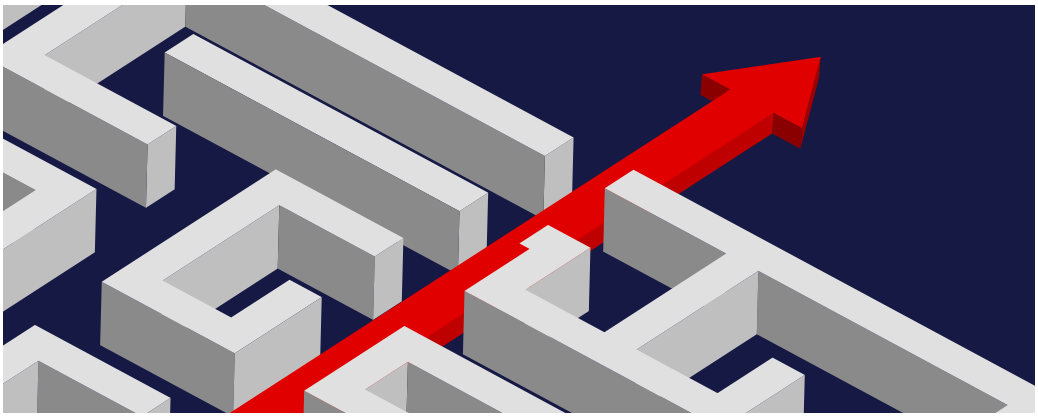
TECHNOLOGY BRIEF
RiskSense Risk-Based Vulnerability Management

Always Know Your Next Move Against Vulnerability Risk Exposure

KEY BENEFITS

- 90% reduction in time spent performing data analysis
- 50-70% faster remediation through detailed risk remediation reporting, orchestration, and automation
- Data-driven prioritization and prediction of trending threats
- Superior visibility on vulnerabilities specifically being exploited by ransomware
- Unified security risk scoring with prescriptive remediation and action prioritization
- Improve compliance and audit with closed loop remediation validation



THE CHALLENGE

Threat and vulnerability management is the toughest job in cybersecurity. Security analysts must wade through piles of vulnerabilities to determine which ones matter today knowing that they'll have to repeat the same process tomorrow with the same incomplete data. The result is "cyber risk mayhem", in which it is impossible to know at the end of the day if the enterprise is more secure or less so. While many active threats continue to use older well-known vulnerabilities, the ransomware epidemic has only increased the urgency for security teams to identify, prioritize, and act to counter the most dangerous and active exploits.

Gartner asserts that by 2022, organizations using risk-based vulnerability management will suffer 80% fewer breaches.[1] Conversely, organizations utilizing CVSS, CWE, and scanner vulnerability scoring suffer from alert overload and threat fatigue. What is needed is the ability to identify the vulnerabilities and risks that pose a real and present danger to the enterprise, resolve them, and then validate that the exposure has been addressed.

USE CASE

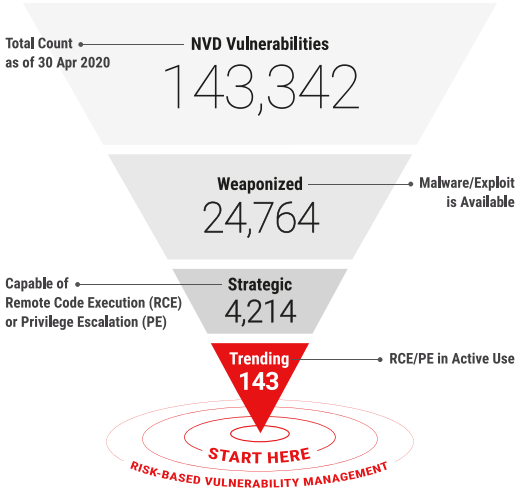
Vulnerability Management as a Data-Driven Tool for Cybersecurity Risk Reduction

Vulnerability scanners continuously find thousands of vulnerabilities. According to RiskSense Labs research, of the 136,000+ known vulnerabilities found in the U.S. NVD2, only about 20% are weaponized, only about 3% are capable of the kind of remote code execution or privilege escalation that makes them truly dangerous, and less than 1/10% are trending in the wild.

RiskSense continuously maps threats to vulnerabilities. The platform then utilizes that mapping to identify trending vulnerabilities that are currently found "in the wild" and require immediate attention. "Trending" status is reached when high-impact vulnerabilities are being actively exploited by attackers in the wild. RiskSense delivers superior interpretation and customizable presentation of an organization's specific threat and vulnerability landscape.

RiskSense's risk-based vulnerability management solution transforms vulnerability management into a key, continuous, and measurable driver of cybersecurity risk reduction. While the number of weaponized vulnerabilities is constantly increasing RiskSense empowers enterprises to achieve their desired cybersecurity risk posture and quickly reduce their attack surface.

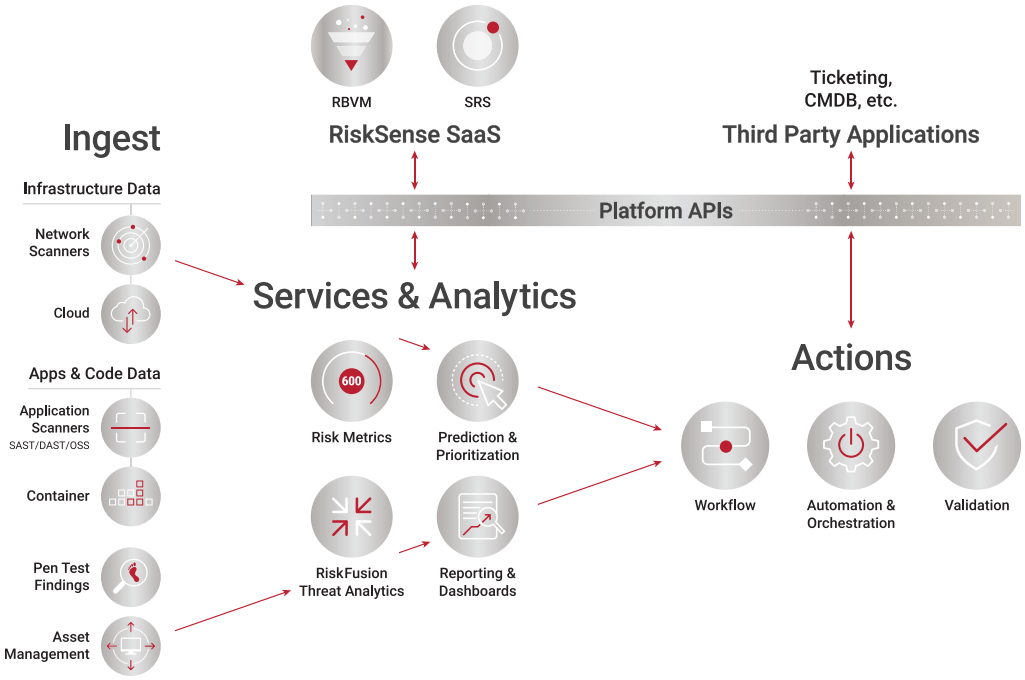
[1] Gartner Group, A Guide to Choosing a Vulnerability Assessment Solution, April 2019



RISKSENSE PLATFORM

Enhanced Risk-Based Vulnerability Management

The RiskSense platform emerged from research done by its founders in conjunction with U.S. Department of Defense and U.S. Intelligence Community to develop the Computational Analysis of Cyber Terrorism against the U.S. (CACTUS) system. The platform leverages human and machine intelligence that embodies the expertise and deep knowledge RiskSense has gained from defending critical networks against the world's most dangerous adversaries.



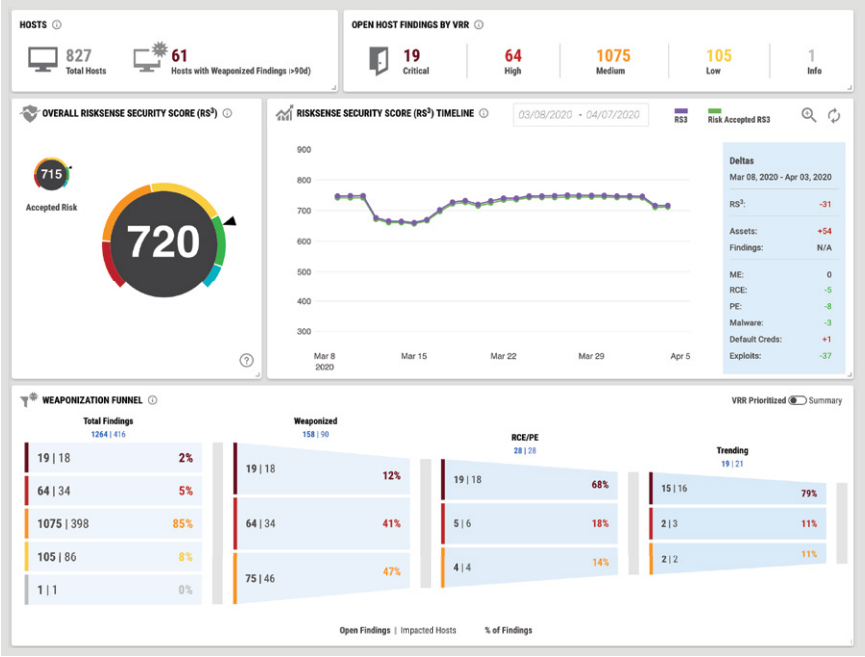
From Scan Data to Actions in Seconds

RiskSense consumes vulnerability data from all leading network and application vulnerability scanners including Tenable, Qualys, WhiteHat, Rapid7, and Veracode. The RiskSense platform coordinates findings from over 100 threat intelligence sources including valuable endpoint telemetry to determine which vulnerabilities have been weaponized, are trending in the wild, and present a material risk to enterprise security. Only RiskSense utilizes its own pen testing and threat research team to identity emerging vulnerabilities before they become

active with cyber criminals. These "manual findings" feed into the RiskSense platform enhancing risk-based vulnerability management.

Rich Functionality to Clear Risk Reduction Results

A RiskSense Security Score (RS³) for each asset, group, and organization is calculated, providing cybersecurity teams quantification of the organizational risk profile and progress towards the desired risk posture. Security teams can drill-down to detailed asset findings and threats from configurable dashboards focused on key concerns of the enterprise attack surface. Remediation recommendations with native workflow and bi-directional ticketing integration, ServiceNow, BMC Remedy, and Jira, provides a fully-informed view of the priorities and current activities.



The RiskSense platform goes beyond common vulnerability management. Users are capable of having both Internal, and an external perspective that shows how attackers may view their organization. Risk- based vulnerability management (RBVM) and Security Rating Service (SRS) delivered by RiskSense accelerate the identification of the patches/fixes that will have the most effect on closing cybersecurity exposure. With RiskSense security teams can automate repetitive tasks and orchestrate workflows to significantly reduce the latency between vulnerability weaponization and remediation. Only RiskSense's platform as a service delivers an enterprise experience with a modern and effective way to counter new threats and undercut the effort it takes to reduce vulnerability risk.

ABOUT RISKSENSE

RiskSense®, Inc. provides vulnerability prioritization and management to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.

RISKSENSE®

LRS IT SOLUTIONS

Contact your LRS account manager to learn more.