Zero Trust OT Cybersecurity Protection for Ports

BlastWave delivers unparalleled security for maritime port OT networks by proactively eliminating the root causes of cyberattacks, rather than merely reacting to their symptoms. We protect your critical operations, from crane control to terminal management, with a robust Zero Trust architecture that combines network cloaking, passwordless MFA, and granular segmentation. This ensures the smooth flow of goods, enhances safety, and safeguards your infrastructure from disruption and theft.

Maritime port operators face a complex web of cybersecurity threats that can disrupt operations, compromise safety, and cause significant economic damage. Here's why they would choose BlastWave to protect their OT networks:

Prevention of Operational Disruptions: Minimizes the risk of cyberattacks that disrupt cargo handling, container movement, and overall port operations, ensuring efficient flow of goods.

Protection of Critical Infrastructure: Safeguards essential systems like crane control, terminal operating systems (TOS), and traffic management, preventing malfunctions and shutdowns.

Enhanced Safety: Helps protect against cyber attacks that could lead to accidents, such as crane collisions, equipment failures, or hazardous material incidents.

Compliance with Regulations: Aids port operators meet maritime security regulations and standards, ensuring compliance, enhancing safety, and avoiding penalties.

Reduced Attack Surface: Network cloaking hides critical assets from hackers, making them harder to find and attack.

BlastShield

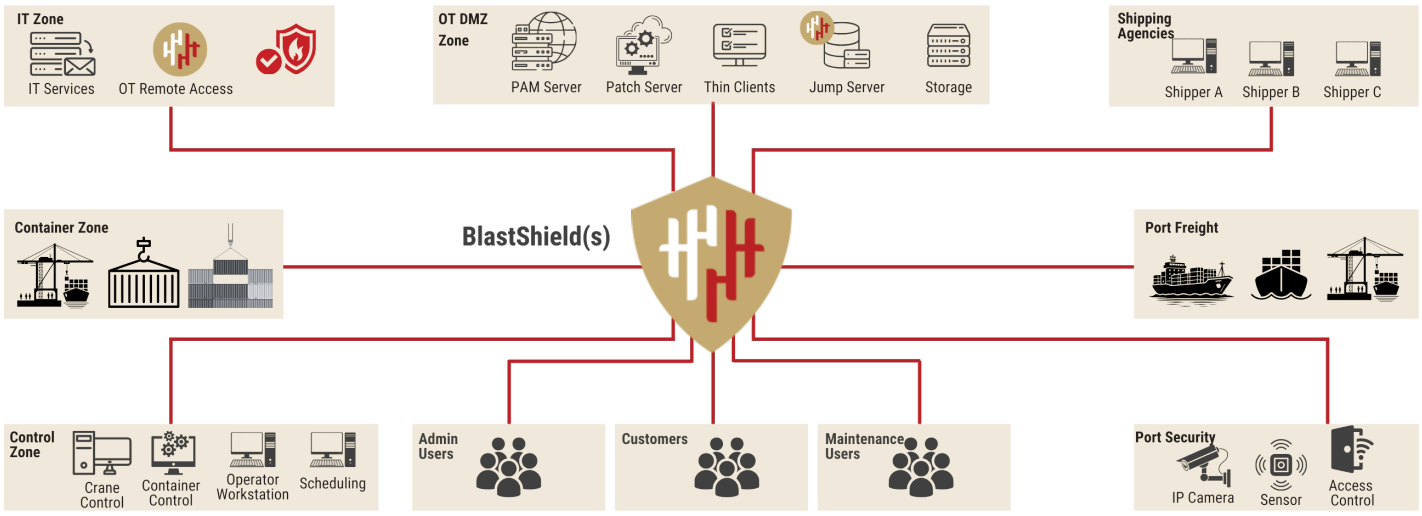
Secure Remote Operations: Enables secure remote monitoring and control of port operations, improving efficiency without compromising security.

Protect Legacy Systems: Provides a "virtual air gap" for vulnerable legacy equipment that cannot be easily updated, mitigating the risk of exploitation.

Protect Against Advanced Threats: Network cloaking and passwordless MFA effectively counter sophisticated AI-driven reconnaissance and phishing.

Mitigation of Ransomware Attacks: Network segmentation and granular access control limit the spread of ransomware, minimizing disruption and data loss.

Figure 1 Potential Threats to a Port's Cyber Infrastructure



BlastShield™: Zero Trust OT Protection for Ports

Ports rely heavily on interconnected Operational Technology (OT) networks. However, this interconnectedness makes them increasingly vulnerable to cyberattacks. Traditional security measures, focused on protecting the network perimeter, are no longer sufficient. Ports need Zero Trust security because it operates on the principle of "never trust, always verify." It assumes that any user or device, inside or outside the network, could be compromised. This approach is essential to mitigate the risks from sophisticated attackers who can bypass perimeter defenses and move laterally through the network, disrupting operations, stealing cargo data, or even causing physical damage.

BlastWave is uniquely positioned to address these challenges for port OT networks. Our Zero Trust platform is purpose-built for the demands of OT environments, including the diverse systems and legacy equipment found in ports. Our solution combines network cloaking to hide critical systems from attackers, passwordless MFA to eliminate the risk of stolen credentials, and software-defined segmentation to create granular control and contain breaches. This comprehensive approach provides the robust security that ports need to maintain efficient operations, protect valuable cargo, and ensure the safety of their facilities

BlastWave's Use Cases for Ports:

Securing Crane Control Systems:

Ports are increasingly run by automated cranes, and the crane operating systems require zero trust protection from unauthorized access and control. This will prevent accidents and damage to cargo/infrastructure.

Securing Loading and Unloading Equipment:

Protecting automated and semi-automated loading/unloading systems also protects the cargo and infrastructure for ports. By securing conveyor systems, AGVs (Automated Guided Vehicles), and other material handling equipment, port safety and security is increased.

Securing Terminal Operating Systems (TOS):

Malicious employees or bad actors will target the core software that manages cargo movement and logistics within the port if they are seeking to disrupt operations. Ensuring the integrity and availability of these systems and the data related to container tracking and inventory ensures that these systems cannot be manipulated or denied service, causing significant loss of revenue and risking the safety of employees.

Securing Access Control Systems:

Ensuring that the systems that manage access control into ports are secure protects the valuable cargo that traverses ports. Unauthorized manipulation of these systems protects the flow of trucks, trains, and ships within the port area.

Securing Surveillance and Security Systems:

Protecting CCTV networks, access control systems, and alarm systems from unauthorized access or tampering is critical to prevent hybrid cyber and physical attacks. Since these systems require high performance security solutions, BlastWave is perfect for these deployments.

Enabling Secure Remote Access:

BlastWave's passwordless MFA prevents phishing attacks against port employees and contractors, eliminating the risk of credential theft and unauthorized access. This is especially challenging for ports when enabling remote maintenance technicians and vendors, both for remote maintenance as well as monitoring of critical port infrastructure. All contractors should be given least privilege access to only the systems they are maintaining to prevent insider threats and preventing lateral movement.

Protecting Against AI-Powered Reconnaissance:

Ports operate with many legacy systems that are unpatchable or vulnerable to known exploits. Hiding these critical network assets from AI-driven scanning and reconnaissance tools prevents attackers from mapping the port's network and identifying vulnerabilities and mitigates the risk of exploitation of known vulnerabilities in legacy devices.

Segmentation and Microsegmentation:

BlastWave's software-defined segmentation and microsegmentation makes dividing the port's network into isolated segments to limit the impact of a breach extremely simple. Microsegmenting critical systems also mitigates risk by providing granular control over access and communication for employees and 3rd party vendors..

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

v20250410

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