

FAQ

Cisco IronPort Hosted and Hybrid Hosted Email Security Services

Cisco IronPort Hosted and Hybrid Hosted Email Security services provide industry-leading anti-spam efficacy, capacity assurance, a dedicated infrastructure and a superior support team. Cisco® understands the importance of maintaining control over business-critical data, and offers a range of service options designed to suit the email protection needs of growing businesses.

GENERAL INFORMATION

What is the difference between Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security?

Cisco IronPort Hosted Email Security is a service that provides Cisco IronPort technology through an infrastructure that is completely maintained in resilient and geographically-diverse Cisco data centers. This option provides email security based on an “in the cloud” or software as a service (SaaS) model. Customers retain access to – and visibility of – the hosted infrastructure for maximum administrative flexibility, provided by comprehensive reporting and message tracking.

Cisco IronPort Hybrid Hosted Email Security is a unique service offering that combines a hosted email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for customers. The hosted infrastructure is typically used for inbound email cleansing, while the on-premises appliances provide granular control – protecting sensitive information with data loss prevention (DLP) and encryption technologies.

Why would I choose Cisco IronPort Hosted Email Security?

A hosted email security solution is suitable when organizations seek any of the following:

- To reduce data center footprint – thus reducing the rack space, power and cooling demand, as well as administrative overhead
- To lower Total Cost of Ownership (TCO)
- To expedite time to deployment for current and future capacity requirements

What are the benefits of the Cisco IronPort Hosted Email Security service?

A key benefit of using Cisco IronPort Hosted Email Security is anti-spam efficacy. Powered by the Cisco SenderBase® Network, which has real-time visibility into the threat landscape, Cisco IronPort Hosted Email Security delivers the industry’s highest spam catch rate (greater than 99 percent) with a less than one in one million false-positive rate.

Unlike other hosted email security solutions, Cisco IronPort Hosted Email Security has no shared hardware. This provides organizations with the highest uptime, while maximizing protection of sensitive data.

The cloud-based, software as a service (SaaS) model minimizes the corporate data center’s energy and physical footprint – reducing power, cooling and operational expenses while supporting corporate environmental initiatives.

With co-managed access, customers retain maximum control of the hosted infrastructure. They are able to access real-time reports and modify configurations without service ticket response delays.

Additionally, capacity assurance guarantees scalable protection for future spam volume growth.



Why would I choose Cisco IronPort Hybrid Hosted Email Security?

A hybrid hosted email security solution is suitable for organizations that want to address some of the following business requirements:

- Leveraging the benefits of a hosted form factor
- Maintaining control of outbound data on-premises
- Simplifying management

What are the benefits of the Cisco IronPort Hybrid Hosted Email Security service?

Cisco IronPort Hybrid Hosted Email Security allows organizations to leverage the efficiencies of the cloud, while maintaining physical control of on-premises equipment to handle sensitive data.

With a common management interface, spanning both hosted and on-premises equipment, Cisco IronPort Hybrid Hosted Email Security delivers unified quarantining, reporting and message tracking capabilities.

Cisco IronPort Hybrid Hosted Email Security provides future capacity assurance for both hosted and on-premises infrastructure at no additional cost.

What is SenderBase and do I have access to it?

Cisco IronPort Email Security services harness the power of the Cisco SenderBase Network. This unique threat tracking database captures data from more than 100,000 organizations worldwide, providing a large and diverse sample of Internet traffic patterns.

SenderBase collects data on more than 30 percent of the world's email traffic and provides a real-time view into security threats from around the world. It measures more than 120 different parameters for any email server on the Internet. This massive database receives more than five billion queries per day, with data streaming in from every continent and network providers, large and small.

SenderBase can be accessed at: www.senderbase.org.

DEPLOYMENT

What does “in the cloud” mean?

“In the cloud” refers to technology that is delivered without the need for deployment of hardware and software at a customer site. Cloud-based services are delivered through hardware and software maintained by the vendor in non-customer data centers.

Do I have access to my appliances “in the cloud?”

Yes. Both Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security provide customers with full access to their hosted email security appliances.

With Cisco IronPort Hosted Email Security, does Cisco manage my entire email infrastructure?

The Cisco IronPort Hosted Email Security service provides a unique co-managed approach. Customers have the ability to get help from Cisco for common tasks through a ticket or call-based system. However, Cisco also provides customers with full access to the infrastructure. This gives customers the highest level of control to manage their environment.



If the appliances are deployed on premises (i.e., in my data center), does that mean I have to manage everything?

Yes. For a Cisco IronPort Hybrid Hosted Email Security deployment, the on-premises equipment is completely managed by the customer. Fortunately, Cisco is always available to provide worldwide support, 24x7x365.

With Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security, does Cisco manage my email inboxes as well?

No. These services provide hosted email security, not hosted mailboxes.

Can I change between Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security?

Yes. Cisco understands that business requirements may evolve and works to help protect customer investments of both time and money. As such, customers may choose to upgrade from Cisco IronPort Hosted Email Security to Cisco IronPort Hybrid Hosted Email Security.

If my organization currently has IronPort® appliances, but would like to move to a hosted or hybrid environment, how should I proceed?

Cisco values and appreciates customers that have selected IronPort technology. To help make existing customer transitions as simple as possible, from both a technical and business aspect, Cisco has instituted upgrade packages. Please contact your local Cisco sales representative for details.

Who configures the appliance features for Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security?

With every sale, hosted or hybrid, Cisco email security experts work with the customer's technical team to ensure that the basic features of the service are configured and enabled. For advanced configuration options, Cisco Advanced Services can be enabled to provide a more customized configuration.

Do my end-users have access to quarantined messages? Do they have access to any other aspect of message tracking?

Both Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security reduce overhead for the customer's email administrator by providing end-users with a hands-on, self-service method to handle quarantined messages. End-users can reach this easy-to-use interface through a personalized URL, and take actions like releasing or deleting the message as well as whitelisting/blacklisting senders without the need for administrator intervention.

Beyond message quarantine information, end-users do not have access to any additional tracking data.

If I have a hosted email security solution, what is the likelihood that I am sharing hardware with a competitor?

Traditional hosted email security vendors base their solutions on a shared infrastructure. While this helps reduce costs, the risk of the "shared fate" phenomenon is that if one customer's mail environment has a problem, it can ripple through other customers sharing that same infrastructure. As a result, many major hosted email security vendors with solutions based on shared infrastructure have recently experienced significant downtime.



PRICE/COSTS

What is the price difference between Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security? Why is one more expensive?

In addition to the hosted infrastructure, Cisco IronPort Hybrid Hosted Email Security provides additional value through on-premises deployment. This involves additional setup costs and is consequently priced higher than Cisco IronPort Hosted Email Security. The exact price difference is dependent upon the deployment specifications selected by the customer.

If we hire five to ten people a year, will my service charge increase drastically? Will I need to purchase more equipment?

No. Cisco IronPort Email Security services are designed to accommodate for changing business needs. There is no increase in cost or equipment for minor deviations in user count. However, if your company experiences significantly increased head-count, it is recommended that you check with a local Cisco sales representative to determine next steps.

Can I get a free trial to test Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security?

Yes. The best way to understand the benefits of Cisco IronPort Email Security services is to participate in the “Try Before You Buy” evaluation program. Interested organizations can receive a 30-day trial of these services at no-cost or no-obligation.

CUSTOMER SUPPORT

What if my service needs maintenance or an appliance is down?

Cisco proactively monitors customers' hosted infrastructures at all times to ensure the highest levels of service. However, if you feel that you have a maintenance or support-related need, Cisco is ready to support you. Support can be reached 24x7x365 by either opening a support ticket or through a call-in number.

Do I have to use the portal? Can't I just call someone to fix the problem?

Cisco prides itself on providing industry-leading support to customers around the clock and across the globe. Customers are welcome to either call in or open a ticket through the support portal.



What is the average time to repair a problem?

Cisco maintains the highest levels of service responsiveness. Cisco’s Service Level Objectives (SLOs) include:

SLO Name	SLO Detail	SLO Targets
Mean Time To Notify (MTTN)	Notify customer of all service-impacting ¹ incidents within X minutes	15 Minutes
Mean Time To Investigate (MTTInv)	Investigate incidents within X minutes	30 Minutes
Mean Time To Isolate (MTTIsol)	Isolate root cause of all incidents within X minutes	90 Minutes
Mean Time To Resolve (MTTR)	Resolve all incidents within X hours	<ul style="list-style-type: none"> • Priority 1 (P1) within 4 Hours • Priority 2 (P2) within 24 Hours • Priority 3 (P3) within 72 Hours
Mean Time To Complete (MTTC) ²	Complete customer-initiated service requests within X hours	<ul style="list-style-type: none"> • Logical Priority 2 (P2) within 24 Hours • Logical Priority 3 (P3) within 72 Hours

¹ All Service Level Objective (SLO) goals are established to provide operational benchmarks for the Cisco IronPort Email Security services on a “best effort” basis.

- Priority 1 incidents on an entitled managed component where the managed component is unavailable and severely disrupting/impacting the customer’s business. Cisco and the customer will commit any necessary resources 24x7 until the incident is resolved/remediated.
- Priority 2 incidents on an entitled managed component where the managed component is unavailable or its functionality is severely degraded and customer’s business is moderately disrupted. Cisco and the customer will commit full-time resources during normal business hours Monday through Friday to resolve/remediate the incident.
- Priority 3 incidents on an entitled managed component where the managed component is unavailable or its functionality is moderately degraded and customer’s business is minimally disrupted. Cisco and the customer are willing to commit resources as available during normal business hours to resolve/remediate the incident and restore service to satisfactory levels.

² All customer-requested RFCs associated with Cisco IronPort Email Security services are, by default, classified as either Priority 2 with a MTTC target of 24 hours or Priority 3 with a MTTC target of 72 hours. Any customer-requested RFCs that are considered by the customer as “emergency” or “urgent” will be treated on a best effort basis by the Cisco SOC and will depend on Cisco SOC engineer availability at the time of submittal. The MTTC SLO target would be to complete the emergency RFC within four (4) hours, like a Priority 1 classified incident.

SUMMARY

Cisco is an industry leader in email threat protection. Cisco IronPort Hosted Email Security and Cisco IronPort Hybrid Hosted Email Security are state-of-the-art service offerings. Regardless of the deployment model, customers get the benefits of hardware capacity assurance, predictable budgetary planning and simplified management. Backed by industry-leading support and corporate stability, these services help organizations worldwide protect and manage their email infrastructures.

TRY BEFORE YOU BUY

Through a global salesforce and reseller network, Cisco offers a free “Try Before You Buy” program for Cisco IronPort Email Security services. For additional information, please contact your local Cisco sales representative or 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, CCIP, 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) P/N 435-0249-1 3/09