FORTINET

WHITE PAPER

# Evolving Retailer Networks Require a New Security Architecture Perspective

## Challenges in Protecting Applications and Data for the Modern Retailer

**Executive Summary**

**Leveraging emerging digital technologies to provide "omnichannel" customer experiences is a smart means of competitive differentiation for retailers. It also opens the door to new security risks, because retailers' attack surface is expanding and the complexity of managing network security continues to increase. This makes it increasingly difficult to protect endpoints, cloud-based applications, web offerings, and other resources that a retailer needs to make available 24x7 to both customers and employees. A retail organization's approach to cybersecurity affects both the performance and availability of its network—placing security decisions front and center for organizations basing their corporate strategy on providing an optimized, omnichannel experience for customers.**

Despite the news headlines proclaiming the demise of brick-and-mortar stores, **54%** of retailers surveyed plan to open new stores in 2019.

## Omnichannel Requires a Seamless Experience

The retail sector is flourishing, both in the United States and elsewhere. In 2018, retail revenue increased 83% for the world's 250 largest retailers (208 companies).[1] Although brick-and-mortar retail failures frequently grab headlines, only 7% of retailers expect the number of physical stores to decrease. Further, 54% plan to open new stores in 2019, and 36% will have more retail locations than they had last year.[2] With all the buzz about online shopping, it may come as a surprise that ecommerce sales accounted for only 14.3% of retail sales in 2018.[3]

At the same time, the retail sector is experiencing a radical and fundamental transformation. Staying competitive requires mastery of technologies that were unthinkable a few years ago. Customers expect retailers to provide both brick-and-mortar showrooms and online shopping experiences that are accessible either from the desktop or on a mobile device. They also expect all of a retailer's environments to provide a seamless engagement experience. Offering omnichannel customer access is crucial to success for most businesses in the sector; however, retailers seem to be falling short. According to 87% of customers, brands need to put more effort into providing a seamless experience.[4] Even traditionally online-only retailers, such as Amazon and Casper, have been opening brick-and-mortar stores to meet customer demands for omnichannel environments.

While shopping in a brick-and-mortar environment, customers still expect a digital experience, so stores must provide a variety of methods through which customers can research and purchase their products. In addition to physical product samples, many stores provide kiosks that enable customers to access product information and place orders, either for delivery or in-store pickup.[5] Even more important, retailers need to support customers' personal smartphones or tablets and provide internet access within their stores.[6]

In addition to the customer experience, retailers are using their networks to provide remote training opportunities to employees, to drive messaging on digital signage, and to support applications such as Voice over IP (VoIP) and video. Like customer-facing storefronts, these applications all benefit not only from assurances that data is safer but also from the performance and availability that better security may afford in the event of a cyberattack.

### Multi-cloud Increases Complexity

At the same time retailers are undergoing digital transformation, they are increasingly turning to cloud-based applications to run crucial business functions. Indeed, the typical company uses 62 different applications in the cloud.[7] In some cases these include not only Software-as-a-Service (SaaS) solutions but also Infrastructure-as-a-Service (IaaS) and/or Platform-as-a-Service (PaaS).

Cloud technologies make a lot of sense in distributed retail establishments, but they further increase network complexity and security concerns. A business running numerous cloud-based applications is likely running a whole host of public and private clouds in a complex, hybrid environment. Because the software is running on hardware outside the four walls of the data center, it resides outside the perimeter security established and maintained by the corporate IT team. Many retail IT leaders rely on software vendors to secure some of these applications. But this isn't enough. The reality is that without centralized visibility and control of multi-cloud environments, customer and other vital data remains at risk.

Enterprises use, on average, 62 different cloud-based applications.

Regulations require retailers to tightly control access to specific types of data that they may capture on their customers and other stakeholders.

### Data-Center Security Challenges

As more applications migrate to the cloud, core network speeds within retailers' corporate data centers are topping 100 gigabits per second. This raises the bar for security throughput, since every essential data-center security task—including SSL inspection, intrusion prevention (IPS), web application security, and email security—introduces latency. Without sufficient security processing power, the cumulative lag can be so great that IT leaders find themselves turning off security provisions in their firewalls and gateways to regain acceptable network throughput. That decision can come back to haunt them, for example, when uninspected SSL traffic is exploited to inject malware or when previously unknown threats escape IPS detection.

### Regulators and Their Own Demands

A host of regulations govern retailers' collection and management of data—from government requirements such as the European Union's (EU's) General Data Protection Regulation (GDPR) to industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS). These regulations encourage retailers to tightly control access to specific types of data that they may capture on their customers and other stakeholders. They also require quick response in the event of a data breach.

To ensure compliance, retail IT leaders are embracing security frameworks such as those from the National Institute of Standards and Technology (NIST). The standards, guidelines, and best practices contained in the NIST Cybersecurity Framework help retail IT leaders document and manage their network security risk, but they also place heavy burdens on the IT organization.

For example, NIST's Criticality Analysis Process Model requires a full inventory of assets, applications, and services in order to prioritize them and assess the impact of their inadequate operation or loss on the organization's goals.[8] A security information and event management (SIEM) system can automatically collect this information, making this potentially onerous task more manageable. But to provide accurate information for analysis, the SIEM must be fully integrated into a network of security devices throughout the retail enterprise.

## Retail Organizations at Significant Risk

The digital transformation in retail still comes with old threats as well as new ones. New variants of malware targeting point-of-sale (POS) systems are on the decline, thanks to Europay, Mastercard, Visa (EMV) chips on credit and debit cards, as well as PCI DSS compliance efforts. However, distributed denial-of-service (DDoS) attacks on devices such as IoT are increasing in frequency, as are ransomware attacks. These trends are true across industries. Yet, in the case of retailers, downtime from a ransomware attack could be particularly problematic for a company with a corporate strategy built, in part, on providing customers access to an online store 24x7.

At the same time, more traditional types of data breaches continue to plague retail organizations that collect valuable financial and sensitive information about customers, employees, and other stakeholders. It's a pressing concern. In 2017, 50% of U.S. retailers experienced a data breach compared to the global average of 27%. Even more troubling is that 75% of U.S. retailers have experienced at least one breach in the past.[9]

In addition to their prevalence, data breaches in the retail sector can be costly. In 2018, the average cost of a data breach in the U.S. was $233 per record stolen.[10] For those subject to GDPR, the prospective costs are even higher. Since the GDPR went into effect, losing the personal data of an EU resident could result in a fine of up to 4% of a company's annual revenue.[11] Regulations in other areas of the world might impose smaller penalties, but even if a data breach doesn't affect any EU residents, resulting fines could still take a big bite out of tight retail margins.

Worse, the reputational damage of a data breach may be even more substantial. Almost one in five consumers (19%) say they will not shop at a retailer that has suffered a cyberattack, and 33% would stop shopping there for an extended period of time.[12]

### Resource Considerations

Coping with these risks will stretch any IT security team to its limits. In the retail sector, however, keeping up with ever-evolving advanced threats is particularly challenging. To start, retail businesses are known for having razor-thin margins. Staffing is tight as well, so security teams are under pressure to work as efficiently as possible. Intensifying the challenges of the sector's notoriously tight budgets, the distributed nature of the typical retail business means a small staff has even more locations and devices to secure.

**In 2017, 50% of U.S. retailers, and 27% of retail businesses around the world, experienced a data breach.**

**49% of U.S. retailers say they are very vulnerable or extremely vulnerable to cyberattack.**

## Retail Security Is Not Keeping Pace

Despite potentially serious consequences of any data breach, many retailers are stuck in a past generation of security. They may use a firewall for edge-of-the-network protection, but if it's from a previous generation, it may not successfully detect and mitigate the latest threats. Moreover, perimeter protection is no longer sufficient for any network. As new technologies they deploy introduce new attack surfaces to their network, retailers need to pursue new avenues of security. But many are failing to do so effectively.

Many retailers now store sensitive data in environments that support digital transformation. For example, U.S. and global retailers rely more heavily on public clouds and big data environments. And although security spending is increasing, it may not be allocated to the most effective areas. For instance, less than a third of retailers are implementing encryption in the cloud.[13] Perhaps that's why 35% of global retail organizations and 49% of U.S. retailers report feeling "very vulnerable" or "extremely vulnerable" to cyberattack.[14]

### Network Complexity Thwarts Security

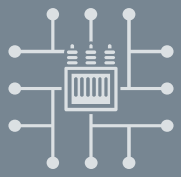
So, what's holding retailers back and causing them to feel they are at serious security risk? One of the most prevalent barriers to securing sensitive data, according to 48% of U.S. retailers and 36% of retailers worldwide, is complexity in the corporate network.[15] That complexity stems from the increasing diversity of retail activities, which often involve several in-person and online POS systems, internet-connected kiosks for customer use, and in-store support for customers' mobile devices. Operational improvements, such as adding IoT devices to the network to automate lighting or HVAC, also add to network complexity. With each of these improvements come new security vulnerabilities.

This situation is exacerbated by a security infrastructure that is becoming increasingly fragmented as security point products are deployed to address these technological changes. Unable to achieve transparent visibility and centralized controls but rather relegated to correlating data and managing security across multiple consoles, retailers find themselves in a constant state of reactive security, unable to respond quickly and effectively to malicious attacks and breaches.

These challenges are intensified when retailers move data storage from on-premises data centers to the cloud. Like companies across a wide range of industries, retailers are improving the efficiency of their IT operations and expanding the applications they provide to end-users by utilizing SaaS applications and other solutions running in public cloud, private cloud, or hybrid cloud environments. In leveraging the cloud, however, retailers allow their networks to break out of the four walls of the corporate environment. This significantly expands the retailer's attack surface, ramping up the challenges in protecting data and applications.

Another challenge emerges when a retailer deploys software-defined wide-area network (SD-WAN) technologies to accelerate data flow between corporate locations and retail stores, as well as between retail locations and internet resources. While greatly improving network performance, SD-WAN solutions eliminate the need to backhaul traffic through the data center, which also means traffic is not protected by the security protocols of the corporate data center. A retailer thinking differently about network connections must also take a new approach to security, or it will create a gaping area of vulnerability for its applications and data.

Because retailers usually have tight margins and limited resources for overhead, their IT—and more so security—teams tend to be small. Security complexity can cause serious headaches, but failing to adopt a new security perspective that supports the business needs of the organization's new solutions—cloud, big data, etc.—places a retailer in peril.



**Among the most prevalent barriers to securing sensitive data, according to 48% of U.S. retailers, is complexity in the corporate network.**

**Security is crucial, but it must not come at the cost of reduced network performance.**

### Performance Demands at Odds With Security Bottlenecks

For some retailers, performance concerns also present a barrier to effective security. Organizations that move from on-premises data centers to cloud-based applications are likely already experiencing performance bottlenecks, as data may have to travel farther and across slower connections.

Giving customers access to the network and connecting new devices, such as IoT, can place an additional drag on the speed of network traffic. Presence analytics, a technology that enables retailers to track customers' physical movement into and through stores, involves the processing of vast quantities of data; thus, it further slows down retailers' networks.

Organizations working to develop a competitive advantage through an omnichannel customer experience cannot afford sluggishness in any of the components of the customer experience. Yet, some retailers, which are already struggling to maintain optimal network performance, find their security infrastructure generates an additional performance burden, especially if they deploy an assortment of point security products for the different facets of the network's ever-expanding attack surface.

## Sophisticated Security Needs to Be a Priority in Retail

For retail organizations using out-of-date or poorly planned security solutions, data breaches and site downtime are a very real possibility. The average retailer experiences 35 cyberattacks per year, and it takes more than six months (197 days) to detect intrusions.[16] The majority of these are advanced threats, designed to bypass conventional security measures.

When undetected, malware can move laterally and do more damage. It can continue poking its way through the corporate network until it finds customer data, credit card information, or other valuable data that the cyberattacker can leverage. Detection and mitigation of attacks need to be top priorities for retailers.

As the competitive landscape shifts toward increased reliance on technology, companies in the retail sector need to reconsider their approach to network, application, and data security. Omnichannel customers account for 27% of all sales, although they make up only 7% of all customers.[17] In addition, retailers with omnichannel strategies achieve 91% greater year-over-year customer retention rates compared to businesses that do not.[18] Companies courting these valuable customers need to shore up their security systems to ensure they're protecting critical data and providing the best possible customer experience.

**The average retailer experiences 35 serious cyberattacks per year, and it takes more than six months to detect intrusions.**

## Conclusion

Whether you are ready for it or not, digital transformation is a reality. Businesses in all sorts of industries are under pressure to adopt leading-edge technologies, but those in the consumer-facing retail sector feel particularly under the gun.

To set themselves up for success, retailers need to embrace digital transformation and give customers an omnichannel shopping experience. However, doing so also opens new doors to cyber criminals poised to take advantage of network complexity and the introduction of new devices, such as POS kiosks, cloud-based applications, or IoT devices. Retailers looking to technology for a competitive advantage—or even just to keep up with their peers—must embrace a security architecture that reflects this new reality.

## References


[1] "Global Powers of Retailing 2019," Deloitte, accessed May 24, 2019.

[2] Bethany Aronhalt, "Setting the record straight on the state of retail and store closures," National Retail Federation, April 15, 2019.

[3] Fareeha Ali, "A decade in review: Ecommerce sales vs. retail sales 2007-2018," Digital Commerce 360, February 20, 2019.

[4] "25 Amazing Omnichannel Statistics every Marketer Should Know," V12, January 9, 2019.

[5] Emma Sopadjieva, et al., "A Study of 46,000 Shoppers Shows That Omnichannel Retailing Works," Harvard Business Review, January 3, 2017.

[6] Nick Hodson, et al., "2017 Retail Trends," PwC, accessed June 13, 2018.

[7] "Fortinet Threat Landscape Report Q3 2017," Fortinet, November 17, 2017.

[8] Celia Paulsen, et al., "Criticality Analysis Process Model," NIST, April 9, 2018.

[9] Garret Bekker, "2018 Thales Data Threat Report—Retail Edition," 451 Research, 2018.

[10] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[11] Drew Del Matto, "Executive Insights: Viewing GDPR as an Opportunity to Drive Competitive Advantage and Create Digital Trust," Fortinet, January 8, 2018.

[12] Tony DeGonia, "2018 Sees Record Number of Online Retail Data Breaches," AlienVault, January 8, 2019.

[13] Garret Bekker, "2018 Thales Data Threat Report—Retail Edition," 451 Research, 2018.

[14] Ibid.

[15] Ibid.

[16] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[17] "Q1 2018 Global Commerce Review," Criteo, May 18, 2018.

[18] "25 Amazing Omnichannel Statistics every Marketer Should Know," V12, January 9, 2019.


FORTINET

www.fortinet.com



June 12, 2019 12:48 AM

D:\Fortinet\White Paper\New Security Architecture\FA - Retail_New Security Architecture_060819

414218-0-0-EN