Best Practices for Selecting a Vulnerability Management (VM) Solution

With attackers using increasingly-sophisticated ways to break into systems, manual methods of locating and inspecting devices on your network are no longer enough. The right Vulnerability Management (VM) solution can monitor your environment, enabling you to: discover devices running in your network, determine whether they are vulnerable to attack, find fixes to the underlying problems, and protect yourself while those fixes are being implemented. New Cloud-based VM technologies make it simple for you to automatically and accurately test your perimeter and cloud systems, DMZ appliances, internal workstations and mobile devices. This checklist of best practices will save you time and help you understand what to look for when selecting a VM solution, whether you have a dozen systems or a million.

Architecture

❑ **Is the VM a software product or a Cloud service?**
VM software products that you install in your network require you to acquire, configure, and manage servers, do backups and handle patch updates. In contrast, modern Cloud-based VM solutions (sometimes called software-as-a-service or SaaS):

- Don't lock you in with up-front investments in equipment.
- Don't require ongoing updates, database backups, etc.
- Can immediately reach your perimeter systems.
- Can be used directly from your browser.
- Scale easily to handle new devices, users and locations.
- Have costs that are more predictable.
- Enable results to be stored in an objective, tamper-resistant way for audits.

❑ **Is the VM a full monitoring solution or just a scanner?**
Older VM products merely scan your network and format the data they find into reports. Newer solutions track the state of your systems to provide an ongoing view of your security. They also make predictions about emerging "Zero Day" vulnerabilities or "Patch Tuesday" issues without requiring new scans.

❑ **Can the VM scan perimeter, internal and cloud systems?**
Today's VM solutions should be used to check systems everywhere – on the Internet, inside your private network, or in the Cloud. Look for solutions that allow you to use a single tool wherever you need it and get a consolidated view of your security.

❑ **How does the VM handle multiple locations?**
This is one of the big ways in which VM approaches differ:

- **On-premise products:** VM software that you install yourself uses your internal corporate network to reach each of the devices being scanned. This can create bottlenecks in slower, congested portions of your network or when scanning through firewalls to reach systems on the Internet.

- **Basic software-as-a-service:** Some limited VM services can only scan external, Internet-facing devices.

- **Cloud services:** Modern VM solutions delivered from the Cloud are specifically designed to check systems in many locations at once. These solutions use secure, remotely-managed scanner appliances (either physical boxes or virtual machines) that can be placed in different portions of your network to make internal scanning efficient and minimize the impact on your infrastructure.

❑ **Do I have to open holes in my firewall?**
You should never have to compromise your security by opening special ports in your corporate firewall.

❑ **Does the VM integrate with other systems?**
Vulnerability scanners can be a crucial source of security intelligence for other security and compliance systems. Look for VM solutions that have robust APIs for integrating with your security information and event management (SIEM), risk management (ERM), or governance (GRC) solutions.

Scanning

❑ **What are the top features to look for in VM scanning?**
Vulnerability management solutions are only as robust as the data they can obtain. Look for VM solutions that:

- Can monitor your perimeter, Cloud and internal systems.
- Discover devices that are lost or hiding in your network.
- Organize devices automatically using customizable rules.
- Scale seamlessly from a few devices to millions.
- Authenticate into devices for detailed scanning.
- Scan internal and external networks efficiently.
- Identify vulnerabilities according to CVE guidelines.
- Track which vulnerabilities get fixed, and when.
- Deliver at least Six Sigma accuracy in scanning.
- Can be used by multiple people without interference.
- Protect scan data against eavesdropping and tampering.

❑ **Can the VM reach all of your systems?**
With today's networks in constant flux, a VM solution must be able to scan your systems, even as they move in and out of your network. Make sure your solution handles Cloud, perimeter and internal devices together in a consistent way.

❑ **Can the VM discover what's actually in your network?**
Devices can be put onto your network by almost any group in your company – and get forgotten just as easily. Look for VM solutions that can search through your perimeter, internal networks, and cloud environments such as Amazon EC2 to discover and catalog the devices actually running there.

❑ **Can the VM organize devices dynamically?**
Many VM solutions allow you to arrange your devices into groups for scanning and reporting. The better VM systems do this dynamically based on what's found on the devices – the OS, its networking, software, etc. Best-in-class solutions go a step further and use modern techniques like "tagging" to programmatically apply labels to each device you encounter as opposed to older labor-intensive groups.

❑ **Can the VM scan large numbers of devices efficiently?**
Modern VM solutions are specifically designed for scalability, allowing you to scan portions of your network in parallel and automatically consolidate the results into a single report. This accelerates scanning without overloading your network.

❑ **Can scans be run automatically – even continuously?**
The real power of VM solutions comes from automation. You should be able to have scans run on any schedule (such as during maintenance windows) or even to repeat continuously.

❑ **Which vulnerabilities does the VM look for?**
The best VM solutions combine vulnerability data from industry-standard sources such as CERT, software vendors such as Microsoft, and information received from world-wide networks of customers. Look for solutions that rigorously test each vulnerability definition for accuracy.

❑ **How often are new vulnerability signatures added?**
With new vulnerabilities being discovered every day, your VM system should be able to use new vulnerabilities as soon as they are published by your VM vendor.

❑ **Can the VM use authentication for deeper scanning?**
Many vulnerabilities can only be detected by examining information on the device itself, not just how the device reacts on the network. Only use VM solutions that allow you to specify credentials for securely logging into devices, databases or applications.

❑ **Can the VM scan virtual images in Amazon's cloud?**
Amazon has very strict rules about how and when virtual machines in EC2 or VPC can be scanned. Look for VM solutions that are pre-approved for scanning in Amazon.

❑ **Does the VM deliver Six Sigma scanning accuracy?**
Accuracy is crucial in a VM solution. A missed vulnerability can leave your network open to attack; invalid issues ("false positives") will waste your time. Look for solutions that use industry-standard processes such as Six Sigma for measuring accuracy and test in your own environment.

❑ **Can multiple people use the VM at the same time?**
Look for VM solutions that allow different people to scan and report simultaneously without interfering with each other.

❑ **Does the VM protect data for audits?**
Auditors will question (and likely reject) vulnerability data that can be manipulated by your organization. Make sure the VM solution stores vulnerability data away from users – for example, in the Cloud – to prevent tampering.

Reporting

❑ **Can the VM tailor reports to different audiences?**
Most modern VM solutions distill the vast amount of data they collect into insights that can drive prompt security actions. Look for solutions that can give you differing levels of information, from executive-level scorecards of the overall security to detailed drill-down reports that reflect your own specific criteria.

❑ **Does the VM offer predictive analysis?**
Advanced VM solutions keep track of the state of each device in order to predict which devices might be vulnerable to new “Zero-Day” attacks or “Patch Tuesday” issues without requiring new scans.

❑ **Can the VM highlight changes across scans?**
To avoid revisiting old issues, look for advanced VM solutions that track whether each vulnerability found is: new, being worked on, already fixed, or accepted as not worth fixing. Best-in-class solutions also provide “differential reporting” that highlights changes from one scan to another.

❑ **Are vulnerabilities easily prioritized in reports?**
Vulnerabilities should be ranked by severity, based on industry standards such as CVSS. This can help you efficiently prioritize how and when to address each issue and is particularly important for complying with mandates which require proof that severe vulnerabilities are being promptly identified and fixed.

❑ **Does the VM offer patch-centric reporting?**
While all VM products can produce lists of individual risks, advanced solutions also can organize vulnerabilities according to the patches that address them. This helps IT teams rapidly eliminate vulnerabilities.

❑ **Can reports help show compliance?**
VM scans are increasingly being required for compliance audits. Look for VM solutions that provide native support for key mandates such as PCI as well as the ability to properly customize reports to your individual needs.

Fixing/Remediation

❑ **What information about the underlying cause does the VM provide about each vulnerability?**
VM solutions exist to help you eliminate vulnerabilities, not just find them. Best-in-class VM solutions provide detailed descriptions of each vulnerability as well as links to the vendor updates or patches needed to fix it.

❑ **Does the VM provide automated trouble-ticketing?**
VM solutions should allow remediation tasks to be assigned according to users’ specific roles and can track what gets fixed and when. Make sure that your VM system provides automated notification of tickets as well as comprehensive reporting on ticket status. Look for solutions that can provide executive summaries across groups of devices of as well as detailed drill-downs per device, vulnerability and user.

❑ **Can you control how remediation tasks are scheduled?**
While VM systems that provide remediation tracking often can at least start with the highest-severity vulnerabilities, it’s also important for you to be able to control the relative priorities of issues found in different systems. This enables your IT team to focus first on fixing the problems that would have the biggest impact on your business.

❑ **Can the VM be used with external ticketing systems?**
If you already have a trouble-ticketing system in place, look for VM solutions also can work with external ticketing systems to automatically generate, track and close tickets.

Administration

❑ **Is system maintenance required for the VM, such as patching software or doing backups?**
On-premise VM solutions are like other software products: they often require never-ending efforts to keep them up-to-date and supplied with enough CPU, memory, disk, database and network resources. Cloud solutions eliminate this burden, allowing you to focus your time and energy on using your VM solution instead of caring for it.

Costs

❑ **What costs are required for the VM?**

This is an important difference between on-premise and Cloud solutions:

Costs of the Solution	On-Premise Software	Cloud Service
Upfront hardware *(servers, storage, infrastructure)*	$	
Software usage	$	$
Distributed scanner appliances for internal networks	*not offered*	$
Maintenance	$	*included*
Support	$	*included*
Deployment professional services	$	
Database admin *(including backup)*	$	
Expansion hardware *(as needs grow)*	$	
Expansion deployment services	$	
Integration with other security systems	*Custom services*	*optional APIs*

- **On-premise software:** Installing VM products in your network can entail a variety of costs – from hardware to personnel. Capacity planning is crucial. Buy too much and you waste money; buy too little and you may end up replacing hardware or paying for additional deployment services as you grow.

- **Cloud service:** Most Cloud-based VM solutions are offered as annual subscriptions that include the latest software, support, and administration of the solution's underlying platform. Incremental services, such as scanners for internal networks, are simply additions to your subscription. As your needs grow, you just adjust your subscription without replacing anything.

❑ **Are consultants required to run the VM?**

It should be your choice. Consultants can be a great resource, particularly for complex projects such as penetration tests that assess your systems at given points in time. They can also help your IT team address difficult issues that are uncovered during vulnerability scans. Many organizations have also found that modern VM solutions make it easy and cost-effective to incorporate vulnerability scanning into their regular, ongoing IT operations.

❑ **Could I save money by using free, open-source VM software instead?**

Open-source packages eliminate the software usage costs associated with on-premise VM solutions, but still leave you with other expenses: hardware, customization, IT, training, and support. At some point, you'll likely need new capabilities. You'll either have to pay outside developers to provide the features you need or increase your internal staff.

Support

❑ **What type of support comes with the VM solution?**

Web application issues can appear at any time, day or night – and often require immediate response. Look for VM solutions that offer 24x7x365 support (telephone, email and online documentation) backed by a contractual service-level agreement (SLA). Many Cloud solution providers include this as part of every subscription.

❑ **Is training included with support?**

Look for VM solutions that offer live and recorded training as well as certification programs. Cloud solution providers often include this in your subscription at no extra cost.

Vendor

❑ **Does the vendor have a reputation for quality, accuracy and usability?**

Web servers, database systems, appliances, workstations, and mobile devices all can provide an entry point into your environment. VM solutions exist to help you protect those systems – and the business behind it. Ask for references from businesses similar to yours.

❑ **Is VM a focus for the vendor, or just a feature of another product?**

Vulnerability scanning is a sophisticated technology that requires deep expertise and commitment. Look for vendors who view their VM solution as a core part of their business, not a bullet on another product's check list.

❑ **Does the vendor make it easy to try the VM in your own network?**

If you can't try it, don't buy it. Test VM solutions in your own environment with the devices you'll need to secure. Cloud services make such testing particularly easy to do.

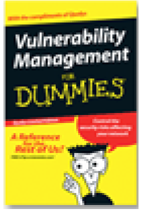
Useful Resources

To try a vulnerability scanner with your own systems:

A free 14-day trial of QualysGuard Vulnerability Management, the industry's leading Cloud-based VM solution, is available at qualys.com/trial. See for yourself why many of the world's premier companies depend upon QualysGuard VM.

To learn more about vulnerability management, please see:

QualysGuard Vulnerability Management lets you quickly and easily discover devices running in your network, determine whether they're vulnerable to attack, understand how to fix them, and protect your business. To learn more, visit qualys.com/vm.



Vulnerability Management for Dummies. This e-book offers a quick, easy-to-read guide to making your network, servers, workstations and other devices more secure. Available at qualys.com/vmfordummies.

The **SANS InfoSec Reading Room on Threats/Vulnerabilities** provides whitepapers on a variety of vulnerability security topics. See sans.org/reading_room/whitepapers/threats/.

Common Vulnerabilities and Exposures is a dictionary of publicly-known information security vulnerabilities and exposures. See cve.mitre.org.

The **Common Vulnerability Scoring System** (CVSS) is an industry standard for rating IT vulnerabilities. See www.first.org/cvss.