CLAROTY



WHITE PAPER

Unlocking Cyber Resilience in Data Center Environments

TABLE OF CONTENTS

Introduction 3

The CPS Cybersecurity Challenge for Data Centers 4

Gaining Visibility Into Data Center CPS 5

Claroty's Recommended CPS Cybersecurity Journey for Data Centers 6

Early Stages of Your CPS Cybersecurity Journey: Asset Inventory and Exposure Management 6

Creating A CPS Asset Inventory With Dynamic Discovery 6

Reducing Your Attack Surface with Exposure Management 7

An Exposure Management Framework 7

Advanced Stages of Your CPS Cybersecurity Journey: Network Protection 8

Closing 9

©Copyright Claroty. All rights reserved

Introduction

The skyrocketing development of AI technologies and the ever-increasing computational requirements of today's society is fueling the demand for data centers. As these organizations continue to embrace digital transformation and prioritize reliability, operational continuity, and sustainability, they face growing complexity in protecting the cyber-physical systems (CPS) that underpin these objectives.

Maintaining uptime is critical for data centers, not only because they support essential services for both businesses and consumers, but also for meeting advanced certification frameworks such as the Uptime Institute's globally recognized standards for data center availability and performance. Achieving Tier III and Tier IV status emphasizes that individual equipment failures should have minimal impact on operations. To consistently achieve these uptime targets and safeguard against cyber threats, data centers must implement a robust CPS cybersecurity strategy that effectively mitigates risks and prevents disruptions.

Cyber-physical systems (CPS) are essential to any data center cybersecurity program because they bridge physical processes—such as cooling, power distribution, and access controls—with digital networks and control systems. Unlike traditional IT cybersecurity programs, which focus primarily on protecting data and digital services, the prevalence of CPS in data centers expands the attack surface and demands close attention to the operational integrity and safety of physical processes. Effective CPS cybersecurity requires a holistic approach that combines traditional IT security measures with specialized techniques to protect physical assets, ensuring safety, operational continuity, and business resilience.



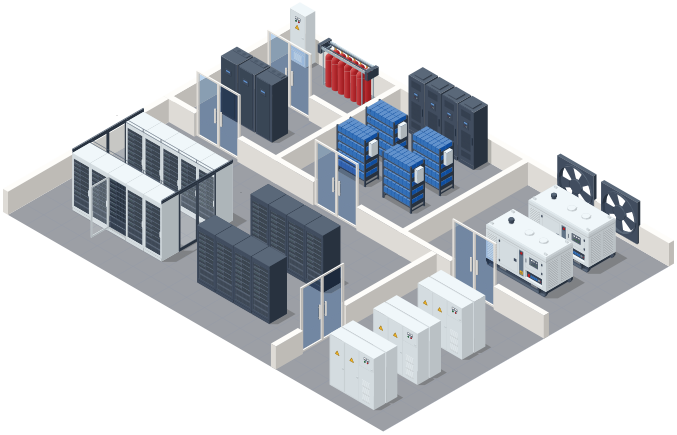
©Copyright Claroty. All rights reserved

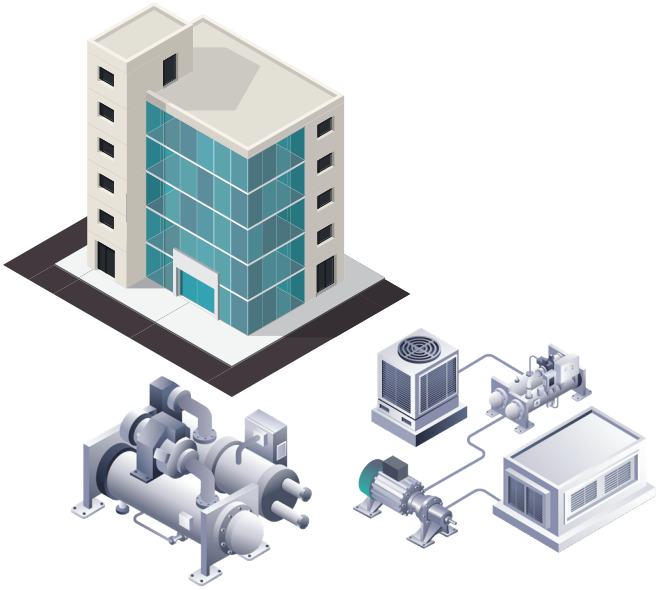
The CPS Cybersecurity Challenge for Data Centers

In the context of data centers, most CPS can be grouped into two categories, each overseen by a distinct system: Data Center Infrastructure Management (DCIM) and Building Management Systems (BMS).

Key Outcomes of DCIM and BMS

DCIM	BMS
• Encompasses a comprehensive suite of processes and tools designed to monitor, track, and manage both IT assets—such as servers and software—and data center physical infrastructure components like cooling systems, power distribution units, and floor space. • Primary goals include optimizing resource use, reducing operational costs, and boosting efficiency through the collection and analysis of key metrics, particularly those related to power consumption and the data center environment.	• Focuses on controlling the broader building environment, and maintains facility elements such as security, power distribution, lighting, and HVAC systems. • Primary goals include maintaining occupant comfort and ensuring operational integrity by automating mechanical tasks, which can range from fine-tuning temperature settings to managing fire detection systems.





While DCIM and BMS solutions offer valuable insights into critical processes, they are not designed to provide the specialized CPS visibility required for effective CPS cybersecurity controls. These systems often depend on manual asset entry, which can lead to incomplete asset inventories. Even when vendors offer automated discovery capabilities, these are typically limited to identifying their own equipment and may fail to detect devices from other manufacturers. This limitation can result in undiscovered assets, creating blind spots in the data center's CPS environment and leaving vulnerabilities unaddressed.

Additionally, DCIM and BMS solutions are not security-oriented and lack the ability to assess an asset's risk exposure. They cannot evaluate an asset's versioning information, which is crucial for identifying associated vulnerabilities and other exposures. Moreover, these systems fail to provide the business-critical context of an asset within the broader CPS environment, a key factor in enabling security teams to effectively assess risks and prioritize remediation efforts.

©Copyright Claroty. All rights reserved

Gaining Visibility Into Data Center CPS

Data centers operate as hyperconnected cyber-physical environments, resulting in an expansive attack surface that traditional IT cybersecurity measures cannot fully address. To effectively safeguard data center CPS, the first step is gaining visibility into a complete inventory of CPS assets. Integrating a dedicated CPS protection platform with existing DCIM and BMS solutions is the optimal approach.

A platform tailored for cyber-physical systems can identify the following critical systems within data center environments—detailing their functions, the most common manufacturers of these devices, and the communication protocols they use to implement their business logic:

System	Detail	Key Manufacturers	Common Protocols
Power Systems	UPS, generators, switchgear, and distribution systems designed for high-availability environments.	Schneider Electric, Eaton, Vertiv, ABB, Fuji Electric, Mitsubishi Electric	SNMP, Modbus, Proprietary, MMS, ICCP
Cooling Systems	Technologies like liquid cooling and airflow management to maintain optimal temperatures for high-density computing.	Trane, Vertiv, Stulz, Daikin, Munters, Airedale	Modbus, BACnet, LonWorks
Safety Systems	Fire detection and suppression mechanisms, Environmental monitoring and leak detection, Emergency Power-Off (EPO) systems, etc.	Bosch, Siemens, Kidde, Halma, Honeywell, Nohmi Bosai	Modbus, Proprietary, LonWorks
Physical Security	Surveillance, access control, and intrusion detection sensors to protect physical assets and infrastructure.	Axis Communications, Hikvision, Genetec, Honeywell, Bosch	RTSP, HTTP, Proprietary, SIP
Building Automation and Management Systems	Typically manage HVAC, lighting, and energy systems at the facility level to ensure operational efficiency,	Siemens, Johnson Controls, Delta Controls, Honeywell, Tridium, Schneider Electric	BACnet, Modbus, KNX
Data Center Infrastructure Management Systems	Provides centralized control and monitoring of power, cooling, safety and security, and IT infrastructure at the floor/rack level. enabling operational efficiency, asset management and capacity planning.	Schneider Electric, Vertiv, Nlyte, Sunbird Software	BACnet, SNMP, Modbus, IPMI

Table 1: Key Systems, Vendors, and Protocols In addition, you can find HVAC, Lighting, Renewable Energy, Environmental Monitoring, and other systems. Advanced analytics tools/platforms are often used for optimization and predictive maintenance.

©Copyright Claroty. All rights reserved

Claroty's Recommended CPS Cybersecurity Journey for Data Centers

This section will outline Claroty's recommended CPS Cybersecurity journey for data centers, which is the following:

1. Gaining a complete and comprehensive **Asset Inventor**y by leveraging an asset discovery methodology that provides comprehensive, safe, efficient, and scalable asset visibility.
2. Reducing the attack surface via **Exposure Management**, a proactive, endpoint-centric solution focused on remediating cybersecurity exposures.
3. Once data centers accomplish these early milestones in the CPS cybersecurity journey, **Network Protection** is an option to further secure the data center environment.

Early Stages of Your CPS Cybersecurity Journey: Asset Inventory and Exposure Management

Creating A CPS Asset Inventory with Dynamic Discovery

Building a comprehensive CPS cybersecurity program around a data center network starts with creating a foundation of in-depth asset visibility. Passive traffic inspection and collection has become the architectural standard in CPS environments because it can analyze machine-to-machine communication with no risk of operational disruption. However, this technique requires complex hardware deployments, scheduled downtime, and can lack visibility into specific asset details like patch-level insights.

Due to these reasons, taking a passive-only approach to discovery creates a longer time to value (TTV) and a higher total cost of ownership (TCO) for data centers. While passive communication is a crucial piece of a complete CPS visibility journey, Claroty's non-passive discovery methods have matured to provide deep visibility and asset understanding without hardware.

Claroty's **Dynamic Discovery** provides a proactive approach to asset identification and profiling that is not reliant on passive monitoring of network traffic. Claroty's multiple Dynamic Discovery methods give data centers the flexibility to easily combine asset discovery techniques based on their CPS visibility needs:



Passive Monitorning

Continuous Monitoring of network traffic to identify asset profiles



Safe Queries

Targeted discovery of assets in their native protocol



Claroty Edge

Speedy, host-based asset profiling through localized queries



Project File Analysis

Regular ingestion of offline configuration files for asset enrichment



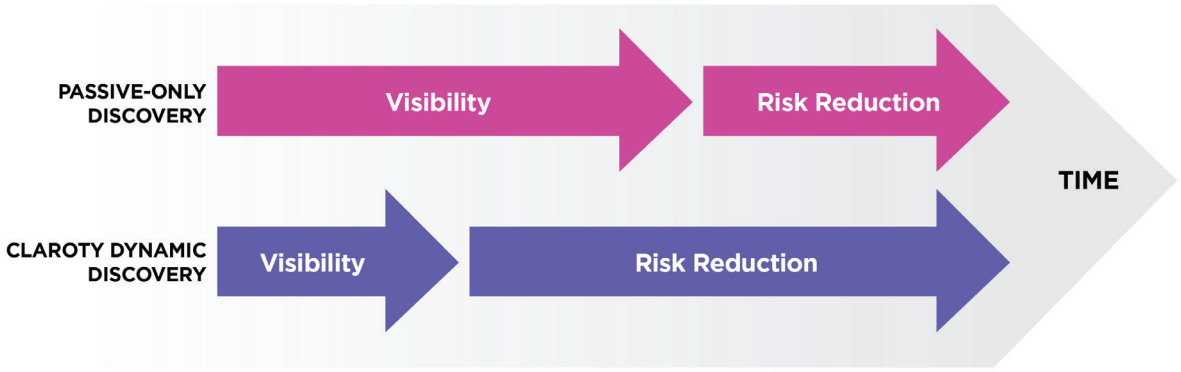
Integrations

Enriching visibility without hardware or configuration changes

©Copyright Claroty. All rights reserved

In data center environments, a verticalized dynamic discovery strategy can entail securely querying CPS assets through BMS/DCIM network protocols such as BACnet, Modbus, and LonWorks, and integrating these results with BMS and DCIM platforms—examples include Schneider Electric's EcoStruxure IT, Siemens' Desigo CC, and Johnson Controls' Metasys. By delivering accurate, granular, and comprehensive asset inventories, Dynamic Discovery lays a solid foundation for effective exposure management in hyperconnected data centers.

Taking a specialized approach to CPS visibility allows data center operators to realize a lower total cost of ownership and faster time to value not only in gaining CPS visibility, but in overall risk reduction.



Reducing Your Attack Surface with Exposure Management

In order to keep up with the continuous pace of digital transformation, data centers must evolve beyond traditional vulnerability management for their cyber-physical systems (CPS) and create a broader and more dynamic program for managing their overall exposure to risk. Traditional vulnerability and risk management strategies fall short in data center CPS because risk-prone exposures such as misconfigurations, use of insecure protocols, and default password usage are rarely taken into account in traditional vulnerability management workflows.

An Exposure Management Framework

Claroty advises that organizations shift into a continuous threat exposure management (CTEM) program that requires implementing more mature, strategy-driven preventative controls with detection and response capabilities. Gartner® defines CTEM as "Continuous Threat Exposure Management (CTEM) programme is a set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exposure and exploitability of an enterprise's digital and physical assets."[1]

Per Gartner®, "At any stage of maturity, a CTEM cycle must include five steps to be completed: scoping, discovery, prioritization, validation and mobilization. Organizations building a CTEM program use tools to inventory and categorize assets and vulnerabilities, simulate or test attack scenarios and other forms of posture assessment processes and technologies. It is important that a CTEM program has an effective and actionable path for infrastructure teams, system and project owners to take action on findings."[1]

Due to the unique nature of CPS environments, we believe that this requires a specialized approach that enables data centers to create an Exposure Management program that takes into account asset complexities, unique governance, and the business critical operational outcomes of data center environments. We feel Claroty provides a series of capabilities tailor-made to support a CPS-specific exposure management process:

©Copyright Claroty. All rights reserved

Continuous Exposure Management Process Stages	We believe Claroty's product functionality maps to each stage of the CTEM lifecycle as follows:
Scoping	Claroty solutions are designed specifically for cyber-physical system and help to identify and prioritize business critical operations. Claroty scopes and maps all relevant CPS assets including OT, IoT, and Building Automation Systems (BAS) in order to set security objectives and risk tolerance.
Discovery	CPS require specialized knowledge to effectively identify and assess exposures. Claroty's Dynamic Discovery techniques profile CPS, map network communications, and correlate vulnerabilities and other exposures.
Prioritization	Claroty's unique risk framework, data feeds from CISA's KEV and the EPSS, and multiple exposure considerations highlight specific attack vectors, assess exploitability and impact, and provide quantified remediation recommendations. In the case of data centers, power, cooling, and physical security are often the most sensitive, which is why Claroty ranks exposures based on business criticality.
Validation	Confirming the exploitability of an exposure requires an intimate understanding of the CPS and environment involved. Claroty simulates attack scenarios and utilizes extensive threat intelligence to validate potential exploits.
Mobilization	Claroty offers actionable guidance on remediation execution by recommending targeted actions to mitigate high-priority risks and improve system resilience. Claroty integrates with a wide variety of enterprise solutions and provides detailed reports to help enable seamless exposure remediation workflows.

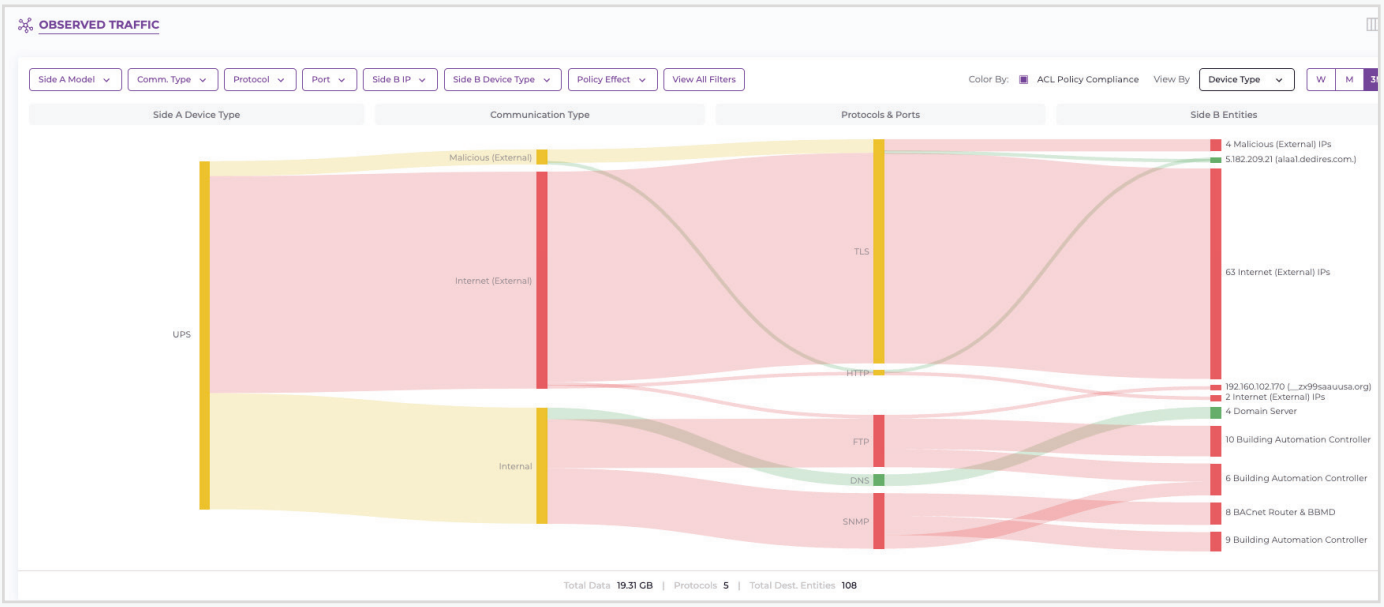
Advanced Stages of Your CPS Cybersecurity Journey: Network Protection

As your CPS cybersecurity program matures to the point where a strong foundation is built around asset identification and exposure management, many organizations take the next step toward advanced risk reduction strategies by implementing network protection controls. Passive monitoring is a prerequisite for this level of control because it observes real-time traffic patterns, ensuring communication policies are tailored to actual network behavior.

©Copyright Claroty. All rights reserved

One critical component of a network protection program is developing a segmentation strategy, which involves defining communication policies around specific asset zones. By segmenting your network in this way, you can create more precise boundaries and controls that enhance your ability to protect business-critical assets while reducing the attack surface. This method ensures that the right communication flows are allowed while preventing unnecessary or malicious traffic.

Effectively segmenting data center networks can be a tedious, error-prone process that entails defining and constantly tuning policies to your unique environment. For this reason, it's important to work with a CPS protection vendor that can not only provide recommended segmentation policies but also simulate network policies to show their potential impact on the environment.



Backed by Claroty's deep domain expertise, Claroty xDome leverages its asset visibility to automatically define and recommend network zones for communication policies. Dynamic policies can be simulated to demonstrate network impact before implementation, helping data centers keep up with the changing conditions within their complex environments.

Closing

Securing data centers against modern cyber threats requires a comprehensive approach to CPS cybersecurity. Claroty addresses the unique challenges posed by cyber-physical systems in data centers, beginning with foundational steps like creating a detailed and complete CPS asset inventory and implementing exposure management techniques. As a comprehensive CPS protection platform, Claroty extends its support of advanced use cases like network protection, evolving with data centers as they progress in their CPS cybersecurity journey. By following a structured, phased approach, data centers can effectively manage risks, enhance visibility, and maintain the safety and reliability necessary to support their mission-critical operations.

References:

[1] Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, 11 October 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

©Copyright Claroty. All rights reserved

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.

©Copyright Claroty. All rights reserved