Gaining Visibility into Industrial Networks at Scale

A modern approach to monitoring industrial environments and building a comprehensive OT asset inventory to effectively secure operations

Contents

Overview

As industrial networks can be quite old and widely dispersed, and are sometimes maintained by third-party contractors, organizations often don't have an accurate inventory of what is on their network. Operations environments are made up 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), and Distributed Control Systems (DCSs). Without comprehensive and detailed visibility into all these assets, industrial organizations have limited ability to understand cyber risks and build a secure communications architecture.

All personas in an OT environment can benefit from having visibility into a network's Operational Technology (OT). OT operators can benefit from process-level visibility to identify and troubleshoot assets. IT operators can gain insight into device communication patterns to help inform policy and improve network efficiency. And security teams can gain insight into device vulnerabilities and deviations from normal device behaviors.

The technology for gaining visibility into OT and automating the creation of a detailed and up-to-date asset inventory 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. Because it analyzes network flows in real time, DPI can also help OT personnel understand what is being communicated. For example, it can permit them to see if someone is attempting to upload new firmware into a machine or trying to change the variables used to run an industrial process.

To collect network packets and perform DPI, vendors of OT visibility solutions typically configure switched port analyzer (SPAN) ports on network switches and employ one of three architectures:

- Duplicate all traffic and send it to a central server that performs DPI.
- Deploy dedicated sensor appliances on each network switch.
- Send traffic to dedicated sensor appliances deployed here and there on the network.

The process of evaluating and testing these solutions initially tends to go well, but when industrial organizations start deploying at scale, they begin to run into issues. Often it's cost-prohibitive to buy, deploy, and manage the number of sensor appliances needed to cover their entire operational environment. Or the networking team doesn't have the resources to deploy the network capacity required to support the additional traffic created by these appliances.

This solution brief describes the limitations of architectures supported by traditional OT visibility solutions and explains Cisco's alternative approach. Gaining comprehensive visibility into the OT environment is the critical first step described in the Cisco® Validated Design (CVD) on Industrial Security. For more information on any of the technologies and best practices found in this solution brief, see the Cisco Industrial Security Design Guide.

Visibility into OT environments: Where you look matters

Beware of hidden costs

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, rather than just from a few aggregation switches, as very little traffic goes through them.

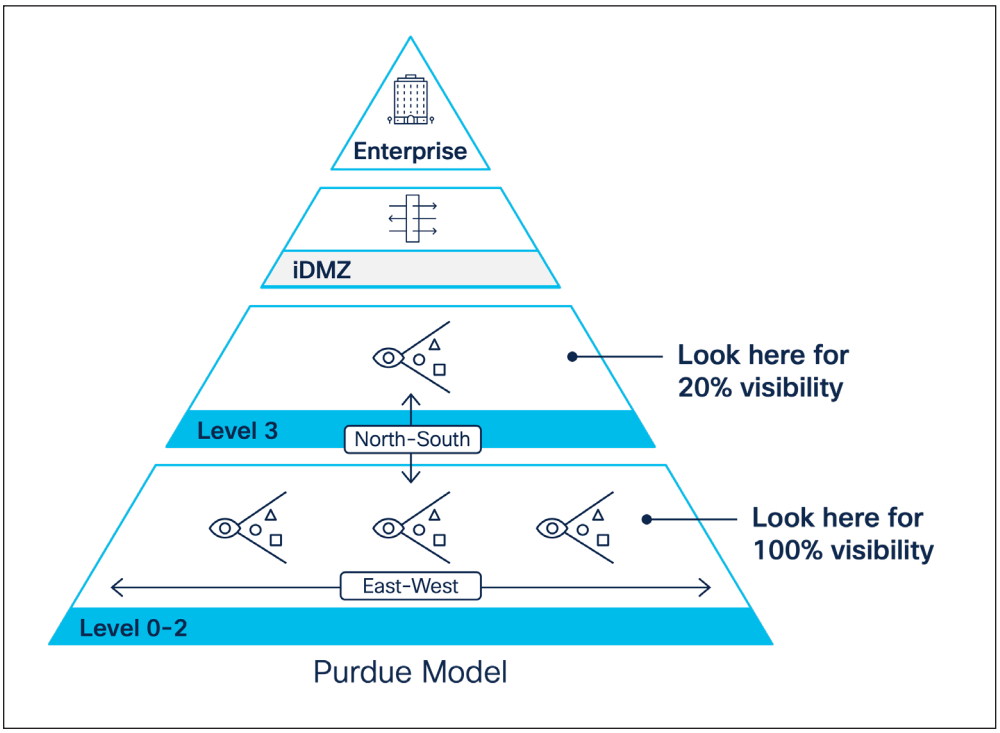

Figure 1. Very little industrial network traffic goes through aggregation switches

To collect network packets and perform DPI, OT visibility solution vendors typically use SPAN, a method that mirrors each packet going through a switch to a local port where a dedicated appliance is connected to analyze the traffic. Although this can be acceptable for a small industrial site or a lab environment, it cannot be seriously considered in large production infrastructure. Installing, managing, and maintaining a fleet of appliances can quickly lead to cost and operational issues, especially for industries where distributed field assets are installed in small cabinets with limited space, such as with roadway operators or energy distribution.

Some OT visibility solutions attempt to address this problem by leveraging remote SPAN (RSPAN), a method that duplicates traffic from a switch that doesn't have a sensor appliance to a switch that has one. While RSPAN helps to reduce the number of appliances required to provide full visibility, it increases the amount of traffic going through the industrial network, so it cannot be considered a valid option for infrastructure where devices are spread across locations that rely on costly WAN connectivity (such as oil and gas pipelines, water or power distribution, roadways, etc.).

In plant networks with highly automated operations generating a lot of ICS traffic (such as manufacturing), the RSPAN approach can quickly become a major issue. The extra volume of data can add unbearable load on the network, resulting in jitter—often an unacceptable compromise for industrial operations where processes need to run as fast as possible and machines must be time-synchronized.

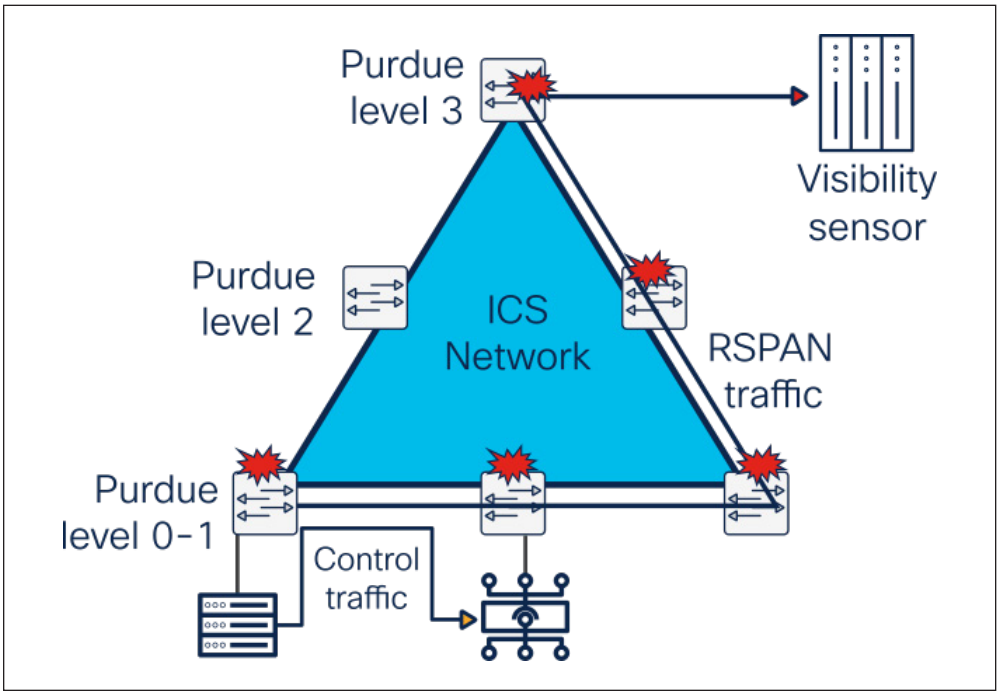

Figure 2. RSPAN introduces jitter, which can cause head-of-line blocking

As a result, organizations have no choice but to deploy an out-of-band SPAN collection network that collects network traffic from every switch in the environment. This approach helps to limit the number of visibility appliances by centralizing DPI capabilities and avoids disrupting the industrial control network by mirroring traffic over a dedicated collection infrastructure. However, this involves significant capital expenditures for additional switches and cable runs. Deploying, managing, and maintaining this network also increases operational complexity. And as the industrial control network grows or changes to meet the needs of the business, the out-of-band SPAN infrastructure must scale and change accordingly, potentially requiring further investment and increased labor costs.

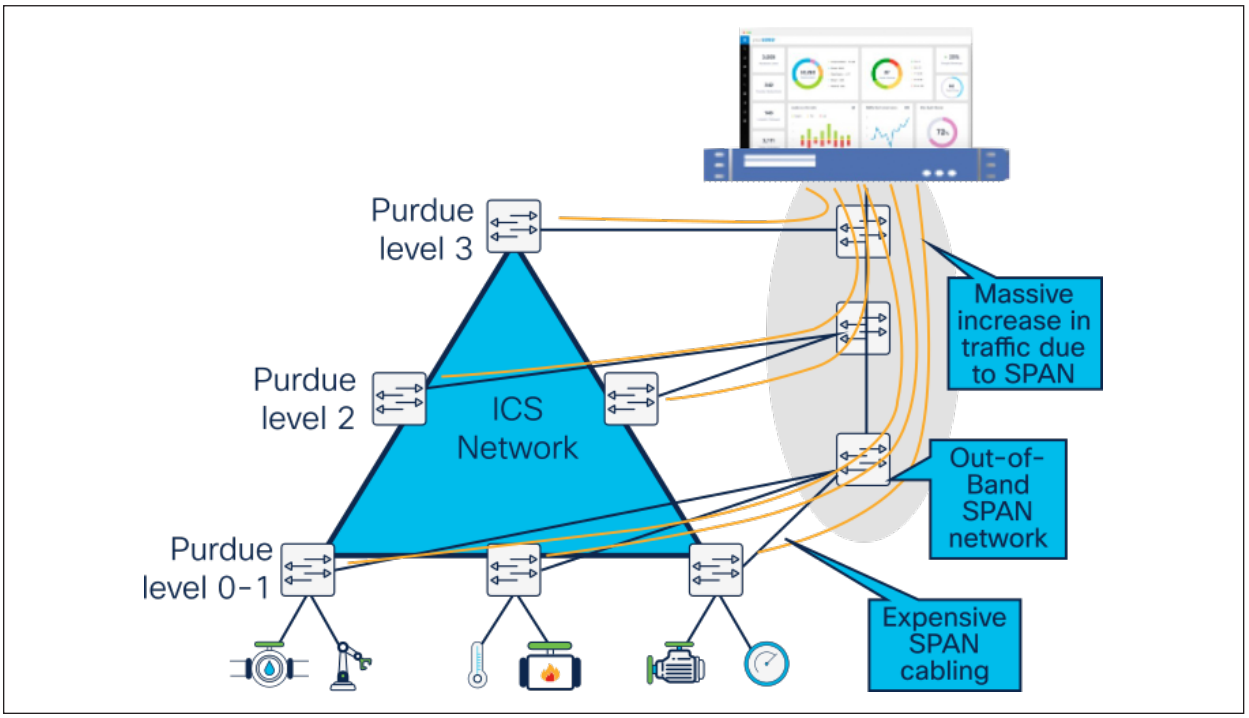

Figure 3. SPAN-based solutions incur huge additional hidden costs

A packet forwarder is not a sensor

In addition to their traditional sensor appliances, several OT visibility solution vendors are offering “light” sensors. Their objective is to help collect network traffic using lower-cost hardware or existing Windows workstations to gain visibility into production cells that would not justify more advanced capabilities. This approach attempts to solve the cost and operational issues associated with deploying numerous visibility sensors in lower Purdue levels but introduces network capacity issues.

Network architects need to understand that these “light” sensors are essentially packet forwarders. They collect industrial network traffic using SPAN ports and compress it before sending it to a central appliance where DPI is performed. Depending on the “light” sensor vendor and make, the compression ratio can be anywhere from 20% to 50%, which means this approach adds about 50% to 80% load on the industrial network and will generally require deployment of an out-of-band collection network.

NAT boundaries limit what you can see

In addition to passive discovery through DPI of industrial network traffic, many OT visibility vendors augment their solution with some sort of active discovery capability. This means that the visibility appliance can query OT assets to collect additional information and enrich asset 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. In addition, 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 or OEMs and often use the same IP addresses. Only a small fraction of IP addresses is translated, generally those of PLCs and Human-Machine Interfaces (HMIs).

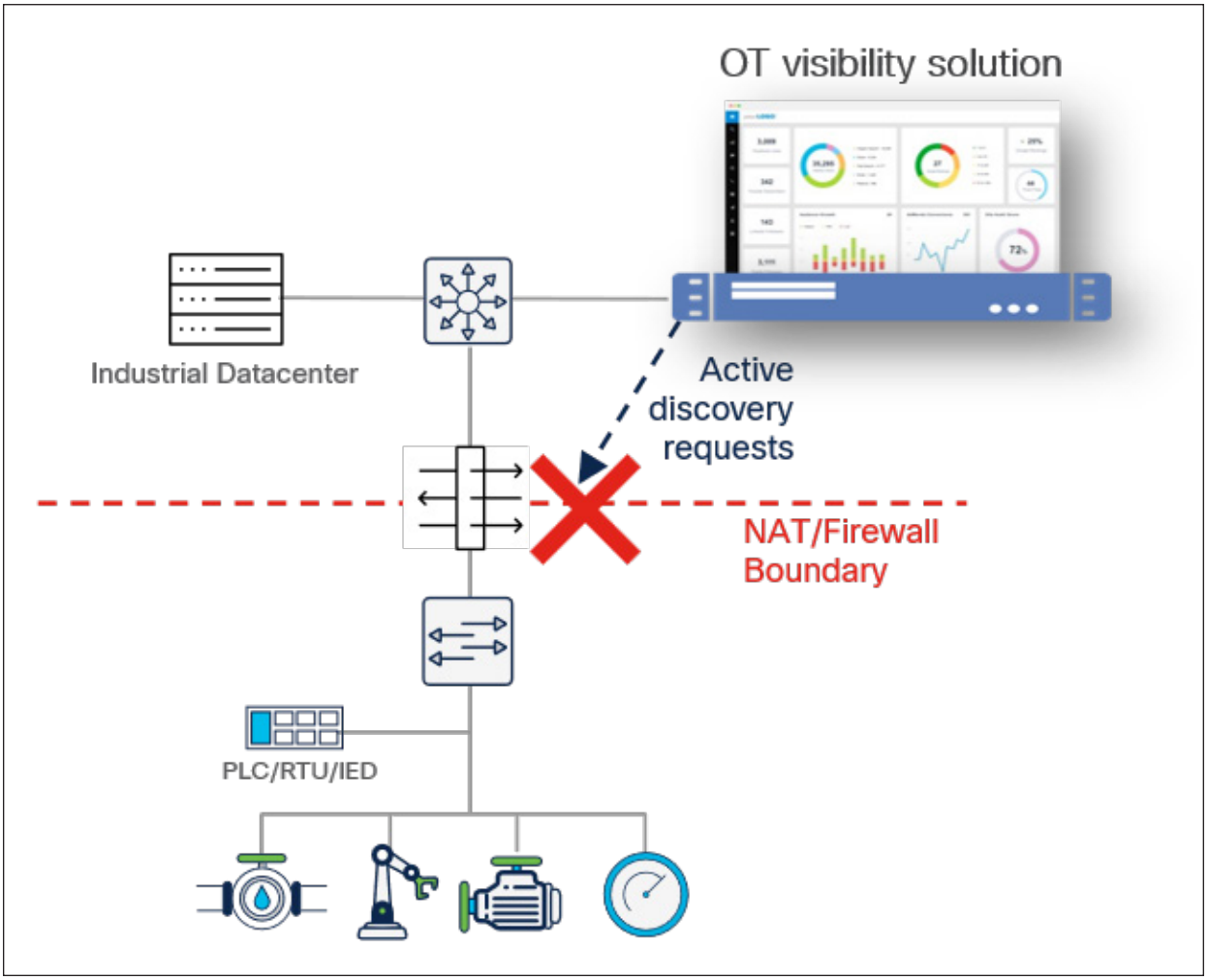

Figure 4. Active discovery requests can be blocked by NAT boundaries

The result is that centralized active discovery solutions cannot query most OT assets (such as I/O, drives, safety controllers, relays) sitting below the NAT boundary, as the IP addresses of these assets are not translated. In the auto manufacturing industry, as an example, it is typical for fewer than 20% of devices in Levels 0 through 2 to have their IP addresses exposed to Level 3. This results in 80% of assets not being visible to a centralized active discovery solution.

The critical need for comprehensive visibility into the OT environment

Securing industrial environments requires continuous visibility into every connected device at every stage, from the moment it enters the environment to the time it is removed. Most cybersecurity regulations require organizations to inventory and profile industrial assets. It is the first function of the NIST cybersecurity framework. It also helps drive compliance with NERC CIP-15 for power utilities in North America and with several NIS2 requirements in Europe.

Industrial cybersecurity projects must seek to have 100% visibility into their industrial infrastructure. If regulatory compliance is a driver, gaining comprehensive visibility is also a prerequisite for an effective risk management strategy, as it helps organizations keep track of vulnerabilities, remote access for vendors, and decommissioned assets. Leaving some assets out of the risk assessment process makes the entire cybersecurity strategy deficient.

Another imperative of any OT security strategy is to build a defensible architecture. The IEC 62443-3 industrial security standard and cybersecurity best practices alike recommend implementing network segmentation in Level 0 to 2 to prevent attacks or malware from spreading. Having 100% visibility enables organizations to use software-based network segmentation solutions such as the one described in the Cisco Industrial Security Design Guide. Visibility-driven segmentation not only helps implement zone segmentation in a matter of weeks instead of months, but it also helps protect industrial operations without the need for complex network modifications or the risk of blocking legitimate flows and causing downtime.

Your network equipment can give you the visibility you need

Eliminating the need for dedicated appliances and SPAN collection

There is a better way to achieve comprehensive OT visibility than deploying a fleet of visibility appliances or costly SPAN collection networks. You can run DPI and active discovery in networking equipment. An industrial-grade switch or router with such capabilities eliminates the need to duplicate network flows and deploy dedicated appliances.

Cisco Cyber Vision, part of Cisco Industrial Threat Defense, is a software solution built into Cisco industrial routers, Cisco Industrial Ethernet switches, and the Cisco Catalyst™ 9300 and 9400 Series platforms to provide comprehensive OT visibility. The Cyber Vision sensor software is an IOx application running within a dedicated CPU core in the switch or router to avoid impacting network performance. It passively captures and decodes network traffic using DPI of industrial control protocols. It can send active queries to assets using the semantics of the protocol at play to enrich their profile and discover dormant devices.

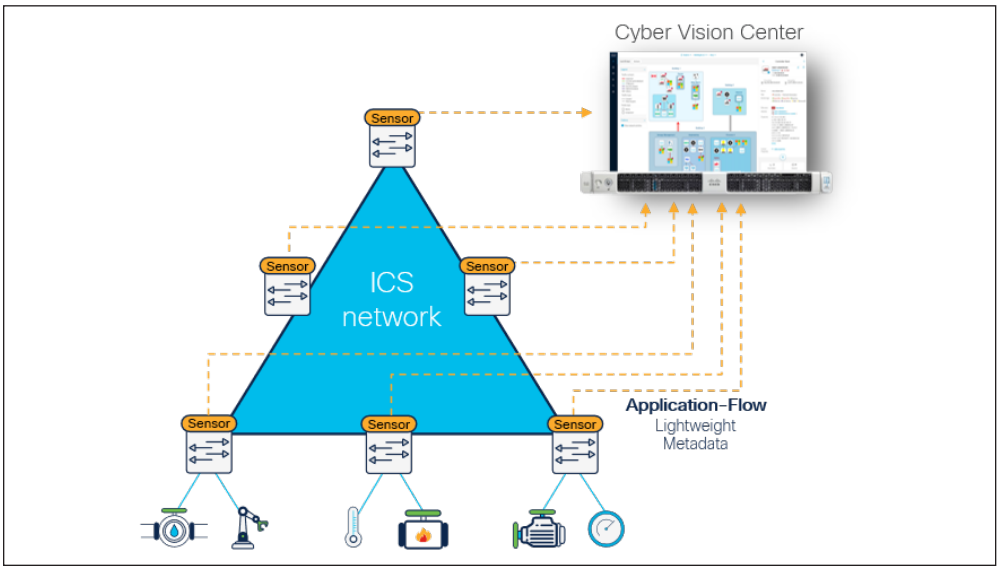

Figure 5. Cyber Vision sensors run DPI in switches or routers and send only metadata to the console

Because the Cyber Vision sensor runs within the switch or router, there is no need to deploy dedicated visibility appliances. Because active discovery requests are sent from the switch or router that connects assets, they are not blocked by NAT or firewall boundaries. And because network traffic is decoded at the edge, the Cyber Vision sensor sends only lightweight metadata to Cyber Vision Center, representing just 2% to 5% extra load on the industrial network, eliminating the risk of jitter caused by RSPAN or the need for an out-of-band SPAN network.

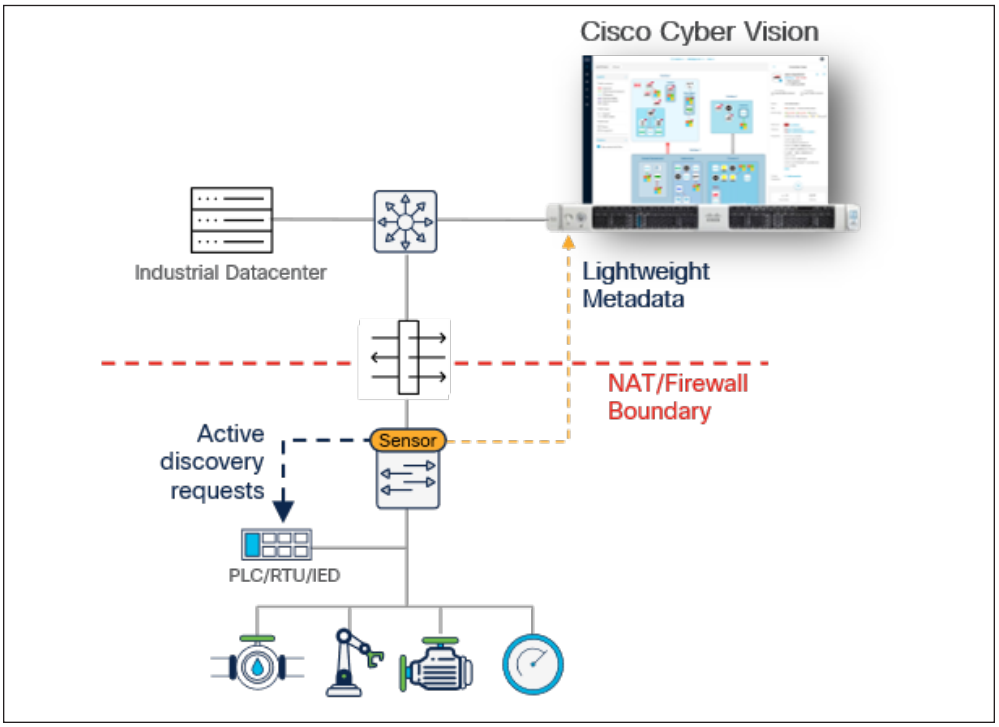

Figure 6. Cyber Vision active discovery requests are not blocked by NAT and firewall boundaries

Gaining 100% visibility into the industrial network is simply a matter of activating a feature within switches and routers. Cost, traffic, and operational overhead are all minimized. Note that there are no licensing implications for deploying sensors at every possible location. Cyber Vision licensing is based on the number of endpoints it detects. A sensor can be deployed on every compatible hardware device in the network. For additional sensor deployment considerations, please refer to the Cisco Industrial Security Design Guide.

Gaining visibility with non-DPI-enabled networking equipment

Not all networking equipment can run the embedded sensor software. Gaining visibility using these local assets will require hardware sensor appliances. Be aware that not all appliances are created equal—to maintain the benefits of not deploying a SPAN architecture, these appliances should:

- Be centrally managed so they are easy to deploy and maintain at scale
- Focus on passive and active discovery features only so they can use low-cost hardware
- Send only metadata to the central console so they don't need extra network resources

The Cyber Vision sensor can also run in industrial compute hardware, such as the Cisco IC3000 Industrial Compute Gateway or any x86 or ARM64 appliance using a Docker version of the sensor software. These hardware sensors connect to the industrial network using SPAN ports, and because low-cost appliances can be used, they can be deployed anywhere you have switches. Unlike "light" sensors, Cyber Vision hardware sensors run DPI to decode network traffic and extract metadata. They add only 2% to 5% load on the industrial network, eliminating the need for out-of-band SPAN collection networks.

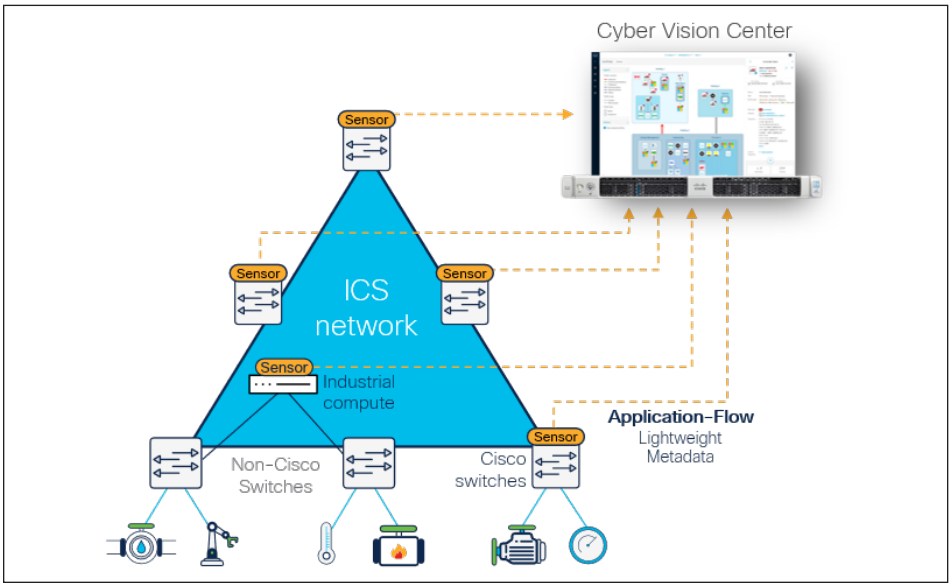

Figure 7. Sensors based on low-cost industrial compute hardware can collect data using a short one-hop SPAN

The benefits of Cyber Vision aren't limited to organizations with Cisco networks. The Cyber Vision sensor offers maximum deployment flexibility to meet the constraints of existing networks while eliminating the need to build out-of-band collection networks:

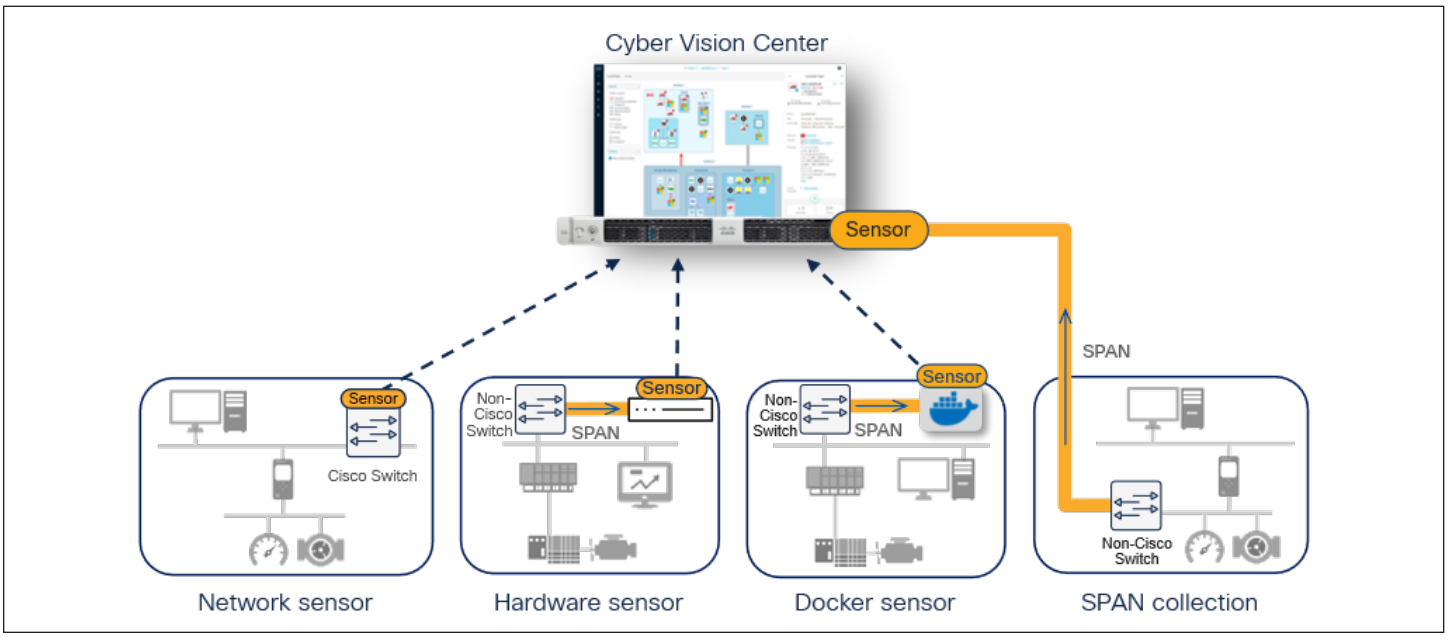

Figure 8. Implementing Cyber Vision in the OT network

- Sensor software is built into select Cisco switches and routers to run DPI and active discovery right where OT assets connect, offering comprehensive visibility without additional network resources.
- Sensors can run in low-cost hardware appliances (Cisco or third party) to gain visibility into third-party networking equipment using a short one-hop SPAN cable.
- Sensors can run in Cyber Vision Center in the industrial data center, allowing the use of an existing out-of-band SPAN network that collects traffic from various equipment in the environment.

Summary

For over 20 years, Cisco has been helping industrial organizations around the globe digitize their operations by developing a market-leading networking and security portfolio that is purpose-built for industrial use cases. Our deep understanding of operational technology requirements, plus our comprehensive networking and cybersecurity portfolio, is a rare combination.

The Cisco Industrial Threat Defense solution is intended to be used by IT, OT, and security teams and their relevant partners and system integrators. Operations will appreciate the ease of use and simple deployment, as well as the broad support for various IACS vendors and protocols. IT network managers will appreciate the ability to apply skills, technology, and applications already deployed in the enterprise when looking to integrate production environments. Security teams will have visibility into industrial assets and security events with context enriched by control engineers.

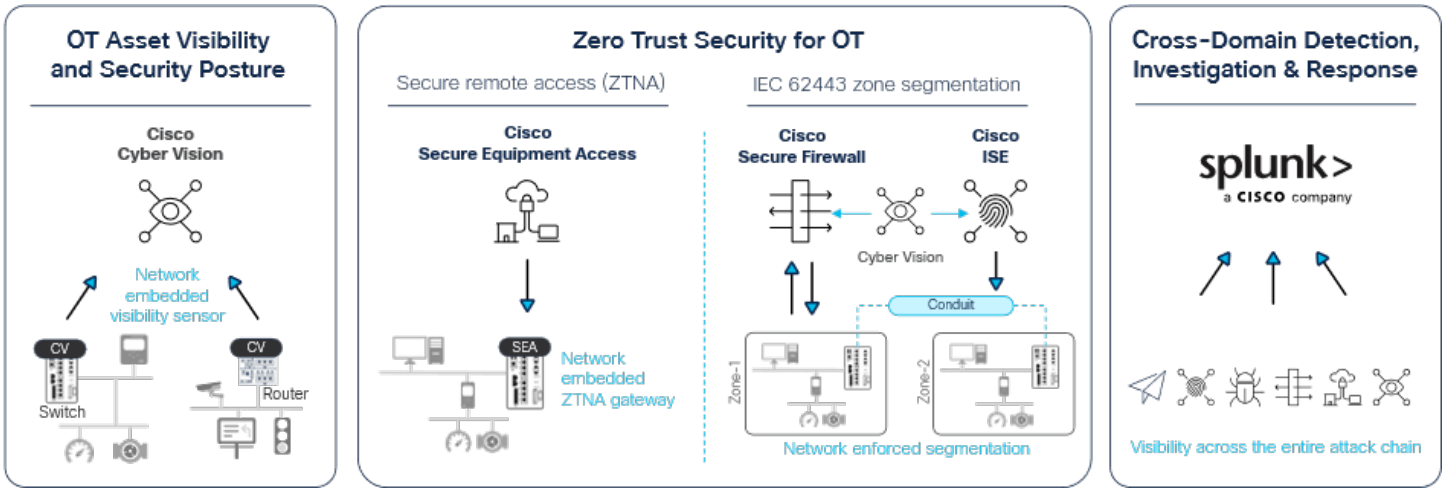

Figure 9. Cisco Industrial Threat Defense embeds visibility sensors into switches and routers

Talk to a Cisco sales representative or channel partner about how Cisco can help you secure your field industrial network. Visit cisco.com/go/iotsecurity or cisco.com/go/cybervision to learn more.

C22-5291701-00 07/25