tenable network security

Nessus® cloud

Cloud-Based Vulnerability Management

Nessus® Cloud is Tenable's hosted, cloud-based vulnerability management solution that combines the powerful detection, scanning and auditing features of Nessus with multi-user support, enabling sharing of scanning resources like scanners, policies, schedules and reports.

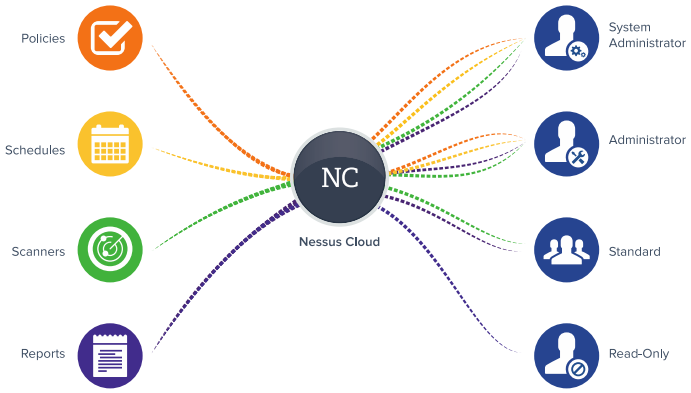
In addition, Nessus Cloud is Tenable's Approved Scanning Vendor (ASV) solution for validating adherence to certain PCI DSS requirements for performing vulnerability scans of Internet facing systems.

Bring the Power of Nessus to Teams

Nessus Cloud enables security and audit teams to share multiple Nessus scanners, scan schedules, scan policies and most importantly scan results among an unlimited set of users or groups.

By making different resources available for sharing among users and groups, Nessus Cloud allows for endless possibilities for creating highly customized work flows for your vulnerability management program, regardless of locations, complexity, or any of the numerous regulatory or compliance drivers that demand keeping your business secure.

In addition, Nessus Cloud can control multiple Nessus scanners, schedule scans, push policies and view scan findings—all from the cloud, enabling the deployment of Nessus scanners throughout your network to multiple physical locations, or even public or private clouds.



As seen in SC MAGAZINE FOR IT SECURITY PROFESSIONALS

June 2016 Review

"What it does – vulnerability management – it does as well or better than any system we've seen"

Key Benefits

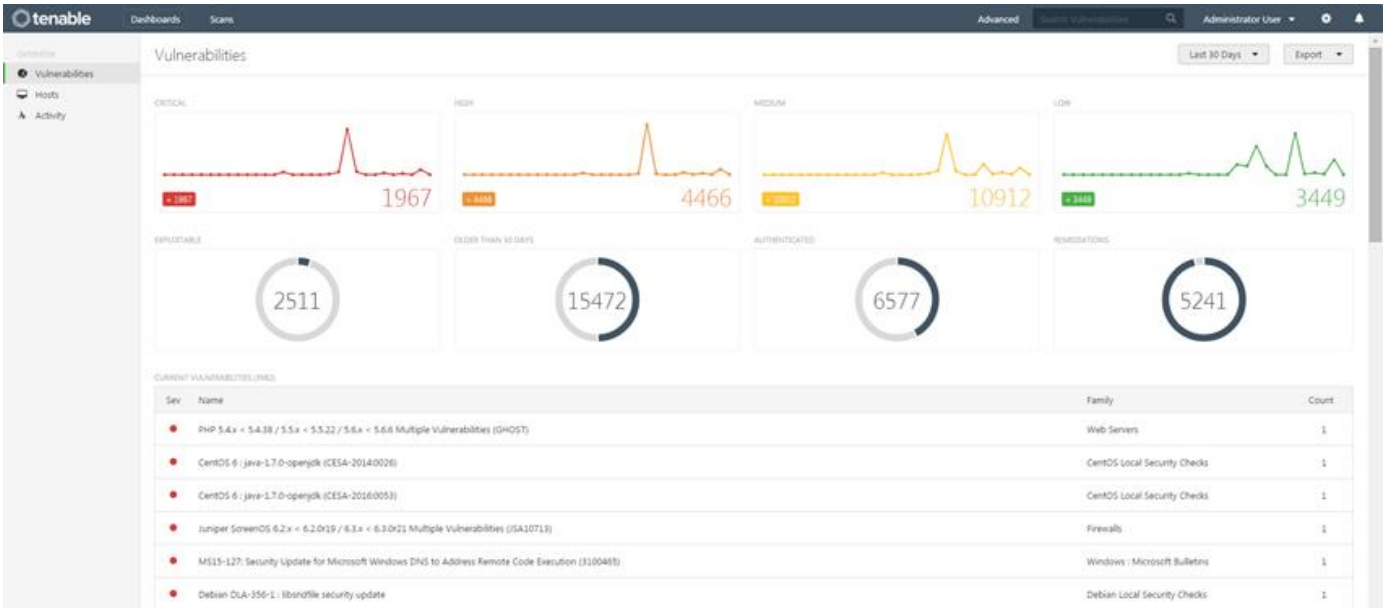
- **Hosted vulnerability management:** No software to deploy or maintain
- **Accurate, proven and fully supported scanning:** Based on the Nessus vulnerability scanner
- **Share resources:** Assign scanners, policies and schedules, and report access to multiple users or groups
- **Assign users:** Delegate additional admins, assign responsibilities and permissions
- **Expand scan coverage:** Nessus Agents scan hard-to-scan assets such as ones not connected to the network during an active scan

Nessus Cloud is a PCI-Certified Approved Scanning Vendor (ASV) Solution

Nessus Cloud is a PCI-Certified Approved Scanning Vendor (ASV) solution that lets merchants and service providers demonstrate their Internet-facing systems are secure according to PCI Data Security Standard (PCI DSS) external network vulnerability scanning requirements.

PCI Security Standards Council™

APPROVED SCANNING VENDOR



Key Features

Cloud Vulnerability Management

External and internal scans can be scheduled to run automatically or performed on demand. The multi-scanner and resource management capability offered by Nessus Cloud enables you to manage your entire scanning program regardless of how many locations you have or how complex the architecture of your network.

Continually Updated

Nessus Cloud is supported by a world-renowned research team and accesses Tenable's continuously-updated database of the world's largest collection of vulnerability and configuration checks. Web-facing applications can be scanned for vulnerabilities that may increase an organization's exposure to risk. External vulnerability scans are conducted against current PCI DSS standards.

Tight Integration and API Extensibility

Nessus Cloud integrates with patch management, Mobile Device Management (MDM) and password vault solutions that complement a strong vulnerability management program.

Cloud Infrastructure Support

Nessus Cloud reduces the attack surface in Amazon Web Services (AWS), Microsoft Azure and Rackspace clouds by auditing and scanning these cloud deployments. Nessus Cloud also includes a pre-authorized scanner for AWS environments.

Remediation Prioritization

Nessus Cloud provides secure access to detailed vulnerability audit and remediation information. Multiple filters and criteria are available to prioritize remediation workflow.

Nessus Agents

Nessus Agents, available with Nessus Cloud and Nessus Manager, alleviate headaches associated with traditional network scanning, like getting credentials, while making it easy to scan a wider array of assets, including ones that are offline.

Most organizations will use a mix of agent-based and agent-less scanning in their Nessus environment. Nessus Agents will be attractive in a number of scenarios, including:

- **Transient Devices**: Scanning of laptops or other transient devices that are not always connected to the local network.
- **Scanning Without Host Credentials**: Assets that you want or need to scan without credentials.
- **Scanning Quickly**: Once deployed, agents use local host resources for scanning and only use network resources to send results back to Nessus Cloud, making it easy if you want or need to scan a large number of assets quickly.

Training

Tenable offers training for those who are new to using Nessus and want the knowledge and skills to maximize use of the product, as well as focused topics like compliance auditing for more advanced users. Courses are available on-demand via the Tenable website.

tenable® network security

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