SOLUTION BRIEF

Deploying and Securing Curbside Operational Models for Restaurants

Executive Overview

As a result of the COVID-19 pandemic, over $25 billion in restaurant industry sales were lost during the month of March 2020 and projected losses are expected to top $225 billion by mid-2020.[1] By necessity, most restaurants have had to quickly adapt their business models for getting food in the hands of their customers. Some examples include delivery services, drive-through sales, curbside pickup, and pop-up restaurants or satellite locations. In support of low- to no-contact point-of-sale (POS) transactions, restaurants must rely on secure wireless technologies to protect themselves and their customers from opportunistic cyber criminals seeking to exploit a vulnerable new attack vector. Fortinet offers several options to help restaurants secure these new services. These include extending the reach of an existing Fortinet Security Fabric to encompass curbside delivery, to adding additional secure wireless access points for on-lot pop-ups, to a Secure SD-Branch solution for new or temporary satellite location transactions.

Many operational responses to COVID-19 don't fully take cybersecurity into account. Existing risks could be missed as security expenditure is cut, controls are relaxed, and IT changes are rushed through without following routine change protocols.[5]

Reinventing Restaurants for Safe and Cybersecure Sales

Most U.S. businesses have been affected in some way by the coronavirus, especially the restaurant industry, where the average profit margin for a business last year was a mere 6.2%—before the effects of the pandemic even started being felt.[2] To survive financially while protecting the health and safety of their employees, a majority of businesses have had to rapidly expand services beyond the four walls of their establishment. Last year, nearly 50% of all restaurant spend came from takeout and delivery sales.[3] As a result of the pandemic, however, a staggering 92% of all restaurant traffic is now off-premises.[4]

Restauranteurs who had already integrated digital and omnichannels practices into their businesses are seeing much greater sales volume and repeat visits than those who have been forced into adopting a digital strategy. Restaurants have had to act quickly to build out or expand capabilities to meet customer demand. This has meant installing new hardware or repurposing existing wireless infrastructure that previously supported guest-access or internal operations in order to secure drive-through, curbside, and pop-up transactions. But the elastic and nimble mindset that comes with rapid adaptation can often overlook cybersecurity. Regardless of the extended operation model in use, organizations must take precautions when it comes to protecting their business networks and the private financial data of customers at a time when criminals are looking for any new vulnerabilities to exploit the situation.

Extending Services to Curbside and Drive-through Customers

One of the ways that many food service businesses are keeping the lights on is by keeping the front door closed and meeting customer demand at street level with curbside delivery or drive-through services. To support secure walk-up order and payment transactions at the restaurant, the wireless network can be extended to a broader physical footprint of the business. Business owners need to ensure the privacy of customer payment card data in compliance with industry standards like the Payment Card Industry Data Security Standard (PCI DSS). At the same time, restaurants must restrict unauthorized access to other parts of their business from patrons or other outsiders.

- **FortiAP** wireless access points enable secure connectivity for curbside or drive-through transactions, including contactless POS applications.
- A **FortiGate** next-generation firewall (NGFW) can provide network segmentation to prevent unwanted communication between devices and unauthorized access to other parts of the network.

FortiGate helps to ensure that customer traffic is kept separate from internal business traffic via unique service set identifiers (SSIDs) or virtual local-area networks (VLANs). It also protects customers from cyber criminals by scanning for rogue access points and attempts to intercept transactions. FortiGate inspects encrypted information for malicious payloads (e.g., malware), monitors network traffic for congestion and potential misuse, and enforces security policies as necessary. It helps restaurants protect the personal data of customers, in compliance with industry standards such as PCI DSS.

A lack of a security infrastructure within the internal network significantly limits an organization's visibility into suspicious traffic behaviors and data flows, which hinders the ability to detect a breach.[6]

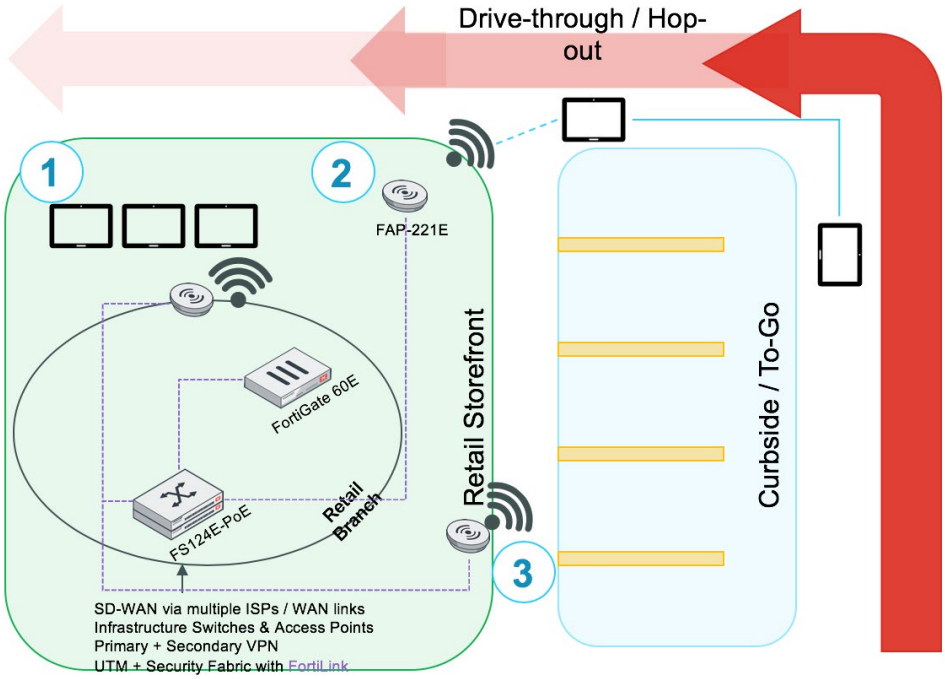

Figure 1: Wireless solutions leveraging existing Fortinet Security Fabric infrastructure.

Location, Location, Location—On-lot Pop-ups and Satellite Outposts

Many full-service restaurants lack the physical space to add a drive-through option. Others may only have limited capacity for meeting curbside demand. For these restaurants, a different operational model may be needed in the form of pop-up or satellite locations. While these new concepts allow restaurants to continue serving customers, they also come with their own set of challenges—especially in areas with limited internet options. The network infrastructure must be easy to deploy while ensuring secure connectivity over a wider geographical model—from as close as 100 feet away or as far as across town.

- **Fortinet Secure SD-WAN** (a built-in feature of FortiGate NGFWs) provides integrated networking and security capabilities for restaurants to support low- to no-contact transactions as a secure extension of the main business's network in on-lot pop-ups.

Fortinet's approach to delivering secure SD-WAN networking provides efficient protection for extending networks to outpost locations by providing consistent security policy enforcement without impacting network performance—while providing simple management in a single pane of glass.

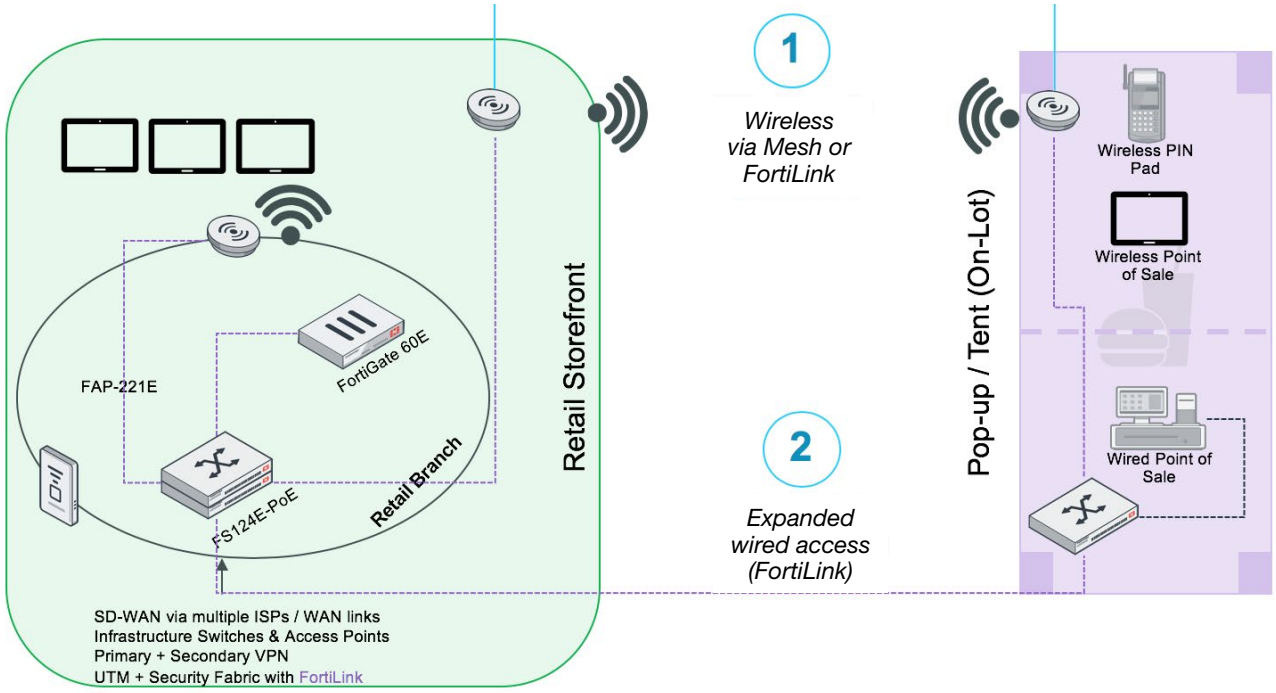

Figure 2: Enabling additional on-lot restaurant concepts via Fortinet wired/wireless solutions.

For off-lot satellite locations—such as food trucks, expanded service pickup points, or distributed branch restaurant locations—restaurants may need to share both networking and security capabilities across a broader geographic area.

- **Fortinet Secure SD-Branch** consolidates networking and security capabilities into a single solution that provides seamless protection for distributed organizations.

The Fortinet Secure SD-Branch solution covers all critical exposures, from the WAN edge, to the branch access layer, to a full spectrum of endpoint devices. It extends Fortinet Secure SD-WAN capabilities across wired and wireless networks while simplifying branch infrastructure management.

Protecting the Expanded Cloud Attack Surface

In order to meet the needs of their customers, restaurants have scaled up their cloud presence to support mobile applications, order-ahead, customer analytics, and more. Even those business that had invested heavily in the cloud before have seen an influx in traffic that may test the limits of their cloud infrastructure. This is where restaurants will need to focus.

- **FortiADC** application delivery controller (in combination with a FortiGate) can provide the necessary cloud load-balancing to ensure availability.
- **FortiWeb** web application firewalls (WAFs) secure sensitive data and access to web front ends.
- **FortiCWP** cloud workload protection ensures availability and security of critical workloads.

In the latest NSS Labs NGFW group test, FortiGate delivered 99.3% security effectiveness and 100% evasions blocking.[7]

Secure SD-Branch secures wired and wireless access points, inspects internal traffic and applications, and leverages network access control (NAC) to protect the organization from device-based threats.[8]

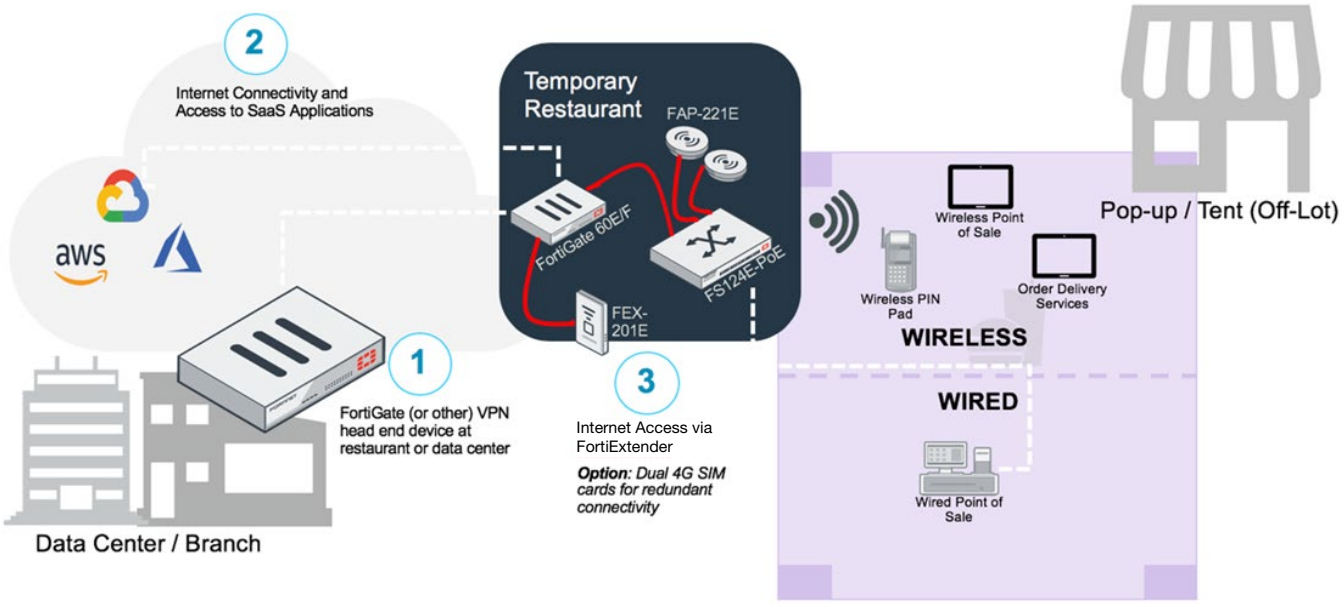

Figure 3: Enabling off-lot restaurant concepts via Fortinet Secure SD-Branch.

Deploy and Secure Expanded Restaurant Services with Fortinet

Within the new normal of keeping businesses afloat, much has changed and will continue to change about the way retail transactions occur. The ability to provide safe and satisfying customer experiences is paramount. By embracing new digital innovations for extended customer service, restaurants can maintain the viability of their businesses in these difficult times. In this pursuit, Fortinet is helping restaurants securely scale their networks to help feed the population and keep everyone safe from unnecessary public exposure.

[1] "Coronavirus Information and Resources," National Restaurant Association, May 4, 2020.

[2] Rory Crawford, "Restaurant Profitability and Failure Rates: What You Need to Know," Modern Restaurant Management, April 11, 2019.

[3] Breck Hapner, "Beating The Odds: Surviving COVID-19 In The Digital Food Space," Fast Casual, April 2, 2020.

[4] Ibid.

[5] "How to manage the cyber-risks of coronavirus COVID-19," PwC, April 3, 2020.

[6] Nirav Shah, "Why Network Segmentation Matters," Fortinet, March 5, 2020.

[7] "Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report," Fortinet, June 19, 2019.

[8] Zeus Kerravala, "How SD-Branch addresses today's network security concerns," Network World, August 12, 2019.

May 6, 2020 11:25 AM

123456-0-0-EN

D:\Fortinet\Solution Briefs\red solution briefs\Retail Popup Curbside\sb-FA-deploying-and-securing-curbside-operational-models-for-restaurants-562020