BlastWave

SOLUTION BRIEF

AI-Resistant Cybersecurity Protection for Data Centers

The Operational Technology Challenge for Data Centers

Data centers require operational technology (OT) networks for building management services. These services are vital to maintaining and protecting data center operations, including power and cooling. Physical data center security also depends on network-connected systems such as access control and remote access.

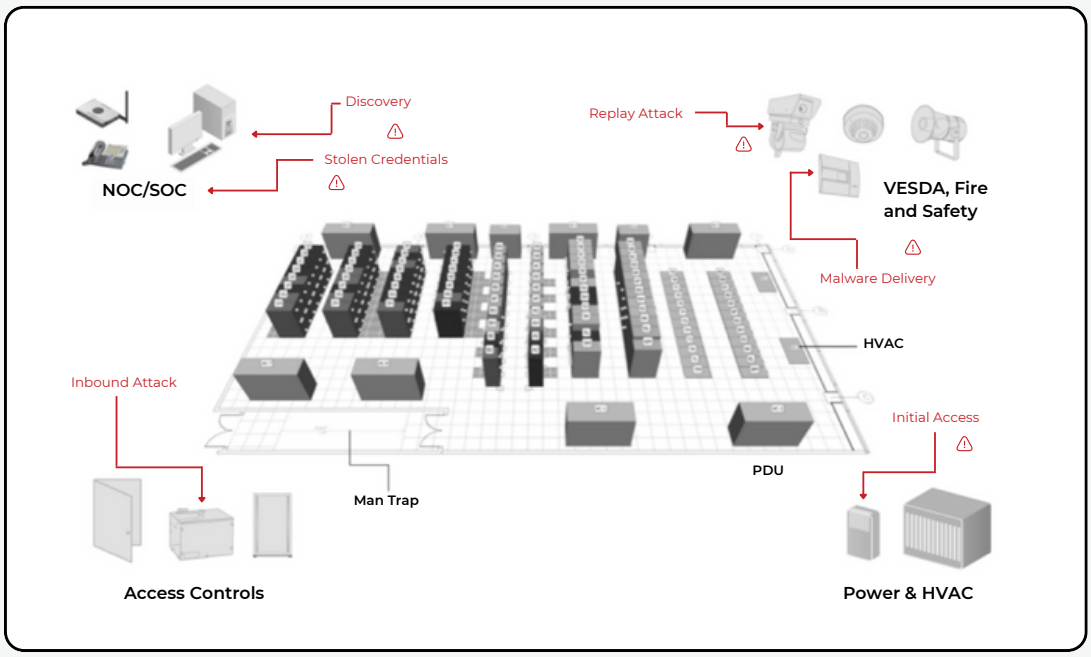
As data centers have become more complex, they have implemented extensive cooling infrastructures to cope with server heat diffusion. A hacker or cybercriminal that can disrupt these systems, even temporarily, can disrupt or demand ransom from the operator to prevent reputation-damaging downtime and revenue loss.

Multiple reports of data centers being attacked through their OT infrastructure have been released, including a data center in Atlanta, Georgia, where hackers penetrated their cooling system, causing temperatures to rise above 100 degrees and damaging servers with a ransom demand for Bitcoin. Networked OT systems that serve the data center market have known CVEs that anyone with access to the network could exploit. The Uptime Institute estimates that 25% of outages cost more than $1M, and 45% cost between $100,000 and $1M.

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 Data Centers



BlastShield™: AI-Resistant OT Security For Data Centers

Data Center OT networks have the same requirements as traditional OT networks, with the additional challenge of highly transient remote access users for maintenance contractors and a very low tolerance for delays in accessing and repairing failures.

OT Cybersecurity Solutions serving this market need to be highly agile and able to grant and revoke access immediately. The solutions also need to support high-performance remote access for solutions like remote video monitoring.

Data Centers that process data for specific industries may be required to comply with existing cybersecurity regulations like PCI DSS, NERC CIP, or HIPAA, which call for capabilities like Secure Remote Access and Network Segmentation.

BlastShield protects Data Center OT systems from discovery by hackers by creating a virtual air gap with Network Cloaking, only allowing biometric-authenticated Secure Remote Access to the devices and leveraging Network Segmentation to create microsegmentation of different device types to prevent lateral movement within an existing flat Layer 2 network.

Network Cloaking

Network Cloaking ensures critical data center environmental 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 data centers' cooling and access control infrastructure. With Network Cloaking, AI-enhanced reconnaissance tools cannot probe the internal workings of the Data Centers because they have no path to reach the internal OT networks from the IT network. This is critical as so many people are 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 data center 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.

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