WHITE PAPER

# Protecting the Hospitality Industry and Its Guests with the Fortinet Security Fabric

## Executive Summary

**The global travel industry accounts for more than 10% of the Global GDP,[1] making it a prime target for attackers. While striving to offer differentiated guest experiences and to control costs, hospitality purveyors are seeing their attack surface expand and a marked increase in network complexity. The Fortinet Security Fabric enables hotels and hotel chains to accomplish a security transformation (SX) that helps move them from a reactive stance on security to a proactive one. Next-generation firewalls (NGFWs) form the basis for the Security Fabric, protecting not only the perimeter of the data center but also data and infrastructure sitting in multiple clouds.**

**Integrated with NGFWs are a variety of security solutions that can be monitored and controlled via a single pane of glass. This enables true automation of security response, monitoring, and reporting. Underlying the entire Security Fabric is an extensive threat-intelligence infrastructure that uses artificial intelligence (AI), machine learning (ML), and other advanced threat-prevention capabilities to detect and remediate unknown threats.**

Increased complexity is the number 1 challenge faced by CIOs.[2]

## The Hospitality Industry Needs SX

As hospitality organizations expand their digital footprint and embrace digital innovation to deliver differentiated guest experiences, many find their data and applications scattered across multiple clouds. According to CIOs, nearly 80% of organizations are introducing digital innovations faster than their ability to secure them against cyberattacks.[3] Beyond these issues, attacks are growing more sophisticated: The majority of breaches take only a few minutes to initiate, but most of those take months to be discovered.[4] The outcome is that manual responses are no longer adequate and teams cannot scale, with only 4% of alerts being investigated.[5]

The only viable response to these alarming trends is for an organization to undergo a security transformation (SX) by moving from a reactive stance to a proactive one that delivers:

- **Broad coverage** across the expanded attack surface
- An **integrated security architecture**
- Integrated **AI-based breach protection**
- **Automated operations, orchestration, and response**

## Key Hospitality Cybersecurity Challenges

Following are some of the key cybersecurity challenges facing hospitality companies today:

### Cost reduction

The hospitality industry is highly competitive and most organizations operate on a thin margin, requiring them to optimize costs across all facets of the operation, including cybersecurity. With the shortage of qualified cybersecurity experts (over 3 million jobs are unfilled today[6]), talent is at a premium. Hospitality organizations must optimize their security investment and balance risk tolerance against risk posture.

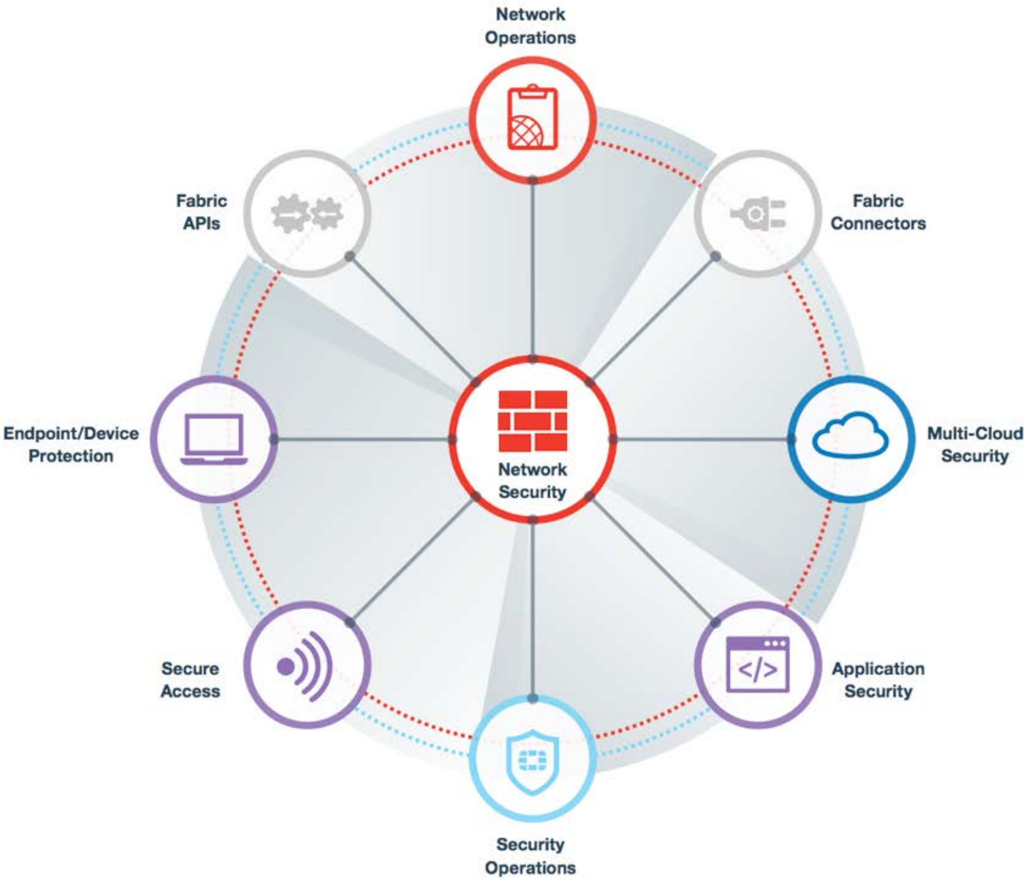

Figure 1: The Fortinet Security Fabric enables multiple security technologies to work seamlessly together, across all environments, and supported by a single source of threat intelligence. This eliminates security gaps in the network and hastens responses to attacks and breaches.

### Visibility

Fragmentation, the result of using point products to plug security holes, has created silos within the security architecture. These silos lead to blind spots that compromise the overall effectiveness of the security architecture. This is a widespread problem, with 77% of organizations saying they rely on nonintegrated point security products to some degree within their organization.[7]

### Operational efficiency

Lack of integration between the different security elements and architectural fragmentation also increase operational inefficiencies. Security architects name the difficulty of implementing disparate products as the top issue they face in their job.[8] With limited staffs and an increasingly complex set of security toolsets to manage, hospitality organizations need integrated security architectures that orchestrate and automate as many workflows as possible.

### Customer experience

As hospitality organizations strive to deliver unique and personalized guest experiences, they rely on a multitude of endpoints and Internet-of-Things (IoT) devices to collect data and deliver the experience.  All of this must be seamless to the guest. Poorly performing Wi-Fi, difficult-to-use/unavailable entertainment services, and security breaches can damage the guest relationship and even the corporate brand.

### Compliance reporting

Hospitality purveyors often retain their customers' payment card information for a much longer period than retailers, with reservations often booked months in advance and charged at the end of the stay. In addition to current regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the EU's General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA), many governments are pushing new regulations that include significant penalties for noncompliance

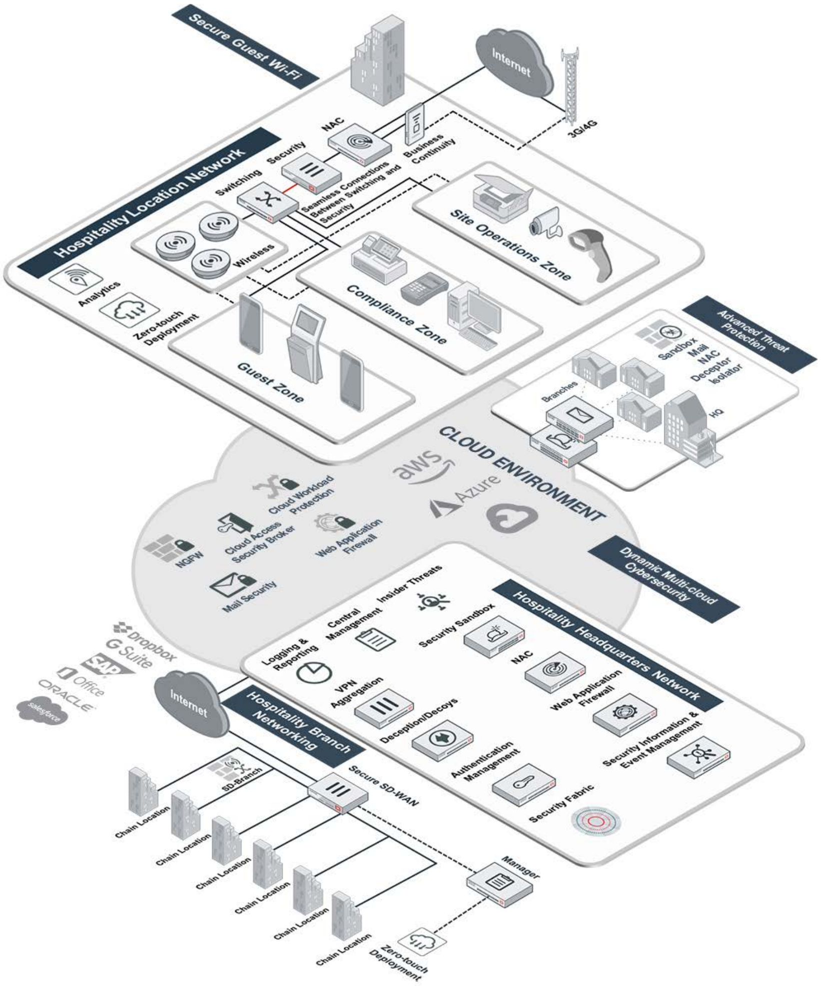

Figure 2: Hospitality organizations have extensive attack surface requirements and must manage growing complexity with a broad, integrated, and automated security architecture.

## Hospitality Cybersecurity Use Cases

Customers expect their data security to be taken as seriously as their physical security. As the hospitality industry embraces digital innovation to improve the guest experience, it is also dealing with an expanded attack surface, increased network complexity, as well as unknown threats and zero-day attacks. The elements of the Fortinet Security Fabric cover the entire attack surface and form an integrated ecosystem that unlocks automation capabilities. In addition to lower risk, the Security Fabric enables hospitality companies to reduce capital expenditures (CapEx) and operating expenditures (OpEx).

Following are the most common security use cases that hospitality organizations face, along with the different Fortinet solutions that form the basis of each.

**65% of hospitality security breaches originate with POS systems.[9]**

### Headquarters Network Cybersecurity

Hospitality headquarters consist of various systems that include back-office operations, reservations, point of sale (POS), guest services, on-demand entertainment, and building controls, among others. Cyber threats pose serious concerns for hospitality organizations that often store personally identifiable information on guests in their reservation and guest management systems for months or even years. This can pose problems with industry and government regulations such as GDPR and PCI DSS.

But cyber risks extend beyond data theft and exposure for hospitality organizations, including ransomware and distributed denial-of-service (DDoS) attacks that can take down everything from physical building systems, to guest services applications, to ecommerce applications. The impact can be significant—ranging from lost revenue, diminished guest experiences, damaged brand, and even physical safety.

Digital innovation is pushing many hospitality organizations to adopt multiple clouds for applications and services, expand their wireless access points, and increasing use of Internet-of-Things (IoT) devices. The realities of a hybrid IT infrastructure include Software-as-a-Service (SaaS) applications and Infrastructure-as-a-Service (IaaS) services across multiple clouds. This requires a comprehensive, integrated security solution consisting of elements such as FortiGate NGFW, FortiWeb web application firewall (WAF), FortiNAC network access control (NAC) for identifying, controlling, and securing all the devices connected to the network, FortiAuthenticator for simplifying identity management, and FortiInsight user and entity behavior analytics (UEBA) for insider threat protection.

**While more than 25% of cyberattacks will target IoT by 2020, less than 10% of IT security budgets will be spent to protect these devices.[10]**

For management and reporting, FortiManager, FortiSIEM, and FortiAnalyzer combine to deliver transparency across every security element and consolidated notifications and alerts that help the network operations center (NOC) and security operations center (SOC) teams to proactively identify, remediate, and resolve network and security events.

### Hospitality Location Cybersecurity

The property is the visible face of the organization to customers. Guests expect secure, dependable, high-performance access to services such as Wi-Fi and on-demand entertainment. Disruptions or security breaches will negatively impact the organization's reputation.

For the business to function, on-site staff needs secure access to corporate resources residing in the data center and multiple clouds. Because payment card information is frequently exchanged between POS devices on location and at headquarters, a multitude of IoT devices are deployed to enhance the guest experience, and guests are accessing the network using their own unsecure devices, there are multiple types of endpoint devices that need to be secured. All of this needs to be secured without an on-site security expert.

Exacerbating the issue is the fact that cyber criminals are attracted to hospitality locations due to the relative affluence of the patrons and perceived ease of breaching the network. Other times the hospitality location may not be the attacker's end goal; they may breach a location's network as a foothold to move laterally until they reach headquarters. Fortinet Secure software-defined wide-area network (SD-WAN) offers hospitality organizations a robust, integrated, and automated approach to achieving the visibility and centralized configuration and security management needed across their distributed branch network.

Fortinet Secure SD-Branch provides secure isolation of business and guest networks and delivers unified access control to protect IoT devices from attack. Using Fortinet Secure SD-Branch extends the full benefits of the Fortinet Security Fabric to the distributed branches. Secure SD-Branch is comprised of FortiGate NGFWs, FortiNAC network access control, FortiSwitch, and FortiAP to deliver consolidation of branch services for network edge and device edge protection.

Endpoints such as in-room entertainment systems are of interest to cyber criminals and create new points of vulnerability. FortiClient is an integrated endpoint security agent that provides pattern-based anti-malware, behavior-based exploit protection, web filtering, and an application firewall. It also provides secure remote access with a built-in virtual private network (VPN), a single sign-on solution, and two-factor authentication.

### Secure Guest Wi-Fi

High-performance wireless access is a basic guest expectation. Poorly functioning Wi-Fi diminishes the experience for leisure and business travelers alike. Wi-Fi performance aside, public Wi-Fi networks are a common target for hackers, as they are relatively easy to penetrate. Once they have gained access to a network, cyber criminals can steal valuable data from a hospitality company, including everything from financial and credit card data to user passwords.

FortiAP allows hospitality sites to run multiple side-by-side guest and business service setup identifiers (SSIDs) isolated and secured by a FortiGate NGFW, which delivers full traffic inspection to protect guests without sacrificing performance. FortiAP enables administrators to centrally manage network traffic security inspection, provides a captive portal with social media integration, and enables URL filtering and rogue access point detection. Additionally, the deep-packet inspection (DPI) feature of FortiGate provides sites with insight into their guests' browsing habits. FortiNAC is also a requisite for identifying all devices trying to connect to the network and then controlling their access. When combined with FortiPresence, organizations can boost the guest experience with personalized real-time offers and measure their effectiveness (Figure 3).

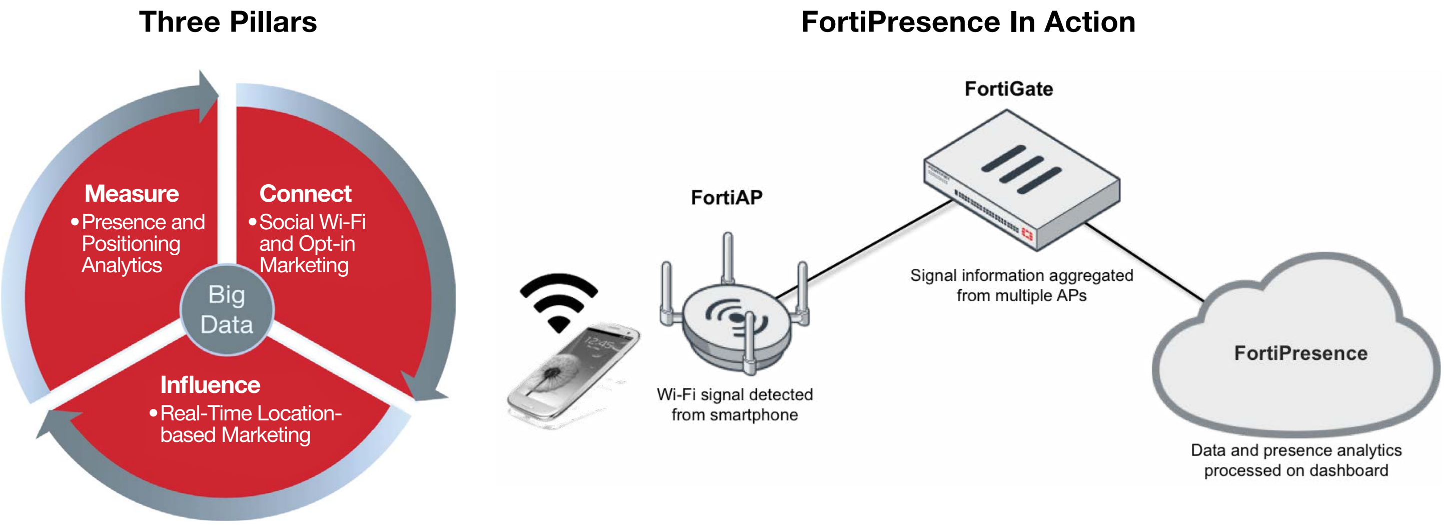
Three Pillars
Measure
• Presence and Positioning Analytics
Connect
• Social Wi-Fi and Opt-in Marketing
Big Data
Influence
• Real-Time Location-based Marketing
FortiPresence In Action
FortiGate
FortiAP
Signal information aggregated from multiple APs
Wi-Fi signal detected from smartphone
FortiPresence
Data and presence analytics processed on dashboard

Figure 3: FortiPresence helps engage customers and potential customers to improve the guest experience and drive revenue.

### Hospitality Branch Networking

As hospitality organizations often have multiple locations, the needs of individual properties can vary greatly. For example, some locations may not require guest Wi-Fi access, whereas others do. Others may even have IoT devices connected to the network that must be secured. Additionally, with communications flowing between different locations, including headquarters, minimal latency is required.

Traditional WANs that rely on multiprotocol label switching (MPLS) route traffic through the data center and the dramatic influx in SaaS, Voice over IP (VoIP), and video traffic creates significant latency that impacts end-user productivity. SD-WAN is seen as a means to solve this performance problem by using the public internet instead.

Yet, many SD-WAN solutions lack the security capabilities needed to protect devices, traffic, and applications on their branch networks. FortiGate Secure SD-WAN offers organizations the ability to deliver SD-WAN through one integrated solution. And with the industry's only SD-WAN ASIC processor and integrated capabilities such as application awareness steering, FortiGate SD-WAN gives hospitality organizations unparalleled performance and scale; this includes dramatically better performance than other options when secure sockets layer (SSL)/transport layer security (TLS) encryption inspection is turned on.

**FortiGate Secure SD-WAN has a TCO 8x better than competitive offerings and can be deployed in under six minutes, as verified by NSS Labs, a leading third-party test laboratory.[12]**

### Advanced Threat Protection

Given their relatively affluent customer base, the length of time credit card numbers remain in guest management systems, and their broad attack surface, hospitality organizations are a prime target for hackers. Bad actors are embracing new technologies such as AI, which enables them to increase the volume and velocity of their attacks, as well as increases their ability to execute unknown attacks and use zero-day exploits.Indeed, up to 40% of all threat traffic and over three-quarters of successful attacks are comprised of unknown and zero-day attacks.[11] The execution of these attacks—from exfiltration of data to manipulation and disruption of operations—happens in minutes versus days or weeks.

As hospitality organizations have a broad and dynamic attack surface, defending and protecting against these advanced threats is not easy. In addition to an integrated security infrastructure, some of the same advanced technology strategies employed by cyber criminals are needed. This is where the Fortinet Security Fabric and FortiGuard Labs threat intelligence, which uses AI to perform rapid threat analysis and classification, are key differentiators. Other Fortinet security technologies also employ AI and ML capabilities to perform data aggregation, reconciliation, and analysis for real-time detection, prevention, and response.

FortiSandbox enables organizations to pinpoint zero-day exploits and unknown threats in a safe, isolated environment and to share that information across the entire Security Fabric. FortiDeceptor uses decoys to lure attackers into revealing themselves before they can steal data or execute commands that disrupt operations. FortiInsight addresses the threat of insiders by using AI and ML to continually monitor users and endpoints for noncompliant, suspicious, or anomalous behavior and share that information across the Security Fabric to affect real-time response.

**As much as 40% of all threat traffic and over 75% of successful attacks are comprised of unknown and zero-day attacks.**

**Dynamic Cybersecurity for Multi-cloud Environments**

Cloud adoption is rapidly expanding across industries, and hospitality is certainly not immune. Rather than building and maintaining IT systems or managing commercial off-the-shelf systems on-premises, hospitality organizations are turning to SaaS applications. And for IT infrastructure, they often elect to use IaaS—including from multiple cloud service providers.

The Fortinet Security Fabric, with FortiGate NGFWs at its center, offers hospitality companies an integrated set of technologies and a dynamic cloud security approach that breaks down silos between applications and services—whether they are hosted on-premises or in different private and public clouds. This provides transparent visibility and centralized policy controls that streamline operations for overstretched security and network teams while improving risk management.

Core capabilities from Fortinet include FortiCASB cloud access security broker (CASB) that enables hospitality organizations to extend advanced security controls across SaaS and IaaS, consolidating threat intelligence from each cloud, intelligently monitoring traffic within and between clouds, and delivering robust reporting and analysis. FortiCWP cloud workload protection (CWP) gives security and DevOps teams the ability to evaluate and monitor cloud security configurations, analyze traffic across cloud resources, and evaluate cloud configuration against best practices. FortiWeb protects cloud-based critical web resources from advanced persistent threats. For organizations running cloud-based email systems, FortiMail affords a secure email gateway to protect email systems—including hybrid email approaches that run email on-premises and in the cloud.

## Fortinet Differentiators for Hospitality Industry Cybersecurity

Though others could be cited, the following are key differentiators when Fortinet solutions for hospitality are compared to other technology options:

### High performance

The FortiGate Security Fabric uses automation and orchestration to ensure maximum protection with minimal manual intervention. FortiGate Secure SD-WAN boosts performance through instant identification and intelligent routing. Branch network performance is enhanced by simplifying security and compliance risk management workflows using Fortinet SD-Branch.

### Flexible integration

The Fortinet Security Fabric is based on an open ecosystem that unifies security solutions and enables them to work together in real time. Fabric APIs, Fabric Connectors, and DevOps Scripts encourage integration and connection between platforms for seamless management. This helps hospitality organizations to integrate their IoT investments across headquarters and all of their branch locations.

### Secure connectivity

Fortinet Secure SD-Branch extends the power of the Fortinet Security Fabric to the branch, enabling reliable, high-speed, secure connections between hospitality locations and the headquarters network with centralized visibility and control. Other technologies such as FortiAP and FortiPresence ensure a safe and reliable guest Wi-Fi experiences.

### Intent-based segmentation

Intent-based segmentation in FortiGate NGFWs enables organizations to shrink the attack surface and to build network access and zones based on business logic and regulatory requirements. In addition to making it more difficult for cyber criminals to exploit vulnerabilities, intent-based segmentation prevents east-west lateral movement across the network.

### Proactive threat intelligence

FortiGuard Labs threat intelligence, along with various integrated Fortinet technologies such as FortiWeb, FortiInsight, and FortiClient, uses AI and ML capabilities to stay ahead of cyber criminals. These capabilities enable hospitality companies to stretch overburdened security and network teams while sustaining a proactive risk approach that keeps them ahead of bad actors and their use of unknown threats and zero-day exploits.

## Conclusion

The Fortinet Security Fabric provides broad, integrated, and automated network security covering a hospitality organization's entire attack surface—from the main campus to the network perimeter to the data center to any number of cloud deployments. Fortinet technologies also support industry-specific needs such as high-performance, secure guest Wi-Fi experiences, in-room entertainment systems, and online reservation systems.

With centralized visibility and control of the entire network and network security architecture, hospitality organizations can move from a reactive security stance to a proactive one. With actionable threat intelligence, security teams can confidently set policies based on knowledge rather than guesswork. And with a fully integrated architecture, organizations can fully automate a wide range of security response and monitoring activities, enabling timely response to advanced threats and the most strategic use of network security talent.

[1] "2018 travel and hospitality industry outlook," Deloitte, 2018.

[2] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[3] "Quarterly Threat Landscape Report: Q4 2018," Fortinet, February 2019.

[4] "2019 Data Breach Investigations Report," Verizon, accessed November 8, 2019.

[5] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO, March 14, 2016.

[6] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens," (ISC)$^2$, 2018.

[7] "The Security Architect and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, November 12, 2019.

[8] Ibid.

[9] "2018 Thales Data Threat Report—Retail Edition," Thales, accessed November 2019.

[10] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed March 21, 2019.

[11] "Advanced Threats: Keeping CISOs on Their Toes: Increasingly Complex Tactics by Adversaries Can Put Security Teams in Reactive Mode," Fortinet, September 21, 2019.

[12] Ahmed Basheer, "Software-Defined Wide Area Network Test Report," NSS Labs, June 19, 2019.

FORTINET®

www.fortinet.com