DRAGOS

SOLUTION BRIEF: DATA CENTERS

Keep The Power On and The Cooling Running

Every server, GPU, and tenant workload depends on operational technology: the building management, power, and cooling systems that keep a data center inside its operating limits around the clock.



Updated November 2026

The Market: AI Is Rewriting Data Center Demand

Data centers have become critical infrastructure. The International Energy Agency projects global data center electricity use will more than double, from about 415 TWh in 2024 to roughly 945 TWh by 2030, with AI as the main driver. In the United States, data centers account for nearly half of all electricity demand growth through 2030.

That growth lands on the facility. AI racks push power density and heat far past what legacy designs expected, and operators are adding liquid cooling, on-site generation, and larger electrical plants to keep up. Uptime Institute reports that power remains the leading cause of impactful outages, that AI demand is straining power and cooling designs, and that cyber incidents are rising with severe, lasting impacts.

Cooling leaves little margin for error. Studies cited by Dragos show that without backup, server rooms can become unacceptably hot within five minutes of a cooling outage. When a cooling issue struck one Singapore data center in 2023, about 2.5 million payment and ATM transactions failed at two banks before service recovered.

Uptime Is Now a Cyber Problem

The systems that hold a data center inside its limits are xOT: chillers, CRAH and CRAC units, liquid cooling loops, UPS, switchgear, generators, fire suppression, and access control, tied together by a building management system (BMS) and data center infrastructure management (DCIM). Regulators have noticed. NIS2 covers data centre service providers in the EU, and Australia's SOCI Act lists data storage and processing as a critical infrastructure sector.

The xOT Security Challenges Facing Data Centers

A data center's IT security program is often mature, while the facility systems underneath it sit outside the security team's view. Those systems run on protocols built to take commands, are reached daily by vendors and integrators, and connect to IT and the cloud for energy reporting and DCIM. An attacker who reaches them does not need to touch a single server to take one offline.

Key Challenges

- BMS, power, and cooling outside the security team's view
- Protocols that accept commands without authentication
- Routine vendor and integrator remote access
- Legacy controllers past end of support
- IT, DCIM, and cloud links that end the air gap
- No reliable inventory of facility devices

Outcomes & Benefits

BUSINESS

- Fewer facility-driven outages and SLA breaches
- Protected tenant trust and revenue
- Evidence for NIS2, SOCI, and customer audits
- Safer growth into AI and liquid cooling

OPERATIONAL

- Visibility into every system that keeps the facility running
- A short, prioritized fix list across BMS vendors
- Faster detection, investigation, and recovery
- A documented history of every setpoint change

© 2026 Dragos, Inc. All Rights Reserved.

Why Attackers Go After Data Center OT

- **A softer target.** Facility systems often sit outside the security team's view, with default passwords and shared vendor logins.
- **Protocols that take orders.** BACnet, Modbus, Niagara Fox, and LonWorks were built for interoperability and often accept commands without authentication.
- **A bridge to the enterprise.** Energy reporting, DCIM, and cloud analytics connect the BMS to IT. The air gap is gone.
- **Old and unpatched.** Legacy controllers sit next to new IoT, many past end of support with no patches coming.
- **Physical leverage.** Cutting cooling or tampering with power protection puts every tenant at risk at once, which raises the pressure to pay a ransom.

By the Numbers

81%

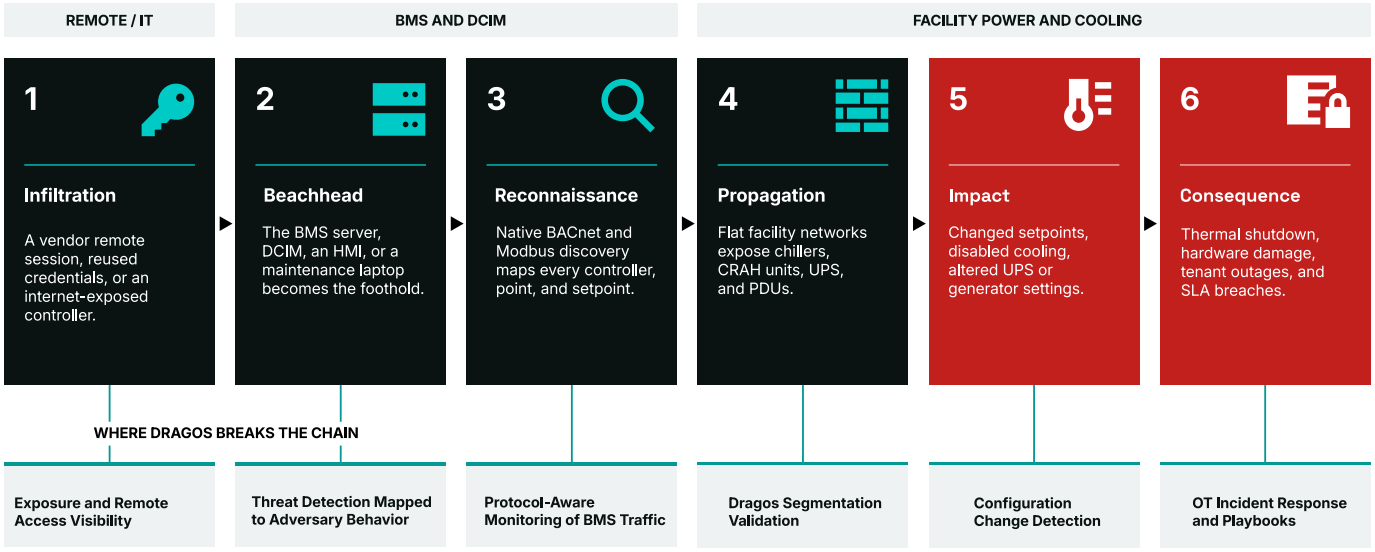
of Dragos services engagements found poor IT/OT segmentation.

73%

of Dragos incident response cases involved exploited or reused VPN and jump-host credentials.

Anatomy of a Breach

How an attack on data center facility systems typically unfolds, from a vendor connection to a thermal shutdown, and where Dragos breaks the chain.



Why it matters: An attacker does not need to reach a single server to take one offline. Steps 1 through 4 run on facility networks most security teams never see, which is where detection must start.

Proven in data centers. A global data center operator gained full visibility across its connected devices and remediated risk across its environment with Dragos. Read "Securing the World's Largest Data Center Environment" on dragos.com.

© 2026 Dragos, Inc. All Rights Reserved.

Recent Attacks and Warning Signs

Nov 2026

U.S. Government Cooling Advisory

CISA, the FBI, and partner agencies urged critical infrastructure operators to harden cooling systems, warning that unpatched or internet-accessible controllers can be altered to force continuous heating and defrost cycles.

Aug 2026

CyrusOne (Claimed)

The ShinyHunters extortion group claimed to have stolen data from the colocation provider, including floor plans, electrical diagrams, access-control records, and badge audits, and demanded $13 million. CyrusOne has not confirmed the physical-security data.

Jun 2026

Data Center UPS and HVAC Flaws

Researchers disclosed critical vulnerabilities in UPS network cards and an HVAC controller common in data centers. Chained together, they could give an attacker remote access to the UPS and let them run code.

Apr 2026

STOR Data Center, France (Claimed)

The pro-Russian group Killnet reportedly targeted the STOR data center and backup-power supplier Alpha Technologies, claiming access to roughly 120,000 UPS devices across 6,000 networks.

Feb 2023

GDS and ST Telemedia Global Data Centres

Hackers stole customer-portal logins for about 2,000 customers of two Asian operators, including some of the world's largest companies, plus logins for GDS surveillance cameras. Experts warned the logins could help attackers gain physical access.

Mar 2022

U.S. Government UPS Advisory

CISA and the Department of Energy warned that threat actors were accessing internet-connected UPS devices, often through unchanged default usernames and passwords.

Sector Signal

5 min

is how long it can take a server room to become unacceptably hot after a cooling outage with no backup in place.

The Threat

Adversaries are studying building systems. The PIPEDREAM framework, attributed by Dragos to CHERNOVITE, can manipulate OPC UA servers common in data center environments, and Dragos also tracks HEXANE and WASSONITE activity against data centers.

© 2026 Dragos, Inc. All Rights Reserved.

Common Protocols in the Data Center

A single facility can run many industrial and building protocols side by side. The Dragos Platform performs deep packet inspection of 600+ industrial protocols, so it understands what each command does, not just that traffic moved.

PROTOCOL	WHERE IT RUNS
BACnet/IP and MS/TP	BMS head ends, chillers, CRAH and CRAC units, air handlers
Modbus TCP / RTU	UPS, PDUs, generators, switchgear, and power meters
SNMP	UPS network cards, rack PDUs, and environmental sensors
OPC UA	BMS, DCIM, and supervisory system integration
Niagara Fox	Supervisory controllers tying multi-vendor BMS together
LonWorks	Legacy building controls, lighting, and fire panels
IEC 61850	Medium-voltage substations on large campuses
EtherNet/IP and PROFINET	PLC-run chiller plants and coolant distribution units



© 2026 Dragos, Inc. All Rights Reserved.

How Dragos Helps Data Centers

Data center operators need three things from facility security: to see every device that keeps the halls running, to know which exposures matter, and to trust the software inside equipment before it reaches the floor. Dragos covers all three, then watches the facility networks continuously.

THE DRAGOS PLATFORM

Detailed Situational Awareness

A multi-detection engine and deep packet inspection show what every BMS, power, and cooling device is doing, not just that it exists.

IN THE DATA CENTER

- Baseline normal traffic between BMS servers, supervisory controllers, chillers, and CRAH units, and query devices directly for deep insights beyond make, model, and firmware
- Spot new vendor sessions, unexpected writes to setpoints, and controllers changing mode
- Keep network history to tell a misconfiguration from an attack
- “Now, Next, Never” prioritization surfaces the 3-6% of vulnerabilities that need action now
- Dragos Device Remediation rotates credentials, pushes firmware updates, and manages certificates on connected devices
- Insights Hub brings alerts, asset context, and recommendations into one view

DRAGOS EXPOSURE MANAGEMENT

One Exposure View, Every Site

A single, continuously updated exposure view across IT, OT, IoT, and cloud, built from safe active discovery, always-on passive discovery, and pre-built integrations, without agents, credentials, or appliances.

IN THE DATA CENTER

- Inventory facility devices across halls, campuses, and colocation sites
- Pull in asset data from DCIM, CMDB, EDR, and cloud tools you already run
- Trace attack paths, multi-homed devices, and choke points between IT and facility networks
- Rank exposures by each device’s operational role

DRAGOS SOFTWARE SUPPLY CHAIN SECURITY

Know What is Inside The Equipment

Binary analysis of firmware and software generates a verified software bill of materials (SBOM), finding embedded vulnerabilities, exposed credentials, and hidden open-source components.

IN THE DATA CENTER

- Vet UPS network cards, PDUs, BMS controllers, and cooling units before they ship to site
- Reachability analysis shows which vulnerable code runs
- Scope the blast radius of a compromised component across every device in under a minute
- Verify vendors with evidence, not attestations

© 2026 Dragos, Inc. All Rights Reserved.

How It Fits Together

Start where you are. Exposure Management delivers an inventory from the tools you already run, and each step builds on the one before it toward full xOT security across every site.

Verify

Software Supply Chain Security checks firmware before equipment is installed.

Discover

Exposure Management and the Dragos Platform inventory every facility device.

Prioritize

"Now, Next, Never" isolates the 3-6% of vulnerabilities to act on first.

Remediate

Dragos Device Remediation rotates credentials and updates firmware.

Monitor & Respond

Threat detection, OT Watch, and Dragos incident response.

Built for Live Facilities

Safe for Running Halls

Passive-first monitoring watches traffic without touching controllers. Where active discovery is needed, queries are paced per host so cooling and power equipment keep running undisturbed.

Works Across Your Vendors

Dragos supports the building and power vendors data centers run, including Siemens, Johnson Controls, Schneider Electric, Honeywell, ABB, Emerson, and Trane, plus BACnet, Modbus, and proprietary protocols.

Siemens	Johnson Controls	Schneider Electric	Honeywell

ABB	Emerson	Trane	BACnet	Modbus	Proprietary Protocols

Scales From One Hall to a Global Fleet

Start with a single facility assessment and grow into multi-region deployment. One inventory and one exposure view follow you across campuses and colocation sites.

© 2026 Dragos, Inc. All Rights Reserved.

Key Requirements and How Dragos Helps

Know Your Crown Jewels

Identify the facility systems whose compromise would cause the greatest operational, safety, or financial impact.

> **How Dragos Helps:** Crown Jewel Analysis, part of the Dragos OT Cybersecurity Assessment, traces your mission down to the controllers, servers, and access paths it depends on.

See Every System That Keeps The Facility Running

Inventory BMS, DCIM, power, cooling, and physical security devices across every site & vendor.

> **How Dragos Helps:** The Dragos Platform builds a contextualized inventory of the controllers, servers, and connected devices that influence facility operations. Dragos Exposure Management adds a single, continuously updated exposure view across IT, OT, IoT, and cloud.

Fix What Matters First

Cut a long vulnerability list down to what an attacker would use.

> **How Dragos Helps:** Only 3-6% of OT vulnerabilities require immediate action. “Now, Next, Never” guidance points your facilities team at those first, then Dragos Device Remediation fixes them across BMS vendors and controller types, rotating credentials, updating firmware, and enforcing secure configurations.

Control Vendor Access and Prove Segmentation

Show that vendor sessions, IT, and DCIM cannot reach controllers they should not.

> **How Dragos Helps:** Dragos Segmentation models the access paths your firewall, router, and switch configurations permit, so teams find overly permissive rules before anyone uses them.

Detect Setpoint Tampering and Respond With Experts

Catch unauthorized changes to cooling, power, and access systems before tenants feel them.

> **How Dragos Helps:** Configuration detections flag changes to controller settings and modes. Threat detection is backed by Dragos xOT Threat Intelligence, OT Watch provides proactive threat hunting, OT Watch Complete adds 24/7 monitoring and triage, and Dragos incident responders bring over a decade of OT-specific experience.

Requirements

- ☑ NIS2 (data center service providers)
- ☑ Australia SOCI Act (data storage and processing)
- ☑ ISA/IEC 62443
- ☑ NIST CSF 2.0
- ☑ SANS Five ICS Critical Controls

One Intelligence Model, Three Views

The Dragos Intelligence Fabric connects three views of the threat into one picture for data center operations.

What Has Happened

More than a decade of OT-specific telemetry, adversary research, and incident response shows how attacks on industrial environments have unfolded and what worked to stop them.

What Is Happening

Dragos xOT Threat Intelligence tracks 26+ OT threat groups and the campaigns targeting critical infrastructure today.

What Is Hiding

OT Watch threat hunters use that same intelligence to search your facility networks for activity your alerts have not caught yet.

© 2026 Dragos, Inc. All Rights Reserved.

About Dragos

Dragos is the global leader in xOT cybersecurity and is purpose-built to protect the industrial and critical infrastructure that civilization depends on.

The Dragos Platform delivers visibility, continuous monitoring, and threat detection across expanded xOT environments at scale. It is powered by the Dragos Intelligence Fabric, built from over a decade of xOT-specific telemetry, adversary research, and incident response. Dragos EmberAI puts that intelligence directly in analysts' hands so each can operate like a professional regardless of their experience. xOT Threat Intelligence delivers finished threat intelligence built exclusively for xOT, produced by the largest private ICS/OT threat intelligence team in the industry. Dragos Expert Services provide direct access to frontline expertise, from security assessments to 24/7 incident response.

No other organization brings xOT-specific technology, intelligence, and services together under one roof.

Dragos protects organizations across electric, oil and gas, manufacturing, water, transportation, mining, and government sectors, operating globally from its headquarters in Hanover, Maryland.

To learn more, visit dragos.com or contact sales@dragos.com.

© 2026 Dragos, Inc. All Rights Reserved.