Cisco IPS Industrial Control Protection

Industrial Control Protection - What Every Customer Needs to Know

Through our IPS offerings, Cisco provides customers with unrivaled industrial control protection. Industrial control protection is a highly specialized branch of network security, and the ramifications of failure can be critical. Cisco® IPS technology provides a set of licensable signatures written by experienced industrial control experts to safely inspect and protect these critical network communications.

IPS Overview

Cisco IPS Sensors deliver high-performance intelligent detection with precision response, extending the IPS capabilities from the network edge to the data center for both IPv4 and IPv6 networks.

Intelligent Detection

Cisco IPS sensors accurately identify, classify, and stop malicious traffic before it affects your business.

- Cisco IPS technology is engineered to prevent malicious activity, through the entire attack lifecycle and at all layers of the application stack.
- Built on advanced Cisco security and network intelligence, modular inspection capabilities can detect and prevent threats to the entire network stack, from Address Resolution Protocol (ARP) to complex enterprise-level applications. Cisco IPS technology protects against advanced application evasions and can normalize even the most fragmented of network traffic.
- Cisco IPS technology provides adaptive vulnerability and anomaly detection. Cisco has focused its signatures on the potential abuse of vulnerabilities, so your ability to detect threats remains intact, even as exploits change. For emerging “zero-day” threats, a Cisco IPS sensor learns about your network, detects both protocol and behavioral anomalies, and mitigates attacks without a signature update.
- With Global Correlation, Cisco led the IPS industry in the use of reputation feeds. Global threat information is turned into actionable intelligence, such as reputation scores, and can also be used for black listing and driving dynamic threat responses.

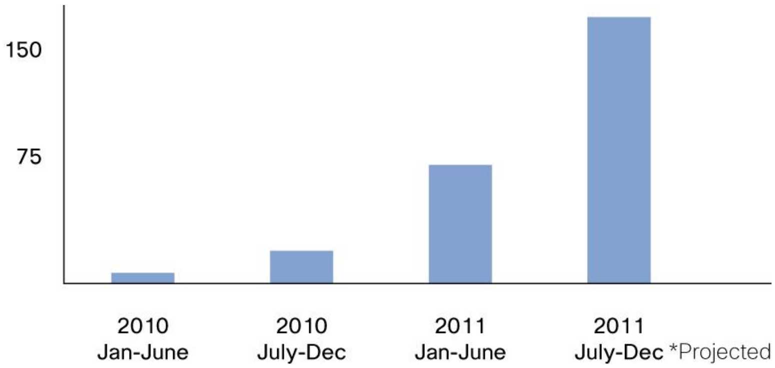
Industrial Control Protection

“Industrial control systems,” or ICSs, is the term used to identify several types of control systems, including supervisory control and data acquisition (SCADA) systems, process control systems (PCSs), and other smaller control system types, such as programmable logic controllers (PLCs), used in critical infrastructures and the industrial sector.

- **ICS threats and vulnerabilities are increasing rapidly.** The past 10 years have seen a significant increase in the number of threats, vulnerabilities, and industrial cyber-attacks targeting ICSs (Figures 1 and 2).
- **The availability of ICSs has increased.** With the introduction of consumer off-the-shelf (COTS) technologies and the interconnectivity between ICSs and IT infrastructures, ICSs have become highly available and vulnerable to threats.

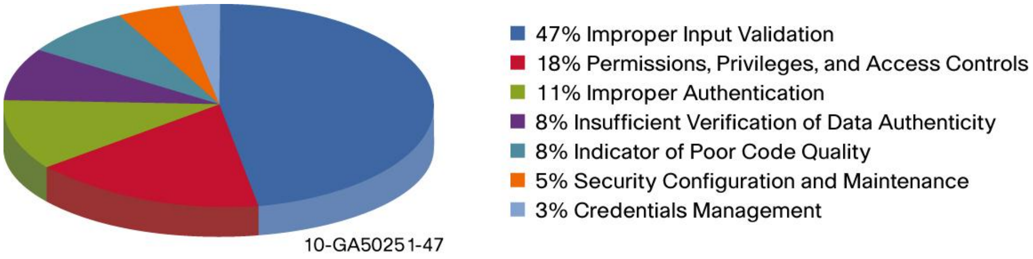
- **Patching is difficult and costly to implement.** Patching requires decreased productivity or plant downtime, or may cause unintended consequences resulting in plant failure. ICSs can remain unpatched in the field for a significant amount of time, leaving operators vulnerable.

Figure 1. Number of ICS-CERT Publically Disclosed Vulnerabilities



Statistics from US-CERT Control Systems Security Program (CSSP) Control Systems Advisories and Reports Archive, July 7, 2011.

Figure 2. Vulnerability Categories Identified in Process Control Systems



Statistics from US-CERT Report: Common Cybersecurity Vulnerabilities in Industrial Control Systems, May 2011.

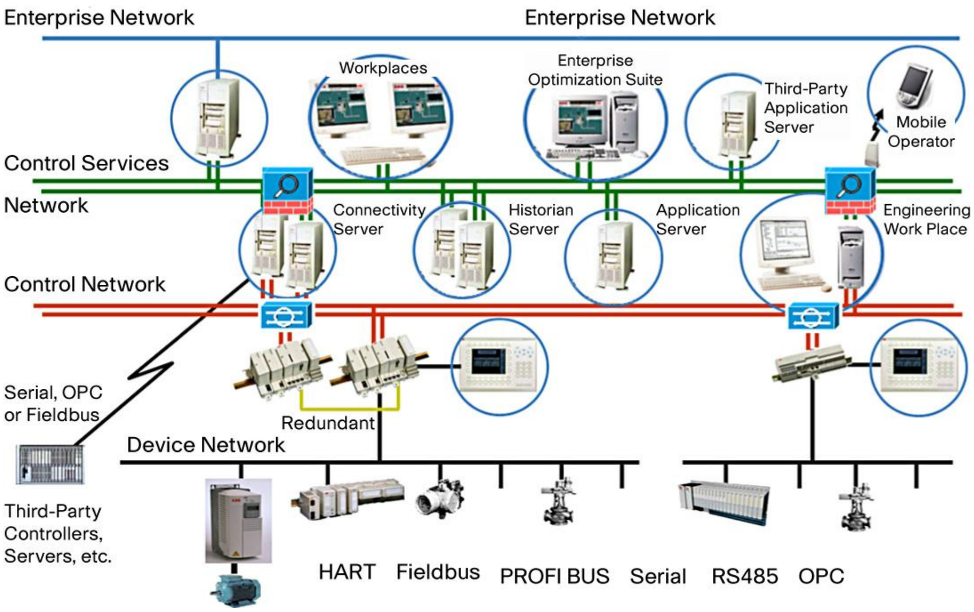
Focus Areas

Industrial equipment and control systems vary across industries, yet retain some commonality. Protocols common across the industrial space may harbor vulnerabilities that are ubiquitous, while some vendors' products may be highly proprietary or may implement standards in a unique fashion. The result is a need for both industry-specific and common platform protections.

Cisco's set of industrial control protection signatures includes a mix of general SCADA protocol detections and specific identifiers that address tools and environments common to most device controlled environments. These signatures will continue to evolve. Cisco will continue to stream new signatures that address general SCADA protocol protections as well as additional oil and gas protections. In addition, focused batch deliverables will target other industries, such as utilities, manufacturing, transport, and natural resource cultivation.

As shown in Figure 3, proper placement of the IPS within the enterprise or control network is critical to protecting industrial systems within the IT infrastructure.

Figure 3. Deployment Scenarios for Cisco IPS Industrial Control Protection



Licensing and Availability

The Cisco industrial control protection signature offering is licensed on a per-device basis and is delivered within the existing IPS signature feed. Customers can buy a platform-specific license and receive these updates if their IPS service is maintained. Please contact your Cisco representative for more information.

Signature Protection

The following are examples of protocols and threats currently covered by the Cisco industrial control protection offering:

Systems: SCADA, DCS, PLC, SIS, RTU

Threats and protections: Known vulnerabilities, policy enforcement, protocol normalization

Ordering Information

Table 1 lists ordering information for Cisco IPS SCADA signatures. To place an order, visit the Cisco Ordering Home Page.

Table 1. Ordering Information

Product ID	Target Platform
L-ASA5510-SCA=	ASA5510 with all AIP variants
L-ASA5520-SCA=	ASA5520 with all AIP variants
L-ASA5540-SCA=	ASA5540 with all AIP variants
L-ASA5585-10-SCA=	ASA 5585 – SSP 10
L-ASA5585-20-SCA=	ASA 5585 – SSP 20
L-ASA5585-40-SCA=	ASA 5585 – SSP 40
L-ASA5585-60-SCA=	ASA 5585 – SSP 60
L-ASA-AIP5-SCADA=	ASA5505-AIP5

Product ID	Target Platform
L-IPS-4240-SCADA=	IPS-4255
L-IPS-4255-SCADA=	IPS-4255
L-IPS-4260-SCADA=	IPS-4260
L-IPS-4270-SCADA=	IPS-4270
L-IPS-ISDM2-SCADA=	IPS-IDSM2
L-ASA5512-SCA	ASA 5512-X
L-ASA5515-SCA	ASA 5515-X
L-ASA5525-SCA	ASA 5525-X
L-ASA5545-SCA	ASA 5545-X
L-ASA5555-SCA	ASA 5555-X
L-IPS4345-SCA=	IPS 4345
L-IPS4360-SCA=	IPS 4360

Software Version Requirements

To operate correctly, Cisco industrial control protection signatures require that the software version of the target platforms listed in Table 1 support the E4 signature engine. Software revisions 7.0 and later have E4 support.

Cisco Services for IPS

Cisco Services for IPS is a comprehensive security service and an integral part of Cisco IPS solutions, enabling operators to receive time-critical signature file updates and alerts. As part of the Cisco Technical Support Services portfolio, Cisco Services for IPS allows your Cisco IPS solution to stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped.

In the context of industrial control protection, it is important to note that the only means of gaining access to Cisco industrial control protection signatures is to have an up-to-date contract for Cisco Services for IPS associated with the intended IPS platform.

For more information on Cisco Services for IPS, please visit http://www.cisco.com/en/US/products/ps6498/index.html.

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 **www.cisco.com/go/offices.**

Printed in USA C78-686161-02 10/12