ManageEngine

GHOSTS OF UNPATCHED VULNERABILITIES PAST:

WHY THEY'RE STILL AN ENTERPRISE'S TOPMOST CONCERN

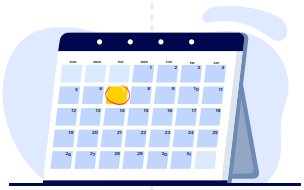
ONE UNPATCHED
VULNERABILITY LATER

It was on a sunny morning in July 2019 when Equifax (one of the top three consumer credit reporting companies in the US), discovered that something suspicious was happening in its network. On further investigation, **Equifax** came to realize that close to **143 million consumer records** were compromised, leading to one of the greatest data breaches of all time.

WHERE DID ALL THIS START?

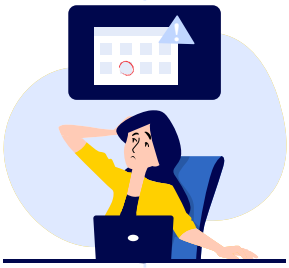
In a vulnerability in Apache Struts for which patches were released on March 7, 2017.

What's most alarming is the time gap that we see between the dates of the attack and the release of the patch. Not only that, but it took two years to discover that nearly 40% of Americans had their personal information stolen.



March 7, 2017

Patches were released for the vulnerability in Apache Struts (CVE-2017-5638).



March 9, 2017

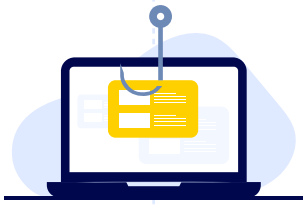
Equifax IT admins were asked to patch the vulnerability but it wasn't done.

March 10, 2017

The initial breach into the Equifax network by exploiting the Apache Struts vulnerability occurred, according to the forensics investigation.

March 15, 2017

Equifax ran a scan to detect the vulnerable systems but the scan wasn't effective enough to flag any of the vulnerable systems.



May - July 2017

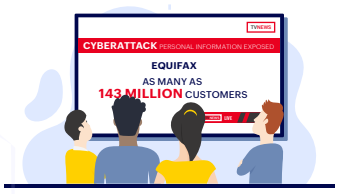
The attackers moved through the network and got access to various servers and databases containing information on millions of people

July 29, 2019

The expired public key certificate that let attackers secretly move tons of encrypted data was discovered and renewed. Following this, the admins were immediately able to sense the suspicious activity happening, which was when they discovered the breach.

August 2019

Top executives sold company stocks expecting a decline leading to insider trading accusations.



September 8, 2019

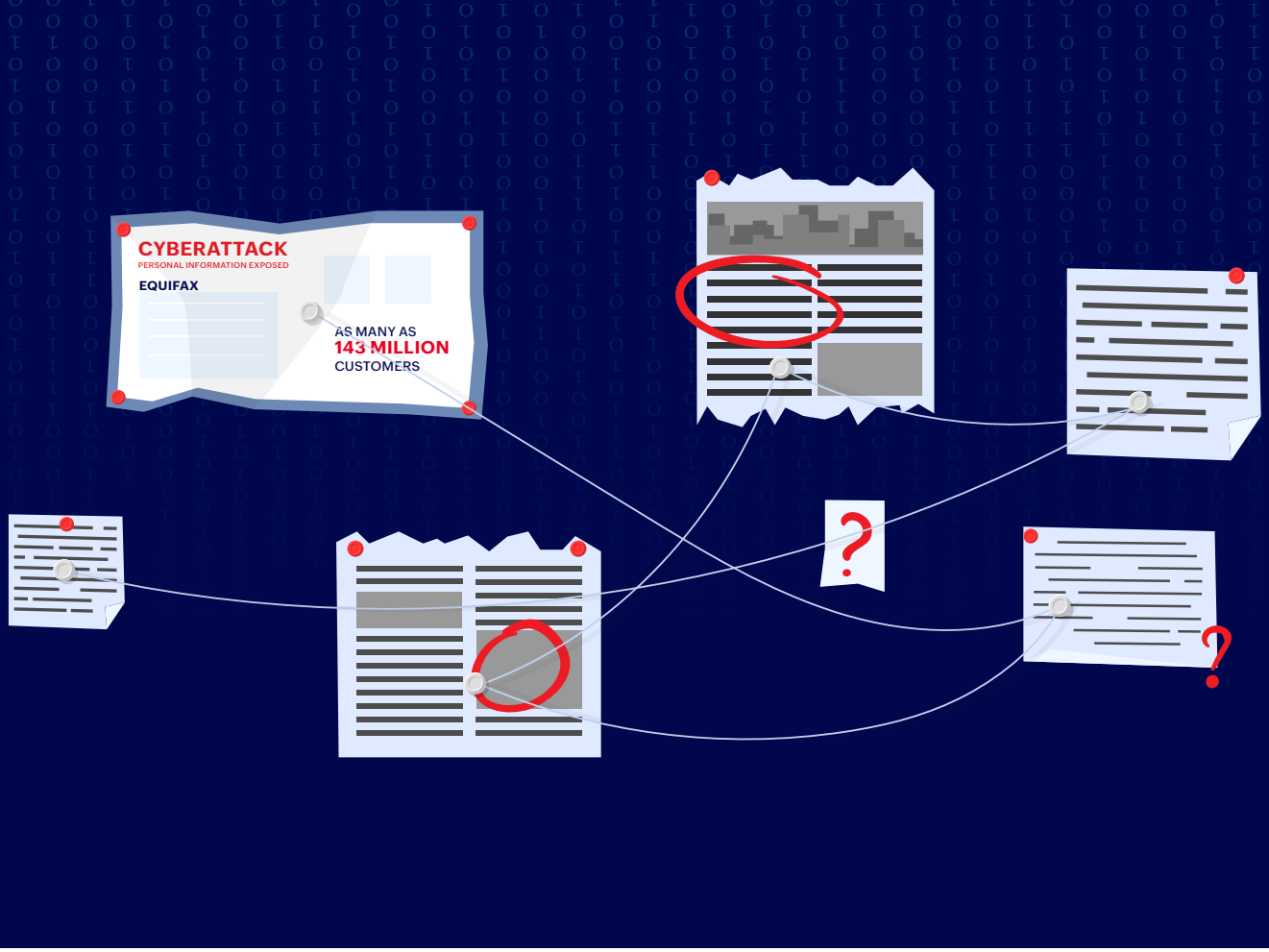
After another month of internal investigation, Equifax publicized the breach.

WE FIND TWO VERY DISTURBING FACTS HERE

1 Massive amounts of data was being covertly stolen from right under Equifax's noses, and it went unchecked in spite of the organization actually having security measures in place.

2 As the breach came to light and the country braced for an onslaught of identity thefts and misdeeds, there was absolute silence. The stolen data never made it on the dark web and was not sold. This led to suspicions of espionage by foreign governments in an attempt to map the behavior of US government officials and other people of interest.

What began as a seemingly simple negligence in patching and renewing security certificates led to the US Department of Justice taking the extremely rare step of charging four members of the Chinese military with the attack.
One organization's poor cybersecurity posture and response to a breach put an entire nation at the mercy of a foreign power. Power plays are not only happening on battlefields; they are happening behind computer screens now, too.



ATTACKING THE OBVIOUS FOR THE WIN

Even as the threat landscape evolves and more innovative and elaborate attacks hit enterprises, it's still known vulnerabilities and non-adherence to basic cyber hygiene that cause some of the worst cyber catastrophes. Take the recent Colonial Pipeline ransomware attack: having a password policy to restrict the reuse of passwords and implementing multi-factor authentication could have helped avoid a national emergency. As mundane as patch management sounds, it should still be a top priority seeing as how many major attacks stem from long-forgotten unpatched vulnerabilities.

According to the recent Ransomware spotlight report, targeting unpatched vulnerabilities still remains the main attack vector that ransomware groups exploit to enter vulnerable networks. The most shocking factor that this report revealed, however, is that **56% of the 223 older vulnerabilities identified prior to 2021 continue to be actively exploited by ransomware groups.**

Below is a list of the top software vulnerabilities that caused waves in 2021. Some of these vulnerabilities date back to 2020, but they are still dangerous and fully capable of taking down an organization that fails to patch them.

ProxyLogon

Marked as **CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065**, ProxyLogon was the first critical vulnerability chaining instance in 2021. When exploited in combination, these vulnerabilities allowed a threat actor to execute remote codes on compromised systems, which then gave them power to access files, mailboxes, and credentials stored on the compromised Exchange Servers. The Chinese state-sponsored threat group Hafnium has been accused of this attack. Though the exact number of affected systems is unknown, it was placed somewhere around 200,000 in March of 2021, two months after the attacks began.

CVE-2021-26855	**CVE-2021-26858**	**CVE-2021-26858**	**CVE-2021-27065**

ProxyShell

Let's just say 2021 wasn't Exchange Server's year, as this popular solution was yet again fell victim to attacks by another set of vulnerabilities. Marked as **CVE-2021-34523, CVE-2021-34473**, and **CVE-2021-31207**, this set of vulnerabilities was found in the Client Access Service (CAS) component of Exchange Server. Very conveniently for the threat actors, the CAS component is commonly exposed to the internet to allow users to access their emails via mobile devices and browsers.

This vulnerability set is an example of vulnerability chaining. Threat actors can execute arbitrary codes and run remote PowerShell sessions to be established in the affected systems if they exploit these vulnerabilities together. Through the months of August and September 2021, there were reports of the ProxyShell vulnerability being exploited to inject ransomware strains such as LockFile, Babuk, and Squirelwaffle. As of August 2021, there were 1,900 Exchange attacks reported.

CVE-2021-34523	**CVE-2021-34473**	**CVE-2021-31207**

Log4Shell

Marked as **CVE-2021-44228**, this vulnerability was discovered in Apache's Log4j library. On exploiting this vulnerability, threat actors can execute arbitrary codes on the affected systems. Once exploited, the threat actor gains complete access to the affected system, after which they can steal data, launch ransomware attacks, or conduct other malicious activities. Since Log4j is an open-source library, it is used in thousands of products and projects around the world, and it isdiversely incorporated, making it hard to track and patch. This vulnerability is a classic example of how quickly and relentlessly a known vulnerability is targeted for attacks. According to reports,

there were approximately 10 million exploit attempts per hour recorded for this vulnerability in the US alone.

CVE-2021-44228

ZeroLogon

Moving further back in the time line, this vulnerability in Windows Server from 2020, marked as **CVE-2020-1472**, is also still part of the threat actor's kit of favorite vulnerabilities to exploit. This was a particularly critical vulnerability as it was found in Microsoft Netlogon Remote Protocol, the service that lets a domain controller authenticate and issue access to thousands of users that are part of an organization's Active Directory. The vulnerability leverages a flaw in the encryption process that allows a threat actor to bypass authentication and impersonate a valid user without even knowing their credentials. This vulnerability's exploit is akin to giving the master key of your network to a threat actor. Once the threat actor impersonates the domain controller, they gain administrative access to the organization's network resources.

CVE-2020-1472

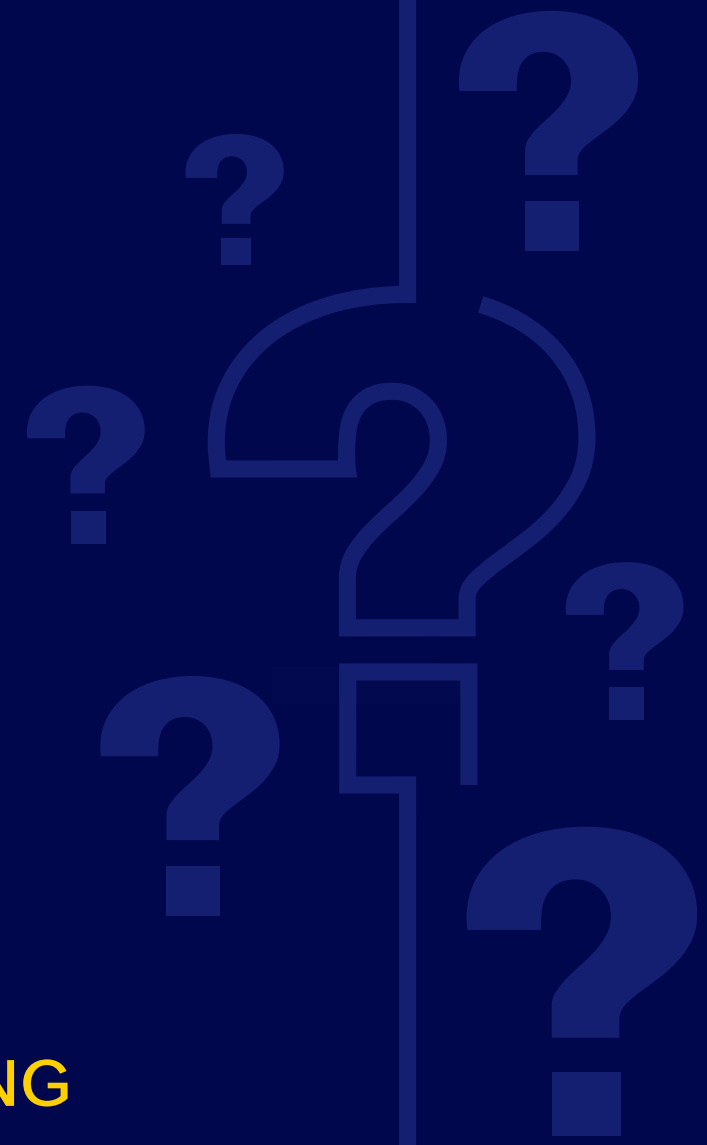
Third-party vulnerabilities

There are few past vulnerabilities in Atlassian, Pulse Secure, and Fortinet that are still being targeted. The only explanation for why vulnerabilities resolved in 2018 and 2019 are still being exploited is a vast number of unpatched systems.

CVE-2021-26084 - Atlassian Confluence Server and Data Center
CVE-2019-11510 - Pulse Secure Pulse Connect Secure
CVE-2018-13379 - Fortinet FortiOS and FortiProxy

After multiple reports and warnings about the show-stopping effects of publicly disclosed software vulnerabilities, what comes as a shock is the fact is that a vast majority of organizations still have unpatched vulnerabilities that were reported anywhere between 2002 and 2018, according to Bitdefender's 2020 Business Threat Landscape Report. The report also illuminated that around 64% of all reported unpatched vulnerabilities during the first half of 2020 involved CVEs that are older than 2018.

CVE-2021-26084	CVE-2019-11510	CVE-2018-13379



SO WHY AREN'T ENTERPRISES PATCHING **KNOWN VULNERABILITIES DESPITE BEING** AWARE OF THE RISKS?

TEMPTING FATE: IGNORING THE KNOWN IN AN INCREASINGLY UNPREDICTABLE ENVIRONMENT

However prepared and proactive enterprises are with their cybersecurity measures, the chances of never falling prey to a cyberattack are slim. A great amount of cyber risk can be mitigated by patching known vulnerabilities and keeping enterprise software up to date. The other part of it depends on how invested an enterprise is on keeping a close eye on the patterns and trends in the threat landscape and shoring up their defenses accordingly.

Even though regular patching seems like one of those rational things that any organization would do to manage publicly disclosed vulnerabilities, it's easier said than done. There are way too many challenges to enterprise patching than one would ideally expect from an essential cybersecurity practice.

01

Don't fix it if it isn't broken

Many enterprises have set processes that just work for them. They have a collection of software that is perfect for their workflows. The pace at which software updates are released is not uniform across vendors, which often means that there's a high chance of incompatibility between software solutions that collaborate when one of them undergoes an update. Dealing with such incompatibility issues can be time-consuming and hamper productivity, both of which are not ideal when it comes to large enterprises. Another reason for not installing regular updates is simply the fear that the updates might be buggy and might hurt the enterprise more than help it's security posture.

In such cases, enterprises would rather run with legacy systems that they know for a fact will work than gamble with the shortcomings of updating on a regular basis. They wouldn't be entirely wrong, either, considering how many problematic updates Microsoft released and rolled back just last year.

02

Patches, patches everywhere

The sheer increase in the number of updates and patches released a year makes it extremely challenging to test, qualify, and deploy them to a vast number of systems. With malware and ransomware being available as a service and the field being extremely lucrative for attackers (the cost of damage due to ransomware is predicted to hit $265 billion annually by 2031), more threat actors have jumped at religiously scanning for and exploiting open vulnerabilities.

The higher the number of vulnerabilities published, the more the onus is on the software vendors to release an update to fix that vulnerability. In 2021, there was a total of 20,169 CVEs logged. Testing out the patches released for all of these publicly disclosed vulnerabilities and installing them is a feat that even organizations with a big IT team would hesitate to undertake.

03

Productivity first, security next

Remember clicking Skip every time our system prompts us to reboot in the middle of a task? Imagine the frustration if your system just reboots without even a prompt. That is what happens when an auto-restart policy is not configured after a patch installation that requires a reboot. Such unplanned reboots and system downtime in a business-critical asset or during a business-critical activity is another reason enterprises prefer not to deploy patches on a regular basis. At the end of the day, it is productivity that comes first. Unless software vendors come up with a solution that allows productivity and security to coexist, regular patching will not become the norm, no matter how essential it is.

04

Tracking down **the vulnerability**

Ever followed the driping sound of a leaking faucet to close a tap? Now this is simple if you live in a place with five taps, but imagine there are 100 taps. By the time you find the leaky faucet and turn it off, you will have lost a significant amount of water.

Granular visibility is a must when it comes to your IT infrastructure. Most software supply chain attacks happen because enterprises do not know what components they are running in their network. This is particularly the case when it comes to third-party applications or software that enterprises run.

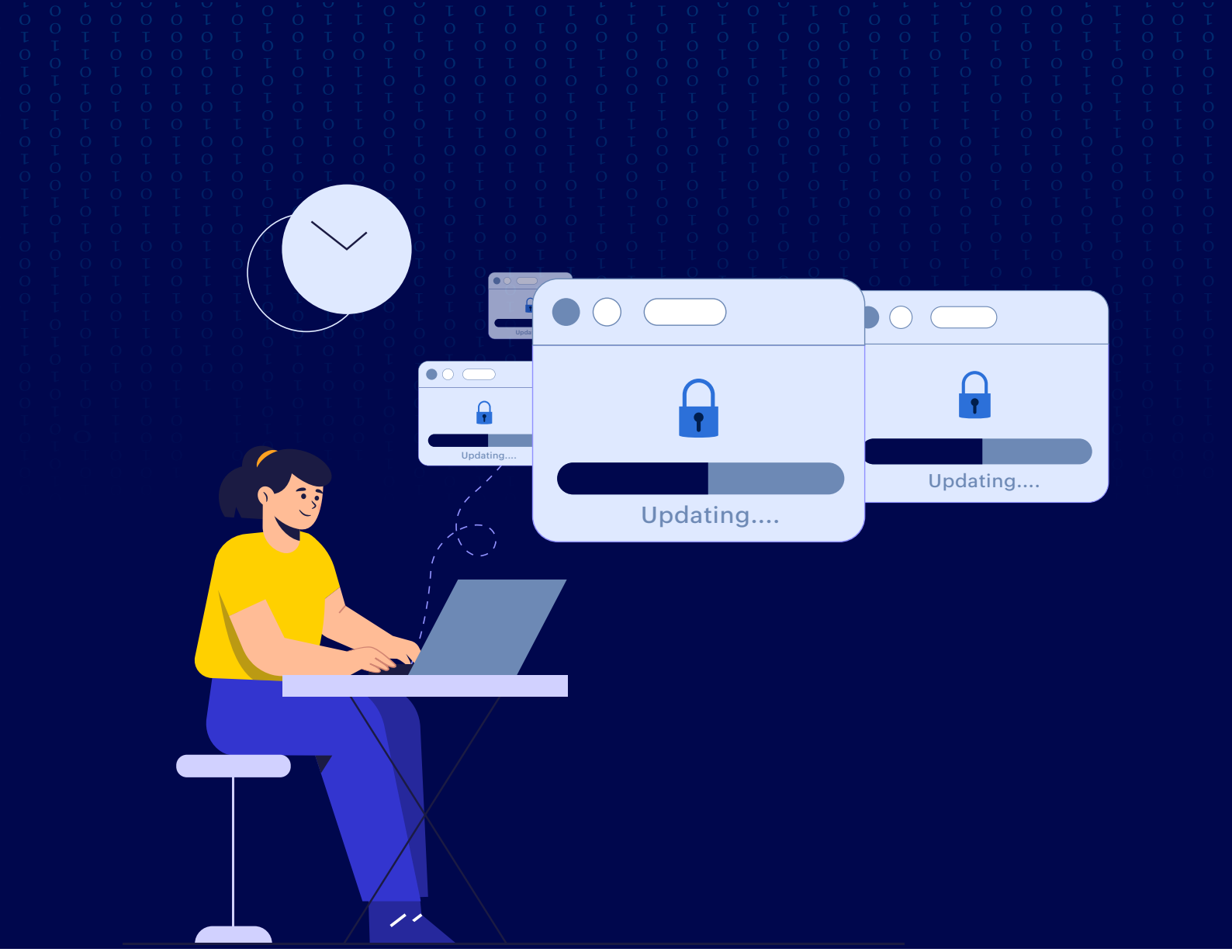
In cases like these, enterprises don't often have the visibility or even control to manage their entire software supply chain. They might not be able to compel the vendors in their supply chain to take prompt mitigation in case of attacks. This is a major contributor to old vulnerabilities still existing unpatched in many enterprise networks.

05

The **blame game**

In large enterprises, vulnerability detection and mitigation is usually handled by different departments. Various departments working like a well-oiled machine is still just a dream, which makes the mitigation processes slow and riddled with gaps. In the advent of an attack, there is a lot of finger pointing, not to mention compatibility issues between various solutions.

There is no guarantee that your patch management solution will support the vulnerability that your detection solution discovered in your network, which just translates to added man-hours spent on updating your systems. This communication gap exists not just at a solution-level; oftentimes, the CISOs of enterprises have difficulties convincing the board about the security challenges the organization is facing and the solutions required to address these challenges. This could hinder the average time it takes organizations to address a vulnerability or issue.



BALANCING ACT: ENSURING SECURITY WITH MINIMUM CHANGES TO ROUTINE

Navigating the challenges that enterprises have when it comes to establishing and sticking to a regular patch management practice is tricky. Often times, IT teams have to tread on thin lines to ensure security without compromising on productivity and employee experience. The strategies followed by organizations to balance their security concerns with the rest of their workload differ with respect to the size of the enterprise, their IT budget, security priorities, IT team size, and so on. However, there are a few best practices that all organizations can follow to analyze and improve their existing security posture.

01

Marie Kondo'ing **the IT infrastructure**

Cutting through the IT clutter is the logical beginning to creating a set routine that ensures cybersecurity. Proper visibility into what is being run in the enterprise is essential to set up your defenses. On a regular basis, IT teams must have software and hardware audits to upgrade old versions, renew expired licenses, and to remove redundant assets and applications.

This alone, however, cannot stop software supply chain attacks, as organizations might not have control over their third-party applications and software. To address this, network defenders need to integrate a standard framework like Cybersecurity Supply Chain Risk Management and check supplier certifications to ensure suppliers follow security practices such as:

- Using a software development life cycle and incorporating secure software development practices.
- Actively identifying and disclosing vulnerabilities while maintaining a vulnerability response program.
- Enabling regular patch management for their software.
- Developing, maintaining, and using approved supplier lists for their products.

Maintaining a comprehensive software and hardware inventory and unifying IT operations, i.e, using one solution to achieve related IT operations, can also help with gaining better visibility and reducing alert fatigue.

02

Automating the **pilot testing of updates**

Testing patches on a pilot group of systems before deploying them company wide is an essential step in the patch management routine. Automating this testing process could not only save you the manual effort, but also make it quicker and error-free. All you have to do is select your test group carefully by incorporating the same versions and flavors of systems that are present in your production environment.

Even though vendors cover the most common use cases and test the updates on a functional level, on an environment level, there are chances of these updates misbehaving. To avoid surprises like the January 2022 Patch Tuesday updates breaking VPN connections, causing Windows Server domain controllers to restart and preventing Hyper-V from starting, it is crucial to test any new update on systems that are running the same set of applications running in your enterprise.

03

Defining a green state **for patch management**

The patch management regime for each organization is unique, which is why it's important for IT teams to sit down and prioritize, what they need updated, what can wait, and what to avoid. Organizations have to come up with a patch compliance criteria that fits them and update their machines based on these criteria. Regularly monitoring to see if this compliance is met, will keep the enterprise systems in the green state.

04

Backups t**o the rescue**

No level of precaution can completely eliminate mishaps, which is why it's important to be prepared for the worst. You should practice taking an image your systems before deploying patches to them. If your patches end up breaking an essential process, you can immediately revert to the previous state by deploying the image. Apart from being a complete savior in case of a breakage, such backups give the IT teams the confidence to create update strategies that involve regular patch management and IT house keeping.

05

Flexible deployments **and reboots**

Regular patch management should not come at the cost of productivity. It is crucial to plan patching schedules during non-business hours or at a time that would cause the least amount of inconvenience to the end user. You don't want to deal with patches getting installed and reboots happening when a user is involved in a business-critical task.

Patch solutions should give end users the option to defer patch deployments and reboots to a later date and time. In contrast, these solutions should also come with an option to install these patches that have been deferred to ensure that the systems are, ultimately, patched and up to date. Flexibility in deployments and reboot schedules is an important criteria that can push organizations to forming regular patching schedules.

06

Say goodbye to fragmented, **siloed security approaches**

Getting approvals and cutting through the red tape is one of the major reasons for enterprise patching being irregular. In organizations with multiple teams and multiple solutions for various endpoint IT requirements, collating data from various solutions into meaningful information, conveying it to the members involved, and getting the approval to carry out an operation, even one as essential as patching, is time-consuming and sometimes futile.

What would greatly help is if endpoint security is handled by one solution that brings all the data you need to a centralized console. Even if there are multiple teams, they can all be given access to this solution or tool, so that all the information teams need is readily available in one place, cutting out the time teams waste explaining things to each other. This also makes it easier to convince the board about the return on security investments, because it's easier to measure the metrics from one solution. Troubleshooting is easy and alert fatigue is greatly reduced when you move your security operations to a single solution.

ENTERPRISE PATCH MANAGEMENT: THE FUTURE

It is foolish to ignore known vulnerabilities and gamble the future of your organization on not being targeted. SOCs have enough on their hands dealing with unknown vulnerabilities and ramping up enterprise security posture to handle unexpected surprises without adding the extra work of dealing with unpatched known vulnerabilities.

Patching regularly will help cut down the amount of time and effort that security teams have to put into dealing with security events. But then again, this is only possible if a proper patch management strategy is charted out and followed. Automated patch management with proper testing and flexible deployment options is the way to go about it. It's even easier if the entire process of vulnerability detection and patch management can be done from a single console. With the sharp increase in endpoints and roaming devices, being physically present to carry out essential IT tasks like updating and fixing them is no longer viable. This is why IT management and security solutions have become part of many organizations, big and small.

This is also why vendors are developing solutions to solve any and all IT problems. It is up to the enterprise security teams to qualify their requirements and pick the solution that best fits their needs. Analyze the threat landscape trends and go for a solution that provides a level of flexibility to change.

Moving forward, enterprises should carefully screen and select security solutions that let them automate most routine tasks and give them granular visibility into vulnerable assets. On a higher level, they should slowly adopt and make the shift to a centralized cybersecurity structure to improve visibility and overall management of their IT operations.

MANAGEENGINE

PATCH MANAGEMENT SOLUTIONS

PATCH MANAGER PLUS

Completely automate the testing and deployment of OSs along with over 850 third-party applications on Window, macOS, and Linux machines.

TRY NOW FOR FREE!

VULNERABILITY MANAGER PLUS

Leverage comprehensive vulnerability assessment, detection, and mitigation from a single console.

TRY NOW FOR FREE!

ENDPOINT CENTRAL

Manage and secure endpoints from a centralized console

TRY NOW FOR FREE!