FORTINET

SECURITY TRANSFORMATION IN HOSPITALITY:

PROTECTING THE GUEST EXPERIENCE FROM BOOKING TO CHECKOUT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digital transformation (DX) is improving the guest experience in the rapidly growing hospitality industry, but such initiatives have the potential of increasing risk if they are not accompanied by a security transformation (SX). The goal of SX is to unify the network security architecture into a broad, integrated, and automated infrastructure—eliminating silos and enabling centralized control and automation. Hoteliers embarking on an SX initiative would do well to consider elements of their networks that are industry-specific as well as those that are common to most organizations. Ultimately, the best solution will enable network security, multi-cloud security, secure software-defined wide-area network (SD-WAN), and automated threat detection and response that is centrally controlled with transparent visibility.

With indirect economic contributions factored in, the global travel industry accounts for more than 10% of global GDP.

"2018 travel and hospitality industry outlook," Deloitte, accessed September 14, 2018.

01: DX COMES TO HOSPITALITY

The global hospitality industry is booming, and DX is making hotels more profitable. Guests now strongly prefer to book online,[1] and once they arrive, technology enhances their stay—often in ways that enhance a hotel's brand.[2] Cutting-edge players are using a combination of artificial intelligence (AI), the Internet of Things (IoT), and near field communication (NFC) to help create a highly individualized travel experience.[3]

The infrastructure supporting these technologies is more complex and distributed than ever, with sensitive data residing in multiple clouds, an array of IoT devices connected to the network, and mobile access to more and more resources. Because of these factors, DX initiatives almost always expand an organization's attack surface.

For hospitality organizations, any vulnerabilities present opportunities for cyber criminals to steal information from their relatively affluent customer base.[4] Valuable transaction and credit card data can be stolen from the point-of-sale (POS) infrastructure as well as card-not-present (CNP) data from phone transactions. A wide array of customer data is vulnerable when a hotel's public Wi-Fi network is compromised. And distributed denial-of-service (DDoS) attacks can result in downtime that incurs missed bookings and poor reviews.[5]

[1] "Distribution of adults in the United States by their preference of hotel booking online or offline 2017," Statista, accessed September 14, 2018.

[2] Elaine Hendricks, "Trends Directing the Future of In-room Entertainment," Hospitality Upgrade, October 25, 2016; "3 Hotels Using Artificial Intelligence To Improve Guest Experience," Event Manager Blog, December 4, 2017.

[3] "2018 travel and hospitality industry outlook," Deloitte, accessed September 14, 2018.

[4] Steve Oates, "Cyber Security Threats Facing Hotel Industry," LinkedIn Blogs, February 10, 2018.

[5] "Timeline: The growing number of hotel data breaches," Hotel News Now, January 10, 2018.

The hospitality industry is poised to grow at a 5% to 6% rate in 2018.

“Now Boarding: The Future of the Travel, Hospitality Industry,” Deloitte, The Wall Street Journal, accessed September 18, 2018

02: DX REQUIRES SX

The fact is that virtually every DX initiative expands an organization's attack surface in some way, taxing last-generation network security infrastructure and increasing risk. As a result, DX requires network security teams to rethink some principles that they have lived by for a long time. Put another way, a DX requires a corresponding SX.[6] In this case, SX requires a strategic, comprehensive approach to security that goes beyond last-generation security principles:

- **From perimeter security to broad coverage.** Heavy dependence on securing the perimeter of a closed data center becomes increasingly obsolete as more and more services and data are sprawled across multiple clouds. In addition, many organizations now allow network traffic to bypass the security controls of the data center via SD-WAN technology.[7] This means that security must be expanded to cover a greatly enlarged attack surface.
- **From siloed security to an integrated architecture.** As organizations add cloud solutions, they often simply activate the built-in security features from the cloud provider. But as multiple clouds are added over time, this results in a different set of security solutions for each cloud and for the on-premises infrastructure. This produces a piecemeal approach to security, not to mention increased risk. This is resolved with SX, which aims to provide centralized visibility and control for the entire infrastructure.
- **From manual threat response to automated detection and response.** Current threats move at machine speed, with 87% of breaches now taking minutes to initiate, while 68% of compromises take months to be discovered.[8] As a result, automated detection and response—including the use of AI and machine learning (ML) to detect unknown threats—are no longer optional. And organizations must ensure that the gathered intelligence is shared companywide.

[6] Patrick Grillo, "Digital Transformation and Security Transformation Need to Walk Hand-in-Hand," Fortinet, June 5, 2018.

[7] Andy Patrizio, "Enterprises are moving SD-WAN beyond pilot stages to deployment," Network World, May 7, 2018.

[8] "2018 Data Breach Investigations Report," Verizon, March 2018.

The number of new malware variants and new malware families increased almost

60%

in a single quarter, from Q1 2018 to Q2 2018.

"Threat Landscape Report Q2 2018," Fortinet, accessed September 12, 2018.

03: HOTELS HAVE UNIQUE VULNERABILITIES

Hotels and hotel chains share many security challenges with organizations of other types, and the need for a broad, integrated, and automated network security architecture is universal. However, the nature of the hospitality business requires special attention to certain elements of the infrastructure:

- **POS systems.** Like retail stores, hotels accept cash and electronic payments onsite, and DX initiatives increase the use of POS systems for products and services beyond lodging. While EMV chips in credit and debit cards have improved security, merchants must take proactive steps to comply with the Payment Card Industry Data Security Standard (PCI DSS) and protect customer and transaction data.
- **Reservation systems.** DDoS attacks can cause downtime in systems, including the hotel's internal reservation system. This prevents rooms from being booked during the downtime. Quite often, this even includes when customers use third-party booking sites.
- **Public Wi-Fi.** Quality Wi-Fi service is often cited as a primary feature sought by hotel guests,[9] and most travelers access such networks without thinking about the risk. Compromised Wi-Fi networks can yield valuable data for cyber criminals, from financial and credit card data to passwords.
- **In-room entertainment.** While televisions and other entertainment systems do not typically contain sensitive data, DDoS attacks and other intrusions can cause downtime that degrades the guest experience, prompting them to write and post negative reviews.

In 2017, the average breach cost the hospitality industry $120 per record stolen.

"2017 Cost of Data Breach Study: United States," Ponemon Institute, June 13, 2017.

[9] Patrick Nelson, "Wi-Fi most important hotel feature, survey says," Network World, December 16, 2014.

04: WHAT TO LOOK FOR IN A SOLUTION

As discussed above, hospitality organizations that embark on an SX initiative would do well to seek a solution that is **broad, integrated**, and **automated**. Rather than adding or maintaining silos, a solution needs to break them down and enable transparent visibility and centralized control, with consistent policies across all clouds and the on-premises infrastructure. Full integration enables true automation of security processes, threat response, and intelligence sharing across the organization.

- **Network security.** Whether an organization is a global hotel chain or a single, independent property, next-generation firewalls (NGFWs) should be deployed to protect the network from advanced threats. The solution will ideally include the ability to roll out large, secure public Wi-Fi networks for guests.
- **Multi-cloud security.** With most organizations utilizing more cloud-based solutions every year, a network security solution should be able to integrate the security architecture of the data center with corporate data and traffic moving into and out of multiple clouds, protecting the expanded attack surface of private cloud, public cloud, and hybrid cloud deployments.
- **Secure SD-WAN.** Larger organizations with multiple locations and multiple cloud-based services can likely improve their network performance by deploying SD-WAN technology. However, doing so allows network traffic to bypass the security controls of the data center. The best network security architecture includes the capability for truly secure SD-WAN.
- **Threat intelligence and protection.** Today's advanced threats move at machine speed, and this means that detection and response must move at machine speed as well. It is no longer optional for organizations to deploy threat detection and response technology that uses AI and ML. While a number of security vendors claim to use these technologies, some are less transparent than others about exactly how deep their AI/ML infrastructure goes. The best systems have ingested vast amounts of data and train their systems using a variety of learning techniques.

“[H]otels must make guests feel that the hotel they visit is as concerned about their personal and financial data as they are about their physical security.”

—Robert Braun

“5 key issues in hotel cybersecurity,” eHotelier Insights, May 19, 2016.

CONCLUSION

Recent trends suggest that the hospitality industry is poised for long-term growth. Unfortunately, this success means that the sector will likely continue to grow as a target of cyber criminals. Verizon noted 1/3 more breaches and incidents at hospitality organizations in 2017 vs. 2016,[10] and the cost of downtime and data loss is increasing. At the same time, DX initiatives are making for a more distributed computing environment with a greatly expanded attack surface.

The best response to these disturbing trends is to move from a reactive stance to a proactive one when it comes to network security. The goal of SX is to create a system that is broad, integrated, and automated—enabling the network security team to stay one step ahead of the bad guys.

[10] "2018 Data Breach Investigations Report," Verizon, March 2018.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

249716-0-0-EN October 5, 2018 9:17 AM

ebook-Security-Transformation-in-hospitality