



Nessus Agents

Confidential and Proprietary

Please note, this offer, which incorporates Tenable's Subscription Agreement, including software usage terms and conditions, supersedes all other prior or contemporaneous communications between the parties (whether written or oral) relating to Tenable's response to this proposal/tender. In the event a customer chooses to make an award based upon Tenable's response herein, only the terms of the Subscription Agreement, as negotiated by the Parties at the time of award, shall govern the license of software from Tenable to the customer. The terms contained in this RFP shall not apply to Tenable's offer, nor to any subsequent award or license. Copies of Tenable's software license agreements can be viewed at:

TABLE OF CONTENTS

I. INTRODUCTION	3
II. WHAT ARE NESSUS AGENTS?.....	4
III. SCANNING.....	5
IV. RESULTS.....	6
V. CONCLUSION.....	7
VI. ABOUT TENABLE	7

I. INTRODUCTION

Digitization and the ever-expanding enterprise have changed the security landscape. The classic, contained enterprise no longer exists. There has been an explosion of new platforms, new asset types and new approaches. The tools and approaches organizations used in the old world of client/server, on premise data centers whose boundaries often consisted primarily of desktop PCs or servers, no longer work.

As the boundaries of the traditional workforce expand, and organizations adopt cloud computing services and an increasingly mobile workforce, the lack of visibility into IT environments becomes a major challenge.

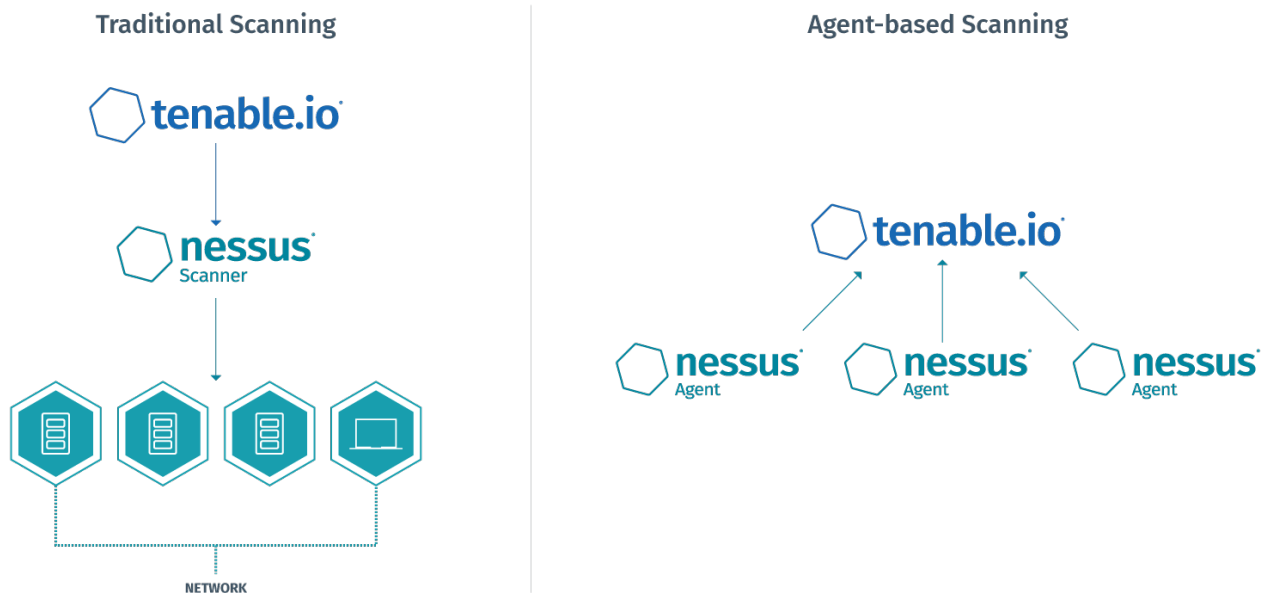
Tenable offers Nessus® Agents to meet the challenges that organizations face in today's modern age of cloud computing and mobility. Nessus Agents extend scan coverage and provide visibility into hard to scan assets-like endpoints and other remote assets that intermittently connect to the internet. When combined with traditional scanning from Nessus you get a unified view of your security and compliance data across all IT assets, giving you instant visibility into vulnerabilities and where to focus.

Nessus Agents also help to address additional challenges that organizations face, such as the management of credentials on target hosts and asset availability.

In some organizations, obtaining and managing credentials can cause considerable problems. Nessus Agents solve this problem because after the agents are initially installed they no longer require host credentials to run future scans, even if the credentials change.

Agents also solve the challenge of asset availability. Geographically distributed sales teams, remote workers and traveling executives can easily create gaps in asset availability during a vulnerability scan. While traditional network scans have to originate from a scanner that reaches out to the hosts being scanned, using Nessus Agents, hosts can run the scan while they're not on the network, and then call back in to Tenable.io™ or On-Prem Agent Manager (for managing agents in Tenable.sc) once they obtain their results.

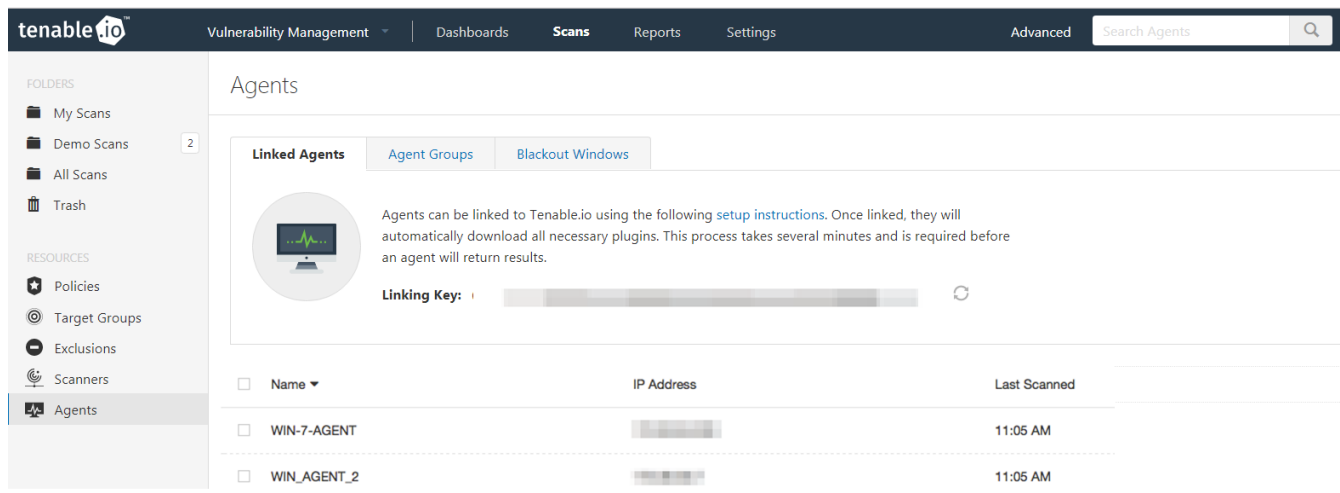
Combining traditional scanning with agent-based scanning helps to eliminate gaps in your scan coverage, increase your visibility and reduce your cyber risk.



II. WHAT ARE NESSUS AGENTS?

Nessus Agents are lightweight programs that are installed locally on a host. Agents collect vulnerability, compliance and system data and report that information back to a manager. Nessus Agents currently support Windows, Mac and many flavors of Linux. To see the latest supported operating systems, visit docs.tenable.com and look for System Requirements in the Nessus documentation.

Agents run under the local SYSTEM account in Windows or root on Unix-based operating systems, and require sufficient privileges to install software under that account on setup. Nessus Agents are packaged for installation on their respective platforms, and after installation, a scriptable command can be used to register the agent with Tenable.io Vulnerability Management or Tenble On-Prem Agent Managers (for Tenable.sc or Tenable.sc Continuous View). Once agents are connected, they send host and vulnerability reports back to one of these managers. Agents are also managed and updated via the managers.



The screenshot shows the Tenable.io interface for managing agents. The top navigation bar includes 'Vulnerability Management', 'Dashboards', 'Scans', 'Reports', 'Settings', and 'Advanced'. A search bar for agents is also present. The left sidebar lists folders like 'My Scans', 'Demo Scans', 'All Scans', and 'Trash', along with resources like 'Policies', 'Target Groups', 'Exclusions', 'Scanners', and 'Agents'. The main content area is titled 'Agents' and features tabs for 'Linked Agents', 'Agent Groups', and 'Blackout Windows'. A section titled 'Linked Agents' contains a circular icon and text explaining that agents can be linked to Tenable.io using setup instructions. Below this is a 'Linking Key' field with a refresh button. A table below lists the linked agents:

<input type="checkbox"/>	Name	IP Address	Last Scanned
<input type="checkbox"/>	WIN-7-AGENT	[REDACTED]	11:05 AM
<input type="checkbox"/>	WIN_AGENT_2	[REDACTED]	11:05 AM

By default, Nessus Agents communicate back to Tenable.io Vulnerability Management or On-Prem Agent Manager in the same way that standard Nessus scanners do: over TCP port 8834 for On-Prem Agent Manager or port 443 for Tenable.io. That communication is encrypted with AES-256 encryption, depending on configuration at the time of installation.

Because Nessus Agents are packaged for easy installation, they can be deployed using software management systems such as Microsoft's System Center Configuration Manager (SCCM). Additionally, the configuration of Nessus Agents can be scripted, which allows administrators to easily deploy agents across multiple systems with minimal effort. All of this can be done without needing to create additional administrator or service accounts on the network.

Once agents are deployed, there are several options for updating them. There's an auto-update option where agents will update themselves as needed. It's also possible to disable the auto-updates and update Nessus Agents with a preferred software configuration management solution. And it's possible to auto-update but specify times when updates should NOT occur, for example, to direct agents to NOT update during 9am-5pm Monday-Friday.

III. SCANNING

Starting an agent-based assessment will look very familiar to existing Nessus users. It is very similar to running a scan in Nessus with a few slight differences. To get started, users will need to select a template from the new “Agents” section of the Scan Library. Instead of selecting a scanner or manually entering targets, users will be provided with an option to select groups of agents to serve as targets for the assessment. Users will then need to specify how long a scan is to run; this is the window of time in which targeted agents can check in and upload their results for a particular assessment.

New Scan / Advanced Agent Scan

[← Back to Scan Templates](#)

Settings | Compliance | Plugins

BASIC ▾

- General
- Schedule
- Notifications
- Permissions

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: My new agent scan

Description: This scan has been created using the Advanced Agent Scan template

Folder: My Scans

Agent Groups: My New Group ×

Scan Window: 1 hour

Agents must report within this timeframe to be visible in scan results.

Save | Cancel

There are four agent scan templates: Basic Agent, Policy Compliance Auditing, Windows Malware and Advanced, which is a combination of the other scan types. Additionally, there are a series of local configuration checks that can be run on the local host. Because each agent runs its local scan independent from other scanners, assessments complete and report their results back to Tenable.io Vulnerability Management or On-Prem Agent Manager quickly.

Scan Type	Capabilities
Basic Agent Scan	Local patch checking and local information gathering, such as users, status of antivirus software, software starting up via the registry, USB device history and more.
Policy Compliance Auditing	Checks hosts against administrator-specified compliance and system hardening and configuration policies.
Windows Malware Scan	Scans for malware on systems connected via Windows agents.
Advanced Agent Scan	A fully customizable agent scan that allows administrators to turn off specific plugins, check for malware and other harmful software, and more.

When a scan is initiated, On-Prem Agent Manager or Tenable.io Vulnerability Management (aka: the Manager) sends instructions to each Nessus Agent to run a configured scan. Once the scan has been initiated on the Manager, each agent in the defined scan group is given a certain amount of time to check back in to the Manager with their results. If an agent is offline or cannot connect back to the Manager within the defined window, it is treated the same way that an offline host would be in a traditional network scan, and doesn't appear in the results. A scan will show as still running while it waits for any agents that have not checked back in with their results.

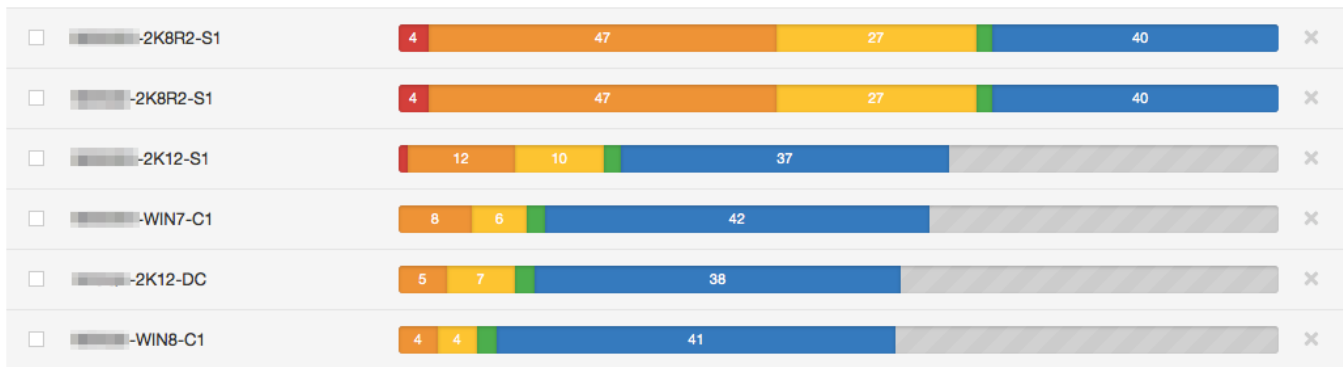
Agent Details

Groups: All
Reported: 7 of 16
Time Left: 18 minutes

When creating scans, administrators can choose between either traditional scans using full Nessus scanners or agent-based scans using Nessus Agents. Each type of scan serves a different role. Traditional, credentialed scans are well suited to assessing servers and static desktops, while agents can be used on laptops and other systems that may need special consideration. To achieve maximum visibility into your network the recommended method is a combination of traditional scans and agent-based scans. Because agents are easily added to existing Tenable.io Vulnerability Management deployments or On-Prem Agent Manager, organizations that simply wish to augment their existing assessment infrastructure with the flexibility that agents provide can do so.

IV. RESULTS

Scan results from Nessus Agents will look familiar to users who have previous experience with Nessus. Results are organized by the hostname of the device on which the agent is installed, and display the number of detected vulnerabilities. Results management, for the most part, remains similar to that of traditional Nessus usage, where reports can be generated and sent to administrators or analysts for action.



However, by using Nessus Agents on individual laptops or workstations, additional reporting options are available for organizations.

V. CONCLUSION

Nessus Agents help organizations meet the challenges of an increasingly mobile workforce by providing visibility into parts of an organization's network that would have previously been difficult or impossible to scan like transient devices and other remote assets that intermittently connect to the internet. Agents provide increased flexibility and scan accessibility, while giving organizations options for scanning their networks and deploying Nessus. Combining traditional scanning with agent-based scanning ensures you have full visibility into all your IT assets to minimize cyber risk.

VI. ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 24,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

COPYRIGHT 2018 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS