SOLUTION OVERVIEW

Claroty Continuous Threat Detection

Comprehensive On-Premise CPS Cybersecurity for The Modern OT Network

Digitalization initiatives and the expansion of remote workforces have transformed enterprises, causing once-isolated operational technology (OT) environments to become interconnected with their information technology (IT) counterparts. The result is the rise of converged IT/OT networks that offer great opportunities to enhance innovation and efficiencies within OT environments. However, as organizations continue to embrace digital transformation they face growing complexity in protecting their cyber-physical systems (CPS) amid expanding threat activity by malicious cyber actors.

Due to their unique architectures, proprietary protocol usage, and environmental and operational constraints, existing IT solutions fall short when protecting CPS. Purpose-build OT security is critical to provide a comprehensive solution for CPS cyber risk reduction enabling quicker time to value and a lower total cost of ownership.

Claroty Continuous Threat Detection (CTD) was created to help operational and/or cyber practitioners overcome the challenges of cyber-physical connectivity. Achieving resilience is far from impossible – and it requires a robust set of requirements that cannot be satisfied by traditional IT-centric solutions. Powered by an unmatched library of CPS communication protocols and in-depth industry knowledge, CTD provides superior visibility to OT environments. This enables the further implementation of core cybersecurity controls that span the entire cyber-physical security journey. These controls cover:

- Exposure Management
- Threat Detection
- Remote Incident Response

At A Glance

- Delivers complete visibility into industrial environments with multiple discovery methods and deployment mechanisms
- Supports the full cyber-physical system (CPS) cybersecurity journey from asset discovery to network integration and optimization
- Detailed network mapping supports automated zoning and virtual network segmentation
- Provides a contextualized root-cause analysis and risk-based scoring for all alerts
- Integrates with Claroty xDome Secure Access to enhance remote session incident response and investigation
- Leverages existing IT infrastructure such as SIEM, Firewalls, SOAR, CMDB tools to extend core cybersecurity capabilities to industrial environments

©Copyright Claroty. All rights reserved

Asset Discovery

Effective OT cybersecurity starts with knowing what needs to be secured. CTD leverages the broadest and deepest OT protocol coverage in the industry and employs multiple discovery methods to ensure the most complete network profile.

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

Claroty CPS discovery methods

This multi-spectral approach helps to uncover parts of the network that are not suitable for a single discovery method and results in unmatched visibility into CPS environments. This depth of discovery is seen across three aspects of visibility:

1. **Breadth of Discovery:** Employ distinct, highly flexible methods that can be combined or used separately to create comprehensive asset profiles
2. **Zone-Based Mapping:** Leverage in-depth asset profiles and communication monitoring to automate virtual segmentation of the OT network into Virtual Zones.
3. **Identify Asset Changes:** Additions to the network, configuration changes, and anomalies are some of the *many variables monitored by CTD to support MoC programs*

Claroty CTD segmentation view with virtual zones

©Copyright Claroty. All rights reserved

Exposure Management

CTD automatically compares each asset in an OT environment to an extensive database of insecure protocols, CVEs, configurations, substandard security practices, and other vulnerabilities tracked by Claroty's award-winning Team82 researchers. As a result, users can identify, prioritize, and remediate risk exposures in OT networks more effectively.

- **Identify Exposures:** Profile assets to identify their exposure to risk, including vulnerabilities, misconfigurations, end-of-life insights, and more
- **Attack Vector Mapping:** Contextualize and validate exposures by analyzing known risks to calculate the most likely scenarios in which an attacker could compromise the network
- **Risk-Based Scoring:** Automatically evaluate and score vulnerabilities based on the unique risk they pose to your network, enabling more efficient and effective prioritization and remediation

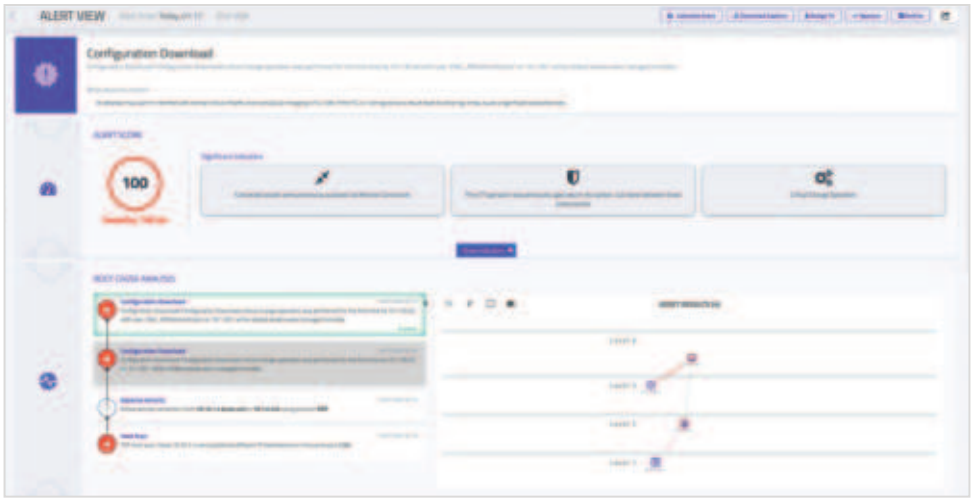
CTD Risk Score comrpised of five unique factors

Threat Detection

Threats to OT networks are often innovative yet can be deceptively simple, exploiting our compulsion toward process adherence to introduce risk. CTD utilizes multiple detection engines to automatically profile all assets, communications, and processes in OT networks, generate a behavioral baseline that characterizes legitimate traffic in order to weed out false positives, and alert users in real-time to anomalies and known, unknown, and emerging threats. Highlights:

- **Detect Known and Unknown Threats:** Characterize legitimate traffic to detect anomalous communications, identify threat signatures, weed out false positives, and alert users in real-time to known, unknown, and emerging threats.
- **Operational Event Alerting:** Continuously monitor critical change operations in the industry environment to help ensure your process integrity and uptime, receiving alerts for actions like configuration downloads which provide insights into the exact code changes within a file.
- **MITRE ATT&CK Alert Mapping:** Incoming alerts are mapped to the MITRE ATT&CK for ICS Framework to help increase the context surrounding the event and assist in identifying known remediation measures.
- **Root Cause Analysis:** Reduce network noise, false positives, and overall alert fatigue by correlating related alerts and indicators into a single chain-of-events, providing a consolidated view of the activities surrounding an alert.

©Copyright Claroty. All rights reserved



Claroty CTD alert view showing root-cause analysis and chain of events

Remote Incident Response

As part of a holistic approach to CPS cybersecurity, CTD and Claroty xDome Secure Access join forces to drive enhanced alert response capabilities across the two solutions–enabling users to detect, investigate, and respond to incidents from any location. As a result, organizations can adapt their overall security posture and workflows for a remote, distributed, or hybrid work environment with:

Receive alerts and related indicators for events during remote sessions directly within CTD

Investigate remote user activity with access to remote logs, live monitoring, and recorded sessions

Respond to remote incident alerts with the ability to immediately disconnect remote sessions

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. This protection begins with Claroty's intimate understanding of CPS networks and all assets within them. Recognizing that no two CPS networks are the same, there cannot be a one-size-fits-all approach to discovering them.

Our 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 asset owners' 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.

CLAROTY

©Copyright Claroty. All rights reserved