BlastWave

SOLUTION BRIEF

AI-Resistant Cybersecurity For Ports

The Operational Technology Challenge for Ports

The maritime industry does the heavy lifting for the United States when it comes to global trade. The integrated network of ports, terminals, vessels, waterways, and land-side connections constituting the Nations Marine Transportation System (MTS) are key to America's prosperity.

The US government announced a major investment in the cybersecurity of America's ports, fortifying this critical infrastructure sector. The MTS supports up to $5.4T worth of economic activity each year, employs 31 million Americans, and supports nearly 95% of the cargo entering the US.

MTS companies rely on connected systems to enable their operations to digitally interact with everything from ship navigation to the movement of cargo. This digitalization has introduced vulnerabilities that, if exploited, could have cascading impacts on America's ports, the economy, and all Americans.

The challenge is that existing IT-oriented security solutions do not provide adequate security in this new AI-enabled cybersecurity landscape. The US DOT Maritime Administration has issued specific guidance on some of the threats to IT and OT systems that BlastWave can help the MTS protect against.

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: Potential Threats to a Port's Cyber Infrastructure

BlastShield™: AI-Resistant OT Security For Ports

BlastShield is an ideal solution to help port OT cybersecurity administrators protect their networks, as it is easily deployed as a simple migration without any changes to the existing IT or OT network architecture. Installing and administering the solution takes an order of magnitude less time and effort than comparable solutions. The user experience is comparable to Apple Pay, with simple biometric authentication granting access to only the devices the user needs.

The Executive Order focuses on several OT cybersecurity challenges BlastShield can solve for ports. It highlights the importance of reducing initial cyber access for adversaries (Network Cloaking), dedicated remote access solutions using MFA (OT Secure Remote Access), and improving segmentation on networks to prevent lateral movement (Microsegmentation).

Network Cloaking

BlastShield's network cloaking provides a first line of AI-resistant security by preventing reconnaissance and breaking the cyber kill chain. It proactively secures systems, making them invisible to potential attackers by blocking all internet access for legacy OT systems. Imagine a hacker scanning a network for surveillance and finding nothing. Valuable OT port assets, from Human-Machine Interfaces (HMIs) to crane operations, vanish from security scans. Network cloaking also creates a virtual air gap for OT systems that do not need access to the internet by only allowing them a hidden private IP address. Network Cloaking prevents AI-powered reconnaissance from scanning your port network to determine known or zero-day vulnerabilities that can be used to impede, destroy, or harm your port infrastructure.

Secure Remote Access

BlastShield provides AI-resistant secure remote access, employing a solid combination of multi-factor authentication (MFA), biometrics, and AES-256 encryption to prevent attacks from breaching our outer defenses. The MFA techniques resist phishing attacks with biometrics and other authentication factors, providing a more secure defense against AI-powered threats. A mesh of P2P tunnels delivers end-to-end protection from the initial login to the final data transmission; all interactions within the BlastShield utilize AES-256 encryption and meet regulatory requirements for data protection.

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. Policy changes take effect in real time, facilitating dynamic and flexible policy enforcement during emergencies or administration changes. Unlike many solutions that use ACLs and VLANs, microsegmentation scales effortlessly to large OT environments. With its detailed segmentation capabilities, BlastShield aids in compliance with stringent regulatory standards, offering necessary tools to protect sensitive data and ensure privacy. BlastShield's microsegmentation solution is innovative, future-ready network security.

BlastShield is an ideal solution for OT Port Cybersecurity, drastically simplifying and strengthening the defenses of this critical industry for the United States.

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