SOLUTION GUIDE

MODERN VULNERABILITY MANAGEMENT with Rapid7

RAPID7

INTRODUCTION

Vulnerability management is evolving quickly.

A decade ago, most vulnerability management programs focused on scanning workstations and servers on corporate networks. Now, most enterprises have recognized that traditional vulnerability assessment tools and practices are too limited, too siloed, and too slow to keep up with today's challenges.

These challenges include:

- A vast attack surface, which includes both physical and virtualized environments, in corporate data centers and on cloud platforms.
- Complex web applications that are hard to test, and that change every day—sometimes every hour.
- Employees who regularly fall victim to phishing and other social engineering attacks.
- Floods of alerts and vulnerabilities that threaten to swamp the teams responsible for patching and remediating systems.

You can read about the fundamental components of a modern vulnerability management program in our whitepaper, The Four Pillars of Modern Vulnerability Management: A comprehensive approach to reducing vulnerabilities across your ecosystem.

In this solution guide, we highlight how Rapid7 is helping our customers evolve their vulnerability management programs to meet today's challenges. We focus on four areas:

1 ENHANCING NETWORK VULNERABILITY ASSESSMENT

Today, your security team needs to monitor a vast attack surface; it encompasses a wide variety of endpoints and applications in corporate data centers and on cloud platforms, and runs on physical servers and in virtualized and container environments. You also need to work closely with IT operations groups to respond to vulnerabilities as soon as they are discovered, before they can be exploited by attackers.

How Rapid7 Can Help

Rapid7 InsightVM provides a highly scalable, robust, and efficient way to collect your vulnerability data, turn it into answers, and minimize your risk. It integrates directly with cloud and virtual services such as AWS, Azure, and VMware to help you achieve complete visibility across your entire computing ecosystem.

In virtual and cloud environments such as VMware and Amazon AWS, Rapid7's Insight Agent can be embedded in the images of your instances, so that every time a new component of the service is spun up, it is automatically monitored for vulnerabilities. InsightVM's integration with these platforms also lets you detect when new devices are deployed and automatically assess them.

InsightVM collects a wide range of data from systems, endpoints, and virtual machines. With the Insight Agent, you can unify network vulnerability data from InsightVM and user behavior and incident detection data from **Rapid7 InsightIDR** in one go for expansive, unparalleled visibility.

InsightVM also integrates with ticketing systems such as ServiceNow and Atlassian Jira so you can automate the handoff of vulnerability data and tasks to the teams responsible for patching and remediation. This automated handoff gives teams access to more data, faster, so they can patch systems and fix misconfigurations quickly and accurately.

Finally, InsightVM can integrate with **Rapid7 InsightConnect**, a security orchestration and automation solution that enables your team to automate time-intensive processes without writing a single line of code. By combining the power of InsightVM and InsightConnect, you can expose your most critical vulnerabilities and determine which assets can be auto-patched. Streamlining remediation this way saves you your most important resource—time—and reduces your chance of making errors.

Want to see these integrations in action?
Try InsightVM free for 30 days now.

2 ADDRESSING WEB APPLICATION VULNERABILITIES

Most dynamic application security testing (DAST) tools and application scanners built into vulnerability assessment tools were designed to detect weaknesses in older web applications built with HTML, PHP, and Perl. Unfortunately, many of these options are still awaiting their invitations into the current decade and cannot effectively test rich web applications built with newer technologies such as HTML5, AMF, SPA frameworks, JSON, REST, and SOAP, nor crawl through multi-step workflows such as shopping cart sequences.

Web application vulnerabilities can also be overlooked when software development groups use Agile development and DevOps techniques to promote new versions of applications into production on a daily or hourly basis, before the security team is aware of them, let alone able to assess them.

How Rapid7 Can Help

Rapid7 InsightAppSec and **Rapid7 AppSpider** enable the security testing of application logic. They "understand" web applications with sophisticated interfaces, APIs, and protocols, and can test applications thoroughly, even when the applications utilize custom parameters, non-traditional authentication processes, and complex workflows such as shopping carts.

By integrating into the early phases of the software development lifecycle (SDLC), these tools can also help security teams "shift left" and keep up with the rapid pace of modern application development.

InsightVM assesses the modern infrastructure needed to support advanced web applications. It enables security organizations to adopt a DevSecOps approach where they collaborate with DevOps teams integrate vulnerability assessment into development, testing, and staging environments, as well as production systems.

With InsightVM you can:

- Embed assessment agents in the images of instances in virtual environments, so every virtual machine can be scanned as soon as it is spun up.
- Assess container registries and container hosts for vulnerabilities and misconfigurations.

Head to www.rapid7.com/try/insight to start securing your modern network and applications.

3 PROTECTING EMPLOYEES AND MITIGATING USER RISK

Research shows that in most organizations, users are the most significant attack vector, and phishing has the greatest impact of any threat type. Yet few enterprises have a robust program for combating phishing and other social engineering attacks. Even fewer take advantage of opportunities to incorporate these programs into their overall vulnerability management strategy.

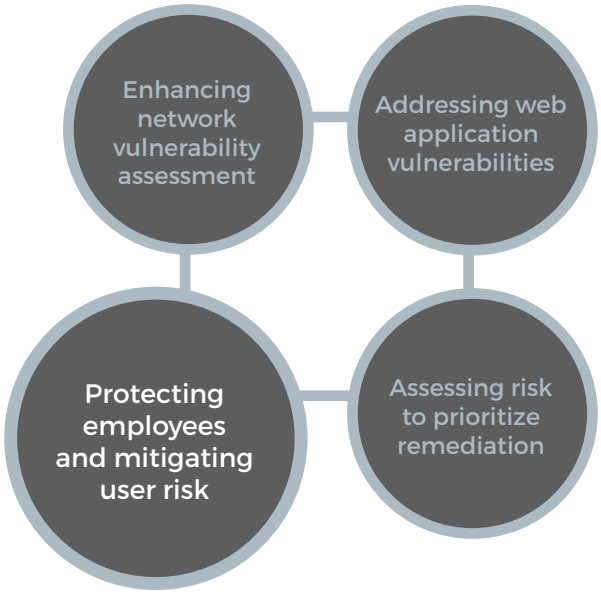
How Rapid7 Can Help

A phishing awareness program can reduce the success rate of phishing emails by educating employees on why phishing is harmful, training them on how to detect and report phishing attempts, and reinforcing the training through phishing simulation.

Rapid7 InsightPhishing is a powerful tool for managing phishing identification, analysis, and simulations.

InsightPhishing makes it easy for employees to report phishing attempts, so IT security groups can quickly analyze and block phishing emails and remediate any systems that have been affected. Additionally, reports showing patterns in phishing attempts help security teams identify weaknesses and quantify risk.

Finally, administrators can use InsightPhishing to create customized phishing emails and simulate targeted attacks on specific departments and individuals. Employees who are deceived into clicking on a link or submitting a form are alerted to theirs missteps and given gentle reinforcement of their anti-phishing training. This type of reinforcement has been shown to reduce clicks on phishing emails by as much as 64% (Ponemon Institute: *The Cost of Phishing & Value of Employee Training*).



InsightIDR provides centralized log management and offers User and Attacker Behavior Analytics to help security teams unify and search data, detect early signs of breaches, and highlight misconfigurations and risky user behaviors to proactively improve your organization's security posture.

Ready to start protecting and training your users? Discover the power of InsightPhishing and InsightIDR today.

4 ASSESSING RISK TO PRIORITIZE REMEDIATION

Today, incident response and IT operations groups are flooded with more alerts and vulnerabilities than they can possibly investigate and remediate. Vulnerability assessment programs must do a better job of prioritizing vulnerabilities correctly, so remediation efforts can focus on the highest-risk issues.

How Rapid7 Can Help

InsightVM calculates risk scores for every asset and vulnerability that it finds during a scan. The scores indicate the potential danger that the vulnerability poses to the enterprise based on factors such as prevalence of the vulnerability in the enterprise, the value of the information assets and systems being protected, the potential impact of interrupted service on business operations, and the likelihood that the vulnerability will be exploited by real attackers.

InsightVM also provides integrated public and propriety threat feeds to show users what assets are impacted by vulnerabilities that are being exploited actively.

This attacker-focused approach provides guidance on which vulnerabilities should be addressed immediately, and which ones can be deferred temporarily.

Familiar with **Rapid7 Metasploit?** It's the world's leading penetration testing tool, and it works in conjunction with InsightVM to keep you more secure: Metasploit allows IT and security organizations to simulate attacks to quantify their impact and establish which vulnerabilities pose the greatest risks to the enterprise, so these vulnerabilities can be the immediate foci of remediation activities.

You can start validating your vulnerabilities with insight from Metasploit in just minutes: Start your InsightVM 30-day free trial today.

ABOUT RAPID7

Rapid7 (NASDAQ:RPD) powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response, and log management for more than 7,000 organizations across more than 120 countries, including 52% of the Fortune 100.

To learn more about Rapid7 or get involved in our threat research, visit **www.rapid7.com**.

RAPID7