Zero Trust OT Cybersecurity Protection for Data Centers

BlastWave builds secure data center OT networks, protecting critical infrastructure like power, cooling, and environmental controls. It hides sensitive systems, ensures only authorized access with strong, passwordless security, and segments the network to contain breaches. This means less risk of disruptions, data loss, and costly downtime, ensuring your data center's continuous and reliable operation. BlastWave's benefits for Data Centers include:

Network Cloaking for Critical Infrastructure: BlastWave's network cloaking technology renders sensitive OT systems, including power distribution units (PDUs), cooling systems, and environmental sensors, invisible to unauthorized users. This prevents reconnaissance and eliminates potential attack vectors, significantly reducing the attack surface.

Passwordless Multi-Factor Authentication (MFA): BlastWave eliminates passwords and thwarts phishing and credential theft. It ensures that only authorized personnel, including data center operators and maintenance technicians, can access critical systems. This is vital for securing remote access and preventing unauthorized control.

Granular Network Segmentation: BlastWave enables the creation of secure zones and conduits, isolating critical systems and limiting lateral movement in case of a breach. This is essential for containing the impact of attacks and protecting sensitive operational data.

Protection Against Advanced Persistent Threats (APTs): BlastWave's network cloaking and strong authentication capabilities effectively counter advanced persistent threats, including those leveraging AI-driven reconnaissance and social engineering.

Improved Compliance and Auditing: BlastWave provides audit trails and reporting, simplifying industry regulation compliance and standards related to data center security.

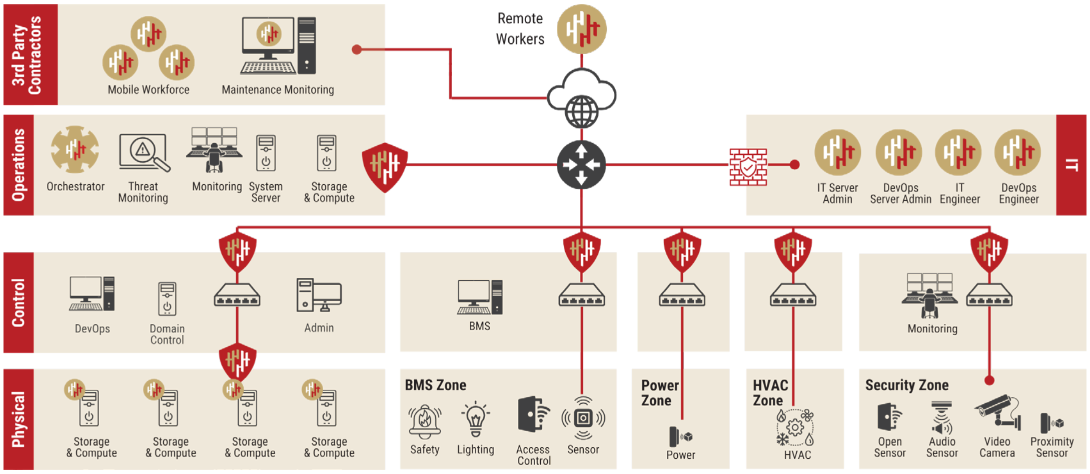
BlastShield

Secure Remote Monitoring and Control: Facilitates secure remote access for monitoring and controlling data center infrastructure

Enhanced Operational Uptime and Reliability: Prevents cyberattacks and contains breaches, minimizing downtime and ensuring continuous and reliable operation.

Improved Compliance and Auditing: Simpliies compliance with industry regulations and standards related to data center security.

Figure 1 Cyberthreats in Data Centers



BlastShield™: AI-Resistant Zero Trust OT Security for Data Centers

BlastWave builds secure data center OT networks, protecting critical infrastructure like power, cooling, and environmental controls. It hides sensitive systems, ensures only authorized access with strong, passwordless security, and segments the network to contain breaches. This means less risk of disruptions, data loss, and costly downtime, ensuring your data center's continuous and reliable operation.

BlastWave implements a true Zero Trust architecture, verifying every connection and enforcing least privilege access. Our solution is designed to ease deployment and management, minimizing disruption to existing data center operations. The system can also protect the back end of data center operations, securing administrator access into key infrastructure systems and devops access using BlastShield's passwordless MFA for high security remote access.

With BlastWave, data center operators and facility managers can significantly enhance their OT security posture, protect their critical systems, and ensure their data center infrastructure's reliable and secure operation. BlastWave delivers a number of key use cases for Data Center OT networks:

Enabling Secure Remote Access and Maintenance:

BlastShield ensures secure remote access for maintenance personnel and vendors to diagnose and repair data center infrastructure. Personnel are limited to access to only necessary systems and data, ensuring least privilege. This access can be time-bound as well, preventing abuse of access and providing more protection to critical systems.

Securing Building Management Systems (BMS):

Since integrated building management systems control all of the local OT systems, securing access to these systems is foundational for data center operators. These systems are an attractive target for hackers seeking to disrupt operations and plant ransomware, and are ideal to protect with zero trust access.

Securing Power Distribution Units (PDUs):

Power interruption are devastating to data centers. Protecting PDUs from unauthorized control, preventing power disruptions and equipment damage, and ensuring accurate monitoring are key use cases.

Securing Cooling Systems (CRAC, Chillers):

Cloaking and passwordless MFA prevents malicious manipulation of cooling systems which could result in overheating and equipment damage, causing downtime and loss of revenue and capital equipment. It also ensures that the environmental monitoring systems are protected from in-flight data manipulation with encryption.

Securing Physical Security Systems:

Physical access control solutions (key card, biometric, etc.) need protection from cyberthreats and hacking to ensure that unauthorized access cannot be granted through electronic means. These systems are also often connected to video surveillance systems , which need protection from tampering and data theft, and require high performance solutions that cannot be delivered with proxy-based security solutions. The alarm systems also require cyber protection against bad actors, as false alarms can weaken security responses to valid intrusions.

Securing DevOps Access:

Developer access to data center infrastructure systems benefits from Zero Trust Access. Developers can be given access only to the systems they are assigned to work on, permissions can be location and time restricted, and credentials cannot be stolen by bad actors seeking to escalate privileges, laterally move, or to live off the land.

Segmentation and Microsegmentation:

Network segmentation is critical in a data center that shares physical and network infrastructure between customers, IT, and OT systems. Each logical infrastructure should have a zero trust barrier that ensures users cannot cross boundaries, preventing the spread of malware, ransomware, and breaches. BlastShield's network cloaking and passwordless MFA create secure zones and conduits between the network segments, and microsegment within each zone to keep systems isolated from lateral movement by malicious insiders, hackers, and bad actors..

BlastShield's unique combination of AI-Resistant Network Cloaking, Phishing-Resistant Secure Remote Access, and Software Defined Segmentation ensures data centers can secure their networks in accordance with numerous industry-specific requirements and keep their infrastructure resilient and operational.

v20250408

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