Securing Data Center Gray Space with Cisco Cyber Vision

Protect systems powering and cooling the data hall by turning your network into a defense system.

A data center's gray space is its operational network–power generators and substations, battery packs, microgrids, switchgear, cooling systems, and building management and security systems. The variety of systems, limited visibility of what is connected, vendor access, and fragmented ownership make data center gray space difficult to secure. The result is a growing attack surface where a cyberattack or an unintended configuration can disrupt power or cooling and shut down the entire datacenter.

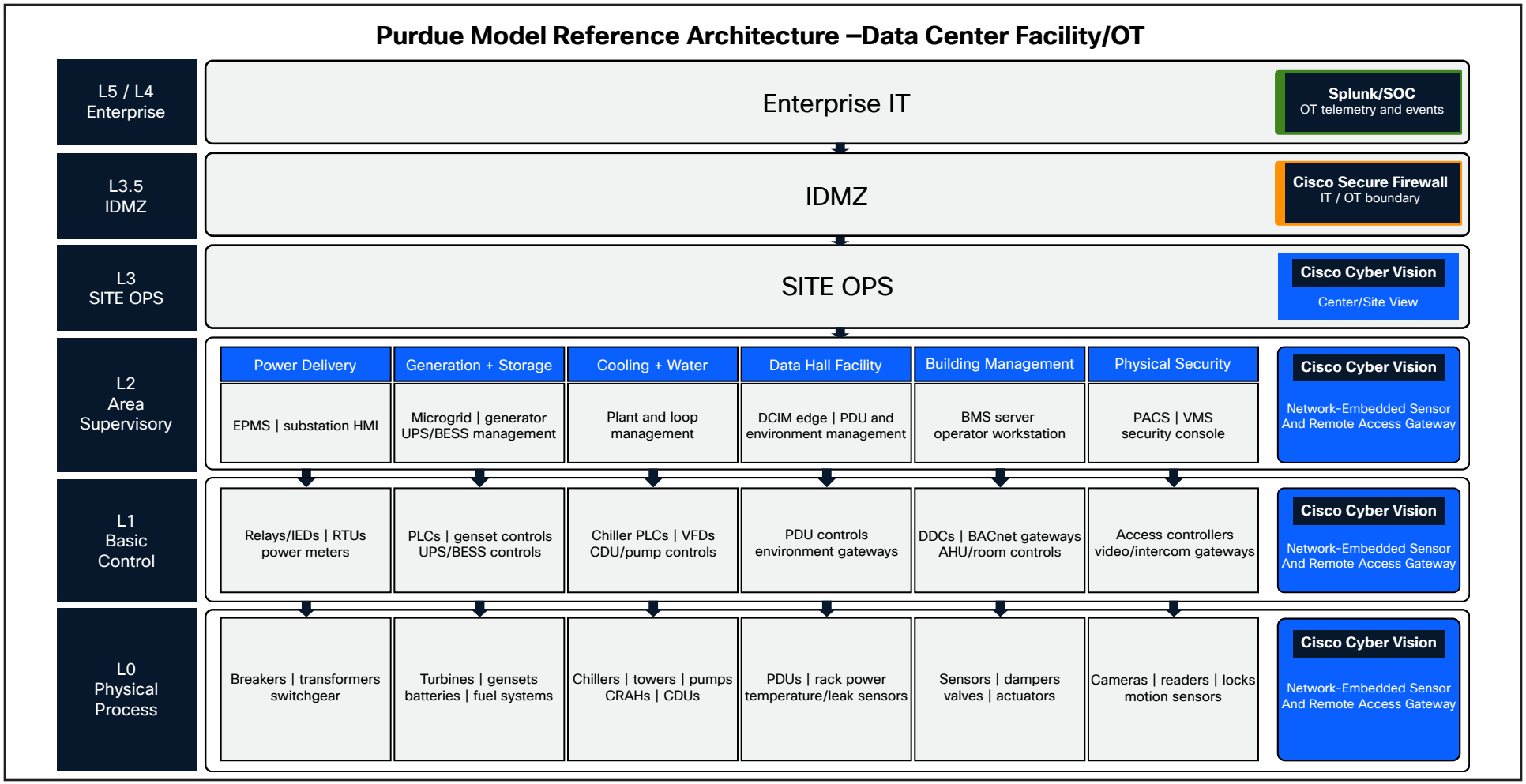
Cisco® industrial switches and routers, combined with Cisco Cyber Vision, provide a network-integrated foundation for securing data center gray spaces – continuously monitoring OT assets, assessing risk, and turning operational context into actionable security policy. With AI-assisted segmentation, controlled remote access, and integrations across Cisco and Splunk, this foundation gives IT, security, and facilities teams a shared view for protecting the critical infrastructure that keeps the data hall running.

Benefits

- **Network-native protection:** Prevent lateral movement of threats by using your network as a defense system without additional hardware appliances.
- **Comprehensive visibility:** See all sanctioned and unsanctioned assets, communications, and remote access backdoors.
- **Current, risk-informed inventory:** Maintain detailed profiles for discovered assets, including identity, vulnerabilities, behaviors, and prioritized risk context.
- **Controlled remote access:** Protect the operational network by offering employees, contractors, and vendors with zero trust remote access to authorized OT assets only.
- **Unified IT/OT operations:** Give all stakeholders a shared understanding on the security posture and OT context for correlation, investigation, and response.

How Cisco Cyber Vision Helps Secure the AI Data Center Gray-Space

Cisco Cyber Vision gives IT, cybersecurity, and facilities teams a common understanding of OT asset inventory, risks, and communications. This visibility can be leveraged to drive network segmentation, with AI-assisted policy recommendations and risk-free simulation, simplifying protection at scale. It enables zero trust remote access to give remote experts access to specific OT assets only when needed. Asset, vulnerability, activity, and security-event telemetry can be operationalized in Splunk for dashboards, correlation, detection, investigation, and response.



Cisco Cyber Vision Across Data Center Gray-Space Use Cases

Gray-Space Domain	Visibility	Segmentation	Secure Remote Access	Operational Outcome
Power Delivery	• Inventory visible Electrical Power Monitoring Systems (EPMS), relays, Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs), meters and switchgear • Map communications, vulnerabilities and dependencies	• Group assets by substation, power train or fault domain • Simulate policies before enforcement	• Limit access to named EPMS, relay and switchgear assets • Apply identity- and time-based controls	• Detect unexpected activity sooner • Contain incidents without exposing the wider power network
Generation + Storage	• Identify microgrid, generator, Uninterruptible Power Supply/ Battery Energy Storage Systems (UPS/BESS) and fuel-control assets • See dependencies between management systems, controllers and equipment	• Separate generation, UPS and battery systems by plant or power train • Preserve required microgrid and load-management flows	• Restrict vendors to assigned generators, UPS or BESS assets • Monitor and audit maintenance sessions	• Protect backup-power availability • Prevent one compromised system from affecting other power sources
Cooling + Water	• Map chillers, pumps, Variable Frequency Drives (VFDs), Coolant Distribution Units (CDUs), Computer Room Air Handling (CRAHs) and cooling loops • Show communications with plant-management and Data Center Infrastructure Management (DCIM) platforms	• Create zones by plant, equipment train, loop or data hall • Preserve required control and monitoring traffic	• Restrict Original Equipment Manufacturers (OEMs) to the chillers, CDUs, pumps or controllers they service Provide approved, time-limited access	• Contain incidents to one cooling train or loop • Accelerate troubleshooting and reduce vendor risk

Gray-Space Domain	Visibility	Segmentation	Secure Remote Access	Operational Outcome
Data Hall Facility	• Identify Power Distribution Units (PDUs), environmental gateways, and rack-level sensors • Map dependencies with DCIM, EPMS and facility systems	• Separate facility systems from production and out-of-band networks • Permit only approved alarm, capacity, and monitoring flows	• Limit maintenance teams to named PDU and environmental assets • Prevent access to production networks	• Protect facility-to-production boundaries • Improve investigation of power, capacity and environmental alarms
Building Management	• Identify visible Building Management System (BMS) servers, operator stations, Distributed Disaggregated Chassis (DDCs), Building Automation and Control Networks (BACnet) gateways, sensors, and actuators • Map control relationships with other facility systems	• Create zones by building, data hall, or building service • Restrict communications to approved BMS, DCIM, and facility flows	• Limit technicians to assigned BMS servers, gateways or controllers • Apply access schedules and session auditing	• Contain a compromised controller or gateway • Accelerate investigation of building and environmental conditions
Physical Security	• Identify visible Physical Access Control Systems (PACS), Video Management Systems (VMS), access controllers, cameras, readers, locks and intercom systems • Map communications and system dependencies	• Separate physical security from enterprise, production and facility-control networks • Create distinct video and access-control zones	• Restrict integrators to named security systems and devices • Provide approved, time-limited and auditable access	• Preserve surveillance and access-control availability • Reduce lateral movement and third-party service risk

Create a Protected, Resilient, and Controlled Foundation for AI-Ready Data Centers

Secure the OT infrastructure that keeps the data hall running.

Keep critical systems connected

Build resilient connectivity around electrical and mechanical fault domains using ruggedized switching, redundant paths, resilient topologies, and appropriate power and uplink designs.

Know what is connected – and at risk

Identify OT assets installed in the data center, their vulnerabilities and risks, and map communications without dedicated appliances or a separate collection network.

Protect operations by restricting communications

Use observed communications and AI-assisted recommendations to create operational zones and micro-segmentation policies. Simulate proposed rules before enforcing boundaries.

Control remote access

Provision identity and context-based remote access to named OT assets with MFA/SSO, schedules, approvals, and auditable sessions – avoiding broad network reach.

Align IT, security, and facilities

Give all stakeholders a shared understanding of connected OT assets, risks, and activities. Unify IT and OT visibility for SOC analysts to view the entire attack chain and run advanced detection, investigation, and remediation.

The Operational Impact

- **Greater resilience** across power, cooling, and facility fault domains
- **Continuous visibility** into connected assets, communications, and risk
- **Smaller blast radius** through operationally informed segmentation
- **Safer, auditable access** for maintenance teams and equipment vendors
- **Faster, coordinated response** across IT, cybersecurity, and facilities

The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more. Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. It's a rare combination.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack.

Start securing your industrial operations with Cisco today

Talk to a Cisco sales representative or channel partner and visit cisco.com/go/OTsecurity to learn more.

C45-6719920-00 09/26