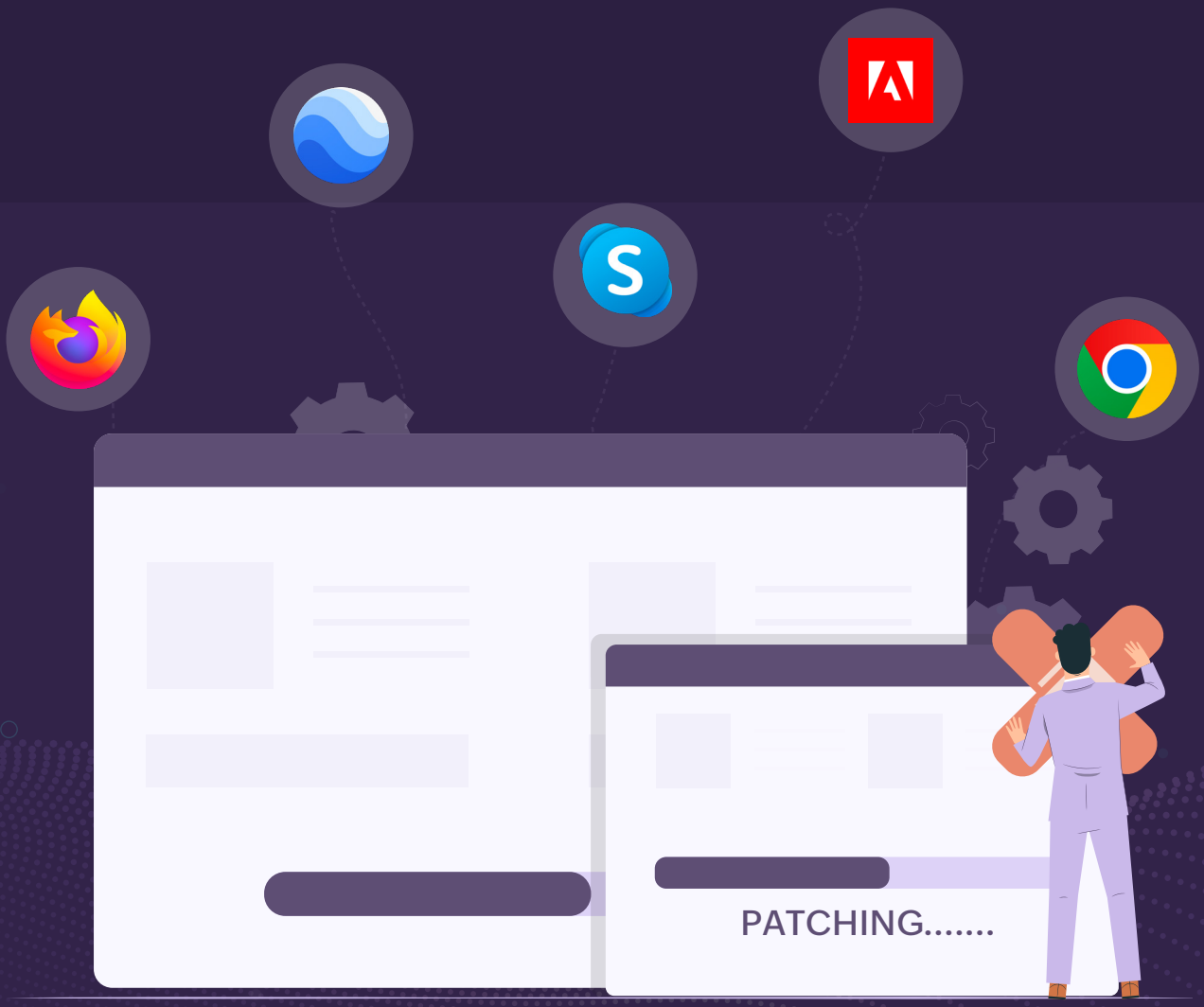
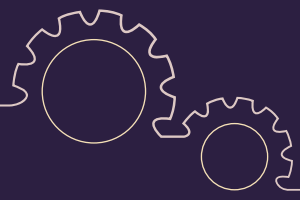
Patch management best practices: **A detailed guide**



ManageEngine

Intro



"It is only when they go wrong that machines remind you how powerful they are."

- Clive James, broadcaster and journalist

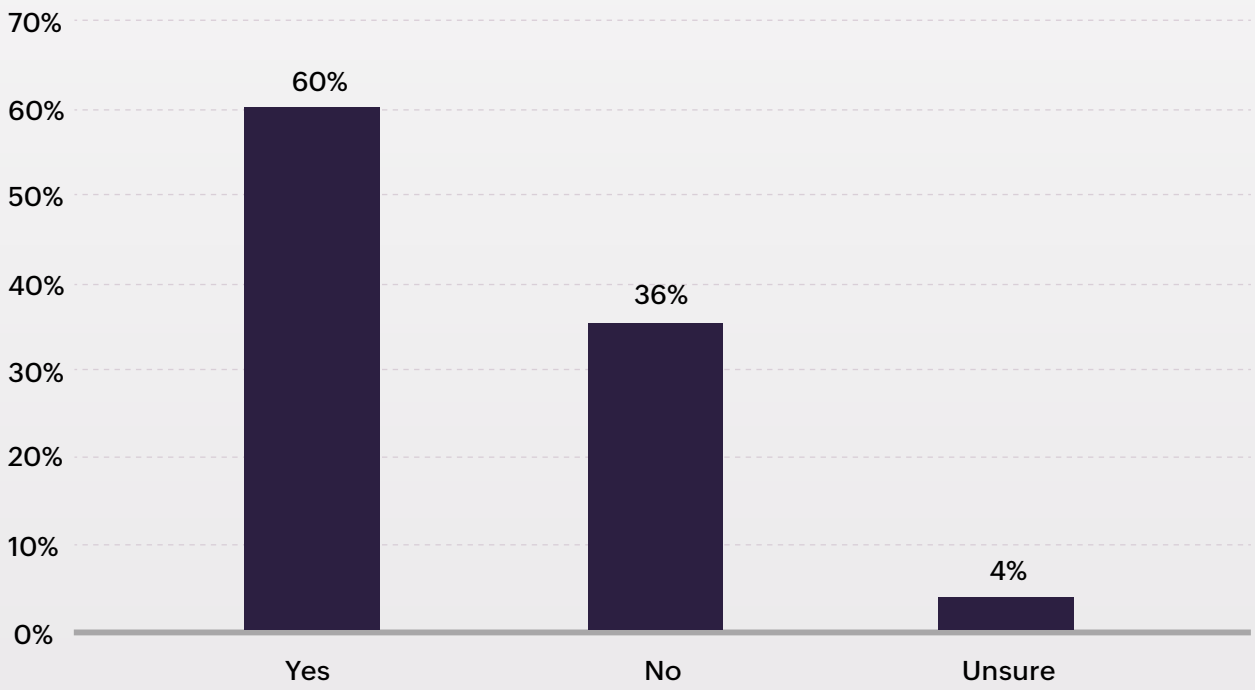
Per Forbes, in 2020, a new organization became a victim of a ransomware attack every 10 seconds.

With the number of cybercrimes rising at such a rapid pace, does your organization have what it takes to fend off attacks?

Financed by ServiceNow, a study by Ponemon Institute found that timely patching is critical to prevent data breaches in an organization.

Furthermore, 60% of the respondents featured in the study stated that one or more of these breaches might have occurred because although patches were available for the known vulnerabilities, they remained unapplied.

FIGURE 1. Did any of these breaches occur because a patch was availale for a known vulneraility but not applied?(2019 study)



This e-book will take an in-depth look at patch management best practices that organizations can follow to scale up their patching game. Furthermore, we'll point out and analyze these best practices for easier understanding.

So, let's dive in.

Patch management best practices:
A detailed guide

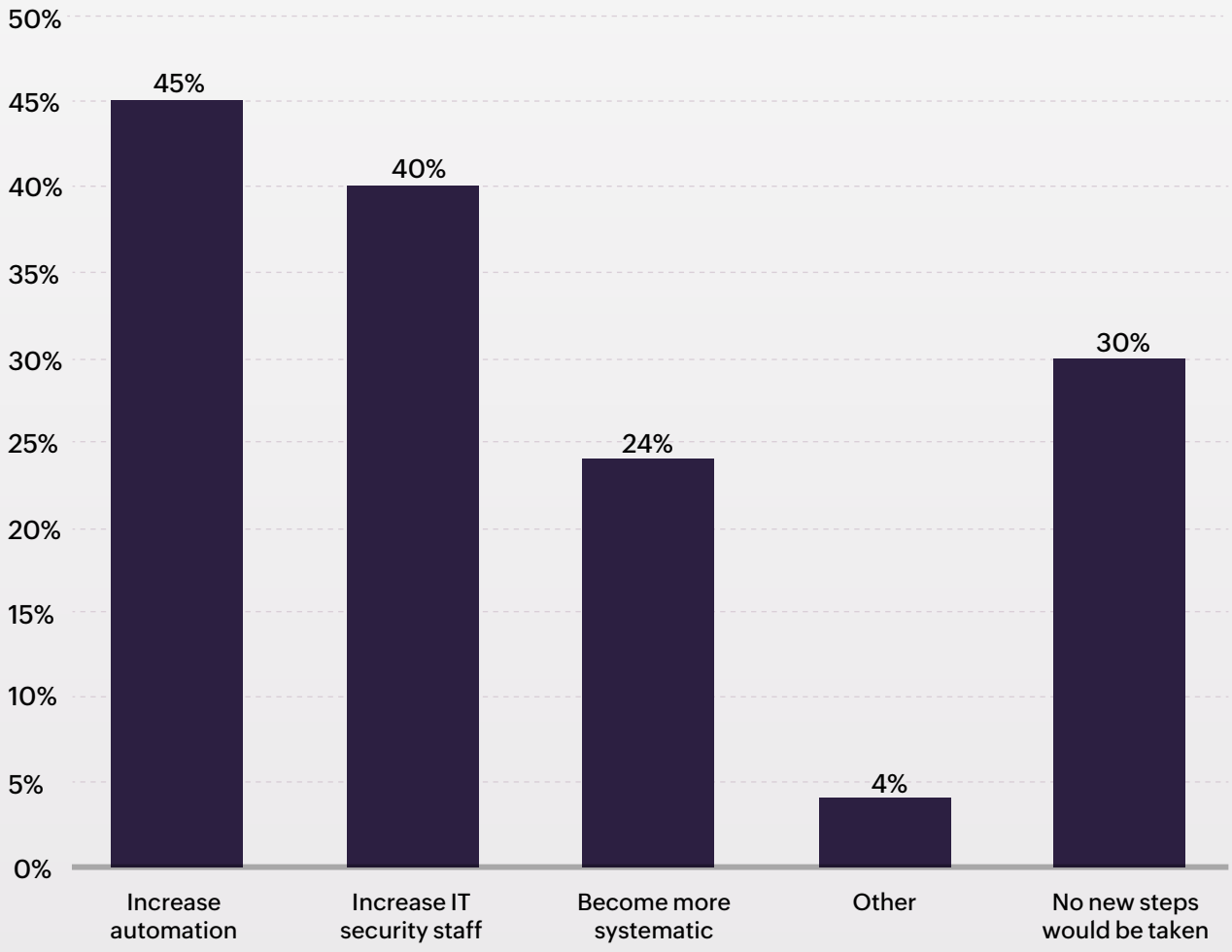
Automate patch management

Checking for new patches, coordinating with teams, testing and installing those patches—all while ensuring user productivity doesn't take a dip. Sounds like a lot, right? And imagine what it's like when all of this is done manually!

The average time it takes to patch a critical vulnerability is 16 days. In fact, one of the biggest reasons for delays in patching vulnerabilities is due to relying on manual processes. The longer unpatched vulnerabilities are out in the open, the more organizations are at risk.

Automating patch management to ensure regular patching should be the first best practice implemented in your organization for better patch compliance.

FIGURE 2. What steps would you take to improve your organization's patch management? More than one response permitted (2019 study)



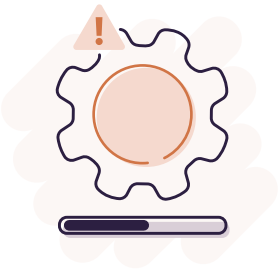
The chart above states that 45% of the respondents in a study believe that increasing automation can improve their organization's patch management.

Evaluate patches in a test environment before deploying them to endpoints

There are instances where certain patches can affect how an endpoint functions or even bring it down. To prevent this, it's always recommended to test patches in a pilot group of endpoints (aka a test environment) before deploying them across the network. As a rule of thumb, your test environment should mirror your network and must consist of all the different operating systems (OSs) used.

Once the patches have been tested and are found to be stable, you can approve and deploy them across the endpoints in the network.

Use a critical updates first approach



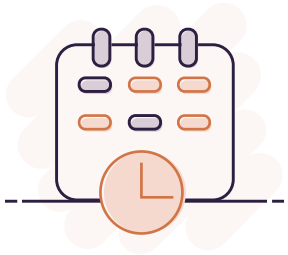
Prioritizing patches and highly vulnerable systems is a must to ensure patch compliance across the network and for effective patch management.

Here are some ways to administer the critical updates first approach:

- Patches with their severity marked as Critical or Important should be tested and deployed first
- Highly vulnerable systems* should be given high priority while patching
- Business-critical endpoints and internet-facing devices should be patched as soon as possible
- Patches of moderate or low severity should be deployed and less vulnerable* systems should regularly be patched as per scheduled maintenance windows

*The vulnerability of a system is defined by the number of missing patches. It varies among organizations as per their risk tolerance and patch management policy.

Schedule auto-deployments twice a week



With tens of thousands of vulnerabilities being recorded every year, it's imperative that you patch systems on a war footing. A good strategy to regularize patching is to schedule deployments twice a week.

Vendors release updates for products like Firefox and Chrome almost every week to mitigate vulnerabilities. With patch deployments scheduled twice a week, you can:

- Ensure that your systems are patched with all the latest updates.
- Test patches thoroughly before deploying them to endpoints across the network.
- Manage and monitor endpoints to check for patch compliance.
- Prevent dips in user productivity due to shutdowns or reboots.

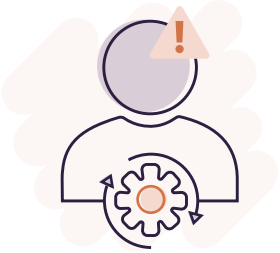
Create configurations to suit your business needs

Creating a patching configuration that suits the entire organization's work schedule is a pretty challenging task. Instead, creating different groups based on domains, OSs, specific hardware, the presence of certain applications, etc. is the ideal option.

Here are some configurations that you can use while creating groups:

- Deployment based on Patch Tuesday schedules
- System groups based on critical business machines and servers
- System groups based on less critical business machines and servers
- Reboot scheduling based on usage and non-working hours

Allow user intervention to prevent drops in business-critical activity



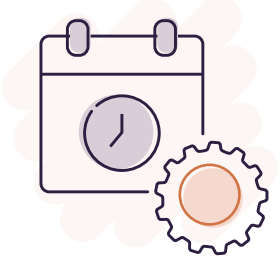
If patch compliance is one side of the coin, user productivity definitely is the second, and striking a fine balance between the two sides is what keeps sysadmins on their toes .Allowing user intervention to skip or delay rebooting is essential to ensure that they're not interrupted in the middle of a business-critical task.

To make sure that patches are applied, you can either notify them about rebooting after a specified interval or force reboot if the situation demands.

Generate detailed patch summary reports

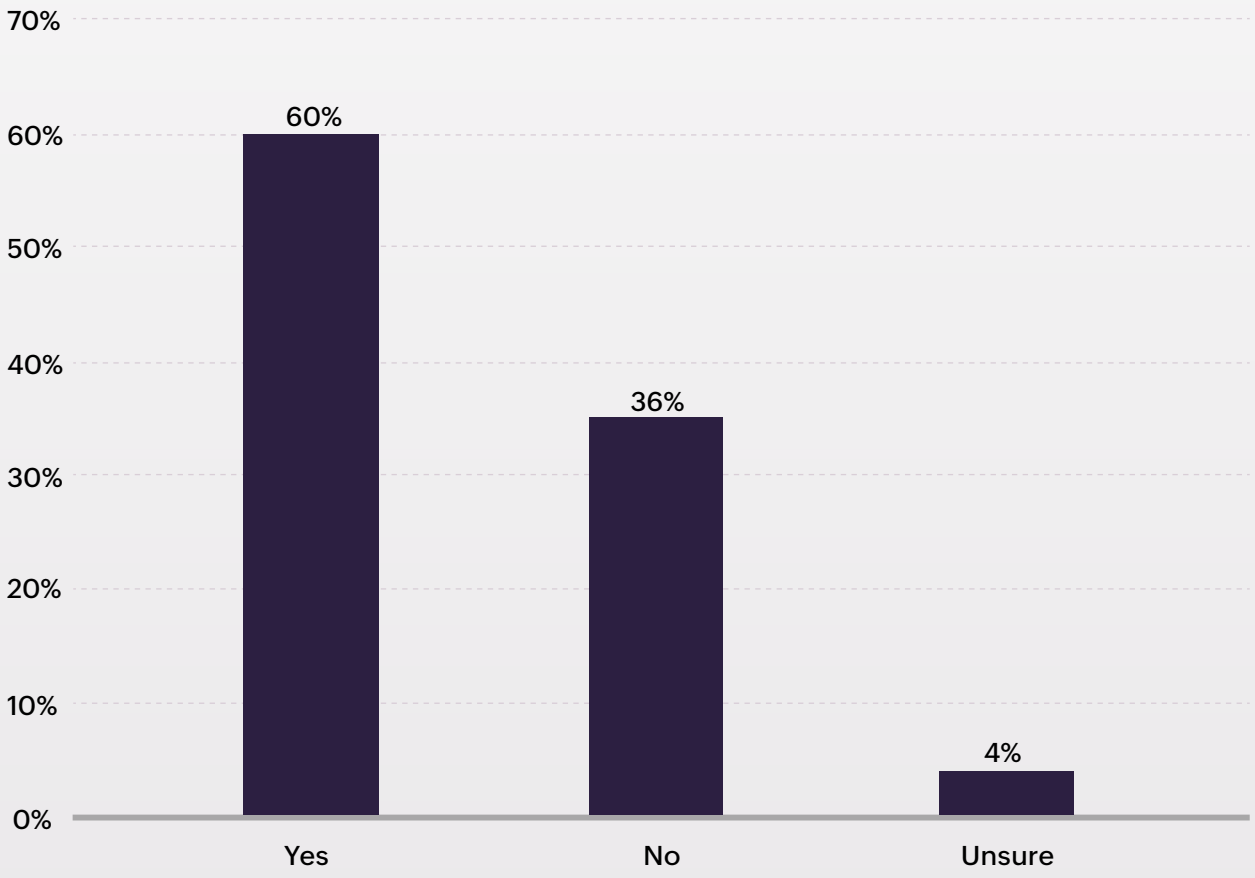
Generating detailed reports is highly crucial for security auditing purposes as well as tracking patch compliance, so you should regularly generate reports that specify patching dates, version details, deployment results, and so on. As an added benefit to monitoring the patching status across the network, you can also track the vulnerabilities mitigated with regular reports.

Patch regularly, not just for zero-days



In the aforementioned Ponemon Institute study, 62% of large organizations acknowledged their inability to patch a known vulnerability, which eventually caused data breaches.

FIGURE 3. Did any of these breaches occur because a patch was availale for a known vulneraility but not applied?(2019 study)



As important as it is to quickly patch zero-days, you should also make sure to have a regular patching schedule.

Patch management best practices for WFH setups

With how common work-from-home (WFH) setups now are, it's becoming increasingly difficult for admins to ensure patch compliance in remote endpoints. Here are some best practices to follow to patch remote endpoints.

Secure communication between remote endpoints and the enterprise's server with an additional security layer

Patching endpoints located within your organization's network doesn't possess as much of a security risk as it does while patching remote endpoints.

Allowing remote endpoints to connect to the organization's server for patching opens it up to a world of chaos. And it is quite obvious that such unsecured communications can lead to a plethora of security breaches.

The solution to this? Use an additional layer of security that acts as an intermediary, thus preventing the enterprise's server from being exposed to the internet. An ideal tool would be using a Secure Gateway Server for communication between the remote agents and the server.

Suspend optional updates and rollups

Prioritize the installation of critical updates in remote endpoints and suspend any other rollups or optional updates to ensure that the endpoints have been patched with the necessary updates. Optional updates and other less critical ones can be deployed as per regular patching schedules.

Create separate APD tasks for remote endpoints

Creating separate automated patch deployment (APD) tasks for remote endpoints makes it easier to deploy patches. Since these remote agents have different requirements and hence different configurations, a separate set of APD tasks will ensure that you can actively monitor their patch compliance, clutter-free.

Use a secure gateway server for communication between remote endpoints and the enterprise's server

Patching endpoints located within your organization's network doesn't pose as much of a security risk as it does while patching remote endpoints. Allowing remote endpoints to connect to the organization's server for patching opens it up to a world of chaos, and it's obvious that these unsecured communications can lead to a plethora of security breaches.

The solution to this? Use a secure gateway server to secure the communication signals between the remote agents and the server.

FAQs

01

How often should patch management be performed?

An ideal patch management routine should consist of **two patch deployment schedules a week**. For zero-day vulnerabilities, they should be patched as soon as possible. However, always ensure that the patches are thoroughly tested on a test group before deploying them to production machines.

02

Which is the best patching solution: agentless or agent-based?

Agent-based solutions are generally considered the best choice since they reduce patch failure more efficiently and are easy to deploy to remote endpoints.

03

Should I go for a point product or a configuration management solution?

The choice depends upon your organization's requirements. For organizations that have a dedicated team to manage and handle patching, point products are the best option. In smaller organizations that prefer managing multiple administrative tasks from a centralized console along with patching, configuration management solutions are the ideal choice.

04

What are the phases in a patch management policy?

An ideal patch management policy includes the following phases: **testing > deployment > generating reports > auditing.**

ManageEngine's solutions for patch management

Patch Manager Plus

A stand-alone patch management solution that completely automates the patching of Windows, Mac, and Linux OSs along with over 850 third-party applications. Ensure hassle-free patch compliance in your network using either the on-premises or cloud version.

FREE TRIAL LEARN MORE

Patch Connect Plus

Unify the management of third-party apps and updates to Microsoft Endpoint Configuration Manager and Endpoint Manager. With an extensive library of over 400 applications, automate the entire patch management cycle for your endpoints.

FREE TRIAL LEARN MORE

Vulnerability Manager Plus

Assess vulnerabilities and mitigate them with automated patch management. You can also manage web server hardening, security misconfigurations, and high-risk software audits to quickly reduce your risk level.

FREE TRIAL LEARN MORE

Endpoint Central

Endpoint Central is a unified endpoint management and security solution that enables patch management, OS and software deployment, mobile device management, remote troubleshooting, and much more, all from a centralized console.

FREE TRIAL LEARN MORE

Conclusion

This e-book covered the best practices to follow while patching endpoints in your organization's network as well as remote endpoints. With an ever-increasing rise in vulnerabilities, following these best practices can improve patch compliance and prevent vulnerabilities across your network.