ARMOR

July 2018

WHITEPAPER

RETAIL'S KEY TO DEFEATING IOT CYBERATTACKS

INTRODUCTION

In the wake of the closing of massive retail stores and competition from online giants, retailers are scrambling to drive customers to their websites and physical stores to propel them along the buying process. To do that successfully, stores are implementing more ways to interact with customers, including adding web-facing applications and installing new technologies online and inside physical stores. These new advancements are already influencing customer behavior and increasing sales, but they come with risk to both on-premises and cloud environments.

Retailers have long been familiar with risks that online devices create. Point-of-sale (POS) systems have now been around for decades, but they're still difficult to secure because they connect to the internet, and hence have been vectors for many highly publicized breaches. As retailers embrace new technologies to create a more seamless shopping experience, they must take care that the speed at which they adopt new technologies does not outpace their ability to protect customer data. Artificial intelligence, IoT and digital transformation are all being used to better engage with customers and to attract more business. But to keep customers happy, a retailer must protect their data.

2 -IN- 5 RETAILERS

ACROSS THE GLOBE

EXPERIENCED A DATA BREACH IN THE PAST YEAR[1].

New cybersecurity solutions are needed to protect environments from the latest attacks that arise from IoT. Device makers are slow at integrating security to their products, which makes it necessary for retailers to see all incoming and outgoing traffic on any devices. Retailers can finally do that without buying or managing equipment like firewalls, intrusion detection/prevention systems (IDS/IPS) and other security tools. Small and medium-sized retailers without large IT security budgets can now have visibility of on-premises, cloud and hybrid environments, and threats that get past prevention solutions can be detected and remediated immediately and automatically.

95% OF BREACHED RECORDS[2]
came from three industries in 2016:

GOVERNMENT | RETAIL | TECHNOLOGY

IT Professionals in the retail space identified the following challenges[3]:

55% Cost and effort of managing remote systems

48% Keeping systems up to date and secure

35% Lack of in-store IT skills

30% Demand for advanced in-store applications

30% Lack of consistency across sites

DIFFICULTIES SECURING THE NETWORK

The future of IoT looks both bright and bleak for retailers. It can open new avenues of business and tear it down in the blink of an eye with just one breach. It's tough enough for retailers to secure their networks even without new technologies. According to the 2017 Thales Data Threat Report, 80 percent of global retail respondents and 55 percent of U.S. retailers indicated that their organizations deploy new technologies, such as cloud, big data, IoT, and containers, in advance of having the security in place to protect them.

88%

OF RETAILERS

consider themselves to be "vulnerable" to data threats.

with 37% stating they are "very" or "extremely" vulnerable[1].

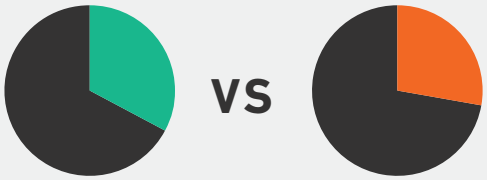
Unless retailers take action, that number is likely to climb with digital transformation. The retail industry presently has one of the highest serious web-facing application vulnerability ratios at 33 percent, compared to 28 percent for finance and healthcare[4]. Retailers respond to cyberattacks on average twice a week and lead the way in data breaches, according to software provider Zynstra. A study it performed in 2017 found that more than half (53%) of retailers will focus on using technology to improve the shopping experience in 2018[3]. The transformation taking place among retailers can be a boon to business, but new securities will be needed to secure their data.

HISTORICAL RETAIL SECURITY

In the past, retailers only had to be concerned with the devices on premises, POS systems, and employees who fell for social engineering attacks. To combat these vulnerabilities, over the past decade endpoint and email server protections have been implemented. To keep up with continual changes in IT, the Payment Card Industry Data Security Standard (PCI DSS) has often changed the requirements to meet PCI compliance and secure data. However, time and again retailers that have been PCI compliant have been breached.

The industry has been trying to find different ways to secure data. In 2017, the National Retail Federation (NRF) conducted a survey and found that 60 percent of small brick-and-mortar retailers had installed chip card readers, and another 10 percent were planning to have them installed by July that same year, bringing the total to 70 percent. But NRF also informed retailers that chip cards do nothing to keep card data from being stolen from computer systems. The chip transmits an encrypted code that confirms that the card is not counterfeit, but the actual account number and other card data are still transmitted in the clear. Credit card data that does not require a PIN allows thieves to make fraudulent credit card charges. Unfortunately, the U.S. still uses chip-and-signature credit cards rather than chip-and-PIN cards, which could stop most credit card fraud.

VULNERABILITY RATIOS



33%
RETAIL

28%
FINANCE & HEALTHCARE

The retail industry has one of the highest serious web-facing application vulnerability ratios[4].

NEW IoT RETAIL TECHNOLOGIES

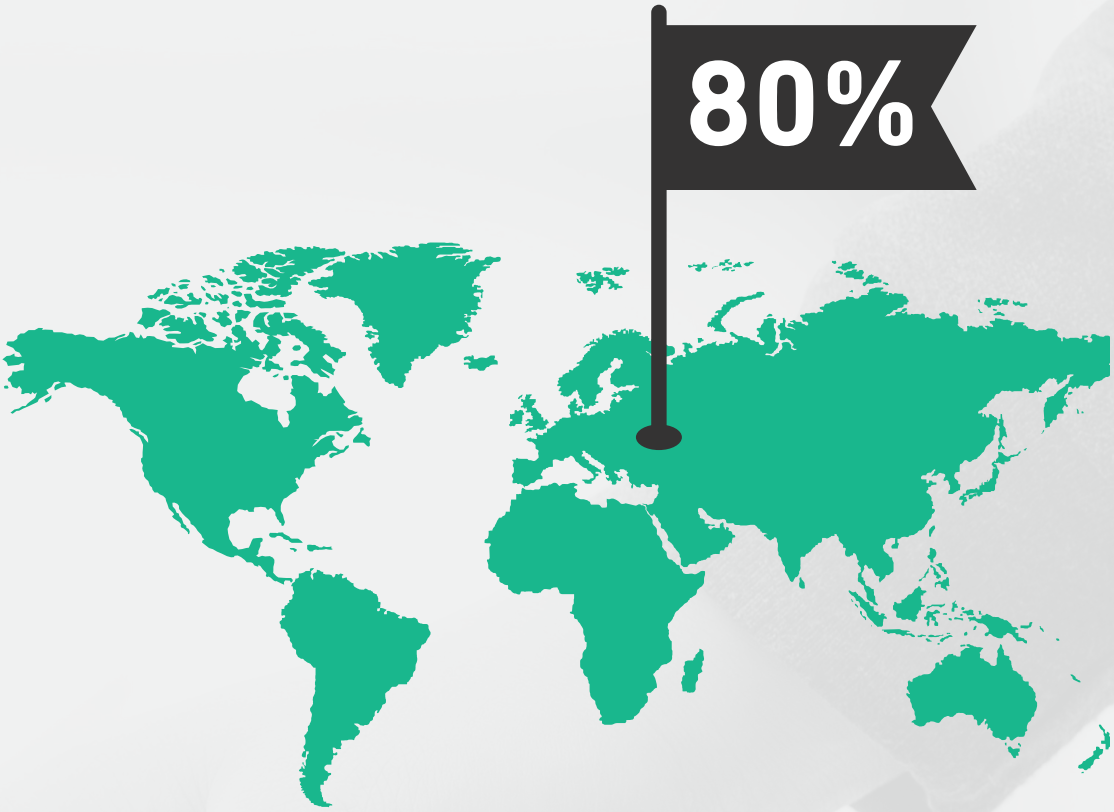
Integrating technology is the only way to continue to enhance the customer experience and stay competitive. Social media, customer-interacting apps, automated robots that converse with buyers, interactive "magic mirrors," "buy online, pick up in store" (BOPUS), real-time inventory across a network of stores, and numerous other new technologies that increase customer satisfaction are just a few examples of digital transformation in retail.

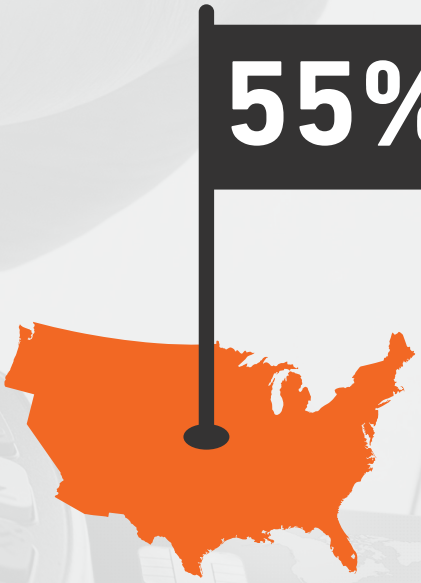
Artificial Intelligence (AI) is helping retailers create interactive design stations that encourage customers to customize clothes, to identify internet leads, and to assist customers in determining what products would be best for them. As technology continues to transform the retail industry, it is critical for businesses to keep cybersecurity top-of-mind and assess the potential impact on risk and security.

53% 

of retailers will focus on using technology to improve the shopping experience in 2018.

The focus on technology in the New Year is especially relevant given that currently only 27% of retailers feel their infrastructure is fully able to support these plans to improve customer experience in store.[4]





80% of global retail organizations and 55% of U.S. retail organizations deploy new technologies such as cloud, big data, IoT and containers in advance of having the security in place to protect them[1].

SOLUTIONS

Securing retail environments requires gaining visibility into all the connected things on a network and in the cloud. A threat can only be remediated if it is identified. If an attacker breaks into a security camera or a web-facing app, a company must be able to spot the traffic and be able to quarantine the threat before malicious activity begins. That's now possible to do even if a company does not have its own security team.

By leveraging the power of the cloud, Security-as-a-Service (SECaaS) providers automatically scale up as a retailer's environment grows with the newest devices and applications. A team of trusted experts that specialize in protecting cloud, on-premises, and hybrid IT environments watch over environments 24/7/365, detect threats as soon as they appear, and automatically remediate them. These outsourced security providers can help organizations meet compliance requirements, alleviate the need to hire and maintain security researchers and analysts, as well as the need to purchase and manage expensive equipment like IDS/IPS, firewalls and SIEM tools.

42% OF RETAILERS

will prioritize enhancing security and compliance of in-store IT in 2018[9].

1

SECAAS PROVIDES A VARIETY OF SECURITY SERVICES, INCLUDING THOSE LISTED BELOW:

- Intrusion detection
- Malware protection with constant updates
- Log and event monitoring
- Active threat hunting
- Vulnerability scanning and patch monitoring

2

WHEN CHOOSING AN SECAAS, LOOK FOR ONE THAT PROVIDES THE FOLLOWING BENEFITS:

- Intelligence-driven, proactive security that provides threat alerts and remediation
- Unified visibility and control for any environment
- Simplified, continuous audit-ready compliance
- Reduced dwell time for attackers
- Pay-per-use consumption
- Supported environments (On-prem, Cloud, and Hybrid)

SOURCES CITED

1. "Thales Data Threat Report," 2017.

2. "Forrester Research, Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses," 2016, published January 2017.

3. "Zynstra, Retail Store IT: Insight Report," 2017.

4. "WhiteHat Security, Application Security Statistics Report, The Case for DevSecOps, Volume 12," 2017.

5. "National Retail Federation, Small Retailers Switching to Chip Cards But Still Worried By Lack of PIN," Aug. 10, 2017.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167