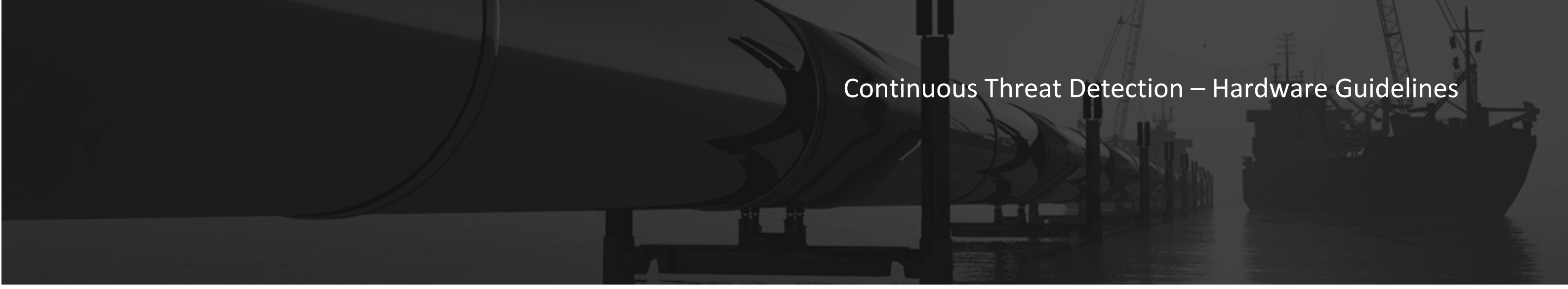
CLAROTY
Clarity for OT Networks

Claroty Hardware Specifications Guide

The US address:
488 Madison, 11th Floor
New York, NY 10022

The IL address:
7 Totseret ha-Arets St, 5th Floor
Tel Aviv-Yafo

Website address:
Claroty.com



Continuous Threat Detection – Hardware Guidelines

The general hardware requirements are listed in the following sections. Since not all networks are the same, it's important to point out the hardware requirements below are Claroty's recommendation based on tests and extensive field experience. The dynamic nature of ICS networks should be taken into account when determining hardware requirements. Factors such as the amount of traffic on the network (represented as Expected Traffic) and the number of assets (represented as Assets) can help to determine the minimum hardware requirements.

The software is designed to operate in virtual or physical environments, as well as container-based deployment options. The nature of virtual environments is to share hardware resources. The specs that are provided in this document make the assumption that resources for the application are available.

The recommended hard drive sizing, described in the sections below, is tuned for the average deployment for storing the data for 1 year. If it's required to store the data for a longer period, a larger hard drive size should be used.

Enterprise Management Console (EMC)

Information such as Assets, Alerts, Baselines and other metadata from all connected CTD Servers are stored in the Enterprise Management Console. The management console provides a single pane of glass aggregating and consolidating data from various deployed Claroty products, across hundreds of facilities and disparate locations. It displays a unified view of Assets, Activities and Alerts – highly suitable for Security and SOC teams.

A detailed summary of specific requirements can be seen below:

	Small Deployment	Mid-range deployment	Large Deployment
Deployment Description	High-performance and expandable rack-mounted appliances for real-time industrial network visibility, cyber security and monitoring		
#CTD Servers	<10	<25	<120
Processor*	6 cores	12 cores	24 (2x12) cores
RAM	16Gb	32Gb	64Gb
Hard Drive	80GB SSD in RAID (+20 GB per site)		
OS	ClarotyOS		
Web portal Access	The web portal has been optimized for use with Google Chrome (latest version)		

* Server grade Intel cores (Xeon) with 2.1Ghz clock rate or above.

Continuous Threat Detection (CTD)

Claroty's Continuous Threat Detection (CTD) is configured to deliver safe, secure and reliable operations in large, complex industrial networks. CTD is fully tuned to support multiple use cases, technical constraints, and environments including environments with limited computing power, small physical footprint requirements, and communication over low-bandwidth links.

CTD Server – Provides deep visibility and extreme detection capabilities across complex multi-vendor OT environments. CTD Server is responsible for continuously analyzing network traffic, detecting behavioral-based anomalies, and aggregating sensor data to offer real-time industrial network visibility, cyber security and monitoring.

CTD Sensor – Provides a secure and easy deployment, as well as powerful services for rapid, reliable, and bandwidth-optimized communication. Lightweight sensors provide full visibility into large distributed environment where multiple tapping point location are required for the same logical network.

For complex and intensive networks, a multi-layered architecture of CTD Sensors and CTD Server is recommended.

Continuous Threat Detection (CTD)

	Small Deployments	Mid-range Deployments	Large Deployments	Very-large Deployments
Deployment Description	High-performance and expandable rack-mounted appliances for real-time industrial network visibility, cyber security and monitoring			
Assets	<300	300-1500	1500-5000	5000-12000
Expected Traffic	100Mbps	200Mbps	500Mbps	1Gbps
Processor*	6 cores	12 cores	16 (2x8) cores	24 (2x12) cores
RAM	16GB	32GB	32GB	64GB
Hard Drive	80Gb SSD or RAID	240Gb SSD or RAID	240Gb SSD or RAID	480Gb SSD or RAID
Network Cards	At least one NIC for management and another NIC connected CTD Servers			
OS	ClarotyOS			
Web portal Access	The web portal has been optimized for use with Google Chrome (latest version)			

* Server grade Intel cores (Xeon) with 2.1Ghz clock rate or above.

Continuous Threat Detection – Active / App DB (ONLY)

For environments requiring the use of Claroty's Active or App DB data collection technology, we recommend using the Medium or Small server configurations – as per the following:

	Small Deployments	Very-large Deployments
Deployment Description	Active or App DB data collection technology	
Max. Protected Assets	<300	<12000
Processor*	6 cores	12 cores
RAM	16GB	16GB
Hard Drive	80Gb SSD or RAID	240Gb SSD or RAID
Network Cards	At least two NICs (Management, Monitoring)	
OS	ClarotyOS	

* Server grade Intel cores (Xeon) with 2.1Ghz clock rate or above.

Continuous Threat Detection Sensors

	Small Deployments	Large Deployments
Deployment Description	Suitable for large distributed environment where multiple tapping point location are required for the same logical network	
Max. Throughput	40 Mbps	200 Mbps
Processor	2 cores	6 cores
RAM	4GB	16GB
Hard Drive	40GB	40GB
Network Cards	At least one NIC for monitoring and another card for connecting to CTD Server	
OS	ClarotyOS	

About Claroty

Claroty's technology has been tested, selected and adopted by the most influential industrial automation control vendors and networking companies in the world. Our strategic partnerships include prominent system integration and managed security services firms worldwide.

The Claroty Platform provides full-spectrum visibility across a rapidly growing, opaque industrial operational technology (OT) attack surface. Claroty's technology delivers award-winning OT threat detection, continuous asset monitoring and management, and risk assessment.

About Claroty

Founded in 2014 by Team8, Claroty is headquartered in New York City and is backed by global investment leaders in cybersecurity, technology and industrial manufacturing, including Bessemer Venture Partners, Temasek Holdings, Siemens, Rockwell Automation, and Schneider-Electric among others.

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