3 TIPS TO SECURE YOUR ENDPOINTS
WITH AUTOMATED PATCH MANAGEMENT

Deploy, install, and update software across all endpoints

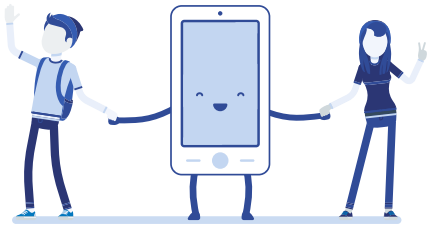
SIGNIFICANCE OF SOFTWARE PATCH MANAGEMENT

Patch management is a critical aspect of the IT security process. However, a manual process for patching no longer works. More than 22,000 software vulnerabilities were disclosed last year, so the volume is large and growing.

Along with that large number of vulnerabilities, there's also an increasing number of security incidents and breaches. IT professionals must incorporate a new strategy that automates patch management to create a robust security layer with the routine and timely installation of patches; time being the most critical element.

Reports say that with the timely deployment of patches, organizations can reduce the likelihood of a breach by 41%.[1] Isn't that mind-blowing? Think about how many breaches companies could have avoided with a proper patch management solution.

Timely deployment of patches can reduce the likelihood of a breach by 41%



Hackers love security flaws, also known as software vulnerabilities. A software vulnerability is a security hole or weakness found in a software application or operating system. Hackers take advantage of this weakness using exploits and wreak havoc on our lives.

IT professionals need more than ad hoc manual processes to prevent this chaos and the resulting damage to the business. A proactive approach involves implementing an effective patch management strategy to keep hackers out of their systems.

MANAGING PATCHES CAN BE A COMPLICATED PROCESS

BUT, IT DOESN'T HAVE TO BE.

There are 3 critical components of any effective patch management strategy. Implement them and your systems and network will be strong.

Kaseya®

TIP SHEET

3 TIPS TO SECURE YOUR ENDPOINTS
WITH AUTOMATED PATCH MANAGEMENT

Deploy, install, and update software across all endpoints

PATCH FROM A SINGLE CONSOLE

Implement an "all-in-one" endpoint management solution that enables centralized management of multiple security functions including patching, antivirus/anti-malware deployment, and backup, across every endpoint.

Small and medium-sized businesses with small, multi-function IT teams need a unified solution that will save them time by allowing them to manage all core IT functions from a single console and avoiding the time wasted jumping from one tool to another. The time saved can be reallocated to other strategic projects that drive business growth.

HOW KASEYA VSA HELPS

VSA provides a proactive solution for unified IT management and comprehensive security along with scalable IT automation for you to:

- Deploy
- Install
- Update

all of your Windows, Mac, and third-party software from a single platform.

AUTOMATE PATCH MANAGEMENT

Do you struggle with manual installation of patches for all your endpoints? Four words: Set it and secure it. Leverage automation to implement proactive scans, and schedule timely patches. Consistent patching is the best way to overcome security risks associated with software vulnerabilities in your IT environment. Critical vulnerabilities should be remediated within 30 days of patch availability.

HOW KASEYA HELPS

VSA enables scheduling of automated patches by:

- Time
- Computer
- Group or user-defined collections of computers

Then, VSA

1. Scans networks for installed and missing security patches
2. Detects and monitors vulnerabilities
3. Maintains patch compliance effectively

of the organizations spend more time navigating manual processes than responding to vulnerabilities[2]

Kaseya®

TIP SHEET

3 TIPS TO SECURE YOUR ENDPOINTS
WITH AUTOMATED PATCH MANAGEMENT

Deploy, install, and update software across all endpoints

BREAK DOWN SILOS

Did you know that many organizations lose approximately 12 days[3] when implementing a patch due to coordination issues between teams? Patch management can be tedious and time-consuming when a company has organizational silos. Once an update is released, permissions are often required for installation, which might not be issued on time, creating a cycle of lag for patch installs.

THAT'S WHEN YOU ARE LIKELY TO FACE CRITICAL ISSUES WITH PATCHES.

HOW KASEYA HELPS

VSA enables the creation of policy profiles for automation of approval, review, or rejection of patch updates. With VSA you can simplify and streamline the process of software updates using standardized, profiles.

Incorporate an automated patch management solution and keep your systems and network secure. Contact Kaseya for a demo.

Sources

1 https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf
2 ibid
3 ibid

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.