Powerful IoT-OT Security Without The Complexity

Data Sheet | **Continuous Threat Detection**

Overview

Continuous Threat Detection (CTD) is the world's most trusted and proven IoT and OT security and monitoring solution. Its award-winning DPI technology, combined with industry-leading protocol support, enables industrial enterprises to enjoy the substantial benefits of networked-control systems without compromising operational resiliency, uptime, and security.

More Coverage

Gain deep and broad visibility across IoT and OT networks

Faster Deployment

Deploy across complex enterprises in under 60 days

Less Noise

Eliminate distracting and time-consuming noise from excess alerts

Key Benefits

Full-Spectrum Cybersecurity Monitoring

CTD provides comprehensive visibility, continuous threat and vulnerability monitoring, and deep insights into ICS networks – in a single solution. CTD continuously monitors all network communications and policy violations that threaten the reliability of your systems, providing the information you need to respond quickly. With Multispectral Data Acquisition, leveraging passive monitoring, active querying, and application database (App DB) parsing, in conjunction with five distinct award-winning behavioral-based anomaly detection engines – you can choose the discovery approach best suited to your organization.

Real-time Visibility And Cybersecurity Leveraging:

- Comprehensive Asset Management
- Continuous Threat and Anomaly Detection
- Real-time Vulnerability Management

Maximize Alert Confidence

CTD's industry-first AI for OT and IoT security proactively minimizes signal-to-noise ratio while reducing troubleshooting and investigation time and effort across various organizational roles and disciplines. Leveraging Claroty's Threat Intelligence (CTI), a highly curated, multi-source, and tailored feed, incident responders and threat hunters can further enrich Root Cause Analytics (RCA) efforts with proprietary research and analysis of OT zero-day vulnerabilities and ICS-specific indicators of compromise (IoC) linked to adversary tactics, techniques, and procedures (TTP).

With an unrivaled record of cumulative intelligence and OT experience, CTD arms your teams with actionable context surrounding associated risks to confidently and proactively respond to threats early in the attack kill chain.

Effective IR and Threat Hunting Efforts Leveraging:

- AI-powered Noise Elimination
- Prioritized Risk-based Indicators
- Optimized Signal-to-Noise Ratio

Simplified At-scale Deployment and Integration

CTD's scalable architecture is fully tuned to support multiple use cases and technical constraints. With a wide variety of deployment options, a flexible architecture, and out-of-the-box integrations, CTD meets your every need while optimizing your Total Cost of Ownership (TCO). Leveraging a virtual appliance, pre-installed with the Claroty OS, you can efficiently deploy at scale enjoying significant reduction in setup times, maintenance and monitoring efforts. Leveraging investments already made in technology, process development, and training, you can align your IT and OT teams – integrating with a wide range of technologies, from network infrastructure to SOC tools and other IT/OT operational systems including:

- **SIEM Solutions:** Claroty's purpose-built OT security platform, together with 3rd party SIEM solutions, enhances OT security visibility serving as an essential building block for removing silos between IT and OT security teams. Integrations include IBM QRadar, Splunk, ArcSight, LogRhythm, RSA NetWitness, and many more.

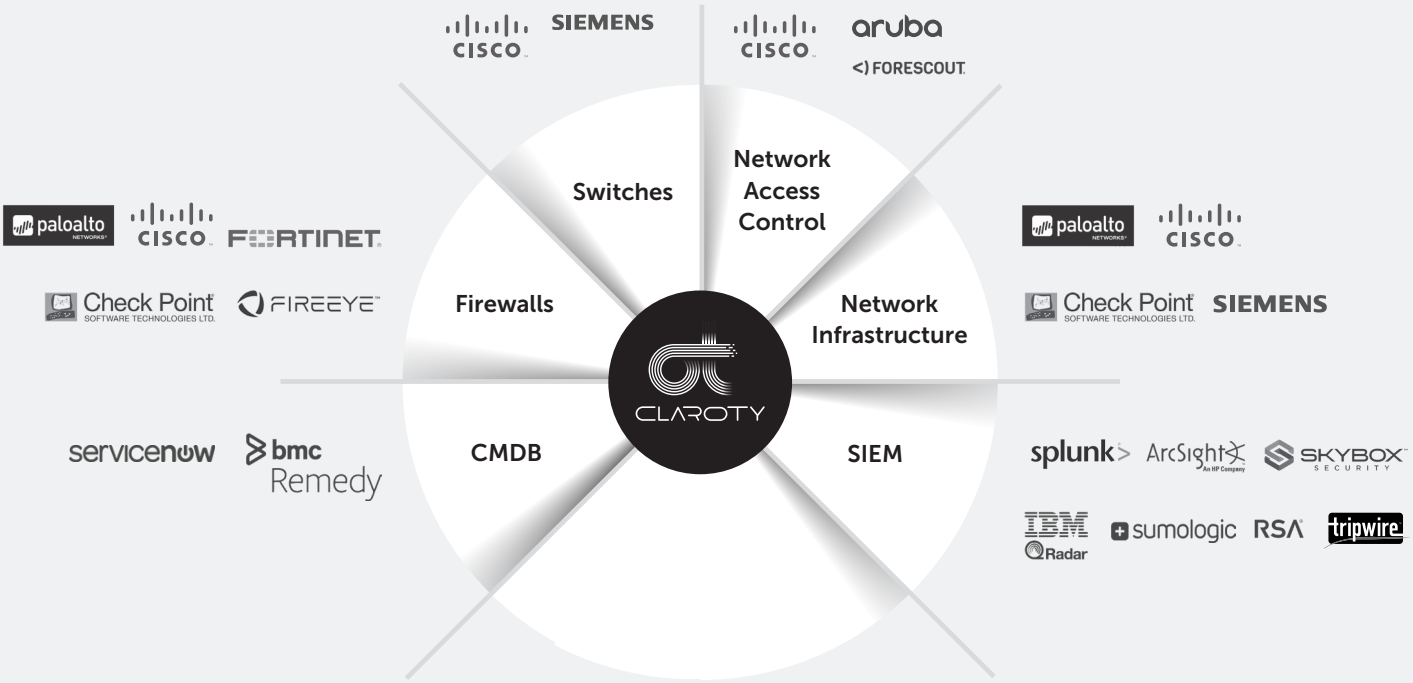
- **CMBD and Ticketing Systems:** Claroty's integration with 3rd party CMDB and ticketing systems delivers streamlined SOC workflows, increasing communication between teams and allowing seamless access to real time OT cybersecurity visibility. Integrations include ServiceNow, BMC Remedy, and many more.

- **Network Access Control (NAC) Systems:** Claroty's integration with Network Access Control systems extends visibility into the lowest levels of OT networks – eliminating silos between IT and OT security teams and delivering a consolidated view across IT/OT. Integrations include Aruba ClearPass, ForeScout CounterACT, Cisco FirePower, and many more.

- **Network Infrastructure:** Claroty's purpose-built OT security platform coupled with 3rd party Network Infrastructure solutions (e.g. firewalls) delivers end-to-end real-time monitoring, threat detection, and unique proactive policy enrichment and real time enforcement. Integrations include Palo Alto Networks, Check Point, Cisco, Fortinet, and many more.

Integrate with Existing SOC/IT Ecosystems Delivering:

- Efficient Deployment at Scale
- Integration with Existing SOC/IT Processes
- Optimize TCO



Another Dimension of OT & IoT Visibility

Claroty delivers comprehensive visibility and understanding into large enterprises with complex IT, OT, and IoT footprints. Leveraging this unique visibility, CTD's Virtual Zones+ tags devices with similar network traffic parameters into logical groups and automatically creates IoT- and OT-specific application firewall-like rules and alerting policies – based on the assets' type and observed communication patterns. Armed with this unique knowledge, you can create and enforce virtual micro-segmentation "zones" and restrict anomalous or non-compliant communications within and across zones.

Improve Your Cyber Resiliency by:

- Accelerating Digital Transformations
- Proactively Enforcing Policies/Rules
- Segmenting OT-IoT Networks

Additional Claroty Products

- Secure Remote Access (SRA) – Minimizes the risks remote users, including employees and third-party vendors, introduce to OT networks.
- Enterprise Management Console (EMC) – Centralized management interface consolidating data from Claroty products across multiple global sites, and displays a unified view of assets, activities and alerts.

About Claroty

Claroty is the industry leader in industrial IoT (IIoT) visibility and security monitoring. Our enterprise-class platform delivers real-time situational awareness of operational technology (OT) networks and detects a wide range of industrial cyber risks, from vulnerabilities to malware and targeted attacks. Fortune 500 companies in fifteen industries trust Claroty to accelerate their digital transformation without sacrificing security or safety. Founded in 2015, Claroty is headquartered in New York City and backed by the world's leading venture and institutional investors.

CLAROTY

Contact Us:

www.claroty.com | contact@claroty.com |