FORTINET INTEGRATES AND AUTOMATES NETWORK SECURITY FOR RETAILERS

Best-in-Class Network Performance and Protection

SOLUTION CHECKLIST

EXECUTIVE SUMMARY

Retailers seeking to deliver omnichannel customer experiences while embracing digital transformation (DX) initiatives must cover a wide range of networking and security requirements. The Fortinet Security Fabric extends protection from the data center to the edges of the network to the cloud. It integrates all of the different security areas under one powerful security platform and automates security processes and threat-intelligence sharing. With the support of best-in-class solutions from Fortinet, retailers are able to deliver powerful network performance while protecting critical customer and corporate assets.

RETAIL SECURITY CHALLENGES

Facing an industry in rapid transition, retailers are focused on growing their businesses by providing omnichannel customer experiences that span web and mobile ecommerce, as well as brick-and-mortar retail outlets. The potential entry points for attacks continue to grow as retailers expand the attack surface by pushing DX initiatives and omnichannel strategies. This broad attack surface, coupled with business-critical customer and corporate data, makes retailers very attractive targets for cyber criminals.

Attacks can come from different directions, and the complexity and disparity of retailer networks makes threat identification, detection, and remediation challenging and time-consuming. Cyber criminals can target data at rest and in motion—from the data center, to the software-defined wide-area network (SD-WAN), to the cloud, to point-of-sale (POS) systems, to Internet-of-Things (IoT) devices, to email, to endpoints, to wireless access points. Criminals can hold data and systems hostage until ransom is paid. They can launch distributed denial-of-service (DDoS) attacks that shut down ecommerce sites and disrupt supply chain operations. The list of possibilities continues to grow.

FORTINET SECURITY FABRIC PROVIDES INTEGRATED PROTECTION FOR RETAILERS

With the assistance of the Fortinet Security Fabric and powerful Fortinet network security solutions, retailers are able to protect their digital assets and infrastructures against threats.

Even though the attack surface for retailers continues to expand due to the adoption of cloud services, rapid growth in IoT, and increases in mobile services and devices, retailers have broad and scalable coverage with the Security Fabric. Additionally, the Security Fabric integrates disparate security elements and point solutions into a coherent platform, which enables the automation of security workflows and threat-intelligence sharing.

Fortinet holds nine different **“Recommended”** ratings from NSS Labs—twice as many as any other network security provider.

Fortinet has been named as a **“Leader”** in the Gartner Magic Quadrant for both enterprise network firewalls[1] and unified threat management.[2]

FORTINET BEST-IN-CLASS SECURITY SOLUTIONS

Integrated within the Fortinet Security Fabric, the following are some of the key solution areas that retailers use today to protect their critical assets and infrastructures and enable more efficient networking and management.

NEXT-GENERATION FIREWALLS: POWERFUL AND SECURE

FortiGate next-generation firewalls (NGFWs) include multiple security and networking controls as well as a Wi-Fi controller. FortiGate NGFWs deliver key security and networking capabilities for retail headquarters, branch offices, and stores. Included functionality such as network intrusion prevention system (IPS), data loss prevention (DLP), antivirus, web filtering, SSL inspection, application control, SD-WAN, and virtual private network (VPN) services are required for network security and secure connectivity.

By design, FortiGate NGFWs deliver top performance, even when all security controls are turned on. Custom-built security processors and parallel-path processing ensure retailers get the security they require without slowing down the network. Consider, for example, high SSL performance recently earned FortiGate its fifth consecutive “Recommended” rating in NSS Labs’ NGFW test results, demonstrating minimal performance degradation and 100% efficacy across all 32 of the cipher suites and emergent ciphers tested.[3] NSS Labs also found Fortinet offers the best price/performance among 10 different NGFW providers.[4]

UNIFIED ACCESS

In addition to comprehensive network and content security, Fortinet also delivers secure unified access. FortiAP wireless access points, easily managed with FortiGate, provide sophisticated security for in-store public Wi-Fi. Retailers can also use FortiAP technologies to segment their networks and isolate IoT traffic to protect against zero-day malware.

Serving as the backbone for wired and wireless traffic, FortiSwitch secure access switches are highly scalable and can be configured to mirror the security policies of the retailer's FortiGate. And FortiNAC network access control enables retailers to see and control all the various endpoints and IoT devices connecting to the network. This is especially critical for retail locations with POS devices and public Wi-Fi.

With a FortiExtender 3G/4G LTE wireless WAN extender, retailers can enable a secondary failover WAN link to improve business continuity. It also provides a primary WAN link for retail POS, remote ATM machines, and remote kiosk systems.

PRESENCE ANALYTICS

FortiPresence, a cloud-based application, allows retailers to measure consumer behavior, connect to customers, and influence them to make purchases. The unique combination of analytics with a sophisticated customer engagement engine (including social Wi-Fi) helps retailers to better engage with customers and increase sales.

FortiPresence leverages the existing onsite Fortinet access points to detect each visitor's smartphone Wi-Fi signal. It then delivers the data needed for retailers to understand visitor traffic and influence/improve their shopping experience in real time. It includes analytics, heat maps, and reporting across one year of stored data.

SD-WAN: LOWER TCO WITH ROBUST SECURITY

Fortinet Secure SD-WAN increases retail network performance and security by replacing separate WAN routers, WAN optimization, and security devices with a single solution that is application-aware, offers automatic WAN path control, and includes multi-broadband support. It also delivers high-performance VPN capabilities that can be deployed across multiple stores and branch offices.

Fortinet is the only NGFW vendor to provide native SD-WAN along with integrated advanced threat protection. This secure, high-performance SD-WAN eliminates the need to backhaul traffic for security checks, accelerating application delivery and improving network performance in corporate offices and retail locations.

In 2018, the NSS Labs comparative test for SD-WAN solutions found that the Fortinet total cost of ownership (TCO) of $5 per Mbps was not only the lowest among the 10 products tested but also only 3.8% of those 10 solutions' $134 average TCO per Mbps.[5] This performance-to-TCO ratio is particularly important for retailers, where margins are typically tight.

CLOUD SECURITY

The Fortinet unified cloud security solution addresses the needs of retailers turning to many different cloud platforms to support DX. Fortinet cloud security enables retailers to achieve security across all their cloud deployments, cloud storage, and SaaS apps with one solution. This eliminates the unmanageable complexity brought on by the typical practice of adding a multitude of disparate point products to address each vulnerability separately.

Our cloud solution enables unified visibility and control, plus policy management, to support risk management and compliance requirements in retail environments. By breaking down silos between the different clouds a retailer relies on, IT staff gain clear and consolidated visibility and incident analysis of threats and mitigation efforts across all the retailer's applications, regardless of where they're housed.

Further, for AWS users, the AWS Security Hub and Fortinet Security Fabric can help organizations establish consolidated visibility and ensure consistent security across their hybrid infrastructures. The combined findings from these different services enable customers to analyze current trends and identify the highest-priority security issues across their AWS environments.

ENDPOINT PROTECTION

The FortiClient endpoint protection platform (EPP) delivers the transparent visibility and centralized security controls that enable retailers to respond quickly and effectively to attacks. It enables cybersecurity staff to discover, monitor, and assess endpoint risks in real time. Compromised systems can be automatically quarantined, minimizing the impact of a breach.

POS applications in particular are very attractive targets that can be best protected with tight integration into the Security Fabric. FortiClient shares endpoint POS telemetry with the Security Fabric, delivering broad endpoint visibility, compliance control, and vulnerability management.

FortiClient covers all the bases with pattern-based anti-malware, behavior-based exploit protection, web filtering, and an application firewall. It integrates with FortiSandbox to detect zero-day threats and custom malware. In addition, it provides secure remote access with built-in VPN, single sign-on, and two-factor authentication for safe network access from retail stores and branch offices.

MAIL SECURITY

Regardless of industry, email remains a favorite target of hackers.[6] Retailers approach email in different ways: some use an on-premises or cloud email client, and some are taking advantage of SaaS apps, such as Office 365. Regardless of location, FortiMail inspects retail employees' email for unwanted and malicious messages and inappropriate/sensitive content. It provides comprehensive security for both incoming and outgoing messages and is easy to deploy, operate, and manage. FortiMail can be used to protect sensitive data of all types, reducing the risk of inadvertent loss and/or noncompliance with regulations like the Payment Card Industry Data Security Standard (PCI DSS).

If email security doesn't share information about attacks with the rest of the security infrastructure, a successful intrusion somewhere else in the retailer's network is possible. Fortinet is the only vendor with email security as part of an integrated and automated fabric architecture, enabling it to automatically generate and share intelligence to address advanced threats across all major attack vectors, which is key to defending distributed retail environments.

WEB APPLICATION FIREWALL

The FortiWeb web application firewall (WAF) uses the latest threat intelligence to protect web applications from sophisticated attacks while lowering management and operational costs. It protects from new malware targeting POS systems as well as the classics like the OWASP Top 10. DDoS attacks on IoT devices and ransomware are on the rise, and downtime from such attacks is especially harmful for retailers. It is important to have an effective WAF without the extra noise caused by false positives.

Fortinet's unique approach uses dual-layer artificial intelligence-based detection engines and machine learning (ML) to intelligently detect threats with nearly no false positives. Already overburdened retailer IT staff can react quickly without wading through large amounts of false positives typical of most WAFs today.

FortiWeb offers flexible deployment options: hardware, virtual machine, cloud application, and as a hosted cloud service for fast deployment and no capital expenditure.

EASY DEPLOYMENT, MANAGEMENT, AND ANALYTICS

For retailers in particular, margins are thin and breaches are costly. An excellent way to save resources while augmenting security is to take the complexity out of security management and enable full visibility. In addition, it is key to meet compliance both with reports for targeted audiences and quick response in the event of a data breach.

Fortinet offers management, analysis, and security information and event management (SIEM) solutions, which allow retailers to see the big picture as well as pinpoint specific events that need immediate attention. Core components of the Fortinet solution include:

- FortiManager, which combines information from both operations (network operations center [NOC]) and security (security operations center [SOC]). It provides a single-pane-of-glass view across the entire Fortinet Security Fabric for full visibility and easy management.
- FortiAnalyzer, a network security logging, analysis, and reporting tool that aggregates log data from all Fortinet security appliances. It provides a comprehensive suite of easily customizable reports that allow quick analysis and visualization of network threats, inefficiencies, and usage. FortiAnalyzer also provides valuable tools for network vulnerability scanning, which is a key requirement for PCI DSS compliance.
- FortiSIEM, which enables visibility and management of Fortinet and Fabric-Ready Partner solutions for smooth operation and greater insight. Reduced cost and complexity with centralized control of the entire network from a single console drives a lower TCO for retailers. Automated reporting helps track retail regulation compliance.

To free up IT resources, retail businesses that manage tens or hundreds of locations can take advantage of FortiDeploy. FortiDeploy is a key capability in FortiManager for one-touch device provisioning with proven scalability to over 10,000 sites. There is no need to have an IT expert at each branch office or retail store.

ADVANCED THREAT PROTECTION

Retail networks require proven, real-time threat intelligence. FortiGuard Labs uses artificial intelligence (AI) to collect, analyze, and classify threats at machine speed with an extremely high degree of accuracy. Specifically, its comprehensive threat detection leverages AI and ML to write signatures for new malware in real time and publishes them across the entire Security Fabric. FortiGuard Labs has three services bundles from which retailers can choose based on their business requirements.

Sandboxing adds a critical layer of protection from previously unknown and sophisticated threats. Retail environments that are widely distributed and offer public Wi-Fi are at risk of advanced threats slipping through. FortiSandbox isolates and inspects suspicious files—including SSL-encrypted traffic—before they have the chance to damage the network. FortiSandbox can then share information about any detected threats with the other security elements in the Fabric.

INTEGRATED SURVEILLANCE

For brick-and-mortar retailers, strong risk management includes physical security. Fortinet offers a network-based security surveillance system that seamlessly integrates FortiCamera and FortiRecorder with FortiGate NGFWs, to monitor any retail location. FortiRecorder captures IP video for easy monitoring, storage, and retrieval. Set up is quick and monitoring is easy through a web browser.

FORTINET IS THE IDEAL PARTNER FOR RETAIL NETWORKS

With more than 375,000 customers, Fortinet is the fastest-growing enterprise network security company in the world, plus the No. 1 most adopted network security solution.

With Fortinet, retailers can take advantage of:

- Independently validated best performance and lowest TCO solutions in many categories
- Powerful security controls that do not impact network performance
- Consistently recommended solutions by industry-respected third parties such as NSS Labs and Gartner
- Award-winning technical support
- Unmatched innovation with three to ten times more patents than other network security companies
- Ground-breaking AI/ML capabilities for faster and more effective protection across the Security Fabric

Fortinet comprehensive, easy-to-manage solutions address the security challenges facing today's retailers as they transform and optimize the omnichannel customer experience. With a unique architecture that saves time and resources while delivering advanced threat protection, Fortinet is the ideal retail security partner for this journey.

> *"Fortinet is the perfect vendor to help Harley-Davidson Dealer Systems deliver on the promise of freedom and security that our dealers expect and deserve."*
>
> *– Bradley Ruff,*
> *Knowledge Center Lead,*
> *Harley-Davidson Dealer Systems*

> *"Our extended IT infrastructure is absolutely critical to everything we do, so it's invaluable to have the seamless protection that Fortinet provides across our physical and cloud-based domains."*
>
> *– Stuart Berman,*
> *Global Security Architect,*
> *Steelcase*

> *"With Fortinet, we can control the entire network remotely at every level all from one console, and we have the threat visibility and reporting to satisfy PCI DSS compliance obligations with ease."*
>
> *– Paul Jackson,*
> *IT Director,*
> *Lush Cosmetics*

[1] Frank Marsala, "Magic Quadrant for Enterprise Network Firewalls," Gartner, July 11, 2017.

[2] Jeremy D'Hoinne, Rajpreet Kaur, and Adam Hils, "Magic Quadrant for Unified Threat Management," Gartner, June 20, 2017.

[3] Nirav Shah, "High SSL Performance Earns FortiGate 5th Consecutive 'Recommended' Rating in Latest NSS Labs NGFW Test Results," Fortinet, July 17, 2018.

[4] Thomas Skybakmoen, "Next Generation Firewall Comparative Report, Total Cost of Ownership (TCO)," NSS Labs, July 17, 2018.

[5] Thomas Skybakmoen, "SD-WAN Comparative Report, Total Cost of Ownership (TCO)," NSS Labs, August 8, 2018.

[6] "Verizon 2018 Data Breach Investigations Report," Verizon, April 2018.

FORTINET®

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

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

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

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Copyright © 2018 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 results may 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. 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.