

Cisco Cloud Security: Choosing the Right Email Security Deployment

TABLE OF CONTENTS

- 1 Executive Summary
- 2 Cloud Email Security
- 4 Hybrid Email Security
- 6 Managed Email Security
- 8 Conclusion

Executive Summary

Enterprises of all sizes face the same daunting challenges – increasing mail volumes and new, evolving threats. The Cisco Cloud Security family of services provides customers superior choice of deployment models built on the solid foundation of industry-leading email security technology that protects 40 percent of Fortune 1000 companies from inbound threats and outbound data loss possibilities.

Today's email-borne threats consist of viruses, spam, false positives, distributed denial-of-service (DDoS) attacks, spyware, phishing (fraud), regulatory compliance violations, data loss and more. Cisco® Cloud Security addresses the issues faced by corporations, both large and small, by incorporating preventive and reactive security measures that are easy to deploy and manage.

While email threats continue to grow and evolve, organizations are demanding more from their IT teams – more protection, more efficiency and more flexibility. To meet these demands, IT teams need more flexibility to architect solutions that address these business imperatives. Flexibility provides choice in deployment options for email security and falls under three broad categories. First, there are customers that want to improve operational efficiency by outsourcing the problem of spam through the use of cloud or software as a service (SaaS) solutions. The second includes customers that want to maintain maximum control of sensitive outbound information through the deployment of on-premises email security infrastructure. The third category encompasses customers that want to use a hybrid (or divided) approach – which includes use of cloud solutions for efficiency while still maintaining the benefits of an on-premises appliance-based deployment.

Having choice, based on an organization's existing and future business needs, is important when selecting a solution and vendor. For email protection, Cisco Cloud Security services provide customers the choice of the available form factors, all built upon the same industry-leading Cisco IronPort® email security technology and backed by the Cisco SenderBase® Network. These form factors suit the needs of any email administrator:

- Cisco IronPort Cloud Email Security
- Cisco IronPort Hybrid Email Security
- Cisco IronPort Managed Email Security

This document discusses the various email security service options offered by Cisco Cloud Security and provides insights into choosing the solution that best fits your organization's business needs.

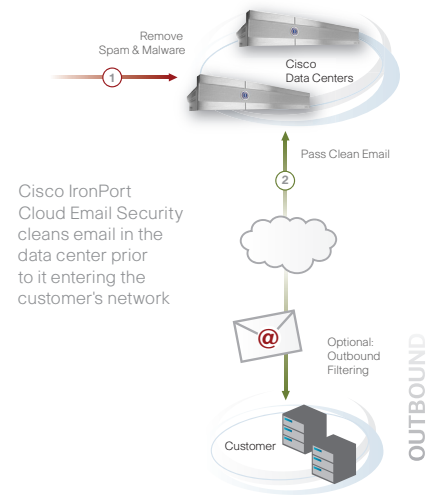
Cloud Email Security

Cisco IronPort Cloud Email Security provides industry-leading email security technology via an email infrastructure deployed in multiple, geographically-diverse Cisco managed data centers.

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

- To reduce data center footprint – thus reducing 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

These business elements are essential when it comes to choosing a cloud solution. However, traditional cloud email security solutions have a number of drawbacks that can seriously limit the effectiveness of the solution. The section below outlines each of these limitations and indicates how Cisco IronPort Cloud Email Security addresses these problems.



Cisco IronPort Cloud Email Security cleans email in the data center prior to it entering the customer's network

Anti-Spam Efficacy

Spam volumes have continued to double year over year. As a result, organizations are recognizing the need for an anti-spam vendor that is effective at catching spam. Every percentage point of missed spam means double the number of actual messages in users' inboxes annually. In addition to having a good spam catch rate, it is equally important to have a low false-positive (legitimate email messages classified as spam) rate. Traditional email security vendors have hovered around the 95 percent catch rate with a very high false-positive rate. The result is that end-users either spend time dealing with spam messages in their inbox or (even worse) keep calling the administrator, with the frustration that their legitimate business email has been classified by the email security vendor as spam and likely quarantined.

Cisco is the industry leader in anti-spam technology. The company consistently delivers a more than 99 percent catch rate and balances this near-perfect statistic with an industry-best rate of less than one false positive per million messages. This is one of the principal differentiators for Cisco solutions and a key reason why customers continue to choose Cisco over the competition.

Maximum Data Protection

Cisco cloud-based email security is unique in that it completely isolates each customer's infrastructure. This not only provides the highest levels of data protection but also alleviates the problems that the typical cloud based email security vendors have experienced, such as downtime and data contamination.

The service provides the highest levels of risk protection from data contamination in a cloud form factor due to the physical separation of customer emails and data.

Outbound Control

Data loss prevention (DLP) is a serious issue for companies, as the number of incidents (and the cost to those experiencing them) continues to increase. Whether it's a malicious attempt, or an inadvertent mistake, data loss can diminish a company's brand, reduce shareholder value, and damage the company's goodwill and reputation. In addition, organizations need to comply with numerous regulations that put strict requirements on how sensitive data needs to be handled.

To help organizations successfully solve their business problems, Cisco offers a fully integrated email DLP solution that provides over 100 pre-defined templates, including HIPAA, SOX, GLBA, and state privacy laws. In addition, integrated encryption provides another level of remediation. Cisco IronPort Email DLP and Cisco IronPort Email Encryption enable a quick and accurate means to protecting sensitive data and achieving compliance in the cloud or hybrid form factor.

Advanced Controls

While even the smallest of organizations are faced with email-borne threats (such as viruses, spam, false positives, DDoS attacks, spyware, phishing, regulatory compliance violations, data loss and more) on a daily basis, traditional cloud email security vendors provide very rudimentary email security controls. The result is that customers have to make do with whatever is provided by the vendor.

Cisco IronPort Cloud Email Security provides the customer a set of advanced, enterprise-grade controls that can be leveraged to strengthen their email security. These include capabilities like bounce verification, SPF, DKIM, TLS, compliance dictionaries, smart identifiers and a slew of advanced content filter rules. All of these advanced controls are available at no extra charge.

Message Tracking

While the performance and accuracy of the security elements are paramount, an equally important aspect is the ability to track messages. Email administrators want to have the flexibility to immediately determine the disposition of a message that passed through the cloud email security solution. With traditional cloud email security vendors, customers have to open a ticket with customer support and then wait (sometimes hours at a length) to get an answer. This can be very frustrating for an administrator – especially in the case where a CEO has called asking about a business-critical email message that was supposed to have been delivered hours ago.

Cisco IronPort Cloud Email Security provides customers with an easy-to-use message tracking interface that allows them to search for messages in real time. As a result, the administrator can respond to critical calls and provide answers within minutes, rather than waiting hours for their vendor to respond to the open ticket.

Reporting

In addition to message tracking, email security reporting is critically important to email administrators. Cisco IronPort Cloud Email Security provides very sophisticated management, monitoring and reporting tools. The service includes a unique reporting system — providing both a real-time and historical look at mail flowing through an organization's email infrastructure. These tools provide administrators with the necessary information to make critical security decisions in real time, export professional, visually rich reports in PDF for management consumption as well as the ability to schedule reports for automatic delivery to particular email addresses.

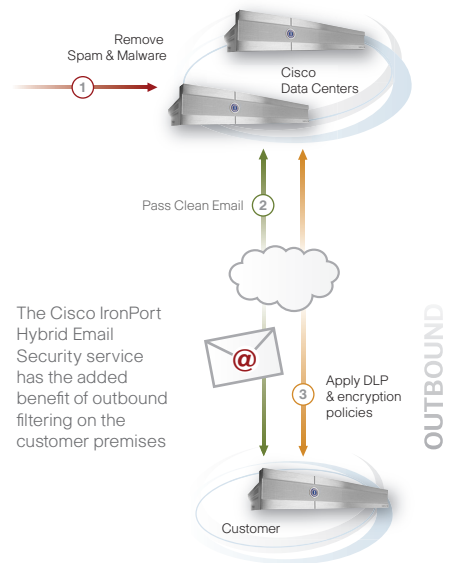
Hybrid Email Security

Cisco IronPort Hybrid Email Security is a unique email security service that provides customers with the choice to deploy email security in the way that best meets their business needs. The architecture includes email security infrastructure divided between cloud-based and on-premises form factors. Organizations typically deploy inbound security controls (anti-spam, anti-virus, etc.) through a cloud infrastructure while protecting sensitive information – through encryption and data loss prevention (DLP) solutions – via on-premises appliances.

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

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

Customers desire a best in class email security solution that helps with business planning predictability. The section below specifies each of these business requirements and describes how Cisco IronPort Hybrid Email Security addresses these problems.



Outbound Control

Similar to the cloud offering, the same features and functionality are available on premises, with the hybrid form factor. If customers prefer to leverage an on-premises solution for advanced content filtering, Cisco IronPort Hybrid Email Security is a unique service that allows customers achieve this goal by dividing the control between the cloud and the on-premises appliance. Customers have the choice to select the method that best works for their environment.

Simplified Management

While a hybrid deployment option makes great business sense, customers still have to deal with tracking and reporting of data spanning both form factors (given that email now flows through two sets of deployments). When a CEO calls the email administrator asking, "What happened to that email I was expecting two hours ago?", the administrator should not have to log in to two separate interfaces to search for messages, or open tickets with a vendor to figure out the disposition of the CEOs message. The interface to search messages across both deployments should be available to provide answers in an expedient manner. Similarly, instead of having to go to multiple interfaces to view reports and download statistics on email flow, a common interface should be available to greatly improve administrator efficiency.

Cisco IronPort Hybrid Email Security provides customers the power of real-time message tracking and reporting in an easy-to-use interface that spans both the cloud and on-premises deployments. Administrators can use the message tracking interface to immediately pinpoint the status of messages of interest. In addition, they can view a large number of pre-canned reports, download them in PDF format, export them to CSV format and even schedule them for email delivery based on time preferences. The tracking and reporting features greatly simplify both administration and management, resulting in significant efficiency gains.

Business Planning Predictability

When choosing a solution, organizations should evaluate not only the technical aspects, but also the business aspects. Today's IT executives have CFO mandates to reduce costs and make them more predictable. These costs include initial and ongoing hardware and software expenditures. Additionally, companies have limited flexibility when it comes to Capital Expenditure (CapEx) budget dollars. Traditional cloud solutions provide customers with benefits including a predictable, per-user per-year pricing model, future capacity assurance required to meet spam volume growth as well as an Operating Expenditure (OpEx) model that provides more flexibility over the CapEx model.

Cisco IronPort Hybrid Email Security provides the same benefits that are offered by traditional cloud vendors, but on both deployment form factors – cloud and on-premises. Customers receive the following additional advantages on the entire infrastructure, available for a simple per-user, per-year price:

- Initial hardware infrastructure
- Ongoing capacity
- Software license
- OpEx vs. CapEx billing

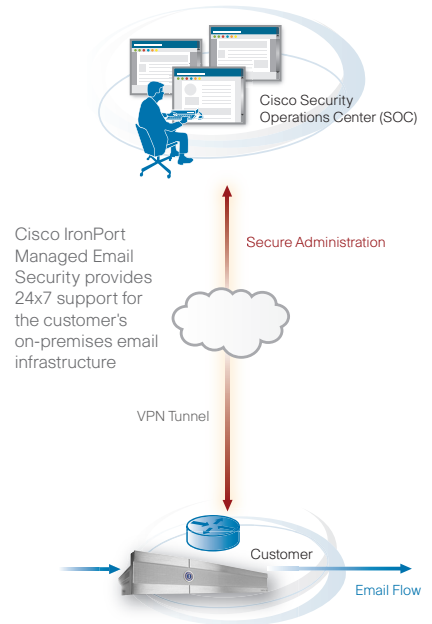
With Cisco IronPort Hybrid Email Security, the software licensing is unique. Customers get hardware, support and software licenses in a single package. The software license can be deployed by the customer wherever they chose — some of the license capacity can be utilized in the cloud and some on premises. For example, many customers will deploy anti-spam and anti-virus in the cloud and encryption and content filtering on-premises. However, for outbound scanning, customers have the flexibility to deploy the anti-virus solution even on their on-premises appliances at no additional cost.

Managed Email Security

Cisco IronPort Managed Email Security is a service that monitors and manages an organization's email delivery infrastructure, allowing IT managers to focus on other strategic initiatives. This service eliminates the need to continuously train personnel and budget for more hardware due to increasing spam volumes. Customers benefit from the highest levels of data security provided by an on-site email security appliance, while taking advantage of the flexibility to delegate some or all of the management and maintenance responsibilities.

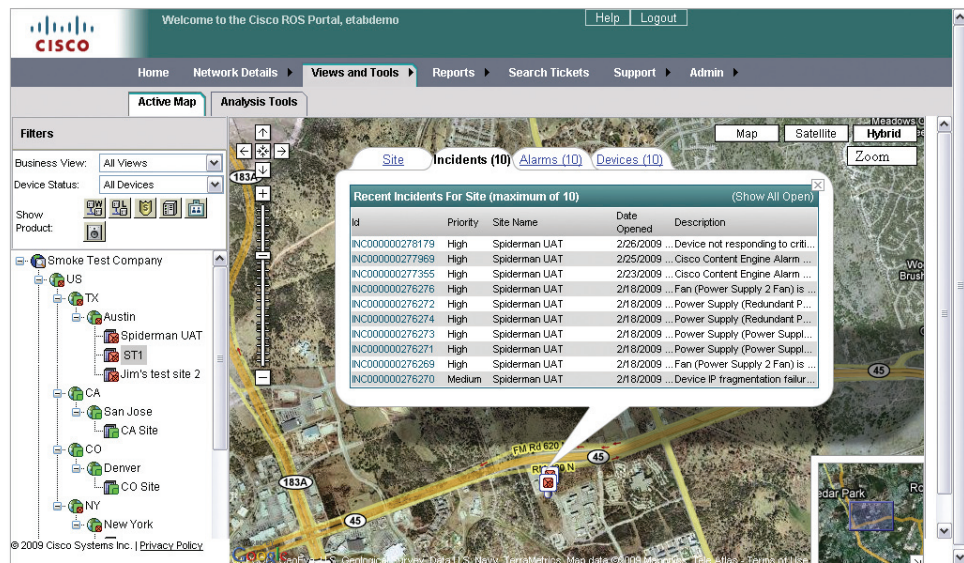
A managed email security solution is suitable for organizations faced with the following challenges:

- Difficulty finding trained personnel
- Free resources to focus on strategic IT initiatives
- The need for an on-premises email security solution with predictable pricing



Remote Monitoring and Management

With Cisco IronPort Managed Email Security, Cisco IronPort appliances are deployed in customer data centers and remotely monitored and managed at all times by email security experts on the Cisco Remote Management Services team. Utilizing a proven, Information Technology Infrastructure Library (ITIL) based methodology and processes, the Cisco team delivers trusted solutions to ensure business continuity. Customers retain ultimate control of their own network, and have real-time visibility into its health and the status through an easy-to-use portal.



Incident record and location image from the customer support portal

Flexible Management Models

Most managed service providers restrict customers from gaining management control to the email infrastructure that is deployed on their own premises. While this may be suitable for some, most email administrators want access to the infrastructure to provide quick and simple responses to queries like, “What happened to my email?” or “Who are the top offenders of the recently added content policy?”. Without management access, administrators will have to depend on the service provider for even the smallest of requests.

With Cisco IronPort Managed Email Security, the customer has a choice when it comes to deciding the best way to manage their email infrastructure. The service provides organizations with two options:

- **Co-Managed Model:** This model offers Cisco as an extension of the customer’s IT team. It provides critical email security management and monitoring support based on organizational needs. The co-management model is flexible and customized to adapt to your business processes. The customer always has full access to all Cisco IronPort appliances in their network, backed by the administrative support of the Cisco services team.
- **Fully-Managed Model:** This model provides an “always on” service whereby all aspects of email security are remotely handled by Cisco experts. This comprehensive service includes ongoing configuration support, incident management, up-to-date ticket tracking, reporting and other operational functions – ensuring the health and welfare of a company’s email infrastructure.

Business Planning Predictability

Like the other deployment options discussed earlier, Cisco IronPort Managed Email Security provides business planning predictability through a single, per-user per-year price that includes:

- Initial hardware infrastructure
- Ongoing capacity
- Software licenses

The result is that customers receive flexibility through an OpEx cost model, versus a CapEx cost model. Cisco IronPort Managed Email Security enables the highest levels of email security with a flexible management model desired by email administrators. With either selection, the important tasks are being managed and monitored by email experts. This model allows administrators to focus on more strategic initiatives, such as growing their business.

Conclusion

The Cisco Cloud Security provides organizations with the opportunity to select the email security infrastructure that is best for them – security leadership with choice, backed by email security experts. Depending upon business needs, customers can choose one of many deployment options including Cisco IronPort Cloud Email Security, Cisco IronPort Hybrid Email Security or Cisco IronPort Managed Email Security. Regardless of the deployment model, customers get the benefits of hardware capacity assurance, predictable budgetary planning and simplified management. Cisco has helped organizations worldwide with email security services, backed by industry-leading support and corporate stability.

For more information about Cisco Cloud Security, please visit:
http://www.ironport.com/products/email_security_services.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.

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)