

FortiScan™-3000C

Automated Compliance and Vulnerability Management

Efficient IT Governance, Risk & Compliance (ITGRC)

Today's businesses are required to address security and compliance risks on their IT infrastructure on a daily basis. ITGRC requirements affect IT security at multiple levels, from the network down to endpoint client machines and other network devices. Vigilance in keeping up with current operating System (OS) vulnerabilities and associated patches is critical as zero-day attacks at the OS level become more sophisticated. Maintaining homegrown and manual security compliance processes is no longer a viable option.

Automating Compliance at the Operating System Level

The FortiScan-3000C provides an enterprise-scale solution that integrates endpoint vulnerability management, industry and federal compliance, patch management, remediation, auditing and reporting into a single, unified appliance. It enables organizations to close IT compliance gaps and implement continuous monitoring for real-time results. The scan engine audits, evaluates the traffic at the OS and application level to help IT organizations comply with internal, industry and regulatory mandates. Organizations realize quick time-to-value with easy to install, intuitive and standard compliance policies (NIST SCAP, FDCC, PCI-DSS, SOX, GLBA, HIPAA) out of the box with regular updates from FortiGuard.

Minimal Impact and Low Total Cost of Ownership (TCO)

Failing to keep up with regulations, vulnerabilities and patches for the OS can have grave cost implications. FortiScan simplifies the process with regular policy updates through FortiGuard for current patches and industry leading remediation that strengthens the integrity and security of operating systems—mitigating threats and managing vulnerabilities to prevent costly breaches.



Keeping up with Compliance

– PCI/DSS, SOX, GLBA, HIPAA

- ✓ Unified platform for auditing, policy and vulnerability management across heterogeneous systems
- ✓ Industry and federal standards based
- ✓ Automated compliance management
- ✓ SCAP certified
- ✓ Periodic updates from FortiGuard
- ✓ Silver award in Information Security Magazine 2010 Readers' Choice Awards

Key Benefits

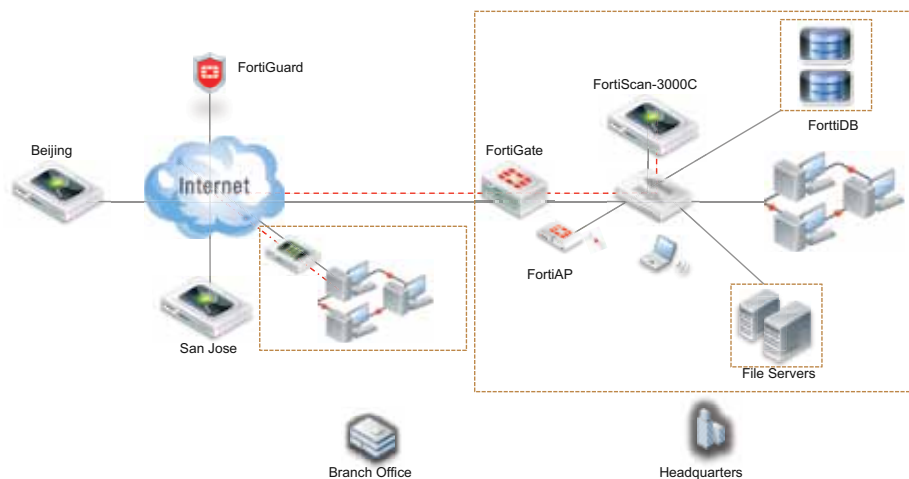
- ✓ Identifies security vulnerabilities and finds compliance exposures on hosts and servers
- ✓ Easy to deploy and manage
- ✓ Delivers patch management with ready-to-deploy remediation and enforcement actions
- ✓ Aids regulatory mandates with compliance reports



Silver award in Information Security Magazine 2010 Readers' Choice Awards



FortiScan Deployment - Large Enterprise-Carrier Network



Feature	Benefit
Vulnerability Management	Identifies security vulnerabilities and compliance exposures through deep inspection with client-resident asset agents – transparent to end users.
Agent-less Vulnerability Assessment	Asset prioritization and profile-based scanning to automatically discover inventory and assess security posture of the OS on networked devices, including mail servers, FTP servers or other UNIX or Windows hosts. Trend and remediation history is also available as part of the reporting.
IS Auditing	Monitors across heterogeneous systems and provides industry-standard benchmarks for IS compliance audits for operating systems; Select from the list of audit benchmarks or create custom policies.
Patch Management and Remediation	Delivers patch management with ready-to-deploy remediation and enforcement actions; remediation capability goes beyond traditional patch management, allowing network managers to change on configurations and potentially mitigate weak settings, including disabling an application or denying a network request.
Reporting and Compliance	Compliance for regulatory mandates with 360-degree reporting and analysis; provides industry, regulatory and best practices for NIST SCAP, FDCC, PCI/DSS, SOX, GBLA, HIPAA, ISO 17799, FISMA, and more. Pre-defined reports and views for compliance are also provided. FortiScan is OVAL compliant.
Integrated Asset Management	Fully integrated Asset management function enables users to run agent-less and agent-based OVAL scans directly on asset groups configured in the product.
Smart Automation	Reduced errors, repeatable processes, and predictable results delivered with an extensive library of templates that enable IT staff to leverage industry standard best practices that produce measurable results.

SCAN ENGINES

- Network discovery, asset prioritization and profile-based scanning
- Innovative, non-intrusive scan engine with extensive network throttling capabilities
- Complete asset inventory with accurate OS detection
- Both agent-less and agent based scanning are available from the same product

COMPLIANCE MANAGEMENT

- Identifies security vulnerabilities and finds compliance exposures on hosts, servers and throughout the network.
- Industry, regulatory and best practices, including templates for ISO 17799, SOX, HIPAA, GLBA, NIST, SCAP, and FISMA.
- All security content complies with the OVAL 5.6 standard
- Performs IS compliance audits
- Common Vulnerability Enumeration (CVE) Search

REMEDIATION/PATCH MANAGEMENT

- Delivers patch management with ready-to-deploy remediation and enforcement actions
- Allows network managers to change configurations and mitigate weak settings.
- Audits and remediates across heterogeneous systems for IS compliance
- Extensive libraries of templates that enable IT staff to leverage industry best practices to produce measurable results.

FLEXIBLE DEPLOYMENT

- Runs on Windows 2000, XP, Vista, Windows 7, server 2003 and 2008, RedHat 9, 3, 4, 5, CentOS 5, Solaris Sparc 9, 10.
- Agent-based or network-based (agent-less) scan
- Role-based security delegation

STANDARDS BASED

- Compliant with SOX, HIPAA, OVAL, XCCDF, CPE, CCE, CVE, CVSS
- Supports the latest SCAP version
- Comes with a comprehensive set of Compliance Benchmarks, Vulnerability database, Remediation templates and Patch policies.

REPORTING

- Automated, list of pre-defined reports include: Executive Security Posture Report, LOB Manager Security Posture Report, Sys admin Security Posture Report, Vulnerability Assessment etc.
- Reports can be executed real-time, scheduled, or sent over email
- 360-degree Reporting , Analysis and Views
- Trending reports, showing a host's remediation history, or how hosts vulnerability changes over time

INTEROPERABILITY

- Easy integration via SNMP, SMTP, Repository Database
- Compliant with OVAL, XCCDF, CPE, CCE, CVE, CVSS

PRODUCT / INTEGRATION

- Secure access to the Repository Schema
- SNMP support
- Support for file (results) uploads via FTP, SFTP, and SCP
- E-mail Alerts
- Integrate with FortiGuard IPS services

RESEARCH

- Backed by an unrivalled vulnerability research team
- Identifies known, published zero-day and unknown vulnerabilities
- Automated updates for latest vulnerability checks and information

Technical Specifications	
Hardware Specifications	
10/100/1000 (Copper, RJ-45)	4
SFP Gigabit Ethernet Interface	2
Console (DB9)	1
USB Interfaces	4
Drive Bays	6
Total Hard Drive Capacity	Up to 6 TB; ships with 2 TB
RAID Storage Management	RAID 0, 1, 5 and 10 (1 is default)
Storage Key (Boot Image)	2 GB USB
Software Specifications	
Asset Agent Licenses	20,000
Agent-less Scans	20,000
Browsers Supported	IE 7.x, IE 8, Firefox 3.x
Environmental Specifications	
Flash Partitioning	Standard partitioning schemes for all sizes of USB or Compact Flash
LED Specification	Standard LED status codes
AMC/FMC/RTM Compatibility	Standard compatibility matrix for all AMC/FMC/RTM expansion modules and associated hardware platform support.

Technical Specifications	
Dimensions	
Height	3.4 in (8.6 cm)
Width	17.4 in (44.3 cm)
Length	26.8 in (68.1 cm)
Weight	57.5 lbs (26.1 kg)
Rack Mountable	Yes
Environment	
Power Required	100-240 VAC, 50-60 Hz 7.0 - 3.5 Amp max
Power Consumption (AVG)	200W
Heat Dissipation	868 BTU
Redundant Hot Swappable Power Supply	Yes
Auto-Switching Universal	110/220 Volts
Operating Temperature	50 – 95 deg F (10 – 35 deg C)
Storage Temperature	-40 to 149 deg F (-40 to 65 deg C)
Humidity	5 to 95% non-condensing
Compliance & Certification	
Compliance	FCC Class A, UL/CB/ CUL, C Tick, VCCI, US EPA Energy Star Compliant
Self-Updating Agent Specifications	
Operating systems supported	Windows 2000 / XP / 7; Windows Server 2000 / 2003; Red Hat Enterprise WS, ES, AS, 3.0, 4.0, 5.0; Sun Solaris 8, 9, 10

Ordering Information		
Product	SKU	Description
FortiScan-3000C	FSC-3000C-E02S	FortiScan-3000C, manages up to 20,000 network assets, 4 10/100/1000 ports, 2TB HDD (up to 6 TB)
	FSC-3000C-E02S-BDL	Bundle - FortiScan-3000C, manages up to 20,000 network assets, 4 10/100/1000 ports, 2TB HDD (up to 6 TB)

Industry Certifications



FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with “return and replace” hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE

Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65-6513-3730
Fax: +65-6223-6784



Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.