DATASHEET

Agentless or Agent-based VM: Which Method Fits Your Needs Best?

It can be hard to know exactly when and how to incorporate agents into your vulnerability management processes. How does your team ensure full scanning coverage for in-network and remote endpoints accessing corporate assets? Will agentless or agent-based scanning yield better results?

There are several instances in which agent-based monitoring offers superior support and protection across your networks. But that doesn't mean you need to opt for a 100 percent agent-based approach, either. In truth, it is not an either/or question. Both methods have their benefits and limitations: A combined scanning strategy using both agentless and agent-based scanning helps ensure all network-connected assets are secured.

> Powerful vulnerability management means mixing and matching your agent-based and agentless strategies — it should never be a matter of choosing one over the other. You'll achieve your richest assessment with a combination of both agentless and agent-based VM.

Combining Agentless and Agent-Based VM

If you're only using agentless scanning for vulnerability management, you might not be getting a complete picture of the vulnerabilities on your network. Agents provide deeper visibility and system efficiency than agentless scanning in several critical areas, such as network load, scanning without credentials, and assets using dynamic IPs.

Agent-based vulnerability management provides additional functionality to solve hurdles associated with agentless scanning and deepens the scope of your vulnerability management assessments. But that doesn't mean you should do away with agentless vulnerability scans. There are certain situations in which agentless scans can discover vulnerabilities that agent-based scans cannot.

Fortra VM

Fortra Vulnerability Management (Fortra VM) supports a combined scanning strategy in which robust agentless scanning technology is enhanced with an agent for seamless coverage for both network and remote devices.

Fortra VM's patented scanning technology identifies and evaluates the security and business risk postures of network devices and applications, while agents scan remote endpoints ensuring, ensuring more comprehensive vulnerability scanning. Scan information from the agent is incorporated and reported via our user-friendly dashboard and included in Security GPA® and Insight peer comparison reports for informed prioritization and reporting.

Together, Fortra VM agentless scanning and an agent extend the scope of vulnerability assessments to shrink your attack surface.

	Main Features & Benefits	Main Limitations
Agent-Based	**No need for key/credential management** • Reduced operational burden of managing credentials across your network **Deeper system insight and visibility** • Leads to a potential reduction in false positives • More accurate (true positive) vulnerability detection **Does not require a live network connection to scan** • You do not lose visibility or scan coverage for devices that have poor, intermittent, or occasional connectivity • Less network traffic/load/noise	**Installed onto a device** • IT overhead for installation and maintenance — yet another line on the software inventory • Competes for resources on the device and potentially impacts performance of other software **OS-specific** • Agents may have OS limitations that prevent them from running on certain devices or unsupported operating systems • Upgrade and refresh cycles need to be in step with OS upgrades (i.e. more work for IT)
Agentless	**No software installation required on target assets** • Immediate/rapid coverage • Discovery of shadow IT • Lower maintenance and overhead from IT teams • Lower resource utilization on the target • Much wider target range as it does not depend on OS **Authenticated Scanning** • Provides a deep level of visibility without the need for an agent • Gives you the ability to audit configurations which supports both security and compliance mandates **Authenticated scanning is mandated by several compliance frameworks** • Aligns systems with specific compliance requirements (PCI DSS 11.3.1.2, etc.)	**Connectivity requirements** • Requires every device to be connected to the network for detection by agentless scanners **Credential Management** • Necessitates more effort toward administration and control of user credentials

FORTRA

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.