SOLUTION OVERVIEW

HOW CLAROTY SUPPORTS THE U.S. PUBLIC SECTOR

CHALLENGE
Protecting operational technology (OT) environments against cyber threats

SOLUTION
A comprehensive platform purpose-built to protect all cyber-physical systems in OT environments

Claroty Capabilities

- **Asset Discovery:** Claroty discovers and profiles all cyber-physical systems across OT, IoT, IIoT, IoMT, & BAS/BMS assets. This information is centralized in a real-time inventory that includes all key attributes per asset.

- **Change Management:** Claroty monitors all cyber physical systems (CPS) assets for changes and connects to CMMS, CMDB, and backup tools to support records integrity and inform preventative maintenance.

- **Vulnerability & Risk Management:** Claroty correlates all discovered assets against the industry's top database of CVEs. It then assesses the risk posed by each vulnerability and offers recommendations for optimizing prioritization and mitigation.

- **Network Segmentation:** Using its real-time network visibility, Claroty defines granular policies that can be easily enforced via existing network infrastructure to jumpstart or strengthen segmentation in accordance with a Zero Trust architecture.

- **Secure Remote Access:** Claroty further hardens the CPS environment with added Zero Trust controls via frictionless yet secure remote access for both internal and 3rd-party users.

- **Threat Detection:** Claroty continuously monitors the CPS environment for known and emerging threats, contextualizes alerts to optimize response, and integrates with SIEM, SOAR, EDR, and other tools for unified IT/OT SOC governance.

- **Endpoint Protection:** Claroty supports robust endpoint rotection by integrating seamlessly with industry leading EDR solutions including CrowdStrike, Tanium, Microsoft, and more.

Company Background

- Founded in 2015 with a mission to secure critical infrastructure.

- Headquartered in NYC with Public Sector offices in Leesburg, VA..

- Supported by $635M in financing, making Claroty the best-funded, most financially stable company in the industry.

- Backed by Industry OT Leaders: The 3 global leaders in industrial automation — Rockwell Automation, Schneider Electric, and Siemens — trust and back Claroty as not only investors but also as customers and partners, working with Team82 to enhance the security of their products.

- Deeply Engaged with the Public Sector: The former head of the NSA, leader of CISA's COVID-19 task force, and founders of the OT cyber coalition are among Claroty's many team members driving private-public sector collaboration.

- Award-Winning: Claroty's 75+ accolades from top-tier, global organizations are a clear testament to the unmatched strength of the company's team, portfolio, roadmap, and mission.

Collection, Deployment & Protocol Support

- **Five Collection Methods:** Claroty offers five flexible collection methods for OT asset discovery that can be easily combined to suit each customer's unique needs. These include:

  1. **'Passive Monitoring'** uses SPAN/TAP port mirroring to copy the traffic sent between assets before extracting their key details via deep packet inspection technology.

  2. **'Safe Queries'** sends non-disruptive, native communications to segments of the environment to reveal the assets present.

  3. **'Project File Analysis'** parses the configuration files that are typically backed up on workstations and include details on PLCs, RTUs, and most/all other assets in the environment.

  4. **'Claroty Edge'** delivers unmatched visibility into all assets in any CPS environment in just minutes without requiring any additional hardware, configuration, or network footprint.

  5. **'Ecosystem Enrichment'** supports asset discovery by harnessing Claroty's 70+ ready-made integrations with CMDB, CMMS, EDR, backup and recovery, asset management, firewall, and dozens of other tools.

- **Coverage of 450+ Protocols:** As the industry leader in protocol coverage, Claroty currently supports over 450 OT & automation protocols.

- **Flexible & Scalable Deployment Options:** Claroty's modular portfolio deploys rapidly and easily on VMs or physical appliances with various on-premise, SaaS, and hybrid options.

Value to the U.S. Public Sector

- **Gain Full Visibility, Your Way:** Claroty is the only vendor to offer 5 distinct collection methods with support for 450+ protocols, helping eliminate unknown devices on your network.

- **Support ZTA Initiatives:** With Claroty's Secure Remote Access (SRA) and ready-made integrations with 70+ security and operational tools, Claroty enables Zero Trust Architecture (ZTA). This includes a seamless extension and unification of tech stacks, workflows, and governance with an Integrated Ecosystem.

- **Harness Renowned Research:** Claroty's world-class research team, Team82, have disclosed a record-breaking 420+ vulnerabilities, driving industry-wide progress while enhancing an organization's protection against threats that matter most.

- **Drive ROI through Cyber & Operational Resilience:** Claroty scales to support all use cases on the full CPS security journey — regardless of maturity level and prioritization of workflows. These characteristics reduce the CapEx and OpEx often associated with the learning curves, requirements, and rigidity of new security initiatives.

About Claroty

Claroty empowers organizations to secure automation, control, and other cyber-physical systems across industrial, healthcare, commercial, and public sector environments: i.e. the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the leading investment firms and industrial automation vendors, Claroty is deployed at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.