FORTRA™

Vulnerability Management Buyer's Guide

10 Essential Questions to Ask Your VM Vendor

Knowledgeable IT, compliance, and security professionals understand the critical role vulnerability management (VM) plays in risk reduction and compliance. From helping ensure availability and uptime to hardening systems against cyberthreats, a solid VM program aligns your organization with cybersecurity best practice frameworks like the Center for Internet Security's CIS Controls.

However, after investing in VM products and services, you may have discovered that some VM solutions have serious limitations. For example, you may experience challenges scaling to large environments, or stretching to support other key controls like integrity and configuration management or meeting various compliance requirements.

Due to rapid adoption of cloud technologies and movement toward hybrid environments, large-scale networks are in a state of constant change. New physical and virtual devices are being added to networks, modified and then removed at a faster pace than ever. Some of these changes are unauthorized and introduce new vulnerabilities. Even if these vulnerabilities are temporary (as in virtual and cloud infrastructures) or on remote or business partner networks, they can still leave the door open for cyber attackers.

How to Use This Guide

This guide is designed to help you choose a new or replacement VM product. If it's been a while since you've evaluated this class of solutions, this guide will also help you navigate the recent advancements in VM technologies. The usability of VM data has improved significantly with newer technologies, now making it a key resource in threat detection and response. The goal of this paper is to tease out the differences between the various VM products and help identify the features that matter most in today's technology ecosystem.

Three Core Problems VM Solutions Solve

The main purpose of VM solutions is to provide accurate risk assessment and actionable information for proactively defending your critical assets from cyberthreats. There are a few other challenges that drive organizations to re-evaluate their VM programs: limited network visibility, identity and access management integration, and mounting pressure to reduce compliance costs.

1. Limited Network Visibility

It's likely that, despite your best intentions, your visibility into the assets you've been tasked to protect is incomplete or outdated. Security teams often don't directly control the assets they're responsible for protecting, and gaining deep insight into these assets can be a challenge. Cloud, virtual and mobile device adoption trends continue to add to the complexity of large networks. This results in security risk visibility blind spots—ideal places for adversaries to launch their attacks.

The first step in gaining complete network visibility is an accurate hardware and software inventory. CIS Control 1, Inventory and Control of Hardware Assets, offers a good explanation as to why an incomplete view of asset inventory is problematic: "Attacks can take advantage of new hardware that is installed on the network but is not configured and patched with appropriate security updates. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal jump points or victims." CIS Control 2, Inventory and Control of Software Assets, requires that you "Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems."

2. Identity and Access Management Integration

Since personnel are a crucial aspect of information security, it's important to keep human resource management changes aligned with your VM system. This ensures that only authorized users have access to the data stored in it. Without tight integration between your directory service and VM solution, administrators must manually create, update,

VISIBILITY IS CRUCIAL

Virtually every major control framework asserts that without comprehensive visibility into all the hardware and software assets on the network, risk and compliance profiles will never be complete and accurate. Approaching VM from multiple perspectives can dramatically improve accuracy because data from a variety of sensors can be correlated to prioritize resources where the next attack is likely to occur.

and delete accounts every time even a minor change is needed.

If those changes aren't reflected in the VM system, employees who need access to vulnerability data may not have it—and those who don't need it could gain access. Larger, multi-unit organizations or managed services providers require multi-tenant capabilities in their VM solution. This lets them optimize sub-account management from a master account and comprehensive role-based access control (RBAC) with each tenant. This makes it easy to segregate data and partition user access

3. Pressure to Reduce Compliance Costs

Every major compliance and regulatory framework, including NIST 800-53, SOX, NERC CIP, MAS TRM and IRS 1075, requires a VM program to protect systems and infrastructure. For example, PCI DSS requires internal and external vulnerability assessments every quarter, and again after any major change to the network. To compound this problem, compliance departments are often under pressure to achieve and maintain compliance while also decreasing operating costs. A VM program is essential for meeting compliance requirements. VM tools may also promise to monitor controls other than VM, but they often fail to provide a scalable solution beyond the VM domain. Additional tools or vendors are required to fully meet integrity monitoring and compliance assessment.

Quality Criteria for VM Solutions

When evaluating VM solutions, buyers should appraise the performance of the technology and ensure it will allow them to quickly answer these critical questions:

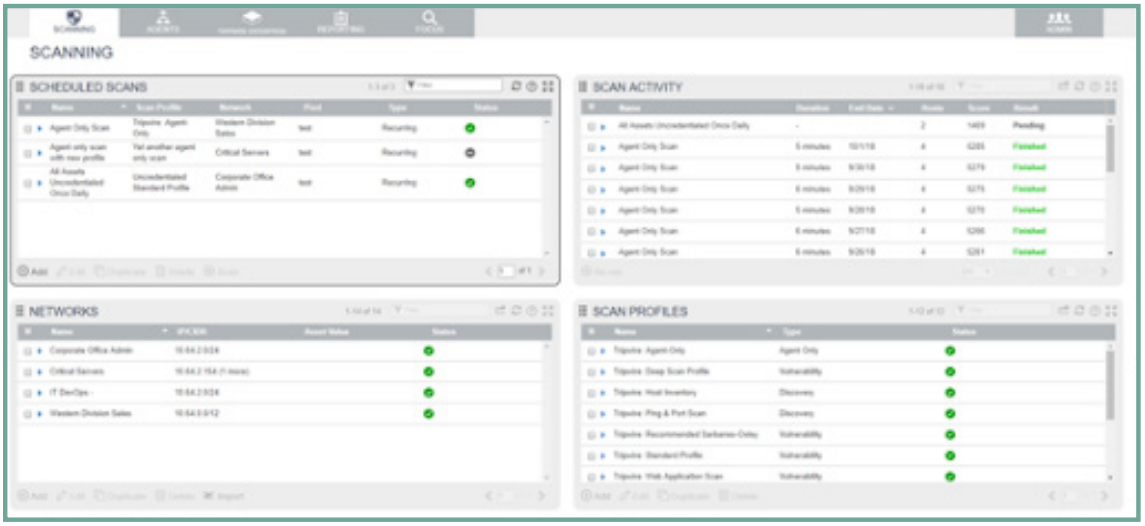
- Which areas of my network present the greatest risk right now?
- Is the most recent high-profile vulnerability present anywhere on my critical infrastructure?
- What are the most effective steps we can take immediately to reduce our security risks?

The following capabilities are what you need to look for in order to find a comprehensive VM solution.

Varied Assessment Methods

Assessment depth can significantly impact the accuracy of results. Deeper assessments gather more detailed information, which the system can use to improve accuracy. There are four main types of vulnerability assessment methods to consider:

- **Agentless discovery:** Look for a solution with unlimited agentless discovery with comprehensive fingerprinting and application/service detection to accurately identify and profile the your assets. This allows you to inventory ports, services, and applications exposed on your network and identify each device type and operating platform.
- **Agentless credentialed scanning:** Credentialed assessments use administrative credentials to inspect file system, registry and configuration files. Credentialed assessments take longer to run, but the additional information gathered dramatically improves both discovery and assessment accuracy.



The Tripwire® IP360™ scanning dashboard

- **Non-credentialed scans:** In contrast, assessments performed remotely or without credentials provide the same view an outside attacker would have. If agent-based or credentialed scanning are akin to white box testing, remote analysis would be black box testing. Less information is gathered about the application footprint of the asset, but more data is available regarding the protocols and services that can communicate with the asset. While white and black box assessments should be performed together for a holistic view of your security posture, it's important you use accurate and reliable methods of testing remotely. In some cases, products rely on banner checks that can lead to inaccurate results. It's better to look for a solution that relies on direct condition tests and inference when reporting vulnerabilities remotely on an asset.
- **Agent-based scanning:** Agent-based scanning can be conducted as a stand-alone process or in tandem with agentless scans to provide a more comprehensive view. A network scan should dynamically recognize when an asset has an agent and optimize the scan by using the data collected by the agent. Ideally, a VM product offers both methods so you can use the one that best balances your organization's requirements for assessment speed versus depth. Combining the in-depth assessment provided by agent-based scanning with non-credentialed remote scanning can be a good strategy when credentialed access isn't viable.

Accurate Detection

Because many VM tools have significant accuracy problems, they deliver too much data and too many alerts. Massive reports that include a lot of undifferentiated data about possible changes or vulnerabilities make it nearly impossible to determine which issues need attention now and which can wait. As a result, valuable resources are wasted investigating events that aren't "bad," such as reporting false positive findings.

In 2017, the Fortra's Tripwire Vulnerability and Exposure Research Team (VERT) tracked 64 confirmed defects filed against our database of over 150,000 conditions, which represented a false positive rate of 0.04 percent. While false positives are easy to track—as they're reported by customers when they're encountered—it's much more difficult to generate a false negative rate. The definition of a false positive is as straightforward as "an incorrect result." A false negative is the lack of a correct result, but not all missing results are false negatives. A false negative occurs when an application or vulnerability that should be found was not. Typically, reported false negatives are better classified as requests for coverage. Once you remove these coverage requests, Tripwire's false negative rate quickly approaches zero.

FEATURE TIP

Aim to implement both agent-based and agentless VM, as each method offers advantages. For example, not all devices are always connected to the network—for example, laptops may be offline for extended periods, and agentless scans can miss them. But with an agent, assessment will take place as scheduled whether the device is connected or not.

Sharing change and vulnerability data between IT operations and security teams makes it easy to optimize resources for specific business goals, yet most VM data isn't easy to share. Many VM tools also waste valuable resources because they require manual effort to export and format data for consumption by other teams.

Thorough Discovery Capabilities

Asset discovery and inventory features and capabilities differ from product to product, but a worthwhile VM product should offer the following discovery capabilities:

- **Continual device inventory:** Your solution should be able to take a continuous inventory of all devices, including wired and wireless devices, virtual machines, cloud instances and containers.
- **Continual software inventory:** Continual inventory of all software applications and versions includes desktop applications, operating systems, ports and services, and protocols.
- **Asset tagging:** Your solution should provide the ability to tag assets by group, technical owner, regional location and criticality.

The process of putting these capabilities in place helps align your organization with CIS Controls 1–3: the top three prioritized controls that create a system hardened against risk from vulnerabilities. CIS Control 3 is Continuous Vulnerability Management: "Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers."

Look for a solution that does device profiler (DP) pooling as well. DP pooling lets you group multiple device profilers into a pool of appliances that can be used to conduct scheduled

scans, as opposed to depending on a single DP to do any given scan. This provides several advantages. First, it gives you the ability to scan a given network faster because the load is divided up among multiple scan appliances. Second, it adds resiliency in that if there's a failure on the part of any particular scan appliance—or if an appliance's connection to the network is lost or becomes degraded—then the other appliances in the pool will pick up the load for the lost or degraded appliance and ensure that the scan completes. Third, it allows you to simplify your scan schedules by allowing larger network blocks to be scanned by dynamically load balancing a scan job across the pool of appliances rather than having to break them up and schedule them manually.

Intelligent Assessment Technology

Intelligent assessment technology ensures frequent and accurate assessments for improved visibility and confidence in security posture assessments.

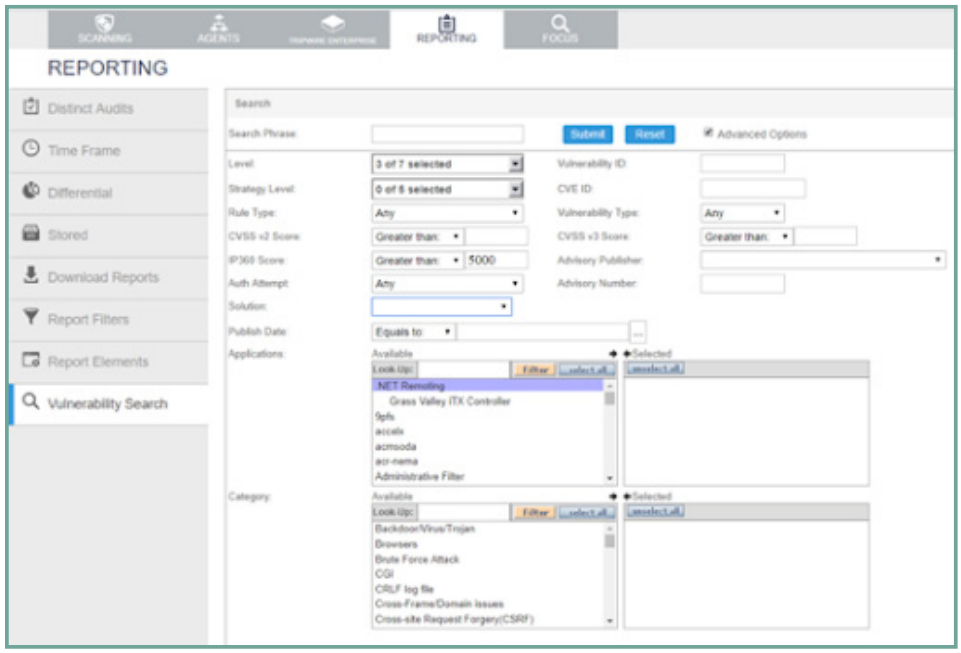
- **Indiscriminate testing:** In this older method, the solution scans through a defined range of asset IPs and indiscriminately checks each asset against a list of known vulnerabilities maintained by the VM vendor. This results in time-consuming checks that may not apply to the device being assessed. For example, this approach will result in checking a Linux machine for a Windows vulnerability. This scenario is also likely to occur when device and application inventory is inaccurate, such as when a NetApp filer running a UNIX-derivative OS is profiled as a Windows device because it's running a Windows SMB/CIFS service.
- **Targeted testing:** This method first inventories and profiles each asset to determine the type of device, operating system, and applications present. It then uses that information to efficiently check for relevant vulnerabilities, skipping checks that don't apply to a particular asset, OS or application version.

Targeted testing offers several advantages:

- Improved assessment speed and efficiency
- Custom tests for OSs, applications and services that exist on a device minimizes resource usage and improves network stability
- Improved accuracy, resulting in fewer false positives
- Ad-hoc assessments limited to vulnerabilities, configurations or software versions specified by the user for faster results

Mobile Asset Management

Many smartphones and tablets—like Apple iOS devices—require special tools for management and assessment. Because of this, many organizations run mobile device assessment separately from their vulnerability assessment and then aggregate the report data. At a minimum, a high-quality VM product should be able to discover the exposed surface area of mobile devices connected to wired and/or wireless networks.



Tripwire IP360 vulnerability search reporting dashboard

Virtual and Cloud Infrastructure

Within large organizations, devices may be owned by different people or departments. They may also exist in many physical and virtual locations. Security teams need to be able to quickly identify the owner, location and criticality of an asset, as it's important when assessing and responding to events on that device.

Many VM solutions require humans to review and keep a current list of assets (as well as their types and configurations) in order to identify their criticality. An automated API-driven workflow for this time-intensive process allows an administrator to define a set of rules in which devices can be categorized based on the unique taxonomy of the organization.

Real-time Data Navigation

Reporting can transform volumes of security data into actionable information that can be used to reduce risk. This not only makes it easier to identify vulnerabilities that need patching, but also to detect misconfigurations that affect compliance or security posture and provide actionable remediation advice.

Constantly-changing technology infrastructure combined with rapidly-emerging vulnerabilities requires organizations to strive for a comprehensive, accurate, real-time view of vulnerabilities—yet many VM solutions produce overly simple reports. These reports provide only a snapshot of vulnerabilities discovered within a specific time period.

Advanced VM solutions offer real-time data navigation and synthesis. For example, they can produce a list of assets that share a specific vulnerability or compare two historical asset assessments to identify new vulnerabilities or applications that have changed. Indexing OS, application, and vulnerability results enables a real-time response to emerging threats by searching the conditions that would make assets vulnerable without having to wait for a signature or the need to run a scan.

Advanced solutions offer benefits in the following areas:

- **Audience-specific report filters:** Look for a solution that provides reports with the appropriate level of detail for a variety of audiences, including auditors who may wish to see proof of compliance, and business executives, who want an overview of the organization's risk posture, graphical views of risk trends and visualization of risk data by organizational hierarchies or geographical location. It must also allow all users to create, save, and share report filters and filter report content to include or exclude data based on asset score, vulnerability type or severity, operating system group, and other characteristics. Your solution should also automate report distribution to users based on their roles.
- **Remediation advice:** Effective VM solutions offer advice on correcting vulnerabilities, including accurate and complete remediation details, potential mitigations, links to patches, vendor advisories and relevant vulnerability information.
- **Transparent vulnerability checks:** These checks provide details about how vulnerabilities are detected so system administrators can manually verify them. A vulnerability may reappear in a report after a patch or other fix has been applied—or misapplied—because the machine is still vulnerable. This can also happen when the device requires a reboot for the patch to take effect. Information on how a vulnerability was discovered helps teams find underlying sources of additional risk to the organization.

System Integrity Monitoring

System integrity monitoring, which includes file integrity monitoring (FIM), is another foundational security control used by most enterprise security teams, but this data often exists in a separate silo from VM data. Correlating these two controls provides critical insights into attack methods and targets. However, it requires coordination across multiple teams, and access might be hindered by internal policies or business processes.

Without "who" data, it's more difficult to know if a change is good or bad. For example, an unauthorized or unrecognized user may be an indicator of "bad" change, but if you know who made the change, you can ask that person about it or investigate further to verify that the account hasn't been compromised. Combining change data that contains "who" information with VM data allows security teams to quickly identify systems at high risk.

Another example of the correlation between robust vulnerability data and detailed FIM data is the versioning and history of a specific file. Without this data, it's hard to connect multiple pieces of information and then conclude whether a change was good or bad.

To determine if a breach is in progress, security teams need to be able to quickly answer these questions:

- When did this change occur?
- What did the configuration of this device look like before the change?

- Are there other changes that have happened in the past on this device?

In order to identify the exact changes taking place, you need detailed information that's only available by comparing reports from different security tools. Change data alone doesn't identify the changes that indicate a potential breach. You need a known, "good" baseline state and a way to do a side-by-side comparison of the change data against that state.

Detailed Risk Scoring

Every organization is different, with different priorities, risk tolerance and unique threats to combat. Standard industry vulnerability scoring systems, such as CVSS, may rate a vulnerability as an 8 on a scale of 1–10, but for your specific organization, the same threat may present a higher or lower risk. CVSS is a good baseline scoring option that allows you to compare vulnerabilities across products. But because you can have 5,000 CVSS "8"s, you're likely to need more granular scoring.

Risk scoring is a good example of how customization can help organizations tailor VM data to their specific business requirements. Many VM systems offer a 1–10 or High/Medium/Low scores. In organizations with thousands—or tens of thousands—of vulnerabilities, these rough scores lose meaning. Your VM solution should be supported by a world-class research team that analyzes conditions and risks rather than relying on automated feeds and scoring metrics.

Accurate, up-to-date vulnerability data combined with a variety of other security solutions provides valuable insights. However, combining data manually from multiple sources is costly and increases response time to breaches and incident detection. Many VM tools offer limited or API-only integration with other security tools. These solutions require expensive internal resources to build and keep necessary integrations current. To be an effective tool in breach detection and prevention, VM solutions should let users instantly view and manipulate the historical and current data they need in real time.

Business Context

You should also look for a solution that can organize hosts and networks in a business-aligned structure. For example, business unit categories like finance and sales, or geographies like North America or EMEA should be offered. This helps the solution apply business context when calculating and trending vulnerability scores.

10 Essential Questions to Ask Your Vulnerability Management Vendor

Asset discovery and inventory features and capabilities differ from product to product, but you'll know if you're purchasing a sophisticated VM solutions by asking the following questions:

1. Does it offer both credentialed and uncredentialed, and agent-based and agentless assessment capabilities so you can choose which method to use for assessments and adjust as needs change over time?
2. Does it conduct accurate breach detection? What is the rate of false positives?
3. Does it perform continual hardware and software inventory and satisfy CIS Controls #1–3?
4. Does it leverage both indiscriminate and targeted testing assessments for optimum accuracy?
5. Does it conduct asset management for occasionally-connected endpoints?
6. Does it quickly identify the owner, location, and criticality of each asset, even in virtual and cloud environments?
7. Is there real-time data navigation and synthesis with audience-specific report filters, remediation advice, and transparent vulnerability checks?
8. Does it perform system integrity monitoring to give you "who" data on important changes?
9. Does it offer detailed risk scoring supported by a team of expert researchers and analysts?
10. Does it provide business context by organizing assets and networks to help you better align with your objectives?

Request A Demo

Let us take you through a demo of Tripwire's security and vulnerability management products and services customized to your specific IT security and compliance needs.
Visit www.tripwire.com/demo today to schedule yours.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-tw-gd-1123-r1-hm)