The days of Wi-Fi zones are over. Our patrons appreciate Wi-Fi that is reliable and fast, so we’re giving it to them. Technology is a big differentiator for us. We’re investing to keep our customers as connected as they want to be, and our tenants as efficient as they can be.

– Martin Menne Co-Owner
San Pedro Square Market

Downtown Social Hub Upgrades Access Network to Meet Surge in Patrons

Business Challenge:
Located in downtown San Jose, California, the Capital of Silicon Valley, San Pedro Square has quite recently come into vogue since the restoration of the San Pedro Square Market. Now faced with 8,000 smartphone-wielding patrons daily, the San Pedro Square Market is exploiting Wi-Fi to improve the visitor experience and maximize operational efficiency.

In recent years, the San Pedro Square area has seen surging numbers of patrons to its bars and restaurants. Around 20 of those establishments are tenants in the San Pedro Square Market (SPSM), which also hosts live music and other events. “As the market became more and more popular, it became clear our network and systems were inadequate for the new era we are entering into,” says Martin Menne, Co-Owner.

Their unsecured guest Wi-Fi was oversubscribed by thousands of daily visitors. Worse, they were getting nothing in return for offering free Wi-Fi, not even basic visitor stats. Guests were gobbling up so much bandwidth that tenants couldn’t do business on it, PoS was not reliable, and voice over Wi-Fi rarely worked. Security was implemented by separate appliances, and their video surveillance was CCTV.

Details
Customer Name: San Pedro Square
Industry: Retail and Hospitality
Location: San Jose, California, USA

Business Impact
- Secure mobile PoS, over a multi-tenant network delivers efficiency for each tenant
- Integrated security end to end, reduces complexity and enables uniform wired/wireless policies
- Able to streamline surveillance infrastructure and dramatically reduce required staffing level
- Generating opt-in marketing list through sign on to captive portal, while protecting network better
- Using visitor presence data to optimize staffing levels and influence marketing strategy
- Prepared for and considering IoT – energy management systems already under network control
CASE STUDY: SAN PEDRO SQUARE MARKET

“We had so many disconnected systems which had grown organically— it was killing our productivity, and not benefiting clients,” recalls Menne. It was time to rethink the network and what was expected of it, and to step up to a new level of service, security and intelligence, fit for “always-connected” customers.

Integrated Network and Security

After considerable research and evaluations, they chose Fortinet’s Secure Access Architecture solution, with a FortiGate 92D, FortiSwitch PoE gigabit switches and FortiAP 802.11ac access points, to replace and upgrade the existing network and security framework.

The FortiGate is both a WLAN controller and Unified Threat Management platform in one. It provides a single pane of glass unifying wired and wireless network management and security management.

Switching to this integrated secure access platform, has dramatically simplified network operations and has provided new levels of visibility and control over the applications being used on the network. They can block patrons from visiting high-risk sites, or watching inappropriate content, and can protect everyone from viruses and cyberattacks – through one console.

“In the past we were reasonably successful at fending off intrusion attacks, and staying off IP blacklists, but it was a lot of work. With Fortinet, everything from access security to virus control is easy and intuitive and we have complete visibility of threats,” notes Menne.

SPSM’s bar operations maintains a separate SSID to ensure PCI-DSS compliance for POS terminals, kiosks and hand-held terminals. SPSM’s general operations staff also has their own SSID for operations. Fortinet identity management enables user traffic from different tenants to be segregated based on the user’s group memberships. This reduces the bandwidth overhead of operating multiple SSIDs.

Guests are isolated from operational and POS traffic through a guest SSID associated with a captive portal. Besides harvesting user registrations for marketing purposes, SPSM can apply unique security policies to guest traffic, to prioritize, block or throttle literally any type of traffic, from Wi-Fi Calling to Facebook.

Social Wi-Fi and Analytics

“We know there’s a wealth of valuable insights to be gained by observing patron traffic patterns. But we didn’t want to bite off more than we can chew,” Notes Brett Houston, from Optio Development, SPSM’s outsourced IT management company. For now, their use of FortiPresence, Fortinet’s presence analytics service, is limited to macro trends such as visitor peaks and troughs, visitor dwell time, conversion rate and traffic flows. “Just these have exposed ways to improve staffing, table placement and signage,” Houston explains.

FortiPresence passively gathers and analyzes anonymous presence information for all Wi-Fi-enabled devices that come in range of the FortiAP access points, even if they don’t log on to the guest portal.

Wi-Fi Calling, Surveillance and IoT

Guest bandwidth demands continue to soar, and SPSM anticipates people will soon be “Wi-Fi Calling” from the network. Fortunately, Fortinet provides granular control over the resources and priority assigned to different apps for different users. “In the world of Guest Wi-Fi, Wi-Fi Calling will separate the men from the boys…we’re ready – Wi-Fi Calling works here!” exclaims Houston.

SPSM is tearing down its analog CCTV network and replacing it with Fortinet IP-based surveillance. Analyzing incidents on the old system was a week-long affair. Now for any moment in time, they can review synchronized playback from a dozen cameras, watch it from an iPhone and burn it to DVD in minutes. “While the new Fortinet camera system is already providing many benefits, we hope in future to synchronize the video with presence analytics data,” adds Houston.

“We built this network for scale and for the future, and we intend to use it,” says Menne. They have already put the energy and resources and priority assigned to different apps for different users. “In the world of Connected IoT, Wi-Fi Calling will separate the men from the boys…we’re ready – Wi-Fi Calling works here!”

Copyright © 2016 Fortinet, Inc. All rights reserved. FortiGate®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions; actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.