SOLUTION BRIEF

Agent-Based Vulnerability Management

When and How to Use Vulnerability Management Agents

Tripwire IP360 Quick Facts

- The complete ABVM solution for organizations and agencies
- Uses the standard Tripwire IP-based licensing structure
- No additional hardware required
- Using agents incurs no additional charge
- Provides granular risk prioritization reporting
- For use in on-premises, cloud and hybrid environments
- Overall footprint <100 MB
- Consumes <2% of CPU resources

When should your security strategy include agent-based monitoring? It can be difficult to discern when and how to incorporate agents into your vulnerability management processes. 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. There are several benefits to using agent-based and agentless vulnerability management solutions both separately and jointly.

Traditionally, Tripwire's vulnerability management solution functioned in a fully agentless capacity covering hybrid environments, including on-premise, cloud and container-based environments. That is until now. With the release of Tripwire® IP360™ 9.0, Tripwire's world-class solution adds its time-tested agent technology to further expand its functionality. Tripwire IP360 9.0 provides agent-based vulnerability management (ABVM) for organizations and agencies with the most granular risk prioritization visibility on the market—while still leveraging the benefits of agentless scans.

Agent-Based vs. Agentless

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, assets using dynamic IPs, and of course, cloud images that have short lives.

Using agents 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.

For example, agentless scans can locate what's not stored on your devices themselves, such as SSL certificates. Powerful vulnerability management (VM) 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.

Six Practical ABVM Use Cases

Agent-based vulnerability management provides additional functionality to solve hurdles associated with agentless scanning. Let's take a look at six VM hurdles you can overcome by implementing agents your organization or agency.

1. Access Credentials

Running a comprehensive and accurate agentless vulnerability scan is impossible without credentialed access to every host. Keeping the required credential information up to date and secure can be a daunting and expensive task, and agentless credentialed scans can bottleneck around credentials if the scan encounters devices it can't access. Agents bypass this issue altogether by already being present on the device, and therefore not requiring credentials.

2. Built-in Cloud Asset Security

Scanning for vulnerabilities in your cloud environments can be a challenge. Remote scanning isn't always an option for images in Amazon Web Services (AWS), for instance. When you're using ABVM with your AWS, Azure or Google Cloud images, you can build the agent directly into your images—giving you greater peace of mind knowing your cloud assets remain secure. You can even have the agent immediately scan a new virtual asset when it is started, to be certain your cloud deployments are always safe and secure.

3. Integrated Event Assessment

Determining how often to assess the vulnerability state of your assets is not a simple task. You need to balance the risk of missing new vulnerabilities that may be introduced, with the requirement to avoid unnecessary network load that may impact the performance of your systems. The Tripwire IP360 agent can help you be more focused in your vulnerability assessment efforts by taking an integrated and event-driven approach to VM. For example, you can combine the configuration management capabilities of Tripwire® Enterprise with the Tripwire IP360 agent to automatically initiate a vulnerability scan when an actionable configuration or file system change is detected on an asset. This ensures you assess the vulnerability impact of system changes immediately when they occur and reduces the requirement for frequent scans of your networks.

4. Increased Efficiency

Installing agents on your endpoints reduces overall network traffic since no network-based scanning is required to discover and assess the state of the assets on your network. Should you choose to combining agentless and agent-based processing for the most complete vulnerability assessment of your endpoints, the collection of the required data is significantly more efficient since much of the information has already been collected and reported by the agent.

5. Dynamic IP Endpoints

Asset reconciliation can be a challenge for organizations using dynamic IP for their endpoints, making it difficult to obtain an accurate asset inventory and to track the vulnerability state of a given asset over time. Agents provide endpoints with universally-unique IDs (UUIDs) that can always be used to identify an asset, providing more accurate asset inventories and allowing you to consistently track vulnerability scoring trends over time.

6. Occasionally-connected Devices

Not all devices are always connected to the network. Laptops may be offline for extended periods, and agentless scans can miss these devices if they are not connected to the network at the time of the scan. This leads to an incomplete asset inventory and vulnerability assessment—which can pose serious security risks. But with an agent, vulnerability assessment will take place as scheduled whether the device is connected to the network or not. Then, when the device is connected to any network serviced by Tripwire IP360, it will report the results of that assessment for review and action, keeping your assets secure—any time, anywhere.

Tripwire IP360

VM for Complex Environments

Whether your organization or agency uses on-premises, cloud or hybrid systems, Tripwire IP360 provides comprehensive asset discovery and inventory. Take advantage of the most granular risk scoring and prioritization reporting on the market in order to address vulnerabilities quickly and thoroughly. It also allows you to combine the findings of agentless and agent-based scans to paint the most complete picture of your environments.

Tripwire Axon-based technology

Tripwire IP360 uses lightweight Tripwire Axon® agents. Tripwire Axon is a unified, modular platform that provides deep insight and flexibility to the Tripwire portfolio. Its resilient and secure design supports offline and connected data while maintaining a small footprint.

Tripwire Axon provides the technological foundation for ABVM. The agent is a compact, native component that works with a variety of enterprise operating systems. It executes rules delivered through regular Tripwire IP360 content updates to identify and score vulnerabilities on the asset, and to inventory the applications and system characteristics of the host.

This information is conveyed across a secure and resilient messaging fabric to Axon Access Points (AAPs) deployed with each Tripwire IP360 Device Profiler. The AAPs receive and forward this data to the Axon Access Point Gateway on the IP360 VnE, where the data collected by the agents is aggregated and stored to a VnE database.

The agent-collected data is then further assessed using Advanced Security Profiling Language (ASPL) rules developed by the Tripwire Vulnerability and Exposure Research Team (VERT). VERT continuously identifies emerging vulnerabilities, creating unique detection signatures that are regularly updated to deliver unprecedented vulnerability discovery coverage.

The output of this process is a set of identified vulnerabilities for the asset, each scored using both Tripwire's proprietary scoring system and the Common Vulnerability Scoring System (CVSS). These scores, along with the detailed scan results, are represented in vulnerability audits and other reports in the same manner as vulnerability results obtained by network scanning, with the exception that the information is flagged in these reports to indicate that it was derived from agent-collected data.

Summary

Robust vulnerability management security strategies implement both agent-based and agentless VM, as both methods offer different advantages. Organizations and agencies use Tripwire IP360 to build a customized scanning and vulnerability management process that foster better efficiency and tighter security.

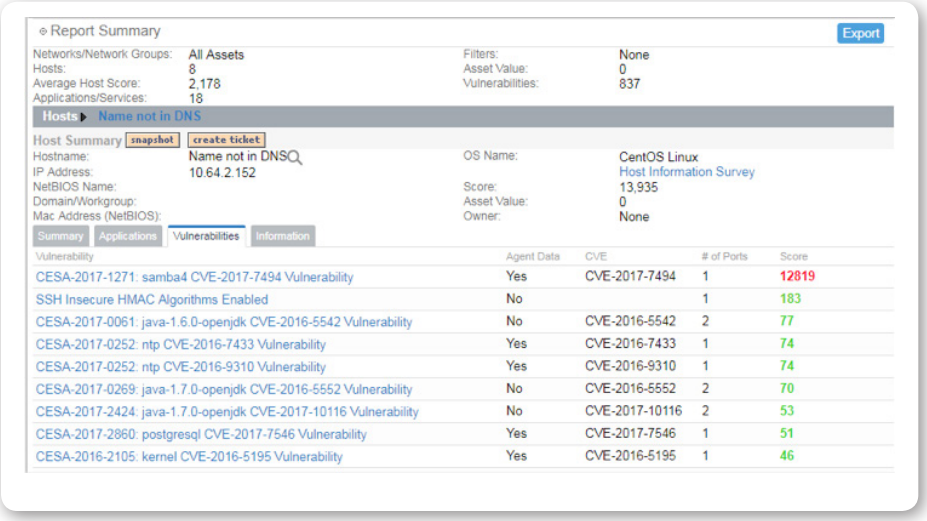

Fig. 1 Reap the benefits of both agentless and agent-based scanning. Agentless scans are augmented with previously collected agent data to improve the efficiency and speed of the scan. Each vulnerability is flagged to indicate if the data was generated from the agent or by remote access to the host.

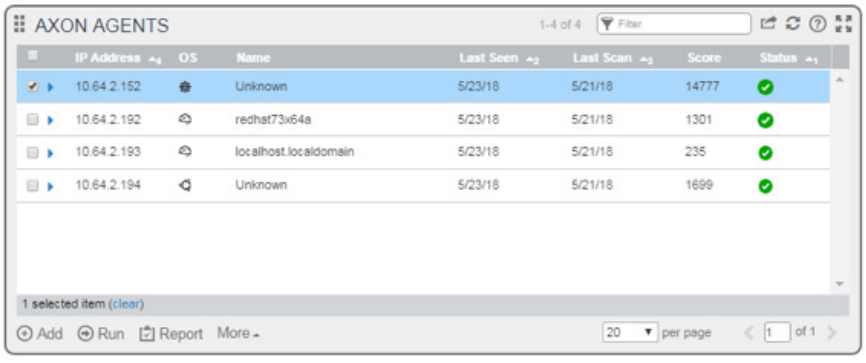

Fig. 2 The Axon Agents widget provides the status of the agent, the date and time it last checked in and last scanned, and the most recent vulnerability score. For any selected agent, you can drill down into the most recent scan report for the asset. You can also initiate an immediate agent scan.

Ready for a Demo?

Let us take you through a demo of Tripwire IP360 and answer any questions you have. Understand how Tripwire's suite of security and vulnerability management products and services can be customized to your specific IT security and compliance needs. Visit **tripwire.com/contact/request-demo/**

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc

SBABVM1a 1806