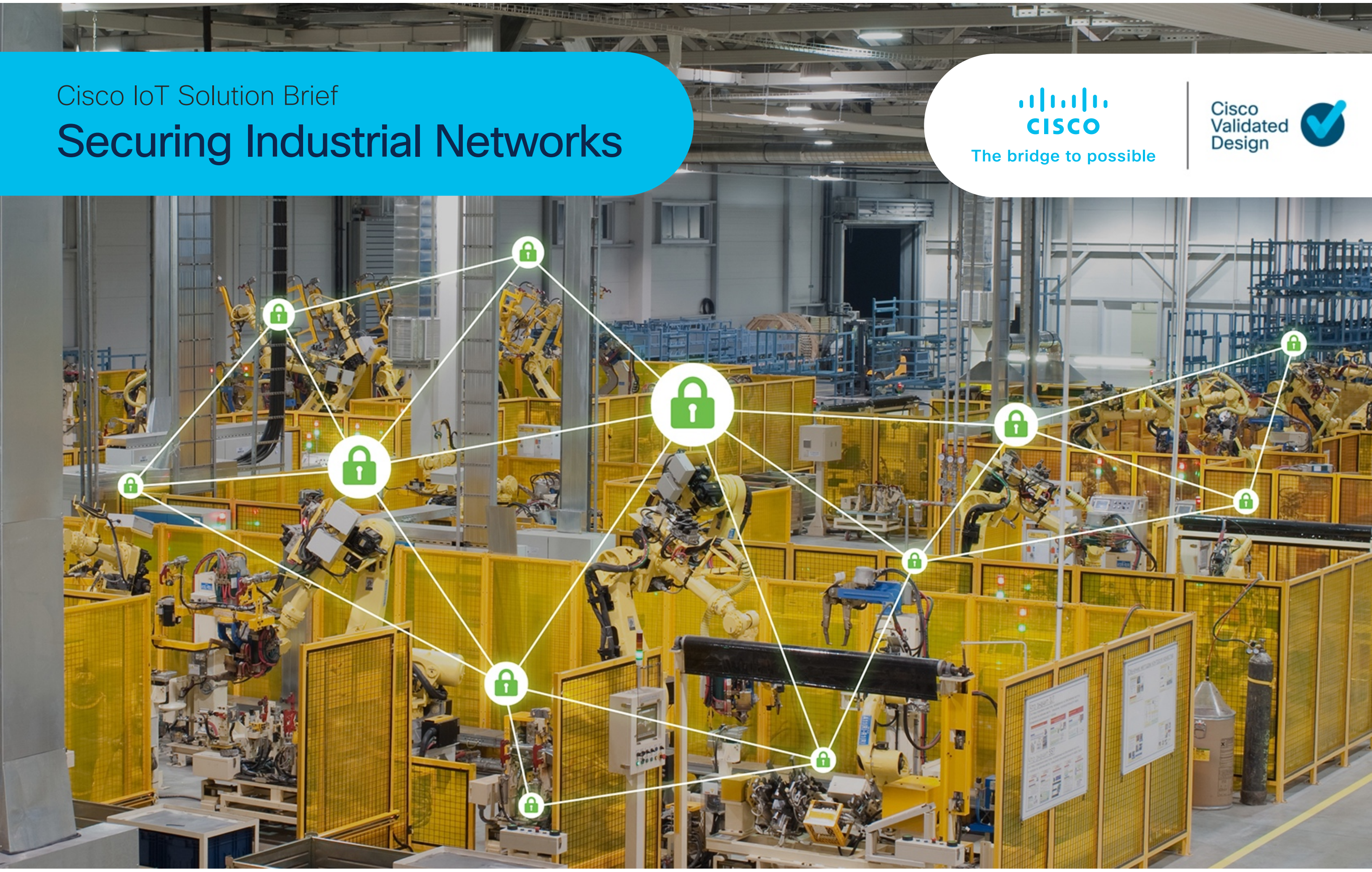
Cisco IoT Solution Brief

Securing Industrial Networks



Benefits

Improve industrial cybersecurity by:

- Discovering and inventorying assets
- Containing security incidents
- Detecting and preventing known attacks
- Protecting against malware
- Integrating enterprise and operations security

Protecting manufacturing operations against cyber threats:

Introduction to Cisco industrial network security

Over the years, manufacturers around the world have been connecting their industrial environments to enterprise networks to automate production and gain operational advantages. Organizations are now deploying Internet of Things (IoT) technologies to migrate to Industry 4.0, optimize production, and build new generations of products and services.

This deeper integration between IT, cloud, and industrial networks is creating many cybersecurity issues that are becoming the primary obstacle to industry digitization efforts.

Media reports regularly highlight cyber attacks on manufacturers across all verticals, wreaking expensive havoc on operations. The growing number of cases shows that industrial networks have become a target and securing them is now the key to ensuring production integrity, continuity, and safety.

Cisco is a leader in securing enterprise networks. Cisco is also a leader in industrial networking. We are leveraging these unique portfolios of products and solutions, together with threat intelligence from Talos®, one of the world's largest security research teams, to make security inherent and embedded in the industrial network.

To help industrial organizations secure their operations, Cisco® Validated Designs (CVDs) provide the core network foundation of architectures that meet the needs of operations and IT. This solution brief is a high-level overview of the reference architecture described in the "Networking and Security in Industrial Automation Environments" CVD.

It describes a security journey for an industrial network, starting with strong foundation-level security and then, as the organization matures, growing into a comprehensive full-spectrum security design.

Securing the industrial network is a journey

Industrial control networks connect devices that have been deployed over a period of many years – sometimes even decades – beginning back when cybersecurity wasn't a concern. When organizations attempt to secure their industrial IoT networks, they encounter three primary issues:

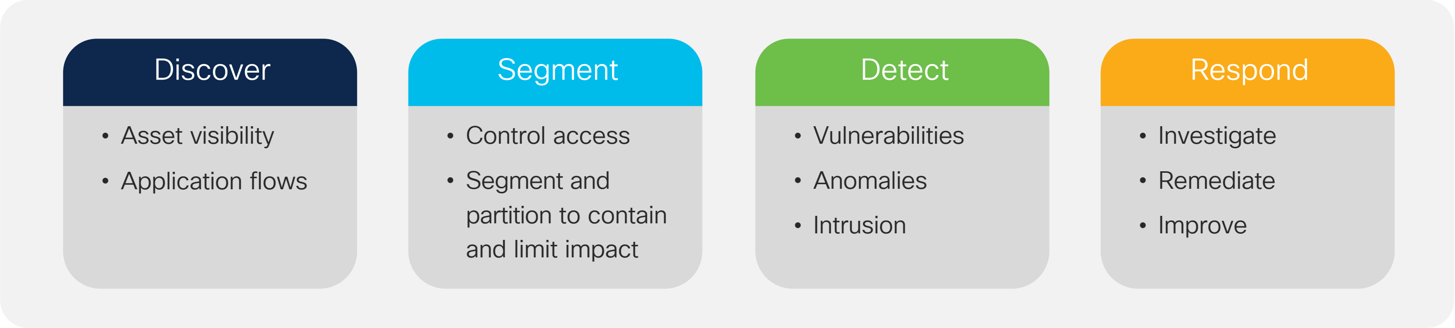
- **A lack of visibility:** Manufacturers often don't have an accurate inventory of what's on their industrial network. Without this, they have limited ability to build a secure communications architecture.
- **A lack of control:** A lack of visibility also means that manufacturers are often unaware of what devices are communicating, and where those communications are going. You cannot control what you don't know about.
- **A lack of collaboration:** OT devices and processes are managed by the operations team. Cybersecurity is generally driven by the IT and security teams. All these stakeholders need to collaborate to build the specific security policies and enrich events with context so that security incidents do not disrupt production.

Addressing these issues and building a secure industrial network will not happen overnight. To help ensure success, Cisco promotes a phased approach in which each phase builds the foundation for the next, so that you can enhance your security posture at your own pace and demonstrate value to all stakeholders when embarking on this journey.

Key requirements

Figure 1 depicts the key requirements for securing industrial networks and can guide the development of a security lifecycle process. Compliance standards often guide security needs as well. This security solution brief provides the blueprints for two designs to meet these requirements.

Figure 1. Key requirements for securing industrial networks



Discover
- Asset visibility
- Application flows

Segment
- Control access
- Segment and partition to contain and limit impact

Detect
- Vulnerabilities
- Anomalies
- Intrusion

Respond
- Investigate
- Remediate
- Improve

Extending IT security to OT through effective collaboration

To successfully secure the OT environment, all stakeholders must work together. Operations understands the industrial environment – the devices, the protocols, and the business processes. IT understands the IP network. And the security team understands threats and vulnerabilities. By working together, they can leverage existing security tools and expertise to protect the industrial network without disrupting production safety and uptime.

Cisco security solutions are built into the industrial networks to monitor operations, feed security platforms with OT context, and enable this crucial collaboration.

Network managers will appreciate the unique simplicity and lower costs of Cisco's edge architecture when looking to deploy OT security at scale. Operations will gain real-time insight into the industrial processes, so they can maintain system integrity and production continuity. Security teams will have visibility into industrial assets and communications with context enriched by control engineers.

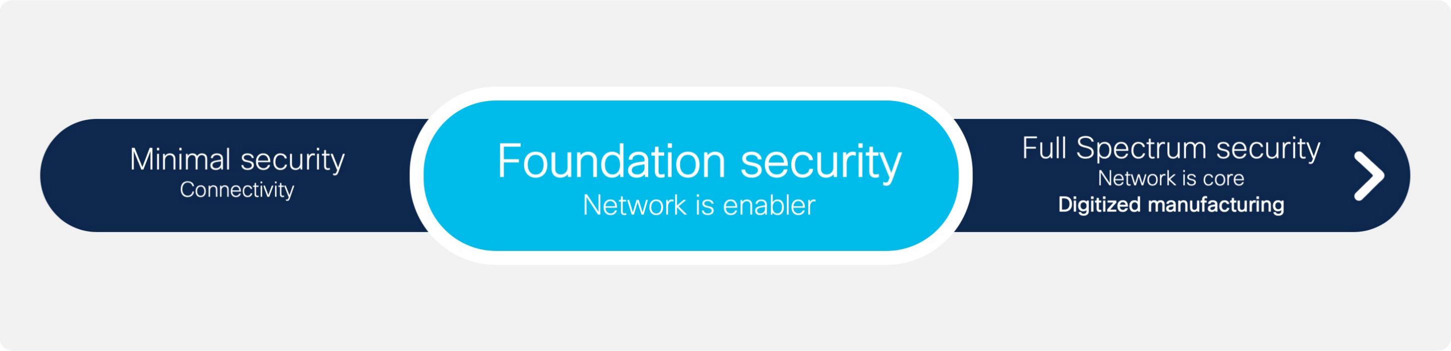
Taking a phased approach to industrial security

Cisco's approach to deploying industrial cybersecurity includes three phases. Initially, there is a minimal level of security consisting of configuring an industrial demilitarized zone (IDMZ) to separate the industrial and enterprise networks. This is the mandatory first step in industrial security, and we are assuming that all have already embraced it, so it will not be discussed in this brief.

But as organizations connect more devices, enable more remote access, and build new applications, the airgap erodes and becomes insufficient. Industrial organizations need to build on this minimal level of security to move to the Foundation and eventually Full Spectrum security models. This CVD is created to protect your investment while your security posture matures.

Many industrial companies are at minimal security – that is insufficient in today's cyber-security environment.

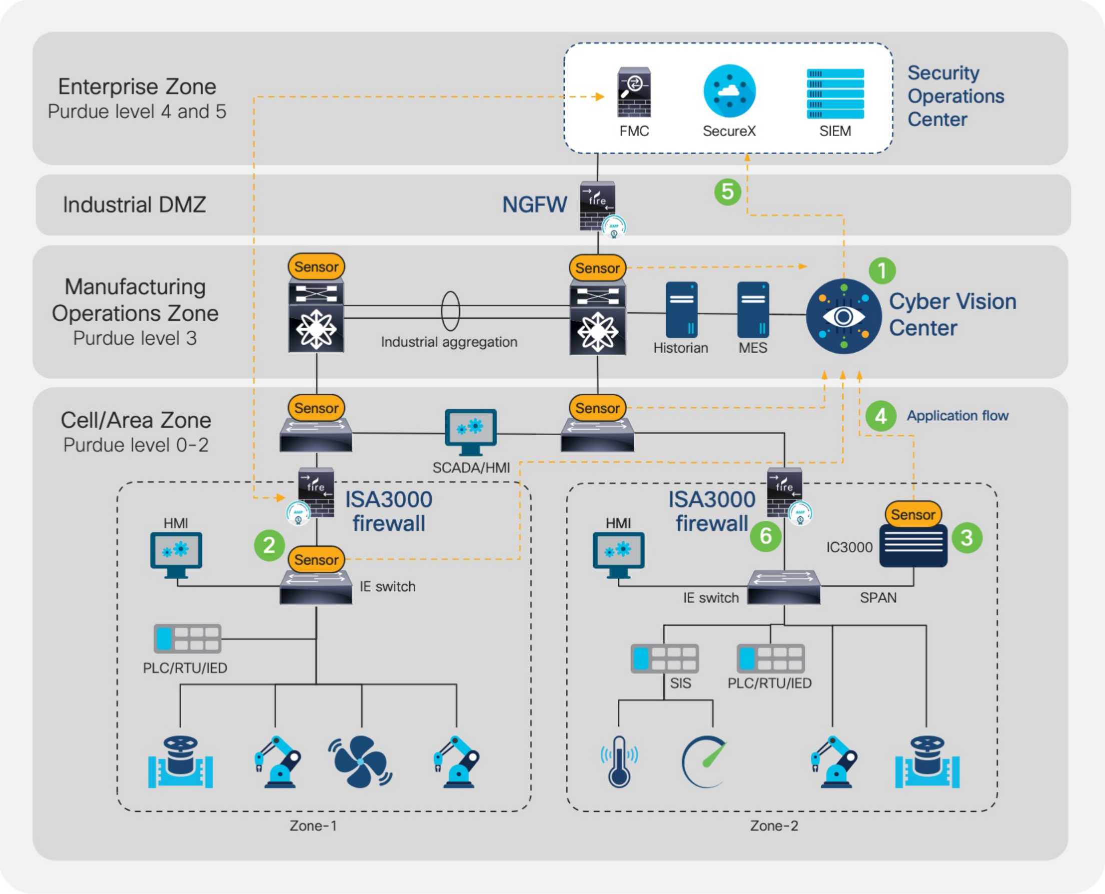
Figure 2. Typical security journey



Design 1: Foundation security

The Foundation security design is a blueprint for a secured, robust, and reliable industrial network. It provides for industrial asset visibility, macro/zone segmentation, zone access control, intrusion detection, threat detection, and response. It enables coordination with information security for consistent access policy management and aggregation of industrial security events in the security operations center (SOC).

Figure 3. Foundation security design



Foundation security features

- Asset visibility
- Macro/zone segmentation
- Zone access control
- Intrusion and malware protection
- Threat response

This design follows the Purdue model. Network management and other networking aspects such as redundancy, etc., are described in detail in the CVD "Networking and Security in Industrial Automation Environments."

1 Cyber Vision Center: Centralized analytics platform

2 Cyber Vision network sensor: Deep packet inspection (DPI) embedded in network infrastructure, eliminating the need for a separate SPAN network

3 Cyber Vision hardware sensor: Dedicated sensor appliance that performs DPI on SPAN traffic

4 Application flow: Lightweight metadata streamed from Cyber Vision sensors to Cyber Vision Center

5 Industrial asset metadata flow: Context, vulnerabilities, and events communicated to the SOC

6 Industrial security appliance: Segments, controls access, and detects and blocks intrusions and malware

Asset visibility

Visibility into the security stance of industrial devices and communications is a key capability. Cisco Cyber Vision provides visibility into all industrial assets and creates inventories that have relevant details such as device type, firmware version, etc. Cyber Vision Center is deployed as a sitewide application. Cyber Vision sensors are embedded into the cell/area network equipment to discover devices, monitor communications, and pass security telemetry to Cyber Vision Center.

These sensors inspect the packets and analyze them for asset details, communications, and industrial control system (ICS) process data. The Center visualizes this information and correlates vulnerability information. Investigations and patching activities can be driven from this. Cyber Vision connects to Cisco Firepower® Management Center and Cisco SecureX™ to provide industrial asset information, enhancing context around devices for policy enforcement.

Cyber Vision

Zone/macro segmentation and malware protection

The industrial network is segmented from the enterprise network by an IDMZ implemented by a Cisco next-generation firewall (NGFW).

The various parts of the industrial network should also be segmented in a way that enables each segment to form a semiautonomous zone. The goal is to limit and contain security incidents within a zone. The ISA/IEC-62443 industrial cybersecurity standard describes how such an approach can be implemented by establishing communication conduits between zones, where access and communication is controlled.

Zones are established by having separate LANs and/or VLANs, with conduits between zones enforced by the Cisco 3000 Series Industrial Security Appliances (ISA3000). The ISA3000 provides the access and communication control, as well as intrusion detection capabilities. The configuration, including access control lists (ACLs) and policies, is managed by Cisco Firepower Management Center. The ISA3000 and Cisco NGFW can also include Cisco Advanced Malware Protection (AMP) to provide protection against malware.

Cisco 3000 Series Industrial Security Appliance

Threat investigation and response

The design envisions a security operations center that consolidates security events and vulnerabilities across the entire organization and manages the response. Cisco SecureX threat response accelerates investigations by automating and aggregating threat intelligence and data across your security infrastructure – both Cisco and third parties – into one unified view.

Solution introduction and operational considerations

Cisco Cyber Vision is a software feature built into the network (Cisco Catalyst® IE3400, 1101 Industrial ISR, Catalyst 9300 Series, etc.). This makes it very easy to deploy at scale, as there is no additional hardware or switch port analyzer (SPAN) connection to deploy. Enabling industrial cybersecurity monitoring is just a question of installing the central console and activating the software within the network. This reduces the risk of a production outage during deployment and needs very low overhead to coordinate with plant operations.

To get the most out of this design, security, operations, and IT must set up an effective collaboration.

There are fewer products, so operationally this design poses low overhead.

Introducing the ISA3000 does need careful planning, as necessary communications can be stopped and access to needed resources can be denied.

Table 1. Foundation security features

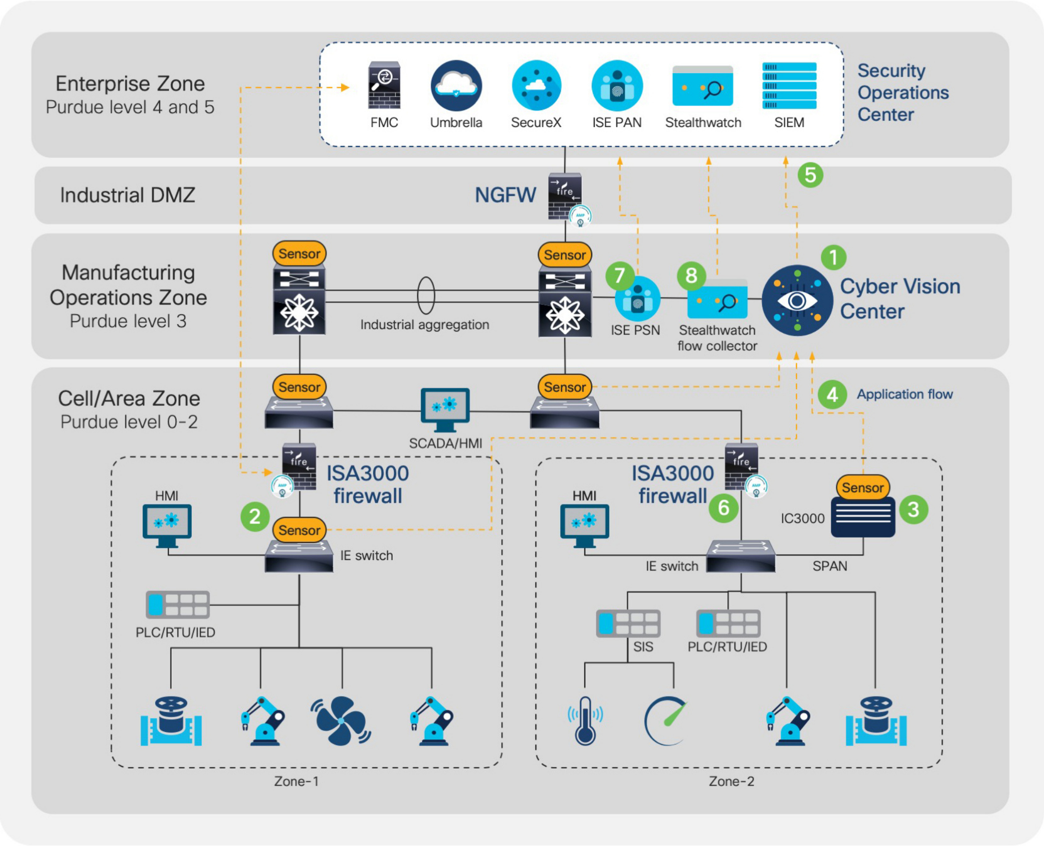
Discover	Asset visibility	Included	Enabled by Cyber Vision and network switches supporting Cisco Cyber Vision sensor – IE3400, IR1101, Catalyst 9300 Series, etc.
	Industrial asset inventory detail	Included	
	Application flows	Included	
	Tracking of ICS process data	Included	
	Baseline ICS application flow	Included	
Segment	Zone/macro segmentation	Included	Zones can be segmented by separate LANs and/or VLANs with access control by ISA3000.
	ICS protocol protection	Included	Provided by ISA3000.
	Isolation of industrial and enterprise networks	Included	NGFW provides IDMZ.
	Device/micro segmentation	In Full Spectrum design	Fine-grained network segmentation to individual device level (Cisco TrustSec®) is described in the Full Spectrum security design.
Detect	Industrial asset vulnerabilities	Included	Cyber Vision will identify known vulnerabilities for industrial assets. It analyses application flows to detect process anomalies.
	ICS process anomalies, attacks	Included	
	ICS communication threats	Included	
	Operational events visibility	Included	
	ICS command filtering	Included	ISA3000 helps ensure plant safety by blocking dangerous asset parameters and unauthorized ICS commands.
	Intrusion detection/protection within industrial network	Included	Provided by ISA3000 for ICS exploits.
	Intrusion detection/protection from enterprise network	Included	Provided by Cisco NGFW.
	Network anomalies	In Full Spectrum design	Provided by Cisco Stealthwatch®, described in the Full Spectrum security design.
	Analysis of malware propagation	In Full Spectrum design	
	Malware protection	Included	Provided by Cisco AMP, available via FTD license.
	DNS security	In Full Spectrum design	Enabled with Cisco Umbrella®, described in the Full Spectrum security design.
Respond	Investigate ICS anomalies	Included	Cyber Vision logging events and application flows.
	Mitigate asset vulnerability	Included	Cyber Vision Center patching guidance to help resolve vulnerabilities or mitigate vulnerability where possible by ISA3000.
	Log events for investigation	Included	Cyber Vision integrates with security incident and event management (SIEM).
	Aggregate threat intelligence	Included	Provided by SecureX threat response.
	Track incidents	Included	Provided by SecureX threat response.
	Improve and optimize segmentation	Included	Provided by Cyber Vision and ISA3000.
	Improve and update baselines	Included	Provided by Cyber Vision.

Design 2: Full Spectrum security

The Full Spectrum security design builds upon the Foundation design. It is a blueprint for a highly digitized, centrally managed, secured, robust and reliable industrial network. In addition to the capabilities of the Foundation security design, it supports micro-segmentation, network anomaly detection, fine-grained access controls to the devices, malware protection, and DNS security.

The design integrates security operations across the enterprise and industrial networks. It brings more of the enterprise security capabilities into the industrial network. The SOC becomes enriched with additional insights into and controls over the industrial network.

Figure 4. Full Spectrum security design



Full Spectrum security features

Foundation security features plus:

- Micro-segmentation (TrustSec)
- Network anomaly detection
- DNS security

This design follows the Purdue model. Network management and other networking aspects such as redundancy, etc., are described in detail in the CVD "Networking and Security in Industrial Automation Environments."

1 Cyber Vision Center: Centralized analytics platform

2 Cyber Vision Network Sensor: Deep packet inspection (DPI) embedded in network infrastructure eliminating the need for a separate SPAN network

3 Cyber Vision Hardware Sensor: Dedicated sensor appliance that performs DPI on SPAN traffic

4 Application flow: Lightweight metadata streamed from Cyber Vision Sensors to the Cyber Vision Center

5 Industrial Asset Metadata Flow: Context, vulnerabilities and events communicated to the SOC

6 Industrial Security Appliance: Segments, controls access and detects and blocks intrusions and malware

7 Identity Services Engine (ISE): Provides capability for micro segmentation and TrustSec. Supports 802.1x

8 Stealthwatch: Detects network anaomolies

Asset visibility and zone/macro segmentation

You cannot protect what you cannot see. Cisco Cyber Vision provides this core capability. The macro-segmentation capability is provided by the Cisco ISA3000 Industrial Security Appliance. These Foundation security capabilities are also available in Full Spectrum security.

Device/micro segmentation

Cisco Identity Services Engine (ISE) enables micro-segmentation to the device level, and fine-grained access control can be created per user and device. Consistent security policies can be created across the entire network based on context. Cisco ISE becomes the policy engine for users and assets that require access to the industrial network.

Cisco ISE is depicted in the Full Spectrum security design, in which the Policy Administration Node (PAN) is in the SOC and the Policy Enforcement Node (PEN) is in the operations zone of the industrial network. ISE can also take in information from Cyber Vision through Cisco pxGrid to get specific device context.

An example of this operation is when Cyber Vision detects a new industrial device in the network. Cyber Vision will send detailed information about this device to ISE, so that the appropriate security policy can be applied based on the asset characteristics. Combining Cyber Vision and ISE is a great way to dynamically enforce zones and conduits. For instance, ISE can be configured to let an ICS controller communicate only with devices within its cell.

Cisco ISE can reduce risks and contain threats to a device by dynamically controlling network access. It enables wireless device onboarding and provisioning with 802.1X. In an industrial environment that needs to capture telemetry data from sensors and other devices, a fine-grained or micro-segmentation capability can help make operations secure.

Network anomaly detection

Cisco Stealthwatch improves threat defense with network visibility and security analytics. It helps gain situational awareness of all users, devices, and traffic on the network, so that threats can be responded to quickly and effectively. Stealthwatch leverages NetFlow data from network infrastructure devices. The data is collected and analyzed to provide a complete picture of network activity.

Malware protection and DNS security

Cisco Advanced Malware Protection (AMP) for Networks can be enabled on the NGFW to detect and protect against malware in content that is downloaded into the industrial zone. AMP can also be enabled on the ISA3000. Cisco Umbrella is deployed for DNS security to block requests to malicious domains.

Threat investigation and response

In the Full Spectrum security design, the SOC can detect a wider variety of threats and respond in a more coherent manner across enterprise and industrial networks. Cisco SecureX integrates intelligence from Firepower Management Center, Cyber Vision, ISE, Stealthwatch, AMP, and Umbrella. This seamless integration among Cisco security products makes deeper investigations very easy, and it also lets you take corrective action directly from its interface without having to log in to another product.

Solution introduction and operational considerations

Cyber Vision and Stealthwatch are built into the network and are easy to introduce. They offer visibility and network anomaly detection capabilities.

Introducing Cisco ISE, however, commands attention. Enabling micro-segmentation and Cisco TrustSec capabilities requires good planning and testing of the Scalable Group Tag (SGT) scheme to ensure that policies are supporting manufacturing needs and are providing the targeted security cover.

To get the most out of this design, security, operations, and IT must work together in a collaborative manner. The skill levels of the personnel need to be in step with these technologies, and operational processes need to be fine-tuned in order to get the best from the large number of products in this design.

Table 2. Full Spectrum security features

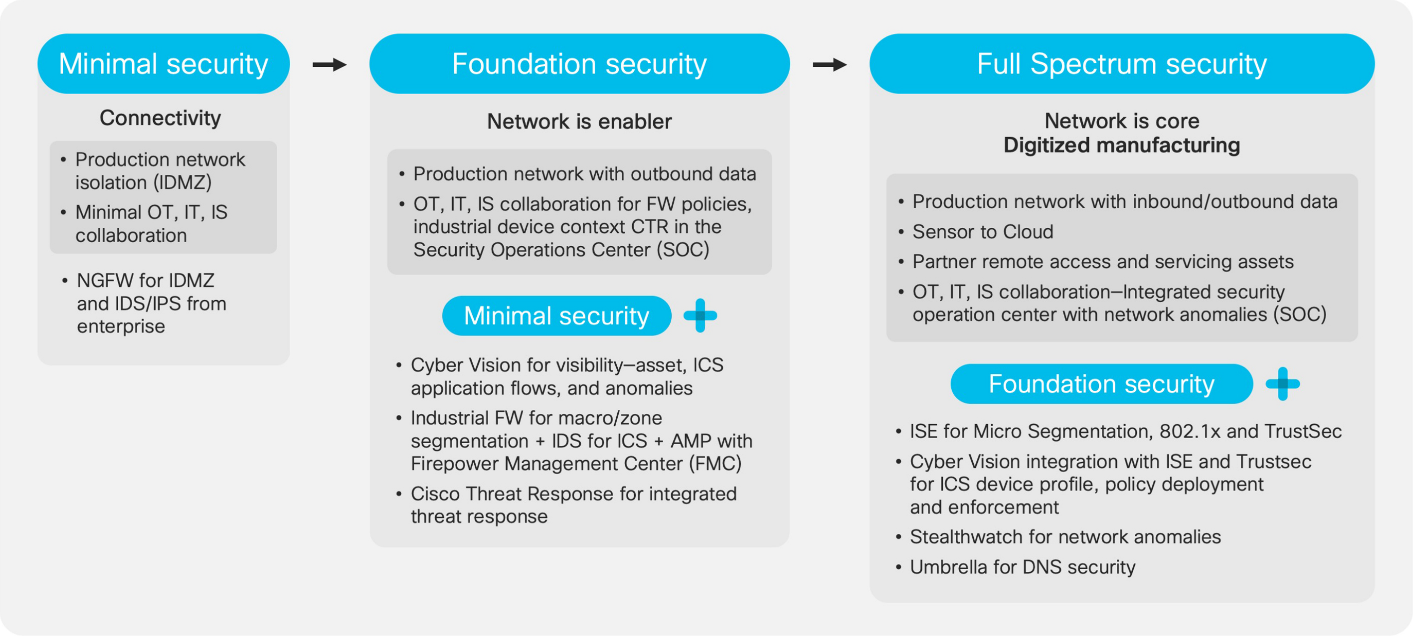
Discover	Asset visibility	Included	Enabled by Cyber Vision and network switches supporting Cisco Cyber Vision sensor – IE3400, IR1101, Catalyst 9300 Series, etc.
	Industrial asset inventory detail	Included	
	Application flows	Included	
	Tracking of ICS process data	Included	
	Baseline ICS application flow	Included	
Segment	Zone/macro segmentation	Included	Zones can be segmented by separate LANs and/or VLANs with access control by ISA3000.
	ICS protocol protection	Included	Provided by ISA3000.
	Isolation of industrial and enterprise networks	Included	NGFW provides IDMZ.
	Device/micro segmentation	Included	Fine-grained network segmentation to individual device level (Cisco TrustSec®)
Detect	Industrial asset vulnerabilities	Included	Cyber Vision will identify known vulnerabilities for industrial assets. It analyses application flows to detect process anomalies.
	ICS process anomalies, attacks	Included	
	ICS communication threats	Included	
	Operational events visibility	Included	
	ICS command filtering	Included	ISA3000 helps ensure plant safety by blocking dangerous asset parameters and unauthorized ICS commands.
	Intrusion detection/protection within industrial network	Included	Provided by ISA3000 for ICS exploits.
	Intrusion detection/protection from enterprise network	Included	Provided by Cisco NGFW.
	Network anomalies	Included	Provided by Cisco Stealthwatch®.
	Analysis of malware propagation	Included	
	Malware protection	Included	Provided by Cisco AMP, available via FTD license.
	DNS security	Included	Enabled with Cisco Umbrella®.
Respond	Investigate ICS anomalies	Included	Cyber Vision logging events and application flows.
	Mitigate asset vulnerability	Included	Cyber Vision Center patching guidance to help resolve vulnerabilities or mitigate vulnerability where possible by ISA3000.
	Log events for investigation	Included	Cyber Vision integrates with SIEM.
	Aggregate threat intelligence	Included	Provided by SecureX threat response.
	Track incidents	Included	Provided by SecureX threat response.
	Improve and optimize segmentation	Included	Provided by Cyber Vision and ISA3000.
	Improve and update baselines	Included	Provided by Cyber Vision.

Foundation to Full Spectrum security evolution

Manufacturing digitization is deepening and evolving. In order to support this evolution and keep your business protected, you need to enhance your security posture. Cisco's comprehensive portfolio of industrial network technologies and security tools lets you evolve from minimal security to Foundation security and to Full Spectrum security, while preserving your investments.

These designs build on each other and maximize reuse of technology, processes, and people. Figure 5 illustrates the applicability of these designs. Minimal security is recommended in all cases. Foundation security can be used by organizations that are digitizing their operations and need to implement a robust security posture. Full Spectrum security is intended to be deployed in organizations where the digitization is mature and the scale of operations has increased the threat surface. One example is when wireless devices become a part of the mainline production network and need 802.1X authentication.

Figure 5. Evolution of security approaches



Minimal security →

Connectivity

- Production network isolation (IDMZ)
- Minimal OT, IT, IS collaboration

- NGFW for IDMZ and IDS/IPS from enterprise

Foundation security →

Network is enabler

- Production network with outbound data
- OT, IT, IS collaboration for FW policies, industrial device context CTR in the Security Operations Center (SOC)

Minimal security +

- Cyber Vision for visibility–asset, ICS application flows, and anomalies
- Industrial FW for macro/zone segmentation + IDS for ICS + AMP with Firepower Management Center (FMC)
- Cisco Threat Response for integrated threat response

Full Spectrum security

Network is core
Digitized manufacturing

- Production network with inbound/outbound data
- Sensor to Cloud
- Partner remote access and servicing assets
- OT, IT, IS collaboration–Integrated security operation center with network anomalies (SOC)

Foundation security +

- ISE for Micro Segmentation, 802.1x and TrustSec
- Cyber Vision integration with ISE and Trustsec for ICS device profile, policy deployment and enforcement
- Stealthwatch for network anomalies
- Umbrella for DNS security

Remote access

Remote access has not been specifically addressed in this brief, as the recommendation is for remote workers and third-party contractors to follow the enterprise supported solution. Cisco provides a well-integrated solution with Cisco AnyConnect® and NGFW that can also include multifactor authentication with Cisco Duo. This solution is described in other designs.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.