EBOOK

PATCH MANAGEMENT POLICY

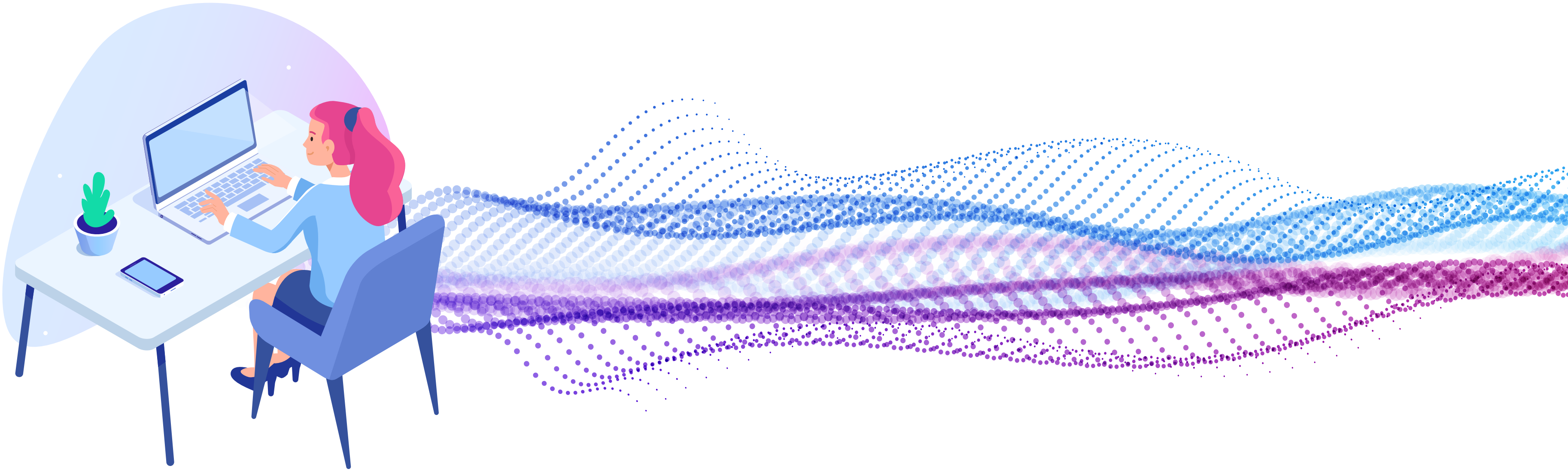
BEST PRACTICES

Introduction

With over 57% of data breaches occurring due to poor patch management[1] and a massive increase in cyberattacks due to remote and hybrid work, it is more imperative than ever to ensure that you have a robust and reliable patch management policy in place that strengthens your security posture. A strong patch management policy is comprised of a set of steps and procedures aimed towards managing and mitigating vulnerabilities in your environment through a regular and well-documented patching process.

It helps MSPs and internal IT teams install and manage patches rapidly and cost-effectively, and scale quickly according to their evolving needs. In other words, it offers you the flexibility to personalize patch management to cater to your business's unique requirements.

We've put together some best practices that will help you optimize your patch management policy, help mitigate your cybersecurity risk and allow you to sleep better at night knowing you've got a reliable policy in place.



Focus on third-party patching

A study by SecureLink and Ponemon reveals that 51% of organizations do not assess the security and privacy practices of all third-parties before granting them access to sensitive and confidential information.[2] It goes without saying that MSPs need to ensure the safety of all their clients' varying IT environments including third-party applications and software.

Third-party patching is an integral component of patch management. In addition to patching your operating system (OS), you must also patch all third-party applications and software to get rid of any vulnerabilities that might otherwise act as entry points for cybercriminals to launch attacks.

Your RMM solution should be able to offer scalable patch management capabilities for both Macs and PCs, as well as have a continuously improving third-party patching module that can meet your future needs.

Focus on a security-first approach

A strong patch management policy always takes a security-first approach. Your policy must allow you to run vulnerability scans based on all security criticalities and patch them accordingly. Being able to build your automated patching with automated approval workflows for critical vulnerabilities will significantly reduce your attack surface.

Having an automated patch strategy that allows you to "set and rest assured" provides confidence to your clients and efficiency to your MSP. Being able to leverage automation provides tremendous control over your processes and allows you to do exactly what you need to do with them each and every time. Choosing an RMM that offers flexible and scalable patch management should be a key aspect of your tool consideration.

Scan and prioritize patching

It is important to be able to deploy a patch management solution that allows you to scan and prioritize patching based on the Common Vulnerability Scoring System (CVSS). Your RMM solution should be able to provide full control and power over scanning and patching, with flexibility to tune accordingly to your business's unique needs.

An RMM solution that is designed to not only cater to a diverse customer base but also to adapt and evolve according to the changes in IT environments (for example, when a new software comes onboard) is crucial for the sustainable scalability of your business.

Follow these 3 strategies to reduce your attack surface

Patch management policy is all about risk mitigation. Securing your endpoints is one of the most effective ways of reducing your attack surface. However, patching is only a part of the strategy to secure your endpoints. Securing endpoints is essentially a multidimensional approach. You need a policy that configures and hardens your endpoints against cyberthreats. Here are strategies you can employ to secure your endpoints:

PATCHING strategy

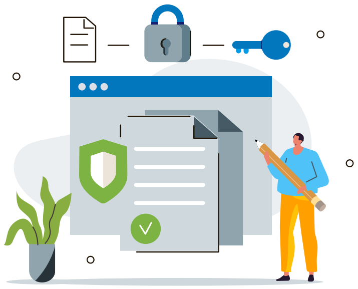
You must secure your endpoints by patching your OS as well as third-party applications. While most other RMM solutions do not provide patching capabilities for both PCs and Macs, some do offer powerful and complete patch management across both Mac computers and PCs.

HARDENING strategy

Securing endpoints is not just about patching. It is also about hardening your configurations using regulatory standards such as CMMC and NIST-171, and implementing these policies within your RMM solution.

AV/AM strategy

Another important aspect of reducing your attack surface is ensuring your AV/AM solutions are deployed properly and working efficiently.



Leverage all the three categories of patching

Another important aspect of a patch management policy is making sure that you are making the most of the following three different categories of patching such as:

Automated —

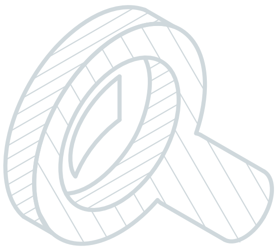
The patch management policy should intuitively automate the most critical vulnerabilities in your system and network.

Approval-based —

Another set of policies should focus on getting appropriate approvals for implementation to make sure they don't interrupt your operations.

Get to it when you can —

The lowest priority/low risk policies should be designed in a way that they can be implemented on an as-needed basis.



Building a strong patch management policy: A Summary

Here's a quick roundup of what you need to do in order to build a strong patch management policy:

- Ensure you have comprehensive and scalable third-party patching
- Focus on a security-first approach
- Scan and prioritize patching based on CVSS
- Ensure you have comprehensive strategies in three key areas to reduce attack surface
    1. Patching
    2. Hardening
    3. AV/AM
- Design patching with level one prioritization as much as possible:
    o Priority level one: Fully automated patching
    o Priority level two: Approval-Based patching
    o Priority level three: 'Get to it when you can' patching

Conclusion

Unlike most RMM solutions that can leave IT professionals vulnerable with limited and/or unreliable policies, Kaseya VSA offers flexible, scalable policy management with tremendous granularity and control over patching. With its service-centric approach, Kaseya VSA enables you as an IT Professional to build your own policy management services based on your best practices, your standards and your vision of running your business.

To learn more about Kaseya's powerful patch management capabilities, request a quick demo now!

Sources

1. Patching best practices, CNP technologies
2. SecureLink and Ponemon

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.