Industrial Plant Network Security with Cisco Secure Firewalls

Establishing resilient defenses to prepare industrial plants for AI and virtualization

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

© 2025 Cisco and/or its affiliates. All rights reserved.

Overview

Cisco's 2024 State of Industrial Networking Report found cybersecurity to be the biggest reported challenge in running and maintaining industrial networks. There is a clear sense that Artificial Intelligence (AI) will boost business growth for those who can successfully use it to run better industrial networks. However, increased network connectivity leads to a continually expanding attack surface. In 2023, the world's critical infrastructure suffered 13 cyberattacks every second, and in 2024, cyberattacks on critical infrastructure surged by 30%.

Safeguarding Industrial Automation And Control Systems (IACS) from cyberthreats is a critical priority, but transforming these intentions into effective actions can be challenging. Given the complexity of IACS and their networks, which often rely on outdated technologies and inadequate security measures, it can be difficult to determine the best starting point.

The promise of zero trust and the use of micro-segmentation technologies sounds great in principle but can sometimes be complex to implement. Enterprise networks have been securing their network infrastructure for years, and IT teams can increment their security posture by building on the foundation of what has come before. When implementing a segmentation strategy in operational networks, micro-segmentation cannot be the starting point. Protecting the plant needs to be done in stages, and given where threats are coming from, we recommend starting by securing these three main control points in plant networks, in the following order: the IT/OT boundary, the industrial data center, and the plant floor.

This solution brief is a subset of the Cisco Validated Design guide (CVD) on Industrial Security and summarizes the design guidance and capabilities contained within the guide. For more information on any of the technologies and best practices found in this solution brief, see the Cisco Industrial Security Design Guide.

Benefits

- Control access to the Operational Technology (OT) network by deploying an industrial "demilitarized zone."
- Protect the critical network while exposing it to new applications such as industrial AI, software-defined industrial automation, and hardware virtualization of the plant floor.
- Protect operations from lateral movement.
- Streamline network segmentation by building dynamic firewall rules, informed by visibility.
- Patch legacy devices virtually with intrusion prevention policies on the firewall.

© 2025 Cisco and/or its affiliates. All rights reserved.

Protecting the operational boundary with Cisco Secure Firewall

The importance of the industrial demilitarized zone

The first step in the journey to securing your industrial network is to restrict logical access to the OT network. A common method is to deploy an Industrial Demilitarized Zone (IDMZ) network with firewalls to prevent network traffic from passing directly between the corporate and OT networks.

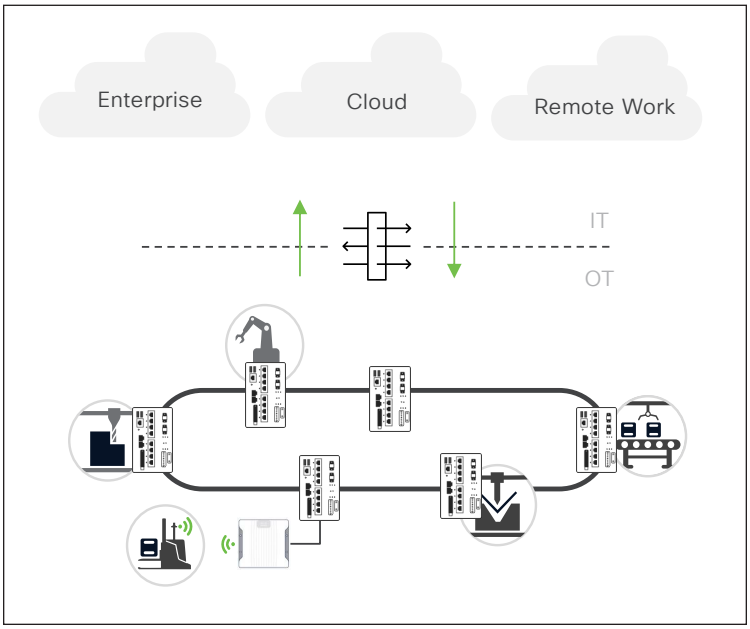

Figure 1. Enforce policy at the IT/OT boundary

The IDMZ offers a network on which to place data and services to be shared between the enterprise and industrial zones. It doesn't allow direct communication between the industrial and enterprise zones but meets the requirements for data and service sharing. With the deployment of an IDMZ firewall, attacks and issues that arise in one zone cannot easily affect the other zone. In well-architected networks, if the enterprise zone is compromised, an IACS or IT network administrator can temporarily isolate operations from the IDMZ until the situation is resolved, ensuring that the most critical parts of the network are not affected by the breach.

Cisco® Secure Firewall brings distinctive threat-focused next-generation security services. The firewall provides stateful packet inspection of all traffic between the enterprise and OT network and enables intrusion prevention (IDS/IPS) and Deep Packet Inspection (DPI) capabilities for inspecting application data between the zones to identify and stop a variety of attacks. Cisco Secure Firewall is the first line of defense adversaries meet when attempting to breach the network and is the enforcement point for least-privilege access for legitimate services to cross the border in a secure way.

© 2025 Cisco and/or its affiliates. All rights reserved.

Moving the IDMZ to the cloud

Typically, IDMZ designs are architected and deployed at one facility and replicated across each production site owned by the organization. One of the challenges with an exclusively onsite IDMZ is the limited ability to meet future demand in a world where the growth of Industrial IoT (IIoT) and IT/OT/cloud convergence requires new capabilities. It can also become challenging for operations staff to maintain IDMZ consistency across multiple sites and deliver consistent security policies.

A hybrid cloud IDMZ model can be an alternative. Like an IDMZ deployed on-premises, it provides a holistic security strategy with the benefit of shared resources and assets, allowing for a more repeatable and consistent architecture, as well as easing operational overhead and complexity. A hybrid cloud IDMZ supports a regional operations center model, which is top of mind for some industrial organizations, especially those with a global footprint. For more information on the hybrid cloud IDMZ model, read our Hybrid Cloud Industrial DMZ white paper.

The rise of industrial AI and the industrial data center

Rising investments in industrial AI and the virtualization of the plant floor are resulting in the Industrial Data Center (IDC) becoming a critical component of operational networks. Virtual programmable logic controllers (PLCs) are an example of this shift, where virtual controllers allow for production plants with a more flexible and modular design. Consolidating the numerous industrial PCs deployed on the plant floor into virtual machines in the IDC is also a great opportunity to drive costs down and increase agility.

In a traditional Purdue model architecture, the IDC would reside in Level 3, the industrial operations zone. This is important to distinguish, as many operational networks that have implemented some level of control have done so at the IDMZ, or Level 3.5. As the IDC becomes more modern, it also becomes more connected, relying on cloud connectivity for services to run as intended. More connectivity leads to an expanded attack surface, and if an attack were to breach the boundary firewall, more protection would be needed.

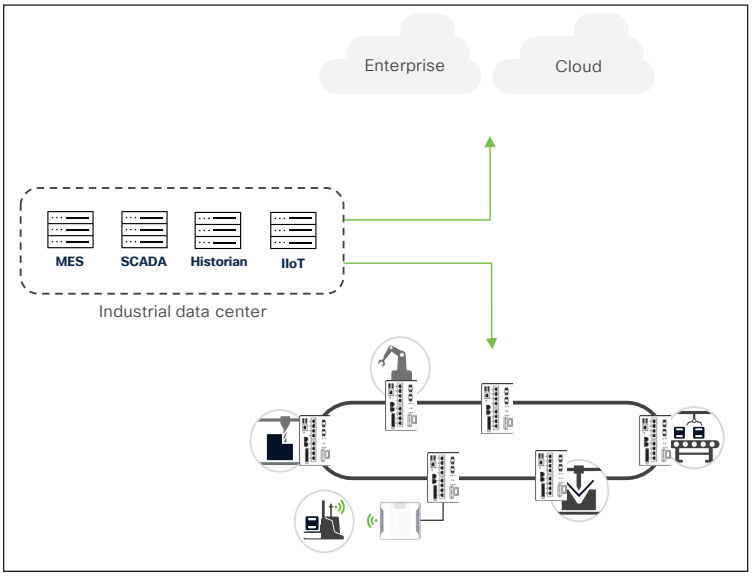

Figure 2. Access control at the industrial data center boundary

© 2025 Cisco and/or its affiliates. All rights reserved.

The IDC must have a segmentation point between it and the plant floor. Micro-segmentation (see the Cisco data center security webpage) of the data center is out of scope for the Cisco Industrial Security Design Guide, but within scope is the firewall that should be placed at the IDC boundary. As modern systems are deployed in the operational network, they will ultimately coexist with legacy systems that need protection from the newly exposed attack vectors.

Ideally, a separate firewall deployment is dedicated to the IDC boundary, even if that firewall is virtual. However, in small plant environments, the same firewall used at the IT/OT boundary could be shared with the IDC or any other "macro zones" in the operational network.

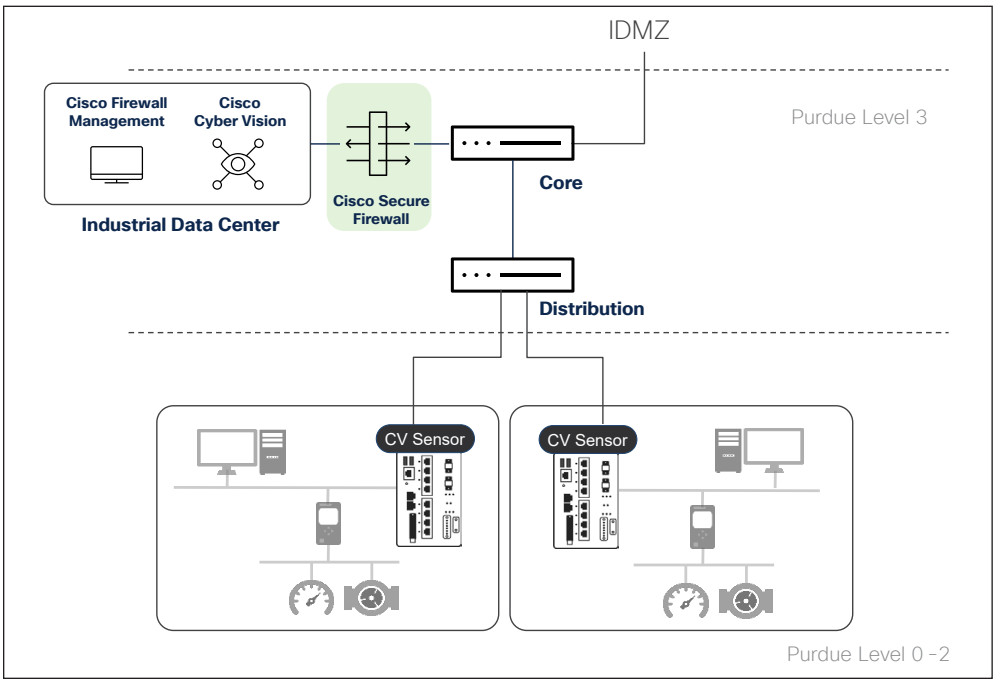

Figure 3. Cisco Secure Firewall at the industrial data center boundary

When using Cisco Secure Firewall for protecting IDC flows in OT environments, consider the following:

- Start with visibility to map out the existing network topology and understand traffic flows and potential bottlenecks. Firewalls cannot be deployed using trial-and-error policies within an operational environment. If you do not understand the flows that will cross an enforcement point, you will likely experience unexpected downtime.
- Choose an appropriate model, keeping in mind the load on the network. Correct sizing of the firewall is critical to avoid an increase in latency and jitter, which is detrimental to OT traffic. Ensure that the firewall can handle the peak loads of the network traffic.
- Deploy access control policies in monitor mode before pushing them to production. Adding the **Monitor** action to an access control rule causes policy matches to be logged, but the system will continue to match traffic against existing rules to determine whether to permit or deny it. This allows administrators to test their policies in production without the risk of erroneous rules causing downtime.

© 2025 Cisco and/or its affiliates. All rights reserved.

- For increased flexibility and ease of use, use **objects** in access control policies. These are reusable configurations that associate a name with a value. For example, when referencing a list of IP addresses in an access control policy (such as a list of engineering workstations on the plant floor), store the list of IP addresses as a policy object. That way, anytime the engineering workstations are referenced in policy, they can be called by name. IP addresses can be added or removed by changing the object, eliminating the need to modify the rules that reference the object.
- Use application control policies to provide read-only access to assets on the shop floor. Introducing machine learning applications into OT networks will typically require some level of visibility into control operations. To accomplish this, MQTT brokers will be introduced to the network, but those brokers often have OT protocol connectors to collect data before publishing to a message bus. Use application control policies in the network to make sure these brokers, or anything else in the IDC that requires access to data over insecure OT protocols, are restricted to read-only rules.
- Consider using a virtual firewall to protect virtualized infrastructure in plant networks. Organizations are looking to reduce their physical footprint, and the firewall is another element of the network that can be virtualized while offering the same level of protection we are accustomed to with physical appliances.
- Implement fail-safe mechanisms to maintain operations if the firewall fails. Clustering allows multiple Cisco Secure Firewalls to function as a single logical firewall. As of release 7.2, clustering is also supported on Cisco Secure Firewall Threat Defense Virtual (FTDv).

Preventing lateral movement on the plant floor

It may seem counterintuitive to leave this topic until last, as this is the main reason operators need a segmentation strategy. How do we ensure that the most critical parts of our networks will not be taken down by a malicious attack?

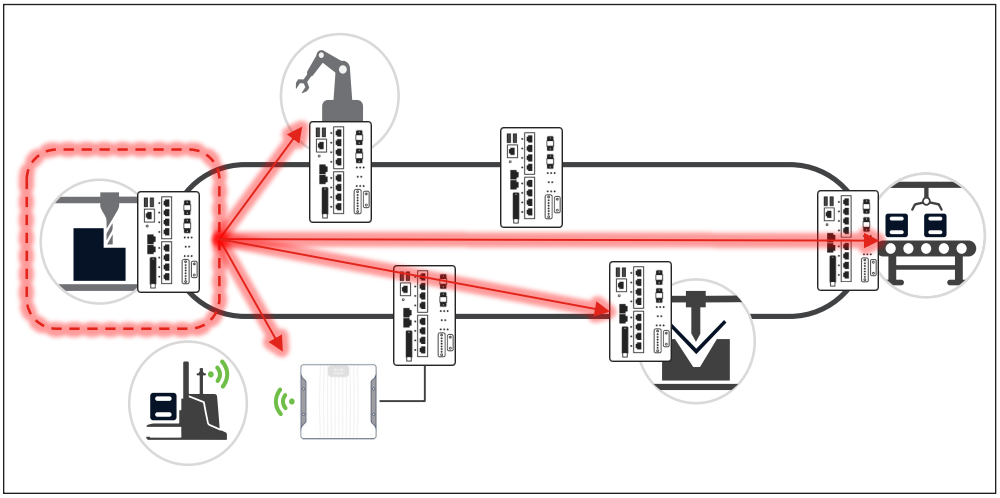

Figure 4. Prevent lateral movement within the OT

© 2025 Cisco and/or its affiliates. All rights reserved.

Security is an architecture, not a product. Defense-in-depth is a strategy, not simply deploying the same policies everywhere. Internet policies should have been covered by the IT/OT boundary firewall, threats from modern assets should be covered by the IDC firewall, and there is a dedicated chapter in the Industrial Security Design Guide on remote access. Preventing lateral movement on the plant floor is the last line of defense. If threats make their way into a system, either through poorly implemented controls, cellular back doors, or a simple USB stick, the blast radius will be reduced to only the system that has been affected.

Using a firewall to route between OT VLANs

The first consideration for preventing lateral movement is to use Cisco Secure Firewall as the termination point for VLANs in OT networks.

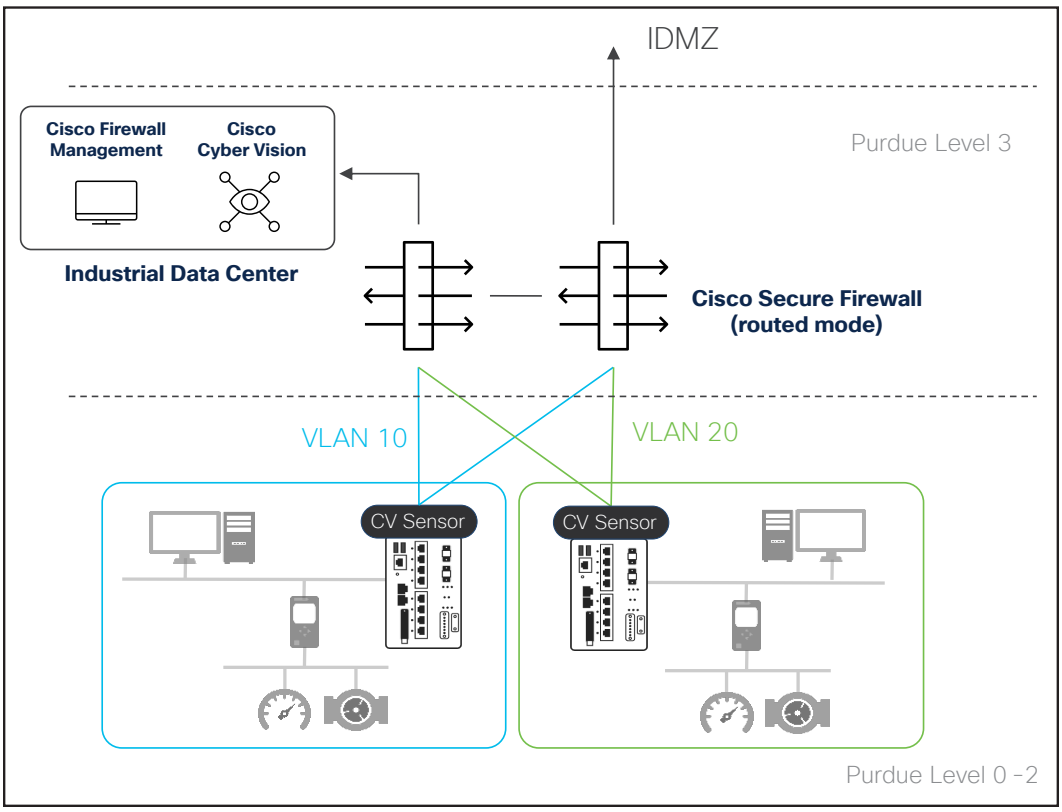

Figure 5. Cisco Secure Firewall as routing point for OT networks

VLANs are often overlooked but are great for separating devices into their own networks. The “problem” with VLAN segmentation is that the segments are not hidden from each other. Devices can simply communicate from one VLAN to the next through a routing point, which in many operational networks is a Layer 3 switch. Many deployments rely on the Layer 3 boundary to implement policies in the network, and while a switch-based enforcement option is discussed in the Industrial Security Design Guide (using Cisco Identity Services Engine), security architects should consider a firewall at this layer of the network.

© 2025 Cisco and/or its affiliates. All rights reserved.

By using Cisco Secure Firewall as the point of routing in an OT network, you will reduce the blast radius to an individual VLAN. This approach works well in greenfield environments, where network architects have the luxury of implementing a network design from scratch and the VLAN structure can be well thought out. It is also useful for transitioning a plant with an existing VLAN structure to a more secure state.

Using a firewall to terminate the VLANs does not have to be an all or nothing approach. For many organizations, the operational network may share IT and OT resources and already use a switched network to route between subnets. In this case, some of those VLANs could be migrated to a firewall, where the gateway of the VLAN is removed from the distribution switch and instead given to the firewall.

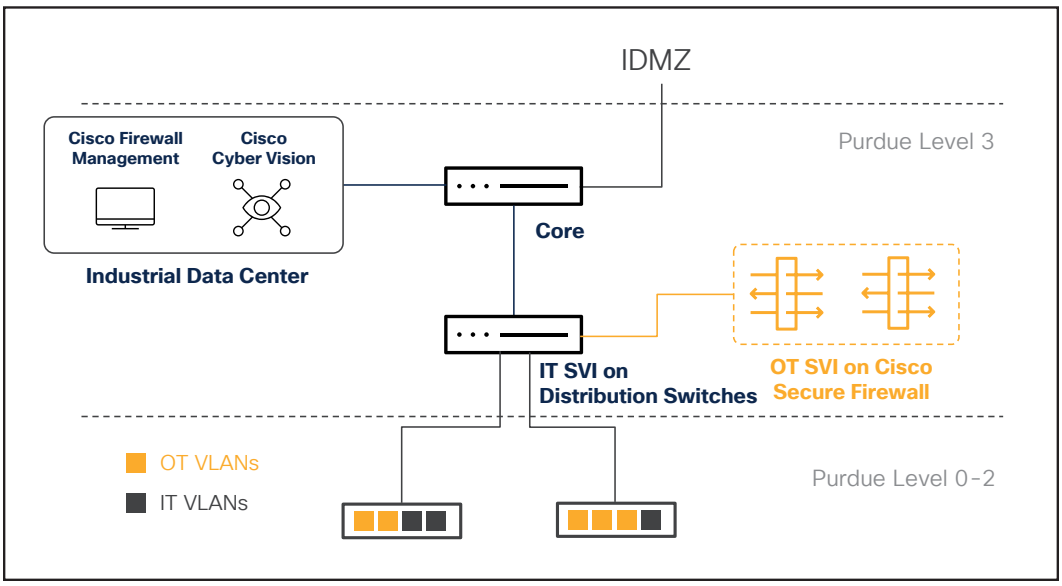

Figure 6. Cisco Secure Firewall for OT VLANs only

In this design, non-OT traffic (or traffic deemed less critical) would continue to use the switching infrastructure to route between VLANs, and selected traffic would be subject to firewall enforcement between networks.

© 2025 Cisco and/or its affiliates. All rights reserved.

Transparent firewalls at the cell/area zone boundary

The reality of OT networks is that many organizations are dealing with a large, flat network, and creating VLAN segments is not always an option. In this scenario, Cisco Secure Firewall can be deployed in transparent mode to act as a bump in the wire for all traffic that traverses the cell/area zone boundary.

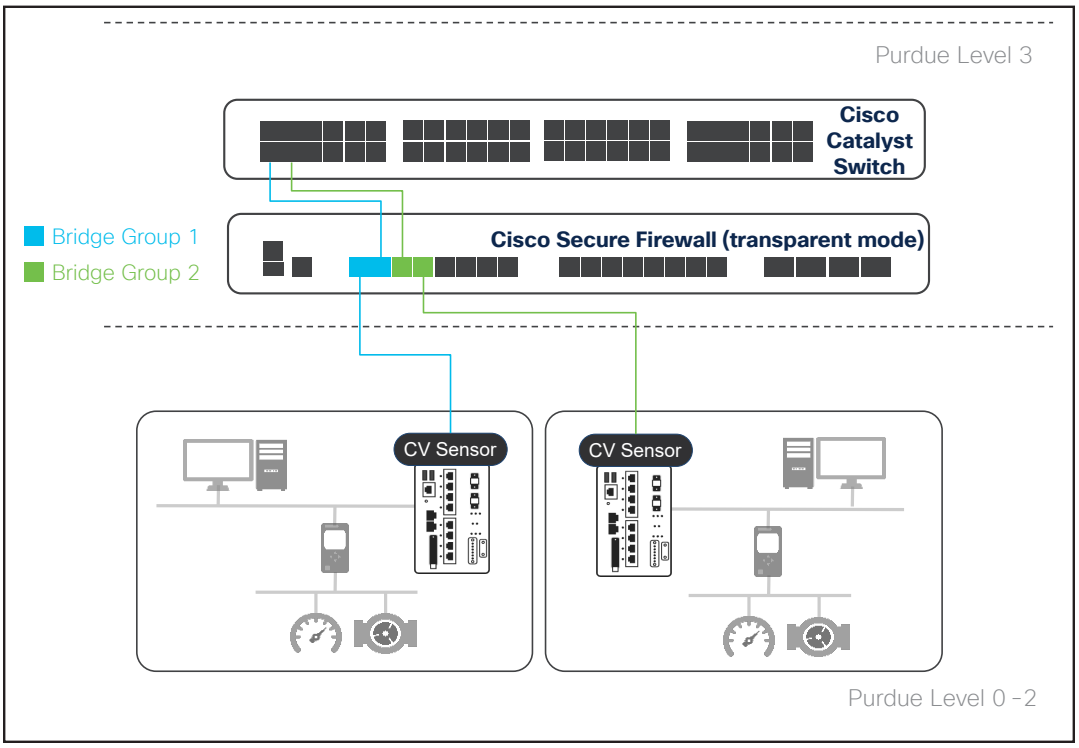

Figure 7. Cisco Secure Firewall in transparent mode

Bridge groups can be used to group firewall ports together to pass traffic between the interfaces. Each directly connected network must be on the same subnet. This deployment mode should be considered for brownfield deployments, where the network is relatively flat and cannot be changed to accommodate VLAN separation. The distribution and core switches will continue to be responsible for passing packets throughout the network, allowing firewall rules to be added without any changes to the network.

Note: There will need to be some period of downtime, as cables will be unplugged to position a firewall in between. To reduce unnecessary outages in production, we recommend provisioning the firewall(s) in a lab environment before moving them into the plant network.

When a firewall is inserted transparently into an OT network, it will interfere with traffic communicating in the same network domain. OT protocols such as Profinet expect deterministic network latency and jitter. When inserting a firewall device into an existing brownfield environment, or even when planning a new deployment, it is of paramount importance to test the end-to-end latency in a staging or Proof of Concept (POC) area to ensure that the firewall can handle data with minimal latency to avoid disrupting real-time operations.

© 2025 Cisco and/or its affiliates. All rights reserved.

Leveraging Cisco Cyber Vision for plant floor visibility to aid in policy creation

Gaining comprehensive visibility into connected assets

As industrial networks can be quite old, be widely dispersed, and involve many contractors, organizations often don't have an accurate inventory of what's on the network. Gaining comprehensive visibility into what's connected to your plant network is critical both to efficiently manage resources and to assess risks so you can prioritize what needs to be fixed to reduce your exposure to cyber risks.

Visibility also helps in implementing network segmentation by giving organizations a good understanding of the normal state of the OT network so that they can distinguish attacks from transient conditions or normal operations within the environment. Whether you are using a risk-based approach, a functional model, or other organizing principle, grouping components into levels, tiers, or zones is a precursor activity before you can consider applying policy to protect and monitor communication between zones. Implementing network monitoring in a passive mode and analyzing the information to differentiate between known and unknown communication may be a necessary first step in implementing security policies.

Cisco Cyber Vision is the software solution built into Cisco industrial routers and Cisco Industrial Ethernet switches to give comprehensive visibility and help implement security policies in industrial networks. It consists of multiple sensors that perform DPI, protocol analysis, and intrusion detection within your industrial network 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, API, and more. It may also run on a hardware appliance or as a virtual machine.

The Cyber Vision sensor software can be hosted on Cisco Industrial Ethernet switches and the Cisco Catalyst™ 9300 and 9400 Series platforms as an IOx application running in a dedicated CPU core to avoid impacting network performance. It passively captures and decodes network traffic using DPI of industrial control protocols. As the sensor software is embedded in the switch, there is no need to deploy dedicated appliances or build an out-of-band Switched Port Analyzer (SPAN) collection network. Because it decodes network traffic at the edge, the sensor sends only lightweight metadata to Cyber Vision Center, adding just 2% to 5% load to your industrial network.

© 2025 Cisco and/or its affiliates. All rights reserved.

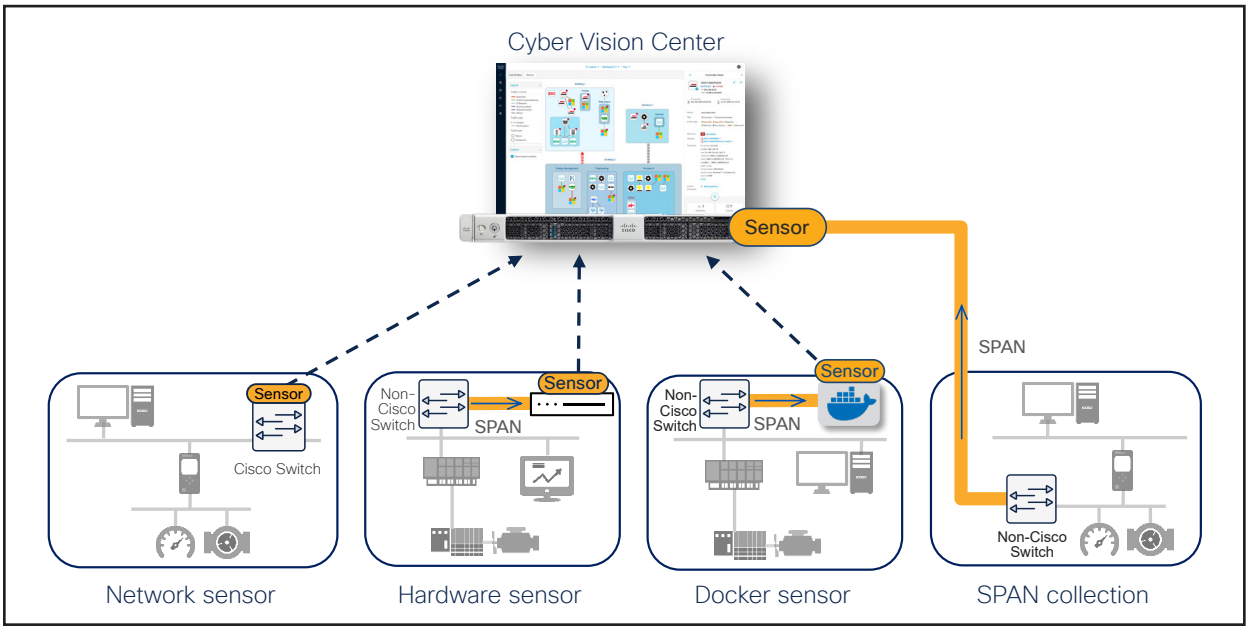

Figure 8. Implementing Cyber Vision in the OT network

Using OT visibility to create firewall policies using CSDAC

The Cisco Secure Dynamic Attributes Connector (CSDAC) was initially created for Cisco Secure Firewall policies to adapt in real time to the changes in public and private cloud workloads and business-critical Software-as-a-Service (SaaS) applications.

Using CSDAC with Cisco Secure Firewall Management Center (FMC)—the centralized management platform for Cisco Secure Firewall—simplifies policy management by keeping the rules up to date without tedious manual updates and policy deployment. With CSDAC, you can centrally manage workload attribute feeds obtained from multiple public and private cloud environments, enabling firewalls to instantaneously adapt to changes in complex and dynamic environments.

CSDAC significantly improves network security with simultaneous propagation of automatic endpoint attributes and contextual awareness, preventing the buildup of outdated firewall rules over time. With CSDAC, the firewall policy becomes more dynamic, more secure, and much easier to manage. As illustrated in the figure below, CSDAC discovers resources and IP addresses and translates this information to dynamic network objects consumed by the firewall. It keeps track of changes in the environment and updates dynamic objects accordingly in near real time.

© 2025 Cisco and/or its affiliates. All rights reserved.

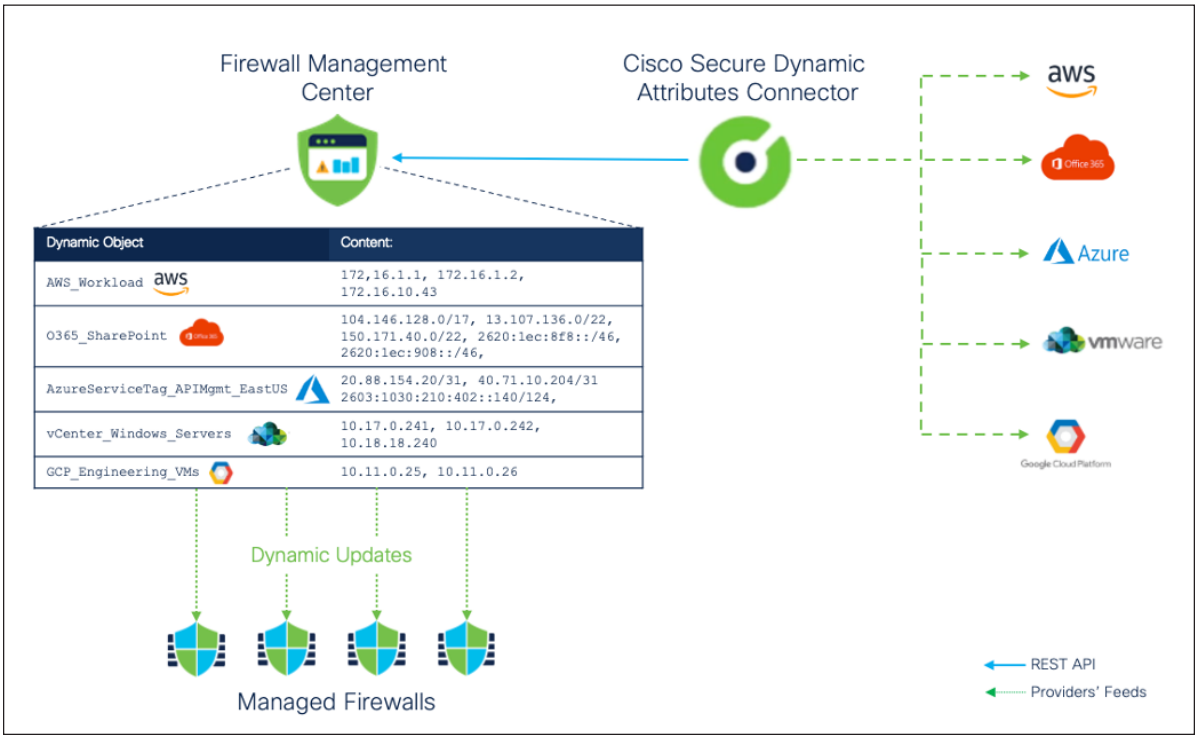

Figure 9 Cisco Secure Dynamic Attributes Connector examples

CSDAC maps IP addresses of resources to dynamic objects, which are then used in access control policy rules. Changes in the environment detected by CSDAC are cascaded in real time to the FMC and, in turn, to the managed firewalls without any administrator action. The figure below illustrates, step by step, how CSDAC dynamically updates firewall policy.

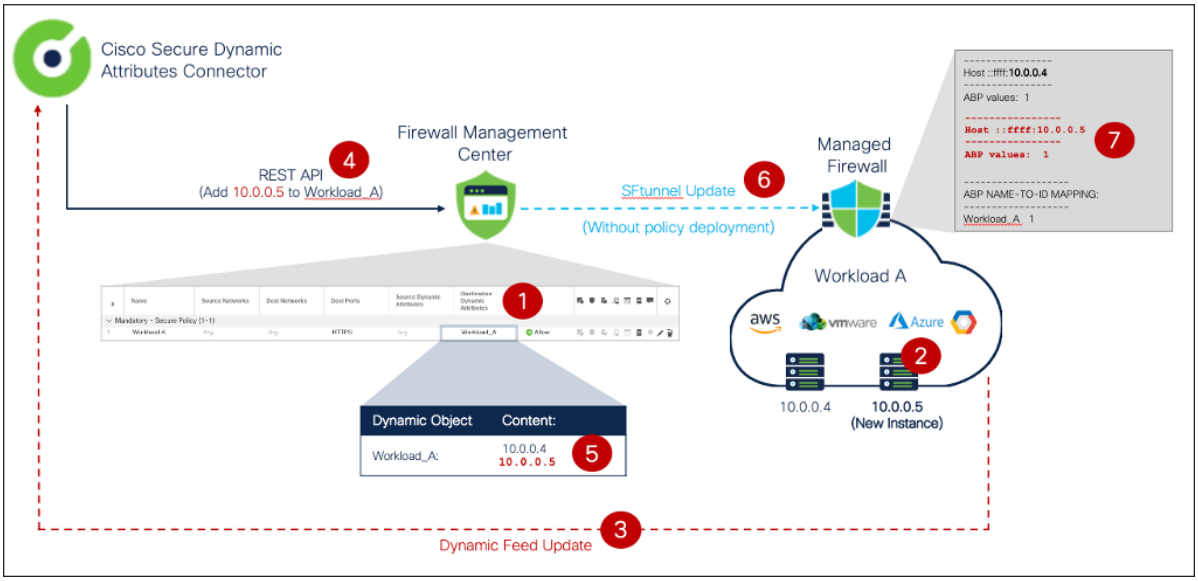

Figure 10. CSDAC dynamic object update

© 2025 Cisco and/or its affiliates. All rights reserved.

1. The firewall protects a workload and is configured with an access control policy containing the dynamic object Workload_A representing cloud resources.
2. CSDAC monitors changes to the workload constantly and detects when a new instance is spun up.
3. CSDAC detects the workload change and evaluates the user-created attribute filters.
4. CSDAC triggers a REST request to update the Workload_A dynamic attribute with the 10.0.0.5 IP address of the new server.
5. Firewall Management Center adds the new IP address to the dynamic object.
6. Immediately after the Workload_A object change, FMC pushes an update to all the managed firewalls using that object in deployed access control policies. The dynamic object update happens automatically and does not require a policy deployment.
7. The firewall updates the new IP address in Snort's identity memory and its policy to allow the new server access.

CSDAC is a software interface that interacts with a public or private cloud provider to retrieve up-to-date network information, categories, and tags. It translates information to dynamic objects used in firewall access control policies on FMC. Architecturally the connectors are software plug-in modules installed in CSDAC, which allows the straightforward addition of new connectors in future releases.

Up to this point, all examples have demonstrated how the firewall can be kept up to date with changes in cloud or data center workloads; however, when deploying policy in OT environments, it is important to have context for both ends of the connection. This is where the Cyber Vision connector can be used.

Cyber Vision connector for CSDAC

Cyber Vision and FMC allow OT segmentation groups defined in Cyber Vision by the OT team to be used for firewall enforcement. This level of automation helps reduce manual workloads, streamlines your security management process by enabling IT/OT collaboration, and helps ensure that your firewall policies remain in lockstep with your industrial processes.

- Cisco Cyber Vision inventories industrial assets and maps their communication activities.
- Operations managers leverage the Cyber Vision maps to group assets into industrial zones.
- Cisco FMC pulls asset group information from Cyber Vision using CSDAC.
- Each Cyber Vision group becomes a dynamic object in FMC, to which the IP addresses of the assets in the group are mapped in real time.
- IT and OT managers work together to define access policies to be applied to each dynamic object.
- Policies defined in FMC are enforced by Cisco Secure Firewalls.
- Any modification to Cyber Vision groups is reflected in FMC dynamic objects in real time and is automatically enforced by Cisco Secure Firewalls, without the need to redeploy policies.

© 2025 Cisco and/or its affiliates. All rights reserved.

For a quick demo of this workflow, please watch this video.

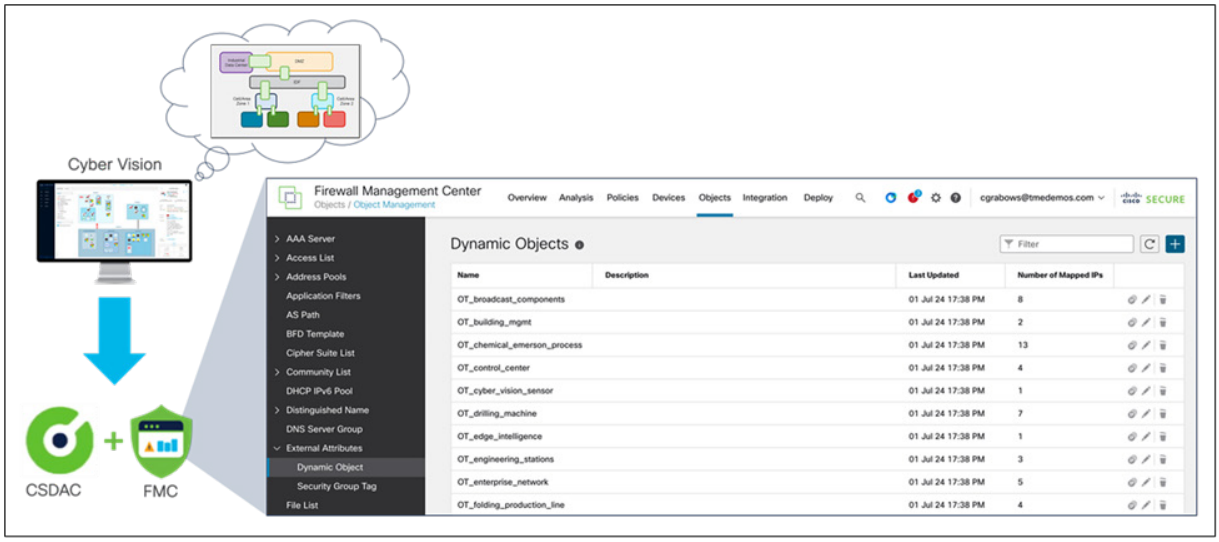

Figure 11. Cyber Vision integration to Cisco FMC via CSDAC

Using CSDAC, OT asset groups created in Cyber Vision are automatically made available to FMC as dynamic objects. IP addresses of OT assets are continuously imported and mapped to dynamic objects, helping ensure that objects are always aligned with the industrial processes defined by the OT team.

The dynamic nature of this integration eliminates the need for manual policy deployment each time there is a change to the Cyber Vision map. Adding an asset to a group in Cyber Vision or moving it to another group will automatically modify the corresponding object in FMC. The access policy configured for this object will apply to this asset in a matter of seconds.

Capability highlights

The intent of this solution brief is not to provide a comprehensive capability list for Cisco Secure Firewall. The Cisco Industrial Security Design Guide provides more detail on capabilities such as the encrypted visibility engine , SnortML rules, and Cisco TrustSec®. However, this solution brief highlights two key use cases for operational networks: OT protocol recognition and virtual patching.

OT protocol recognition

In its most basic form, a firewall provides access control policies that inspect and/or control network traffic across a boundary. Cisco Secure Firewalls can control traffic based on:

- Simple, easily determined transport and network layer characteristics—source and destination IP, ports, protocol, and so on.
- The latest contextual information on the traffic, including characteristics such as reputation, risk, business relevance, application uses, or URL visited.

© 2025 Cisco and/or its affiliates. All rights reserved.

- Realm, user, user group, or ISE attribute.
- Security Group Tag (SGT).
- Characteristics of encrypted traffic; you can also decrypt this traffic for further analysis.
- Whether unencrypted or decrypted traffic contains a prohibited file, detected malware, or intrusion attempt.
- Time and day (on supported devices).

One common way to control the flow of traffic through a modern firewall is the use of application-aware policies. Cisco Secure Firewall currently identifies over 7000 specific applications. Using access control rules, application traffic can be trusted, blocked, or allowed but passed on for deep packet analysis and threat inspection.

Applications can be identified regardless of whether they are operating on standard network ports. In some cases, the presence of specific applications operating over nonstandard ports may indicate a policy violation or an attempt to evade firewall controls. Cisco Secure Firewall can identify these nonstandard connections and generate alerts or block traffic as needed.

More information on application control features in Cisco Secure Firewall can be found in the online documentation. The Industrial Security Design Guide highlights the ability to detect SCADA protocols throughout the plant network. Whether it is Modbus messages or Ethernet/IP between Rockwell devices, Cisco Secure Firewall not only understands that the application is present in the communication but also knows the specific function codes being used by the system. For example, it understands whether a newly deployed IIoT device is reading data from a PLC (i.e., Modbus Read) or is attempting to manipulate data in the control loop (i.e., Modbus Write). It can also do per-packet inspection and per-packet control to help ensure that only the relevant permissions are enabled between devices, which is especially important as modern systems look to retrieve critical information for data analytics and operators need peace of mind in knowing that read-only access is enforced over the network.

Virtual patching

Traditional patching methods, although effective, may not always be feasible due to operational constraints and the risk of downtime. When a zero-day vulnerability is discovered, there are a few different scenarios that play out. Consider two common scenarios:

- A newly discovered vulnerability poses an immediate risk and the fix or the patch is not available.
- The vulnerability is not highly critical, so it's not worth patching it outside the usual patch window because of the production or business impact.

In both cases, one must accept the interim risk and wait either for the patch to be available or for the patch window schedule.

© 2025 Cisco and/or its affiliates. All rights reserved.

Virtual patching, a form of compensating control, is a security practice that allows you to mitigate this risk by applying an interim protection or “virtual” fix to known vulnerabilities in the software until it has been patched or updated. Virtual patching is typically done by leveraging an Intrusion Prevention System (IPS) such as Snort®. When Cisco Secure Firewall is deployed in the plant network, IPS policies can be enabled to give peace of mind that known vulnerabilities cannot be exploited over the network.

Cisco Secure Firewall portfolio

The Secure Firewall brand encompasses the Adaptive Security Appliance (ASA) and Threat Defense solutions. For the purposes of the design guide, any reference to Cisco Secure Firewall is referring to the Firewall Threat Defense (FTD) portfolio, otherwise known as Cisco Secure Firewall Threat Defense.

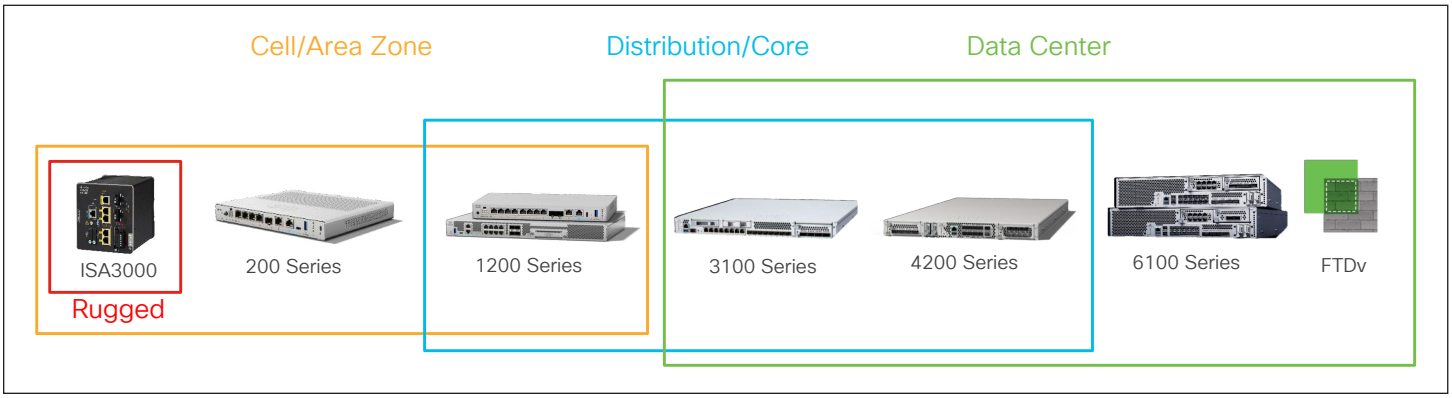

Figure 12. Cisco Secure Firewall portfolio

The choice of firewall will ultimately be determined by the throughput requirements for a given use case. A dedicated firewall for securing data traveling into and out of the cell/area zone will have much smaller throughput requirements than a data center appliance. For more information on each firewall’s specifications, such as performance metrics, see the Cisco Secure Firewall webpage.

© 2025 Cisco and/or its affiliates. All rights reserved.

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 OT 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 of 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.

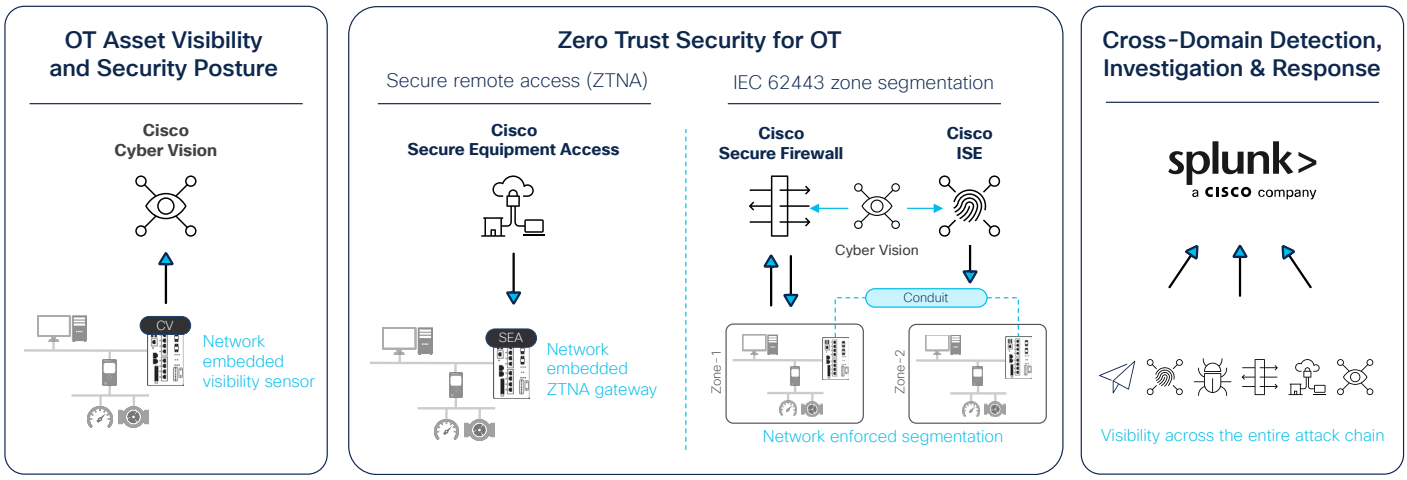

Figure 13. Cisco's Industrial Threat Defense OT security solution

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

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)
C22-5286595-00 07/25