Securing Today’s Convenience Stores with Fortinet
Executive Summary

Today’s convenience stores (C-Stores) rely on a variety of digital tools to support an evolving retail engagement model that includes everything within the store interior and the forecourt. This can involve point-of-sale (POS) infrastructure, self-service kiosks, intelligent building systems, digital signage, fuel dispensers, guest Wi-Fi, security cameras, loyalty system integration, and store-in-store services. Plus, today's stores contain a wide array of Internet-of-Things (IoT) devices, such as walk-in cooler sensors and occupancy sensors. Protecting these critical systems against cyberthreats is paramount for compliance and maintaining brand value.

The Fortinet Security Fabric offers C-Store operators a broad set of network and security technologies that seamlessly integrate for transparent visibility and real-time threat-intelligence sharing. This level of integration unlocks automation that enables lean network and security teams to work faster and more efficiently while also allowing them to reduce risk.

Digital Complexity Brings Greater Risks to C-Stores

Convenience stores are attractive targets for cybercriminals due to the sensitive information they handle within the forecourt and inside the store. Retail POS applications handle vast amounts of customer data, including credit card information and personally identifiable information (PII), that can be leveraged to extort money or cause reputational harm. Hackers can also exploit a compromised system in order to access other applications and systems across the organization and even find their way into third-party partner systems. A successful breach can cause compliance issues with Payment Card Industry Data Security Standards (PCI DSS) and General Data Protection Regulation (GDPR) and significantly damage brand reputation.

Additionally, as C-Store operators implement new digital tools to improve customer engagement, the chances of a security breach become even greater. Expanding adoption of self-checkout technologies, guest Wi-Fi, computer vision tools, and consumer loyalty apps have introduced new potential points of vulnerability for retailer systems and data.

C-Stores also have numerous IoT devices within their network landscape to help ensure convenience, cleanliness, and safety. Self-service, outdoor payment systems at the pump present their own unique challenges. Device exposure and requirements for 24×7 forecourt access compound the need for supplemental protection. Fuel tank sensors, walk-in cooler temperature sensors, robot floor cleaners, and interactive digital signage are just some of the vast proliferation of nontraditional compute devices being introduced, and most have little-to-no built-in security.

On-site fuel management systems carry additional safety and compliance requirements that traditional retailers don’t have to consider. Increasing adoption of food service within C-Stores adds systems for ticketing, delivery, and inventory management, all of which expand the attack surface. All of these newly adopted tools, systems, and devices deployed across modern environments create new potential points of exploitation for cybercriminals. To complicate matters further, when all those device connections need to be maintained in rural or remote branch locations, supporting an “always-on” experience for customers can become even more challenging.

As electric vehicles (EVs) become a larger portion of the automobile market, another disturbing risk is posed by the widespread installation of potentially unprotected EV charging stations across the country. Today's connected EV charging stations need significant technology upgrades, regulations, and standards to address cybersecurity vulnerabilities. Some EV providers want to facilitate distributed energy resources (DERs) and have utility requirements based on the location, which could increase risks even further.
Complexity is the enemy of security, so as the digital footprint expands within the C-Store, associated security risks also rise. Many organizations have tried to manage their expanding attack surfaces by deploying an array of “bolted-on” point security solutions to defend each new network edge being created. Unfortunately, the use of separate, siloed cybersecurity products inhibits effective detection of potential threats and automated responses to incidents. The resulting vendor sprawl has now grown too difficult and too expensive for most retailers to manage, exacerbated by the acute shortage of skilled cybersecurity staff across all business sectors.

A Platform-Based Approach to Security

Addressing the complex needs of C-Stores first calls for end-to-end integration of the network and security architecture. An integrated security platform can offer broad security support with visibility and protection of the entire digital attack surface.

An effective platform provides comprehensive security capabilities while elegantly converging network access into its infrastructure. Foundational capabilities should include next-generation firewalls (NGFWs), wireless access points (APs), switches, and cellular transport capabilities such as wireless wide area network (WWAN). These devices should be designed to seamlessly function as a complete network and security ecosystem.

Integration also enables automation to reduce security management complexity. It can eliminate the need for manual processes and workarounds that slow response to threats, while helping to streamline things like compliance reporting processes. It also allows you to leverage threat intelligence from across your network, as well as from global threat feeds that dynamically update throughout the day, keeping your organization ahead of emerging threats and real-time attacks.

Most importantly, a platform approach can enhance security at critical points across the organization and:

- **Protect any edge and any app at scale** with advanced threat protection, convergence of network and security, secure sockets layer (SSL) decryption, and network automation
- **Deliver complete and simplified access layer security** with direct and integrated control, configuration, and management, which extends the NGFW to the local area network (LAN) edge
- **Offer secure, business-outcome-driven wide area networking (WAN)** with reduced cost and complexity, better application performance, and integrated security
- **Control every device on every network** with simplified network deployment, automatic device discovery, and policy application at scale, including IoT and guest devices

**Why Fortinet?**

Whether it’s a single convenience store, a small regional chain, or an enterprise brand with thousands of locations, Fortinet can help C-Store operators address their ever-evolving network and security challenges. The Fortinet Security Fabric provides a platform with comprehensive visibility across the attack surface, seamless security integration, proactive threat intelligence, and automation that accelerates threat response and critical workflows.

**Secure networking for branch locations.** C-stores need fast and scalable connectivity to enable seamless transactions in support of sales, inventory, purchasing, and other activities. Fortinet solutions provide high-speed, reliable in-store networking to support a good customer experience. Secure software-defined wide area networking (SD-WAN) provides efficient routing of traffic between retail locations and cloud infrastructure without sacrificing protection. A recent survey showed that 53% of respondents have already deployed an SD-WAN solution at their branch locations.6
**Comprehensive protection.** The Fortinet Security Fabric combines a comprehensive suite of solutions that cover a wide range of threats such as malware, phishing, and ransomware. This ensures that your C-Store is protected across all stages of the attack cycle. The Security Fabric also includes endpoint security to protect devices that are connected to networks, such as POS systems, ATMs, gas pumps, kiosks, and IoT devices. Endpoint security helps prevent cybercriminals from accessing sensitive information such as credit card data.

**Advanced threat intelligence.** Breaches are on the rise. Eighty-four percent of organizations experienced one or more cybersecurity intrusions in the past 12 months (up from 80% from last year). FortiGuard Labs uses artificial intelligence (AI) and machine learning (ML) to generate threat intelligence that is shared via the Fortinet Security Fabric in real time. This keeps all parts of your security infrastructure aware of the latest attack variants for rapid detection and response.

**PCI compliance for POS.** Fortinet simplifies PCI-DSS compliance processes. Centralized visibility into the entire network and security landscape along with preconfigured PCI-DSS reporting templates dramatically decrease the need for manual workflows and costs associated with demonstrating regulatory compliance.

**Ease of management.** Fortinet security solutions are easy to manage, so you can focus on business instead of getting caught up in IT complexity. Centralized management tools allow administrators to monitor and manage the security and networking of all store locations from a single dashboard.

**Fortinet Solutions for Convenience Stores**

Fortinet SD-Branch consolidates secure SD-WAN functionality with industry-leading security capabilities for C-Store branch locations. This includes FortiGate NGFWs, FortiAP access points, FortiSwitch switches, and FortiExtender for flexible 5G, LTE, and Ethernet connectivity. Providing a simplified approach to access-level security with integrated switches and AP controllers, flexible connectivity options, advanced threat protection, and simplified template-based deployment with streamlined administration are just a few of the key capabilities provided by the Fortinet SD-Branch solution.

FortiEDR endpoint detection and response provides transparent visibility across all endpoints, including POS systems. It combines next-generation antivirus (NGAV), application communication control, virtual patching, and automated EDR for real-time blocking, threat hunting, and incident response in a single agent.

FortiAnalyzer analytics enhances security across physical, virtual, and cloud environments using analytics-based detection that drives faster responses to cyber risks.

FortiManager central management provides single-pane-of-glass visibility and automated compliance reporting at scale.

**Retailers Around the World Choose Fortinet**

Comprehensive cybersecurity is essential for protecting C-Stores from the latest cyberthreats across an ever-expanding attack surface, and to ensure the frictionless, always-on experience your customers expect. The Fortinet Security Fabric provides consistent, dependable, and secure network experiences to retail organizations around the world. Globally, more than 660,000 businesses trust Fortinet with their security, making FortiGate the world’s most deployed network security solution.
Securing Today's Convenience Stores with Fortinet

6. "The US electric vehicle charging market could grow nearly tenfold by 2030: How will we get there?" PwC, October 3, 2022.