EBOOK

PATCH MANAGEMENT POLICY

PRO TIPS

Introduction

Anyone who uses a computer regularly should be familiar with the terms “software update” or “patch.” Patches are pieces of code applied to existing programs, applications, operating systems (OS) or browsers to improve their performance, add new features or fix vulnerabilities.

Patching your software and devices is, without question, necessary. Without it, cybercriminals can exploit vulnerabilities in your system and get an unfettered view of your confidential data. They can even take control of your entire IT infrastructure. Over the next five years, the cost of cybercrime is expected to **increase by 15%** annually, reaching $10.5 trillion by 2025.

Although companies understand the importance of patching, updating hundreds of systems and applications on time can get complex, tiresome and time-consuming. With a good patch management policy, companies can make patching more streamlined, expeditious and less monotonous.

In this eBook, we’ll discuss what makes a good patch management policy that can be used it as a guide to enhance your current policy or design one from scratch.

What is patching?

When you think of patching, the first thing that comes to mind is probably Windows OS patches. At the enterprise level, however, patches are applied to everything from software and computer systems to routers and switches.

Patching is a crucial and fundamental step in securing a company's IT infrastructure since cybercriminals are only too happy to exploit vulnerabilities that haven't been patched. By exploiting a vulnerability in any of the devices, applications or access points, threat actors can penetrate a company's internal network system and execute their nefarious schemes.

What is a vulnerability? A vulnerability is a flaw in a software code that not only makes the application perform poorly but also gives cybercriminals an access point to deploy harmful malware and other network-damaging exploits. An exploit is a computer program designed to take advantage of a system, application or network vulnerability.

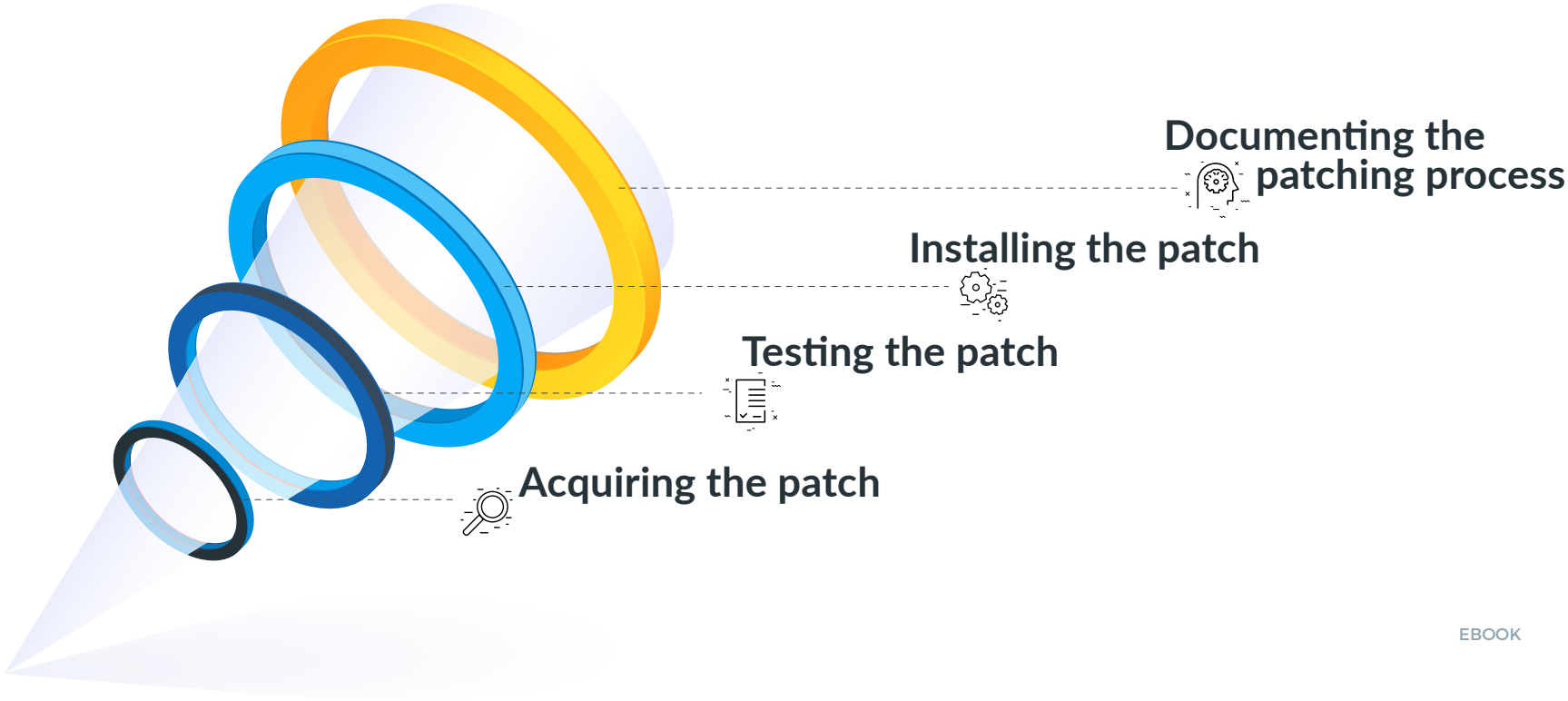
Cybercriminals can create their own exploit kits or purchase them on the dark web for use against newly identified vulnerabilities. The best way to keep external threats from affecting your business is to deploy patches the moment they are released. Patches not only fix bugs and vulnerabilities but also add new features to applications, increasing their functionality and productivity in the process.

What is a patch management policy?

Patching is a continuous process that requires companies have a patching policy in place.

A patch management policy is a set of guidelines and procedures designed to effectively monitor each step of the patch management lifecycle. It helps ensure that vulnerabilities get managed and mitigated promptly. Implementing and enforcing an effective patch management plan will enable your company to reduce its security risk profile, increase system uptime, meet patch-related compliance requirements and take advantage of the application's latest features.

Patch management is important not only for ensuring security against cybercrime, but also for maintaining the smooth functioning of systems and devices. We can broadly divide patch management into four key steps:



Hiccups and delays are an inevitable part of any process. It's likely that patching several applications across multiple environments (ie., onsite, remote, hybrid, cloud) will sometimes run into problems. A well-crafted patch management policy anticipates these problems and provides guidance on how to address them. A sound patch management policy sets the ground rules that ensure patching is conducted in a systematic and timely way.

It is the responsibility of every employee to read and understand their company's patch management policy. In general, a patch should be applied only by an IT professional who is familiar with the process and knows how to address any potential problems that may arise during the task. It's never a good idea to have employees apply patches directly. This can not only result in an infected patch being applied, but can also lead to system malfunctions causing business to cease.

Since patching is a multistage process, a patch management policy must also identify the stakeholders responsible for running the various stages of the patching lifecycle. Additionally, it is a good way to assign task ownership to the IT staff and ensure operational efficiency.

Lastly, it's crucial to document the patching procedure. Documentation provides a detailed description of each step of the patching cycle and will function as a guide for future patching activity. Furthermore, these documents can serve as the necessary paperwork for compliance and cyber insurance and can guide management to make the right policy decisions as the business environment and technology landscape change.

Manual vs. automated patch management

Generally, patch management involves checking the applications in use for missing patches, getting them from the application vendor, deploying the patch and writing a report on the process after deployment.

Performing this task manually for a few systems won't strain your IT staff. Now consider what it would be like to do this for thousands of systems and hundreds of applications. There will be chaos, IT staff will be under strain and the margin of error will be high. At the same time, while companies strive to complete this herculean task, threat actors will be doing their utmost to find that one unpatched system that will give them access to your company's network.

Since manual patch management is not an effective process at scale, businesses can purchase patch management solutions to automate the process and free up their resources and time. The patch management market size is predicted to grow from $652 million in 2021 to $1.084 billion by 2026 according to Market Data Forecast.

The IT department can update any type of endpoint or application using patch management tools, regardless of its configuration or location. Businesses can even use the tools to create patching policies tailored to their business requirements and IT infrastructure.

This results in a more secure organization and a less-stressed IT staff that is able to focus on strategic initiatives.

Patch management and cybersecurity

Patch management policies improve a company's security posture by enabling them to anticipate and address software security risks that, if not addressed in a timely manner time, leaves the company vulnerable to cyberattacks. Patching provides protection from cyberattacks in two ways.

In the most obvious way, patches fix software vulnerabilities that serve as backdoors for cybercriminals. The IBM Cost of a Data Breach Study found that the average cost of a breach in 2021 was $4.2 million per incident — the highest rate ever recorded in the last 17 years.

Security solutions, such as antivirus and antimalware (AV/AM) software, require timely patches so that they can continue functioning without a glitch and keep the company safe from external threats.

Sometimes, software developers and users may not detect a vulnerability for days or even months. In contrast, if a hacker discovers a vulnerability first, the software vendor has zero days to fix it. A zero-day vulnerability is a flaw in a network or software that hasn't been patched or for which a patch isn't available. Since Google's Project Zero was founded in July 2014, it has compiled data on "in the wild" zero-day exploits, with 2021 being the biggest year on record. Google collects data for publicly known cases of zero-day exploits as part of Project Zero. Phishing messages are common vectors for zero-day threats. In fact, Google disclosed that 68% of the phishing messages that it stops are zero-day attacks.

Zero-day vulnerabilities open companies up to a variety of security issues. A hacker who discovers this vulnerability can exploit it in a number of ways, adversely impacting programs, data, computers or networks. Hackers can also exploit zero-day vulnerabilities to install malicious software, like ransomware, that gives them the power to remotely manipulate IT infrastructures, spy on confidential communication or disrupt operations.

A zero-day vulnerability is a flaw in a network or software that hasn't been patched or for which a patch isn't available.

Features of a responsive patch management policy

Patch management policies must strike a balance between cost-effectiveness and security. Here are some steps to follow while developing patch management policies, frameworks and processes.

1. Perform an asset inventory

In essence, asset inventory is the process of taking stock of all the IT assets within your ecosystem. As a starting point, make a list of all the hardware and software assets you own, and categorize them according to their type, configuration, IP address, importance for business, susceptibility to a cyberattack, geography and such. Knowing the details of each asset will give you a full picture of your IT network. In addition, it will enable your technicians to access detailed information on any assets or asset group with a quick scan. Once you have your assets mapped, you can make informed decisions when creating policies guidelines and rolling out patches. It is important to conduct asset inventories at regular intervals to keep track of devices that have been added.

Today, companies can use IT asset inventory software to provide an accurate asset inventory and resolve discrepancies quickly. Such software reduces the risk of fraud and errors associated with manual processes.

Standardize your assets

This technique can be used in conjunction with the previous step. While standardizing assets may be easier said than done, grouping devices with similar characteristics will streamline patching and vulnerability remediation. Standardization will allow you to apply patches to a set of systems with a single click. This will result in faster patching and a significant time saved for your IT staff.

2. Make a list of security tools

Cybersecurity solutions such as firewalls, vulnerability management tools and AV/AM tools must be patched proactively because they are the first lines of defense for your network. Make sure you identify the location, operational status and the assets your security applications protect when taking the inventory. Not only will this information ensure that your critical applications are patched quickly, but it will also enable your system administrators to react rapidly to an incident and contain it before it spirals out of control.

3. Assign patch management roles to your team

First and foremost, never let your employees manage patches. Your IT staff should be in charge of this task. Be sure to assign the various steps in the process to your IT wizards. They must also be aware of their roles and responsibilities to ensure that the process moves forward smoothly. If you use an automated patch management tool, the person responsible for overseeing and administering it should be familiar with the processes and practices you follow as a business.

4. Choose the right patch management software

According to industry reports, IT security teams spend four days a week manually prioritizing vulnerabilities, which delays remediation teams from getting started on critical work or causes them to waste time and effort on low-priority vulnerabilities. In addition to this, the report found that the time spent on manual triage equates to an average annual remediation cost of $63,474. This emphasizes the need for automated patching solutions.

According to MarketsandMarkets, the global security and vulnerability management market is projected to grow from $13.8 billion in 2021 to $18.7 billion by 2026. The process of manually patching systems can be time-consuming, creating a heavy backlog. This means cybercriminals targeting your business will have more time to carry out their nefarious schemes. Using an automated patch management system eliminates the need for human intervention since the tool quickly identifies applications that need patching and even sources patches from vendors when they become available.

Additionally, these tools offer automated patch testing and deployment features that make patching more efficient while also improving business security. According to an IBM Security X-Force Threat Intelligence Index, automated security catches an estimated 40% more threats than conventional security, including zero-day exploits.

5. Test patches

On the surface, patching might seem like a simple process where a patch is released, then IT staff applies it to various systems with a click of the mouse. However, there is much that goes on between getting a patch and applying it.

First and foremost, there is no guarantee that all patches will be compatible with your IT environment, especially in this day and age with technology changing so rapidly. Patch management errors can cripple your IT infrastructure, making it a very attractive target for cybercriminals.

Generally, the test environment is a replica of the real IT environment. It includes servers and samples of critical business applications in order to give an accurate picture of your IT infrastructure's response to a patch. Testing patches prior to implementation is necessary to ensure that they don't adversely affect the performance of the applications in use.

Some businesses struggle with testing patches because they lack the infrastructure to do so. To tackle this, patches are first rolled out to non-critical systems, and if they do not disrupt functionality, they are then pushed out to the rest of the infrastructure.

6. Create a patch schedule

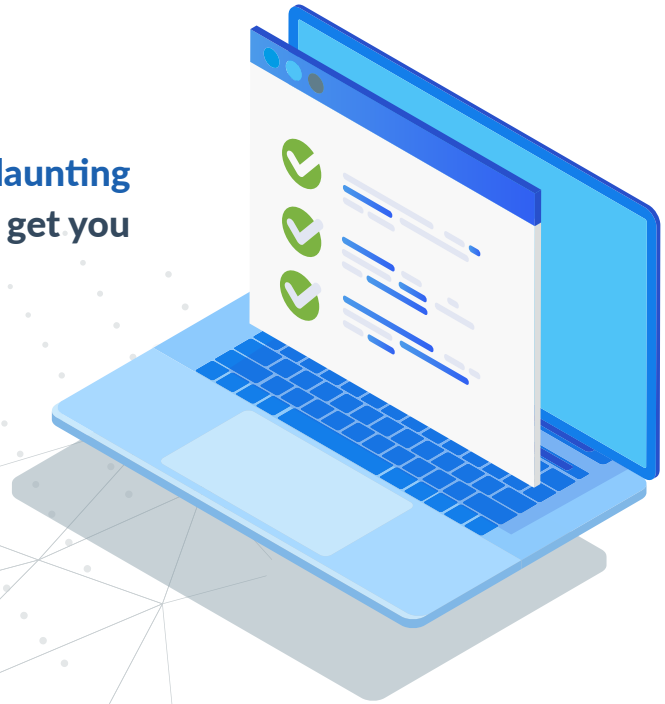
A patch management schedule specifies how frequently devices and applications must be scanned for vulnerabilities and when they should be updated. By establishing a schedule, patches can be deployed as soon as they are available, without too much delay. A schedule determines how long it will take to test a patch. The time needed for testing a patch is determined by its security implications and the device or application for which it is intended.

7. Document your patching schedule

Documentation is an essential component for measuring the efficiency and effectiveness of your patch management process. By documenting the factors that worked and those that failed when patching, policies and procedures can be improved. Having a good patch management document will also help you meet security compliance requirements because it provides a detailed view into your patching environment.

Patch management best practices

Following best practices can make even a task as gargantuan and daunting as patch management manageable and easy. Here are some tips to get you started on the right foot.



Set clear expectations

IT staff must take their duties and tasks seriously and be punctual in order for a patch management policy to be effective. To ensure patching tasks are completed on time, define clear roles and responsibilities for each team member and hold them accountable. As a result, adopting risk mitigation practices will become more commonplace at work.

Regularly update inventory and software

This is patching 101. To ensure that a patch management strategy works, it is essential to keep all the hardware and software up to date and review asset inventory frequently. Your strategy is certain to yield good results if you don't skip this step.

Document how security tools are configured

The IT staff of a company comes and goes, bringing with them their own understanding of tools, systems and practices. As a consequence, common tasks like configurations, which must be carried out according to company policy, can become a hassle. A documented set of guidelines allows any new employee to configure tools and systems in accordance with company policies without making mistakes. The same is true for patch management.

Keep a list of common vulnerabilities

Keep a list of all software vulnerabilities that are commonly targeted by cybercriminals. Also, identify the areas in your IT infrastructure that are most likely to be exploited. Furthermore, you must anticipate the kind of malware cybercriminals might use against your IT infrastructure and leverage this information to develop a robust defense strategy. Using this information, you can devise a patching strategy that addresses the most vulnerable systems first.

Have a disaster recovery process

Cybercrime like a zero-day attack can affect any company. Having a plan regarding what to do if a breach occurs is just as important as taking preventive steps. Disaster recovery plans should include step-by-step instructions for protecting and retrieving data in such scenarios. How should a vulnerability be handled in the event it is exploited? How will you contain and isolate affected systems, networks and applications? How to securely recover backed up data? It's a good practice to test your backup and restore plan on a regular basis. Increasing cyberthreats indicate a need to regularly test the backup plan to prevent data loss and minimize downtime.

According to IDC's State of Data Protection and Disaster Recovery Readiness: 2021 report, 95.1% of organizations suffered a malicious attack in the past 12 months while 36.6% suffered more than 25 attacks. Of the respondents who reported being attacked, 80.3% indicated that at least one attack resulted in data corruption. The fact that 43% of respondents had unrecoverable data within the last year is of greater concern.

Most importantly, there should be a clear process to patch the vulnerability that served as the pathway for the attack.

How Kaseya VSA helps with patch management

Over 99.9% of vulnerabilities are exploited over a year after they are discovered. Effective patch management can dramatically reduce this number. A single missed patch is all it takes for vulnerabilities to expose your system to downtime, data loss and non-compliance with regulations.

With **Kaseya VSA**, you can streamline patch management for Windows, Mac and third-party applications. Using the software management feature, you can view vulnerabilities and deploy patches immediately or schedule them for later deployment. This feature also allows you to create device profiles and be notified of missing updates.

The software management module provides a hierarchical view of your system to manage your environment down to the last detail and make sure it's secure. It will show you which devices have vulnerabilities, which machines have vulnerabilities, what percentage of devices are vulnerable and which systems comply with your policies. This report will also show you what's causing the most vulnerabilities in your environment, like third-party applications or operating systems.

With a wealth of data at your fingertips, you can effectively implement patches and ensure that your endpoints are protected. Learn about software management as well as other powerful VSA features, by **requesting a demo today.**

About Kaseya

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

02072022