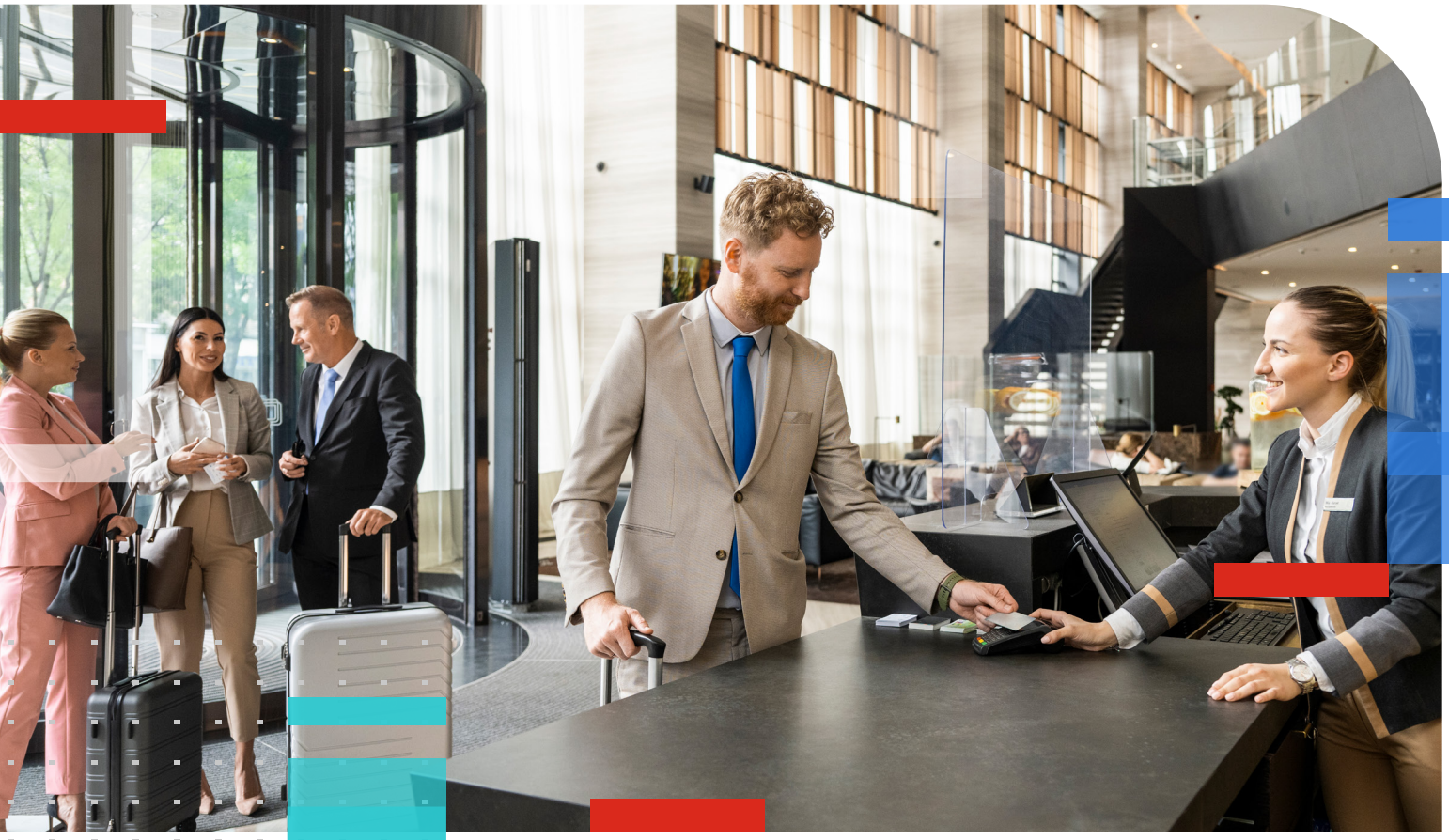
WHITE PAPER

Securing the Always-On Guest Experience

The Fortinet Security Fabric Protects Hospitality with Converged Network and Security



Executive Summary

Modern hotel operations rely on various digital assets to support an evolving guest engagement model and create operational efficiencies through back-of-house automation. Guests today demand frictionless experiences and tight integrations that create seamless engagement during their stays. Organizations within the hospitality sector are rapidly adopting new capabilities, such as contactless check-in, artificial intelligence and machine learning (AI/ML)-based tools like computer vision, occupancy sensors, integration with on-site stores and single-pay services, comprehensive guest wireless options, and location-aware services. These new tools help eliminate mundane tasks, increase operational efficiencies, and establish visibility for new cybersecurity controls. This in turn allows human staff to focus on creating exceptional customer experiences, such as precise delivery of food and drink to a hotel's pool area while directly supporting broader guest loyalty programs and direct-to-consumer marketing opportunities.

From ransomware to data breaches, the hospitality industry has been a prime target for cyberattacks in recent years, and things seem to be getting worse.[1]

But while the hospitality and gaming industry has embarked on a massive digital transformation journey to remain competitive and enhance sustainability, these new functions and capabilities have created network infrastructure complexity that is amplifying other critical business challenges. This includes needing to support connections for a growing diversity of devices, issues with staff hiring and retention, and increasing cyberattacks across the broader hospitality ecosystem that target the valuable personally identifiable information (PII) of guests. Complexity is the enemy of both efficiency and security. The Fortinet Security Fabric offers an integrated platform that simplifies networking and security while offering seamless protection for today's critical hospitality use cases.

Today's Hospitality Industry Challenges

The hospitality industry has experienced some unique challenges over the past 36 months, including side-effects of rapid digitization, staffing shortages, and evolving guest expectations.

Providing and protecting the always-on guest experience: Guests no longer simply accept the role of technology in their experiences and transactions; they actually demand it. They expect a measure of empowerment in the form of mobile and self-service technologies, such as mobile reservations, mobile and kiosk check-in and check-out, and mobile room keys.

Guestroom technologies today depend on reliable, secure connectivity. If hotel properties lose connectivity to essential services, guests will notice, and that can have long term brand reputational harm. Resiliency, security, and reliability are paramount in any modern hospitality environment. Understanding the needs of systems and services and then implementing a solution that provides these key attributes is what allows hoteliers to continue to run their businesses.

Guest interactions may now occur from anywhere, at any time, not just while on-site. Preference tracking can enhance personalization that elevates guest experiences. But adding these capabilities can create additional challenges. All systems need to be connected and visible in order to provide a unified commerce ecosystem that guests can leverage, while at the same time supporting potential direct-to-consumer marketing opportunities. Organizations are only as strong as the weakest link in this chain.

Guest connectivity: Ample wireless availability remains perhaps the most critical factor in determining a positive guest experience. Rooms must be capable of accommodating the connectivity demands of families that travel with multiple devices per person. With ever-increasing bandwidth consumption needed to support all the new guest services that come with digitization, what was good enough three years ago isn't good enough today.

In addition, the rise of the hybrid workforce and increasing business leisure travel have significantly added to these connectivity burdens. Seamless videoconferencing capabilities are now a mainstay of virtually every industry. Whether guests are traveling for professional or personal reasons, they won't stay at locations where they cannot also perform remote work duties as needed.

To make matters worse, increasing wireless traffic offers expanded opportunities for cybercriminals to intercept sensitive data or disrupt services. Secure guest connectivity is more important than ever before.

Explosion of IoT and connected devices: Hoteliers are seeing immense benefit in deploying connected Internet-of-Things (IoT) devices to gain visibility into areas they never had access to before, helping to ensure convenience, cleanliness, and safety for guests. Some examples are building management systems, deployed technologies in guest conference centers, as well as some point of sale payment terminals for store-in-store locations, restaurants, and other retail transactions. It also includes smart IoT environmental controls that help organizations conserve resources and improve sustainability of operations.

At the same time, IoT technologies can introduce vulnerabilities to hospitality networks from across their digital supply chain, and most devices include little-to-no built-in security of their own. Hospitality security leaders need visibility to identify all IoT connections on the network and microsegmentation capabilities to stop attacks from moving laterally across the network from a compromised device.

Employee satisfaction: While network infrastructure is expanding to keep up with higher guest expectations and bring new business capabilities, the hospitality industry as a whole is also facing staffing shortages.[2] Though many sectors have shown recovery from recent job losses, the hospitality industry remained down 6.7% from pre-pandemic levels (more than 1.1 million jobs) at the end of 2022.[3] These shortages include skilled IT staff needed to manage all the new digital technologies and secure new threat exposures, placing both the organization and guest privacy at risk.

On top of general staff shortages, high employee turnover is an issue at the location level in terms of impact on customer experiences as well as introduction of insider risks (both malicious and unintentional). With the hospitality industry's elevated churn rate, new employees must be continually hired and trained, costing the organization both time and money. Supporting the next generation of hospitality workforce means reducing the burdens of mundane tasks and doing more to make their work feel meaningful. Improving retention will require better engagement, refining communications expectations with younger staff, and being able to onboard new colleagues in a timely manner.

Network and security challenges in hospitality

- Ever-evolving guest expectations, including a reliable, "always-on" network experience
- Rapid rate of hotels adopting new technologies
- Support for a growing number and diversity of device connections
- Evolving property management systems and integrations
- High turnover of staff increases risk of insider threats both unintentional and malicious
- Economic considerations (no security team has an infinite budget)

Securing the guest experience from advanced threats

All combined, these challenges can amplify one another through increasing complexity, too many changes, too many risks, and not enough hands to help untangle things. When it comes to protecting the organization and guests from cyberthreats, infrastructure complexity is especially important to understand. Complexity is the enemy of security, and this problem is only going to intensify over time. In fact, over half (56%) of hospitality IT leaders cite cybersecurity as one of their C-suite's top-three business concerns, ahead of issues such as inflation (52%), retaining and hiring talent (48%), and supply chain and logistics management (50%).[4]

Despite this awareness, security is often an afterthought when deploying a new technology, and many silos exist within network and security groups across the hospitality sector. This leads to several different cyberthreat exposures:

- **Data theft:** Attacks where sensitive information (including guest PII data) is compromised by an outsider attacker or even a malicious insider.
- **Ransomware and malware:** Sophisticated phishing attacks can introduce malicious code to your network, which can then exfiltrate sensitive data and disrupt operations.
- **Supply chain:** Cyberthreats throughout the broader hospitality ecosystem (such as vendors and suppliers) can be nearly as disruptive as an in-house attack.

The consequences of a successful attack can be damaging to organizations of any size, with the average hospitality industry data breach costing nearly $3 million.[5] And a mere 37% of hospitality professionals report feeling fully prepared to respond to cybersecurity attacks and threats.[6]

A Platform-Based Security Approach

One of the top-three security issues reported by hospitality organizations today is a lack of visibility of vulnerabilities across all infrastructure.[7] To address this critical problem, organizations need to simplify and consolidate their infrastructures. An integrated security platform can provide comprehensive security capabilities while elegantly converging network access into the infrastructure. This approach enables broad visibility and protection across the entire digital attack surface.

In terms of specific security capabilities, the platform should combine next-generation firewalls (NGFWs), wireless access points (APs), access switches, and wireless wide area networking (WAN) gateways. This kind of solution integration eliminates security management complexity while enabling security and networking to work together as a unified ecosystem. It also supports automated functions that help streamline things like compliance reporting processes. A platform-based approach can also share threat intelligence from across the network and leverage global threat feeds that dynamically update throughout the day for real-time protection against emerging threats and attacks.

Less than half (37%) of hospitality professionals say they are fully prepared to respond to cybersecurity attacks and threats.[8]

Finally, an integrated platform reinforces security at critical points across the broader organization:

- **Protection for any edge and any app at scale:** Advanced threat protection, network and security convergence, secure sockets layer (SSL) decryption, and network automation
- **Complete and simplified access layer security:** Direct and integrated control, configuration, and management, which extends the NGFW to the local area network (LAN) edge; a converged platform for the IT network and operational technology (OT) systems for business management
- **Secure, business outcome-driven WAN:** Reduced cost and complexity, better application performance, and integrated security
- **Control of every device on every network:** Simplify network deployment, automatically discover devices, and apply policies at scale, including IoT and guest devices

Why Fortinet

Fortinet enables the hospitality and gaming industry to offer the best possible guest experiences by providing a complete secure networking solution throughout the entire guest journey. The Fortinet Security Fabric supports digital transformation and consolidation that allows you to quickly and safely scale all aspects of your operations when needed to meet demand and offer the latest amenities at pace. It establishes unified visibility and helps enforce consistent, policy-based controls across all parts of your network infrastructure, including IoT, smart devices, and connected OT systems, such as fountain controls at large casinos.

Secure networking for every location: To ensure the always-on customer experience, Fortinet SD-Branch includes software-defined wide area networking (SD-WAN) capabilities, which dynamically distributes branch and remote location traffic across multiple WAN links. This provides cost-efficient branch connectivity to resources in the corporate data center and in the cloud. Fortinet delivers fast, scalable, and flexible secure SD-WAN for cloud-first, security-sensitive, and global enterprises.

SD-Branch combines FortiGate NGFWs, FortiAP access points, FortiSwitch switches, and flexible 5G, LTE, and Ethernet connectivity with FortiExtender. It provides full unified threat management capabilities, including anti-malware and intrusion prevention. It also supports network segmentation and microsegmentation for policy enforcement at the access level and visibility into east-west network traffic to prevent lateral movement of threats. This in turn helps retailers meet strict PCI DSS compliance requirements.

Protection against advanced threats: The Fortinet Security Fabric provides a foundation for establishing a zero-trust network. It enables you to rapidly adjust your security posture to defend against newly discovered attacks across an ever-expanding attack surface. The Fortinet Security Fabric combines a comprehensive suite of solutions that cover a wide range of threats, such as malware, phishing, and ransomware. This ensures that your organization is protected across all stages of the attack cycle.

It also includes endpoint security to protect devices that are connected to networks and prevent cybercriminals from accessing sensitive guest PII. FortiEDR endpoint detection and response provides transparent visibility across all endpoints, including guest devices, point-of-sale systems, ATMs, kiosks, and IoT products.

Advanced threat intelligence: Breaches are on the rise. Eighty-four percent of organizations experienced one or more cybersecurity intrusions in the past 12 months (up from 80% from last year).[9] FortiGuard Labs uses advanced AI/ML capabilities to generate threat intelligence that is shared via the Fortinet Security Fabric in real time to keep all parts of the security infrastructure aware of the latest attack variants for rapid detection and responses. In addition, FortiAnalyzer enhances security across physical, virtual, and cloud environments using analytics-based detection that drives faster responses to cyber risks.

The global cost of cybercrime was estimated at $8.4 trillion dollars in 2022 and is expected to surpass $20 trillion by 2026.[10]

Simplified management: Fortinet provides a single, unified platform for managing IT, IoT, and OT access functions. This enables comprehensive visibility of all business management systems with proper signatures. FortiManager allows you to manage multiple locations and departments from a single dashboard with limited IT staff.

Fortinet security solutions are designed to be easy to manage, so businesses can focus on business instead of IT complexity. The Fortinet Security Fabric platform helps you to operate with a high level of automation, save time with zero-touch deployment, and gain networkwide visibility and control from a single pane of glass, on-site to the cloud or multiple clouds.

Hospitality Use Cases and Benefits

The Fortinet platform supports critical use cases specific to the challenges of today's hospitality industry:

- **The always-on experience:** Fortinet ensures your guest experiences can be delivered without interruption, while securing the latest amenities and digital capabilities.
- **Secure networking:** The Fortinet Security Fabric tightly integrates network infrastructure and security architecture, enabling the network to scale and change without compromising security.
- **Instant business agility:** With security at the core, your network can evolve, expand, and adapt without concerns that a new edge, gap, or blind spot could compromise operations.
- **Hyper-scale device control:** Control every device on every network and simplify network deployment. Fortinet automatically discovers new devices and applies security policies at scale, including IoT and guest devices.

Fortinet also provides several key benefits for security leaders in hospitality organizations, including:

- **Protecting the guest experience:** Bring new guest experiences online without compromising security. Protect any edge and any application at scale with advanced threat protection, convergence of network and security, SSL decryption, and network automation.
- **Ensuring secure, reliable connectivity:** Get complete and simplified access layer security with direct and integrated device control, configuration, and management by extending NGFW protection to the LAN edge. Network access control capabilities ensure that only authenticated users and authorized devices that are compliant with security policies can enter the network.
- **Simplifying operations:** Ensure that your business systems run perfectly every time for guests while reducing the training and management burdens on human staff. Secure, business outcome-driven WAN reduces costs and operational complexity, provides better application performance, and simplifies infrastructure through integrated security capabilities.

Retailers Around the World Choose Fortinet

Comprehensive cybersecurity is essential for protecting the hospitality and gaming industry from the latest cyberthreats across an ever-expanding attack surface. It also helps ensure the frictionless, always-on experience your customers expect. The integrated Fortinet Security Fabric platform provides consistent, dependable, and secure network experiences to retail organizations around the world. Globally, 680,000+ businesses trust Fortinet with their security, making FortiGate the world's most deployed network security solution.

[1] "This is personal: Cybersecurity and the hospitality industry," HLB, June 16, 2022.

[2] "Persistent Hotel Staffing Shortages 'Alarming' But Offer Opportunity," Business Travel News, March 24, 2023.

[3] "Leisure & Hospitality Employment Update," U.S. Travel Association, October 2022.

[4] "Research: 56% of Hospitality IT Leaders Cite Cybersecurity As a Top Business Concern," Hotel Technology News, September 28, 2022.

[5] "Cost of a Data Breach Report 2022," IBM, July 2022.

[6] "Research: 56% of Hospitality IT Leaders Cite Cybersecurity As a Top Business Concern," Hotel Technology News, September 28, 2022.

[7] Ibid.

[8] Ibid.

[9] "2023 Cybersecurity Skills Gap," Fortinet, March 2023.

[10] "Estimated Cost of Cybercrime Worldwide," Statista, November 2022.

[11] "The Secure Network Journey," Fortinet, August 2023.

September 27, 2023 4:29 PM

2342631-0-0-EN