Unleash the Power of AI in Midstream Oil and Gas Operations



© 2026 Cisco and/or its affiliates. All rights reserved.



Benefits

Accelerate AI deployments in production facilities

- Increase output and profitability with increased asset uptime with resilient communications
- Reduce deployment and operational costs with tools to automate setup and monitoring
- Improve safety and security of critical assets with embedded security capabilities in network infrastructure

AI-ready network and security infrastructure for oil and gas

Oil and gas companies remain focused on achieving profitable growth. To reach this goal, they are identifying optimizations to make pipeline assets more efficient and productive, while simultaneously enhancing the safety and security of their operations and personnel. While these have long been core objectives, the emergence of AI technology offers new potential to significantly improve safety, efficiency, and profitability. However, a primary obstacle to the deployment of AI workloads is the readiness of industrial networks. These new workloads impose increased demands on the network involving performance, power, reliability, and security. At the same time, scrutiny of cybersecurity and compliance requirements is increasing.

AI technology in the oil and gas sector requires vast amounts of data, much of which originates from field assets and operations. Cisco's industrial and enterprise networking, security, and management tools provide the critical capabilities necessary to help customers connect, secure, and operate their widely distributed assets in support of their AI applications. This paper outlines Cisco's solutions for industrial networking and security within midstream oil and gas operations, pipelines, and transportation.

© 2026 Cisco and/or its affiliates. All rights reserved.

Business drivers

Deploying AI-ready industrial networks for midstream operations provides significant benefits, including:

- **Maximizing revenue and profit:** Increasing the uptime of critical assets through resilient and secure connectivity.
- **Optimizing processes and assets:** Supporting digitization initiatives and enabling the seamless flow of data into AI applications.
- **Enhancing safety:** Ensuring reliable communication with field assets and personnel and reducing the need for field excursions and truck rolls through secure remote access.
- **Being able to scale and automate management:** Using consistent IT management platforms to deploy, monitor, and maintain networks.
- **Strengthening security:** Protecting critical pipeline infrastructure to ensure business continuity and compliance with evolving regulatory requirements.

© 2026 Cisco and/or its affiliates. All rights reserved.

Key challenges

Midstream assets are typically distributed across vast geographical areas, often located in remote and inhospitable environments. Maintaining resilient communication with these assets is critical yet presents significant challenges:

- **Remote locations that lack infrastructure and services:** Assets are frequently located where power and communications are expensive and hard to find. For example, many sites run on solar power and need low-powered infrastructure. Or a site may have access only to expensive low-bandwidth cellular or satellite wireless communications, requiring edge data processing to efficiently gather and send data.
- **Harsh conditions:** Equipment must be ruggedized to withstand extreme temperatures, vibration, shock, and hazardous (explosive) environments, as well as limited airflow. Hardware must be specifically designed to perform reliably under these conditions.
- **Lifecycle longevity:** Infrastructure is expected to remain operational for over a decade with minimal onsite maintenance. Solutions that reduce the need for in-person updates significantly lower operating costs, improve safety, and mitigate risk.
- **Operational expertise:** Field personnel are highly trained in operational roles but may not possess specialized IT or security expertise. Consequently, simplicity, automation, and robust remote management tools are critical for the effective deployment and maintenance of field network and security infrastructure.

Key use cases

Backhauling data

Pipeline operations are run out of centralized centers where SCADA applications help operators monitor and maintain the system. The applications need data from the pipeline assets (valves, motor, sensors, controllers, etc.) to supply the SCADA system. Additionally, ever more data is needed to drive optimizations and improvements from AI applications. Handling this data requires a resilient, multimodal communication architecture that integrates wired, cellular, wireless, and satellite connectivity. Cisco's industrial routers and access points are engineered to thrive in these demanding conditions, offering versatile backhaul capabilities while helping ensure simplified deployment and management.

Secure remote access

Secure remote access allows operators to manage these systems more efficiently and safely than when dispatching field personnel, thereby increasing uptime, reducing operational costs, and minimizing safety risks. Given the critical nature of these assets, remote access must adhere to stringent security standards, which is also an increasingly important compliance requirement. Cisco's industrial network infrastructure supports Cisco® Cyber Vision's auditable, role-based, and time-bound secure remote access, providing a robust, highly secure connection through our cloud-based head-end.

Edge operations

Communications for remote midstream assets are often expensive, and bandwidth constrained. Nonetheless, collecting and processing field data remains critical to delivering business value. To reduce the costs and complexity associated with transmitting raw data over backhaul links, it is essential to deploy data collection and processing applications at the network edge. Cisco's network infrastructure provides integrated IOx compute services to host these applications directly on edge devices or to provide high-speed connectivity to industrial PCs (IPCs) operating within the edge network.

Worker productivity

Even with secure remote access capabilities, operational personnel must occasionally visit field sites. To maximize productivity during these visits, staff require seamless access to local systems, enterprise networks, and the internet. Cisco's industrial access points address this need by integrating Cisco Ultra-Reliable Wireless Backhaul and Wi-Fi into a single infrastructure, helping ensure robust, high-performance connectivity for field workers.

© 2026 Cisco and/or its affiliates. All rights reserved.

What is critical for “AI-ready” midstream networks?

It is no longer sufficient for industrial networks to just support industrial applications, such as industrial control and SCADA systems, in the field. These industrial networks need to provide the ability to collect, process, and backhaul much more information and data from the industrial assets to feed into not just the SCADA systems but also the AI-driven predictive maintenance and other applications that help increase uptime, improve product quality, and enable safer operations. The networks need to operate in harsh, remote conditions where physical access comes at a cost. They need to be easy to deploy and manage, often by operators with limited networking and security backgrounds. And with increased access to industrial assets, the network has a key role in providing improved cybersecurity.

An AI-ready industrial network has the following requirements:

- **Ruggedized connectivity** is needed in harsh, remote locations, with the ability to backhaul via cellular, satellite, and fiber communications.
- With uptime being so critical, the network infrastructure must be highly **reliable, resilient, and available** to keep the operations going.
- Network infrastructure must be **easy to deploy and manage** to minimize deployment of field technicians and, when working in the field, to simplify the tasks that need to be performed.
- The network must be **secure,** providing visibility, protection, detection, and response for industrial automation systems as more AI-driven access to the devices and data is needed.
- **Edge computing** is needed to collect and process data from field assets to be backhauled over WAN communications with sometimes limited bandwidth.

Ruggedized connectivity in remote locations

Pipelines run through some of the harshest and most remote locations. Equipment, including the network infrastructure, must be designed and tested to run in those conditions for extended periods of time with minimal failures and must be easy to deploy, replace, and manage. In addition, connectivity to those locations can vary widely, involving satellite, cellular, or fiber. The assets mostly connect via Ethernet, but many also use serial buses.

Cisco’s industrial network infrastructure—switches and routers—was designed to operate and connect in these conditions, withstanding extreme temperatures, shock, vibration, low power, corrosion, and electromagnetic interference and resisting ingress of particles and liquids. The switches and routers are modular, meaning that the same base unit can be configured with various cellular (LTE/4G, 5G, 5G Red Cap, etc.), Ethernet, and satellite connectivity options from the remote locations. The new 5G Red Cap (reduced capacity) Pluggable Interface Module (PIM) helps maintain lower operational costs for low SCADA traffic use cases. And the new compact Cisco IR1001 Rugged Secure Router is designed to operate using less than 6 watts—helpful in locations where only solar energy is available.

© 2026 Cisco and/or its affiliates. All rights reserved.

Reliable, resilient, and available

Uptime is a key consideration for any production environment. Industrial applications often operate continuously for weeks, months, or years, and any downtime, especially unplanned, results in significant loss of production output and costs, directly impacting the bottom line. The network infrastructure is critical to those industrial applications. Therefore, resiliency mechanisms work at all levels of the network: in the access networks where the devices connect and in the backhaul/WAN networks that connect the field to the enterprise. For IT considerations, minor network disruptions measured in hundreds of milliseconds may seem minimal, but those disruptions in an Industrial Automation and Control System (IACS) may result in significant outages and could bring production to a halt.

The backhaul WAN networks are also critical to operations. Cisco industrial routers support resilient WAN connectivity. By integrating SD-WAN, the network gains intelligent path steering and automated failover, helping ensure that critical data backhaul and safety monitoring remain active even if a primary link degrades or fails. This synergy simplifies management for operators with limited on-site IT resources while delivering the secure, persistent connectivity essential for maintaining operational uptime across dispersed midstream assets.

Lastly, Cisco's industrial network infrastructure was built to operate for extended periods in harsh production environments. High Mean Time Between Failures (MTBF) values are a hallmark of their design, reflecting the use of high-quality, industrial-grade components engineered to withstand extreme temperatures, shock, vibration, and electromagnetic interference with very high MTBF.

Easy to deploy and manage

Midstream assets are often deployed and managed by non-IT personnel with limited networking expertise. For these scenarios, the network infrastructure must be easy to deploy and scale onto a large number of assets. The network devices are designed for easy, zero-touch deployment and replacement, using either USB or SD-Flash to deploy, update or replace the devices, minimizing the level of skill needed, reducing truck rolls, and speeding deployment.

Cisco's routing and switching and management tools also support key software-defined functions with zero-touch deployments, automated network configurations/upgrades, and monitoring that identifies issues and uses AI capabilities to prioritize and recommend fixes. Once connected, Cisco's software-defined management platforms, Catalyst® Center and Software-Defined WAN (SD-WAN), support automated deployment, configuration, management, and AI-driven problem resolution.

Cisco Catalyst Center is the AI-powered network management and automation platform that serves as the centralized controller for network operations. It simplifies network management by providing a single dashboard for design, policy definition, provisioning, assurance, and platform integration. Catalyst Center automates device deployment and configuration, enforces zero-trust policies, and delivers analytics and visibility across wired and wireless environments.

SD-WAN is a technology that simplifies the deployment, operation, and management of wide-area networks by using software to control network connectivity and traffic management across diverse WAN connections such as broadband internet, 4G, LTE, 5G or Multiprotocol Label Switching (MPLS). It enables enterprises to connect distributed assets such as well-heads, pipelines, processing facilities, and operations centers over large geographic distances more efficiently and securely. SD-WAN improves application performance by dynamically routing traffic over the best available path, reduces operational costs by leveraging lower-cost links, and enhances security with integrated threat protection and segmentation.

© 2026 Cisco and/or its affiliates. All rights reserved.

Industrial cybersecurity

Cybersecurity has always been a challenging consideration for midstream oil and gas systems. Most industrial automation systems have limited security capabilities, lacking strong authentication and encryption. Often, industrial automation technology is deployed and operated for long periods of time and rarely, if ever, updated with software and security patches. Many systems operate with outdated and/or unsupported products and technology. And the additional access required to drive AI applications only increases the threat surface.

Cisco provides an unparalleled set of cybersecurity capabilities tailored for industrial midstream systems, including:

- **Full visibility into connected assets, vulnerabilities, and activities.** Cisco Cyber Vision revolutionizes how you gain comprehensive visibility into your OT environment. It embeds Deep Packet Inspection (DPI) and safe active discovery capabilities into your Cisco switches and routers, turning your entire industrial network into a powerful visibility sensor.
- **Secure WAN connectivity to protect distributed pipeline assets.** Cisco industrial routers integrate the best of SD-WAN networking with built-in next-generation firewall (NGFW) features, malware protection, intrusion detection and prevention (IDS/IPS), and Virtual Routing and Forwarding (VRF) to segment critical SCADA traffic.
- **Secure remote access with self-service zero-trust network access made for OT with Cyber Vision.** Cisco offers a purpose-built ZTNA cloud service for industrial needs. It makes it simple for OT teams to grant remote access.

For many Oil and Gas customers, cloud-based technologies are considered a security risk for operational critical technologies. Except for the remote access capability, all the Cisco software is designed to operate on-premises, enabling strict segmentation between OT and IT operations.

Edge computing

Backhaul communications can be expensive and data-rate driven. Yet, there is a lot of important data to be coming from the field sensors and assets. To save on operational expenses, it's often critical to collect and analyze data streams near where they are generated. Cisco's industrial routing and switching products offer a range of compute resources to run data collection applications on the network infrastructure in the field. The deployment, configuration, and monitoring of the applications for routers can be managed in Cisco's SD-WAN, and routers/switches in Catalyst Center.



© 2026 Cisco and/or its affiliates. All rights reserved.

Midstream oil and gas reference architecture

The AI-ready industrial network reference architecture shows how midstream assets interact with industrial automation applications. The solution supports connecting pipeline assets via wired, cellular, and satellite connectivity.

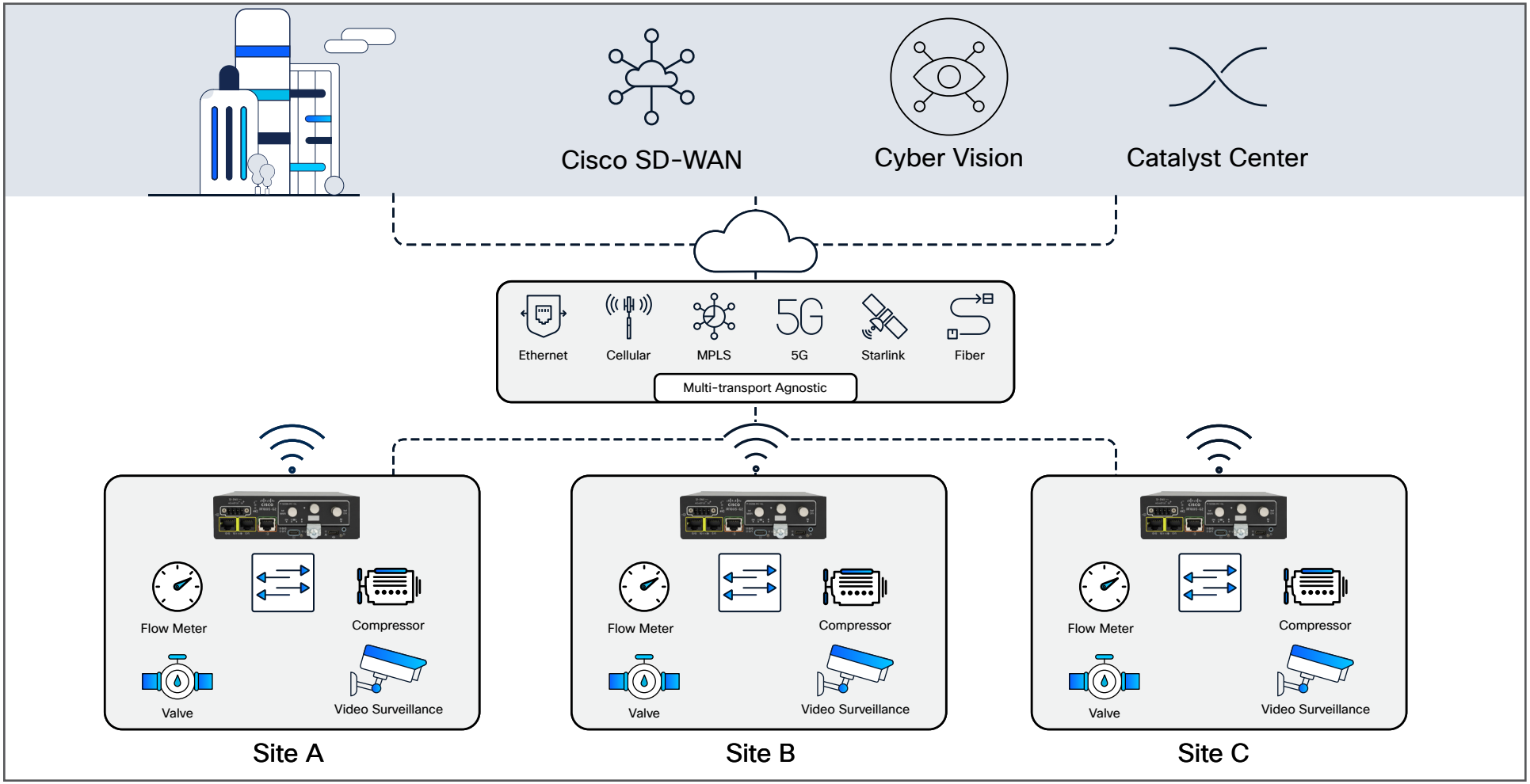


Figure 1. Midstream oil and gas architecture

© 2026 Cisco and/or its affiliates. All rights reserved.



Cisco Catalyst IE3100

Cisco IE3500 (with 4-port 2.5Gb 4PPoE expansion module)

Cisco IE3500H

Cisco Catalyst IE9300

Figure 2. Cisco industrial switches

The following are the key Cisco components:

Cisco Industrial Ethernet (IE) switches: Available in DIN-rail, IP67-rated, and rack-mount form factors, the Cisco Catalyst IE9300, IE3500, and IE3100 Rugged Series and the Catalyst IE3500 Heavy Duty Series switches deliver high-speed ports including 1 Gbps, 2.5 Gbps, and 10 Gbps options to support demanding industrial AI applications, and offer high-wattage Power over Ethernet (PoE) (up to 90W per port, up to 720W total per switch), enabling flexible deployment of cameras and sensors. They integrate robust security with Cisco Trust Anchor, TrustSec segmentation, and Cyber Vision for zero-trust remote management of connected assets. These switches offer high-capacity, low-latency Layer 2 and 3 switching, all managed by Cisco Catalyst Center.

Cisco IR1000

Cisco IR1100

Cisco IR1800



Figure 3. Cisco industrial routers

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco industrial routers are rugged, modular platforms designed to provide secure, reliable, and scalable connectivity in harsh industrial environments. These routers support a variety of WAN connectivity options including Ethernet, 5G, 5G Red Cap, LTE (public and private). They offer built-in edge compute resources and advanced multilayer security features such as next-generation firewall, intrusion prevention, malware protection, and integrated Cisco Cyber Vision for OT security visibility. The portfolio includes models like the ultra-compact, low-power Cisco IR1000 Rugged Series Secure Routers, the compact and resilient Cisco Catalyst IR1100 Rugged Series Routers, and the versatile Cisco Catalyst IR1800 Rugged Series Routers. These routers support multiple management tools, including Cisco Catalyst SD-WAN and Catalyst Center, allowing IT and OT teams to manage connected operations at scale. Cisco Industrial IoT routers help ensure continuous, secure connectivity and edge computing capabilities to optimize operational efficiency and security in demanding upsteam/midstream environments.

Cisco Cyber Vision: In an era of increasing cyberthreats, security cannot be an afterthought. Cisco integrates security directly into the network fabric, helping ensure that your vision systems are protected without compromising production availability.

Cisco Cyber Vision combines the three OT security capabilities every industrial organization needs into a single, network-native solution: continuous visibility into your OT security posture to help reduce the attack surface, AI-assisted network segmentation to protect industrial operations, and secure remote access to control risks from remote experts.

With Cyber Vision you can identify every camera, IPC, and server on the network and flag any anomalous behavior. Segmentation with Cyber Vision allows you to microsegment the network to help ensure that a camera can communicate only with its designated vision server. If a device were to become compromised, the threat would be unable to move laterally to other critical assets or production lines.

Systems integrators and vendors often need remote access to tune vision systems. Cyber Vision allows for auditable, role-based, and time-bound remote connections, eliminating the risk of uncontrolled access.

Cisco Catalyst Center is a powerful network management system that leverages AI to connect, secure, and automate network operations. It simplifies the management of Cisco Catalyst network infrastructure, including IE switches, helping ensure a consistent user experience across wired and wireless networks.

Cisco SD-WAN is a on-premises or cloud-managed WAN management solution. SD-WAN manages any type of connection, whether it's the internet, broadband, MPLS, 5G/LTE, or satellite. It automates provisioning, configuration, and management, enabling centralized control with seamless policy enforcement across remote devices such as routers and firewalls. Cisco SD-WAN offers AI-driven insights and predictive path recommendations to proactively optimize application traffic and prevent disruptions. It is built on a zero-trust security model with identity-based microsegmentation and centralized policy enforcement, providing comprehensive protection from premises to cloud and edge.

© 2026 Cisco and/or its affiliates. All rights reserved.

Summary

The AI-ready industrial network solution provides a network and security platform on which midstream oil and gas companies can quickly, resiliently, and securely deploy AI/ML applications. The Cisco solution overcomes customers' barriers to AI/ML deployments: accessing the critical data, securing production systems, and simple, scalable networking solutions. The solution provides a proven blueprint for connecting AI/ML and SCADA applications to remotely located pipeline assets and devices, improving industrial security, data access, and operating reliability. Following this best practice blueprint with Cisco market-leading technologies will help speed deployment time, decrease risk and complexity, and improve security and operating uptime.

Talk to a Cisco sales representative or channel partner and visit www.cisco.com/site/us/en/solutions/industries/energy/oil-gas/index.html to learn more.



© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C22-6543402-00 11/26