Our Mission
Claroty’s mission is to protect industrial control networks from cyber-attacks; ensuring the safe and reliable operation of the world’s most critical infrastructures. Claroty enables customers enjoy the substantial benefits of increasingly networked-control systems compromising operational resiliency, personnel safety, or the security of core assets.

Your Result
With Claroty, your cybersecurity and engineering teams are armed with a solution that gives them visibility and tells them exactly what is happening across their complex industrial network. This means better security and reduced downtime, for your critical OT environments.
Leading Industrial Cybersecurity Company

Our mission is to protect industrial control networks from cyber-attacks; ensuring safe and continuous operation of the world most critical infrastructures.

Claroty was conceived and is actively supported by the world famous Team8 foundry. With substantial funding from an unrivaled syndicate of global investors—including some of the most important industrial automation companies on earth—Claroty has built the leading company in industrial cyber today.

Claroty’s technology has been tested, selected and adopted by the most influential industrial automation control vendors and networking companies in the world. Our strategic partnerships also include prominent system integration and managed security services firms worldwide.

Claroty has assembled an unprecedented executive team and attracted a premier interdisciplinary team of cybersecurity and industrial control system experts. We leveraged deep ICS knowledge and experience gained from industry and elite cyber units of the Israeli Defense Forces to design and build a platform for protecting your plants, processes and operations from cyber threats.

Our fully integrated cybersecurity platform, with its award-winning suite of products, provides extreme visibility into industrial networks — enabling unparalleled cyber threat protection, detection and response. Our technology is designed specifically for industrial control-networks and will "do no harm" to the underlying industrial processes these critical networks run.

Claroty has very large-scale production deployments across six continents and nine industrial segments. With offices around the globe and an unmatched team, technology and partnerships, Claroty is the company that will be there to protect your critical industrial processes over the long-haul.
Fortune 500 Customers

- Chemical & Petrochemical
- Discrete & Process Manufacturing
- Power and Electrical
- Oil and Gas
- Pharmaceutical
- Mining
- Food & Beverage
- Transportation
- Waste Water Treatment

Strategic Partners

- Rockwell Automation
- SIEMENS
- Schneider Electric
- Cisco
- PwC
- KPMG
- Dimension Data
- Kudelski Security
- Belden

Global Reach

Marquee Investors

- Rockwell Automation
- SIEMENS
- Schneider Electric
- Temasek
- Bessemer Venture Partners
- TEAM8
- ICV
- OP Investments
- Clearvision Ventures
Value Proposition

A single day of downtime can cost $20 Million!

Because industrial systems are critical, they will continue to be targeted; and because they are increasingly connected, they will be impacted even when they are not specifically targeted. Attacks in 2017 alone resulted in billions of dollars in losses to operators globally.

Critical infrastructure and other industrial systems were commissioned decades ago and often continue to operate with outdated, insecure control systems and SCADA devices. These critical systems were simply not designed with cybersecurity in mind and are exposed to cyber-attacks.

While industrial systems, especially older versions, contain numerous vulnerabilities attackers can exploit, ICS software and underlying industrial protocols in widespread use today lack even basic security controls. After gaining access to industrial networks, attackers can simply run legitimate software to issue commands that many controllers will execute without any security checks. Advanced threats will do more to remain stealthy and cause serious damage, but industrial systems can and will be compromised by less experienced adversaries as well.

Claroty’s integrated ICS cybersecurity suite was designed to address these inherent shortcomings and to protect the safety of people, industrial assets, and critical processes from cyber-attacks.

With Claroty, you can reduce risks to your industrial operations, minimize unplanned downtime and address regulatory requirements.
The Claroty Difference

- Technology powered by Claroty’s CoreX engine and world-class Claroty Research team
- Comprehensive, protection, detection and response in one integrated platform – yielding unmatched cyber-risk management and best in class TCO
- Extreme visibility into OT networks – powering industry-leading threat detection/ response, and unique vulnerability insights
- The industry’s first virtual segmentation for OT networks, combined with automated micro-segmentation support for unrivaled protection
- Proven, scalable, enterprise-class software with centralized multi-site management that has battle-tested in very large distributed deployments
- Claroty supports integrations with a wide range of security software, network infrastructure and IT operations products for improved security and reduced cost
- OT safe with Zero impact to existing systems and processes
Bringing Clarity to OT Networks
Extreme Visibility and Advanced Security for Industrial Control Systems

Claroty’s Multispectral Data Collection Capabilities provides:

Complete Network and Asset Visibility - Claroty provides a live window into ICS Networks, automatically identifying and tracking how assets are configured and changing over time. It builds a deep understanding of the communication patterns between assets—down to I/O level—communications that control the physical process.

Unique Insights - The Claroty Research team has an unmatched understanding of ICS network protocols and experience in protocol analysis. This deep knowledge provides customers with detailed insights about the inner workings of their industrial control networks.

Unmatched Threat Detection - Claroty leverages advanced behavior-based anomaly detection to rapidly detect early signs of malicious activity, discovers threats and process anomalies across the complete “cyber kill chain” and enables comprehensive ICS threat hunting. This deep knowledge makes it easy for IT/OT teams to stay on top of current ICS risks.

Proactive Protection - With complete visibility and detailed asset information, Claroty identifies threats present in the industrial network generating actionable alerts combined with operational context for detailed insights.

If you can’t see it, you can’t secure it.

If you don’t own it, you can’t analyze it.
Claroty has made a multi-million-dollar investment into the most extensive ICS lab in the industry. This investment has been paying dividends – allowing us to design, implement, and validate our unique methodologies on actual off-the-shelf devices and hardware — and simulate accordingly.

Leveraging this unique ecosystem, our research engineers ensure we continually evolve our solutions to provide the best possible protections available.
End-to-End

Fully Integrated Platform
Fully Integrated Platform

Claroty’s integrated ICS suite protects the safety of people, assets, and critical processes from cyber-attacks. The platform provides security teams with extreme visibility into industrial control networks, real-time monitoring, network segmentation, control over employee and 3rd party remote access, and integration with existing SOC, cybersecurity and network infrastructure.

Claroty Platform
- Provides extreme visibility into ICS Networks
- Identifies security gaps – including known and emerging threats and vulnerabilities
- Automatically generates current state of OT process-level communications and presents an ideal network segmentation strategy
- Detects security posture changes
- Enables proactive threat hunting with actionable threat information
- Secures, monitors, and records remote connections to ICS assets

Enterprise
Management
Console

Advanced Threat Detection
Continuous Vulnerability Monitoring
Network Segmentation
Secure Remote Access
Security Posture Assessment

End-to-End

Protect
Proactively discover and eliminate vulnerabilities, misconfigurations and unsecure connections.

Control
Implement network segmentation and manage remote access by enforcing granular access policies and recording sessions.

Detect
Continuously monitor and detect malicious activity and high-risk changes throughout the attack “kill-chain”.

Respond
Receive context rich alerts for rapid triage and investigation, and automate response using existing network infrastructure.

Claroty CoreX Technology
This advanced engine powers the Claroty Platform and is the foundation on which Claroty’s integrated suite of products is built on. It was specifically designed to ensure safe, secure and reliable operations in large, complex industrial networks.
CoreX Technology

Clarioty’s advanced CoreX engine powers the Claroty Platform and is the foundation on which Clarioty’s integrated suite of products is built on. It was specifically designed to ensure safe, secure and reliable operations in large, complex industrial networks.

Monitoring
CoreX establishes a high-fidelity baseline model of the OT network and employs advanced, behavior-based anomaly detection, coupled with a powerful intrusion detection engine to rapidly discover known and unknown threats. The system continuously monitors OT environments for changes and analyzes the network to uncover vulnerabilities by engaging Clarioty’s proprietary knowledge base.

Visualization
The sophisticated visualization engine depicts network nodes and communications pathways down to the lowest levels of the OT network—down to the serial and fieldbus networks that control physical processes. Advanced filtering combined with active animations delivers a complete picture of the network and how nodes are communicating.

Data Collection
With multispectral data collection, CoreX analyzes industrial networks and provides nearly 100% visibility into the OT environment. Using proprietary dissectors for all major IT and ICS protocols and configuration files, the system safely extracts fine-grained details about both IT and industrial assets in the OT network, discovers how the assets are configured and communicating, and deciphers the automation system conversations across serial and IP-based networks—all the way down to the I/O level. With multispectral data collection, customers can employ one or multiple modes to meet the unique technical, operational, deployment and cost requirements present in different industrial environments.

Scalable Architecture
Clarioty’s advanced CoreX engine was specifically designed to ensure safe, secure and reliable operations in large, complex industrial networks and is fully tuned to support multiple use cases, technical constraints, and environments including sites with limited computing power, requiring a smaller physical footprint, and scenarios where communication over low-bandwidth links is necessary.
Claroty's flagship product, Continuous Threat Detection, provides extreme visibility, continuous threat and vulnerability monitoring, and deep insights into ICS networks. It was specifically designed to ensure safe, secure and reliable operations in large, complex industrial networks – ensuring zero impact to the underlying operational processes and improved cyber resiliency.

Continuous Threat Detection extracts precise details about each asset on the industrial network, profiles all communications and protocols, generates a fine-grain behavioral baseline that characterizes legitimate traffic, and alerts you to network changes, new vulnerabilities and threats. The alerts the system generates provides the contextual information you need to investigate and respond quickly.

Real-time Threat Monitoring

Leveraging the advanced anomaly detection capability in CoreX, the system delivers superior threat detection and provides alerts across the full “cyber kill chain” – from early reconnaissance activity to later-stage attacks designed to impact control systems and processes. The system enables unparalleled threat hunting capabilities for a range of threats – a critical aspect for SOC and OT teams when investigating and responding to alerts. A key differentiator is the system’s context-rich alerts – ensuring SOC teams have immediate situational awareness and the details required to rapidly investigate issues and collaborate with “shop floor” teams for rapid remediation.
Virtual OT Network Segmentation

Leveraging our understanding of how your industrial automation system is configured and communicating, we use proprietary algorithms to group assets into logical segments and generate an ideal “virtual segmentation” scheme. Armed with this knowledge, and the associated baseline communications details, your teams can implement firewall policies—from port and protocol rules to application layer policies—or to construct appropriate VLANs. This unique capability provides cost-effective option for segmenting lower levels of OT networks where blocking is prohibited.

Continuous Vulnerability Monitoring

Claroty provides deep insights into your ICS environment-enabling to proactively identify and fix configuration and other network hygiene issues that can leave your network vulnerable to attack or lead to operational issues. Claroty continuously monitors the network for new known vulnerabilities, leveraging security intelligence curated by Claroty Research, making it easy for IT/OT teams to stay on top of current ICS risks. A key differentiator is the system’s ability to provide precise CVE matching – down to the precise firmware versions for industrial devices.
Clarity

Secure Remote Access

Secure Remote Access is the policy-based access control product within the Clarity Platform. It enables organizations to safeguard their networks from the threats introduced by unmanaged and unmonitored remote access.

Secure Remote Access is designed to minimize the risk remote users, including employees and contractors introduce to industrial networks. The system provides a single, managed interface through which all remote users connect and authenticate prior to performing software upgrades, periodic maintenance and other system support activities.

Network administrators employ the system to control which users are granted access to industrial control assets and for what purpose. The system enforces password management and access control policies, governs remote connections and monitors and records remote access sessions.

Product Highlights

- Proactive Access Control – Through granular user and asset policies governing which assets authorized users can see and access, when they can log into each asset and the authentication-level required for access.

- Password Vaulting – Securely store user and asset credentials. Eliminate shared passwords schemes, easily manage password changes and avoid risks from valid passwords of non-active users.

- Workflow Based Controls and Real-Time Monitoring – Using manual access requests and permissions and “over-the-shoulder” real-time video visibility into all remote user activity— including a “red button” ability to terminate ongoing sessions.

- Activity Reports – Filtered by user, asset or session and providing video recordings of all remote sessions.

Product Benefits

Monitor

SRA enables system administrators continuously monitor and audit privileged users, sessions, and assets, including which ICS devices are being accessed, by which user, and the total number of users who have access to each asset.

Secure

If a contradiction between the stated remote access purpose and the actual activity occurs, system administrators can immediately terminate the remote session, preventing network disruption, and improving overall cyber resiliency.

Audit

Following the remote session, system administrators and auditors can playback a full video recording of each session, as well correlate specific reports filtered by user, asset or session to facilitate retrospective auditing.
Claroty Security Posture Assessment

Claroty’s Security Posture Assessment is an offline assessment product that provides security teams with visibility and insights into the OT network’s security risk posture. The tool consumes a PCAP (packet capture) data file, collected from a network switch, and produces a comprehensive analysis of the ICS network. The report provides a summary and detailed analysis of the assets and communications discovered on the industrial network, pinpoints vulnerable assets and uncovers network configuration and other “network hygiene” issues that can provide attackers a pathway or impact critical processes.

**Product Highlights**

- **Consolidated view of operational and security risk** – instantly detect all of your OT vulnerabilities, providing a consolidated view of cyber risks across your entire ICS network.

- **Context-aware Intelligence** – deep visibility into the network’s assets, networking, and infrastructure along with a consolidated view of common vulnerabilities, threats, and common mitigation steps.

- **Actionable mitigation and remediation** – provide security teams with contextual mitigation recommendations to reduce the attack surface and strengthen the overall security posture.

- **Fully automated process** – fully automated report generation that does not require prior ICS knowledge and is considerably faster than manually generated reports.

**Product Benefits**

- **Asset Discovery**
  Automatically identify assets across the entire ICS network for inventory and management tasks as well as regulatory and internal audit requirements.

- **Detailed Network Analysis**
  Create a detailed report on the various control process devices and how they communicate within and across the network, including specific visibility on their communication paths and associated devices.

- **Comprehensive Insights**
  Provides a holistic picture and risk assessment across the entire ICS network.
**Enterprise Management Console**

Claroty’s Enterprise Management Console is a centralized server that aggregates data from Claroty products deployed across multiple sites and displays a unified view of assets, activities, alerts, and access control.

The ideal product for IT/OT SOC deployments – providing security teams with immediate visibility and alerts across the entire industrial control system complex.

The Enterprise Management Console can be easily integrated with various SIEM, log management, and security analytic products; enabling security teams to correlate OT and IT issues and gain real-time situational awareness across their networks.

**Integrations**

Claroty exports alert data via Syslog into leading SIEM products (e.g., Arcsight, Splunk, QRadar, etc.). SOC analysts can utilize existing analytic tools to filter and correlate alert data – enriching their existing IT security knowledge with data and insights into OT security.

**Product Highlights**

Multi-site View of Traffic, Assets, and Activities – receive consolidated cross-site asset, alert, and activity data, which can be filtered and analyzed to proactively search for operational and spot important security trends.

Unified Dashboard for a Comprehensive View – consolidated view of all the data Claroty products generate: alerts, assets, sites, and remote connections, providing full visibility into the enterprise industrial control system posture.

Integration with Security Tools – send alert data to various SIEM, log management, and security analytic products enabling the security team to correlate OT and IT and gain real-time situational awareness to active and potential threats.

**Product Benefits**

- **Centralized OT Visibility and Cybersecurity**
  Integration with existing security tools provides security teams with comprehensive real-time metrics across the entire infrastructure, including threats, risks and anomalies.

- **Streamlined SOC Operations**
  Consolidated ICS cybersecurity, risk metrics, and at-a-glance dashboards from thousands of assets across hundreds of distributed sites and remote facilities.

- **Efficient, Remote System Management**
  Easy maintenance and update mechanisms allows SOC and Security teams to remotely upgrade in-the-field deployed systems with a click of a button.
Claroty products are deployed as virtual appliances or installed on physical servers. Products within the Claroty Platform are integrated with each other and with existing cybersecurity tools, network infrastructure and IT systems—enabling you to leverage your current investment in tools, processes and training. For widely distributed environments, our sensor technology can be deployed on switches and other network infrastructure—providing flexibility and reduced cost for the most demanding use cases.

**Extreme Visibility / Continuous Monitoring**

- **Level 0** Field Devices I/O
  - Fieldbus I/O visibility
  - Profile and monitor nested devices external communication

- **Level 1** Control Network
  - PLC actions: Start, Stop, Monitor, Run, Reboot, Program, Test
  - Authentication to PLC
  - Maintain PLC privileged operations

- **Level 2** Process Network
  - Firmware download
  - Configuration download
  - Logic change
  - Corrupt OT packet
  - Online edits to PLC projects
  - Anomalous protocols behavior
  - Detect process communication halts

- **Level 3** Operations
  - Plaintext passwords
  - Unencrypted communication
  - Detect external connection (Internet)
  - Traffic activity summary
  - Proactively detect bad configurations
  - Simulate potential attack vectors
  - Unsecured protocols
  - Asset used ports

- **Level 4** Enterprise IT
  - Detect known attacks (MitM)
  - Detect network reconnaissance attempts
  - Signature-based detection
  - Unauthorized cross level/zone communication
  - Proactively detect nonresponsive devices
  - Connecting to Internet/corporate network DMZ
  - Detect misconfigurations (IP conflicts, dynamic IP)
  - New assets in the network
Passive: Continuous, Real-time Monitoring of OT Networks

- ABB Bailey
- ABB DMS system
- ABB HC800 (Infininet)
- ABB Spirit
- ABB Symphony Plus
- Alstom E-Terra
- BACNET
- NetBIOS Browser (UDP 138)
- Cisco Discovery Protocol (CDP)
- Control Technologies Inc. (CTI)
- Microsoft DCE RPC
- ABB DCS Service Manager
- Emerson DeltaV
- DACP
- DHCP
- DNS
- Emerson Ovation
- Emerson ROC Plus
- ETHERNET/IP
- Foundation Fieldbus (FF)
- Foxboro LLC
- FTP – SEL
- Siemens FWL LOAD (firmware upload)
- GE-ALM
- GE Bentley Nevada (BNC3500)
- GE-EGD
- GE-EGD-CMP
- GE PAC8000 (AXE)
- GE QuickPanel (TRAP+HTTP)
- GE SDI (MarkVie)
- GE SDI Classic (MarkVie)
- GE SRTP
- HART-IP
- HiDiscovery – Hirschmann LLC
- Honeywell C200 – Ftebcip
- Honeywell Experion – CNTComm (C300, EHPM)
- Honeywell EpicMo (C300 management)
- Honeywell Firewall CF9
- HTTP
- HTTP-XML (specific schemes)
- IEC101
- IEC103
- IEC104
- Lantronix Serial GW
- LLDP
- Mitsubishi Melsec
- MMS
- Modbus
- Modbus Modsoft
- Modbus Concept
- Modbus Eltec
- Modbus Exectool
- Modbus Schneider
- NetBios Datagram Service
- Niagara Tridium (BMS)
- Microsoft NTL.MSSP (Auth protocol)
- Omnimiflow Flow computer
- OPTO
- OPTO MMP

Active: Precise, Periodic Queries of OT and IT Assets

- DNP3
- Hirschmann Discovery Query
- Modbus Information Object
- Net Bias
- Profinet-DCP Query

OSIsoft PI
Siemens P2
POP3
ProConoS (TCP 20547)
Profinet DCP
Profinet I/O
Microsoft RDP
MOTT
RCDP
Redlion Crimson

Rockwell CIP
Rockwell PCCC
S7Comm Plus
S7Comm Plus
Microsoft SAMR
Microsoft CIFS (SMB)
SNMP
SSH
Synchrophasor
Telnet - DeltaV

BP Query
CIP Query
WMI Query
TCP Port Scan
Beckhoff Query
BACnet Query

App DB: Offline Enrichment of OT Asset Data

- Schneider – Modicon, Quantum
- Schneider – Concept
- Schneider Triconex – Tristation
- Yokogawa – CentumVP/CS3000
- Yokogawa – Prosafe

Honeywell – Experion
Honeywell – EHPM
GE – rx3i,9030
GE – Bently Nevada
ABB – AC800M

1 The list shows many of the most commonly used protocols. Claroty will add support for additional protocols in accordance with specific customer needs. For a full list of supported protocols, visit www.claroty.com