Risk-Based Vulnerability & Patch Management from Ivanti

Overwhelming volumes of vulnerabilities. Inadequate information that misrepresents vulnerability risk. Time-consuming, error-prone manual processes. Friction between IT and security teams that delays — or blocks — remediation efforts.

These are the hallmarks of legacy vulnerability management — an approach that leaves organizations highly exposed to attacks, despite their best efforts. All the while, the most critical vulnerabilities remain unaddressed.

Overcome these issues with Ivanti's risk-based vulnerability and patch management solution, which empowers you to manage cybersecurity risk more efficiently and effectively.

Implement risk-based prioritization

Organizations are drowning in vulnerabilities. Separating those that need to be remediated from those that can be ignored is effectively impossible using most popular prioritization methods. Not only do these methods miscalculate the risk associated with many vulnerabilities, they represent just one step of an often prolonged vulnerability management process.

Move from detection of vulnerabilities and weaknesses to remediation in minutes — not months — with a contextualized, risk-based view of your cybersecurity posture. Ivanti's risk-based vulnerability and patch management solution continuously correlates an organization's infrastructure with internal and external vulnerability data, threat intelligence, manual pen test and research-based findings, and business asset criticality to measure risk and prioritize remediation activities accordingly.

74%

Percentage of ransomware vulnerabilities not rated Critical under CVSS v3.[1]

Unlike the Common Vulnerability Scoring System (CVSS), Ivanti's proprietary scoring algorithm accounts for active threat context when assigning a risk rating to a vulnerability. Our solution also specifically identifies remote code execution, privilege escalation and ransomware vulnerabilities, and vulnerabilities that are trending and active. This information helps organizations focus on vulnerabilities that pose the most credible, high-impact risks.

Streamline your vulnerability management processes

53%

Percentage of IT and security professionals that say organizing and prioritizing vulnerabilities takes up most of their time.[2]

Legacy vulnerability management is a never-ending process that entails vulnerability scanning, data gathering, result interpretation, prioritizing, patching and reporting. Many of these steps involve manual tasks that introduce human error into the process, causing critical vulnerabilities to fall through the cracks. These labor-intensive, time-consuming tasks also delay the patching of vulnerabilities that do get identified and prioritized.

Eliminate vulnerability management mistakes and reduce mean time to remediation with these advanced capabilities:

- Quickly arrive at a fully informed plan of attack with continuous correlation and analysis of security data.
- Automate common or repetitive tasks with playbooks.
- Set vulnerability closure due dates automatically with service-level agreement automation.
- Gain near-real-time awareness of pertinent events with automated notifications.
- Pass CVEs from security to IT via an API — not email or chat — and map them to available patches automatically.
- Distribute thoroughly tested patches to thousands of machines in minutes with autonomous patch configurations.

Foster collaboration between IT and security stakeholders

Lack of cooperation between teams

#1 challenge in defending against cyberattacks per security and IT decision makers.[3]

In vulnerability management, the security team determines the risks to the business. Their decisions influence what needs to be patched and by when. Meanwhile, the IT team — which conducts the patching — is responsible for keeping the organization's systems online. When these objectives conflict, negotiations between the teams can impede patching and leave the organization at risk of attack.

Bridge the gap between IT and security to ensure timely resolution of vulnerabilities by arming both sides with the same visibility and intelligence. With Ivanti's risk-based vulnerability and patch management solution, patch admins have access to the same risk ratings, vulnerability intelligence and dashboards as the security team. This ensures everyone is on the same page about prioritization decisions.

Available patch reliability insights indicate when a patch is prone to fail and cause downtime in real-world environments. These insights let IT and security alike know when a temporary mitigation may be required until a vulnerability can be remediated with a reliable patch.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Cyber Security Works, Cyware, Ivanti, Securin. (2023). *2023 Spotlight Report – Ransomware Through the Lens of Threat and Vulnerability Management.* https://cybersecurityworks.com/ransomware/
2. Ivanti. (2021). *Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace.* https://www.ivanti.com/resources/v/doc/ivi/2634/712cff539c8a
3. ExtraHop. (2022). *Cyber Confidence Index 2022.* https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/