

# Guest Experience vs. Restaurant Security

These days, restaurants are being hit from all sides. Discretionary income is down for many households. Some choose to bypass the traditional dining out experience in favor of food trucks, third-party food delivery, and meal kit subscriptions. Restaurant operators are forced to find new ways to earn the loyalty of the twenty-first century diner, and increasingly that means going digital to create an engaging, personalized experience from soup to nuts and beyond.

In this new context, an app-enhanced hospitality platform can serve as the ultimate destination ambassador. For example, kiosks or mobile apps can allow diners to place orders, play games, pay the check, calculate the tip, and add or redeem loyalty points right at the table.

On the other hand, rarely a day goes by without news of an online security breach. As if adapting to changing guest expectations were not challenging enough, operators must also focus on another moving target—maintaining a truly secure network that is not only PCI compliant, but that also protects the brand against breaches.

These increased demands are competing for a piece of the budget driven by tight margins, pitting IT and security teams against the marketing department, which is measured on the effectiveness of customer loyalty and retention programs. Funding network connectivity and remote site management can lead to cost-cutting measures that weaken the guest experience and threaten diner patronage.

How can an operator meet all these requirements? We see three potential approaches:

1. Invest in in-house IT skills and networking expertise to manage an enterprise private cloud
2. Outsource IT/security to an experienced Managed Services Provider (MSP) for secure cloud WAN services
3. Augment in-house expertise with the skills and benefits of an MSP

A viable solution must address the operator's business goals, competitive realities, timeframe, budget and IT/security skill constraints with a focus on profitable expansion. This argues against taking on costly security and IT labor. In other words, most operators are best served by targeting investment on core business competencies and turning to an MSP that offers a secure cloud and software-defined WAN solution (secure SD-WAN) to provide the infrastructure for the digital piece of the guest-experience solution.

In any WAN solution, in-house or outsourced, security is always a primary concern, and restaurants generally lack onsite IT and security staff. By contrast, as the cloud-services market has matured, concerns about security are being diluted by a "lack of resources and expertise,"

An MSP that offers SD-WAN service complemented with a private cloud can be one of the most secure, nimble and cost-effective ways to go beyond mere checklist PCI compliance to protect the brand against breaches and deliver innovative guest experiences.

However, sifting through the offerings for managed services can be difficult. Making a true comparison between solutions can be a challenge due to the variability of architectures. Because of the mission-critical nature of a WAN, the procurement process must drill down to the nuts and bolts of implementation, but the initial stages of evaluation can be streamlined by assuring that the offering includes certain essential attributes.

Download the white paper to learn more about selecting the secure SD-WAN solution that best fits your requirements.