BlastWave

SOLUTION BRIEF

Zero Trust Protection for Operational Technology

Zero Trust Protection for OT is Possible

Protecting the critical infrastructure that powers nation-states worldwide is not just a big task; it's crucial. Too many people have given up on protecting their OT assets and are content to monitor them to see when something goes wrong. However, the potential risks are too high to be complacent. Zero Trust for OT is crucial and should be prioritized since the return on mitigation is so high.

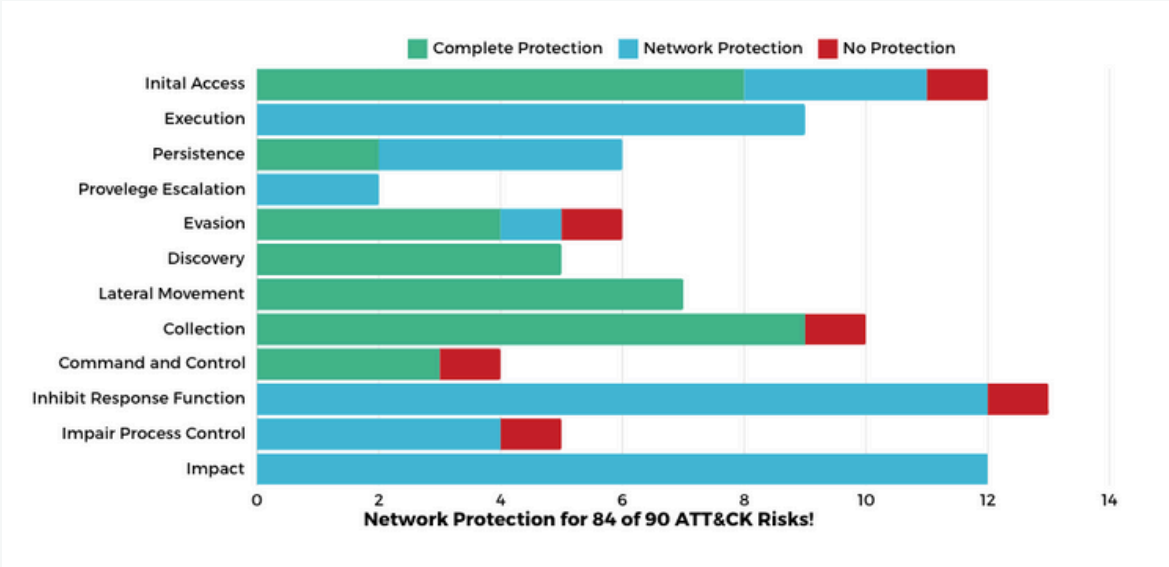
In the US, published specifications like NIST 800-207 (Zero Trust Architecture), the NIST Cybersecurity Framework 2.0, CISA's Zero Trust Maturity Model 2.0, and the DoD Zero Trust Reference Architecture have helped guide critical infrastructure and operational technology companies to build secure networks. These documents provide guidelines on how to structure a secure architecture to resist cyberattacks. A key first step in Zero Trust is protecting the network from attack, thereby drastically reducing the load on detection, response, and recovery.

The MITRE ICS AT&CK framework outlines several attack vectors (Discovery, Initial Access, and Lateral Movement) that pose the biggest external and internal threats to OT networks. BlastWave's Zero Trust Protection blocks entire classes of risk (as defined by the MITRE ICS ATT&CK framework), dramatically altering the cybersecurity landscape for OT network administrators. By blocking remote risk factors and minimizing the attack surface, BlastWave's Return on Mitigation (ROM) is far superior to investing in other OT cybersecurity solutions, providing network protection for 84 of 90 ICS tactics.

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: Zero Trust Protection and the MITRE ATT&CK ICS Matrix



Yes, protection for OT networks is not just a possibility but a reality.

Let's be clear: Our approach to Zero Trust for OT is distinct from Zero Trust for IT. When a CISO determines the desired outcome of an Operational Technology Protection purchase, several things are required.

OT networks should not be open to the Internet. Hackers should not be able to discover that the OT network exists. An OT device rarely needs to connect to the Internet directly. What you can't see, you can't attack. BlastWave's Network Cloaking blocks Discovery in OT networks.

Granting access to OT networks is like giving a user the keys to the kingdom. Passwords must be eliminated—credentials are stolen online with frightening regularity, and 90% of successful hacks begin with a phishing email. BlastWave's Passwordless MFA, which is not vulnerable to phishing, MFA bombing, or session hijacking, blocks Initial Access to OT networks.

Microsegmentation is not just a feature; it is a necessity for OT. Individual devices cannot be trusted to be secure, as they can be a decade out-of-date and no longer supported by the vendor—but they still must run. To mitigate the risk of insider threats, users should only be able to access the devices they require to do their job, not all of the devices on the flat Layer 2 network. BlastWave's Software-Defined Microsegmentation blocks Lateral Movement in OT Networks without network redesign or massive reconfigurations.

A comprehensive solution will provide Network Cloaking, Passwordless Secure Remote Access, and Software-Defined Microsegmentation, eliminate multiple classes of risk, and provide a superior Return on Mitigation (ROM) for your OT Cybersecurity Protection investment.

Network Cloaking

Network Cloaking ensures that OT networks of any type are invisible to external threats. Rather than just obfuscating these systems, they do not appear in any scans or probes from a hacker, blocking the initial points of entry for AI-enabled hacking. Network cloaking assists in compliance with zero trust specifications by preventing access to vulnerable devices. With Network Cloaking, AI-enhanced reconnaissance tools cannot probe into the internal workings of networks because they have no path to reach the internal OT networks.

Secure Remote Access

BlastShield provides OT Secure Remote Access to OT systems, enabling real-time management of all systems without exposing them to cyber threats. BlastShield's phishing-resistant MFA biometric authentication protects against GenAI-powered phishing attacks and MFA hijacking. BlastShield creates a full mesh of P2P encrypted tunnels to secure sensitive but unclassified traffic from remote users to OT networks and any agent-enabled systems, protecting against Man-in-the-middle attacks without pushing users to use only a single vulnerable browser-based interface.

Network Segmentation

BlastShield simplifies the challenge of microsegmentation by creating simple peer-to-peer encrypted and authenticated tunnels to each device or group of devices without complex firewall rulesets. IT and OT network staff and temporary contractors are permitted access to only the systems they are responsible for, and privileges can be granted and revoked in real-time. BlastShield prevents lateral movement by Secure Remote Access users within the network and can even provide lateral movement protection at Layer 2 for local network connections.

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