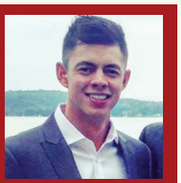
Ron Robinson,
SVP, Sales, Cybera



Kyle Welch,
President,
Chicago Scoops

Keys to Managing Threat Exposure

How SD-WAN offers a simple, cost-effective way to standardize security

CHICAGO SCOOPS, fast-growing franchisee of the Cold Stone Creamery brand, is lighting up applications fast and securely, while avoiding greater margin pressure and maintaining its people-first approach. *HT* talks to Kyle Welch, president of Chicago Scoops LLC and Ron Robinson, SVP of sales at Cybera (*cybera-murtec.com*) to find out how they collaborated to standardize security across 30+ stores in one month.

HT: As restaurants have access to more customer data what are some issues operators face making sure guest data is secure at all touchpoints?

KW: Building a successful franchise is about hiring and training great people and setting up the right systems and processes from the start. I put security on a par with sanitation and we wanted to be proactive about protecting our customers and brand from day one. Security and PCI compliance is a black-box to most of the franchise community, no matter how experienced they are. There are lots of variables like PCI-related questionnaires, technology scanning vendors, firewall and intrusion detection vendor options etc. Many stores have minimal security or unprotected Wi-Fi, and residential Internet access is on the same connection as the payment network. Most franchisees have few to no IT and security personnel to address these security challenges. Being able to lean on vendors who can provide a one-stop cost-effective solution and turnkey service really helps.

HT: What are some keys to help restaurants manage what often winds up being a "mixed bag" of connectivity to standardize a security and compliance program across multiple locations?

KW: You bring up two essential points. One is at the macro-level that requires standardization of security across all store locations so a franchisee can take an easy, template-based approach that can scale for future store growth. The other aspect is more directed at the individual store-level that requires securing connectivity inside each store since each may have varying networks, some having minimal security or insufficiently secured networks carrying card holder data. To address the "mixed bag" of applications and connectivity within a store, Chicago Scoops implemented Cybera's secure software-defined-WAN solution (SD-WAN). This solution virtualizes the network so all network intelligence is handled in software. Stores can be configured and security enforced using their cloud. What this means for the operator is mission critical applications like payments and loyalty programs can co-exist with public applications like Wi-Fi on a single network while providing application-specific security and end-to-end network segmentation and encryption. Each application is isolated into its own dedicated logical network, preventing its traffic from mingling with other application traffic on the network. That means there is no data breach propagation between applications. Moreover, because the solution is software-based, it can work on top of stores' existing networks with no re-design or expensive integration services.

HT: How can restaurants address security and safeguard guest data when they have minimal technical support staff?

RR: Operators should consider turnkey security services that are very "low-touch" in their evaluation of security solutions. By that, I mean a security solution that is world class in quality, but can also be implemented by store personnel with no security or IT expertise in minutes, eliminating the expenses associated with dispatch technicians. Make sure your vendor takes a proactive approach to monitoring your network 24x7x365, making the security solution worry-free.

HT: What should operators keep in mind regarding cloud-based or on-premise security solutions?

RR: The operative word here is "simplicity." The thrust of the challenge for most franchisees is achieving enterprise-grade security with little to no IT/security staff and doing so cost-effectively across one store or many stores. Security solutions that abstract the intelligence and complexity of security into the cloud, leaving operators with only a very simple store device that can be installed quickly by store personnel should be table-stakes. Operators should look to vendors that take a defense-in-depth approach to security by consolidating security functions such as firewall, intrusion detection, multi-factor authentication, security event management etc. that would normally reside in numerous devices, increasing complexity of management and cost, into that single consolidated in-store device. Finally, selecting a vendor that takes a software-defined approach to security will further ensure the security solution can be "over-laid" on the operator's existing network, eliminating costly network redesign and upgrades. The result? Fast, secure application turn-up that allows operators to focus on what matters most – the customer experience. HT

Cybera®
cybera-murtec.com