

### Automated Compliance and Vulnerability Management Platform for the Operating System Level

#### 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. Most businesses rely on a collection of point products and manual processes when attempting to solve this problem. Driven by an increasing number of regulatory mandates, increasing costs of achieving and maintaining compliance, increased IT risk (e.g., security breaches) that may even affect Standard & Poor evaluations of risk, customer and shareholder confidence, security compliance programs are fast becoming an essential component of any enterprise IT Strategy. ITGRC requirements affect IT security at multiple levels, from the network down to endpoint client machines and other network devices. IT departments need to keep up with new regulations and modifications to existing regulations to pass audits, while reducing costs, complexity and redundant work. 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

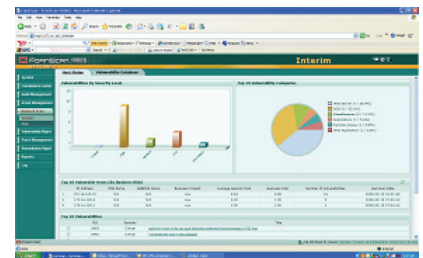
FortiScan provides a centrally managed, enterprise-scale solution that enables organizations to close IT compliance gaps, and implement continuous monitoring in order to audit, evaluate, and comply with internal, industry, and regulatory policies for IT controls and security at the OS level. Organizations realize quick time-to-value with easy to install, intuitive, high value standard compliance policies (NIST SCAP, FDCC, PCI-DSS, SOX, GLBA, HIPAA) ready out-of-the-box with regular updates by FortiGuard to ensure OS regulatory compliance requirements are met. FortiScan dedicated hardware appliances easily plug into the network for fast deployment. FortiScan integrates endpoint vulnerability management, industry and federal compliance, patch management, remediation, auditing and reporting into a single, unified appliance for immediate results. A centralized administration console facilitates management of multiple FortiScan appliances across the enterprise.

#### Key Solution Features and Benefits

- Vulnerability Management (VM)** 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.
- 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 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, GLBA, HIPAA, ISO 17799, FISMA, and more. Pre-defined reports and views for compliance are also provided.
- Smart Automation** Reduced errors, repeatable processes, and predictable results delivered with an extensive libraries of templates that enable IT staff to leverage industry standard best practices that produce measurable results.



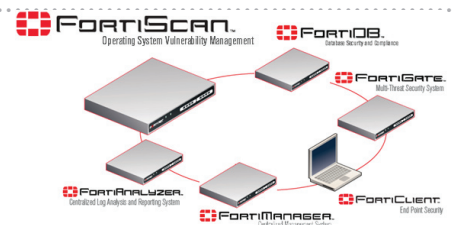
FortiScan appliance



FortiScan Web Interface

#### Minimal Impact and Low Total Cost of Ownership (TCO)

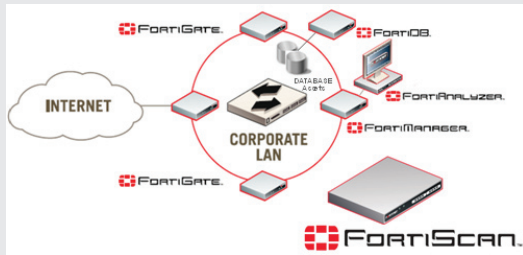
Failing to keep up with regulations, vulnerabilities and patches for the OS can have grave cost implications. FortiScan simplifies the process with regular policy updates through FortiGuard for current patches and industry leading remediation advice that strengthens the integrity and security of operating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



## TYPICAL APPLICATIONS

### FortiScan-1000B

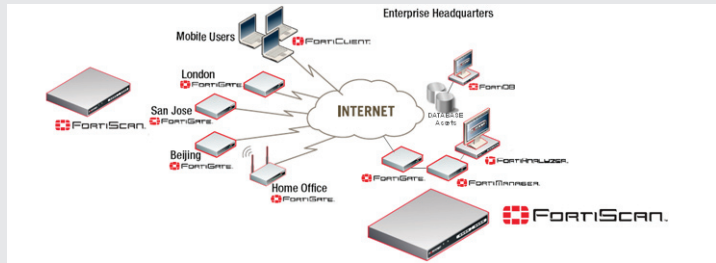
Agent-less Deployment  
Central Corporate LAN



Small-Medium Enterprise Network

### FortiScan-1000B

Thousands of IT Assets per FortiScan-1000B  
Remote Offices and Branches



Medium-Large Enterprise Distributed Network

## FortiScan Models



Feature	FortiScan-1000B
Security Hardened Platform.....	Yes
Asset Agent Licences.....	2,000
Agent-less Scans.....	Unlimited
10/100/1000 Ethernet.....	4
Number of Drive Bays.....	2
Total Hard Drive Capacity.....	2 x 1 TByte
Storage key (boot image).....	1 GB USB
RAID Storage Management.....	Yes (0, 1)
Redundant Hot Swap Power Supplies.....	No

Dimensions (H, W, L) .....	1.7 x 16.7 x 30.4 in. (4.3 x 42.6 x 77.2 cm)
Weight.....	39 lbs (17.7 kg)
Rack Mountable.....	Yes
AC Power Required.....	100-240 VAC, 50-60 Hz, 4.8 Amp (Max)
Auto-switching universal.....	110/220 Volts
Average Power Consumption.....	295 Watts
Operating Temperature.....	50 to 95 deg F (10 to 35 deg C)
Storage Temperature.....	-40 to 149 deg F (-40 to 65 deg C)
Humidity.....	5-95% non-condensing (twmax=38C)
Regulatory.....	FCC Class A Part 15 / CE Mark

Browser Support.....	Internet Explorer 7.x, Firefox 3.x
----------------------	------------------------------------

Feature	FortiScan Administration Console
System Requirements.....	1.0 GHz CPU, 1024 MB RAM, 80 GB HDD
Operating System support.....	Windows 2000 / XP; Windows Server 2000 / 2003

Feature	FortiScan Asset Agents
Operating System support.....	Windows 2000 / XP; Windows Server 2000 / 2003; Red Hat Enterprise WS, ES, AS 3.0, 4.0 and 5.0; Sun Solaris 8, 9 and 10
Footprint.....	500 KB

### FortiCare™ Support Services

- 24 x 7 x 365 FortiCare Web Service <sup>[1]</sup>
- 8x5 Web-Based Technical Support <sup>[2]</sup>
- 1-Year Limited Hardware Warranty
- 90-Day Limited Software Warranty

<sup>[1]</sup> Annual renewal required to maintain service

<sup>[2]</sup> 24 x 7 Telephone Technical Support available.

## About Fortinet (www.fortinet.com)

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection—including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam—designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: firewall, antivirus, IPSec, SSL, network IPS and anti-Spyware. Fortinet is privately held and based in Sunnyvale, California.

## FORTINET®

### 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](http://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  
61 Robinson Road, #09-04 Robinson Centre  
Singapore 068893  
Tel: +65-6513-3730  
Fax: +65-6223-6784

Copyright© 2009 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. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract 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. FSC-R1D1-0409-2P