Patching Your Healthcare Systems

Amid increasing security threats and subsequent exploitations, it's paramount for healthcare organizations to protect their systems against vulnerabilities, privacy violations and other risks. Patch management solutions from Ivanti offer system administrators the solutions they need to keep their systems stable and their endpoints protected, so they can focus on what they do best.

Protect your IT environment and your patients – you can't afford not to

It's no secret your app environment needs to be secure — especially when data center systems host your patients' Electronic Health Records (EHRs) and other highly sensitive information. Security breaches continue to rise in the healthcare industry, and HIPAA compliance is table stakes. In 2023, more than 124 million records were compromised in healthcare hacking incidents – with an average of 215,269 healthcare records stolen in each incident.[1]

Then there are the financial and legal ramifications of a breach, not to mention the lingering effects on reputation and patient trust. Large data breaches increased by 93% from 2018 to 2023, and ransomware attacks increased by 278% over the same period.[2] These attacks caused extended stays in hospitals, poorer patient outcomes, delays in diagnosis and treatment and diversions to other healthcare facilities. These negative impacts have put patient safety at risk, yet they are largely preventable.

2023 saw a major increase in enforcement actions by state attorneys general; 15 settlements were reached with HIPAA-regulated entities to resolve violations of HIPAA and state consumer protection laws; that is compared with three settlements in 2022, four in 2021 and three in 2019.[1]

70% **of breached PHI occurs in network servers[1]**

Most of these cases resulted from failure to implement appropriate safeguards to ensure data security and breach response failures, which violated the HIPAA Security Rule. One settlement imposed a $550,000 penalty and impacting 1.2 million individuals due to patch management failure, lack of encryption and a lack of security testing.[3]

Beyond your OS – patch your entire domain

Patching your Windows and macOS systems is often top –of mind – but those are only a portion of your domain. What about machines running Linux? Across the physical and virtual servers of your data center and your endpoint devices there are also numerous third-party applications that require regular attention.

Grow your patch domain to include Java, Adobe and thousands more applications. Close the third-party app-patching gap and reduce risks to endpoints and your data center — even directly from within the Microsoft Endpoint Manager console. Ivanti's patching solutions simplify, automate and prioritize patching processes, resulting in reduced risk, increased insights and improved cross-functional relationships.

Deploy priority patches faster

Fast deployment of the most critical patches is a desired goal for any IT team. Still, many struggle with a process that takes too long — potentially leaving healthcare systems exposed to risk.

You need to shorten the time from Critical Vulnerabilities and Exposures (CVE) read-out to the time patches are applied. What can take hours of manual review can be reduced to minutes by building patch lists from imported CVEs automatically.

You're given a consolidated list of relevant patches and can review specific lists of affected software, remove any patches you don't want to apply immediately, then continue to the scan-and-deploy stage. If it suits your environment, you also have the option to push out updates automatically.

See and report on patch status

Gain confidence that systems are performing and protected, from the data center to the endpoints at the point of care and everywhere in between.

Whether you need to demonstrate regulatory compliance, confirm protection against a recent malware threat or simply gain peace of mind, visibility is key. You want to be able to confirm at any time that your IT environment is stable and secure — including insights on patch status, real-time security outbreak alerts and more.

Patch on your schedule

Healthcare facilities often run 24-7. How do you ensure effective patching of all systems and stations without impacting the productivity of nursing and clinical staff? You must be able to control the maintenance window so care can be administered without interruption.

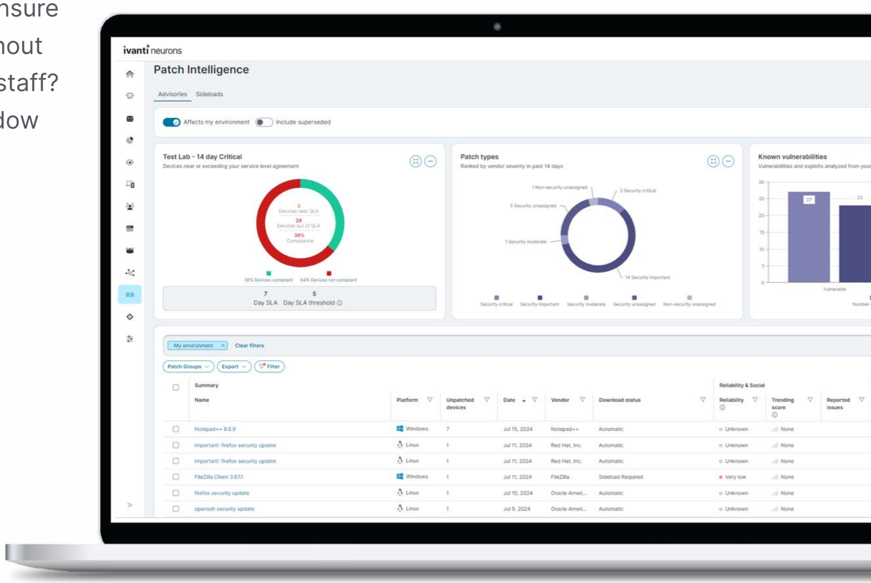
Owning the patch schedule means being able to designate specific stations for patching, while alternate access remains online for staff.

It also means having control to elevate the priority of urgent security patches, ahead of general bug fixes and software updates. Stitching together prioritized patches with the right schedule keeps systems secure and your healthcare workers productive. Automate the patch process and you further reduce risks associated with manual patching.

Find the solution that fits: on-premises, cloud or hybrid

When you're ready to migrate from on-prem to the cloud, do so confidently with the strength of Ivanti's patch technology.

With Ivanti, you can transition from on-prem patch management to the cloud at your own pace instead of being forced to "rip and replace." Ivanti's migration experience provides visibility into the devices managed in the cloud alongside those managed via on-prem Ivanti patch management solutions.



	Summary						Reliability & Social		
☐	Name	Platform	Unpatched devices	Date	Vendor	Download status	Reliability	Trending score	Reported issues
☐	Notepad++ 8.6.9	Windows	7	Jul 15, 2024	Notepad++	Automatic	Unknown	None	
☐	Important: firefox security update	Linux	1	Jul 11, 2024	Red Hat, Inc.	Automatic	Unknown	None	
☐	Important: firefox security update	Linux	1	Jul 11, 2024	Red Hat, Inc.	Automatic	Unknown	None	
☐	FileZilla Client 3.67.1	Windows	1	Jul 11, 2024	FileZilla	Sideload Required	Very low	None	
☐	firefox security update	Linux	1	Jul 10, 2024	Oracle Ameri...	Automatic	Unknown	None	
☐	openssh security update	Linux	1	Jul 9, 2024	Oracle Ameri...	Automatic	Unknown	None	

[1] The HIPAA Journal, "Security Breaches in Healthcare in 2023", 21 January 2024.

[2] The HIPAA Journal, "HHS Publishes Healthcare Sector Cybersecurity Strategy", 7 December 2023.

[3] The HIPAA Journal, "NY AG Fines Medical Management Company $550,000 for Patch Management Failures", 24 May 2023.

Prescription for Patching Healthcare Systems

Use Case Solutions	Common Tasks
Ivanti Neurons for Patch Management	Our most comprehensive risk-based patch management solution provides actionable threat intelligence, patch reliability insight and device risk visibility.
Ivanti Neurons for Patch for Intune	Deploy limitless third-party application updates within Intune as part of your existing application lifecycle management workflows.
Ivanti Patch for Configuration Manager	Download patch information and distribute patches for hundreds of applications automatically, including those most often attacked.
Ivanti Security Controls	Scan systems for missing patches — from Windows and Linux to physical/virtual servers and more.
Ivanti Patch for Endpoint Manager	Establish and automate consistent policies for patching all your assets — even those that are mobile, remote or asleep.
Ivanti Endpoint Security for Endpoint Manager	Gain insights about your environment, get help detecting security incidents and take swift action automatically. Locking down users' endpoints is not your only option for defense.

Maintain a healthy IT environment that's secure against threats and compliant with healthcare regulations. Get to know the patching solutions in Ivanti's security portfolio.

For more information, or to contact Ivanti, please visit ivanti.com.

About Ivanti

Ivanti elevates and secures Everywhere Work so people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued, and we are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com