

# Cisco Cyber Vision

Bringing unprecedented scale and simplicity to IoT security

## Highlights

### Visibility embedded in your industrial network

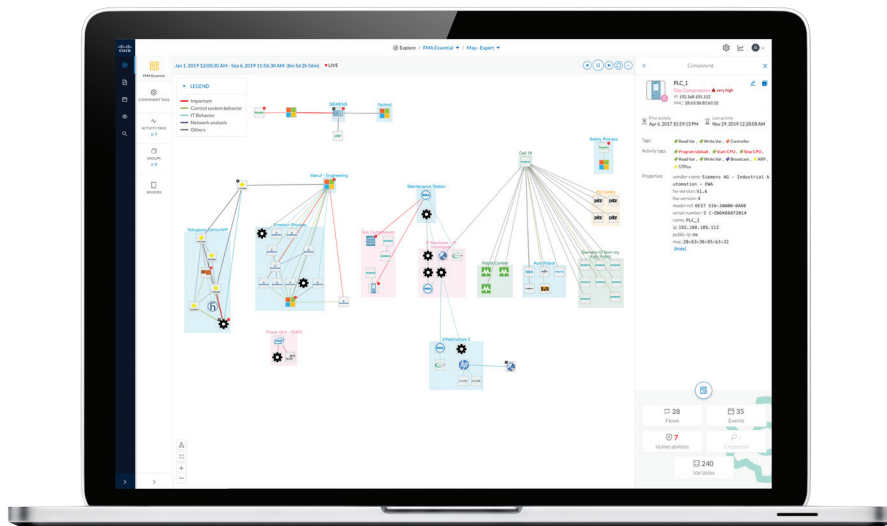
Know what to protect. Cisco Cyber Vision is embedded in your industrial network so you can see everything that connects to it.

### Operational insights for OT

Maintain system integrity and production continuity. Cisco Cyber Vision keeps track of process data, asset modifications, and variable changes.

### Holistic threat detection

Detect threats before it's too late. Cisco Cyber Vision identifies known and emerging threats as well as process anomalies and unknown attacks. Fully integrated with the Cisco security portfolio, it extends the IT security operations center (SOC) to the OT domain.



Industrial control systems (ICS) are ever more connected to corporate IT networks. You are now also deploying Industrial Internet of Things (IIoT) technologies. This deeper integration between IT, cloud, and industrial networks is creating many security issues that are becoming the primary obstacles to your industry digitization efforts.

Cisco® Cyber Vision gives you full visibility into your ICS, including dynamic asset inventory, real-time monitoring of control networks and process data, and comprehensive threat intelligence, so you can build secure infrastructures and enforce security policies to control risk.

Combining a unique edge monitoring architecture and deep integration with Cisco's leading security portfolio, Cisco Cyber Vision can be easily deployed at scale so you can ensure the continuity, resilience, and safety of your industrial operations.

## The essential tool for securing your industrial network

### Security assessments

Securing your OT infrastructure starts with having a precise view of your asset inventory, communication patterns, and network topologies. Cisco Cyber Vision automatically builds an accurate list of all your industrial assets and detailed network maps so you can define what needs to be done.

### Network segmentation

Industrial security best practices suggest migrating networks toward architectures compliant with IEC62443 zones and conduits to avoid having an attack spread to your entire industrial infrastructure. Cisco Cyber Vision integrates with Cisco Identity Services Engine (ISE) to create asset groups and leverages Cisco industrial network equipment to dynamically enforce segmentation policies.

## OT security you can deploy at scale

Cisco Cyber Vision leverages a unique edge computing architecture that enables security monitoring components to run within Cisco's industrial network equipment.

No need to source dedicated appliances and build a dedicated out-of-band network.

Network managers will appreciate the unique simplicity and the lower costs of the Cisco Cyber Vision architecture when looking to deploy OT security at scale.

### Extending cybersecurity to the OT domain

As the industrial domain is exposed to both traditional IT threats and custom-made attacks aimed at modifying the industrial process, you need holistic threat detection techniques. Cisco Cyber Vision combines protocol analysis, intrusion detection, behavioral analysis, and OT threat intelligence to detect asset vulnerabilities, and any attack tactic.

### Enabling a converged IT/OT SOC

Leverage the time and money you have invested in your IT cybersecurity environment to monitor your industrial network and manage threats to your OT domain. Cisco Cyber Vision brings detailed information on OT assets and threats to Cisco Firepower® firewalls, the ISE access controller, and the Stealthwatch® traffic analyzer so you can build and enforce security policies without disrupting production.

### Driving governance and compliance

Whether you're responsible for a critical site or a small factory, you need detailed information to comply with the latest regulatory requirements (EU NIS, NERC CIP, FDA, etc.). Cisco Cyber Vision logs all events from your ICS so you can run efficient audits, build incident reports, and work with both IT and OT teams to drive actions.

## What can Cisco Cyber Vision do for you?



#### Security leaders

Feed your IT security platforms (firewalls, access controllers, etc.) with OT context to build OT security policies and easily enforce them across the industrial network.



#### SOC teams

Collect security events from the industrial domain into your SIEM platforms so you can take the proper measures without disrupting production.



#### Chief information security officers (CISO)

Have the proper tools to build a unified approach to IT and OT cybersecurity, and drive governance and compliance.



#### Control engineers

Have a dynamic assets inventory that also identifies vulnerabilities, malfunctions, and abnormal behaviors so you can keep production going.



#### Network managers

Leverage your Cisco industrial network equipment to deploy security monitoring at scale and drive network segmentation projects.