Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)

Improve cybersecurity posture with true risk-based vulnerability management and prioritization

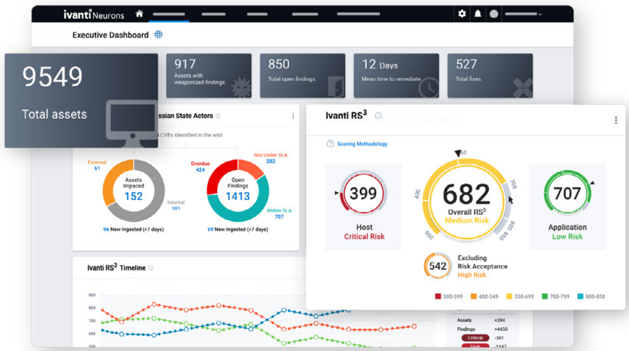
Evolve your vulnerability management strategy to a risk-based approach with Ivanti Neurons for RBVM. This SaaS offering enables you to efficiently and effectively prioritize the vulnerabilities and weaknesses that pose you the most risk for remediation to better protect against data breaches, ransomware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

Time for a new approach to vulnerability management

There are over 270,000 known vulnerabilities.[1] Fortunately, organizations don't need to remediate every vulnerability and weakness that appears in their IT environments. Unfortunately, identifying the rare vulnerability or weakness that poses them significant risk is a time-consuming, error-prone process for organizations using traditional approaches to vulnerability management.

Before such organizations can even begin prioritizing vulnerabilities and weaknesses for remediation, they must first gather a range of disparate data — from scanner findings to threat intelligence — normalize that data and prepare it for use. When done manually, these processes can take days, weeks or months to complete, and always involve human error.

The prioritization process is no better. Consider ransomware vulnerabilities. Seventy-four percent 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.[2]



On top of all 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.[3] This friction between vulnerability management stakeholders can slow remediation and leave the organization prone to attack.

Introducing Ivanti Neurons for RBVM

Measure and control your true cybersecurity risk to better protect against cyber threats like data breaches and ransomware with the capabilities found in Ivanti Neurons for RBVM. These capabilities come packaged in a single interface so you can phase out the 'swivel chair' approach that's defined vulnerability management practices of the past.

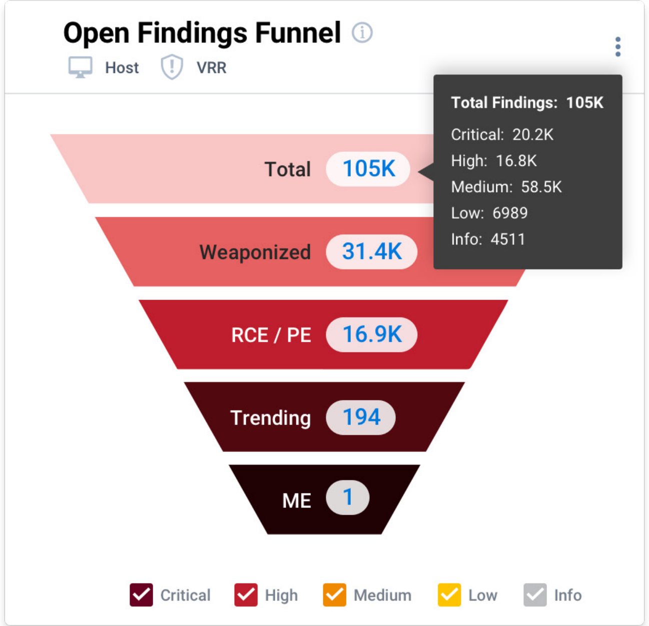
Key capabilities

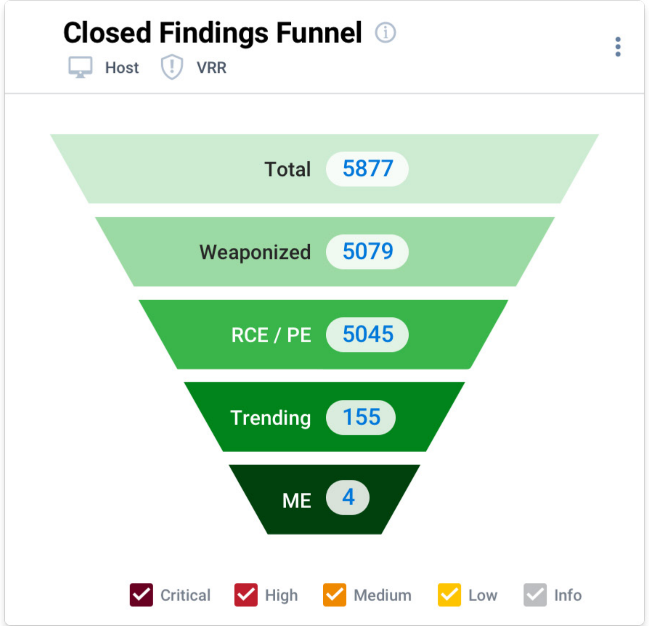
Prioritize immediate actions based on threat risk

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.
- Business asset criticality.

Best of all: you arrive at a fully informed plan of attack with little to no manual effort required.



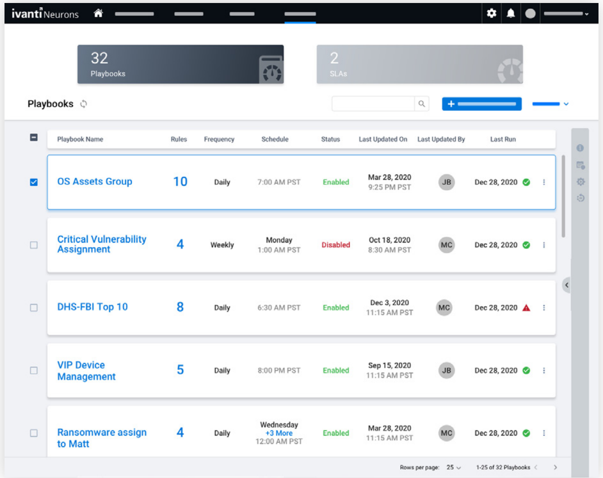


Further, unlike CVSS, Ivanti's proprietary Vulnerability Risk Rating (VRR) lets organizations accurately measure impact and determine the likelihood a vulnerability will be exploited. Ivanti Neurons for RBVM also specifically identifies remote code execution, privilege escalation, ransomware, and trending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

Focus on remediation, not administration

Improve your cybersecurity posture without all the time, effort and errors traditionally associated with doing so through a range of automations and other efficiency-enhancing features:

- Create playbooks to automate common or repetitive tasks traditionally handled by security analysts.
- Set vulnerability closure due dates automatically if desired with service-level agreement automations.
- 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 CVEs — using system views pushed by the Ivanti security team.
- Deliver prioritized vulnerabilities directly to Ivanti Neurons for Patch Management for remediation — no more sending CSVs of CVE IDs via email and chat.



☐	Playbook Name	Rules	Frequency	Schedule	Status	Last Updated On	Last Updated By	Last Run
☑	OS Assets Group	10	Daily	7:00 AM PST	Enabled	Mar 28, 2020 9:25 PM PST	JB	Dec 28, 2020 ✓
☐	Critical Vulnerability Assignment	4	Weekly	Monday 1:00 AM PST	Disabled	Oct 18, 2020 8:30 AM PST	MC	Dec 28, 2020 ✓
☐	DHS-FBI Top 10	8	Daily	6:30 AM PST	Enabled	Dec 3, 2020 11:15 AM PST	MC	Dec 28, 2020 ⚠
☐	VIP Device Management	5	Daily	8:00 PM PST	Enabled	Sep 15, 2020 11:15 AM PST	JB	Dec 28, 2020 ✓
☐	Ransomware assign to Matt	4	Daily	Wednesday +3 More 12:00 AM PST	Enabled	Mar 28, 2020 11:15 AM PST	MC	Dec 28, 2020 ✓

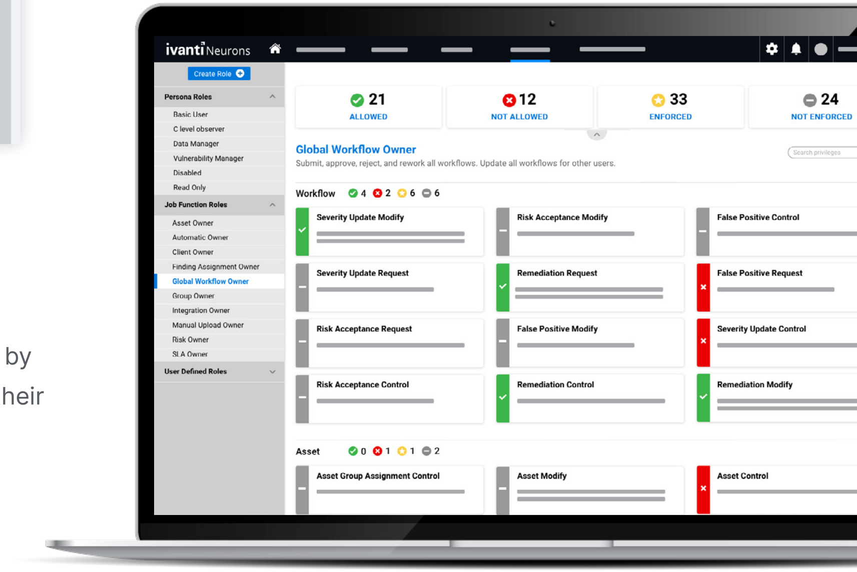
Rows per page: 25 1-25 of 32 Playbooks

Enable better collaboration amongst security stakeholders

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

Once inside the product, users have access to dashboards designed for personnel from the SOC to the C-suite. 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 product quantifies an organization's risk profile in the form of an Ivanti RS^3 score. This score ensures all security stakeholders are in alignment on the organization's overall security level. Bidirectional integrations with ticketing systems like Ivanti Neurons for ITSM improve coordination between those working to improve that security level.



Global Workflow Owner

Submit, approve, reject, and rework all workflows. Update all workflows for other users.

Workflow ✓ 4 ✗ 2 ★ 6 − 6

✓ Severity Update Modify
− Risk Acceptance Modify
− False Positive Control
− Severity Update Request
✓ Remediation Request
✗ False Positive Request
− Risk Acceptance Request
− False Positive Modify
✗ Severity Update Control
− Risk Acceptance Control
✓ Remediation Control
✓ Remediation Modify

Asset ✓ 0 ✗ 1 ★ 1 − 2

− Asset Group Assignment Control
− Asset Modify
✗ Asset Control

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 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 which 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 business criticality, threat intelligence and external accessibility.
Automation	Replace a range of manual tasks with automation so employees 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. Similarly, direct other users to important information within the product using deep links.
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	Quickly discover how top critical vulnerabilities — like Log4j and those associated with Patch Tuesday releases — manifest themselves in your environment by utilizing threat-based views. Also create and share your own custom views.
Threat-based views	Quickly 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.
Neurons integrations	Pair Ivanti Neurons for RBVM with Ivanti Neurons for ASOC to extend risk-based vulnerability management across a greater area of your attack surface. Leverage out-of-the-box 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.

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 we 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. Data pulled from Ivanti Neurons for Vulnerability Knowledge Base on June 29, 2023
2. 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/
3. ExtraHop, "Cyber Confidence Index 2022", 1 March 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/