AT A GLANCE

Powering DoD/DoW Zero Trust for OT

Securing Mission-Critical Operational Technology (OT) in Defense Environments with The Claroty Platform

The OT Cybersecurity Challenge in Contested & Distributed Environments

The DoD/DoW operates a vast network of operational technology (OT) and cyber-physical systems (CPS) that are critical to mission readiness, national security, and defense infrastructure. As these systems modernize and adopt more connected technologies, their cyber attack surface expands, increasing exposure to nation-state threats. OT/IT convergence, strict compliance requirements, and contested environments make securing these systems uniquely complex—challenges that traditional IT security tools cannot address.

Implementing a Zero Trust framework tailored for OT enables DoD/DoW organizations to build resilient, secure networks. Claroty supports these frameworks at the Target and Advanced levels by providing deep asset visibility, threat detection, network protection, and facilitated information sharing to safeguard critical systems.

The Claroty Platform

The Claroty Platform provides a **unified OT security solution** for the DoD/DoW, enabling organizations to **monitor, manage, and protect mission-critical systems** without relying on multiple point solutions. Flexible deployment (on-premises, portable, or cloud) aligns with mission requirements, compliance mandates, and scalability needs. Backed by Claroty's Team82 threat research group and a broad partner ecosystem, Claroty delivers **rapid time-to-value, actionable insights** on known and unknown threats, reduced cyber risk, and **lower total cost of ownership**—regardless of OT program scale or maturity.

Claroty's Role in Advancing the DoD/DoW Zero Trust Strategy

The below visual illustrates how our platform maps to OT activity requirements across all seven Zero Trust pillars. By aligning security

Key Features & Benefits

- **Rapid, Comprehensive Asset Visibility** - OT and broader CPS assets in minutes (without hardware or network upgrades) to gain deep, context-rich insights.
- **Continuous Monitoring** - Real-time OT network and vulnerability visibility.
- **Prioritized Remediation** - Impact-sensitive guidance for faster, more effective mitigation using EPSS, KEV, and other context.
- **Deployment Agility** - Flexible deployment that delivers rapid, on-demand OT security across on-premises, portable, cloud, and even disconnected or remote mission environments.

controls with operational requirements, our solution enables mission assurance, strengthens compliance, and ensures resilient, secure operations, enabling defense organizations to proactively manage risk in complex, high-stakes environments.

User		Device		Application & Workload	Data		Network & Environment
1.1.1 ■	1.6.1 ■	2.1.1 ■	2.4.3 ▨	3.1.1 ■	4.1.1 ■	4.4.5 □	5.1.1 ■
1.2.1 ■	1.7.1 ■	2.1.2 ■	2.5.1 ▨	3.2.1 □	4.2.1 ■	4.4.6 □	5.1.2 ■
1.2.2 ■	1.8.1 ■	2.1.3 ■	2.6.1 ▨	3.2.2 □	4.2.2 ■	4.5.1 □	5.2.1 ■
1.3.1 ▨	1.8.2 ■	2.1.4 ■	2.6.2 ▨	3.2.3 □	4.2.3 □	4.5.2 □	5.2.2 ■
1.3.2 ▨	1.8.3 ■	2.2.1 ■	2.7.1 ▨	3.3.1 □	4.3.1 ■	4.5.3 ■	5.2.3 ■
1.3.3 ▨	1.9.1 ■	2.3.1 ■	2.7.2 ▨	3.3.2 ■	4.3.2 ■	4.5.4 ■	5.3.1 ■
1.4.1 ■	1.9.2 ■	2.3.2 ■		3.3.3 ■	4.4.1 □	4.6.1 □	5.3.2 ■
1.4.2 ■	1.9.3 ■	2.3.3 ■		3.4.1 ▨	4.4.2 □	4.6.2 □	5.4.1 ■
1.5.1 ■		2.4.1 ■		3.4.2 ▨	4.4.3 ■	4.7.1 □	5.4.2 ■
1.5.2 ■		2.4.2 ▨		3.4.3 ▨	4.4.4 □		5.4.3 ■
				3.4.4 □			

Automation & Orchestration		Visibility & Analytics	
6.1.1 ■	6.6.1 ■	7.1.1 ■	7.3.2 ■
6.1.2 ■	6.6.2 ■	7.1.2 ■	7.4.1 ■
6.1.3 ■	6.6.3 ■	7.1.3 ■	7.5.1 ■
6.1.4 ■	6.6.4 ■	7.2.1 ■	7.5.2 ■
6.2.1 ▨	6.7.1 ■	7.2.2 ■	
6.2.2 ■	6.7.2 ■	7.2.3 ■	
6.3.1 ■		7.2.4 ■	
6.5.1 ■		7.2.5 ■	
6.5.2 ▨		7.2.6 ■	
6.5.3 □		7.3.1 ■	

■ Covered

▨ Covered via Integration

□ Not Applicable

Visit clarotygov.us to download a complete mapping of Claroty and partner solutions to all Target and Advanced-level requirements with detailed, product-by-product capabilities to meet them.

About Claroty

Claroty empowers organizations to secure automation, control, and other cyber-physical systems across industrial, healthcare, commercial, and public sector environments: i.e. the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability 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 is headquartered in New York City with U.S. federal headquarters in Leesburg, VA. To learn more, visit clarotygov.us.