WHITE PAPER

Invisible OT: How to Hit DoW's Zero Trust for OT Timeline Without Touching a Single PLC

Zero Trust Protection for Compliance with Department of War Mandates

BlastWave

TL:DR

The Department of War (DoW) has issued a definitive mandate to adopt Zero Trust (ZT) principles across Operational Technology (OT) and Control Systems. This directive, codified in Zero Trust for Operational Technology - Scope and Purpose and underpinned by DTM 25-003, represents a shift from perimeter-centric security models to a data-centric, continuously authenticated architecture. The urgency of this transition stems from the convergence of IT and OT environments, where legacy industrial protocols, flat network topologies, and air-gapped assumptions no longer provide sufficient defense against sophisticated nation-state actors.

This paper analyzes how BlastWave's software-defined perimeter (SDP) and microsegmentation architecture enable DoW Agencies to comply with the **Zero Trust Operational Technology Activities Outcomes** framework without disrupting the operational environment.

BlastWave directly supports 20 of the 86 Target Level requirements and indirectly supports 14 other requirements that require API or BlastWave input to achieve comprehensive compliance. The protection offered by BlastWave is the first step in Zero Trust Compliance, providing "air cover" for agencies as they implement the remaining Target and Advanced requirements.

BlastWave serves as a foundational architectural pillar for the Network, User, and Device pillars, specifically addressing critical requirements for secure remote access, network cloaking, and lateral movement prevention through microsegmentation. By acting as a secure cryptographic overlay that renders critical assets invisible to unauthorized entities, BlastWave directly addresses the DoW's requirement to "transition away from trusted networks" to an environment of "continuous authentication and fine-grained policy enforcement". BlastWave uniquely accomplishes this without requiring changes to the underlying network, enabling a transition from a firewall- and VPN-based architecture to a Zero Trust network with minimal disruption to the OT network.

While BlastWave provides the essential connectivity and segmentation fabric, Zero Trust is inherently an ecosystem approach. No single product meets all the requirements of the seven pillars. Therefore, the analysis includes a gap analysis to identify the specific "Partner Product Classes" such as Enterprise SIEM, Identity Providers (IdP), and Endpoint Detection and Response (EDR) required to complement the BlastWave deployment and achieve full compliance with the Target and Advanced levels of the DoW mandate.

CONTENTS

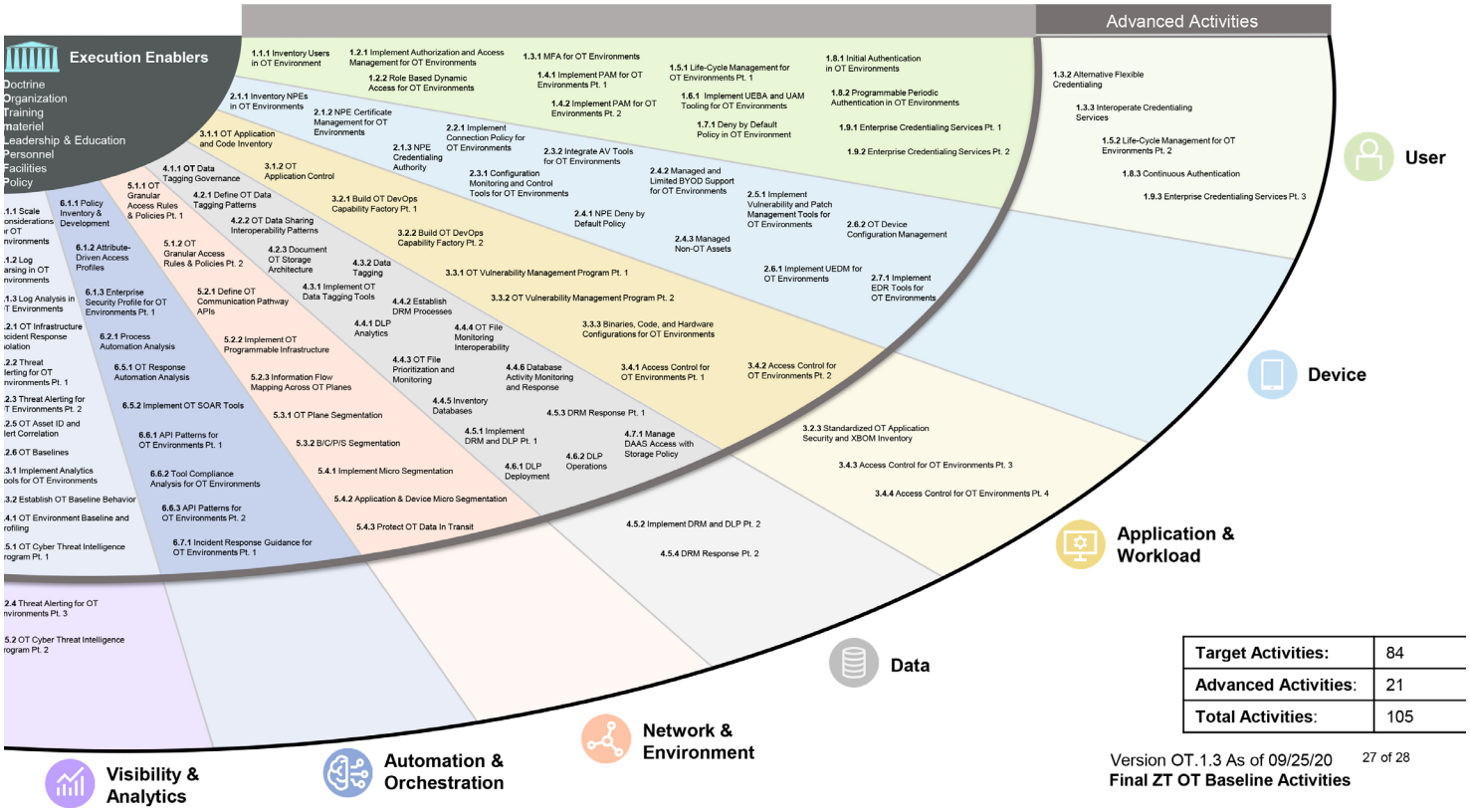
Zero Trust in the OT Domain

The Operational Context and the Fallacy of the Air Gap

The fundamental premise of the DoW's Zero Trust strategy is the recognition that the "trusted network" concept is obsolete. In traditional OT environments, security relied heavily on the Purdue Model's stratified architecture, assuming that separation between the Enterprise Layer (Level 4/5) and the Process Control Layer (Level 0-2) via firewalls or air gaps was sufficient. However, the digitization of industrial processes, the requirement for predictive maintenance data, and the integration of IIoT (Industrial Internet of Things) devices have perforated these boundaries.

The ZT for OT Activities and Outcomes explicitly states that applying standard IT security approaches to OT can be "ineffective and potentially dangerous". OT environments prioritize operational availability and safety above all else. Active scanning can crash a Programmable Logic Controller (PLC); automated patching can violate safety certifications; and multifactor authentication (MFA) can impede emergency response if not designed for the factory floor.

The DoW has adapted its initial IT-based Zero Trust requirements with new requirements tailored for OT, and released its "fan chart" with the requirements, shown below:



Target Activities:	84
Advanced Activities:	21
Total Activities:	105

Version OT.1.3 As of 09/25/20 27 of 28
Final ZT OT Baseline Activities

BlastWave's architecture addresses this dichotomy by functioning as a non-intrusive overlay. It does not require re-architecting the legacy switching fabric or upgrading the firmware of fragile controllers. Instead, it wraps these assets in a secure enclave, satisfying the DoW's requirement for "continuous and reliable operations" while enforcing rigorous access controls.

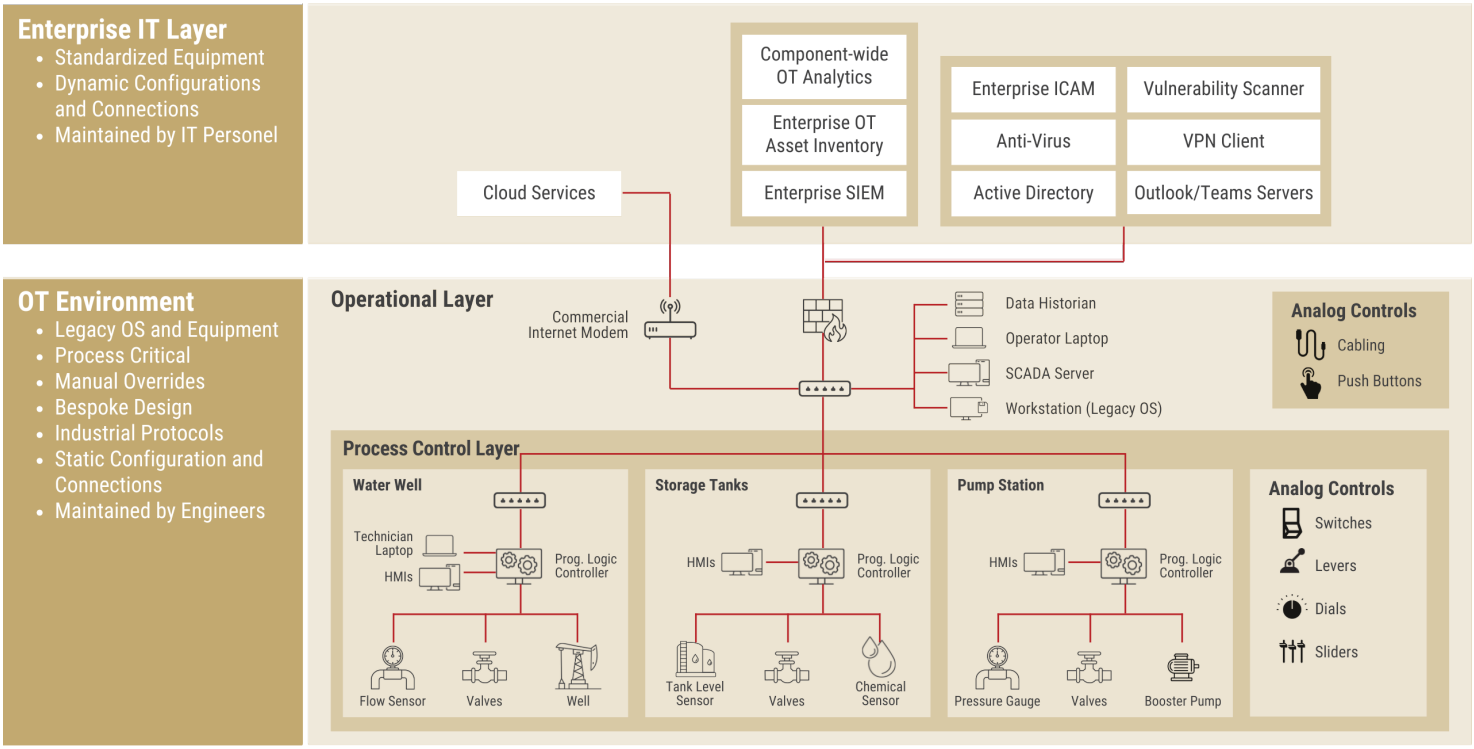
Defining the Protected Surface: Operational vs. Process Control Layers

The DoW guidance simplifies the traditional Purdue Model into two primary zones for Zero Trust implementation:

1. **The Operational Layer:** Encompassing layers 4 and 5, this includes HMIs, engineering workstations, and data historians. It is the interface between the IT world and the physical process.
2. **The Process Control Layer:** Encompassing layers 0-2, this includes the PLCs, sensors, actuators, and Safety Instrumented Systems (SIS) that physically manipulate the environment.

The mandate requires that ZT principles apply "up to and including the point of demarcation" and extend to the boundary of Weapon Systems or Defense Critical Infrastructure.

BlastWave acts as the unified policy enforcement engine across both layers. By deploying gateways at the ingress of the Operational Layer and shielding the Process Control Layer, BlastWave ensures that a compromise in the enterprise IT network cannot propagate laterally into the critical control zone, a direct response to the "prevent lateral movement" objective of the Target Level ZT activities. In fact, the entire Operational and Process Control Layers are undiscoverable to the Enterprise IT Layer due to BlastWave's Network Cloaking.



Target vs. Advanced Maturity Models

The compliance framework differentiates between Target Level and Advanced Level activities.

- **Target Level:** The minimum set of capabilities to manage known threats. These include activities like establishing inventories, implementing MFA, and enforcing microsegmentation.
- **Advanced Level:** Capabilities that enable adaptive responses, such as automated dynamic policy adjustment based on threat intelligence and behavioral analytics.

This analysis demonstrates that BlastWave enables fast Target Level compliance, providing an immediate "stop-gap" against lateral movement. Since BlastWave acts as an overlay ot the OT environment, it deploys far more quickly than firewall-based protection mechanisms, and the most challenging requirements to comply with (the protection and segmentation mandates) can lay the foundation for total compliance. At the same time, its API-first architecture lays the groundwork for Advanced Level orchestration.

The following sections specify which activities in the OT Fan Chart BlastWave directly impact compliance, as well as those in which BlastWave contributes to multi-system or API-based compliance.

Pillar 1: User Inventory and Access Control

The User pillar focuses on ensuring that only authorized human actors can access OT resources. Given the prevalence of shared accounts and static passwords in legacy OT, this is a significant modernization challenge.

Inventory and Credentialing (1.1.1.OT - 1.2.1.OT)

Requirement Analysis: The DoW mandates identifying all user accounts (local, privileged, and shared) and implementing an Authorized Credentialing Service. The goal is to migrate away from hardcoding local "admin/admin" credentials in PLCs towards a centralized Identity Provider (IdP).

BlastWave Compliance: BlastWave integrates with DoW-approved IdPs (e.g., Azure AD, Okta, CAC/PIV systems) to serve as the Policy Enforcement Point (PEP). While BlastWave is not the directory itself (Activity 1.1.1.OT is a process/partner requirement), it enforces the directory's authority.

If an admin disables a user in the central IdP, BlastWave immediately revokes their network access to the OT enclave, fulfilling the outcome of Activity 1.2.1.OT by ensuring rigorous enforcement of the attributes defined in the credentialing service before establishing a network session. BlastWave also supports a self-contained passwordless MFA and hardware (FIDO2 keys) options to supplement partner authentication.

Role-Based Dynamic Access (1.2.2.OT)

Requirement Analysis: This Target Level activity requires "strict role-based access controls before access or connection". It explicitly highlights remote and third-party access, requiring that vendors access only the specific equipment they maintain. This requirement means that traditional VPNs are not sufficient because they are often binary; once a vendor tunnels in, they usually have network-level visibility of the entire subnet.

BlastWave Solution: BlastWave replaces the VPN concentrator with a micro-perimeter. Through its "Software-Defined Perimeter" architecture, segmentation configurations grant an authenticated user access to a "Segment of One." A technician servicing a Siemens turbine sees only that turbine. They cannot ping the neighboring Rockwell controller or scan the network for other assets, thereby failing to satisfy the requirement to limit third-party access to the "account of least privilege required to perform work".

Multifactor Authentication (1.3.1.OT)

Requirement Analysis: MFA implementation is non-negotiable for Target Level ZT. However, the guidance acknowledges the need for "alternative authoritative credentialing solutions" where standard IT MFA might interfere with operations (e.g., in a clean room or tactical environment).

BlastWave Solution: BlastWave supports FIDO2-compliant passwordless authentication, allowing operators to authenticate using hardware tokens (like YubiKeys) or biometrics, which are faster and more secure than typing complex passwords on HMI touchscreens. By enforcing this MFA at the network ingress, BlastWave ensures that no packet reaches the OT asset until strong authentication is complete, fulfilling the "Verify Explicitly" principle.

Privileged Access Management (1.4.1.OT - 1.4.2.OT)

Requirement Analysis: The mandate requires procuring a PAM solution to manage critical privileged use cases.

BlastWave Solution or Partner Integration: BlastAccess can meet the requirements of a PAM solution that leverages BlastShield's authentication capabilities. For networks that already have a PAM in place, BlastWave serves as the secure transport layer for PAM. While a PAM product manages vaulting and credential rotation, BlastWave ensures that access to the PAM interface and from the PAM jump host to the target device is cryptographically secured and segmented, creating a defense-in-depth architecture in which the PAM solution is hidden from the general network and accessible only via BlastWave-secured tunnels.

Authentication Lifecycle (1.8.1.OT - 1.8.3.OT)

Requirement Analysis: The DoW requires authentication "at the start of every session" (Target) and eventually "continuous authentication" (Advanced).

BlastWave Solution: BlastWave enforces session-based authentication. Unlike a firewall rule that remains open based on IP address, a BlastWave ties a session to the user's cryptographic identity. If the risk profile changes (for instance, if the user moves to an unauthorized location), the session can be terminated immediately (Activity 1.8.3.OT). This capability moves the DoW closer to the "transaction-based authentication" goal of the Advanced state.

Pillar 2: Device Inventory and Protection

The Device pillar addresses the security of the vast array of hardware in the OT environment, from Windows-based engineering workstations to embedded PLCs and sensors.

Non-Person Entity (NPE) Management (2.1.1.OT - 2.1.3.OT)

Requirement Analysis: The DoW requires a centralized inventory of NPEs and the deployment of X.509 certificates to supported devices. The challenge in OT is that many legacy devices (Process Control Layer) cannot host certificates or agents.

BlastWave Solution: BlastWave solves the "unmanageable device" problem through its Gateway architecture. For legacy PLCs that cannot accept an agent or certificate, a BlastWave Gateway sits in front of them (physically or virtually). The Gateway holds the X.509 certificate on behalf of the legacy assets behind it. To the rest of the network, the legacy PLC is a fully authenticated, encrypted node, allowing the DoW to achieve the outcome of Activity 2.1.2.OT ("NPEs are managed via available PKI") without a "rip and replace" of legacy hardware.

Connection Policy and Compliance (2.2.1.OT)

Requirement Analysis: The guidance mandates "compliance-based network authorization". Devices should not be allowed to connect if they do not meet security standards.

BlastWave Solution: BlastWave does not natively include device posture checks in its admission policy. However, it is in our roadmap to validate with the EDR solution deployed on any system before initiating a secure connection. In this solution, before establishing a tunnel, the BlastWave agent checks the connecting device (e.g., a maintenance laptop) for required security attributes (such as running antivirus software, specific OS patches, or disk encryption). If the device fails the check, deny network access to the device until it passes the compliance check, enforcing the Target Level requirement for "compliance-based network authorization" at the edge.

Protection of Configuration Files (2.3.1.OT)

Requirement Analysis: Configuration control solutions must ensure that files (e.g., ladder logic) are not altered or uploaded except by authorized individuals.

BlastWave Solution: While BlastWave does not inspect the content of the ladder logic file (a Data pillar function), it secures the transport mechanism. By restricting who can connect to a PLC's engineering port, BlastWave significantly reduces the attack surface for unauthorized configuration changes. Only a user with the specific "Engineer" role and a verified device can open the connection required to upload new logic. BlastAccess acts as a PAM to allow or disallow file transfers to the remote system, providing an additional barrier against malware when using a remote desktop.

BYOD and Non-GFE Assets (2.4.2.OT - 2.4.3.OT)

Requirement Analysis: Bring Your Own Device (BYOD) and non-Government Furnished Equipment (non-GFE) are generally restricted but may be authorized with deviation processes.

BlastWave Solution: BlastWave authenticates secure BYOD needed for 3rd-party maintenance activities on a military installation. By creating an encrypted, containerized session from the BYOD asset to the specific OT resource, BlastWave prevents the unmanaged device from laterally exploring the network. The "Default Drop" policy ensures that when a malware-compromised BYOD device attempts to scan the network, it fails, protecting the OT environment from the "dirty" device.

.

Endpoint Detection and Response (2.7.1.OT)

Requirement Analysis: The implementation of EDR tools is a Target Level requirement.

Partner Integration: BlastWave is not an EDR. However, it enhances EDR effectiveness. By microsegmenting the network, BlastWave forces an attacker to execute code on endpoints to move laterally (since network scanning is blocked), increasing the likelihood that the deployed EDR solution (e.g., CrowdStrike, SentinelOne) will detect the adversary's behavior. BlastWave and EDR function as complementary controls: BlastWave protects the network, and EDR protects the compute host.

Pillar 3: Applications and Workload

This pillar focuses on securing the software that runs the critical infrastructure, from SCADA masters to HMI applications.

Application Inventory and Control (3.1.1.OT - 3.1.2.OT)

Requirement Analysis: The DoW requires an inventory of all applications and the implementation of application control solutions to prevent unauthorized execution.

Partner Integration: This is primarily the domain of Allowlisting software (e.g., Carbon Black, McAfee Application Control). BlastWave's role is to ensure that the management consoles for these application control systems are themselves secured and accessible only to authorized administrators, preventing adversaries from disabling the protections.

Application and Code Security (3.2.1.OT - 3.2.3.OT)

Requirement Analysis: These activities focus on DevOps and DevSecOps processes, including CI/CD pipelines and Software Bill of Materials (SBOM).

BlastWave Solution: For OT environments moving toward modern DevOps (e.g., updating containerized applications on edge gateways), BlastWave can secure the CI/CD pipeline. By ensuring that the code repository and the build server communicate only through mutually authenticated tunnels, BlastWave prevents "man-in-the-middle" attacks on the software supply chain during deployment.

Access Control for Workloads (3.4.1.OT)

Requirement Analysis: All applications and capabilities must support a complete Attribute-Based Access Control (ABAC) solution.

BlastWave Solution: BlastWave extends ABAC to the network layer. Traditionally, firewalls use static rules (IP A can talk to IP B). BlastAccess can extend that to policies based on application attributes on BlastAccess servers and a BlastShield policy. For example, a policy can state that "Only the SCADA Server Application can communicate with the Historian." In this scenario, only the certified application is present on the server, preventing rogue applications from being used. BlastWave can block any upload to the remote desktop, enforcing ABAC at the workload level and blocking any unauthorized protocols from that server as well.

Pillar 4: Data

The Data pillar is often the most challenging in OT due to the prevalence of proprietary, binary protocols that resist standard tagging and inspection.

Data Tagging and DRM (4.1.1.OT - 4.5.4.OT)

Requirement Analysis: The mandate calls for governance of data tagging, DRM, and Data Loss Prevention (DLP) solutions.

Gap Analysis: BlastWave acts as the "pipe," not the "packet inspector." It does not open the payload to read data tags or enforce DRM.
Partner Integration: The DoW requires partner solutions for Data Classification (e.g., Titus, Boldon James) and DLP (e.g., Symantec, Forcepoint). BlastWave supports these tools by ensuring that the data flows through the inspection points defined by the architecture. For example, BlastWave can force all file transfer traffic to route through a DLP scanning node before reaching its destination, facilitating the enforcement of Activity 4.6.1.OT (DLP Deployment).

Database Monitoring (4.4.5.OT - 4.4.6.OT)

Requirement Analysis: Monitoring of databases (e.g., Historians) for anomalous activity is required.

BlastWave Role: BlastWave protects the database from unauthorized connection attempts. While it does not monitor SQL queries themselves (a Database Activity Monitoring function), it ensures that only authorized application servers can open connections to the database port, drastically reducing the risk of SQL injection attacks originating from unauthorized hosts.

The Data pillar is often the most challenging in OT due to the prevalence of proprietary, binary protocols that resist standard tagging and inspection.

Pillar 5: Network

This pillar represents the core of the BlastWave value proposition. The DoW guidance emphasizes segmentation, encryption, and the removal of implicit trust, all native capabilities of the BlastWave platform.

Granular Access Rules and Policy (5.1.1.OT - 5.1.2.OT)

Requirement Analysis: The mandate requires the creation of "granular access rules and policies" and the definition of data flow patterns.

BlastWave Solution: BlastWave operates on a "Zero Trust Default Drop" model. No traffic is allowed unless explicitly permitted, forcing the creation of granular rules. Unlike a firewall, where "Allow Any" rules often creep in for troubleshooting, BlastWave requires specific identity-to-identity mapping, aligning perfectly with the requirement to define persistent and ephemeral data flows. BlastWave makes this simple in large-scale OT environments with thousands of devices by creating user and device groups that drastically accelerate and simplify configuration for least-privilege access.

Programmable Infrastructure (5.2.2.OT)

Requirement Analysis: DoW Components must implement programmable communication pathways that utilize Segmentation Gateways and Authentication Decision Points integrated into SDN.

BlastWave Solution: BlastWave is a programmable SDN overlay. It functions as a distributed Segmentation Gateway. The "Authentication Decision Point" is the BlastWave Orchestrator, which validates identities, and the "Segmentation Gateway" is the BlastWave Edge/Gateway software. This architecture allows policies to be updated programmatically via an API (fulfilling 6.6.1.OT) without manually configuring Access Control Lists (ACLs) on hundreds of physical switches.

OT Plane Segmentation (5.3.1.OT)

Requirement Analysis: The guidance mandates segmentation between control, data, and management planes. In legacy OT, this was done physically (separate cables).

BlastWave Solution: BlastWave enables Cryptographic Plane Segmentation between gateways and/or remote user connections, ensuring that all traffic leaving the local network is encrypted. Further segmentation is policy-based. Traffic from specific devices to remote devices or users must be explicitly allowed by policy, and a system must be prohibited from sending or receiving management-plane traffic unless approved. If the end device supports tagged VLANs or multiple connections, the BlastShield solution will segment each connection separately, with unique policies applied to each.

Microsegmentation (5.4.1.OT - 5.4.2.OT)

Requirement Analysis: This is a critical Target Level activity. Microsegmentation is essential to OT networks, where lateral movement is the most common malware technique. Nation-state hackers leverage lateral movement to live off the land and hide from detection systems.

BlastWave Solution: BlastWave enables microsegmentation down to the individual host level, independent of network VLANs. In an OT network, software-defined segmentation ensures that re-IPing devices to create smaller subnets is not needed, reducing operational risks. BlastWave overlays the existing flat network, logically enforcing segmentation. For example, HMI-A can only talk to PLC-A, even if HMI-B and PLC-B are on the same subnet, preventing a compromised HMI from attacking other controllers (Lateral Movement Prevention).

Data in Transit Protection (5.4.3.OT)

Requirement Analysis: The DoW requires protection for data in transit per policy. Protocols like Modbus, DNP3, and Telnet send credentials and data in clear text, so when those communications cross insecure boundaries, encryption must be used to secure the traffic.

BlastWave Solution: BlastWave's microsegmentation (when paired with L2 port isolation mode) ensures that even local LAN traffic is not broadcast across the entire network, but instead managed with BlastShield's segmentation policies. BlastWave encapsulates all traffic leaving the local area network in AES-256-encrypted tunnels, effectively upgrading legacy, clear-text protocols to military-grade encryption standards without requiring changes to endpoint devices. This "Protocol Cloaking" ensures that even if an adversary gains physical access to the network switch, they cannot sniff sensitive operational commands.

Pillar 6: Automation and Orchestration

The scale of DoW operations requires that security be automatable. The "human in the loop" remains critical for OT, but orchestration is the future in an automated OT environment.

Policy Inventory and Development (6.1.1.OT - 6.1.4.OT)

Requirement Analysis: The DoW requires a catalog of access control policies and the establishment of attribute-driven access profiles.

BlastWave Solution: The BlastWave Orchestrator serves as the centralized repository for all access policies. It provides a single pane of glass where administrators can view, audit, and modify access rules across the entire OT estate. This centralization simplifies the "Policy Inventory" requirement by replacing decentralized firewall configurations with a unified policy database.

SOAR Integration (6.5.2.OT)

Requirement Analysis: The implementation of Security Orchestration, Automation, and Response (SOAR) tools is a Target Level activity.

Partner Integration: BlastWave integrates with SOAR platforms (e.g., Splunk SOAR, Palo Alto XSOAR) via REST API. When the SOAR platform detects a threat (e.g., from the SIEM), it can trigger a BlastWave policy change to isolate the infected host. BlastWave enables the Response part of SOAR by providing the enforcement mechanism that the SOAR tool drives.

API Patterns and Interoperability (6.6.1.OT - 6.6.4.OT)

Requirement Analysis: The mandate requires establishing API standards to ensure tool interoperability.

BlastWave Solution: BlastWave is built on an API-first architecture. Every function available in the GUI is accessible via API, allowing DoW agencies to create custom workflows or integrate BlastWave into existing "Single Pane of Glass" dashboards, ensuring that the OT security stack acts as a cohesive system rather than a collection of point products.

Pillar 7: Visibility and Analytics

You cannot secure what you cannot see. This pillar focuses on logging, monitoring, and threat intelligence.

Log Parsing and Analysis (7.1.2.0T - 7.1.3.0T)

Requirement Analysis: DoW Components must identify, collect, and map all log sources.

BlastWave Solution: BlastWave generates high-fidelity access logs. It records who connected, from where, to what, for how long, and denied access. BlastWave exports the logs in standard formats (Syslog) to the Enterprise SIEM. While BlastWave is not the log parser (Activity 7.1.2.0T is a SIEM function), it provides the critical "Access Data" that the SIEM needs to detect anomalies.

Incident Response Isolation (7.2.1.0T)

Requirement Analysis: A critical requirement is the ability to "physically or logically" disconnect infrastructure during an incident to prevent further damage.

BlastWave Solution: BlastWave provides a "Digital Kill Switch." In the event of a detected compromise, security teams can instantly revoke the certificates associated with a specific zone, site, or user group, logically air-gapping the compromised segment within milliseconds, stopping the spread of the attack (e.g., ransomware) without requiring personnel to pull cables at remote sites. This capability is essential for meeting the "prevent further intrusion" requirement of 7.2.1.0T.

Threat Alerting (7.2.2.0T - 7.2.4.0T)

Requirement Analysis: Implementation of SIEM and threat alerting rules is required.

Partner Integration: BlastWave feeds the SIEM. The BlastWave logs are particularly valuable for "Deviation Anomaly" detection (7.2.3.0T). Since BlastWave enforces a Zero Trust model, any denied connection attempt is a high-fidelity indicator of compromise (IoC). In a trusted network, a denied packet might be noise; in a BlastWave network, it means someone is scanning a dark network. Feeding this signal to a partner SIEM allows for rapid, high-confidence alerting.

Compliance Analysis: BlastWave Compliance

The following table summarizes the specific requirements that BlastWave addresses directly through its native capabilities.

Activity ID	Activity Name	Requirement Summary	BlastWave Solution Architecture
1.2.1.0T	Authorization & Access Mgmt	Authorize users based on attributes; enforce policy.	**SDP Gateway:** Enforces attribute-based access policy at ingress. Users without valid attributes (via IdP) are invisible to the network.
1.2.2.0T	Role-Based Dynamic Access	Strict role-based access for remote/third-party; least privilege.	**Micro-Perimeter:** Creates "Segment of One" tunnels. Vendors see only the specific asset they are authorized to maintain, not the subnet.
1.3.1.0T	MFA for OT Environments	Implement MFA or approved alternative (technical/procedural).	**Biometric MFA:** Enforces FIDO2/Biometric authentication at the gateway, enabling strong auth even in restrictive OT environments.
1.8.1.0T	Initial Authentication	Authenticate users at the start of every session.	**Session-Based Access:** Every connection request is cryptographically verified and authenticated before a TCP handshake is allowed.
1.8.2.0T	Periodic Authentication	Programmable periodic authentication on a session basis.	**Time-Bound Policies:** Policies can force re-authentication after set intervals, fulfilling the periodic check requirement.
2.1.2.0T	NPE Certificate Management	Deploy X.509 certificates to supported NPEs.	**Automated PKI:** Automatically issues and rotates X.509 certificates for all gateways and agents, managing the identity lifecycle for the device.
2.2.1.0T	Connection Policy NPE Deny by Default	Enforce compliance-based network authorization.	**Posture Checks:** Roadmap to verify device health (OS patch level, AV status) before allowing tunnel establishment. Non-compliant devices are blocked.
2.4.1.0T	NPE Deny by Default	Block unauthorized remote/local NPE access.	**Default-Drop Firewall:** Only explicitly allowed, authenticated flows are permitted; all other traffic is dropped by default
2.4.2.0T	BYOD Support	Non-GFE devices must follow deviation/risk processes.	**Secure Container:** Isolates BYOD sessions in encrypted tunnels, preventing lateral contamination from unmanaged devices.
3.4.1.0T	Access Control (ABAC)	Applications must support full ABAC.	**Network-Layer ABAC:** Enforces attribute-based control at the packet level, effectively wrapping legacy apps in an ABAC layer.
5.1.1.0T	OT Granular Access Rules	Create granular access rules and policies.	**Host-to-Host Policy:** Enables definition of policies at the individual asset level, independent of network topology or IP addressing.
5.2.2.0T	Programmable Infrastructure	Implement Segmentation Gateways integrated into SDN.	**SDN Overlay:** Acts as the programmable overlay, providing API-driven control of distributed segmentation gateways.
5.3.1.0T	OT Plane Segmentation	Segment control, data, and management planes.	**Cryptographic Isolation:** Separates management and control traffic into distinct segments, ensuring logical-plane separation.
5.3.2.0T	B/C/P/S Segmentation	Limit lateral movement across Base, Camp, Post, Station.	**SD-WAN Fabric:** Extends microsegmentation across the WAN, isolating geographically distinct sites while sharing a backhaul.
5.4.1.0T	Micro Segmentation	Segment VLANs, devices, endpoints, services.	**Host Isolation:** Decouples security from the VLAN. Segmentation is applied at the host/gateway level, eliminating lateral movement risks.
5.4.3.0T	Protect OT Data in Transit	Encrypt data in transit per policy.	**Universal Encryption:** Encapsulates all traffic (including legacy clear-text protocols) in AES-256 encrypted tunnels.
6.1.1.0T	Policy Inventory	Catalog access control policies.	**Centralized Policy Engine:** Provides a single, auditable repository for all access rules across the OT estate.
6.6.1.0T	API Patterns	Establish API standards for interoperability.	**RESTful API:** Full API coverage allows for integration with DoW automation stacks and dashboards.
7.2.1.0T	Incident Response Isolation	Capability to logically disconnect infrastructure during incidents.	**Instant Revocation:** Enables "Digital Kill Switch" capability to logically air-gap compromised zones instantly via policy update.
7.5.1.0T	OT CTI Program	Integrate data feeds with enforcement points.	**Dynamic Blocklists:** Can ingest threat intelligence feeds (IPs, domains) to block known malicious actors at the edge automatically.

Partner Ecosystem Gap Analysis

Zero Trust is a journey that requires a stack of technologies working in concert. While BlastWave provides the "Connect" and "Protect" layers, the following chart identifies the requirements where BlastWave acts as a consumer or integrator, necessitating a partner solution to fulfill the DoW mandate.

Partner Requirements Chart

Activity ID	Requirement Summary	Gap Analysis / BlastWave Role	Required Partner Product Class
1.1.1.OT	**Inventory Users:** Document inventory of all accounts (local, privileged, service).	BlastWave consumes identity but does not crawl devices to list local accounts.	**Identity Governance & Administration (IGA)** (e.g., SailPoint, Saviynt)
1.9.1.OT	**Enterprise Credentialing:** Implement DoW-approved Credentialing Services (IdP).	BlastWave relies on the IdP for user attributes. It is not an identity directory.	**Identity Provider (IdP)/PKI** (e.g., Okta, Azure AD, DoW PKI, Keycloak)
2.1.1.OT	**Inventory NPEs:** Centralized inventory for NPEs; passive discovery.	BlastWave secures recognized devices but is not a passive asset-discovery engine.	**OT Asset Discovery & Visibility** (e.g., Dragos, Armis, Nozomi, DarkTrace) Claroty, Industrial Defender
2.3.1.OT	**Configuration Monitoring:** Ensure config files (ladder logic) are not altered.	BlastWave protects the connection to the device but does not inspect file payloads.	**OT Change Management** (e.g., Rockwell AssetCentre, Auvesy-MDT) ServiceNow
2.5.1.OT	**Vulnerability Management:** Patch standards; risk-based assessment.	BlastWave mitigates risk via cloaking but does not scan for CVEs or apply patches.	**Vulnerability Management** (e.g., Darktrace, Nozomi, Dragos, Armis) Claroty, Industrial Defender
2.7.1.OT	**Implement EDR:** EDR solutions for Operational IT and Process Control.	BlastWave protects the network; EDR protects the host execution environment.	**Endpoint Detection & Response (EDR)** (e.g., CrowdStrike, Nozomi, DarkTrace) SentinelOne
3.1.1.OT	**App Inventory:** Inventory software applications, cloud, on-prem.	BlastWave controls app access but does not inventory installed software.	**Software Asset Management (SAM)** (e.g., ServiceNow, Flexera)
3.2.1.OT	**DevOps Capability:** CI/CD and Infrastructure as Code pipelines.	BlastWave secures the pipeline connection, but is not the CI/CD tool itself.	**DevOps/CI/CD Platform** (e.g., GitLab, Jenkins, CloudBees)
4.2.1.OT	**Data Tagging:** Define tagging, labeling, and classification patterns.	BlastWave transports data packets; it does not tag data inside the payload.	**Data Classification & Governance** (e.g., Boldon James, Titus)
4.4.1.OT	**DLP Analytics:** Establish DLP types and recognition patterns.	BlastWave encrypts tunnels but does not perform Deep Packet Inspection (DPI) for DLP.	**Data Loss Prevention (DLP)** (e.g., Symantec DLP, Forcepoint, McAfee)
4.4.5.OT	**Database Inventory:** Identify and document databases.	BlastWave restricts access to DB ports but does not scan for DB instances.	**Database Activity Monitoring (DAM)** (e.g., Imperva, IBM Guardium)
6.5.2.OT	**Implement SOAR:** Procure SOAR solutions; human-in-the-loop.	BlastWave acts as the enforcement arm for SOAR but is not the orchestration engine.	**SOAR Platform** (e.g., Splunk SOAR, Swimlane)
7.2.2.OT	**Threat Alerting (SIEM):** Implement a SIEM and ingest CTI feeds.	BlastWave sends logs to SIEM but does not act as the primary log aggregator.	**SIEM** (e.g., Splunk, Elastic, Microsoft Sentinel)
7.3.1.OT	**Implement Analytics:** Tools to analyze baseline behavior.	BlastWave provides network data; specific behavioral analytics requires specialized tools.	**User & Entity Behavior Analytics (UEBA)** (e.g., Dragos, Nozomi, Darktrace, Armis) Claroty, Industrial Defender

Overcoming OT-Specific Implementation Hurdles

The ZT for Operational Technology Activities and Outcomes document explicitly warns of the dangers of applying IT-centric security tools to OT environments. This section analyzes how BlastWave's architecture mitigates these specific risks.

The "Brownfield" Reality

Most DoW OT environments are "brownfield" deployments, a mix of modern IIoT sensors and 30-year-old legacy controllers running unpatched firmware. Re-architecting these networks to achieve segmentation (Activity 5.3.1.OT) using traditional firewalls requires changing IP addresses, re-cabling, and extensive downtime, luxuries that mission-critical systems cannot afford.

BlastWave Strategic Advantage:

BlastWave operates as a transparent bridge or gateway, enabling quick deployment into an existing network segment without requiring IP changes to the protected assets. The "Invisible Overlay" capability allows DoW engineers to implement Zero Trust segmentation immediately, creating a secure enclave around legacy assets without disrupting the underlying process communications. BlastWave's secure overlay directly addresses the DoW's need for "flexible and adaptable" solutions that do not rigidly adhere to the 5-layer Purdue topology, resulting in faster deployment and lower maintenance requirements.

Safety System Isolation

Safety Instrumented Systems (SIS) are the last line of defense against physical catastrophe. The DoW guidance implies that ZT implementation must not compromise safety performance.

BlastWave Strategic Advantage:

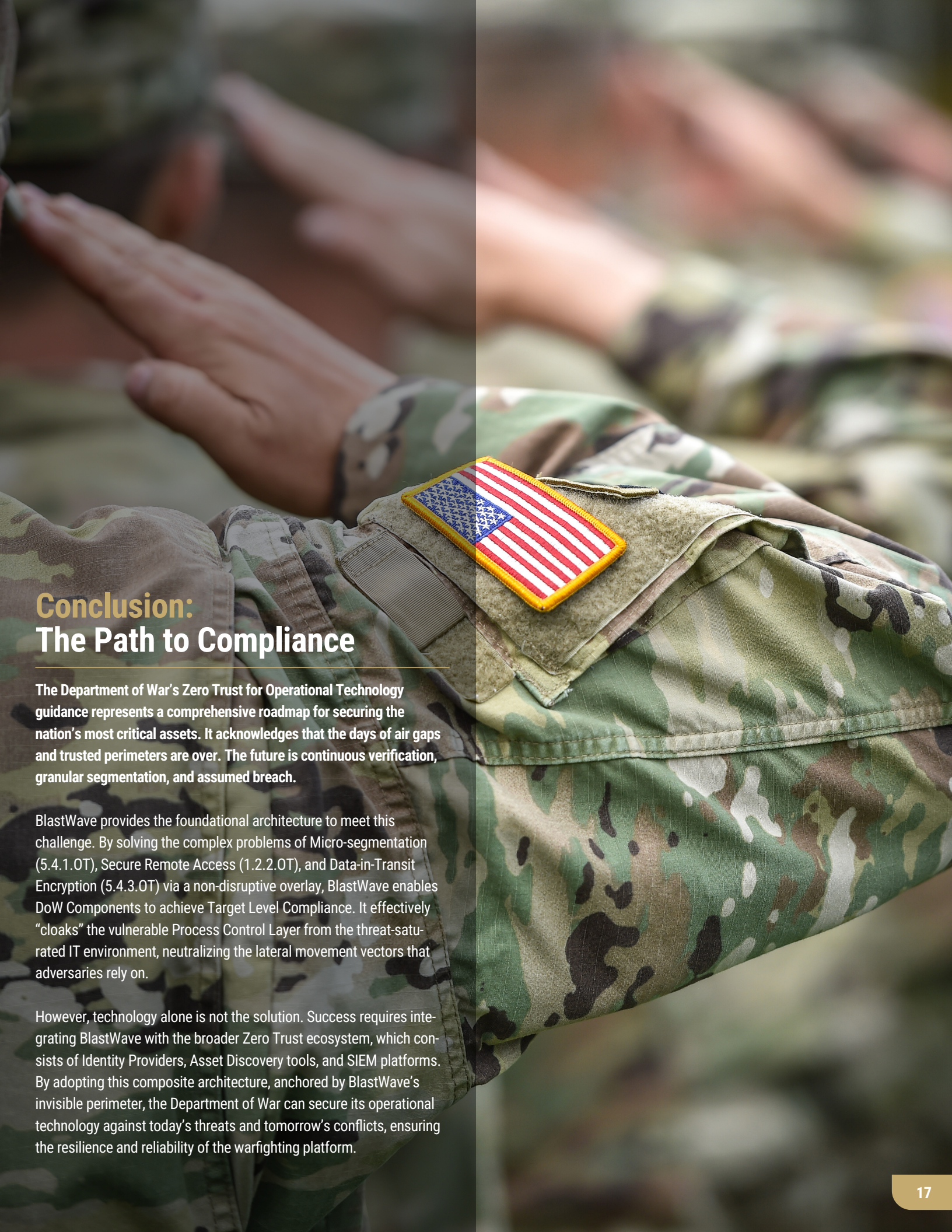
BlastWave supports the creation of "Safety Zones" that are logically isolated from the rest of the Operational Layer. By using the "Deny by Default" policy (Activity 1.7.1.OT), BlastWave ensures that no external entity (not even a compromised administrator workstation) can communicate with the SIS unless explicitly authorized and authenticated with high-assurance credentials, protecting the integrity of the safety systems while allowing for necessary data extraction (e.g., for compliance reporting) through strictly controlled, unidirectional-style tunnels.

Bandwidth Constraints at the Tactical Edge

The requirement to support "Base, Camp, Post, and Station" implies deployment in tactical environments where bandwidth is scarce, and latency is critical. Traditional VPNs and heavy encryption protocols can introduce unacceptable latency for real-time control loops.

BlastWave Strategic Advantage:

BlastWave utilizes a lightweight, peer-to-peer mesh architecture. Unlike hub-and-spoke VPNs that backhaul traffic to a central concentrator (adding latency), BlastWave facilitates direct, encrypted connections between the user and the resource. The protocol overhead is minimal, ensuring that the "significant need for continuous and reliable operations" is met even over constrained satellite or radio links.



Conclusion:
The Path to Compliance

The Department of War's Zero Trust for Operational Technology guidance represents a comprehensive roadmap for securing the nation's most critical assets. It acknowledges that the days of air gaps and trusted perimeters are over. The future is continuous verification, granular segmentation, and assumed breach.

BlastWave provides the foundational architecture to meet this challenge. By solving the complex problems of Micro-segmentation (5.4.1.OT), Secure Remote Access (1.2.2.OT), and Data-in-Transit Encryption (5.4.3.OT) via a non-disruptive overlay, BlastWave enables DoW Components to achieve Target Level Compliance. It effectively "cloaks" the vulnerable Process Control Layer from the threat-saturated IT environment, neutralizing the lateral movement vectors that adversaries rely on.

However, technology alone is not the solution. Success requires integrating BlastWave with the broader Zero Trust ecosystem, which consists of Identity Providers, Asset Discovery tools, and SIEM platforms. By adopting this composite architecture, anchored by BlastWave's invisible perimeter, the Department of War can secure its operational technology against today's threats and tomorrow's conflicts, ensuring the resilience and reliability of the warfighting platform.

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

v20250808

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.

©2025 BlastWave Inc.

BlastWave

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