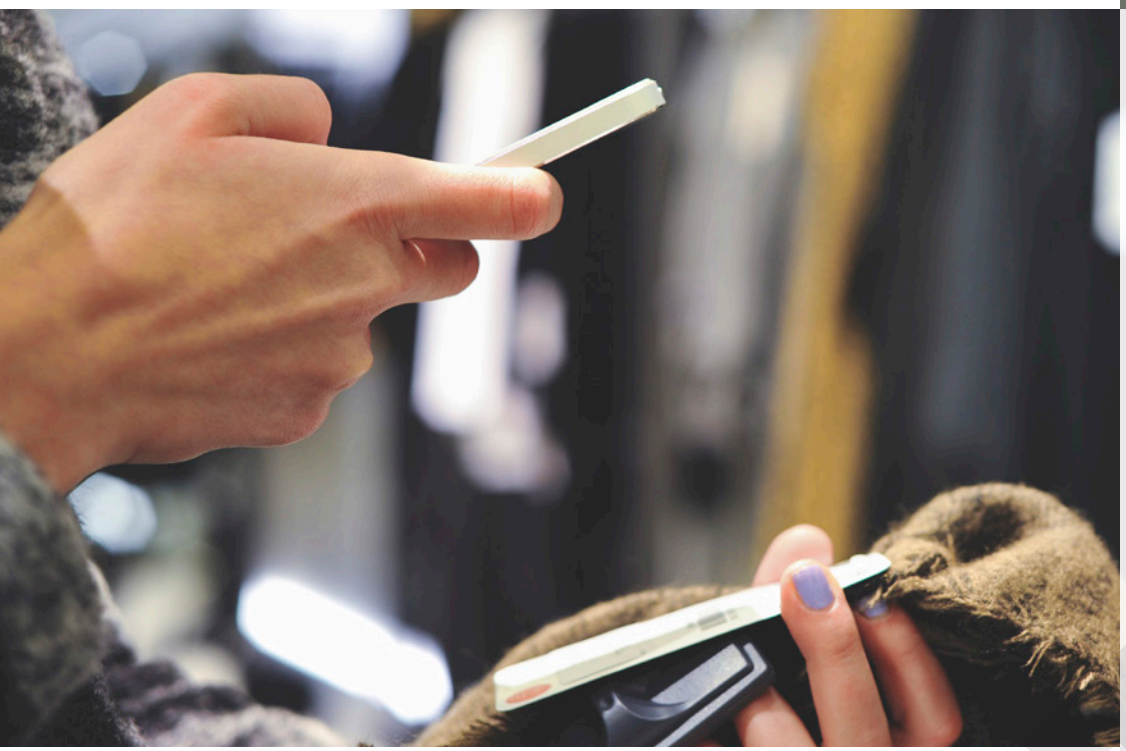

SECURE ACCESS

With a secure access architecture that enables retailers to choose a controller or cloud-managed deployment model, without compromising security, Fortinet wireless solutions enable retailers with locations of any size to embrace the omni-channel model and transform the in-store experience.

Fortinet Secure Access for Retail

Enabling Omni-channel Retail with Secure Wi-Fi

Retail stores are struggling while e-tailers enjoy double-digit annual growth. To compete, savvy bricks-and-mortar retailers know they must embrace omni-channel and exploit the omnipresence of smartphones and the emerging Internet of Things to transform the in-store experience and give customers what they want, the way they want it.

The omni-channel model allows brick-and-mortar retailers to interact with customers face to face and digitally in the stores, online through e-commerce sites and push marketing, and through mobile retail apps. But whether you are a multinational chain or a small boutique, providing such capabilities requires a new level of secure access supported by secure back-end applications geared toward customer engagement.

Wi-Fi is given as the enabling access technology. Pervasive free Wi-Fi in food and beverage, apparel and consumer goods stores has made it almost mandatory in every retail outlet. But guest access and social login only scratch the surface of what is possible. The full scope of retail Wi-Fi applications is still unfolding.

Wi-Fi is assuming a principal role in retail operations and marketing. Beyond merely facilitating in-store Internet access and inventory management, progressive retailers are using wireless networks to power digital advertising, point-of-sale, building automation, surveillance and voice services and to produce invaluable consumer analytics in the process. This requires a comprehensive security framework to protect against all manner of cyberthreats from access to applications.

The downside of the exponential growth in the number and variety of devices and applications accessing the network is that it enlarges the attack surface for cybercriminals—lurking out there armed with ever-more persistent and sophisticated threats—to target. This puts the entire business at risk.

When the same network is used by shoppers and retail associates alike, it is critical that your network security is capable of detecting and preventing advanced threats and mitigating risks, to proactively protect critical business assets (infrastructure, applications, data and services).

- Choice of premise and cloud-based network and security management
- Comprehensive threat protection with either deployment model
- Able to properly secure digital displays, mPOS terminals, cameras and Internet of Things devices
- Rich set of options for guest access and social login
- Complete PCI-DSS/CISP compliance with easy reporting
- Unmatched visibility and control of applications and utilization
- Security kept up to date through regular signature updates from FortiGuard Labs
- Advanced visitor presence and positioning intelligence

Fortinet's innovative Secure Access Architecture and internal segmentation cybersecurity strategy enable retailers to seamlessly segment devices and access layers across wired and wireless networks, ensuring the network is secured from all points of access.

With two purpose-built premise and cloud-managed wireless offerings, a line of PoE switches and an industry-leading cooperative security fabric, Fortinet gives retailers the maximum choice of Wi-Fi deployment models without compromising on the level of security protection provided.

Retail WLAN Challenges

Deployment

With stores of different sizes in remote locations, it is no wonder retailers are cautious about deploying wireless networks at all their retail outlets. Beyond the obvious cost concerns, there are major setup issues too. Managing the RF space and maintaining performance can be particularly challenging, especially in multi-tenant settings where space for network gear is often scarce and remote configuration and management needs to be fast, simple and secure.

Cybersecurity

From securing 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, and stay up to date. Should your network become the victim, or the host, for identity theft or malicious attacks, your company's reputation is at stake, and the cost of "brand" repair can be staggering.

Mobile devices and emerging Internet of Things (IoT) devices are the latest target for malware and other security threats, and unsecured retail networks are an oasis for hackers. But retailers need to allow unknown devices onto their networks and support headless devices such as beacons, cameras and building automation sensors, which often lack adequate on-board security and must be protected by the network.

Future-Proofing

Emerging technologies such as face recognition, biometric scanning and Internet of Things applications are evolving rapidly and could even tip the balance in favor of traditional retailers. As these technologies are introduced into retail environments, the WLAN must offer the flexibility, performance and application control to handle a broad mix of traffic.

It may need to handle biometrics, video and voice services, payment transactions and advertising, while simultaneously serving patrons and harvesting consumer analytics from store visitors. It must be possible to tailor centrally managed policies for each site depending on what is deployed and push them out to remote sites in a coordinated way.

Showrooming

Not having Wi-Fi turns customers away. Having it leads to showrooming—Catch 22! How can retailers embrace showrooming and make it work in their favor? Consider the progressive car insurance company that openly compares its quote to those of leading competitors. They recognized the problem—the Internet makes it easy to price-shop insurance—and wrapped a winning strategy around it. Fortinet's wireless solution enables sophisticated Presence Analytics and empowers retailers to do the same.

Fortinet Secure Access Architecture

With a choice of two distinctly different WLAN deployment models, Fortinet's Secure Access Architecture allows retail organizations to select the best match for their operational needs, without compromising security.

As a recognized leader in cybersecurity, Fortinet provides a complete solution for secure access in thousands of remote locations over any type of WAN, with protection that far exceeds the requirements of PCI and CISP compliance.

Fortinet's Secure Access Architecture enables retailers with multiple locations to handle wireless protocol and RF-level attacks, as well as all forms of malware and cyber threats in both premise and cloud-managed WLAN deployment models.

Both Fortinet WLAN offerings can easily handle the QoS, bandwidth, security and regulatory requirements placed on retail networks carrying POS financial information alongside different traffic types from shoppers and retail associates, making sure that each gets the right security and priority treatment. Centralized policy management on-premise or in the cloud provides complete control and flexibility over the application policies and security services implemented at each retail location.

Fortinet also has a full line of PoE switches that can be managed as one with Wi-Fi and security through a "single pane of glass," either via the enterprise network or the cloud.

Complementing the two WLAN solutions, Fortinet's Wi-Fi Presence Analytics and customer engagement platform known as FortiPresence allows retailers to gather real-time consumer analytics and use it to understand and influence shopper behavior.

Fortinet Secure Access Solutions Overview

Integrated Secure Access Offering

What makes the Integrated wireless solution so unique is the unification of the network and security afforded by FortiGate. Comprising a family of thin access points, managed via an on-premise FortiGate security appliance, the solution simplifies day-to-day operations and provides unprecedented visibility and control of users, devices and applications.

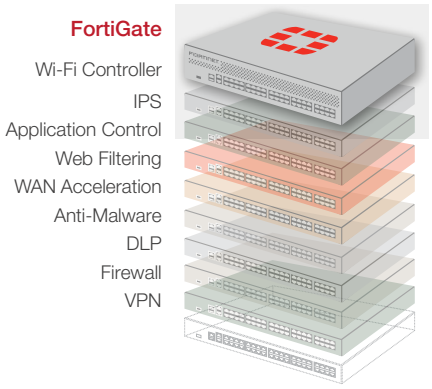

FIGURE 1: FORTIGATE CONSOLIDATED SECURITY PLATFORM

The FortiGate platform unifies security and network management by consolidating

all the functions of network firewall, IPS, anti-malware, VPN, WAN acceleration, web filtering and application control together with WLAN control in a single, high-performance appliance.

A full range of indoor and outdoor 802.11ac APs provides ample options for providing coverage from the parking lot to the storeroom. This includes plenum-rated models for concealed deployment in certain areas and ruggedized models for outdoor deployment in any conditions.

Equipped with LAN and WAN ports, the FortiGate family meets the connectivity and security needs of any size location. For smaller sites, FortiWiFi appliances integrate an entry-level FortiGate with a full-featured AP to provide a network-in-a-box solution equipped with WAN ports, VPN and a complete suite of security services.

Alternatively, depending on WAN capacity, another economical option is to place individual FortiAPs at remote sites and tunnel traffic back to corporate for centralized security processing instead of using local FortiGate or FortiWiFi appliances.

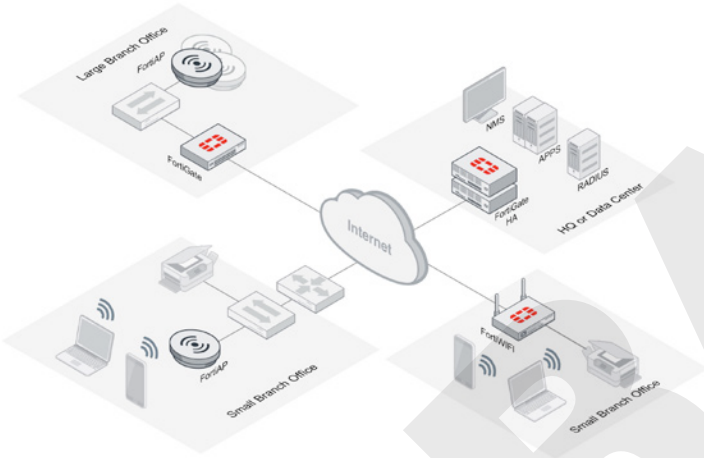

FIGURE 2: INTEGRATED SOLUTION OFFERS FLEXIBLE DEPLOYMENT OPTIONS

The integrated solution enables effortless onboarding of business and staff-owned devices as part of a complete portfolio of identity management and cybersecurity measures, which can be applied to any guest, employee or device regardless whether it is connected by wire, Wi-Fi or VPN.

Network and security management is unified through a "single pane of glass." This extends to Fortinet's high-density FortiSwitch PoE switches, which can power everything from APs to IP cameras and VoIP phones.

Key FortiGate Features for Retail

Guest Access: Guest access and seamless self-service onboarding utilizing a selection of social login, customizable captive portals, device integrity checks, virus scan and a broad choice of user authentication options.

Threat Management: Comprehensive protection against wireless protocol and RF attacks, malware, key loggers, viruses and zero-day attacks across all devices and operating systems. Complete PCI-DSS/CISP compliance with streamlined compliance reporting.

Up-to-Date Protection: Kept continually up to date through frequent automated updates from FortiGuard Labs, which researches the latest attacks to provide your network with immediate protection.

Application Control: Complete application visibility and precision control of the network with signatures for over 4,000 applications, lets retailers prioritize, throttle or block literally any applications at a group, user or device level.

Unified Management: Can administer the same (or different) policies to the wired and wireless network and manage everything through a "single pane of glass," not a collection of separate management consoles.

No Hidden Licenses: All security services are included as standard. There are no costly surprises as you activate new security features—only added protection.

Cloud Secure Access Offering: The Cloud wireless solution is far and away the industry's most secure cloud Wi-Fi solution, unlike any other. It is based on the FortiCloud provisioning and management service and FortiAP-S access points—a new class of intelligent access points which applies the same security services available in a FortiGate on the AP itself.

The FortiAP-S series is quite unique. Equipped with extra memory and twice the processing power of typical thin access points, the FortiAP-S series performs real-time security processing on board the AP. Configuration management and reporting via FortiCloud provide visibility of user, device and application usage, comprehensive threat analysis, and all the identity management tools needed for retail device onboarding and guest access through captive portals.

This unique approach avoids backhauling traffic over the WAN for security processing by delivering complete protection at the network access edge, with the simplicity and convenience of cloud WLAN management and the minimalistic equipment footprint of a single access point, other than WAN CPE. This solution is ideal for retailers with established security policies in corporate offices but limited store network security.

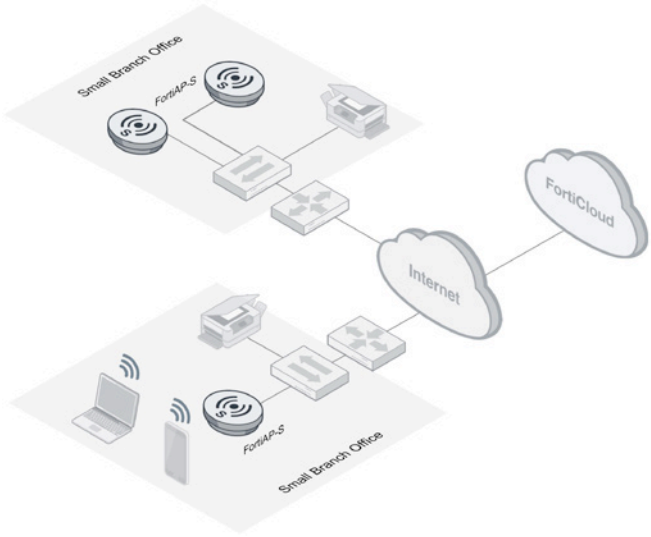

FIGURE 3: FORTINET CLOUD WIRELESS WITH COMPLETE SECURITY

Key FortiAP-S Features for Retail

Low CAPEX and OPEX: FortiCloud provisioning and management removes the cost of deploying and maintaining on-premise WLAN controllers and management appliances.

Complete Protection: Complete Wi-Fi and cyberthreat protection, from IPS to malware scanning and URL filtering, assures PCI-DSS/CISP compliance—all kept up to date through frequent automated updates from FortiGuard Labs.

WAN Efficiency: Secures access in remote offices without the cost and complexity of WAN backhaul or local security appliances. Corporate users can still be authenticated against RADIUS servers over the WAN if desired.

No Management Fees: Unlike other solutions that have exorbitant per-AP subscription fees, there are no recurring charges for full-featured cloud management through FortiCloud.

Application Control: Exceptional visibility and control allows IT to prioritize, throttle or block literally any application, at the device or user level.

Powering Retail Applications with Fortinet

Fortinet's Secure Access Solution empowers bricks-and-mortar retailers to address the needs of todays "connected" shoppers and compete with online-only stores by using their networks for much more than basic guest access.

By doing so, in-store retailers can raise customer engagement, drive loyalty and sales, and give marketing much-needed visibility into consumer behavior. Fortinet's Secure Access Solution supports the widest range of retail applications:

Video Surveillance	Monitor stores and parking areas remotely, with more flexibility and lower cost than CATV
Theft Prevention	Place Wi-Fi-enabled passive RIFD 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 and line-bust by taking orders and payments at the customer's side
Communications	Keep staff connected and fully mobile using VoIP on mobile devices and badges
Presence Analytics	Use visitor data to measure customer loyalty, and merchandising, and optimize staffing
Social Wi-Fi Opt-In	Fuel your marketing by providing in-store Wi-Fi access in return for customer opt-in
Real-Time Offers	Combine presence and big data to market to customer devices and on digital signage
Digital Ads	Use Wi-Fi-enabled digital displays, from flat panels to smart shopping carts for tatgeted advertising
Operations	Enable Wi-Fi barcode scanners for stock taking and inventory management

Secure Access Summary

For a growing number of in-store retailers, the online/omni-channel debate is over. Forward-thinking retailers are embracing the omni-channel retail model and recognize that secure in-store Wi-Fi belongs at the heart of the solution.

To succeed with omni-channel strategies, retailers must leap beyond "free Wi-Fi" for guests and streamlining operational activities by using their networks to transform the in-store experience, while harvesting customer data and consumer analytics to fuel informed omni-channel marketing strategies.

The wireless network must become a springboard to exploit new technologies such as beacons, face recognition, mobile payments and a host of IoT applications, without adding to the security risks. All this requires a comprehensive security framework that offers total protection from cyberthreats of all types, from Wi-Fi intrusion to malware and viruses, all at a price point that makes sense for large numbers of locations.

Fortinet's Secure Access Solutions provide that framework, giving retailers the flexibility to choose between premise-managed, cloud-managed and hybrid deployment models to best fit their network topology and organizational needs, without compromising world-class security or their budget.

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
Valbonne
06560, Alpes-Maritimes,
France
Tel: +33.4.8987.0500

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

April 26, 2016