# Full-Stack Software-Defined Manufacturing – Cybersecurity AI Edge-to-Multicloud Connectivity

## Accelerating AI-powered autonomous operations: A comprehensive cybersecurity solution that unifies and protects IT and OT manufacturing assets

# Value statement

The Cisco and Rockwell Automation Full-Stack Software-Defined Manufacturing solution enhances production quality, efficiency, and plant resilience by offering operational visibility and preparing for future AI insights and autonomous operations, helping businesses stay competitive as they evolve.

Cisco® Industrial Threat Defense is a preintegrated and modular solution offering all the security capabilities you need to protect, detect, and remediate across IT and OT environments and is a critical component of the Full-Stack Software-Defined Manufacturing reference design.

It provides a regulatory-compliant cybersecurity strategy from edge to cloud, encompassing not only network security and intrusion detection, but also robust recovery capabilities, protocol-level data privacy, and advanced endpoint protection—crucial for maintaining plant availability, ensuring trust across the manufacturing ecosystem, and supporting ongoing innovation and growth.

### Visibility and asset management

- Simplify OT security: Cisco's embedded sensors and automated discovery cut complexity and cost, while integrations with platforms like Rockwell Automation's Verve and FactoryTalk® AssetCentre enhance asset management capabilities.
- Enable comprehensive lifecycle management: Extend visibility and control with recovery planning, product vulnerability notifications, and firmware revision management for OT assets—helping ensure proactive risk mitigation and operational resilience.
- Unify IT/OT security: Cisco SecureX® correlates Cyber Vision insights with enterprise data for faster, more effective threat response.

### Segmentation and access control

- Contain breaches: Cisco's ISA/IEC 62443-complaint architecture segments your network, limiting the impact of cyber incidents.
- Deploy dynamic security: Adapt security policies in real time with Cisco TrustSec®, enabling flexible and secure software-defined manufacturing.

### Threat detection and response

- Accelerate incident response: Cisco SecureX unifies IT and OT security, enabling faster investigations and remediation.
- Defend against known and unknown threats in your software-defined manufacturing environment with Cisco's comprehensive approach.

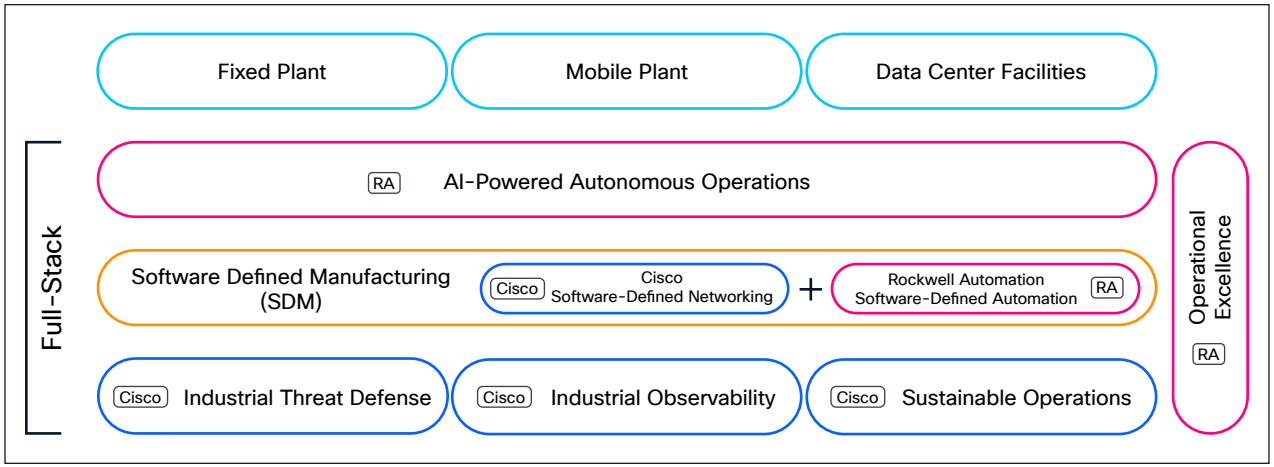



Figure 1. Components of the Full-Stack Software Defined Manufacturing solution

## Overview

Software-Defined Manufacturing (SDM) and Operational Technology (OT) digitization require seamless communications with IT and cloud resources. As a result, industrial security solutions must now span and unify OT and IT domains. They must also be deeply integrated within industrial networks to gain full visibility and enforce policies at the lowest levels of the infrastructure.

As manufacturers increasingly rely on interconnected systems, cloud-based platforms, and data-driven automation, the attack surface expands exponentially. Legacy OT systems, designed without security in mind, become vulnerable entry points for sophisticated cyberthreats. The traditional air-gapped approach is no longer sufficient, requiring a new paradigm that integrates security into the very fabric of the manufacturing environment. The complexity of managing diverse OT assets, coupled with the need for real-time threat detection and response, demands a holistic and adaptive security architecture.

- Protect what matters most and maintain production uptime with Cisco Industrial Threat Defense.
- Uncover your industrial cybersecurity posture: Easily inventory your OT/ICS assets and their behaviors with solutions that use your network as a sensor to provide full visibility at scale—and the insights you need to reduce the attack surface.
- Control and secure OT remote access: With easy-to-use, cloud-delivered secure remote access built into our network equipment, you avoid shadow IT—and your OT teams can manage industrial assets from anywhere.
- Protect operations: Enforce ISA/IEC62443 zones and conduits and prevent threats from spreading. Use your network as the enforcer to easily implement a zero-trust microsegmentation strategy.
- Find and block threats across IT and OT: With OT insights in your IT security tools, you can detect, investigate, and resolve threats across IT and OT—all from a single console.

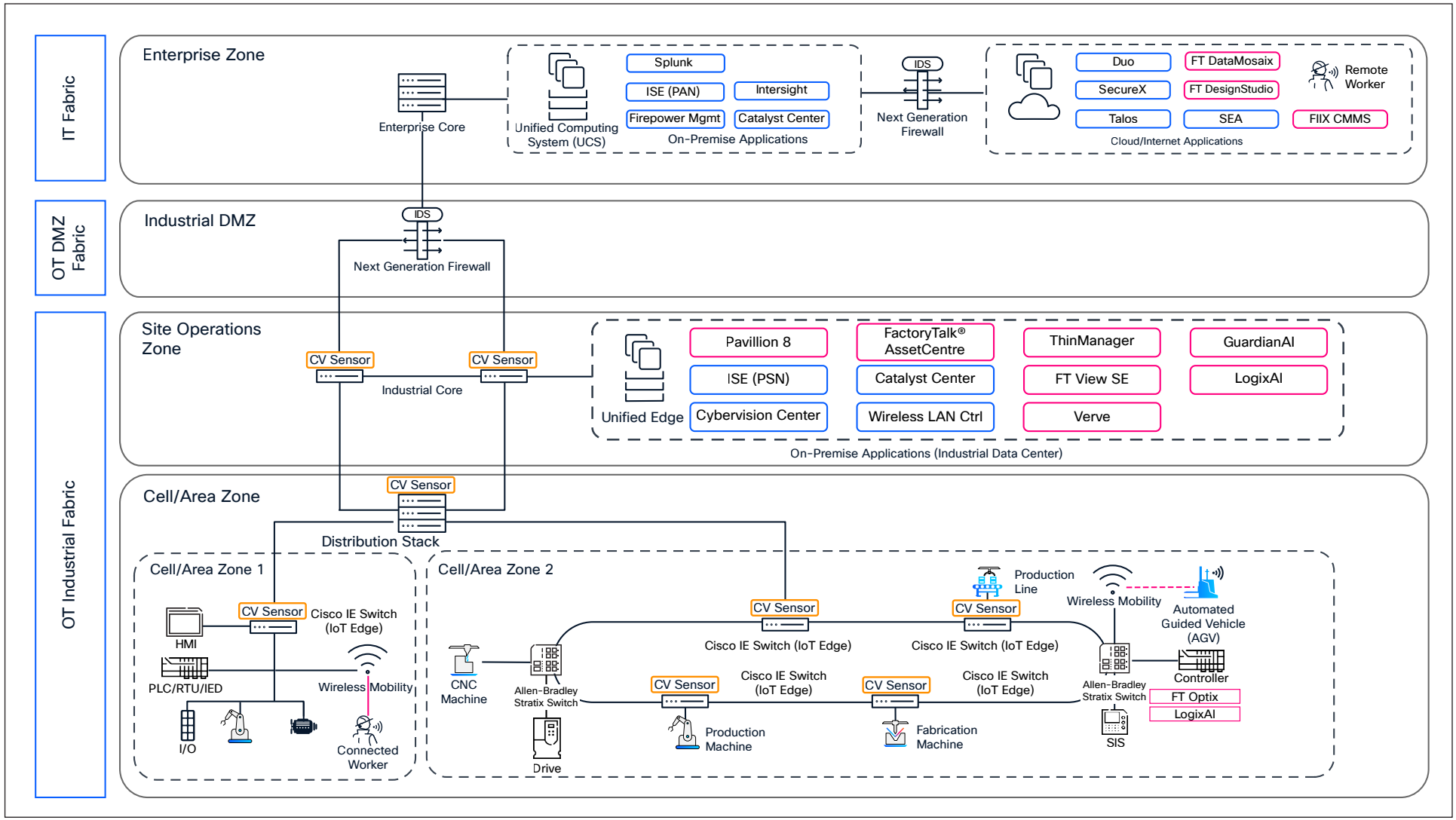



**Figure 2. Full-Stack Software-Defined Manufacturing reference design**

## Benefits

- Gain real-time insights into all OT assets, communications, and vulnerabilities, enabling proactive monitoring and improved operational reliability.
- Minimize the risk of cyberattacks and limit the impact of security incidents through robust network segmentation and access control.
- Identify and block malicious activity in real time, preventing disruptions to production and helping ensure business continuity.
- Accelerate investigations, automate response actions, and minimize the impact of security incidents.
- Reduce the burden on security teams and streamline security operations through unified and integrated architecture.



# Comprehensive cybersecurity for critical infrastructures and industrial operations

As the manufacturing sector is embracing new technologies such as Software-Defined Manufacturing (SDM) to bolster its infrastructure resilience and reliability, a recent report by Cisco on the state of industrial networking has identified cybersecurity as the biggest challenge in operating and maintaining industrial networks. Obstacles to protection include asset discovery, digital transformation, legacy infrastructure, and an overstretched workforce.

Customers operating in the manufacturing sector face an increasingly complex and threatening cybersecurity landscape, necessitating a robust and integrated security solution for their Software Defined Manufacturing environments. The following key market trends are driving this need:

- A continued push toward digital transformation to connect previously isolated OT systems to enterprise networks and the cloud. This increased connectivity expands the attack surface and creates new vulnerabilities.
- The pursuit of autonomous operations, driven by the need for greater efficiency and productivity. Securing these autonomous systems, which rely heavily on data-driven automation and interconnected systems, is crucial to prevent disruptions and ensure reliable operation.
- Sophisticated attacks, including ransomware, supply chain attacks, and targeted intrusions, that are increasingly targeting OT and Industrial Control System (ICS) environments. These attacks can have devastating consequences, including production downtime, equipment damage, safety incidents, and financial losses.
- Increasing regulatory pressure on manufacturing organizations to comply with cybersecurity standards and regulations, such as the ISA/IEC 62443, NIST, and country regulations and guidelines. Failure to comply can result in significant fines, legal liabilities, and reputational damage.

Finally, there is a growing need to support future innovation and growth, onboarding of new OT vendors, and reduced complexity, leading to:

- Improved plant resilience, availability, and uptime
- IEC62443, TSA, and NIST compliance
- Support for future innovation and growth
- Reduced overall complexity of the system

## How it works

Cisco Industrial Threat Defense is a comprehensive and highly modular OT security solution that uses the industrial network as the fabric to easily enable advanced OT security capabilities at scale. It's a platform that unifies security across IT and OT domains to help detect advanced threats and orchestrate the response, protecting the global enterprise.

Cisco Industrial Threat Defense is a preintegrated and modular solution offering all the security capabilities you need to protect, detect, and remediate across IT and OT environments:

- Cisco Cyber Vision: Easily gain visibility into OT and ICS assets at scale. Understand your OT security posture, detect threats, and drive cybersecurity best practices.
- Cisco Vulnerability Management: Adopt a risk-based approach to vulnerability management and prioritize patching with real-world exploit data and predictive modeling.
- Cisco Secure Endpoint: Protect OT workstations, control USB device use, and detect threats sooner with advanced endpoint protection powered by Cisco Talos® intelligence.
- Cisco Secure Equipment Access (SEA): Control remote access to your OT/ICS assets with Zero-Trust Network Access (ZTNA) that's made for OT and is easy to deploy at scale.
- Cisco Secure Firewall: Build your Industrial Demilitarized Zone (IDMZ), restrict communications within the industrial network, and block zero-day attacks to protect your OT and IT networks.
- Cisco Identity Services Engine (ISE): Enforce ISA/IEC62443 zones and conduits and control access to critical OT assets with a zero-trust framework.
- Cisco Security Service Edge (SSE): Enable secure connectivity to cloud resources, control traffic across sites, and expose shadow IT.
- Cisco Extended Detection and Response (XDR) and Splunk®: Get a unified view of IT and OT data to correlate events, detect advanced threats, and orchestrate response across your security stack.
- Cisco Talos: Beat OT cyberthreats with our industry-leading threat intelligence and help from expert threat hunters to prepare, test your defense, respond, and recover from a breach.

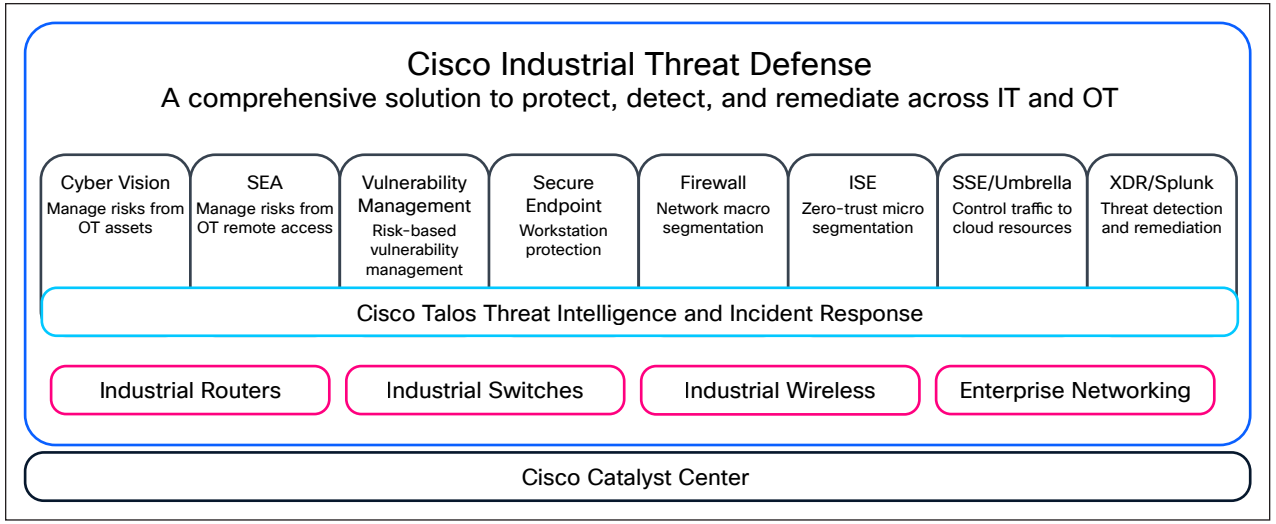



**Figure 3. Cisco Industrial Threat Defense**

Key capabilities of Cisco Industrial Threat Defense include the following:

- Gain OT visibility at scale: The network automatically inventories industrial assets, their communication patterns, and their security posture.
- Protect operations with network segmentation: OT visibility lets you easily build zones and conduits enforced by networking equipment.
- Secure remote access to OT assets: Control remote access from vendors and contactors with ZTNA designed for OT.
- Detect advanced threats faster: Eliminate gaps with a unified view of IT and OT security data, advanced AI/ML detection models, and OT-specific threat intelligence.
- Unify your defense: Better protect the global enterprise with out-of-the-box integration across your security stack, enabling advanced response orchestration.

Secure your OT/ICS with your existing setup:

- Enjoy OT cybersecurity built into switches and routers: Use your network as a sensor and enforcer. Deploy ICS security that sees more, does more, and scales simply.
- Use your IT security solutions to protect industrial operations: Take advantage of your Cisco security solutions to protect your OT/ICS as well as your IT.
- Keep your existing security tools: Integrate third-party tools. Cisco Industrial Threat Defense is modular and works with what you already have.

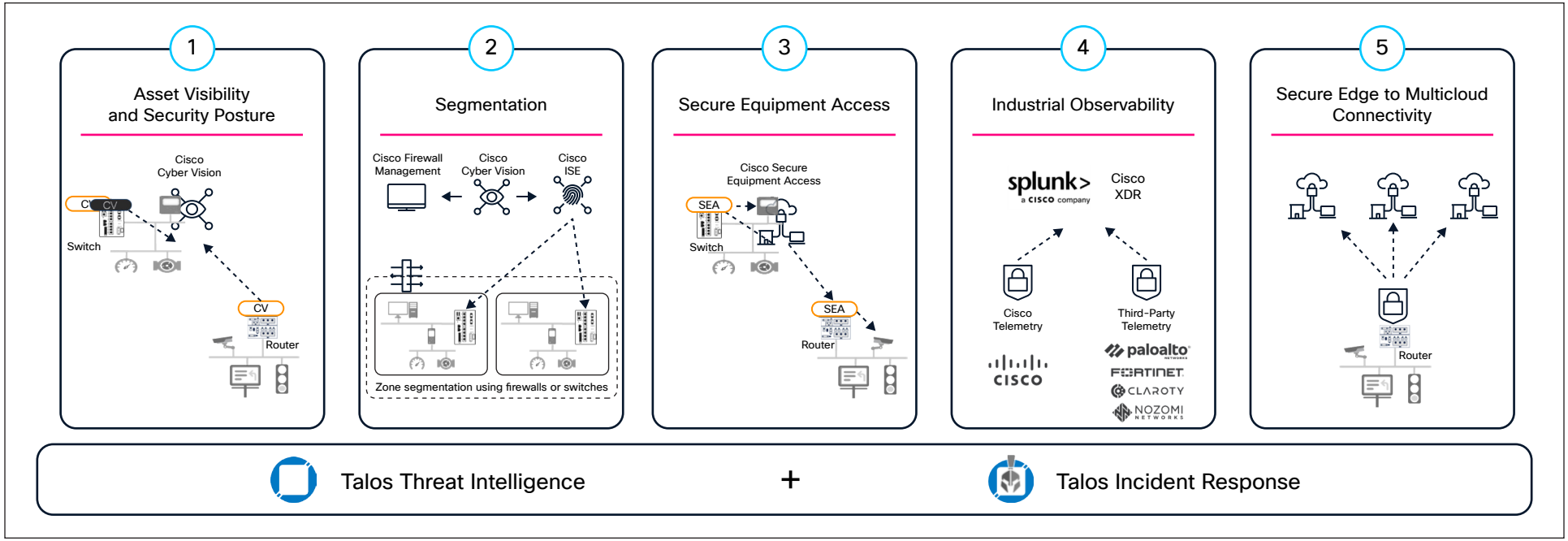



**Figure 4. Capabilities of Cisco Industrial Threat Defense**

"Manufacturing is the sector most targeted by cyber criminals. In response, firms are investing in cybersecurity solutions to protect increasingly connected infrastructure and smart factories, with 86% maintaining or increasing OT expenditure.

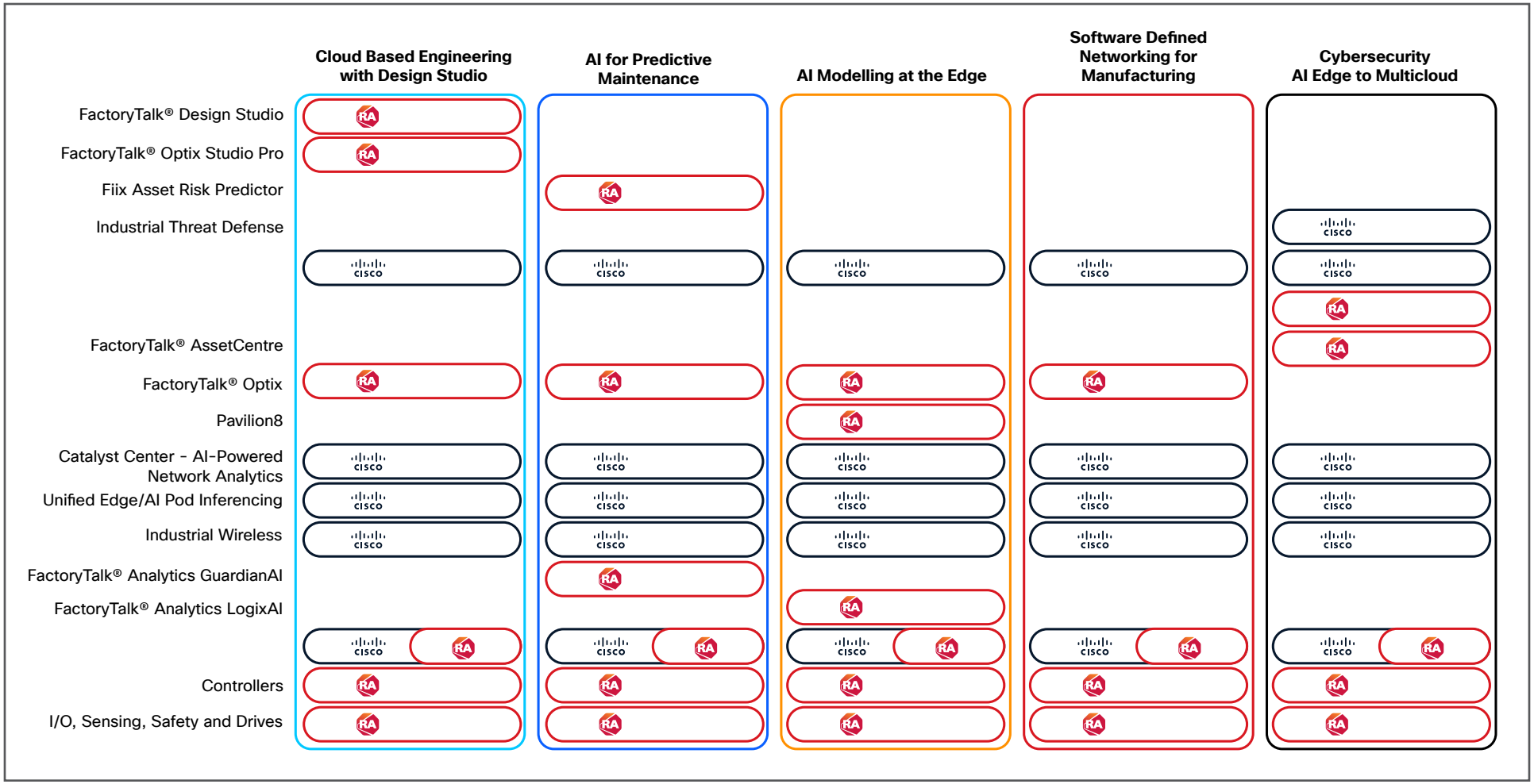
- Cybersecurity is the #1 challenge faced when running industrial infrastructure.
- Twenty percent more respondents said cybersecurity compliance was extremely important in their operational network this year compared to last year.
- Cybersecurity is the #1 investment priority for the next one to two years."

2024 State of Industrial Networking Report for Manufacturing, Cisco

## Use cases

Table 1. Use cases for Cisco Industrial Threat Defense

| Use case | Description and benefits |
|---|---|
| **Life sciences manufacturing** | Protect sensitive lab and production data, help ensure regulatory compliance (e.g., FDA, GxP), and secure remote access to critical systems. |
| **Mining** | Enable ruggedized network security and wireless mesh connectivity for remote operations, helping ensure safe and resilient autonomous mining systems. |
| **Tire manufacturing** | Secure high-speed production lines and quality control systems, and prevent downtime with predictive threat detection and endpoint protection. |
| **Data center** | Integrate Cisco ACI® and Nexus® platforms for secure segmentation, workload mobility, and hybrid cloud protection. |
| **Food and beverage manufacturing** | Comply with food safety standards, protect processing and packaging systems, and secure supply chain data. |
| **Oil and gas** | Protect sensitive lab and production data, help ensure regulatory compliance (e.g., FDA, GxP), and secure remote access to critical systems. |



## Forrester names Cisco a Leader in OT cybersecurity

Forrester praises Cisco Industrial Threat Defense as a comprehensive OT security solution that's simple to deploy at scale and that unifies IT and OT security to better protect critical infrastructures.

For additional information, visit https://blogs.cisco.com/security/cisco-named-a-leader-in-the-forrester-wave-ics-security

## The future of industrial network security

Explore IDC recommendations for building future-ready industrial operations as you accelerate OT digitization. Key starting points include embedding OT security into the network, fostering collaboration between IT and OT teams, and unifying visibility across IT, OT, and cloud.

For additional information, visit https://www.cisco.com/site/us/en/products/security/industrial-security/idc-infobrief.html



# How Rockwell Automation and Cisco provide expertise to customers

Rockwell Automation and Cisco bring together their respective strengths in OT and IT to offer comprehensive solutions for modern manufacturing challenges. Here's how they provide their expertise to customers:

Converged Plantwide Ethernet (CPwE): Rockwell Automation and Cisco have developed the CPwE architecture, a set of tested and validated designs that help manufacturers build a secure, scalable, and resilient network infrastructure. This architecture integrates IT and OT systems, helping ensure seamless connectivity and robust security.

LifecycleIQ® Services: Rockwell Automation's LifecycleIQ® Services, enhanced by Cisco's Cyber Vision solution, offer advanced cybersecurity threat detection and response capabilities. These services help manufacturers protect their networks from cyberthreats and ensure business continuity.

Digital transformation solutions: Together, Rockwell Automation and Cisco provide solutions that support digital transformation initiatives. These solutions include industrial IoT, predictive analytics, and smart manufacturing technologies that enhance operational efficiency and agility.

Industry-specific expertise: The partnership offers tailored solutions for various industries, including water and wastewater, food and beverage, life sciences, mining, and oil and gas. This industry-specific expertise helps ensure that the solutions meet the unique challenges and regulatory requirements of each sector.

Training and support: Rockwell Automation and Cisco provide extensive training and support to help customers implement and manage their network infrastructure. This includes hands-on training, virtual labs, and access to a wealth of resources and documentation.

## Learn more

For additional information, visit Cisco and Rockwell Automation - Cisco

For additional information on Cisco software-defined networking, visit Software-Defined Networking (SDN) Definition - Cisco

For additional information on Cisco Catalyst™ Center, visit Cisco Catalyst Center Network Management - Cisco

For additional information on Cisco Industrial Threat Defense, visit Products - Cisco Industrial Threat Defense At a Glance - Cisco

## The Cisco and Rockwell Automation Advantage

Cisco and Rockwell Automation have been global strategic partners for over 18 years, leading the digital transformation for the connected enterprise by bringing industrial automation together with industrial networking and security solutions. Today, Cisco and Rockwell Automation are once again leading change in the industrial automation landscape as it evolves to embrace full-stack Software Defined Manufacturing and enabling the shift from automation to autonomy.

Cisco is a global leader in IT networking and cybersecurity, with decades of experience securing enterprise networks, bringing a deep understanding of IT security principles, technologies, and best practices.

Rockwell Automation is a global leader in industrial automation and control systems, with unparalleled expertise in OT environments, industrial protocols, and manufacturing processes.

Only Cisco and Rockwell Automation can deliver the full-stack combination of AI-enabled autonomous operations, software-defined manufacturing, Industrial Threat Defense, industrial observability, sustainable operations, and operational excellence.



C22-5814050-01 08/26