# Cisco® Secure Ops Solution

Overview

Cisco® Secure Ops Solution supports cyber-security risk management and compliance for industrial automation environments. It is a combination of on-premise technology, processes, and managed services that helps companies implement and maintain perimeter security between enterprise and operational networks, as well as layered security controls. Through increased organization transparency, central leadership is able to better understand risks and compliance, as well as make informed investment decisions.

Cisco® Secure Ops delivers a standardized, integrated and comprehensive approach to security. It is supported and embraced by automation suppliers such as Yokogawa and Rockwell, and technology providers such as McAfee and Symantec, and provides a framework for a wide range of partners to participate.

High-Level Secure Ops Architecture
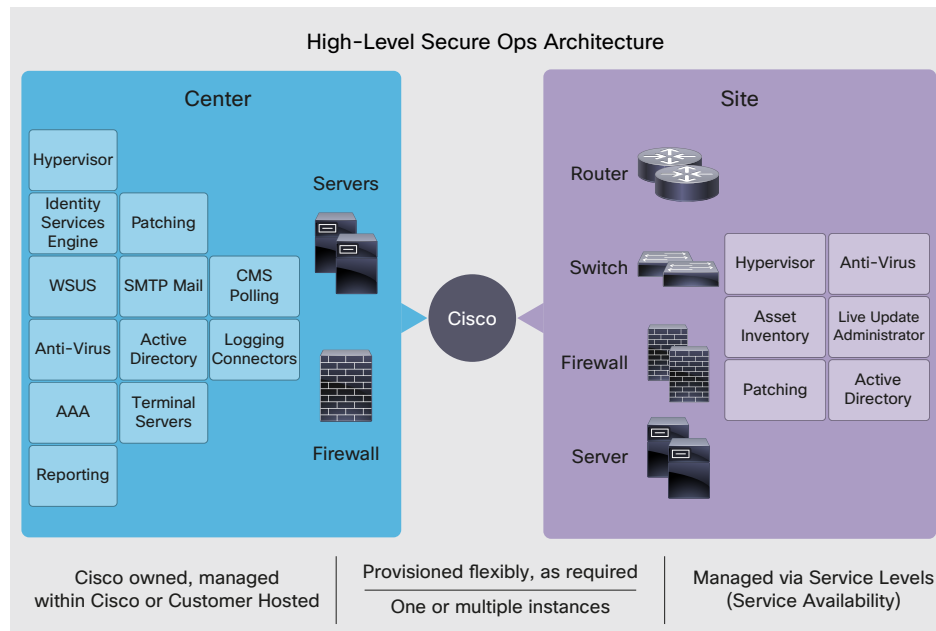
Core Capabilities

- Situational awareness dashboards (network status, access & inventory management, security compliance and assurance)
- High-availability infrastructure (for system-to-system and user-to-system connectivity)
- Secure process control access
- Asset discovery and inventory
- On-premise backup/restore capabilities
- Automated Windows and automation vendor qualified patches
- Automated signature update, approved by automation suppliers
- Automated, daily log collection and management
- Globally supported 24 hours a day, 365 days a year using a "follow the sun" support model
- Proactive performance and fault monitoring
- Global security incident response and monitoring services
- Security event correlation and incident notifications

Network availability and performance monitoring and reporting

Benefits

Cisco® Secure Ops provides a wide range of benefits across the organization:

- **Business leaders** with situational awareness for security maturity and compliance within various parts of the business.

- **Site leadership and management** with simplified management, lowered complexity and increased consistency across individual sites, leading to optimized operational costs.

- **Site technical leaders** with a technical solution to help manage security and compliance on a per-site basis as well as valuable tools to increase it through standardized interfaces and capabilities.

Cisco® Secure Ops Solution provides critical infrastructure security as-a-service, and customers who implement the solution have experienced:

- Less site down time, risk reduction
- Increased site productivity and lower operational costs
- Improved, and in some cases, automated compliance
- Future-proof architecture that evolves with you

Challenges and Solutions

Operators of industrial control networks have historically relied on a combination of "security by obscurity" and physical segmentation to protect their networks against cyber-attack. More recently, this viewpoint has begun to evolve as:
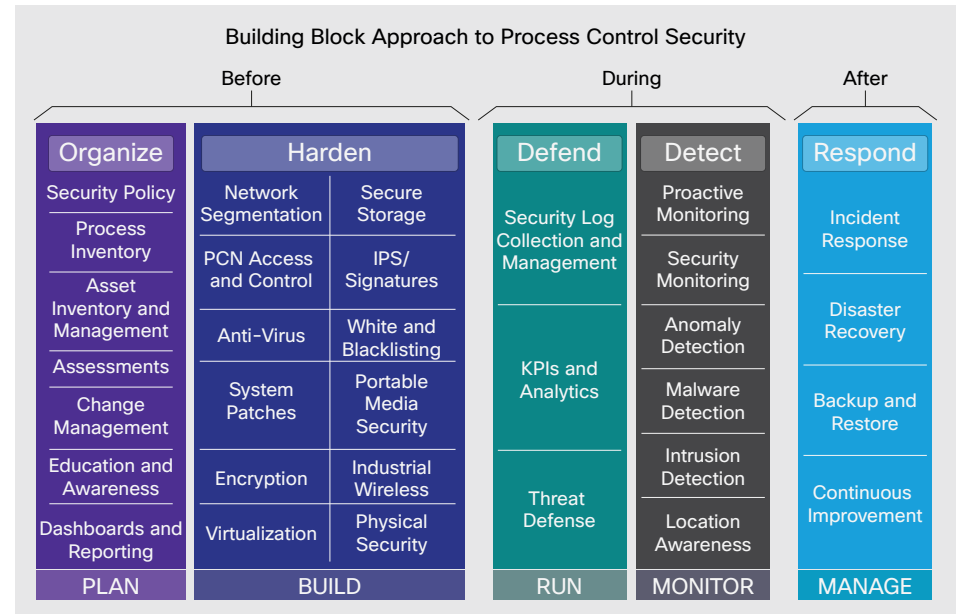
- Maintaining multiple networks is prohibitively expensive.
- Interconnecting industrial systems, networks, and data applications to enable better information flow and decision-making opportunities have become highly desirable.
- Proactive monitoring is needed to avoid risks impacting process control networks such as device failures.

It's clear that a more robust, flexible, and secure solution is required. The solution must connect networks and enable monitoring and data flow over a secure network; be flexible and capable of being deployed into brownfield environments; deliver defense-in-depth features to organize, harden, defend, and respond to threats.

Cisco has developed Secure Ops to provide an integrated and standardized solution for securing industrial control networks, protect against risks, improve efficiency, and reduce site downtime. Customers can choose to implement security controls using a building block approach that allows them to address various attack vectors as their business demands.

Why Cisco Services

Cisco Services makes networks, applications, and the people who use it work better together. Today, the network is a strategic platform in a world that demands better integration between people, information, and ideas. The network works better when services, together with products, create solutions aligned with business needs and opportunities.

Building Block Approach to Process Control Security

Before			During		After
Organize	**Harden**		**Defend**	**Detect**	**Respond**
Security Policy	Network Segmentation	Secure Storage	Security Log Collection and Management	Proactive Monitoring	Incident Response
Process Inventory	PCN Access and Control	IPS/ Signatures		Security Monitoring	Disaster Recovery
Asset Inventory and Management	Anti-Virus	White and Blacklisting	KPIs and Analytics	Anomaly Detection	Backup and Restore
Assessments	System Patches	Portable Media Security		Malware Detection	
Change Management	Encryption	Industrial Wireless		Intrusion Detection	Continuous Improvement
Education and Awareness			Threat Defense	Location Awareness	
Dashboards and Reporting	Virtualization	Physical Security			
PLAN	**BUILD**		**RUN**	**MONITOR**	**MANAGE**

The unique Cisco lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

Cisco and its partners can help to maximize your experience and return on investment from the planning to building and managing of your Cisco Secure Ops solution. Cisco Services provides expert consulting and integration services to help ensure your successful implementation. www.cisco.com/web/services/index.html

For More Information

For more information about the Cisco Secure Ops solution, please visit: www.cisco.com/web/strategy/energy/external_oil.html.