WHITE PAPER

Securing the Store of the Future

Enabling Retailers To Securely Deliver Exceptional Customer Experiences

Executive Summary

Retailers large and small face a variety of challenges—everything from vulnerable internet-connected point-of-sale (POS) systems and devices to online ordering, delivery programs, maturing real-time inventory processes, and a rapidly expanding Internet-of-Things (IoT) landscape. These risks, changes in consumer behavior, and other market realities pressure companies to accelerate their digital transformation initiatives. With the proliferation of point security products and the increasingly sophisticated threat landscape, grocery stores, restaurants, and department or big box stores face significant hurdles due to complexity and time-to-market considerations. These problems are exacerbated by cybersecurity staffing shortages that often lead to significant security gaps. Cyber criminals are all too aware of these challenges, so retail operations are attractive targets.

A security platform for retailers needs a foundation that facilitates enhanced visibility, real-time security policy enforcement, and threat-intelligence sharing. Fortinet offers the comprehensive and integrated Fortinet Security Fabric with FortiOS at the core. This broad platform approach provides tight integration and unlocks the automation that helps network and security teams reduce risk and work more quickly and efficiently.

The Transformation Spectrum

Although the move to digital transformation has created challenges for retailers, technology is a true enabler. Thanks to advances in technology, retailers can marry in-store and online interactions and adapt to new markets and operational models quickly. Whether they're scaling out in-store infrastructure or expanding to a multi-cloud strategy, retailers who want a competitive edge will continue to embark on digital transformation initiatives. The transformation journey is a spectrum with retailers today falling between the Store of Yesterday at one end, the Store of Today in the middle, and the Store of Tomorrow at the other end (see Figure 1).

Retail Technology Challenges

Risk and compliance: Adherence to Payment Card Industry (PCI) requirements and growing data privacy regulations

Threat landscape: Increased risk from the shift from storing data only on POS devices to storing it in cloud and other environments

End-to-end visibility: Expanded networks that now include multiple clouds, mobile devices, POS systems, and work-from-home

Network performance: Support for bandwidth-intensive applications and digital growth

Operational efficiency: Automation and orchestration to manage increased complexity

Cost sensitivity: Predictable capital and operational spending and future-proofing infrastructure

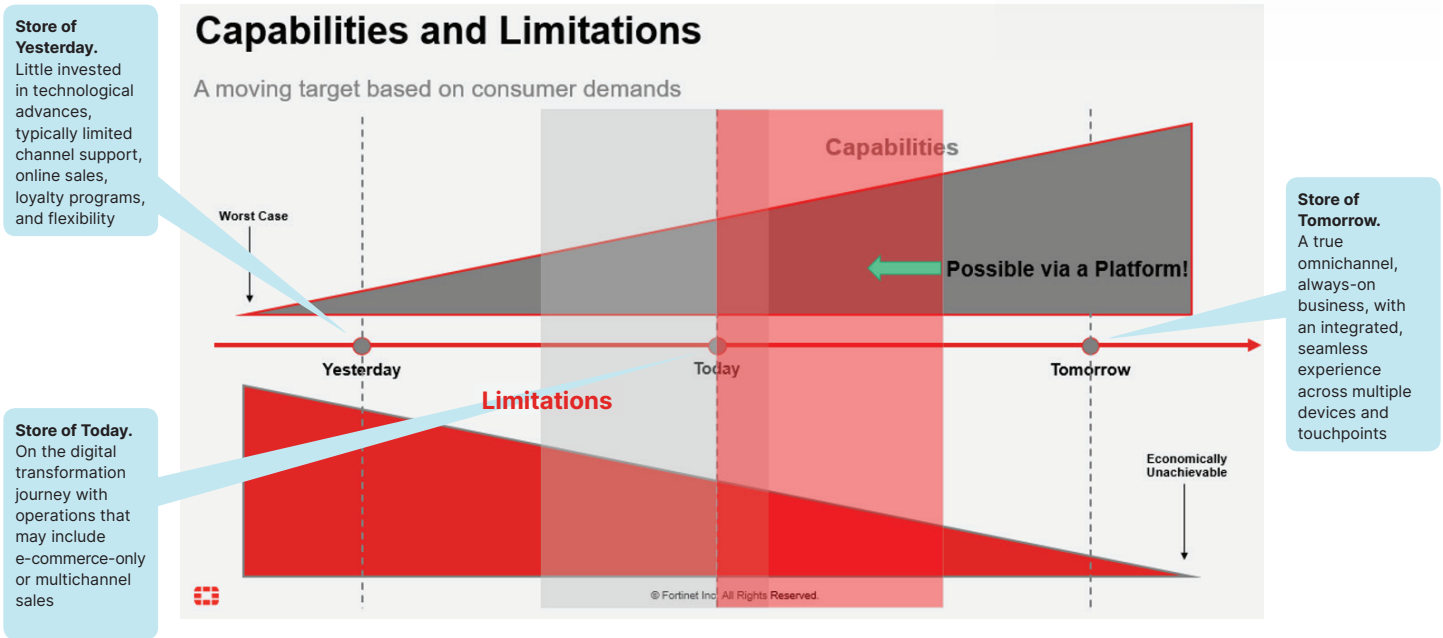

Figure 1: The transformation scale shows retail digital capabilities and limitations.

Increased Cybersecurity Risk

The digital transformation initiatives in the retail industry have the potential to increase risk. Applications are generally the main attack vector because threat actors know that the perimeter has changed and there are more discrete places to exploit. Cyber crime has increased and is causing greater financial impact and business disruption. Even though new attack vectors such as cloud-based Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) e-commerce and inventory systems increase, retailers continue to be at risk from POS attacks that target both immediate gain and access into retail networks.

From a cybersecurity perspective, the network perimeter is now harder to define. Because network edges are everywhere, many organizations have had to deploy an array of point security solutions. Unfortunately, this approach does little to meaningfully integrate and automate systems. The resulting vendor sprawl has now grown too difficult and too expensive for many retailers to manage successfully.

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

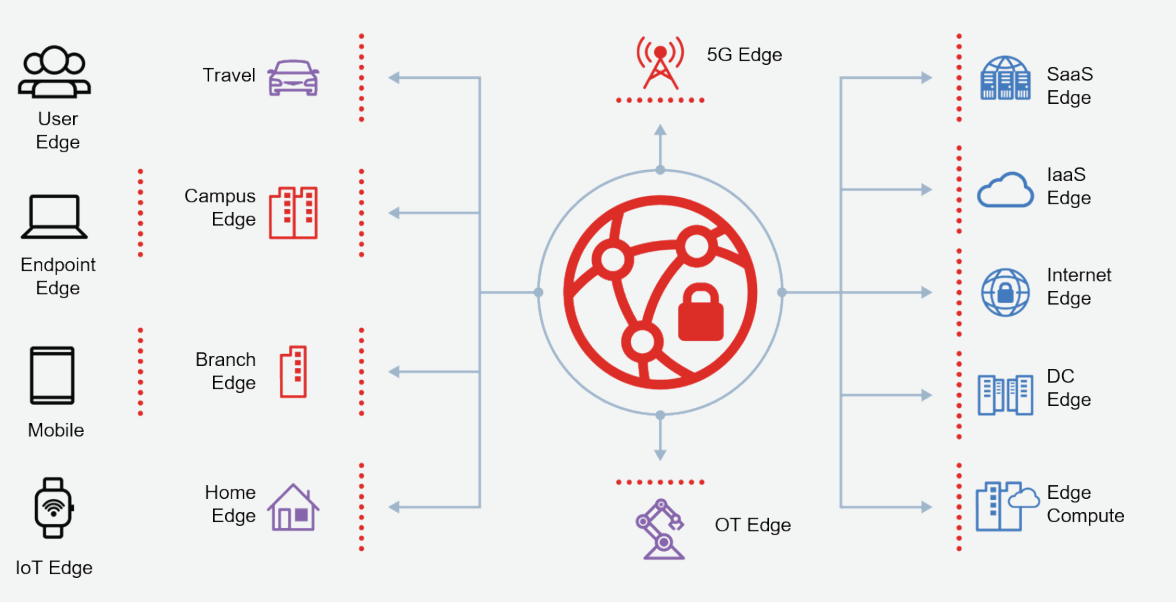

Figure 2: The explosion of edges has increased risk.

The Benefits of a Platform Approach

Instead of simply protecting network perimeters, retailers must shift to protecting data spread across the many edges, users, systems, devices, and critical applications across the network. Streamlining operations with a single security platform offers many benefits.

- **Protect any edge and any app at scale.** Advanced threat protection, convergence of network and security, secure sockets layer (SSL) decryption, and network automation
- **Complete and simplified access layer security.** Direct and integrated control, configuration, and management, which extends next-generation firewall (NGFW) to the local-area network (LAN) edge
- **Secure, business outcome-driven wide-area networking (WAN).** Reduced cost and complexity, better application performance, and integrated security
- **Control every device on every network.** Simplify network deployment, automatically discover devices, and apply policy at scale

A Cybersecurity Platform That Spans Endpoints, the Network, and the Cloud

Speed is the key to stopping or mitigating the damage from an attack. Breaking the attack sequence and protecting the organization requires security teams to detect and rapidly adjust security quickly. To effectively protect against newly discovered tactics across an ever-expanding attack surface, time is of the essence.

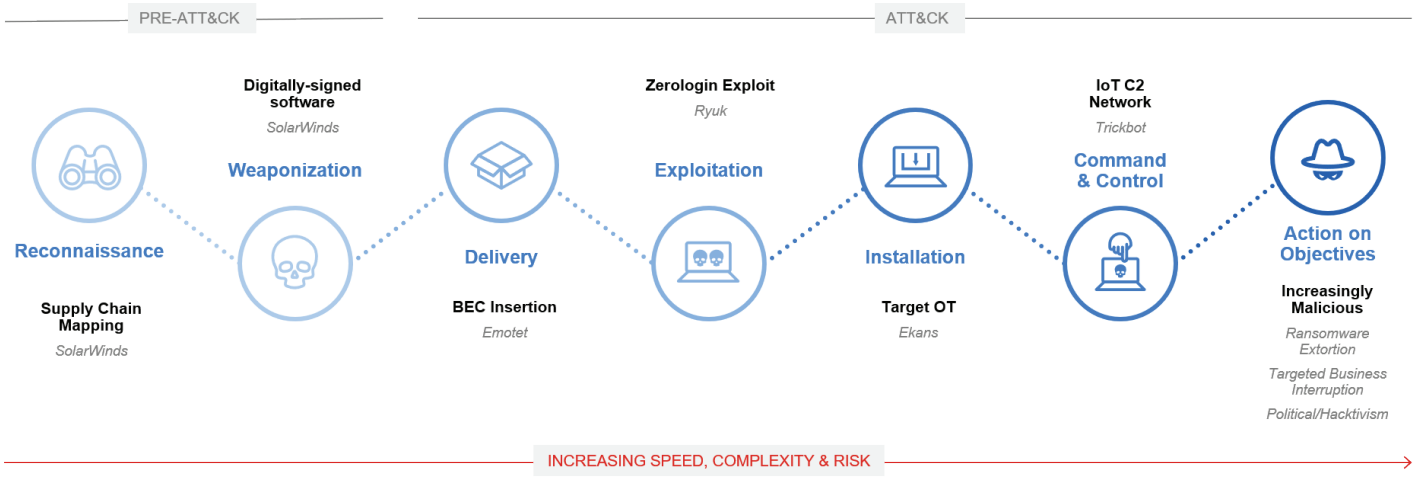

Figure 3: Dwell time can be the most damaging aspect of an attack.

For effective retail security, you need to start with a security platform that rests on three pillars: security-driven networking, zero-trust access, and adaptive cloud security. Building, securing, and managing these environments doesn't have to be challenging, time-consuming, and expensive. You should look for a security platform that offers broad security support with visibility and protection of the entire digital attack surface. This platform should include firewall, access points, and connectivity technologies that are designed to work together as a complete security system. It should support fast and efficient operations with integration and automation that reduces management complexity while leveraging threat intelligence that is shared throughout the network.

The Fortinet Security Fabric is a comprehensive, integrated broad security platform that meets retailer needs. The Fortinet Security Fabric can help if you have 1–10 sites with standard requirements or if you have more than 10,000 sites with complex parameters. The Fortinet Security Fabric has FortiOS at the center (see Figure 4).

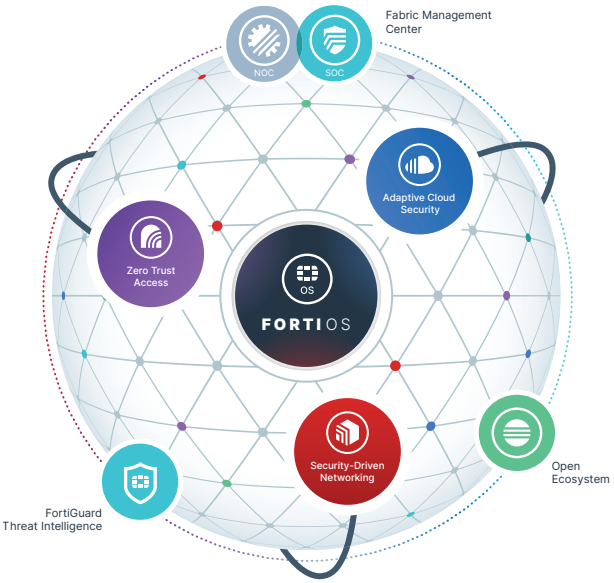

Figure 4: The Fortinet Security Fabric.

Several key elements included in the Fortinet Security Fabric allow for consolidation of technology, simplified management, and the acceleration of converged network and security.

- **FortiGate** is an industry-leading NGFW that natively provides secure software-defined wide-area networking (SD-WAN).
- **FortiExtender** provides secure cellular transport enabling retailers to protect the always-on experience.
- **FortiSwitch** provides robust security and connectivity for the LAN edge using Zero Trust Network Access (ZTNA) and network access control (NAC).
- **FortiAP** offers high-performance wireless access and analytics.

In 2021, there were more than 79,000 incidents investigated and 5,258 confirmed data breaches with 725 incidents taking place in retail alone. System intrusion, social engineering, and basic web application attacks represented 77% of breaches.[2]

Retailers require flexible, scalable security across all network edges. The network is at the core of the Fortinet Security Fabric. Security-driven networking provides secure high-performance connectivity between users, applications, and devices into the cloud. It helps retailers manage internal and external risk by using internal segmentation, automated threat protection, and policy enforcement. It also can be extended with dynamic cloud security that provides protection across all cloud environments including hybrid, public, and private cloud services.

Finally, adopting a zero trust network access architecture enables the identification and control of users, applications, and devices both on and off the network, and security operations driven by artificial intelligence (AI) help ensure that your cyber defenses can keep up with the accelerating threat landscape.

Use Cases

Organizations of every size in the retail and hospitality markets constantly face a variety of security challenges, from vulnerable internet-connected POS systems and devices to online ordering and delivery programs. Fortinet offers a comprehensive and integrated platform that addresses these issues. Retailers can securely deliver exceptional customer experiences and transform their operational model to meet their consumers no matter where they are. At the same time, they can maintain exceptional security, gain visibility, and obtain customer insights that have never been possible before.

The Fortinet approach to delivering a secure SD-Branch network architecture provides efficient protection for all of your business's critical business processes. Secure SD-WAN provides consistent security policy enforcement and easy management while increasing network performance. The Fortinet Secure SD-Branch solution covers everything from the WAN edge, to the store access layer, to endpoint devices. Even across wired and wireless networks, your system can be secured consistently and completely, from supply chain to consumer online ordering to physical store management, all with a single platform.

Conclusion

Many retailers struggle to cover all the security gaps and manage countless point security products and advanced threats. From vulnerable internet-connected POS systems and devices to online ordering, third-party delivery systems, and an expanding IoT landscape, retailers are accelerating digital transformation initiatives to meet today's market realities. But with Fortinet's holistic security fabric platform, retailers can deliver exceptional customer experiences consistently and securely.

[1] "Retail Cybersecurity Statistics," Fortinet.

[2] "2021 Data Breach Investigations Report," Verizon, May 2021.

www.fortinet.com

August 19, 2021 7:16 PM

1168964-0-0-EN