Better Together:

Vulnerability Scanners & Ivanti Risk-Based Solutions

Vulnerability scanners are essential cybersecurity tools, but other software is needed to create a strong vulnerability management stack. Ivanti's risk-based solutions get the most out of scanner data while making vulnerability management processes more efficient and effective. The result: you minimize cybersecurity risk along with the time and effort spent on vulnerability management.

Aggregation

Vulnerability Scanners

Modern enterprises must use multiple scanners – network, SAST, DAST, OSS, container – endpoint detection and response (EDR) software, and other tools to achieve comprehensive coverage in their security posture management efforts. Without an automated way to aggregate output from their tools, companies are forced to manage the flood of disparate data these siloed sources produce manually.

This process is time-consuming and prone to errors. It requires security analysts to gather, normalize and prepare volumes of data for the vulnerability prioritization process. All of these steps delay – and sometimes outright prevent – remediation of vulnerabilities.

Further, manual prioritization of vulnerabilities based on insufficient scoring methods, like the Common Vulnerability Scoring System (CVSS), is also prone to leaving the riskiest vulnerabilities unresolved.

20x

increase in scan cadence over the past decade[1]

Ivanti Risk-Based Solutions

Ivanti Neurons for Risk-Based Vulnerability Management (RBVM) and **Ivanti Neurons for App Security Orchestration & Correlation (ASOC)** use automation to measure risk and prioritize remediation activities.

These risk-based solutions work by correlating data from network scanners, application scanners and other tools with threat intelligence and a range of other security data. Asset criticality is also incorporated into the correlation process to contextualize prioritization for every environment.

Leveraging these capabilities, you can move from detection of the vulnerabilities and weaknesses that pose your organization the most risk to remediation in minutes – not months.

BLACKDUCK

Qualys.

CROWDSTRIKE

RAPID7

edgescan

tenable.io™

Coverage

Vulnerability Scanners

No scanner can identify every vulnerability in an environment. Instead, they'll identify only those vulnerabilities for which their developers have created plugins or detection signatures.

Even with an arsenal of scanners, companies will still have gaps in coverage. Plus, without an easy way to aggregate the data from those scanners, many high-risk vulnerabilities are still destined to fall through the cracks.

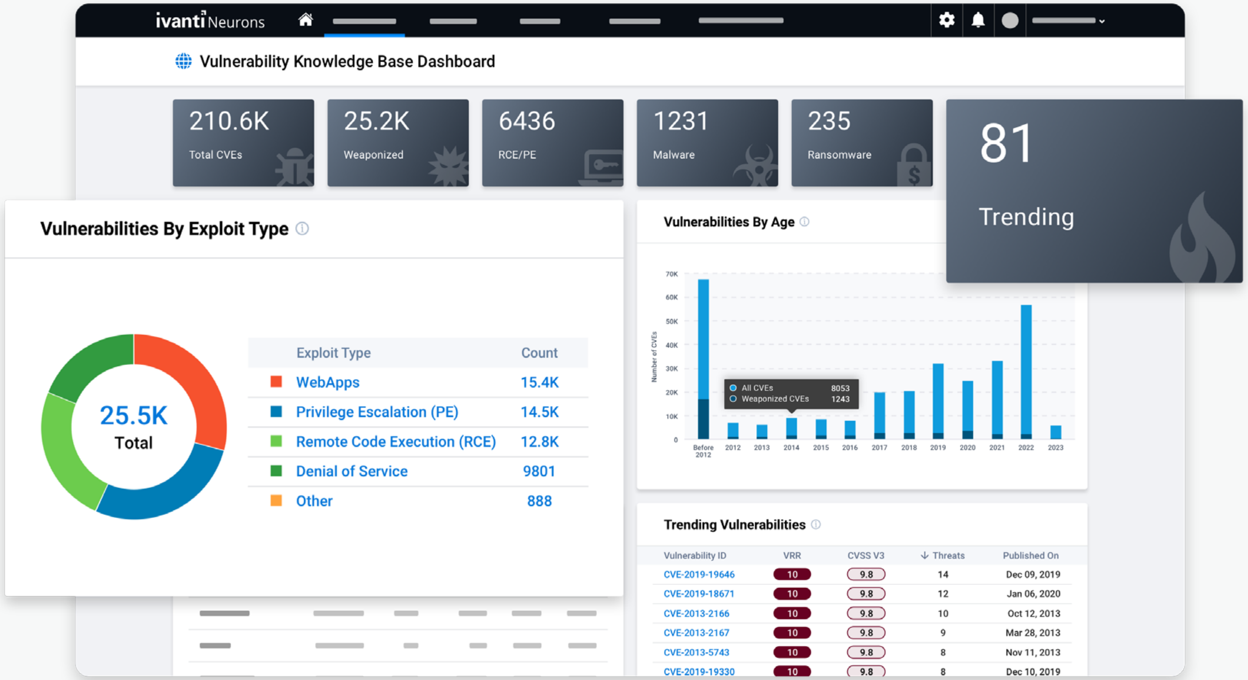
Ivanti Risk-Based Solutions

Ivanti Neurons for RBVM and ASOC increase an organization's coverage by aggregating data from disparate scanners. And instead of seeing vulnerabilities spread out across separate scanner screens, Ivanti lets users view them all in the same place – with a unified risk scoring methodology applied to all issues and assets.

Users can track issues based on the scanner they originated from within Ivanti Neurons for RBVM and ASOC as well. And while those Ivanti solutions offer intel on issues detected by scanners, **Ivanti Neurons for Vulnerability Knowledge Base (VULN KB)** contains details on all vulnerabilities and weaknesses. This information enables organizations to understand what's going on globally, like which vulnerabilities are trending.

20

ransomware vulnerabilities
go undetected by
popular scanners[2]



Vulnerability Knowledge Base Dashboard

210.6K Total CVEs

25.2K Weaponized

6436 RCE/PE

1231 Malware

235 Ransomware

81 Trending

Vulnerabilities By Exploit Type

25.5K Total

Exploit Type	Count
🟥 WebApps	15.4K
🟦 Privilege Escalation (PE)	14.5K
🟩 Remote Code Execution (RCE)	12.8K
🟩 Denial of Service	9801
🟧 Other	888

Vulnerabilities By Age

Trending Vulnerabilities

Vulnerability ID	VRR	CVSS V3	↓ Threats	Published On
CVE-2019-19646	10	9.8	14	Dec 09, 2019
CVE-2019-18671	10	9.8	12	Jan 06, 2020
CVE-2013-2166	10	9.8	10	Oct 12, 2013
CVE-2013-2167	10	9.8	9	Mar 28, 2013
CVE-2013-5743	10	9.8	8	Nov 11, 2013
CVE-2019-19330	10	9.8	8	Dec 10, 2019

Prioritization

Vulnerability Scanners

Scanners make it difficult to determine if threats like ransomware are present in an organization's environment. Achieving that level of visibility in a scanner usually requires customers to write scripts or apply a multitude of filters.

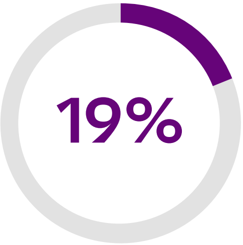
Further, scanners don't typically offer insight on how they determine the severity levels they assign to vulnerabilities. If 100 different vulnerabilities in an organization's environment are marked as critical, the organization must treat all 100 the same, even if only one is tied to ransomware or some other type of threat.

Ivanti Risk-Based Solutions

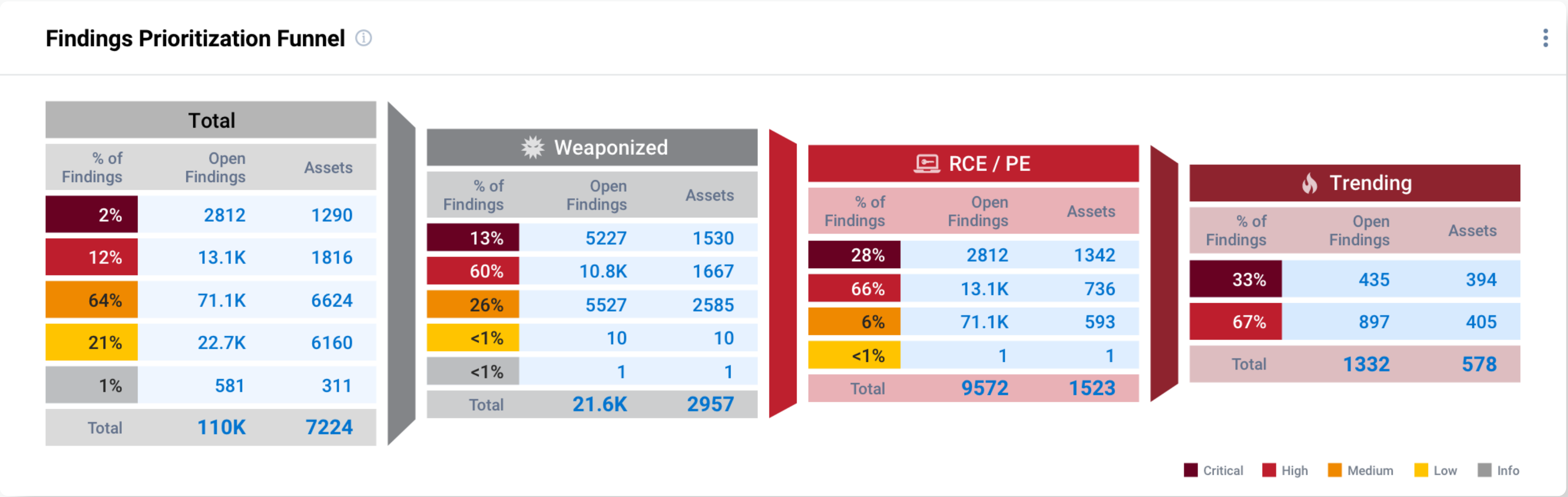
A dashboard revealing an organization's exposure to vulnerabilities being exploited directly and indirectly by ransomware comes standard in Ivanti Neurons for RBVM and ASOC. Readymade views let users filter assets and findings for those impacted by ransomware and other threats as well.

Ivanti is the only organization that offers such quick and easy ransomware visibility. Beyond ransomware, our tools also identify remote code execution (RCE), privilege escalation (PE), and trending and active vulnerabilities to further aid vulnerability prioritization.

Organizations also have the option to prioritize vulnerabilities based on their specific criteria. Ivanti offers countless ways for users to pinpoint assets and findings in need of attention, from proprietary risk scoring to asset criticality.



increase in the count of ransomware vulnerabilities in 2022[2]



Findings Prioritization Funnel ⓘ

Total

% of Findings	Open Findings	Assets
2%	2812	1290
12%	13.1K	1816
64%	71.1K	6624
21%	22.7K	6160
1%	581	311
Total	110K	7224

Weaponized

% of Findings	Open Findings	Assets
13%	5227	1530
60%	10.8K	1667
26%	5527	2585
<1%	10	10
<1%	1	1
Total	21.6K	2957

RCE / PE

% of Findings	Open Findings	Assets
28%	2812	1342
66%	13.1K	736
6%	71.1K	593
<1%	1	1
Total	9572	1523

Trending

% of Findings	Open Findings	Assets
33%	435	394
67%	897	405
Total	1332	578

■ Critical ■ High ■ Medium ■ Low ■ Info

Workflow Routing

Vulnerability Scanners

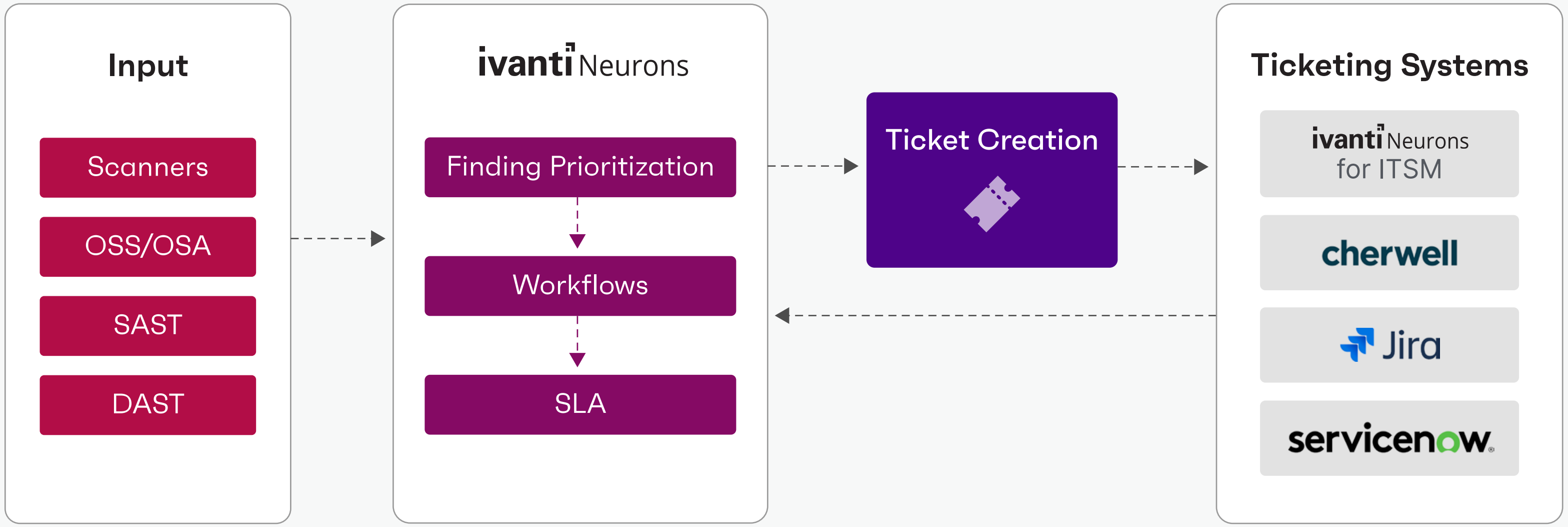
When a vulnerability requires attention, it must be routed to the proper personnel. Complex routing is common in modern enterprises. Infrastructure, DevOps and SAST/DAST tickets all go to different ticketing systems used by the different teams that own remediation in those areas – IT, development and so on.

The ability to organize and route these tickets automatically is typically not found in scanners. Only organizations that can scan for vulnerabilities, prioritize them, route tickets, create audit logs and more using a homogeneous set of tools from a single vendor are immune to the issue – if such a vendor even exists.

Ivanti Risk-Based Solutions

Ivanti Neurons for RBVM and ASOC aggregate data from all an organization's scanners into a single system. When a vulnerability in need of attention is identified by Ivanti's risk-based solutions, users can quickly open a ticket in the proper external ticketing system from within the Ivanti user interface.

Bidirectional integrations with ticketing systems ensure data consistency. When a ticket is updated in either the Ivanti system or the ticketing system, the state is accurately reflected in both.



Automation

Vulnerability Scanners

Organizing assets and responsible parties and assigning due dates based on adopted policies are tasks that must be completed manually at organizations with heterogeneous vulnerability management tech stacks. Further, users in such situations must do so multiple times across multiple tools.

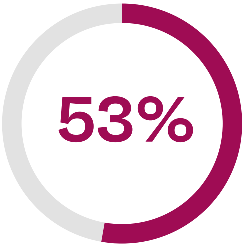
These and other administrative tasks keep security analysts from focusing on remediation efforts.

Ivanti Risk-Based Solutions

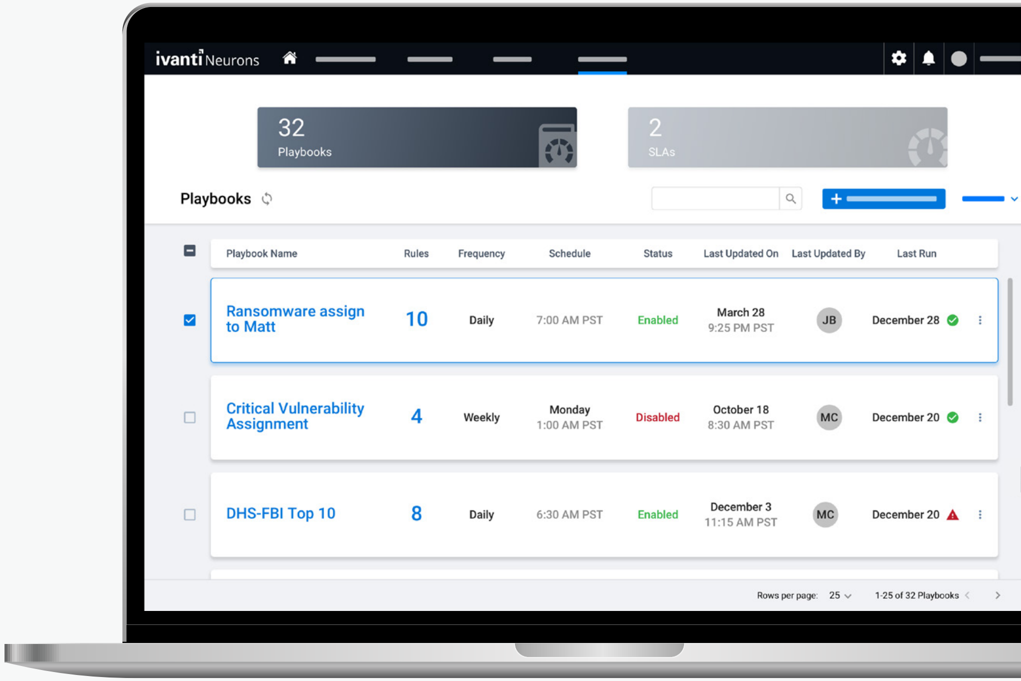
Playbooks in Ivanti Neurons for RBVM and ASOC enable the automation of common or repetitive tasks so users can focus time and effort on remediation actions rather than administration. These automated playbooks run on a continual basis and can organize assets into groups or tags.

Service-level agreement (SLA) automations in Ivanti's risk-based solutions auto-assign due dates to findings. Due dates are based on criteria specified by the organization, such as VRR, asset criticality, and date of finding discovery.

And with all your scanner data in the same system, you only need to configure these automations in one spot. You also benefit from having uniform processes applied to all findings and assets versus being bogged down by different processes in different tools.



of IT and security professionals spend most their time organizing and prioritizing vulnerabilities[3]



▬	Playbook Name	Rules	Frequency	Schedule	Status	Last Updated On	Last Updated By	Last Run
☑	Ransomware assign to Matt	10	Daily	7:00 AM PST	Enabled	March 28 9:25 PM PST	JB	December 28 ✓
□	Critical Vulnerability Assignment	4	Weekly	Monday 1:00 AM PST	Disabled	October 18 8:30 AM PST	MC	December 20 ✓
□	DHS-FBI Top 10	8	Daily	6:30 AM PST	Enabled	December 3 11:15 AM PST	MC	December 20 ⚠

Rows per page: 25 ⌄ 1-25 of 32 Playbooks

Reporting

Vulnerability Scanners

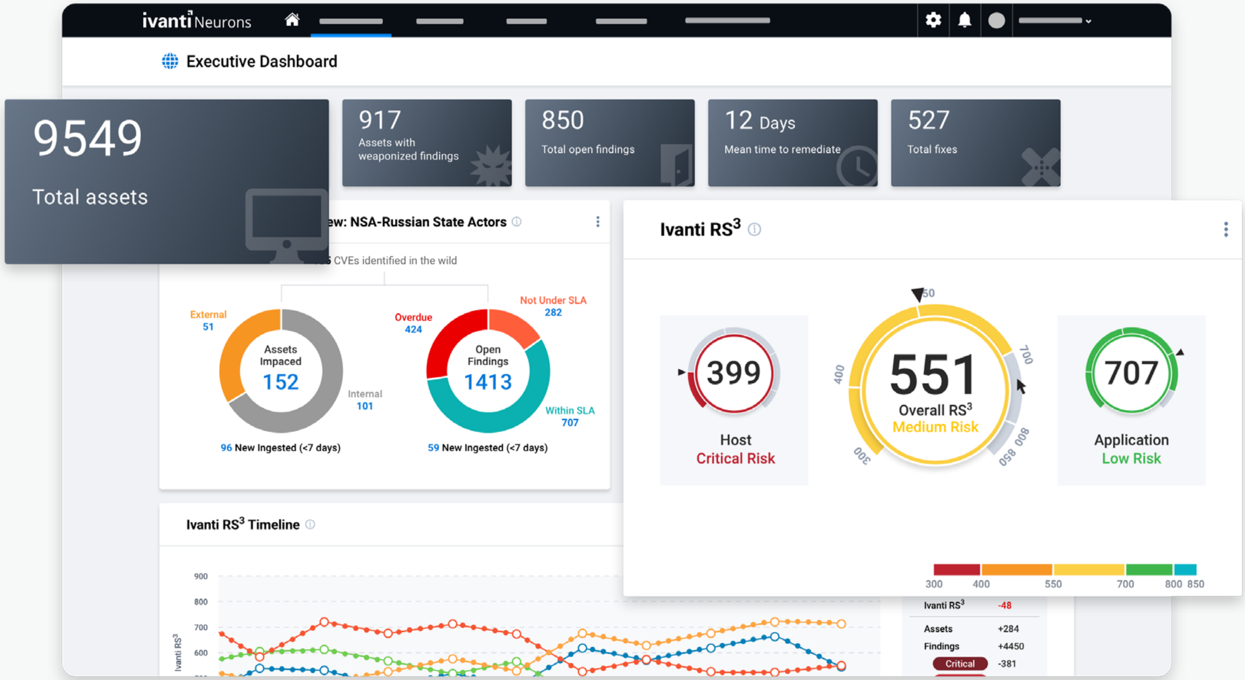
Siloed scanners make reporting a tedious task. Running compliance reports across multiple scanners for an audit period is extremely difficult when dealing with disparate datasets.

Ivanti Risk-Based Solutions

A single source of truth is needed to achieve reliable reporting. By aggregating and normalizing the data generated by each of an organization's scanners, Ivanti Neurons for RBVM and ASOC provide one.

Ivanti's risk-based solutions deliver time-based information. Not only do they tell you what the current state of your environment is, they can also tell you what happened in a specific timeframe, such as an audit period.

Also, with all their scanner data in the same system, organizations set the same yardstick for their entire environment. For example, they can view unified risk scoring for all issues and assets versus having to rely on varied risk scoring methodologies in separate scanners.



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 the only technology company that finds, manages and protects every 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

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

1. Veracode. "State of Software Security (SOSS) Report Volume 12". https://www.veracode.com/state-of-software-security-report
2. Cyber Security Works, Cyware, Ivanti, Securin. "2023 Spotlight Report - Ransomware Through the Lens of Threat and Vulnerability Management". https://cybersecurityworks.com/ransomware/
3. Ivanti. "Patch Management Challenges". https://www.ivanti.com/resources/v/doc/ivi/2634/712cff539c8a