RAPID7

VULNERABILITY MANAGEMENT BUYER'S GUIDE

CONTENTS

01 INTRODUCTION

Exploiting weaknesses in browsers, operating systems, and other third-party software to infect end user systems is a common initial step for security attacks and breaches. Finding and fixing these vulnerabilities before the attackers can take advantage of them is a proactive defensive measure that is an essential part of any security program.

Vulnerability management (VM) is the process of identifying, assessing, and remediating vulnerabilities based on the risk they pose to your organization. The core technology component of this process is typically a vulnerability scanner, which discovers assets connected to your network and scans them for vulnerabilities such as the Heartbleed Bug. However, modern vulnerability management programs increasingly make use of agents to get live vulnerability data from devices, particularly endpoints and devices that are difficult to traditionally scan. They also need to consider application and user vulnerability assessment.

This expansion beyond traditional network scanning is driven by the modern network. Today, corporate networks are constantly changing and expanding, often without explicit approval from the security team. So working together with other internal teams is critical. A modern vulnerability management program needs to go beyond just scanning and fixing; it should help automate the discovery of assets across the cloud, virtual, and application development environments, as well as automate the prioritization and remediation of these vulnerabilities as much as possible.

The four essential components of an effective vulnerability management program:

Prepare: Start by defining the scope of your VM program, including what you will scan, how, and how often. You also need to identify what are the most important assets, who owns these assets, and where they are located.

Assess: Scan your network for vulnerabilities, insecure device and software configurations (or "misconfigurations"), compliance with internal and external security policies, and other mitigating controls in place.

Remediate: Prioritize vulnerabilities for remediation based on information about the threat landscape and how critical the asset is to the business, and then communicate the effort required to the person doing the remediation.

Track Progress: Finally, you need to know how you're doing in improving the effectiveness of your VM program. You can do this by establishing a baseline, setting metrics for success, and tracking progress towards your goals

02 KEY COMPONENTS

Solution Architecture

The solution architecture lays the groundwork for your VM program and can affect your ability to optimize scanning performance and quickly scale your deployment.

Flexible Deployment

Every organization's systems and network infrastructure are different; your VM solution should provide flexible deployment options and full control over scanning. The ability to optimize your VM solution for your organization's specific needs is critical for increasing the speed and accuracy of your assessments.

Does the solution's architecture provide flexibility to tune scanning configuration for optimal performance?

Distributed Scanning

Managing scans from a central location and aggregating scan data increases your VM program's efficiency and reduces impact on your network. A distributed architecture includes a central console for managing operations, reporting, and administration, with multiple remotely deployed scan engines to cover the entire IT environment.

Does the solution support centralized management of distributed scan engines?

Internal & External Scanning

Internal scanning assesses the security of your network from inside the firewall; external scanning is performed remotely from the outside. Using both internal and external scanning gives you a complete view of your organization's risks.

Can the solution perform both internal and external scanning?

Agent Based Assessment

Agents can be used to continuously monitor assets that may be challenging to reach via traditional scanning, such as remote low-bandwidth networks or remote workers. They allow in-depth scanning without supplying system credentials, and they can also be embedded in virtual or cloud golden images to automatically provide visibility to new infrastructure as it's spun up. A vendor with multiple products should have a "universal agent" approach, where a single agent can collect data for multiple solutions to ease deployment.

Does the vendor allow agent based scanning? How lightweight is the agent? How easy is it to automate agent deployment or connection? Can the agent be used for multiple solutions?

Endpoint Monitoring

As more organizations have focused on securing their servers, attackers have adapted by targeting users and endpoints. Endpoints and users are a difficult area of the network to manage, especially for companies with remote workers or contractors who rarely connect to the network. A VM solution should continuously monitor these devices even when they are off the network, typically through the use of agents. Agents need to be easy to install and lightweight so as not to take up much network bandwidth.

How does the solution monitor remote users and endpoints that disconnect from the network? Can users easily create dashboards to understand the risk of endpoints?

Scalability

As your environment grows, your VM solution also needs to grow, quickly and easily. Ideally, you should be able to increase capacity by adding scan engines to your existing deployment at little or no additional cost. For larger environments, the solution vendor should have proven experience with similar size deployments. The ability for a vendor to offload some or all data processing to a cloud platform also makes scaling up to larger environments and datasets much easier.

Can the solution scale quickly and easily? Do additional scan engines need to be purchased for larger environments? Does the vendor offer a cloud platform for processing data and analytics?

Network Vulnerability Assessment

Network vulnerability assessment is an important technology for identifying risks in your environment, but an effective security program requires a comprehensive solution that does more than list vulnerabilities.

Discovery

You need to know what assets you have before you can assess and manage the risk they pose. Scanning your entire network to discover and inventory all assets, including their OS, applications, and services, is foundational to an effective VM program. Assets should be automatically categorized based on multiple attributes, not just the IP address, and be easily tracked over time.

Does the solution automatically discover and categorize assets? Can the solution track assets even if their IP addresses change?

Unified Vulnerability & Configuration Assessment

Finding assets, vulnerabilities, and misconfigurations in a single assessment scan minimizes impact on your network, gives faster scan times, and reduces management overhead. The solution should provide unified user interface and reporting for vulnerability and configuration assessments for a complete view of your security risk and compliance posture.

Can the solution perform discovery, vulnerability, and configuration assessments in a single unified scan?

Container Assessment

Containers provide incredible flexibility for application and DevOps teams to quickly roll out and update apps, but present unique security challenges; they're often deployed without the security team's knowledge, and vulnerabilities in container images can impact multiple applications if not addressed quickly. Modern VM solutions should be able to assess container images, as well as automatically identify container hosts to provide visibility on where containers are deployed.

Can the solution integrate with private and public container registries to assess images? Does the solution automatically identify container hosts? How is container assessment priced compared to vulnerability assessment?

Authenticated Scans

Deep scanning using credentials to authenticate into assets gives you greater visibility into risks and provides additional information such as device configurations. In contrast, remote scanning only provides an outsider's view of assets. Look for a solution that supports authenticated scans with a wide range of OS, database, network, and application layer credentials.

Does the solution support authenticated scans with the ability to configure and manage credentials centrally? What credential management products does the solution integrate with?

Virtual & Cloud Environments

Virtualization and cloud technologies enable organizations to spin up assets on demand, but pose a challenge as many solutions don't differentiate scanning of real and virtual assets. The solution should be able to dynamically discover and assess the risk of virtual and cloud assets to secure these environments.

Can the solution automatically discover and assess the risk of virtual and cloud assets through direct integration?

Network Changes

Most organizations perform monthly or quarterly vulnerability scanning; however, modern networks change minute to minute, with new devices joining the network and new vulnerabilities being released outside of regularly scheduled windows. An effective VM tool will be able to detect new devices and vulnerabilities between your scheduled scans, with minimal false positives.

Can the solution detect and assess new devices that join the network in between scans?

Scanning Frequency

Changes in your network are occurring frequently. By establishing a regular scan schedule, you can ensure that security risks are found and fixed in a timely manner. Scans should be scheduled to run automatically on a monthly, weekly, or even daily basis, and within specific time windows to minimize network disruption.

Does the solution support a calendar for defining scan schedules and approved time windows?

Prioritization & Remediation

A common challenge among security teams is determining which vulnerability and assets to focus on first and establishing an effective work flow to address them as soon as possible.

Risk Scoring

With vulnerabilities in an organization reaching thousands or even millions, you need an advanced risk scoring algorithm to determine which systems to fix first. Simply using the industry standard CVSS is not sufficient for effective prioritization. The risk score should incorporate threat metrics such as exposure to exploits and malware kits, and how long the vulnerability has been available to automate the prioritization of vulnerabilities.

Does the solution provide a granular risk score that takes into account threat intelligence and temporal metrics?

Business Context

An effective vulnerability prioritization approach requires additional information about your assets, such as where it's located, what its role is, who owns it, and its relative importance. This contextual business intelligence enables you to prioritize business-critical systems and data for remediation. The solution should also be able to automatically modify risk score based on an asset's criticality.

Can the solution prioritize remediation efforts for business-critical assets?

Vulnerability Validation

Combining scanning with penetration testing allows you to validate whether the identified vulnerabilities pose actual risk to your organization. This allows you to prioritize remediation and create exceptions for vulnerabilities that could not be exploited. The integration between VM and penetration testing solutions should be automated and data should flow seamlessly between the two.

Does the solution provide built-in integration with a popular penetration testing tool for vulnerability validation?

Can you return vulnerability validation results back into the solution for risk prioritization and management?

Remediation Planning

After you find and prioritize risks, someone needs to fix them. For an efficient remediation work flow, use reporting that allows you to create a plan for the top steps to reduce overall risk. This should include the actions required in language that the person performing the remediation will understand, time required for completion, and related patches, downloads, and references.

Does the solution provide prioritized remediation plans that include IT operations level instructions?

Remediation Assignment

Who performs remediation can depend on where the asset is located, its role, and who owns it. A delay between finding the risk and assigning remediation tasks means the asset is unprotected for longer. Remediation plans should be automatically sent to the asset owner according to the business context.

Can the solution automatically assign remediation tasks after each scan according to the business context?

Remediation Analytics

Remediation is a continuous process that can always be improved; a good VM solution should help identify weak points in the vulnerability remediation work flow so you can get ahead of potential problems, and understand your progress

Does the solution allow you to track remediation progress? Does the solution provide data around who has been most/least effective with remediation?

Reporting

Vulnerability scans can produce an overwhelming amount of information, so it's important to be able to identify what's really important and present it in a clear, concise, and actionable format.

Consolidated Reporting

By aggregating data collected from every scan engine and agent for reporting, you can centrally manage prioritization and remediation across your entire network, as well as analyze security risk and compliance trends. The solution should present vulnerabilities, configurations, policy compliance, and other asset information such as installed applications in a single unified interface.

Does the solution aggregate scan data for consolidated reporting?

Does the solution provide a single, unified interface for vulnerabilities, configurations and asset information?

Report Templates & Customization

Out-of-the-box report templates should be available to meet a variety of users' needs, such as executive level reports to show the risk posture across the organization and IT operations level reports to detail remediation steps. The templates should be fully customizable and support a variety of formats.

Does the solution provide both pre-configured and fully customizable report templates for a variety of audiences?

Report Scheduling & Distribution

The faster reports are sent, the quicker vulnerabilities are fixed. The solution should allow reports to be generated and distributed ad hoc, automatically after every scan, or on a regular schedule, and allow you to specify who the reports are delivered to via email, as well as who can access them via the interface.

Does the solution provide report scheduling capabilities?

Can you specify report access via email and within the interface?

Asset and Vulnerability Filtering

Which systems may be affected by a new "zero-day" vulnerability? Asset and vulnerability filtering can be used to answer complex security questions and quickly gain insight into risks across your organization. You should be able to filter vulnerabilities in reports by both severity and categories based on platform, software, protocol, vulnerability type, and service affected.

Does the solution support asset and vulnerability filtering by attributes, category, and severity?

Asset Groups

Assets in the solution should be able to be grouped by technical attributes such as the operating system installed, or user-defined attributes like location, owner, or criticality. Look for a solution that provides the ability to dynamically update these groups based on newly discovered assets and asset information, and allows you to create reports based on these groups.

Can you automatically categorize assets based on multiple attributes and create reports for these asset groups?

Dashboards

Vulnerability data provides a lot of information about risks present within your network, but visualizing and acting on that information can be a challenge. Dashboards help technical and non-technical team members understand at a glance how vulnerabilities are affecting security. Effective dashboards are easily customize-able and query-able, and update as information is identified.

Does the solution have dashboards that are easy to use and customize?

Database Queries

Sometimes you may need to perform advanced analysis on vulnerability and asset data specific to your organization's or security team's needs. The solution should support running SQL queries directly against the reporting data model and output the results in a format for creating pivot tables, charts, and graphs.

Does the solution allow SQL queries to be run against the reporting data model?

Compliance & Configuration Assessment

Insecure configurations and missing controls are a leading source of risk, which is why some VM solutions also provide the ability to scan for configurations, controls, and policy compliance.

Compliance Assessment

Vulnerability assessment is a key requirement for many security standards and regulations, for example Payment Card Industry Data Security Standards (PCI DSS). Pre-built scanning and reporting templates makes the process of showing compliance with such policies easy and efficient. For PCI compliance, the vendor should be an Approved Scanning Vendor (ASV).

Does the solution provide templates for assessing policy compliance?

Is this a separately installed product or module with additional costs?

Configuration Assessment Ensuring your systems are configured securely according to industry benchmarks and best practices is a critical component in a unified security assessment solution. Configuration and compliance assessments should be performed at the same time as vulnerability scanning with the results presented in a unified interface. In addition, configuration policies should be fully customizable via the user interface to meet your specific requirements.	Does the solution perform configuration and compliance assessments in a single scan with unified reporting? Can you centrally manage and modify policies within the user interface?
Controls Assessment Most organizations invest significant amounts of time and resources into putting mitigating controls in place to defend against the real and current threats they face. Assessing how well these controls have been deployed and how effective they are based on industry best practices helps you to identify any gaps in your security program. Look for a VM solution that goes beyond compliance to monitor the effectiveness of your controls.	Does the solution track your controls deployment and effectiveness?

Administration

Role-Based Access Different groups of users within your organization may need different levels of access to scan data. The solution's role-based access controls (RBACs) should support pre-defined roles, the ability to modify or add new roles, and the set permissions for functionality such as modifying scan configuration, asset grouping, reporting, and other administrative functions.	Does the solution support both pre-defined and custom role-based access? Are you able to set permissions for user functionality and visibility of devices?
Exceptions Management Occasionally you'll come across a vulnerability that either cannot be fixed or is considered an acceptable risk to the business. The work flow for submitting this exception for approval should be automated for easy auditing and management. You should be able to create exceptions at the instance, asset, scan group or global level, and add a reason for the exception.	Does the solution provide an approval work flow for vulnerability exceptions? Can you configure user permissions for submission, approval, and expiration?
Application Updates Regular application updates ensure that you can take advantage of the latest features and performance enhancements. You should be able to choose between automatic and manual updates, with a process for updating the application in offline environments.	Does the solution support automatic, manual, and offline application updates?
Coverage Updates To keep up with a constantly changing threat landscape, you'll need a VM solution that provides frequent updates for new vulnerability checks. For critical coverage updates, such as Microsoft Patch Tuesday vulnerabilities, the vendor should offer service-level agreements for guaranteed turnaround.	Is there a regular cadence for new vulnerability checks, including an attached SLA for critical vulnerabilities?

Integration

Virtual & Cloud Environments

You can integrate your VM solution with virtual and cloud platforms such as VMware and Amazon Web Services (AWS) to enable dynamic discovery and assessment of assets in these environments. Look for a vendor that is officially certified by the virtual or cloud platform provider, and offers pre-built integration for quick and easy setup with reduced management overhead.

Does the solution support integration with virtual and cloud environments?

IT Security Solutions

Many VM solutions provide pre-built integrations with other security solutions in your environment, such as network topology tools, IDS/IPS, IT GRC and SIEM products. These integrations can provide centralized reporting and management, and the ability to correlate additional contextual information about an asset to increase alert accuracy and reduce false positives.

Does the solution support integration with other security solutions?

Enterprise Ticketing System

If your organization already uses a ticketing system like ServiceNow, then integration allows you to leverage your existing service request work flow for vulnerability remediation. This enables your IT operations team to quickly resolve or escalate issues, and the business to track their progress.

Does the solution support integration with enterprise ticketing systems?

Does the solution provide the ability to customize ticket content and depth?

Custom Integrations

In some situations, you may need to develop a new integration or make enhancements to an existing integration for your organization's specific requirements. Your VM solution should provide access to a two-way public API with all major functionality available through the interface.

Does the solution offer a two-way public and language-independent API?

Are there any additional costs or fees associated with using the API?

Vendor

Market Analysis

Choose a vendor that is well-known and proven in the industry. Market research organizations and industry publications like Gartner and SC Magazine provide analysis and comparisons of VM solutions. Look for a vendor who is consistently rated an industry leader in the last few years.

List any reviews or ratings from market analysts over the last five years.

Company Focus

For a best-of-breed solution, choose a vendor that is committed to VM as a core product offering and not just as an acquisition for their portfolio. They should be continuously investing in innovations in this space and be able to articulate their product roadmap and vision for future developments.

List major innovations and developments in the solution over the past year.

Customer Satisfaction Not all customer support is created equal. Look for vendors that offer a 24x7 two-tier support model to ensure that your issues are resolved by the first person you talk to as much as possible. Ask to talk to or get references from the vendor's other customers with businesses similar to yours.	List customer satisfaction scores and first call resolution rate.
Training & Certification Formal product training and certification can help you get the most out of the product, reduce time spent troubleshooting, and drive greater productivity. Certifications also help your organization identify prospective employees who are able to get up and running with your VM solution sooner.	Does the vendor offer virtual and on-site product training and certification?
Managed Services Professional managed services can help you maximize your return on investment by tweaking your deployment, scan configuration, processes and reporting to meet best practices. They can also help you build custom scripts, interfaces and integrations for your organization's specific requirements.	Does the vendor offer services for deployment and optimization?
Application and User Vulnerability Assessment Tools Network vulnerability assessment is just one piece of a modern vulnerability management program. The vendor you partner with should provide solutions that help you assess application and user vulnerabilities as well, and these solutions should all be integrated to help build a cohesive vulnerability management program.	Does the vendor provide products for application and user vulnerability assessment? Are these products integrated?

03 OTHER CONSIDERATIONS

Pricing

Pricing and licensing for VM solutions can vary greatly —some vendors offer a perpetual license where you pay upfront with ongoing charges for maintenance and support, while others offer subscription-based services where you pay the whole cost of the solution on an annual or monthly basis. When calculating the ROI, take into account the total cost of ownership, as well as any hidden costs for components or modules you may need to add over time. Training and deployment is often recommended to get the most out of a vulnerability management program, so those costs should also be considered.

Some open-source or low-end tools provide a single vulnerability scanner with limited functionality at no or very low upfront cost. However, you'll probably find that your ongoing costs for maintaining a VM program is much higher as administration, reporting, and customization becomes more time and resource consuming with such tools.

Metrics for Success

Are your VM efforts making a difference? Here are some metrics to help you track progress and spot areas for improvement:

- Number of vulnerabilities identified and remediated
- Length of time to identify and resolve high-risk vulnerabilities
- Number of previously unknown assets/services/applications discovered
- Time and cost to complete prioritization and remediation process
- Percent reduction in error rate of tasks handed off to IT operations
- Time and cost to prepare for compliance audits
- Percent increase in compliance audits passed successfully
- Length of time spent on admin work and reporting

About InsightVM

InsightVM is Rapid7's premier vulnerability management solution, providing a fully available, scalable, and efficient way to collect vulnerability data, turn it into answers, and minimize your risk. InsightVM is the evolution of our award-winning Nexpose product, and utilizes the power of the Rapid7 Insight Platform, our cloud-based security and data analytics solution.

The Rapid7 Insight Platform brings together Rapid7's library of vulnerability research, exploit knowledge, global attacker behavior, internet-wide scanning data, exposure analytics, and real-time reporting. InsightVM uses this platform to enable IT and security teams to collaborate and partner together through the use of continuous endpoint monitoring, dynamic dashboards, and end-to-end remediation work flows.

As a core component of Rapid7's security data and analytics platform, InsightVM promotes an active, analytics-driven approach to cybersecurity. Try it for free today at: www.rapid7.com/insightvm.

In addition to InsightVM, Rapid7 also offers Nexpose, an award-winning on-premise vulnerability management product. Learn more about all of our vulnerability management solutions at www.rapid7.com/solutions/vulnerability-management.

About Rapid7

With Rapid7, technology professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.