

Transforming the Retail Store Experience With Wi-Fi

Executive Summary

Today, the omnipresence of smartphones and the emergence of the Internet of Things (IoT) put Wi-Fi center stage as a strategic imperative in retail. To prevail in the mobile age, savvy retailers know that Wi-Fi belongs at the heart of the shopping experience and they need to extract maximum value from their Wi-Fi infrastructure investment.

The full scope of retail Wi-Fi applications is yet to unfold, and retailers who take advantage of it are in position to thrive in this new connected environment. However, retailers embracing Wi-Fi must balance the need for security with the flexibility of allowing almost any type of device onto the network.

Fortinet delivers a secure wireless local-area network (WLAN) solution that helps retailers securely maximize efficiency and proactively influence in-store sales. It provides complete protection against everything from wireless protocol and radio frequency (RF) attacks to malware and viruses, while easing the burden of Payment Card Industry (PCI) compliance. The Fortinet WLAN solution enables retailers to transform the shopping experience and convert walk-bys into walk-ins, showroomers into loyal customers, and loyal customers into brand ambassadors.

Retail Challenges

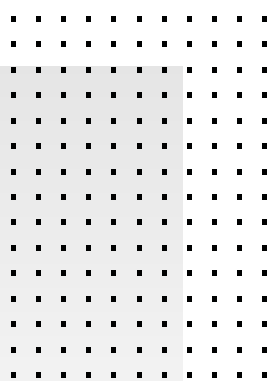
With stores of different sizes in multiple remote locations, it is no wonder retailers are cautious about deploying wireless networks at all their retail outlets. Beyond setup difficulties, managing the RF space and maintaining performance can be particularly challenging, especially in multitenant environments. Remote locations require plug-and-play setup, self-optimizing capabilities, and functional consolidation.

Looking beyond PCI compliance, security should always be a top priority in retail. Mobile platforms and IoT devices are targets for malware and other security threats, yet retailers need to let these devices onto their networks. From ensuring secure payment transactions to preventing malicious activity on Wi-Fi networks, retailers need integrated security solutions that combat the latest threat vectors and zero-day attacks.

New capabilities are evolving rapidly. As these technologies are introduced into the retail network, Wi-Fi solutions must adapt to provide the feature flexibility, performance, and application control to handle a broad mix of traffic, which could include biometrics, video, voice services, payment transactions, and advertising. At the same time, the solution needs to be able to serve patrons and harvest consumer analytics from store visitors. It must be possible to tailor application policies for each site depending on what is deployed centrally and push those policies out to remote sites.

Fortinet Solution Overview

Fortinet offers a secure WLAN solution that is ideal for retailers with multiple locations. It can be deployed to thousands of remote locations over any type of wide-area network (WAN) and can deal with every type of wired and wireless threat, far exceeding the minimum requirements of PCI compliance. Fortinet WLANs can easily handle the quality of service (QoS), bandwidth, security, and regulatory requirements placed on retail networks. The WLANs can carry financial information alongside different traffic types, ensuring that each gets the right security, resources, and priority. Centralized policy management offers complete control and flexibility over application policies and implemented features at each location. The Fortinet FortiDeploy solution enables zero-touch deployments at remote sites, which reduces the burden on IT staff during rollouts.



24% of cyberattacks target retailers. Retail has become the number one target for cyber criminals with more breaches than any other business sector.¹

Fortinet Access Points

Fortinet access points (APs) provide complete coverage for all indoor, outdoor, and remote situations. They work in conjunction with a local or centralized FortiGate WLAN controller that combines WLAN control, virtual private network, firewall, and unified threat management features into one platform. The family of Wi-Fi 6 access points supports the full set of enterprise features, including location tracking, rogue AP detection, wireless intrusion detection system (WIDS), bridging and mesh services, QoS, and bandwidth management without the need for special feature licenses. Retailers can mix and match the features they need for different deployment scenarios without licensing compliance obstacles and hidden costs. The APs are also easy to install at remote locations; just plug and play with no on-site IT staff required. The APs use automatic radio resource provisioning and spectrum sampling to automatically optimize radio settings and will automatically discover the FortiGate WLAN controller. Once discovered, a tunnel is created between the AP and the WLAN controller, which provides secure access to corporate resources, guest onboarding, and centralized policy enforcement.

Retailers that deploy Wi-Fi systems are able to home in on the needs of existing customers and transform casual browsers into loyal new patrons.²

FortiGate Network Security Platform

At the heart of the Fortinet WLAN solution is the FortiGate network security platform, which consolidates the functions of the WLAN controller with firewall, intrusion prevention, antivirus, antispam, WAN optimization, web content filtering, and application control. With the FortiGate, retailers can safely run multiple business service set identifiers (SSIDs) and guest SSIDs side by side with complete separation and different policies for each. Retailers can give customers Wi-Fi access through a branded hot spot and request that they opt in using a social login or other authentication method.

Fortinet goes far beyond meeting PCI compliance requirements such as rogue AP and wireless intrusion prevention. FortiGates provide total protection against wireless protocol and RF attacks, as well as malware, keyloggers, viruses, and zero-day attacks on all devices regardless of the operating system. Secured by FortiGuard, which continually researches the latest attacks, each FortiGate receives daily updates with newly discovered virus and malware signatures for continuous, up-to-date protection. With more than 3,300 application signatures, the FortiGate uses hardware-based, deep Layer 7 inspection to provide bandwidth guarantees and prioritization for critical applications. Inappropriate content can be blocked, bandwidth abusers can be throttled, devices can be quarantined, and showroomers can be monitored. A FortiGate also provides a complete solution for bring-your-own-device (BYOD) onboarding of employee-owned devices. It lets you enforce virus and integrity checks and use a wide range of authentication types.

FortiPresence Wi-Fi Presence Analytics

Using the Fortinet FortiPresence Wi-Fi presence analytics, retailers can gather customer analytics, engage with customers, and drive in-store sales. By turning the omnipresence of smartphones into an asset and not a threat, retailers can combat showrooming with marketing strategies that incorporate Wi-Fi and social media and use in-store Wi-Fi to build loyalty and influence consumer purchases in real time. Retail marketers can use presence and positioning analytics to measure the effectiveness of merchandising and marketing campaigns and to optimize staff rosters to match customer flow.

FortiLink Network Access Control

IoT devices are increasingly used by successful retailers to set themselves apart from the pack. Yet often these devices are rolled out before a satisfactory method to secure them is in place. The FortiLink network access control (NAC) provides profiling of IoT devices on the network using multiple information and behavior sources. The FortiLink NAC then works within the FortiGate to implement segmentation policies on the wireless network to ensure these critical customer experience devices are secured appropriately. Should something malicious happen to a device, indication of compromise services can react in seconds to contain threats before they spread. The FortiLink NAC offers a broad and customizable set of automation policies that can onboard IoT devices and keep them secure.



Powering Retail Applications With Fortinet

Fortinet WLANs empower retailers to go beyond providing basic internet access and streamlining operational activities. They can transform customer engagement, drive loyalty and sales, and give marketing much-needed visibility into consumer behavior.

By combining enterprise-grade WLAN infrastructure with unified threat management and presence analytics, the Fortinet wireless solution supports the widest range of retail-specific functionality:

Video Surveillance	Monitor stores and parking areas remotely with more flexibility and lower cost than closed-circuit television (CCTV)
Theft Prevention	Place Wi-Fi-enabled passive radio-frequency identification (RFID) readers anywhere, avoiding cabling costs
Asset Tracking	Track valuable assets to avoid misplacement using active Wi-Fi RFID tags
Customer Service	Enable fast product, price, and inventory searches on in-store kiosks and sales associates' mobile devices
Point of Sale	Reduce delays by taking orders and payments at the customer's side
Communications	Keep staff connected and fully mobile using Voice over Internet Protocol (VoIP) on mobile devices and badges
Presence Analytics	Use visitor data to measure customer loyalty and merchandising and to optimize staffing
Social Wi-Fi Opt-in	Fuel your marketing by providing in-store Wi-Fi access in exchange for customer opt-in
Real-time Offers	Combine presence and big data to market to customer devices and to include on digital signage
Digital Ads	Use Wi-Fi-enabled digital displays such as flat panels and smart shopping carts for targeted advertising
Operations	Enable Wi-Fi barcode scanners for stock-taking and inventory management

Address the Needs of Shoppers

To address the needs of today's connected shoppers and compete with online retailers, brick-and-mortar stores need sophisticated wireless networks that deliver much more than basic operational support and customer service. They must also provide the analytics and consumer intelligence marketers need to measure customer behavior and respond to online shopping alternatives. Emerging technologies could even tip the balance in favor of traditional retailers, assuming retailers have a suitable network foundation to handle the varied bandwidth, application priorities, and requirements related to PCI compliance and stringent data, network, and personal security. The Fortinet secure WLAN solution provides that foundation and combines it with advanced consumer analytics and application intelligence to give retailers a competitive advantage. For more information about Fortinet Wi-Fi solutions for retail, please go to www.fortinet.com/wireless.

¹ "Retail Cybersecurity Statistics," Fortinet.

² Comcast Business, "How Wi-Fi analytics can help shape retail customer outcomes," San Francisco Business Times, August 12, 2021.



www.fortinet.com