Nessus® Professional

Nessus has been deployed by more than one million users across the globe for vulnerability, configuration and compliance assessments

Nessus Professional Vulnerability Scanner

Nessus® Professional, the industry's most widely deployed vulnerability assessment solution helps you reduce your organization's attack surface and ensure compliance. Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and more.

Nessus supports more technologies than competitive solutions, scanning operating systems, network devices, next generation firewalls, hypervisors, databases, web servers and critical infrastructure for vulnerabilities, threats and compliance violations.

With the world's largest continuously updated library of vulnerability and configuration checks, and the support of Tenable's expert vulnerability research team, Nessus sets the standard for vulnerability scanning speed and accuracy.

Nessus Features

Reporting and Monitoring

- Flexible reporting: Customize reports to sort by vulnerability or host, create an executive summary or compare scan results to highlight changes
  - Native (XML), PDF (requires Java be installed on Nessus server), HTML and CSV formats
- Targeted email notifications of scan results, remediation recommendations and scan configuration improvements

Complete Vulnerability Coverage

- Virtualization & cloud
- Malware & botnets
- Configuration auditing
- Web applications

Key Benefits

- **Reduce the attack surface**: Prevents attacks by identifying vulnerabilities that need to be addressed
- **Comprehensive**: Meets the widest range of compliance and regulatory standards
- **Scalable**: Start with a Nessus Professional single user license and move to Nessus Manager or Tenable.io as your vulnerability management needs increase
- **Low total cost of ownership** (TCO): Complete vulnerability scanning solution for one low cost
- **Constantly updated:** New content continually being added by the Tenable research team

Scanning Capabilities

- Discovery: Accurate, high-speed asset discovery
- Scanning: Vulnerability scanning (including IPv4/IPv6/hybrid networks)
  - Un-credentialed vulnerability discovery
  - Credentialed scanning for system hardening and missing patches
  - Meets PCI DSS requirements for internal vulnerability scanning
- Coverage: Broad asset coverage and profiling
  - Network devices: firewalls/routers/switches (Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage
  - Offline configuration auditing of network devices

- Virtualization VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server
- Operating systems: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries
- Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
- Web applications: Web servers, web services, OWASP vulnerabilities
- Cloud: Scans the configuration of cloud applications like Salesforce and cloud instances like Amazon Web Services, Microsoft Azure and Rackspace
- Compliance: Helps meet government, regulatory and corporate requirements
- Helps to enforce PCI DSS requirements for secure configuration, system hardening, malware detection, web application scanning and access controls

- Threats: Botnet/malicious, process/anti-virus auditing
  - Detect viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes, web services linking to malicious content
  - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, SCAP, SOX
  - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA, PCI
- Control Systems Auditing: SCADA systems, embedded devices and ICS applications
- Sensitive Content Auditing: PII (e.g., credit card numbers, SSNs)

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

Deployment and Management

- Flexible deployment: software, hardware, virtual appliance deployed on-premises or in a service provider's cloud.
- Scan options: Supports both non-credentialed, remote scans and credentialed, local scans for deeper, granular analysis of assets that are online as well as offline or remote.
- Configuration/policies: Out-of-the-box policies and configuration templates.
- Risk scores: Vulnerability ranking based on CVSS, five severity levels (Critical, High, Medium, Low, Info), customizable severity levels for recasting of risk.
- Prioritization: Correlation with exploit frameworks (Metasploit, Core Impact, Canvas and ExploitHub) and filtering by exploitability and severity.
- Extensible: RESTful API support for integrating Nessus into your existing vulnerability management workflow.

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