

The header image features a dark background with a grid pattern. Overlaid on this are several glowing, orange-red, abstract shapes that resemble flames or data streams, creating a sense of dynamic energy and security.

# FORTINET WHITEPAPER

## **LOWERING COSTS OF NETWORK SECURITY FOR LARGE RETAIL CHAIN STORES**

**Strategies for Securing Hundreds of Stores on a Tight Budget**



[www.fortinet.com](http://www.fortinet.com)

## Contents:

OVERVIEW	PAGE 3
REQUIREMENTS OF ENDPOINT SECURITY FOR RETAIL	PAGE 4
OPTIONS TO IMPLEMENT RETAIL SECURITY	PAGE 5
COMPARING TOTAL COST OF OWNERSHIP FOR SECURITY OPTIONS	PAGE 8
SUMMARY	PAGE 8
ABOUT FORTINET	PAGE 9

>> *When the network goes down, commerce transactions halt and cash registers stop ringing*

## OVERVIEW

For retail businesses with many stores, network connectivity linking all sites has become the glue of critical operating processes. The Point of Sale now automatically ties into accounting and inventory control systems, customer relationship management applications and other business services. The network is vital, yet invisible, to store clerks and staffers - until it stops working. For when the network goes down, commerce transactions halt and cash registers stop ringing.

There's not much you can do to counter outages in the public network short of buying access lines from multiple carriers. But retail businesses can directly stop outages caused by a familiar hazard: computer worms, viruses, spyware and other mischief launched by hackers over the Internet. Each can damage PCs and systems used at the Point of Sale and halt retail operations.

Network security issues per se are not new, but traditionally they were a concern only at the corporate office. Since connectivity to PCs at the Point of Sale became a critical part of retail businesses, security now must be addressed for all network endpoints.

In this whitepaper, Fortinet surveys the challenges of providing security to a large organization of retail stores. We review pros and cons for options implementing network security to all endpoints, including:

- Traditional self-integrated, best-of-breed strategy using servers and standalone software-based security applications;
- Point solution appliances providing single-purpose security applications such as a firewall or VPN;
- Unified Threat Management (UTM) appliance integrating all security applications into just one high performance device for each store.

Fortinet makes UTM appliances, which are the fastest-growing segment of the endpoint security market and are projected by International Data Corp. to dominate sales over standalone applications and appliances by 2008<sup>1</sup>. The analysis presented in this whitepaper shows the power of using the scalable FortiGate family of UTM solutions from Fortinet. With Fortinet, a retail organization with hundreds of stores can quickly deploy and operate a full suite of high performance security solutions to all endpoints for about one fourth the costs of traditional solutions and standalone appliances.

>> *Each of these security applications can and should be installed at every retail network endpoint*

## REQUIREMENTS OF ENDPOINT SECURITY FOR RETAIL

There is nothing particularly unusual about technical security requirements for retail stores. While computing there is on a smaller scale compared to the corporate headquarters, the basic needs for protection from hazards transmitted over the Internet are similar. Typical security applications and functionality necessary for retail stores include:

**Antivirus Gateway.** Detects and eliminates viruses, worms and spyware in real time. Scans incoming and outgoing email attachments, FTP, and HTTP traffic.

**Firewall.** Inspects content in network packets to ensure no unauthorized traffic passes into or out of the intranet. With adequate performance, a firewall can be deployed in-line for real-time protection.

**Intrusion Detection and Prevention.** Stops attacks at network perimeter by analyzing traffic for worms, viruses and other hazards. Analysis techniques include behavior-based learning and heuristics in addition to signatures defining known hazards.

**VPN.** Enables secure communications tunnels across the public Internet between computing devices. With adequate performance, a VPN can authenticate users, encrypt data and manage sessions.

**Antispam.** Eliminates entry to the intranet of junk email, file attachments and web access of blacklisted websites, domains and key words.

**Traffic Shaping.** Optimizes or guarantees network performance with packet classification, queue disciplines, policies, congestion management, quality of service, and fairness techniques. Improves latency, service availability and bandwidth utilization for cost efficient, high performance networking.

**Web-based Content Filtering.** Processes all Web content to block inappropriate material and malicious scripts from Java Applet, Cookies and Active X scripts entering the intranet. Assures improved productivity by minimizing time wasted on non-business use of the network.

Each of these security applications can and should be installed at every retail network endpoint. The biggest challenge is operational - how to deploy them and manage their use in a cost-effective manner.

## OPTIONS TO IMPLEMENT RETAIL SECURITY

Security managers for large retail organizations have several options for implementing network security at each retail store location. Implementations of security technologies described above fall under three general categories: traditional, self-integrated best-of-breed solutions; point solution appliances; and unified threat management appliances. Pros and cons to each approach are considered in this section.

**Comparison of Options for Retail Security**

Issue	UTM / Fortinet	Point Appliances	Server / Best of Breed
<b>Integration of security</b>	yes	limited	limited
<b>Deployment</b>	simple	simple	complex
<b>Administration</b>	simple	simple with one; complex with many	complex
<b>Updates (software, signatures)</b>	simple	simple	complex
<b>Reporting</b>	enterprise-wide, automatic	enterprise-wide requires manual integration	enterprise-wide requires manual integration
<b>Scalability</b>	unlimited	limited	limited
<b>Reliability</b>	good because only one unit required for each store; excellent with fault-tolerant option	multiple appliances at each store required for full security; creates many failure points	multiple servers at each store required for full security; creates many failure points
<b>Performance</b>	excellent with ASIC-based acceleration technology	good, but add operational complexity since multiple appliances at each store are required for full security	good, but add operational complexity since multiple servers are required at each store for full security
<b>Recurring software licenses</b>	none; you own the software	about 20% per year	about 20% per year
<b>18-month TCO</b>	about one-fourth the cost of other options	excessive	excessive

**TRADITIONAL SELF-INTEGRATED, BEST-OF-BREED**

The do-it-yourself approach is how most security managers learned their profession. It entails purchasing, deploying and operating several servers and software for each best-of-breed security application at headquarters and each store location.

Self-integration is a huge process with two aspects: (1) provisioning hosts for each security application, and (2) implementing each security application on respective hosts. Each store will need several servers to host security applications because performance drags to a stop if you try and run all security applications on one host.

The do-it-yourself approach is popular because it's familiar - acquisition, installation and operations are like other things managed by the IT staff. But tradition comes at a high cost. It's expensive to purchase, deploy and manage multiple servers for security at hundreds of retail stores. And it's not just the high cost of management. Most stores simply do not have enough people with technical wherewithal or time to maintain those servers.

There are recurring annual costs for security software licenses. Licensing costs geometrically rise for organizations with hundreds of stores.

Enterprise security data integration and reporting is another tedious process. Security data from the distributed application servers must be manually assembled and synthesized for an enterprise view. Manual security data integration and reporting is too slow and ineffective for rapid response to new vulnerabilities.

>> *The multitude of separate boxes represents many more potential points of failure, any one of which could expose the entire network to risk of attack.*

**POINT SOLUTION APPLIANCES**

Appliances appeared on the IT scene during the late 1990s. A point solution appliance is a network-attached box with a hardened operating system and a limited applications set such as firewall or IPS. Its message of simplicity is appealing. Instead of acquiring, installing and maintaining a server for hosting a security application, all you to is plug the appliance into the network and perform a minor setup configuration. There is much less fuss than with using a traditional server, so acquisition and operations costs should be lower.

These benefits have strong appeal for situations like a retail store, which often has no resources for security or systems administration. But what appears simple on the surface has a different connotation for hundreds of stores. Appliances that do only one or two things are not scaleable. They require each store to have multiple appliances for the full range of security applications. The result brings the same cumbersome administration issues experienced by organizations that operate multiple host servers at each store.

Synthesizing security information from multiple non-integrated appliances also remains a time-consuming process for multi-store retail operations. This overhead hinders keeping stores secure by making it too difficult to accurately and regularly assess vulnerabilities and guide remediation.

Like the traditional server / best-of-breed solutions, point appliances also require an annual fee for software maintenance, which becomes onerous with multiple appliances at hundreds of stores. Finally, the multitude of separate boxes represents many more potential points of failure, any one of which could expose the entire network to risk of attack.

<b>Total Cost of Ownership (rollups)</b>			
	<b>FORTINET</b> Units: 250	<b>SINGLE FUNCTION APPLIANCES</b> Units: 250	<b>SOFTWARE-BASED HOST SERVER SECURITY APPLICATION</b> Units: 250
<b>Purchase, Install and Operate</b>			
1st six months	\$532,996	\$7,503,000	\$9,505,900
2nd six months	\$264,996	\$648,000	\$1,125,900
3rd six months	\$264,996	\$1,285,500	\$1,125,900
<b>18-Month Total:</b>	<b>\$1,062,988</b>	<b>\$9,436,500</b>	<b>\$11,757,700</b>
<b>Security Administration</b>			
1st six months	\$846,000	\$1,710,000	\$3,150,000
2nd six months	\$846,000	\$1,710,000	\$3,150,000
3rd six months	\$846,000	\$1,710,000	\$3,150,000
<b>Total:</b>	<b>\$2,538,000</b>	<b>\$5,130,000</b>	<b>\$9,450,000</b>
<b>Grand TCO - 18 Months</b>	<b>\$3,600,988</b>	<b>\$14,566,500</b>	<b>\$21,207,700</b>
	Delta to Appliances <b>-75%</b>	Delta to Cost of Fortinet Soltn = 305%	Delta to Cost of Fortinet Soltn = 489%
	Delta to Host Server <b>-83%</b>		
	Percent Total of Appliances = 25%		
	Percent Total of Appliances = 17%		

>> *Many solutions carry hidden operational costs that, during the first 18 months of deployment, can grow to half or more of the acquisition cost.*

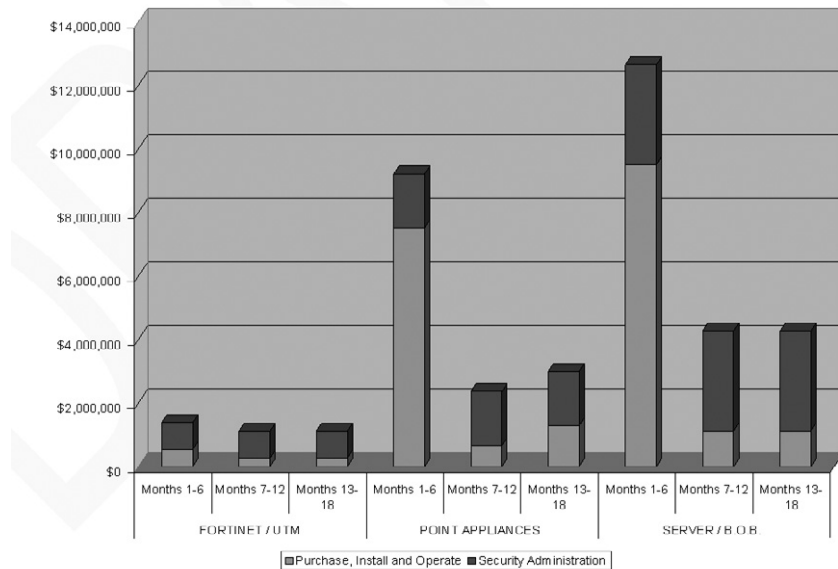
**UNIFIED THREAT MANAGEMENT APPLIANCES**

The UTM is an integrated security gateway appliance that merges all security applications into one high-performance box. It provides the benefits of an appliance but easily scales to hundreds or even thousands of stores. The UTM architecture fully integrates all security functions - including data synthesis and centralized management of all devices. UTMs from Fortinet uniquely use ASIC acceleration technology to power all security applications in one convenient appliance. Fortinet UTMs cost less to operate and manage than point appliances and servers; they include the option of fault-tolerant configurations to eliminate any point of failure.

**COMPARING TOTAL COST OF OWNERSHIP FOR SECURITY OPTIONS**

Calculating the total cost of ownership for your retail security solution is a crucial. Many solutions carry hidden operational costs that, during the first 18 months of deployment, can grow to half or more of the acquisition cost. The only number that really matters is TCO for your unique solution. But for purposes of general comparison, Fortinet prepared a sample 18-month TCO analysis for the three solution options described above. We picked 18 months because that is the typical number chief information officers must defend when they make large-project budget proposals to the corporate executive committee. Our analysis projects two types of costs: (1) purchase, installation and operations, and (2) security administration for a retail chain of 250 stores.

**18-Month TCO for Security of 250 Retail Stores**



**PURCHASE, INSTALLATION AND OPERATIONAL COSTS**

Acquisition and operational costs carry different assumptions for each solution category. For the UTM / Fortinet Model, we assumed one device for each of the 250 stores, three large units for the corporate office and Web hosting provider, plus centralized management and distribution software. The model also calculated an average monthly total cost for system administration of UTM appli-

>> *"We purchased Fortinet systems for less than the engineering services alone were going to cost to install Checkpoint firewalls"*  
 - Gold's Gym

ances in all stores. There were no recurring software costs because software is owned by the user.

For the Point Appliances Model, we assumed similar calculations except that each store requires a group of devices instead of just one compared to the UTM solution. This model included a 20% recurring annual cost for software maintenance.

Calculating costs for the Server / Best of Breed Model was more complex. For the server, we incorporated assumptions for the hardware, RMA and support; space/rack plus air conditioning; free operating system software, system administration costs; deployment and configuration; maintenance and patches; backup and restore; redundancy/fail-over/UPS; audit logs/system; security maintenance; capacity planning; and event modeling. For security applications, we incorporated expenses for the software and assumed a 20% recurring annual cost for software maintenance.

SECURITY ADMINISTRATION COSTS

The security administration costs included projections for time required each month to perform tasks such as adjusting configurations, signatures and databases; running the security application; coordination for remedial action; running reports; and centrally consolidating reports for enterprise-wide perspectives. Each of these tasks corresponded to the various security applications, including firewall, VPN, intrusion prevention system, anti-virus, anti-spam, and content filtering.

TOTAL COST OF OWNERSHIP FINDINGS

For a 250-store retail chain, our 18-month TCO model projected the UTM / Fortinet solution to be 25% of the total for a point appliance solution, and 17% of the total for a traditional server / best of breed solution.

SUMMARY

Ensuring the security of network-attached systems in retail chain stores is vital to ongoing operations. Ease of administrating security is especially important considering the limited technical experience of a typical store clerk. This whitepaper described three security implementation strategies for retail stores, including server-based best-of-breed, point solution appliances, and unified threat management appliances such as the scalable Fortinet family of solutions. UTM is the simplest security architecture, making it easier to deploy and manage - especially for businesses with hundreds of retail establishments and limited technical resources at each site. UTM is the only architecture that enables automated reporting of enterprise security performance and provides for the fastest response to new vulnerabilities. The total cost of ownership for UTM in a network of 250 retail stores is about one-fourth the costs of server-based or point appliance solutions.

We invite your organization to contact its Fortinet sales representative to learn more about our total security solutions for large-scale retail businesses, and see how the 18-month TCO analysis applies to your distributed operation's security requirements.

## ABOUT FORTINET (WWW.FORTINET.COM)

Fortinet is the confirmed leader of the Unified Threat Management market. The company's award-winning FortiGate™ series of ASIC-accelerated antivirus firewalls, winner of the 2004 Security Product of the Year Award from Network Computing and the 2003 Networking Industry Awards Firewall Product of the Year, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time - without degrading network performance. FortiGate systems are the only security products that are quadruple-certified by the ICSA (antivirus, firewall, IPSec, NIDS), and deliver a full range of network-level and application-level services in integrated, easily managed platforms.

### SALES

Please contact us at [sales@fortinet.com](mailto:sales@fortinet.com) or phone toll-free in the U.S. (866) 868-3678 or +1(408) 235-7700.

### POTENTIAL PARTNERS

Please contact us at [partners@fortinet.com](mailto:partners@fortinet.com) or visit us at [www.fortinet.com](http://www.fortinet.com).

"Worldwide Threat Management Security Appliances 2004-2008 Forecast and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance," International Data Corp., Sept. 2004; see Table 6 on p. 12

Copyright 2005 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiClient, FortiWiFi, FortiGuard, FortiOS, FortiProtect, and FortiASIC are registered trademarks of Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. WPR1190503

