ivanti

# Ivanti Neurons for Risk-Based Vulnerability Management

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

**Ivanti Neurons for Risk-Based Vulnerability Management helps organizations evolve their vulnerability management strategy to a risk-based approach. This SaaS solution enables organizations to prioritize the vulnerabilities that pose them the most risk so they can better protect against data breaches, ransomware and other cyber threats.**

## Time for a new approach to vulnerability management

Over three-quarters of businesses have been impacted by an IT security vulnerability over the past year.[1] That comes as no surprise at a time when the National Vulnerability Database (NVD) currently contains over 134,000 vulnerabilities, and 61 more are added every day.[2]

The good news is that organizations do not need to remediate every vulnerability and weakness. In fact, only 4% of all Common Vulnerabilities and Exposures (CVEs) have been publicly exploited.[3] The bad news is that identifying the select vulnerabilities and weaknesses that pose them significant risk is difficult for organizations relying on traditional approaches to vulnerability prioritization.

For example, patching only critical vulnerabilities based on the Common Vulnerability Scoring System (CVSS) v3 would cause an organization to miss out on patching 73.61% of ransomware vulnerabilities.[2] That represents a major gap for the 71% of security and IT decision makers that use the CVSS to score and prioritize vulnerabilities[4] – especially at a time when the average cost of a ransomware attack has reached over $4.6M.[5]

Further complicating matters is the fact that organizations usually cannot begin prioritizing vulnerabilities and weaknesses for remediation until after data has been gathered from a range of disparate sources – from internal scanners to external threat intelligence sources – normalized and prepared for use. These processes are often conducted manually and can take weeks to complete. It's no wonder 53% of security and IT professionals spend most of their time organizing and prioritizing vulnerabilities.[6]

As if the situation were not already difficult enough, security and IT decision makers actually cite the lack of cooperation between their network, security and cloud operations teams as the top challenge they face as they attempt to defend against cyberattacks.[7] Communication and collaboration between security stakeholders across all parts of the organization often suffers due to a lack of relevant and timely reporting.

## Introducing Ivanti Neurons for RBVM

Ivanti Neurons for Risk-Based Vulnerability Management (RBVM) helps organizations measure and control their true cybersecurity risk so they can better protect against data breaches, ransomware and other cyber threats. Ivanti's proprietary Vulnerability Risk Rating (VRR) quantifies adversarial risk so customers can take risk-based prioritized action. A range of automations increase the efficiency and effectiveness of vulnerability management processes. Additionally, role-based access control (RBAC) plus information available in both ready-made and customizable views enable better communication and collaboration among security stakeholders.
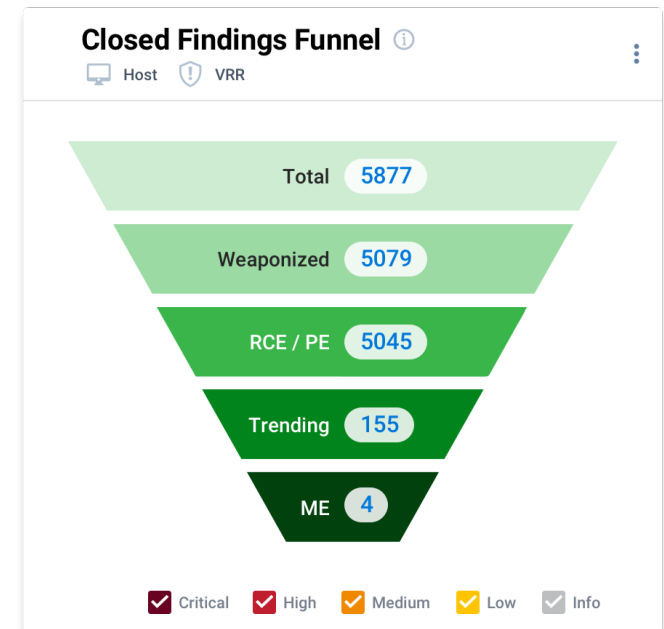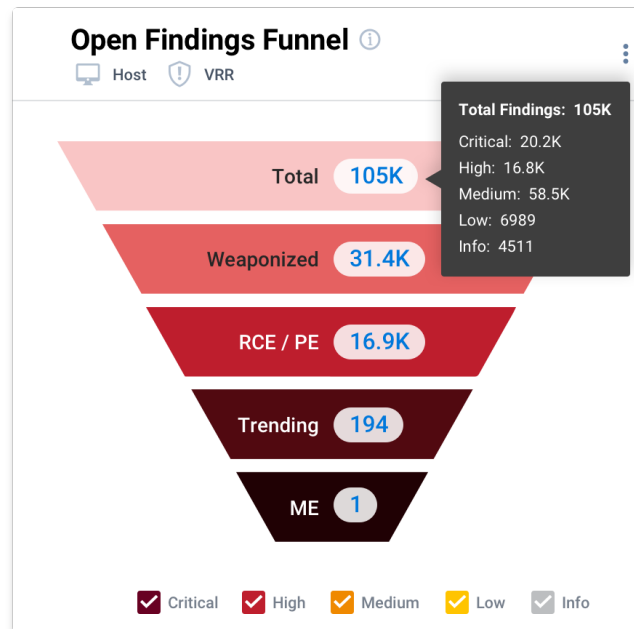
# Key capabilities

## 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 continuously correlates an organization's infrastructure with comprehensive internal and external vulnerability data, threat intelligence, human pen test findings and business asset criticality to measure risk, provide early warning of weaponization, predict attacks and prioritize remediation activities.

Unlike CVSS, the platform's proprietary VRR scoring enables organizations to accurately measure impact and determine the likelihood that a vulnerability will be exploited. Ivanti Neurons for RBVM also specifically identifies remote code execution (RCE) and privilege escalation (PE) vulnerabilities, vulnerabilities with ties to ransomware, and vulnerabilities that are trending and active. This information helps organizations focus on those vulnerabilities that pose them the most risk.

### Open Findings Funnel ⓘ

🖥 Host   ⚠ VRR                                    ⋮

| | |
|---|---|
| Total | 105K |
| Weaponized | 31.4K |
| RCE / PE | 16.9K |
| Trending | 194 |
| ME | 1 |

**Total Findings: 105K**
Critical: 20.2K
High: 16.8K
Medium: 58.5K
Low: 6989
Info: 4511

☑ Critical   ☑ High   ☑ Medium   ☑ Low   ☐ Info

### Closed Findings Funnel ⓘ

🖥 Host   ⚠ VRR                                    ⋮

| | |
|---|---|
| Total | 5877 |
| Weaponized | 5079 |
| RCE / PE | 5045 |
| Trending | 155 |
| ME | 4 |

☑ Critical   ☑ High   ☑ Medium   ☑ Low   ☐ Info

## Improve the efficiency of vulnerability management processes

Ivanti Neurons for RBVM helps you increase your cybersecurity posture while decreasing the time and effort required to do so:

- The platform continuously correlates and analyzes comprehensive internal and external vulnerability data, threat intelligence, human pen test findings and business asset criticality to help users arrive at a fully informed plan of attack – a process that typically takes weeks to conduct manually.
- Playbooks enable the automation of common or repetitive tasks so users can focus time and effort on remediation actions rather than administration.
- Service-level agreement (SLA) automations allow for vulnerability closure due dates to be set automatically.
- Automated, customizable notifications provide near-real-time alerts outside the platform that link users directly to a platform page containing information related to the subscribed event.
- System filters pushed by the Ivanti security team allow for easy filtering of hosts and host findings by trending criteria that reveal their exposure to the top critical vulnerabilities on a regular basis (e.g., ransomware, trending CVEs, FBI/DHS/CISA top 10 exploited vulnerabilities or cross-site scripting).
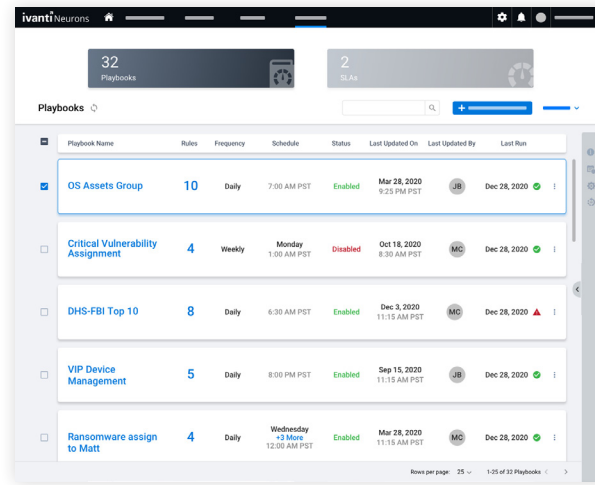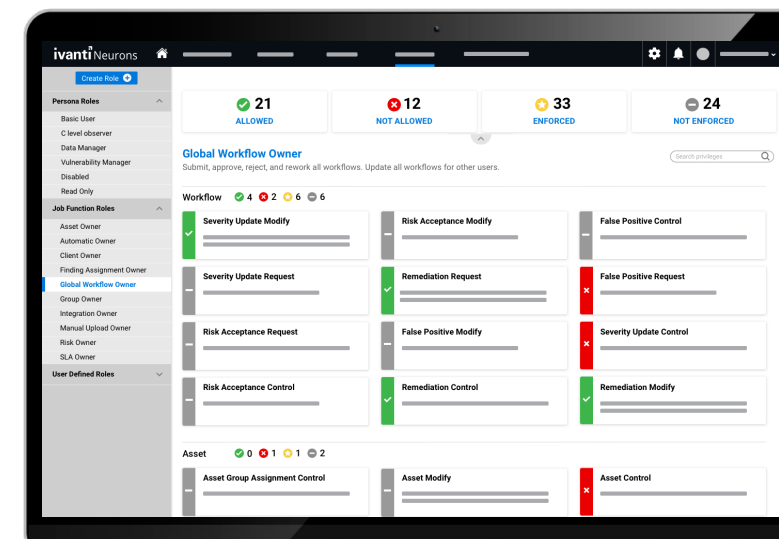


## Enable better collaboration amongst security stakeholders

Facilitate improved communication and cooperation among security stakeholders from across the organization – both those on the technical side and the business side – by providing them each with timely information relevant to their roles. Ivanti Neurons for RBVM employs RBAC to enable organizations to safely provide platform access to all applicable personnel.

Once inside the platform, users have access to a range of ready-made dashboards designed for different personas, from security practitioners to executives. These standard dashboards can also be modified to fit more specific use cases. Further, user widgets enable users to create fully customized dashboards that meet the exact needs of different roles and teams.

To further foster collaboration, Ivanti Neurons for RBVM allows users to create deep links to share their exact current view of a platform page with other users. This helps bridge communication gaps between siloed teams by enabling all teams to literally get on the same page. Users also possess the ability to share dashboards, export templates and filters.

Last but not least, the platform quantifies an organization's risk profile in the form of an Ivanti RS$^3$ score that ensures all security stakeholders are in alignment on the organization's overall security level. Bidirectional integrations with ticketing systems – including Ivanti Neurons for ITSM – improve coordination between stakeholders working to improve that security level by enabling them to maintain visibility throughout the remediation process without the additional burden of leaving their preferred system.

**ivanti**

# Features & functions

| Feature | Function |
|---|---|
| Diverse data sources | Achieve a wide view of cyber risk with a platform that ingests data from network scanners, endpoints, databases and IoT devices, vulnerability findings from over 100 independent 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, the business criticality of assets, numerous threat intelligence sources and external accessibility. |
| Automation | Eliminate a range of manual tasks with the platform's many automation capabilities 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 the platform's notification engine. Similarly, direct other users to important infor-mation within the platform by leveraging deep links. |
| Customizable data organization | Uncover actionable insights with user widgets that allow for the creation of highly customized dashboards and a group-by capability that permits the pivoting of data in list views. |
| Dashboards | Realize superior visual query and risk discovery capabilities across assets and infrastructure via ready-made and customizable dashboards with drill-down capabilities in every view. |
| Filters | 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. |

## 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.

## ivanti

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

1.  Vulcan Cyber, Pulse, "How Are Businesses Mitigating Cyber Risk?", 2021. https://l.vulcancyber.com/hubfs/Infographics/Pulse research project - 2021-07-23 - How are Businesses Mitigating Cyber Risk.pdf
2.  Cyber Security Works, Cyware, Ivanti, "2022 Ransomware Spotlight Report", 26 January 2022. https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report
3.  Cybersecurity and Infrastructure Security Agency (CISA), "Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities", 3 November 2021. https://cyber.dhs.gov/bod/22-01/
4.  Vulcan Cyber, Pulse, "How are Cyber Security Teams Prioritizing Vulnerability Risk?", 2021. https://l.vulcancyber.com/hubfs/Infographics/Vulcan_2021-11-22_How%20are%20Cyber%20Security%20Teams%20Prioritizing%20Vulnerability%20Risk_v1.pdf
5.  IBM Security, "2021 Cost of a Data Breach Report", 28 July 2021. https://www.ibm.com/security/data-breach
6.  Ivanti, "Patch Management Challenges", 7 October 2021. https://www.ivanti.com/resources/patch-management-challenges
7.  ExtraHop, "Cyber Confidence Index 2022", 1 March 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/