CLAROTY

Overview

THE CLAROTY PLATFORM

The Industrial Cybersecurity Solution

The Claroty Platform is a complete industrial cybersecurity solution that comprises Claroty's Continuous Threat Detection (CTD), Secure Remote Access (SRA), and Edge technologies. The platform seamlessly integrates with any industrial environment regardless of its scale, architecture, or the maturity of existing cybersecurity programs. Highly flexible and rapid deployment options enable The Claroty Platform to reveal and protect all OT, IoT, and IIoT assets within the network while automatically detecting the earliest indicators of threats to those assets via proprietary detection technologies. Further extending the value of these controls, Claroty maintains a vast integration ecosystem, robust API, and employs the industry's only solution for integrated remote incident management capabilities that span the entire incident lifecycle.

Claroty CTD

- Rapidly discovers and manages all assets to deliver full industrial network visibility
- Detects known & zero-day threats and behavioral and operational anomalies in real-time
- Automatically enriches alerts with root-cause analysis, risk information, & reputational context
- Correlates OT remote-user activity with anomalous events & malicious indicators
- Continually monitors for full-match vulnerabilities and provides AI-driven network zoning & segmentation
- Can be deployed on-premises or via CTD.Live, a SaaS-based option that supports enterprise-wide industrial cybersecurity data management

Claroty SRA

- Secures, controls, & streamlines industrial network remote access
- Minimizes risk introduced by remote & third-party users
- Enforces IT/OT security best practices in accordance with Zero Trust & Least Privilege principles
- Provides over-the-shoulder monitoring of all OT remote sessions for unauthorized changes, live troubleshooting, & emergency disconnections
- Enables ongoing auditing for maintenance, compliance, & forensic purposes
- Offers highly available, flexible configuration options, as well as directory services and antivirus solution integrations

Claroty Edge

- Provides nearly instantaneous visibility into all OT, IoT, and IT assets in an industrial environment
- Enhances the speed, ease, and effectiveness with which risks & vulnerabilities can be identified and managed
- No hardware, network changes, configuration, or any physical footprint required
- Suitable for any network, regardless of geographical spread or architecture
- Helps optimize incident response efforts including impact assessments, scoping, and post-incident forensics
- Excels in providing detailed information, instantly, for audit & compliance or M&A due diligence purposes.

Detect → Investigate → Respond

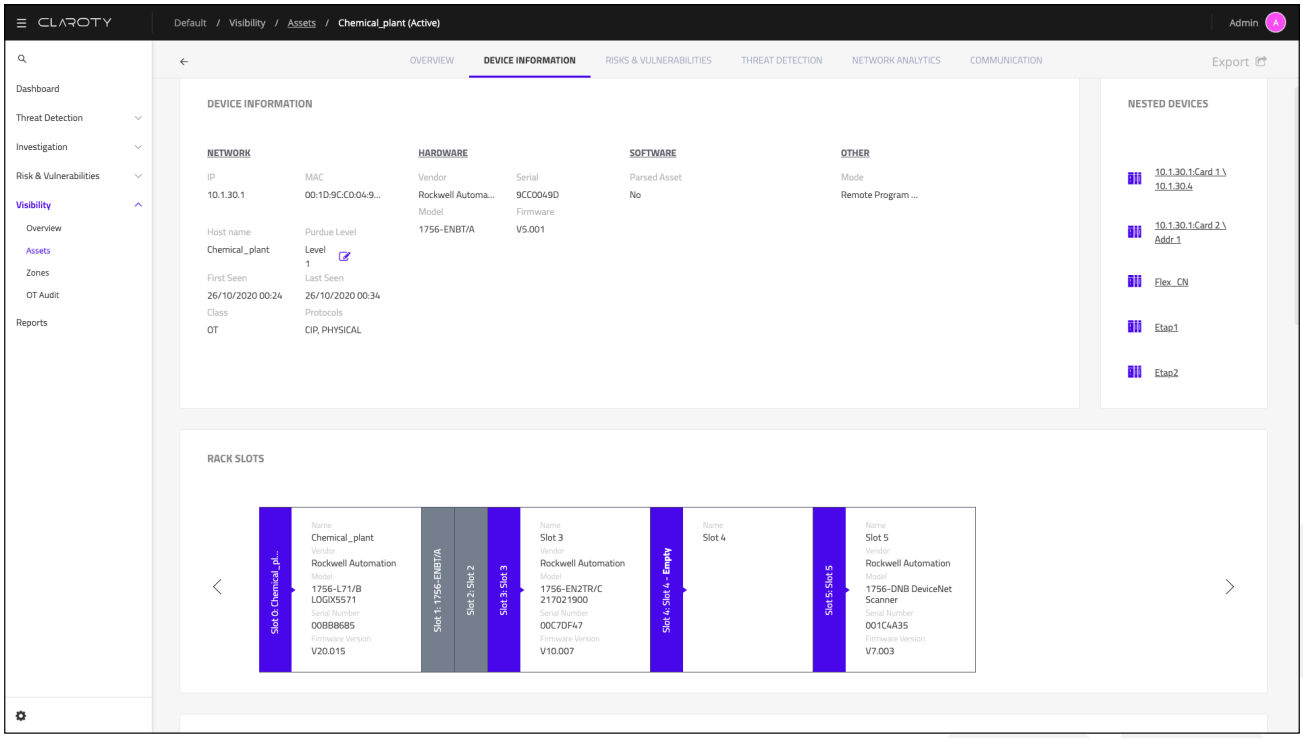
Protect your industrial environment across the broadest attack surface area with the industry's most extensive set of industrial cybersecurity controls and fully integrated remote incident management capabilities.

Copyright © 2021 Claroty Ltd. All rights reserved

Reveal

Effective industrial cybersecurity starts with knowing what needs to be secured. The Claroty Platform supports the industry's most comprehensive list of protocols found in industrial environments; these include an unmatched range of both proprietary and standard OT, IoT, IIoT, BMS, and IT protocols. This in-depth understanding of network communication provides unparalleled asset, network, and process visibility:

- **Asset Visibility** encompasses all devices on an industrial network, including serial networks, as well as extensive attributes about each device such as model number, firewall version, and custom asset attributes.
- **Network Visibility** includes all network sessions, including remote access, 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 industrial assets are involved.



CTD Asset Details page

Protect

The Claroty Platform provides insights into the inherent risks present within a network. These include things like critical vulnerabilities and misconfigurations, poor security practice among staff and vendors, and unreliable, unmonitored, and inefficient remote access mechanisms. This empowers users to not only identify and prioritize these areas of risk, but to deploy proactive controls and mitigations to manage network exposure.

- **Virtual Zones:** Automatic virtual network segmentation based on network communication under normal circumstances, creating a cost-effective alternative to physical segmentation and provides a mechanism for real-time alerts to cross-zone violations.
- **Attack-Vector Mapping:** Identifies and analyzes vulnerabilities and risks within the industrial environment to calculate the most likely scenarios in which an attacker could compromise the network.
- **Remote Access Control:** SRA uses a combination of multi-factor authentication, use-and-group-based tiered access permissions, and just-in-time provisioning to strictly control, monitor, and streamline remote access onto the network.

Copyright © 2021 Claroty Ltd. All rights reserved

Detect

Claroty's resilient threat detection model profiles all assets, communications, and processes in the industrial network to establish the fine-grain behavioral baselines that empower our five threat detection engines. The Claroty Platform equips enterprises with the ability to respond quickly and effectively when alerts surface, providing the context and information required to save minutes in situations where seconds count.

Claroty Threat Detection Engines

Anomaly Detection	Security Behaviors	Known Threats	Operational Behaviors	Custom Rules

Powered by the latest threat intelligence, Claroty continuously monitors for both known and unknown threats, automatically weeding out false positives, linking related alerts into a chain of events, and providing clear directions on how to mitigate threats before they impact operations.

- **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 Monitoring & Auditing:** OT remote sessions can be monitored live and full-length recordings can be easily audited.

Connect

Interconnectivity across enterprises has resulted in the rise of converged IT/OT industrial networks with complex and expanded attack surfaces. The Claroty Platform removes the barriers that have long limited industrial networks from being securely and effectively connected to what enables the rest of the business, resulting in more efficient operations and a lowered total cost of ownership through integration synergies:

- **Integration Ecosystem:** Claroty maintains a broad range of IT security tools such as SIEM, SOAR, and CMDB solutions, simplifying system management and reducing the industrial cybersecurity learning curve.
- **API Explorer:** Built on the Swagger framework, the API Explorer empowers users to harness the vast amount of network information provided by CTD to build custom feeds outside of the Claroty environment.
- **Claroty Edge & CTD.Live:** The instant visibility into assets and network risks provided by Edge paired with the cloud-based report-building capabilities of CTD.Live help to connect an organization's cybersecurity program with its governance, enterprise-wide risk, and compliance programs.

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

Copyright © 2021 Claroty Ltd. All rights reserved