tenable™

Nessus NP™
Professional

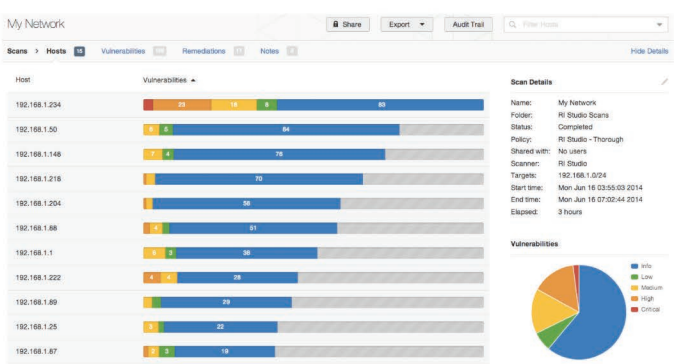
Nessus has been deployed by more than one million users across the globe for vulnerability, configuration and compliance assessments

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.



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

SC MAGAZINE

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

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