Cisco Industrial Security

A comprehensive OT security solution fused into the network to protect industrial operations at scale

Industrial organizations today face a perfect storm of cybersecurity threats, operational complexity, and evolving regulatory requirements. Securing Industrial Control Systems (ICS) and Operational Technologies (OT) is a top priority, but you might wonder where to start. Underlying networks can be very complex and often involve legacy technologies and inadequate security procedures.

For over 20 years, Cisco® has been helping industrial organizations digitize and secure operations. Our deep understanding of operational technology requirements plus networking and security solutions that are purpose-built for industrial use cases is a rare combination. Not only does Cisco offer comprehensive OT security capabilities, we're also fusing security with the industrial network to provide better visibility, simpler deployment at scale, lower costs, and eliminate gaps in defense.

Benefits

- Gain full visibility into connected assets, vulnerabilities, and activities
- Protect distributed field assets with advanced and secure WAN connectivity
- Secure remote access with self-service zero-trust network access made for OT
- Safeguard operations by implementing ISA/IEC 62443 zones and conduits
- Enforce micro-segmentation policies that do not interfere with OT processes
- Better detect advanced threats with unified visibility across IT and OT domains
- Simplify remediation with workflows orchestrating tasks across your security technologies

Gaining visibility into industrial networks at scale

You can't protect what you can't see. Without detailed, real-time visibility into every connected OT asset and their communications patterns, your industrial network remains vulnerable. And your ability to protect operations from cyber threats is compromised. Traditional approaches to OT visibility rely on dedicated appliances or SPAN collection networks, leading to unbearable hidden costs and operational headaches preventing you to deploy at scale.

Cisco Cyber Vision revolutionizes how you gain comprehensive visibility into your OT environments. It embeds Deep Packet Inspection (DPI) and safe active discovery capabilities into your switches and routers, turning your entire industrial network into a powerful visibility sensor.

Cisco's innovative approach means:

- Get OT visibility at scale by using your network infrastructure as the sensor.
- Lower costs by eliminating the need for out-of-band collection networks. Cyber Vision adds only 2–5% load on the network.
- Identify all industrial assets, their profiles and vulnerabilities, even those sitting behind NAT or firewall boundaries.
- Benefit from Cyber Vision even in non-Cisco networks by using compute hardware or SPAN collection networks to gain visibility.
- Visualize activities between assets to drive segmentation policies and detect abnormal behaviors.
- Drive regulatory compliance by documenting networks and assets as required by IEC 62443, NIS2, NERC CIP-015, and more.

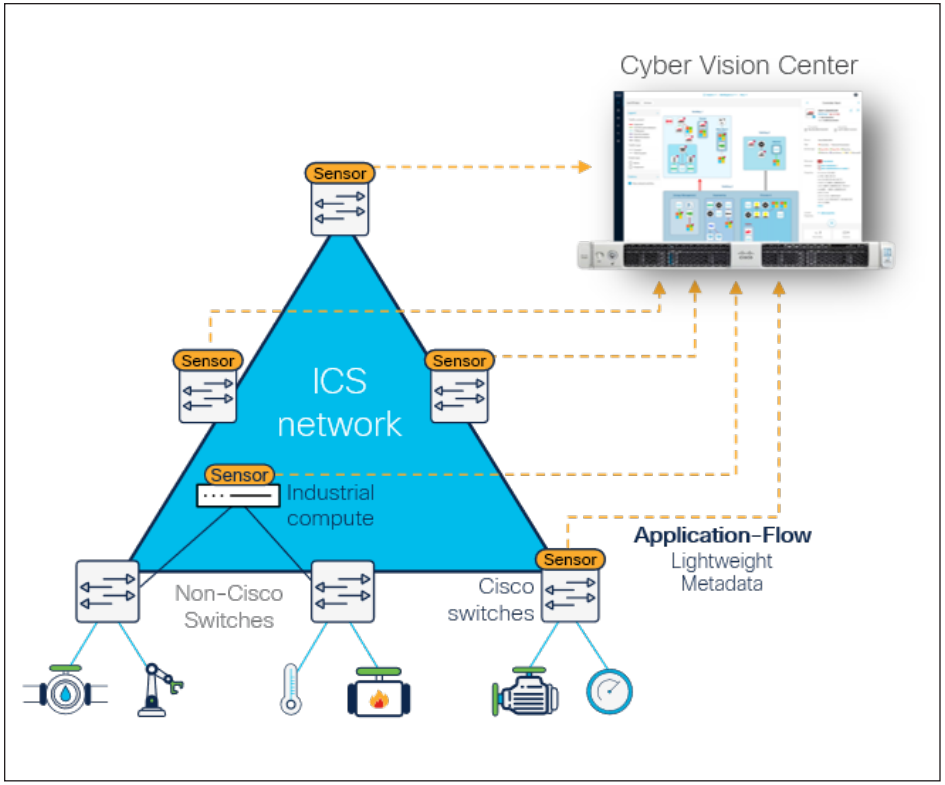

Figure 1. Cisco Cyber Vision runs DPI in switches or routers and sends only lightweight metadata to the console

Learn how to gain comprehensive OT visibility with Cisco Cyber Vision in this **solution brief**.

Securing distributed field industrial networks

Many industrial operations depend on distributed assets: pipelines, power grids, water treatment facilities, renewable energy sites, EV charging stations, roadways, transportation systems, and more. In these rugged, distributed environments, organizations have traditionally faced a dilemma: choose solutions optimized for advanced WAN connectivity or those focused on robust cybersecurity.

Cisco eliminates this trade-off. Our industrial routers redefine connectivity by seamlessly integrating the best of SD-WAN networking with comprehensive OT security. They are purpose-built for industrial settings, packing advanced and modular WAN capabilities alongside built-in Next-Generation Firewall (NGFW) features, malware protection, zero-trust remote access, and comprehensive visibility into assets, behaviors, and vulnerabilities.

Cisco's innovative approach gives you defense-in-depth across your entire distributed industrial infrastructure:

- Next-generation firewall to control traffic to and from remote sites
- Malware protection and threat intelligence
- Asset visibility through integrated Cyber Vision capabilities
- Zero-trust remote access capabilities built in
- Traffic prioritization to ensure critical commands reach equipment reliably
- Simplified centralized deployment and management at scale
- Consistent security policies from headquarters to field sites
- Lower total cost of ownership with modular hardware that evolves when your needs or technologies change

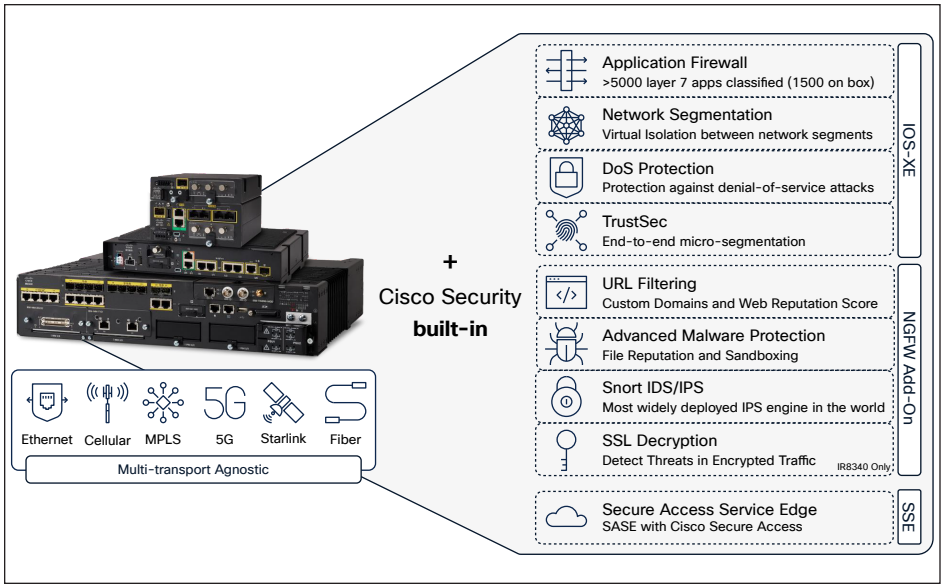

Figure 2. Cisco industrial routers are the foundation of agile and resilient distributed industrial operations

Learn about securing distributed field industrial networks with Cisco in this solution brief.

Protecting industrial plant networks

The drive for plant modernization, fueled by advanced industrial automation, controller virtualization, and industrial AI, is transforming operational networks. Cisco Secure Firewalls provide robust protection at critical control points: the IT/OT boundary, industrial data centers, and the plant floor, preventing lateral movement. They offer advanced threat prevention and granular control over specific OT protocols, even enabling virtual patching for legacy systems to minimize downtime.

Complementing this, Cisco Cyber Vision delivers unparalleled visibility into your connected industrial assets to help build and update firewall rules so they are always aligned with your industrial processes. This eliminates tedious manual configuration and fosters critical IT/OT collaboration.

Cisco's industrial security solution helps you drive macro-segmentation to enable secure industrial modernization:

- Control traffic in and out of your industrial plants, industrial data centers, and large plant floor segments.
- Segment industrial zones in a dynamic manner with firewall rules updated using real-time visibility from Cyber Vision.
- Prevent malware spread and isolate security incidents to avoid extensive downtime.
- Safeguard outdated devices with virtual patching blocking malicious traffic before it reaches them.
- Protect industrial control systems with application-aware policies capable of filtering SCADA and OT function codes.

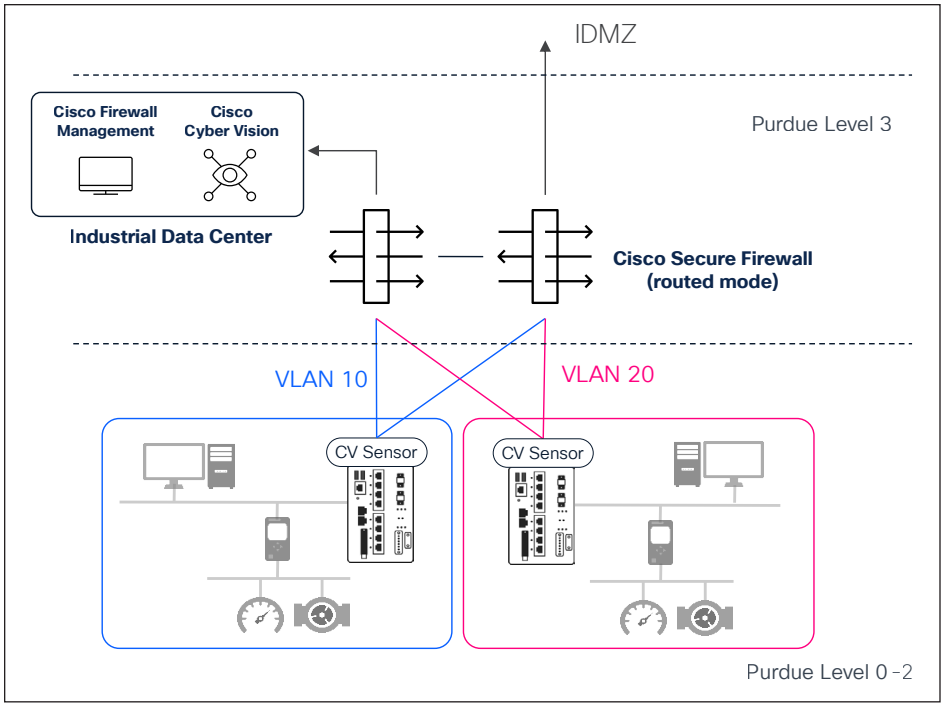

Figure 3. Cisco Secure Firewall deployed in Level 3 can terminate OT VLANs to enforce zone and conduit segmentation

Learn about protecting plant networks with Cisco in this solution brief.

Driving micro-segmentation in industrial settings

Modern industrial operations demand connecting an ever-growing number of OT and IoT assets. You need a simple, adaptive way to enforce the right access policies to all these devices based on industrial process constraints and the needs of the OT teams.

Cisco delivers a unique, integrated approach combining Cisco Cyber Vision with Cisco Identity Services Engine (ISE). Cyber Vision provides unparalleled visibility into all industrial assets, enabling OT teams to intuitively group devices into logical zones. This intelligence automatically feeds into Cisco ISE, enabling policy-based enforcement that adapts instantly when OT experts move, add, or change assets.

- Segment your OT networks in weeks, not years with comprehensive visibility and deep insights into all assets.
- Enforce granular micro-segmentation for individual devices or small groups to elevate or deny specific privileges.
- Automatically adjust policies as OT assets are moved, added, or changed, ensuring continuous protection without disrupting operations.
- Secure every port of physically accessible network equipment to prevent unauthorized connections.
- Drive IT/OT collaboration by giving OT teams the tools they need to document industrial processes and inform security policies.

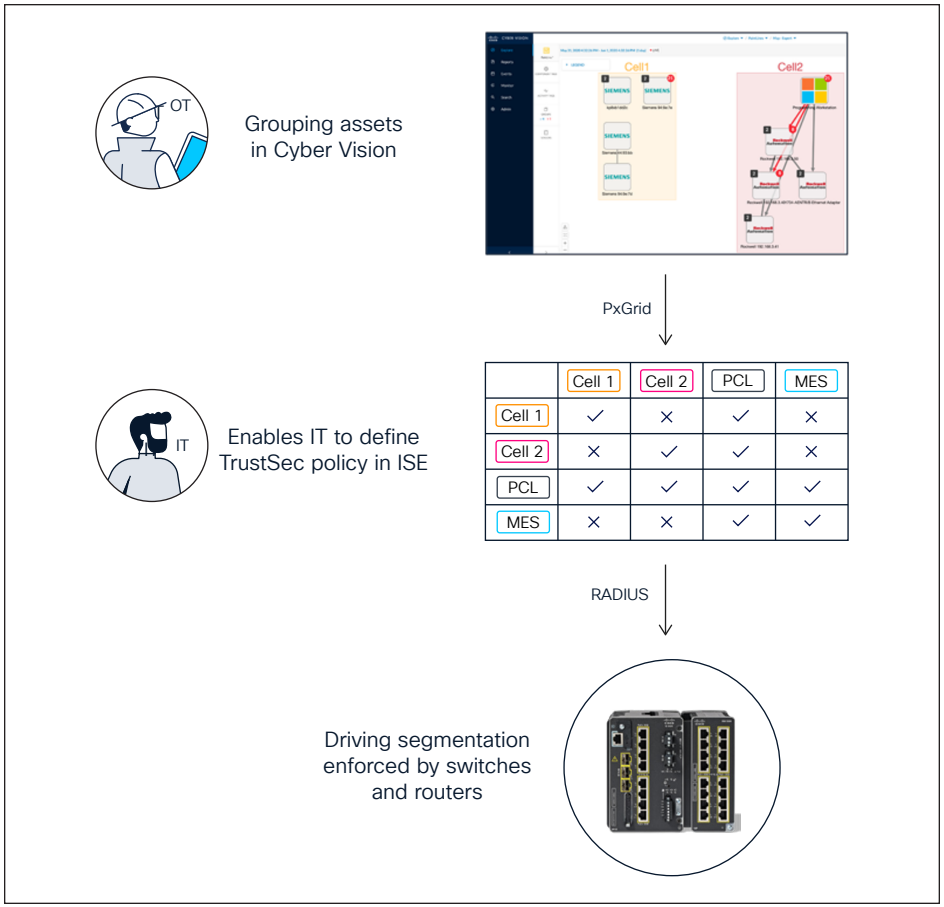

Figure 4. The Cisco OT micro-segmentation solution makes it simple to define access policies for OT assets while keeping OT teams in control

Learn about streamlining micro-segmentation in industrial networks with Cisco Cyber Vision and ISE in this solution brief.

Enabling secure remote access for industrial operations

Providing remote access to OT assets is critical to run and troubleshoot operations. Yet, traditional VPN solutions offer broad network access and are too complex to secure. Generic Zero-Trust Network Access (ZTNA) solutions are not designed to manage the frequent changes in remote users and the large number of assets typical of industrial operations. The unique scale, distributed nature, and IP addressing issues in OT demand a specialized approach.

With Cyber Vision's Secure Equipment Access (SEA), Cisco offers a purpose-built ZTNA cloud service for industrial needs. It makes it simple for OT teams to grant remote access, for IT teams to enforce least privilege access policies across sites and assets, and for remote users to access OT assets they need to service. It embeds the ZTNA gateway into Cisco switches and routers, enabling large-scale deployment without dedicated hardware.

Key benefits include:

- Enforce granular least-privilege access to control exactly who accesses what, when, and how.
- Manage all users, assets, and policies from a single cloud portal for all sites.
- Empower OT teams to easily manage remote access to run the business while complying with security policies.
- Easily deploy at scale with the ZTNA gateway software embedded in Cisco industrial networks.
- Drive compliance with robust security controls and comprehensive audit trails.

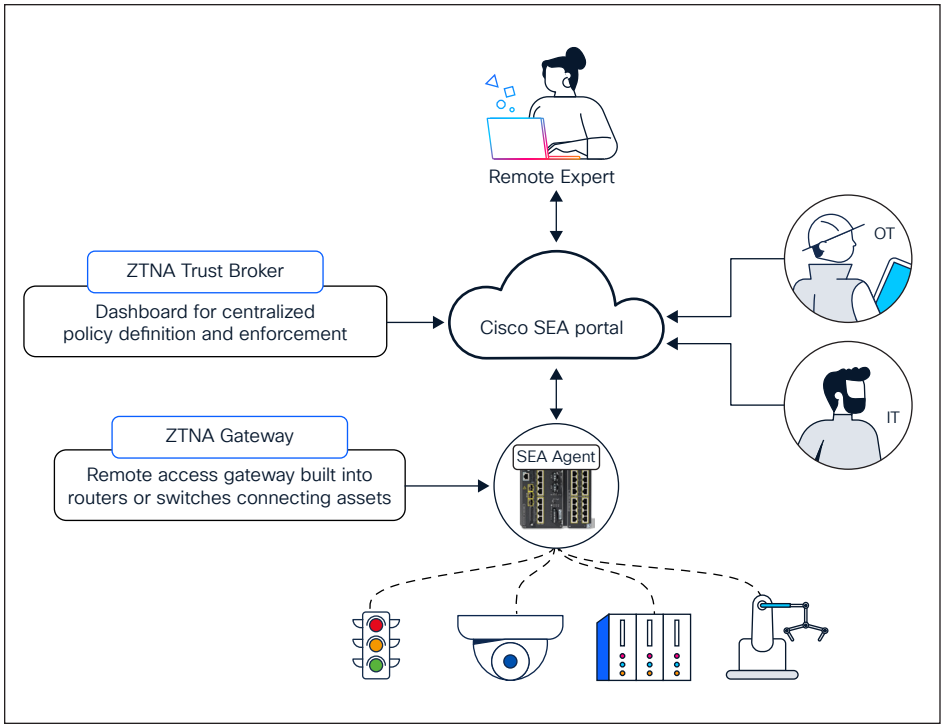

Figure 5. Cisco SEA is a self-service zero-trust remote access solution built into switches and routers, purpose built for OT workflows

Learn about Cisco's zero-trust remote access for industrial networks in this solution brief.

Investigating and responding to OT security threats

When security incidents occur, you need Threat Detection, Investigation, and Response (TDIR) capabilities to assess risks, understand the situation, and remediate threats quickly. Industrial security teams often struggle to act effectively because they lack comprehensive context and don't have the tools to guide them for fast, confident response.

Cisco Extended Detection and Response (XDR) simplifies security operations, providing a streamlined approach to quickly launch forensic investigations and remediation playbooks. It connects your entire security stack and threat intelligence feeds (Cisco and third party) to give you a complete view of threats and activities across your IT and OT networks. It is built into Cisco Cyber Vision offering a simple way to integrate powerful TDIR to your OT security practice.

Together, Cisco XDR and Cisco Cyber Vision offer key benefits:

- Quickly report OT security events to security analysts and manage cases using the XDR ribbon built into Cyber Vision.
- Launch detailed investigations with a single click, enriching observables with Talos® threat intelligence and data from other security tools in one console.
- Accelerate remediation using out-of-the-box and custom workflows to automate responses.
- Improve incident response with seamless information flow between SecOps, NetOps, and OT teams.

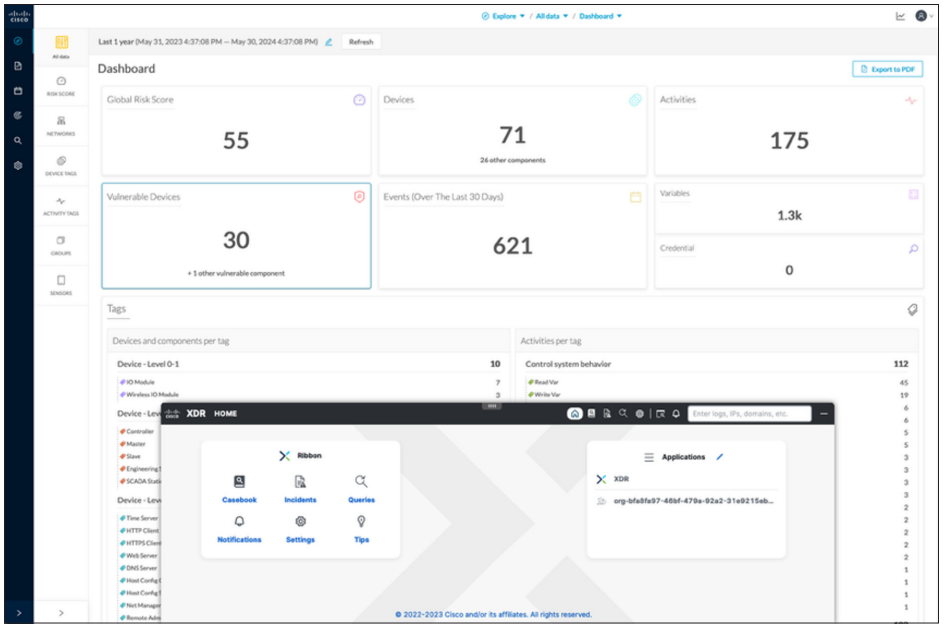

Figure 6. The Cisco XDR ribbon in Cyber Vision streamlines investigation and remediation orchestration across your entire security stack

Learn how to easily add powerful TDIR capabilities to your OT security practice in this solution overview.

Unifying IT and OT visibility to drive security operations

Industrial organizations with mature security operations and complex compliance requirements need an advanced Security Incident and Event Management (SIEM) solution to ingest, correlate, and analyze data from a large number of sources, enabling powerful analytics, advanced dashboards, and tailored reporting. Splunk Enterprise Security has been the SIEM market leader for over a decade and offers a wide range of features that are purpose-built for OT security management.

Advanced integration with Cisco Cyber Vision enables Splunk to unify visibility across IT and OT domains to help security teams to better detect, investigate, and remediate threats that may originate from IT and target OT (and vice versa). Custom dashboards help monitor the OT security posture across all sites and build views tailored to the exact needs of the OT teams.

Together, Splunk and Cyber Vision offer key benefits:

- Unify visibility across IT and OT domains to give security analysts a comprehensive view of the entire attack chain.
- Get a continuously updated IT and OT asset inventory augmented by multiple data sources to add rich context to security events, and identify compliance gaps and security control weaknesses.
- Drive compliance reporting with data that spans IT and OT systems and OT-specific use case libraries such as NERC-CIP compliance reports and MITRE ATT&CK ICS correlation rules.
- Detect advanced threats and anomalies in OT environments with AI and machine learning models.
- Monitor your OT security posture across all industrial sites with out-of-the-box and custom dashboards that can blend insights from security and production tools.

Figure 7. Splunk offers out-of-the-box and custom dashboards to drive OT security operations and meet the needs of OT teams

Learn how to extend the power of Splunk to drive OT security operations in this product brief.

Start securing your industrial operations with Cisco today

Talk to a Cisco sales representative or channel partner today.

Visit cisco.com/go/OTsecurity to learn more.

The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe 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.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack. Browse our library of validated design guides here: cisco.com/go/iotcvd.

C22-3370508-02 02/26