OT Zero Trust Protection for Government OT Networks

Securing the Government's Critical Infrastructure to Protect Vital Services

BlastWave

BlastWave is a Zero Trust shield for government OT networks, protecting critical infrastructure like defense OT water systems, power grids, and transportation.

It hides sensitive systems from hackers, ensures only authorized access with strong passwordless security, and segments networks to contain breaches. This strengthens national security, protects essential services, and provides peace of mind knowing vital infrastructure is safeguarded. With BlastWave, government agencies can deploy a Zero Trust solution that protects their networks from hackers and malicious insiders.

CONTENTS

Zero Trust OT Protection for Governments

Escalating Threat Levels for Government OT

Government-operated Operational Technology (OT) networks, the backbone of essential public services such as power generation, water treatment, transportation, and critical manufacturing, face an escalating barrage of sophisticated cyber threats.

These threats emanate from diverse actors, including nation-states intent on disruption or espionage, and cybercriminals motivated by financial gain. The potential consequences of a successful cyberattack on these systems are severe, ranging from widespread service disruptions and substantial economic damage to immediate risks to public safety and national security.

Compounding this vulnerability is the proliferation of Artificial Intelligence (AI)-powered attack tools. These advanced tools can automate and refine reconnaissance efforts, create highly deceptive phishing campaigns, and generate novel malware, effectively lowering the skill threshold for attackers and significantly enhancing the capabilities of sophisticated adversaries. Indeed, government bodies such as the UK's National Cyber Security Centre (NCSC) have issued specific warnings regarding these AI-augmented threats targeting critical national infrastructure, underscoring the urgent need for a more resilient security posture**.**

Zero Trust: A Strategic Paradigm Shift

In response to this increasingly perilous threat landscape, governments worldwide are mandating or strongly recommending a strategic pivot towards a Zero Trust Architecture (ZTA).

This security model fundamentally departs from traditional perimeter-based defenses, which operate on an assumption of implicit trust once inside the network. ZTA, conversely, is founded on the principle of "never trust, always verify," operating under the assumption that breaches are not only possible but probable, or may have already occurred. Consequently, no user, device, or application is granted inherent trust based merely on its network location or ownership.

Zero Trust principles advocate for a data-centric security approach, moving defenses from static network perimeters to focus on protecting users, assets, and resources directly. Access to these resources is granted strictly on a per-session basis, enforced through dynamic policies, and requires continuous verification of identity, device security posture, and other contextual attributes.

The overarching objective is to prevent unauthorized access to sensitive data and critical control systems, and to limit the potential impact of any security breach by rigorously containing lateral movement within the network.

Common Zero Trust Principles Emphasized Across Government OT Initiatives

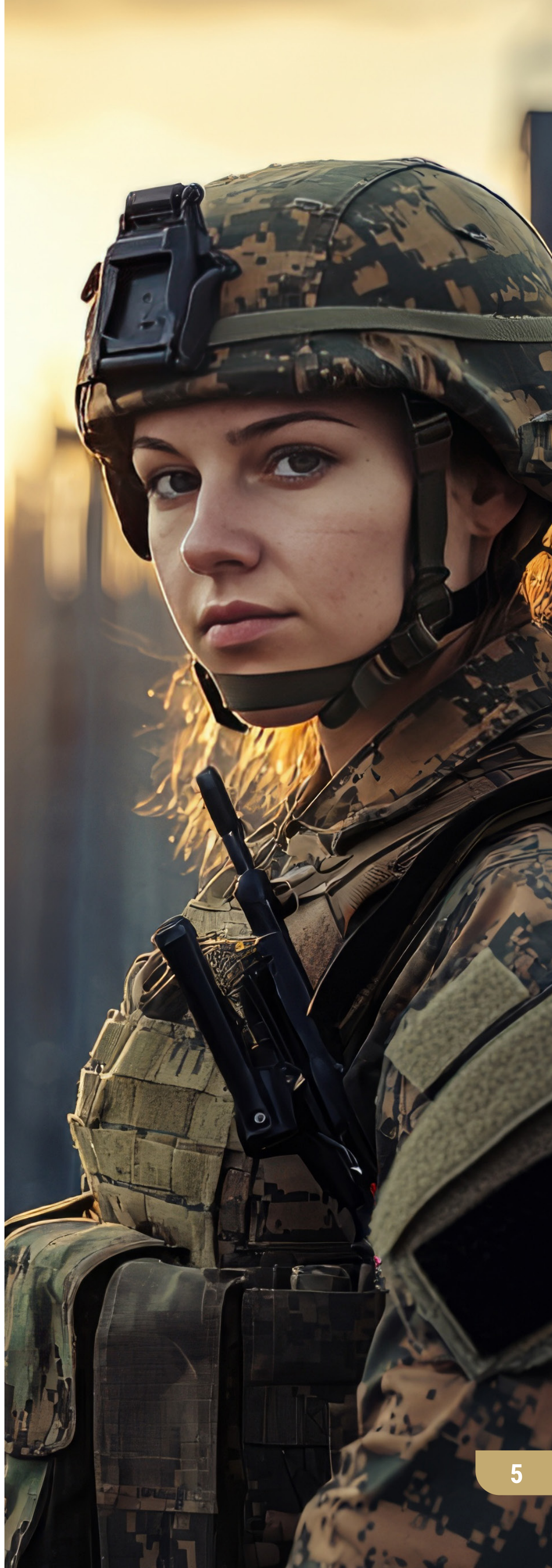
Across these varied directives and frameworks, several common ZT principles are consistently emphasized as crucial for securing government OT environments worldwide:

Strong Identity and Access Management (IAM): Rigorous verification of all users (employees, contractors, vendors) and devices attempting to access OT resources, with a strong push towards phishing-resistant MFA and enterprise-managed identities.1

Network Segmentation and Microsegmentation: The division of OT networks into smaller, isolated security zones (often aligning with the IEC 62443 model of zones and conduits) to contain threats and limit lateral movement. Microsegmentation applies these controls at an even more granular, asset-specific level.1

Continuous Monitoring, Detection, and Response: Implementation of capabilities for deep visibility into OT network traffic, device behavior, and security events to enable real-time anomaly detection and rapid incident response.

Secure Remote Access: Establishment of secure, authenticated, and least-privilege pathways for any remote access to OT systems, whether for internal personnel or third-party vendors.



Government OT Networks with BlastWave

BlastWave's Zero Trust Approach

BlastWave implements a true Zero Trust architecture, verifying every connection and enforcing least privilege access. Our solution is based on the following Zero Trust capabilities:

Network Cloaking for Sensitive Systems

BlastWave's network cloaking technology renders critical infrastructure components, including control systems, SCADA devices, and remote sensors, invisible to unauthorized users. This proactively prevents reconnaissance and eliminates potential attack vectors, significantly reducing the attack surface. BlastShield's secure overlay enables protection without network addressing or architecture changes to cope with overlapping IP addresses common in OT.

Passwordless (MFA)

By eliminating passwords, BlastWave thwarts phishing and credential theft, ensuring only authorized personnel, including government employees and approved contractors, can access sensitive systems. This is crucial for securing remote access and preventing unauthorized control.

Granular Network Segmentation and Microsegmentation

BlastWave enables the creation of secure zones and conduits, isolating critical systems and limiting lateral movement in case of a breach. This is essential for containing the impact of attacks and protecting sensitive data, aligning with government cybersecurity standards.

Secure Remote Access

BlastWave facilitates secure remote access for maintenance, monitoring, and control of geographically dispersed assets, including water treatment plants, power substations, and transportation systems. Access is strictly controlled, ensuring the least privilege and time-limited access, vital for maintaining operational continuity.

Compliance with Government Security Standards

BlastWave helps agencies comply with an increasing number of government standards:

United States:

OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" (January 2022): This memorandum establishes specific ZT goals and implementation timelines for Federal Civilian Executive Branch (FCEB) agencies.

CISA's Zero Trust Maturity Model (ZTMM v2.0) (April 2023): This model provides a comprehensive roadmap for agencies to plan and implement their ZT strategies.

NIST SP 800-82 Revision 3, "Guide to Operational Technology (OT) Security" (September 2023): This is a pivotal document for government OT security. Revision 3 explicitly integrates ZTA concepts (referencing NIST SP 800-207) into its guidance for OT environments.

Department of Defense (DoD) Zero Trust Strategy and Roadmap: The DoD has established its own comprehensive ZT strategy, with the goal of achieving "Target Level ZT" by Fiscal Year 2027. It is expected that an OT-specific strategy will be released in 2025.

International:

Canada (CCCS): Has published guidance such as ITSAP.10.008 on the ZT security model, referencing CISA and NIST frameworks, emphasizing principles like continuous verification.

United Kingdom (NCSC): Offers ZTA design principles and specific guidance for OT security, stressing "Secure by Design" and addressing the unique safety and reliability requirements of OT.

Australia (ACSC): Its 'Foundations for Modern Defensible Architecture' promotes ZT principles like "never trust, always verify" and "assume breach," intended for high-level application across all environments, including OT.

European Union (ENISA): ENISA advocates for enhanced cybersecurity across critical sectors, including recommendations for ZT-based access management and robust segmentation for OT in critical infrastructure like space systems.

This international alignment on fundamental ZT principles facilitates global cybersecurity cooperation and the development of common standards, benefiting both governments and solution providers.

BlastShield Use Cases for Government OT Networks

Securing Critical Infrastructure:

- Protecting water and wastewater treatment facilities from unauthorized access and control.
- Safeguarding power grids and substations from cyberattacks that could disrupt energy supply.
- Securing transportation systems (traffic control, rail, aviation) from malicious manipulation.

Protecting Defense Systems:

- Securing military installations and control systems from cyber espionage and sabotage.
- Protecting weapon systems and communication networks from unauthorized access.
- Securing logistical and supply chain systems.

Securing Public Safety Networks:

- Protecting emergency response systems (911, dispatch) from disruption.
- Securing communication networks used by first responders.
- Protecting surveillance and monitoring systems.

Protecting Federal, State, and Local Government Facilities:

- Securing building automation systems (HVAC, lighting, security) in government buildings.
- Protecting data centers and critical servers.

Securing Remote Infrastructure:

- Protecting remote monitoring and control systems for environmental monitoring and natural resource management.
- Securing remote communication networks.

Enabling Secure Remote Access:

- Providing secure remote access for government employees and contractors to maintain and manage critical infrastructure.
- Enabling secure collaboration and data sharing between government agencies.

Compliance with Government Security Standards:

- Assisting with compliance requirements related to cybersecurity, such as NIST, CMMC, and others.
- Providing audit trails and reporting for security assessments.

Protecting against AI powered reconnaissance:

- Hiding critical network assets from AI-powered reconnaissance software.

Phishing protection:

- Using passwordless MFA to prevent phishing attacks against government employees and contractors.

Segmentation and Microsegmentation:

- Using network segmentation and microsegmentation to limit the blast radius of a cyber attack.

Zero Trust Architecture:

- Implementing a Zero Trust architecture to protect the entire network.

Protecting Legacy systems:

- Protecting legacy systems that cannot be patched.

BlastWave

BlastWave's Approach:

BlastWave implements a true Zero Trust architecture, assuming no user or device is inherently trustworthy. We verify every connection, enforce least privilege access, and continuously monitor network activity to detect and respond to threats in real-time. Our solution is designed to be easy to deploy and manage, minimizing disruption to existing operations.

By implementing BlastWave, governments can strengthen their OT security posture, protect their critical assets, and ensure their facilities' continuous and secure operation in the face of evolving cyber threats.

BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to
www.blastwave.com

v20250829

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