Ivanti Neurons for RBVM

Prioritize vulnerabilities based on true risk and streamline your response

It can take as long as 231 days—over 7.5 months—to identify a cybersecurity breach.[1] Those breaches are costly too: A single one averages $2.6 million for the public sector.[2] With so much at stake, adhering to mandates like Executive Order 14028[3] on Improving the Nation's Cybersecurity is critical to keeping our nation's data safe.

The complex tech stacks commonly used to manage risk within the public sector can be a drain on costs, setup timeframes and security training timelines. These tech stacks are also the most commonly reported barrier to global cybersecurity excellence[4] within government. They can make parsing through vulnerability data more difficult as it passes between platforms. Agencies need to be able to identify critical risks without overcompensating or adding extra burden onto security teams.

Evolve your vulnerability management strategy to a risk-based approach with Ivanti Neurons for Risk-Based Vulnerability Management (RBVM). This software-as-a-service (SaaS) offering enables you to efficiently and effectively prioritize the vulnerabilities and weaknesses that pose the most risk for remediation and better protect your agency against data breaches, ransomware and other cyber threats.

Time for a new approach to vulnerability management

There are over 294,000 known vulnerabilities[5], and government consistently ranks third among the most targeted industries for cybersecurity threats[6]. Fortunately, agencies don't need to remediate every vulnerability and weakness that appears in your organization's IT environment. However, identifying the rare vulnerability or weakness that poses a significant risk is a time-consuming, error-prone process if you're using more traditional approaches to vulnerability management.

Before your organization can even begin prioritizing vulnerabilities and weaknesses for remediation, you must first gather a range of disparate data—from scanner findings to threat intelligence—then normalize that data and prepare it for use. When done manually, these processes can take days, weeks or months to complete. And there's always a high probability of human error in any manual process. Couple that with a lack of cybersecurity personnel in the public sector, and you have a recipe for overworked security teams and overlooked vulnerabilities[7].

The prioritization process is no better. Consider ransomware vulnerabilities: 74% aren't rated Critical under CVSS v3, and 156 are missing from the CISA Known Exploited Vulnerabilities (KEV) catalog. Additionally, three highly popular scanners still haven't added plugins and detection signatures for a combined 20 ransomware vulnerabilities.

On top of that, security and IT decision-makers actually cite the lack of cooperation between their teams as the top challenge they face in defending against cyberattacks.[8] This friction between vulnerability management stakeholders can slow remediation and leave organizations prone to attack.

Key capabilities

Prioritize immediate actions based on threat risk
Move from detection of vulnerabilities and weaknesses to remediation in minutes—not months—with a contextualized, risk-based view of your organization's cybersecurity posture. Ivanti Neurons for RBVM measures risk and prioritizes remediation activities through a process that involves continuous correlation of an organization's infrastructure with:

- Internal and external vulnerability data
- Threat intelligence
- Manual pen test and research-based findings
- Asset criticality

Unlike CVSS, Ivanti's proprietary Vulnerability Risk Rating (VRR) lets organizations calculate the impact and determine the likelihood that a vulnerability will be exploited. Ivanti Neurons for RBVM also identifies remote code execution, privilege escalation, ransomware, and trending and active vulnerabilities. This information helps agencies focus on vulnerabilities that pose the most risk.

With Ivanti Neurons for RBVM, you get a fully informed plan of attack with little to no friction or manual effort.

Focus on remediation, not administration

Improve your cybersecurity posture through a range of automations and other efficiency-enhancing features:

- Create playbooks to automate common or repetitive tasks handled manually by security analysts
- Automate vulnerability closure due dates that align with your agency's service-level agreements
- Receive near real-time alerts outside the product that link back to a product page containing information related to the subscribed event
- Easily filter hosts and host findings by trending criteria that reveal their exposure to the top critical vulnerabilities—like ransomware and trending Common Vulnerabilities and Exposures (CVE)—using system views pushed by the Ivanti security team
- Deliver prioritized vulnerabilities directly to Ivanti Neurons for Patch Management for remediation—no more sending CSV files of CVE IDs via email and chat

Enable better collaboration among security stakeholders

Cultivate communication and cooperation among security stakeholders from across the organization by providing them with timely and relevant information. Ivanti Neurons for RBVM employs role-based access control (RBAC) so product access can be provided safely to all applicable staff.

With Ivanti Neurons for RBVM, users have access to dashboards designed for everyone from the SOC to the CISO and department heads. They can modify these dashboards to fit more specific use cases or even leverage user widgets to create custom dashboards that meet the exact needs of different roles and teams.

Additionally, the solution quantifies an organization's risk profile with an Ivanti RS3 score. This score ensures all IT and security stakeholders are in alignment with the organization's overall security level. Bidirectional integrations with ticketing systems, such as Ivanti Neurons for ITSM, improve coordination between those working to improve that security level.

Features & functions

Feature	Function
Diverse data sources	Achieve a wide view of cyber risk with a product that ingests data from network scanners, endpoints, databases and the Internet of Things (IoT) devices, vulnerability findings from 100+ sources, manual findings from research and pen testing teams, and custom data sources.
Threat engine	Gain unparalleled insights on vulnerabilities—like those that are tied to ransomware—via human-generated and AI-driven threat intelligence sourced from Ivanti Neurons for Vulnerability Knowledge Base.
Vulnerability Risk Rating (VRR)	Quickly determine the risk posed by a vulnerability with numerical risk scores that consider the intrinsic attributes of the vulnerability, plus its real-world threat context.
Ivanti RS^3	Attain a quantified view of your organization's risk profile via a proprietary scoring methodology that considers VRR, asset criticality, threat intelligence and external accessibility.
Automation	Replace a range of manual tasks with automation so staff can focus on remediation actions and strategic initiatives rather than administration.
Alerts and notifications	Gain instant awareness of pertinent events via near real-time alerts sent from a notification engine for faster risk mitigation. Use deep links to direct other users to important information within the product.
Customizable data organization	Uncover actionable insights with user widgets that allow for the creation of custom dashboards, plus the ability to pivot data in list views.
Dashboards	Dashboards are fully customizable, allowing users to create and share custom views. These dashboard views provide an opportunity to quickly discover top vulnerabilities and identify how they might manifest in a specific environment.
Threat-based views	Discover how specific threats like BlueKeep, WannaCry or the FBI/DHS/CISA top 10 exploited vulnerabilities manifest themselves in your organization's environment by utilizing threat-based filters. Also, create and share your own custom filters.
Integrations	Leverage integrations with Ivanti Neurons for ITSM and Ivanti Neurons for Patch Management to empower vulnerability management practitioners throughout the organization to perform their tasks more efficiently and effectively.

It's more important than ever for public sector security teams to have the tools they need to achieve a strong cybersecurity posture. With Ivanti Neurons for RBVM, agencies can identify, prioritize and manage critical risks without overcompensating or adding an extra burden onto security teams. Put the focus on remediation and enable better collaboration among security and IT stakeholders with Ivanti Neurons for RBVM.

About Ivanti

Ivanti elevates and secures Everywhere Work so that 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 one of the only technology companies that finds, manages and protects each 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 are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit www.ivanti.com and follow @GoIvanti.

ivanti

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

1. Ivanti: "Ivanti for the Department of Defense: Preserve National Security with Ivanti." 2022. https://www.ivanti.com/resources/v/doc/ivi/2693/267003ec9fdf
2. IBM Security: "Cost of a Data Breach Report 2023." July 2023. https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258
3. The White House Briefing Room, Presidential Actions: "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
4. Ivanti: "Government Cybersecurity Status Report: 4 Important Ways to Take Action and Drive Change in 2023." 2023. https://rs.ivanti.com/ivi/2747/a856c631661d.pdf
5. Data pulled from Ivanti Neurons for Vulnerability Knowledge Base on November 30, 2023.
6. Ivanti: "Ivanti for the Department of Defense: Preserve National Security with Ivanti." 2022. https://www.ivanti.com/resources/v/doc/ivi/2693/267003ec9fdf
7. Cyber Security Works, Cyware, Ivanti, Securin, "2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management", 16 February 2023. https://www.securin.io/ransomware/
8. ExtraHop, "Cyber Confidence Index 2022", 1 March 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/