Prioritize vulnerabilities like an attacker with Active Risk

Identify and prioritize remediation for the vulnerabilities most likely to exploit your cloud and on-prem environments

It's an all-too-familiar scenario: Thousands of vulnerabilities are identified across your hybrid ecosystem. An overwhelming portion of them are labeled as "critical" in bright red, giving no clear direction on which remediation efforts will have the most risk reduction.

Active Risk is Rapid7's vulnerability risk-scoring methodology designed to help security teams prioritize the vulnerabilities that are actively exploited or most likely to be exploited. Our approach takes into account the latest version of the Common Vulnerability Scoring System (CVSS) available for a vulnerability and enriches it with multiple threat intelligence feeds, including proprietary Rapid7 research, to provide security teams with a threat-aware vulnerability risk score.

Rapid7 customers using our vulnerability risk management solutions will now be able to leverage the same vulnerability risk scoring methodology to prioritize vulnerabilities on their on-prem assets and cloud resources.

Latest CVSS + **Real-Time And Predictive Threat Intelligence Based On** CISA KEV, Metasploit, Rapid7 research - Project Lorelei and AttackerKB, ExploitDB and more = **Active Vulnerability Risk Score (Range: 0 - 1000)** Prioritize vulnerabilities actively exploited in the wild or most likely to be exploited

Security teams can use Active Risk to:

Prioritize actively exploited vulnerabilities

At any given time, security teams are dealing with thousands of vulnerabilities. Teams can use a data-driven approach, based on threat intelligence from sources like CISA KEV, Metasploit, and many more, to know which vulnerabilities are actively being exploited in the wild; and prioritize remediation for those critical vulnerabilities first.

Key Benefits

- Prioritize actively exploited vulnerabilities
- Leverage real-time and predictive threat intelligence
- Normalize vulnerability risk scoring across cloud and on-prem environments
- Communicate the risk posture cross-functionally

Leverage real-time and predictive threat intelligence

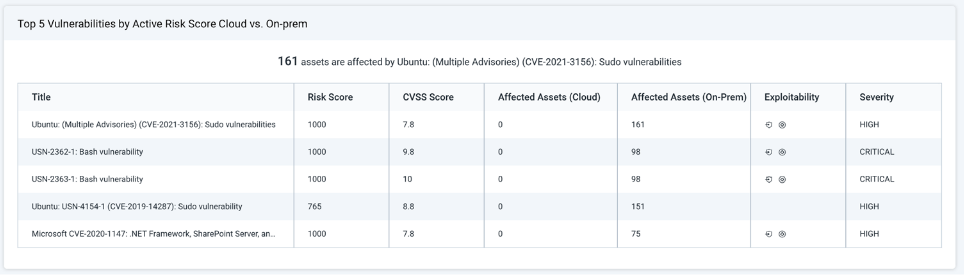
Active Risk augments the latest CVSS score with intelligence from Rapid7's Project Lorelei and AttackerKB to monitor for active attacks and provide real-time threat intel updates. Predictive values based on our expert research in AttackerKB, indicate the likelihood of a vulnerability being exploited and the value that vulnerability would provide to an attacker if successful.

Normalize vulnerability risk scoring across cloud and on-prem environments

Active Risk is built into our Vulnerability Management solutions like Cloud Risk Complete (cloud and on-prem assets), InsightVM (on-prem/remote assets), InsightCloudSec (cloud resources) to provide a consistent vulnerability risk-scoring methodology. It uses a normalized score range (0-1000) to simplify risk comprehension by security and non-security stakeholders.

Communicate the risk posture cross-functionally

Get buy-in from remediation teams to prioritize patching for vulnerabilities with a high risk score within set SLAs. Communicate the risk posture to executive stakeholders by providing context on which vulnerabilities need to be prioritized and where the riskiest assets lie. Security teams can leverage Active Risk dashboard cards (Vulnerability Findings by Active Risk Score Severity and Vulnerability Findings by Active Risk Score Severity and Publish Age) in InsightVM and Executive Risk View in our Cloud Risk Complete solution to support cross-functional conversations.z



Top 5 Vulnerabilities by Active Risk Score Cloud vs. On-prem

161 assets are affected by Ubuntu: (Multiple Advisories) (CVE-2021-3156): Sudo vulnerabilities

Title	Risk Score	CVSS Score	Affected Assets (Cloud)	Affected Assets (On-Prem)	Exploitability	Severity
Ubuntu: (Multiple Advisories) (CVE-2021-3156): Sudo vulnerabilities	1000	7.8	0	161	⊙ ◎	HIGH
USN-2362-1: Bash vulnerability	1000	9.8	0	98	⊙ ◎	CRITICAL
USN-2363-1: Bash vulnerability	1000	10	0	98	⊙ ◎	CRITICAL
Ubuntu: USN-4154-1 (CVE-2019-14287): Sudo vulnerability	765	8.8	0	151		HIGH
Microsoft CVE-2020-1147: .NET Framework, SharePoint Server, an...	1000	7.8	0	75	⊙ ◎	HIGH

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit: **https://www.rapid7.com/try/insight/**