Overview

THE CLAROTY PLATFORM

A Complete OT Security Solution

The Claroty Platform comprises Claroty's Continuous Threat Detection (CTD), Enterprise Management Console (EMC), and Secure Remote Access (SRA) systems. This single, agentless solution seamlessly integrates with existing IT security infrastructure and provides the industry's broadest range of Operational Technology (OT) security controls across four areas: visibility, threat detection, vulnerability management, and triage & mitigation.

Continuous Threat Detection (CTD)

- Automatically discovers & manages all assets to deliver full OT visibility
- Detects known & zero-day threats in real time
- Continually monitors for exact-match vulnerabilities
- Provides AI-driven network zoning & segmentation

Secure Remote Access (SRA)

- Secures, controls, & streamlines OT remote access
- Minimizes risk introduced by remote & third-party users
- Enforces IT-OT security best practices
- Enables ongoing auditing for maintenance & compliance

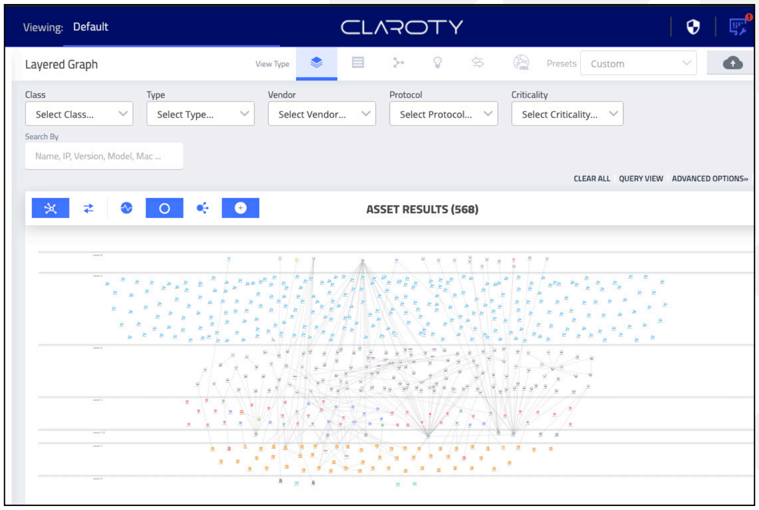
Enterprise Management Console (EMC)

- Deploys rapidly & safely with zero risk of downtime
- Delivers a unified IT-OT view designed for the SOC
- Consolidates alerts & risk analysis across sites
- Integrates seamlessly with IT security infrastructure

Visibility

The Claroty Platform leverages unmatched protocol coverage and discovery methods to achieve full OT visibility, including:

- **Asset Visibility** encompasses all devices on an OT network, including serial networks, as well as extensive attributes about each device such as model number and firewall version.
- **Network Visibility** includes all network sessions along with their bandwidth, actions taken, changes made, and other relevant details.
- **Process Visibility** tracks all OT operations, as well as the code section and tag values of all processes with which OT assets are involved.



Vulnerability Management

The visibility provided by The Claroty Platform extends to vulnerabilities and risks present within OT networks. Core capabilities and features include:

- **Full-Match CVEs:** Real-time discovery and assessment of exact-match CVEs in network assets
- **Attack Vectors:** Automatically provides the most likely scenario of network compromise
- **Risk Dashboard:** Customizable dashboard that provides an overview of risk analytics

Threat Detection

CTD utilizes five detection engines to automatically profile all assets, communications, and processes in your OT network to detect anomalies and both known and zero-day threats in real-time.

Claroty Threat Detection Engines

- Anomaly Detection
- Security Behaviors
- Known Threats
- Operational Behaviors
- Custom Rules

These capabilities are strengthened by automatic threat intelligence updates from the Claroty Cloud that include:

- Proprietary threat and vulnerability research from the Claroty team
- Indicators of compromise (IoC)
- The latest Common Vulnerabilities and Exposures (CVE) data from the National Vulnerabilities Database (NVD)

Triage & Mitigation

All aspects of The Claroty Platform work together with an extensive integrations ecosystem to streamline and expedite triage & mitigation processes.

- **Contextual Alert Risk Scoring:** A single metric produced by a unique algorithm to provide context around the circumstances that trigger each alert.
- **Root Cause Analysis:** All events related to the same attack or incident are grouped into a single alert to provide a consolidated view of the chain of events, as well as a root-cause analysis.
- **Remote Session Auditing:** Network session recordings can be audited to trace the root cause of alerts and pinpoint key details about them.

About Claroty

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.

CONTACT US

contact@claroty.com