tenable™

Nessus NM™ Manager

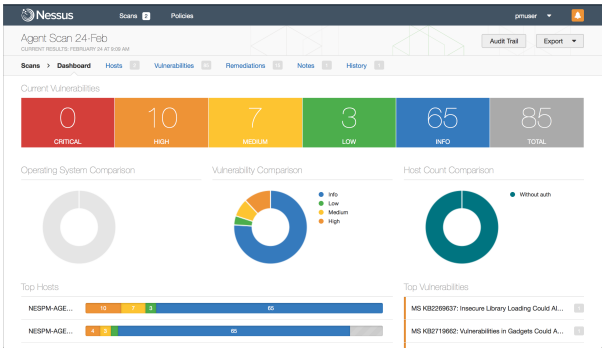
Nessus Manager extends the power of Nessus to security and audit teams, with centrally managed distributed scanning

Vulnerability Management for Teams

Nessus® Manager combines the powerful detection, scanning and auditing features of Nessus, the world's most widely deployed vulnerability scanner, with extensive management and collaboration functions to reduce your attack surface.

Nessus Manager enables the sharing of resources including Nessus scanners, scan schedules, policies and scan results among multiple users or groups. Users can engage and share resources and responsibilities with their co-workers; system owners, internal auditors, risk & compliance personnel, IT administrators, network admins and security analysts. These collaborative features reduce the time and cost of security scanning and compliance auditing by streamlining scanning, malware and misconfiguration discovery, and remediation.

Nessus Manager protects physical, virtual, mobile and cloud environments. Nessus Manager is available for on-premises deployment. Tenable.io™ Vulnerability Management is available for organizations looking for a cloud-hosted solution. Nessus Manager supports the widest range of systems, devices and assets, and with both agent-less and Nessus Agent deployment options, easily extends to mobile, transient and other hard-to-reach environments.



Multi-Scanner Support

Nessus Manager enables the control of multiple Nessus scanners making it easy to extend scanner coverage over complex networks, cloud deployments and geographically distributed locations. Users may schedule scans, push policies and view scan results across multiple scanners from a single, central console.

Integration

Nessus Manager integrates with patch management solutions from IBM, Microsoft, Red Hat and Dell to help ensure that software updates are applied to systems and assets in accordance with their criticality to the organization.

Nessus Manager also integrates with Mobile Device Management (MDM) solutions from Microsoft, Apple, Good, MobileIron and AirWatch to enable organizations to add mobile devices to the vulnerability management program.

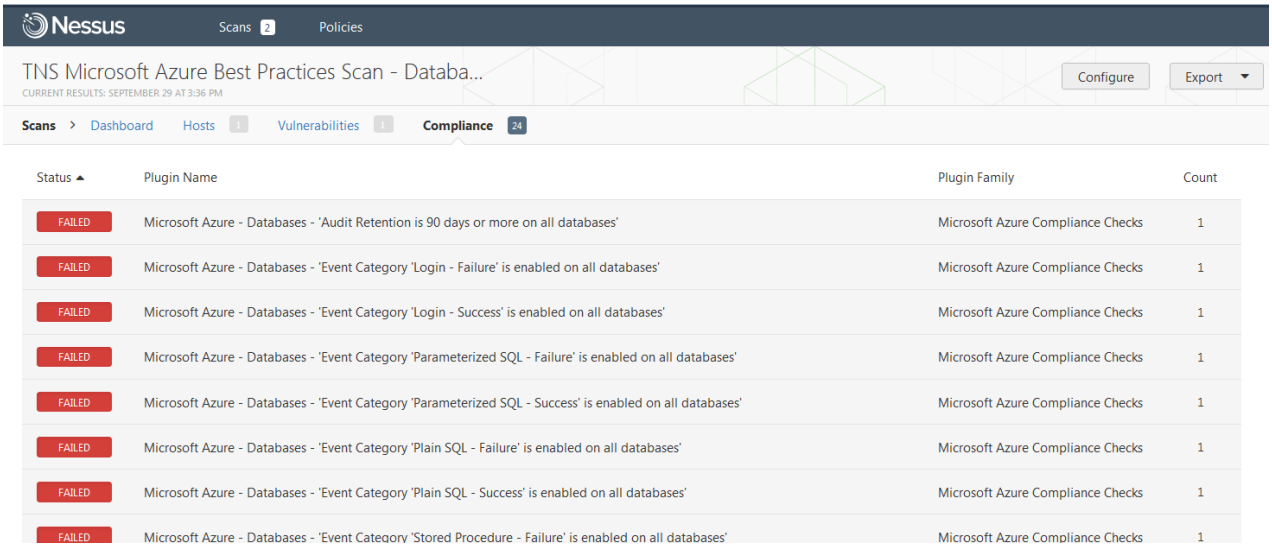
Password vault integration with CyberArk makes credential management easier for organizations using the CyberArk solution.

Nessus Manager reduces the attack surface and helps ensure compliance by auditing and scanning cloud deployments such as Microsoft Azure, AWS and Rackspace.

Key Benefits

- Accurate, proven and fully supported scanning: Based on the Nessus vulnerability scanner
- Share resources to improve team efficiency: Assign scanners, policies and schedules, and report access to multiple users or groups
- Expand scan coverage: Use Nessus Agents to scan transient devices like laptops or assets where you do not have host credentials
- Improve risk analysis: Include context from existing infrastructure and partner frameworks
- Integrate with core technologies: Nessus Manager lets you leverage your investment in complementary technologies like patch and mobile device management

SC MAGAZINE



Nessus Manager includes a number of configuration audits for cloud deployments such as Microsoft Azure, Amazon Web Services, Rackspace and others.

Role-Based User Levels

Nessus Manager allows for the addition of multiple users and introduces four user roles: System Administrator, Administrator, Standard and Read-Only. Each user may be assigned various levels of access to resources based on individual or group association. The System Administrator and Administrator have the authority to manage users and groups. Groups can be established based on departments, job function, duties or responsibilities, geography – whatever works best to fit your specific needs.

Research Team

Vulnerabilities and new threats are constant, so the Tenable Research Team provides frequent updates to Nessus Manager to help organizations combat advanced threats, zero day vulnerabilities and new types of regulatory compliance configurations.

The Nessus Advantage

Customers choose Nessus because it offers:

- Highly accurate scanning with low false positives
- Comprehensive scanning capabilities and features
- Scalable to hundreds-of-thousands of systems
- Easy deployment and maintenance
- Low cost to administer and operate

Nessus Agents

Nessus Agents, available with Tenable.io 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 Manager, 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™

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