BlastWave

SOLUTION BRIEF

AI-Resistant Cybersecurity Protection for Manufacturing

The Operational Technology Challenge for Manufacturing

As of 2023, IBISWorld estimates that the US has over 600,000 manufacturing businesses, and SCMO estimates that there are over 10,000,000 worldwide. Manufacturing output was over $16T in 2022, making it a prime target for hackers looking to generate ransoms. IBM's X-Force Threat Intelligence Report lists Manufacturing as the top-attacked OT industry, accounting for 58% of all attacks and 25% of all industry attacks.

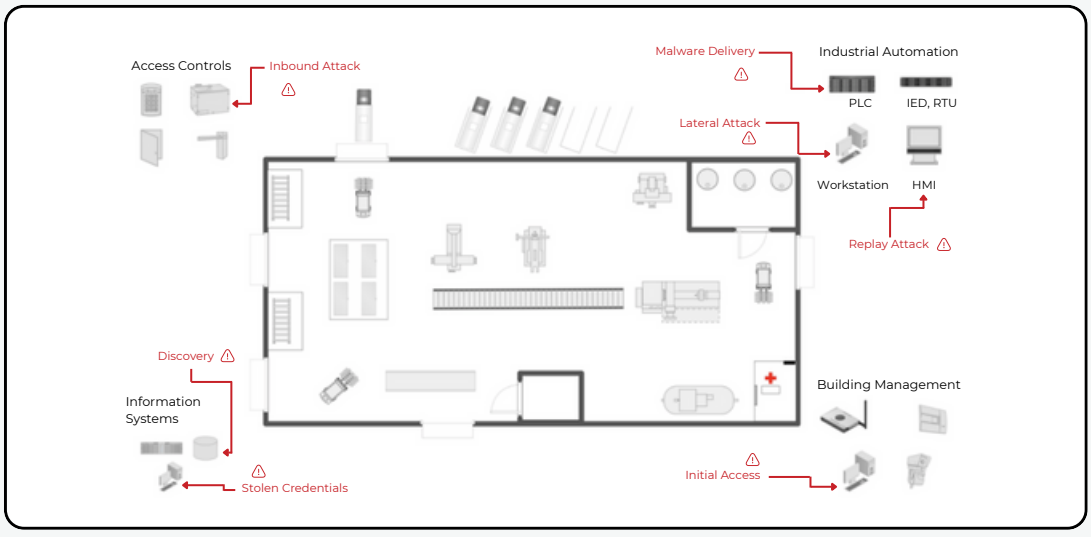
As manufacturing moves into the era of Industry 4.0 and beyond, the challenge of protecting their cyber-physical OT networks has become a business imperative. Cyber attacks can cause manufacturing companies to incur enormous losses in operations and revenue by forcing the closure of one or more plants while addressing the damage done. Although it brings tremendous operational advantages, the fact is that the more connected your OT environment is, the bigger the risk.

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:

- 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: Cyberthreats in Manufacturing



BlastShield™: AI-Resistant OT Security For Manufacturing Systems

As the age of Industry 4.0 expands, the 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, but following the NIST Cyber Security Framework, NIS2 Directive, Cyber Resilience Act, or IEC 62443 provides strong guidance on best practices for the industry.

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, 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 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 for network security.

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