Zero Trust Protection for Operational Technology

OT Networks are the guardians of essential services, the keepers of systems that power our communities and industries. The weight of ensuring uninterrupted operations, safeguarding critical assets, and protecting against ever-evolving cyber threats rests squarely on these networks. OT networks, unlike typical IT environments, are the lifeblood of our infrastructure, and their disruption can have profound, real-world consequences. This isn't just about data; it's about safety, reliability, and the very foundations of our daily lives. That's why your networks demand a level of protection that goes beyond conventional security measures.

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.

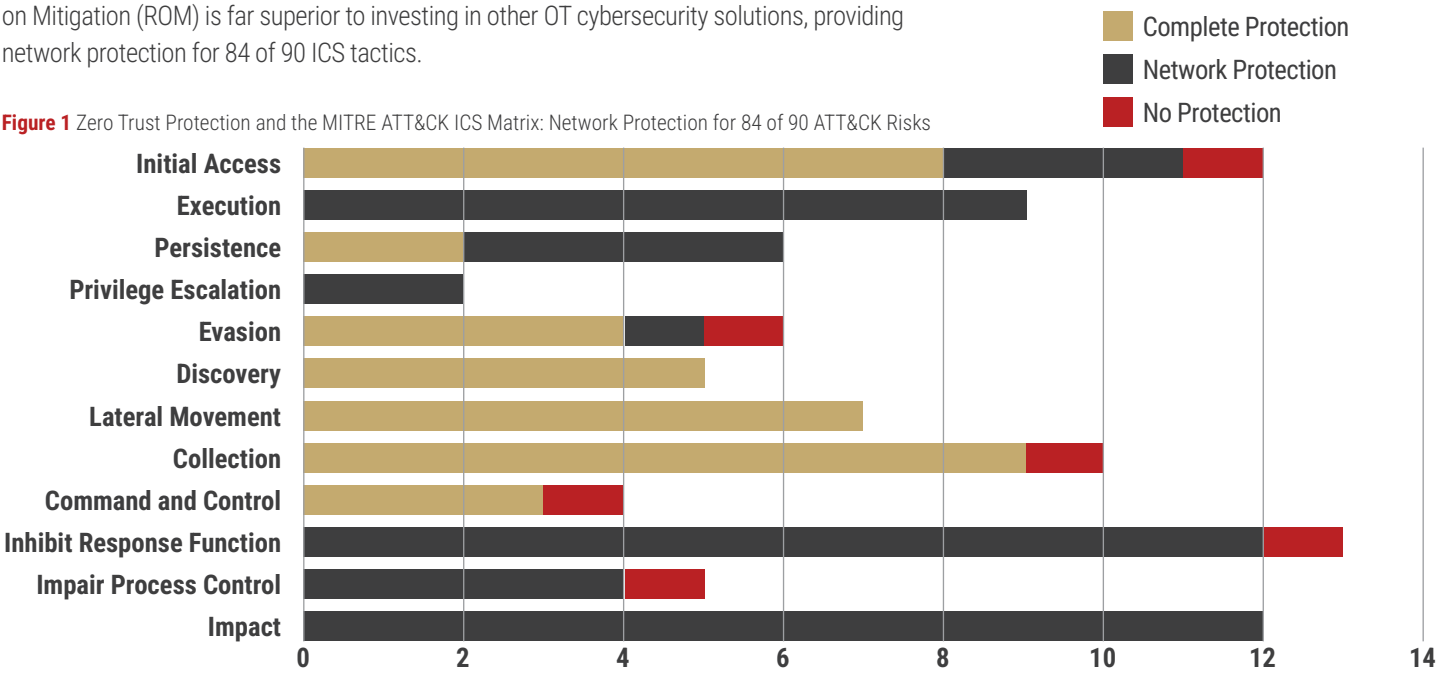
BlastShield

Stops the Discovery attack vector with AI-resistant Reconnaissance to prevent device discovery and vulnerability exposure with **Network Cloaking**

Stops Initial Access 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 Zero Trust Protection and the MITRE ATT&CK ICS Matrix: Network Protection for 84 of 90 ATT&CK Risks



Protection for OT networks is not just a possibility but a reality

The desired outcomes for OT are very different than for IT. Zero Trust for OT requires a different cybersecurity protection solution than Zero Trsut for IT, as the firewalls that have tried to protect OT networks over the past years have failed to deliver real protection.

BlastWave implements Zero Trust uniquely by focusing on eliminating the root causes of cyberattacks, rather than solely reacting to their symptoms. We go beyond traditional identity and access management by integrating network cloaking, passwordless multi-factor authentication (MFA), and software-defined segmentation into a unified platform. Network cloaking renders critical assets invisible to unauthorized users, preventing reconnaissance and eliminating a key initial attack vector. Passwordless MFA eliminates the vulnerabilities associated with traditional passwords, thwarting phishing and credential theft. Granular segmentation creates micro-perimeters, limiting lateral movement and containing breaches.

This holistic approach, purpose-built for OT environments, allows BlastWave to deliver a more robust and effective Zero Trust solution. By addressing the fundamental weaknesses that attackers exploit, BlastWave provides a proactive defense that strengthens security posture while simplifying management. We're not just adding layers of complexity; we're reimagining security from the ground up, ensuring that critical infrastructure remains protected in the face of evolving cyber threats

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

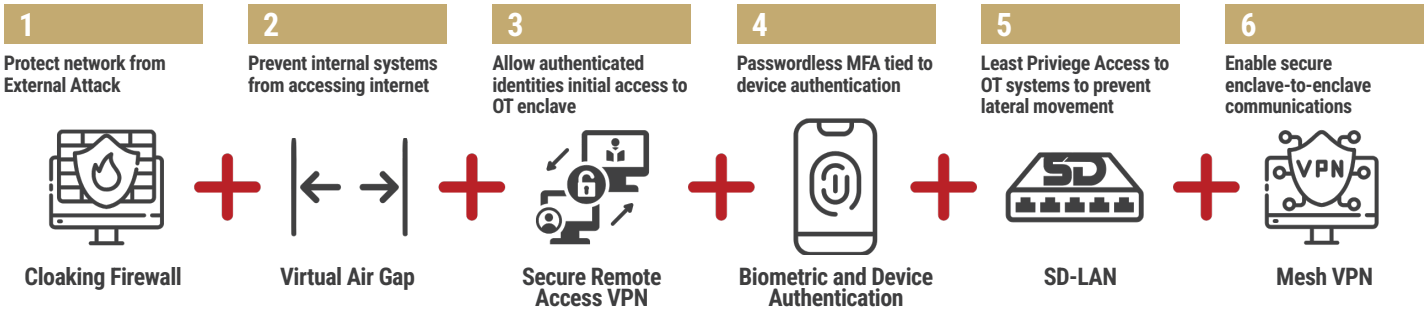
Network Cloaking ensures that OT networks of any type are invisible to external threats. Rather than just obfuscating these systems, they do not appear in any scans or probes from a hacker, blocking the initial points of entry for AI-enabled hacking. Network cloaking assists in compliance with zero trust 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 Software-Defined 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.



v20250104

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499