Solution Brief

Security
Intelligent Venues

Intelligent Venues Deliver Security-Enabled Guest Experiences with the Fortinet Security Fabric

Security-driven networking powered by Fortinet Secure Processing Units (SPUs) and Intel® technology offers a multi-layered security approach to protect the expanding attack surfaces of intelligent venues.

Cutting-edge technologies are driving intelligent venues

Businesses and civic organizations are creating next-generation intelligent venues by harnessing cutting-edge technologies like edge computing, 5G, and the Internet of Things (IoT). They are also connecting operational systems for gains including energy-efficiency.

With the Fortinet Security Fabric, IT and operations teams benefit from a set of solutions that protects distributed networks as a single system. Gartner states that by moving from multiple point security solutions to a cybersecurity mesh architecture like the Fortinet Security Fabric, organizations can help reduce financial losses from cybersecurity attacks by 90 percent.[1]

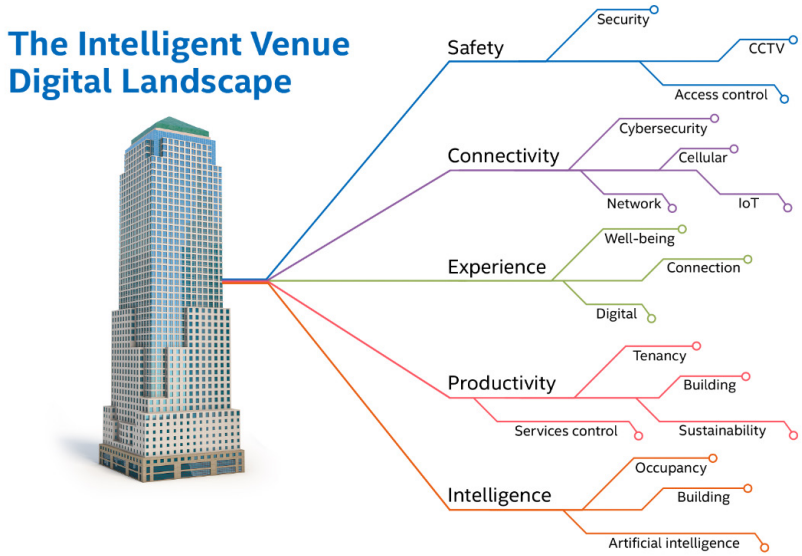

Figure 1. Adding devices and connecting systems expands the attack surface of intelligent venues

At an intelligent stadium, hotel, or museum, each visitor enjoys a frictionless and immersive experience. Guests leave with lifelong memories, and venue owners can count on return visits and customer loyalty. The bottom line is a higher return on investment (ROI).

To add intelligence, venues start by connecting devices. These could be IoT sensors, cameras, or even customers' mobile phones. Venues also build out modern, connected operational technology (OT) systems with the goal of delivering energy-efficient options. But with these changes, the attack surface expands. Heating, ventilation, and air conditioning (HVAC) sensors, safety and security systems, and mobile devices all become potential targets. Using increasingly automated and innovative digital methods, bad actors have more opportunities to break in and disrupt businesses.

To counter the threat, venues must evolve their concept of a "network perimeter." In today's intelligent venues, open applications and data move freely across multiple network edges, flowing to and from mobile phones, IoT sensors, cameras, and more. Security needs to be *everywhere*.

One approach is to deploy point solutions. Venues might procure one solution for the HVAC system, another to protect the guest experience software, and a third to protect Wi-Fi networks. But each point solution requires management overhead and specialized knowledge. This increases complexity dramatically, and ultimately, this approach becomes unsustainable.

Fortinet and Intel offer a better way

Fortinet and Intel have collaborated to offer an alternative. The Fortinet Security Fabric, powered by Fortinet SPUs and Intel technologies, weaves together physical and digital security technologies from each company to scale security enforcement. Because the Fortinet Security Fabric makes use of best-in-class processor technologies, it delivers comprehensive security without affecting the performance of devices or systems.

The following three intelligent venue use cases illustrate the benefits of how the Fortinet Security Fabric:

- Aims at detecting threats and helps enforce security everywhere
- Is designed to close security gaps and reduce complexity
- Helps enable faster time to prevention and shorter mean time to resolve (MTTR)

Intelligent stadium

An intelligent stadium offers wide expanses of attack surfaces that extend from the stadium all the way to a guest's home, via their mobile phone. Additionally, intelligent stadiums are attractive targets for bad actors looking to make a political statement.

Scenario: A football fan leaves his comfortable couch to attend a game, lured by the promise of an immersive, connected experience. He receives player status updates on his phone on the way to the game, is assigned a parking spot close to his entrance, purchases concessions with a cashless transaction, and even uses an augmented reality (AR) application on his phone to superimpose himself within the game for posting to social media. Wayfinding applications on digital signs minimize lines at the concession stand, and connected OT systems in the restroom optimize lighting and electricity usage to minimize operational expenses. Safety systems monitor the environment for hazards to help ensure that everyone gets home safely.

Security challenges:

- Deliver a customer experience that is free from the worry of identity theft, data loss, and hacking.
- Know what's on the network and why it's there. Identify any vulnerabilities that can open doors to the entire network.
- Protect against ransomware and sophisticated hacks, including those attempted by politically motivated bad actors, that might disrupt operations, damage a company's reputation, or lead to large financial losses.

Solutions:

The Fortinet Security Fabric, powered by both Fortinet SPUs and Intel technologies, offers a portfolio of solutions to address these challenges. The core of Fortinet Security Fabric consists of FortiGate Next Generation Firewall (FortiGate NGFW). FortiGate NGFW provides deep visibility and security in a variety of form factors, including virtual firewalls and appliances. FortiGate NGFW also delivers fast, scalable, and security-enabled software-defined wide area network (SD-WAN) solutions on-premises and in the cloud. These SD-WAN solutions can be used in intelligent stadiums to request fast, scalable, and flexible connectivity among different network environments. Fortinet's security-enabled networking approach uses one operating system and consolidates SD-WAN, FortiGate NGFW, advanced routing, and Zero Trust Network Access (ZTNA) application gateway functions. FortiGate NGFW and SD-WAN offer intelligent stadiums:

- Artificial intelligence (AI)-powered security that scales to stadium-size venues
- The ability to see applications, users, and devices—even when encrypted—to help detect and prevent threats
- Connectivity and protection at any edge and at any scale, with support for SD-Branch, SD-WAN, and 5G

Other Fortinet solutions that benefit intelligent stadiums include FortiNAC, Fortinet's network-and-access-control solution powered by Intel® Xeon® Scalable processors. With FortiNAC, intelligent stadium teams can control device access—a critical step in helping secure stadium networks.[2]

FortiNAC also simplifies onboarding and management of IoT devices from HVAC sensors to motion detectors. It can be used with Intel® Secure Device Onboard (Intel® SDO) service, an automated cloud-independent service that enables a device to be provisioned onto a network in seconds.[3]

Intelligent hospitality

An intelligent hotel with an attached casino is an attractive target for fraud and identity theft because of its high volume of financial transactions. The business itself could also be a ransomware target. And the physical building must be kept safe from fire and water damage.

Scenario: A guest checks into her hotel wirelessly and enters her assigned room using the loyalty application on her mobile phone. She enjoys a personalized experience—restaurant reservations, dry-cleaning services, and a spa package—based on an analysis of her past stays at the hotel. In the background, smart OT systems minimize electricity and water usage to lower operational expenses, while safety systems monitor for physical threats like fire and flooding.[4] Later that evening, the guest receives a personalized offer for a casino gambling package on her phone, so she visits the casino to play blackjack after dinner.

Security challenges:

- Help secure the information of guests using loyalty applications and Wi-Fi networks.
- Monitor devices that are on the network, and proactively identify both external and internal vulnerabilities.
- Protect against breaches into casino point-of-sale systems.

Solutions:

Intelligent hotels and casinos also benefit from the Fortinet Security Fabric powered by both Fortinet SPUs and Intel technologies. Again, FortiGate NGFW with fast and secure SD-WAN solutions plays a major role within Fortinet Security Fabric. Intelligent hotels and casinos use FortiGate NGFW with Intel Xeon processors and SD-WAN solutions to:

- Avoid breaches and business disruptions by minimizing ransomware and other cyberattacks.
- Deliver security at hyperscale to keep up with business growth.
- Deliver seamless user experience and operational efficiency with automated security at any location.

Intelligent hotels and casinos can also use analysis tools like FortiSIEM, which brings that data together for a comprehensive view of security and availability. This tool is also powered by Intel Xeon processors, and it helps identify insider and incoming threats that might pass traditional defenses.[5]

ISVs enhance security solutions for intelligent venues

ISVs that build software solutions for intelligent venues on top of Fortinet Security Fabric solutions powered by Intel Xeon Scalable processors can enhance protection even further by using additional Intel technologies:

- **Intel® Software Guard Extensions (Intel® SGX):** Helps protect data in use via unique application-isolation technology
- **Intel® Deep Learning Boost (Intel® DL Boost):** Takes AI performance to the next level to identify patterns and trends
- **Intel® Advanced Vector Extensions 512 (Intel® AVX-512) Vector Neural Network Instructions (VNNI):** Boosts deep learning (DL) performance for intrusion detection and analysis

Intelligent museum

An intelligent museum is an attractive attack target because numerous visitors potentially expose their data when they make purchases in the museum store and take guided tours using mobile device applications. The art itself is a valuable target for theft and must also be protected from environmental damage, such as from water and heat.

Scenario: A family visits a local smart museum and enjoys an immersive multimedia experience interacting with the art exhibits. The French Impressionist exhibit is monitored by IoT sensors both to prevent theft and to identify physical threats like water leaks. Throughout the museum, connected OT systems optimize air quality, lighting, and energy use. At lunch, the family eats in the museum's restaurant and pays through a cashless transaction. While visiting the museum's store, each parent receives a personalized offer within the museum's loyalty application.

Security challenges:

- Keep contact information, demographic details, and donation records of visitors and patrons secure.
- Constantly monitor systems and devices to identify any security vulnerabilities.
- Monitor collections and exhibits to prevent theft or environmental damage and maintain overall building and occupant security.

Solutions:

Intelligent museums can make use of Fortinet Security Fabric portfolio solutions starting with FortiGate NGFW and SD-WAN solutions. FortiNAC and FortiSIEM, both powered by Intel Xeon processors, provide access control and threat monitoring and identification.

Fortinet and Intel collaboration enables high-performance security

Fortinet and Intel have a long history of enterprise security leadership. Fortinet's unparalleled networking and security solutions, and Intel's high-performance processors and other components, can help secure intelligent venue networks and aim to deliver seamless, immersive guest experiences. Fortinet Security Fabric offers venue owners opportunities to support reduced operational expenses and improve energy efficiency, while simultaneously helping build customer loyalty, supporting brand reputation, and helping increase innovation—all while helping extend security wherever it needs to be.

Get started with Fortinet today. Visit fortinet.com/solutions/industries.

[1] Fortinet. "Fortinet Security Fabric." May 2022. fortinet.com/solutions/enterprise-midsize-business/security-fabric.
[2] Fortinet. FortiNAC Datasheet. fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf.
[3] Intel. "Intel® Secure Device Onboard." intel.com/content/dam/www/public/us/en/documents/product-briefs/intel-secure-device-onboard-product-brief.pdf.
[4] Sans Analyst Program. "Next-Generation Cybersecurity Smart Buildings." Sponsored by Fortinet and Dragos. October 2021. fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-sans-next-gen-cybersecurity-smart-buildings.pdf.
[5] Fortinet. FortiSIEM Datasheet. May 2022. fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf.

Printed in USA 1222/SMR/PRW/PDF Please Recycle 348490-001US