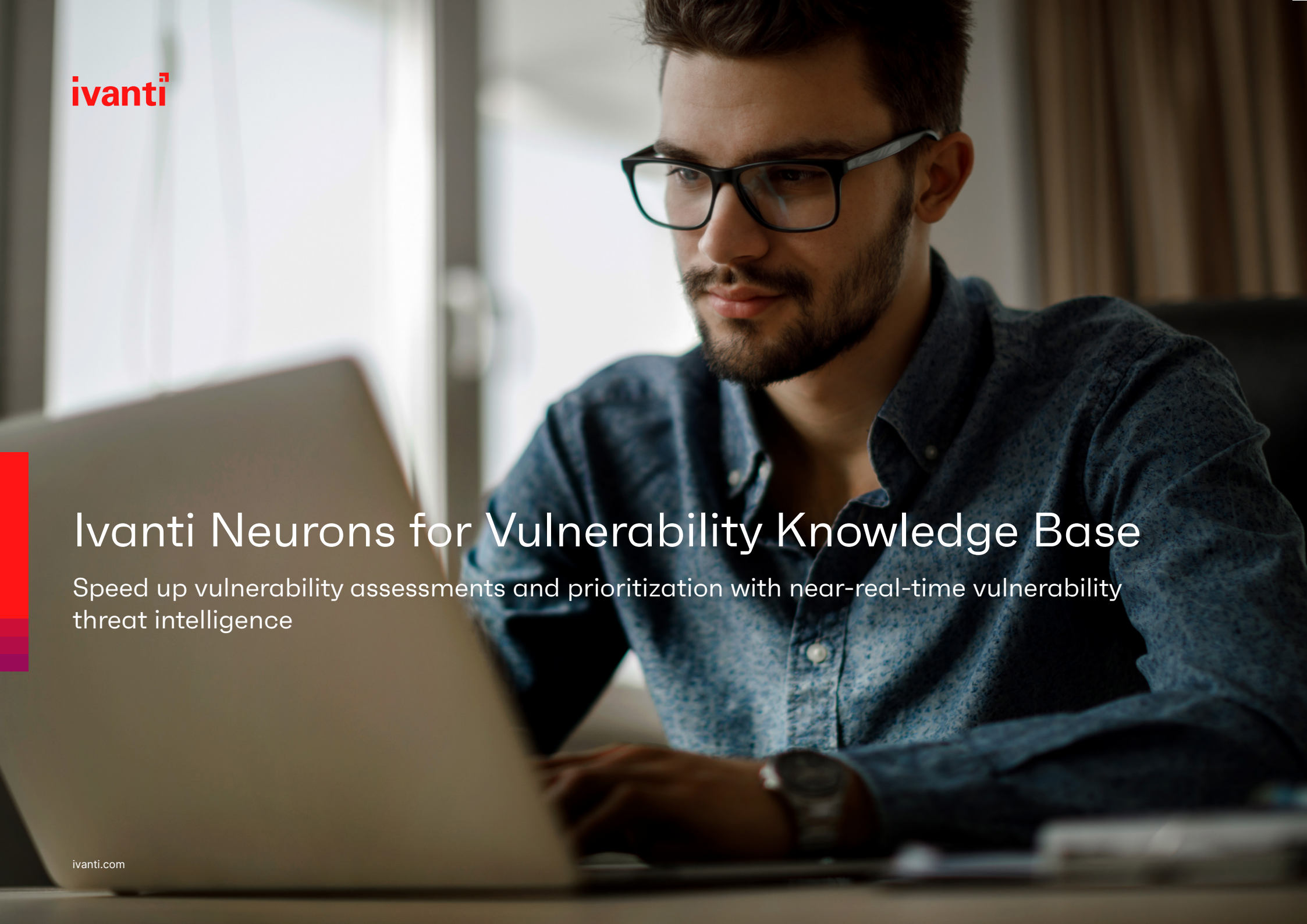


Ivanti Neurons for Vulnerability Knowledge Base

Speed up vulnerability assessments and prioritization with near-real-time vulnerability threat intelligence

Ivanti Neurons for Vulnerability Knowledge Base arms security experts with authoritative and immediate vulnerability threat intelligence plus risk-based scoring of vulnerabilities based on real-world threat information so they can analyze and assess the effect of a vulnerability on their organization and quickly pivot to planning mitigation and remediation strategies.

Vulnerabilities require a faster response

Seventy-four percent of organizations take a day or longer to mitigate or remediate critical vulnerabilities.[1] In an age where 42% of known exploited Common Vulnerabilities and Exposures (CVEs) are being used by cyber adversaries on day zero of disclosure in the National Vulnerability Database (NVD), these organizations leave themselves open to significant risk.[2]

Multiple factors commonly prohibit organizations from staging a faster response to vulnerabilities. For starters, there is often significant latency between the time a vendor publishes a vulnerability and the time of NVD disclosure. For example, in 2021, that latency equaled an average of 13.7 days for ransomware vulnerabilities.[3]

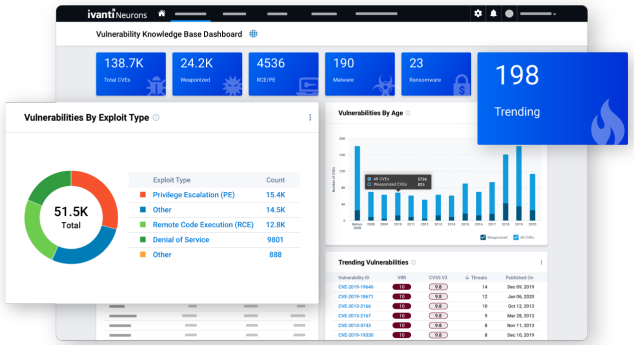
The scanners security teams use present a similar issue. These tools only provide information on vulnerabilities and weaknesses after they have been discovered, cataloged, entered into the tool and then scanned for. This process can take anywhere from minutes to months past when that information is needed.

Scanners have other gaps as well. For instance, a comparison of three of the most popular scanners found that the best of the bunch could only detect 77% of ransomware vulnerabilities.[3] Additionally, even the best scanner will only contain information on vulnerabilities and weaknesses that are found within an organization's environment, offering no insight into those vulnerabilities and weaknesses that have evaded detection or may not yet be present in the organization's environment.

The ability for an organization to respond to vulnerabilities is often further delayed by the need for security practitioners to correlate the information from scanners with information from online searches and other manual methods of research. Additionally, manual research efforts are only effective if the information they are targeting is available and accurate.

Introducing Ivanti Neurons for VULN KB

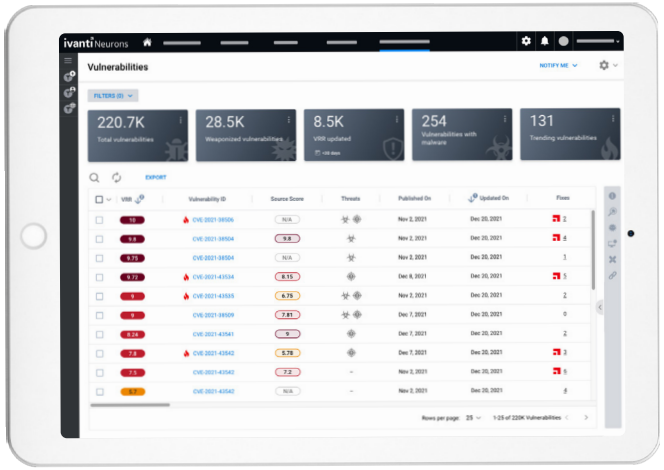
Ivanti Neurons for Vulnerability Knowledge Base (VULN KB) provides pen testers, red teamers, security analysts and other security experts with the near-real-time vulnerability threat intelligence they need to speed up vulnerability assessments and prioritization. Easy access to research from the highest fidelity sources and industry-leading exploit writers enables those experts to quickly pivot from analyzing and assessing the effect of a vulnerability on their organization to planning mitigation and remediation strategies. Risk-based scoring of vulnerabilities that is constantly updated based on real-world threat information aids them in their efforts.



Key capabilities

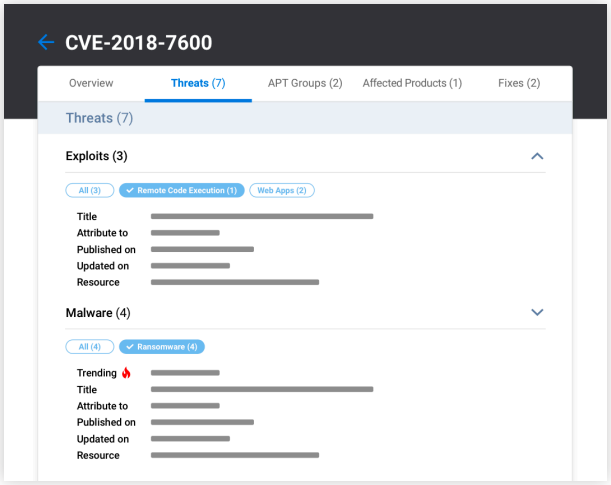
Gain a global view of CVEs and CWEs

Access detailed information on all vulnerabilities (CVEs) and weaknesses (CWEs), not just those identified by your scanners. Ivanti Neurons for VULN KB enables you to increase your knowledge of the security landscape and understand what's going on globally – for example, which vulnerabilities are trending. Knowing what a threat can do to your organization's critical systems can help you better protect those systems from cyberattacks.



Perform in-depth vulnerability assessments and prioritization

Find all the information you need about any vulnerability or weakness in one location to help you identify the greatest risks to your organization based on actual exploitability. Ivanti Neurons for VULN KB puts an automated and expert-led collection of authoritative vulnerability threat intelligence at your fingertips. Its intelligence comes from the highest fidelity sources and industry-leading exploit writers.

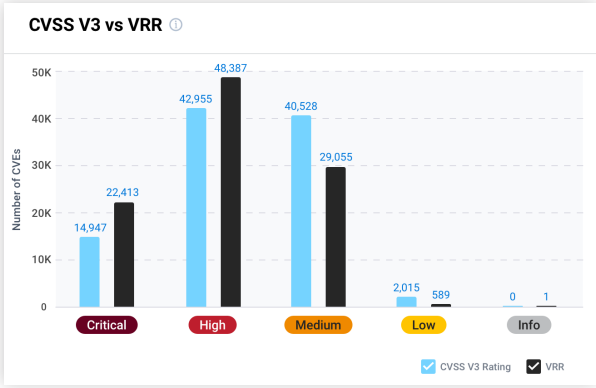


The platform includes all perspectives of vulnerability risk:

- CVE and CWE NVD details.
- Identified remote code execution (RCE) and privilege escalation (PE) capabilities.
- Weaponized exploits and malware.
- Associated exploits trending in the wild.
- Ties to ransomware variants.
- Association with APT groups.
- Ivanti Vulnerability Risk Rating (VRR).

Speed up mean time to mitigate

Create informed plans based on threat context to mitigate risk exposure from vulnerabilities and weaknesses without having to wait for scan findings. Ivanti Neurons for VULN KB provides immediate access to detailed information on all known CVEs and CWEs, even those CVEs coming from CVE Numbering Authorities (CNAs) before they are officially scored by the NVD. Additionally, VRR scores within the platform are constantly updated based on real-world threat information to ensure security and IT teams always have a current perspective of the cyber risks their organization faces.



Trending Vulnerabilities

Vulnerability ID	VRR	CVSS V3	Threats	Published On
CVE-2012-1723	10	N/A	98	Jun 12,2012
CVE-2017-11882	10	9.8	961	Nov 14, 2017
CVE-2012-0507	10	N/A	90	Feb 14, 2021
CVE-2007-1036	10	9.8	9	Feb 21, 2007
CVE-2018-7602	10	9.8	9	Jul 19, 2018
CVE-2021-3156	9.59	9.8	9	Jan 26, 2021
CVE-2021-34527	10	9.8	8	Jul 01, 2021
CVE-2021-34473	10	8.1	8	Jul 13, 2021
CVE-2017-0037	10	8.1	8	Feb 26, 2017
CVE-2017-9805	910	7.5	8	Sep 05, 2017

Features & functions

Feature	Function
Diverse data sources	Achieve a wide view of cyber risk with a platform that ingests vulnerability findings from over 100 independent sources plus manual findings from research and pen testing teams.
Vulnerability KB dashboard	Leverage insightful visualizations on vulnerabilities and weaknesses, including their threat context, to improve vulnerability management processes.
Vulnerabilities list view	Find detailed information on all known vulnerabilities in the Ivanti database, plus all associated threat data, such as trending, ransomware, exploits and more.
Weaknesses list view	Access a full list of available software weaknesses as defined by MITRE plus detailed information on each.
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.
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 with deep links.

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. ExtraHop, "Cyber Confidence Index 2022", 1 March 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/
2. 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/
3. 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