nessus Network Monitor

DATA SHEET

Continuous monitoring uncovers unauthorized devices, vulnerabilities and untrusted relationships with deep packet inspection.

PRODUCT OVERVIEW

Nessus® Network Monitor provides continuous visibility into the systems and services running on your networks, for unmatched asset insight. From legacy assets to the latest technologies, it illuminates blind spots so you can see and protect your entire environment. Nessus Network Monitor detects new and unmanaged assets – spanning operating systems, network devices, hypervisors, databases, mobile devices, web servers, cloud applications, IoT devices and more. As part of Tenable.ot, Nessus Network Monitor offers enhanced OT support – including asset discovery and protocol detection – for passively monitoring industrial control systems (ICS), SCADA systems and other operational technology. This gives security teams a safe and non-intrusive way to discover and monitor sensitive critical infrastructure systems.

The product's patented network discovery and vulnerability analysis technology delivers continuous monitoring and profiling non-intrusively. It monitors IPv4, IPv6 and mixed network traffic at the packet layer to determine topology, services and vulnerabilities. Nessus Network Monitor serves as an integrated component of Tenable.io™ Tenable.ot™ Tenable.sc™ and Tenable.sc Continuous View®, enabling full visibility into traditional and modern assets.

NESSUS NETWORK MONITOR BENEFITS

Core and distinguishing benefits of continuous monitoring with Nessus Network Monitor include identifying all devices and applications, vulnerabilities and detecting BYOD/mobile devices:

- Discover the full set of devices, applications and services active on your networks, including BYOD/mobile and other non-corporate owned assets – and the connections between them
- Accelerate vulnerability remediation by eliminating blind spots that would otherwise exist between active scans
- Discover and identify vulnerabilities in sensitive systems (such as OT systems) that cannot be actively scanned due to the risk of disruption or performance impact (requires Tenable.ot)
- Immediately identify potential security exposures created by vulnerable assets and new or rogue systems
- Demonstrate compliance with both internal policies and regulatory requirements by validating appropriate asset configurations

KEY FEATURES

Continuous Asset Discovery and Vulnerability Detection
Nessus Network Monitor continuously monitors network traffic for a variety of security-related information including:

- Detecting new assets added to a network
- Accelerate vulnerability remediation by eliminating blind spots that would otherwise exist between active scans
- Passively determining the operating system of each active host
- Applying more than 8,000 asset and vulnerability checks, covering a wide range of devices, communication protocols and asset categories — from IT to OT. As part of the Tenable.ot, Nessus Network Monitor delivers:
    - Coverage of ICS and SCADA systems in industrial, manufacturing, energy and oil & gas companies
    - Support for systems from dozens of manufacturers are supported including ABB, Emerson, GE, Honeywell, Rockwell/Allen Bradley, Schneider Electric and Siemens
- Detecting vulnerabilities on communicating systems and the protocols and applications used
- Summarizing top hosts, vulnerabilities, applications, operating systems and connections

Nessus Network Monitor delivers continuous monitoring and profiling of assets in a non-intrusive manner. The product analyzes network traffic at the packet level to provide visibility into both server- and client-side vulnerabilities with full asset discovery.

Nessus Network Monitor easily installs in networks and passively detects devices on your network, including virtual- and cloud-based devices, BYOD/mobile devices and even discovers jailbroken iOS devices. Nessus Network Monitor scales to meet the future demands of monitoring virtualized systems, cloud services and the proliferation of devices

Network, Web, FTP Monitoring
Nessus Network Monitor offers extensive web and FTP activity monitoring through direct analysis of the packet stream. By passively monitoring any HTTP or FTP transaction, Nessus Network Monitor can determine and report useful information about each host on your network, such as:

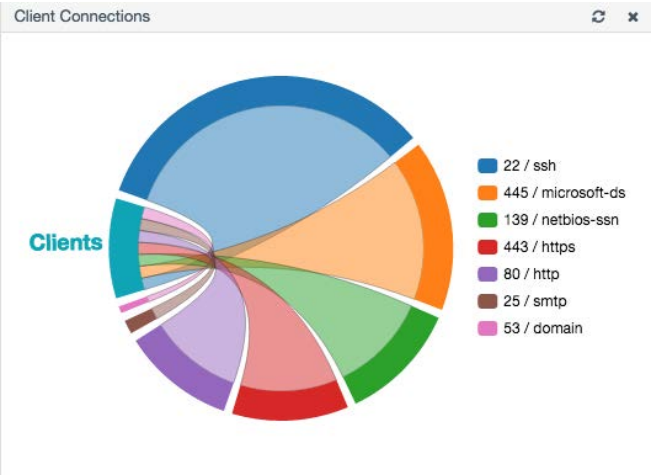
- All client and server web-based vulnerabilities and Applications
- Complete list of all web-agents used on each host
- Passive enumeration of all files shared via FTP

nessus Network Monitor

DATA SHEET

- Real-time logging of web GET, POST or file download
- Real-time logging of FTP file GET or PUT
- Real-time logging of DNS query monitor

This data is useful to analyze insider activity and malware infection or advanced threat compromise. Many of these logs can be sent to Tenable Log Correlation Engine® for further analysis, correlation, search and long-term storage.



Agentless Monitoring & Clientless Access
Nessus Network Monitor offers advanced protocol analysis of the Microsoft SMB protocol. If Nessus Network Monitor is deployed on the interior of a network where it can see Active Directory network traffic, it can automatically learn:

- Each system's hostname and workgroup name
- A list of all files shared on any folder
- The logins and file downloads from a network share in real time

The ability to passively determine this information in real time has tremendous forensic and situational awareness value. For large networks, passively determining all shared folder contents makes identification of potentially sensitive data much easier. Using Tenable.sc Continuous View, with the integrated Nessus Network Monitor and Log Correlation Engine modules, enables forensic analysis of employee activity and malware activity by examining records of files shared over the network.

SQL Database Logging & Monitoring
Nessus Network Monitor can also look at network traffic and identify SQL devices and the vulnerabilities associated with them, and log this activity in real time. Logs can be sent to the Log Correlation Engine for search, storage and analysis of attacks, including SQL injection from web services. Full instrumentation of all SQL activity can be achieved by combining the Nessus Network Monitor data with Nessus® SQL database configuration and vulnerability auditing data, as well as log data gathered from an SQL database server with a Log Correlation Engine agent.

Passive Topology Discovery & Service Identification Analysis
Data analysis for specific client or server vulnerabilities is performed by reconstructing both sides of network communications. Unique protocols, such as HTTP, SMTP and FTP, have specific strings that identify the version of the service. Nessus Network Monitor identifies these and associates them with specific vulnerability plugins or tests.

Identification of TLS-Encrypted Applications
Unless organizations deploy relatively expensive devices to decrypt TLS, they are blind to the use of web applications that may pose significant security risk and/or violate acceptable use policy. Nessus Network Monitor can identify a number of TLS-encrypted applications without deploying additional network devices. Example applications are Dropbox, Tor uplink and Golang.

PCI DSS COMPLIANCE

The PCI DSS requires accurate and comprehensive identification of all systems involved in the transmission, processing or storage of credit card data. These systems collectively comprise the "cardholder data environment" (CDE) where the PCI DSS controls must be consistently applied and validated on an annual basis. Organizations must also provide evidence of procedures to maintain the integrity of the CDE. Nessus Network Monitor not only monitors known data flows in and out of the CDE but also identifies undocumented data flows, particularly of unencrypted payment card information.

DEPLOYMENT OPTIONS

Nessus Network Monitor is available at two performance levels: standard (1 Gbps), included as a data sensor with Tenable.io™ Tenable.ot™ and Tenable.sc Continuous View or high performance (10 Gbps) – as a standalone product.

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