Cisco Cyber Vision

Contents

Cisco® Cyber Vision enables organizations to ensure the continuity, resilience, and safety of their industrial operations by providing continuous visibility into their ICS infrastructures and controlling the risks of cyber attacks.

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 cyber security 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, so they can ensure process integrity, 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
Comprehensive visibility	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.
Operational insights	Maintain process integrity by tracking unexpected variable changes and Programmable Logic Controller (PLC) program modifications. Cyber Vision supports operations to work more efficiently and with reduced risk.
Vulnerability detection	Keep your industrial assets safe. Cyber Vision alerts you to hardware and software vulnerabilities that need to be patched.
Intrusion detection (IDS)	Uncover the cybersecurity threats coming from your IT network. Cyber Vision detects known and emerging threats to keep you protected.
Anomaly detection	Keep your ICS safe from unknow attacks and malfunctions. Detect illegitimate modifications to your industrial assets and processes such as unexpected program downloads or variable changes.
Edge architecture	Easily deploy ICS security at scale. Cyber Vision is built into your network equipment for reduced hardware spending and minimal impact to industrial control network traffic.
OT tags	Immediately understand what each device is doing. Cyber Vision translates each application flow 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.
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.
Deep Packet Inspection (DPI)	Track the content of all application flows. Cyber Vision "understands" the ICS protocols you use so it can profile your industrial assets and detect abnormal behaviors or malfunctions.
OT flight recorder	Meet compliance requirements. Cyber Vision maintains the history of all events and application flows, including variable accesses so you can easily run forensic searches and build incident reports.
Deep IT security integration	Build a unified OT/IT SOC. Cyber Vision feeds your IT security platforms with OT context so you can enforce security policies without disrupting production.

Security built into your industrial network

Deploying OT cybersecurity can quickly become very complex, especially if the industrial network is dispersed across an entire country or many remote industrial sites. For your OT cybersecurity project to be successful, you must be able to scale it easily and at a reasonable cost across your entire organization.

Cisco Cyber Vision leverages a unique edge computing architecture that enables security monitoring components to run within Cisco's industrial network equipment. There's no need to source dedicated appliances and think about how to install them. 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.

Visibility

Securing your OT infrastructure starts with having a precise view of your asset inventory, communication patterns, and network topologies. Cisco Cyber Vision gives OT teams and network managers full visibility into their assets and application flows so they can implement security best practices, drive network segmentation projects, and improve operational resilience.

Cisco Cyber Vision automatically uncovers the smallest details of the production infrastructure: vendor references, firmware and hardware versions, serial numbers, PLC rack slot configuration, etc. It identifies asset relationships, communication patterns, changes to variables, and more. This wealth of information is shown in various types of maps, tables, and reports that maintain a complete inventory of industrial assets, their relationships, their vulnerabilities, and the programs they run.

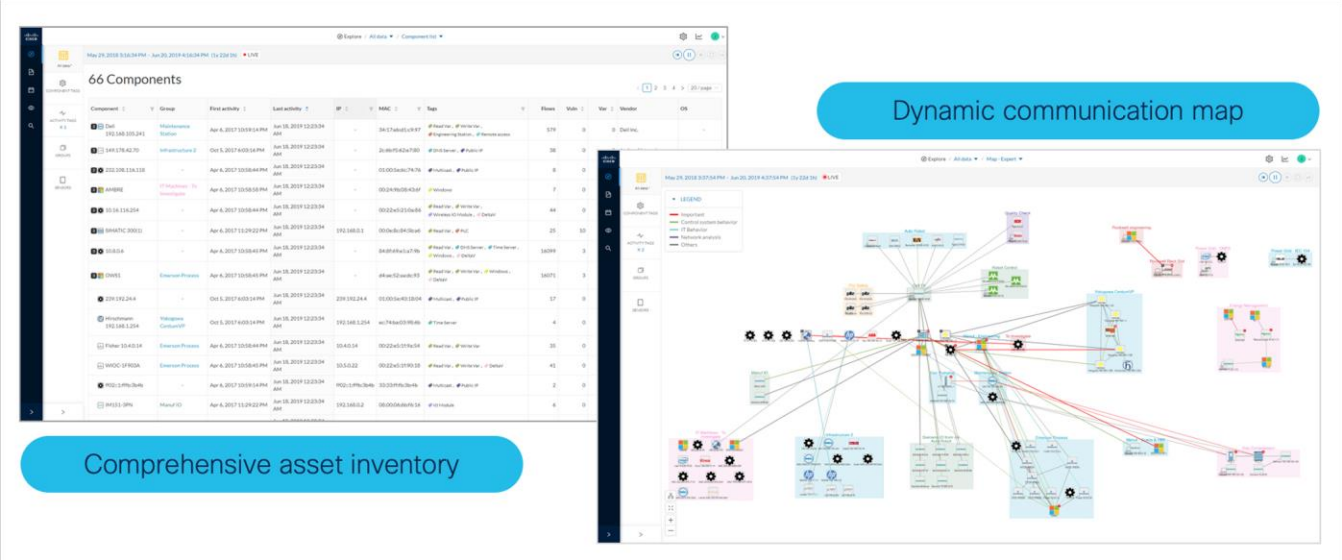

Figure 1.
Examples of Cyber Vision information displays

Operational insights

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 take action to maintain system integrity and production continuity. Cyber experts can easily dive into all this data to analyze attacks and find the source. Chief information security officers have all the necessary information to document their incident reports.

Cisco Cyber Vision "understands" the proprietary OT protocols used by automation equipment, so it can track process anomalies, errors, misconfigurations, and unauthorized industrial events. It also records these events, becoming the "flight recorder" of the industrial infrastructure.

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.

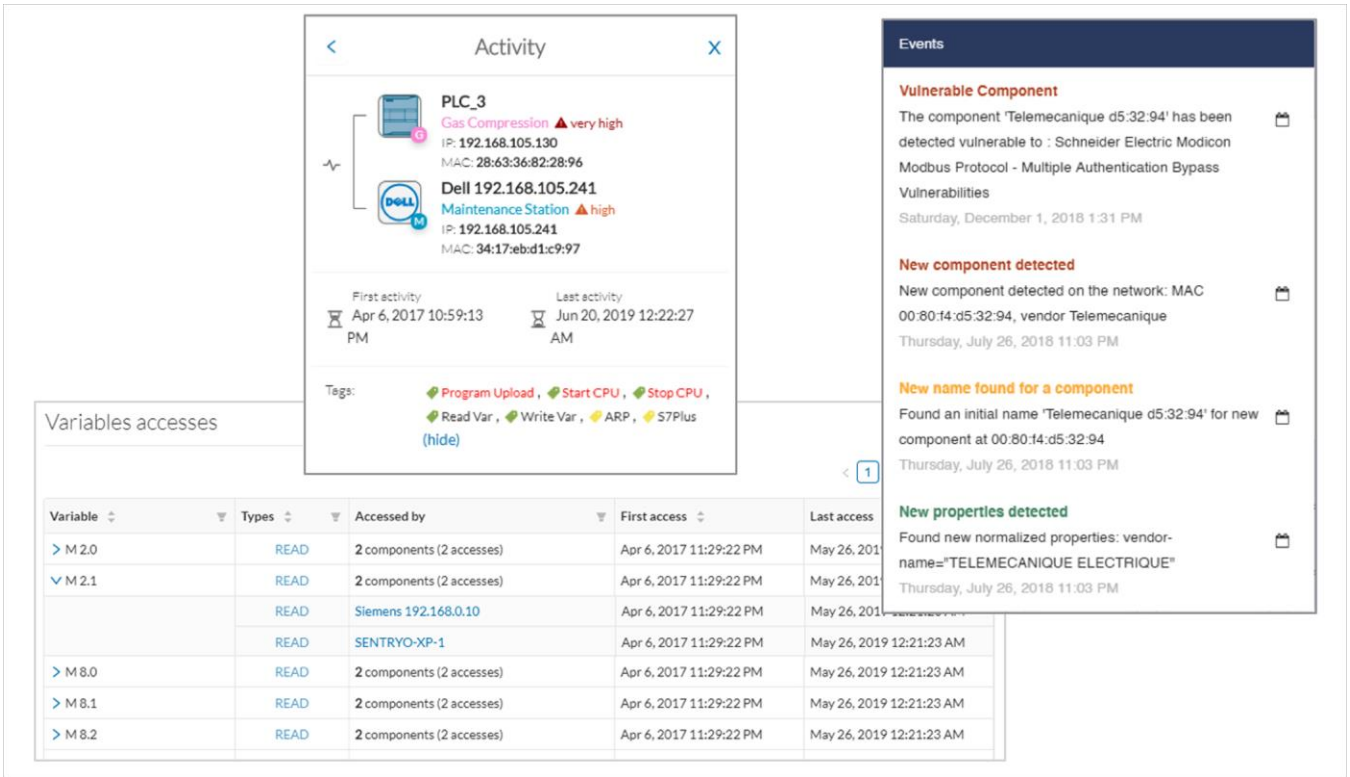

Figure 2.
Operational insights

Threat detection and remediation

With industrial networks ever more connected to IT networks, protecting them from the usual IT threats, such as malware or intrusions, becomes increasingly important. And because attacks on industrial networks generally look like legitimate instructions to assets, you also need to detect those unwanted process modifications. To secure an industrial network, you need a variety of threat detection mechanisms.

Cisco Cyber Vision combines protocol analysis, intrusion detection, and behavioral analysis to detect any attack tactic. This holistic approach helps ensure that Cyber Vision can detect both known and unknown attacks as well as malicious behaviors that could be warning signs of an attack. Cyber Vision integrates seamlessly with IT SOCs so security analysts can trace industrial events in their Security Information and Event Management (SIEM) system for OT/IT correlation and automatically trigger firewall filter rules in the event of an attack.

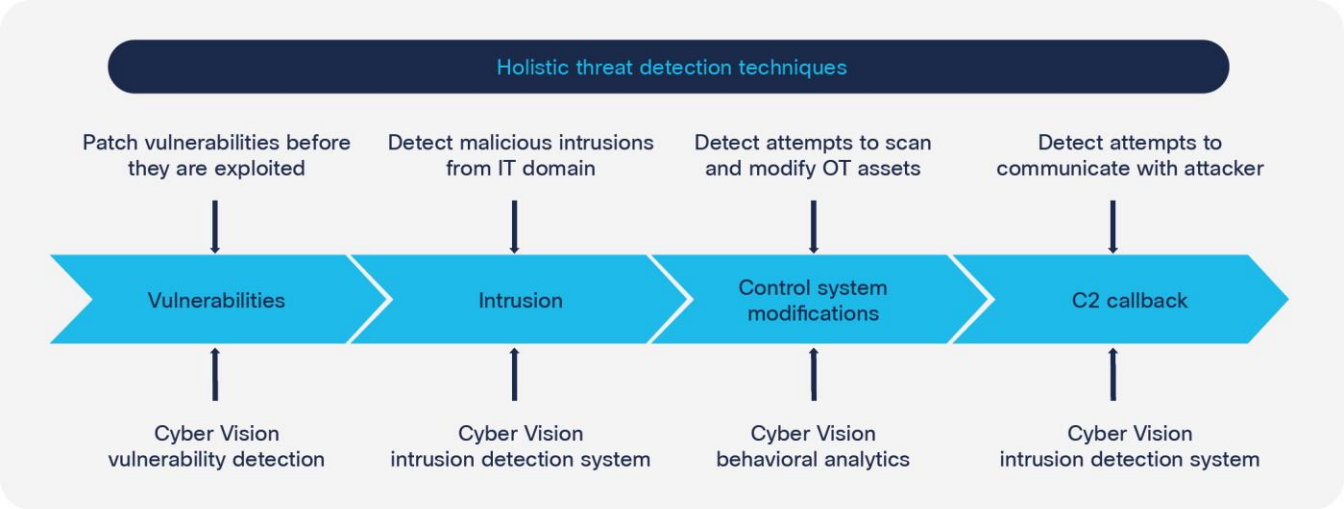

Figure 3.
Detecting and remediating threats

Platform support

Cisco Cyber Vision is built on a two-tier architecture consisting of multiple sensor devices that perform deep packet inspection, protocol analysis, and intrusion detection at the edge 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, and more. It may be run on a hardware appliance or as a VMware virtual machine, and the sensor runs on the Cisco IC3000 Industrial Compute Gateway.

Table 2. Platforms for Cyber Vision products

Product components	Platforms supported
Cyber Vision Sensor hardware appliance	Cisco IC3000 Industrial Compute
Cyber Vision Center hardware appliance	Cisco UCS® C220 M5 Rack Server
Cyber Vision Center software appliance	VMware ESXi 6.x or later

Please visit the product pages for the Cisco UCS 220 M5 and the IC3000 Industrial Compute Gateway for hardware specifications.

Licensing

Cisco Cyber Vision is licensed using a recurring subscription model based on the number of endpoints monitored and is available in 1-, 3-, and 5-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.

Table 3. Licensing tiers

Licensing levels	
Essentials	**Advantage**
• Asset discovery and inventory • Vulnerability detection • Operational insights	Includes Essentials plus: • Anomaly detection • Third-party integration

Endpoint license packs are available for 100, 250, 500, 750, 1000, 2500, 5000, 7500, and 10,000 endpoints.

Intrusion Detection System (IDS) licensing is available to Advantage subscribers and is licensed per IC3000 sensor appliance deployed.

System requirements

The Cyber Vision Center hardware appliance is available in the configuration shown in the table below. Requirements for the Cyber Vision Center as a virtual machine depend on the volume of data the platform will have to collect and analyze.

Table 4. Specifications for the Cyber Vision Center hardware appliance

Characteristic	Cyber Vision Center hardware appliance	Minimum VM requirements*
CPU	Intel® Xeon® 2.3 GHz with 16 cores	Intel Xeon, 4 cores minimum
Memory	64 GB	8 GB minimum
Storage	800-GB SSD RAID-1 or 800-GB SSD RAID-10	50-GB SSD minimum
Virtualization software	NA	VMware ESXi 6.x or later

* These minimum VM requirements support monitoring of up to 500 devices

Ordering information

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

Table 5. Cyber Vision product IDs

Product ID	Product description
CV-LICENSE	Cyber Vision subscription license
CV-CNTR-M5S5	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server)
CV-CNTR-ESXI	Cyber Vision Center software appliance for VMware ESXi (included with Cyber Vision subscription)
IC3000-2C2F-K9	Cyber Vision Sensor hardware appliance (Cisco IC3000 Industrial Compute)
CV-IDS-IC3K-PROMO	Cyber Vision Sensor IDS license for IC3000-2C2F-K9

Warranty information

Please refer to the respective data sheets for the IC3000 Industrial Compute Gateway and Cisco UCS 220 M5 Rack Server for warranty information.

Cisco Environmental sustainability

Please refer to the respective data sheets for the IC3000 Industrial Compute Gateway and Cisco UCS 220 M5 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.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-743222-00 01/20