BlastWave

SOLUTION BRIEF

AI-Resistant Cybersecurity for Building Management

Operational Technology Challenge for Building Management

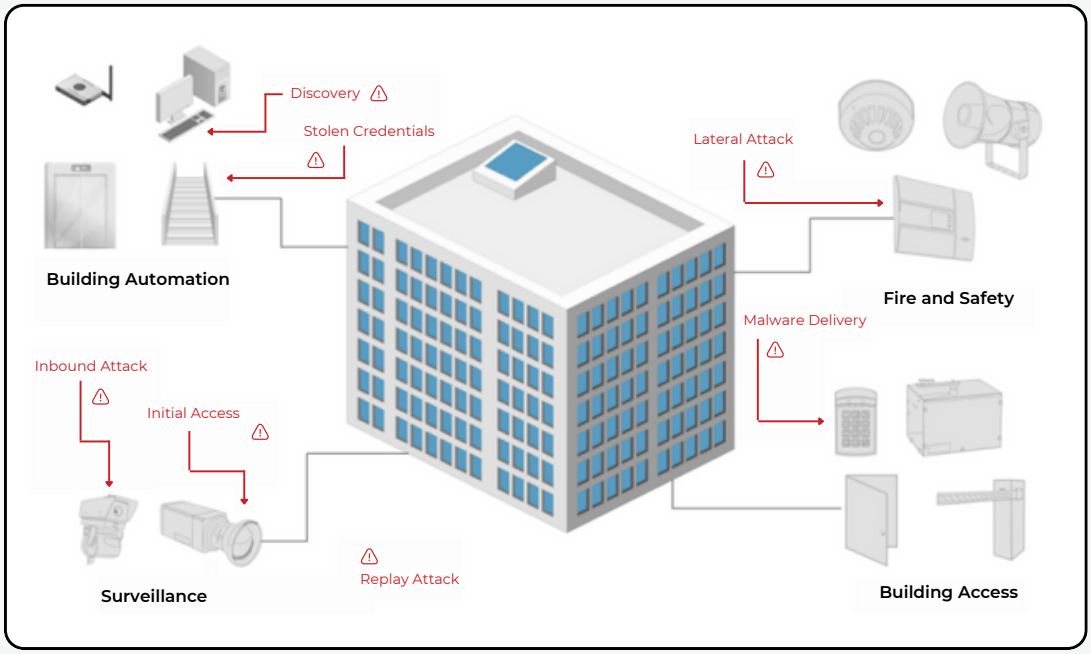
Smart Building's potential to enhance productivity, optimize energy usage, and streamline processes has positioned it as a growth market for the future. Reports and Data forecast that the global Smart Building market will surge to $189 billion by 2030 from $72.6 billion in 2021. The Building Automation System (BAS) poses a significant vulnerability for smart buildings as it controls critical functions such as heating, ventilation, lighting, security, and air conditioning. Interconnectivity among lighting, climate, and elevator systems in smart buildings often lacks robust security protocols.

The increased number of entry points for hackers expands the attack surface, rendering businesses within smart buildings more susceptible to cyber threats. In smart buildings, the seamless functioning of interconnected systems heavily relies on a diverse range of IoT devices for communication. Disturbingly, fifty-seven percent of IoT devices are susceptible to medium- or high-severity attacks, making them attractive targets for malicious actors. Poorly controlled remote access is a common vulnerability in BMS, as demonstrated by the Target hack in 2013. Access through an HVAC contractor account allowed hackers to obtain credit and debit card data for over 110 million accounts without directly attacking the POS.

BlastShield Advantages:

- Reconnaissance-Proof Software Defined Perimeter to prevent device discovery and vulnerability exposure with Network Cloaking
- Phishing-Resistant Biometric Multifactor Authentication for Regulatory-Compliant Secure Remote Access
- Delivers Least Privilege Access Policies and prevents Lateral Movement with Network Microsegmentation

Figure 1: Cyberthreats in Building Management



BlastShield™: AI-Resistant OT Security For Building Management

One clear need in Building Management is to separate IT and OT security solutions. The IT solutions for building management are constantly reconfiguring with new tenants joining and leaving and new devices connecting to the network constantly. Strong network segmentation ensures that no IT security vulnerabilities can be used to access the OT networks.

Real-time OT Secure Remote Access is also a mandatory requirement for effective building management. Granting and revoking access for temporary maintenance contractors and ensuring that they only have access to the devices that they are repairing is crucial, as shown by the Target hack.

The entry point to most BAS is the Building Management Systems (BMS). BlastShield protects these systems from the outside world, introducing a software-defined perimeter incorporating a zero-trust architecture. With BlastShield, IT organizations gain secure remote access, network segmentation, and network cloaking, rendering critical systems undiscoverable to attackers and mitigating the risk of unauthorized access.

Network Cloaking

Network Cloaking ensures critical building management systems become invisible to external threats. Rather than just obfuscating these systems, they do not appear in any scans or probes from a hacker. BlastShield ensures strong OT cybersecurity for building management environmental and access control infrastructure. With Network Cloaking, AI-enhanced reconnaissance tools cannot probe the internal workings because they have no path to reach the internal OT networks from the IT network. This is crucial, as IT compromises are likely with so many people accessing the IT networks from systems with known vulnerabilities. Network cloaking proactively secures systems, making them invisible to potential attackers by blocking all internet access for legacy OT systems. It also creates a virtual air gap for OT systems that do not need access to the internet by only allowing them a hidden private address.

Secure Remote Access

BlastShield provides OT Secure Remote Access to critical building management systems, ensuring OT managers can monitor and manage them without exposing them to cyber threats. BlastShield's phishing-resistant MFA biometric authentication protects against GenAI-powered phishing attacks and MFA hijacking. A full mesh of P2P encrypted tunnels is created to secure traffic from remote users to the data center facility and any agent-enabled systems, protecting against Man-in-the-middle attacks. Policy changes take effect in real-time, facilitating dynamic and flexible policy enforcement during emergencies or administration changes. This is a mandatory capability for Secure Remote Access in a highly dynamic BMS environment.

Network Segmentation

BlastShield exceeds traditional segmentation by advancing the concept of microsegmentation as a superior security alternative. Unlike broad segmentation strategies, microsegmentation allows for incredibly detailed control, segmenting networks down to the level of individual devices, systems, protocols, or users. By isolating network segments, BlastShield effectively prevents the lateral movement of threats within the network, a critical defense mechanism against external and internal threats. Unlike many solutions that use ACLs and VLANs, microsegmentation scales effortlessly to large OT environments. BlastShield's microsegmentation solution is innovative and future-ready for network security.

About BlastWave

BlastWave prevents AI-powered cyber attacks on critical infrastructure with a unique combination of Zero Trust Cybersecurity capabilities and delivers industrial-grade security with consumer-grade ease-of-use. Visit www.blastwave.com to learn more