

[Home](#) / [Blog](#) / [Agent-Based vs. Agentless Scanning: Choosing the Right Vulnerability Scanning Method](#)

Agent-Based vs. Agentless Scanning: Choosing the Right Vulnerability Scanning Method

Posted on August 27, 2021

Preventable Attacks

Another day, another data breach. Cybercrime is on the rise, and the only way to stop a cyberattack is to think like an attacker. In many cases, the bad actor's first step is scanning the victim's systems for vulnerabilities that allow them to gain a foothold. According to [Forrester's State of Application Security](#), 39% of external attacks exploited holes found in [web applications vulnerabilities](#), with another 30% taking advantage of software flaws. Based on these figures, nearly 70% of these attacks are preventable.

One thing is clear, proactive identification and remediation of vulnerabilities are critical to the strength of your cybersecurity program. But where do you start? Sure, you need vulnerability scanning, but how do you know what tools best fit your needs?

[Vulnerability scanning](#) comes in three basic flavors — agent-based, agentless, or a hybrid of the two. Which of these is best for you depends on the environment and your organizational needs. Let's take a look at each option.

Agent-Based Scanning

Agent-based scanning is suitable for organizations with a geographically diverse workforce, particularly if the organization includes remote workers. This is the more traditional type of vulnerability scanner.

'Agents' are a software package deployed to each device that needs to be tested. Once installed, the agent collects data that indicates whether the device may have vulnerability issues. The agent passes this data back to collection servers and information gathered across the entire infrastructure is then consolidated into a 'single pane of glass' interface for analysis. This simplifies the administration and analysis process for the security team and helps address adherence to regulatory data protection compliance requirements.

Advantages of Agent-based Vulnerability Scanning

There are many environments where agent-based scanning is preferred. In environments that are widely distributed or have numerous remote employees, agent-based scanning is most effective. This allows the agent to return scan results to the collection server, even if they are located behind private subnets or non-corporate networks.

Some advantages of agent-based scanners include:

RELATED PRODUCTS

[Digital Defense](#)[Fortra Vulnerability Management](#)

RELATED SOLUTIONS

[Vulnerability Management](#)

Orca Security Ltd.

Exhibit 2104

Wiz v. Orca

IPR2024-00863, -00864, -00865

Ex. 2104-001

Device credential requirements

Agent-based scanners are designed to circumvent the need for credentials as the agents are installed directly on a device.

Reduced network traffic

Pre-installed agents reduce network traffic, and frequent network scans are replaced by rules that set event-driven or periodic scheduled scans.

No IP limitation

Another advantage of agent-based scanning is that it is not limited by IP. Assets using dynamic addressing or that are located off-site behind private subnets are still accessible with agent-based scanning as they connect back to the servers.

Coverage of disconnected devices

Devices that aren't perpetually connected to the network can still be scanned. Agents wait until a connection to the internet is re-established and then send data back to the server; thus, a scheduled scan can be paused and restarted if an interruption in the connection occurs. This feature can be desirable in a WFH environment or for active business travelers with intermittent Wi-Fi.

BYOD support

The increasing use of personal devices for corporate usage creates legitimate security concerns for organizations. Having agents installed provides the data on a device's security, such as if the device is fully patched. This intelligence can help to enforce corporate security policies.

Challenges with Agent-Based Vulnerability Scanning

One of the drawbacks of agent-based vulnerability scanning is that they are operating system (OS) dependent and generally can't scan network assets like routers, switches, and firewalls. However, most agent-based scanning solutions will have support for multiple common OSes.

Agent-based scanning also comes with administrative overhead as new devices added to the network must have agents installed. While updates of agents are usually automated, new installs and changes in scanners will require extra work for IT staff.

Agentless Scanning

Agentless scanning does not require agents to be installed on each device and instead reaches out from the server to the assets. While the data collected is similar to an agent-based approach, it eliminates installing and managing additional software on all devices. In this respect, this approach is a highly lightweight method to scan for security vulnerabilities.

Advantages of Agentless Vulnerability Scanning

There are many environments where agentless scanning is preferred. For environments where most of the devices are located within corporately controlled networks, agentless scanning allows for wider network analysis and assessment of all varieties of network devices.



- **Additional data:** Agentless scanning can provide some gap data not provided by Agent-based scanning. For example, agentless vulnerability scanners can locate [SSL certificates](#) that aren't stored on a device.
- **Network scanning:** Agentless scanning can observe the entire network and identify all hosts and devices connected. This allows the identification and scanning of assets that might be missed by agent-based scanning.
- **Agnostic:** There are no OS compatibility requirements to detect and scan assets. This allows for [IoT \(Internet of Things\)](#) and network-based devices such as routers and switches to be included in scans.

Challenges with Agentless Vulnerability Scanning

A severe drawback of the use of agentless scanning is the requirement for a consistent network connection. In a remote work environment with users behind home networks, their devices are not accessible to agentless scanners.

Agentless access also does not have the depth of visibility that agent-based solutions do. Agent-based software can see vulnerabilities hidden from remote solutions because it has [privileged access to the OS](#).

Best of Both Worlds

Using only agent-based or agentless scanning as the sole solution leaves gaps in the data collected. While agentless solutions provide a deeper view of the network than agent-based approaches, they fall short for remote workers and dynamic cloud-based environments. The symbiotic nature of agentless and agent-based vulnerability scanning offers a third option with unique advantages.

The combination of the two approaches allows more in-depth data to be collected. Issues about whether a device is off-site or managing agents for on-premises infrastructure are eliminated. In this way, organizations that need comprehensive visibility can create a highly efficient vulnerability scanning ecosystem.

Learn more about which vulnerability scanning approach is best for your organization and how Fortra Vulnerability Management can provide the best of both worlds.

LEARN MORE



AREAS OF EXPERTISE

- Infrastructure Protection
- Email Security & Anti-Phishing
- Data Protection
- Managed Security
- Compliance
- Managed File Transfer
- Automation

ABOUT

- About Fortra
- Security & Trust Center
- Newsroom
- Careers
- Partners
- Our Team
- Our Products

GET IN TOUCH

- Support
- Request Pricing
- info@fortra.com
- Join Our Mailing List

IBM Power Solutions

✕

Hi there! Can you tell me what you're looking for? 😊



1

f

twitter

in

✕

Hi there! Can you tell me what you're looking for? 😊



1

f

in

🐦