CLAROTY
Clarity for OT Networks

Solution Brief

Bringing Clarity To OT Network

Claroty enables customers to secure and optimize the industrial control networks that run the world's most critical infrastructure. The company's enterprise-class OT security platform is designed to address the unique safety and reliability requirements necessary to protect industrial networks– e.g., industrial control systems, SCADA, industrial IOT and others.

Finally, A Complete OT Security Platform

Claroty enables engineers, operators, and cyber security professionals to protect and optimize even the most complex OT networks with a single holistic platform.

Claroty Platform

Monitoring *Alerting* *Management*

The Claroty Difference

Deepest Visibility into OT networks

Supports all major ICS equipment vendors' open and proprietary protocols

Continuous, real-time monitoring

Full contextual information with each alert

Fully passive, monitoring – no impact to OT systems

Support for both Serial and Ethernet networks

Enterprise-class

Centralized multi-site management

Fast, simplified, agentless deployment

Powered by the world class Claroty Research team

Extreme Visibility: Diving Deep Into OT Networks

Claroty dives deep into the network, uncovers hidden information, and generates actionable insights to secure and optimize even the most complex OT environments.

Reducing The Network Into Granular Elements

Claroty explores the deepest level of OT protocols to identify the smallest elements encapsulated in the traffic.

Extracting Critical Information and Monitoring Changes

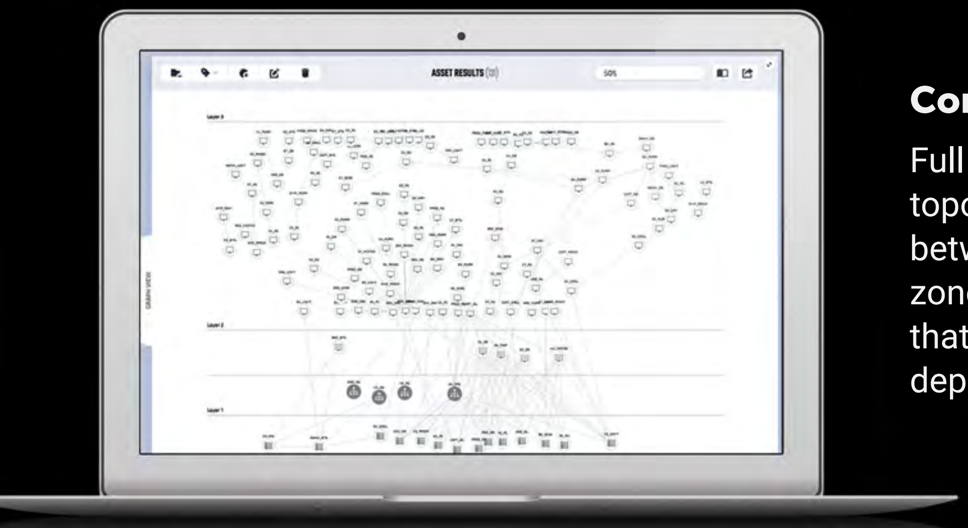
Claroty monitors network communication to establish an operational baseline so that it can better pinpoint anomalous behavior.

Generating Actionable Insights

Claroty applies native OT analytics and produces detailed alerts, complete with actionable insights for improved cyber security and operational resilience.

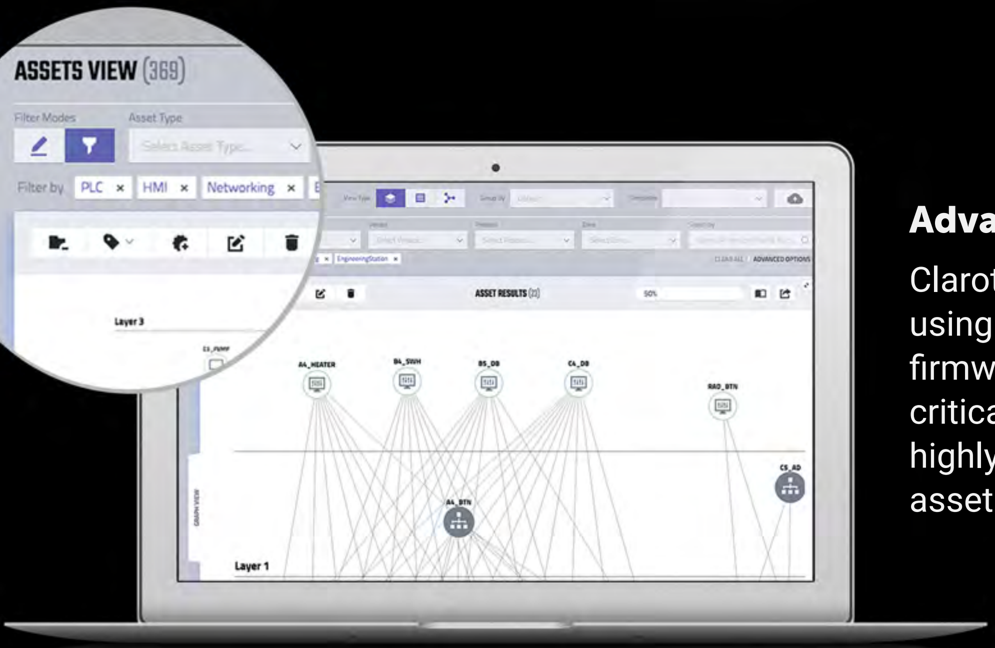
Claroty
See | Know | Secure

Claroty is able to safely see the widest array of OT systems and dive deeper into the communications protocols than any other vendor in the market. The platform not only gathers a large amount of data on individual control system assets such as PLCs, engineering stations and HMIs, but also inspects and interprets all the communications between assets.



Complete Network View

Full representation of the network topology, revealing all connections between assets, across all different zones and levels. It is the only product that unveils hidden interfaces and dependencies between OT and IT assets.



Advanced View Filters

Claroty lets you create any custom view using a set of filters, including: protocol, firmware version, name, asset type, criticality, risk level, more. This enables highly targeted investigation of distinct asset groups within the network.

All The Data Needed About Your Environment

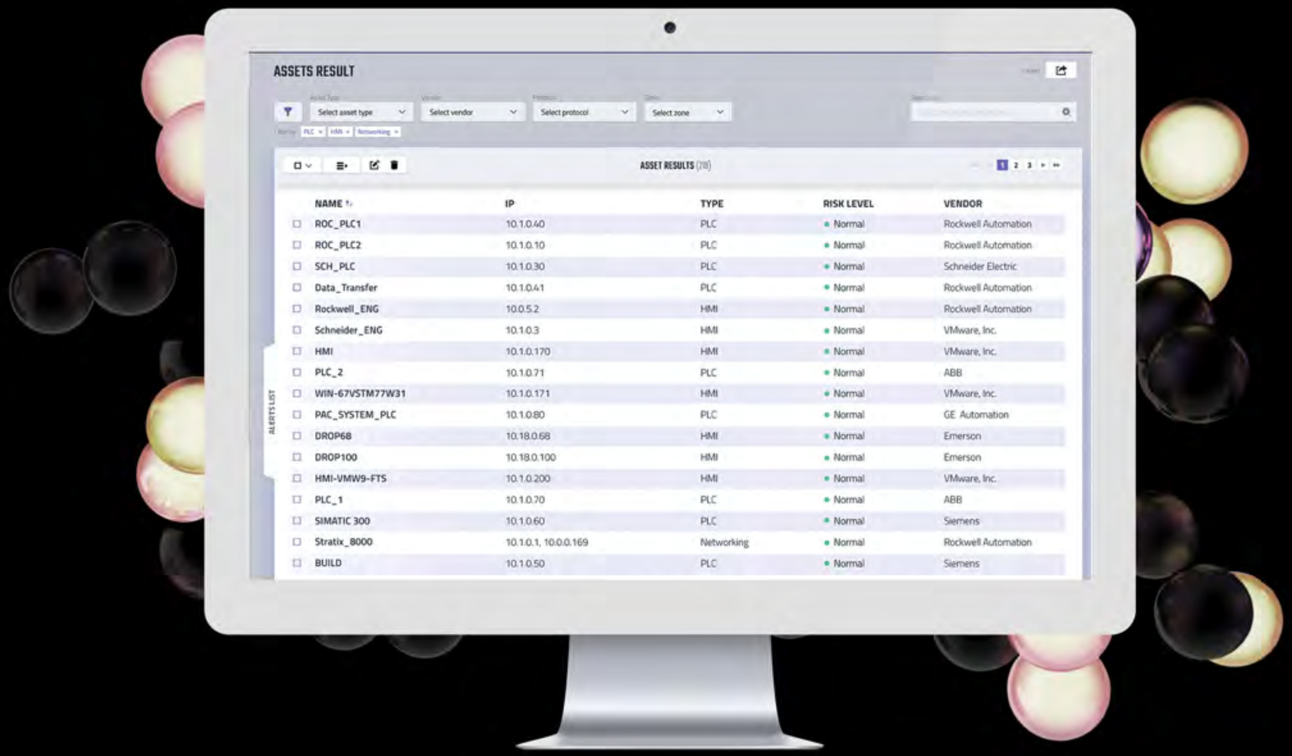
Claroty provides detailed asset and communications information presented in various dashboards and tables.

Asset Unique Descriptors:

- IP Address
- MAC Address
- Equipment vendor
- Equipment type (PLC, HMI, Engineering
- Workstation, Switch, etc.)
- Asset model number
- Asset serial number
- Firmware version running on the asset
- Physical data (rack slots)
- And more

Asset Communications:

- Asset connections within the ecosystem
- Open and proprietary protocols the asset utilizes (CIP, S7,S7+,Ovation,Modbus, Vnet/IP, etc.)
- Commands the asset sends and receives:
  - Data Acquisition
  - Programming
  - Operation
  - Diagnosis
  - Alarm & Events
  - Authentication
  - And more



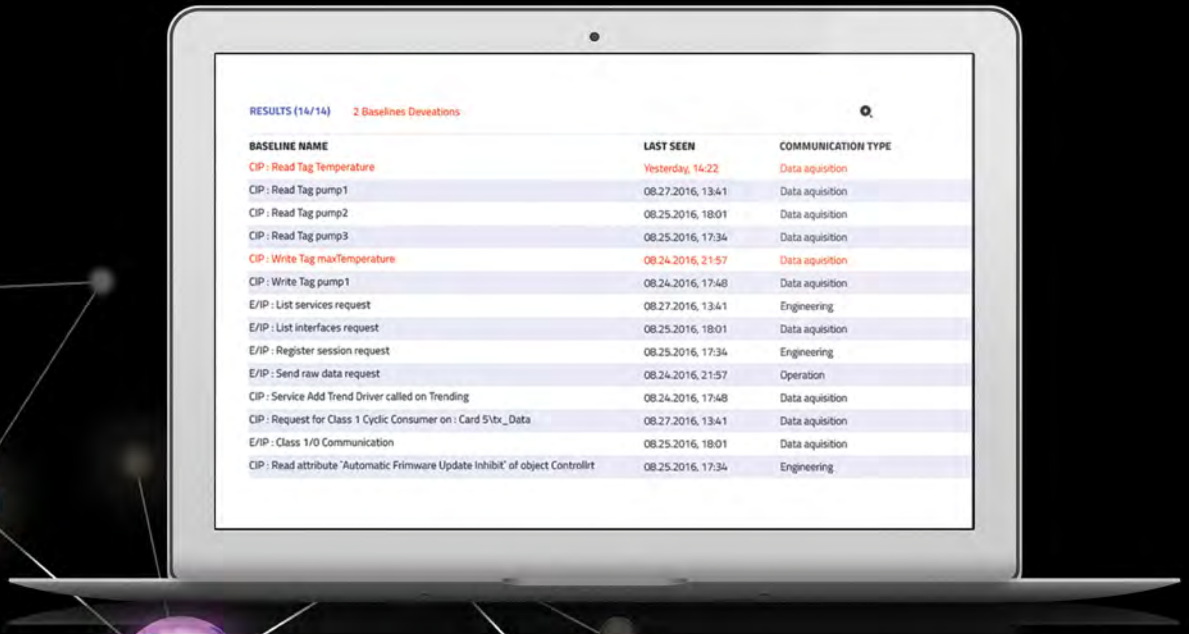
NAME	IP	TYPE	RISK LEVEL	VENDOR
ROC_PLC1	10.1.0.40	PLC	● Normal	Rockwell Automation
ROC_PLC2	10.1.0.10	PLC	● Normal	Rockwell Automation
SCH_PLC	10.1.0.30	PLC	● Normal	Schneider Electric
Data_Transfer	10.1.0.41	PLC	● Normal	Rockwell Automation
Rockwell_ENG	10.0.5.2	HMI	● Normal	Rockwell Automation
Schneider_ENG	10.1.0.3	HMI	● Normal	VMware, Inc.
HMI	10.1.0.170	HMI	● Normal	VMware, Inc.
PLC_2	10.1.0.71	PLC	● Normal	ABB
WIN-67VSTM77W31	10.1.0.171	HMI	● Normal	VMware, Inc.
PAC_SYSTEM_PLC	10.1.0.80	PLC	● Normal	GE Automation
DROP68	10.18.0.68	HMI	● Normal	Emerson
DROP100	10.18.0.100	HMI	● Normal	Emerson
HMI-VMW9-FTS	10.1.0.200	HMI	● Normal	VMware, Inc.
PLC_1	10.1.0.70	PLC	● Normal	ABB
SIMATIC 300	10.1.0.60	PLC	● Normal	Siemens
Stratix_8000	10.1.0.1, 10.0.0.169	Networking	● Normal	Rockwell Automation
BUILD	10.1.0.50	PLC	● Normal	Siemens

Claroty
See | Know | Secure

Extreme visibility enables the construction of fine-grained behavioral models of your OT networks. The advanced models and algorithms provide security and engineering teams with deeper insights, superior anomaly detection, and more detailed and actionable alerts.

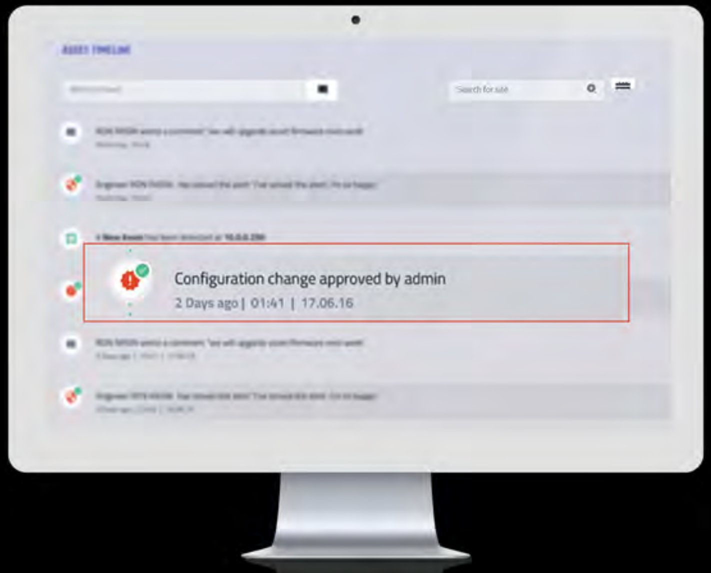
Baseline Deviations

The platform automatically discovers the assets across your OT networks and observes network traffic to learn, for each asset in the network, the finite set of connections, conversations, and commands that represent the legitimate behavior–the system baseline. Advanced algorithms are applied to the baseline to detect anomalies that may indicate an attack or another problem.



RESULTS (14/14) 2 Baselines Deveations

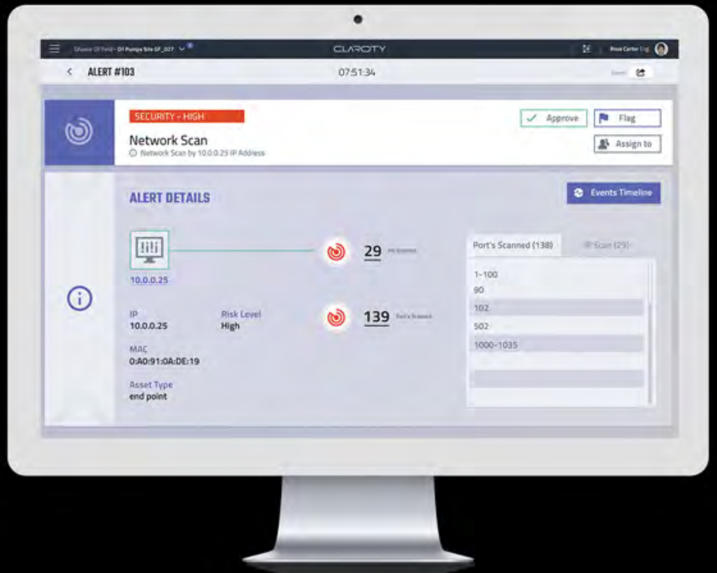
BASELINE NAME	LAST SEEN	COMMUNICATION TYPE
CIP : Read Tag Temperature	Yesterday, 14:22	Data aquisition
CIP : Read Tag pump1	08.27.2016, 13:41	Data aquisition
CIP : Read Tag pump2	08.25.2016, 18:01	Data aquisition
CIP : Read Tag pump3	08.25.2016, 17:34	Data aquisition
CIP : Write Tag maxTemperature	08.24.2016, 21:57	Data aquisition
CIP : Write Tag pump1	08.24.2016, 17:48	Data aquisition
E/IP : List services request	08.27.2016, 13:41	Engineering
E/IP : List interfaces request	08.25.2016, 18:01	Data aquisition
E/IP : Register session request	08.25.2016, 17:34	Engineering
E/IP : Send raw data request	08.24.2016, 21:57	Operation
CIP : Service Add Trend Driver called on Trending	08.24.2016, 17:48	Data aquisition
CIP : Request for Class 1 Cyclic Consumer on : Card 5\tx_Data	08.27.2016, 13:41	Data aquisition
E/IP : Class 1/0 Communication	08.25.2016, 18:01	Data aquisition
CIP : Read attribute 'Automatic Frimware Update Inhibit' of object Controllrt	08.25.2016, 17:34	Engineering



Configuration change approved by admin
2 Days ago | 01:41 | 17.06.16

Critical Changes

The Critical Changes model monitors normal but high risk changes to your OT environment. The model is combined with real-time monitoring across the OT network which reconstructs network traffic and knows which systems and commands are initiating potentially risky changes to critical assets such as PLCs. The system alerts operators and security teams about changes that could damage system integrality and adversely impact operational process.



ALERT #103 07:51:34

SECURITY - HIGH

Network Scan

Network Scan by 10.0.0.25 IP Address

ALERT DETAILS

10.0.0.25

IP
10.0.0.25

Risk Level
High

MAC
0:A0:91:0A:DE:19

Asset Type
end point

29

139

1-100
90
102
502
1000-1035

Malicious Activity

This deterministic and behavioral model catalogues activity that should not take place within OT networks and generates alerts when this potentially malicious activity takes place. The model incorporates known attacker techniques and attack vectors.

Claroty
See | Know | Secure

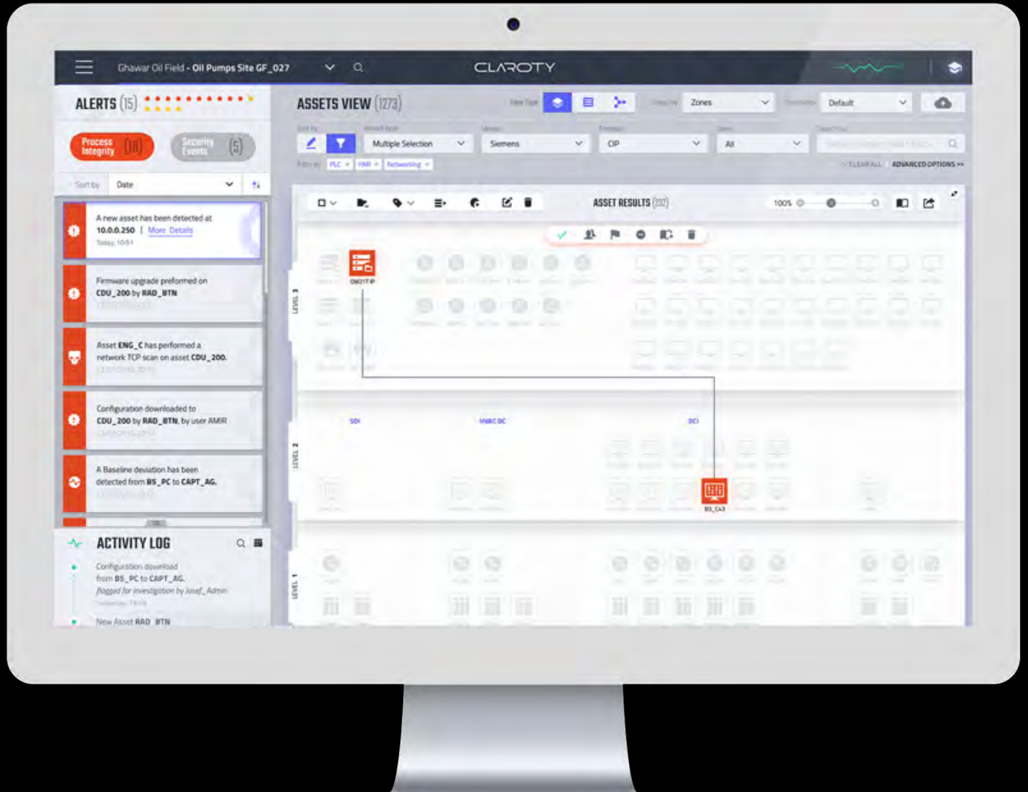
With extreme visibility Claroty provides deeper insights into your environment–enabling you to proactively identify and fix configuration issues that can leave your network vulnerable to attack and to highlight other operational issues. This level of visibility, combined with Claroty's knowledge of OT networks provides you with streamlined and much more contextually rich alerts–enabling you to quickly understand and respond to security threats and other issues that can affect process integrity.

OT Insights

OT networks often feature unmonitored blind spots. These blind spots often conceal misconfigurations, and hide potentially insecure connections that are not routinely investigated or addressed by either OT or IT teams. Claroty provides clear visibility into the topology of your network. This enables you to spot unnecessary dependencies between critical systems and pinpoint other network configuration issues to enhance network design, reduce risk, and improve process integrity and efficiency.

Context Rich Alerting

Unlike other systems that generate a large number of low level alerts, Claroty summarizes multiple associated events into a single robust alert that tells the whole story. The result is less noise and the context necessary to quickly investigate and respond to the real security and integrity issues that could harm your process.



A new asset has been detected at 10.0.0.250 | More Details

Firmware upgrade preformed on CDU_200 by RAD_BTN

Asset ENG_C has performed a network TCP scan on asset CDU_200.

Configuration downloaded to CDU_200 by RAD_BTN, by user AMIR

A Baseline deviation has been detected from BS_PC to CAPT_AG.

Configuration download from BS_PC to CAPT_AG. *flagged for investigation by Josef_Admin*

New Asset RAD_BTN

Multisite Management

Larger customers typically operate multiple sites, and require cross-site visibility and management, enabling the tracking of attack trends and operational patterns across their entire ecosystem. Claroty Enterprise Manager provides a unified view and configuration dashboard, delivering full visibility across all monitored sites.

Integration

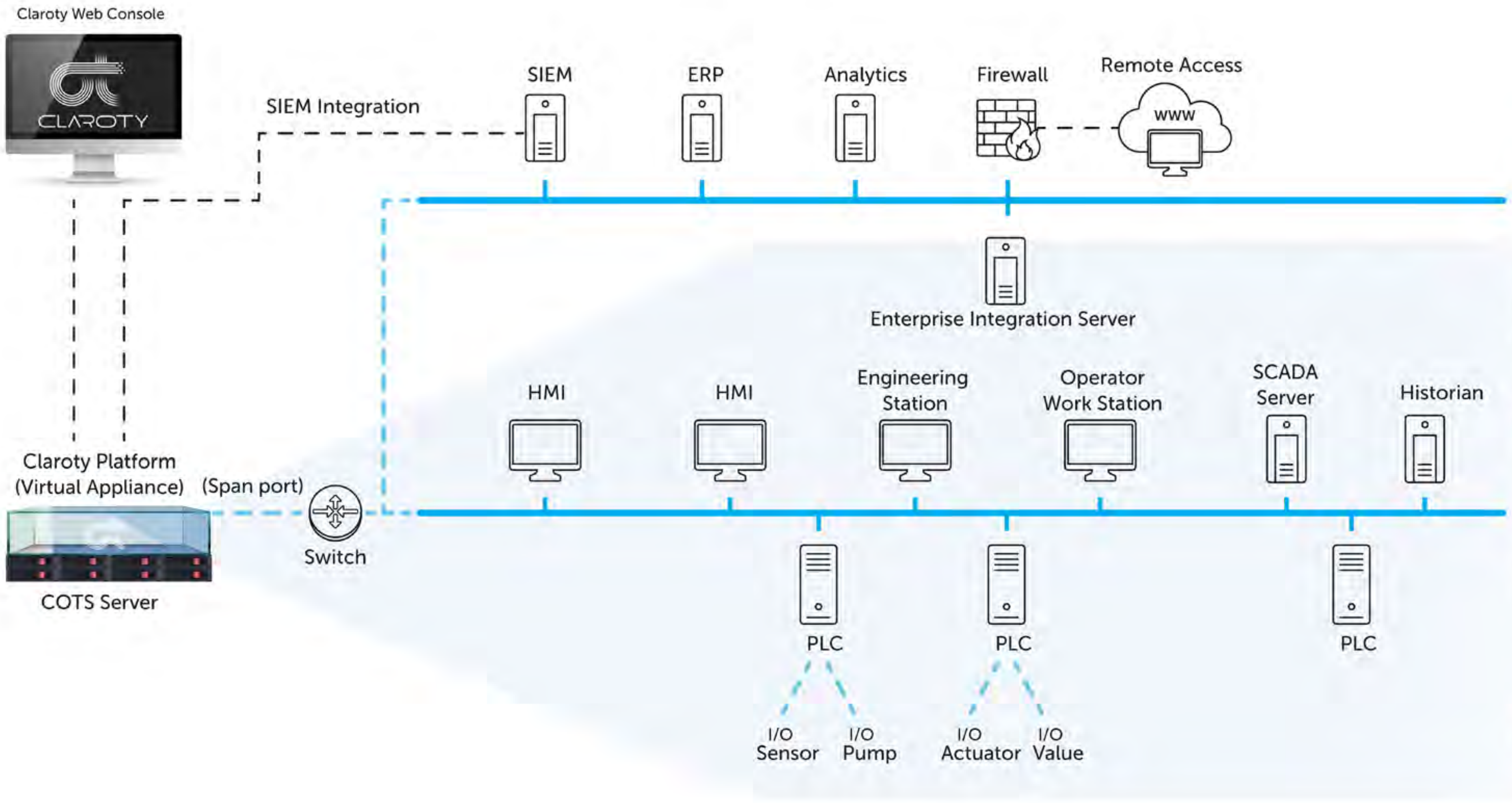
Claroty exports alert data via Syslog into leading SIEM products (e.g., Arcsight, Splunk, QRadar, etc.). SOC analysts can utilize existing analytic tools to filter and correlate alert data–complementing their existing IT security knowledge with data and insights into OT security. This integration makes Claroty the ideal solution for any SOC manager that wishes to add complete visibility into OT environments.

Sampling of Security and Process Integrity Alerts:

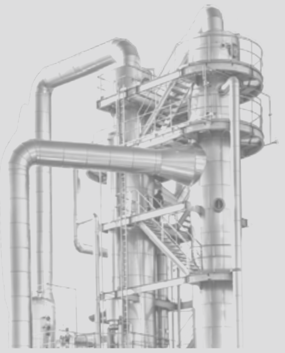
- New Asset - new asset appears in the network
  Communication Down - malfunction of communication vector within an asset
- Scanning Attacks - asset scans open ports of multiple other assets
- Man in the Middle Attacks - attacker transparently intercepts and alters communication between two assets
- Network Storm - extreme volume of broadcast traffic
- Configuration Download - engineering station downloads new configuration to PLC
- Configuration Upload - engineering station uploads current configuration from PLC
- Mode Change - PLC mode transition (Program, Run, Monitor etc.)
- Firmware Upgrade - change in PLC firmware

Claroty In-Depth

The Claroty Platform is deployed as virtual appliance and connects to SPAN ports on Ethernet networks, or to customized sensors on serial networks. The appliance dissects the relayed traffic, extracting a comprehensive set of data for each system asset and how that asset is communicating in the network. The web-based console provides a multifaceted view into the data.



Level 4 (IT Network)	▪ Classic attack : MITM, Scanning Attacks (Port, Network) ▪ Non-responsive assets ▪ Unauthorized cross level\ zone communication	▪ Connection to Internet\ corporate network DMZ ▪ IP conflict ▪ New asset in the network
Level 3 (Manufacturing Operations)	▪ Weak password (FTP / TFPTP / RDP / DCERPC) ▪ Unencrypted communication (Telnet) ▪ Insecure Internet connection	▪ Traffic activity summary Bad configuration (NTP / DNS / DHCP/ etc.) ▪ Bad network topology ▪ Asset used ports
Level 2 (Supervisory)	▪ Firmware download ▪ Configuration Download ▪ Logic change ▪ Corrupted OT packet ▪ Online edit to PLC projects	▪ Anomalous protocol behavior ▪ Communication Changes (Down/Overload, etc.)
Level 1 (Process Control)	▪ PLC actions : Start, Stop, Monitor, Run, Reboot, Program, Test ▪ Authentication to the PLC	
Level 0 (Field Devices)	▪ Fieldbus I/O visibility	



Technical Specifications

Supported Protocols*

IP Networks Protocols	Industrial Networks Protocols	Supported ICS Vendors
TCP/IP SNMP SSH HTTP / HTTPS Telnet FTP SMB / CIFS DNS ICMP IGMP Browser FTP SMB2 CDP LLDP DCE/RPC DHCP V4/V6 ARP VNC TFTP NTP RDP SSL NTLMSSP ATSVC SMB-PIPE	Modbus (including Schneider extension) Siemens S7/S7-Plus Siemens P2 EtherNet/IP + CIP (including Rockwell extension) PCCC/CPSv4 GE SRTP VNet/IP Emerson Ovation DCS protocols Emerson DeltaV DCS protocols Melsec/Melsoft FTE ABB 800xA DCS protocols MMS (including ABB extension) Sattbus OPC DA/AE/UA IEC104 DNP3 Profinet-DCP Bacnet	Siemens Allen Bradley (Rockwell) Schneider Emerson GE ABB Yokogawa Mitsubishi Honeywell

* The table reflects many of the the most commonly used protocols. Claroty will add support for additional protocols in accordance with customers' needs. Please contact us to learn more.

Software Hardware Requirements

Virtual Environment	Physical Appliance	Client Browser
Virtual environment that will support a Linux RedHat/Centos 7 image. Virtual environment must have a dedicated physical Ethernet Port that will be utilized to monitor the SPAN port traffic.	The hardware chosen must support Linux RedHat/Centos 7. Must have a dedicated physical Ethernet Port that will be utilized to monitor the SPAN port traffic within the appliance and management port.	To access the Site and Central Appliance, the portal has been optimized for use with the Google Chrome browser minimum installed version: 16.0.912

CLAROTY
Clarity for OT Networks

Industrial Networks Secured

Our Mission

Claroty was conceived to secure and optimize OT networks that run the world's most critical infrastructures.

Claroty empowers the people who run and protect industrial systems to make the most of their OT networks. By discovering the most granular elements, extracting the critical data, and formulating actionable insights, Claroty provides extreme visibility and brings unparalleled clarity to OT networks.

Your Result

Better security, efficiency and integrity for your critical OT environments.

www.claroty.com