

WHITE PAPER

6 Reasons Why an Agent is Crucial for Your Cyber Security Defense



Beyond Traditional Network Scanning

Traditional vulnerability management is a cornerstone in a modern cyber security defense. The success of vulnerability management is not least based on its efficiency and simplicity. It is easy to get started, and you get broad coverage without major interference to your systems and devices. Public systems and networks are scanned from the cloud and local infrastructure using a locally installed probe that scans everything within its reach.

Using this technology, organizations can find, remediate, and follow up on vulnerabilities found in systems to strengthen their cyber security defense. But what about computers and the growing remote workforce using laptops? Here traditional vulnerability management has a weakness. The solution is a lightweight endpoint agent.

Agent-Based Vulnerability Management

With a drastically growing remote workforce, many organizations are looking into how to get complete coverage without the need for complex infrastructure or software. A lightweight endpoint agent will not only enable broader coverage. It also solves some of the "itches" that traditional vulnerability management has experienced since it was first established over 20 years ago. Here are six reasons why you also should adopt agent-based vulnerability management – as an addition to traditional vulnerability management.



Covering Remote Workers

The pandemic has drastically increased the number of remote workers. Traditional vulnerability management only scans systems and devices found within its reach, meaning that remote devices, such as laptops, will not be covered. A lightweight endpoint agent will scan laptops wherever they are. The agent will regularly collect and send data from the device to the vulnerability management platform for processing. Using less than 5 % CPU, the agent operates in the background without any impact on the users.



Stronger Defense against Ransomware

Over 90% of all attacks start with a fake email – so-called social engineering. Cybercriminals trick people into clicking on malicious files or documents that infect the computer with a virus. Sometimes this virus is the starting point of a ransomware attack. The virus will take advantage of any exploitable software vulnerability on the computer, using the infected computer to exploit other vulnerabilities and spread further into the organizations' network and systems.

Using a lightweight endpoint agent, you can find these vulnerabilities before they cause any harm. Together with Phishing & Awareness Training, this will create a solid first line of defense.



Scan without Actual Scanning

Although the vulnerability management scanning technology is well developed and safe, it can still have a negative impact on your systems and networks. Using a lightweight endpoint agent, you will simultaneously get more data out of the system and minimize the risk of negatively impacting systems.



Complete Coverage

One of the keys elements when working with vulnerability management is to have as complete coverage as possible to avoid blank spots. Remember that a hacker only needs one way into your systems. Using a lightweight endpoint agent, you can cover all laptops as well as systems.



More Data without Authentication

One of the challenges with traditional vulnerability management is that scanning is performed from outside of the system. Accordingly, these scans will only detect vulnerabilities that can be found from the outside. You can solve this by running authenticated scans. However, this requires the system to be within your network and you need to hand out credentials or use some other technology for authentication. Using a lightweight endpoint agent, you will get full access to the system wherever it is, safely and securely – without the need for credentials.



Follow Devices over Time

One of the challenges with vulnerability management is to follow mobile devices, like laptops, over time. Traditional vulnerability management requires static IP addresses as the unique identifier for tracking. Computers in office networks are usually connected using the DHCP protocol (Dynamic Host Configuration Protocol). This makes tracking based on IP addresses impossible. With a lightweight endpoint agent, you create a virtual band between the vulnerability management platform and the device, making it possible to track it over time. Together with Phishing & Awareness Training, this will create a solid first line of defense.



WHITE PAPER

6 Reasons Why an Agent is Crucial for Your Cyber Security Defense

The Benefits of an Agent

This is why you should use an agent together with traditional vulnerability scanning.

- ✓ It covers your remote workers wherever they work.
- ✓ It covers every corner of your environment.
- ✓ You'll get a complete picture based on in-depth data.
- ✓ It's a good alternative for systems that you don't want to scan.
- ✓ You're able to track and follow mobile devices, like laptops, over time.
- ✓ It helps to strengthen your defense against ransomware and virus attacks.



HOLM SECURITY

Lightweight Endpoint Agent

Holm Security provides a powerful lightweight endpoint agent called Device Agent. The agent is fully integrated with our platform with traditional scanning techniques. We love to tell you more about how our agent-based solutions can help you improve your coverage and accordingly strengthen your cyber security defense.

Get Started Today