CLAROTY

Data Sheet

CLAROTY CONTINUOUS THREAT DETECTION (CTD)

Full Visibility and Fundamental Controls for Industrial Networks

The Industrial Cybersecurity Challenge & Claroty CTD

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 industrial networks with complex and expanded attack surfaces that IT security teams are increasingly responsible for protecting. The challenge is the OT portions of these industrial networks typically comprise proprietary protocols and unfamiliar assets, making them incompatible with IT security tools and invisible to IT security teams.

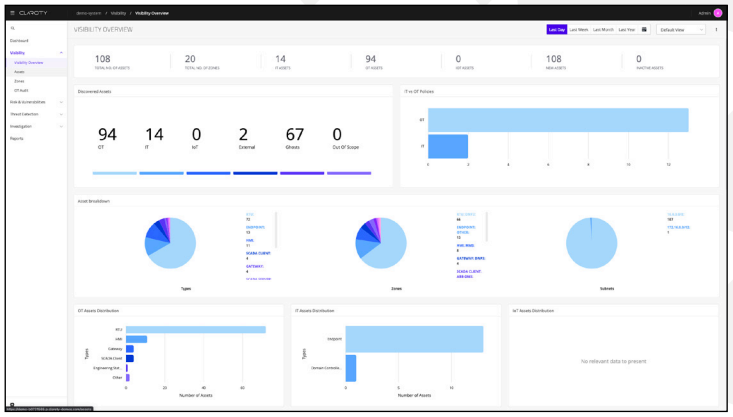
Claroty Continuous Threat Detection (CTD) was created to help both IT and OT teams overcome this challenge. As the foundation of The Claroty Platform's comprehensive industrial cybersecurity capabilities, CTD is backed by an unmatched library of industrial protocols, three unique asset discovery methods, proprietary DPI and virtual segmentation technology, and the renowned Claroty research team. This solution empowers customers to reveal and protect their OT, IoT, IIoT assets, detect and respond to the earliest indicators of threats, and seamlessly extend their existing enterprise security and risk infrastructure and programs to harden their industrial networks.

CTD extends the same controls IT security teams use to minimize risk in IT environments to OT environments. These controls cover:

- OT Visibility & Asset Management
- Network Segmentation
- Threat & Anomaly Detection
- Vulnerability Management
- Remote Incident Management
- Scalable Data Management & Controls

Key Features & Capabilities

- Extends fundamental IT security controls to OT environments
- Delivers complete visibility into previously invisible industrial networks
- Continuously detects anomalies, known and emerging threats, and zero-day attacks
- Automatically provides root-cause analysis and risk-based scoring for all alerts
- Includes real-time threat intelligence updates via the Claroty Cloud
- Reveals the frequency and potential impact of alerts received by peers via Wisdom of the Crowd
- Enables users to receive and respond alerts related to remote activity via Secure Remote Access (SRA)
- Seamlessly integrates with existing IT security infrastructure and and workflows



CTD Visibility Overview

Industrial Visibility & Asset Management

Effective industrial cybersecurity starts with knowing what needs to be secured. CTD leverages the broadest and deepest industrial protocol coverage in the industry and unmatched Passive, Active, and AppDB scanning capabilities to provide comprehensive industrial visibility and asset management controls, resulting in a highly detailed, centralized inventory of all OT, IoT, and IIoT assets, processes, and connections. Claroty is the only vendor to offer this caliber of visibility across all three dimensions integral to effective risk calculation and reduction for industrial networks:

1. **Asset Visibility:** This encompasses all OT, IoT, and IIoT assets on an industrial network, including serial networks, as well as extensive attributes about each asset, including model number, firewall version, and card slot, among others.
2. **Session Visibility:** This includes all industrial network sessions along with their bandwidth, actions taken, changes made, connectivity paths, and other details relevant to industrial network sessions.
3. **Process Visibility:** This includes tracking of all industrial operations, the code section and tag values of all processes with which OT, IoT, or IIoT assets are involved, and any abnormal changes to these assets' process values that could indicate threats to process integrity.

Threat & Anomaly Detection

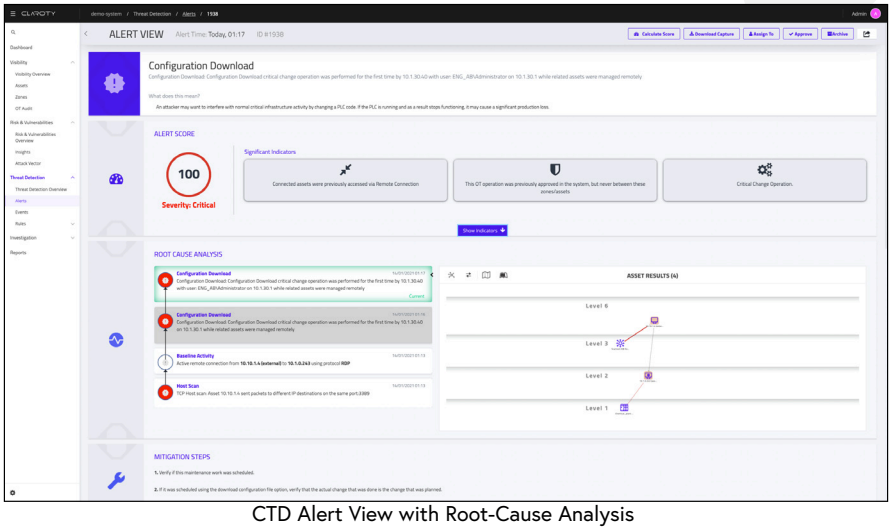
Threats to industrial networks are often innovative yet deceptively simple, exploiting our compulsion toward process to introduce risk. CTD utilizes five detection engines to automatically profile all assets, communications, and processes in industrial networks, generate a behavioral baseline that characterizes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

OT Specific Threat Intelligence: CTD includes industrial-specific threat intelligence that is updated in real-time via the Claroty Cloud to support swift detection of threats.

Contextual Alert Risk Scoring: This single metric is based on the unique context in which each alert is triggered, enabling users to easily filter out false positives and quickly understand and prioritize alerts for triage and mitigation.

Wisdom of the Crowd: Claroty's Wisdom of the Crowd capability utilizes anonymized information from similar events across Claroty's customer base to provide context into the frequency and potential impact of the alert, enabling users to respond more effectively and efficiently.

Root Cause Analysis: This feature groups all events related to the same attack or incident into a single alert, providing a consolidated view of the chain of events, as well as a root-cause analysis. The result is a higher signal-to-noise ratio, fewer false positives, reduced alert fatigue, and thus more efficient and effective triage and mitigation.



CTD Alert View with Root-Cause Analysis

Network Segmentation

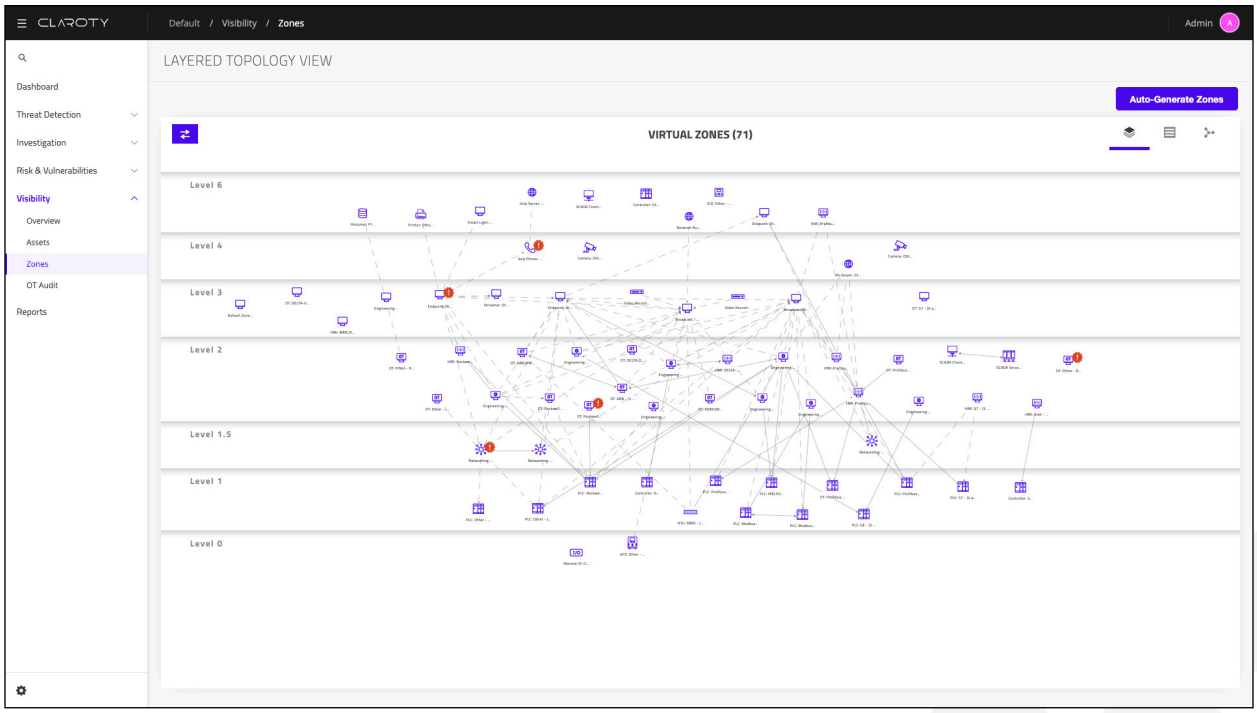
The extensive visibility CTD provides enables it to automatically map and virtually segment industrial networks into Virtual Zones, which are logical groups of assets that communicate with one another under normal circumstances. Key benefits:

Cross-zone violations yield real-time alerts that are automatically scored based on risk to help security teams prioritize

Customers without existing physical or logical segmentation can use Virtual Zones as a cost-effective alternative

Customers seeking to implement physical or logical segmentation accelerate such initiatives using Virtual Zones as the blueprint

Customers can integrate CTD with their existing firewalls and network access control (NAC) products to proactively enforce policy-based segmentation and mitigate active attacks



CTD Virtual Zones in Layered View

Vulnerability Management

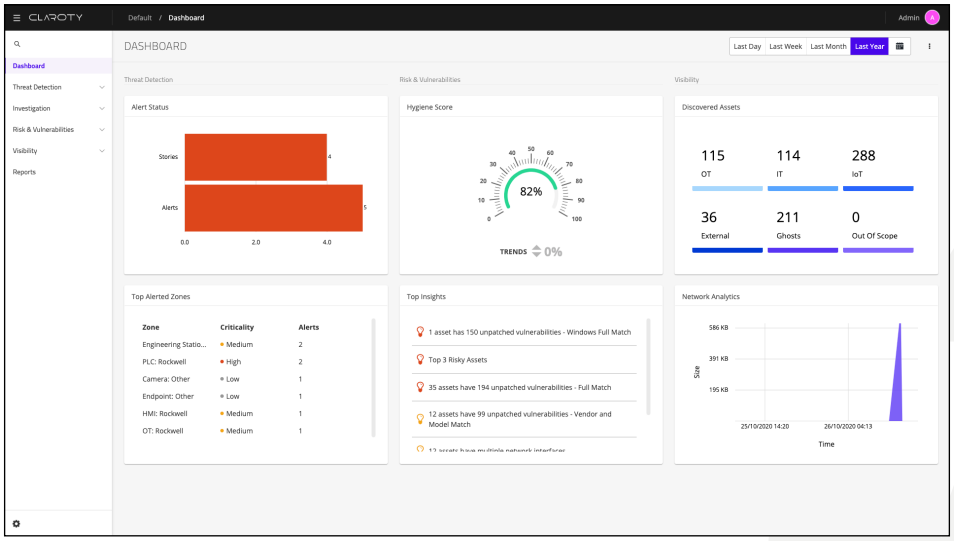
CTD automatically compares each asset in an OT environment to an extensive database of insecure protocols, configurations, substandard security practices, and other vulnerabilities tracked by Claroty, as well as to the latest common vulnerabilities and exposures (CVE) data from the National Vulnerability Database. As a result, users can identify, prioritize, and remediate vulnerabilities in industrial networks more effectively. Highlights:

- **Full-Match Vulnerabilities:** The complete visibility, including granular details about each OT, IoT, and IIoT asset, provided by CTD facilitates easy and accurate identification of exact-match vulnerabilities.
- **Attack Vector Mapping:** This feature identifies and analyzes all vulnerabilities and risks in an OT environment to automatically calculate the most likely scenarios in which an attacker could compromise the environment. It also provides mitigation recommendations for each scenario.
- **Risk-Based Prioritization:** All vulnerabilities are automatically evaluated and scored based on the unique risk they pose to each OT environment, enabling more efficient and effective prioritization.

Remote Incident Management

As part of a holistic approach to industrial cybersecurity, CTD and Claroty Secure Remote Access (SRA) join forces to distinguish The Claroty Platform as the industry's first industrial cybersecurity solution to offer fully integrated remote incident management capabilities. These capabilities span the entire incident lifecycle, enabling users to detect, investigate, and respond to industrial cybersecurity incidents across the broadest possible attack surface from any location. As a result, organizations can easily evolve and adapt their overall security posture and workflows for a remote, distributed, and/or highly variable work environment. Highlights:

- **Receive Alerts Related to OT Remote User Activity:** CTD triggers alerts when remote users partake in unauthorized or abnormal activities — such as configuration downloads or servicing assets outside of predetermined maintenance windows — while connected to the OT environment via SRA. These alerts contain contextual information including the SRA user, session intent, indicators, assets involved, and a root-cause analysis to support prioritization and triage efforts.
- **Investigate OT Remote User Activity:** All CTD alerts related to OT remote user activity includes a direct link to the associated SRA session and the ability to monitor that session live. If the session is no longer active, the alert will link directly to a full-length video recording that can be viewed for investigation purposes.
- **Respond to OT Remote User Activity:** All CTD alerts related to OT remote user activity also enable administrators to immediately disconnect the associated SRA session if deemed necessary as a response action in order to prevent, contain, and/or remediate any damages caused by unauthorized changes or other activities conducted by OT remote users.



CTD Dashboard View

Scalable Management, Analytics, and Deployment Options

The Enterprise Management Console (EMC) supports multi-site CTD deployments with centralized data, analytics, and administrative controls. The EMC can be deployed either on-premises or in The Claroty Cloud. Highlights include:

- **Analytics & Reporting:** In multi-site installations of CTD each server sends data directly to the EMC for aggregation and display, providing the operator with a consolidated, cross-site view of assets and their data.
- **Centralized Alert Management:** EMC enables users to receive and respond to alerts from across CTD sites, including those that are triggered by remote session activity via SRA.
- **Integrations:** EMC seamlessly integrates with existing IT security tools, simplifying system management and reducing the industrial cybersecurity learning curve by enabling customers to utilize existing systems.
- **CTD.Live:** A SaaS-based deployment option for the EMC that utilizes The Claroty Cloud and uniquely supports digital transformation and the modernization of industrial cybersecurity programs. CTD.Live scales as you scale, and provides automatic updates that include The Claroty Platform's latest features, fixes, and improvements.

CLAROTY

About Claroty

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership. Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America, and deployments on all seven continents.

To learn more, visit **www.claroty.com**.

CONTACT US

contact@claroty.com