WHITE PAPER

Securing Mission-Critical OT: How Claroty Powers Compliance with the DoD/DoW's Zero Trust for OT Framework

TABLE OF CONTENTS

I. Overview

To address the pressing challenge of increased adversary targeting against U.S. Department of Defense (DoD) / Department of War (DoW) networks, the Zero Trust framework for Operational Technology (OT) enables DoD/DoW organizations to establish a resilient network environment. Implementing solutions that align with the DoD/DoW Zero Trust (ZT) Strategy Target and Advanced level activities and capabilities for this unique mission space, the DoD/DoW can significantly enhance its overall security posture, and safeguard critical infrastructure assets from evolving threats.

OT solutions that align with the DoD/DoW ZT Strategy Target and Advanced level activities and capabilities should provide cyber vulnerability baselining, advanced threat indications and warnings, anomaly detection, and facilitate information sharing. Such capabilities will enable real-time response actions to disrupt attacker Industrial Control System (ICS) cyber kill chains, expedite recovery to restore normal operations, and enable machine-to-machine sharing of threat indicators and mitigations to thwart adversary re-use of attacks. This paper will outline what OT-specific capabilities are necessary for these unique networks, how they are different from IT and therefore must embrace different considerations, and how they align with the DoD/DoW's ZT for OT framework.

Complete mapping of how the Claroty Platform directly supports the Department of Defense / Department of War's Zero Trust for OT framework can be found in Section III.

Applying Zero Trust in OT: Key Challenges and Actions

OT will play a prominent role to the evolving Department of War. Dominating the modern battlespace requires mastering OT security, both defensively for U.S. mission assurance and offensively against adversaries. Offensive operations demand resilience from attacks. Similarly, disrupting an adversary's power grid, air defense, or transportation systems requires a deep understanding of their OT.

Protecting these systems is uniquely difficult due to their critical mission roles. Unlike IT, they run physical processes where a single security failure can cause real-world consequences, including catastrophic equipment damage, safety risks, and loss of life. Downtime is not just an inconvenience; it can disrupt mission readiness, halt production, shut down utilities, or cripple transportation networks, directly undermining national security.

Unlike IT, OT systems are typically low-latency and high-bandwidth, which makes traditional IT techniques ineffective. These environments often rely on shared credentials, lack centralized management, and include End-of-Life (EoL) assets that are difficult to patch or require downtime for maintenance. Point-to-point communication can make anomalies easier to detect, but it also creates constraints. The challenge is further compounded by the use of hundreds of vendor-specific OT protocols, many of which are insecure or encrypted, limiting visibility and complicating threat detection.

Because of these unique challenges, OT security controls must be tailored to operational realities rather than borrowed from IT. Practitioners need approaches that account for safety and operational consequences, unlike IT's focus on confidentiality, integrity, and availability (CIA). Effective solutions must reflect this difference to manage risk across devices, systems, and networks, recognizing that mission-critical OT systems directly impact lives, operations, and national security.

Due to these differences, Zero Trust for OT requires a tailored approach. Below are **key considerations** and **recommended actions** OT leaders should take when applying Zero Trust principles in operational environments:

1. **Asset Protocol and Visibility Gaps:** DoD/DoW cyber-physical systems span a wide range of mission-critical functions, from industrial control systems and building automation to weapons systems. Each system has its own unique OT protocols and operational constraints that must be considered when applying the ZT security controls.

   Action: Deploy Zero Trust solutions designed with deep OT protocol support to gain complete visibility into all OT assets, including legacy systems. Ensure monitoring tools can interpret vendor-proprietary traffic and provide contextual visibility across mixed IT/OT networks.

2. **Patching Limitations of Legacy Systems:** OT environments often rely on decades-old equipment, proprietary protocols, and systems that cannot be easily patched or replaced.

   Action: Use Zero Trust techniques that don't require invasive changes. Instead, rely on network-based segmentation, protocol-aware continuous monitoring, and compensating controls to protect legacy assets.

3. **Identity and Access Management:** Shared accounts and limited centralized management are common in OT, making strong identity governance more difficult than in IT.

   Action: Enforce least-privilege access by introducing identity-aware, role-based access, and strong MFA, while also incorporating compensating controls such as session recording and just-in-time access.

4. **Mission-Critical Operations:** Zero Trust controls in OT must be mission-aware and context-driven, focusing on the systems and processes where disruption would have the greatest operational or safety impact.

   Action: Leverage asset zoning to group devices by operational impact. This enables security teams to apply Zero Trust policies in an impact-centric way, supporting both vulnerability management and network segmentation without introducing unnecessary risk to critical processes.

5. **Threat Alerting:** In OT, many threat indicators do not resemble traditional IT cyberattacks. Instead, they appear as deviations from normal operations, such as unauthorized configuration changes, unexpected controller mode shifts, or unplanned firmware updates, which can disrupt processes and compromise mission-critical operations.

   Action: Deploy an OT-aware monitoring solution that establishes behavioral baselines for assets, continuously tracks configuration changes, and alerts on anomalous or unauthorized activity. This ensures Zero Trust policies adapt to operational realities and provide early warning before adversaries can cause disruption.

II. Implementation Journey for Zero Trust in DoD/DoW OT Environments: Key Use Cases

This paper explores five critical use cases that form the foundation of a Zero Trust strategy for OT and Cyber-Physical Systems (CPS) within DoD/DoW environments: asset discovery and inventory, vulnerability and risk management, secure remote access, network segmentation, and threat detection. Each domain addresses a key component of ZT implementation and reflects the evolving cybersecurity needs of defense missions.

Asset Discovery and Inventory ensures that every device, system, and connection is known and continuously monitored. This is an essential prerequisite for any ZT architecture.

Vulnerability and Risk Management identifies and prioritizes vulnerabilities and insecure configurations, enabling risk-informed decision-making and remediation planning.

Secure Remote Access provides controlled, monitored, and policy-driven connectivity for authorized users while protecting critical systems from misuse or compromise.

Network Segmentation limits lateral movement and enforces security zones aligned to operational function and mission priority.

Threat Detection delivers continuous monitoring and real-time alerting for both known and unknown threats, using behavioral baselines and threat intelligence tailored to OT systems.

Together, these use cases operationalize Zero Trust principles in a way that supports mission continuity, safety, and resilience across the DoD/DoW's diverse and high-consequence OT environments.

OT Asset Discovery and Inventory: The Foundation of Zero Trust Controls

Zero Trust Requirements Supported by Claroty					
Device	**Applications & Workload**	**Data Environments**	**Network**	**Automation & Orchestration**	**Visibility & Analytics**
2.1	3.3	4.1	5.2	6.1	7.1
2.2		4.2	5.3	6.2	7.2
2.3		4.3	5.4	6.3	7.3
2.4		4.4		6.5	7.4
2.5		4.5		6.6	7.5
2.6				6.7	
2.7					

In the DoD/DoW's Zero Trust strategy, asset visibility is the foundation upon which every other Zero Trust control is built. The principle of "never trust, always verify" begins with knowing exactly what exists in the environment. Without a comprehensive and continuously updated asset inventory, agencies cannot enforce segmentation, implement remote access identity controls, assess risk, or detect anomalies effectively across operational technology (OT) environments.

OT networks are notoriously opaque, often composed of legacy systems, proprietary protocols, and air-gapped or intermittently connected devices that were never designed with visibility or cybersecurity in mind. This complexity is compounded in mission-critical DoD/DoW environments where safety, availability, and real-time performance are paramount. Traditional IT discovery techniques, like active scans, can disrupt these fragile systems, posing unacceptable risks to the continuity of operations.

To safely and comprehensively discover and inventory OT assets, agencies must use a **multi-discovery method approach** that balances operational integrity with visibility depth. This includes:

- **Passive Monitoring:** By observing network traffic over a period of time, passive monitoring tools can identify assets, communication patterns, protocols in use, and behavioral baselines without touching the endpoints. This method is foundational for OT because it introduces no risk of disruption, but it may miss intermittently connected or silent assets.
- **OT-Native Queries:** Protocol-aware queries can communicate with devices in a read-only and non-invasive manner. These methods are carefully tailored to OT protocol standards and are invaluable for enriching passive data and discovering idle assets.
- **Manual File Ingestion:** In air-gapped or high-security networks, operators often rely on manually collected engineering files, such as PLC project files, configuration backups, or device inventories exported from vendor tools. Modern asset discovery platforms can parse these files to yield detailed asset fingerprints, firmware versions, and logic metadata.
- **Integration with Existing Systems:** Asset data already lives in existing tools across the technology stack, from CMDBs to endpoint management platforms to vendor-specific historian systems. Leveraging API integrations with these systems enriches the asset inventory and helps correlate IT and OT systems under a unified visibility strategy.

Vulnerability and Risk Management: Prioritizing Risks Based on Mission-Critical Outcomes

Zero Trust Requirements Supported by Claroty				
Device	**Applications & Workload**	**Data Environments**	**Network**	**Automation & Orchestration**
2.1	3.3	4.1	5.2	6.2
2.2		4.2	5.3	6.3
2.3		4.3	5.4	6.5
2.4		4.5		6.6
2.5				

Once OT asset visibility is established, the next critical use case to meet Zero Trust requirements is vulnerability and risk management, which should be a continuous process of identifying, assessing, prioritizing, and reducing risk across operational systems. In DoD/DoW environments, vulnerability and risk management must be context-driven and asset-aware, focusing efforts on the most critical exposures.

Historically, vulnerability management has relied on frameworks like the **Common Vulnerability Scoring System (CVSS)** to quantify the technical severity of vulnerabilities. While CVSS remains useful, it was not designed for OT environments, where thousands of legacy devices may share the same software version but differ in operational criticality, exploitability, and patch feasibility.

To move beyond blanket severity scores and toward impact-centric prioritization, a modern Vulnerability and Risk Management strategy for OT cannot be evaluated in a vacuum. Devices supporting critical operational functions, such as Fire Control Units (FCUs), Stores Management Systems (SMS), Embedded GPS/Inertial Navigation Systems (EGI), Automated Test Equipment (ATE), and even FRCS, should be treated with elevated priority, even if the vulnerability itself is moderate. Mapping vulnerabilities to operational impact ensures that exposure management is based on potential impact to the DoD/DoW's outcomes.

In addition to an impact-centric approach to prioritizing vulnerabilities, other exposures such as unsecured remote access, substandard password usage, and anomalous network communication should be evaluated as part of an exposure management program.

Operationalizing Vulnerability and Risk Management with the CTEM Process

To translate vulnerability and risk intelligence into measurable risk reduction and strengthen business continuity, the DoD/DoW can adopt a Continuous Threat Exposure Management (CTEM) framework purpose-built for operational technology (OT) environments. By aligning this approach with trusted vulnerability and risk intelligence sources, such as CISA's Known Exploited Vulnerabilities (KEV) Catalog and the Exploit Prediction Scoring System (EPSS), agencies can establish a more advanced, data-driven process for prioritizing vulnerabilities and associated assets. This comprehensive assessment method enables organizations to identify, categorize, and mitigate network-wide exposures more effectively. This approach is more commonly known exposure management.

The following five steps outline Claroty's recommended approach to OT and broader CPS exposure management, which aligns closely with the principles of Gartner's Continuous Threat Exposure Management (CTEM) framework.

1. **Identify Critical Operational Processes**
   Begin by identifying which systems support critical mission functions, such as navigation, refueling, maintenance and repair operations, and even weapons controls. Asset criticality should be defined not just by technical characteristics, but by operational dependencies, safety impact, and potential mission disruption. Identifying a hierarchy of operational processes will inform risk mitigation for the most critical assets first. This is a critical step not only for risk prioritization, but also for implementing Zero Trust, as it informs measures like virtual network segmentation for the most critical asset zones.

2. **Discover and Validate Exposures**
   The next critical step is uncovering exposures that traditional vulnerability management often misses. Active discovery techniques, such as OT-native queries, offer a unique, non-disruptive approach to gain valuable exposure data, such as:

   - **Exploitability Validation:** An asset may have a known CVE with a "Critical" CVSS score, but a vulnerability management team needs to determine if the asset is truly exploitable. Active discovery techniques can verify an asset's patch level, helping security teams assess whether it remains vulnerable. Being able to definitively confirm if a system with a known exploit is actually at risk, especially during ransomware attacks, adds vital context for effective risk remediation.
   - **End-of-Life Asset Indicators:** OT environments often contain EoL assets that no longer receive security patches. Active discovery can identify EoL assets, enabling teams to validate where compensating controls are necessary to prevent unpatchable systems from causing unexpected downtime.
   - **Open Ports:** Active discovery can validate open network pathways between source and destination devices, providing visibility into potential access points. This helps identify anomalous or malicious connections that could otherwise go undetected.
   - **Installed Applications on Host Devices:** On devices running Windows operating systems, active discovery uncovers installed applications, providing deeper visibility into software inventories that may introduce risk or compliance concerns.

3. **Prioritize Exposures by Operational Impact**
   Rather than defaulting to technical severity scores, security teams should prioritize exposures based on their operational impact. Devices supporting critical operational functions, such as Vehicle Management Systems, Automated Refueling Systems, and Launch control systems, should be treated with elevated priority, even if the vulnerability itself is moderate. Mapping vulnerabilities to **operational impact** ensures that exposure management aligns with mission risk.

   In addition to this impact-focused approach, external threat intelligence can provide valuable context. CISA's **Known Exploited Vulnerabilities (KEV)** catalog highlights vulnerabilities that are actively exploited in the wild, signaling which issues pose immediate and credible threats. Meanwhile, the **Exploit Prediction Scoring System (EPSS)** estimates the likelihood that a vulnerability will be exploited in the near future, offering a predictive dimension to prioritization. An OT-specialized solution will automatically correlate internal knowledge of process criticality with external vulnerability data, resulting in a prioritization model that is both grounded in the DoD/DoW's operational reality and responsive to evolving threat landscapes.

4. **Validate Attack Paths and Network Segmentation**

   Beyond isolated vulnerabilities, security teams must understand how attackers could chain multiple exposures together and move laterally within the OT network to reach critical assets. This is where attack path analysis and microsegmentation validation come into play. Simulated lateral movement paths can identify policy gaps or architectural weaknesses that allow low-risk exposures to become high-impact breaches. While covered in more depth in the **Virtual Network Segmentation** section, this step is vital in closing the loop on prioritization and exposure mapping.

5. **Mobilize Remediation**

   Critically, remediation in OT environments must be mission-aware, meaning changes must be validated for safety, scheduled with operators, and sometimes substituted with compensating controls.

   This five-step cycle enables the DoD/DoW to move from reactive vulnerability scanning to proactive, Zero Trust-aligned exposure reduction. By embedding threat intelligence, operational context, and architectural validation into a repeatable process, DoD/DoW organizations can continuously harden their OT environments against both known and emerging threats.

Securing Remote User Access to OT Networks (Air Gapped or Cloud-Connected)

Zero Trust Requirements Supported by Claroty					
User	**Device**	**Data**	**Network**	**Automation & Orchestration**	**Visibility & Analytics**
1.1	2.1	4.4	5.1	6.1	7.2
1.2	2.2	4.5	5.2	6.2	
1.4	2.3		5.3	6.6	
1.5	2.4		5.4	6.7	
1.6					
1.7					
1.8					

In DoD/DoW operational environments, cyber-physical systems, including ICS/SCADA, FRCS/BMS, and IoT devices, span a wide range of mission-critical contexts, from low-bandwidth or air-gapped networks afloat or in the field, to remote deployments across military installations and other defense facilities. Remote OT access in these contexts is a mission-enabling necessity.

While remote access enhances operational continuity, supports rapid issue resolution, and reduces the need for on-site personnel to access geographically dispersed assets, adoption remains behind, with only 45% of agencies having fully implemented remote OT access.[2]

Risks Posed by IT Remote Access Solutions

Remote access scenarios for unplanned, emergency, and routine maintenance must all be considered to maintain OT-related safety and uptime. Yet, the use of VPN-based and/or other standard IT solutions for OT remote access among remote personnel and contractors creates critical security challenges and risks for the DoD/DoW's OT environments. Standard IT solutions are unable to fully implement role-based access controls and enforce access policies, Principles of Least Privilege (PoLP) to restrict access to critical assets, and provide administrators the option to terminate access when necessary.

Risks Posed by Remote Users and Third Parties

In addition to the risks posed by traditional IT remote access solutions, remote users introduce unique challenges in OT environments. In DoD/DoW environments, where mission-critical systems and national security operations are at stake, remote access significantly expands the attack surface. This includes risks such as unauthorized access, human error, and malicious activity, including the transfer of harmful files or lateral movement across segmented networks. In military contexts, these threats can disrupt logistics, physical security systems, or even weapons platform operations.

Large DoD programs often involve multiple layers of contractors, including system integrators, program primes, and subcontractors. Each layer introduces additional access points and potential vulnerabilities that must be considered when securing OT environments.

To align with the DoD/DoW Zero Trust for OT framework, remote access must be tightly controlled, continuously verified, and actively monitored. The following OT-specific remote access controls support requirements under multiple Zero Trust pillars and help reduce risk across DoD/DoW operational environments:

Role-Based Access Controls (RBAC): Access is granted strictly based on the user's function, ensuring that personnel can only interact with systems and data necessary for their role.

Time-Based Access Control: Limiting remote access to predefined, approved timeframes reduces the opportunity for unauthorized or unsanctioned activities.

Vaulted Credential Management: Remote users do not retain direct access to their credentials, thus preventing unauthorized access and enabling varying levels of privileges for secure OT network access.

Live recording and continuous monitoring of user activity: Helps administrators have comprehensive oversight and control over third-party file transfers for enhanced security.

Network Segmentation: Establishing Security Zones and Monitoring Network Behavior

Zero Trust Requirements Supported by Claroty				
Device	**Data**	**Network**	**Automation & Orchestration**	**Visibility & Analytics**
2.2	4.1	5.2	6.2	7.2
2.4	4.2	5.3	6.3	7.3
	4.3	5.4	6.5	7.4
	4.5		6.6	

Effective network microsegmentation is a cornerstone of implementing a Zero-Trust architecture within DoD/DoW OT environments because it reduces the attack surface and limits the blast radius of potential intrusions. Grounded in continuous monitoring, micro segmentation enables precise control over communications by grouping assets into security zones based on their real-time network traffic and operational roles.

Establishing Network Zones:

The first step in microsegmentation is to establish network zones in order to limit lateral movement, reduce the attack surface, and layer protection of critical assets by zoning off, or segmenting, the network. The DoD/DoW's OT networks are complex environments that require segmentation strategies aligned with both mission priorities and real-world operational constraints. While the foundational goal is to group assets into logical zones based on their operational function and established baselines, the DoD/DoW can further enhance segmentation by applying more granular classification approaches, such as:

Network Architecture: Segmenting based on existing network topology and communication pathways to reflect operational workflows.

Security Sensitivity and Risk Tolerance: Grouping assets by criticality and risk to prioritize protections for mission-essential systems and higher-risk assets, such as EoL assets.

Geographic Location: Accounting for physical site separation or facility-specific operational contexts.

Access Sensitivity: Differentiating zones based on the level and type of access required by users, devices, and systems.

Network Policy Simulation

Following the establishment of network security zones, the next step in advancing a Zero Trust network protection strategy is leveraging **network policy simulation**. This process begins with mapping normal network communication behavior between zones. Comprehensive mapping of network traffic enables administrators to clearly identify communication flows, assess risks, and design effective segmentation strategies tailored to their network topology.

Once granular network traffic mapping is complete, it's important to simulate and refine network communication policies to ensure that they fully account for an OT environment's unique requirements and do not negatively impact system functionality. An OT-specialized solution will recommend expert-defined segmentation policies at both the zone and device level to minimize uncertainty and enforce segmentation without introducing additional risk to the network.

Policy Enforcement and Alerting on Deviations

After creating and testing segmentation policies based on device behavior and communication patterns, the next step is to enforce these policies and continuously monitor for any deviations. Existing tools like Network Access Control (NAC) and firewalls act as Policy Enforcement Points (PEPs), carrying out the access decisions made by Policy Decision Points (PDPs). The PDPs assess device status and communication context to decide whether access should be allowed, and the PEPs enforce those decisions in real time.

PEP Technologies for Implementing Segmentation:

Zone-Based Segmentation	Device-Based Segmentation
Firewalls: Deployed at the boundaries between security zones, firewalls provide granular, policy-driven control over network traffic. They enforce strict access controls, monitor ingress and egress, and are critical for preventing unauthorized lateral movement and restricting communication flows to those explicitly permitted.	**Network Access Control (NAC):** NAC systems dynamically evaluate and enforce device compliance and posture before granting network access. Ideal for environments with diverse and mixed device populations, NAC enables continuous assurance that only authorized and compliant devices participate in OT network communications.

When implemented effectively, segmentation acts as both a preventative control and an enabler of continuous monitoring, threat detection, and secure interoperability between IT and OT systems. Network segmentation reinforces the following additional Zero Trust controls:

- **Threat Detection and Alerting on Deviations:** Continuous monitoring integrated with policy enforcement systems generates alerts on deviations from the defined baselines and segmentation policies. Early detection of unauthorized communication attempts or unusual device behaviors empowers security teams to swiftly address anomalous behavior.
- **Vulnerability and Risk Management and Attack Path Validation:** Virtual segmentation allows security teams to understand and simulate attack paths. By validating network traffic in real time, security teams can proactively uncover and close off critical avenues of lateral movement.
- **Supporting Compliance and IT/OT Boundary Management:** Policy enforcement also facilitates compliance with federal mandates and DoD/DoW cybersecurity frameworks. Properly defined zones create clear IT/OT boundary policies, enabling leadership and operators to maintain the visibility needed into OT network processes without compromising operational integrity. This separation protects critical OT assets from threats originating in the IT environment, significantly reducing the risk of lateral movement and insider threats.

Threat Detection: Continuous Monitoring for OT Anomalies and Malicious Threats

Zero Trust Requirements Supported by Claroty					
Device	**Applications & Workloads**	**Data**	**Network**	**Automation & Orchestration**	**Visibility & Analytics**
2.1	3.1	4.4	5.2	6.2	7.1
2.2		4.5		6.5	7.2
2.3				6.6	7.3
2.4				6.7	7.4
2.6					7.5
2.7					

Continuous monitoring of OT and CPS assets is a foundational component of threat detection within the DoD/DoW's Zero Trust for OT framework. By continuously monitoring device communication patterns, security teams can develop accurate behavioral baselines. These baselines are essential for identifying legitimate device interactions versus anomalous or unauthorized communications.

Threats to OT systems fall into two broad categories: **unknown operational anomalies** and **known signature-based threats**, each requiring distinct detection strategies.

Detecting OT Operational Anomalies

In OT environments, many threat indicators do not resemble traditional cyberattacks. Instead, they manifest as deviations from normal operational behavior. Unmonitored events such as unauthorized configuration changes, controller mode shifts, or firmware upgrades can disrupt OT processes and compromise mission-critical operations.

OT-specific security solutions equipped with deep packet inspection (DPI) can monitor these low-level, process-oriented activities down to the code or command level. This enables visibility into:

- Configuration file uploads/downloads
- Key state changes or controller mode changes
- Firmware modifications
- Protocol-specific communications

By baselining expected behavior and flagging anomalies, these tools allow DoD/DoW security teams to detect unauthorized or erroneous changes early and respond in accordance with the management-of-change process. These operational insights serve as a natural extension of Zero Trust's continuous monitoring and directly support multiple pillars of the DoD/DoW Zero Trust model, including **Device, Automation & Orchestration,** and **Visibility & Analytics.**

Detecting Known Threats

Alongside behavioral anomalies, OT environments must also defend against known threats that are identifiable through threat intelligence and recognized indicators of compromise (IOCs). These include:

- Malicious IP addresses and DNS queries
- Zero-day attacks
- OT-targeted malware signatures
- Suspicious traffic patterns or lateral movement between zones

Detection of these threats relies on deep integration of real-time threat intelligence feeds with the specific context of DoD/DoW OT environments. This ensures that relevant IOCs are correlated with actual asset configurations, network topologies, and operational processes, allowing threat alerts to be validated and prioritized based on impact.

Threat Detection Capabilities to Look for in an OT Solution

A mature threat detection strategy in DoD/DoW OT environments must go beyond basic alerting. Effective solutions should provide the following capabilities:

- **OT Environment Baselining:** Establishing expected behavioral patterns for OT assets, networks, and processes to detect deviations in real time. This requires deep protocol awareness and the ability to monitor configuration changes, operational commands, and communications that indicate potential compromise.
- **Root Cause Analysis:** Correlating multiple alerts and security events into a cohesive threat narrative, enabling security teams to identify the true origin, scope, and potential mission impact of an incident rather than chasing isolated alerts.

- **Threat Intelligence Correlation:** Integrating real-time threat intelligence with the specific context of DoD/DoW OT and CPS assets. This ensures that IOCs and tactics, techniques, and procedures (TTPs) are mapped directly to mission-critical environments, allowing analysts to prioritize alerts based on operational relevance.
- **Robust Ecosystem Integrations:** Support seamless integration with existing security tools such as SIEM, SOAR, and EDR/XDR platforms to enable end-to-end incident detection, investigation, and response. This ensures OT threat detection is not siloed but instead part of the broader DoD/DoW cyber defense posture.

These capabilities help detect early-stage attacks and improve operational resilience by reducing false positives, accelerating response, and supporting Zero Trust's mandate for continuous visibility and enforcement.

III. The Claroty Platform: Securing OT as Part of ZT for OT

Backed by award-winning threat research from Claroty's Team82, widely cited by and leveraged within the US federal government, and a breadth of technology alliances, the Claroty platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value, and lower total cost of ownership.

The Claroty Platform is comprised of:

Continuous Threat Detection (CTD) On-Premises or Portable	**xDome Secure Access** On-Premises or SaaS-Powered	**xDome** SaaS-Powered
A robust on-premises or portable solution (available through Claroty's hardware partners) that delivers comprehensive cybersecurity controls across the entire OT cybersecurity journey. With flexible deployment options tailored to your scalability, cost, and compliance needs, this solution is ideal for air-gapped and other specialized environments.	Designed with the unique architectures, needs, and operational nuances of defense OT environments in mind, xDome Secure Access helps organizations increase productivity, minimize risk, and reduce the complexity of secure access to OT networks.	A highly flexible, modular SaaS solution that supports the entire OT cybersecurity journey—from asset discovery and vulnerability management to network segmentation and threat detection. xDome delivers rapid time to value, reduced risk, and a low total cost of ownership.

Claroty will continue to accelerate support to U.S. government entities with the specially designated xDome for Government and the pursuit of Federal Risk and Authorization Management Program (FedRAMP) High Impact Level authorization. Working with well-known FedRAMP services provider, Coalfire Federal, Claroty expects xDome for Government to reach full authorization by early 2026.

Specifically in the context of the DoD/DoW ZT for OT, per pillar:

DoD/DoW ZT for OT PILLAR	Claroty Product	Claroty Support
User	**xDome Secure Access**	• Centralizes policy-based remote access purpose-built for OT environments to manage contractors, OEM vendors, and facilities teams across all defense locations. • Enforces just-in-time access controls, including time-based restrictions, session timeouts, and automatic revocation to ensure access is granted only when necessary. • Eliminates third-party user credential access by leveraging password vaulting and assigning role-based, least-privilege access. • Records and monitors all remote sessions for auditing, threat detection, and compliance with security policies.
Device	**CTD** **xDome** **xDome Secure Access**	**CTD / xDome:** • Leverages OT-native active discovery. • Provides comprehensive vulnerability information about assets across IT, IoT, and OT systems. • Detects and alerts for OT threats and can be configured to syslog accordingly for SIEM monitoring. **xDome Secure Access:** • Provides Privileged Access Management (PAM) for accounts to remotely access OT systems when integrated with an IdP SAML integration.
Application & Workload	**CTD** **xDome** **xDome Secure Access**	**CTD / xDome:** • Inspects device application inventory using active discovery techniques. This is further amplified with integrations (MDM, EDR, XDR, etc.) to allow users to fully grasp their IT, IoT, and OT estate. • Provides comprehensive visibility for IOT/OT systems to ensure vulnerability management with CVSS, KEV, and EPSS data, enriching against tracking for risk mitigation. **xDome Secure Access:** • Provides Privileged Access Management (PAM) for accounts to remotely access OT systems when integrated with an IdP SAML integration.

Data	**CTD** **xDome** **xDome Secure Access**	**CTD / xDome:** • Supports device tagging to be used for creating logical asset zones • Monitors changes on OT assets and can route these types of alerts to a SIEM via integrations. **xDome Secure Access:** • Monitors net new files uploaded on OT assets and records remote sessions.
Network & Environment	**CTD** **xDome**	**CTD / xDome:** • Provides recommended segmentation policies that can be easily and automatically enforced via existing PEP infrastructure. • Enables continuous monitoring and behavioral baselining to understand how assets communicate under normal circumstances, allowing for automatic alerts to any policy violations. • Simulates network policies to show the potential impact on the environment prior to enforcement.
Automation & Orchestration	**CTD** **xDome** **xDome Secure Access**	**CTD / xDome:** • Provides attribution at the site level for users and roles, and can give permissions and rules for what devices/systems remote users can see per site. • Provides integration and interoperability across SOAR, SIEM, EDR, and IdP for OT security ecosystem alignment. • Provides robust APIs across Claroty's product portfolio, which are leveraged for interoperability out of the box. • Enables advanced threat detection and data enrichment by which IR teams can leverage for planning, detection, response, and recovery operations. **xDome Secure Access:** • Provides policy enforcement layer on top of IdP for standards and alignment for accessing OT systems, including RBAC.

Visibility & Analytics	**CTD xDome**	**CTD / xDome:** • Provides rich logging and reporting for IOT and OT systems with standardized logging that can be output to a SIEM to inform detection, threats, and response activities. • Enables continuous monitoring and behavioral baselining to understand how assets communicate under normal circumstances, allowing for automatic alerts to any policy violations or malicious threats. • Establishes an OT Cyber Threat Intelligence (CTI) program powered by five detection engines, 18,000+ pre-built signatures, and MITRE ATT&CK for ICS alert mapping—continuously enhanced by Claroty's data and Team82 research teams to evolve detections, ingest new threat intelligence, and integrate with SIEM/syslog tools.

Accelerating Zero Trust Outcomes Through Claroty's Ecosystem Integrations

Claroty's platform helps the DoD/DoW achieve its Zero Trust goals by leveraging an extensive ecosystem of technology partners. These integrations, which span across solutions like SOAR, SIEM, EDR, and IdP, enable the DoD/DoW to extend its existing IT security controls and governance to its operational technology (OT) environments, effectively closing critical security gaps.

Claroty designs its platform to integrate seamlessly with existing IT and OT security infrastructure, leveraging the broadest set of CPS security solutions through partnerships with leading technology providers such as Cisco, Fortinet, ServiceNow, CrowdStrike, Axonius, and other key members of its Technology Alliance Program, to:

- **Provide Unified Visibility:** By integrating with tools like CMDBs, EDRs, and SIEMs, Claroty aims to give organizations a single, comprehensive view of all IT, OT, IoMT, and IoT assets across their extended Internet of Things (XIoT). This helps break down traditional IT/OT silos.
- **Enhance Existing Investments:** Claroty believes in extending the value of a customer's existing security tools. The Platform's Ecosystem Enrichment collection method specifically leverages data from dozens of other technologies to enhance visibility and protection.
- **Improve Operational Efficiency:** By feeding OT/CPS data into IT workflows and tools, the platform enables faster incident response, more informed decision-making, and better collaboration between IT, OT, and security teams. This can lead to reduced downtime and security risks.
- **Extend Security Controls:** Claroty's technology integrations, some of which are highlighted in the ZT for OT table above, span SOAR, SIEM, EDR, and IdP. The integrations allow organizations to extend their established IT security controls and governance to their OT environments, closing security gaps.

Through its Technology Alliances Program (CTAP), Claroty strategically partners with OT and cyber-physical systems (CPS) manufacturers to deliver interoperable solutions.

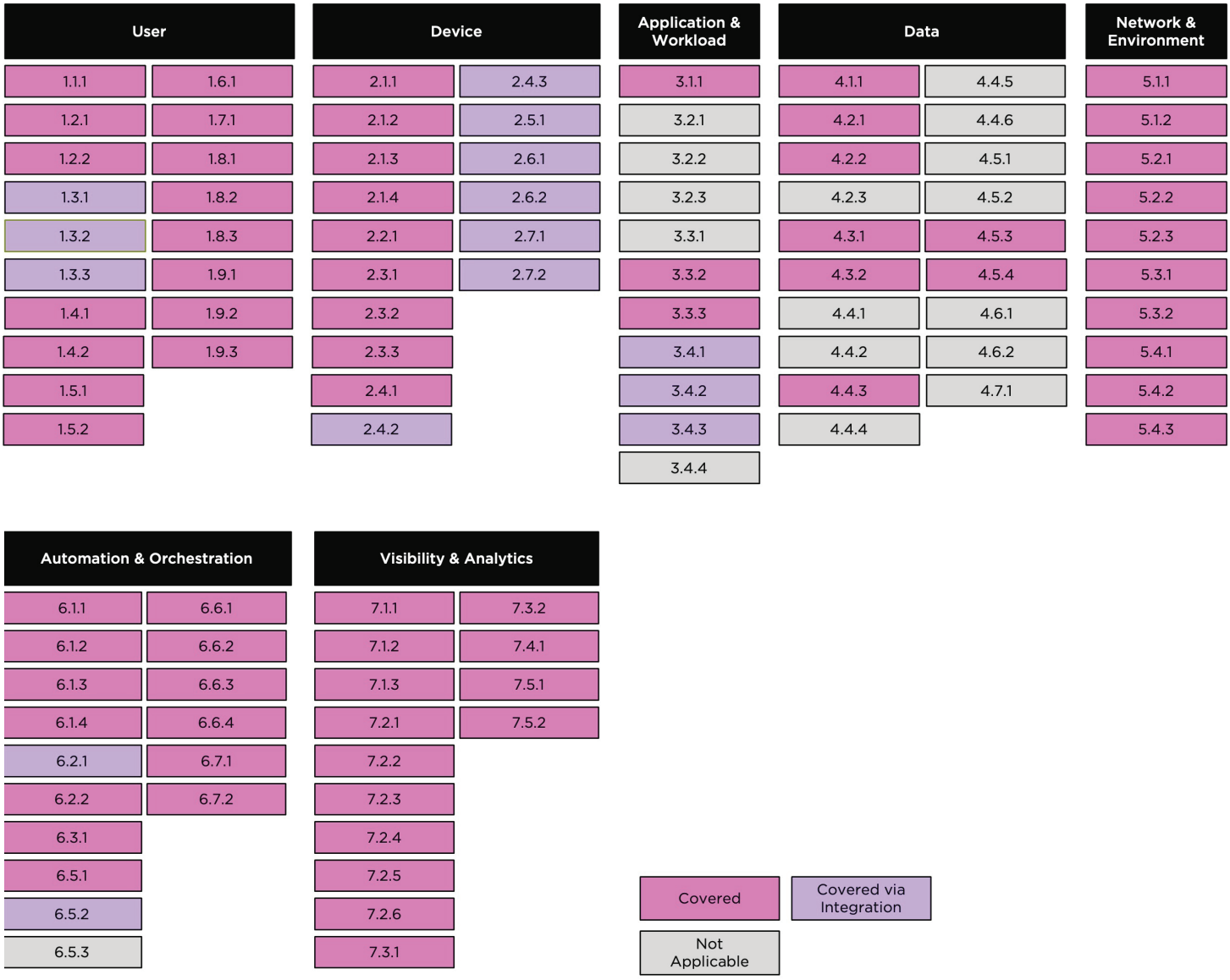
This “better together” approach provides the DoD and DoW with comprehensive insights, interoperability, and mitigation capabilities to defend mission-critical systems against evolving cyber threats. To explore Claroty’s full list of integrations, visit: https://claroty.com/platform/integrations.

Integrations Categorized by Pillar

User	Device	Applications & Workloads	Data	Network	Automation & Orchestration	Visibility & Analytics
IdP	EDR/XDR	EDR/XDR	EDR/XDR	Firewall	EDR/XDR	EDR/XDR
	MDM	IT Vulnerability Management Solutions	MDM	NAC	MDM	MDM
	SIEM	MDM	SIEM	Network Infrastructure/ Network Management	SIEM	SIEM
	SOAR	SIEM	SOAR		SOAR	SOAR
		SOAR				

Complete Mapping to DoD/DoW Zero Trust for OT Requirements

To demonstrate how the Claroty Platform directly supports the Department of Defense / Department of War's Zero Trust for OT framework, the following visual maps our product capabilities to OT activity requirements across all seven Zero Trust pillars. This representation provides a clear, holistic view of how our solution enables mission assurance by aligning security controls with operational realities, ensuring both compliance and operational resilience.



The Claroty Difference

Claroty, founded in 2015 and headquartered in New York, stands at the forefront of ZT solutions for OT networks in the private sector, which includes 20% of Fortune 100 companies. The Claroty team has developed active and passive software solutions specifically designed for cyber hardening of OT and DCI networks. These purpose-built solutions, collectively referred to as The Claroty Platform, are actively deployed across the United States, safeguarding all 16 sectors of critical infrastructure and effectively mitigating cyber risks in hundreds of millions of devices. The Platform has been deployed in thousands of locations and facilities spanning over 50 countries across all seven continents, in critical infrastructure from manufacturing facilities, to power systems, oil and natural gas installations, and other critical assets.

Positioned highest for Ability to Execute and furthest for Completeness of Vision, as of 2025, Claroty has been named a **Leader in the first-ever Gartner® Magic Quadrant™ for CPS Protection Platforms.**

Claroty Differentiators for DoD/DoW OT Zero Trust Implementation

1. **Unmatched Speed and Depth of Visibility**
   - Rapid asset discovery in minutes without hardware upgrades
   - Broadest and deepest protocol coverage
   - Deep asset context to power accurate vulnerability insights and risk assessments
2. **Accelerated Threat Response and Risk Reduction**
   - Continuous vulnerability and OT network visibility
   - Context-sensitive remediation prioritization
   - Accelerated detection and response (MTTD/MTTR) with actionable alerts
3. **Enterprise-Scale Resilience and Mission Readiness**
   - Reduced threats and attack surface across OT and CPS environments
   - Increased mission agility in responding to rapidly changing national and global realities

With a proven track record of success and a global footprint, Claroty continues to lead the charge in advancing OT cybersecurity, ensuring the cyber resilience of the world's critical infrastructure.

References:

[2] MeriTalk, in partnership with Claroty, Guardians of Government, Vol. 2: Fortifying the Cyber-Physical Frontier, September 2025

About Claroty

Claroty empowers organizations to secure automation, control, and other cyber-physical systems across industrial, healthcare, commercial, and public sector environments. The company's unified platform integrates with Agencies' existing infrastructure to provide comprehensive controls for visibility, exposure management, threat detection, and secure remote access. Backed by the leading investment firms and industrial automation vendors, Claroty is deployed at thousands of sites globally. The company headquartered in New York City with U.S. federal headquarters in Leesburg, VA. To learn more, visit clarotygov.us.