WHITE PAPER

# BlastWave and Nozomi Networks

## Solution for the Department of War Zero Trust Operational Technology Compliance

NOZOMI NETWORKS

BlastWave

## TL:DR

**Directive-Type Memorandum (DTM) 25-003 (July 2025), and its follow-on "Zero Trust for Operational Technology Activities and Outcomes" guidance (November 2025) establishes a new architecture for Department of War (DoW) OT networks. The foundational premise of this mandate is the obsolescence of the "trusted network" concept, particularly the stratified Purdue Model, in favor of a zero-trust architecture (ZTA) that emphasizes granular segmentation and the assumption of breach.**

The DoW has established a "fan chart" of 105 distinct activities (84 Target and 21 Advanced), organized across seven pillars: User, Device, Applications & Workload, Data, Network & Environment, Automation & Orchestration, and Visibility & Analytics.

To meet these requirements without compromising operational continuity, a joint solution that combines Nozomi Networks' visibility and detection capabilities with BlastWave's Zero Trust identity enforcement and cloaking mechanisms provides a comprehensive approach.

This architecture provides 85 out of 105 total activities (81% total coverage), specifically addressing 69 of the 84 Target Level requirements and 16 of the 21 Advanced activities. This technical analysis explores the synergy of the "OT Intelligence Layer" and the "Identity Enforcement Layer" in the context of the DoW mandate.

This approach solves the primary challenge of OT zero trust: how to implement rigorous security without disrupting operations. By "cloaking" vulnerable legacy assets and providing a "Digital Kill Switch" for incident response, the Nozomi Networks and BlastWave solution enables the DoW to secure its most critical infrastructure against today's threats and tomorrow's conflicts. As components work toward the September 30, 2027, Target Level compliance deadline, this joint architecture provides the essential "air cover" and "connective tissue" needed to ensure the resilience and reliability of the operational environment.

# CONTENTS

# The Convergence of Intelligence and Enforcement

**The joint Nozomi Networks and BlastWave architecture is built upon the premise that visibility without enforcement is insufficient, and enforcement without real-time monitoring is ineffective in OT. Nozomi Networks provides deep, OT-native visibility and behavioral analytics, functioning as the central intelligence layer that identifies assets, protocols, and anomalies.**

BlastWave acts as the software-defined perimeter (SDP) and microsegmentation fabric, providing the "air cover" needed to protect legacy assets while agencies implement longer-term Target and Advanced requirements.

This joint solution simplifies the Purdue Model by separating it into two primary implementation zones: the Operational Layer (supervisory systems, HMIs, and engineering workstations) and the Process Control Layer (PLCs, sensors, and actuators).

By deploying Nozomi Guardian sensors for telemetry and BlastWave gateways for asset isolation, the solution ensures that a compromise in the enterprise network cannot propagate laterally into critical control zones. Just because an IT manager deploys a firewall does not mean that their network is now fully protected.

| Joint Solution Strategic Alignment | Nozomi Networks Platform (Operational Visibility) | BlastWave SDP (Enforcement) |
|---|---|---|
| **Pillar Focus** | Visibility & Analytics, Device, Network Enabler | Network & Environment, User, Device Protection |
| **Technical Mechanism** | Passive & Safe Active Scanning, AI/ML Behavior Baselines | Cryptographic Overlay, Network Cloaking, Microsegmentation |
| **OT Constraint Mitigation** | Safety-centric design, air-gapped support | Non-intrusive overlay, no IP changes, bandwidth optimization. |
| **Key Capability** | OT-aware UEBA and threat intelligence | Digital Kill Switch and "Segment of One" access |

The combined Nozomi Networks and BlastWave solution addresses the "brownfield" reality of military installations, where modern IIoT sensors often coexist with 30 year old controllers running unpatched firmware. The Nozomi platform identifies these vulnerabilities, while BlastWave "cloaks" them from the network, reducing the effective attack surface without requiring a "rip and replace" of mission critical hardware.

**User**

| Execution Enablers | |
|---|---|
| Doctrine<br>Organization<br>Training Material<br>Leadership and Education<br>Personnel<br>Facilities<br>Policy | **1.1.1** Inventory Users in OT Environment<br>**1.2.1** Implement Authorization and Access Management for OT Environments<br>**1.2.2** Role-Based Dynamic Access for OT Environments<br>**1.3.1** MFA for OT Environments<br>**1.4.1** Implement PAM for OT Environments Pt.1<br>**1.4.2** Implement PAM for OT Environments Pt.2<br>**1.5.1** Life-Cycle Management for OT Environments<br>**1.6.1** Implement UEBA and UAM Tooling for OT Environments<br>**1.7.1** Deny by Default Policy in OT Environment<br>**1.8.1** Initial Authentication in OT Environments<br>**1.8.2** Programmable Periodic Authentication in OT Environments<br>**1.9.1** Enterprise Credentialing Services Pt.1<br>**1.9.2** Enterprise Credentialing Services Pt.2 |
| **Advanced Activities** | **1.3.2** Alternative Flexible Credentialing<br>**1.3.3** Interoperate Credentialing Services<br>**1.5.2** Life-Cycle Management for OT Environments Pt.2<br>**1.8.3** Continuous Authentication<br>**1.9.3** Enterprise Credentialing Services Pt.3 |

**COLOR KEY: COMPLIANCE PARTIAL ENABLES**

**Joint Compliance:** TARGET: 52 ADVANCED: 12
**Partial:** TARGET: 4 ADVANCED: 1
**Enables:** TARGET: 13 ADVANCED: 3
**OT ZT Totals:** TARGET: 69 ADVANCED: 16
**Total: 85/105**



NOZOMI NETWORKS BlastWave

# Analysis of DoW OT Zero Trust Requirements

**Overall, the joint solution delivers compliance, partially supports compliance, or supports compliance for 85 of 105 total activities (81% total coverage), specifically addressing 69 of the 84 Target Level requirements and 16 of the 21 Advanced activities. The solution chart is shown below and is detailed for each section of the requirements.**

| Device | Application and Workload | Data | Network and Environment | Automation and Orchestration | Visibility and Analytics |
|---|---|---|---|---|---|
| **2.1.1** Inventory NPEs in OT Environments<br>**2.1.2** NPE Certificate Management for OT Environments<br>**2.1.3** NPE Credentialing Authority<br>**2.2.1** Implement Connection Policy for OT Environments<br>**2.3.1** Configuration Monitoring and Control Tools for OT Environments<br>**2.3.2** Integrate AV Tools for OT Environments<br>**2.4.1** NPE Deny by Default Policy<br>**2.4.2** Managed and Limited BYOD Support for OT Environments<br>**2.4.3** Managed Non-OT Assets<br>**2.5.1** Implement Vulnerability and Patch Management Tools for OT Environments<br>**2.6.1** Implement UEDM for OT Environments<br>**2.6.2** OT Device Configuration Management<br>**2.7.1** Implement EDR Tools for OT Environments | **3.1.1** OT Application and Code Inventory<br>**3.1.2** OT Application Control<br>**3.2.1** Build OT DevOps Capability Factory Pt.1<br>**3.2.2** Build OT DevOps Capability Factory Pt.2<br>**3.3.1** OT Vulnerability Management program Pt.1<br>**3.3.2** OT Vulnerability Management program Pt.2<br>**3.3.3** Binaries, Code, and Hardware Configurations for OT Environments<br>**3.4.1** Access Control for OT Environments Pt.1<br>**3.4.2** Access Control for OT Environments Pt.2 | **4.1.1** Data Tagging Governance<br>**4.2.1** Define OT Data Tagging Patterns<br>**4.2.2** OT Data Sharing Interoperability Patterns<br>**4.2.3** Document OT Storage Architecture<br>**4.3.1** Implement OT Data Tagging Tools<br>**4.3.2** Data Tagging<br>**4.4.1** DLP Analytics<br>**4.4.2** Establish DRM Processes<br>**4.4.3** OT File Prioritization and Monitoring<br>**4.4.4** OT File Monitoring Interoperability<br>**4.4.5** Inventory Databases<br>**4.4.6** Database Activity Monitoring and Response<br>**4.5.1** Implement DRM and DLP Pt.1<br>**4.5.3** DRM Response Pt.1<br>**4.6.1** DLP Deployment<br>**4.6.2** DLP Operations<br>**4.7.1** Manage DAAS Access with Storage Policy | **5.1.1** OT Granular Access Rules & Policies Pt.1<br>**5.1.2** OT Granular Access Rules & Policies Pt.2<br>**5.2.1** Define OT Communication Pathway APIs<br>**5.2.2** Implement OT Programmable Infrastructure<br>**5.2.3** Information Flow Mapping Across OT Planes<br>**5.3.1** OT Plane Segmentation<br>**5.3.2** B/C/P/S Segmentation<br>**5.4.1** Implement Segmentation<br>**5.4.2** Application & Device Micro Segmentation<br>**5.4.3** Protect OT Data in Transit | **6.1.1** Policy Inventory & Development<br>**6.1.2** Attribute-Driven Access Profiles<br>**6.1.3** Enterprise Security Profile for OT Environments Pt.1<br>**6.2.1** Process Automation Analysis<br>**6.2.2** Tool Interoperability for OT Environments<br>**6.3.1** Implement OT Data Tagging and Classification tools<br>**6.5.1** OT Response Automation Analysis<br>**6.5.2** Implement OT SOAR Tools<br>**6.6.1** API Patterns for OT Environments Pt.1<br>**6.6.2** Tool Compliance Analysis for OT Environments<br>**6.6.3** API Patterns for OT Environments Pt.2<br>**6.7.1** Incident Response Guidance for OT Environments Pt.1 | **7.1.1** Scale Considerations for OT Environments<br>**7.1.2** Log Parsing in OT Environments<br>**7.1.3** Log Analysis in OT Environments<br>**7.2.1** OT Infrastructure Incident Response Isolation<br>**7.2.2** Threat Alerting for OT Environments Pt.1<br>**7.2.3** Threat Alerting for OT Environments Pt.2<br>**7.2.5** OT Asset ID and Alert Correlation<br>**7.2.6** OT Baselines<br>**7.3.1** Implement Analytics Tools for OT Environment<br>**7.3.2** Establish OT Baseline Behavior<br>**7.4.1** OT Environment Baseline and Profiling<br>**7.5.1** OT Cyber Threat Intelligence Program Pt.1 |
| **2.1.4** Automated NPE Discovery<br>**2.3.3** OT Device Security Stack with C2C<br>**2.7.2** Implement Extended Detection & Response (XDR) tools for OT Environments | **3.2.3** Standardized OT Application Security and XBOM Inventory<br>**3.4.3** Access Control for OT Environments Pt.3<br>**3.4.4** Access Control for OT Environments Pt.4 | **4.5.2** Implement DRM and DLP Pt.2<br>**4.5.4** DRM Response Pt.2 | | **6.1.4** Enterprise Security Profile for OT Environments Pt.2<br>**6.5.3** IAC within OT Environments<br>**6.6.4** API Patterns for OT Environments Pt.3<br>**6.7.2** Incident Response Guidance for OT Environments Pt.2 | **7.2.4** Threat Alerting for OT Environments Pt.3<br>**7.5.2** OT Cyber Threat Intelligence Program Pt.2 |

# Pillar 1: User Identity and Access Governance

**The User pillar focuses on ensuring that only authorized human actors can access OT resources, a task complicated by the prevalence of shared local accounts and static passwords in legacy systems. The DoW mandate requires a transition from local authentication to a centralized, role-based, and continuously verified model (Activities 1.1.1.OT through 1.9.3.OT).**

Nozomi Networks facilitates this by providing User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) specifically tuned for industrial environments. By monitoring network-level and endpoint user events, including keystrokes, macro execution, and USB insertions via the Nozomi Arc sensor, the platform creates a precise behavior profile for every asset. When an identity (either a Person Entity or a Non-Person Entity) deviates from its baseline, Nozomi can utilize an API to BlastWave to quarantine the user or revoke access.

BlastWave serves as the Policy Enforcement Point (PEP) for these identities, replacing binary VPNs with a micro-perimeter architecture. Through its Software-Defined Perimeter (SDP) model, BlastWave grants authenticated users access to a "Segment of One".

This directly satisfies Target Activity 1.2.2. In OT (Role-Based Dynamic Access), a technician servicing a specific system (such as a building automation server) can only see and communicate with that exact asset. They are unable to ping neighboring controllers or scan the subnet for other targets, thereby preventing lateral movement at the earliest stage of an intrusion.

**Technical Mapping: User Pillar Activities**

| Activity ID | Activity Name | Joint Implementation Mechanism |
|---|---|---|
| **1.1.OT** | Inventory Users in OT Environment | BlastWave's local user authentication contains a full user inventory. When integrating with DoW systems, those systems must contain the user inventory. |
| **1.2.1.OT** | Authorization & Access Mgmt | BlastWave enforces attribute-based access policy at ingress. Users without valid attributes (via IdP) are invisible to the network. |
| **1.2.2.OT** | Role-Based Dynamic Access | BlastWave creates "Segment of One" tunnels. Vendors see only the specific asset they are authorized to maintain, not the subnet. |
| **1.3.1.OT-1.3.2.OT** | MFA and Alternate Credentialing for OT Environments | BlastWave provides phishing-resistant, password-less MFA using FIDO2 keys or biometrics, ensuring strong authentication before any network packet reaches the OT asset. It can also integrate with other DoW-approved credentialing systems. |
| **1.4.1.OT-1.4.2.OT** | Implement PAM for OT | BlastWave monitors and records critical sessions. BlastWave secures the transport layer for these PAM interfaces. |
| **1.5.1.OT-1.5.2.OT** | Life-Cycle Management for OT Environments | BlastWave is the enforcement point for enforcing lifecycle management for OT users. |
| **1.6.1.OT** | UEBA and UAM Tooling | Nozomi embeds UEBA functionalities to learn normal system interactions, while Arc sensors provide endpoint-level monitoring of USB and macro events. |
| **1.7.1.OT** | Deny by Default Policy in OT Environments | BlastWave silently drops any traffic not cryptographically authenticated. |
| **1.8.1.OT-1.8.3.OT** | Continuous Authentication | BlastWave ties sessions to cryptographic identities; if Nozomi detects the user's risk profile changes or they move to an unauthorized location, the session is terminated instantly. |
| **1.9.1.OT-1.9.3.OT** | Enterprise Credentialing Services | BlastWave and Nozomi can integrate with SSO supported by any DoW-approved credentialing authority. |

The Advanced requirement for Enterprise Credentialing (1.9.3.OT) is achieved through BlastWave's ability to act as a proxy for legacy assets. By placing a "BlastShield Node" in front of an unmanaged controller, the joint solution forces all connection requests to authenticate via DoW-approved credentialing services (e.g., CAC/PIV systems) before the traffic is permitted to pass, effectively extending modern identity security to equipment that was never designed for it.

# Pillar 2: Authoritative Inventory and Device Security

**The Device pillar addresses the security of the heterogeneous hardware landscape in OT, ranging from engineering workstations to deeply embedded sensors and actuators. The mandate requires an authoritative, centralized inventory of Non-Person Entities (NPEs) and the deployment of cryptographic certificates (Activities 2.1.1.OT through 2.7.2.OT).**

Nozomi Networks serves as the primary engine for Activity 2.1.1.OT (Inventory NPEs). It utilizes passive network discovery by default to identify assets without disrupting process timing, supplemented by safe active discovery to find devices that are online but not communicating. This inventory includes critical metadata such as firmware version, hardware serial number, and known vulnerabilities, which feeds directly into the Component-wide vulnerability management program (Activity 2.5.1.OT).

BlastWave addresses the "unmanageable device" problem identified in the DoW guidance. Many legacy OT devices cannot host agents or X.509 certificates as required by Activity 2.1.2.OT. The BlastWave Gateway architecture allows the gateway to hold the certificate on behalf of the legacy asset. This creates a "cryptographic enclave" around the device, satisfying the DoW's requirement for certificate-based identity without requiring a "rip and replace" of operational hardware.

**Technical Mapping: Device Pillar Activities**

| Activity ID | Activity Name | Joint Implementation Mechanism |
|---|---|---|
| **2.1.1.OT** | Inventory NPEs in OT Environment | Nozomi uses passive network asset discovery to inventory all NPEs in the OT environment. |
| **2.1.2.OT-2.1.3.OT** | NPE Certificate Management and Credentialing for OT | BlastWave gateways can act as proxy authentication for NPEs that cannot load certificates. |
| **2.1.4.OT** | Automated NPE Discovery | Nozomi utilizes active network discovery to discover network devices that are online but not actively communicating. |
| **2.2.1.OT** | Implement connection Policy for OT Environments | BlastWave enforces configured policies to ensure only authorized assets can communicate on the OT network. |
| **2.3.1.OT, 2.3.3.OT** | Configuration Monitoring | Nozomi identifies and generates alerts when remote configuration attempts, ladder logic downloads, or operational state changes are detected in PLCs. BlastWave has a roadmap to enable C2C configuration on client endpoints. |
| **2.4.1.OT-2.4.3.OT** | NPE Deny by Default | BlastWave's "Network Cloaking" renders NPEs invisible to the enterprise network; if a device (including BYOD and non-OT devices) is not explicitly authorized, it cannot discover or communicate with the asset. |
| **2.5.1.OT** | Vulnerability & Patching | Nozomi provides vulnerability assessments and patch recommendations; BlastWave provides a "virtual air gap" to mitigate the risk of exploiting unpatched assets. |
| **2.6.2.OT** | OT Device Configuration Management | Nozomi asset risk management system helps provide visibility into asset software and firmware versions and provides patch recommendations and vulnerability assessments for each analyzed asset. |
| **2.7.1.OT-2.7.2.OT** | Implement EDR Tools | Nozomi Arc delivers OT-optimized EDR directly to endpoints and integrates with leading IT EDR vendors, while BlastWave segmentation forces attackers to attempt endpoint exploits where they are more easily detected. |

The implementation of Extended Detection and Response (XDR) for OT (Activity 2.7.2.OT) is achieved by unifying Nozomi's native sensors (network, endpoint, and wireless) into a single AI-powered platform that integrates with enterprise IT XDR stacks like CrowdStrike Falcon or Microsoft Defender. This ensures that the DoW maintains a continuous, high-fidelity security posture from the tactical edge to the data center.

# Pillar 3: Application and Workload Protection

**This pillar focuses on securing the software that governs critical infrastructure, from SCADA masters and data historians to the engineering workstations used to program PLCs. The mandate requires preventing unauthorized modifications to these applications and implementing strict execution controls (Activities 3.1.1.OT to 3.4.4.OT).**

Nozomi Networks monitors application integrity by identifying and alerting on anomalous interactions between engineering workstations and controllers. For example, if a SCADA application attempts an unauthorized operational state change or a firmware update, Nozomi flags the event as an alert. The platform's vulnerability management console provides deep context into the software supply chain, including affected binaries and equipment lifecycle data, supporting Target Activity 3.3.1.OT (Vulnerability Management Program).

BlastWave extends Attribute-Based Access Control (ABAC) to the network layer (Activity 3.4.1.OT). While traditional firewalls use static IP-based rules, BlastWave permits traffic only between certified application instances. For instance, a policy can specify that "Only the SCADA Server Application can communicate with the Historian".

This ensures that even if an attacker gains control of a server, they cannot use rogue applications to communicate with critical workloads, effectively enforcing workload isolation at the network level.

### Application Security Synergy

The joint solution further secures the modern OT DevOps lifecycle (Activity 3.2.1.OT). For environments that use containerized applications on edge gateways, BlastWave ensures that CI/CD pipelines communicate via mutually authenticated cryptographic tunnels. This prevents man-in-the-middle attacks on the software supply chain, ensuring that only verified code is deployed to the tactical edge.

| Application Security Activity | Nozomi Intelligence Contribution | BlastWave Enforcement Contribution |
|---|---|---|
| **3.1.2.OT Application Control** | Monitors for unauthorized config changes and ladder logic modifications. | Secures the management consoles for application control systems to prevent tampering. |
| **3.2.1. Build OT DevOps Capability Factory** | N/A | Secures the CI/CD pipeline transport for secure software updates. |
| **3.3.1.OT-3.3.2.OT OT Vulnerability Management Program** | Provides a comprehensive vulnerability management console, with extensive information about affected assets, patches available, workarounds, and equipment lifecycle. Integrates extensively with SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response), and other enterprise security consoles to provide a unified view of IT, OT, and IoT threats. | Provides a "virtual air gap" that mitigates the risk of exploitation of unpatched assets. |
| **3.4.1.OT-3.4.4.OT Access Control for OT Environments** | Identifies application identities and communication patterns for policy creation. | Enforces network-level ABAC policies, blocking unauthorized protocols. Microsegmentation is appropriately implemented at the level of risk for each system in the OT network. |

# Pillar 4: Data-Centric Security in Industrial Contexts

**Pillar 4 is often the most difficult to implement in OT due to the prevalence of proprietary, clear-text protocols that resist standard tagging and inspection. The DoW mandate requires methods for protecting data in transit and detecting unauthorized exfiltration (Activities 4.1.1.OT through 4.7.1.OT).**

Nozomi Networks addresses Target Activity 4.4.1.OT (DLP Analytics) by baselining all industrial communications. By analyzing cross-Purdue and external traffic flows, the platform identifies anomalous data movement that could indicate a ransomware attack or the exfiltration of sensitive operational data. This intelligence is shared via API with enterprise SIEM platforms for broader correlation with database-integrity-monitoring events (Activity 4.4.6.OT).

BlastWave serves as the "cryptographic pipe" for data protection. It provides end-to-end encryption for all traffic leaving the local area network using AES-256. This effectively upgrades legacy, insecure protocols to military-grade standards without requiring any changes to the underlying PLC firmware or switching fabric.

This "Protocol Cloaking" ensures that even if an adversary gains physical access to the network, they cannot intercept sensitive operational commands or data.

### Data Protection Implementation Matrix

| Requirement Area | Technical Execution | Solution Mapping |
|---|---|---|
| **Data Tagging & Patterns** | Nozomi maps data flow patterns and attributes across the environment, identifying data exfiltration or ransomware attempts. | Activity 4.1.1.OT / 4.2.1.OT |
| **Data in Transit Protection** | BlastWave encapsulates clear-text protocols in secure, identity-bound tunnels. | Activity 5.4.3.OT |
| **Exfiltration Detection** | Nozomi detects unusual communications between Purdue levels or to the Internet. | Activity 4.3.1.OT-4.3.2.OT |
| **File Activity and Database Activity Monitoring** | Nozomi telemetry enhances SIEM analytics to track access to high-value files and data stores. | Activity 4.4.1.OT, 4.4.3.OT, 4.4.4.OT, 4.5.1.OT, 4.5.2.OT, 4.6.1.OT |

# Pillar 5: Software-Defined Network and Environment Segmentation

**The Network pillar is the operational core of the joint Nozomi-BlastWave value proposition. The DoW guidance emphasizes removing implicit trust and implementing granular segmentation to halt lateral movement (Activities 5.1.1.OT to 5.4.3.OT).**

Nozomi Networks provides the visibility necessary to define granular access rules (Activity 5.1.1.OT). By mapping every network flow and communication pathway in real time, the platform creates the factual ground truth needed to write security policies and ConOps. This ensures that microsegmentation rules are based on actual operational requirements rather than theoretical models that might inadvertently block critical process traffic.

BlastWave functions as the distributed Segmentation Gateway (Activity 5.2.2.OT). It enables microsegmentation down to the individual host level, independent of network VLANs. This "Zero Trust Default Drop" model ensures that no traffic is permitted unless explicitly allowed by an identity-to-identity policy.

This approach is particularly effective for "Brownfield" deployments, as it overlays the existing flat network and logically enforces segmentation without requiring IP address changes or network re-cabling.

### Cryptographic Plane Segmentation and Cloaking

The joint solution enables Cryptographic Plane Segmentation (Activity 5.3.1.OT) by separating control, data, and management traffic across separate cryptographic and policy enforcement enclaves. BlastWave ensures that a system is prohibited from sending or receiving management-plane traffic (such as remote configuration attempts) unless approved by a specific policy. BlastWave's peer-to-peer mesh architecture facilitates direct, encrypted connections that minimize latency, addressing the bandwidth constraints at the tactical edge (Activity 5.4.3.OT).

| Network Pillar Activity | Nozomi "Intelligence" Role | BlastWave "Enforcement" Role |
|---|---|---|
| **5.1.1.OT-5.1.2.OT Granular Access Rules** | Discovers assets and attributes that inform the creation of access rules. | Operates on a "Default Drop" model, requiring explicit rules for all traffic. |
| **5.2.1.OT-5.2.3.OT Define IT Communication Pathways and APIs** | Identifies communication pathways used in OT networks. | Enforces policies to enable only authorized systems and protocols to communicate across the OT network, including APIs for dynamic policy creation. |
| **5.3.1.OT-5.3.2.OT Plane Segmentation** | Identifies communication pathways across Purdue levels to find plane overlaps. | Enforces cryptographic segmentation between control and management planes. |
| **5.4.1.OT-5.4.2.OT Host-Level Microsegmentation** | Maps network data flows to define microsegment boundaries. | Logically enforces segmentation at the host level, independent of VLANs. |
| **5.4.3.OT Data in Transit Protection** | Monitors for clear-text protocols crossing insecure boundaries. | Encrypts all traffic leaving the local network via AES-256 tunnels. |

# Pillar 6: Automation and Orchestration via API Interoperability

**The scale of DoW operations requires that security be automatable and integrated into the broader enterprise defense stack. Pillar 6 (Activities 6.1.1.OT to 6.7.2.OT) focuses on normalizing policy artifacts and defining API standards to ensure tool interoperability.**

Nozomi Networks acts as the connective tissue that turns zero-trust policy into actionable intelligence. Through its Open Source Software Development Kit (SDK) and REST APIs, Nozomi integrates deeply with SIEM and SOAR platforms, feeding alerts, context, and asset identities into orchestrated workflows. This enables automated audit logging and governance processes required by Target Activity 1.7.1.OT.

BlastWave is built on an API-first architecture, allowing its orchestrator to be driven by external security tools (Activity 6.6.2.OT). When an enterprise SOAR platform (e.g., Splunk SOAR or Palo Alto XSOAR) receives an alert from Nozomi regarding a compromised workstation, it can programmatically call the BlastWave API to isolate the infected host.

This integration enables the "Response" part of the zero-trust framework, providing the enforcement mechanism that passive visibility tools lack.

### Integrated Automation Framework

1. **Policy Inventory:** BlastWave Orchestrator serves as the centralized repository for all access policies, serving the enforcement point for all of Activity 6.1.1.OT-6.1.3.OT.
2. **Tool Interoperability:** Nozomi integrates with NAC, PAM, and SIEM platforms via its N2OS SDK, fulfilling the requirement for tool interoperability in OT (Activity 6.2.2.OT) as well as 6.6.1OT-6.6.4.OT.
3. **Incident Response Guidance:** Nozomi provides the telemetry for incident analysis, while BlastWave enables the logical air-gapping of compromised segments, supporting and enabling Activities 6.5.1.OT, 6.5.2.OT, 6.7.1.OT and 6.7.2.OT.

# Pillar 7: Visibility, Analytics, and the Digital Kill Switch

**The Visibility and Analytics pillar is the strongest area of alignment for the joint solution, focusing on logging, monitoring, and threat intelligence (Activities 7.1.1.OT to 7.5.2.OT). The DoW mandate requires that infrastructure be designed for physical or logical disconnection during a detected incident (Activity 7.2.1.OT).**

Nozomi Networks provides the AI-powered analytics required to detect advanced threats and process anomalies. The platform continuously baselines and profiles every device, pinpointing deviations that need attention without creating alert fatigue. This satisfies Target Activity 7.3.2.OT (Establish OT Baseline Behavior) and Activity 7.4.1.OT (Baseline and Profiling). Alerts are correlated to specific Person Entities (PEs) and NPEs, providing security teams with the accurate information needed for rapid triage (Activity 7.2.5.OT).

BlastWave provides the "Digital Kill Switch" capability required to meet Activity 7.2.1.OT (Incident Response Isolation). In the event of a detected compromise (such as a ransomware outbreak or unauthorized command-and-control communication), security teams can instantly revoke the cryptographic certificates associated with a specific zone or user group.

This logically air-gaps the compromised segment within milliseconds, stopping the attack's spread without requiring personnel to physically disconnect equipment at remote sites.

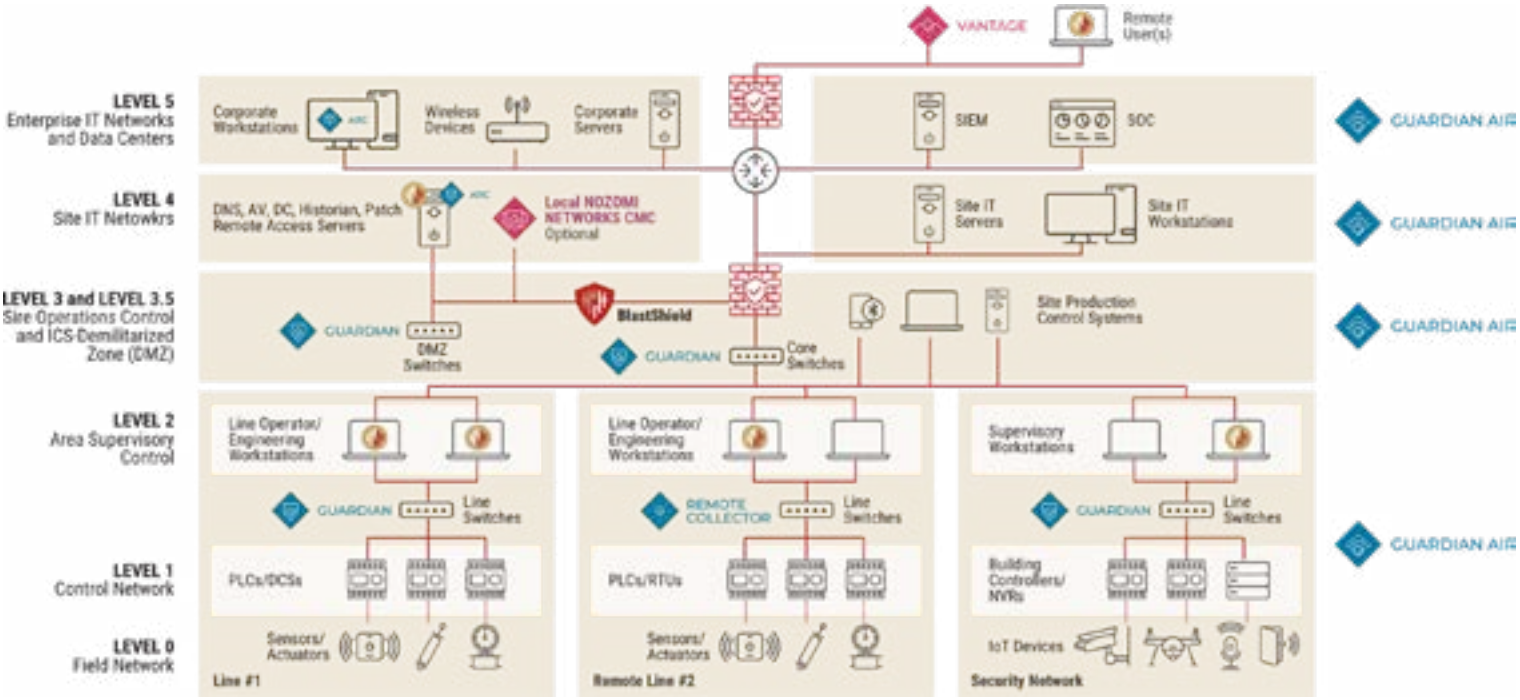
### Visibility Pillar Technical Outcomes

| Activity ID | Activity Name | Technical Delivery |
|---|---|---|
| **7.1.2.OT-7.1.3.OT** | Log Parsing in OT | Nozomi maps vendor log content to machine-consumable patterns for ingestion into the enterprise SIEM. |
| **7.2.1.OT** | Incident Response Isolation | BlastWave enables instant logical air-gapping of infrastructures via authentication revocation driven by Nozomi APIs. |
| **7.2.2.OT-7.2.4.OT** | Threat Alerting for OT Environments | Nozomi uses AI/ML to develop deviation anomaly rules that detect advanced threats utilizing high-fidelity data feeds. |
| **7.2.5.OT-7.2.6.OT** | OT Asset ID and Baselines | Nozomi implements an alert management system that tracks assets and events; uses advanced AI/ML algorithms to detect trends, attack vectors, and anomalous behavior. |
| **7.3.1.OT-7.4.1.OT** | Implement Analytics Tools, Establish Baseline Behavior | Nozomi provides AI-powered analysis of all data sources to identify trends and attack vectors. Nozomi establishes an environment baseline as a reference for future anomaly alerts. |
| **7.5.1.OT-7.5.2.OT** | CTI Program | Nozomi threat intelligence used to drive threat prevention polices on BlastWave systems. |



NOZOMI NETWORKS BlastWave

# Joint Solution Architecture




The joint BlastWave and Nozomi solution provides a robust Zero Trust architecture for OT environments by securing the industrial lifecycle from Field Networks to Enterprise IT for DoW. By deploying BlastShield at critical junctures, including the ICS-DMZ and between Site IT and Site Operations, the solution enforces strict identity-based access control and network cloaking for local workstations and remote users. This ensures that high-value assets such as PLCs, RTUs, and engineering workstations are protected from unauthorized discovery and lateral movement, directly addressing the core Zero Trust requirements for securing operational technology.

This integrated approach combines Nozomi Networks' advanced visibility and threat detection via its Central Management Console (CMC) with BlastShield's proactive prevention capabilities. While Nozomi monitors the Site Production Control Systems to feed critical data to the SIEM and SOC, BlastShield serves as the secure enforcement layer for all OT and site-level servers and workstations.

Together, they provide a comprehensive defense-in-depth strategy that ensures continuous monitoring and unshakeable protection across all levels of the Department of War's industrial stack.

# Mitigating OT-Specific Implementation Hurdles

**The DoW guidance explicitly warns that applying standard IT security tools to OT can be "potentially dangerous". The Nozomi and BlastWave solution is engineered specifically to mitigate these risks through a non-intrusive, safety-first design targeted for OT environments.**

### The "Brownfield" Reality and Network Continuity

Most military OT environments are "brownfield" deployments where re-architecting the network is impossible due to operational risks. BlastWave functions as an invisible overlay, enabling microsegmentation (Activity 5.4.1.OT) without requiring IP address changes or firmware upgrades for legacy controllers. This allows DoW components to hit zero-trust timelines "without touching a single PLC," providing immediate security outcomes without the risk of downtime.

### Safety System Integrity

Safety Instrumented Systems (SIS) are the last line of defense against catastrophic failure and must not be compromised by security controls. BlastWave supports the creation of "Safety Zones" that are logically isolated from the rest of the Operational Layer. By using "Deny by Default" policies, the joint solution ensures that no external entity (not even an authenticated administrator) can communicate with the SIS unless explicitly authorized and verified with high-assurance credentials, protecting the integrity of the safety process while allowing for controlled data extraction.

### Bandwidth and Tactical Edge Performance

Requirements to support "Base, Camp, Post, and Station" imply deployment in tactical environments where bandwidth is scarce. BlastWave's lightweight, peer-to-peer mesh architecture optimizes bandwidth by enabling direct connections between users and resources, avoiding the backhaul latency of traditional VPNs. Nozomi's sensors are similarly optimized, providing high-fidelity monitoring even in isolated or air-gapped systems, ensuring that mission operations are enhanced rather than hindered by security implementation.

# Synthesis: A Cohesive Strategy for FY 2027

**The DoW's Zero Trust for Operational Technology mandate represents a significant paradigm shift, moving from a "trust but verify" model to "never trust, always verify." This transition is not merely a compliance exercise but a foundational requirement for securing the warfighting platform against modern, sophisticated threats.**

The joint solution from Nozomi Networks and BlastWave offers a unique combination of deep OT visibility, analytics, and cryptographic enforcement, addressing 85 of the 105 activities in the DoW framework. By leveraging Nozomi for visibility and analytics and BlastWave for microsegmentation and cloaking, DoD components can achieve Target Level compliance (69/84 activities) while establishing the groundwork for Advanced maturity (16/21 activities).

This approach solves the primary challenge of OT zero trust: how to implement rigorous security without disrupting operations. By "cloaking" vulnerable legacy assets and providing a "Digital Kill Switch" for incident response, the Nozomi Networks and BlastWave solution enables the DoW to secure its most critical infrastructure against today's threats and tomorrow's conflicts. As components work toward the September 30, 2027, Target Level compliance deadline, this joint architecture provides the essential "air cover" and "connective tissue" needed to ensure the resilience and reliability of the operational environment.

v20260902

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

Prevent industrial cyberattacks, and ensure the world's critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at **www.blastwave.com**

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS