




PORTFOLIO OVERVIEW

Claroty Industrial Solutions





Digital transformation has created converged industrial environments where OT assets operate with various other cyber-physical systems (CPS) - including IoT, IT, BAS, and other connected assets. While this connectivity offers clear operational benefits, it also introduces risk in the form of an expanded attack surface, threatening operational availability, integrity, and safety. Traditional IT security measures fall short in safeguarding CPS due to their unique architectures, proprietary protocol usage, and environmental and operational constraints.

Claroty provides comprehensive CPS security solutions that are tailor-made for manufacturing and critical infrastructure networks. These solutions integrate with and protect these environments, regardless of scale, architecture, or existing cybersecurity ecosystems.

 <p>xDome Platform</p> <p>Broad CPS security within a modular, SaaS-powered platform including exposure management, network protection, secure access, and threat detection solutions. xDome delivers reduced risk with the quickest time to value and a low cost of ownership.</p>	 <p>xDome Secure Access</p> <p>Designed with the unique architectures, needs, and operational nuances of CPS environments in mind - helping organizations increase productivity, minimize risk, and reduce the complexity of secure access to CPS networks.</p>	 <p>Continuous Threat Detection (CTD)</p> <p>Comprehensive on-premises solution that excels in CPS discovery-revealing risk and monitoring for malicious activity that can impact OT networks through superior exposure management and threat detection capabilities.</p>
---	---	---

CPS Protection with Claroty

Claroty's unrivaled industry expertise across a variety of manufacturing and other critical infrastructure sectors and breadth of cyber-physical-system (CPS) knowledge sits at the foundation of our comprehensive portfolio of cybersecurity solutions. Recognizing that no two CPS networks are the same, there cannot be a one-size-fits-all approach to discovering them.

 <p>Passive Monitoring</p> <p>Continuous monitoring of network traffic to identify asset profiles</p>	 <p>Safe Queries</p> <p>Targeted discovery of assets in their native protocol</p>	 <p>Claroty Edge</p> <p>Speedy, host-based asset profiling through localized queries</p>	 <p>Project File Analysis</p> <p>Regular ingestion of offline configuration files for asset enrichment</p>
--	---	--	--

Claroty CPS discovery methods

Claroty employs multiple discovery methods to identify all assets within the operational network, including those that use unique or proprietary protocols, are air-gapped, or are otherwise unreachable through passive-only means. These capabilities enable Claroty to provide the broadest, built-for-CPS solutions around Exposure Management, Network Protection, Secure Access, and Threat Detection.

Exposure Management	Leverage exploitability insights and potential impact of risks on business operations for exposed assets in order to create a programmatic approach to CPS-specific continuous exposure management.
Network Protection	Create production-aligned zone and communication policy recommendations for various CPS based on in-depth insight into operational context and best practices, driving network segmentation and anomaly detection.
Secure Access	Purpose-built secure access solution using in-depth asset profiles and policies to provide privileged access and identity management & governance within a single, unified platform.
Threat Detection	Detect known and unknown threats, as well as operational changes, with continuous monitoring of asset behavior and dynamic threat intelligence feeds - protecting operational integrity of CPS environments.

These solutions, paired with cloud-based or on-premises deployment modes, eliminate the need to purchase and maintain multiple point products and provide the flexibility to choose the deployment approach that best suits your scalability needs, cost considerations, and compliance requirements. This dynamic approach to CPS cybersecurity is why Claroty is able to help critical infrastructure enterprises **reduce the cyber risk** that results from increased connectivity with the quickest **time-to-value (TTV)** and a lower **total cost of ownership (TCO)**—regardless of the scale or maturity of the asset owners’ CPS cybersecurity program.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial, healthcare, commercial, and public sector environments: the Extended Internet of Things (XIoT). The company’s unified platform integrates with customers’ existing infrastructure to provide a full range of controls for visibility, exposure management, network protection, threat detection, and secure access.

Backed by the world’s largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.