



Fortinet Simplifies Security Compliance with Vulnerability and Audit Appliance

Fortinet - a market-leading network security provider and worldwide leader of unified threat management (UTM) solutions - today broadened its security product portfolio with the introduction of a new vulnerability management (VM) and compliance solution for desktops, laptops, servers, and other network attached devices.

Targeted at enterprises and government organisations, the FortiScan-1000B appliance enables organisations to quickly determine their security and compliance posture through an automated vulnerability discovery, auditing, patch management, remediation and reporting process that is easy to deploy and manage.

Charles Cote, Fortinet regional director South Pacific commented, Most organisations face significant challenges when trying to understand whether all of their servers, computers, and network devices are patched to the correct level, and adequately protected. Our new FortiScan appliance greatly simplifies security compliance management by scanning systems to look for problems, patching software problems on computers, and providing detailed audit style reports. FortiScan allows organisations to significantly reduce ongoing security compliance costs, while providing senior executives and compliance officers with the information they need to readily understand the IT security risks they face.

FortiScan works alongside FortiDB, FortiWeb and FortiGate to offer organisations an end-to-end security compliance strategy that extends across computers, databases, web applications, and the network itself.

FortiScan performs the following security functions as part of a comprehensive vulnerability management system:

Vulnerability Management: Identifies security vulnerabilities and finds compliance exposures on hosts, servers and throughout the network transparently to end-users. Endpoint VM is achieved through a client-resident agent, while network-level VM is accomplished through agent-less network analysis.

Auditing: Audits and

monitors across heterogeneous systems and provides industry-standard benchmarks for IS compliance audits for operating systems. Users can either select from the list of audit benchmarks or customize their own audits based on standard frameworks.

Patch/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/Compliance: Aids compliance for regulatory mandates with 360 degree reporting and analysis. FortiScan provides industry, regulatory and best practices templates for ISO 17799, SOX, HIPAA, GLBA, NIST, SCAP, FISMA etc. Pre-defined reports and views for compliance are provided.

Fortinet has integrated the Vulnerability Scanner module from its FortiAnalyzer family of logging, analysing and reporting appliances into FortiScan. The Vulnerability Scanner is a network-based VM module designed to automatically discover, inventory and assess the security posture of servers, hosts and other devices. The C5 Compliance platform and the FortiAnalyzer VM module are combined on a security-hardened hardware platform to form FortiScan-1000B.

The FortiScan-1000B provides a powerful solution for organizations that require compliance with regulatory mandates such as PCI-DSS, SOX, GLBA, and HIPAA, and other government and defence force regulations.

Like the rest of Fortinets product line, FortiScan-1000B will also rely on the FortiGuard subscription service to automate FortiScan policy, remediation, vulnerability database updates in real-time.

FortiScan-1000B leverages technology acquired in 2008 from Secure Elements, a risk and IT security compliance company. Secure Elements C5 Compliance software solution was the leader in its class and forms the basis for the FortiScan-1000B appliance.

The FortiScan-1000B appliance comes with two terabytes of storage and can support up to 2,000 network assets. Additional information on FortiScan appliances can be found at <http://www.fortinet.com/products/fortiscan/>.

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, web filtering, spyware prevention, and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and a unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting capabilities. 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 VPN, SSL VPN, Network IPS, and Anti-spam. Fortinet is privately held and based in Sunnyvale, California.

Copyright 2009 Fortinet, Inc. All rights reserved. The symbols and denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinets trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiDB and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements herein attributed to third parties and Fortinet does not separately endorse any such statements. Fortinet is not responsible for customers' legal compliance.