Cisco Cyber Vision

Cisco® Cyber Vision is a cybersecurity solution purpose-built for industrial organizations and critical infrastructures. It offers comprehensive operational technologies (OT) security capabilities to help reduce the OT attack surface, prevent threats from spreading, secure remote access activities, and extend IT security to industrial settings to build cyber-resilient industrial networks.

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

© 2025 Cisco and/or its affiliates. All rights reserved.

Product overview

As you are digitizing your industrial operations, the deeper integration between industrial networks, IT, and cloud resources is exposing your industrial control systems (ICS) and OT assets to cyberthreats. You need a solution to help you ensure the continuity, resilience, and safety of your industrial operations.

Cyber Vision provides continuous visibility into your OT security posture, so you have the insights to reduce your attack surface. Its deep integration with Cisco's leading security portfolio helps protect operations with network segmentation that can be implemented in weeks, not years. Its zero trust network access (ZTNA) capabilities empower operations teams with self-service remote access to OT assets while letting you enforce least privilege policies.

Cyber Vision uses a unique edge architecture that embeds OT security features into your industrial network. There are no dedicated security appliances to deploy or out-of-band collection networks to build. The network that connects your assets profiles everything that connects to it, detects malicious traffic and abnormal activities, enforces IEC 62443 zones and conduits, and controls who can remotely access your assets. That's OT security you can deploy at scale.

© 2025 Cisco and/or its affiliates. All rights reserved.

Features and benefits

Table 1. Features and benefits

Feature	Benefit
Real-time visibility into your OT asset inventory and security posture	You can’t secure what you don’t know. Build your OT security practice with a detailed inventory of all your industrial assets that’s automatically generated and always up-to-date. Strengthen your OT security posture by driving actions informed by comprehensive visibility into vulnerabilities, communication patterns, malicious traffic, abnormal behaviors, and more.
OT network segmentation	Protect industrial operations by implementing IEC 62443 zones and conduits. Cyber Vision helps control engineers group assets into zones (production cells, buildings, substations, etc.) so IT has all the information to enforce the right segmentation policies using Cisco ISE or Secure Firewall.
Zero trust remote access	Empower operations teams with self-service remote access that lets you enforce least privilege policies thanks to Cisco Secure Equipment Access now included with Cyber Vision.
Network-embedded sensors	Easily deploy OT security at scale thanks to Cyber Vision sensors embedded in select Cisco networking equipment: ▪ No need to deploy dedicated appliances. Gaining OT visibility is just a software feature to activate in your switches and routers, saving both CAPEX and OPEX. ▪ No need for additional network resources or complex network setups. Cyber Vision sensors send lightweight metadata to the Cyber Vision Center, representing only 2% to 5% additional network traffic. ▪ Identify all OT assets with ease, even those in the lowest Purdue levels, thank to the Cyber Vision sensor running in the switches that connect them to the network.
Hardware and Docker sensors	Easily deploy Cyber Vision sensors in brownfield environements when runing the sensor software in routers or switches is not possible. ▪ Eliminate the need to build a SPAN collection network by deploying Cyber Vision sensors within the industrial network. Install the sensor software on a Cisco IC3000 industrial compute gateway or any compute hardware running Docker and use just a short 1-hop SPAN to gain visibility from existing switches. ▪ Use your existing SPAN collection infrastructure to send traffic from existing switches to the Cyber Vision Center where the sensor software is installed to decode traffic, extract information, and send active queries to assets.

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Benefit
Combined OT visibility sensor and ZTNA gateway	Simplify deployment at scale by using Cisco industrial network equipment to run the Cyber Vision sensor and the Secure Equipment Access ZTNA gateway software simultaneously (select models only).
Zero-touch provisioning	Automate enrollment of Cyber Vision sensors and deploy large scale infrastructures in minutes. Easily keep sensors up-to-date without any manual task or service interruption.
Passive and active discovery	Cyber Vision monitors your industrial operations by passively capturing and decoding network traffic using Deep Packet Inspection (DPI) of industrial control protocols. More information can be collected with active discovery that sends extremely precise and nondisruptive requests in the semantics of the specific ICS protocol at play.
Distributed edge active discovery	Get comprehensive and detailed visibility on all connected assets, even those deployed in the lowest levels of the Purdue model. Because the sensor is running in switches that assets are connected to, Cyber Vision's active discovery requests are not blocked by firewalls or Network Address Translation (NAT) boundaries.
Global view on all your sites	Drive governance and compliance with detailed security information on all your industrial sites. The Cyber Vision Global Center seamlessly aggregates data from all local centers so that CISO and security teams have centralized visibility into assets and events per site and across sites.
Inventory reports	Stay on top of your asset inventory with formally crafted executive summary reports showcasing meaningful visualizations and breakdowns of your assets. Customize and white-label the reports as per your needs and share it with stakeholders as a Word or PDF document.
OT tags	Immediately understand the role of each device and what it is doing. Cyber Vision translates application flows into human-readable tags, so you know what is going on, even if you're not a protocol expert.
Vulnerability detection	Keep your industrial assets safe. Cyber Vision alerts you to hardware and software vulnerabilities that need to be patched.

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Benefit
Risk scoring	Focus on immediate threats and prioritize actions to quickly improve your security posture. Cyber Vision calculates risks for each device, as well as for specific site, line or any dataset. It even provides guidance on what can be done to proactively reduce risks.
Map views	Visualize the activity of your control network. Cyber Vision offers several types of maps to show your assets and their communications. Quickly spot threats and anomalies, thanks to color coding.
Preset views	Easily dive into your dataset by using preset and custom views that highlight what really matters to you, helping you focus your detection strategy and share targeted information with colleagues.
Operational insights	Reduce downtime and improve network efficiency. Cyber Vision monitors all OT events to spot device problems before they disrupt production and help operations troubleshoot issues faster. It identifies problematic network patterns so IT can optimize configurations and network performance.
Security insights	Quickly understand your current security status, identify anomalies and vulnerabilities, and respond to threats. Cyber Vision offers various dashboards, reports, and event histories to easily spot security issues and share information with all stakeholders.
Security posture reports	Better drive OT security governance with detailed reports on the security posture of your industrial operations or any specific parts of your operations, including Remote Access reports to detect rogue remote access gateways deployed in the OT environment.
Intrusion detection (IDS)	Uncover the cybersecurity threats coming from your IT network. Cyber Vision integrates the Snort IDS engine leveraging Talos® subscription rules (including Shared Object rules) to detect known and emerging threats such as malware or malicious traffic.
Anomaly detection	Detect deviations from what normal process behaviors should be. Easily create multiple baselines to profile your industrial operations or focus on what is most critical to you (such as a particular asset or specific behaviors such as remote access). Deviations immediately trigger alerts.

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Benefit
Correlate IT/OT security events	Enhance your security event management practice. Cyber Vision is pre-integrated with leading SIEM and SOAR platforms such as Splunk or QRadar, and can forward OT events and alerts to any other tool using Syslog. To avoid event fatigue, it even lets you choose which event types should be shared.
IT/OT collaboration	Leverage OT knowledge of industrial assets and processes. Cyber Vision helps build a collaborative workflow between IT and OT to efficiently secure production. OT can report security events by providing additional context. IT can add custom properties to OT assets and groups to document specificities, dependencies, and stakeholders.
Extend IT security to OT	Build a unified OT/IT SOC. Cyber Vision is fully integrated with Cisco IT security platforms and feeds them with rich details on OT assets and events. Creating OT security policies and remediating threats using existing IT tools is now much easier.
Rich integration with IT	Easily share OT context with your IT tools. Cyber Vision comes preintegrated with third-party solutions such as ServiceNow's OT Management, and has a rich REST API to build your custom integration. The API Explorer helps you write and test API calls via a friendly user interface and comes with code samples to get you started.
On-premise or in the Cloud	Deploy where and how you prefer. On premise using a hardware or a virtual appliance, or in the cloud. Cyber Vision can be installed on Amazon Web Services or Microsoft Azure.
Information assurance and compliance	Protect your organization's data and comply with information security standards using Cyber Vision in FIPS 140-2 mode.

© 2025 Cisco and/or its affiliates. All rights reserved.

OT visibility you can deploy at scale

Security built into your industrial network

Cisco Cyber Vision’s unique edge computing architecture embeds security monitoring components within our industrial network equipment. There’s no need to source dedicated appliances and think about how to install them. There’s no need to build an out-of-band network to send industrial network flows to a central security platform. Cyber Vision enables the industrial network to collect the information required to provide comprehensive visibility, analytics, and threat detection. Network managers will appreciate the unique simplicity and lower costs of the Cyber Vision architecture for deploying OT security at scale.

To learn more about why Cyber Vision stands apart when it comes to gaining comprehensive OT visibility, please read the solution brief.

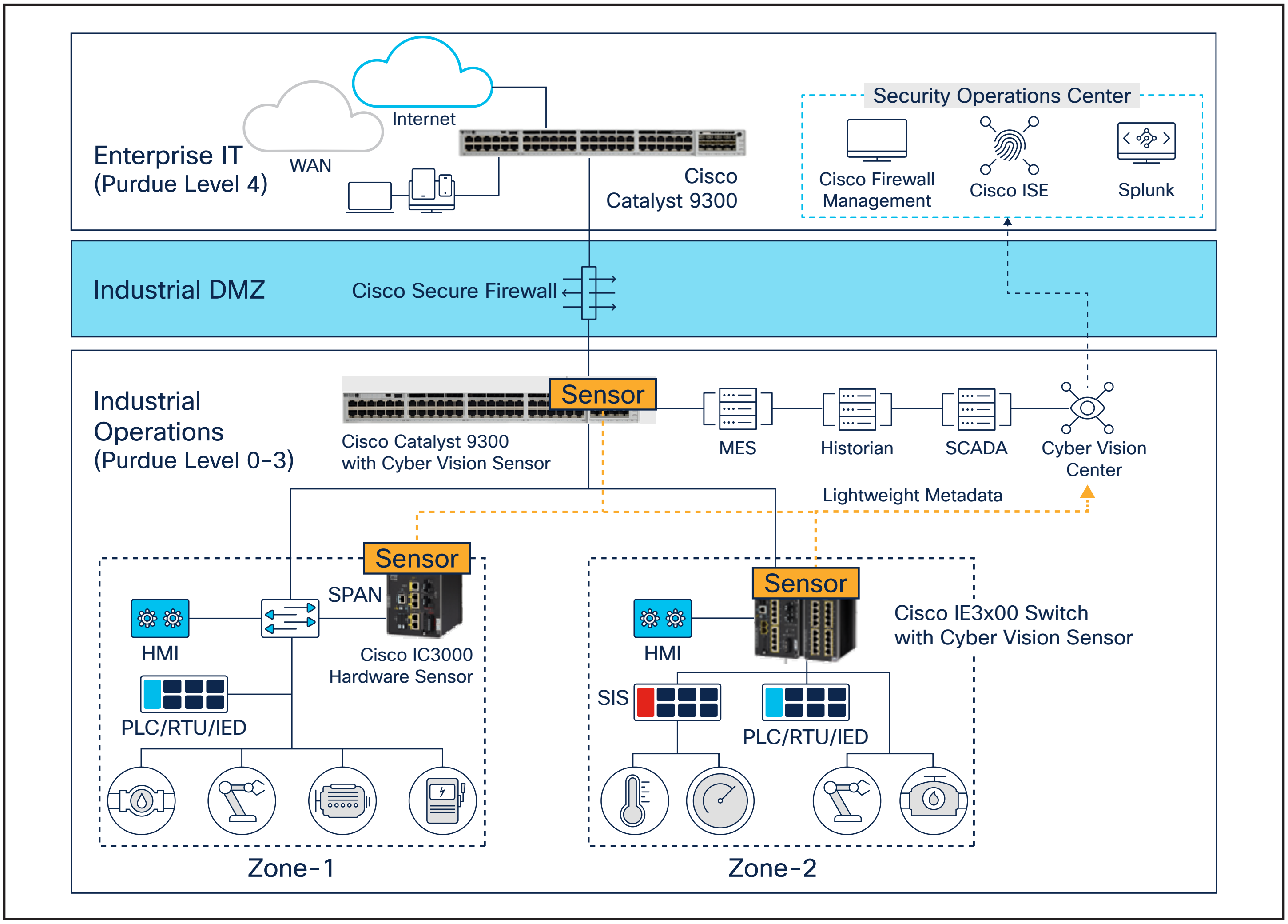


Figure 1. Cyber Vision uses a nonintrusive edge architecture for gaining visibility at scale without impacting network performance

© 2025 Cisco and/or its affiliates. All rights reserved.

Comprehensive visibility

Cyber Vision leverages passive and active discovery mechanisms to identify all your assets, their characteristics, and their communications. Active discovery queries are extremely precise and nondisruptive. They use the semantic of the protocols at play to gather details on all your industrial assets, including Windows-based systems. Because queries are initiated from Cyber Vision sensors embedded in Cisco network equipment forming the industrial network, they are not blocked by firewalls or NAT boundaries, resulting in comprehensive visibility.

This wealth of information on assets, communication maps, and operational and security events can be access by local OT and IT team members. It can also be aggregated in a Cyber Vision Global Center, for large organizations to gain global visibility across all sites and drive governance and compliance.

Security posture

Cisco Cyber Vision combines protocol analysis, intrusion detection, vulnerability detection and behavioral analysis to help you understand your security posture. It automatically calculates risk scores for each component, device and any specific parts of your operations to highlight critical issues so you can prioritize what needs to be fixed. Each score comes with guidance on how to reduce your exposure so you can be proactive and build an improvement process to address risks.

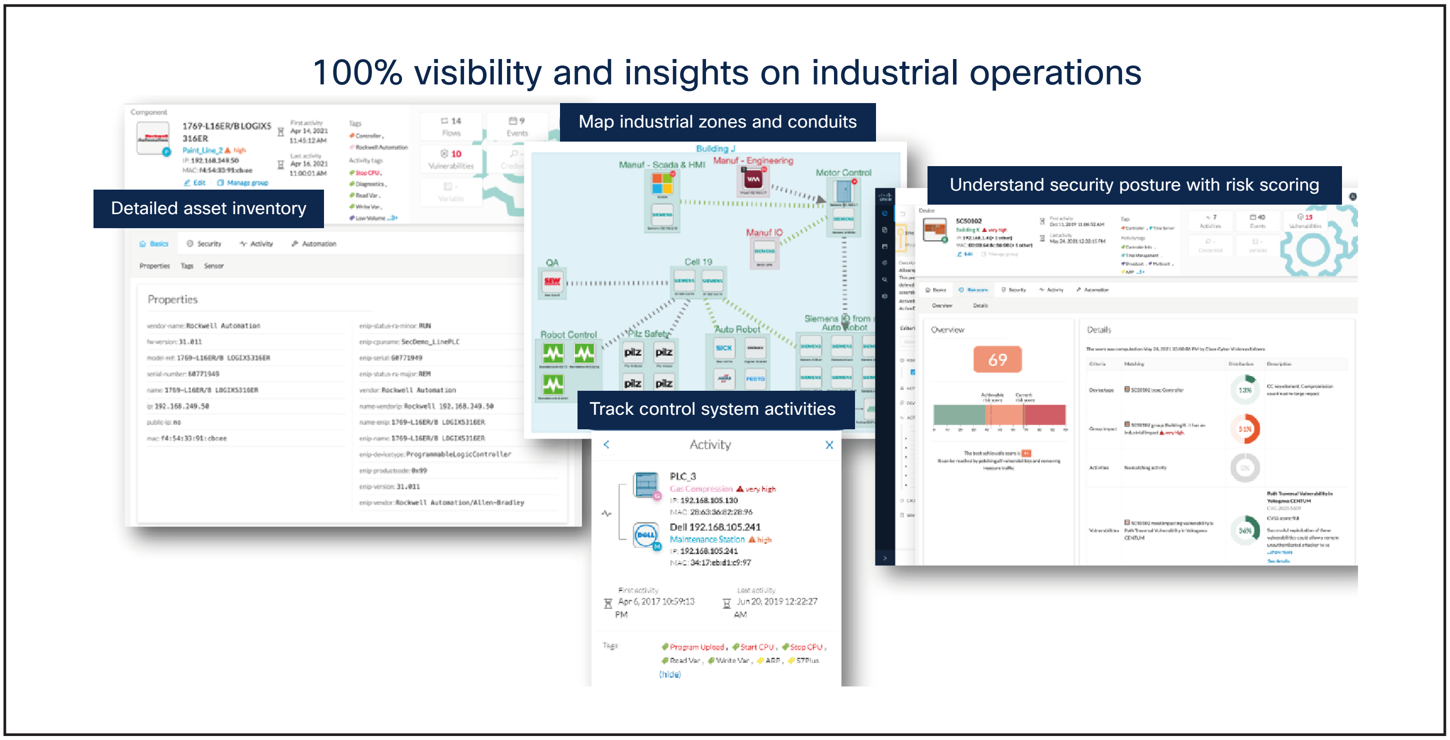
Cyber Vision’s detection engine leverages threat intelligence from Cisco Talos, one of the world’s leading cybersecurity research team and the official developer of Snort signature files. The Cyber Vision threat knowledge base is updated every week to include the latest list of asset vulnerabilities and IDS signatures.

Operational insights

Cisco Cyber Vision automatically uncovers the smallest details of the production infrastructure: vendor references, firmware and hardware versions, serial numbers, rack slot configuration, etc. It identifies asset relationships, communication patterns, and more. Information is shown in various types of maps, tables, and reports.

Cisco Cyber Vision gives OT engineers real-time insight into the actual status of industrial processes, such as unexpected variable changes or controller modifications, so they can quickly troubleshoot production issues and maintain uptime. Cyber experts can easily dive into all this data to investigate security events. Chief information security officers have all the necessary information to document incident reports and drive regulatory compliance.

The product uses tags to highlight asset roles and communication contexts, so that any OT and IT team member can easily understand the industrial infrastructure and operational events, regardless of the asset brand or references. IT teams can then work with OT staff to drive best practices such as patching vulnerable assets, tracking default password uses, improving network segmentation, and more.



100% visibility and insights on industrial operations

Detailed asset inventory

Map industrial zones and conduits

Understand security posture with risk scoring

Track control system activities

Properties

vendor-name: Rockwell Automation
fw-version: 31.011
model-ref: 1769-L16ER/B LOGIX5316ER
serial-number: 60771949
name: 1769-L16ER/B LOGIX5316ER
ip: 192.168.249.50
public-ip: no
mac: f4:54:33:91:cb:ee

enip-status-ra-minor: RUN
enip-cpuname: SecDemo_LinePLC
enip-serial: 60771949
enip-status-ra-major: REM
vendor: Rockwell Automation
name-vendorip: Rockwell 192.168.249.50
name-enip: 1769-L16ER/B LOGIX5316ER
enip-name: 1769-L16ER/B LOGIX5316ER
enip-devicetype: ProgrammableLogicController
enip-productcode: 0x99
enip-version: 31.011
enip-vendor: Rockwell Automation/Allen-Bradley

Activity

PLC_3
Gas Compression very high
IP: 192.168.105.130
MAC: 28:63:36:82:28:96

Dell 192.168.105.241
Maintenance Station high
IP: 192.168.105.241
MAC: 34:17:eb:d1:c9:97

First activity: Apr 6, 2017 10:59:13 PM
Last activity: Jun 20, 2019 12:22:27 AM

Tags: Program Upload, Start CPU, Stop CPU, Read Var, Write Var, ARP, S7Plus (hide)

Figure 2. Gain operational insights into your assets, industrial processes, communication flows and your security posture

Protect operations with adaptive network segmentation

Network segmentation is a key pillar to protecting your industrial network. Cyber Vision streamlines the workflow so segmentation can be implemented in weeks, not years. It helps control engineers to group OT assets according to their functions in the industrial process, creating logical zones and conduits, and documenting how the industrial network should be segmented. IT/NetSec teams now have the information they need to create access control policies that will not disrupt production.

Cisco Secure Firewall

Cyber Vision asset groups created by control engineers are automatically shared with Firewall Management Center (FMC) so IT can create firewall rules restricting communications within the industrial network. Because OT asset groups are shared as dynamic objects via the Cisco Secure Dynamic Attribute Connector (CSDAC), any change made in Cyber Vision is automatically reflected in FMC, keeping rules up-to-date without tedious manual updates and policy deployment.

To learn more about how Cyber Vision and Cisco Secure Firewall work together, please read the solution brief.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Identity Services Engine (ISE)

Prevent lateral movement by enforcing identity-based micro-segmentation policies in your industrial control network. Cisco ISE denies all communication by default and uses Cyber Vision asset groups to allow activities only between assets that have explicit allow policies associated to them. Because asset profiles are shared with Cisco ISE through pxGrid, any change to Cyber Vision assets is instantaneously pushed to ISE to update policies and enable adaptive micro-segmentation in the industrial network. Just move an asset to another group in Cyber Vision to have ISE automatically apply the corresponding security policy to this asset.

To learn more about how Cyber Vision and ISE work together, please read the solution brief.

Secure remote access to OT assets

Remote access is key for operations teams, maintenance contractors, and machine builders to manage and troubleshoot OT assets without time-consuming and costly site visits. Cyber Vision comes with comprehensive zero-trust network access (ZTNA) capabilities purpose-built for OT workflows. Powered by Cisco Secure Equipment Access, Cyber Vision's OT remote access features enables easy enforcement of least-privilege remote access policies based on identities and contexts, such as robust authentication via MFA or SSO, time schedules, remote access protocols being used, remote user posture check, and more. Remote users never have access to the entire IP network and can only have access to the assets they are given permission to access.

© 2025 Cisco and/or its affiliates. All rights reserved.

Enrich IT security tools with OT context

Cyber Vision's detailed asset inventory and visibility into OT events provide value to both operations and IT security teams. Out-of-the-box integrations with Cisco's security portfolio, as well as with a broad set of third-party solutions, extend Cyber Vision's insight to the security operations center (SOC) to help detect threats traversing IT and OT domains and use your IT security tools to protect your industrial operations as well as your IT.

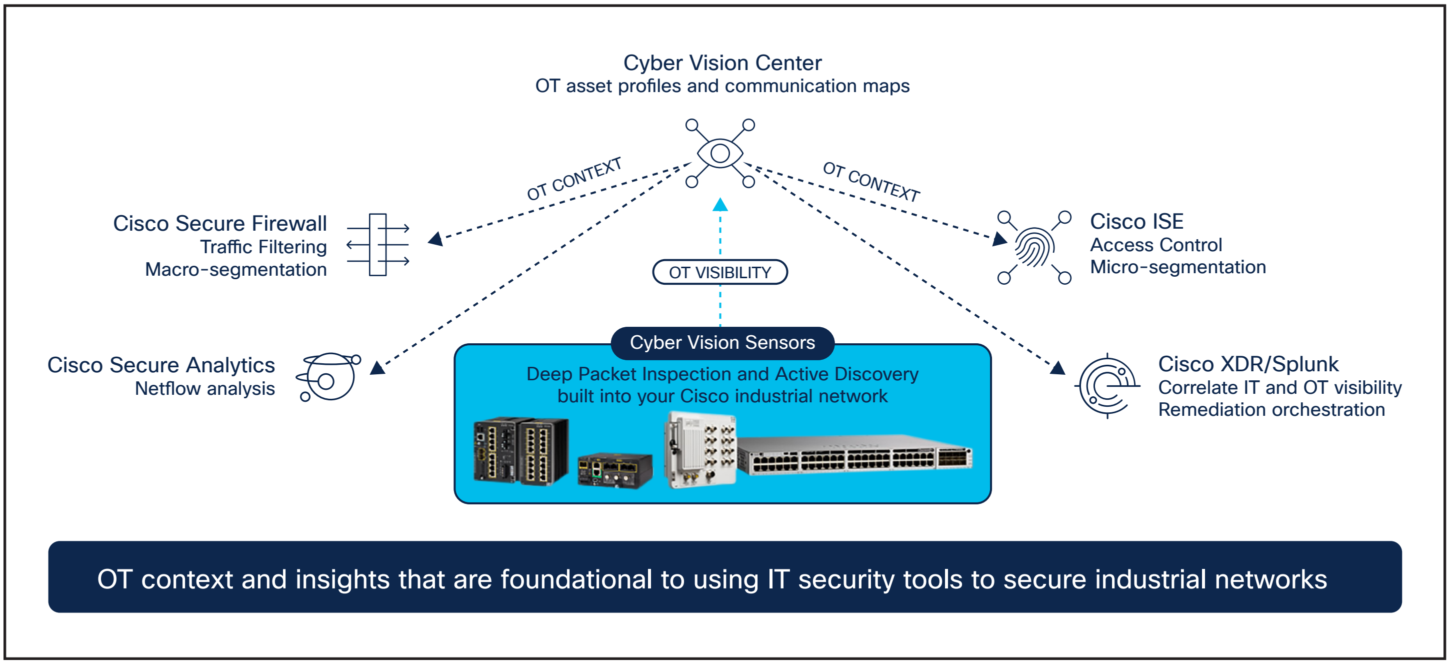

Cyber Vision Center
OT asset profiles and communication maps
OT CONTEXT
OT CONTEXT
Cisco Secure Firewall
Traffic Filtering
Macro-segmentation
Cisco ISE
Access Control
Micro-segmentation
OT VISIBILITY
Cisco Secure Analytics
Netflow analysis
Cyber Vision Sensors
Deep Packet Inspection and Active Discovery
built into your Cisco industrial network
Cisco XDR/Splunk
Correlate IT and OT visibility
Remediation orchestration
OT context and insights that are foundational to using IT security tools to secure industrial networks

Figure 3. Cyber Vision extends your IT security operations to OT by feeding your existing tools with context on industrial assets and events

Cisco XDR

Are you seeing an abnormal behavior in Cisco Cyber Vision? Just click the "Report to XDR" button to create a case in Cisco XDR for an analyst to investigate and launch remediation via specific playbooks and custom workflows. The XDR ribbon always available on the Cyber Vision user interface makes it even easier to trigger remediation workflows and quickly contain threats. The ribbon highlights all observables Cyber Vision has detected (IP and MAC addresses, usernames, hostnames, URLs, and more) so you can easily pivot to XDR with OT context and launch detailed investigations. Cisco XDR leverages intelligence from Cisco Secure Endpoint, Secure Network Analytics, Secure Firewall, Umbrella, Talos intelligence feeds, and other connected technologies (Cisco and third party) to give you a complete view of threats and activities across your IT and OT networks.

To learn more about how Cyber Vision and Cisco XDR work together, please read the solution brief.

© 2025 Cisco and/or its affiliates. All rights reserved.

Splunk

Many OT security incidents originate from the IT domain. Incidents starting in the industrial network can propagate to the enterprise network as well. You need unified visibility across IT and OT for security analysts to detect threats faster and protect the global enterprise. Cyber Vision feeds OT security events into Splunk so security analyst can correlate IT and OT events to better detect threats and remediate security events using their entire security stack. Cyber Vision shares OT asset profiles with Splunk Asset Risks Intelligence (ARI) which aggregates asset inventory from all connected tools to provide security analysts with a comprehensive view on everything connected to the global infrastructure and associated risks.

Cisco Secure Network Analytics

Extend behavioral analytics by looking at telemetry from your network infrastructure. Cisco Secure Network Analytics uses Cyber Vision insights to add context to the network flows it monitors and speed up incident response and forensics by pinpointing ICS assets on alarms.

REST API

Cyber Vision exposes functionality and data access through a REST API. This allows for custom integration of third-party and homegrown applications for compliance and risk reporting, system and event monitoring, dashboards, and more. The built-in API Explorer offers a friendly Swager user interface to build your own API calls, test them, and generate code easily. Out-of-the-box integrations are available such as with ServiceNow OT Management.

Common Event Format (CEF)

Cyber Vision discovery and event data may be output in Common Event Format (CEF) syslog for consumption by any number of third-party applications such as SIEM solutions, Security Orchestration, Automation, and Response (SOAR) platforms, and more. Free add-ons are available for easy integration with Splunk and QRadar.

© 2025 Cisco and/or its affiliates. All rights reserved.

Platform support

Cisco Cyber Vision is built on a unique edge architecture consisting of multiple sensor devices that perform deep packet inspection, protocol analysis, safe active query of assets, and intrusion detection within your industrial network. An aggregation platform known as Cyber Vision Center stores data coming from the sensors and provides the user interface, analytics, behavioral analysis, reporting, alerting, API, and more. The Cyber Vision Center can run on a hardware appliance or as a virtual machine on premises or in a private or public cloud. The Cyber Vision sensors are supported on the platforms listed in the table below.

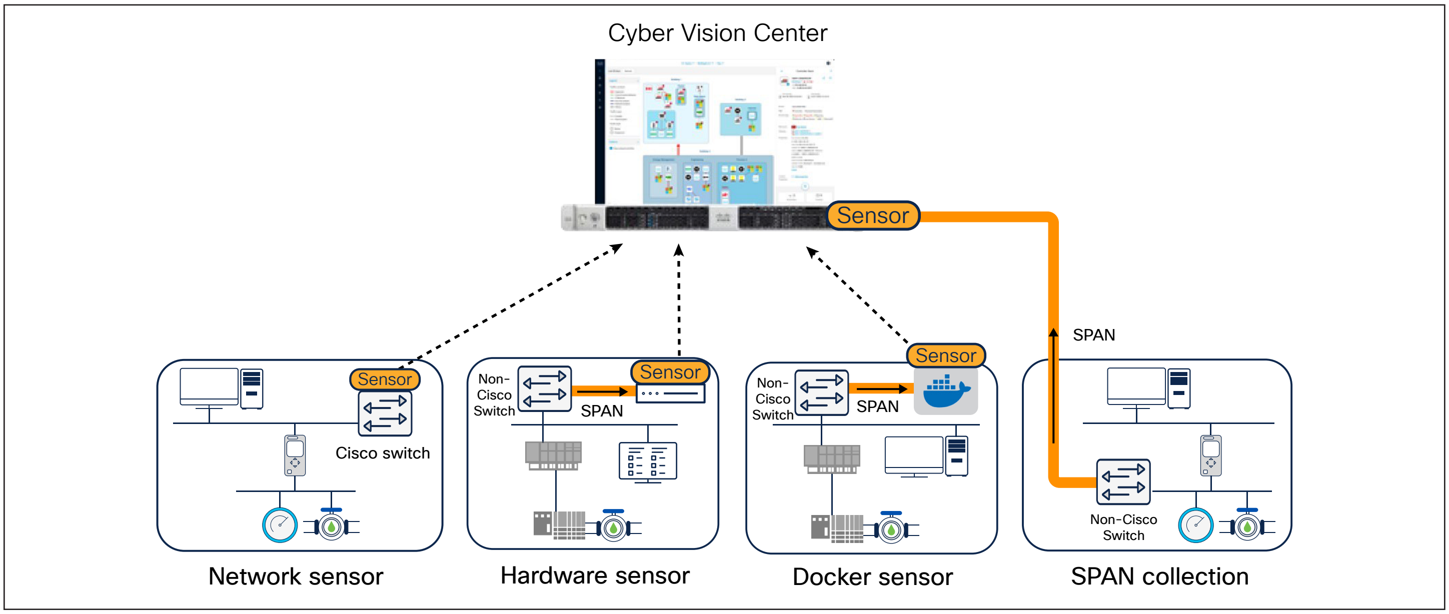


Figure 4. Cyber Vision is simple to deploy in any environment, event if not using Cisco networking equipment

On select platforms, the Cyber Vision sensor can simultaneously run a ZTNA gateway agent enabling zero trust remote access using Cisco Secure Equipment Access which is included with the Cyber Vision Advantage license. Please refer to the [Cisco Secure Equipment Access datasheet](#) for more information on remote access features and performance.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Sensor platforms

Table 2. Platforms for the Cyber Vision Sensor

Platforms	Combined visibility sensor and ZTNA gateway	Visibility sensor only	ZTNA gateway only
Industrial Ethernet switches			
Cisco IE3500 Rugged Series switch	●		
Cisco IE3500 Heavy Duty Series switch	●		
Cisco Catalyst IE3400 Rugged Series switch	●		
Cisco Catalyst IE3400 Heavy Duty Series switch	●		
Cisco Catalyst® IE3300 Rugged Series switch (models with 4 GB RAM only)	●		
Cisco Catalyst IE3100 Rugged Series switch			●
Cisco Catalyst IE3100H Heavy Duty Series switch			●
Cisco Catalyst IE9300 Rugged Series switch	●		
Rockwell Stratix 5800 switch		●	
Enterprise switches			
Cisco Catalyst 9300 Series switch	●		
Cisco Catalyst 9300X Series switch		●	
Cisco Catalyst 9400 Series switch		●	
Industrial routers			
Cisco Catalyst IR1100 Rugged Series router		●	●
Cisco Catalyst IR1800 Rugged Series router		●	●
Cisco Catalyst IR8300 Rugged Series router		●	
Industrial compute			
Cisco IC3000 Industrial Compute Gateway (IC3000-2C2F-K9)		●	
Any x86 or arm64 compute hardware supporting the Docker virtualization engine (version 27.0 minimum) with 2GB of dedicated RAM minimum (4GB if using the IDS engine).		●	

© 2025 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Center platforms

Table 3. Platforms for the Cyber Vision Center

Center type	Platforms supported
Center hardware appliance	Cisco UCS C225 M6N Rack Server (CV-CNTR-M6N configuration)
Center virtual appliance	VMware ESXi software appliance Microsoft Hyper-V software appliance Nutanix AHV software appliance
Center cloud appliance	Amazon AWS software appliance Microsoft Azure software appliance

Table 4. Cyber Vision Center hardware appliance specifications

Item	CV-CNTR-M6N
Form factor	1RU Cisco UCS C225 M6N Rack Server
Processors	AMD 2.85GHz 7443P with 24 cores
Memory	Eight 16GB RDIMM SRx4 3200MHz
RAID	Software enabled RAID will provide RAID 1 or RAID 10 depending on number of drives
Internal storage	Two or Four 1.6 TB NVMe Extreme Perf. High Endurance drives
Embedded Network Interface Cards (NICs)	Dual 10GBASE-T Intel x710 Ethernet ports
Power supplies	Hot-pluggable, redundant Cisco UCS 1050W AC Power Supply for Rack Server

© 2025 Cisco and/or its affiliates. All rights reserved.

Item	CV-CNTR-M6N
Management	Cisco Intersight™ Cisco Integrated Management Controller (IMC) Cisco UCS Manager
Rack options	Cisco ball-bearing rail kit or friction rail kit with optional reversible cable management arm

Please refer to the Cisco UCS C225 M6N Rack Server data sheets for additional hardware specifications.

Cyber Vision Center hardware appliance performance

Table 5. Cisco Cyber Vision Center (Standalone/Local) hardware appliance scale

Item	CV-CNTR-M6N
Max components	50,000
Max number of sensors	300
Max number of flows stored	16 million

Table 6. Cisco Cyber Vision Global Center scale

Item	CV-CNTR-M6N
Max components synced	150,000
Max number of registered centers	20

© 2025 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Center virtual appliance specifications

Table 7. Minimum specifications* for the Cyber Vision Center virtual appliance

Characteristic	Private Cloud	Public Cloud
CPU	x86 server CPU with 10 cores minimum	x86 server CPU with 10 cores minimum
Memory	32 GB minimum	32 GB minimum
Storage	1 TB SSD minimum	1 TB SSD minimum
Virtualization software	▪ VMware ESXi 6.x or later ▪ Microsoft Hyper-V on Windows Server 2016 or later ▪ Nutanix AHV software appliance	▪ Amazon Web Services ▪ Microsoft Azure

***These VM requirements support monitoring of up to 10000 endpoints.**

The Cisco Cyber Vision Center virtual appliance may be downloaded directly from software.cisco.com.

© 2025 Cisco and/or its affiliates. All rights reserved.

Licensing

Cisco Cyber Vision is licensed using a recurring subscription model based on the number of endpoints monitored and is available in 1-, 3-, 5-, and 7-year terms. Licensing is available in two tiers–Essentials and Advantage–that provide different levels of capabilities to meet your particular requirements. The product uses Cisco Smart Licensing with the option for Specific License Reservation (SLR) licenses for air-gapped networks. Please note that a current subscription license includes access to Cyber Vision Center and sensor software, which may be downloaded directly from software.cisco.com.

The Cyber Vision Advantage license includes a Cisco Secure Equipment Access Advantage license for the same number of endpoints.

Cisco IE3500 and Catalyst IE9300 Rugged Series Network Advantage license-based switch SKUs (eg. IE-3500-8T3S-A, IE-9310-26S2C-A, etc.) come with a 3 years limited term and 24 endpoints Advantage license of Cyber Vision and Secure Equipment Access at no extra costs. Licenses for additional endpoints can be purchased separately.

Table 8. Licensing tiers

Licensing levels	
Essentials	Advantage
Inventory ▪ Device inventory ▪ Identify communication patterns ▪ Generate inventory reports **Vulnerability** ▪ Identify device vulnerabilities ▪ Export vulnerability data **Activities** ▪ Track control system events **Restful API** ▪ REST API programming interface	Includes Essentials features, plus: **Security Posture** ▪ Device Risk Scoring ▪ Security posture reports ▪ Remote access reports **Intrusion Detection (IDS)** ▪ Snort IDS on supported sensors ▪ Talos community signatures (New rules may be added 30 days after release) **Behavior Monitoring** ▪ User-created baselines for asset behaviors ▪ Alerts on deviations **Secure Remote Access** ▪ Zero Trust Network Access (ZTNA) purpose-built for OT workflows, powered by Cisco Secure Equipment Access.

© 2025 Cisco and/or its affiliates. All rights reserved.

Licensing levels	
Essentials	Advantage
	Advanced integration ▪ Cisco XDR Ribbon ▪ pxGrid integration with Cisco ISE ▪ SIEM integration – Splunk, QRadar ▪ ServiceNow OT Management integration
	Talos subscriber rules option for Cyber Vision IDS
	(Requires Cyber Vision Advantage; licensed per IDS sensor deployed) ▪ Talos subscription signatures, specifically curated for industrial networks ▪ Immediate rules availability ▪ 15x more rules compared to community signatures

Endpoint license packs are available for any number of endpoints required. IDS is available on the Cyber Vision Center as well as on the Cisco IC3000 hardware sensor, the Docker sensor, the Catalyst IR8300 Rugged router and the Catalyst 9300, 9300X or 9400 switches.

© 2025 Cisco and/or its affiliates. All rights reserved.

Ordering information

Cisco Cyber Vision is available for order today. Please visit the Cisco Ordering home page for more information.

Table 9. Cyber Vision product IDs

Product ID	Product description
CV-LICENSE	Cyber Vision subscription license*
CV-CNTR-M6N	Cyber Vision Center hardware appliance (Cisco UCS C225 M6N Rack Server)
IC3000-2C2F-K9	Cyber Vision Sensor hardware appliance (Cisco IC3000 Industrial Compute Gateway)
CV-IDS-CNTR	Talos subscriber rules license for the IDS running on the Cyber Vision Center (hardware and virtual appliance) or the Docker sensor
CV-IDS-IC3000	Talos subscriber rules license for Cyber Vision IDS on IC3000-2C2F-K9 sensor
CV-IDS-IR8300	Talos subscriber rules license for Cyber Vision IDS on Catalyst IR8300 sensor
CV-IDS-C9000	Talos subscriber rules license for Cyber Vision IDS on Catalyst 9300/9300X/9400 sensor

* The Cyber Vision Advantage license includes the Cisco Secure Equipment Access Advantage license for the same number of endpoints.

© 2025 Cisco and/or its affiliates. All rights reserved.

Warranty information

Please refer to the respective data sheets for the IC3000 Industrial Compute Gateway and the Cisco UCS C225 M6N Rack Server for warranty information.

Cisco environmental sustainability

Please refer to the respective data sheets for the IC3000 Industrial Compute Gateway and the Cisco UCS C225 M6N Rack Server for sustainability information.

Cisco and Partner Services

Services for planning, deploying, and support

Services provided by Cisco and our certified partners are available to help you through the assessment, design, deployment, and operational phases of your Cisco Cyber Vision project. Whether you need some expert advice, support throughout the entire project, or something in between, we, together with our partners, have the experts and expertise to help you be successful. For more information, visit https://www.cisco.com/go/services.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

© 2025 Cisco and/or its affiliates. All rights reserved.

Document history

New or revised topic	Described in	Date
Added support for Catalyst IE9300 Rugged switches, FIPS compliance	Version 4.1.4	January 2023
Added details on visibility features and availability of others	Version 4.2	April 2023
Added support for UCS M6, Catalyst 9300X switches, and new features	Version 4.3	November 2023
Removed UCS M5. Added support for Cisco XDR and FMC CSDAC	Version 4.4	April 2024
Added support for Catalyst IR1800 Rugged routers and ZTP	Version 5.0	July 2024
Added Docker sensor and new features	Version 5.1	December 2024
Added ZTNA remote access capabilities, Nutanix support, licensing updates, and new features	Version 5.3	August 2025

© 2025 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)