BlastWave

SOLUTION BRIEF

Zero Trust OT Protection for Aerospace Manufacturing

The Zero Trust Protection Challenge for Aerospace

Unlike traditional manufacturing, the aerospace sector faces a unique set of operational and regulatory challenges in cybersecurity. In addition to the typical OT cybersecurity issues, aerospace manufacturing is held to the highest precision and quality control standards. With billions of dollars and often human lives at risk, the cybersecurity risk is amplified for intrusion, denial of service, and subtle tampering, underscoring the need for a robust cybersecurity solution.

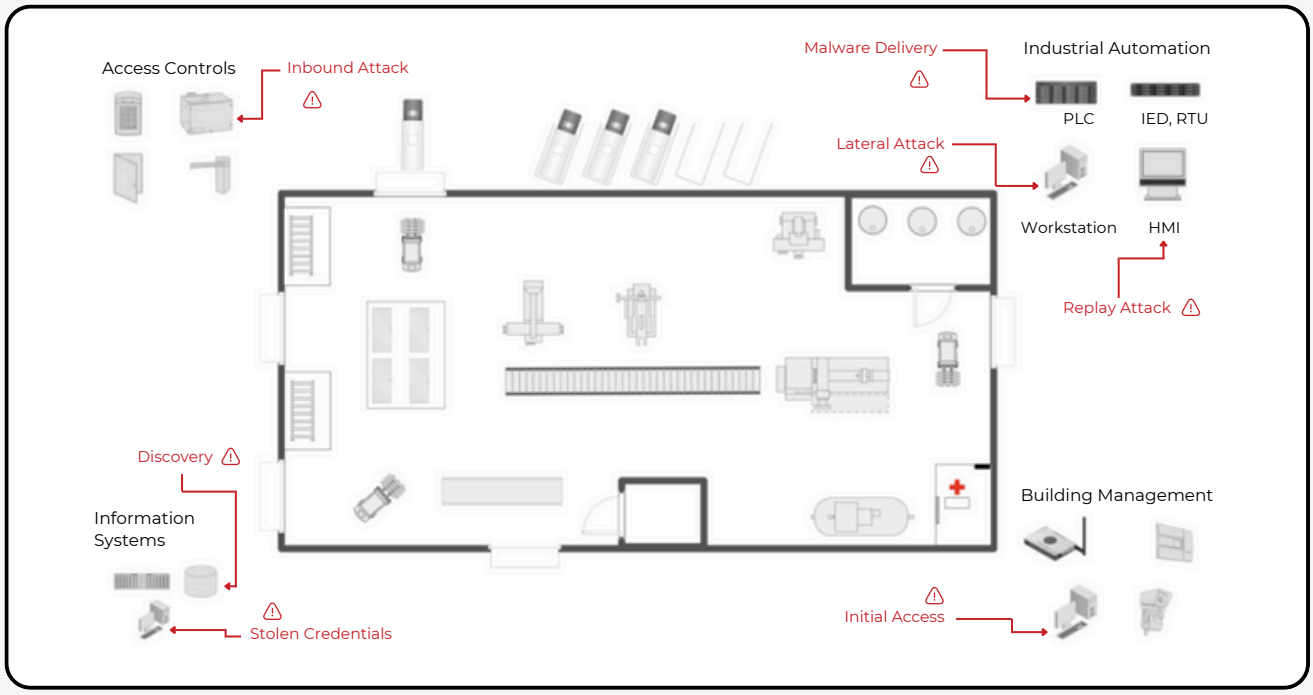
Manufacturing is already a target for criminal hackers due to the value of their products and the extreme cost of downtime. Aerospace manufacturing must also contend with hostile nation-state-sponsored hackers seeking to affect the balance of power in space by disrupting their production. They must also deal with espionage from hostile nation-states and business competitors seeking to glean operational and manufacturing techniques to catch up or surpass aerospace capabilities.

Aerospace manufacturing companies must isolate their OT networks from their IT networks and deploy a cybersecurity solution optimized for the OT environment. Highly secure OT networks practice defense in depth, including using a security solution different from the IT domain to ensure that a failure or vulnerability in the IT arena doesn't compromise their OT cybersecurity.

BlastShield Advantages:

- **Stops the Discovery attack vector** with a Reconnaissance-Proof to prevent device discovery and vulnerability exposure with Network Cloaking
- **Stops Iniital Acess attack vector** with Phishing-Resistant Biometric Multifactor Authentication for Regulatory-Compliant Secure Remote Access
- **Stops Lateral Movement attack vector** with Least Privilege access policies and software-defined Microsegmentation

Figure 1: Cyberthreats in Aerospace Manufacturing



BlastWave Copyright 2024

BlastShield™: AI-Resistant Zero Trust OT Protection For Aerospace Manufacturing Systems

As the age of Industry 4.0 expands, the aerospace manufacturing industry encounters a growing threat landscape in terms of cybersecurity, with operational and information technology environments becoming more interconnected. This integration poses a big challenge since legacy solutions with significant security weaknesses are frequently involved.
Manufacturing companies do not have a consolidated set of regulations like some industries. However, following the NIST Cyber Security Framework, NIS2 Directive, Cyber Resilience Act, or IEC 62443 provides vital guidance on best practices for the industry, especially defense-related aerospace manufacturing.

BlastShield provides a PKI-authenticated secure gateway to the OT environment, where Industrial control systems, PLCs, IEDs, RTUs, turbine controllers, valves, and IoT devices remain in service for decades, long after vendors halt support. These systems often cannot be patched but require access to internal monitoring systems. BlastShield protects these 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 that critical yet outdated legacy infrastructure such as PLCs, DCSs, RTUs, SCADA, and HMIs 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 the manufacturing logistics chain. With Network Cloaking, Nation-State AI-Enhanced reconnaissance tools cannot probe into the internal workings of the manufacturing plant because they have no path to reach the internal OT networks. 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 manufacturing 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 plant 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 Software-Defined 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.

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

BlastWave Copyright 2024