nessus Agent

DATA SHEET

Nessus Agents™ compliment traditional scanning to give you visibility into additional IT assets—like endpoints, and other remote assets that intermittently connect to the internet. They collect asset and system information and send it back to Tenable.io® or Tenable.sc™ (formerly SecurityCenter) for analysis. You get a low footprint agent that extends scan coverage and increases scan flexibility.

WHY YOU NEED NESSUS AGENTS

You can't protect what you can't see. Digitization and the ever-expanding enterprise have changed the security landscape. As the boundaries of the traditional workplace expand, and organizations adopt an increasingly mobile workforce, the lack of visibility into your IT environment is a major challenge.

Scan performance and host accessibility are also a challenge. Many organizations have employees who telecommute or bring their laptops home at night. Because traditional scanning solutions required systems to be accessible when a scan was executed, if those laptops weren't VPN-connected when a scan was happening, they wouldn't get scanned, leaving you blind to their vulnerabilities.

Nessus Agents compliment traditional scanning to extend your scan coverage and give you visibility into all assets.

Using Nessus Agents helps solve these problems. Nessus Agents are a lightweight program that can be installed on any asset—in the cloud or on-prem—to perform scans and collect vulnerability and compliance data from hard to reach assets.

EXTEND SCAN COVERAGE BEYOND TRADITIONAL SCANNING

Nessus Agents work where it's not practical or possible to do network scans. They are a critical tool in the broader data collection arsenal and our preferred method for scanning assets like endpoints and other transient devices that are not always connected to the corporate network or that may need special consideration. Traditional scans are well suited to assessing assets like servers and static desktops. To get the greatest visibility into your entire network a combination of traditional scanning with Nessus and agent-based scanning with Nessus Agents is recommended. Combining traditional scanning with agent-based scans gives you a unified view of your data, across all IT assets, giving you get instant visibility into vulnerabilities and where to focus.

KEY BENEFITS

- **Extend scan coverage** to laptops and other transient devices.
- **Remove credential headaches –** once deployed, agents no longer require host credentials to run future scans
- **Reduce network scan performance overhead**
- **Easy to deploy and can be installed anywhere**
- **Highly secure –** including leveraging encryption to protect your data
- **Scan quickly –** perform rapid scans on demand with little network impact

QUICKLY SCAN ENDPOINTS AND OTHER TRANSIENT DEVICES

With Nessus Agents, you no longer need to worry about excluding assets that are offline during a scan window or not connected to the network. The lightweight agent is installed locally on an endpoint or any other host—a laptop, virtual system, desktop and/or server. The agent runs as a service on each asset—that non-administrative users cannot disable.

Agents receive scanning instructions from Tenable.io or Tenable.sc, perform scans locally and identify vulnerabilities, policy-violating configurations and malware on hosts where they are installed. They check in when they can connect to the management platform and then report the scan results back to the platform to mitigate missing systems scans.

Agents can perform scans at any time, even when the endpoints they're running on aren't connected to the corporate network. And because each agent runs its local scan independent from other scanners, assessments complete and report their results back to Tenable.io or Tenable.sc quickly.

nessus Agent

DATA SHEET

SIMPLIFY CREDENTIAL MANAGEMENT WITH AGENT-BASED SCANNING

Nessus Agents make it easier to do credentialed vulnerability scans because after the agents are installed, they don't need ongoing host credentials. When you first install Nessus Agents (either manually or with a software management system), you install them under the local SYSTEM account in Windows or root on Unix-based operating systems. The agents then inherit the permissions of the account used for installation so they can perform credentialed scans, even if the credentials on the system have changed.

Even better, Nessus Agents are easily deployable and auto update once deployed, so you don't need to worry about ongoing agent management.

MINIMAL IMPACT ON SYSTEMS AND NETWORK

Nessus Agents can be installed anywhere—on any host—in the cloud, mobile, on-prem or on any endpoint. They're designed to have minimal impact on the system and the network, giving you the benefit of direct access to all hosts without disrupting your end users. Nessus Agents average footprint is 1.6MB on disk, they use less than 40 MB of RAM at rest.

They can be deployed using most software management systems. Once deployed, Nessus Agents automatically download and install regular updates without requiring a reboot or end user interaction. Agents also ease scanning systems over segmented or complex networks. And because agents rely on local host resources, they can reduce network bandwidth need, which is important for remote facilities connected by slow networks

SYSTEM REQUIREMENTS FOR NESSUS AGENTS

Nessus Agents support Mac, Linux and Windows operating systems.

Your hosts must be able to reach Tenable.io on port 443, or On-Prem Agent Manager over HTTPS port 8834.

OTHER TENABLE SOLUTIONS

Tenable provides the world's first Cyber Exposure platform to see and secure any asset on any platform. This integrated suite supports Nessus Agents and includes:

Tenable.io for Vulnerability Management
Tenable.io Container Security
Tenable.io Web Application Scanning
Tenable.io PCI ASV
Tenable Lumin
Tenable.sc (formerly SecurityCenter)

TRY IT TODAY

Try Nessus Agents with a free 60-day trial of Tenable.io:
https://www.tenable.com/how-to-buy

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**