Cisco Cyber Vision

Cisco® Cyber Vision enables organizations to ensure the continuity, resilience, and safety of their industrial operations by providing continuous visibility into their Industrial Control Systems (ICS) to understand their security posture, improve their industrial networks efficiency, and extend IT security to their industrial operations.

Contents

Product overview

The deeper integration between IT, cloud, and industrial networks is exposing your Industrial Control Systems (ICS) to cyber threats. As you begin to capture the benefits of your industry digitization efforts and start deploying Industrial Internet of Things (IIoT) technologies, you need a cybersecurity solution to help you ensure the continuity, resilience, and safety of your industrial operations.

Cisco Cyber Vision has been specifically designed for industrial organizations to gain full visibility into their industrial networks, providing precise information on their OT security posture so they can build secure infrastructures, drive regulatory compliance, and enforce security policies to control risks.

Cisco Cyber Vision combines a unique edge monitoring architecture and deep integration with Cisco's leading security portfolio. Built into your Cisco industrial network equipment, it can be easily deployed at scale to monitor your industrial assets and their application flows in real time. It is the ideal solution to feed your IT Security Operations Center (SOC) with OT context, so you can build a unified IT/OT cybersecurity architecture.

Features and benefits

Table 1. Features and benefits

Feature	Benefit
Unique edge architecture	Easily deploy OT security at scale. Cyber Vision sensors are embedded in select Cisco networking equipment so you don't have to deploy dedicated appliances or build an out-of-band SPAN collection network. Cyber Vision can also monitor industrial networks built with third-party equipment.
Zero-touch provisioning	Automate enrollment of Cyber Vision sensors and deploy large scale infrastructures in minutes. Keep sensors always up-to-date without any manual task or service interruption.
No network overload	No need for additional network resources. Cyber Vision sensors decode industrial network traffic at the edge and only send lightweight metadata to the Cyber Vision Center. This unique architecture only adds 2% to 5% load to your industrial network.
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.
100% visibility	Only Cyber Vision's distributed edge active discovery can give you 100% visibility into your industrial network. It sends targeted inquiries to assets from sensors embedded in network equipment, so these messages are not blocked by firewalls or Network Address Translation (NAT) boundaries, resulting in 100% visibility.
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.
Dynamic asset inventory	Build appropriate security policies and increase operational efficiency. Cyber Vision gives you real-time, detailed visibility into your industrial assets, their communication patterns, and application flows.

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.
Document zones and conduits	Easily build security policies. Cyber Vision lets you group assets into zones (production cells, buildings, substations, etc.) so operation teams can share logical network information with IT and build security policies according to ISA/IEC 62443.
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.
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.
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.
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.
Vulnerability detection	Keep your industrial assets safe. Cyber Vision alerts you to hardware and software vulnerabilities that need to be patched.

Feature	Benefit
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.
Correlate IT/OT security events	Enhance your security event management practice. Cyber Vision is pre-integrated with leading SIEM and SOAR platforms such as IBM QRadar or SPLUNK, 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 others) 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 many third-party solutions such as firewalls or 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.

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.

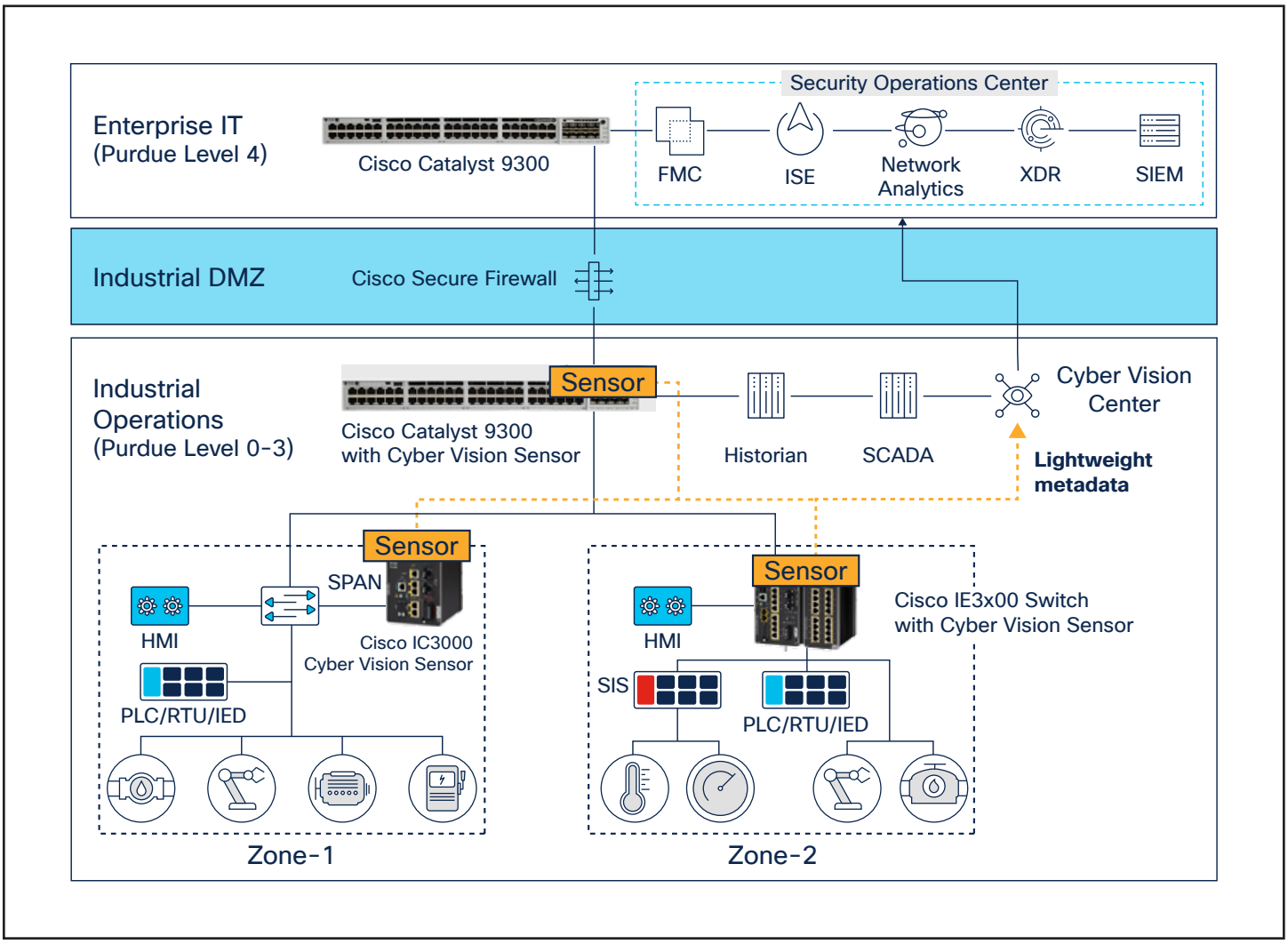

Figure 1. Cyber Vision's network sensors provide the flexibility for gaining visibility at scale without impacting network performance

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.

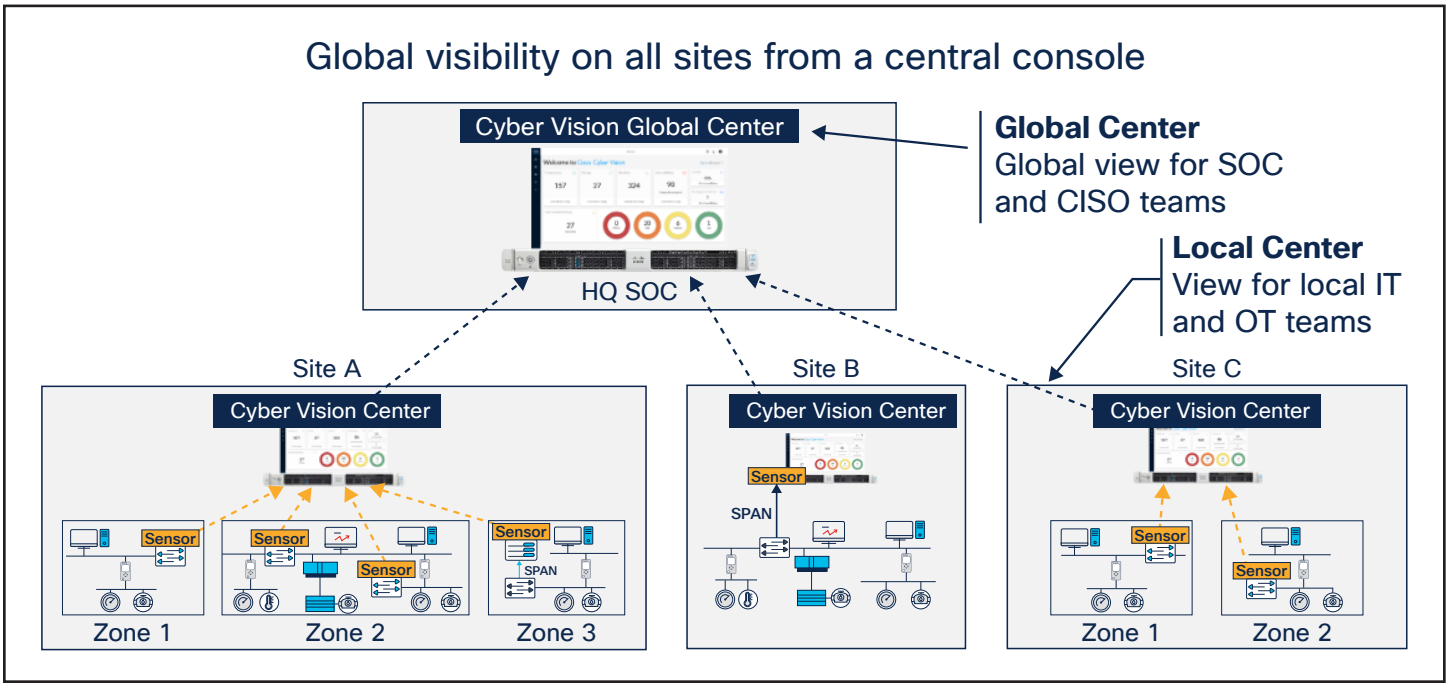

Figure 2. Cyber Vision leverages a nonintrusive edge architecture to offer detailed information to local and global stakeholders

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.

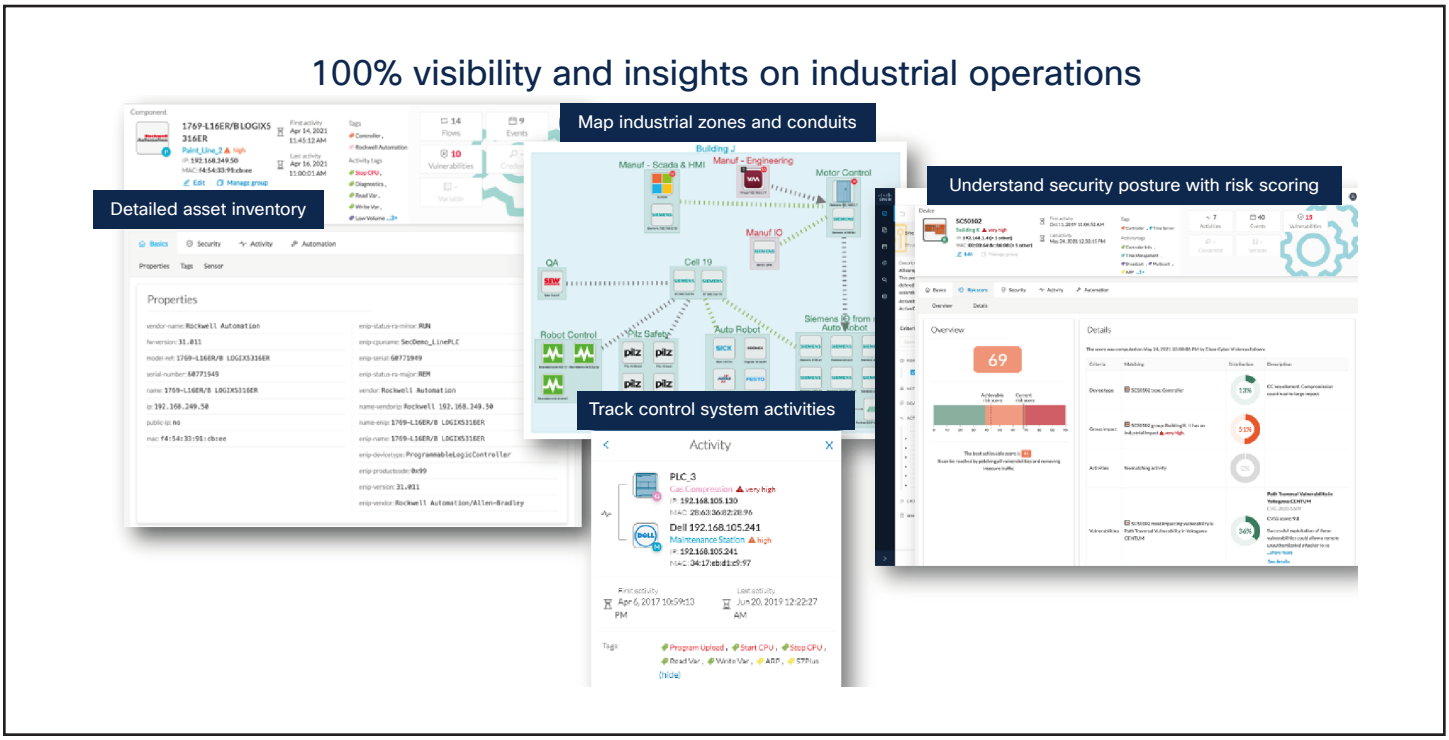

Figure 3. Gain operational insights into your assets, industrial processes, communication flows and your security posture

IT security integrations

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 risk and compliance monitoring and reporting, security policy enforcement, and much more. It extends the IT SOC to the OT domain.

Cyber Vision integrates seamlessly with leading SIEM systems such as IBM QRadar or SPLUNK so security analysts can trace industrial events in their existing tools and start correlating OT/IT events. Leveraging Cyber Vision's rich API, IT and OT teams can feed any existing tool with deep knowledge on industrial assets, network traffic, and security posture.

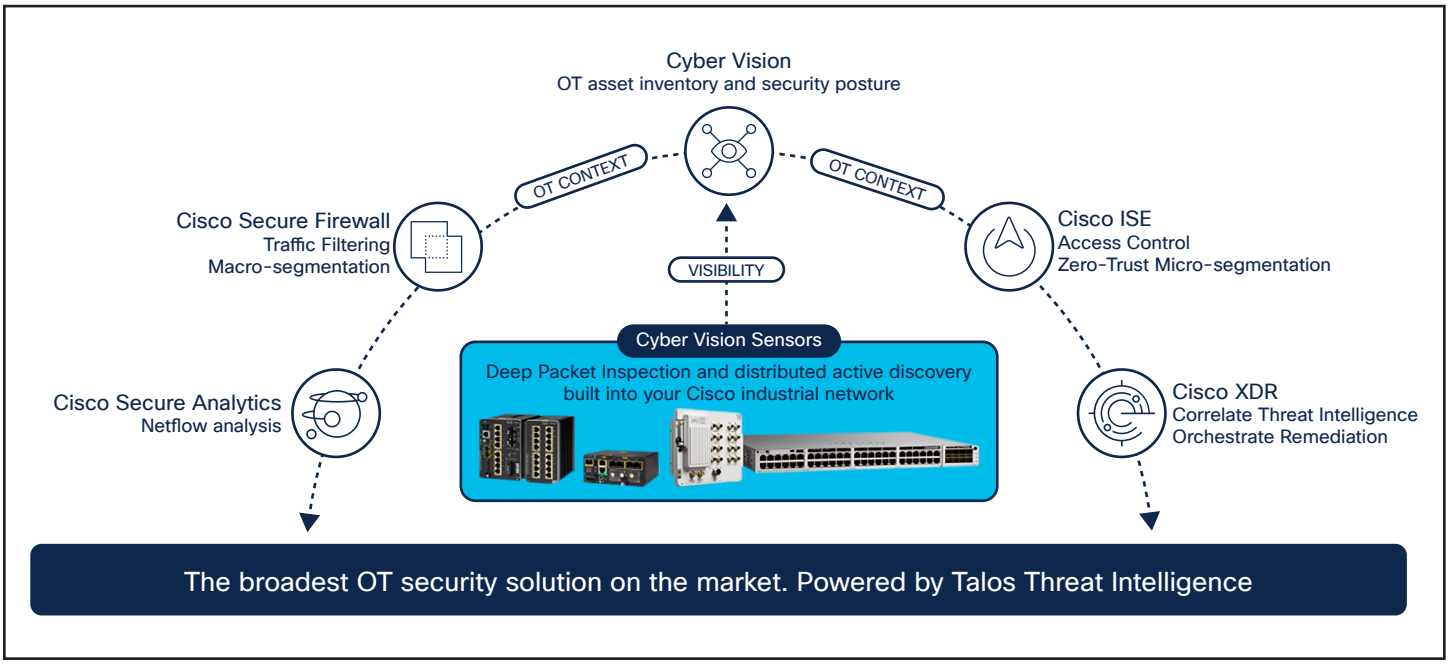

Figure 4. Cyber Vision extends your IT security operations to OT by feeding your existing tools with context on industrial assets and events

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.

Cisco Secure Firewall

Network segmentation is a key pillar to securing your network and protecting critical processes. Cyber Vision can share asset groups created by control engineers with Firewall Management Center (FMC) to influence access control policies managed by Cisco Secure Firewall and restrict 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.

For more information on using dynamic attributes in Cisco Secure Firewall policies, please read this documentation.

Cisco Identity Services Engine (ISE)

Extend software-based network segmentation policies to your industrial control network and start enforcing zero trust security. Cyber Vision shares discovered hosts, protocols, communications patterns, and more with Cisco ISE through pxGrid to extend ISE's awareness and policy enforcement into the control network. Cisco ISE can also leverage asset groups created by control engineers in Cyber Vision to automatically build secure zones and drive dynamic micro-segmentation of 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.

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 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 IBM QRadar and Splunk OT.

Platform support

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

Table 2. Platforms for Cyber Vision products

Product components	Platforms supported
Hardware sensor appliance	Cisco IC3000 Industrial Compute Gateway (IC3000-2C2F-K9)
Network sensor	Cisco Catalyst® IE3300 Rugged Series switch (models with 4 GB RAM only) Cisco Catalyst IE3400 Rugged Series switch Cisco Catalyst IE3400 Heavy Duty Series switch Cisco Catalyst IE9300 Rugged Series switch Cisco Catalyst IR1100 Rugged Series Routers Cisco Catalyst IR1800 Rugged Series Routers Cisco Catalyst IR8300 Rugged Series Router Cisco Catalyst 9300 and 9300X Series switch Cisco Catalyst 9400 Series switch Rockwell Stratix 5800 switch
Center hardware appliance	Cisco UCS C225 M6N Rack Server (CV-CNTR-M6N configuration)
Center software appliance	VMware ESXi software appliance Microsoft Hyper-V software appliance Amazon AWS software appliance Microsoft Azure software appliance

Cyber Vision sensor hardware specifications

Please refer to the associated data sheets for hardware specifications:

- Cisco IC3000 Industrial Compute Gateway
- Cisco Catalyst IE3300 Rugged Series switch
- Cisco Catalyst IE3400 Rugged Series switch
- Cisco Catalyst IE3400 Heavy Duty Series switch
- Cisco Catalyst IE9300 Rugged Series switch
- Cisco Catalyst IR1100 Rugged Series Routers
- Cisco Catalyst IR1800 Rugged Series Router
- Cisco Catalyst IR8300 Rugged Series Router
- Cisco Catalyst 9300 and 9300X Series switch
- Cisco Catalyst 9400 Series switch
- Rockwell Stratix 5800 switch

Cyber Vision Center hardware appliance specifications

Table 3. 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

Item	CV-CNTR-M6N
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
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 4. 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 5. Cisco Cyber Vision Global Center scale

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

Cyber Vision Center virtual appliance specifications

Table 6. Minimum specifications* for the Cyber Vision Center virtual appliance

Characteristic	Private Cloud	Public Cloud
CPU	Intel Xeon, 10 cores	Intel Xeon, 10 cores
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	• 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.

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.

Table 7. Licensing tiers

Licensing levels	
Essentials	Advantage
Inventory • Device inventory • Identify communication patterns • Generate inventory reports **Vulnerability** • Identify device vulnerabilities • Generate vulnerability reports **Activities** • Track control system events • Generate device activity reports **Restful API** • REST API programming interface	Includes Essentials features, plus: **Security Posture** • Device Risk Scoring • Security posture 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 **Advanced integration** • Cisco XDR Ribbon • pxGrid integration with ISE • Firepower Host Attribute integration • SIEM Integration – Splunk, IBM 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 Catalyst IR8300 Rugged router and the Catalyst 9300, 9300X or 9400 switches.

Ordering information

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

Table 8. 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 Cyber Vision Center IDS (hardware and virtual appliance)
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

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.

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

C78-743222-07 07/24