RAPID7

WHITEPAPER

4 Key Pillars of Modern Vulnerability Risk Management

A comprehensive approach to reducing vulnerabilities across your ecosystem

TABLE OF CONTENTS

Introduction: The Traditional Vision of Vulnerability Management Is Outdated

Time for a new perspective

A decade ago, most enterprises could get away with addressing vulnerabilities in silos. One team would scan servers and desktop computers on the enterprise network, looking for misconfigurations in systems and vulnerabilities in commercial software applications. When problems were discovered, they were thrown over the wall for system administrators and operations groups to fix. Application developers were responsible for policing internally developed web applications. Other specialists worried about the susceptibility of employees to social engineering attacks. Rarely was anyone responsible for analyzing how different types of vulnerabilities might interact to expose critical data and intellectual property.

That vision of vulnerability management is too inefficient and expensive for today's enterprise. Computing environments are far more complex. IT and security groups must monitor a much larger attack surface. Infrastructures and web applications can change on a daily, even hourly basis. Cybercriminals and hackers have learned how to exploit chains of weaknesses in systems, applications, and people. Traditional vulnerability management tools and practices are too limited, too siloed, and too slow to keep up with these challenges.

Security organizations must rethink their vulnerability management programs to monitor dynamic computing environments, respond in minutes, and address weaknesses in people as well as technology.

Toward a modern vulnerability risk management program

Security organizations must rethink their vulnerability management programs. They need to monitor complex, dynamic computing environments, and respond in minutes or hours when issues are discovered — not days or weeks. They need to address weaknesses in people as well as technology. Also, security professionals must be able to think like attackers in order to understand which vulnerabilities pose the greatest risks to the enterprise.

In this whitepaper, we will explore how enterprises can address these challenges and evolve toward a modern vulnerability risk management program using shared visibility, analytics, and automation.

We will discuss how they can:

- **Enhance traditional network vulnerability assessment to handle more complex computing infrastructures**
- **Achieve complete ecosystem visibility**
- **Strengthen their ability to test complex, rapidly changing web applications**
- **Increase resilience to phishing and other social engineering attacks**
- **Use penetration testing to assess overall risk and better prioritize remediation efforts**

Enhancing Network Vulnerability Assessment

Enterprises today need to step up their game

Network vulnerability assessment is changing: It is time to think about complete ecosystem visibility.

It is no longer enough to scan the corporate network quarterly or monthly for vulnerabilities on servers and desktops. Security teams must be able to monitor the entire attack surface, including cloud platforms and virtualized and containerized environments. Even more, they need to cope with the dynamic nature of these environments, where new instances of applications and services can be spun up on virtual machines at a moment's notice.

Operational issues are part of the picture, too. Because teams need to monitor more data on more types of endpoints and platforms, they have to minimize the number of new endpoint agents and assessment tools. If different tools are used for each computing platform, it becomes difficult to share data and achieve "single pane of glass" visibility. Finally, organizations need to ensure that vulnerabilities, once detected, can be remediated quickly, before they can be exploited by attackers.

Complete ecosystem visibility

One of the key principles for a modern vulnerability risk management program and the overarching practice of SecOps is "complete ecosystem visibility." That means integrating vulnerability assessment scanning solutions with virtual services like VMWare, and with Infrastructure as a Service (IaaS) platforms such as AWS and Azure. Why?

This integration enables the organization to obtain immediate insight into risks created by changes in the computing infrastructure. For example, in virtual environments, a vulnerability assessment agent can be embedded in the images of your instances. That way, every time a new component of the service is spun up, it can be scanned for vulnerabilities. This eliminates the window of exposure that would other-wise last until the vulnerability was detected in the next scheduled scan.

"Complete ecosystem visibility" involves integrating vulnerability assessment scanning solutions with virtual services, as well as IaaS platforms, applications, and other cloud environments.

Cloud environments pose a special challenge, because security organizations often aren't informed when new infrastructure is deployed on IaaS platforms. Vulnerability assessment tools can be integrated with AWS, Azure, and other cloud platforms to detect when new devices are deployed and automatically assess them. They can also ensure that golden images are hardened before deployment. For additional visibility, agents can be embedded in these images just as with virtual machines.

Simplified assessment

Security teams should be able to monitor more types of data on more types of endpoints without multiplying the number of agents and assessment solutions they use.

However, many devices have limited connectivity to the corporate network. Several are too sensitive to be scanned by traditional assessment methods, or require credentials that security may be hesitant to broadcast widely. But there is a solution: modern agents that can safely assess these devices, and send data back securely to a central vulnerability assessment tool.

A "universal agent" can make this approach even more scalable and sustainable by collecting a wide range of data from systems, endpoints, and virtual machines, and by sharing the results with multiple vulnerability assessment solutions.

Integrating scanning tools with internal ticketing systems automates the handoff of vulnerability tasks to the IT operations team, giving them access to more data, faster, with less chance of losing information.

Automating remediation workflows

The third key to agile vulnerability risk management is the automation of remediation workflows. Integrating scanning tools with internal ticketing systems automates the handoff of vulnerability data and tasks to the IT operations team. This automated handoff gives operations teams access to more data, faster, with less chance of crucial information being lost. It enables them to patch systems and fix misconfigurations quickly and accurately.

When members of the security team have visibility into vulnerability-related issues in the ticketing system, they can track progress, flag delays in critical remediation tasks, and provide additional support to the operations team. Security analysts can move beyond the stage of merely hoping for prompt fixes.

When it makes sense, remediation can be even further automated by integrating vulnerability risk management products with an orchestration tool. For example, security teams
can create and apply patches in concert with operations teams. Some organizations may choose to go even farther, allowing security teams to auto-patch systems by themselves, while being monitored and supported by the operations team.

Enterprises should automate as much of their remediation cycle as makes sense for their business. This not only shortens remediation cycles, but also helps security and operations teams work together harmoniously, giving them more time to focus on strategic tasks.

How can Rapid7 help you step up your network vuln assessment?

Our accompanying **solution guide** has the answers (and more).

Addressing Web Application Vulnerabilities

Rich web applications can be an Achilles heel

Most organizations are familiar with traditional dynamic application security testing (DAST) tools, which were originally designed to detect weaknesses in web applications built with older technologies like HTML, PHP, and Perl.

But these legacy tools are frequently unable to effectively test rich web applications built with HTML5, Action Message Format (AMF), Single Page Application (SPA) frameworks and libraries, and toolkits, services, and protocols such as JSON, REST, GWT, SOAP and XML-RPC. Typically, the tools cannot systematically assess the back ends and APIs of these applications. They also have trouble coping with custom parameters and non-traditional authentication processes. Often, they cannot crawl through multi-step workflows such as shopping cart sequences.

Long story short, these limitations mean that attackers can find ways into the back end of modern web applications, and often to the types of protected personal information and intellectual property that is most critical to the enterprise.

Understanding modern web applications

A modern vulnerability risk management program needs tools that can address these issues. For example, advanced DAST solutions are available that employ a "universal translator" to "understand" and test applications with sophisticated interfaces, APIs, and protocols. They can handle custom parameters and advanced authentication processes, and automatically detect vulnerabilities in complex application workflows like shopping carts.

The risk of continuous application deployment

Security groups are often hard-pressed to keep pace with the speed of change of production applications brought about by techniques such as agile development, continuous integration (CI), continuous delivery (CD), DevOps, and containers. These allow software development organizations to respond much faster to customer and business needs; new application code can be put into production on a weekly, daily, hourly, or even minute-by-minute basis.

Unfortunately, security is often left behind when application code moves swiftly from development, to staging, and into production. New code can be exposed to outsiders on the Internet for days or weeks without being scanned for vulnerabilities and coding errors — this opens the way for costly data breaches.

In fact, security teams may not even be aware that modified code has been deployed on cloud platforms and in containerized and virtualized environments.

Toward DevSecOps

One way to address these challenges is to work toward a DevSecOps approach. The concept is to adopt tools and processes that allow software developers, security staff, and the operations people who manage application deployment to work together and integrate security into every phase of the software development lifecycle (SDLC).

Toward this goal, vulnerability risk management can be integrated into the SDLC to cover development, testing, and staging environments as well as production systems. Vulnerability assessment agents can be embedded in the images of instances in virtual environments, so every virtual machine can be assessed for vulnerabilities and misconfigurations as soon as it is spun up. Vulnerability risk management tools can be integrated with container registries, so images can be assessed before they are deployed.

Vulnerability risk management can be integrated into the software development lifecycle to cover development, testing, and staging environments as well as production systems.

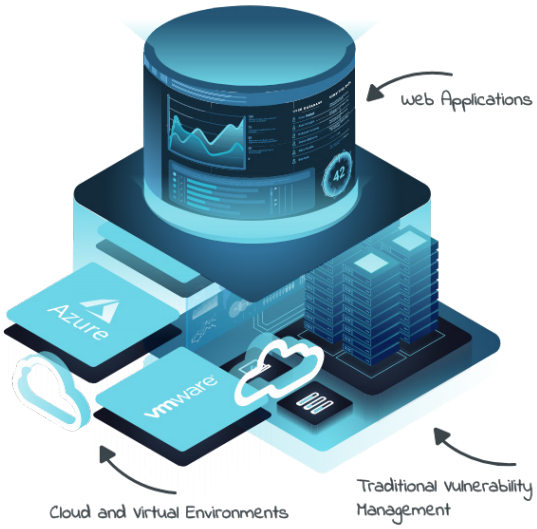
In addition, automation can be applied to CI and CD processes. For example, continuous integration tools can be configured to kick off automated tasks in the build pipeline. The CI tool can call the API of a vulnerability risk management or DAST product and cause it to check for vulnerabilities in the application code, down to the level of containers and virtual machines.

This SDLC-wide approach to securing software ensures that vulnerabilities are detected before an application build is promoted to the next level or put into production. That includes vulnerabilities to application-level threats such as SQL injection, XSS (cross-site scripting), and CSRF (cross-site request forgery) attacks, as well as OS, web server, and container vulnerabilities.

When issues are discovered in the coding or testing phases of the software development lifecycle, they can be sent to a ticketing and incident tracking system for immediate resolution by the application development team.

Including vulnerability risk management in DevSecOps processes will:

- **Reduce risk, by eliminating vulnerabilities before new code is exposed to attackers.**
- **Cut costs, by identifying security "defects" early in the software development lifecycle, when they are easier and less expensive to fix.**
- **Speed up the release of secure new features and applications by making security an integral part of the development process, rather than a hurdle to overcome at the end.**



Wondering how Rapid7 helps you graduate to the application layer of your VM program?

Our accompanying solution guide, **Modern Vulnerability Management with Rapid7**, can help.

Mitigate Risk at Every Layer

Don’t let anything — or anyone — be the weak link

Modern vulnerability risk management programs must not only increase resilience to phishing and other social-engineering attacks, they must also extend protection beyond critical infrastructure. When an attack is discovered, IT organizations need to be able to respond quickly.

Mitigating user risk with incident detection and response

Incident detection and response technologies can identify and reduce the risk of attacks on users. For example, user behavior analytics (UBA) and security analytics products monitor user behaviors and detect anomalies indicative of active compromise. Feeding vulnerability context to these tools enables them to more thoroughly investigate and prioritize incidents.

Information can also flow the other way. Analytics tools can identify groups that handle critical assets and individuals with compromised credentials, so these can take priority when assessing and remediating vulnerabilities.

Our solutions are built to help you address the challenges outlined in this whitepaper.

Learn more in our accompanying solution guide, **Modern Vulnerability Management with Rapid7**.

Assessing Overall Risk: Vulnerability Modeling and Penetration Testing

Severity scores and real risks

A key characteristic of a successful vulnerability management program is the ability to prioritize vulnerabilities correctly, so remediation efforts can focus on the highest-risk issues. This is particularly important today, when the high volume of vulnerabilities detected can be (and often is) overwhelming.

Common Vulnerability Scoring System (CVSS) ratings can be useful in some contexts, but they are essentially generalizations of potential severity across a wide range of industries and company types. They do not take account of the business context in individual industries, much less individual enterprises.

A modern vulnerability risk management program must supplement third-party rating systems like CVSS with two techniques:

1. A risk scoring system customized for the business context of the specific enterprise.
2. Penetration testing to validate the risk scores based on real-world conditions and existing compensating controls.

Risk scoring based on potential impact and likelihood of exploit

Advanced vulnerability risk management tools include a capability to model the real risk of vulnerabilities based on a variety of factors related to the potential impact of a vulnerability on a specific enterprise, and the likelihood of it being exploited.

Potential impact depends on factors such as the prevalence of the vulnerability in the enterprise, the value of the information assets and systems being protected, and the potential impact of interrupted service on business operations.

The likelihood of a vulnerability being exploited is linked to factors such as the accessibility of the vulnerability to attackers, the availability of exploit modules and malware kits tailored for the vulnerability, and the skill required to exploit the vulnerability.

These factors can be weighed and combined to create scores that reflect the real risk of each vulnerability for a specific enterprise much more accurately than generic severity rating systems.

Penetration testing to assess overall risk

Penetration testing, or pen testing, is often treated as a standalone activity, performed by a group of specialists who don't need to interact with the rest of the IT organization. But there is a strong argument to be made that pen testing should be coordinated with other elements of a modern vulnerability risk management program.

Here's our case.

Pen testing can identify vulnerabilities that appear to be severe, but pose relatively little risk to the organization. It can pinpoint others that might seem innocuous on their own, but that can be exploited in sequence to reach an attacker's target. For example, a pen tester might find that one vulnerability with a high CVSS severity score only affects a few endpoints that have no access to central databases, while another vulnerability with a lower score could be exploited by cybercriminals to access key intellectual property. Moreover, the first vulnerability might require extensive skills to exploit, while the second can be leveraged by a less experienced hacker with a kit.

Hence, pen testing should be treated as a core part of the modern vulnerability risk management program. Information from network scans, application tests, phishing simulations, and other sources of vulnerability information should be shared with testers, who can then use that information to perform tests that assess the actual risk to the organization posed by each type of vulnerability.

Also, the results of the pen tests must be analyzed and disseminated to the groups that prioritize and remediate vulnerabilities in the short term , and to the managers who make decisions about how to strengthen cybersecurity defenses over the long term.

Conclusion

With a modern vulnerability risk management program formed through the SecOps mindset, organizations can:

- **Step up their game with network scanning to include complete ecosystem visibility, simplified assessment, and automated remediation workflows.**
- **Better address web application vulnerabilities by analyzing more complex applications and by adopting DevSecOps practices to keep up with applications that can change daily or hourly.**
- **Mitigate user risks by linking incident detection and response capabilities with vulnerability risk management.**
- **Assess overall risk using customized risk scoring and pen testing to prioritize vulnerabilities based on their real risk to the specific enterprise.**

Evolving toward such a program requires thinking through the value of each area and finding opportunities to integrate the different areas.

But the rewards are dramatic, giving security groups the ability to:

- **Monitor today's vastly expanded attack surface.**
- **Keep up with quickly changing infrastructure and applications.**
- **Work collaboratively with IT operations and application development groups to identify and remediate vulnerabilities of all kinds, faster.**
- **Reduce the ability of attackers to exploit the largest attack vector in most organizations: the users.**
- **Accurately determine which vulnerabilities pose the greatest risk to the enterprise, to make best use of remediate resources in the short term, and to focus on the most effective defenses in over the long term.**

How does Rapid7 fit in the picture?

To learn more about how to evolve your vulnerability risk management program, visit **www.rapid7.com/vm**.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on Twitter.