SOLUTION OVERVIEW

Claroty Edge

Delivering A Comprehensive Asset Inventory in Minutes

The CPS Visibility Challenge

Building a comprehensive cyber-physical systems (CPS) security program starts with creating a foundation of in-depth asset visibility with a complete inventory of all OT, IoT, and BAS assets across an organization's entire CPS environment. However, gaining this caliber of visibility can be challenging for many reasons, including:

- Standard IT solutions are typically incompatible with and unsafe for CPS networks.
- Traditional asset inventory solutions often require hardware that can be costly, complex, and time-consuming to deploy.
- Many CPS environments are geographically isolated and/or airgapped, making them difficult to access in order to install hardware.
- Traditional asset inventory methods such as passive data collection may not be compatible or otherwise suitable for all networks and use cases under all circumstances.

The Solution

Claroty Edge is a highly flexible, Windows- and Linux-compatible edge data collector that delivers complete visibility into cyber-physical system (CPS) networks within minutes—without requiring network changes, sensors, or a physical footprint at lower network levels. It operates as a one-time, agentless executable but also supports periodic, scheduled runs for ongoing visibility. Deployable in both on-premises and SaaS-based environments, Claroty Edge is an ideal solution for organizations seeking rapid, non-disruptive asset discovery across a wide range of industrial, healthcare, public sector, and commercial settings.

Claroty Edge Benefits At a Glance

Complete Visibility: Claroty Edge provides a comprehensive inventory of your managed and unmanaged CPS assets and all risks and vulnerabilities affecting them.

Zero Changes & No Hardware: Claroty Edge safely leverages your existing architecture without requiring you to deploy hardware at lower levels of the network.

Results in Minutes - Not Days: Claroty Edge deploys and delivers full visibility into any network in less than 10 minutes.

Highly Flexible Deployment: Claroty Edge's flexible cloud, on-premises, Docker-enabled Linux container, and Windows platform deployment options make the solution fully suitable for connected, air-gapped, and cloud-enabled networks.

How It Works

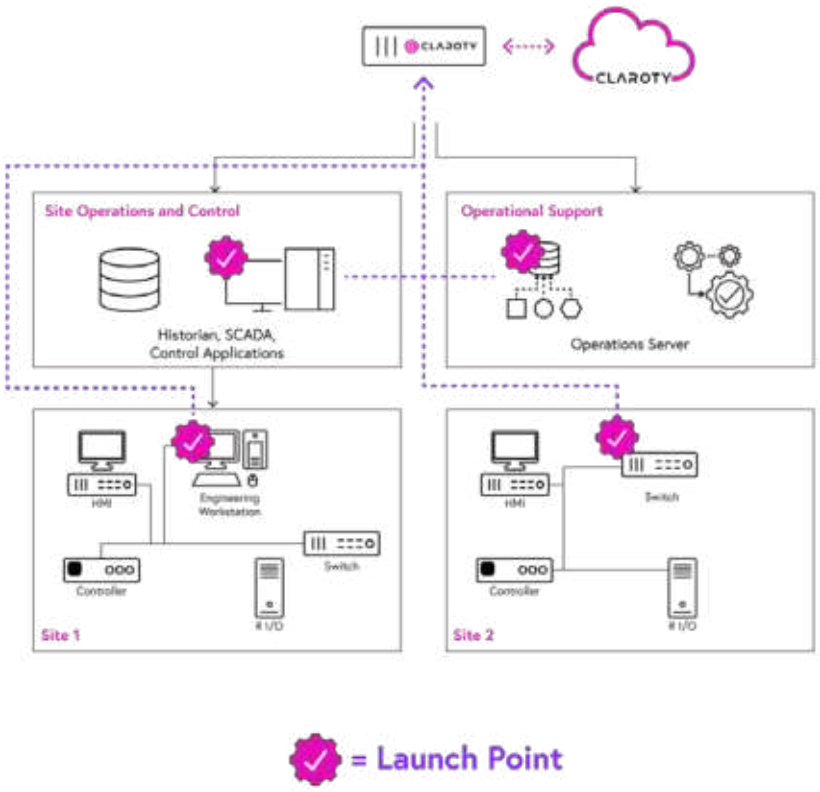
Claroty Edge performs automated, non-intrusive asset discovery by issuing safe, vendor-specific queries to devices on the local subnet of the host where it runs.

- **Granular asset details:** Captures IP/MAC addresses, operating system, firmware version, installed patches, device type, and more.
- **Point-in-time discovery:** Executes one-time discovery on demand, with optional support for periodic, scheduled runs.
- **Subnet-specific scope:** Limits discovery to only the subnets the host device is directly connected to, ensuring precise, localized visibility.

How To Deploy

Claroty Edge deploys as a lightweight, agentless executable that deploys quickly on both Windows and Linux-based hosts.

- **Zero hardware requirements:** Install Edge to host devices — no need to provision new hardware.
- **Docker-enabled flexibility:** Run Edge as a container on Linux-based infrastructure—like switches, firewalls, or edge servers—ideal for air-gapped or segmented environments without dedicated hosts.
- **On-demand execution:** Once deployed, Edge can be run as a one-time executable or for periodic, automated execution.



Claroty Edge deploys as a lightweight executable on Windows and Linux hosts to automatically query assets on the local subnet. In air-gapped environments, Edge can deploy to Linux-based devices via Docker containers, eliminating the need for host devices.

Key Use Cases

CPS Asset Inventory

- Gain complete, near-instantaneous visibility into all OT, IT, IoT, and BAS assets with asset information such as IP, MAC, OS, Install Patches, Model, Serial, Firmware, Asset Type, and more.
- This instant, accurate inventory creates a strong foundation for effective cybersecurity, enabling key outcomes such as exposure management, audit readiness, and M&A due diligence.

Active Exposure Discovery

- Edge's unique, non-disruptive queries help uncover critical exposure data that traditional vulnerability management often misses.
- Easily identify and validate the severity of vulnerabilities and other exposures – such as missing critical patches, end-of-life indicators, and open ports – to inform risk management prioritization.

Other use cases include:

- **Audit & Compliance:** Easily, quickly, and effectively support audit requests and report compliance for your CPS network, resulting in greater confidence in your reporting, a reduced risk of failed audits, and stronger compliance and overall security posture.
- **M&A Due Diligence**: Conduct M&A due diligence on target companies' CPS networks more easily, quickly, and effectively, leading to a rapid fulfillment of M&A requirements and clear insight into operational risk posture — all while adhering to LOI specifications.

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection — whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.

CLAROTY