

SOLUTION BRIEF

Deploying and Securing Curbside Operational Models for Restaurants

Executive Summary

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.

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

Restaurateurs 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.

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

- 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.

[illegible]

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










- 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.

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

1.
Wireless via Mesh or FortiLink

2.
Expanded wired access (FortiLink)

Retail Storefront

Retail Branch

SD-WAN via multiple ISPs/WAN links
infrastructures switches & access points
Primary + Secondary VPN
UTM + Security Fabric with FortiLink

Protecting the Expanded Cloud Attack Surface


<https://creativecommons.org/licenses/by-nc-sa/4.0/>
3

- **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.

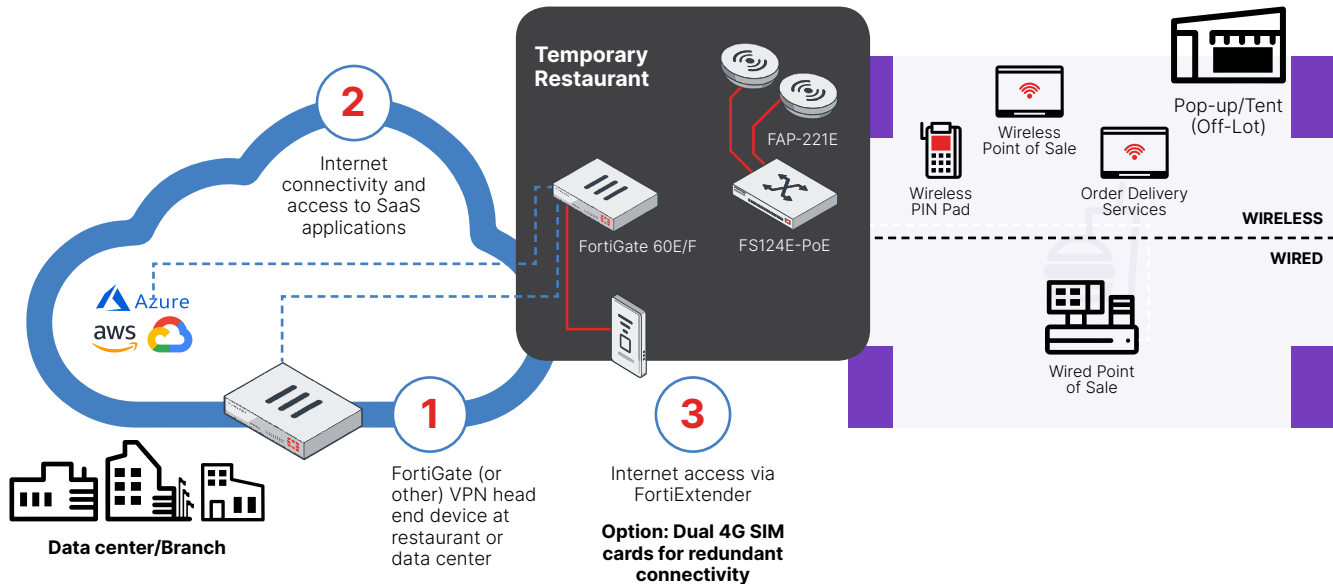


Figure 3: Enabling off-lot restaurant concepts via Fortinet Secure SD-Branch.

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.