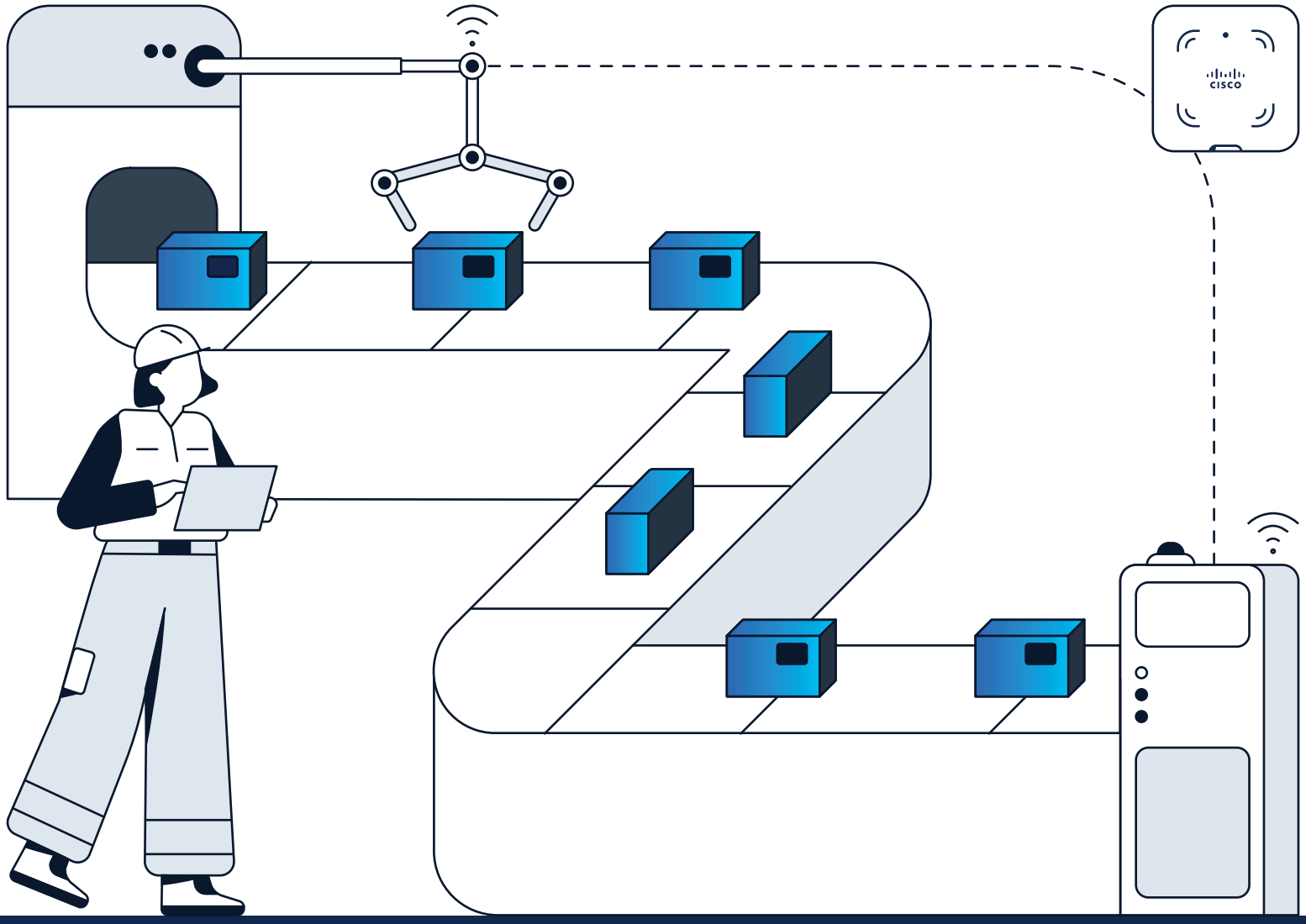
Cisco Solutions for Smart Manufacturing



Manufacturing solutions overview and benefits

In their pursuit of Industry 4.0's potential, manufacturers are embracing digitization. This digital transformation empowers them to enhance efficiency, gain valuable insights, and safeguard their operations. Industrial IoT, AI, robotics, and Zero-Trust cybersecurity are key technologies facilitating these advancements. To fully realize these benefits, a robust industrial network infrastructure is crucial. This network must be scalable, secure, and seamlessly connect to enterprise systems.

Cisco solutions for manufacturers

Cisco® empowers manufacturers to achieve their smart manufacturing goals by providing high-performance and resilient industrial networks. Our Infrastructure is designed and tested to operate in a range of environmental conditions where Industrial applications exist. Cisco industrial networks leverage our established enterprise network architecture, and act as the backbone for collecting, securing, managing, and analyzing manufacturing data. With a secure integration with the IT infrastructure, these networks allow data to flow in and out of factories seamlessly, enabling manufacturers to make informed, data-driven decisions that improve productivity, quality, and innovation while maintaining security and operational resilience.

Moreover, Cisco industrial networking equipment utilizes the same tools that IT teams already know and trust, thereby minimizing training requirements and streamlining network deployment, management and security.

Build a robust foundation for smart manufacturing

Cisco rugged, secure, and resilient Industrial Ethernet (IE) switches constitute the foundational element of industrial networking infrastructure. These versatile switches offer deployment flexibility with DIN-rail, rackmount, and IP67-rated wall-mount options. Designed for harsh industrial environments, IE switches are ruggedized to withstand demanding conditions. They leverage the well-established and extensible Cisco Internetwork Operating System (Cisco IOS®) XE familiar to network administrators. IE switches are supported by Cisco Catalyst Center network management system, which automates deployment and assures performance. Furthermore, IE switches provide comprehensive support for industrial communication protocols, including CC-Link, EtherNet/IP, PROFINET, and Modbus. They also facilitate network resilience through redundancy protocols such as Resilient Ethernet Protocol (REP), Media Redundancy Protocol (MRP), and Device Level Ring (DLR).

Unify security with networking

Cisco Industrial Ethernet (IE) switches enable robust industrial cybersecurity and minimize the need for dedicated industrial security appliances. This is achieved through a secure-by-design approach and embedded security features as software functions:

- **Cisco Trustworthy solutions:** Cisco industrial networking equipment is developed following the Cisco Secure Development Lifecycle (SDL), a part of Cisco Trustworthy Solutions, which embeds cybersecurity from product planning through end-of-life. This lifecycle is certified to meet the IEC 62443-4-1 standard, ensuring a secure-by-design approach that reduces vulnerabilities and risks throughout the product lifecycle.
- **Unmatched visibility:** Cisco Cyber Vision, running in Industrial Ethernet switches, inventories all connected assets, maps their communication activities, and highlights their vulnerabilities. It provides continuous visibility into Industrial Control Systems (ICS), the overall security posture, and the insights needed to reduce the attack surface. It profiles all connected devices to help you build segmentation policies. It detects malicious traffic and abnormal behaviors, so you can defend operations effectively.
- **Adaptive network segmentation to protect operations:** Cyber Vision helps implement adaptive OT segmentation in weeks, not years, to protect industrial operations at scale. It lets control engineers group OT assets, creating logical zones and conduits matching their industrial processes. IT can now create access control policies in Cisco Identity Services Engine or Cisco Secure Firewall that will not disrupt production. Cisco industrial switches enforce these segmentation policies aligning with the industry standard ISA/IEC 62443 for industrial automation and control systems security.
- **Zero-trust remote access to OT assets:** The built in Secure Equipment Access gateway enables zero-trust network access (ZTNA) capabilities purpose-built for OT workflows. It empowers operations teams with self-service remote access and lets them easily enforce least-privilege access policies so they can control risks from remote users accessing OT assets for remote configuration, monitoring, or troubleshooting.

Enable smart manufacturing innovations

The Cisco industrial network enables smart manufacturing innovations by delivering a secure, agile, and high-performance infrastructure that connects diverse industrial devices and systems, facilitating real-time data collection and processing.

- **Machine vision:** Machine vision systems in manufacturing offer significant benefits by enabling real-time, automated inspection and defect detection, which improves product quality and reduces downtime. By providing a secure, high-performance infrastructure that eases machine vision deployment by providing high-bandwidth data exchange, synchronization and power over ONE cable. A Cisco industrial network enables vision systems to quickly analyze images for defects, leveraging AI and advanced analytics.
- **Software-defined industrial automation:** While well accepted in the enterprise, virtualization in operations is considerably less adopted. With a high-performing, resilient, secure, and deterministic network, Cisco industrial and enterprise networking can provide uninterrupted connectivity between virtualized hardware, including Industrial PCs (IPC) and Programmable Logic Controllers (PLCs), and machines leading to lower OpEx, greater flexibility, faster innovation, and more efficient utilization of resources.

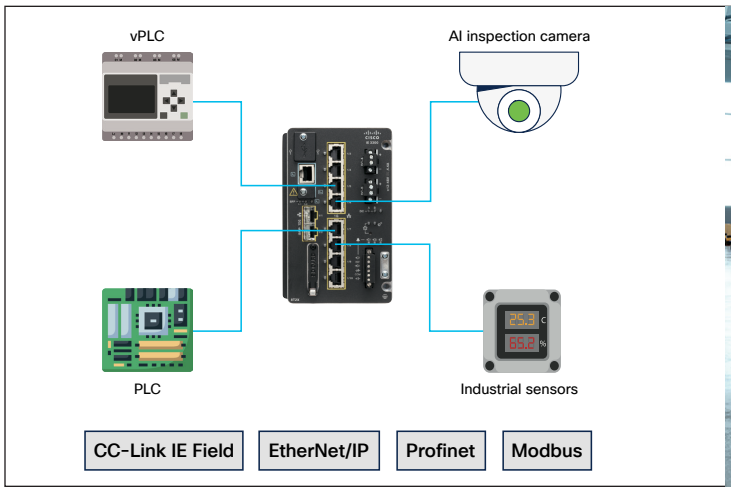
- **Digital twins:** Digital twins offer transformative benefits in manufacturing by providing real-time virtual replicas of physical assets, processes, or even entire factory floors. These virtual counterparts, fed by live data from sensors and industrial equipment, allow manufacturers to simulate scenarios, predict outcomes, and optimize operations without disrupting physical production. Cisco industrial networks enable digital twins by providing the high-speed, reliable, and secure connectivity necessary to transport large amounts of data in near real-time between manufacturing systems, IT, and digital twin platforms in datacenters and cloud.
- **Industrial AI:** The Cisco industrial network facilitates a seamless connection between IT and OT domains, enabling the real-time flow of production data. Cisco provides common networking infrastructure, management tools, and security from device-to-cloud, providing the assurance that secure communications drive Industrial AI applications. By leveraging this reliable data stream, manufacturers can gain valuable insights, make informed decisions, and realize their AI strategies.

Derive actionable insights from Splunk

Splunk offers significant value to manufacturing operations by providing a platform to centralize, analyze, and gain insights from a vast amount of data generated across various manufacturing systems. Splunk empowers manufacturers transform their data into actionable insights. With these insights, manufacturers can improve efficiency and productivity, enhance quality control, obtain better supply chain visibility, mitigate security threats, etc.

Add flexibility with reliable wireless

Reliable wireless connectivity is paramount for the effective operation of autonomous robots and vehicles. Wireless communications must function effectively in environments with obstacles and radio frequency interference to ensure real-time responsiveness. Cisco's Ultra-Reliable Wireless Backhaul (URWB) technology addresses these challenges by offering ultra-low latency and seamless handoffs between access points as devices move around the plant floor. Operating within the same unlicensed spectrum as Wi-Fi, it is the ideal choice for the demanding requirements of autonomous systems. Cisco offers wireless access points that integrate URWB with Wi-Fi, equipping manufacturers with the right solution for today's deployments and future-proofing your infrastructure for increased automation and AI, while avoiding duplicating infrastructure to support different technologies.



A converged security and network architecture for manufacturing