NextPerimeter.com // 888-286-4816

NEXT PERIMETER

IMPORTANCE OF PATCH MANAGEMENT

TO AVOID BUSINESS VULNERABILITIES

TABLE OF CONTENTS

How many of us have received an update notification and clicked the “Remind me later” button? We’re busy at work and think “I’ll do it later,” or “it’s probably not important”.

It happens to the best of us. However, this seemingly innocent event can have grave consequences for businesses.

WHAT THIS E-BOOK WILL COVER:

- What is patch management?
- What are the different types of patches?
- What is the purpose of patching?
- How important is proactive patching to businesses?
- Patch management by the numbers
- Patch management for cybersecurity and risk mitigation
- Patch management lifecycle and process
- Patch management best practices for 2020
- Patch management and compliance
- The value of working with a patch management partner

PATCH MANAGEMENT DEFINITION

Patch Management is the process by which businesses/IT procure, test, and install patches (changes in code or data) intended to upgrade, optimize, or secure existing software, computers, servers, and technology systems to maintain operational efficacy or mitigate security vulnerabilities. While simple in nature, most growing businesses struggle to identify critical patch updates, testing and installing patch releases to fix problems as they occur. In fact, the average time to patch is 102 days (about 3 and a half months) according to Ponemon.

It's no surprise that with over 16,500 security vulnerabilities reported in 2018, it's virtually impossible for a small or medium-sized business with strained IT resources to keep up and protect your company.

Patch management is a time consuming and often misunderstood task, yet the impact can have devastating effects.

57%

of cyberattack victims stated that applying a patch would have prevented the attack.

34%

say they knew about the vulnerability before the attack.

The window between the disclosure of a vulnerability and exploitation has shortened, forcing companies to race and deploy a patch before cybercriminals can compromise systems.

WHAT ARE THE DIFFERENT TYPES OF PATCHES?

Software patches fix existing vulnerabilities or bugs as they are found after a piece of software or hardware has been released. There are several types of patches:

HOTFIX: A hotfix patch is designed to fix a specific issue and unlike typical patches, these hotfixes are developed and released as soon as possible to limit the effects of a software issue. Hotfixes can be applied while the software or system is still running (hot), without the need to restart or close the program. A hotfix may not be publicly disclosed.

SECURITY PATCHES: A security patch is a change applied to an asset to correct the weakness described by a vulnerability. This corrective action will prevent successful exploitation and remove or mitigate a threat's capability to exploit a specific vulnerability in an asset. Patch management is a part of vulnerability management – the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities (security risks).

CLOUD BURSTING AND FLEXIBILITY: With a hybrid environment, organizations can take advantage of "cloud bursting," a process by which an application or resource runs in an on-site private cloud until a threshold is met or spike in demand (think online shopping or tax filing season), initiating a "burst through" from the private cloud to a secure public cloud environment to tap into more computing resources. This approach offers virtually unlimited scalability and significant cost savings.

POINT RELEASE: A point release (also known as a dot release) is a small or relatively minor update intended to fix an error or flaw of a piece of software without adding features.

MAINTENANCE RELEASE: Incremental update between service packs or software versions to fix multiple outstanding issues.

WHAT ARE THE DIFFERENT TYPES OF PATCHES?

SERVICE PACK (SP) OR FEATURE PACK (FP): Major patches that comprise a collection of updates, fixes, or feature enhancements to a software program delivered in the form of a single installable package. These typically fix many outstanding issues and normally includes all the patches, hotfixes, and maintenance/security patches released before the service pack. Most of us are familiar with Windows Service Packs, for example Microsoft began rolling out the Windows 10 Version 1903 Update service pack on May 21, 2019, which became available to all users on June 6th. Microsoft Windows 10 Version 1903 introduced privacy setting updates, more control over how Windows updates are applied, a sandbox for professional users, password-less login, screen mirroring for Android phones, enhanced troubleshooting, and security features.

UNOFFICIAL PATCHES: These patches are created by a third-party or a user community, most often because of a lack of support from the original software developer (e.g., the software company went out of business) or when a software product has reached its defined end-of-life. Like an ordinary patch, these are designed to correct bugs or software flaws. Nefarious individuals can introduce unofficial patches to create security vulnerabilities. While this is rare and quickly reported, we recommend only installing patches from trusted sources and for businesses to avoid unofficial patches.

MONKEY PATCHES: Like unofficial patches, a monkey patch (also known as a guerrilla patch) is an update designed to extend or modify the behavior of a plugin or software product locally without altering the source code.

What is the purpose of patching?

Patches are designed to repair a vulnerability or flaw identified after an application or software is released. As we've learned, there are many types of patches.

Unpatched software can make the device a vulnerable target of exploits. Software patches are a critical component of IT operations and security.

For this article, we'll focus on official patches (hotfixes, point releases, security patches, and service packs).

HOW IMPORTANT IS PROACTIVE PATCHING TO BUSINESSES?

Cyberattacks are becoming ubiquitous and have been recognized as one of the most strategically significant risks facing the world today.

67%

of SMBs have experienced a cyberattack in the past year.

(Ponemon – Keeper)

Despite this, only 7% of CEOs of businesses with less than 500 employees believe a cyberattack is "very likely."

Unfortunately, organizations will continue to fall victim to cyberattacks because many small-to-mid-sized businesses do not have the resources necessary to track security trends, respond to security incidents, and update controls.

Cyber threats come in many forms, including malicious insiders, DDoS, ransomware, website vandalism, cyber espionage, and theft of IP. The number one attack vector afflicting SMBs is phishing/social engineering cyberattacks.

Accenture's 2019 Cost of Cybercrime Study found that 85% of organizations experience phishing and social engineering attacks.

Artificial intelligence and machine learning capabilities are growing at an unprecedented rate. These technologies have many widely beneficial applications. Unfortunately, cybercriminals are tapping into AI and bots to organize coordinated attacks and distribute phishing schemes, spam, steal identities, and malware attacks.

Now two years after the largest ransomware outbreak in history, attack attempts involving ExternalBlue continue to increase, reaching historic peaks according to ESET.

Why?
Do we learn from the past?

Unfortunately, not everyone does, or individuals might not understand the critical threat that patches prevent. For example, according to research by Shodan, there are over 400,000 computers located in the United States that have not patched their systems to prevent hackers from exploiting this vulnerability.

Poor security practices and lack of patching are likely reasons why malicious use of the EternalBlue exploit has grown continuously since the beginning of 2017. This low hanging fruit is too attractive and lucrative for cybercriminals to pass up.

PATCH VULNERABILITIES BY THE NUMBERS

57%

of data breaches are attributed to poor patch management.

Source: Ponemon

48%

of 3,000 businesses surveyed reported one or more data breaches in the last two years.

Source: Service Now + Ponemon Institute Study – Today's State of Vulnerability Response

29.9%

According to Edgescan, the average time to patch high-risk vulnerabilities increased by 22.9% from 64 days in 2017 to 83 days in 2018.

Source: Edgescan Vulnerability Stats Report 2020

16,555

security vulnerabilities were released in 2018.

Source: CVE Details

92%

of web applications with security flaws or weaknesses that can be exploited.

Source: ImmuniWeb

37%

of breach victims confirmed they don't scan their systems for vulnerabilities

Source: Service Now + Ponemon Institute Study – Today's State of Vulnerability Response

34%

of breach victims knew they were vulnerable before they were breached

Source: Service Now + Ponemon Institute Study – Today's State of Vulnerability Res

65%

of businesses state that it is difficult to prioritize patches.

Source: Service Now + Ponemon Institute Study – Today's State of Vulnerability Response

82%

of employers report a shortage of cybersecurity skills

Source: CSIS – Cybersecurity Workforce Gap

71%

believe this talent gap causes direct and measurable damage to their organizations

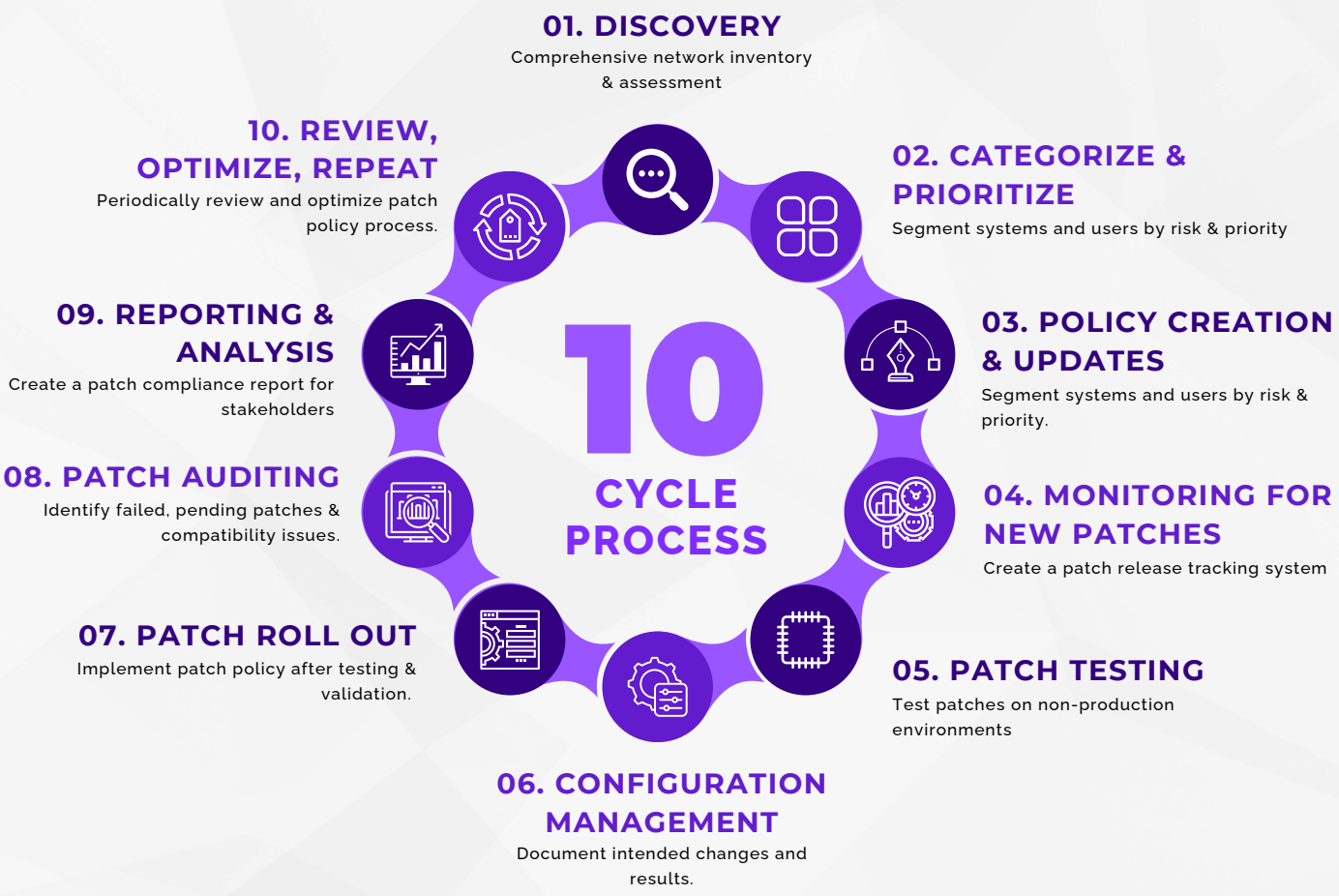
Source: CSIS – Cybersecurity Workforce Gap

PATCH MANAGEMENT FOR CYBERSECURITY AND RISK MITIGATION

Prompt patching is vital for cybersecurity. When a new patch is released, attackers use software that looks at the underlying vulnerability in the application being patched. This is something that hackers perform quickly, allowing them to release malware to exploit the vulnerability within hours of a patch release. Security patches prevent hackers and cybercriminals from exploiting vulnerabilities that could halt operations. Imagine if a hacker encrypted all your data, servers, and computers for a ransom. Does your team have the resources, expertise, and recent backups needed to keep your business running?

By now, we should have a good grasp on how important an effective patch management procedure is to the cybersecurity of your business, clients, and customers. So, what does an effective patch management process look like?

We'll review below the patch management lifecycle below.



STEP 1: DISCOVERY

Before implementing a patch management process, any IT professional worth their weight will have a comprehensive network inventory or will conduct an IT assessment to understand the types of devices, hardware, systems, operating systems, OS versions, and third-party software and applications are in use across your business. As businesses grow, IT resources become strained and it's not uncommon for systems to become neglected or forgotten. Spreadsheets are difficult to keep up with. So internal IT may lose track of the many systems and programs in use.

STEP 2: CATEGORIZE & PRIORITIZE

Now that we have a good grasp on our IT environment and infrastructure, we need to segment the systems and/or users according to their risk level and priority. At the user-level, you might prioritize the C-suite and users that frequently need to share, download, or install programs. Specifically, we can rate users that frequently need to share documents over email or online as 'high risk' since they are more vulnerable from outside threats. Looking at hardware, you might prioritize the company's server and business-critical hardware over a laptop that is infrequently used.

STEP 3: POLICY CREATION & UPDATES

Next, we develop patching requirements by deciding which systems, users, and software need to be patched; under what conditions, and the frequency these systems/users need to be updated. For instance, you might wish to make sure some systems or users are patched automatically and with greater regularity (liking patching employee laptops weekly) versus a server or network firewall which might require more manual and less frequent updates.

STEP 4: MONITORING FOR NEW PATCHES AND VULNERABILITIES

Modern businesses utilize a range of systems, software, and digital products, each with their own patch release and vulnerability disclosure schedules. While time-consuming, it's vital that your team takes the time to catalog each technology vendor, their primary page used for vulnerability disclosures, and product notifications (e.g., SonicWall Product Notifications). Creating an organized patch release tracking system or notification feed will save your team hours (possibly days) over a year. Another example is "Patch Tuesday" for Microsoft who has a pattern of releasing patches on the second (sometimes fourth) Tuesday of each month.

STEP 5: PATCH TESTING

Before rolling out patches, especially on mission-critical elements like business servers, create a non-production test environment, deploy the patch, and monitor for incompatibility or performance issues. If creating a test environment is not possible, we recommend testing patches on a small segment (two users) to assess if any adverse effects occur.

STEP 6: CONFIGURATION MANAGEMENT

After the testing phase, document the intended changes and results. Should your rollout go awry, you'll be able to quickly identify and troubleshoot unintended changes.

STEP 7: PATCH ROLLOUT

Now that your team has validated the patches, you will want to follow the Patch Management Policy established in step three to rollout as needed.

STEP 8: PATCH AUDITING

Following patch rollout, take a moment to identify any failed or pending patches. Monitor these for incompatibility issues. We recommend reaching out to a few tech-savvy end-users that can help provide feedback if needed.

STEP 9: REPORTING

Each business unit has stakeholders, IT is no different. Prepare a monthly patch compliance report to share with the C-suite and executives when needed. This will ensure everyone understands the importance of patch management and the fruits of your labor.

STEP 10: REVIEW, OPTIMIZE, AND REPEAT

As with most business processes, periodically review, update, and repeat steps 1 through 9. Look for systems that have reached their End-of-Life (EOL), outdated hardware/machines, review policies quarterly, and revise as needed to ensure the effectiveness of your patch management policy.

PATCH MANAGEMENT BEST PRACTICES FOR 2020

01. Take a “Critical Updates First” approach and patch exploitable vulnerabilities as soon as possible

After the testing phase, document the intended changes and results. Should your rollout go awry, you’ll be able to quickly identify and troubleshoot unintended changes.

02. Implement a data backup and recovery plan

Every business should already have a Backup and Disaster Recovery Plan, complete with on-site and off□site (cloud) full-system image backups. If your company does not, you can learn about the 11 key elements of an effective Disaster Recovery Plan in our recent post. With system image backups in place, your team can easily rollback any computer or servers that experience incompatibility or performance issues post-patch. These backups can save you hours, hard-earned money, and frustration if anything goes wrong while rolling out major patches across the organization.

03. Make proactive patch management a core practice of your policy

Taking a proactive approach to your patch management strategy will prevent your business from frequently going into emergency patching mode like many companies experienced with the WannaCry outbreak in 2017. Instead, by focusing on releasing patches as they occur, based on severity level, CVSS score, product name, and the prioritization model you created in step 3 above. This will allow your team to focus on strategic objectives that grow your business.

04. Centralize and automate your patching process

While patching can be time-consuming, automated patch management allows you to save time and reduce errors. Most patch management software enables you to automate each stage of the patching process, from scanning applications of devices, downloading missing patches, as well as scheduling and deploying patches based on designated policies to reporting.

PATCH MANAGEMENT BEST PRACTICES FOR 2020

05. Utilize a principle of lease privilege (POLP) approach for end users

Many organizations often allow employees to have admin privileges with their company devices. This is especially common in the SMB space. What happens? Most employees will dismiss or ignore important updates, patches, and security vulnerability updates. A frequently overlooked patch management best practice that is to not give full admin rights to end-users. While it's the responsibility of the IT department to execute a least-privilege policy to restrict employees, end-users really should only have a minimal amount of access or the privileges necessary to meet the demands of the role within an organization.

06. Patch and update "golden images at least once a quarter

"Golden images" are master software/system images used by IT as a template to set up and deploy new devices. When your company orders a new laptop or onboards a new employee, IT will often have a preconfigured system image that contains all the business applications, software, settings, privileges, and operating system necessary for the new user to hit the ground running. When your master images already have the most up-to-date software and security patches, your team won't have to do the same research again when setting up a new device.

PATCH MANAGEMENT, COMPLIANCE, AND RISK MANAGEMENT

As security breaches continue to increase, compliance regulations will continue to evolve to protect consumers. Government institutions, healthcare services, and financial sectors are among the most heavily regulated, but other industries are rapidly creating their own security compliance rules and guidelines. Implementing patch management is commonly required by security frameworks or standards, such as PCI DSS, CIS Critical Security Controls for Effective Cyber Defense, ISO 27001 Annex A, and NIST.

In June 2018, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) clarified in their OCR Cybersecurity Newsletter hat promptly patching systems is a crucial element for covered entities and business associates to remain HIPAA compliant, going so far to explain that patch management is a requirement under –– 45 C.F.R. § 164.308(a)(1)(i)(A), 45 C.F.R. § 164.308(a)(1)(i)(B), 45 C.F.R. § 164.308(a)(5)(ii)(B) and 45 C.F.R. § 164.308(a)(8).

Due to the complexity of modern IT environments, the patch management process can be a major undertaking.

However, failure to comply could potentially result in significant legal penalties for your business. Patch management ensures your business stays compliant and protects customers, consumers, and stakeholders. **Here are a few compliances best practices you can implement to secure your business:**

- Know who your vendors are and what security protocols they have in place
- Require certain levels of security compliance and protection from all third-party vendors, with a zero-tolerance policy towards vendors that do not meet your security compliance standards
- Implement multi-factor authentication to reduce access to your environment via third-party connections
- Implement strict access control policies for your business applications, equipment, hardware, and software to reduce the risk of potential third-party vulnerabilities or tampering

VALUE OF WORKING WITH A MANAGED PATCH MANAGEMENT PARTNER

A solid patch management process is an essential requirement for any size business. Unfortunately, most organizations do not have the expertise, software, or mature processes/systems in place to effectively secure their infrastructure.

Manually checking for and applying patches in is almost an impossible task. Do you prioritize servers or employee workstations or third-party applications? Do you focus on security fixes or compatibility updates? And how do you keep track of which patches have been applied? These are tough questions for any IT team. IT teams are struggling to keep on-premises, data center, and cloud infrastructure up to date with the latest versions of operating systems, databases, and third-party applications.

Without the right investments in people, process, and technology, an organization can quickly fall behind on critical patches that address security and compliance requirements.

Rather than forcing already strained internal IT teams to update critical systems manually, many small and medium-sized businesses look to partner with Next Perimeter. As a Managed Service Provider (MSP), we have the expertise, software, and mature systems in place to effectively secure your infrastructure using time-tested patch management processes that has evolved over 13 years.

We create a comprehensive Patch Management Policy for your business, use patch management tools to automate the mundane, and have our engineers on standby to provide human intervention when needed to ensure that your entire network of devices, databases, servers, applications, and systems are protected. Your business will remain up to date with latest features, functionality, security, and capabilities offered by application and OS vendors resulting in improved employee productivity, security, and compliance.

Automation provides an auditable change management process and helps plug exploitable holes in your security posture while complying with various regulatory mandates such as PCI DSS, HIPAA, NIST, FFIEC, GLBA, SOX, FERPA, and others.

CONCLUSION

- **Patches are not an option, they are a requirement** for secure to prevent security breaches, data theft, data loss, PII and PHI violations, reputation issues, and legal penalties. They protect your business.
- High-risk and critical security patches need to be **deployed as fast as possible** (within days) to prevent hackers from exploiting vulnerabilities.
- Hundreds of thousands of systems and thousands of businesses could have prevented the WannaCry ransomware attack of 2017 **had they deployed the security patches promptly**, saving hundreds of millions or billions of dollars in lost revenue and damages.
- **57% of data breaches** are attributed to poor patch management.
- Prompt patching is **vital** for cybersecurity.
- End users should have the **least** number of privileges necessary to fulfill their role
- Patch management is a **requirement** of HIPAA and looks to mitigate compliance or regulatory risks.
- Taking end users out of the patch management process will result in **more secure environments.**
- These aren't OS-specific issues. **Everyone is vulnerable.**
- Many small- and medium-sized businesses work with Managed IT Services Providers to ensure an **effective patch management policy** is implemented.

Call **Next Perimeter** today to learn how our Patch Management solution reduces the risk of having a security breach and all the related problems that come with it.

Prevent data theft, data loss, PII and PHI violations, reputations issues or even legal penalties today by calling 888-286-4816.

WHAT SETS US APART?

It All Starts in the Cloud

Your .com is what ties your business to the web, allowing you to get your email and collaborate online. Whether you're using Google Workspace or Microsoft 365, **Next Perimeter** has you covered. Your team can leverage our certified experts for matters concerning your email deliverability, DNS records, licensing concierge, and more.

Your Team and Workstations are Fully Covered

When your team logs into your corporate environment today, what types of protections exist? **Next Perimeter**, by default, deploys endpoint security and hardware monitoring to every workstation that we manage, ensuring productivity is at an all-time high. Your team will enjoy unlimited round-the-clock support for everyday issues ranging from authentication to hiccups with their equipment.

Battle-Tested SOPs

Whether we will handle all of your IT, or collaborate with an internal team, our procedures have been perfected against millions of business scenarios. Our system has been trained to adapt to each customer as their organizations evolve.

Future-Proofed for Compliance

We know you want your cybersecurity to be reliable, predictable, functional, and cost-effective - that's why we've simplified cyber so it's back-of-mind. By signing up for Essentials, you've created a predictable path toward future compliance needs as our agents can fulfill virtually all requirements they might ask for with simple per-user/device pricing.

NEXT PERIMETER

Let's Work Together

Phone
888-286-4816

Mail
sales@nextperimeter.com

Website
NextPerimeter.com

About Us

As a leader in cloud-first cybersecurity and IT support, Next Perimeter protects businesses from modern threats, whether in the office or remote. Our Zero Trust architecture and SaaS posture management deliver a secure, optimized endpoint experience without the need for servers or office space.

Our SASE network as a service replaces traditional VPNs with an always-on, secure connection, ensuring high-speed, reliable network security across the globe. Specializing in holistic threat detection and response, we safeguard your digital assets with cutting-edge AI-powered solutions.