What is a Vulnerability Management Solution?

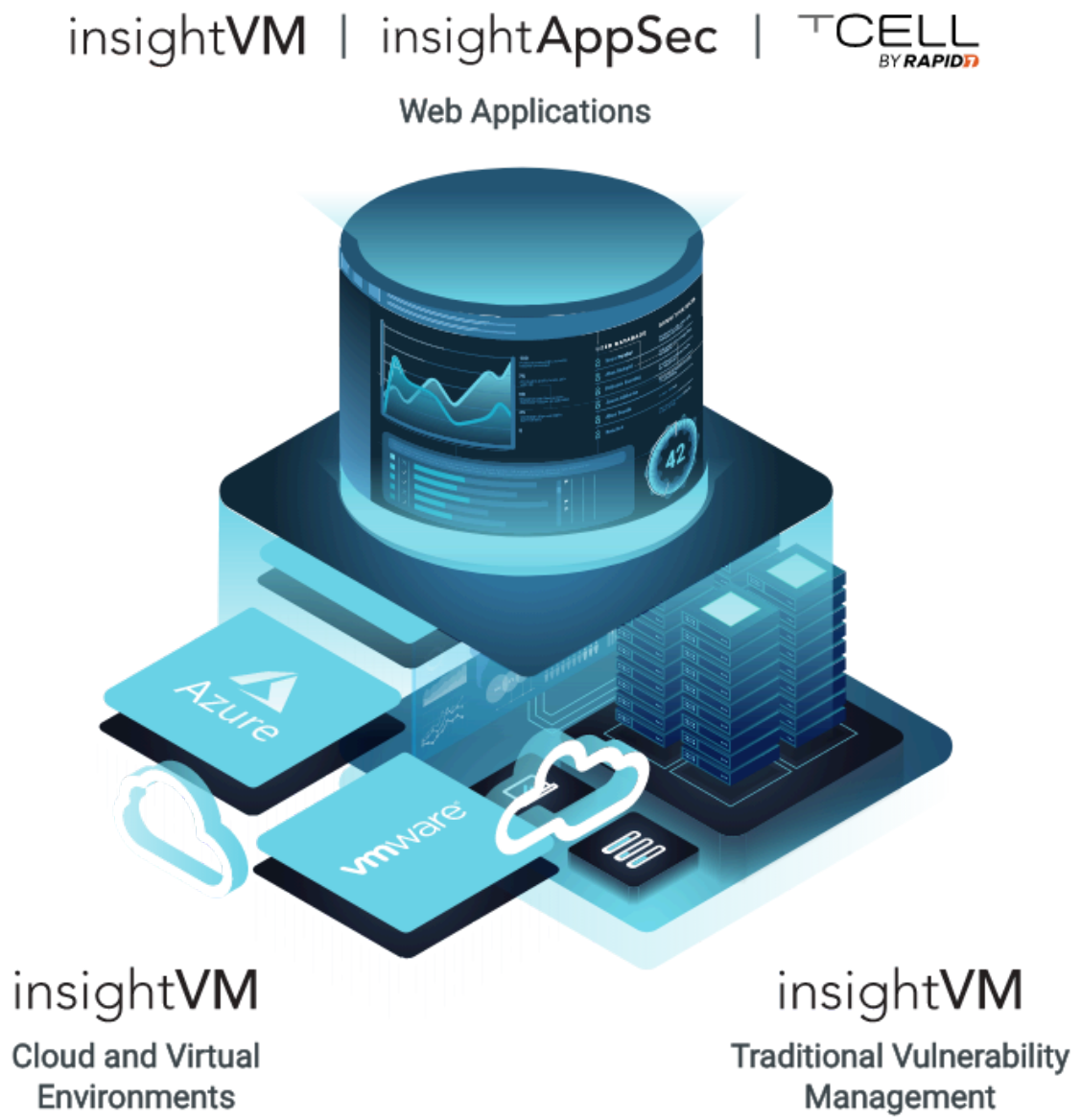
Vulnerability management is a continuous cybersecurity process that includes identifying, evaluating, treating, and reporting software and network vulnerabilities. Properly monitoring and responding to pressing, complex issues are essential components of vulnerability management and information security as a whole.

Why do we need vulnerability monitoring?

Software and network vulnerabilities are constantly at risk of being exploited by attackers with intentions to insert destructive malware attacks, compromise system infrastructure, and steal sensitive user data. Furthermore, these malicious actors leverage both tried-and-true and constantly evolving methods for breaking through your perimeter.

Modern network technologies like cloud computing and containers have created an unprecedented spike in productivity. Many corporate jobs can now be done from the comfort of your living room or your local coffee shop, and deploying a new application or data center takes a fraction of the time and cost it once did. The growing adoption of IaaS and virtualization, compounded by our growing reliance on fast and quick-built applications, creates unique security challenges; it's becoming increasingly difficult for security teams to know *what* is on their network, let alone defend it from attack.

Security teams must work closely with their IT and application development counterparts to understand the risk of these changing environments at at every layer, and look at application, network, and user risk together rather than in silos.



Understanding Risk at Every Layer

Rapid7's vulnerability management product, InsightVM, is built to anticipate these shifts in the way modern IT environments should be secured. In turn, InsightVM equips you to gain clarity into your risk, extend security's influence across the organization, and see shared progress with other technical teams. Securing your infrastructure is a start, securing your entire attack surface is the main event.

Fast-track the development of your vulnerability risk management program with our Getting Started toolkit.

VM Solution Best Practices

For a vulnerability management program to be truly effective, there are four key "pillars" that must be established:

Visibility of your complete IT environment

Effective vulnerability management starts with knowing what's out there—this includes your local, remote, cloud, containerized, and virtual infrastructure. To ensure you're not missing a single corner of your perimeter, it's important that your vulnerability management solution dynamically identifies and assesses assets as soon as they join your network, and identifies all of your externally-facing, internet-connected assets for a complete view of your risk.

Curious what vulnerability risk management looks like across a complete attack surface?

Extensibility and technology integration

Your VRM solution must enable integration, orchestration, and automation of the tools and processes across your stack. InsightVM also received the highest possible scores in the Forrester Wave™ for its extensibility and Partner Ecosystem.

Reporting on the progress that matters most

Tracking the goals and metrics most relevant and impactful to your team is critical; so is communicating those milestones to peers and leadership. InsightVM is designed to track your progress and drive alignment across the organization.

Risk prioritization unique to your business

Identify and prioritize risk with complete coverage of your environment and the addition of business criticality to assets. InsightVM also received the highest possible score in the criteria of Vulnerability Enumeration and Risk-Based Prioritization.

Building a Modern Program and Proving Its Efficacy

Proving the efficacy of a vulnerability risk management program is based on successful execution

in three crucial areas: gaining clarity into risk and across teams, extending security's influence, and seeing shared progress. Let's dive deeper into each of these.

To overcome traditionally tedious vuln management and prove value to leadership step-by-step, scale the mountain and read our Ebook, 4 Steps to Prove the Value of Your VM Program.

Gaining Clarity Into Risk and Across Teams

Not only do you need visibility into vulnerabilities, but you also need clarity into the operations, objectives, and impact of security programs for stakeholders across the organization. The result is a deeper understanding of risk and alignment towards common goals.

Achieve Visibility of Your Entire Attack Surface

Securing a modern environment requires full visibility into your entire attack surface, which includes on-premises, remote, cloud, virtual, and containerized assets. It even extends to the application layer. Monthly or quarterly vulnerability scans simply aren't enough to keep up with attackers and your own shifting ecosystem; you have to go deeper to continuously monitor the modern network.

InsightVM and InsightIDR share a universal agent for collecting live vulnerability and user data from endpoints wherever they're located, letting security teams closely analyze critical vulnerabilities and behavior trends with dynamic dashboards. These capabilities enable you to identify both the weakest entry points to your network and the fastest way to fix them.

InsightVM integrates directly with Project Sonar, a Rapid7 research project that conducts internet-wide surveys across more than 70 different services and protocols to gain insights into global exposure to common vulnerabilities. Attack Surface Monitoring with Project Sonar in InsightVM enables you to identify and assess all external-facing assets, both known and unknown.

We know effective, smarter vulnerability management goes beyond just scanning, and InsightVM lets you do just that. Learn more about InsightVM's unique approach to getting visibility into your dynamic environment.

Accurately Assess Your Ever-Changing Ecosystem

Once all assets in your environment are properly inventoried, you then need to assess them for risk. A good vulnerability risk management solution will be able to assess your environment with minimal impact to your network performance and a reduced number of false positives compared to other solutions on the market.

InsightVM looks at the assets in your environment and makes sure it understands them, their functions, and fingerprints. Based on the unique profile of each asset, InsightVM performs targeted vulnerability checks. In doing so, the overhead needed to run assessment, as well as false positives, are reduced.

Policy Assessment evaluates your assets against industry best practices such as CIS Benchmarks, DISA STIGS, and PCI to help determine your organization's adherence and compliance to these standards.

Prioritize Vulnerabilities Like an Attacker

There's more to risk prioritization than just pinpointing vulnerabilities with the highest CVSS scores; determining where to focus your team's efforts requires you to account for malware

exposure, exploit exposure, and vulnerability age into prioritizing vulnerabilities. InsightVM leverages a Real Risk Score that factors in the above criteria and adjusts to the criticality of certain assets in your unique environment. To keep you prepared in the face of active threats, Integrated Threat Feeds are included (at no cost) that show you critical, named vulnerabilities (such as celebrity zero-days) that are currently present in your environment. The feeds are informed by public data as well as proprietary threat intelligence and adversary research that's continuously gathered under our own roof.

Extending Security's Influence

By enabling collaboration and influencing their peers in IT and development, security professionals using InsightVM can achieve a more efficient vulnerability risk management process. InsightVM provides the foundation for security teams to expand their influence and eliminate silos by having a common language and shared objectives.

Between the notifications of high criticality vulnerabilities and back-and-forth email communications that frequently come with vulnerability assessment, we don't often get to ask ourselves, "what is the true effectiveness of my vulnerability risk management program?" This question becomes increasingly difficult to answer when the completion of remediation tasks spans multiple teams and projects. This is where Goals and SLAs come in.

With Goals and SLAs in InsightVM, you can ensure that you're making (and tracking) progress toward your goals and service level agreements (SLAs) at an appropriate pace, and maintaining compliance with the standards you've set for your program.

Learn more about InsightVM's unique ability to break down the silos of IT, Security, and DevOps teams below.

Seeing Shared Progress

Progress refers to advancing the security program at an organization. It's about recognizing and celebrating goals reached that contribute to the reduction of risk. This results in accelerated achievement and support from leadership.

More Efficient, Cross-Functional Remediation

Vulnerability remediation remains one of the most effective ways to decrease risk in your organizations, yet many organizations struggle with remediating even traditional infrastructure, making modern environments even larger blind spots. Remediation programs need to be as fluid and automated as the infrastructure they seek to secure. Therefore, it's critical to integrate your vulnerability risk management process with internal ticketing tools and track SLAs so that remediation efforts can seamlessly fold into IT teams' existing workloads, minimizing the manual finding and fixing of vulnerabilities.

Accelerating Vulnerability Management Through Automation

InsightVM provides IT-Integrated Remediation Projects that allow security teams to automatically work within their existing IT workflows, plan and monitor remediation progress live, and directly integrate with leading IT ticketing.

Even More Efficiency with Measuring and Reporting on Progress

Equally important to tracking progress made is communicating it effectively to technical and executive teams.

With Live Dashboards, you can easily create custom and full dashboards for every stakeholder and query each card with simple language to track progress of your security program. InsightVM also over static reports for stakeholders at all levels in the organizations, including leadership.

Query Builder in InsightVM lets you query assets, vulnerabilities, and solutions using an intuitive UI. In other words, slice and dice data without relying solely on complex query languages.