Integration Brief

CLAROTY CONTINUOUS THREAT DETECTION & CHECK POINT NEXT-GENERATION FIREWALL

Integrated End-To-End Security

The integrated Check Point and Claroty solution adds ICS intrusion detection and passive OT monitoring to the comprehensive Check Point security suite. Standard Check Point Security network infrastructure such as the 1200R and 5200 Rugged Security Appliances secure perimeters, the IT to OT connection and zones within industrial networks.

Claroty's Continuous Threat Detection (CTD) connects to SPAN or mirror ports on a standard Check Point Security Gateways or Check Point Rugged Security Appliances and automatically identifies industrial assets and network activity to provide real- time cybersecurity monitoring and process integrity alerts. Aggregated alerts are communicated directly into the Check Point Smart Management Console.

With unified reporting, organizations can detect any threat to the application, process or network, providing granular visibility of SCADA traffic and facilitating attack forensics. Integrated network and endpoint threat forensics reveal the entire sequence of an attack event – providing a complete view across the enterprise and control networks.

Business Drivers

While enterprises have made great strides in protecting their IT business networks, industrial control system (ICS) networks remain at risk. Commissioned decades ago, without cybersecurity in mind and sometimes running outdated software, many of these networks and underlying assets are being increasingly targeted with sophisticated cyberattacks. In fact, a number of documented attacks such as Industroyer CrashOverride, WannaCry, BlackEnergy and STUXNET have created significant operational damage, disrupting both environmental and human safety alike.

Until now, gaining comprehensive, real-time visibility into of ICS networks, underlying protocols, and processspecific devices has been extremely challenging and has left industrial enterprises largely blind to potential security risks. Without contextual insight, industrial operations were unable to safely protect the control network from cyberattacks and avoid production disruptions.

Integration Specs

Requirements

Claroty CTD v4.1+ | Check Point NGFW

Highlights

- Extreme Visibility of industrial control system networks allows critical infrastructure organizations to assess, monitor and mitigate potential threats
- Improved Threat Hunting via real-time contextual alerting and immediate implications on process integrity and cyber resiliency
- Zero Impact on Industrial Control Networks operating in a non-intrusive manner, does not require the installation of endpoint agents, and with no downtime or disruption to industrial networks

About Claroty CTD

Claroty CTD provides full visibility and security controls for OT environments. Powered by Claroty's proprietary DPI technology, CTD extracts precise details about each asset on the OT network, profiles all communications and protocols, generates a behavioral baseline that characterizes legitimate traffic, and alerts you in real-time to anomalies, exact-match vulnerabilities, and known and zero-day threats

About Check Point NGFW

Check Point gateways provide superior security beyond any Next Generation Firewall (NGFW). Best designed for Sandblast Network's protection, these gateways are the best at preventing the fifth generation of cyber attacks with more than 60 innovative security services. Based on the Infinity Architecture, the new Quantum Security Gateway™ line up of 15 models can deliver up to 1.5 Tbps of threat prevention performance and can scale on demand.

Architecture Components

The Claroty Platform is a fully-integrated solution which plugs into the operational network without the use of agents. It is purpose-built to provide realtime situational awareness and deep visibility for ICS networks. The tiered deployment model supports monitoring of multi-switch environments and numerous network topologies. The solution is quick and easy to deploy, has zero impact on the network and does not affect the integrity industrial processes. Claroty leverages the following elements as part of the installation:

- **Continuous Threat Detection (CTD)** Server is a physical or virtual server that provides real-time cybersecurity and operational visibility of industrial control networks within distributed network environments and architectures.
- **Continuous Threat Detection (CTD) Sensor Lightweight** devices that operate as remote extensions of the CTD Server. Used in sites with limited physical reach or across multiple remote isolated sites with limited out-of-band aggregation capabilities.
- **Secure Remote Access (SRA)** Minimize the risks remote users, including employees and 3rd parties, introduce to OT networks using a fully manageable interface that all external users connect through, to perform software upgrades, periodic maintenance, and other support activities on assets within industrial control system networks.
- **Enterprise Management Console (EMC)** Provides asingle pane of glass aggregating and consolidating data from various Claroty products. The centralized management interface displays a unified view of assets, activities and alerts making it highly suitable for enterprise-wide Security Operations Centers (SOC).

Sample Deployment Architecture

The figure below shows the integration of Check Point's firewall and Claroty's solutions in a converged IT and OT environments, based on the Purdue model layer architecture. In this scenario, Claroty's Continuous Threat Detection analyzes I/O level traffic while the Check Point firewalls are placed in strategic detection and prevention point allowing to block or limit communications for a single node or between nodes to effectively prevent disruption of critical operations.

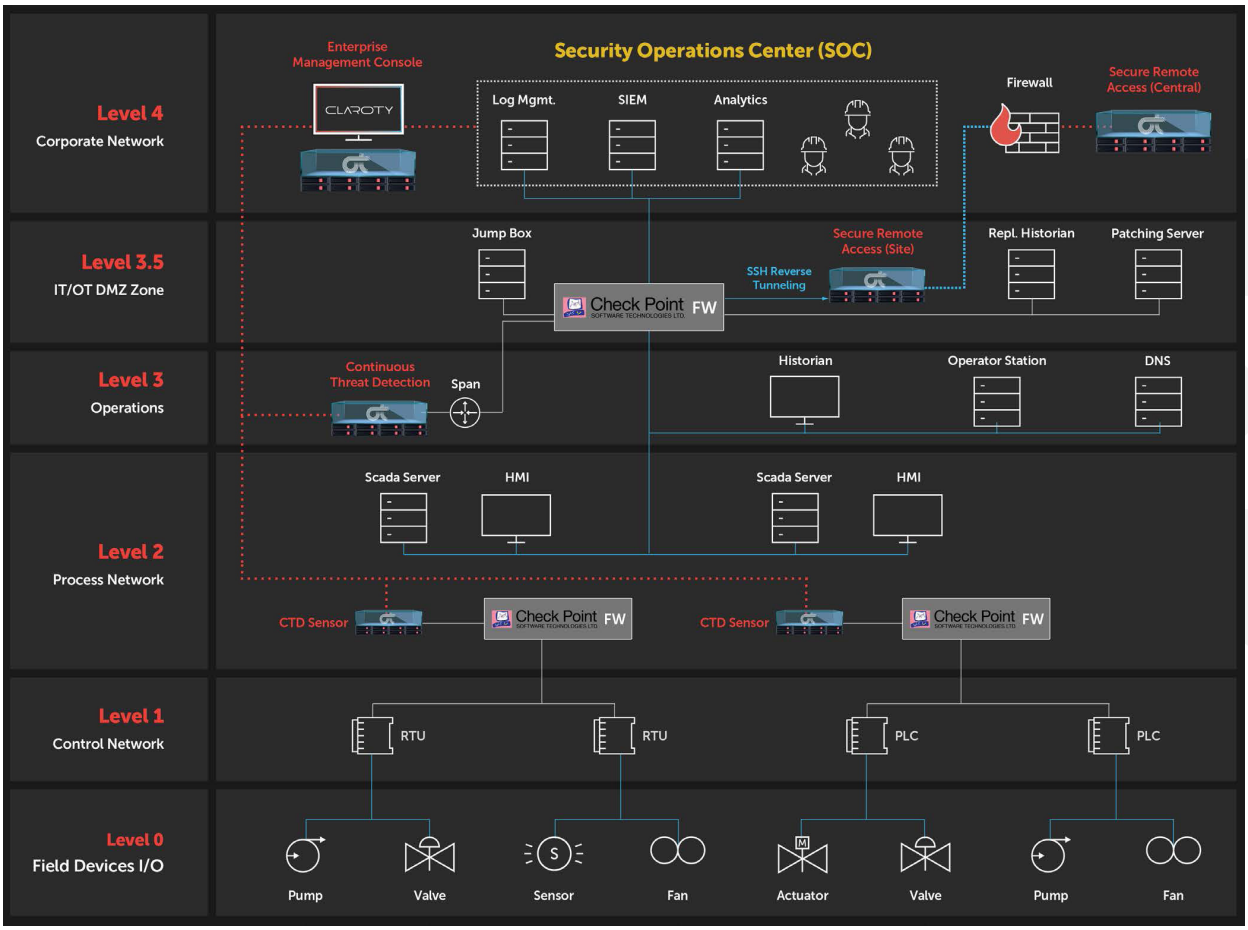

Figure 1 - CTD provies OT asset details to Check Point's Firewall

Real-Time Cybersecurity and Visibility

The Claroty solution is available in multiple form factors supporting a wide range of industrial control systems, protocols[1] and easily integrates with existing IT/OT applications. It solves an important part of the ICS security problem providing comprehensive, real- time cybersecurity and visibility for industrial control networks. All achieved with zero impact to the process and underlying assets. Below are some unique capabilities as integrated into the Check Point Management Console:

- Provides extreme visibility into ICS Networks
- Identifies security gaps - including known vulnerabilities and network hygiene issues
- Detects security posture changes
- Continuously monitors for known and unknown threats
- Enables proactive threat hunting

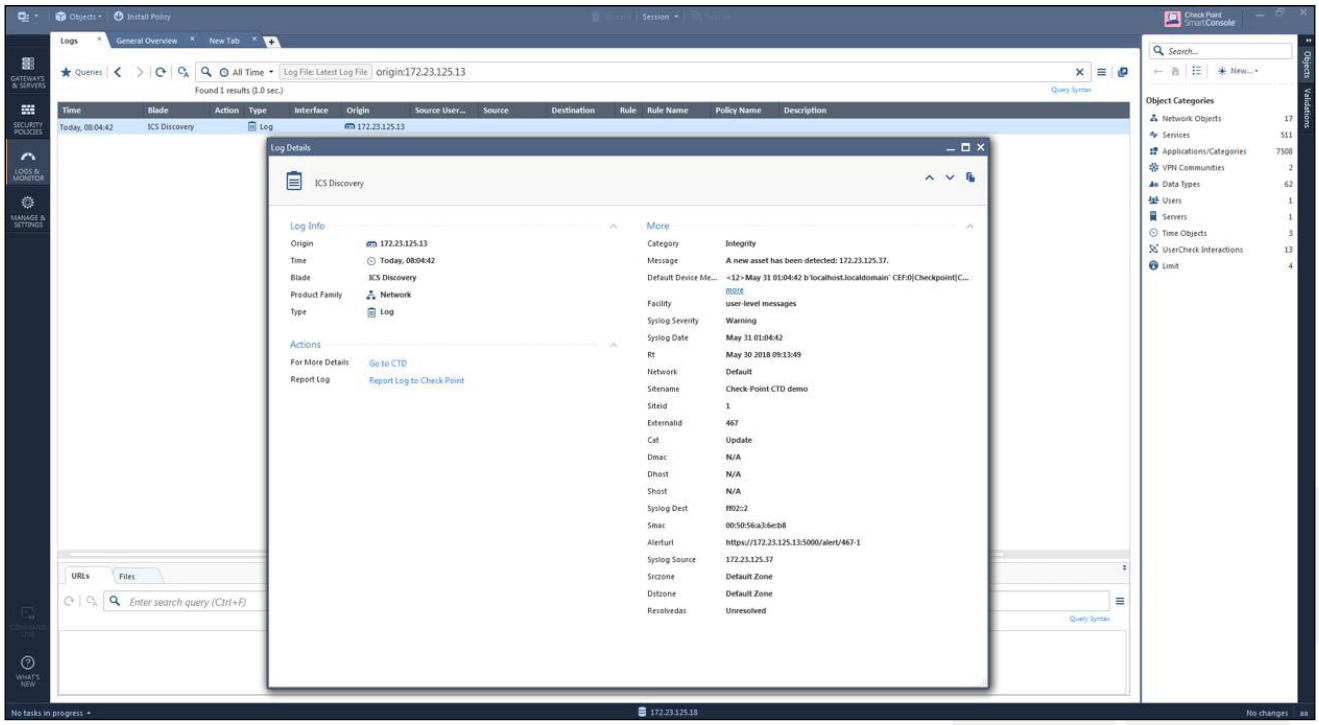

Figure 2 - CTD alerts shown within the Check Point Smart Management Console

[1] The list shows many of the most commonly used protocols, to see the full list of protocols supported by The Claroty Platform visit www.claroty.com. Claroty will add support for additional protocols in accordance with customer needs. Contact us to learn more.

Common Use Cases

Unified View Across IT-OT: Check Point firewalls are placed in strategic detection and prevention points whereas Claroty's solution automatically identifies and classifies assets across the ICS network. Together, the solutions provide a consolidated view of the assets across IT and OT environments. It continuously updates asset inventory ensuring accurate, up-to-date device properties, classification, configuration and network context in a single-source-of-truth repository. Additionally, it allows to proactively block or limit communications for a single node or between nodes to effectively prevent disruption of critical operations.

Real-Time OT Threat Detection: Claroty helps administrators identify and remediate issues that can impact security and operations, such as software vulnerabilities, network misconfigurations, clear-text passwords, unsecured connections, and many more. By generating and sharing context-rich actionable alerts with the Check Point firewall – SOC and Security teams have immediate situational awareness and the details required to rapidly investigate issues and collaborate with "shop floor" teams to resolve problems

The Need for Network Segmentation: The need to proactively segment between the IT and OT networks as well as within the OT network environment (aka micro segmentation, zones, etc.) to prevent accidental spillover from the Enterprise IT to the OT network.

The tight Integration between Claroty's Continuous Threat Detection and Check Points' solutions leverages existing network infrastructure to achieve the following:

- Automated network segmentation policy creation – leveraging existing network infrastructure, organizations can proactively generate micro-segmentation policies for OT-specific network assets
- Automate Virtual Segmentation – organizations looking to segment lower levels of Purdue model where proactive blocking is prohibited can leverage Claroty's automated virtual zones creation engine. In this scenario, any cross-zone communication violation immediately raises an alert.
- Stopping Attacks in Real-Time –leverage existing network infrastructure, organizations can proactively mitigate active attacks. In this scenario, an alert coming from Claroty's Continuous Threat Detection (CTD) results in an automatically quarantined/isolated rogue device.

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