RAPID7

BUYER'S GUIDE

Evaluating Vulnerability Assessment Solutions

How to define your needs
and choose the right vendor

TABLE OF CONTENTS

Introduction

Vulnerability management (VM) is the process of identifying, evaluating, treating, and reporting security vulnerabilities in business processes, web applications, and systems (as well as the software that runs on them). This process needs to be performed continuously in order to keep up with new systems being added to networks, changes made to systems and applications, and newly discovered vulnerabilities over time.

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

Solution Architecture

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

A modern VM program, in turn, must monitor a complex, dynamic computing environment, and respond in minutes or hours when issues are discovered. It should enhance traditional network vulnerability assessment to handle more complex computing infrastructures. This enables you to:

- Achieve complete visibility of your ecosystem
- Strengthen your ability to test complex, rapidly changing web applications
- Increase resilience to phishing, other social engineering attacks, and abnormal user behaviors
- Use penetration testing to assess overall risk and better prioritize remediation efforts

Read more about Building a Modern Vulnerability Management Program.

The core technological component of this process is typically a vulnerability assessment (VA) tool, which discovers assets, endpoints, and containers connected to your local, virtual, and cloud environments. It then scans them via engines, agents, and container registries for vulnerabilities. Modern programs are increasingly leveraging 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 increasing complexities of 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 VM program, which has a VA solution at its core, needs to go beyond just scanning and fixing; it should help automate and orchestrate critical tasks (such as: the discovery of assets across cloud, virtual, and application development environments) as well as leverage that automation to accelerate the prioritization, remediation, and (when appropriate) containment of these vulnerabilities or assets.

The ideal VM partner and associated solutions help enterprises address these challenges and adapt to modern security environments using shared visibility, analytics, and automation—principles core to the practice of SecOps.

Four essential steps to execute an effective Proof of Concept (POC) for a Vulnerability Assessment tool:

Prepare: Start by defining the scope of your vulnerability assessment (VA) initiative, including what you need to assess, how, and how often. Identify cumbersome and repetitive tasks that could potentially be improved by the automation capabilities of the solution. You also should be documenting the most important assets, who owns these assets, and where they are located.

Assess: During the POC, assess your network for vulnerabilities, insecure device and software configurations (or "misconfigurations"), compliance with internal and/or external security policies, and other compensating controls in place.

Remediate: Prioritize vulnerabilities for remediation based on intelligence on the threat landscape and how critical the asset is to the business. Ensure that the tool assists you in effectively implementing automated processes while communicating with the people and technologies involved in executing remediation.

Track Effectiveness: Finally, determine if the VA tool will be effective in impacting your overall VM program. You can do this by establishing a baseline, setting metrics for success (e.g. risk reduced, time saved), and tracking progress towards your goals.

01 Key Components

Flexible Deployment

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

ASK VENDORS

- Does the solution's architecture provide flexibility to tune scanning configuration for optimal performance?
- Do additional solutions need to be purchased to leverage automation?

Distributed Scanning

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

ASK VENDORS

- Does the solution centralize 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.

ASK VENDORS

- 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 can also be embedded in virtual or cloud golden images to automatically provide visibility into new infrastructure as soon 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.

ASK VENDORS

- Is the vendor's agent lightweight?
- How easy is it to deploy?
- How much value does it provide?

Endpoint Monitoring

As more organizations have focused on securing their servers, attackers have adapted by targeting users and endpoints. Endpoints and users are difficult areas of the network to manage, especially for companies with remote workers or contractors who rarely connect to the network. A VA solution should continuously monitor these devices even when they are off the network, ideally through the use of agents. Agents should be simple to deploy using your software management and orchestration tools and possess a small footprint so as to not impact network performance.

ASK VENDORS

- How does the solution monitor remote users and endpoints that disconnected from the network?

Scalability

As your environment grows, so should your VA solution. 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 similarly-sized deployments. The ability for a vendor to offload some or all data processing to a cloud platform also makes scaling to large environments and datasets much easier.

ASK VENDORS

- Can the solution scale quickly and easily?

Network Vulnerability Assessment

Network vulnerability assessment is important for identifying risks in your environment, but an effective security program requires a comprehensive solution that does more than just 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 vulnerability management program. Assets should be automatically categorized and tracked based on multiple attributes, and not just their IP addresses.

ASK VENDORS

- Does the solution automatically discover and categorize assets?

Unified Vulnerability & Configuration Assessment

Finding assets, vulnerabilities, and misconfigurations in a single assessment 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.

ASK VENDORS

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

Container Assessment

Containers provide incredible flexibility for application development and DevOps teams to quickly roll out and update apps, but they 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 VA solutions should be able to identify container hosts, assess container images stored in registries, and assess containers during the build process by being integrated in the team's CI/CD tool.

ASK VENDORS

- Can the solution automatically identify container hosts, assess container images stored in registries, and integrate with your CI/CD tool?

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.

ASK VENDORS

- 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 they pose a challenge as many solutions don't differentiate scanning of real and virtual assets. Your solution should be able to dynamically discover and assess the risk of virtual and cloud assets to secure these environments.

ASK VENDORS

- 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 VA tool will be able to detect new devices and vulnerabilities between your scheduled scans with minimal false positives.

ASK VENDORS

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

Scanning Frequency

Changes in your network are constantly occurring. 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.

ASK VENDORS

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

Prioritization

A common challenge among security teams is determining which vulnerabilities and assets to focus on first based off of their criticality to your business and what attackers are actually doing in the wild.

Risk Scoring

With vulnerabilities in an organization reaching thousands or even millions in number, 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 (accurate) prioritization of vulnerabilities.

ASK VENDORS

- 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.

ASK VENDORS

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

Threat Feeds

In addition to the exploitability of identified vulnerabilities, it's also critical to consider their timeliness. Forward-thinking VA solutions incorporate threat intelligence and knowledge of current attacker methods to help prioritize truly critical vulnerabilities — especially in response to zero-day threats.

ASK VENDORS

- Is there an additional cost for access to threat intelligence?
- Is the intelligence tailored to represent what is relevant for your environment?

Vulnerability Validation

Combining scanning with penetration testing allows you to validate whether identified vulnerabilities pose actual risk to your organization. This allows you to prioritize remediation and create exceptions for vulnerabilities that could not be exploited.

ASK VENDORS

- Does the VA vendor also offer a penetration testing tool for vulnerability validation, allowing you to have a single support and billing contact?

Remediation

Remediation is the most critical step of a vulnerability management program. Unfortunately, this is also where many programs fall flat. Solutions must assist in fostering necessary—yet elusive—collaboration between security, IT, and development teams to address vulnerabilities as soon as possible.

Automated and IT-Integrated Patching

The patching process is often comprised of back-and-forth tasks between security and IT teams. Automation can offload the more repetitive steps from your workload by integrating with IT's existing tools and workflows, such as ticketing systems and patch management softwares.

ASK VENDORS

- Does the solution offer built-in integrations withyour existing security and IT solutions to streamline the patching process?

Automated Containment

Not every vulnerability can be remediated upon discovery. With the automated implementation of compensating controls, you can temporarily (or permanently) decrease your exposure from these vulnerabilities through existing network and endpoint systems.

ASK VENDORS

- Can the solution leverage your existing firewall, network access control (NAC), and endpoint detection and response tools to contain threats?
- Does the solution support both full isolation of assets and selective containment of specific services?

Planning for Remediation

After you find and prioritize risks, it's important to also fix them. To create an efficient remediation process, use reporting that pinpoints the most actionable and impactful steps to reduce overall risk. This should include the actions required in the terminology and language that the person performing the remediation will understand, as well as time required for completion and related patches, downloads, and references.

ASK VENDORS

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

Role Assignment

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

ASK VENDORS

- 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 VA solution should help identify weak points in the vulnerability remediation workflow so you can get ahead of potential problems, and understand your progress.

ASK VENDORS

- Does the solution allow you to track remediation progress?
- Does the solution provide data around efficiencies (or inefficiencies) in the remediation process?

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.

ASK VENDORS

- Does the solution provide a unified view of vulnerabilities, configurations, and asset information?

Report Templates & Customization

An effective vulnerability prioritization approach requires additional information about your assets, such as where they're located, their role, who owns them, and their 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.

ASK VENDORS

- Does the solution provide scheduling capabilities for context-rich reporting?

Asset and Vulnerability Filtering

Which systems might 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 severity, platform, software, protocol, vulnerability type, and service affected.

ASK VENDORS

- 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.

ASK VENDORS

- Do you need to manually check that a vulnerability was correctly remediated?

Remediation Validation

When the IT team reports that a vulnerability has been remediated, the solution should be able to automatically validate that the issue has been resolved. In the event that remediation efforts are unsuccessful, the solution should automatically re-open the task in the IT team's ticketing solution.

ASK VENDORS

- Do you need to manually check that a vulnerability was correctly remediated?

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 both technical and non-technical team members understand how vulnerabilities are affecting security posture at a glance. The most effective dashboards are easily customizable and query-able, and update in real time as information is identified.

ASK VENDORS

- 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.

ASK VENDORS

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

Compliance & Configuration Assessment

Insecure configurations (i.e. "misconfigurations") and missing controls are a leading source of risk, which is why some vulnerability assessment 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 make the process of showing compliance with such policies easy and efficient. For PCI compliance, the vendor should be an Approved Scanning Vendor (ASV).

ASK VENDORS

- 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 the vulnerability assessment, 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..

ASK VENDORS

- Does the solution perform configuration and compliance assessments in a single scan with unified reporting?

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 VA solution that goes beyond compliance to monitor the effectiveness of your controls.

ASK VENDORS

- Does the solution track your compensating 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 permissions for functionalities such as modifying scan configuration, asset grouping, reporting, and other administrative functions.

ASK VENDORS

- Does the solution support both pre-defined and custom role-based access?

Exceptions Management

Occasionally you'll come across a vulnerability that either cannot be fixed or is considered an acceptable risk to the business. The workflow for submitting this exception for approval should be automated for easy auditing and management. You should also be able to create exceptions at the instance, asset, scan group, or global level, and add reasons for the exception.

ASK VENDORS

- Does the solution provide an approval workflow for vulnerability exceptions?

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.

ASK VENDORS

- 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 VA 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 (SLAs) for guaranteed turnaround.

ASK VENDORS

- Is there a regular cadence for new vulnerability checks, including an attached SLA for critical vulnerabilities?

Integration

Virtual & Cloud Environments

You can integrate your VA solution with virtual and cloud platforms such as VMware, Amazon Web Services (AWS), and Microsoft Azure 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 integrations for quick and easy setup without the management overhead.

ASK VENDORS

- Does the solution support integration with your virtual and cloud environments?

IT Security Solutions

Many VA 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..

ASK VENDORS

- Does the solution support integration with other security solutions?

Enterprise Ticketing Systems

If your organization already uses a ticketing system like Atlassian Jira or ServiceNow, technology integrations allow you to leverage your existing service request workflow for vulnerability remediation. This enables your IT operations team to quickly resolve or escalate issues for better tracking.

ASK VENDORS

- Does the solution support integration with enterprise ticketing systems?

Automation and Orchestration Tools

Security automation and orchestration tools are rapidly becoming the glue that hold security programs together. When evaluating new VA solutions to add to your technology stack, ensure that the solution integrates with your automation and orchestration solutions.

ASK VENDORS

- For more advanced use cases, does the solution integrate with robust automation and orchestration solutions?

RESTful API

Make the most of your existing investments in security: When you want to create your own custom integrations or workflows, ensure that your VA solution offers a RestFul API that follows the OpenAPI v2 specification to ensure flexibility and interoperability.

ASK VENDORS

- 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 analyses and comparisons of vulnerability assessment (sometimes referred to as vulnerability risk management, or VRM) solutions. Look for a vendor who is consistently rated an industry leader in the last few years.

ASK VENDORS

- Are any reviews or ratings from market analysts available from the last five years?

Company Focus

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

ASK VENDORS

- Do I know of any 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 24/7, two-tier support model to ensure that your issues are resolved by the first person you talk to. Ask to speak with or get references from the vendor's other customers who conduct businesses similar to yours.

ASK VENDORS

- How does the solution's customer satisfaction scores and first call resolution rate fare?

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 VA solution sooner.

ASK VENDORS

- Does the vendor offer virtual and on-site product training and certification?

Deployment Services

Professional 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.

ASK VENDORS

- Does the vendor offer services and best practices 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.

ASK VENDORS

- Does the vendor provide products for application and user vulnerability assessment?
- Are these products integrated?

02 Additional Considerations

Pricing

Pricing and licensing for vulnerability assessment (VA) 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 with such tools, ongoing costs for maintaining a vulnerability management program become much higher as administration, reporting, and customization becomes more time and resource consuming.

Managed Service

An ideal VA solution should help your team be more efficient, not monopolize (precious) time. In some cases — even with the best technologies — your team may simply not have the capacity to run a vulnerability management program. If that's the case, look for vendors who provide a managed service offering. The managed vulnerability management service should be built on a VA tool that meets the criteria outlined in this guide, and the criteria set by your organization.

Metrics for Success

Are your vulnerability management 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
- Measure of risk and its change over time

A Vulnerability Assessment Tool for Your Modern Ecosystem

And now, a quick plug from us here at Rapid7:

InsightVM from Rapid7 utilizes the power of the Insight platform and the heritage of our award-winning Nexpose solution to help you tackle your modern vulnerability assessment challenges. With InsightVM, you gain complete visibility of your complex ecosystem, prioritize risk using attacker analytics, and remediate with SecOps agility so that nothing is left unseen across your cloud, virtual, remote, local, and containerized infrastructures.

“Rapid7 has already implemented what VRM will look like in the future.”

— The Forrester Wave™: Vulnerability Risk Management, Q1 2018

By leveraging InsightVM’s advanced analytics and automation and orchestration technology, you can discover vulnerabilities in real time and quickly determine their severity in the context of your business for more actionable prioritization. Then, remediation or containment is simplified and automated through integration with your IT team’s existing workflows and tools — a process made easy by InsightVM’s extensive technology integrations.

To experience InsightVM in your environment, sign up for a 30-day free trial at:

www.rapid7.com/try/insightvm

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.

To learn more about Rapid7 or get involved in our threat research,

visit www.rapid7.com.