PROTECTING HOTELS AND GUESTS WITH THE FORTINET SECURITY FABRIC

WHITE PAPER

EXECUTIVE SUMMARY

The hospitality industry is seeing healthy growth, but it is also seeing a growing threat landscape that threatens that growth. 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 sandbox analysis to detect and remediate unknown threats.

HOTELS NEED SX

The hospitality industry is currently enjoying healthy growth as properties compete for customers with a variety of enhancements to the guest experience. Like most organizations, hotels and hotel chains are expanding their digital footprint, and many now find their data and applications scattered across multiple clouds. At the same time, the current threat landscape features huge increases in malware volume[1]—and increasing percentages of the total are unknown or zero-day threats.[2] On top of that, attacks are now moving at machine speed, with the result that manual threat response is no longer adequate.[3]

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

- From perimeter security to **broad coverage** across the expanded attack surface
- From siloed security to an **integrated security architecture**
- From manual threat response to **automated detection and response**

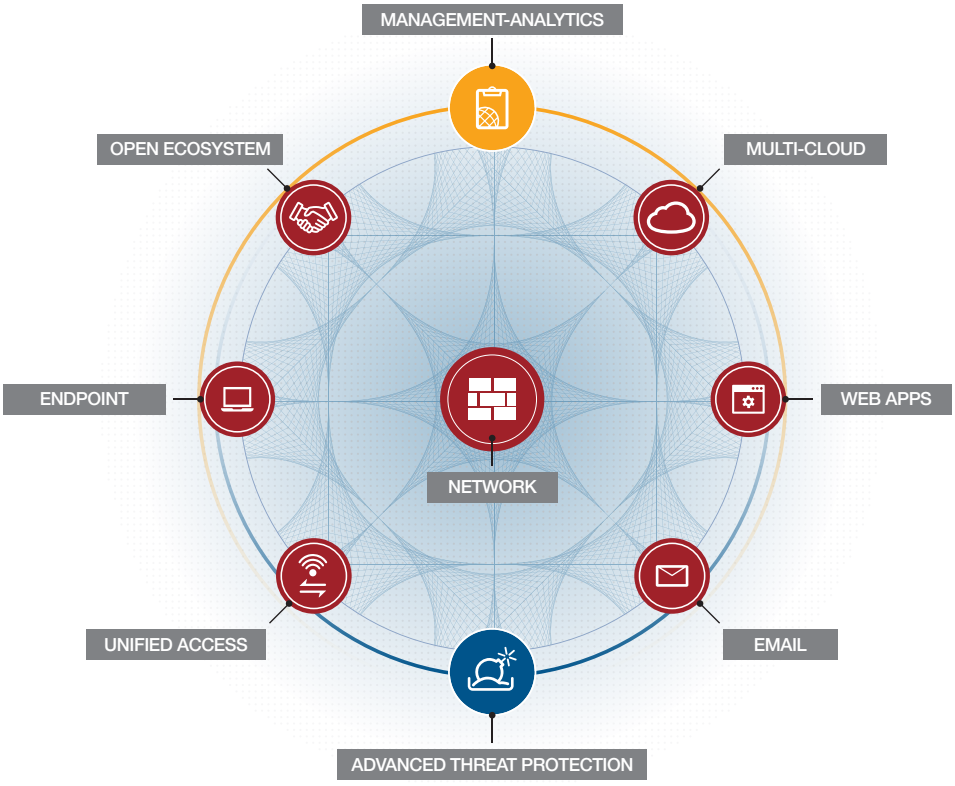
85% of CISOs say security is a major barrier to digital transformation.[4]

THE FORTINET SECURITY FABRIC ENABLES SX

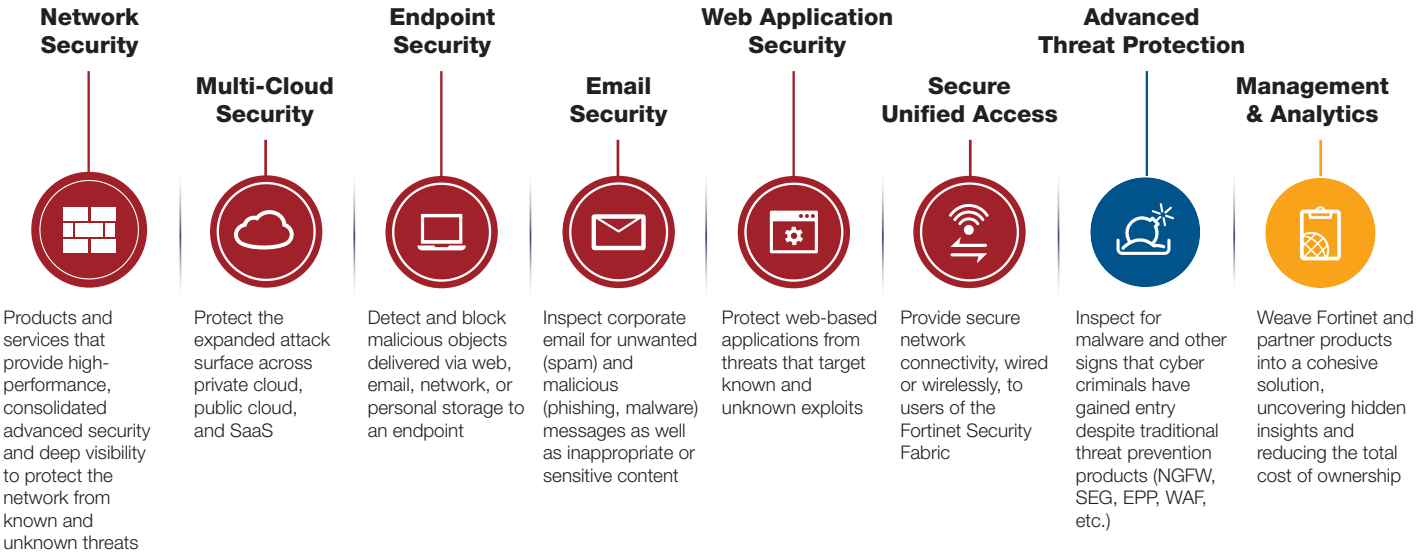
The Fortinet Security Fabric consists of a comprehensive set of network security technologies that work together and are supported by a single source of threat intelligence. The Security Fabric enables an organization to achieve true SX:

- **Broad protection**, with the ability to protect every part of an organization's expanded attack surface, from multiple clouds to Internet of Things (IoT) and mobile devices.
- **An integrated security architecture** that enables transparent visibility and centralized control from a single pane of glass.
- **Automated threat detection and response** using advanced AI and ML techniques to identify unknown threats by their characteristics and respond at machine speed.

The different elements of the Fortinet Security Fabric allow protection to be expanded over time in accordance to the customer's technology and business requirements—without ripping and replacing the underlying architecture or relying on nonintegrated point products. It also enables the integration of third-party security solutions from dozens of Fortinet Fabric-Ready Alliance Partners that have developed connectors using Fortinet's open API. This flexibile approach to integration makes for a proactive approach to security that dynamically adapts to the evolving threat landscape and organizations' increasingly complex IT Infrastructure.



THE FORTINET SECURITY FABRIC INTEGRATES ALL ASPECTS OF NETWORK SECURITY FOR CENTRALIZED VISIBILITY AND CONTROL.



THE FORTINET SECURITY FABRIC DELIVERS BROAD PROTECTION FOR AN ORGANIZATION'S ENTIRE ATTACK SURFACE.

THE FABRIC DELIVERS BROAD SECURITY

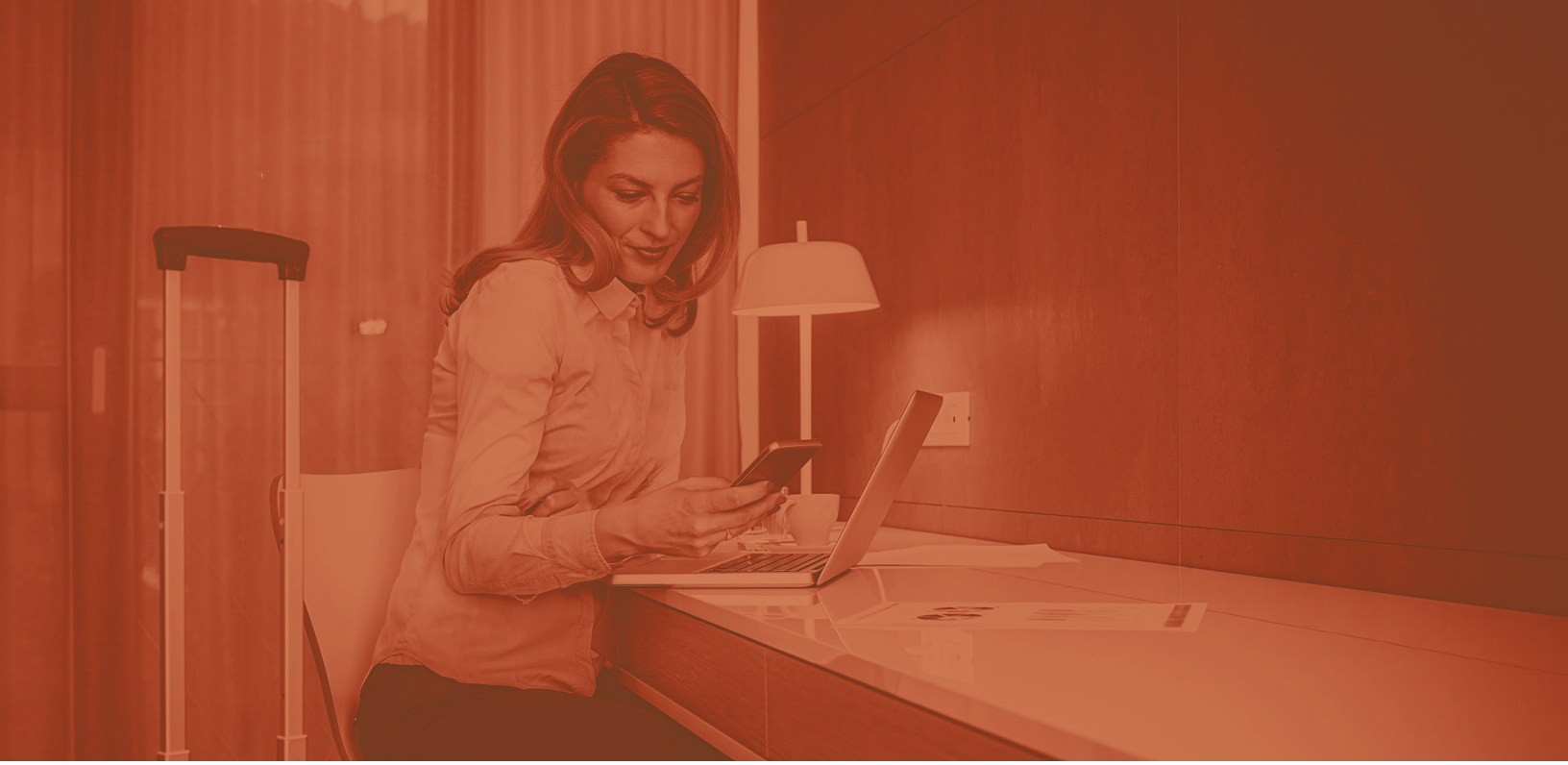
The different elements of the Fortinet Security Fabric cover an organization's entire attack surface with broad and integrated security protection. This coordinated, multilayer approach enables automation of security practices and a proactive stance on network security. These are the primary elements of the Security Fabric:

- **NGFWs.** The Security Fabric is built around FortiGate NGFWs, which utilize purpose-built security processors and threat intelligence from FortiGuard Labs to deliver protection against advanced threats. While prior generations of firewalls focused on protecting the perimeter of a data-center infrastructure, FortiGate NGFWs protect the entire attack surface, from on-premises infrastructure, to multiple clouds, to IoT devices.

  FortiGate is available in appliance, virtual machine, and cloud formats. It includes built-in intrusion prevention, web filtering, anti-malware, and application control. And it integrates seamlessly with all of Fortinet's other security solutions and many third-party ones, so that stakeholders can have an enterprise view of the entire security architecture in real time. Internal segmentation capabilities can be used to prioritize critical services and provide them with additional protection without degrading performance.

- **Multi-cloud security.** Native integration with all the major cloud providers enables the different parts of the infrastructure to talk to each other and for threat intelligence to be shared throughout. It also enables each cloud provider's built-in security solutions to be integrated into the Security Fabric as needed for complete protection. Whether an organization uses public cloud, private cloud, or hybrid cloud approaches—or a combination of the three—Fortinet ensures that the same policies, practices, and response protocols are applied across the infrastructure.

- **Endpoint security.** Endpoints are of increasing interest to cyber criminals because of the proliferation of IoT and mobile devices on corporate networks—many of which do not have adequate security at the device level. For example, in-room entertainment systems can be vulnerable endpoints in hotels. 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.



- **Email and web application security.** Web applications and email systems have long been favorite targets of hackers because they provide access to valuable information and are relatively easy to exploit—whether with malware or with DDoS attacks. At hospitality organizations, booking systems are often cloud-based these days. The FortiWeb web application firewall (WAF) protects critical cloud-based applications from advanced persistent threats using shared intelligence from the Security Fabric. And the FortiMail secure email gateway applies similar protection from advanced threats targeting the email system.
- **Secure unified access.** FortiAP wireless access points and FortiSwitch devices work seamlessly with the FortiGate NGFWs to extend robust network security from the network core to the access layer and make secure Wi-Fi possible for both guests and employees. The solution offers three distinct deployment options, giving hotel chains the flexibility to choose the option that best fits their wireless requirements. Furthermore, it ensures business continuity by providing 100% connectivity uptime to operations via 3G/4G cellular backup with FortiExtender.

46% of travelers say that in-room Wi-Fi is a "must have" amenity.[5]

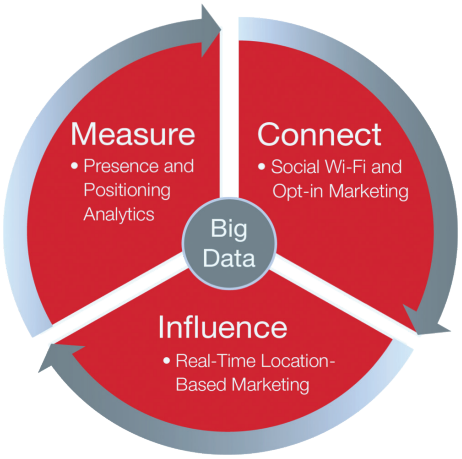
- **Advanced threat protection.** Given the expanded attack surface at digital enterprises and the increasing sophistication of attacks, a hotel's network security must be supported by the best threat intelligence delivered in real time. FortiGuard Labs maintains one of the world's largest networks of more than 3 million threat sensors. Detailed analysis of potential threats by FortiSandbox filters threats as they come in and adds to the global threat intelligence network that supports the Fortinet Security Fabric.

  In addition to sandboxing, FortiGuard Labs analysts have maintained a self-evolving detection system (SEDS) known as FortiGuard AI for more than six years. FortiGuard AI uses advanced AI and ML techniques that train the system to adapt to changes in the threat landscape and become more accurate over time at detecting advanced and unknown threats. Intelligence from FortiGuard AI is available at machine speed via automatically generated signatures across the Fortinet Security Fabric. Response can then be automated according to policies set by the organization.
- **Management and analytics.** Fortinet management and analytics solutions provide simplified, centralized administration of the Fortinet Security Fabric solutions and actionable information on an organization's current security posture. The FortiSIEM security information and event management solution actually enables the consolidation of the security operations center (SOC) and network operations center (NOC) functions with a single pane of glass. This breaks down the barrier between NOC and SOC, giving hotel organizations a comprehensive view of their entire network so that threats can be identified and addressed quickly. Furthermore, Fortinet analytics solutions help manage and monitor compliance, increase application availability, and save IT resources.

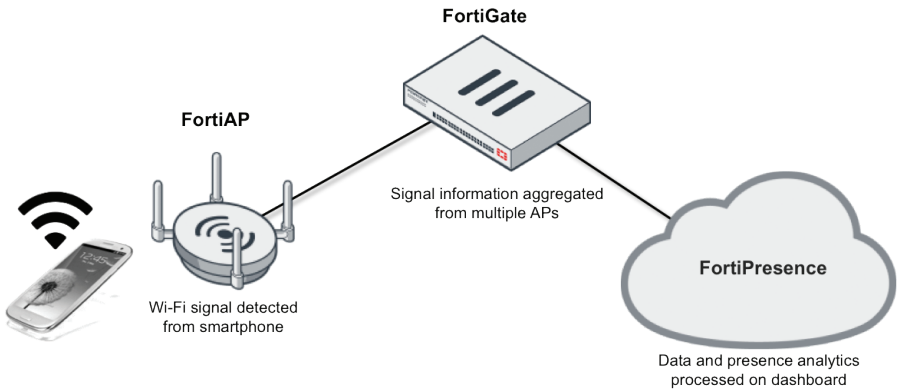
- **Secure SD-WAN.** A large percentage of organizations are evaluating SD-WAN, and many are deploying it in 2018. While a traditional WAN that routes all network traffic through the data center and makes exclusive use of expensive multiprotocol label switching (MPLS) circuits to all branch locations, SD-WAN makes use of the public Internet when it provides the most efficient route. This improves network performance—especially for branch locations and remote users accessing cloud resources—but also expands the attack surface beyond the security infrastructure of the data center. The FortiGate secure SD-WAN solution enables hotel chains to securely improve network performance at individual properties.
- **Presence analytics.** Improving the guest experience helps hotels differentiate themselves and can drive additional revenue. Online bookings can be tracked so the hotel owner knows what customers are interested in, and can deliver targeted marketing. With FortiPresence, hotel organizations can now track and influence the buyer's experience with a unique combination of statistical analytics and a sophisticated customer engagement engine, including social Wi-Fi while guests are onsite, to influence buying decisions, increase booking sizes, and attract new customers.

74% of firms conducted SD-WAN trials in 2017, and many are deploying it this year.[6]

Three Pillars



FortiPresence in Action

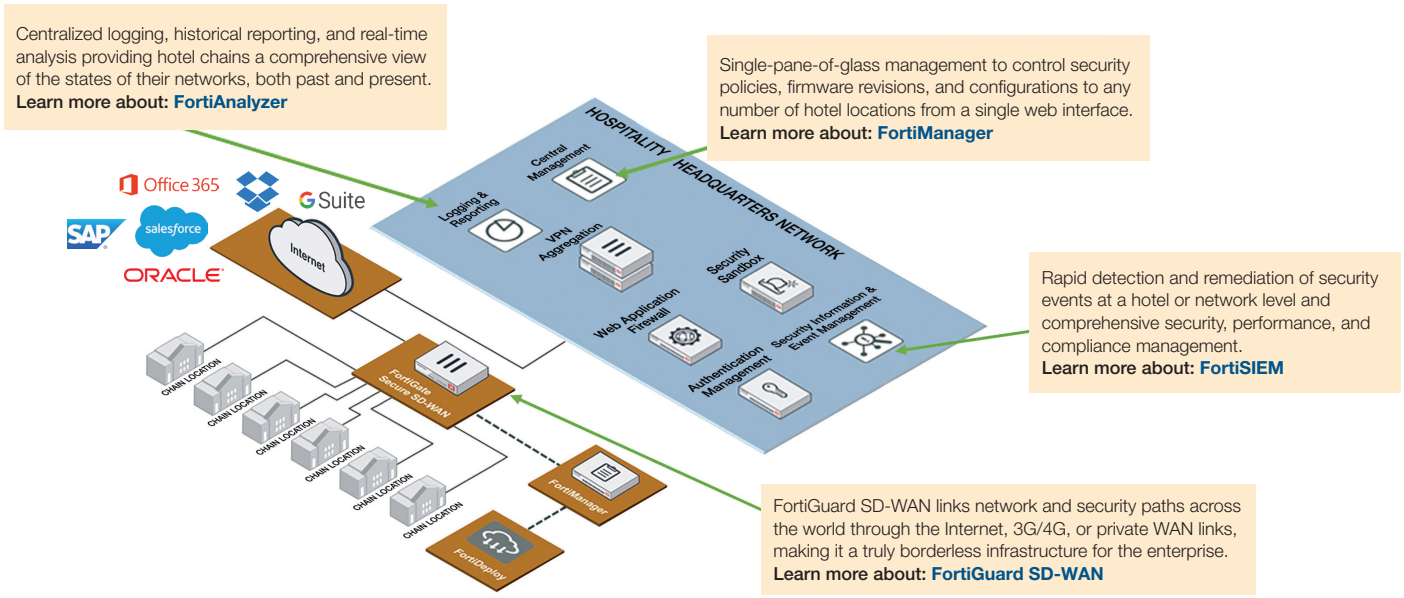


FORTIPRESENCE HELPS ENGAGE CUSTOMERS AND POTENTIAL CUSTOMERS TO IMPROVE THE GUEST EXPERIENCE AND DRIVE REVENUE.

RECOMMENDED ARCHITECTURE COVERS HEADQUARTERS AND INDIVIDUAL PROPERTIES

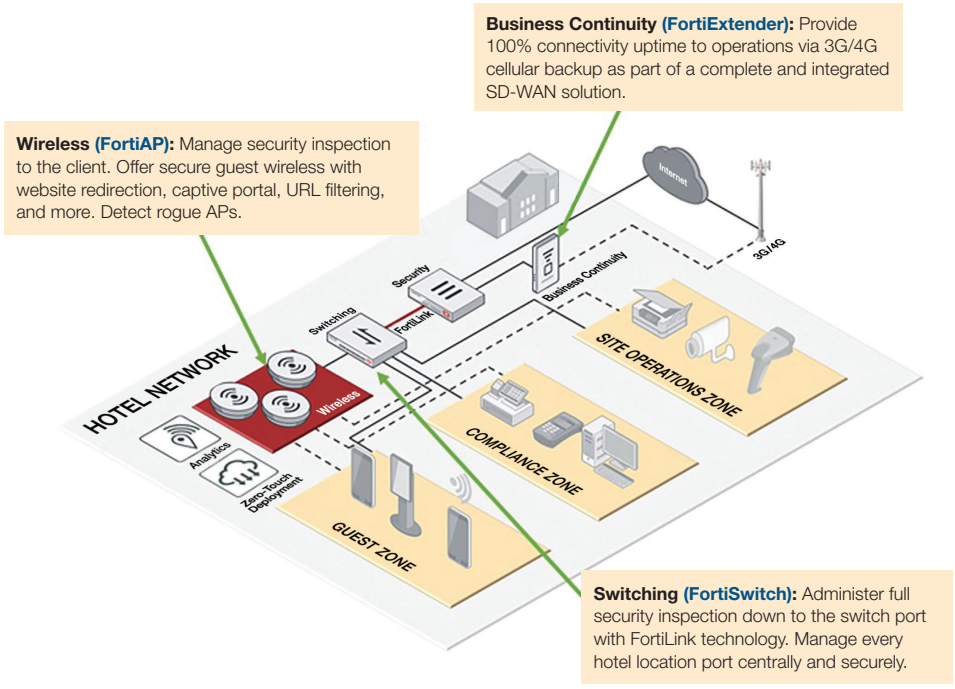
For hotel chains, the Fortinet Security Fabric can protect both the headquarters infrastructure and individual properties—whether corporate-owned or franchised—and facilitate communication and intelligence sharing between the two.

- **Headquarters network.** For hotel chains that have a central headquarters, the Fabric enables centralized control of remote locations—whether traffic moves on a traditional WAN or SD-WAN. Security administration, sandboxing, and other security functions would take place at the headquarters data center.



THE ARCHITECTURE OF A TYPICAL FORTINET SECURITY FABRIC DEPLOYMENT AT A HOTEL CHAIN'S HEADQUARTERS.

- **Individual property network.** The infrastructure at individual properties enables secure guest Wi-Fi, site operations, business continuity, and compliance monitoring.



THE ARCHITECTURE OF A TYPICAL FORTINET SECURITY FABRIC DEPLOYMENT AT AN INDIVIDUAL HOTEL.

CONCLUSION

The Fortinet Security Fabric provides broad, integrated, and automated network security covering a hospitality organization's entire attack surface—from cloud to data center. The solution allows for industry-specific needs such as securing guest Wi-Fi, in-room entertainment systems, and reservation systems, and provides flexibility on the exact way the solution is architected.

With centralized visibility and control of the entire network and network security architecture, 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] "Threat Landscape Report Q2 2018," Fortinet, accessed September 12, 2018.

[2] According to analysis by FortiGuard Labs, zero-day malware makes up 28% to 40% of all malware on a given day.

[3] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[4] "Security Implications of Digital Transformation Report," Fortinet, July 26, 2018.

[5] Jelisa Castrodale, "Hotel guests use Wi-Fi within seven minutes," USA Today, April 6, 2016.

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

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
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

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

249763-0-0-EN

October 16, 2018 10:32 AM

wp-hospitality-security-fabric