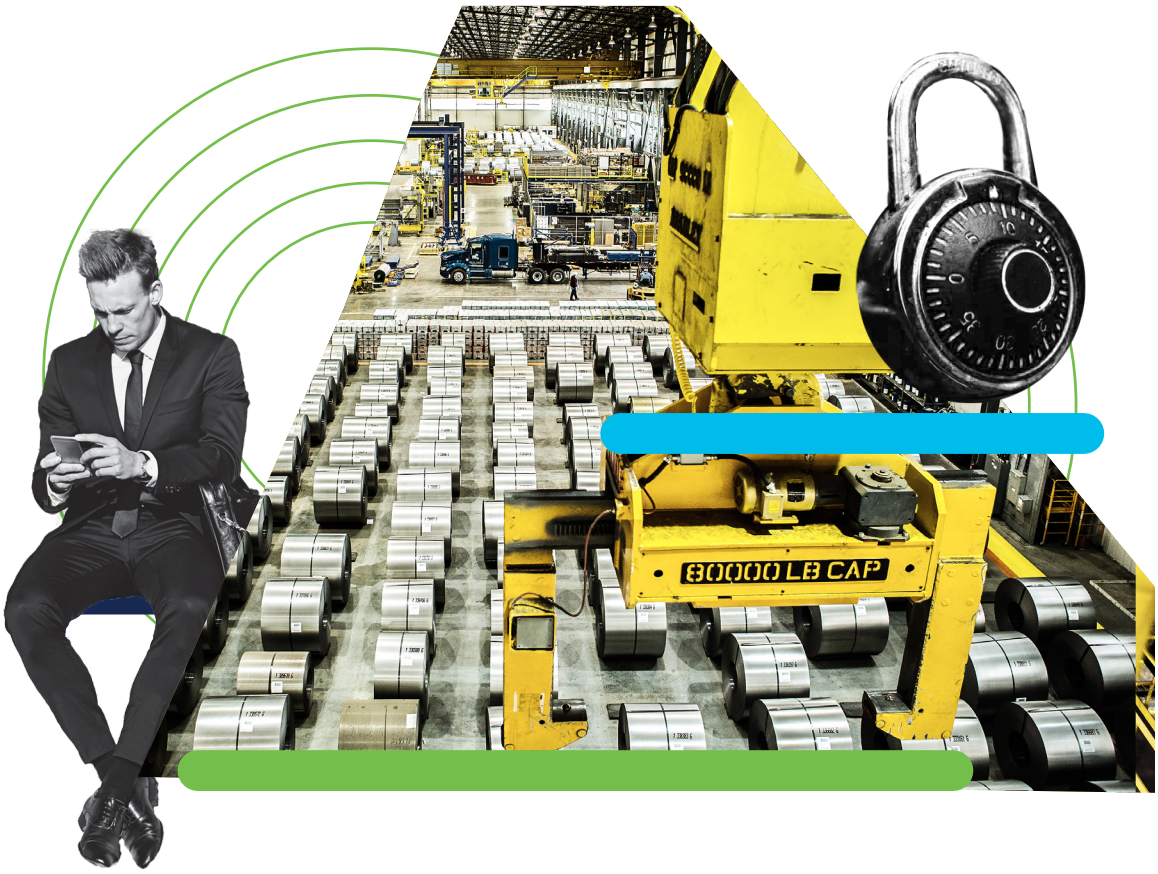
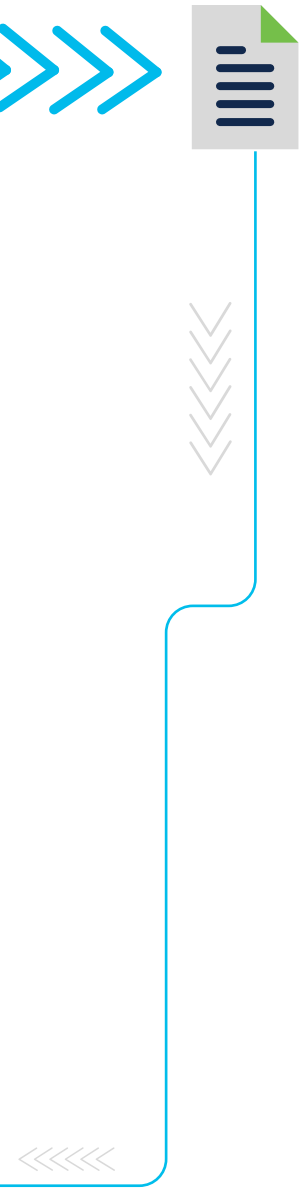
CISCO
SECURE

White paper
Cisco public

Harness the Power of Networking to Secure Industrial Operations



Contents



Executive overview

Protecting industrial networks and critical infrastructures against cyberthreats has always involved deploying point security products from different vendors: industrial firewalls, remote access gateways, asset visibility solutions, and more. Integrating many point products increases a network's cost and complexity to a level that may lead to gaps in defenses. As operational networks are becoming more complex and cyberthreats more prevalent, there must be a better way to secure operations at scale without putting an undesirable burden on IT and OT teams.

In all industries, organizations are accelerating digitization of their operations infrastructures and upgrading their networks to connect more assets and support more traffic. Rather than relying on the same old approach to network security, organizations should grab this network refresh opportunity to build a converged networking and security architecture in which security is built into the networking devices themselves.

Because it connects all systems and devices, the network is clearly in the best position to help protect operations. It can provide extensive visibility into connected assets and communication patterns, enabling the insights needed for threat detection. As all inbound and outbound traffic goes through an industrial switch or router, these networking devices are also best positioned to enforce security policies and provide remote access to devices.

This white paper explains how modern industrial network equipment can embed a full range of advanced security applications to build a converged architecture that will bring simplicity, ease of deployment, and cost savings and help scale industrial security to protect operations.

Traditional ways to secure operations are insufficient

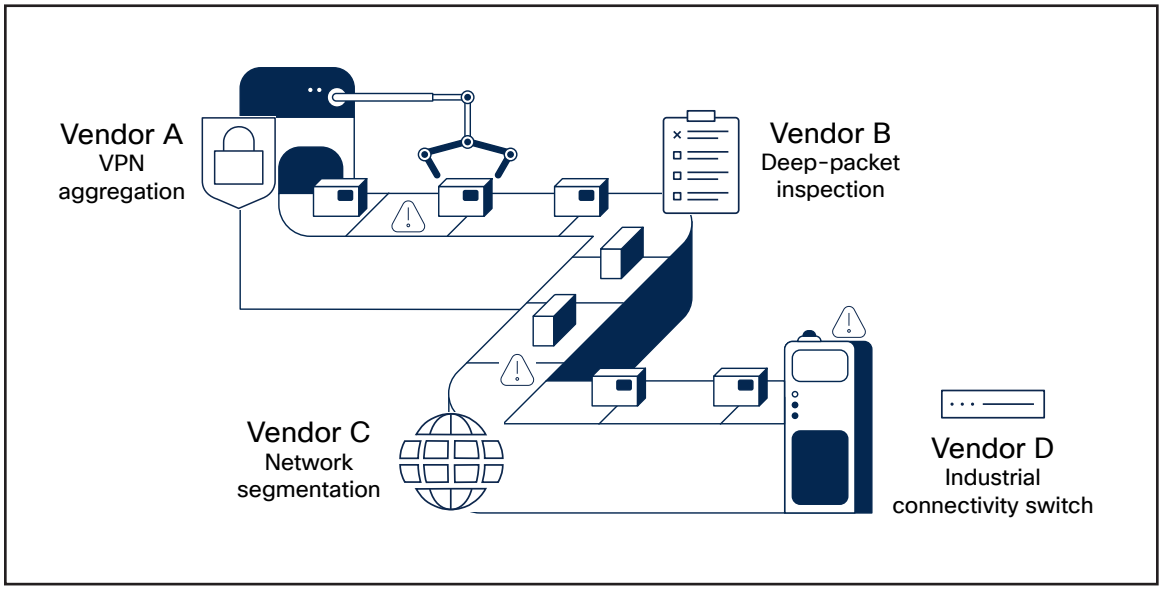
Deploying firewalls to build a Demilitarized Zone (DMZ) between your Operational Technology (OT) and Information Technology (IT) domains is the mandatory first step to secure operations. But as you move forward with digitizing your operations environment and deploying Industry 4.0 technologies, you are connecting more devices, enabling more remote access, and building new applications. Seamless communications between IT, cloud, and industrial networks are needed, and the airgap approach to industrial security is no longer sufficient.

Solutions designed to secure industrial networks typically monitor network traffic to gain visibility into assets, behaviors, malicious activities, and threats. They also rely on deploying rugged firewalls to segment industrial networks and build zones and conduits as recommended by the ISA/IEC-62443 security standards.

The process of evaluating and testing these solutions initially tends to go well – after a successful proof of concept, industrial organizations begin to deploy at scale. That is where they begin to run into issues.

Often, it is cost prohibitive for organizations to buy the number of security appliances they need to cover their entire operations environment. Or the networking team does not have the resources to deploy, maintain, and manage a fleet of security appliances. The additional traffic created to gain visibility on a large scale would likely necessitate a separate network – which would also require the resources to deploy, maintain, and manage it.

Figure 1. Integrating security point products with the network can be complex and hard to scale



Similar issues hamper secure adoption of remote access to industrial assets for operations staff, vendors, and contractors. Remote access is key for managing and troubleshooting OT assets without time-consuming and costly site visits. Many organizations have installed their own solutions, such as cellular gateways or remote access software, that are put in place without strong security controls. Another popular remote access method uses VPNs that may be secure but are complex to implement without providing unlimited and uncontrolled access to the whole network.

Fortunately, you can empower your industrial network to easily provide visibility at scale, contain threats by enforcing ISA/IEC-62443 zones and conduits, and enable Zero-Trust Network Access (ZTNA) for remote users.

Empower your network to provide visibility at scale

The need for visibility

Operations environments are typically made of many industrial assets (such as valves, actuators, drives, robots, power breakers, etc.) managed by Industrial Control System (ICS) devices, such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), Distributed Control Systems (DCSs), etc. Many OT devices were deployed years or decades ago, back when cybersecurity was not a concern, and today are defenseless against malicious traffic such as Distributed Denial-of-Service (DDoS) or vulnerability exploits. To further complicate matters, some devices can be deployed and managed by third-party contractors.

When organizations attempt to secure their industrial networks, they encounter two primary issues:

- **A lack of visibility:** Organizations often do not have an accurate inventory of what is on the network. Without this, they have limited ability to understand risks and build a secure communications architecture.
- **A lack of control:** A lack of visibility also means operators are often unaware of which devices are communicating with each other or even which ones might be receiving communications from the outside. You cannot control what you do not know.

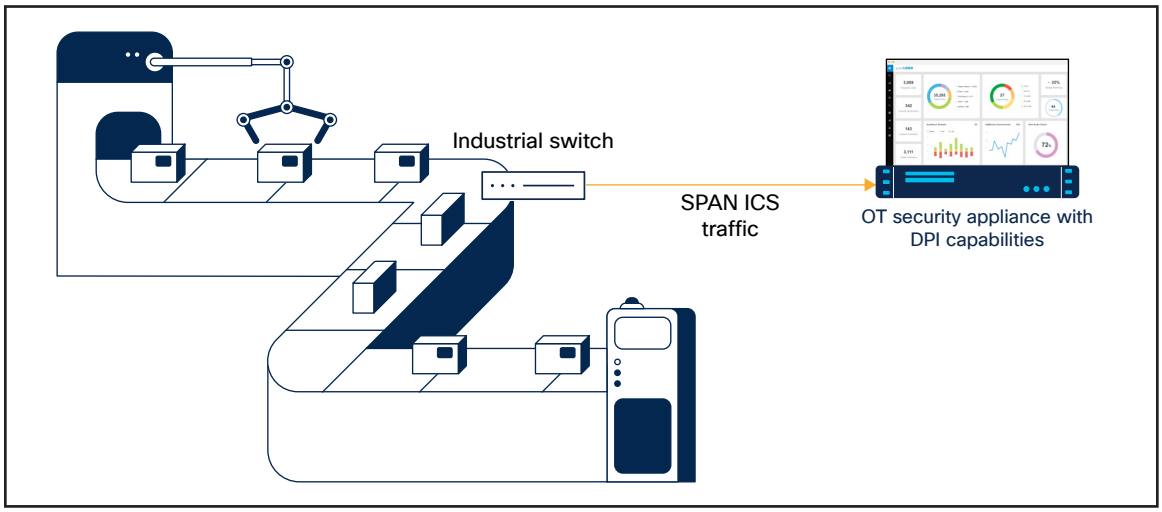
The first step, then, to securing an industrial network is to obtain visibility. You need to understand what devices are on the network, what they are communicating, and where those communications are going.

Beware of hidden costs

The technology to gain visibility into operations is available today. Deep Packet Inspection (DPI) decodes all communication flows to extract information from message contents in addition to packet headers. It gathers asset information such as the model, brand, part number, serial number, firmware and hardware version, software vulnerabilities, rack slot configurations, and more. It also helps you understand what is being communicated over the network. For example, you can see if someone is attempting to upload new firmware into a machine or trying to change the variables used to run the industrial process.

When collecting network packets to perform DPI, traditional security solution providers typically configure Switched Port Analyzer (SPAN) ports on network switches and send all traffic to a central server or dedicated appliances installed here and there in the operational network.

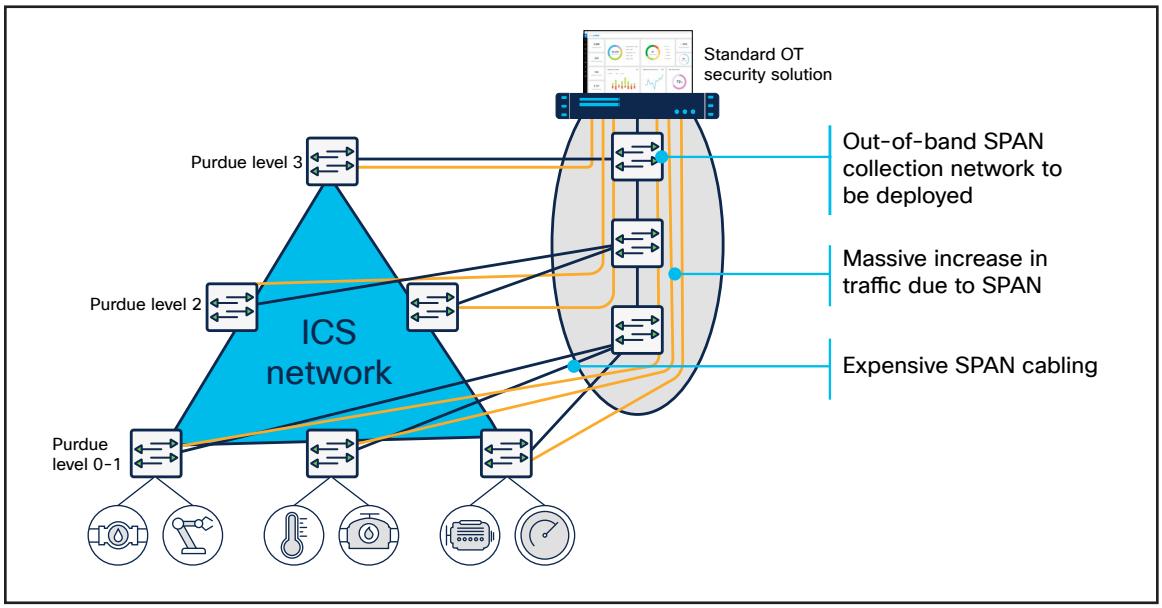
Figure 2. Typical OT/ICS visibility solutions depend on SPAN



It is important to note that in an industrial network, most traffic occurs behind a switch at the cell layer, because that is where the machine controllers are deployed. Gaining comprehensive visibility requires collecting east-west traffic from every switch in the network, and not just from a few aggregation switches, as very little traffic goes through them.

Although this can be acceptable for a small industrial site, it cannot be seriously considered in highly automated operations that generate a lot of ICS traffic (such as manufacturing), or when devices are widely spread in locations with no or poor network connectivity (such as oil and gas pipelines, water or power distribution, roadways, etc.).

Figure 3. SPAN-based solutions incur huge additional hidden costs



Connecting security appliances to network switches addresses the issues associated with duplicating network traffic. The appliance collects and analyzes network traffic locally and only sends data to a server for additional analysis. However, installing, managing, and maintaining dedicated hardware can quickly lead to space and operational issues. And because most industrial traffic is local, gaining full visibility will raise cost and complexity to intolerable levels.

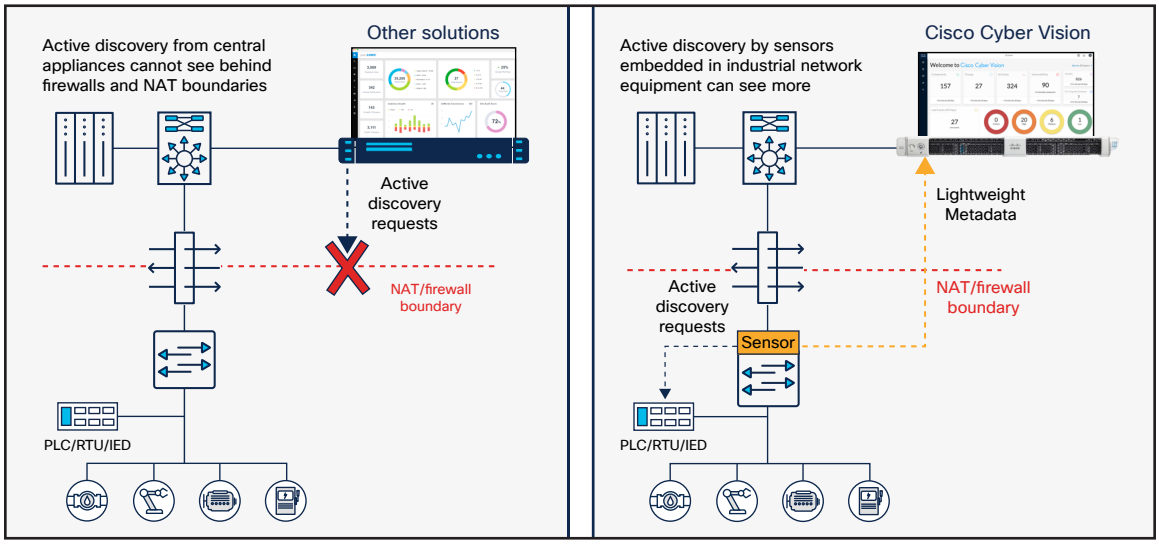
NAT boundaries limit what you can see

In addition to passive discovery through DPI of industrial network traffic, many ICS detection vendors augment their solution with some sort of active discovery capability. This means that the visibility appliance now also queries OT assets to collect additional information and build comprehensive profiles. When considering active discovery, decision makers are focusing on the risk of disrupting industrial processes if discovery messages are not formatted properly and sent with caution over the industrial network. Although this is a valid concern, it eclipses a bigger issue: whether discovery messages can reach assets.

In many industrial sites, zone-based firewalls prevent inbound communications from reaching assets. Large industrial sites make heavy use of Network Address Translation (NAT). In discrete manufacturing, for instance, machines and control systems are built in a standardized manner by machine builders and systems integrators and often use the same IP addresses. Only a small fraction of IP addresses are translated, generally those of PLCs and Human-Machine Interfaces (HMIs).

The result is that centralized active discovery solutions cannot communicate with the vast majority of ICS devices (such as I/O, drives, safety controllers, relays) sitting below the NAT boundary whose IP addresses are not translated. In the auto manufacturing industry, as an example, it is typical for less than 20% of devices in levels 0 through 2 to be visible to a centralized active discovery solution. This results in an 80% gap in visibility.

Figure 4. Active discovery requests sent by Cisco Cyber Vision sensors are not blocked by NAT boundaries and can reach 100% of industrial devices



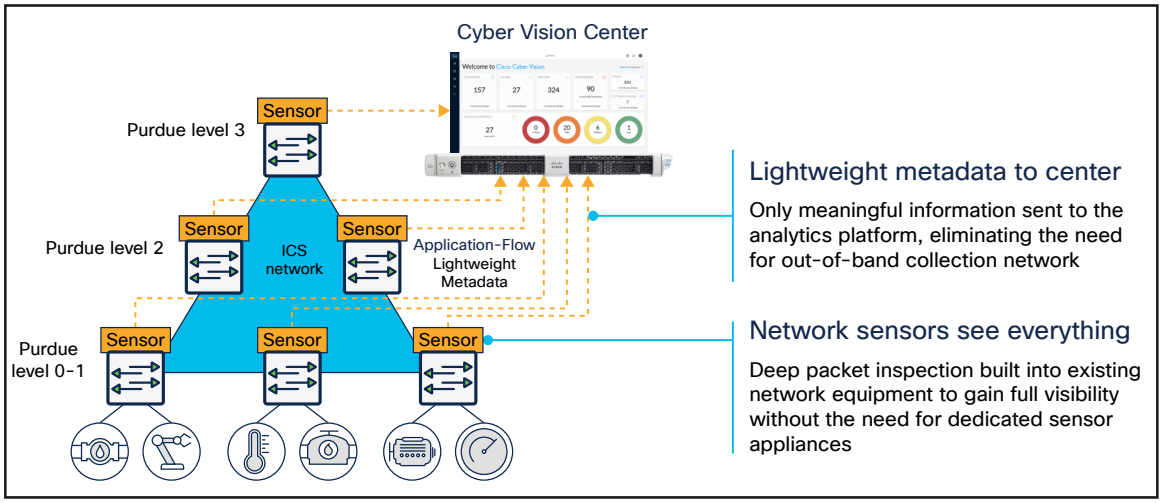
Your network equipment can give you the visibility you need

Embedding DPI and active discovery capabilities into networking equipment helps enable full visibility at scale. A switch or router with native DPI capability eliminates the need to duplicate network flows or to deploy additional appliances. Obtaining visibility is simply a matter of activating a software feature. Cost, traffic, and operational overhead are all minimized.

Cisco has embraced this approach. Cyber Vision leverages a unique edge computing architecture that enables security monitoring components to run within industrial network equipment but can also run using SPAN collection networks to analyze traffic coming from switches and routers that do not support this capability. Active discovery requests are initiated by Cyber Vision sensors embedded in network equipment deployed at the cell layer, right where industrial assets are connected. They are not blocked by firewalls or NAT boundaries, resulting in comprehensive visibility.

A DPI-enabled switch or router decodes traffic locally to extract meaningful information. It sends only lightweight metadata to a central server, which runs the analytics and anomaly detection. That metadata represents about 3% to 5% of general traffic. It is so lightweight that it can be transferred over the industrial network without causing congestion or requiring extra bandwidth.

Figure 5. OT/ICS visibility built into networking equipment is more scalable and sees everything



Embedding DPI and active discovery into networking equipment affords both IT and OT unique benefits. IT teams can leverage the existing infrastructure to secure industrial operations without having to source, deploy, and manage additional hardware. Because these network elements see all industrial assets and traffic, OT teams can obtain visibility into every component of the ICS and gain insights they have never had before.

As you evaluate OT security solutions, be aware of their architectural implications. Embedding security capabilities into industrial network equipment is the best option to simplify deployment, make it scalable, and enable you to see more. Look for industrial switches and routers with computing capabilities capable of doing DPI of industrial protocols, and not just packet compression and forwarding.

Empower your network to contain threats

Define zones and conduits

The ISA/IEC-62443 security standards require the industrial network to be segmented into zones and conduits. The objective is to restrict communications between assets to keep attacks from spreading and disrupting the entire production infrastructure.

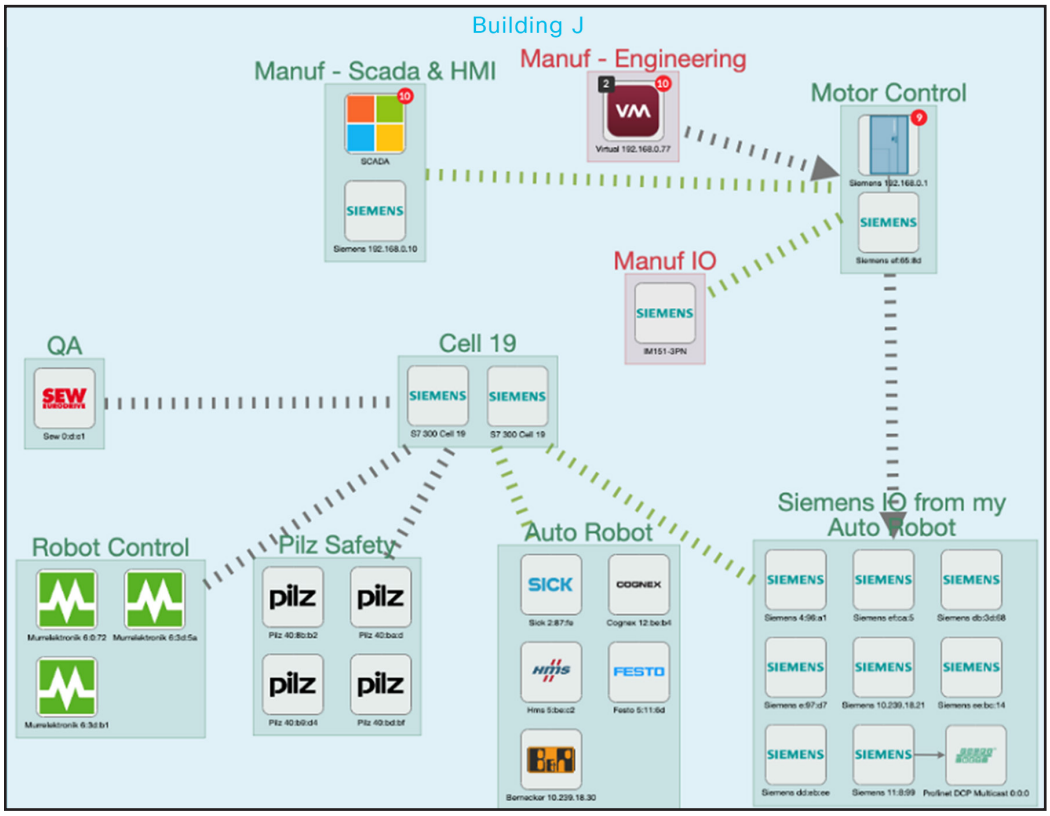
A zone is a collection of assets that have common security requirements. For example, an automobile plant may have a production line for welding and another for painting. There is no reason that equipment on the welding line would need to interact with anything in the paint shop. Placing each in its own zone limits any damage if equipment in one zone gets infected.

Conduits support communication between zones. Under the least privilege principle, OT assets can communicate only with assets in their zone. If assets need to communicate outside of their zones, security policies must be defined, and communication can occur only through the communication conduit.

Implementing such an architecture will greatly improve security, as well as overall network performance, compared to a flat network where all devices share the same bandwidth. It will also, however, require an accurate inventory of all connected assets and a perfect understanding of their roles and communication needs in the industrial process.

Visibility is foundational to building zones and conduits. It allows operations engineers to get a clear view of how their industrial network operates, to better plan for safety and production continuity, and to work together with IT teams to document critical business processes with their associated devices.

Figure 6. Grouping OT assets using Cisco Cyber Vision helps OT and IT teams work together to define zones and conduits



Next, IT and OT can work together to group assets into zones, decide how those zones should communicate with each other, and define their criticality to the organization in order to better understand risks, prioritize threat detection, and manage alarms.

IT personnel often lack an understanding of the OT environment and how it works. OT visibility solutions such as Cisco® Cyber Vision enable operations teams to document their industrial process in a way that helps build a collaborative workflow with IT, giving the context it needs to build security policies that will drive segmentation.

Enforce segmentation policies

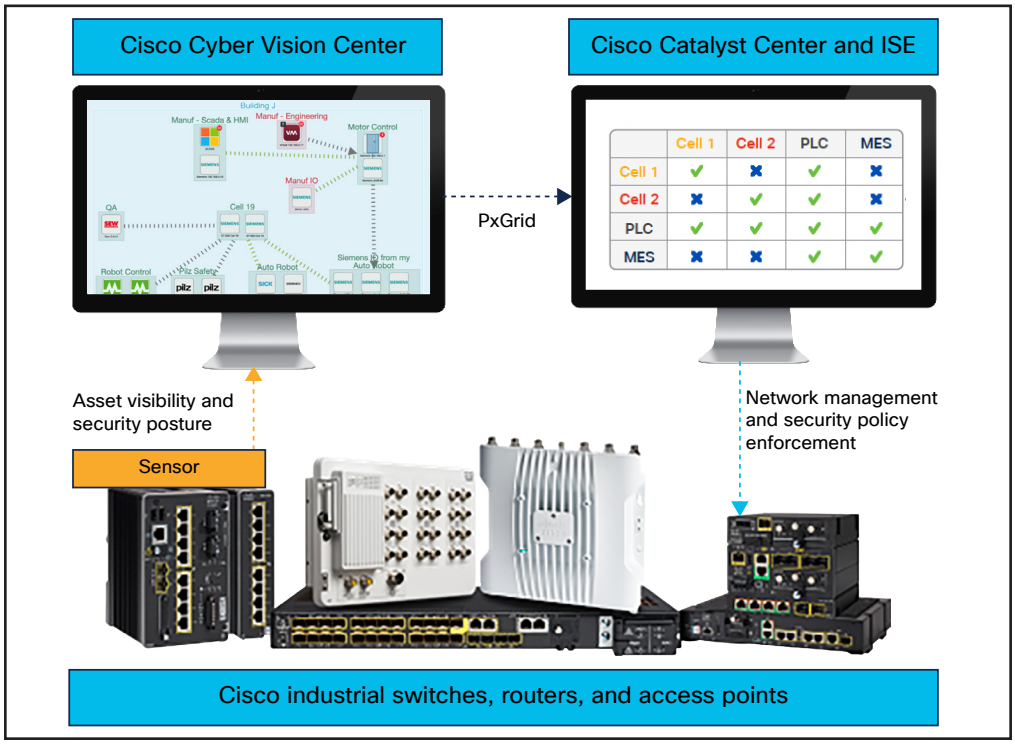
Now that the industrial network is well documented, IT can focus on segmenting the network to implement the zones and conduits defined with OT. To achieve this, many would recommend deploying firewalls to control access to each zone. Although such an architecture has been widely used to segment IT networks, it will quickly prove to be unpractical in OT/ICS environments.

Firewalls are perfect for building an industrial Demilitarized Zone (iDMZ) or secure remote site connectivity. But using firewalls for zone segmentation in industrial plants leads to deployment issues similar to those IT is facing with visibility appliances. Not only can it be very expensive, it also requires reconfiguring the industrial network.

Moreover, maintaining these firewall rules can become a challenge, as OT often has to deploy new assets, move others, reconfigure zones, and more. Industrial networks are not as static as one would think. Operations personnel generally do not have the skills required to configure firewall rules and cannot be dependent on IT for every move, add, and change.

Fortunately, it is possible to segment industrial networks to enforce security policies without using firewalls. Solutions such as Cisco Identity Services Engine (ISE) work with your network switches, routers, and wireless access points to restrict communications according to the zones and conduits you have defined. It leverages groups defined in Cyber Vision to allow or deny communications for each asset. When a change is required, you can just move the asset to another group in Cyber Vision. ISE will automatically instruct the network to apply the corresponding security policy.

Figure 7 Cisco Cyber Vision and ISE enable a dynamic and automated approach to policy enforcement



This software solution simplifies industrial security projects. It is easier to deploy, scale, and maintain than using zone-based firewalls. It also empowers the operations team to take an active role in defining and managing zones and conduits, helping IT and OT to work together in building and securing the industrial network.

Empower your network to provide secure remote access

The move toward zero-trust network access

The principles of zero-trust security, popular for years in IT, are now increasingly being applied to operations. The zero-trust framework stipulates that no one or nothing can be trusted by default and that users, applications, and devices should be granted access only to the resources they need at a given time to do their job. Visibility and segmentation are key parts of such an architecture, as is Zero-Trust Network Access (ZTNA), which focuses on offering remote users secure access to resources.

In many organizations, machine builders, maintenance contractors, or the operations teams themselves have installed their own remote access solutions: cellular gateways or software products that IT is not controlling. These backdoors are at odds with the OT security projects undertaken by the IT/CISO teams and create a shadow-IT situation that makes it difficult to control who is connecting, what they are doing, and what they can access. On the other hand, VPNs have the drawbacks of being always on, with all-or-nothing access, and requiring complex firewall rules to control what remote users have access to.

ZTNA solutions provide secure remote access that starts with a default deny posture and adaptively grants access only to specific resources at specific times based on identity and context policies. They rely on gateways to create a communication path to the OT assets.

But in distributed field networks, there is often no space to install dedicated hardware. When space is available, having to maintain dedicated ZTNA gateway hardware just to access a few OT assets puts an undesirable burden on customers. In larger industrial networks, the ZTNA gateway is centralized in the iDMZ to limit cost and complexity, but many OT assets sit behind NAT boundaries and are not visible from the iDMZ.

Operations networks need distributed ZTNA

With Secure Equipment Access (SEA), Cisco is solving the challenges of deploying secure remote access to OT at scale. It embeds the ZTNA gateway function into Cisco industrial switches and routers. Enabling remote access is now a software feature to activate. There is no dedicated hardware to install and manage. No complex firewall rules to configure and maintain. Cisco is making it very simple to deploy secure, zero-trust remote access at scale in industrial environments.

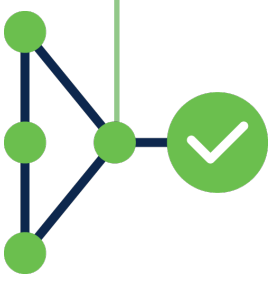
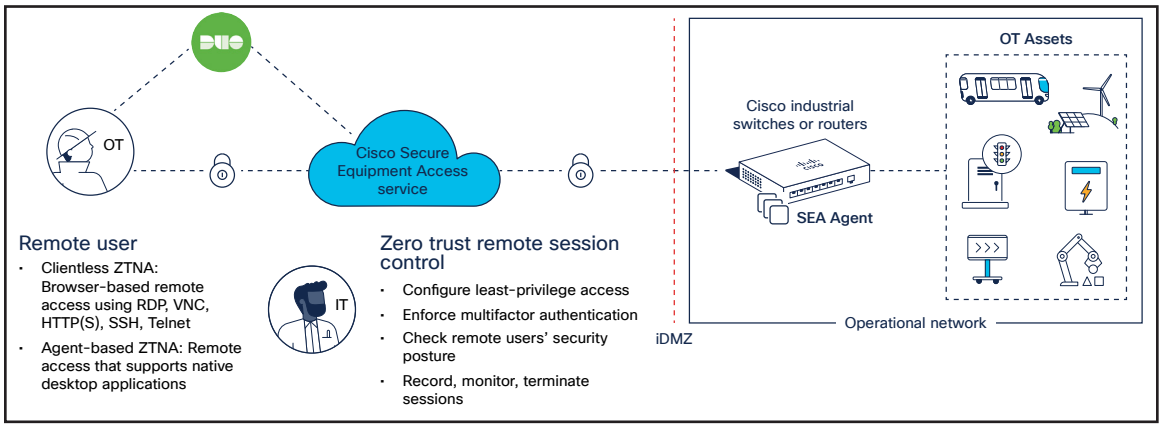


Figure 8. Cisco SEA embeds secure remote access capabilities into industrial switches and routers



Distributing the ZTNA gateway functionality anywhere in the network lets you remotely access every asset, whatever its IP address or your NAT strategy. The switch or router that provides connectivity now also provides remote access to these assets. And the same network equipment can enforce microsegmentation policies to prevent lateral movement to other assets, when the asset is used as a jump host. Cisco Secure Equipment Access combines easy deployment at scale, simple remote access to all OT assets, and unmatched security.

Your network can be the sensor, the enforcer, and the gateway

Operational networks require advanced cybersecurity capabilities. The traditional approach consisting of deploying dedicated appliances for OT visibility, threat detection, zone segmentation, and secure remote access is proving to be too complex to deploy, too costly to scale, and in some cases just impractical.

As we define the networking standards of the future, Cisco is bringing the latest advances in IT to industrial networking equipment today. Our market-leading industrial switches and routers embed advanced cybersecurity capabilities that let you gain visibility at scale, implement microsegmentation to build secure industrial zones, and make zero-trust network access work with the specific constraints of industrial operations. Only Cisco offers such advanced security capabilities in industrial switches and routers today.

When working on your industrial cybersecurity project or thinking of expanding or refreshing your industrial network, do yourself a favor: Avoid sourcing, installing, and managing additional appliances for every cybersecurity feature you need. Not only will this have a positive impact on your sustainability objectives, it will also let you easily scale your industrial security project with the limited number of skilled IT/OT networking professionals you have.

Remember, securing your operations is a journey, but industrial network equipment that gives you the best of connectivity and provides an anchor for security can put you well on your way. To get started, please reach out to us for a free, no obligation, one-on-one consultation with one of our industrial security experts.

Learn more

- Cisco industrial networking
- Cisco industrial security
- Industrial security reference architecture
- What is ISA/IEC-62443-3-3 and how do I comply?
- Zero-trust network access for OT
- Cisco Identity Services Engine and Cyber Vision Working Together