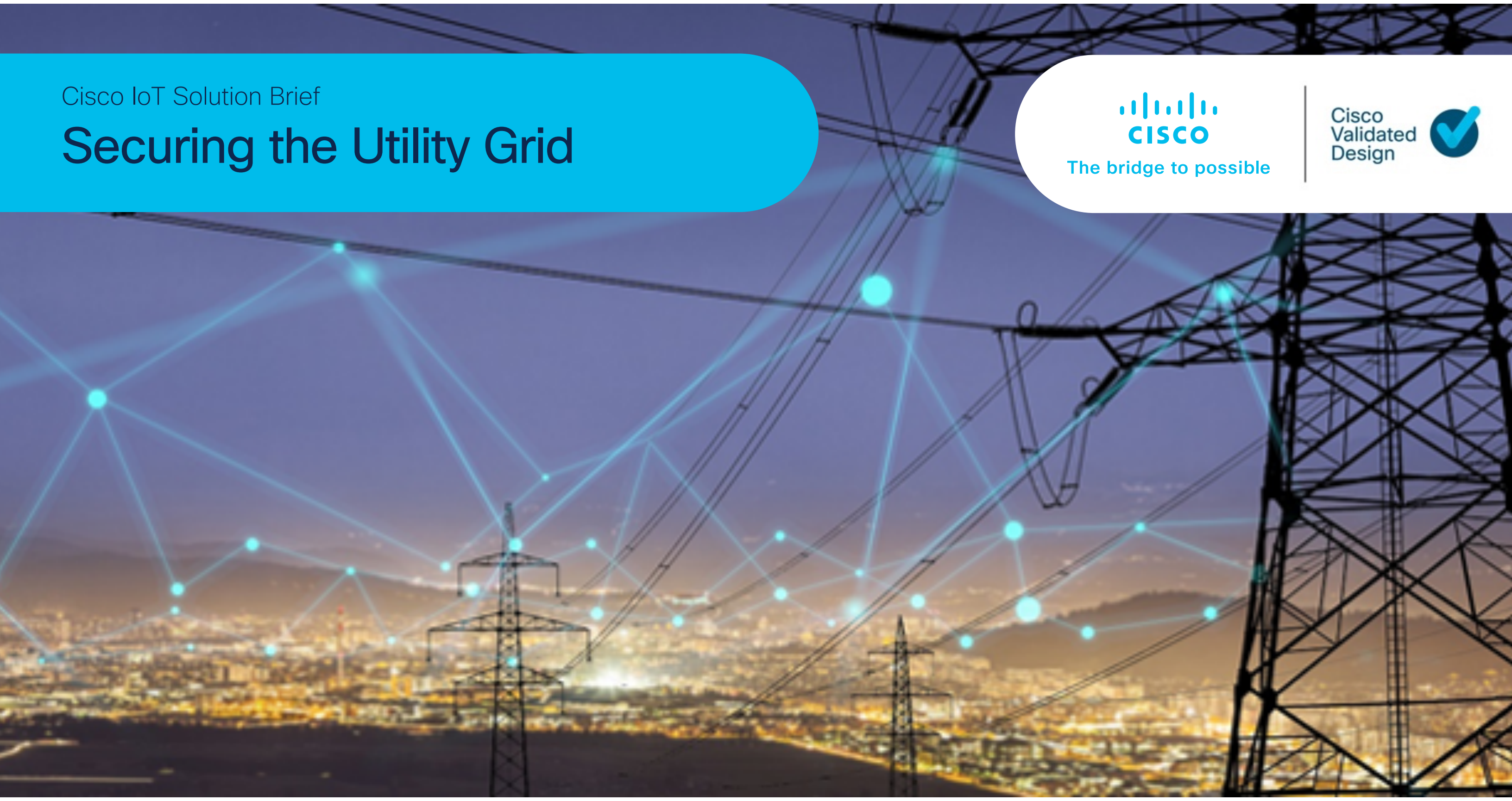
Cisco IoT Solution Brief

Securing the Utility Grid

The bridge to possible

Cisco Validated Design



Securing the Grid:

Introduction to Cisco Grid Security Solutions

Benefits

Improve industrial cybersecurity and compliance by:

- Asset inventory & discovery
- Secure access at the edge
- Security incident containment
- Threat detection & mitigation
- Malware protection
- Secure data transport

The cyber security of the utility grid and the associated operational monitoring and control networks have caused increasing concern and regulatory mandates on a global level. Organizations simply cannot modernize the utility grid without incorporating cybersecurity – it is a requirement for operating in the 21st century. Cybersecurity must be a key component of a grid modernization effort.

While utilities are transforming operations infrastructure toward grid modernization, cyber threats become a major concern. Significant changes in the operational model and adoption of newer more cost-effective technologies are being driven by flat to declining revenues and grid stability issues. The legacy, often proprietary, control systems are no longer efficient to operate and are virtually impossible to secure. The adage "You cannot secure what you cannot see" has never been more applicable. Asset visibility, controls to mitigate attacks, and the cooperation between Information Technology (IT) and Operations Technology (OT) are required.

A comprehensive security architecture with proven integration is a more operational and cost-effective answer. Integrating IT and OT around security and leveraging the experience of IT with implemented systems, are the right approaches. A well thought-out, implemented, and operationally-effective security posture requires a partnership between IT and OT and starts at the foundation – the network.

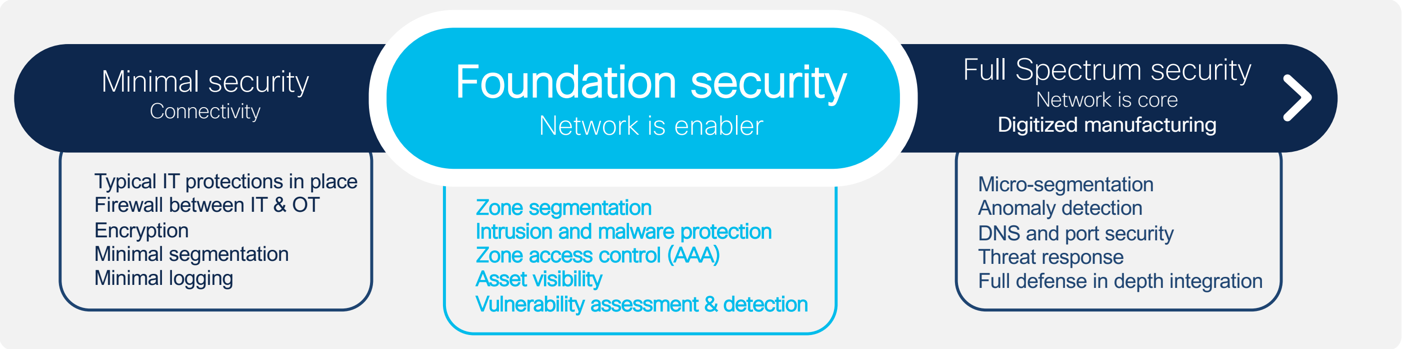
The Grid Security CVD provides a holistic cybersecurity architecture to protect utility networks and processes while addressing the key security and compliance concerns of the utility grid operators.

The journey to securing the utility network

Control networks connect devices that have been deployed over a period of many years – sometimes even decades – when cybersecurity wasn’t a concern. When utilities attempt to secure their operational network, they encounter three primary issues:

- A lack of visibility: Utility operators 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 visibility also means operators are often unaware of which devices are communicating, and where those communications are going. You cannot control what you cannot see.
- 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 does not disrupt production.

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



Minimal security
Connectivity

Typical IT protections in place
Firewall between IT & OT
Encryption
Minimal segmentation
Minimal logging

Foundation security
Network is enabler

Zone segmentation
Intrusion and malware protection
Zone access control (AAA)
Asset visibility
Vulnerability assessment & detection

Full Spectrum security
Network is core
Digitized manufacturing

Micro-segmentation
Anomaly detection
DNS and port security
Threat response
Full defense in depth integration

The move from Minimal phase to Foundational is about establishing, controlling and segmenting zones and traffic flows between those zones. Separation of IT and OT is one example and should be completed as defined in Minimal. The idea to take it to the next level is to segment and monitor traffic across the WAN and provide segmentation in the substations with logging. An IoT “aware” firewall is a perfect fit here.

Key requirements

The figure above depicts the key requirements as part of the journey to secure operational networks and can guide the development of a security lifecycle process. The ability to leverage the network with device identification, separation, and segmentation based on security levels and application criticality now enables an effective security posture. This posture can protect, detect, and respond to advanced cybersecurity threats as part of this comprehensive security lifecycle. Compliance standards such as NERC-CIP and others are addressed in this guide as part of that complete security lifecycle. This security solution brief and the Cisco Grid Security CVD provide the blueprints to meet these requirements.

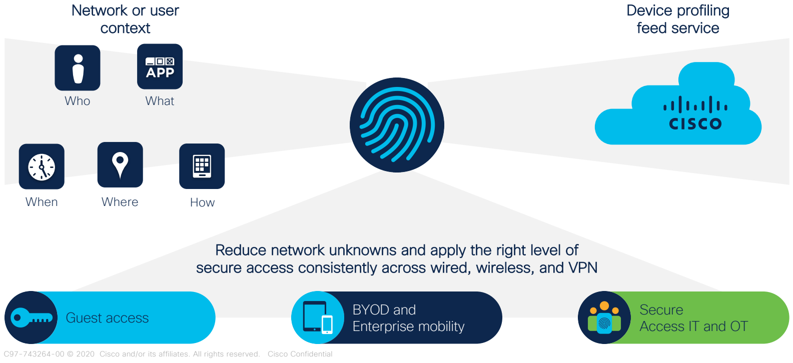
Foundational security

Identify: Unknown and unpatched assets

The utility grid has gone virtually unchanged for many years with assets operating in place for decades. Asset discovery often requires time consuming, costly, and even hazardous manual inspections that are error prone and may easily become obsolete. This is a security risk and a compliance issue. Cisco Cyber Vision can discover these devices automatically, providing significant levels of device detail and security posture assessments.

Protect: Lack of separation and segmentation

Separation and segmentation are the basis of security best practices, providing numerous points of inspection. Separating and controlling the flow of malicious traffic are best accomplished at the network level.


Network or user context
APP
Who
What
When
Where
How
Device profiling feed service
cisco
Reduce network unknowns and apply the right level of secure access consistently across wired, wireless, and VPN
Guest access
BYOD and Enterprise mobility
Secure Access IT and OT
C97-743264-00 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Many regulatory bodies such as NERC-CIP, IEC, NIST, ENISA and others are dictating the separation and segmentation of operational and monitoring, control traffic, physical security, and the wider IT traffic from each other throughout the network. The ruggedized industrial security appliance ISA 3000 with next generation firewall (NGFW), TrustSec, and encryption techniques are part of the Cisco Secure Architecture that leverages these tools to achieve the system-wide segmentation required.

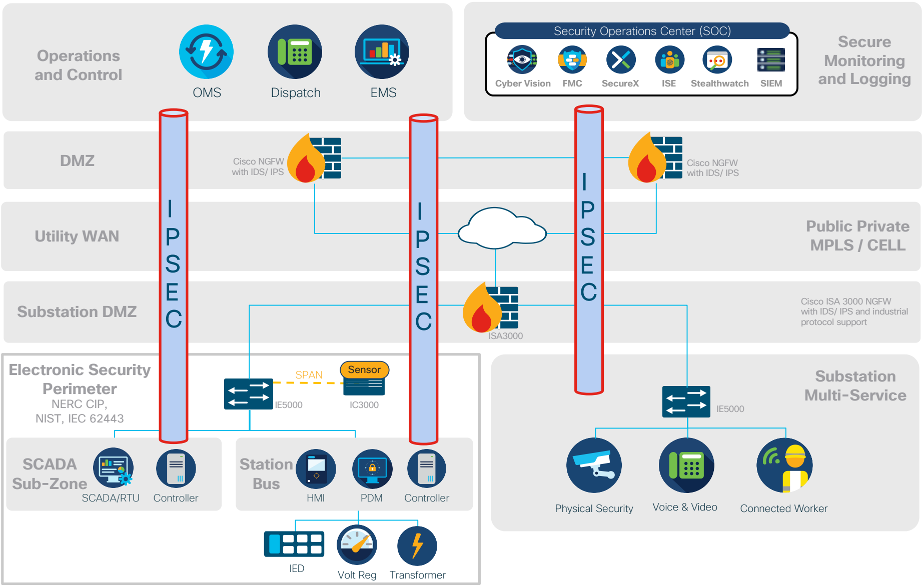
Protect: Secure remote access

Remote access security starts by establishing trust in the device and the device user identity before access to the network is granted. Secure access allows a utility to reduce costly manual intervention and the ability to leverage trusted third parties. The Cisco ISA 3000 firewalls establish a secure demilitarized zone (DMZ) and inspection points.

Remote workers use Cisco AnyConnect from their devices to connect into the trusted network. The Cisco Identity Service Engine (ISE) uses standards-based tools like 802.1x and MAC profiling with profiles on each edge port. All features are supported on the Cisco industrial Ethernet switching portfolio including the IE3400, IE4000, and IE5000 family.

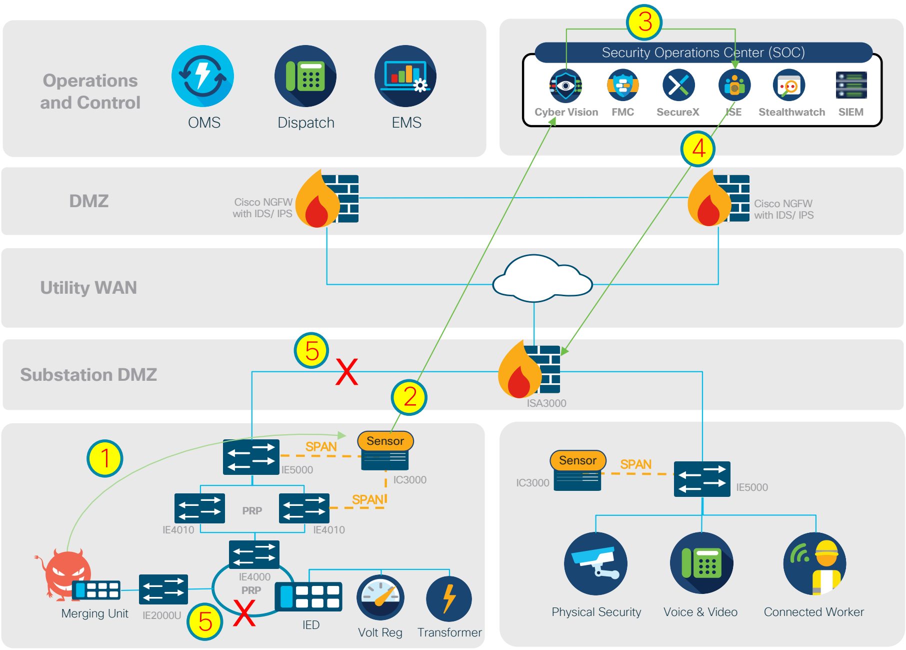
Protect: Data privacy and integrity

Grid operators depend on secure data transport for real-time data monitoring, remote operational modifications and results. Compliance mandates separation of critical data and the encryption of data exiting a physical perimeter. Logging information must also be securely delivered and maintained. Data privacy is a foundational tenant of our secure architecture. Data security leverages port security on Cisco industrial Ethernet switches, and uses a wide variety of encryption technologies on the ISA 3000 or any of the Cisco Industrial Routers IR1101, IR807, or CGR-2010.



Detect and respond

Utilities face several challenges when it comes to detecting and responding to cybersecurity attacks. The first is a lack of visibility. Operators can only stop malicious activities they can see. Another is a lack of reliable mitigation. Stopping cyberattacks requires a variety of cybersecurity technologies working together seamlessly, including a fully integrated security architecture that can discover threats and provide the information necessary for mitigation. The solution includes Cyber Vision, Stealthwatch, SecureX and the ISA 3000 industrial firewall.



Detection & Remediation:

1. Bad actor / Compromised device
2. Passive monitoring and detection
3. Alert to ISE / SIEM
4. Policy push to ISA3000 / IE switch
5. Bad actor blocked

Compliance requirements

A well-architected and comprehensive security solution can provide a secure, compliant, and operationally efficient OT network. A single system is easier to maintain, more reliable and trusted, with fewer integration costs and ongoing operational costs, thus reducing both capex and opex over the life of the system. The components and architecture described here are all part of a comprehensive NERC CIP compliant posture. Patching, asset information, data privacy, segmentation, detection and trust are all key parts of the current NERC CIP mandates.

A matrix mapping NERC-CIP mandates to Cisco solutions is located at the end of this document.

Full Spectrum Security

Micro-segmentation (TrustSec)

SecureX

Port security

Anomaly detection

DNS security

Full integration

Defense in depth

A solid security architecture leverages a defense-in-depth approach. This guide details the integration of multiple security tools and devices to accomplish this in an OT environment, which Cisco refers to as Internet of Things (IoT) Threat Defense. This holistic “full spectrum” security solution addresses the unique requirements of the utility network with best practices and compliance requirements like those found in NERC CIP and IEC 62443 and the NIST framework.

This solution is based on industry-leading innovations in Cisco IoT security and networking technologies that are built into Cisco Cyber Vision, Cisco 3000 Series Industrial Security Appliances (ISA), Cisco IC3000 Industrial Compute Gateway, and Cisco Industrial Ethernet IE3300, IE3400, IE4000, IE5000 Series Switches with integration with Cisco Identity Services Engine (ISE), Cisco Stealthwatch®, and Cisco TrustSec®.

These integrated systems improve operational capabilities and protection to systems; the integration and centralized management significantly reduce operational costs, time and exposure for the utility. This is the benefit of a one-source system versus integrating numerous point products from multiple vendors.

A validated security solution

Cisco’s team of validation engineers build out these solutions based on detailed use cases from real-world environments and scenarios. They test the full solution to the limit of its capabilities and document the results in a Cisco Validated Design (CVD). These documents can be found here: www.cisco.com/go/iotcvd

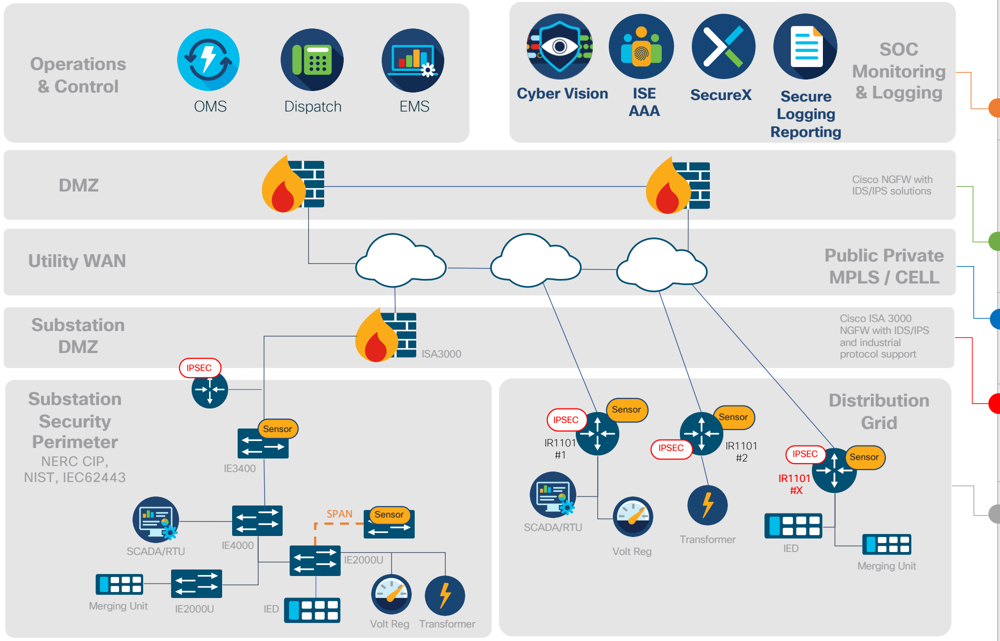
Cisco is a leader in securing enterprise networks. Cisco is also a leader in industrial networking. We are leveraging these unique portfolios of products and solutions, together with threat intelligence from Talos®, one of the world’s largest security research teams, to make security inherent and embedded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

Cisco is not only “IT approved” but is “IT preferred”, helping you streamline and accelerate security deployments in the industrial spaces.

GRID SECURITY
Cisco Validated Design
Tested Implemented Proven

Grid Security Architecture

A holistic security solution for utility industry



Cisco Security Feature	
Operational Control Monitoring Logging	• AAA identity services • Network management • Asset inventory • Anomaly detection • Grid Wide services • Traffic enforcement Ops Centre to industrial DMZ, north/south
IT / OT Segmentation and Industrial DMZ	• Access control lists (ACLs) • Intrusion detection systems (IDS) and intrusion prevention systems (IPS) • VPN services • Portal and remote desktop services • Application and data mirrors
Wide Area	• Traffic enforcement (Control to Subs North-South) • QoS prioritization • VPN / encryption • Netflow
Industrial Segmentation (ISA3000)	• Industrial deep packet inspection (DPI) • Stateful firewall and intrusion prevention (IPS) • Hardware bypass
Secure Edge Services and Segmentation	• Layer 2 NAT • 802.1X • MAC Authentication Bypass (MAB) • Quality of Service marking • Netflow (IE3x00 and IE4000 only) • TrustSec tagging (IE3x00 and IE4000 • Edge compute (IE3x00 only) • IPSEC encryption in hardware

Cyber Vision

Cisco Cyber Vision is an asset inventory, network monitoring and threat-detection platform specifically designed to secure industrial control systems (ICS). It enables industrial organizations to gain full visibility into their industrial networks so they can ensure process integrity, build secure infrastructures, drive regulatory compliance, and enforce security policies to control risks.

Port security

The Cisco IE3300, IE3400, IE4000, IE5000 Series switches deliver Gigabit connectivity to the Cisco ruggedized switching portfolio with superior high-bandwidth switching capacity and proven Cisco IOS Software. The Cisco IE Switching Series provides highly secure access to support resilient and scalable networks while adhering to industry compliance requirements.

ISA 3000 Industrial Security Appliance

The Cisco ISA 3000 Industrial Security Appliance is a next generation firewall specifically designed for harsh industrial environments. Fully certified for deployment in power grid networks and substations (IEC 61850-3 and IEEE 1613) it leverages threat intelligence from Cisco Talos to detect intrusions, is fully integrated with Cisco Firepower Management Center to enforce access control and security policies, and also offers industrial protocol decoders to control communication content and compliance.

Stealthwatch

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 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.

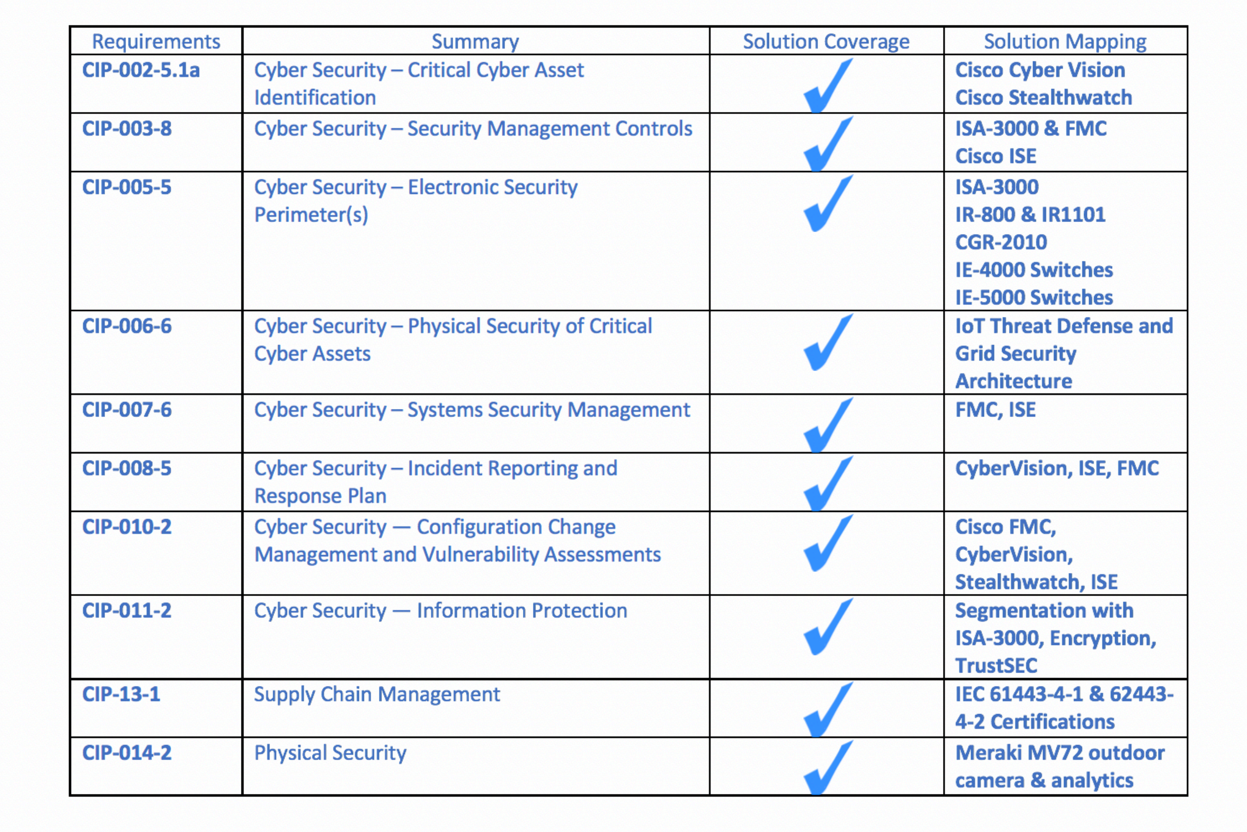
SecureX

Cisco SecureX integrates intelligence from Firepower Management Center, Cyber Vision, Identity Services Engine, Stealthwatch, Advanced Malware Protection and Umbrella. This seamless integration among Cisco security products makes deeper investigations really easy, and it also lets you take corrective action directly from its interface without having to log into another product.

Identity Services Engine

Cisco Identity Services Engine (ISE) enables micro-segmentation to the device level and fine-grain 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.

Mapping NERC-CIP compliance with Cisco security solutions



Requirements	Summary	Solution Coverage	Solution Mapping
CIP-002-5.1a	Cyber Security – Critical Cyber Asset Identification	✓	**Cisco Cyber Vision** **Cisco Stealthwatch**
CIP-003-8	Cyber Security – Security Management Controls	✓	**ISA-3000 & FMC** **Cisco ISE**
CIP-005-5	Cyber Security – Electronic Security Perimeter(s)	✓	**ISA-3000** **IR-800 & IR1101** **CGR-2010** **IE-4000 Switches** **IE-5000 Switches**
CIP-006-6	Cyber Security – Physical Security of Critical Cyber Assets	✓	**IoT Threat Defense and Grid Security Architecture**
CIP-007-6	Cyber Security – Systems Security Management	✓	**FMC, ISE**
CIP-008-5	Cyber Security – Incident Reporting and Response Plan	✓	**CyberVision, ISE, FMC**
CIP-010-2	Cyber Security — Configuration Change Management and Vulnerability Assessments	✓	**Cisco FMC, CyberVision, Stealthwatch, ISE**
CIP-011-2	Cyber Security — Information Protection	✓	**Segmentation with ISA-3000, Encryption, TrustSEC**
CIP-13-1	Supply Chain Management	✓	**IEC 61443-4-1 & 62443-4-2 Certifications**
CIP-014-2	Physical Security	✓	**Meraki MV72 outdoor camera & analytics**

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**.