ivanti neurons

Ivanti Neurons for Patch Management

Reduce threat exposure and risk by prioritizing and remediating vulnerabilities

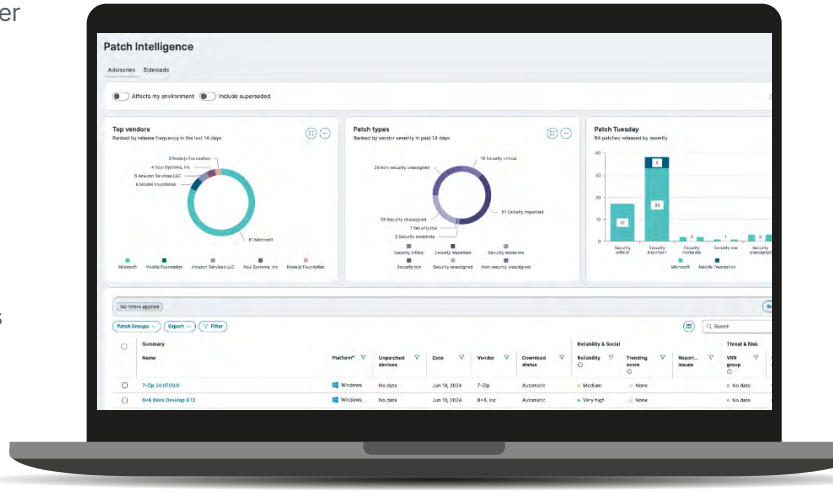
Ivanti Neurons for Patch Management is a cloud-native solution that provides actionable intelligence and device risk visibility across Windows, macOS, Linux and third-party applications. Prioritize and remediate vulnerabilities with insights on active risk exposure, patch reliability and device compliance. Protect against an array of threats, including ransomware.

Risk-based patch management

Ransomware attacks increase in frequency and severity every year – with devastating impact on businesses. Research puts the average total cost of a data breach at $4.88 million – a 10% jump from 2023 and the biggest increase since the pandemic.[1]

Attacks are only going to increase as technology and AI advance. Ransomware as a service (RaaS) enables just about anyone to launch an attack – no security knowledge or coding expertise required. An increase in vulnerabilities leads to an increase in risk; exploitation of vulnerabilities increased 180% year over year.[2] Research from Google shows that zero-day exploits have increased by 50% year over year.[3] Worse yet, the age of AI hacking is here. Researchers at the University of Illinois trained AI agents to autonomously hack websites to discover and exploit zero-day vulnerabilities.[4]

Patching to fix common vulnerabilities and exposures is one of the best things an organization can do to counter ransomware attacks. Unfortunately, 71% of IT and Security professionals find patching overly complex and time-consuming.[5] That may be due to the overwhelming volume of vulnerabilities. Well over 230,000 vulnerabilities are listed in the US National Vulnerability Database (NVD).[6] While only a small percentage are tied to ransomware, and an even smaller percentage are active exploits, identifying which ones pose the most risk to your organization can be tricky.



Ivanti Neurons for Patch Management provides actionable threat intelligence, patch reliability insight and device risk visibility across Windows, MacOS, Linux and third-party applications. These key insights enable IT teams to prioritize and remediate the vulnerabilities that most endanger their organization. By leveraging Ivanti Neurons for Patch Management to increase the efficiency and effectiveness of their patching efforts, organizations can better protect themselves from data breaches, ransomware and other threats that stem from software vulnerabilities.

Key features and capabilities

Risk-based prioritization

Ivanti Neurons for Patch Management uses a risk-based prioritization strategy to target patches that address critical vulnerabilities first – especially those related to ransomware. By focusing on patches that mitigate the highest risks, IT teams can efficiently allocate resources to other strategic priorities, streamline the patch management process and enhance security effectiveness. This approach promptly addresses severe vulnerabilities, significantly reducing the risk of ransomware and other security breaches – and thereby maintaining a robust defense in a complex threat environment.

Active threat context

Enhance your IT security by prioritizing critical vulnerabilities with an advanced Vulnerability Risk Rating (VRR) system. This rating surpasses traditional CVSS scores by including real-world risk evaluations. Our VRR system ranks patches using detailed insights into adversarial risks, such as intelligence on exploits and ransomware-related vulnerabilities. Strengthened by high-quality data and expert validation from penetration testing teams, the VRR system directs remediation efforts effectively, significantly boosting your defenses against active and potential threats.

Deploy by risk

As vulnerabilities increase, vendors consistently release updates to address them. This is crucial for mitigating risks, particularly with zero-day exploits or public disclosures. However, aligning these continuous updates with organizations' typical monthly maintenance schedules is challenging – leaving security gaps for weeks.

The Deploy by Risk feature supports multiple parallel deployment tasks: monthly regular maintenance, weekly priority updates and immediate zero-day patches. This enables automatic update management that keeps systems current with the latest patches regardless of release timing.

> "63% of IT and Security professionals report that siloed data slows security response times."[7]

Ring Deployment

Ring deployment is an out-of-the-box solution for managing software rollouts with precision and control, making your operations more resilient and reducing downtime. Creating deployment rings lets you group devices strategically based on your organizational needs and risk tolerance. With options for both automated and manual patch promotion, you can thoroughly test and validate patches in smaller groups before broader distribution, getting critical updates adopted quickly while minimizing risk. Comprehensive ring status views give you real-time insights into deployment progress for predictability and proactive issue resolution. This phased approach lets you confidently manage patch cycles, improve compliance, safeguard systems against vulnerabilities and maintain productivity across the organization.

From on-premises to cloud

Start your journey from on-prem patch management to the cloud with Ivanti Neurons for Patch Management. Our cloud-native solution lets you transition 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 with on-prem Ivanti patch management solutions.

Patch reliability

Patch reliability is crucial for system integrity and security. Ivanti leverages crowdsourced sentiment, anonymized deployment data and advanced testing to assess patch effectiveness and safety before deployment. The Ivanti Neurons Agent autonomously configures and distributes tested patches to thousands of devices quickly, identifying potential issues early. IT teams can make informed patching decisions, minimizing the risk of faults and enhancing IT environment stability and performance. This method reduces downtime and ensures continuous protection against vulnerabilities.

Heterogenous on one platform

A heterogeneous platform is crucial for upholding strong security standards across diverse IT environments, allowing for efficient and proactive IT security risk management. Ivanti Neurons for Patch Management supports Windows, MacOS, Linux and third-party applications with a unified management experience that simplifies oversight of various systems and boosts productivity.

Using a single platform provides consistent security policies and boosts operational efficiency without switching between different patch management systems. It reduces complexity and the risk of oversight, ensuring comprehensive protection and visibility across all endpoints. By quickly identifying vulnerabilities and inconsistencies, this comprehensive approach prevents breaches, reduces downtime and recovery costs and safeguards organizational assets.

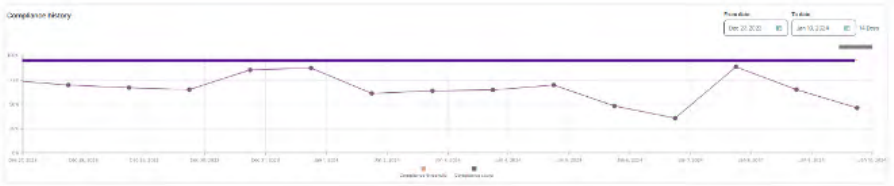
Compliance reporting

Compliance reporting in patch management is crucial. Ivanti’s automated system focuses on risk-based KPIs that reflect real-world risks. It ensures all patches are documented and meet regulatory standards, greatly reducing non-compliance. The system aligns patch management with security needs by basing SLAs on the update’s release date rather than typical IT operational timelines. This is crucial as security teams face challenges with continuous patch cycles. By recalibrating SLAs from a vulnerability exposure standpoint, IT departments can better meet security requirements while managing operational demands – strengthening the organization’s overall security framework.

Changing How We Measure: “Exposure Time”

Chasing the numbers:

Updates release continuously. It is nearly impossible to achieve compliance.



Measure what matters:

A risk-based KPI allows teams to focus on real-world risk and achieve compliance.

Breaking down barriers between IT and Security

Create parity across IT and Security teams by offering equal access to crucial information such as SLA tracking and risk-based intelligence. This fosters a comprehensive view and a common language that promotes quick and effective cross-functional actions. A unified approach reduces friction and enables coordinated responses to stakeholders. Sharing insights on patch reliability, derived from crowdsourced data and deployment telemetry, allows for proactive evaluations and prevents failed deployments to ensure compliance with SLAs. This strategy improves coordination and strengthens the organization's security posture.

About Ivanti

Ivanti breaks down barriers between IT and security so that Everywhere Work can thrive. Ivanti has created the first purpose-built technology platform for CIOs and CISOs – giving IT and security teams comprehensive software solutions that scale with their organizations' needs to enable, secure and elevate employees' experiences. The Ivanti platform is powered by Ivanti Neurons - a cloud-scale, intelligent hyper automation layer that enables proactive healing, user-friendly security across the organization, and provides an employee experience that delights users. Over 40,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com and follow @GoIvanti.

ivanti neurons

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

1. IBM, "Cost of a Data Breach Report 2024," 2024. https://www.ibm.com/reports/data-breach
2. Verizon, "2024 Data Breach Investigations Report," 2024. https://www.verizon.com/business/resources/reports/dbir/
3. Google, "A Year in Review of Zero-Days Exploited In-the-Wild in 2023," March 2024. https://cloud.google.com/blog/topics/threat-intelligence/2023-zero-day-trends
4. Richard Fang, Rohan Bindu, Akul Gupta, Qiusi Zhan, Daniel Kang, "Teams of LLM Agents can Exploit Zero-Day Vulnerabilities," 2 June 2024. https://arxiv.org/abs/2406.01637.
5. Ivanti, "Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace," 7 October 2021. https://www.ivanti.com/resources/v/doc/ivi/2634/712cff539c8a.
6. Securin, "Ransomware Report 2023 Year in Review," 2024. https://www.securin.io/ransomware-report-2023-year-in-review-download/.
7. Ivanti, "2024 State of Cybersecurity Report," 2024. https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report