BlastShield Technical

BlastWave: OT Challenges

BlastWave provides Zero Trust OT cybersecurity protection specifically designed for the energy industry. At the core of this protection is BlastShield™, a solution that creates a secure, private overlay network for all connected systems and devices. A key feature of this overlay is "cloaking," which effectively hides public-facing IP addresses, rendering critical infrastructure invisible to potential attackers on the public internet.

By placing all systems on this BlastShield Overlay Network, energy companies can mask their assets, including vulnerable legacy systems, and implement dynamic network segmentation without requiring a complete network redesign. This approach fundamentally changes security by moving beyond traditional, often ineffective, perimeter defenses and establishing a resilient Zero Trust architecture.

The Five Issues Plaguing OT Networks

Energy companies face unique and critical cybersecurity challenges. Operational technology (OT) networks are often vulnerable due to a combination of legacy infrastructure and modern connectivity demands. These vulnerabilities can be summarized by five common issues:

1. **Public-Facing IP Addresses:** Many Industrial Internet of Things (IIoT) devices and even core SCADA systems are configured with public IP addresses, making them easily discoverable and accessible targets for attackers scanning the internet.
2. **Legacy Systems:** Nearly every OT environment contains older equipment that cannot be easily patched or updated. These systems often have well-known, unpatched vulnerabilities that attackers can readily exploit.
3. **Lack of Network Segmentation:** To prioritize high availability, many OT networks are "flat," meaning there are few internal barriers to stop an intruder. Once inside, an attacker can move laterally across the network with ease, leaving many vulnerable devices exposed.
4. **Weak Passwords:** A significant percentage of IIoT devices are deployed using factory default passwords. On average, 70% of these devices remain unchanged, creating a simple entry point for unauthorized users. This weakness is a primary vector for credential theft, which BlastWave's passwordless MFA is designed to prevent.
5. **Device Inventory Challenges:** The rapid proliferation of new devices makes it difficult for operators to maintain an accurate and up-to-date inventory. This lack of visibility can lead to unauthorized devices connecting to the network and transmitting data without the knowledge of the owner-operators, sometimes to foreign adversaries.

BlastShield™

BlastShield Features

- Phishing-resistant MFA authenticates the remote pilot-in-command before connection
- Device cloaking that hides the public IPaddress and web services of the aircraft, control stations and cloud servers
- Simple orchestration replaces complex PKI and firewall management
- On-premises Orchestrator for air-gapped networks

Five Key Strategies to Stop Hackers and Malicious Insiders

BlastWave eliminates these issues by implementing a robust Zero Trust architecture that addresses the root causes of network vulnerabilities. The following five strategies are key to stopping and frustrating both external hackers and malicious insiders:

1. **Inventory Everything and Identify Vulnerabilities:** The foundational step in securing any network is to have a complete and accurate inventory of all connected devices. This allows operators to identify which systems are present, what vulnerabilities they may have (such as being unpatchable legacy systems), and what their communication patterns should be.
2. **Cloaking (IP Masking):** BlastShield hides public-facing IP addresses by placing all systems and IIoT devices on a private BlastShield Overlay Network. This network cloaking makes assets invisible to external reconnaissance, effectively eliminating the public attack surface. This strategy also dramatically reduces the risk posed by legacy systems, as they are no longer discoverable by attackers, creating a "virtual air gap" that protects them from exploitation.
3. **Network Segmentation:** BlastShield achieves dynamic, software-defined segmentation, allowing for granular control over network traffic. This is accomplished by creating micro-perimeters around devices or groups of devices, effectively implementing virtual firewalls. This method contains the impact of any potential breach by limiting an attacker's ability to move laterally across the network. This can be deployed without requiring a costly and disruptive network redesign or downtime.
4. **Secure Remote Access:** BlastWave utilizes passwordless multi-factor authentication (MFA) to provide secure remote access for employees, vendors, and contractors. This approach is resistant to phishing and prevents attackers from gaining access even if they have stolen valid employee credentials, which is a major source of security breaches. It enables efficient remote monitoring, maintenance, and control without compromising security.
5. **Egress Policies:** By defining authorized communication pathways within the segmented network, BlastShield can enforce strict egress policies. This ensures that devices only transmit data to approved destinations. Any attempt by a compromised or unauthorized device to send data to an external, unapproved server is immediately identified and shut down, preventing data exfiltration.

v20260330

Prevent industrial cyberattacks, and ensure the world's critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at **www.blastwave.com**

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS