WHITE PAPER

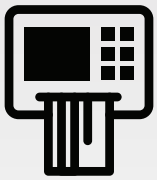
Fortinet Retail Cybersecurity Solutions

Protecting Retailers Against Advanced Threats While Providing Positive Shopping Experiences

Executive Summary

Fortinet offers retailers a broad set of network and security technologies that are seamlessly integrated and automated with the Fortinet Security Fabric. For retailers seeking to address a number of use cases—ranging from creating omnichannel shopping experiences to improving the efficiency of business operations, Fortinet solutions solve the major network infrastructure and security issues. High-performance solutions with both best-in-class network and security capabilities from Fortinet address a wide range of retail use cases.

With deep integration within the Fortinet Security Fabric that offers broad coverage across the entire retail attack surface and artificial intelligence (AI)-driven threat intelligence from FortiGuard Labs, Fortinet breaks down silos in the cloud and on-premises, from headquarters to the remote and branch locations. This provides retailers with transparent visibility and real-time security workflows and threat-intelligence sharing. This level of integration also unlocks automation that enables lean network and security teams to work more efficiently and faster while also allowing them to reduce risk—all at a low total cost of ownership (TCO).



87% of retail firms experienced at least 1 malicious intrusion in the past year—over half had 3.[1]

According to Fortinet research, 11 of 13 Fortune 100 retailers use Fortinet solutions for their network security.

Introduction

Retailers present cyber criminals with an attractive target. Customer payment card data is transmitted across the network and stored on-premises and in public and private clouds. At the same time, the arrival of omnichannel customer experiences creates challenges in branch retail locations where customers demand high performance and secure connections, while retailers seek insights on customer behaviors that can be used to deliver better engagement. And faced with acute cybersecurity staffing shortages, retailers struggle to cover all their security gaps—something that is exacerbated by the proliferation of point security products and the advanced threat landscape.

Key Features of the Security Fabric and Fortinet's Approach to Retail Cybersecurity

Fortinet enables retailers to address the challenges with the Fortinet Security Fabric, which gives them seamless integration of all security aspects while unlocking automation of workflows and threat intelligence. Additionally, prebuilt Fabric Connectors give retailers the ability to integrate third-party Fabric Partner solutions, while the open application programming interface (API) architecture of the Security Fabric allows retailers to add other security solutions quickly and easily.

Key capabilities of Fortinet cybersecurity solutions for retail include:

Visibility

With the Fortinet Security Fabric, retailers achieve centralized visibility and control of all point security products deployed in their network. Built-in connectors and an open API framework allow integration and management of all security solutions.

Automation

Fortinet solutions support automated threat detection and response, policy enforcement, and compliance report generation, all of which increase the effectiveness of retail IT staff. Automation includes prebuilt workflows and reporting for industry standards like the Payment Card Industry Data Security Standard (PCI DSS) and security standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Proactive threat intelligence

Threat intelligence created via AI and machine learning (ML) is communicated across the Security Fabric in real time, stopping rapidly evolving threats that target point-of-sale (POS) systems, cloud deployments, and other retail network infrastructure.

High performance

FortiGate next-generation firewalls (NGFWs) offer the industry's lowest latency and allow deep inspection of secure sockets layer (SSL)/transport layer security (TLS) encrypted traffic with minimal impact on network performance in speed or throughput.[2] This is crucial in a retail setting, where consumers expect high performance from every company touchpoint.

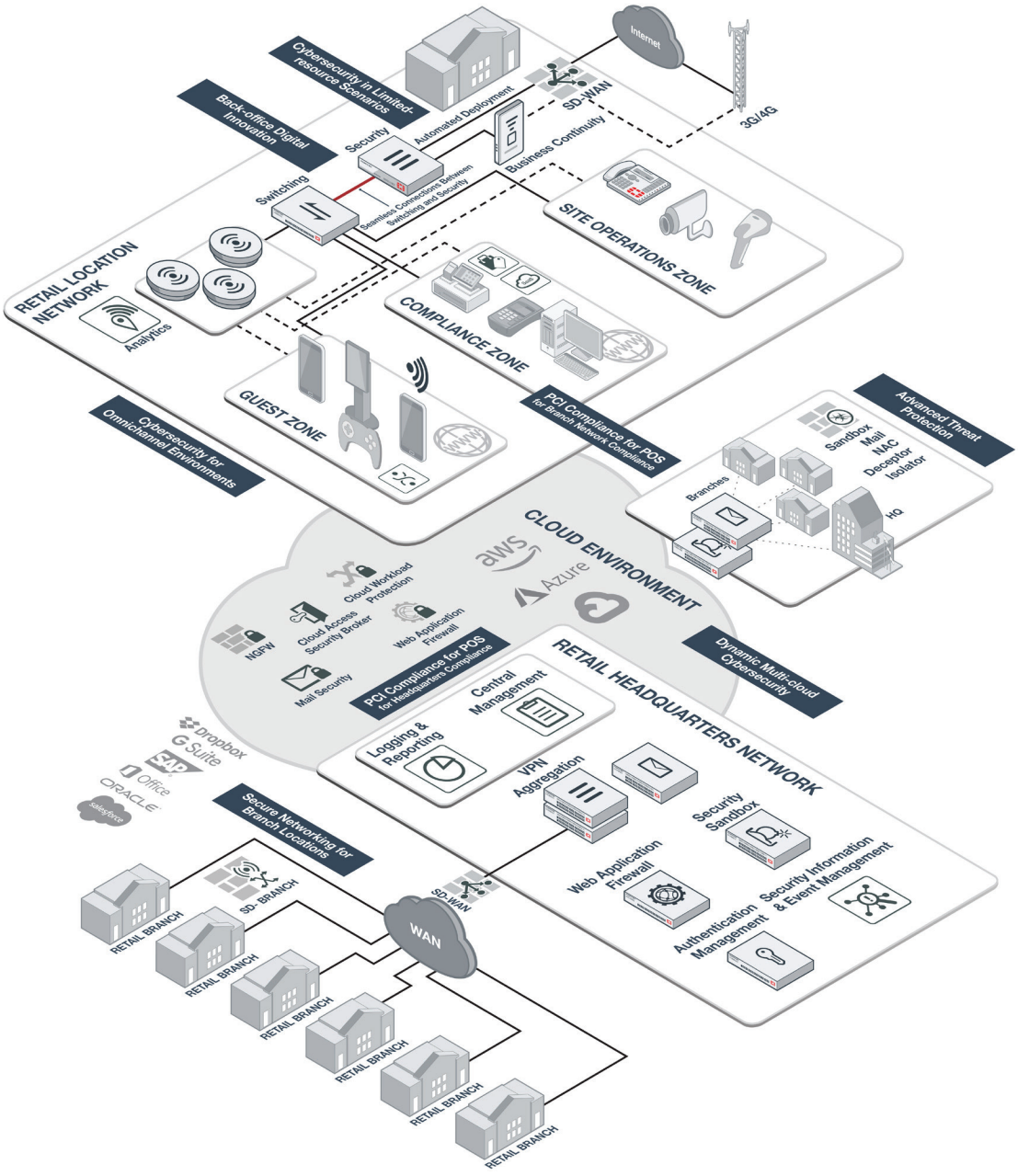


Figure 1: Retail cybersecurity solutions from Fortinet protect the organization's entire network—from POS devices to cloud infrastructure—while helping to maintain compliance with PCI DSS and other regulations and standards.

Use Cases

Fortinet solutions enable retailers to address numerous use cases. These include:

Cybersecurity for omnichannel environments

Retailers can use Fortinet to provide a flexible and personalized in-store shopping experience for customers while maintaining network security and collecting valuable business intelligence. Guest wireless networks include a captive portal for social media login, and advanced visitor presence and positioning analysis allows dynamic location-based advertising.

Fortinet offers retailers a broad portfolio for protecting their omnichannel environments, starting with FortiGate Secure SD-WAN and Fortinet Secure SD-Branch capabilities that consolidate security and network technologies at branch locations into one solution that delivers low TCO at high performance. FortiFone and FortiVoice give retailers plug-and-play Voice-over-IP (VoIP) capabilities that connect directly to the network. FortiPresence provides retailers the ability to send instant deals and special offers based on location-based analytics. FortiMail protects customer service and employee email accounts, ensuring that systems are safe from ransomware and other threats that could impact customer experience.

Cybersecurity in limited resource scenarios

Retailers are operating widely dispersed store locations that may have very different network and security needs. Scaling retail operations with a shortage of skilled cybersecurity resources requires greater efficiency through automation and centralization.

Here, Fortinet solutions allow retailers to secure all their locations without requiring on-site security staff. FortiDeploy enables them to preconfigure security solutions and complete setup automatically once network and security devices reach their destination, while FortiGate NGFWs centralize visibility and control of a location's security infrastructure. With FortiManager and FortiAnalyzer, retailers can achieve full visibility of networks spanning 10,000+ locations and control security configurations and policies of distributed retail locations from a single web interface.

PCI compliance for POS

Achieving PCI DSS compliance is simpler with Fortinet. Centralized visibility into deployed POS devices and preconfigured PCI DSS reporting templates dramatically decrease the manual processes and overhead associated with demonstrating regulatory compliance. The Fortinet Security Fabric provides real-time telemetry information for Fortinet solutions and the Fabric-partner ecosystem using built-in connectors. For security products that are not part of the Fabric-partner ecosystem, an open API framework gives retailers the means to quickly and easily integrate additional solutions into the Security Fabric.

With FortiManager and FortiGate NGFW, retailers can automatically detect and identify devices on the network and manage and enforce policies from a centralized location to ensure compliance with regulations such as PCI DSS. FortiAnalyzer provides out-of-the-box PCI DSS report templates and comprehensive, historical network visibility to simplify auditing and reporting for PCI DSS and a number of other regulations and standards.

FortiGuard Labs extracts threat intelligence from over 100 billion security events daily.[3]

Intrusions Experienced in Retail[4]

(in the past 12 months)

- Malware, 50%
- Spyware, 44%
- DDoS, 36%
- Phishing, 24%
- Insider threats, 23%
- Mobile breach, 23%
- Ransomware, 23%
- Zero-day attacks, 17%
- SQL injection, 15%
- Man-in-the-middle attacks, 11%

Impact of Intrusions in Retail[5]

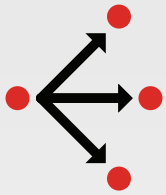
(in the past 12 months)

- 42% had a degradation in brand awareness
- 40% experienced an operational outage that impacted revenue
- 39% suffered an operational outage that affected productivity
- 33% had an operational outage that put physical safety at risk
- 30% lost critical business data

Secure networking for branch locations

Retailers need fast and scalable connectivity to enable seamless transactions in support of sales, inventory, purchasing, and other activities. Fortinet solutions provide high-speed, reliable in-store networking to support a good customer experience and secure SD-WAN for efficient routing of traffic between retail locations and cloud infrastructure without sacrificing security.

In addition to the above, retailers can improve efficiency by consolidating network and security architecture, centralizing device visibility and management, and optimally routing over 5,000 types of application traffic via FortiGate Secure SD-WAN and Fortinet Secure SD-Branch. Further, plug-and-play solutions like FortiVoice and FortiFone provide VoIP communications directly over the network. For business resiliency, FortiExtender ensures 100% connectivity uptime using 3G/4G cellular backup integrated with Secure SD-WAN.



Fortinet Secure SD-WAN offers the industry's lowest latency and a TCO 8x better than competitive offerings.[6]

FortiGuard Labs is credited with over 720 zero-day discoveries, more than any other security vendor.[8]

79% of enterprises and 78% of SMBs run workloads in the cloud. 81% of enterprises and 72% of SMBs consider security a challenge to this trend.[9]

Advanced threat detection

Based on Fortinet research, 87% of retail organizations have suffered some kind of an intrusion. Moreover, analysis by FortiGuard Labs[7] shows that up to 40% of new malware detected on a given day is zero day and/or previously unknown. Retailers must go beyond threat detection as usual.

FortiGuard Labs' AI- and ML-generated threat intelligence is shared via the Fortinet Security Fabric in real time, informing point security products of the latest threats. FortiSandbox and FortiIsolator protect the network against potential threats by analyzing external content in an isolated environment before it enters the network. With FortiInsight and FortiDeceptor, retailers can detect internal threats based upon user and entity behavior analytics (UEBA) and use of false targets designed to tempt attackers.

Back-office digital innovation

Many retailers are utilizing headless Internet-of-Things (IoT) and radio-frequency identification (RFID) technologies to streamline processes related to inventory and logistics. These additional—and often insecure—network nodes expand the attack surface. Retailers must consider a security-driven strategy to such network expansions that does not unduly drive up costs.

One cost-efficient approach is to leverage Fortinet Secure SD-Branch to run side-by-side business and guest networks, allowing IoT devices to be isolated from the public Wi-Fi network. FortiNAC automatically detects IoT devices on the networks and allows centralized visibility and control and automated responses to common threats. FortiAP provides high-speed, reliable network access with integrated security that can be centrally managed via FortiGate NGFW and allows centralized port-level switch monitoring using FortiSwitch.

Dynamic multi-cloud cybersecurity for retail

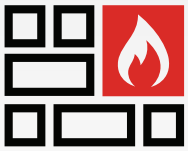
Retailers operate large networks of geographically distributed branch locations, making the use of cloud services a logical choice. However, network infrastructure that sprawls over private clouds, public clouds, and on-premises data centers often creates a very siloed environment that is difficult to secure. Retailers operating multi-cloud deployments can use Fortinet cloud security offerings to centralize visibility, configuration management, and policy enforcement across multiple cloud security providers (CSPs).

Retailers can also centralize visibility, configuration management, and access control over multiple cloud environments by deploying FortiCASB and FortiCWP. FortiGate NGFW is available as a virtual machine (VM) or Software-as-a-Service (SaaS) in the cloud, providing integrated protection to cloud deployments. Cloud-based email and web applications can be protected against attack by deploying FortiMail and FortiWeb, which use the latest technology and intelligence from FortiGuard Labs to protect against advanced and rapidly evolving threats.

Conclusion

Retail organizations are under constant threat, whether attackers are trying to steal customer financial data or sabotage a retailer's operations. As retail networks grow more complex, including multi-cloud infrastructure and deployment of IoT devices over multiple locations, Fortinet solutions, linked by the Fortinet Security Fabric, can ensure that retailers have the centralized visibility and control that they require to protect their networks against evolving threats and to maintain regulatory compliance. Using Fortinet solutions, retailers can integrate their networking and security infrastructure, providing high-speed, reliable connections to retail locations, and glean valuable business insights that can be leveraged to drive additional customer conversions.

Fortinet holds nine different "Recommended" ratings from NSS Labs—more than any other network security provider.[10]



Fortinet is a "Leader" in the Gartner Magic Quadrant for enterprise network firewalls.[11]

[1] Findings based on a series of survey studies with different retail/hospitality/travel personas conducted by Fortinet. Research report forthcoming.

[2] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, October 14, 2019.

[3] "FortiGuard Security Services," Fortinet, October 2019.

[4] Findings based on a series of survey studies with different retail/hospitality/travel personas conducted by Fortinet. Research report forthcoming.

[5] Ibid.

[6] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, October 14, 2019.

[7] "Using AI to Address Advanced Threats That Last-Generation Network Security Cannot," Fortinet, June 8, 2019.

[8] "FortiGuard Security Services," Fortinet, October 2019.

[9] "RightScale 2019 State of the Cloud Report," Flexera, 2019.

[10] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, October 14, 2019.

[11] "Rajpreet Kaur, et al., "Magic Quadrant for Network Firewalls," Gartner, September 17, 2019.

FORTINET

www.fortinet.com

July 16, 2021 7:11 PM

516437-A-0-EN