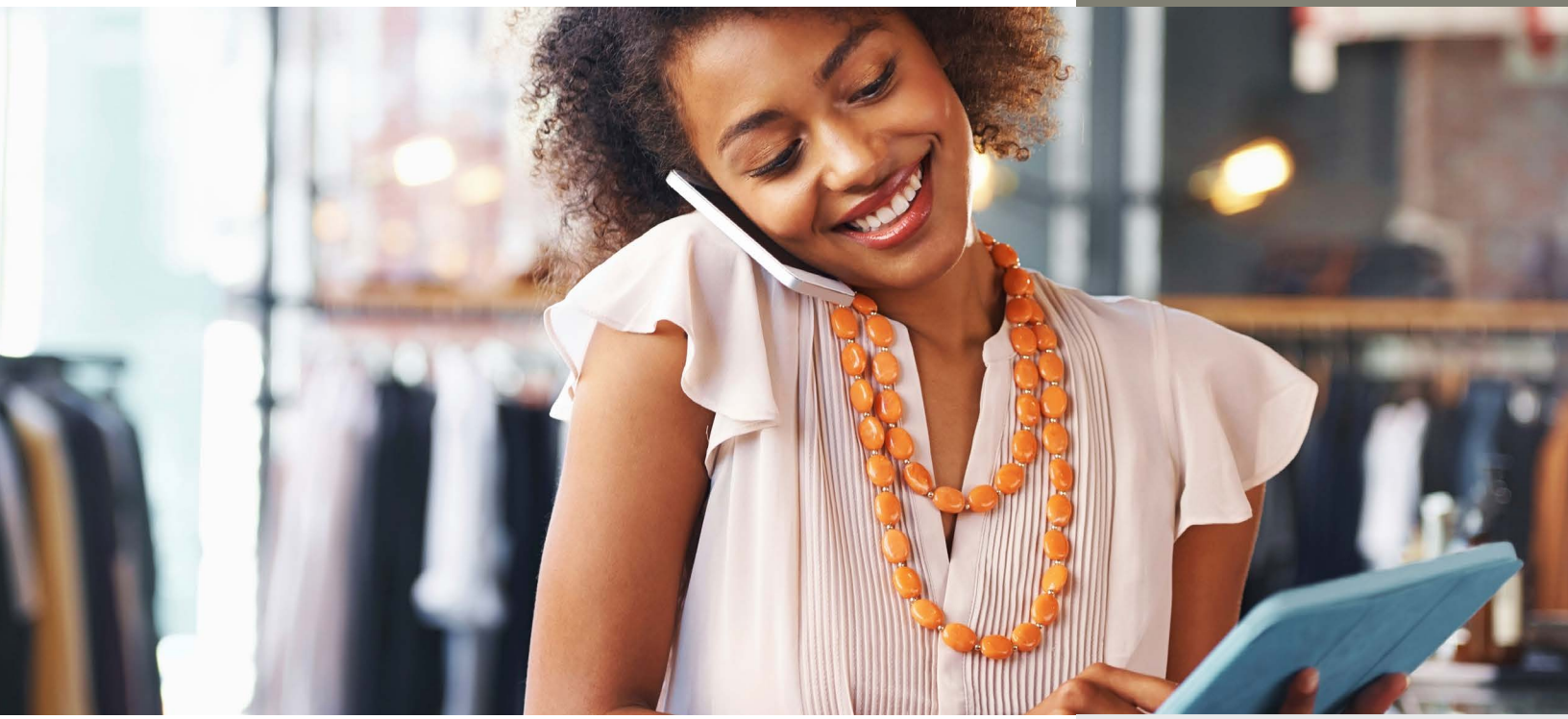


Keeping the Store Open: Fighting the Cyber Criminal in the Retail World

Introduction

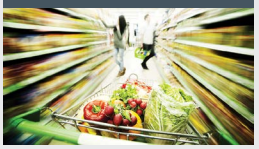
As the most recent wave of attacks have confirmed, the retail sector remains among the top industries to be targeted by cyber criminals. To protect themselves and their customers, retailers need comprehensive yet cost-effective network security solutions to mitigate risk to their business and prevent the financial and reputational damage created by a data breach.

While threats increase, retail IT teams are under pressure to reduce costs and to develop existing and new retail channels. Given the squeeze on IT budgets, in-store comprehensive network security measures may not always be a priority.

This solution guide examines the challenges facing retail chains to cost effectively counter the growing challenge from the cyber criminal while at the same time leveraging technology at the store level to better attract and retain customers in this age of online shopping and e-tailers.

Pain Points of the Typical Retail Network

CONNECTIVITY

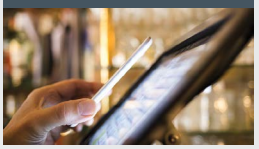


SECURITY

PERFORMANCE

COST

MANAGEABILITY



SECURED BY FORTIGUARD®

Retail Store Data, IT and Network Security Challenges

- Protecting systems and data from the increasingly sophisticated threat landscape
- Ensuring an excellent customer experience with high performance and availability of secure connected services
- Scaling security solutions from kiosk to superstore and managing their distributed deployment cost effectively
- Providing visibility and control of an increasingly complex in-store environment without burdening resources
- Supporting the evolution and migration to high-speed broadband public network and web applications.
- Protecting the increased use of in-store wireless networks and wireless connected devices
- Supporting planned/future rollout of new innovative services such as presence analytics
- Supporting ongoing and changing compliance requirements

The bottom line: How can today's retailers protect themselves cost effectively without endangering their competitive posture?

Retail Store Challenges

Retail IT security managers generally have two options for implementing comprehensive network security solutions; a centralized approach with all security systems at the network's central site or data center or a distributed approach, equipping each store with an array of systems. Both options have certain advantages but each one also comes with significant disadvantages.

The traditional approach to network security follows that of the network itself, a centralized architecture with all of the functionality consolidated at the head of the network. The in-store architecture would typically be a simple router with the in-store network behind it. This approach has the advantages of reduced cost and simplified management but without any real security functionality at the branch the potential for an in-store breach is significant. This approach also makes it more difficult to securely deploy new applications or technologies.

The distributed approach will push out some of the security functions to the store itself. While this will give greater protection to the in-store systems, this typically involves the use of discrete appliances for different functions. The two main drawbacks of this approach are cost and scalability. The third is the lack of on-site IT resources in such a complex environment.

A hybrid approach combining elements of the centralized and distributed architectures is also an option, pushing out some of the centralized functionality to the remote location. The primary problem with this approach is that the platform used to consolidate these technologies, typically the network router, is not really designed to handle both networking and security functions simultaneously and can impact performance.

The question is whether a solution exists that is both cost effective and has high security efficacy for both the central location/data center as well as the remote location. A solution that is capable of dealing with the evolution of the threat landscape and the growing attacks happening daily in the retail world.

Today's Retail Network and Security Requirements

For retailers with many geographically dispersed shops or stores, having secure network connectivity and linking all sites to the head office has become the glue of critical operating processes such as the Point of Sale (PoS), accounting, inventory control, pricing, customer relationship management applications and other business services. The in-store store network is vital, yet invisible, to staff and shoppers alike until it stops working. When the network goes down, transactions halt, customers go elsewhere and cash registers stop ringing.

So what is needed for today's complex in-store security?

1. **Advanced Threat Protection**
   Protecting against advanced malware attacks requires a solution that integrates advanced security capabilities throughout the entire network. It requires a solution that integrates the security fabric into the network infrastructure, eliminating weak links throughout the network.

2. **Performance**
   With an increasing number of end points and applications and higher volumes of data, the network must be able to support the performance demands being placed on it.

But at the same time, the necessary security functions cannot be permitted to slow down the network. In the highly competitive retail environment, unnecessary delays in the sales process will result in lost customers. The network must maintain stringent levels of performance throughout the course of the day.

3. **A comprehensive in-store network**
   An in-store network can be considered as an independent entity but at the same time part of a much larger organism. While connectivity to main network is a key element, a secure in-store network, supporting both wired and wireless connectivity is critical for supporting existing applications and enabling new applications and services.

4. **Migration to lower cost public networks**
   Today's network planners have more connectivity options today than ever before. Traditional leased lines have been largely replaced with higher speed and lower cost options like DSL and MPLS services and wide area Ethernet. However, a still lower cost option is available – broadband Internet access. But leveraging the Internet for mission critical applications requires a robust in-store security solution to prevent data breaches.

5. **Adopting innovative in-store services**
   E-commerce and e-tailers have changed the face of the retail market. To fight back, traditional retailers have to find ways of improving the retail experience and promoting increased customer loyalty and sales. In-store technology, particularly wireless, is a key enabler for these initiatives. While wireless technology provides the flexibility to enable key initiatives, if not implemented correctly it is also a convenient entry point for the cyber criminal.

6. **Supporting PCI DSS compliance**
   With in-store networks carrying payment card transactions there is a mandatory requirement to satisfy Payment Card Industry (PCI) compliance requirements. The in-store network must be able to evolve as the PCI DSS standards evolve.

The Fortinet Connect and Secure Solution for Retail

Fortinet's Connect and Secure Solution for Retail is a complete, end to end networking and security solution that addresses the key issues that a distributed retail network is subjected to on a daily basis.

More Security - More Control - More Intelligence

Fortinet's Connect and Secure Solution for Retail enable retailers to secure multiple, geographically dispersed sites, systems and critical applications such as inventory control and point-of-sale (POS). Fortinet protects sensitive customer information and complies with industry best practices and regulations. The Connect and Secure Solution is built on five key principles; Network Security, Connectivity, Performance, Cost and Manageability.

Network Security

Security has to be at the center of any network. Without a strong security capability effective against today's threat landscape the network cannot meet the expectations placed on it. FortiGate is the heart of the Connect and Secure solution, consolidating multiple network security and networking functions into a single, high performance and cost effective platform. The FortiGate product line offers a wide range of models to meet the needs of the smallest to the largest site in the network.

If FortiGate is the heart of Connect and Secure, FortiOS has to be its soul. FortiOS is the intelligence powering each FortiGate, allowing it to be individually tailored to meet a site's specific security and networking requirements.

In order to be truly effective, the FortiGate must be able to keep up with the constant changes in the threat landscape that the network will encounter throughout its lifetime. FortiGate relies on FortiGuard, Fortinet's in-house threat protection service to ensure round the clock effectiveness.

However, network security is only half of a strong security solution. Authentication and access control are also key components of the overall solution and crucial in allowing intelligent policy to be applied to users and devices. The FortiGate is capable of providing user authentication locally or working cooperatively with central authentication systems such as RADIUS, Active Directory or FortiAuthenticator. With FortiAuthenticator as part of the security infrastructure, these authentication methods can be strengthened even further with Single Sign-On (SSO), 802.1x Port Access Control and certificate management. FortiAuthenticator also supports Two Factor Authentication (2FA) through FortiToken. Once a user or device has been identified and authenticated, policies can then be applied to control access to network resources and applications.

Connectivity

Devices, users and applications need to connect to the network by whatever access method is most convenient and best meets their requirements. Both wired and wireless connectivity requirements are satisfied by FortiGate's integrated Ethernet and WiFi capabilities. If more Ethernet connectivity is required, additional ports can be provided by FortiSwitch, which is also available in a range of different models. Through an integrated switch controller, FortiSwitch is easily managed through the FortiGate. Both FortiGate and FortiSwitch support Power over Ethernet (PoE), simplifying deployment of network attached devices such as wireless access points.

Since every FortiGate includes a wireless controller, wireless users and devices are easily integrated into the security fabric of the network. Depending upon site requirements, the wireless network can be fully self-contained by the FortiGate, referred to as FortiWiFi, or the FortiGate can be paired with Fortinet Access Points, FortiAP, to provide the necessary network coverage. FortiAP's are easily connected to the FortiGate via a standard Ethernet cable and take advantage of the FortiGate or FortiSwitch's PoE capability for easy installation. FortiAP's are available in a wide range of models for both interior and exterior applications.

Performance

While the FortiGate is capable of consolidating multiple functions onto a single platform, the question must be asked at what tradeoff. The ability to support these multiple functions while maintaining industry leading levels of performance is due to the FortiGate's architecture based on custom developed Application Specific Integrated Circuit (ASIC) technology. Each FortiGate relies on FortiASICs to perform specific functions, Network Processing (NP) and Content Processing (CP), to complement the central processor and deliver unparalleled performance. The latest version of the Network Processor, NP 6, also accelerates wireless traffic, further improving the overall performance of the FortiGate. Desktop versions of FortiGate also benefit from this investment through Fortinet's System on a Chip (SoC) with all security and networking function on a single ASIC

Cost

The Connect and Secure solution addresses the cost issue from several difference perspectives. The first is the elimination of redundant devices. Since the FortiGate consolidates multiple security functions into a single appliance the need for discrete appliances, one for each function, is eliminated. The same holds true for routing and switching. The combination of routing protocol support in FortiOS and high Ethernet port density in the FortiGate eliminates the need for separate routers and switches.

Since each FortiGate also includes a wireless controller the incremental cost for wireless connectivity is simply a matter of how many FortiAPs are needed for the location. There is no licensing cost for providing wireless access, either via the FortiGate or FortiWiFi models.

Finally, on most models of the FortiGate, licensing of the different software features is “a la carte”, that is you can pick and choose only the features that are appropriate for the site. The consolidation of network and security devices and selective software pricing allows the Connect and Secure solution to reduce both upfront and recurring costs for a superior TCO.

Manageability

Although Connect and Secure is a comprehensive solution it does consist of several different elements. The ability to centrally configure and manage the different elements is crucial as is defining and implementing consistent policy for users and devices. While individual FortiGate appliances can be managed locally through their web-based Graphical User Interface (GUI), a larger environment should take advantage of FortiManager to provide a “single pane of glass” management capability for the entire network.

Complementing FortiManager is FortiAnalyzer, providing centralizing reporting, event logging and analysis, allowing you to turn individual alarms and events into a comprehensive view of the state of the network.

Addressing Retail’s Requirements

The Connect and Secure solution comprehensively addresses the needs of the retail environment. The typical retail network can have up to thousands of sites, ranging from the data center to the smallest kiosk. In this environment, with so many possible infiltration points, protecting the in-store network is paramount. But installing multiple security products is time consuming, costly and difficult to manage.

FortiGate, with its full range of security and networking features provides a scalable and cost effective solution. Multiple security functions such as Anti-Virus (AV) and Intrusion Prevention (IPS) can be easily enabled, and cost effectively licensed, on the FortiGate to meet the specific needs of each site. With FortiGate as the backbone of the network, the network infrastructure and security fabric of the network are fully integrated.

Since FortiGate is a powerful networking firewall, it also allows customers to take advantage of lower cost, broadband Internet connections to connect some or all of the remote sites to the main network. FortiGate’s networking and security features provide a secure Virtual Private Network (VPN) connection to the main network and that the remote site is protected against Internet borne threats. Another advantage of using a broadband Internet connection is having a local Internet breakout. Internet traffic originating from the remote site will access the Internet locally while business traffic will be routed through the VPN connection to the network/data center.

A growing trend in the retail environment is the use of wireless connectivity in the store. Facilitating inventory with handheld scanners, equipping staff with tablets to improve the customer experience or deploying analytics to better understand consumer behavior, wireless technology has made and continues to make a significant impact. Access to the wireless network can also be extended to the customer. The question is how to secure the enterprise’s traffic and keep customers, and their traffic, away from resources on the network.

As the use of wireless technology is a fairly recent evolution in the retail industry, the issue has been how to integrate the wireless network with the existing in-store network. The easiest approach is to overlay the wireless network with the wired network. The downside of this approach is that while connected to the in-store network the wireless network is outside of

whatever security policies are in place that network. Yes, access to the network will have some sort of pre-shared key (WPA-PSK) and the access points might have some basic firewall functionality in them but as long as the wireless network is not an integrated extension of the in-store network it will be a weak link in the security chain. FortiGate addresses this issue through its full featured wireless capability, giving the in-store wireless network the same level of security as the wired network. Device and user identification and authentication are exactly the same regardless of the connection technology. Network access, based on successful identification and authentication, would allow customers, as guests, to access only the Internet or other predefined sites. FortiGate also supports multiple SSIDs with separate login so that a guest could only "see" the guest network.

A secure in-store wireless network also enables the use of presence analytics to better understand customer behavior. Fortinet's Presence Analytics solution, taking advantage of WiFi equipped smartphones and other mobile devices, can capture data that gives true insight into buying behavior, analyze the effectiveness of window displays and even trigger on the spot in-store promotions. All of this is designed to give the traditional retailer a competitive advantage against e-tailers. Please look to the Fortinet Retail WiFi Solutions Guide for more information about this powerful and innovative solution.

Since debit and credit card transactions are the lifeblood of the retail industry it's imperative that these transactions, and the data resulting from them, are made as secure as possible. An industry group, the Payment Card Industry (PCI) has developed a set of best practice standards, Data Security Standard (DSS) for any business who handles payment cards. The PCI-DSS standards define a set of 12 recommended actions to protect the cardholder data. Fortinet's Connect and Secure Solution is designed to help retailers meets PCI-DSS requirements today and to continue to do as the standards evolve.

Conclusion

In order to remain competitive in today's changing world, retailers will need to find innovative solutions to create value, reduce operating costs and mitigate risks, and maintain customer confidence and loyalty throughout the business. For retailers with many geographically dispersed shops or stores, secure in-store networks and network connectivity linking all sites to head office is critical to business operating processes. When the network is breached, sensitive customer data can be compromised with serious consequences to the business.

With Fortinet's Connect and Secure solution, a retail organization with hundreds of stores can quickly deploy and operate comprehensive high performance security solutions to all endpoints for a fraction of the costs of traditional solutions and stand-alone appliances.

The scalability of the Fortinet solution supports the evolution and growth of a retailer's IT and network infrastructure, so that they can easily and cost-effectively tailor the solution to meet their specific needs. The combination of world-class network security, connectivity and central management allows a retailer to have robust security for network resources no matter where data is stored or accessed. Retailers can easily deploy and centrally manage the solution throughout the distributed network, from kiosk to superstore. This helps supporting multi-channel operations and innovative services such as presence analytics and customer Internet access, as well as providing a high security posture and the tools to maintain compliance with PCI-DSS.

Retailers can have a world-class security solution that is scalable, cost-effective and easy to manage, which supports the growth of new applications and wireless networking in-store without affecting the end-user experience, increasing deployment costs or increasing staff burdens.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright © 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other resultsmay 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 certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. 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 covenants, representations,and guarantees pursuant hereto, whether express or implied. 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.