# Industrial Security

Protecting industrial operations against cyberthreats

## Overview

Protecting Industrial Control Systems (ICS) from cyberthreats is top of mind. But as underlying networks are often very complex, using legacy technologies and poor security procedures, one could wonder where to start.

For over 15 years, Cisco has been helping industrial organizations digitize their operations by developing a market-leading networking portfolio that is purpose-built for industrial use cases. Our deep understanding of operational technology requirements plus a comprehensive cybersecurity portfolio is a rare combination.

Cisco's security architecture simplifies complexity across the network by implementing a model that focuses on the areas an organization must secure. This model treats each area holistically, focusing on today's threats and the capabilities needed to secure each area against those threats.

This solution brief is a high-level overview of the reference architecture described in the Cisco® Validated Design dedicated to industrial security. It is a fully tested and validated solution addressing critical business challenges. The design provides comprehensive guidance, with configuration steps that help ensure effective, secure deployments for our customers.

## Securing industrial networks is a journey

People are just as critical to the process of effective cybersecurity as the technology that has been deployed. To successfully connect and secure the industrial environment, all stakeholders must work together: Operational Technology (OT) teams understand the industrial environment and the operational processes, Information Technology (IT) teams understand IP networking, and the security team understands threats and vulnerabilities. By working together, they can leverage existing networking and security technologies, tools, and expertise to protect the industrial network without disrupting production safety and uptime.

The Cisco industrial security solution is intended to be used by IT, OT, and security teams and their relevant partners and system integrators. Operations will appreciate the ease of use and simple deployment, as well as the broad support of various ICS vendors and protocols.



## Benefits

- Gain full visibility into connected assets, vulnerabilities, and activities.
- Prioritize actions by identifying assets that have the highest cyber risks.
- Control access to the OT network by deploying an industrial DMZ.
- Protect operations by implementing ISA/IEC62443 zones and conduits.
- Enforce micro-segmentation policies that do not interfere with your OT processes.
- Investigate incidents by leveraging intelligence from all your IT security tools.
- Remediate threats with workflows orchestrating tasks across your security technologies.

IT network managers will appreciate the ability to apply skills, technology, and applications already deployed in the enterprise when looking to integrate production environments. Security teams will have visibility into industrial assets and security events with context enriched by control engineers.

To help ensure success, Cisco promotes a phased approach in which each phase builds the foundation for the next, so that you can enhance your security posture at your own pace and demonstrate value to all stakeholders when embarking on this journey.

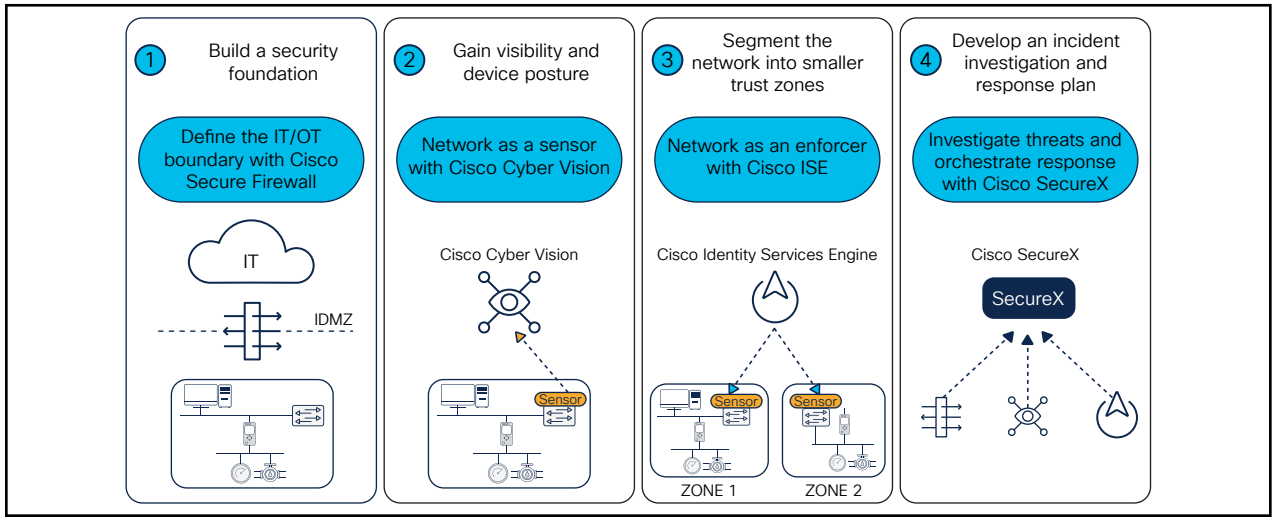


**Figure 1. Cisco's phased approach to deploying industrial security successfully**

## How it works

### Build a security foundation

A solid and flexible network architecture is a key success criterion for robust and certified security. Poor network design creates a huge vulnerability and hinders the concepts of segmentation and extensibility, as well as the integration of cybersecurity controls and physical security measures. The first step in the journey to securing your industrial network is to restrict logical access to the OT network. A common deployment method is an Industrial Demilitarized Zone (IDMZ) network with firewalls to prevent network traffic from passing directly between the corporate and OT networks.

Cisco Secure Firewall brings distinctive threat-focused next-generation security services. The firewall provides stateful packet inspection of all traffic between the enterprise and OT networks and enables intrusion prevention and deep packet inspection capabilities for inspecting application data between the zones, to identify and potentially stop a variety of attacks. Cisco Secure Firewall is the first line of defense that adversaries meet when attempting to breach the network and is the enforcement point for least privilege access for legitimate services to cross the border in a secure way.

For more information on the IDMZ, see Securely Traversing IACS Data Across the IDMZ Using Cisco Firepower Threat Defense. The subsequent capabilities are described in the Cisco Validated Design dedicated to industrial security.

# How it works

## Gain visibility and device posture

After defining and securing the network perimeter, the second stage of our security journey is to apply security within the industrial network. Organizations may want to understand the normal state of the OT network as a prerequisite for implementing network security policies to help distinguish attacks from transient conditions or normal operations within the environment. Implementing network monitoring in a passive mode and analyzing the information to differentiate between known and unknown communication may be a necessary first step in implementing security policies.

In OT environments, network-based monitoring capabilities are typically deployed using Switched Port Analyzer (SPAN) ports instead of inline network taps that could create a communication point of failure. Cisco Cyber Vision provides a unique approach that uses sensors embedded into network equipment (switches, routers, and gateways) to collect packets flowing through the industrial infrastructure. Using a combination of passive and active discovery techniques, the sensors leverage advanced knowledge of industrial protocols to decode and analyze packet payload through Deep Packet Inspection (DPI).

This lets Cyber Vision profile each endpoint, identify vulnerabilities, maintain a precise asset inventory, and map all communications activities between endpoints and resources. Cyber Vision also integrates the Snort® IDS engine leveraging Talos® threat intelligence to detect known and emerging threats such as malware or malicious traffic. With all this information, it automatically calculates risk scores so you can prioritize what needs to be fixed and understand how to reduce your exposure to cyber risks.

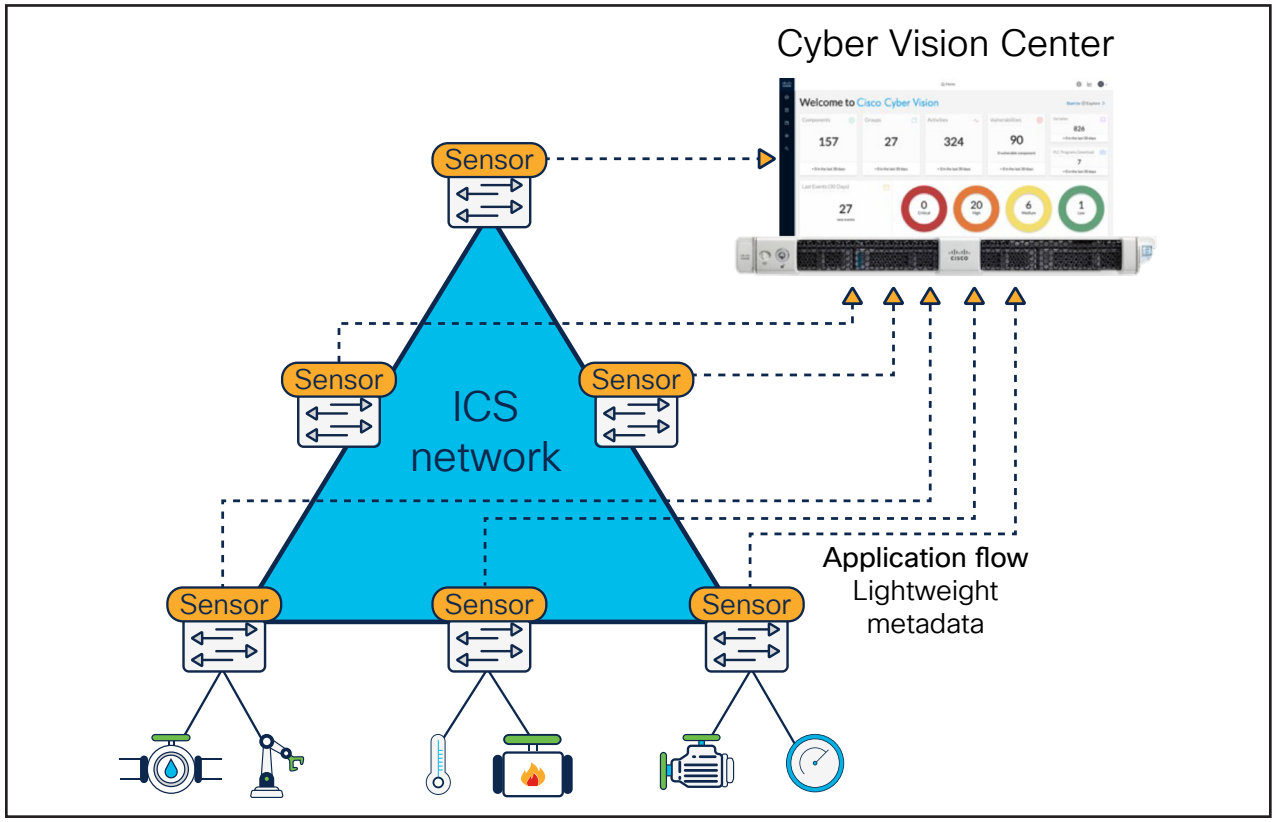


**Figure 2. The Cisco industrial network lets you see everything that connects to it**

# How it works

## Segment the network into smaller trust zones

ISA/IEC 62443 recommends that systems be separated into groups called “zones” that will be able to communicate with each other through communication channels called “conduits,” whether they are physical, electronic, or process-based. The principle of least privilege can then be applied as data traverses the conduit, to give users only the rights they need to perform their work, thus preventing unwanted access to data or programs and blocking or slowing an attack if an account is compromised.

Cell/area zones offer organizations a starting point for segmentation of the control network. The main goal for segmentation is to minimize the impact of any potential breach. The reference architecture recommends that organizations make use of a distribution switch stack to transport data to and from different cell/area zones in the network.

While organizations are gaining visibility using Cyber Vision and understanding the normal operating state of their networks, policy can be applied to larger functional zones based on VLAN or network location. For example, endpoints in the fabrication shop zone probably require no communication with endpoints in the welding shop zone and can be distinctly identified by the network infrastructure they are physically connected to.

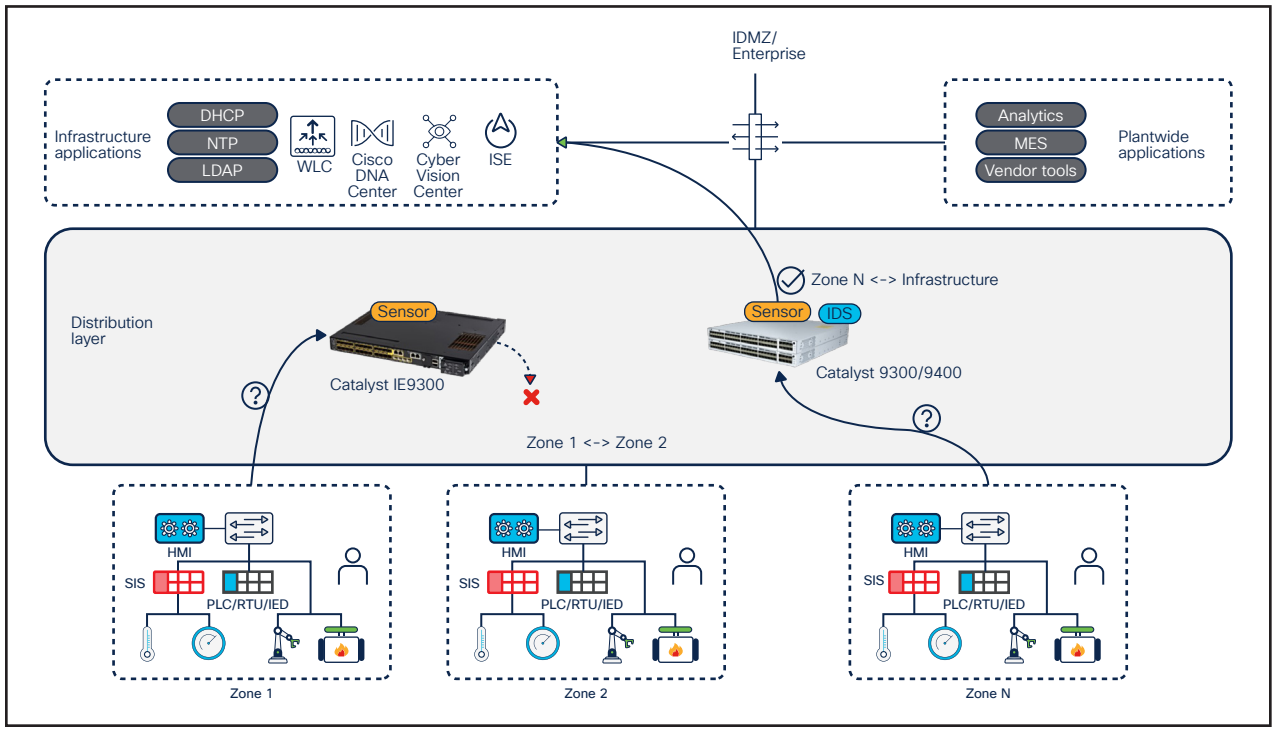


Figure 3. Leveraging the network to enforce access policies and build secured zones

Cisco Identity Services Engine (ISE) uses Cisco TrustSec® technology to logically segment control system networks. Cisco TrustSec classification and policy enforcement functions are embedded into Cisco switching, routing, wireless LAN, and firewall products. A Cisco TrustSec policy group called a Security Group Tag (SGT) is assigned to an endpoint, typically based on that endpoint's user, device, and location attributes. The SGT denotes the endpoint's access entitlements, and all traffic from the endpoint will carry the SGT information. The SGT is used by switches, routers, and firewalls to make forwarding decisions.

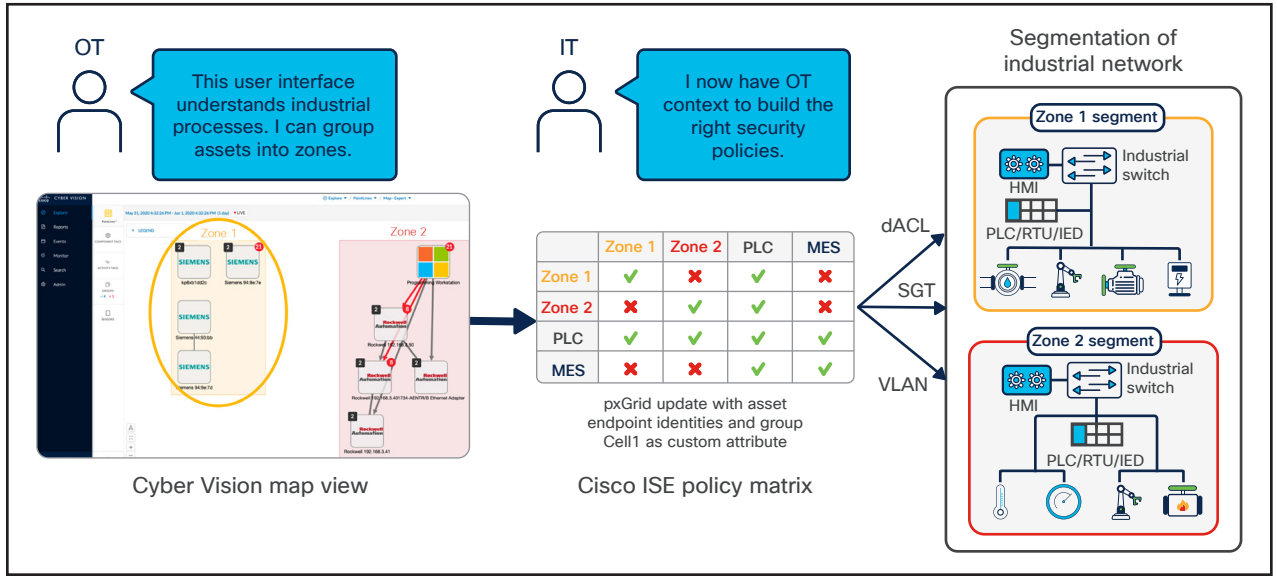


**Figure 4. Visibility into OT assets enables dynamic segmentation**

Cyber Vision can be integrated directly with ISE. Cyber Vision shows assets and their communications in maps that operations teams can easily relate to their industrial processes. This gives administrators the opportunity to group assets into logical zones based on the business role these devices play on the network. ISE can leverage the asset groupings to implement more granular policy further in the network switches that support SGTs. When the organization is ready to implement micro-segmentation policies, the groups can be made smaller, and conduits can be monitored to help ensure that policy will not interfere with the daily operations of the business.

## Develop an incident investigation and response plan

The final consideration in the journey to securing your industrial network is the ability to detect and respond to potential threats. The NIST cybersecurity framework outlines five core cybersecurity principles: Identify, Protect, Detect, Respond, Recover. The first three steps of our journey covered the capabilities needed to identify the people and assets in your network, protect them through the use of network policies, and detect the occurrence of a cybersecurity event. The Respond function supports the ability to contain the impact of a potential cybersecurity incident.

Cisco SecureX™ is an incident investigation and response platform that aggregates intelligence from both Cisco security product and third-party sources, which enables security analysts to identify whether observables such as file hashes, IP addresses, domains, and email addresses are suspicious. When you start an investigation, context is automatically added from integrated Cisco security products, so you know instantly which of your systems was targeted and how.

# Industrial Security CVD

## Features

- Visibility into OT assets and activities
- Securing the IT/OT boundary
- Hybrid macro- and micro-segmentation with TrustSec
- Intrusion and malware protection
- Threat investigation and response

When you see abnormal behavior in Cyber Vision, you can promote the incident to Cisco SecureX for further investigation, leveraging intelligence from additional sources to gain a full understanding of the threat. Has the device reached out to a malicious URL? Has a suspicious file been seen residing on an endpoint? The SecureX ribbon located on the Cyber Vision user interface makes it easy to analyze potential threats and launch remediation via native and custom playbooks.

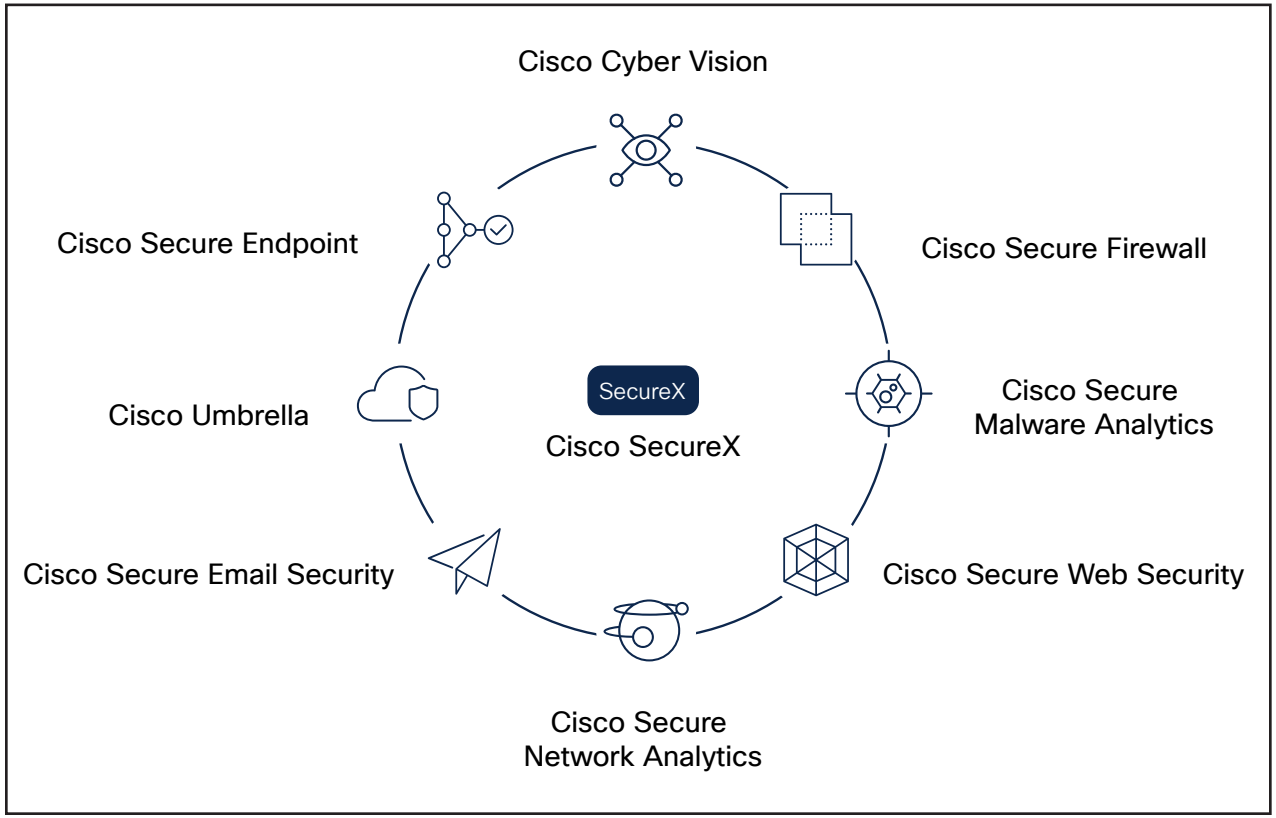


**Figure 5. Investigate across your security stack**

## The Cisco advantage

For more than 15 years, Cisco has been helping industrial organizations around the globe to 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.

The Cisco industrial security solution provides organizations with a phased approach to securing their industrial networks. This approach involves building the foundation with good network design and secure components, using the network to gain visibility across the plant floor, and then finally implementing policy back into that same network infrastructure. Following this best practice blueprint with Cisco market-leading technologies will help decrease deployment time, reduce risk, lower complexity, and improve overall security and operating uptime.

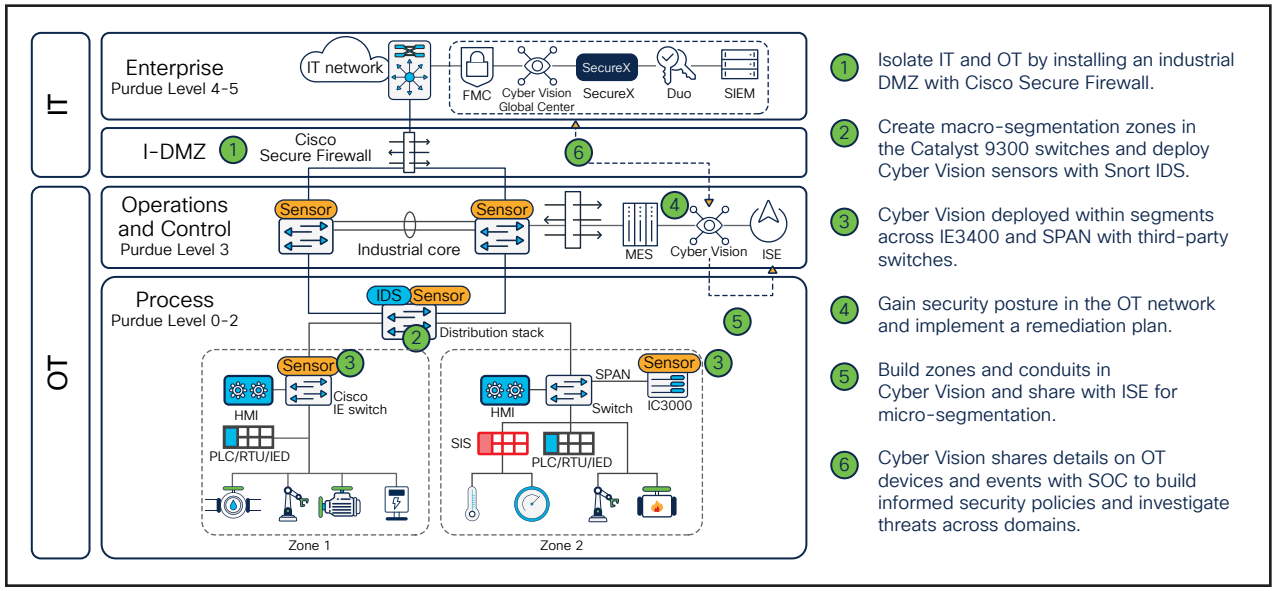


**Figure 6. Cisco's industrial security solution architecture**

## Learn more

For more details on Cisco's industrial security solution, read the Industrial Security Design Guide. You can also talk to a Cisco sales representative or channel partner and visit cisco.com/go/iotsecurity.


C22-3370508-01 08/24