Windows, macOS and Linux OSs. All-around patching solution Learn more about Patch Manager Plus NinjaOne Patch Management. This solution supports remote management and monitoring of Windows, macOS and Linux, as well as over 135 third-party applications running on Windows. It automates patch identification, approval and deployment, as well as reporting on update operations. Automated and Secure IT Asset Management Learn more about NinjaOne (ex-NinjaRMM) Atera. This remote monitoring and management cloud platform offers powerful patch management automation, custom scripting, network discovery, trouble ticket management, automatic report generation, real-time alerts... Managed Service Providers (MSP) Software Learn more about Atera How do you choose your patch management software?Choosing a patch management solution involves a number of important criteria: Operating systems supported, Process automation solutions, Patch status and compliance reporting, Functional coverage of patch management processes (inventory, testing, evaluations, etc.), ease of use, Pricing. The chosen solution must also be adapted to the size and complexity of your IT assets.What role does artificial intelligence play in patch management?The use of artificial intelligence in patch management considerably enhances the performance and efficiency of various processes. AI enables the intelligent automation of processes to combat vulnerabilities through : Rapid detection and identification of vulnerabilities, Intelligent prioritization of patches, Automated deployment of patches and asset updates, Follow-up management, Automatic generation of documentation and compliance reports. By integrating an approach based on predictive analysis, artificial intelligence continuously improves patch management strategy. See all software Computer Security Invest in effective patch management for a secure futureWith companies constantly being targeted by sophisticated cyberattacks, automated management of security patches, bugs and functional updates must be part of your cybersecurity strategy. Security flaws are systematically exploited by cybercriminals to penetrate IS, steal data and install malware for criminal purposes. By installing patch management software with artificial intelligence, you can protect your information system simply and effectively. Article translated from French Skip to content AI Hybrid cloud Learn how to use our cloud products and solutions at your own pace in the Red Hat® Hybrid Cloud Console. Products Training Learn Discover resources and tools to help you build, deliver, and manage cloud-native applications and services. Partners Find solutions from our collaborative community of experts and technologies in the Red Hat® Ecosystem Catalog. Search ConsoleDocsSupportFor you Log in Console access Event registration Training & trials World-class supportA subscription may be required for some services.Log in or register Patch management is an administrator's control over operating system (OS), platform, or application updates. It involves identifying system features that can be improved or fixed, creating that improvement or fix, releasing the update package, and validating the installation of those updates. Patching—along with software updates and system reconfiguration—is an important part of IT system lifecycle management and vulnerability management. Patches are new or updated lines of code that determine how an operating system, platform, or application behaves. Patches are usually released as-needed to fix mistakes in code, improve the performance of existing features, or add new features to software. Patches are not newly compiled OSs, platforms, or applications—patches are always released as updates to existing software.Patches can also impact hardware—like when we released patches that altered memory management, created load fences, and trained branch predictor hardware in response to the Meltdown and Spectre attacks of 2018 that targeted microchips. Because modifications like these are usually quicker to distribute than minor or major software releases, patches are regularly used as network security tools against cyber attacks, security breaches, and malware—vulnerabilities that are caused by emerging threats, outdated or missing patches, and system misconfigurations. Because patching without a clearly defined patch management process can get messy. Enterprise IT environments can contain hundreds of systems operated by large teams—requiring thousands of security patches, bug fixes, and configuration changes. Even with a scanning tool, manually sifting through data files to identify systems, updates, and patches can be onerous. Patch management tools help generate clear reports on which systems are patched, which need patching, and which are noncompliant.Learn how Red Hat Satellite simplifies patch managementPatch management best practicesUnpatched and out-of-date systems can be a source of compliance issues and security vulnerabilities. In fact, most vulnerabilities exploited are ones already known by security and IT teams when a breach occurs.Identify systems that are noncompliant, vulnerable, or unpatched. Scan systems daily.Prioritize patches based on the potential impact. Calculate risk, performance, and time considerations.Patch often. Patches are usually shipped once a month or sooner.Test patches before placing them into production.Patching strategy should also account for cloud and containerized resources, which are deployed from base images. Ensure that base images are compliant with organization-wide security baselines. As with physical and virtualized systems, scan and patch base images regularly. When patching a base image, rebuild and redeploy all containers and cloud resources based on that image. Implementing a vigilant patch management policy takes planning, but patch management solutions can be paired with automation software to improve configuration and patch accuracy, reduce human error, and limit downtime.Automation can drastically reduce the time IT teams spend on repetitive tasks, like identifying security risks, testing systems, and deploying patches across thousands of endpoints. Managing these time-consuming processes with reduced manual input frees up resources and enables teams to prioritize more proactive projects.For example, a handful of Red Hat® Ansible® Automation Platform modules can automate portions of patching processes, including invoking HTTP patch methods, applying patches using the GNU patch tool, and applying (or reverting) all available system patches. For many organizations, multiple servers work together for one customer, and these servers—since their functions are intertwined—must be rebooted in a specific order when patches are deployed. With Ansible Automation Platform, the Ansible Playbook ensures this happens correctly and consistently, so IT teams don't have to. With more than 500 servers using Red Hat Enterprise Linux under their charge, Emory's IT team knew they had a difficult road ahead if they had to install the patch manually, which would expose the university's infrastructure to cybersecurity threats. The solution was to use an Ansible Playbook to apply the patches automatically to each server. While patch deployment and remediation across all servers would have taken up to two weeks, it took only four hours.Read the case studyADB has significantly reduced the time needed to complete provisioning, patching, and other infrastructure management tasks with Ansible Automation Platform. The organization saves around 20 work days per month with automated patching processes and around 2 hours per incident with automated data recovery. Read the case studyTextiles manufacturer Glen Raven adopted Ansible Automation Platform to optimize processes that were previously handled manually, such as infrastructure management, patching, and certificate automation. They moved from time-consuming, disruptive patching to an automated process that completes patching in 35 minutes.Read the case study LinkedInYouTubeFacebookXProduct trial centerRed Hat StoreBuy online (Japan)ConsoleContact salesContact customer serviceContact trainingSocial Red Hat is an open hybrid cloud technology leader, delivering a consistent, comprehensive foundation for transformative IT and artificial intelligence (AI) applications in the enterprise. As a trusted adviser to the Fortune 500, Red Hat offers cloud, developer, Linux, automation, and application platform technologies, as well as award-winning services. © 2025 Red Hat [Please note that this template serves only as a starting point. You can customize it to suit your organization's specific patch management requirements, processes, and policies.] [Your organization's name] patch management policy1. Overview This patch management policy outlines the procedures and guidelines for effectively managing software patches within [your organization's name]. Patch management is a critical component of our cybersecurity strategy. It aims to reduce security risks, enhance system reliability, and ensure infrastructure stability. 2. Purpose The purpose of this policy is to establish a structured approach to identify, assess, prioritize, test, and deploy software patches. By adhering to this plan, we aim to promptly address vulnerabilities, minimize security threats, and protect digital assets from unauthorized access. 3. Scope This policy applies to all software, applications, operating systems, and devices used within [your organization's name], including on-premises and remote systems, as well as mobile devices used for work-related purposes. It also includes all employees, contractors, and third-party vendors with access to organizational systems. 4. Policy 4.1 Patch identification and prioritization [Specify your methods for identifying patches, such as automated scanning tools and vendor advisories. Describe the criteria for prioritizing patches based on feasibility, severity, criticality, and potential impact.] 4.2 Patch testing and approval [Describe your procedures for testing patches in a controlled environment. Include the process for obtaining approvals from relevant stakeholders before deployment, particularly with regard to change management in production systems.] 4.3 Patch deployment [Explain the methods for deploying patches, including scheduled maintenance windows, automated deployment tools, and tracking mechanisms.] 4.4 Rollback plan [Outline a contingency plan for rolling back patches if unexpected issues or adverse effects arise. Emphasize why this is important.] 4.5 Patch monitoring and reporting [Describe the process for monitoring systems after patch deployment to ensure effectiveness and stability.] 5. Policy compliance 5.1 Responsibilities [Specify the roles and responsibilities of those involved in the patch management process.] 5.2 Training and awareness [Detail initiatives to educate employees about the importance of patch management and their roles in maintaining a secure IT environment.] 5.3 Review and revision [Outline the frequency and process for reviewing the patch management policy for continued improvement.] 5.4 Noncompliance [Explain the consequences of failure to comply with the policy statement, including potential security concerns, disciplinary action, or additional security measures.] By following this patch management policy, [your organization's name] commits to maintaining a secure, reliable, and resilient IT infrastructure that protects our assets and supports our business operations. [Your organization's name] [Date]