Cisco Services for Intrusion Prevention System

Keep your Cisco® Intrusion Prevention System (IPS) devices fortified against ongoing security threats with a comprehensive service that includes around-the-clock technical support, hardware replacement, software and signature file updates, and dynamic global threat information.

Protect your network against threats and malicious or damaging attacks.

Cisco Services for IPS support improved business continuity by helping to:

- Protect sensitive information
- Maximize availability and reliability of the network
- Control expenses through increased stability of network operations
- Minimize the potential economic effect of business disruptions
- Mitigate risk through security intelligence

Service Overview

Security attacks can be isolated and local, organized and global. The method of attack might be familiar, such as denial of service; a more sophisticated blended threat using social engineering techniques; or even an invisible threat, such as infections of legitimate websites. The results of undetected, uncontained security breaches are well known, including expensive repair and restoration, lost revenue, compromise and loss of vital data, disruption of business, and damage to your company's reputation.

A proactive security strategy will enable your network to automatically protect and defend against new threats of any type, from any source. Cisco Services for IPS, together with your Cisco Intrusion Prevention System, play one of the most important roles in the coordinated response of the network by protecting your enterprise from new threats at the network perimeter and beyond.

Cisco Services for IPS provide around-the-clock global intelligence and protection updates for the latest security threats, system software updates, technical assistance from experts in networking and security, and advance hardware replacement options. With Cisco Services for IPS, you no longer have to wonder if your intrusion prevention system has the most up-to-date information to defend against attacks from local and global threats. Cisco Services for IPS not only help you reduce risk exposure, but also help support the productivity of internal staff who are charged with maintaining security systems.

Dynamic Protection Services Counter Organized Threats

Cisco Security Intelligence Operations (SIO) provide threat identification, analysis, and remediation to help provide the highest level of security for Cisco customers. The Threat Operation Center within SIO includes more than 500 security analysts dedicated to 24x7x365 threat research spanning five global locations. These engineers analyze traffic patterns from Cisco SensorBase, the world's largest real-time traffic monitoring network, generating rules for services such as Cisco global correlation in near real time and releasing timely signature updates. Following are just some of the ways in which Cisco Services for IPS provide the timely information and resources you need for proactive threat defense.

Signature Updates

Cisco's comprehensive view of the Internet threat landscape is used to create the new signature files that are vital to protecting your network against the latest threats and vulnerabilities. Our threat analysts and experts identify vulnerabilities and develop new and updated signature files for IPS devices. Cisco tests existing and new protections against a constantly growing library of validated exploits. Signature files are thoroughly tested, both internally and externally through our signature partners, to make sure that they are of the highest quality.

With Cisco Services for IPS, your IPS device has the ability to receive automated signature updates to monitor emerging threats and vulnerabilities and provide protection before they affect your infrastructure. Signature updates are generally released on a weekly basis. Depending on the urgency of the vulnerability, the severity of the potential damage, and the credibility of the source, Cisco might release new signatures within hours of discovery. Updates can be delivered proactively to your Cisco IPS device or managed by your security team.

Global Correlation and Reputation Updates

Cisco Services for IPS give you access to dynamic protection capabilities such as global correlation and reputation updates, available only from Cisco. With global correlation, your Cisco IPS receives global threat updates from the Cisco SIO throughout the day, usually as frequently as every five minutes, enabling your Cisco IPS to stop twice as much malicious activity as IPS devices that rely on local inspection and evaluation only.

Global correlation taps into the global threat information in the Cisco SensorBase Network, which receives constant threat notifications from hundreds of thousands of real-world Cisco IPS, firewall, web, and email security deployments around the globe, combined with hundreds of partner information feeds. Cisco's complex global correlation algorithms, along with hundreds of security analysts, turn all of this contextual data into the global correlation threat updates.

Reputation updates are used in conjunction with global correlation to monitor sender activity and give senders a reputation score that can block the worst attackers outright.

Table 1 shows the features and benefits of Cisco Services for IPS.

A Comprehensive Approach to Intrusion Prevention Services

The comprehensive Cisco Services for IPS include:

- Dynamic protection and access to threat management information:
  - Signature updates
  - Cisco global correlation and reputation updates*
  - Cisco IntelliShield Search Access
  - Cisco IPS Threat Defense Bulletin
- Operating system and IPS engine updates
- Around-the-clock technical assistance
- Cisco.com support tools and applications
- Advance hardware replacement with faster response time and on-site options

*Available on selected IPS products.

Table 1. Cisco Services for IPS Features and Benefits

Features	Deliverables	Benefits
· Signature Updates	· Access to new network signature files and file-based network layer protection algorithms to protect against network attacks · Cisco provides signature updates for many forms of attacks within hours of identifying the new threats or vulnerabilities · New signature updates are generally released at least weekly, and critical signatures might be released within hours of identifying a vulnerability	· Supports immediate containment of threats and helps prevent potential network outage or performance degradation · Cisco Services for IPS is available for: – Cisco IPS appliances – Blades for Cisco Catalyst® 6500 Series switches and integrated services routers – Adaptive security appliances – Integrated services routers with IPS integrated in the Cisco IOS Software
· Cisco Global Correlation and Reputation Updates*	· Real time updates on the global threat environment beyond the perimeter · Global correlation and reputation information is updated from the Cisco SensorBase Network as frequently as every five minutes	· Detects more threats earlier and more accurately to protect critical assets from malicious attack · Allows visibility to multipoint attacks including serial attackers, botnet harvesters, malware outbreaks, and "dark nets" · Global correlation and reputation updates block known attackers before they have the chance to investigate and attack critical assets
· Cisco IntelliShield Search Access	· Access to Cisco IntelliShield Alert Manager database for detailed research on the latest threats and vulnerabilities	· Supports your efforts to manage a secure network infrastructure
· Cisco IPS Threat Defense Bulletin	· Email bulletin with comprehensive information on breaking threats and vulnerabilities and Cisco IPS protections, as well as timely information on product updates and notices and access to a security research library	· Helps reduce risk with proactive notification and detailed information on emerging threats
· Operating System and IPS Engine Releases	· Provides new performance enhancements and new IPS functionality within the licensed feature set with access to the following types of intrusion prevention operating system software releases: – Maintenance updates, engineering patches, and service packs (such as 6.0 to 6.0.2) – Minor updates (such as 6.0 to 6.1) – Major updates (such as 6.0 to 7.0)	· Helps provide investment protection by making new IPS features and functionality available to enhance network threat prevention · Enhances the overall security of network and network-connected assets and the integrity of sensitive business, employee, and customer information
· Technical Assistance	· Gives your staff remote access to security engineers in the Cisco Technical Assistance Center (TAC)	· Helps to improve staff productivity and operational efficiency
· Cisco.com Support Tools and Applications	· Registered access to technical support tools and applications on Cisco.com	· Provides assistance 24 hours a day, seven days a week, anywhere in the world · Helps solve known problems quickly and provides tools to open and manage your relationship with Cisco

Features	Deliverables	Benefits
· Advance Hardware Replacement	· Offers the following advance replacement options: – Next business day – Same business day within four hours, 5 days a week – Same business day within 2 or 4 hours, 7 days a week · Options for on-site engineer to replace parts are also available for above response times	· Provides flexible options for advance hardware replacement · Helps maximize uptime to help ensure continuous network threat protection

* Cisco global correlation and reputation updates are available on Cisco IPS42xx appliances, ASA 55xx with IPS modules, IPS modules (IDSM-2) for Cisco Catalyst switches, and AIM-IPS and NME-IPS modules for integrated services routers. Cisco global correlation is not currently available for Cisco IOS Software based devices (IPS on Cisco IOS Software) or ASA-5505-AIPS.
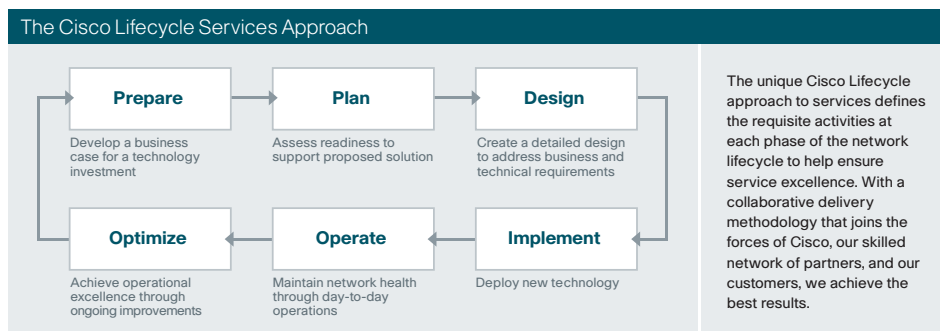
Availability

Cisco Services for IPS are available globally and can be ordered through your local Cisco account representative or Cisco Certified partner. You can find a Cisco certified partner in your area by searching in the partner locator at www.cisco.com/go/partnerlocator. For a complete list of the technical services available for your Cisco products and applications, visit our Service Finder tool at www.cisco-servicefinder.com.

Why Cisco Services

Cisco Services make networks, applications, and the people who use them work better together. Cisco provides a comprehensive set of security products and services to help prevent business disruption. Cisco Services for IPS help your network defend itself against many threats and allow you to respond quickly and effectively in the event of an attack. Whether using the IPS technology in routers and switches or relying on the overlay protection delivered by our security appliances, Cisco provides many threat defense devices that can rapidly identify and eradicate network threats.

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.

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.

The Cisco Lifecycle Services Approach

Prepare — Develop a business case for a technology investment

Plan — Assess readiness to support proposed solution

Design — Create a detailed design to address business and technical requirements

Implement — Deploy new technology

Operate — Maintain network health through day-to-day operations

Optimize — Achieve operational excellence through ongoing improvements

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.

For More Information

For more information about Cisco Services for IPS, visit www.cisco.com/go/services/ips or contact your local account representative.

For more information about Cisco Technical Services, visit www.cisco.com/go/ts.

Cisco Services.
Making Networks Work.
Better Together.

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.**

C78-554808-00 08/09