SOLUTION BRIEF

Protecting Smart Buildings with the Fortinet OT Security Platform

EXECUTIVE SUMMARY

Attacks on Internet-of-Things (IoT) devices now make up roughly 33% of infected devices, according to The Association of Foreign Real Estate Investors (AFIRE).[1] This is deeply concerning news for builders, owners, operators, and tenants of smart buildings that rely heavily on connected devices to help optimize energy usage, operational efficiency, and preventive maintenance in addition to improving occupants' well-being and satisfaction. AFIRE specifically notes that connected elevators, smart heating, ventilation, and air conditioning (HVAC) meters, printers, coffeemakers, interactive kiosks, and other seemingly innocuous connected devices became cybercriminal favorites in 2020[2] and continue to be targeted today. A growing number of commercial, corporate, and residential properties feature this kind of smart infrastructure enabled by connected IoT devices. While digital transformation offers significant benefits to owners and occupants, smart buildings also require digital connections. This gives bad actors a larger attack surface at the very same time a growing skills gap has made recruiting and retaining expert cybersecurity personnel a critical challenge.

The Fortinet OT Security Platform offers commercial, corporate, and residential smart-building owners the industry's highest-performing cybersecurity platform. It offers full visibility, controlled access, and robust threat detection and response while still achieving all the benefits that smart-building technology delivers. Fortinet's combination of proven, scalable security equipment, deep knowledge, and skilled personnel creates a comprehensive, manageable security environment from RFP, design, and deployment through the entire life cycle.

Growth and Challenges of Smart Buildings

A "smart building" is a building with infrastructure attached to the internet or IoT devices deployed in the building, such as utility meters, HVAC systems, elevators, vending machines, and building information management systems (BIMS), to name a few. These systems leverage data, communications networks, physical equipment, and automation to enhance building operations and tenant experiences. They also use a blend of IT for dealing with the flow of data and information and OT, which deals with the control and management of physical processes. This blend means that smart buildings also present a unique, expanded set of security challenges that must be solved, especially as this market continues to grow. The global smart-building market size is projected to grow from $96.96 billion in 2023 to $408.21 billion by 2030, at a CAGR of 22.8%.[4] As the use of smart-building infrastructure and devices increases, so does the likelihood of more attacks and the potential for two expensive, dangerous outcomes.

Smart buildings: A wide scope of attacks

- **Ransomware, India:** Hackers demanding payment took control of a hotel's lighting, heating, and air conditioning systems.
- **Malicious operation, Finland:** Hackers created a fire risk by causing a smart building's heating system to overheat.
- **Data breach, United States:** Hackers behind a massive Target data breach entered through the company's HVAC system.[3]

When physical meets cyber

Transforming typical building infrastructure into smart infrastructure requires the integration of physical and cyber. There is no longer protection via “air gaps” or “security by obscurity.” OT and IT systems have an interdependence that improves the service. But the ability for malicious actors and intruders to control physical components such as elevators, lighting, HVAC systems, or building security systems creates new risks with serious consequences.

A larger attack surface

With the digital transformation that drives the growth of smart buildings, the intersection between the physical and cyber increases the size of the attack surface. Connected components on a network, such as surveillance cameras, occupancy sensors for lighting, keyless entry readers, and HVAC systems, become new potential entry points for bad actors. Because buildings are becoming more digital and the technology is relatively new, builders often don’t staff required expertise to add cybersecurity controls to protect these technologies. Contamination of the supply chain with components already embedded with malware is also a real threat.

Increased external threats

Because infiltration of smart buildings can threaten life (such as in hospitals and healthcare facilities) or even national security if a restricted-access premise is breached, they are attractive targets. Nation-states and hacktivists want to cause socio-political disruption or steal sensitive intelligence, while other cybercriminals are looking to profit by holding data or essential building services like lighting or HVAC for ransom.

> *“Smart buildings are the future of architecture, but their success depends on robust cybersecurity measures that protect both the building’s occupants and the infrastructure that supports them.”* [6]
>
> — **Michael Kaiser,** Executive Director of the National Cyber Security Alliance

With commercial, corporate, and residential structures continuing to evolve through digital transformation into smart buildings, Fortinet helps builders, owners, and operators overcome these unique security challenges by delivering cybersecurity protection at scale, legacy-system protection, enhanced compliance, and security as a service. The Fortinet OT Security Platform also offers futureproofing as this sector continues modernizing and new innovations are incorporated to keep ahead in the competitive real estate industry.

Cybersecurity for Smart Buildings

To thrive throughout digital transformation, building owners and operators relying on smart technologies need to rethink their security posture and move toward a seamless, comprehensive, and zero-trust cybersecurity strategy for their smart infrastructure. The Fortinet cybersecurity platform unifies the best of current IT network security capabilities with an in-depth understanding of the OT security requirements including applications and protocols and offers:

- **Visibility:** FortiNAC network access control (NAC) and FortiGate next-generation firewall (NGFW) provide comprehensive visibility into the network by continuously monitoring and analyzing traffic, user behavior, and device activities. This visibility helps identify potential security threats and vulnerabilities in real-time, ensuring proactive threat mitigation. FortiNDR network detection and response (NDR) offers deep visibility into network vulnerabilities, threats, and malicious network behavior through its patented artificial intelligence and machine learning (AI/ML) techniques. FortiNDR can integrate with Fortinet or third-party security solutions to support response and remediation actions for any detected network anomalies.

- **Secure Networking:** FortiGate serves as the cornerstone of the network infrastructure, offering advanced firewall, intrusion prevention system (IPS), virtual private network (VPN), and secure software-defined wide area network (SD-WAN) capabilities. FortiAP access point and FortiSwitch secure network switch provide secure wired and wireless connectivity while FortiManager, a central management and policy orchestration platform, centralizes network management—making it easier to configure, monitor, and maintain the network infrastructure. FortiAnalyzer, a centralized network analysis and troubleshooting solution, offers centralized logging, monitoring, and reporting capabilities and includes tailored compliance reports mapped to well-known cybersecurity frameworks.
- **Zero Trust Network Access:** Zero trust network access (ZTNA) ensures secure access to applications or devices hosted anywhere, whether users are working remotely or in the offices. FortiNAC, FortiAuthenticator, and FortiPAM play vital roles in ZTNA implementation. FortiNAC enforces strict access policies based on user and device identities, ensuring that only authorized users and devices can access network resources. For enhanced security, FortiToken provides multi-factor authentication (MFA) and can integrate with FortiAuthenticator for single sign-on. FortiPAM combined with FortiClient provides role-based access control and privileged access management capabilities to roll out zero-trust across internal and external users and critical systems at scale so that the users are restricted based on their roles and can perform their activities securely and safely.
- **Endpoint Detection and Response:** A smart infrastructure has an increased number of endpoints and securing these endpoints is critical to ensure end-to-end security. FortiEDR, an endpoint detection and response solution, is an essential part of the Fortinet Security Fabric that can detect and respond to suspicious behavior or threats across a large number of endpoints, minimizing the risk of security breaches in the smart infrastructure.

The Fortinet OT Security Platform is tailored to meet the security requirements of smart buildings. It encompasses a broad portfolio of security solutions, covering detection, prevention, containment, and recovery. Implementation of the Fortinet OT Security Platform assures both providers and users that the cybersecurity requirements for smart infrastructure are met. This includes addressing security audit requirements from regulators and demonstrating compliance. Likewise, the security architecture team can trust that the smart infrastructure adheres to industry-compliant security implementation. Ultimately, the Fortinet OT Security Platform offers an end-to-end security solution.

Enhancing Cyber Resilience Through the Fortinet OT Security Platform

With its breadth and depth, the implementation of the Fortinet OT Security Platform ensures that critical operational resources and data are protected from cyberthreats. As a result of this security implementation, business activities and services remain uninterrupted, and occupant safety and comfort are maximized. Fortinet supports the key outcomes that building owners and operators utilizing smart infrastructure need most, including:

- **Maintaining Reliability:** Cyberattacks can shut down vital equipment such as keyless entry systems, lighting, elevators, and climate control. Attacks can also expose sensitive data or lead to a loss of control over building management systems. All of these risks affect a building owner or operator’s ability to deliver the experience customers rely on. Fortinet’s commitment to constantly delivering updated threat identification and protection mitigates the risk of disruptions due to cyberattacks like ransomware and security breaches.
- **Ensuring Compliance:** According to Finantrix, the cybersecurity regulatory landscape in the real estate sector is likely to evolve as technologies advance and threats increase in sophistication.[5] There are serious protections with penalties in place around data privacy. Fortinet both simplifies regulatory reporting and supports standards-based security implementation for smart buildings.
- **Managing Reputational Risk:** Smart building owners and operators who don’t take security seriously risk severe institutional and personal damage to the reputations of those involved in theft of sensitive information or accidents due to cyber intrusions. Partnering with Fortinet, a respected industry leader in cybersecurity, helps mitigate the exposure to reputational risk due to cyber-driven data breaches or disruption of systems and services.

Through a comprehensive and scalable security technology platform, Fortinet can secure smart buildings and related infrastructure, catering to entities of all sizes—from the smallest independent organizations to the largest public operators. Regardless of the size or extent of smart infrastructure, Fortinet offers cybersecurity for every user, system, and network.

Fortinet OT Security for Smart Buildings

Building owners and operators are under immense pressure to increase sustainability, reduce carbon footprints, and ensure that occupants are kept comfortable and safe at all times. Smart building technology is an exciting way to improve quality of life and optimize operations while reducing environmental impact, but digital transformation comes with increased security challenges.

The Fortinet OT Security Platform protects modern and legacy systems by scaling to meet all needs in an approach that provides the equipment, knowledge, and expert personnel to create a comprehensive security environment for smart-building owners and operators. Fortinet has been rated by Westlands Advisory as the sole leader in the 2023 IT/OT Network Protection Platforms Navigator,[7] and delivers broad, integrated, and automated digital security for all infrastructure innovations.

[1,2] Noelle Brisson and Michael Savoie, "Get Smart: Developing a Holistic Approach to Risk Management for Smart Buildings," AFIRE, October 18, 2022.

[3] "Cyber Security and Smart Buildings," #smartcities, April 16, 2023.

[4] "Smart Building Market Size, Share & COVID-19 Impact Analysis," Fortune Business Insights, accessed November 23, 2023.

[5] "Ensuring Safety in Smart Buildings: The Importance of Cybersecurity and Automation," Waylay, March 14, 2023.

[6] "Smart Buildings and Cybersecurity Threats," Finantrix, August 4, 2023.

[7] "Fortinet Recognized as the Sole Leader in the Westlands Advisory 2023 IT/OT Network Protection Platforms Navigator™," Fortinet, July 27, 2023.

www.fortinet.com

February 2, 2024 7:59 PM

123456-0-0-EN