WatchGuard®

Vulnerability and Patch Management

watchguard.com

Table of contents:

The importance of patch management in organizations

Software patches tend to be a hassle for IT administrators. Prioritizing and deploying them is a time-consuming task, not just for them, but for users too. Computers and servers often have to be restarted, which leads to interruptions to work. Because of this, updates are often put off, and recommended patches are ignored. However, what may seem like an innocent action could end up having serious consequences for organizations.

Likewise, IT administrators can have serious difficulties ensuring that all the systems in their network have the necessary patches installed. Software patches and updates are critical when it comes to ensuring an organization has a hardened cybersecurity stance, since they stop software and systems from being vulnerable to security threats.

Vulnerabilities in numbers

A total of 18,103 vulnerabilities were reported in 2020, at an average rate of 50 CVEs per day, by security professionals, researchers, and vendors.[1] Given these figures, it is perhaps unsurprising that it is extremely difficult for organizations with limited IT resources to maintain and protect their infrastructure.

Patch management is a task that can require a great deal of time and resources, and it is often difficult to get an overview of your assets and applications, prioritize patches, and even to be able to swiftly patch critical programs and systems. Companies need to be able to manage patches as efficiently as possible, otherwise they could have a huge negative impact on their productivity, as well as their cybersecurity.

24.1%[2] of vulnerabilities belong to five companies: Software in the Public Interest (SPI), SUSE, Oracle, IBM, and Microsoft.

The most widely used third-party applications are the main target for hackers. According to the Common Vulnerabilities and Exposures (CVE)[3] index, applications like Java, Adobe, Google Chrome, Mozilla Firefox, and OpenOffice, among others, have the highest number of vulnerabilities. As such, simply patching operating systems is not enough.

Another factor to consider is the increase in the number of attackers with the skills needed to discover vulnerabilities at a higher speed. Once found, they deploy programs that automate the exploitation of these new vulnerabilities, which are widely distributed, sometimes even going viral. The result of this combination of threats, vulnerabilities, and consequences poses a significant risk to companies. However, surprising though it may seem, it isn't undiscovered vulnerabilities that pose the greatest danger.

Sources:

1. SCMagazine - Vulnerabilities hit record high in 2020, topping 18,000
2. Cybersecurity alert – TechRepublic
3. attack.mitre.org – MITRE

Known vulnerabilities, high-risk vulnerabilities

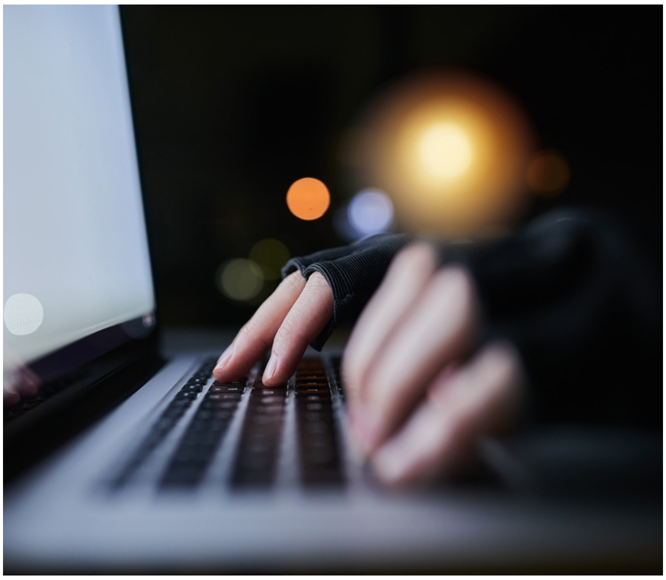
The exploitation of vulnerabilities is currently still the number one cause of most security breaches. Notorious cases such as WannaCry, Petya and BlueKeep, which caused havoc worldwide, are still fresh in everyone's mind. Only a small number of attacks occur as a result of true unknown vulnerabilities (zero day attacks), since most are caused by known vulnerabilities.

Last year, hackers typically exploited known and fixed vulnerabilities to target unpatched systems, with many of these having been disclosed within the past two years.[4] By contrast, zero day vulnerabilities have accounted for approximately 0.4% of the vulnerabilities in the past decade.

It is important to remember that hackers also have access to public exploits to carry out their attacks, which they do not hesitate to exploit, knowing full well that most companies do not patch their systems. In fact, 80% of successful attacks exploit vulnerabilities that have known patches that have not been applied.

In light of these facts, it is clear that companies should focus their efforts of controlling and mitigating known vulnerabilities that are exploited over and over; they are a greater, more real risk than other kinds of threats.

The time between a vulnerability being disclosed and it being exploited has also shortened considerably, forcing companies to work against the clock to deploy patches before cybercriminals can compromise their systems using a range of attack vectors.



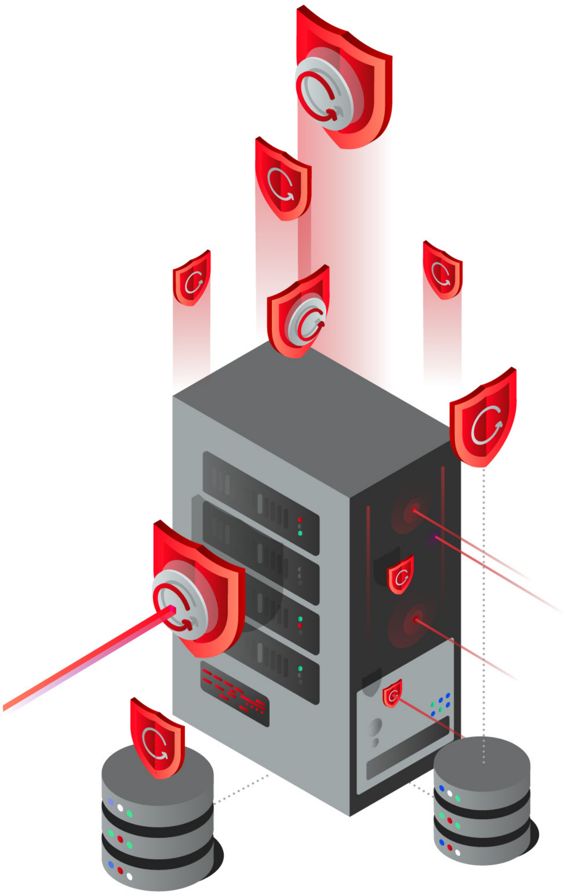
57% of victims of cyberattacks say that applying a patch would have prevented the attack. 34% say that they knew about the vulnerability before the cyber attacks.[5]

Sources:
[4] Cybersecurity & Infrastructure Security Agency – CISA
[5] Cost and consequences of gaps in vulnerability response – Ponemon

Patch management

A / WHAT PATCH MANAGEMENT INVOLVES

This is the process by which organizations, or more specifically their IT departments, download and install patches (changes in code or data) intended to update, optimize, or secure software, computers, servers, and systems. The aim is to make sure these components work properly or to mitigate security vulnerabilities. Although it might seem like a simple task, most companies struggle to identify which critical patch updates they need to install first. Therefore, prioritizing patches is key for administrators. In fact, according to Ponemon, the average time it takes companies to patch applications or systems is 97 days.[6] However, the average time it takes to see a cyberattack once a patch is released for a critical security vulnerability is 43 days,[7] meaning there is an average risk gap of 59 days.



Sources:
6. State of Endpoint security risk 2020 – Ponemon
7. Cost and consequences of gaps in vulnerability response – Ponemon

B / WHAT TYPES OF PATCHES ARE THERE?

There are different kinds of patches, and each of them is developed for a specific purpose: to correct a bug or specific vulnerability. The following are just a few examples: Hotfix, service patches, maintenance versions, Monkey patches, etc.

In this document we'll focus on the two types that we consider most important, since their aim is to correct critical security vulnerabilities that are commonly exploited by attackers and are therefore the most important for companies and security experts.

- **Security patches affect both operating systems and third-party software:** A security patch is a change made to an application or program in order to fix bugs or flaws that cause vulnerabilities. Applying this kind of patch prevents vulnerabilities from being exploited or will eliminate or mitigate the ability of threats to exploit a vulnerability in an asset. Patch management is part of vulnerability management: the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities (security risks).

- **Service Pack (SP) or Feature Pack (FP):** These are important patches that comprise a collection of updates, fixes, or feature enhancements for a piece of software. They tend to solve a lot of pending problems, and usually include all the patches, hotfixes, maintenance and security patches released before the service pack.

C / WHAT PURPOSE DO PATCHES SERVE

Patches are designed to repair a vulnerability or security gap identified after an application or a piece of software has been launched.

Unpatched software can expose all endpoints to exploits, providing a great opportunity for hackers to successfully launch attacks. Software patches are a critical component of operations for administrators and security experts.

In the technological sector, and more specifically in the software sector, it is often the case that, once an application has been launched, it needs to be fixed or even modified. Because of this, it is a good idea to develop a process similar to the software lifecycle, where different phases are established to allow analysis, evaluation, and the regular application of patches to solve any problems that may arise.

Patch Management Lifecycle

Patch management can be the most effective tool for protecting your company against vulnerabilities and the least costly to maintain, if efficiently implemented. In this section, we will explain how to establish a routine patch management procedure, with the aim of integrating it into your company's standard operations. In this cycle or procedure, there are six phases.[8]

Identification of assets and base software:

Identifying assets and the base software installed on them, as well as their patch level, is a complex task, but one that improves both security and operability. Having this base allows you to make changes to the system without risks and makes it possible to return to a previous known functional state should a problem occur when installing an update or patch.

Availability:

The current list of patches must be reviewed based on the inventory of assets and software, identifying which patch affects each asset.

Applicability:

Patches that are published are not always valid for all devices. This means that it is important to check whether a specific update is suitable for the assets in your process.

Acquisition:

Obtaining the update file from an official source, as well as checking that the patch is legitimate, is not always easy. The use of hashes is not common for patches related to control systems.

Validation:

The purpose of validation is to ensure that the update won't have a negative impact on the process. To validate the patch or update, test assets need to be used, following the rollout phases. The validation is intended to check what implications the update could have, which could include changes to firewall policies, settings changes, etc.

Roll-out:

A rollout package needs to be created in the validation process. The package must contain the update files and installation instructions, as well as a list of assets where the rollout needs to be carried out.

Sources:
[8] Patch management in control systems – INCIBE-CERT

Keep known vulnerabilities out of your IT infrastructure with WatchGuard Patch Management

WatchGuard Patch Management is a solution that simplifies the complex patch management lifecycle for operating systems and third-party software. As a result, the attack surface is reduced, and the capacity to prevent and contain incidents caused by system vulnerabilities is strengthened.

The solution is integrated into WatchGuard Security's endpoint security solutions, which means that it requires no new agents or management consoles. It provides centralized real-time visibility into the status of vulnerabilities, patches, pending updates, and unsupported or EOL software on computers and servers, both inside and outside the corporate network. Its management tools allow you to automate the discovery, scheduling, installation, and monitoring of the critical patches and updates that your organization needs, all in real time and in a simple, intuitive format.

The main benefits and features of WatchGuard Patch Managment

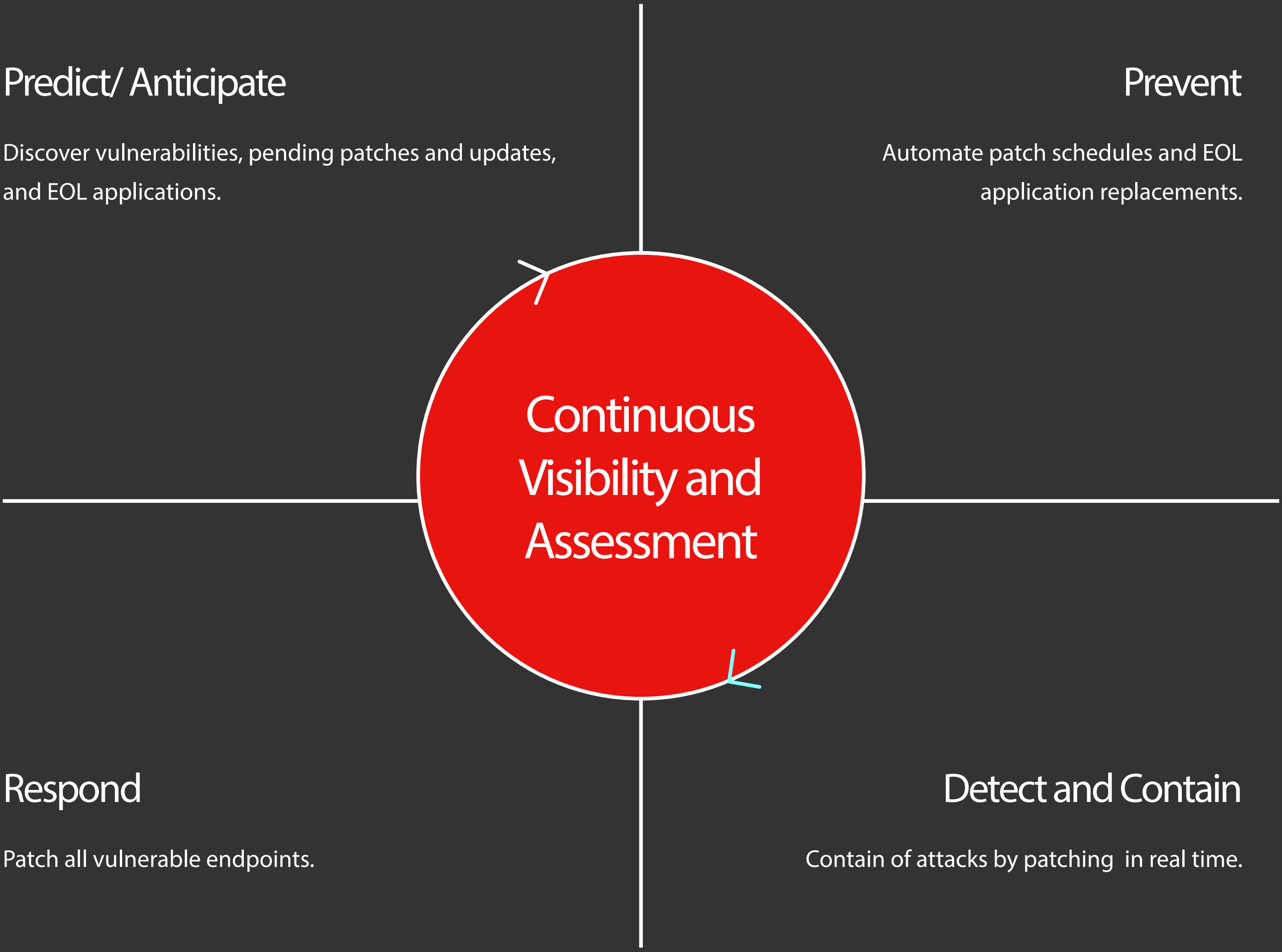
- Audit, monitor, and prioritize updates for operating systems and applications. It allows you to see the status of pending patches and updates for the system and hundreds of third-party applications, and it even allows you to roll back patches.
- Prevent incidents by systematically reducing the attack surface caused by vulnerabilities. Managing patches and updates allows you to get ahead of vulnerability exploits.
- Contain and mitigate attacks that exploit vulnerabilities, immediately applying critical updates from the Cloud console. The console correlates detections with vulnerabilities, thus minimizing response, containment, and remediation time, by applying updates as needed from the console. What's more, it allows you to isolate affected computers from the network, containing both real and potential attacks.
- Reduce operational costs, as it requires no agent deployments or updates on endpoints, simplifying management without overloading computers or servers. Minimize the effort of remote updates from the Cloud console. Immediate, automatic visibility of vulnerabilities, updates, and EOL applications.

Patch management is a process that must be done regularly and needs to be as comprehensive as possible in order to be effective. This does not mean that all systems should be treated equally, however; every company needs to prioritize their assets and ensure that the most critical are protected first.

That said, it is important to ensure that patches are deployed on all machines, and not just those that are the most valuable or important to the business. Furthermore, patches not only require an effort from system administrators, but they may also require the support of the company to agree on a specific maintenance window.

Attack Protection

Adaptative Security Architecture



Predict/ Anticipate

Discover vulnerabilities, pending patches and updates, and EOL applications.

Prevent

Automate patch schedules and EOL application replacements.

Continuous Visibility and Assessment

Respond

Patch all vulnerable endpoints.

Detect and Contain

Contain of attacks by patching in real time.

Find out how WatchGuard Patch Management can help you to simplify vulnerability management by streamlining the update and security patch process.

For more information visit our website

WatchGuard

NORTH AMERICA SALES 1.800.734.9905 INTERNATIONAL SALES 1.206.613.0895 WEB www.watchguard.com

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. Part No. WGCE67452_110221