Vulnerability Management Buyer's Guide

Buyer's Guide

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 a vulnerability scanner, which discovers assets connected to your network and scans them for over 60,000 known vulnerabilities, for example the Heartbleed Bug.

With increasingly complex IT environments, vulnerability scans can produce an overwhelming amount of information. Filtering through results to find the true risks that matters to your business can be a challenging and time-consuming task. A good VM solution does more than just scanning – it also helps you to prioritize vulnerabilities to drive effective risk reduction.

Overview of VM Program

There are four essential components in an effective VM 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 to improve 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 has different systems and network infrastructure, so your VM solution should provide flexible deployment options and full control over scanning. The ability to optimize the 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 scanning from a central location and aggregating scan data increases the efficiency of your VM program and reduces impact on your network. A distributed architecture includes a central console for managing scan 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 Systems can look different when scanned from different viewpoints. Internal scanning assesses the security of your network from inside the firewall, while 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?
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.	Can the solution scale quickly and easily? Do additional scan engines need to be purchased for larger environments?

Scanning

Vulnerability scanning is an important technology for identifying risks in your environment, but an effective security program requires a comprehensive solution that does more 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 also 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?
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?
Virtual & Cloud Environments Virtualization and cloud technologies enable organizations to spin up assets on demand, but pose a security challenge as many solutions don't differentiate between scanning of real and virtual assets. The solution should be able to dynamically discover and assess the risk of virtual and cloud assets in order to secure these environments.	Can the solution automatically discover and assess the risk of virtual and cloud assets through direct integration?
Web Application Scanning In 2013, web application attacks were the most common type of attack resulting in a security breach[1]. Given the likelihood of compromise, it's important to choose a solution that provides the ability to scan web applications for the OWASP Top 10 categories, the industry standard for the most critical web application security risks.	Can the solution scan for vulnerabilities and misconfigurations in web apps including the OWASP Top 10 categories?
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 scheduling of scans within specific time windows and repeated at defined intervals?

Prioritization & Remediation

A common challenge among security teams is determining which vulnerability and assets to focus on first and establishing an effective workflow 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 figure out which systems to fix first. Simply using the industry standard Common Vulnerability Scoring System (CVSS) is not sufficient for effective vulnerability prioritization. The risk score should incorporate threat metrics such as exposure to exploits and malware kits, and how long the vulnerability has been available.	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 to the business. This contextual business intelligence enables you to prioritize business-critical systems and data for remediation. The solution should also provide the ability to automatically modify the risk score based on the criticality of an asset.	Can the solution prioritize remediation efforts for business-critical assets?
Vulnerability Validation Combining scanning with penetration testing allows you to validate whether the vulnerabilities you have identified pose actual risk to your organization. This allows you to prioritize validated vulnerabilities for remediation and create exceptions for vulnerabilities which could not be exploited. The integration between the VM and penetration testing solutions should be automated and data should flow seamlessly between the two solutions.	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 workflow, 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 for an asset can depend on where it's located, what its role is, who owns it. A delay between finding the risk and assigning the remediation task means the asset is unprotected for longer. Remediation plans should be automatically sent to the asset owner after each scan according to the business context for immediate action.	Can the solution automatically assign remediation tasks after each scan according to the business context?

Reporting

Vulnerability scans can product 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 to consolidate for reporting, you can centrally manage the prioritization and remediation workflow, as well as analyze security risk and compliance trends across your organization. The solution should present vulnerabilities, configurations, policy compliance, and other asset information such as installed applications and running services 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, for example 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 so that you can tweak them to your organization's requirements.	Does the solution provide both pre-configured and full customizable report templates for a variety of audiences?
Report Scheduling & Distribution The faster reports are sent after a scan, the quicker vulnerabilities are fixed or decisions are made. Reports should be able to be generated and distributed on an ad hoc basis, automatically after every scan, or on a regular schedule. The solution should also allow you to specify who the reports are delivered to via email, as well as has access to 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 such as location, owner and 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?
Database Queries Sometimes you may need to perform advanced analysis on asset and vulnerability data that is specific to the needs of your organization or security team. The solution should support the ability to run SQL queries directly against the reporting data model and output the results in a standard format for creating pivot tables, customized 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 workflow 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 workflow for vulnerability exceptions? Can you configure user permissions for submission, approval and expiration?

Administration, continued

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 turaround.	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 workflow 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?
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 supports are 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?
Professional 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.	Does the vendor offer services for deployment and optimization?

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 over three years, as well as any hidden costs for components or modules you may need to add over time.

Some open-source or low-end tools provide a single vulnerability scanner with limited functionality at no or a 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:

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

About Nexpose

Rapid7 Nexpose is a unified vulnerability management solution that analyzes risks across vulnerabilities, configurations, and controls. Contextual business intelligence automatically accounts for the criticality of assets within your environment, including virtual assets and assets in the public cloud. Integration with Metasploit, the world's most used penetrations testing software, enhances its ability to evaluate vulnerabilities with an awareness of the threat landscape. With Nexpose, you discover, prioritize, and remediate the risks that matter.
Try Nexpose for free today:
www.rapid7.com/products/nexpose

About Rapid7

Rapid7's IT security data and analytics solutions collect, contextualize and analyze the security data you need to fight an increasingly deceptive and pervasive adversary. Unlike traditional vulnerability assessment or incident management, Rapid7 solutions uniquely provide insight into the security state of your assets and users across virtual, mobile, private and public cloud networks. They enable you to fully manage your risk, simplify compliance, and identify, investigate and stop threats faster. Our threat intelligence, informed by members of the Metasploit open source community and the industry-leading Rapid7 Labs, provides relevant context, real-time updates and prioritized risk. Our solutions are used by more than 25% of the Fortune 1000 and nearly 3,000 enterprise, government and small business organizations across 78 countries. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.