Zero Trust OT Cybersecurity Protection for Building Management

BlastWave secures building management OT networks by eliminating the root causes of cyberattacks, like password vulnerabilities and network visibility, ensuring uninterrupted operation of critical systems like HVAC and security. We provide robust, yet easy-to-use Zero Trust protection, enabling secure remote access and operational efficiency, so you can focus on creating safe and comfortable building environments. Building management customers would choose BlastWave to protect their OT networks for these critical reasons:

Phishing-resistant Secure Remote Access: Passwordless secure remote access for employees, maintenance personnel, and vendors eliminates credential theft as an initial attack vector.

Protection of Legacy Systems: Enforces a "virtual air gap" for legacy building automation systems (BAS) that cannot be easily updated, mitigating vulnerabilities and reducing the attack surface of smart buildings,

Prevents Unauthorized Control of Building Management Systems: Zero Trust architecture prevents unauthorized access to building control systems, reducing the risk of malicious manipulation that result in risk for tenants.

Compliance with Building Security Standards: BlastWave deployment can meet industry standards and regulations related to building security and data protection .

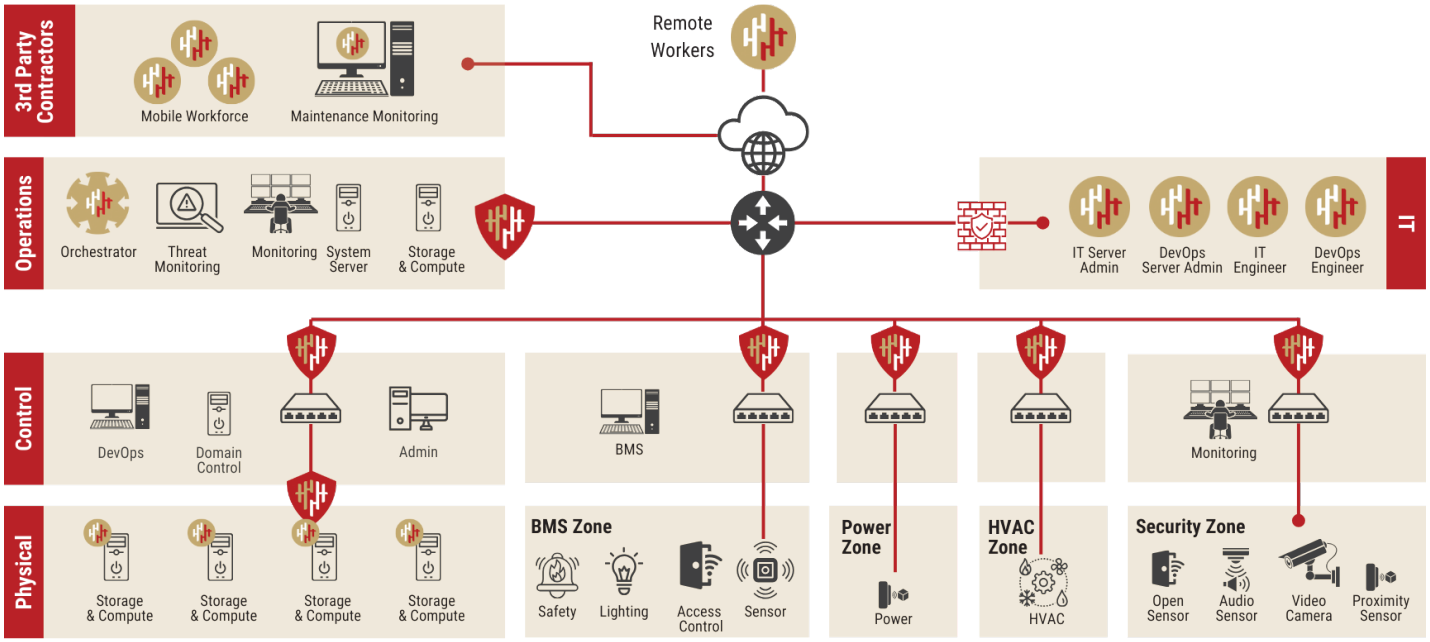
BlastShield

Safeguards Critical Building Systems like HVAC, lighting, security, and fire suppression systems, preventing disruptions that impact tenant safety.

Mitigates Physical Security Risks by securing access control and surveillance systems, preventing unauthorized entry and protecting sensitive areas.

Improves Operational Efficiency by securing remote access and automated monitoring capabilities, streamlining building operations.

Figure 1 Cyberthreats in Building Management



BlastShield™: Zero Trust OT Protection for Building Management

In Building Management, a crucial requirement is the distinct separation of IT and OT security solutions. The dynamic and historical vulnerabilities of IT solutions, with frequent reconfigurations due to tenant changes and new device connections, underscores the importance of robust network segmentation between OT and IT. This ensures that no IT security vulnerabilities can be exploited to breach the OT networks, making a strong OT DMZ with BlastShield a crucial part of a Building Management OT Cybersecurity deployment.

Building Management networks are uniquely challenging for OT cybersecurity, as often the physical infrastructure is intermingled with the IT infrastructure, separated only by VLANs. BlastWave's Software Defined Segmentation ensures that the OT network has a zero trust barrier with IT, and that the OT network can be segmented to deliver key use cases to Smart Building sand each critical subsystem:

Securing Building Automation Systems (BAS):

Gaining access to the BAS is like getting the keys to the kingdom. Ensuring Zero Trust Access to the BAS and protecting it from unauthorized access and control, as well as securing data collected and transmitted by BAS is the foundation for BAS cybersecurity.

Enabling Secure Remote Maintenance:

Smart buildings have a constant need to allow temporary access and ongoing access to maintenance personnel and vendors to diagnose and repair building systems. BlastWave's Zero Trust solution limits access to necessary systems and data for each user, ensuring least privilege and passwordless access to prevent credentials theft.

Securing HVAC Systems:

Protecting heating, ventilation, and air conditioning systems from unauthorized control and manipulation ensures comfortable, safe tenants. Ensuring that secure remote monitoring and maintenance of HVAC equipment is secure also minimizes downtime.

Securing Lighting Control Systems:

Malicious manipulation and control of automated lighting systems has become a concern for building operators as more smart lighting systems come online. Securing these systems ensures that energy is not wasted on lighting tenants can work in a hassle-free environment.

Securing Access Control Systems:

Unauthorized control and entry through vulnerable to hacked access control systems is a primary concern for theft, vandalism, and corporate espionage for building owners. Key card, biometric, and other access control systems must be shielded from discovery and denial of service attacks to prevent unauthorized entry and manipulation.

Securing Video Surveillance Systems:

Hackers and criminals seek to manipulate, eliminate, and delete video surveillance when targeting a business,. Protecting CCTV and other video surveillance systems from tampering and data theft is a critical component to protect with zero trust access and microsegment in a BMS deployment, as well as securing video storage and transmission to/from remote sites with encrypted tunnels.

Securing Fire Suppression Systems:

Malicious fire alarm activation and suppression systems must be segmented and secured from unauthorized control and false alarms. Repeated triggering of false alarms directly affects the safety and security of tenants.

Protecting against AI powered reconnaissance:

Knowledge of the systems used in a building can be valuable information for criminals and hackers planning malicious activities. Cloaking these assets behind BlastWave ensures that this knowledge cannot be used to leverage known vulnerabilities with AI-powered attacks.

Phishing protection:

Using passwordless MFA prevents phishing attacks against building operators, tenants, and contractors. Removing this attack vector dramatically reduces the attack surface and the risk for building owners.

Zero Trust Architecture:

Implementing a Zero Trust architecture protects and secures legacy systems that cannot be patched, protects data from building sensors, protects the data collected from sensors that monitor temperature, humidity, occupancy, and other building conditions. BlastWave ensures that tenants are fully protected from cyberattacks and manipulation of safety and security systems that keep their business operational.

v20250409

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499