CLAROTY

TEAM82

State of CPS Security: Data Center Exposures

Locking down the attack paths available to threat actors that put data centers at risk.

By Team82

Table of Contents

Executive Summary 3

Key Findings 5

The Riskiest Data Center Exposures 6

Severe Exposures One Hop Away 8

Power Monitoring 9
Power Distribution Units (PDUs) 10
HVAC/Cooling 10
Building Management and Automation Systems (BMS, BAS) 11

Exploitable Exposures within Data Center Assets 12

OT Control Systems 12
Power Monitoring and UPS 13
IoT/Smart Centers 14
BMS 15

Recommendations 16

1. Exposure Management for Data Center Assets 16
2. Implement Zero-Trust Segmentation 16
3. Harden BMS 17
4. Threat Detection, Monitoring for Lateral Activity 17

About Claroty 18

About Team82 18

Executive Summary

Cyber-physical systems (CPS) are the foundational piers of modern data centers. Building management systems (BMS), building automation systems (BAS), power distribution, monitoring and control systems, uninterruptible power supplies (UPS), generators, cooling infrastructure, environmental monitoring platforms, and data center infrastructure management (DCIM) solutions make up this CPS ecosystem, all of which support uptime and reliability requirements, service efficiency, and physical safety.

Rarely are these critical business assets directly connected to the internet, yet despite that reality, they are not inherently protected from cyberattacks. Direct connectivity is not always a prerequisite for compromise. Many times, adversaries are no more than "one hop" from an exposed CPS asset, after having gained a foothold inside the data center. Data center asset exposures are reached via indirect pathways into operational environments through interconnected IT systems, third-party remote access, remote management services, and trusted network relationships.

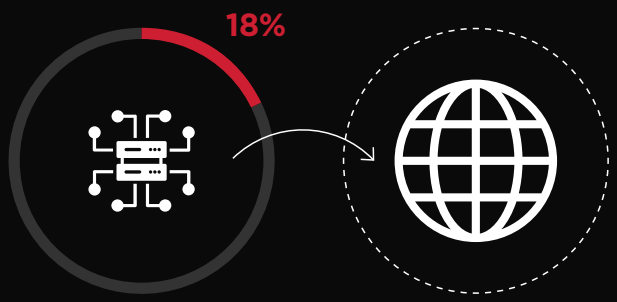
Attack paths may then lead threat actors to exploitable CPS weaknesses such as insecure communication protocols, known exploited vulnerabilities (KEVs), unmanaged remote access technologies, flat network architectures, weak authentication mechanisms, and misconfigured asset communications. Gaining access to operational infrastructure that controls critical data center functions poses serious consequences. Successful attacks against CPS inside data centers can disrupt cooling operations, affect power distribution, compromise environmental controls, interfere with backup generation systems, and degrade overall operational resilience. Operators, meanwhile, may be operating under a false sense of security that hardware redundancy is an adequate control in the event of an incident. Yet many of these hardware backups may contain the same exposures leaving them vulnerable to the same exploits that caused the incident—and the resulting downtime—in the first place.

Any downtime has business and services impacts. The demand for artificial intelligence (AI) in business and society is fueling enormous data center growth, and raising the stakes for keeping facilities secure and resilient in the face of incidents. Any interruption could lead to cascading consequences for businesses and critical services. For facility operators, outages or equipment damage from an incident could lead to failures in meeting strict service-level agreements with customers. Data center managers also face regulatory consequences as the result of an incident, in addition to contractual penalties, and financial losses associated with downtime.

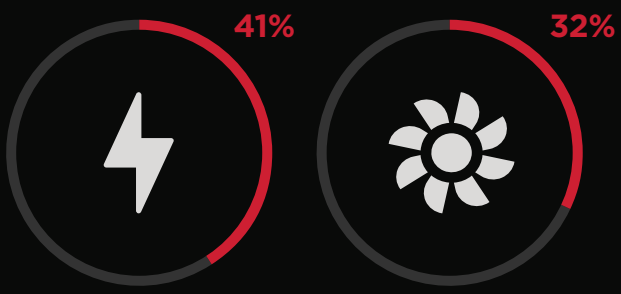
This research examines the most prevalent exposures that place data center CPS at risk despite limited direct internet connectivity. It explores how attackers exploit interconnected digital ecosystems to access operational infrastructure, identifies common classes of vulnerabilities and exposures that enable lateral movement, and provides insight into the evolving threat landscape facing modern data center operations.

Based on Claroty Team82's analysis of 750,000+ CPS assets across the world's biggest data center facilities, here are some key findings:

Key Findings



18% (32,000+) of more than 174,000 data center infrastructure assets are one hop away from a system making risky outbound connections to the public internet



Power distribution units (41%) and **HVAC/ cooling systems (32%)** have the highest percentage of assets one hop away from a risky connection to the public internet

Building management systems contain some of the riskiest exposures, **with 88% communicating over insecure protocols and 40% containing outdated firmware**

80%

More than 80% of OT control systems, power monitoring, and IoT systems communicate over legacy, insecure protocols such as BACnet and MODBUS

23%

23% of IoT devices such as environmental sensors, asset tracking tags, and IoT gateways contain known exploited vulnerabilities (KEVs)

The Riskiest Data Center Exposures

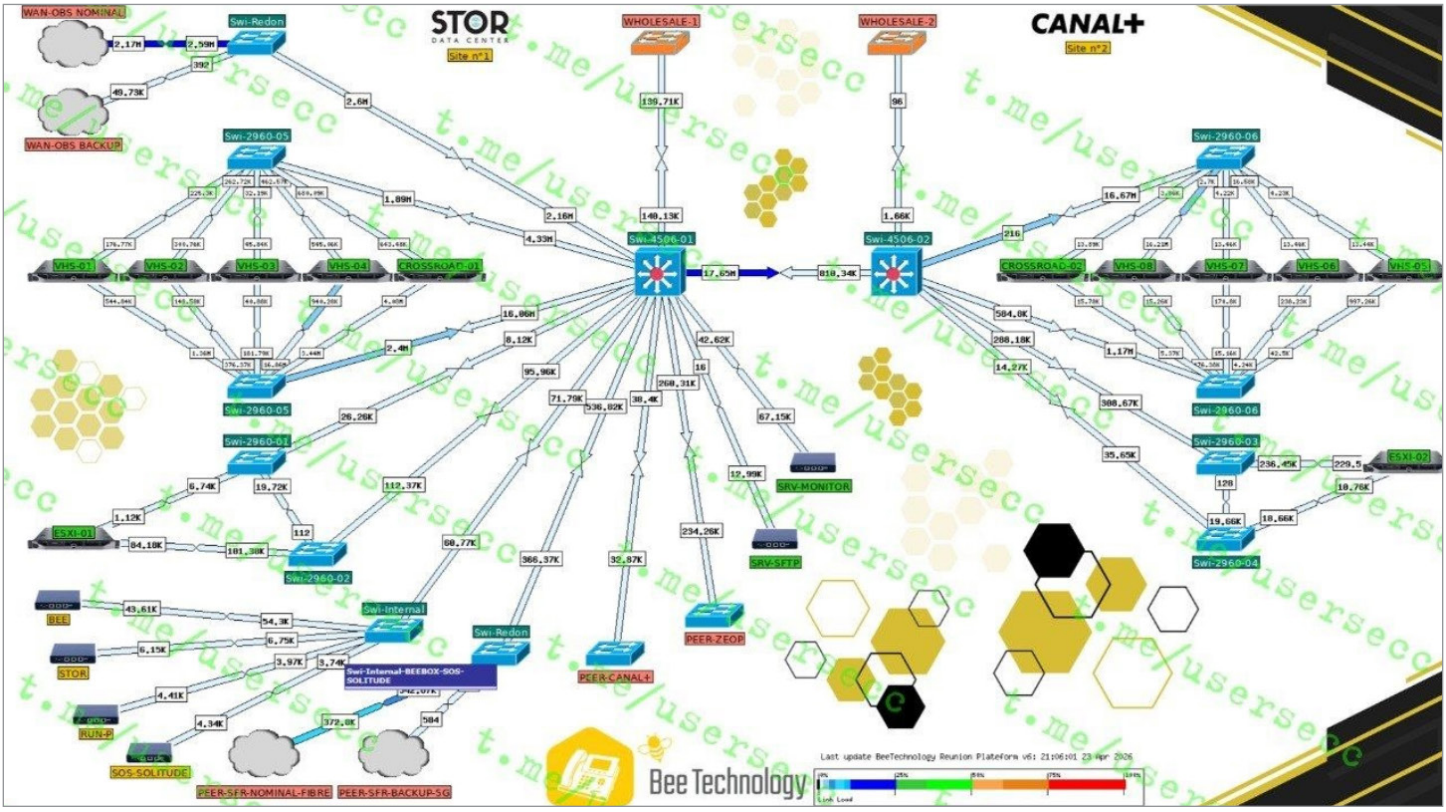
One Breach, Potential Global Impact

In April 2026, a report from threat intelligence company Vecert said a Russian hacktivist group known as Killnet had carried out an attack on France's STOR data center and Alpha Technologies.

Energy and monitoring data were exfiltrated, and the attackers claimed to have access to 120,000 uninterruptible power supply (UPS) devices across 6,000 networks, Vecert said. This was a significant breach with potential global impact on energy infrastructure worldwide.

Vecert added that the attack included a compromise of backup power systems supplied by Alpha Technologies, posing a further threat to services worldwide.

With data centers on par with other critical infrastructure worldwide, it's no surprise that threat actors see the value in disrupting data center operations, often for geopolitical gain or financial profits.



KILLNET ATTACKERS DEMONSTRATE THEIR ALLEGED CONTROL OVER HMIS THAT SHOW STATUS AND LOCATION OF CRITICAL DATA CENTER ASSETS.

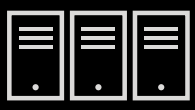
Data centers are increasingly at the heart of the global economy. Five gigawatt-scale data center campuses are expected to come online this year in the United States, introducing a scale of electricity consumption for each campus that is on par with the output of a nuclear power plant. Driving this hypergrowth among data centers globally is the training and operation of machine-learning models such as large-language models (LLMs) that are at the forefront of AI adoption.

The availability and resilience of these facilities depend not only on servers and networking equipment but also on an extensive CPS network responsible for maintaining the physical conditions necessary for continuous operations. A disruption affecting any of these systems can have cascading effects on facility operations, potentially resulting in widespread and costly service interruptions.

Our research looks at a set of data center assets inside some of the world's biggest facilities. This number includes operational technology (OT) assets (BMS, process control, and more) and data center infrastructure assets (power monitoring and distribution, UPS, HVAC, fire management, and more), below.

DATA SET FOR THIS REPORT

The scope of this report includes an array of data center assets, including building and power management systems, and infrastructure assets responsible for cooling, physical security, and fire protection systems.

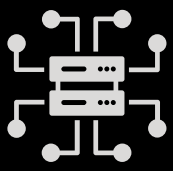


750,000+

total data center assets

191,000+

operational technology assets

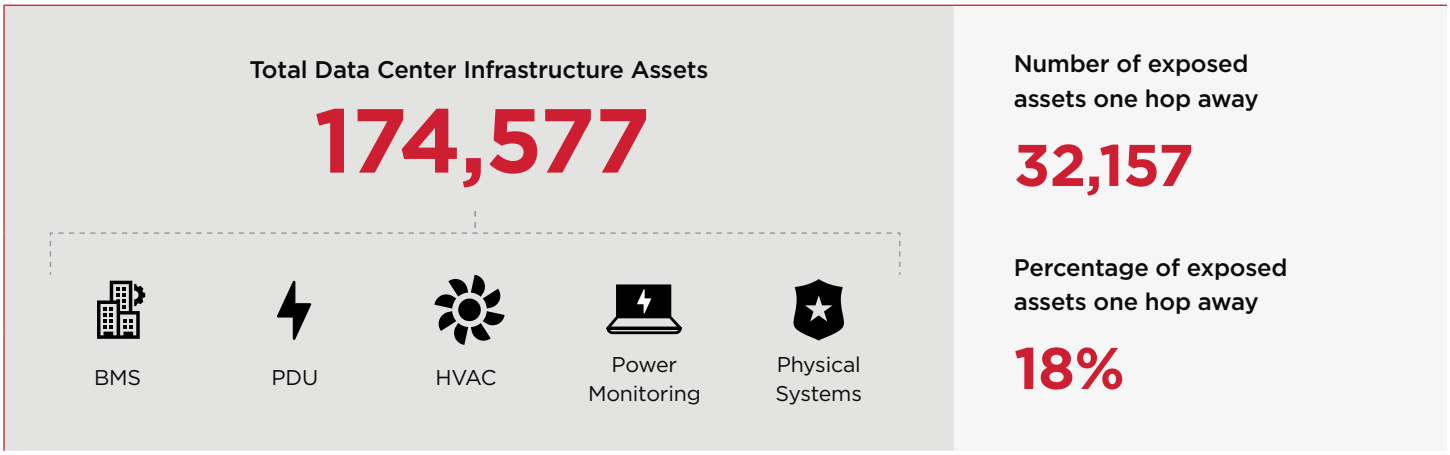


174,000+

data center infrastructure assets

Severe Exposures One Hop Away

Our research found that while direct internet exposure of these assets is relatively low, there are severe exposures including rampant insecure protocol usage, legacy operating systems, outdated firmware, KEVs, and others that are one hop from interconnected IT or networking infrastructure. This means the risk is outbound-dependent with internal systems checking out to or communicating with shared network infrastructure that happens to have an internet-facing component.



The growing convergence of IT and OT has further expanded the CPS attack surface. Data center organizations seeking greater visibility, automation, energy efficiency, sustainability reporting, and predictive maintenance capabilities are integrating operational systems with enterprise applications and cloud-based services. While these initiatives deliver measurable business value, they also create additional opportunities for attackers to traverse environments that were once largely isolated.

By examining these indirect attack vectors, the research seeks to provide data center executives, cybersecurity leaders, and operational stakeholders with a more accurate understanding of how cyber risk manifests within modern facilities.

Understanding these exposure pathways is increasingly important as threat actors shift their focus from traditional information theft toward operational disruption. For organizations whose business continuity depends on uninterrupted data center operations, identifying and mitigating one hop away exposures from data center infrastructure assets may represent one of the most effective strategies for reducing cyber-physical risk and strengthening operational resilience.

Let's quantify some of the exposures, first from a one hop lens, and then to overall assets. First, for context, here's a look at the percentages of internet-exposed assets in our data set.

Internet-Exposed Data Center Assets

Devices	Total	Percentage of Internet-Exposed Assets
IoT	96,108	6%
IT	289,010	3%
OT	191,110	1%
Data Center Infrastructure	174,577	0.4%
Total	**750,805**	**3%**

While only **0.4%** of total data center infrastructure devices are directly exposed to the internet (993 out of 174,577), an alarming **18.42% (32,157 devices)** are exactly **one hop away** from an exposed system. Let's break down the data further for four key areas: power monitoring, power distribution, HVAC, BMS:

Power Monitoring

Power monitoring is essential for many functions inside data centers, not only for tracking systems such as UPS and generators, but also in measuring efficiency of functions such as power usage, or tenant billing. They track numerous parameters such as current and voltage and have visibility into not only main utility feeds, but also generators, server rack usage, and event outlets.

Within our data set, power monitoring is a perfect illustration of the risk outlined in this research because 20% sit adjacent to internet-exposed systems, yet we track zero that are internet exposed.

Power Monitoring

29,954	0	5,833	20%
Total Devices	Internet-Exposed Devices	Devices One Hop from Internet Exposed System	Percentage of Devices One Hop from Internet Exposed Systems

Power Distribution Units (PDUs)

PDUs are highly intelligent data center assets, providing power to the technology backbone supporting key services inside the facility; those assets include servers, storage systems, and networking gear. They act as a high-end power strip, and are either floor- or rack-mounted, and take power from a main source like a UPS or generator, and feed it to the hardware or racks where servers and networking equipment are mounted. PDUs are essential in preventing power surges or sudden shutdowns, and integrate with data center infrastructure management systems, which provide a centralized view into facility performance, including power.

PDUs represent the highest risk in the entire data set by percentage, with four of 10 one hop away from an internet-exposed system. Because PDUs physically distribute power directly to individual server racks, an attacker breaching the outer perimeter can pivot into the PDU layer to cycle power, abruptly shut down racks, or cause systemic hardware damage across thousands of customer payloads.

PDUs

6,486	14	2,668	41%
Total Devices	Internet-Exposed Devices	Devices One Hop from Internet Exposed System	Percentage of Devices One Hop from Internet Exposed Systems

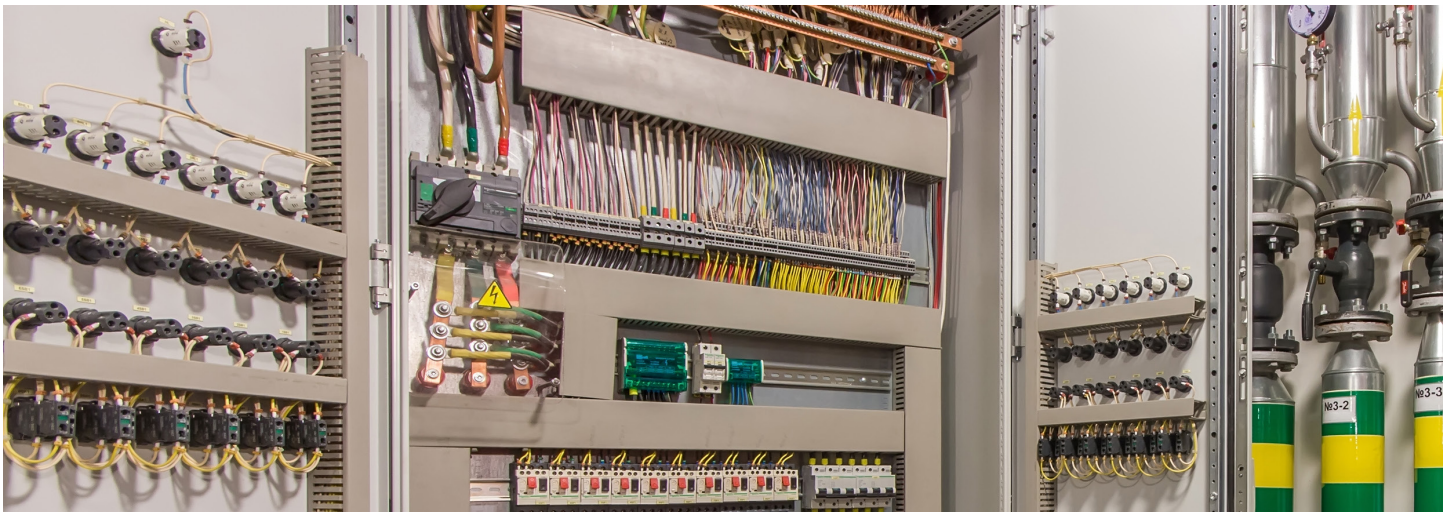
HVAC/Cooling

Heating, ventilation, and air conditioning (HVAC) systems may be the most essential facility management system operating inside data centers. HVAC controls the harsh and fluctuating temperatures inside a facility where one rack of equipment can produce more than 100,000 BTUs per hour of heat, requiring immense cooling capacity to keep assets running properly and preventing catastrophic downtime. Cooling and ventilation account for close to half of a data center's total electricity consumption; efficiency is paramount in order to minimize power usage and effectiveness.

Our data set shows, again, minimal direct connectivity of HVAC systems (one system), but one in three HVAC systems are adjacent to internet-exposed assets.

HVAC

3,695	1	1,204	33%
Total Devices	Internet-Exposed Devices	Devices One Hop from Internet Exposed System	Percentage of Devices One Hop from Internet Exposed Systems



Building Management and Automation Systems (BMS, BAS)

BMS is the center hub, a platform that oversees data centers' mechanical, electrical, and electromechanical systems (integrated physical and electrical systems that power and cool data centers). Heating, cooling, and power management systems are just three of the core components that feed data into a BMS, which is used to adjust temperatures, airflow, and humidity controls, as well as tracking power consumption, monitoring backup systems including generators, and overseeing fire and physical safety systems.

BMS is a key system in preventing downtime by automatically—or manually—adjusting temperature controls, optimizing power levels to prevent surges or sudden shutdowns, and also plays a role in predictive maintenance.

These systems are complex and our data shows a consequential percentage of BMS one hop from an internet-exposed system. An attacker able to access a BMS has a central view of many critical processes, and would have a lethal tool at their disposal in causing disruptions or physical damage to a facility.

BMS

39,335	266	5,410	14%
Total Devices	Internet-Exposed Devices	Devices One Hop from Internet Exposed System	Percentage of Devices One Hop from Internet Exposed Systems

While these assets are not directly connected to the internet, attackers do have pathways to target critical data center infrastructure systems because these internal systems communicate with internet-facing components.

Exploitable Exposures within Data Center Assets

Let's now look at exposures presented by different classes of data center assets within OT, IoT, and data center infrastructure. Now that we've identified which segments of data center infrastructure are adjacent to internet-exposed assets, let's examine which exposures an attacker may target if they can successfully move laterally to an asset.

OT Control Systems

OT control systems such as supervisory control and data acquisition (SCADA) or programmable logic controllers (PLCs) have key roles inside data centers carrying out either data collection or physical actions in order to keep processes stable. SCADA systems gather data from sensors, such as leak and humidity sensors for example, and other infrastructure assets in order to trigger alarms or alerts in the event of an incident. PLCs may have a role in adjusting cooling valves or relays for backup power.

These assets, however, suffer from many of the same exposures plaguing OT in other critical industries such as manufacturing or water and wastewater. Legacy technology deployed a decade or two ago may leave behind a trail of exploitable vulnerabilities, or insecure connectivity to the internet for remote maintenance. Communication between these assets is often carried out over protocols that lack basic security features such as authentication or data encryption that preserves the integrity of process data. For example, 83% of all OT devices use MODBUS as a communication protocol, which lacks basic authentication and transmits data in cleartext. Our research also shows a high concentration of known exploitable vulnerabilities (KEVs) and outdated firmware on OT assets that are ripe for exploitation should an attacker be able to reach them inside the data center.

OT Controls

81,420	613	11,498	85%	48%
Total Devices	Internet-Exposed Devices	Devices Containing KEVs	Percentage of Devices Communicating over Insecure Protocols	Percentage of Devices Running Outdated Firmware

Power Monitoring and UPS

Power systems inside the data center also pose risks to uptime, reliability, and safety should an attacker successfully make the one hop and laterally reach these infrastructure assets. They contained the most KEVs among data center infrastructure assets, yet relatively low percentages overall. Where these devices were most vulnerable was with insecure protocols with 86% of UPS and 82% of power monitoring systems using insecure protocols, again mostly MODBUS. Power monitoring systems also had a notably high percentage of devices running outdated firmware.

Power Monitoring

30,610	0	833	82%	59%
Total Devices	Internet-Exposed Devices	Devices Containing KEVs	Percentage of Devices Communicating over Insecure Protocols	Percentage of Devices Running Outdated Firmware

UPS

16,057	86	101	86%	23%
Total Devices	Internet-Exposed Devices	Devices Containing KEVs	Percentage of Devices Communicating over Insecure Protocols	Percentage of Devices Running Outdated Firmware

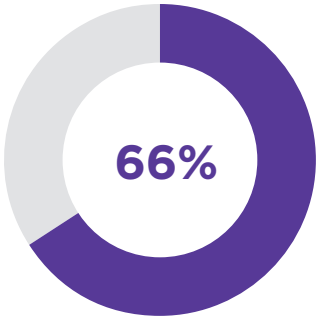
IoT/Smart Sensors

Internet-of-things (IoT) devices, some of which have been at the center of large breaches in the last two decades, are invaluable operational tools inside data centers. Connected smart devices collect telemetry data and communicate over sometimes weak protocols to DCIM platforms. These devices include environmental sensors, asset tracking tags, and also gateways that are fed data from numerous sensors. Gateways transmit metrics to the cloud where it's processed for preventative maintenance, and other analytics-driven insights.

Notoriously, IoT assets are insecure. Some lack the processing capabilities to support security features such as encryption, while others may not have the form factor to accept firmware updates. IoT assets at the edge also present threat actors with an attractive target to gain a foothold in data center infrastructure and then moving laterally onto exposed CPS assets.

Our data shows that nearly a quarter of the IoT devices contain KEVs, and present a real risk to facilities. IoT devices also communicate over insecure protocols at a percentage on par with OT control systems and some data center infrastructure.

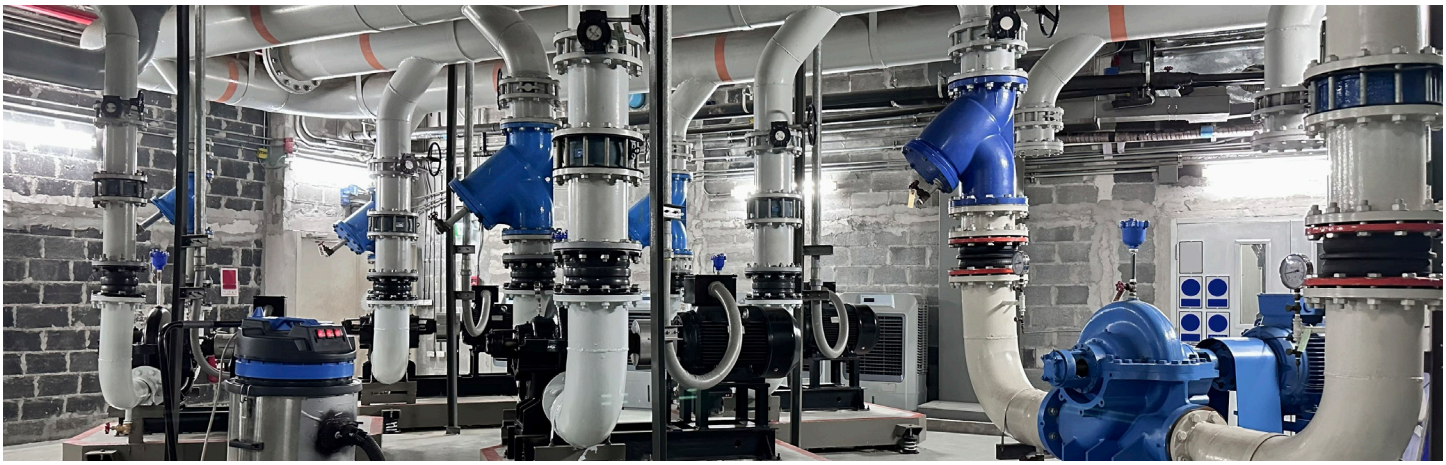
Clear-Text Trouble



66% of general IoT devices communicate via plain-text over HTTP, a higher percentage than any other **OT (52%)** or **IT asset (7%)**.

IoT

2,150	88	23%	72%	37%
Total Devices	Internet-Exposed Devices	Devices Containing KEVs	Percentage of Devices Communicating over Insecure Protocols	Percentage of Devices Running Outdated Firmware



BMS

BMS is responsible for overseeing the heartbeat of a data center, its environmental controls, fire suppression, elevators, and much more. An attacker able to make the one hop from an adjacent system communicating with a BMS may find a bevy of risky exposures at their disposal.

Although relatively few BMS within our data set (less than 1%) are directly exposed to the public internet, our research uncovered a handful of concerning exposures that data center operators should be aware of, starting with the prevalence of insecure protocols. Close to 90% of BMS in our data set communicate using insecure protocols, primarily BACnet (42% of BMS). BACnet implementations lack authentication and encryption, communicating in clear text. Meanwhile, 40% of BMS contain outdated firmware, a significant exposure given the lag between firmware update development and distribution from manufacturers, and implementation by data center operators.

As for KEVs, our data shows a relatively low percentage of BMS containing exploitable vulnerabilities; 800 devices or 1% of our data set. This is still a critical exposure because any lateral leap into these unpatched KEV devices gives an attacker the ability to trigger exploits that could effectively knock a data center offline without touching a single server.

BMS

66,395	369	800	88%	40%
Total Devices	Internet-Exposed Devices	Devices Containing KEVs	Percentage of Devices Communicating over Insecure Protocols	Percentage of Devices Running Outdated Firmware

Recommendations

Our research demonstrates that while data center infrastructure and the assets that ensure uptime, reliability, and safety inside facilities are rarely directly communicating to the public internet, they still contain exploitable exposures that can be targeted by a determined attacker, often just one digital hop away.

Here are four recommendations for data center operators to mitigate this risk.

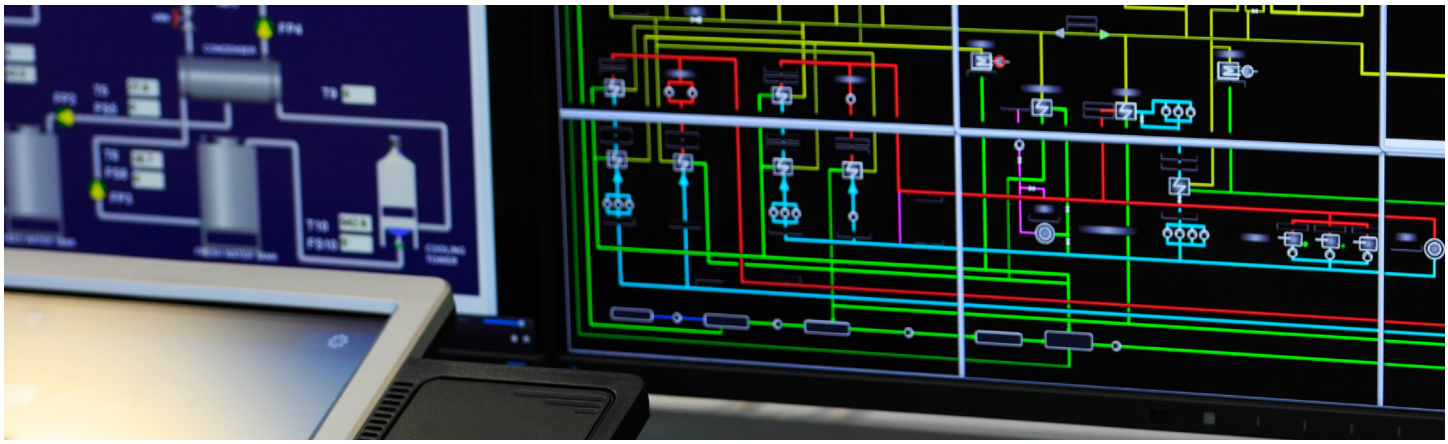
1. Exposure Management for Data Center Assets

Exposure management for data center infrastructure and assets has moved beyond defending assets at the perimeter, toward requiring an understanding of communication pathways between assets that may not be directly connected to the internet, but are, as we've demonstrated, one hop away from a reachable IT or networking asset.

The primary exposure for these foundational data center assets is the presence of outdated firmware. Unlike IT software, which benefits from automated patch cycles, updating a UPS or BMS controller requires planned downtime, carries operational risk, and is frequently left exposed. This legacy firmware leaves devices vulnerable to KEVs for long periods of time. When a perimeter asset or networking device is compromised, an attacker can bridge the gap to the internal facility network, leveraging these unpatched vulnerabilities to establish a foothold on the infrastructure that keeps the data centers running.

Compounding this risk is the reliance on inherently insecure legacy protocols such as MODBUS and BACnet. Designed decades ago for closed automation loops, these protocols lack native authentication, or encryption. Anyone who can reach a MODBUS or BACnet endpoint can issue command strings—such as modifying power thresholds on a PDU. Because these protocols transmit data in cleartext, an attacker one hop away can capture traffic, understand how packets communicate, and the pathways they take before triggering an attack.

Data centers must continuously map risky internal attack paths. By mapping these one hop exposure paths and enforcing rigid segmentation, data centers can neutralize the risks of outdated firmware and insecure protocols, ensuring that an exposed asset does not translate into a catastrophic physical facility outage.

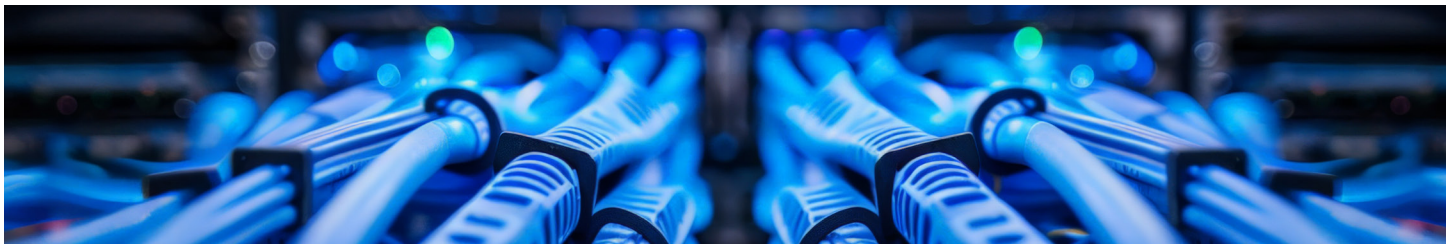


2. Implement Zero-Trust Segmentation

Segmentation—and microsegmentation—are the primary controls limiting the blast radius of a cyberattack. Implementing strict, zero-trust network segmentation between IT and facility systems is paramount. With our research demonstrating the reachability of data center infrastructure via internal communication with adjacent systems and the exposures putting that infrastructure at risk, segmentation is the fundamental cybersecurity control we recommend.

This is especially critical for data centers where flat networks are prevalent. Segmentation via VLANs, for example, limits how much lateral movement a threat actor can achieve and the potential disruption of services or physical damage to assets. By limiting unnecessary connections and isolating key assets or infrastructure components via segmentation, data centers can shrink the exposures attackers covet.

Zero-trust segmentation, meanwhile, further isolates key assets and infrastructure by putting strict access controls in place. Operators can enforce restrictive security policies that enforce least-privilege approaches to zero-trust, ensuring that identities are validated for each request. This is especially important for assets with exposures that cannot easily be mitigated or remediated. For more granular protection, microsegmentation can be applied to protect internal communications, and allows operators to isolate workloads for specific applications.



3. Harden BMS

With BMS overseeing much of the critical data center infrastructure, hardening these management platforms is a critical part of any security strategy. Segmentation is a critical control specific to BMS, which should operate on an isolated physical or VLAN away from corporate networks and other IT, IoT, or OT assets containing risky exposures. BMS should not be directly connected to the internet, though our research revealed hundreds with outbound communication to the public network, often in clear text.

A zero-trust architecture implements strict device and user authentication controls, blunting the impact of the use of weak protocols such as BACnet for communication. Zero-trust approaches are also important because many BMS sit on flat networks where east-west communication pathways between assets is commonplace. A compromise of one asset could jeopardize the BMS if an attacker is successfully able to move laterally on the network to these high-value systems.

BMS also operates often on outdated firmware and legacy operating systems that are no longer supported with security updates. A combination of segmentation and zero-trust further hardens BMS that can no longer be easily patched.

4. Threat Detection, Monitoring for Lateral Activity

Threat detection for CPS in a data center involves continuously monitoring the physical facility infrastructure and the digital systems that control them. The goal is to detect, isolate, and mitigate malicious attacks and operational anomalies before they disrupt server operations

Asset discovery and inventories catalog CPS assets in a facility and feed that to a threat detection solution. They must be protocol aware and listen for CPS- and OT-specific protocols such as BACnet, MODBUS, SNMP and others watching over machine-to-machine communication. A baseline of asset behaviors that aligns with operations is determined and any deviations trigger alerts.

Attackers are aware of the legacy exposures present in modern data centers, and a successful exploit can bring a facility to its knees. State actors can impede critical services within a region with a takedown of a critical data center, giving them a geopolitical advantage during a kinetic conflict, or merely sowing societal chaos as a result.

Criminal entities can also leverage data center exposures to launch ransomware attacks that could impact environmental controls or other infrastructure vital to a facility's well-being. Ransomware continues to be a profitable business and data centers with critical exposures are at risk, especially if assets are internet-facing.

As data centers continue to evolve into critical infrastructure globally, their protection is of utmost importance to the ongoing AI boom, economic and national security. Our report identifies the riskiest exposures inside these sensitive facilities, and demonstrates how a determined attacker with access inside a data center could move laterally to exploit an exposed device that may not necessarily be facing the public internet.

About Claroty

Claroty empowers organizations to protect the mission-critical infrastructure that underpins modern life. The AI-powered Claroty Platform serves as the single source of operational truth, providing the deepest visibility and broadest protection across cyber-physical systems (CPS), leveraging five core solutions: asset inventory, exposure management, network protection, secure access, and threat detection. Claroty helps organizations operationalize CPS protection through a programmatic approach designed to reduce risk, maintain operational integrity, and meet compliance–whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). 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.

About Team82

Team82, the research arm of cyber-physical systems (CPS) protection company Claroty, is an award-winning group of researchers known for threat research, OT and medical protocol analysis, and discovery and disclosure of industrial, healthcare, and commercial product vulnerabilities. Committed to strengthening CPS cybersecurity and equipped with the industry's most extensive testing lab, the team works closely with leading vendors to evaluate the security of their products. As of March 2026, Team82 has discovered and disclosed more than 700 vulnerabilities. Visit: Claroty.com/Team82

CLAROTY

TEAM82