

Enabling Reliable & Secure Retail Networks



Security, Compliance & New Services in One Solution

FORTINET[™]

All-in-One Security Appliances for Retail Applications

Ensuring Operational Efficiency & Productivity

Are your distributed retail locations secure and in compliance with the latest regulations? Do you want to add wireless “Hot Spot” or Internet kiosks to enhance your customers’ experience in your stores? Do you know the impact of that decision? Are you confident that your security posture is up to the task?

Success in the retail market is more than just the right product at the right location. In today’s environment, Internet and networking technologies play a pivotal role in delivering consistent consumer experiences while tightly managing costs, improving productivity and helping to maximize profitability. Information technology networks provide point-of-sale (POS), inventory management, access to corporate information systems and many other valuable services, which are essential elements critical to retail business operations. These networks must be cost-effective, consistent across each retail location, and always available to deliver continuous, secure flows of information and data throughout all facets of the retail chain.

The potential downsides of these advances are the number of security threats associated with using such an open and ubiquitous network as the Internet. These systems have the potential to be vulnerable to a host of security risks—from hackers and criminals intent on disrupting the business, stealing goods or services and accessing sensitive customer data. Retailers who can cost-effectively manage these challenges and implement protective barriers for their business will experience exciting opportunities for enhanced productivity and revenue growth.

Fortinet retail security solutions offer data protection and access control, maximum up-time, ease of deployment, compliance, and new services such as Hot Spot wireless. These solutions allow retailers to cost-effectively face these challenges and embrace the new opportunities technology offers.

Assessing Risks and Enabling New Business Opportunities

As retail operations evolve networks from “closed” dial-up and frame relay network access methods to “open” broadband Internet access, the security risks escalate. And for retailers looking to leverage the ease of deployment and new service opportunities associated with wireless solutions, they too can be particularly vulnerable if not properly secured.

Choosing the right network protection is essential to realizing the benefits of this transition. Many point products exist that perform single functions such as network firewall or antivirus protection; however, assembling multiple point products into a comprehensive solution is complex, costly and difficult to maintain. Most retail businesses do not have and cannot afford the staff to maintain such complex solutions. Furthermore new threats are emerging daily, many of which are new blended threats that require an integrated security solution with unified threat management capabilities that can identify and block these complex threats.

Moreover, the credit card industry has mandated retail businesses and service providers that store, process, or transmit cardholder data must comply with a set of network security requirements, as defined by the Payment Card Industry (PCI) Data Security Standard—or face significant fines.

To stay on the cutting edge of technology, retailers are transforming the retail business model and enabling new applications -- improving customer satisfaction, attracting and retaining customers, increasing profitability and generating new revenue streams. But while technology offers exciting new business opportunities for the retail space, there are risks that mandate a level of network security to protect and manage the overall retail operation.



Fortinet retail security solutions offer a cost-effective approach to security and compliance while improving efficiency and ultimately productivity.

Key Retail Security Selection Criteria

Mitigating risk is critical when selecting a security solution for your retail network. Here are the key criteria that should be considered when determining a technology partner and platform to implement a reliable security platform that enables the business and ensures compliance with the latest regulations.

Data Protection & Access Control—Requires implementing a protective barrier around your retail operation allowing only “trusted” devices or users while blocking hackers, worms, and other threats from entering your network and damaging POS systems and accessing customer information.

Maximum Up-Time—Continuous operation is critical to business profitability. With POS systems and other applications depending on the broadband network—reliability is critical.

Ease of Deployment—Space is a premium in the retail environment so choose a compact solution that can fit, ideally on a shelf, table or wall, without requiring special installation facilities or technical personnel.

Compliance—Cost-effectively achieving PCI compliance requires a unified security appliance. While monitoring and maintaining PCI compliance requires a solution enabling centralized policy and update management, comprehensive real-time monitoring, logging and reporting, and with built-in tools for vulnerability assessment and historical forensic analysis.

Hot Spot Wireless—Hot Spots attract and retain customers; yet wireless presents unique security challenges. Transmissions over the wireless link can be intercepted and unauthorized access obtained, making wireless access points a prime target for hackers. Sharing a broadband connection is cost-effective but traffic must be managed such that retail operations are not degraded or impacted in anyway.

Jenny Craig

“We chose Fortinet’s FortiGate and FortiManager systems because of the comprehensive feature set, pricing and centralized management of Fortinet’s network security platform.”

– Jeff Nelson, IT Director



Pierre Lang Jewelers

“We needed a lot of functionality that the Linux-based firewall could not easily provide. We had to implement more De-Militarized Zones (DMZ) behind the firewall, bring in antivirus capabilities at the edge of the network and setup an effective intrusion detection system.”

– Antonia Ebner, Head of IT Department

Security Compliance Regulations in Retail Environments

The Payment Card Industry (PCI) Data Security Standard defines twelve basic requirements for compliance:

Build and Maintain a Secure Network

1. Install and maintain a firewall
2. Do not use vendor-supplied defaults

Protect Cardholder Data

3. Protect Stored Data
4. Encrypt transmission of cardholder data and sensitive information

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

In addition, retailers must monitor and report known or suspected security breaches and must take immediate action to investigate the incident. Retailers are subject to fines, up to \$500,000 per incident, if found to be out of compliance with the PCI standards at the time of the incident.

Fortinet All-in-One Security Solutions for Retail

Fortinet retail security solutions offer a cost-effective approach to security and compliance while improving efficiency and ultimately productivity. The easy-to-install, maintain and update multi-threat security appliances deliver a complete set of security features and make managing and protecting even the largest retail networks a hands-off, yet secure and compliant, experience.

What to look for when choosing an Integrated Retail Network Security Solution

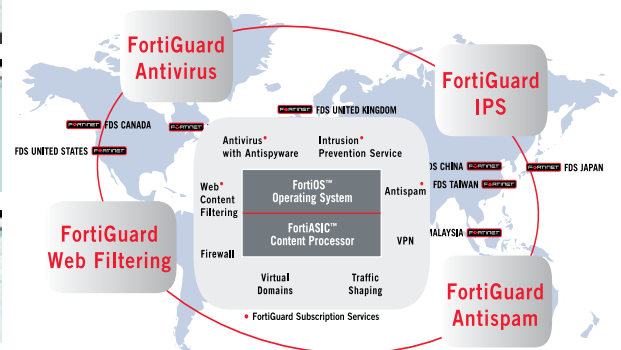
Retail Broadband Network Security Checklist	Fortinet Provides
<input type="checkbox"/> Data Protection & Access Control <ul style="list-style-type: none"> ✓ Firewall ✓ IPSec or SSL Virtual Private Network ✓ Security Services: Antivirus, Antispam, Antispyware, & Web Content Filtering ✓ Intrusion Detection and Prevention ✓ Near wire-speed hardware acceleration 	<p>Fortinet retail security appliances are all-in-one security solutions providing retail businesses protection against blended attacks, such as denial of service, viruses, worms, SPAM and theft of information and services, to ensure continuous retail operations, protection of sensitive customer information and enforcement of appropriate usage policies. Fortinet solutions are secure, hardened appliances that utilize ASIC-based hardware acceleration and a purpose-built operating system to achieve maximum performance.</p>
<input type="checkbox"/> Maximum Up-Time <ul style="list-style-type: none"> ✓ Network access failover via dialup modem ✓ Multiple high-availability configuration options ✓ Clustering of wireless access points 	<p>Fortinet retail security appliances purpose-built secure, hardened platforms that are field proven for reliability and quality. Unlike many competitive solutions, Fortinet can keep your business running under the most challenging conditions with multiple high-availability configurations as well models available with automatic fail-over to dialup modem should your broadband connection fail for any reason.</p>
<input type="checkbox"/> Deployment <ul style="list-style-type: none"> ✓ Compact appliance: shelf, table or wall mounting ✓ Easy-to-use graphical user interface ✓ Central management system support ✓ Wide variety of networking options ✓ Integrated wireless access point 	<p>Fortinet retail security appliances are compact, space efficient units that fit easily in any retail environment without requiring special racks or equipment closets. Truly plug 'n play, non-technical personnel can install in as little as 30 minutes. Furthermore, management and reporting functions are accessible at the retail store and from central management locations.</p>
<input type="checkbox"/> Compliance <ul style="list-style-type: none"> ✓ Multi-threat security appliance to meet critical threat mitigation objections ✓ Centralized policy and update management ✓ Comprehensive real-time monitoring, logging and reporting ✓ Supports vulnerability assessment and analysis 	<p>Cost-effectively achieving compliance to industry security standards are a major challenge for retail businesses. Fortinet's retail security solutions are tailored to meet retail customers' unique security and compliance challenges offering cost-effective, easy to deploy, multi-threat devices that address the PCI Data Security Standard while improving efficiency and ultimately productivity.</p>
<input type="checkbox"/> Hot Spot Wireless <ul style="list-style-type: none"> ✓ Integrated wireless access with security gateway ✓ Built-in traffic shaping ✓ Network segmentation to separate customer and retailer data 	<p>Fortinet bundles secure wireless services into a single compact appliance enabling retail operational efficiencies as well as the ability to extend Internet services to customers safely, securely and without impact to retail operations. All-in-one secure Internet access is a compelling value that attracts customers to visit, stay and shop.</p>



FortiGate Multi-Threat Security Appliances



FortiManager Central Management and FortiAnalyzer Logging & Reporting



FortiGuard Security Services and FortiCare Technical Support



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
 4 Place de La Defense
 92974 Paris La Defense Cedex, France
 Tel +33-4-8987-0510
 Fax +33-1-5858-0025

APAC SALES OFFICE-HONG KONG
 Fortinet Incorporated
 Room 2429-2431, 24/F Sun Hung Kai Centre
 No.30 Harbour Road, WanChai, Hong Kong
 Tel +852-3171-3000
 Fax +852-3171-3008