TENABLE Network Security®

Product Features & Tech Specs

SecurityCenter

Tenable SecurityCenter enables real-time scanning, log analysis, compliance auditing and security monitoring.

Alerting Actions
- Create ticket
- Email one or more users
- In-system event notification
- Launch existing Nessus scan
- Send syslog

Alerting Logic
- Greater than, less than, equal and not equal for any query
- Independent policy alerting schedules
- Event IP count queries
- Event count queries
- Event port count queries
- Vulnerability IP count queries
- Vulnerability count queries
- Vulnerability port count queries

Asset Discovery and Filtering
- IP address watch lists
- Nessus scan results
- Passive Vulnerability Scanner discovered nodes
- Log Correlation Engine IP address queries
- Manual IP list upload
- API IP list upload
- Regular expressions
- Classification by OS
- Classification by app
- Classification by domain
- DNS and name patterns
- LDAP
- Boolean logic to filter assets

Configuration Audit Policy Management
- Upload new .audit policies
- Associate .audit policies with scan policies
- Share .audit policies with organization
- Share .audit policies with Nessus ProfessionalFeed users

Console Login Authentication
- TNS local authentication (username/passwords)
- LDAP authentication
- Enforce custom login banners
- Digital Certificate, including DoD Common Access Card (CAC)
- CoSign authentication

Credential Management for Scanning
- Role based access to stored credentials
- Kerberos
- SNMP
- SSH
- SU/SUDO
- Telnet
- Windows Domain
- Web authentication

Dashboard Data Sources
- Vulnerabilities
- Missing patches
- Configuration information
- Any log events
- User activity
- Network activity
- Nessus Perimeter Service scans

Dashboard Graph Types
- Tabbed interface of multiple dashboards
- Bar charts
- Pie charts
- Single and multiple trend lines
- Programmable tables with icons, bars, and texts
- Dashboard import and export
- Up-to-date Dashboards downloadable from Tenable Blog

Data Analysis Output
- Export results as CSV
- Save matching IP addresses as Asset List
- Open ticket for matching IP addresses
- Save filter as query for re-use
- SecurityCenter Report Import/Export
- Auto Report at end of scan
- Auto Report on an alert
- SecurityCenter Report sharing

Data Filtering Options
- IPv4 and IPv6 addresses
- Ports
- Protocols
- Event type and name
- Asset
- User
- Date or time range
- Inbound, outbound, external events
- Plugin family
- Scan Policy
- Plugin ID
- Severity
- Active, Passive or Compliance plugins
- Matching text searches
- Days since vulnerability was observed
- Days since vulnerability was found
- Reoccurring vulnerabilities
- Re-casted severity adjustments
- Risk Accepted vulnerabilities
- Specific SecurityCenter repository

Data Management
- Scan results stored in separate repositories
- Repository sharing with multiple SecurityCenters
- Manual Nessus scan result uploads
- SC4 API for automatic data queries
- CSV data exports
- Full saved log search results text download
- Individual scan results saved for retention and download

TENABLE Network Security®

7063 Columbia Gateway Drive • Suite 100 • Columbia, MD 21046
410.872.0555 • www.Tenable.com

Detailed Event and Vulnerability Analysis Tools

- Asset summary
- Event and type summary
- Plugin family summary
- Protocol summary
- List each unique OS
- List each event
- Summarize events by date
- Summarize events by sensor
- Summarize events by user
- Severity summary
- Summary by Class C addresses
- Summary by Class B addresses
- Summary by Class A addresses
- Summary By IP address
- Summary by port
- Vulnerability summary
- Detailed syslog display
- Detailed vulnerability details
- Trend matching events
- CVE summary
- IAVA Summary
- Microsoft patch summary
- User activity summary
- DNS Summary

Distributed Scanner Support

- Push latest plugins to remote scanners
- Support for up to 512 Nessus scanners
- External and internal Nessus deployment
- Grouping of Nessus scanners into zones
- Load balanced scans across multiple scanners
- Multiple Passive Vulnerability Scanners
- Status updates for managed, unmanaged, and Perimeter Service scanners

Log Search

- Boolean logic to search logs
- Search limited to specific dates
- Saved searches can be re-launched
- Distributed searches with multiple Log Correlation Engines

Licensing

- Licensed by active nodes
- No need to tell Tenable your IP addresses
- Unlimited discovery scans
- Upgrades for increased IP counts easily procured and added to production systems
- Includes up to 512 Nessus scanners
- Passive Vulnerability Scanner and Log Correlation Engine purchased separately

Report Chapter Types

- Custom paragraph
- Tables
- Pie chart
- Bar chart
- Single and multiple trend lines
- Automatically creates individual report sections for each IP, port, user, or vulnerability, based on custom filters

Report Filter Options

- Vulnerability discovery date
- Last seen vulnerability date
- Asset-based report filtering
- Nessus plugin family
- Port, protocol and IP address
- Events by user
- Normalized and true IDS event names
- Vulnerability correlated IDS events
- IAVM
- Exploit availability
- Vulnerability recurrence
- Plugin name
- CVE
- Microsoft patch
- CVSS score
- Vulnerability text strings
- Log text strings

Report Template Types

- CIS
- FISMA
- FDCC
- Common IT audits
- Common network monitoring reports
- OWASP 2010
- SANS CAG
- PCI
- Missing Patches
- Nessus Plugin Families
- Up-to-date Report Templates downloadable from Tenable Enterprise Reporting Blog

Report Output Formats

- PDF
- Password protected PDF
- Watermark for PDF reports
- RTF
- CSV
- 3D Visualization
- Log search text results
- Footer, Header and Table of Contents management
- Multiple landscape and letter layouts

Scan Policy Management and Schedules

- Daily, weekly, monthly and yearly
- Support for any Nessus scan preference
- Separate scan scheduled per asset
- Independent credentials used for scans
- Dozens of default scan policies
- Email notification of scan results
- Scan schedule copying
- Launch, pause and stop buttons for scans
- Nessus Policy Import/Export

Scan Types

- Nessus network vulnerability scans
- Nessus credentialed patch audits
- Nessus credentialed configuration audits
- Nessus Patch Management (IBM Tivoli, Red Hat Satellite, Microsoft WSUS/SCCM, VMware Go) scans
- Nessus web application audits
- VMware vSphere/ESX/ESXi
- Reactive scans based on emergence of new hosts, prior scan results, IDS events, detected system changes

Scheduled Actions

- Automatic compliance alerts
- Nessus vulnerability, patch and config scans
- Automatic Dashboard updates
- Report creation with optional email delivery
- Nessus and Passive Vulnerability Scanner plugin update and distribution
- Dynamic asset list creation

Ticketing

- Automatic creation based on policy alerting
- Manual creation based on vulnerability analysis
- Manual creation based on log/event analysis
- Association of security data with ticket

User Access Control

- Organizational resource sharing
- Role-based user creation
- Custom role profile creation
- Scan policy sharing
- Access limited to authorized assets
- User grouped into organizations
- Logging of user actions