White paper
Cisco public

The bridge to possible

Extending Zero-Trust Security to Industrial Operations

Executive summary

It seems that hardly a day passes without news of yet another security breach. No industry appears to be immune. One of the troublesome aspects is that hackers have been able not just to obtain confidential data on organizations' customers, but also to penetrate and halt industrial operations – which could have far graver implications for individuals and even larger communities.

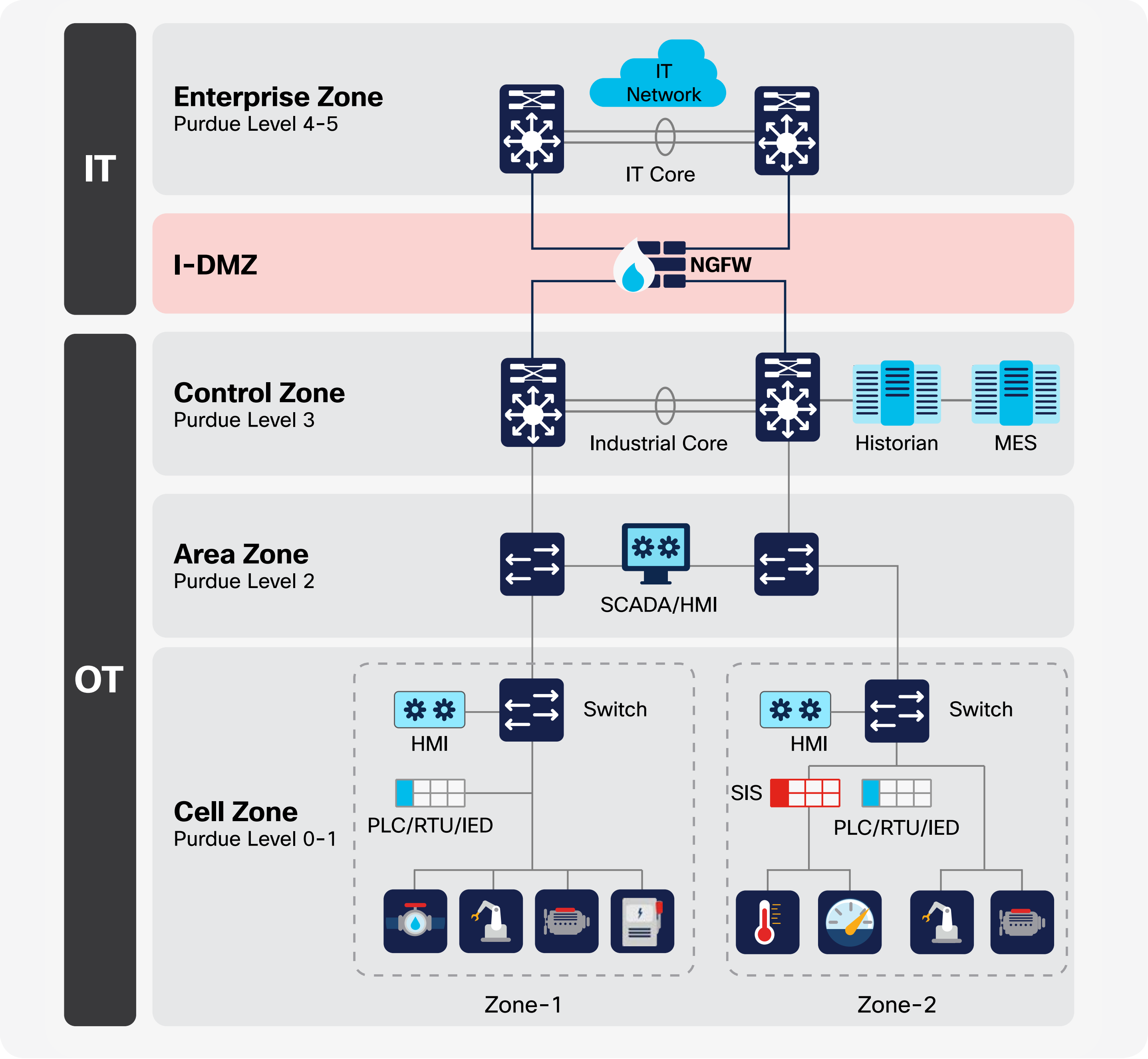
Traditionally, organizations have separated their back-end industrial operations from their front-office ones. The networks serving the operations were kept isolated, as there was really no communication between those devices and the outside world. However, with rapid digitization and increased interest in using automation and analytics to increase production, improve worker safety, and perform predictive maintenance, for which operational data is critical, those networks are now increasingly being connected to the enterprise.

Unfortunately, security considerations often take a back seat. Exposing Operational Technology (OT) to the outside world without proper evaluation of risks can be disastrous. In this paper, we discuss what cybersecurity leaders need to think through and describe a proven solution that has been adopted in leading organizations around the world.

The traditional way to secure OT networks

Perhaps the best-known operating model for the industry is the Purdue Enterprise Reference Architecture, which was developed in the 1990s to address the increasing use of computers to control manufacturing processes.

Figure 1. The Purdue Enterprise Reference Architecture



As shown in Figure 1, the Purdue model defines several levels of enterprise control, from the actual physical processes at Level 0, intelligent devices at Level 1, control systems with Supervisory Control and Data Acquisition (SCADA) and Human-Machine Interfaces (HMI) at Level 2, manufacturing and operations systems with management and control at Level 3, and business, logistics, and enterprise control at Level 4 and above.

A DMZ layer separates the core Industrial Operations (OT) from the enterprise (IT) layers, shielding OT from direct access by IT systems and the internet.

The Purdue model guides enterprise design, provides industrial security through separation of layers, and defines how machines and control functions should interact, but is based on a strict hierarchical view of data flow. With the advent of ever more intelligent IoT devices in the lower layers that generate actionable data to applications that may reside in any layer of the model and in the cloud, organizations need to go beyond just deploying firewalls to build an industrial DMZ. While this is still necessary, it is not sufficient.

IT and OT – together in security

Traditionally, IT has been more conscious of the need for security. This is to be expected because IT serves many groups of users, whether they be local, remote, guests, employees, contractors, etc. Even within a single group of users there could be subgroups such as HR, finance, and managers who have different access needs. IT also maintains databases and applications that employees and customers use. These assets may reside in captive data centers or in public clouds. The trend in which people and applications reside beyond the traditional boundaries of organizations has accelerated even more in the recent past.

The advent of the hybrid work environment and the distribution of sensitive data and applications invalidates previous assumptions that an organization could be secured solely by placing firewalls around its perimeter. In addition, the more advanced and insidious nature of threats has shown that they can penetrate security perimeters. As a result, devices, even within the perimeter, cannot stay trusted.

The zero-trust security framework came into being to address these trends. According to this model, no user or device can be inherently trusted, whether inside or outside the perimeter, until trust can be established. Once established, each endpoint should be provided only the minimum level of access that it needs to adequately perform its job, it should be monitored for any signs of compromise, and mitigation should be performed if any anomalous behavior is detected. Table 1 lists possible threats and the corresponding zero-trust solution for each threat.

Table 1. Threats and zero-trust response

	Threat	Zero-trust solution
Establish trust	Unauthorized endpoints or devices with unhygienic posture can disrupt productivity.	No network access until endpoint trust is evaluated and established.
Enforce trust	Noncritical assets with unrestricted access can make the entire infrastructure vulnerable.	Provide confined access to essential services and resources through macro- and micro-segmentation.
Verify trust	Compromised endpoints can infect other assets in the network through lateral movement.	Continuously evaluate trust and apply adaptive controls to isolate threats in real time.

Implementing zero-trust security brings up a lot of questions that you need to resolve. Such as:

- How do you identify what is connecting to your network?
- How do you determine and define the level of access it needs?
- How do you set up the network to allow each endpoint only the minimum level of access?
- How do you monitor the possibility that endpoints that are already part of your network are infected?
- And finally, how do you stop a threat when one has been identified and restore the secure working environment?

Over the past several years, IT has developed tools and procedures to resolve each of these questions, and many of those tools and processes can now be applied to OT networks.

Unique challenges of securing OT networks

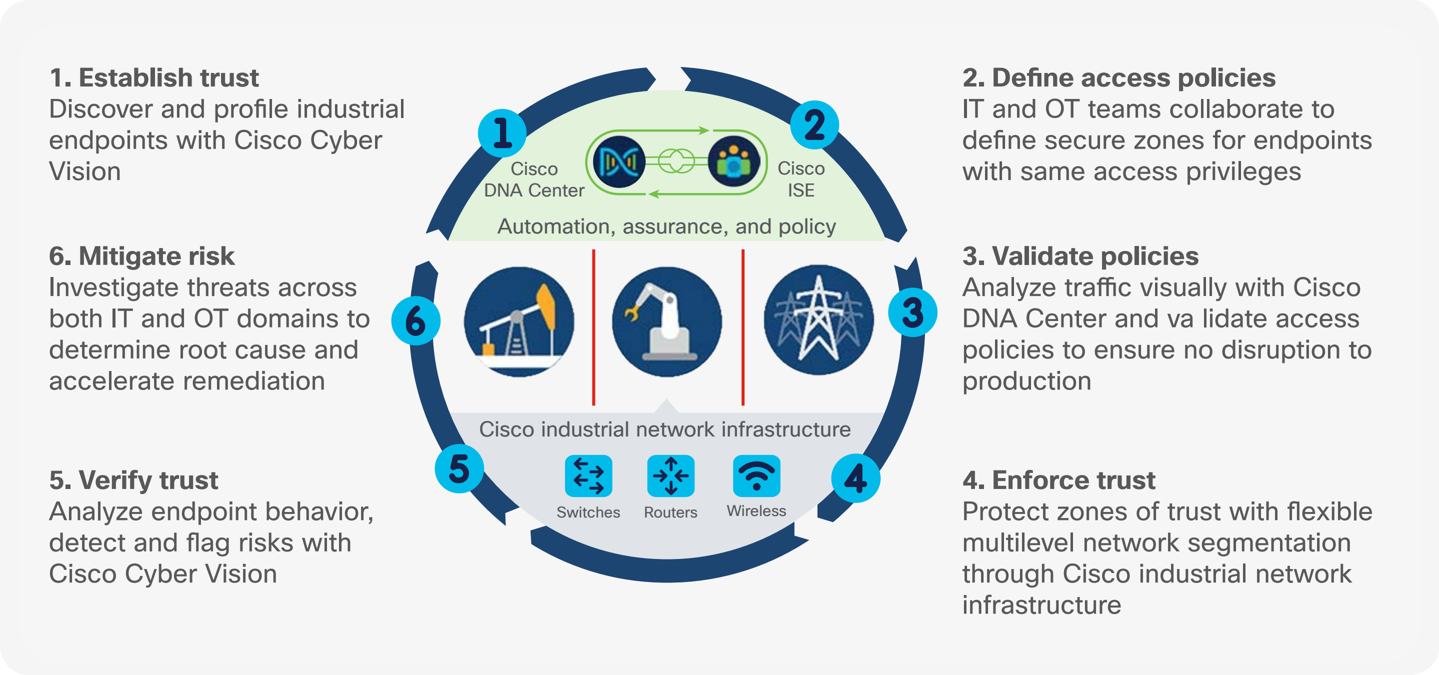
With OT no longer operating in a silo and starting to incorporate many of the same technologies that IT uses, such as remote access, data collection and analytics, Artificial Intelligence, and Machine Language (AI/ML), and various applications in data centers and cloud, there is now a need to extend zero-trust security to OT.

Table 2. OT and IT have different security requirements

Security challenge	IT context	OT context
What does it mean to be secure?	Security in an IT context refers to safeguarding data and computing resources from external threats.	Traditionally, security in OT has referred to worker safety and physical security.
How aware are the teams?	IT teams manage, secure, and process data and are aware of its sensitive and confidential nature.	OT teams manage processes running 24/7/365. Workers are often less aware of how to avoid data breaches and external threats.
How quickly can vulnerabilities be addressed?	IT equipment is known, modern, and controlled internally. It can usually be shut down, replaced, and updated at will.	OT devices can be 10 to 20 years old or more and are often managed by third parties. Updates and patches are harder to deploy, and downtimes are less acceptable.
How well is the network prepared to be secured?	IT networks have gone through many upgrades over the years and are now segmented.	OT networks have been deployed over the years with few or no security policies and are generally flat.
How easy is it to find security incidents?	IT attacks can be well identified (virus, worms, denial-of-service attacks, etc.). The impact of incidents may result in loss of data or disruption to IT services.	OT attacks can look like legitimate instructions to industrial control systems. Impacts can range from faulty production to lost revenues and even bodily injury, death, or damage to the environment.

And while the zero-trust questions can be daunting for IT, they are even more difficult for OT because of the vast variety and age of endpoints, proprietary communications protocols, and the need for the endpoints to run nonstop for production processes. All these factors mean that tools and control that work for IT cannot easily be used for OT, and adaptation is required.

Figure 2. Steps in implementing zero-trust security for OT networks



1. Establish trust
Discover and profile industrial endpoints with Cisco Cyber Vision

2. Define access policies
IT and OT teams collaborate to define secure zones for endpoints with same access privileges

3. Validate policies
Analyze traffic visually with Cisco DNA Center and va lidate access policies to ensure no disruption to production

4. Enforce trust
Protect zones of trust with flexible multilevel network segmentation through Cisco industrial network infrastructure

5. Verify trust
Analyze endpoint behavior, detect and flag risks with Cisco Cyber Vision

6. Mitigate risk
Investigate threats across both IT and OT domains to determine root cause and accelerate remediation

1
2
Cisco DNA Center
Cisco ISE
Automation, assurance, and policy
6
3
Cisco industrial network infrastructure
5
4
Switches
Routers
Wireless

As shown in Figure 2, the zero-trust model relies on the network to provide the trust. Zero trust in OT networks is achieved through the following steps:

1. Identify endpoints and establish trust: Securing your operations starts with an accurate inventory of what is using your network. Devices may have been added over the years on an ad hoc basis. Therefore, the first step is to identify and profile each endpoint. Vital information about them such as their make, model, software version, and role in the industrial process is important to determine whether they are acceptable and comply with the organization's policies.

2. Define access policies: After you determine each endpoint's business role, you can begin to define the resources and other endpoints they need access to in order to do their jobs. Collaboration between IT and OT teams is crucial here, as IT defines the policies, but OT must provide the detailed interaction information IT needs to create trust zones and specify communications between these zones.

3. Validate policies: It is important that the defined access policies do not impose undue restrictions on the endpoints and prevent them from fulfilling their purpose. Therefore, it is necessary to observe industrial network traffic to ensure that these policies are not breaking industrial processes and to further refine these policies if needed.

4. Enforce trust: The validated policies can now be enforced by segmentation that effectively carves the network and creates virtual overlays that group endpoints and resources. Communications within and between segments is controlled. Such control helps contain potential threats by limiting their spread.

5. Verify trust: Even when all endpoints are placed in appropriate zones and are working normally, they need to be monitored continuously for any indications of abnormal behavior to help ensure that they always remain compliant and trustworthy. In this way, any new vulnerabilities can be identified quickly in endpoints that may have been compromised after initially being profiled.

6. Mitigate risk: Once a breach or any other abnormality has been identified, it can be contained, either automatically based on rules, or more often, manually after assessing the scope of the problem and deciding on a solution with due consideration of its effects on production.

Cisco solution for zero-trust security in OT networks

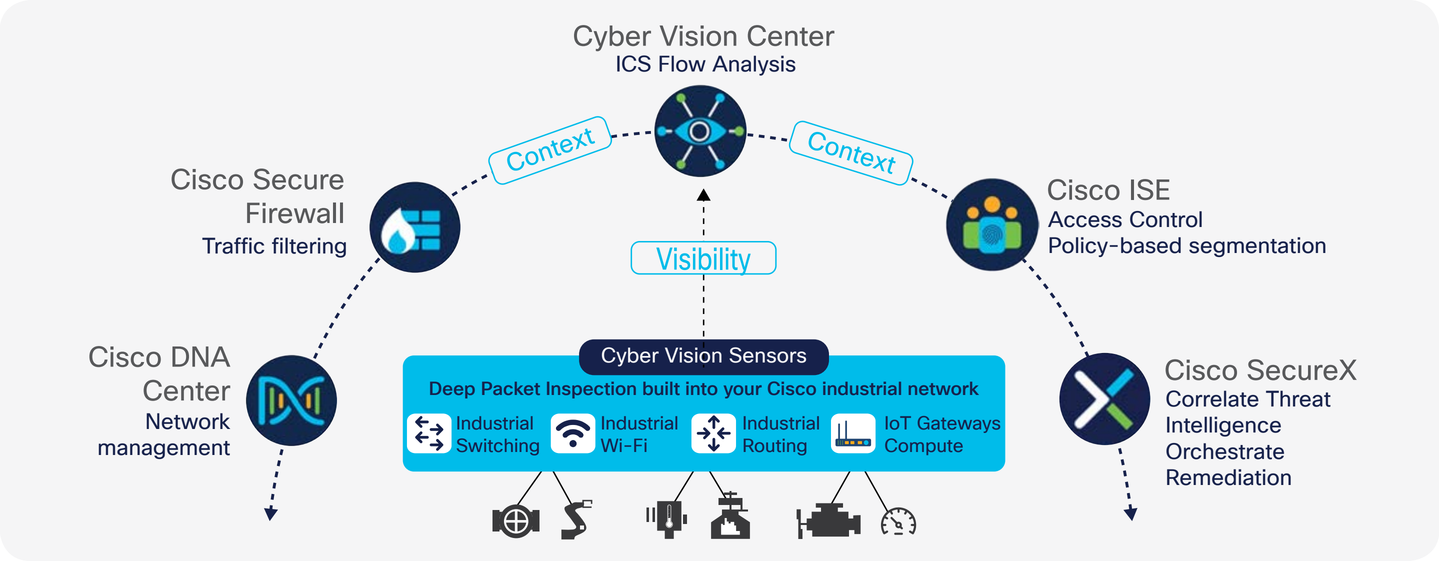
Cisco has a full portfolio of networking and security products that work together to help you achieve zero-trust security in your OT network.

Table 3. Solution components

Security challenge	OT context
	Cisco® Cyber Vision Cyber Vision is a visibility and threat detection solution dedicated to industrial control systems. It maintains a dynamic inventory of all industrial devices and detects threats and abnormal behaviors in real time so you can control OT endpoint compliance and leverage your IT security tools to build security policies that will enforce zero trust in your industrial networks.
	Cisco industrial networking infrastructure Cisco Catalyst® Industrial Ethernet switches and routers provide industry-leading reliability and performance, support industrial protocols and standards, and are purpose built for harsh environments. They can run edge applications including Cyber Vision that obviate the need to use a dedicated appliance and build an out-of-band network.
	Cisco Identity Services Engine (ISE) ISE is a critical component of Cisco's zero-trust security strategy for the workplace. It authenticates and authorizes connecting endpoints and facilitates creation of, stores, and dynamically enforces access policies in the network infrastructure that segment the network.
	Cisco DNA Center Cisco DNA Center is a powerful network controller and management dashboard that lets you build, visualize, control, and secure your access network. It uses extensive automation and deep AI/ML-supported analytics, provides leading visibility into connected endpoints and their interactions, and integrates with ISE to define and enforce access policies.
	Cisco Secure Firewall ISA3000 Industrial Security Appliance The ISA3000 is a foundational component of your IoT/OT security journey. It combines the proven security of Cisco Secure firewalls with the visibility and control of industrial protocols and applications from automation vendors such as Omron, Rockwell, GE, Schneider, Siemens, and others in a hardened enclosure, making it ideally suited for industrial use.
	Cisco SecureX™ SecureX™ aggregates and correlates threat intelligence sources and data from multiple security technologies – Cisco and third party – into a single view. It unifies your security experience with a customizable dashboard of operational metrics and automates threat hunting and investigation workflows.

All of these components are integrated with each other to provide all functions necessary for a complete zero-trust security solution, from endpoint identification to detection and removal of threats.

Figure 3. Integration between components helps ensure complete zero-trust security for OT networks

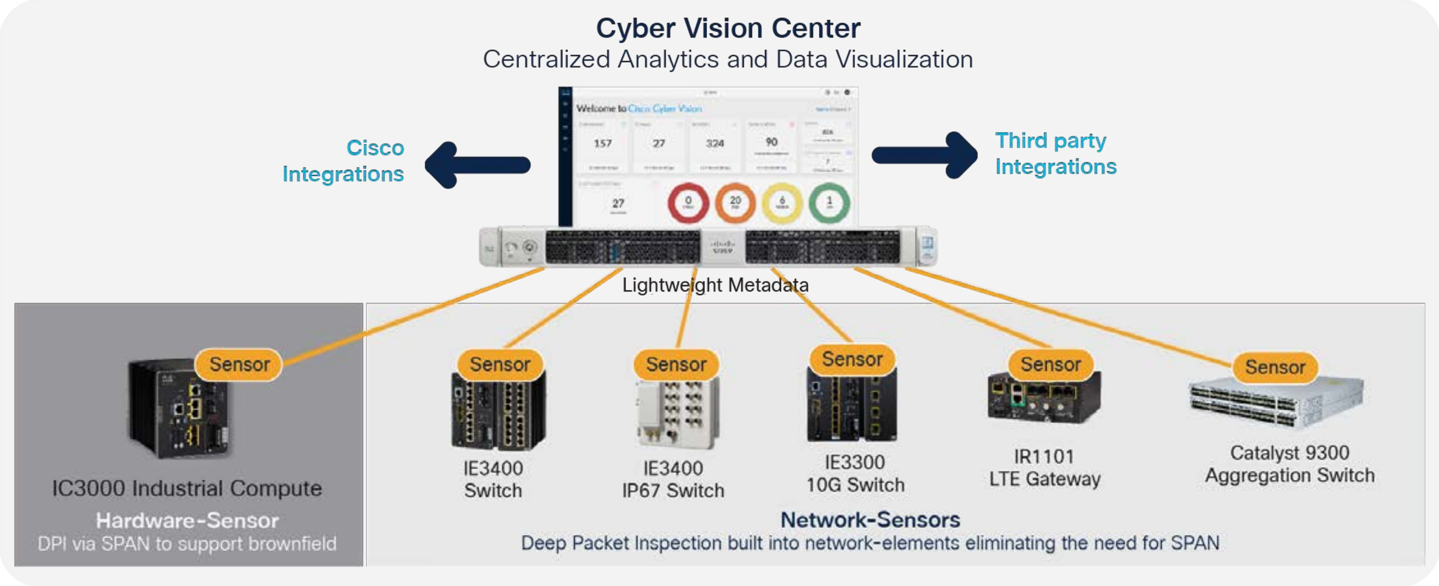


The path to zero trust for OT networks

Step 1: Identify endpoints and establish initial trust

Cyber Vision uses sensors embedded into network equipment (switches, routers, and gateways) to collect packets flowing through the industrial infrastructure. Using a combination of passive and active discovery techniques, the sensor leverages advanced knowledge of industrial protocols to decode and analyze packet payload through Deep Packet Inspection (DPI). This lets Cyber Vision profile each endpoint, detail its interactions with other endpoints and resources, and build an asset inventory.

Figure 4. Cisco Cyber Vision Center collects data from the network

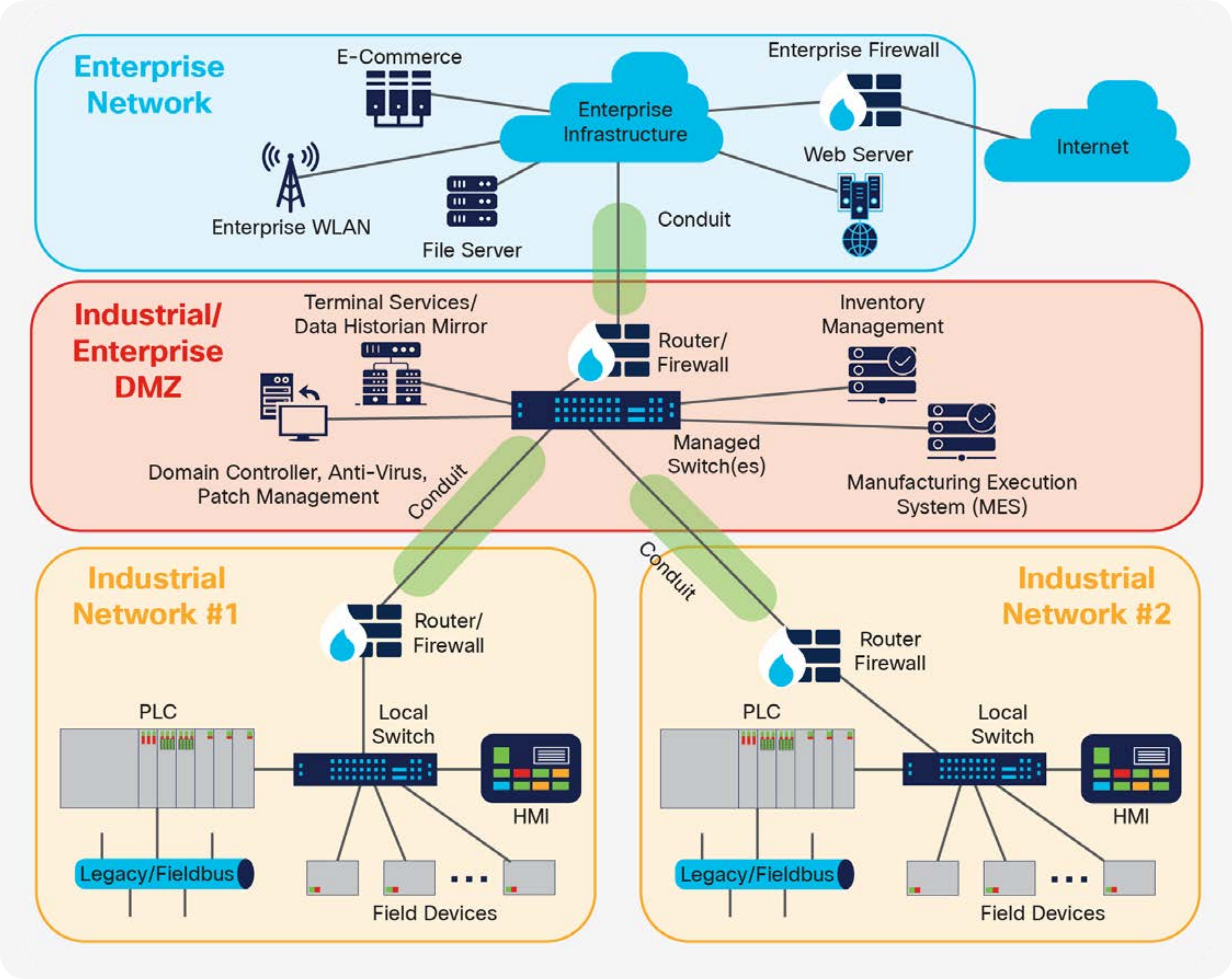

Cyber Vision Center
Centralized Analytics and Data Visualization
Cisco Integrations
Third party Integrations
Welcome to Cisco Cyber Vision
157
27
324
90
27
0
20
6
1
Lightweight Metadata
Sensor
IC3000 Industrial Compute
Hardware-Sensor
DPI via SPAN to support brownfield
Sensor
IE3400 Switch
Sensor
IE3400 IP67 Switch
Sensor
IE3300 10G Switch
Sensor
IR1101 LTE Gateway
Sensor
Catalyst 9300 Aggregation Switch
Network-Sensors
Deep Packet Inspection built into network-elements eliminating the need for SPAN

Cyber Vision sensors are easy to deploy in OT networks, as they run as software on Cisco industrial network infrastructure and don't require a separate appliance, although a dedicated appliance is available if the OT network consists of equipment that cannot run the sensors. The sensors send data about connected endpoints to a central dashboard called Cyber Vision Center, which helps you visualize each endpoint and its interaction with others in a maplike format. This map view is particularly useful for the OT team to group endpoints according to the actual industrial process logic so that IT can build policies depending on which groups can communicate with which other groups.

Step 2: Define and validate access policies

Defining effective access policies in the network requires collaboration between IT and OT teams.

Figure 5. Securing industrial operations by configuring zones and conduits as per ISA99/IEC 62443

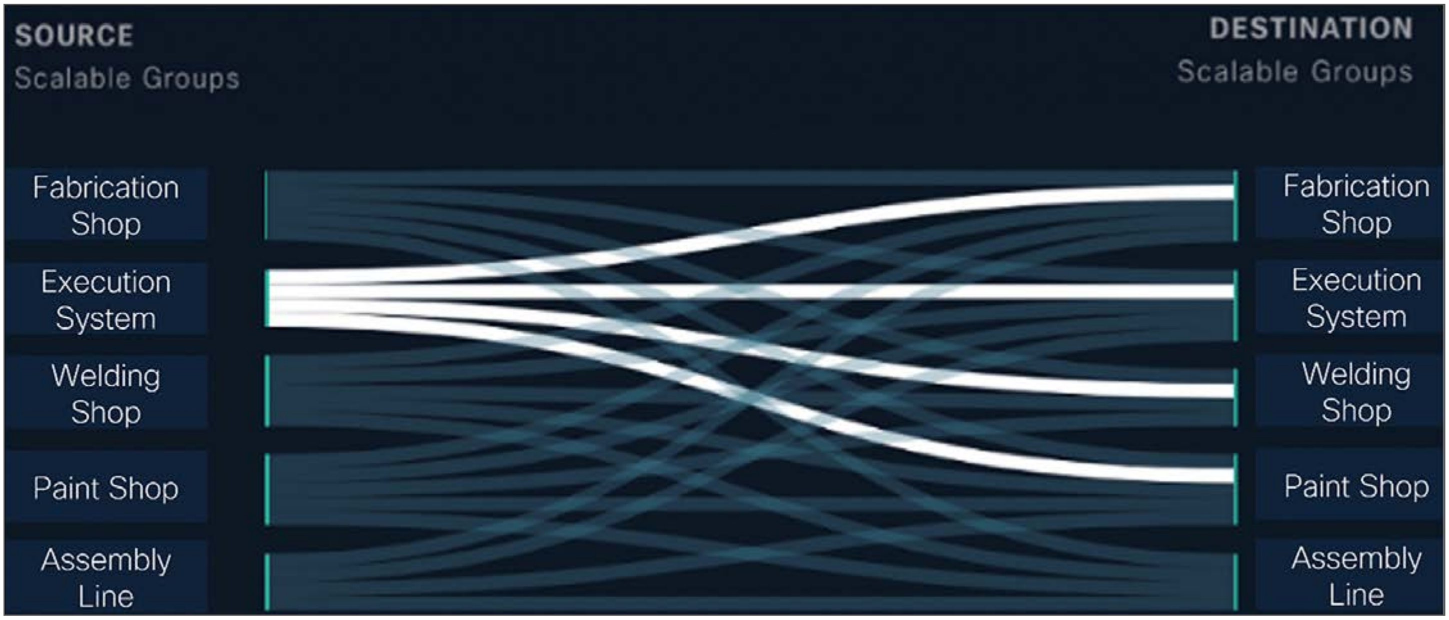


The ISA99/IEC 62443 standards for industrial cybersecurity define zones as groups of devices with similar security requirements, a clear physical border, and the need to talk to each other. For example, an automobile plant may have a production line for welding and another for painting. There is no reason why equipment in welding would need to interact with that in the paint shop. Placing each in its own zone limits any damage if equipment in one zone gets infected. Conduits define the limited interaction allowed if equipment in different zones does need to communicate with each other. Access policies formalize zones and conduits in the OT network.

Cyber Vision can be integrated directly with Cisco ISE. This integration enables Cyber Vision to share rich industrial context about the assets deployed in the environment. Once OT administrators have grouped assets in Cyber Vision, this information is automatically shared with Cisco ISE. ISE can leverage the asset details and groupings to identify security policies that must be applied. Endpoints can be assigned to the appropriate zones and their communications tagged with a Scalable Group Tag (SGT) that enables the network devices to define and enforce the appropriate access policy.

Step 3: Validate policies for compliance

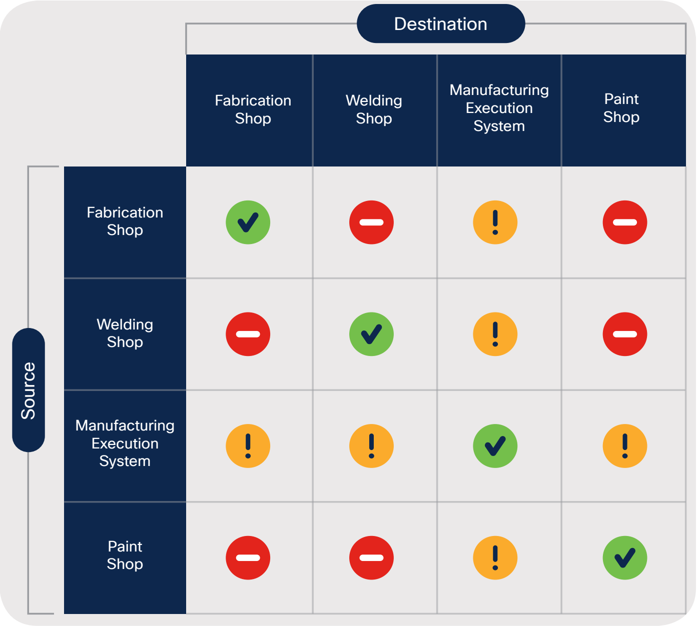
Figure 6. Cisco DNA Center provides a visual mapping of traffic flows between groups



Validation of policies is required before their enforcement. Cisco DNA Center provides a dashboard to visualize interactions between groups that it learns from ISE, as shown in Figure 6. Cisco DNA Center also provides granular details for each interaction such as the application, protocol, port numbers, etc. With this information, you can adjust the defined policies as necessary to make sure they do not hinder any legal interactions.

Step 4: Enforce trust through network segmentation

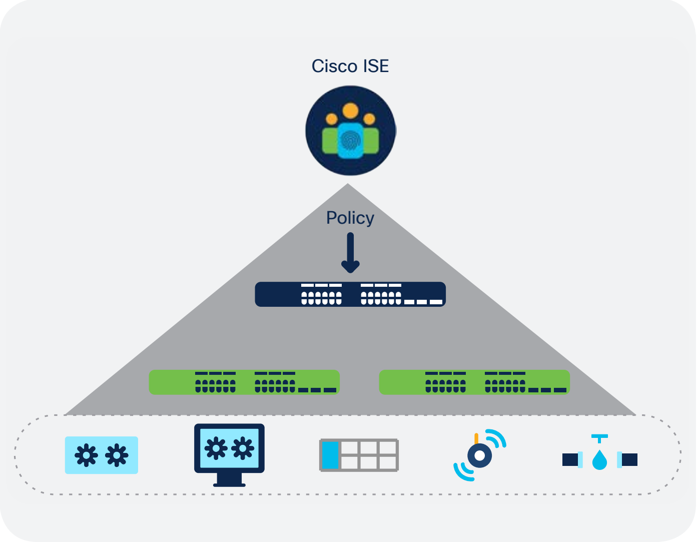
Figure 7. Policies are defined in Cisco DNA Center using a matrix



Source \ Destination	Fabrication Shop	Welding Shop	Manufacturing Execution System	Paint Shop
Fabrication Shop	✓	⛔	!	⛔
Welding Shop	⛔	✓	!	⛔
Manufacturing Execution System	!	!	✓	!
Paint Shop	⛔	⛔	!	✓

Once policies are validated, you can author them either in Cisco DNA Center or in ISE using an easy-to-use matrix – each cell of which defines the communication that is allowed between the source and destination groups. Figure 7 shows such a matrix in Cisco DNA Center in which endpoints within the same zone are allowed to freely interact with each other but not with endpoints in other zones. For example, while endpoints in the Fabrication Shop zone can communicate with each other, they cannot communicate with those in the Welding Shop zone. Endpoints in each of the zones can communicate with the Manufacturing Execution System, but only as constrained by the conduit definitions.

Figure 8. ISE sends access policies to the industrial networking infrastructure



The defined policies are now sent to ISE, which in turn configures the Catalyst Industrial Ethernet switches and routers to enforce the policy restrictions on each of their ports as appropriate for the endpoint connected to that port. Applying these policies segments the network so that each zone is now protected and communication between zones is tightly controlled through the defined conduits.

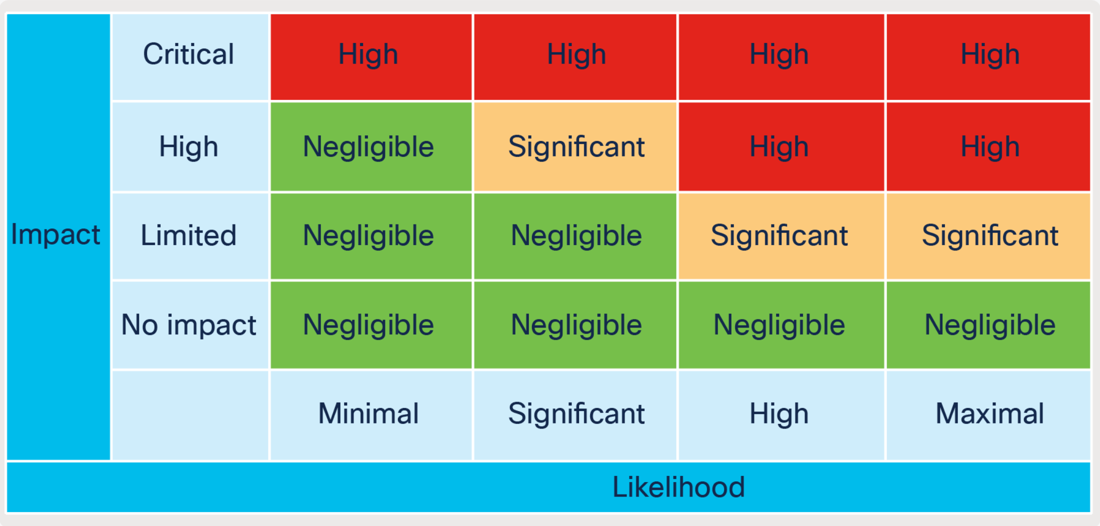
This process of defining, validating, and enforcing access rules gives OT control over their security standards. Once this process is implemented, adding new endpoints, and modifying policies as needs change, becomes easy. For example, if in the future the need arises for certain communication between the Production Shop and the Assembly Line, a new policy can be defined in the policy matrix and the infrastructure easily reconfigured.

Step 5: Continuously verify trust

Cyber Vision continuously evaluates the security posture of connected endpoints. It automatically calculates a risk score for every endpoint to help security administrators be proactive in limiting the threat exposure to industrial processes. Risk scores are the product of the likelihood of a threat and its potential impact, where likelihood depends on the asset activities, vulnerabilities, and exposure to external IP addresses, and impact depends on the asset type and its criticality to the industrial process.

Individual risk scores are aggregated to evaluate the security posture of industrial zones and make it easier to prioritize corrective actions such as applying vulnerability patches or installing industrial firewalls so that industrial endpoints can remain secure.

Figure 9. Cyber Vision evaluates risk based on its potential impact and likelihood of its happening



Impact	Critical	High	High	High	High
	High	Negligible	Significant	High	High
	Limited	Negligible	Negligible	Significant	Significant
	No impact	Negligible	Negligible	Negligible	Negligible
		Minimal	Significant	High	Maximal
Likelihood					

However, even if risks are kept to a minimal level and access policies are properly enforced, it is possible that subsequent attacks may breach a zone, infecting control systems such as SCADA, Programmable Logic Controllers (PLCs), and HMI. Such infections may cause these controllers to alter the behavior of the industrial equipment they control, leading to production quality issues, stoppage of production, or even damage to machines and the production infrastructure. Therefore, all such controllers must be monitored continuously for signs of any anomalous behavior that might indicate that they have been compromised. Cyber Vision analyzes all industrial communication contents along with an advanced baseline engine to track abnormal behaviors.

Step 6: Mitigate risk

IT has two ways to deal with an identified risk in an endpoint. They can effectively remove the endpoint from the network, either by reducing its access privileges or by turning off the switch port it is connected to. These methods might work well where an offending printer or the email service can be placed offline temporarily while being fixed, but it is clearly not an option in OT, where a machine cannot simply be stopped in its tracks. Mitigation of identified threats in industrial settings requires close cooperation between IT and OT security groups.

While the appropriate response to each threat will need to be evaluated based on the impact of the threat, IT and OT teams should work beforehand to develop a playbook that can be executed without delay when a breach is discovered. Mitigation decisions may be beyond the capability of tools. The chain of command for key decisions must be established. For example, cases in which production needs to be halted, and who will take the responsibility for it, should be documented.

Cisco SecureX provides a single-platform approach to security. It integrates with key security tools and provides the orchestration you need between those tools to execute the workflows you have defined.

Get started

Security considerations for OT networks cannot be taken in isolation from IT. Threats affect both IT and OT and can spread from one side to the other. As networks have converged, security measures must now converge too. IT and OT teams must share the mechanisms for network control, threat detection, and response for maximum efficiency and effectiveness across the entire organization. Not all of these mechanisms need to be adopted at once; you can incorporate them gradually in steps and start your journey to zero-trust security.

Please refer to the following for more information and to get started:

- Visit the Cyber Vision webpage
- Read the Extending Zero Trust Security to Industrial Networks blog post
- Read the IT and OT Cybersecurity: United We Stand, Divided We Fall white paper
- Contact us