Ivanti Neurons for Patch Intelligence

Risk-based vulnerability management protects your organization from security threats and evolving risks by reducing time to patch and prioritizing the most critical patches for deployment. Sixty percent of breaches involve vulnerabilities where a patch was available but not applied.[1]

Ivanti Neurons for Patch Intelligence helps you prioritize vulnerabilities based on active risk exposure, reliability and compliance.

Focus on what matters

Understand your adversarial risk with Vulnerability Risk Rating (VRR), treat-context for exploits and malware insights from RiskSense. There are numerous application security and vulnerability assessment tools to choose from with overlapping insights. RiskSense VRR provides a common, threat-based prioritization that is capable of looking across all assets, scanner type and vendor. RiskSense VRR is designed to decipher cybersecurity risk from the widest angle possible, using an algorithm that intelligently separates and elevates the riskiest weaknesses, taking in the highest fidelity vulnerability and threat data, and human validation of exploits from penetration testing teams.[2]

Understand known exploits and malware risk per CVE with the Ivanti Neurons for Patch Intelligence RiskSense integration. Insight into denial of service, privilege escalation, remote code execution, web application, ransomware and exploit kit vulnerabilities support the risk-based prioritization of the greatest risks in your environment.

Reduce time to patch

Achieve faster SLAs with patch reliability and trending insight to focus testing efforts and reduce time to patch. Continuous assessment via supervised and unsupervised machine learning provides real-time intelligence on vulnerability exploits that are actively trending. Reduce your research efforts with crowdsourced insight from a variety of sources, Ivanti Neurons for Patch Intelligence provides reliability insight in one centralized view.

Understand compliance

Only 40% of organizations have cybersecurity compliance practices to track vulnerabilities.[3] Ivanti Neurons for Patch Intelligence identifies non-compliant systems with feature-rich compliance reporting. Take risk-based prioritized patch action with visibility into the out-of-compliance machines in your environment.

Focus on what matters		Reduce time to patch		Understand Compliance	
Feature	**Capabilities**	**Feature**	**Capabilities**	**Feature**	**Capabilities**
RiskSense VRR Group and VRR Group	• Vulnerability Risk Rating (VRR) categories: - Critical: 10-9 - High: 8-7 - Medium: 6-4 - Low: 3-1 - Info: 0 • A 0-10 scale where higher is more severe, just like CVSS. • Factors not only the scanner reported severity, but weaponized associations and whether the RiskSense penetration testing team has demonstrated exploitation of the flaw or weakness during one of the hundreds of real-world assessments they have completed.	Reliability	• Helps to determine the stability of the patch. • Patch Intelligence gathers data from a variety of sources to provide a confidence score for updates to supplement your patch testing efforts. • Derived from the number of successful and failed installs, with other stability metrics, such as reported issues from vendors or users.	Compliance Reporting	• Devices Exceeding SLA chart allows you to easily see how many devices within your environment are nearing or exceeding your service level agreement (SLA) and the percentage of devices that are compliant, and not. • Configurable SLA report allows you to define the security severity and number of days for the SLA limit. Define an SLA threshold for when you would like to be warned that an endpoint is nearing your SLA limit.
Exploits and Malware Threat Context	• Exploits - Denial of Service - Privilege Escalation - Remote Code Execution - Web Application • Malware - Ransomware - Exploit Kit	Trending	• Indicates the level of social media attention a patch is receiving. • The content of the posts could be negative i.e. problems with installing, or positive i.e. fixes issued for any problems.		

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

ivanti neurons

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

[1] csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
[2] www.risksense.com/wp-content/uploads/2020/08/1-Pager-RiskSense-VRR.pdf
[3] www.comptia.org/content/research/cybersecurity-trends-research