

Cisco IronPort Hybrid Email Security

A FLEXIBLE SERVICE OFFERING TO MEET
UNIQUE EMAIL SECURITY NEEDS



Cisco® IronPort Hybrid Email Security is a unique service offering that provides maximum flexibility by dividing control between the customer site and Cisco cloud infrastructure. Based on the same industry-leading technology that protects 50 percent of Fortune 1000 companies from inbound and outbound email threats, Cisco IronPort® Hybrid Email Security service reduces the on-site data footprint, while still allowing customers to maintain control of confidential information within their physical boundaries. Like Cisco IronPort Cloud Email Security, this hybrid service enables customers to retain access to – and visibility of – both the on-premises and hosted infrastructure. For customers who require that sensitive data remain physically on premises, the hybrid solution provides the ability to deliver advanced control with encryption, data loss prevention (DLP), and on-site LDAP integration. With comprehensive reporting and message tracking, maximum administrative flexibility is assured. This service is all-inclusive – with software, hardware and support bundled together for simplicity.

THE CISCO CLOUD SECURITY DIFFERENCE

The Cisco Cloud Security family of services leverages Cisco IronPort technology to deliver inbound and outbound protection for email and ScanSafe technology for web filtering. It is supported by a world class infrastructure of 33 global data centers, with 7 years of 100 percent uptime, over 100 dedicated engineers and industry-leading service level

agreements (SLAs). The cloud is fully integrated into the Cisco Secure Borderless Network architecture to address the new paradigm of dissolving borders. Cisco Cloud Security helps customers strengthen security, enable collaboration and address compliance requirements.

FEATURES

Today's email security threats consist of various viruses, spam, false positives, distributed denial of service (DDoS) attacks, spyware and phishing (fraud).

Cisco utilizes multiple methods to provide the utmost in comprehensive email security, incorporating preventive and reactive measures to maximize defense.

Proven Spam Protection

Cisco IronPort technology blocks all types of undesirable email messages using a multi-layered scanning architecture. This enables Cisco IronPort Hybrid Email Security to deliver the industry's highest spam catch rate, greater than 99 percent, with a less than one in one million false-positive rate.



FEATURES (CONTINUED)

Cisco IronPort Reputation Filters provide an outer layer of defense using data from the Cisco SenderBase® Network to perform a real-time email traffic threat assessment and identify suspicious email senders.

Cisco IronPort Anti-Spam utilizes the industry's most innovative approach to threat detection, based on the unique Cisco IronPort Context Adaptive Scanning Engine (CASE), to determine:

- "What" content the message contains
- "How" the message is constructed
- "Who" is sending the message
- "Where" the call to action of the message takes you

Powerful Virus Defense

By offering a high-performance virus scanning solution, Cisco provides a multi-layered approach to virus filtering.

Cisco IronPort Virus Outbreak Filters are a critical first layer of preventive defense against new outbreaks – detecting and stopping viruses, hours before traditional virus signatures are available.

McAfee and Sophos anti-virus technology is fully integrated to enable traditional virus detection methods and ensure maximum protection against even the most complex virus attacks.

Sophisticated Outbound Control Protects Sensitive Information

Outbound control is just as important as inbound security. By applying additional message safeguards and policies, outbound control helps protect and secure sensitive information.

Cisco IronPort Email DLP provides protection for sensitive data with a fully integrated, comprehensive, accurate and easy solution. This feature has more than 100 predefined policies, ranging from government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the US and the Data Protection Act in the UK to industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS). These policies leverage sophisticated content analysis techniques and are specifically tuned to virtually eliminate false positives and maximize catch rate. Additionally, administrators can easily build custom policies to identify company-specific intellectual property or sensitive data.

In a single user interface, administrators can configure anti-spam, anti-virus, content filtering, encryption, and email DLP actions on a per-user basis. Administrators can access real-time and scheduled reports to view violations by policy, severity, and senders.

Encryption Ensures Secure Communication

Business-class email provides security and enhances visibility and control. Cisco IronPort Email Encryption secures authenticated confidential data to comply with partner, customer or regulatory requirements. This enables simple, secure communication from the gateway to any recipient inbox – while TLS, PGP and S/MIME technology ensure security between partner email gateways. Encryption is available through the Cisco Registered Envelope Service or on the Cisco IronPort Encryption Appliance.

Guaranteed read-receipts allow the sender to know precisely when a message sent using Cisco IronPort Email Encryption was delivered and viewed by each recipient.

Message expiration and locking enables messages to be locked (preventing the recipient from viewing them) up until they are actually viewed, even after delivery to the recipient's inbox.

Comprehensive Administration and Easy Access for Co-Management

A comprehensive support portal provides customers the ability to create a customized homepage and quickly access their unique security interests, including:

- historical events/tickets
- geographical data
- security graphics
- trends
- network status
- performance

Consolidated and robust reporting options analyze traffic data from geographically diverse infrastructure deployments to provide fully integrated security reporting.

Message tracking gives customers real-time visibility into messages for tracking down message disposition. Instead of having to search through log files, the administrator can use the flexible tracking interface to locate messages. Tracking spans both cloud and on-premises deployments.

Service Level Agreements (SLAs)

Cisco IronPort Hybrid Email Security provides high-performance email security backed with an industry-leading guarantee. Customers will receive money back if any of the below mentioned SLAs are violated by Cisco:

- 99.999 percent uptime
- 99 percent spam catch rate
- No more than 1 in 1 million false-positive rate
- 100 percent known virus catch guarantee



BENEFITS

Maximum Data Protection With Cisco IronPort Hybrid Email Security, your data is fully protected and remains private from start up through physical separation, prohibiting data contamination. The Cisco data center has full redundancy on multiple levels, maintaining that your email infrastructure is highly available.

Simplified Pricing This pricing model includes all hardware, software, service and support. Pricing is determined by the number of users in the contract per year.

Capacity Assurance Cisco IronPort Hybrid Email Security provides a service with the capacity to protect users and maintain peak performance. When spam volumes increase, organizations typically have to purchase new hardware to maintain protection. Cisco alleviates worry from increasing spam volumes, and last minute budgeting for the cost of new hardware. Additional capacity is always included with the simple per-user, per-year pricing model.

Co-Managed Support Share management responsibility between the customer and Cisco. This single interface provides the following benefits:

- access to Cisco knowledge base
- direct assistance in resolving problems
- real-time health information
- always on access to tracking data
- reduction in resource and training expenses
- higher efficiency

Backed by Cisco Security Intelligence Operations (SIO)

Cisco SIO is a security ecosystem that identifies, analyzes, and defends against threats. It consists of three components:

- Cisco SensorBase: The world's largest threat monitoring network and vulnerability database
- Cisco Threat Operations Center: A global team of security analysts and automated systems that extract actionable intelligence
- Dynamic updates: Real-time updates automatically delivered to Cisco security devices, along with best practice recommendations

SUMMARY

Cisco IronPort Hybrid Email Security is a "best of both worlds" service, providing leading email security in a unique form factor. It enables superior flexibility and choice while keeping costs predictable, thereby simplifying budgetary planning. Customers appreciate the co-managed support model, with the highest level of protection from email security experts, and the peace of mind that confidential information is safe and secure on premises.

TRY BEFORE YOU BUY

The best way to understand the benefits of Cisco IronPort Hybrid Email Security is to participate in the "Try Before You Buy" evaluation program. For additional information, please visit: www.ironport.com/try.



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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)