

# Ivanti Neurons for Patch Management

## Efficiently prioritize and remediate vulnerabilities

Ivanti Neurons for Patch Management is a cloud-native patch management solution with actionable intelligence on active risk exposure, patch reliability and device compliance, health and risk that helps organizations better protect against threats, including ransomware.

### Risk-based patch management

Ransomware attacks are increasing in frequency and severity every year. The impact on companies is devastating. Research puts the average total cost of a ransomware breach at \$4.62 million – excluding the cost of the ransom.<sup>1</sup>

Unfortunately, the situation is likely to get worse before it gets better. Ransomware as a service (RaaS) enables just about anyone to launch an attack – no security knowledge or coding expertise required. On top of that, the number of Common Vulnerabilities and Exposures (CVEs) into networks nearly quadrupled in 2020.<sup>2</sup> Worse yet, ransomware attackers are increasingly targeting midmarket companies to avoid the media attention that comes from attacking large enterprises.<sup>3</sup>

Patching to fix CVEs is one of the best things an organization can do to counter ransomware attacks. Unfortunately, 71% of IT and security professionals



find patching to be overly complex and time-consuming.<sup>4</sup> That may be due to the overwhelming volume of vulnerabilities that exist. There are well over 100,000 vulnerabilities listed in the US National Vulnerability Database (NVD). 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. From 2018-2020, using CVSS v3 scoring, if you were to patch only critical vulnerabilities, your coverage against ransomware would only be about 35%.<sup>2</sup>

Ivanti Neurons for Patch Management provides actionable threat intelligence, patch reliability insight and device risk visibility that enables IT teams to prioritize and remediate the vulnerabilities that pose the most danger to 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

### Proactively patch against active exploits

Prioritize remediation based on adversarial risk, with intelligence on known exploits and threat-context for vulnerabilities – including ties to ransomware. Ivanti's Vulnerability Risk Rating (VRR) better arms you to take risk-based prioritized action than CVSS scoring by taking in the highest fidelity vulnerability and threat data plus human validation of exploits from penetration testing teams.

### Achieve faster SLAs with patch reliability and trending insight

Save time and avoid failed patch deployments with patch reliability insights from crowdsourced social sentiment data and anonymized patch deployment telemetry. This information enables you to evaluate patches based on their reliability in real-world applications before deploying them. Additionally, service-level agreement (SLA) tracking, which provides visibility into devices nearing SLA, enables you to take action on devices before they are out of compliance.

### Transition from on-premises to cloud patch management

Start your journey from on-prem patch management to the cloud with the strength of Ivanti's patch technology. Ivanti Neurons for Patch Management is a cloud-native solution that allows you to transition from on-prem patch management to the cloud at your own pace instead of being forced to "rip and replace". Such gradual transitions are enabled by the solution's single pane of glass experience that provides visibility into the devices that it manages in the cloud alongside those managed via on-prem Ivanti patch management solutions.

### Streamline patch management processes

Improve operational efficiencies by eliminating the need to jump between siloed patch management solutions. Ivanti Neurons for Patch Management provides visibility into all the endpoints in your environment via a single pane of glass. Advanced vulnerability insights and patch intelligence further improve operational efficiencies by enabling you to effectively prioritize patch efforts so you focus only on what matters. Further, when it's time to patch, autonomous Patch Configurations deployed to the Ivanti Neurons Agent on devices distribute thoroughly tested patches to thousands of machines in minutes.

## 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 96 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](https://www.ivanti.com)



[ivanti.com/neurons](https://www.ivanti.com/neurons)

1 800 982 2130

[sales@ivanti.com](mailto:sales@ivanti.com)

1. IBM Security, "2021 Cost of a Data Breach Report", 28 July 2021. <https://www.ibm.com/downloads/cas/OJDVQGRY>
2. RiskSense, Cyber Security Works, "Ransomware Through the Lens of Threat and Vulnerability Management", 9 November 2021. [https://www.ivanti.com/resources/v/doc/white-papers/spotlight\\_ransomware2021\\_risksensecsw](https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw)
3. Coveware, "Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021", 21 October 2021. <https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>
4. Ivanti, "Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace", 7 October 2021. <https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges>