Secure Networking for AI Data Center Gray Spaces

Enabling resilient data center operations with purpose-built secure rugged networking for power, cooling, and physical security.

AI workloads require data center owners to deploy massive compute capabilities. These data center white spaces depend on gray spaces working constantly behind the scenes to deliver reliable power, dissipate heat, and secure the facilities. Yet these interconnected systems often run on fragmented networks, leaving critical operations at perpetual risk of unplanned downtime and security threats, and overburdening teams managing disparate tools across multiple vendors.

Cisco® brings together decades of networking leadership combined with more than 20 years of expertise digitizing harsh industrial environments to connect the entire AI data center on a unified network foundation. Our purpose-built rugged networking and OT security portfolio enables data center owners to reduce silos, apply consistent policies, simplify operations, and strengthen resilience across the systems that keep AI running.

Benefits

- **Resilient connectivity:** Purpose-built rugged networking for demanding gray space environments
- **Simplified operations:** Unified management with tools IT already knows and love
- **Built-in security:** Continuous visibility across facilities, connected assets, and cyber risks
- **Layered defense:** The network contains threats without interrupting critical operations
- **Sustainable industrial-grade infrastructure:** Reduced power and cooling needs. Long life for minimized hardware refresh disruption

Power systems: Keep power flowing and AI processing

AI infrastructure places unprecedented demands on power substations, generators, UPS systems, battery energy storage, and electrical distribution. Connecting these systems requires precise timing, industrial protocols, rapid failover, and equipment engineered to withstand electromagnetic interference, voltage surges, heat, and vibration. A network failure can obscure critical telemetry, delay fault diagnosis, and disrupt the systems responsible for keeping every rack online.

Cisco brings proven utility networking capabilities into the data center with rugged Industrial Ethernet switches purpose-built for these demanding environments. Embedded OT visibility and identity-based segmentation help identify vulnerabilities and contain cyber threats. Resilient connectivity to the control platforms helps maintain dependable power operations from the utility connection to the rack.

Cisco's focused approach enables:

- Continuous connectivity with rugged DIN-rail and rack-mount switches, including high-density fiber downlinks to grid assets
- Utility-grade networking with support for IEC 61850 protocols, precision timing, and resilient Media Redundancy Protocol, Parallel Redundancy Protocol, and High-availability Seamless Redundancy (MRP, PRP, and HSR) architectures
- Improved security posture with visibility into connected assets, vulnerabilities, and behaviors
- Layered defense against cyber threats with AI-assisted microsegmentation enforced by switches
- Simplified maintenance and troubleshooting with least privilege remote access to OT assets
- Fast and simple deployment and management with Cisco Catalyst® Center and zero-touch provisioning

Cooling systems: Protect the thermal lifeline of AI

High-density AI racks generate enormous heat, making cooling a mission-critical system. Chillers, cooling distribution units (CDUs), pumps, valves, and water-treatment systems must exchange control data continuously to maintain safe operating conditions, reduce overcooling, and improve water usage effectiveness (WUE). Harsh mechanical environments, industrial ring topologies, and legacy controllers make conventional enterprise networking a poor fit.

Cisco Industrial Ethernet switches bring rugged, secure connectivity directly to cooling equipment—withstanding extreme temperature, humidity, and dust without requiring climate-controlled network cabinets. Industrial resiliency protocols maintain communications through network faults, while Cyber Vision identifies cooling assets, vulnerabilities, and anomalous activity. Integrated segmentation, secure remote access, and centralized management help contain threats, streamline maintenance, and simplify operations across facilities and sites.

Cisco's focused approach enables:

- Rugged, high-density DIN-rail and rack-mount switching for pumps, sensors, valve controllers, and CDUs
- Resilient ring networking to ensure continuous communications between cooling assets
- Automatic discovery of connected assets, vulnerabilities, and anomalous activity
- OT-aware segmentation that helps prevent threats from moving laterally across critical systems
- Zero-trust remote access for safer, faster maintenance and troubleshooting of cooling assets
- Rapid network expansion through Cisco Catalyst Center and zero-touch provisioning

Building management systems: Make the entire facility more resilient

The building management system (BMS) coordinates HVAC, environmental sensors, alarms, lighting, fire systems, and other facility automation. It must integrate equipment from multiple vendors, generations, and protocols while remaining continuously available. When these systems operate on unmanaged or fragmented networks, teams lose visibility of what is connected and security policies become inconsistent. Network failures can hide alarms, while weak segmentation can expose critical controls.

Cisco provides a secure, scalable network foundation for bringing BMS connectivity under consistent governance. Cisco Industrial Ethernet switches connect controllers and sensors of all types throughout the facility, while Cisco Catalyst Center centralizes provisioning, monitoring, and policy management. Integrated capabilities such as OT-aware asset intelligence, identity-based segmentation, and zero-trust remote access create layered protection without disrupting or redesigning sensitive control processes.

Cisco's focused approach enables:

- One Industrial Ethernet switching portfolio to connect all BMS equipment
- Faster deployment and simpler management with familiar tools such as Catalyst Center and the Cisco Meraki® dashboard from Cisco Cloud Control
- Automated discovery of BMS assets, vulnerabilities, and anomalous behaviors
- Robust security with AI-assisted microsegmentation enforced by switches
- Least-privilege remote access for safer, more efficient OT asset maintenance and troubleshooting

Physical security: Secure the facility and the network behind it

AI data centers require uninterrupted surveillance, perimeter monitoring, access control, and security operations across large campuses. Cameras and other security devices are often installed outdoors, on rooftops, at gates, or in unconditioned spaces where extreme temperatures, moisture, and dust challenge standard networking equipment. A rugged, resilient network is essential both to maintain physical-security coverage and to prevent compromised devices to become a pathway into facility or IT systems.

Cisco Industrial Ethernet switches combine high-performance rugged connectivity with high-wattage Power over Ethernet (PoE), simplifying the deployment of power-hungry and bandwidth thirsty cameras, access-control systems, and sensors. Identity-based network access control restricts each device to only the resources it needs, while Cisco's platform approach brings network and video operations together—helping teams deploy, monitor, and protect physical security infrastructure across facilities of any size.

Cisco's focused approach enables:

- Rugged and IP67-rated switching for equipment deployed in exposed locations
- Ultra-reliable wireless backhaul connectivity where fiber is not an option
- High-wattage PoE to easily deploy security devices through a single connection
- Simplified video monitoring and investigation with Meraki cameras and the Meraki Vision Portal
- Identity-based microsegmentation to help prevent unauthorized network access and lateral movement
- Centralized, scalable operations through familiar tools such as Catalyst Center and the Meraki dashboard from Cisco Cloud Control

Create a secure, resilient, and controlled network foundation for AI data centers

Industrial-grade resilience for continuous AI

Keep every gray space system connected with rugged Cisco Industrial Ethernet switches. Ensure these critical systems run uninterrupted with support for resilient network topologies, redundant paths, and resistance to harsh environmental constraints.

OT security embedded into the network

Turn Cisco switches into distributed cybersecurity equipment to protect the OT systems that run the data center. With Cisco Cyber Vision, the Cisco network sees all connected assets, identifies risks, enforces microsegmentation, and provides zero-trust remote access.

Industrial networking simplified for IT

Extend familiar Cisco tools, skills, and policies into gray spaces with Cisco IOS® XE, Catalyst Center, Meraki dashboard from Cisco Cloud Control. Use zero-touch provisioning, centralized assurance, and management to easily operate rugged networks at scale.

Engineered to achieve peak operational efficiency

Build a sustainable data center with energy-efficient Cisco Industrial Ethernet switches designed for low power consumption and a long operational life. Collect comprehensive telemetry to improve Power and Water Usage Effectiveness (PUE/WUE).

The Cisco advantage

For more than 20 years, Cisco has helped critical infrastructure organizations connect, secure, and modernize the operational systems that keep essential services running. Cisco brings that experience to AI data centers with an integrated portfolio of industrial switches, network management, embedded OT security, and secure remote access solutions purpose-built for demanding gray space environments.

Build secure, resilient gray space operations with Cisco today

Learn more about the anatomy of AI data centers in this blog and schedule a personalized demo with a Cisco data center expert for a deep dive into how our industrial networking solutions can serve the needs of your data center.

C45-6719919-00 09/26