



SecurityCenter

NEXT GENERATION SECURITY CONSOLE

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

Tenable SecurityCenter provides a centralized portal to organize, distribute, manage and report network security information to users across multiple organizations and to articulate the detected activity to executive management.

SecurityCenter organizes network assets into categories through a combination of network scanning, passive network monitoring and integration with existing asset and network management data tools. SecurityCenter correlates all this information with enterprise-wide log data to provide a comprehensive view of system and network activity. Organizations that deploy SecurityCenter experience an immediate increase in communication and effectiveness between their security, IT, management and audit teams.

KEY FEATURES

- > Flexible dashboards
- > Unlimited users with role-based access
- > Supports log aggregation/event monitoring (LCE)
- > Patch auditing
- > Multi-scanner management and distributed scanning
- > Asset management/monitoring
- > Web-based interface
- > Supports passive scanning (PVS)
- > Configuration auditing
- > Compliance reporting
- > Vulnerability repositories

KEY BENEFITS

- > Combines three solutions into one fully-integrated solution for a holistic view of your organization
- > Provides information gathering and operational status monitoring
- > Delivers security and vulnerability intelligence on-demand to responsible personnel
- > Provides extensive correlation and analysis tools to deliver out-of-the-box value
- > Quickly identifies and escalates security threats to the responsible party, mitigating risk of system downtime or service level disruptions
- > Provides incident management and advanced workflow to enable fast and effective incident response time
- > Provides flexible reporting with built-in compliance templates for accurate audit and compliance reports

PRODUCT HIGHLIGHTS

Unified Security Monitoring™

SecurityCenter provides critical business and technical advantages by combining three distinct solutions/markets into one fully integrated solution.

- > Real-time vulnerability and patch assessments plus vulnerability lifetime management using a combination of host-based, network and 24x7 passive vulnerability assessment technologies
- > Critical security event monitoring using log and event aggregation and normalization
- > Security event alerting using statistical network anomaly-based alerting and signature-based correlation alerts
- > Custom compliance monitoring using a combination of agentless configuration audit files designed for specific government regulations, best practices or company specific configurations, and signature-based alerting when defined alert criteria for non-compliance have been met

Return on Investment

Tenable's SecurityCenter benefits the bottom line by delivering:

- > Automation of tasks related to scanning, discovering and organizing network vulnerabilities and intrusion events
- > Management of events from multiple IDS sources such as Snort, Real-Secure, Dragon, Intrushield, Bro, NFR and NetScreen IDP (requires LCE module)
- > Commercial support for multiple Nessus® scanners that can be managed and updated from a single instance of SecurityCenter

Compliance Reporting and Analysis

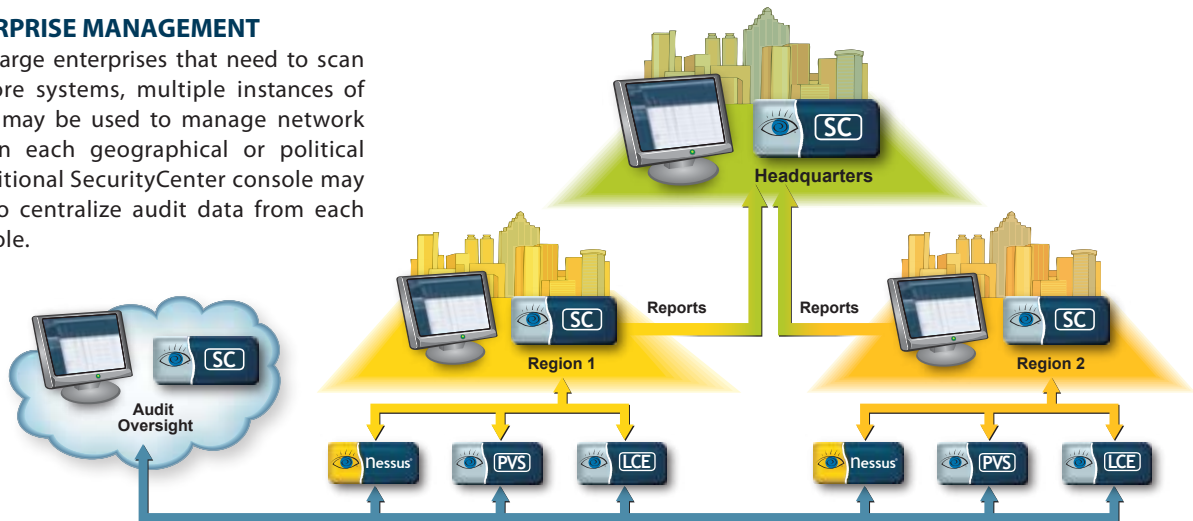
Tenable SecurityCenter can help detect and measure compliance with various regulatory and industry-established standards and report deviations from these standards. Audits are performed entirely with credentials and do not require the use of an agent.

Tenable's list of pre-configured audit policies include but are not limited to the following:

- > CIS audits for Unix and Windows
- > Microsoft vendor recommendations
- > PCI DSS configuration setting
- > FDCC and SCAP audits
- > DISA STIG audits

TIERED ENTERPRISE MANAGEMENT

For extremely large enterprises that need to scan 100,000 or more systems, multiple instances of SecurityCenter may be used to manage network auditing within each geographical or political region. An additional SecurityCenter console may be deployed to centralize audit data from each region or console.



TENABLE PRODUCT SUITE



SecurityCenter

Tenable SecurityCenter provides continuous, asset-based security and compliance monitoring. It unifies the process of asset discovery, vulnerability detection, data leakage detection, event management and configuration auditing for small and large enterprises.



Nessus® Vulnerability Scanner (Nessus®)

Tenable Network Security's active vulnerability scanner, Nessus®, is the world leader in active scanners, featuring high-speed discovery, asset profiling and vulnerability analysis of your security posture.

Passive Vulnerability Scanner (PVS)



Tenable Network Security's Passive Vulnerability Scanner is a network discovery and vulnerability analysis software solution, delivering real-time network profiling and monitoring for continuous assessment of your security posture in a non-intrusive manner.

Log Correlation Engine (LCE)



Tenable Network Security's Log Correlation Engine is a software module that aggregates, normalizes, correlates and analyzes event log data from the myriad of devices within your

infrastructure.



ProfessionalFeed™ Subscription

Commercial organizations that use the Nessus vulnerability scanner must purchase a ProfessionalFeed™ subscription to obtain support, updates to their database of vulnerability checks and compliance auditing.



Hardware Appliance

The Tenable Appliance that is available pre-installed on hardware comes in Series 100 and 200 models. Only available in the US.



VM Appliance

The Tenable Appliance for the Virtual Machine (VM) is available for VMware Server, VMware Player, VMware ESX, VMware Workstation and VMware Fusion. Currently the Nessus® and SecurityCenter applications are available on the appliance with LCE and PVS to be released soon.

HOW TO PURCHASE

To schedule an evaluation or request pricing, please contact: