Cisco Hybrid Email Security

This flexible service offering is designed to meet the unique security needs of inbound and outbound email management.

Cisco® Hybrid Email Security is a unique service offering that facilitates the deployment of your email security infrastructure both on premises and in the cloud. You can change the number of on-premises versus cloud users at any time throughout the term of your contract, assuming the total number of users does not change. This allows for deployment flexibility as your organization's needs change.

All deployment options are based on the same industry-leading technology that protects 40 percent of Fortune 1000 companies from inbound and outbound email threats. Cisco Hybrid Email Security simplifies the adoption of cloud services and reduces the onsite data footprint, yet customers maintain control of confidential information. Like Cisco Cloud Email Security, this hybrid service gives customers the ability to retain access to—and visibility of—both their on-premises and their cloud infrastructure. Its comprehensive reporting and message tracking also provides for highly flexible email administration. The service includes licenses for running on-premises Cisco Email Security Appliances (physical and virtual) and the Cisco Cloud Email Security service. The only additional purchase required is hardware if physical appliances will be deployed.

The Cisco Cloud Security Difference

The Cisco Cloud Security family of services uses Cisco Talos technology to deliver inbound protection and Data Loss Prevention (DLP) and the Cisco Registered Envelope Service for outbound protection.

Features

Today's email security threats consist of various viruses, spam, ransomware, phishing (fraud), spoofing and advanced malware. Cisco uses multiple methods to provide the utmost in comprehensive email security, incorporating preventive and reactive measures to strengthen your defense.

Effective Spoofing Attack Protection

Forged Email Detection protects against spoofing attacks, which focus on executives also known as high-value targets. Forged Email Detection helps you block these customized attacks. This feature provides detailed logs on all attempts and actions taken.

Proven Spam Protection

Cisco technology blocks all types of undesirable email messages with a multilayered scanning architecture. Cisco Hybrid 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.

Cisco 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 Anti-Spam uses the industry's most innovative approach to threat detection, based on the unique Cisco 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

Our high-performance virus-scanning solution provides a multilayered approach to virus filtering.

Cisco Virus Outbreak Filters are a critical first layer of defense against new outbreaks. They detect and stop viruses hours before traditional virus signatures are available.

McAfee and Sophos antivirus technologies are fully integrated to provide traditional virus detection and deliver protection against even the most complex virus attacks.

Cisco Advanced Malware Protection is available as an add-on that provides file reputation and sandboxing in the cloud to block advanced malware that would otherwise pass undetected through traditional antivirus scanners. The AMP system can now be deployed completely on premise with the AMP private cloud license. This is important for customers who have stringent policy requirements that do not allow for the use of the AMP public cloud, yet they continue benefitting from the AMP public cloud updates.

Auto remediation of malware for Office 365 customers with AMP, retrospective security helps remediate breaches faster and with less effort. Customers simply set their email security solution to take automatic actions on those infected emails.

Sophisticated Outbound Control of Sensitive Information

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

Email DLP provides protection for sensitive data with a fully integrated, comprehensive, accurate, and easy-to-deploy solution. This feature has more than 100 predefined policies, covering government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the Data Protection Act in the United Kingdom as well as industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS). These policies use sophisticated content analysis techniques and are specifically tuned to virtually eliminate false positives and increase the 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 antispam, antivirus, 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 for Highly Secure Communication

The Cisco Registered Envelope Service provides security and enhances visibility and control. It safeguards authenticated confidential data to comply with partner, customer, and regulatory requirements. This service facilitates simple, highly secure communication from the gateway to any recipient inbox. At the same time, Transport Layer Security (TLS) and Secure/Multipurpose Internet Mail Extensions (S/MIME) technology helps ensure security between partner email gateways.

Guaranteed read receipts, a feature of the Cisco Registered Envelope Service, allow the sender to know precisely when a message was delivered and viewed by each recipient.

Message expiration and locking prevents the recipient from viewing a message, even after delivery to the recipient's inbox.

ZixGateway with Cisco Technology
In addition to the Cisco Registered Envelope Service, we have partnered with ZixCorp to offer on-premises encryption with our ZixGateway with Cisco Technology. It integrates transparently with our Cisco Email Security Appliance to automate the protection of your most sensitive email content.

Automated key management automates the keys and certificates required to send and receive encrypted emails.

Fully transparent delivery means that highly secure messages and replies are delivered transparently with no password needed.

Superior TLS support is a given because it is a part of configuring the best method of delivery. The gateway also gives compliance and security officers control of and visibility into the way sensitive data is delivered.

Delivery to anyone is for recipients who do not have email encryption capabilities. The gateway offers two delivery methods: ZixPort and Cisco PXE. ZixPort is a highly secure portal that can be branded and integrated in your corporate portal. Cisco PXE (for PostX Envelope) is a push technology that delivers encrypted email in boxes directly to users.

A reporting dashboard gives compliance and security officers superior visibility. The customizable dashboard provides instant access to information about the encrypted email traffic, including what delivery method was used and who the top senders and receivers are.

Comprehensive Administration and Easy Access for Co-Management

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

- Historical events and 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 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 Hybrid Email Security provides high-performance email security backed by an industry-leading guarantee. Customers will receive money back if the solution fails to meet any of these SLAs:

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

Exceptional data protection: With Cisco Hybrid Email Security, your data is protected and remains private from start through physical separation, prohibiting data contamination. The Cisco data center has full redundancy on multiple levels, keeping your email infrastructure highly available.

Capacity assurance: Cisco Hybrid Email Security provides a service with the capacity to maintain peak performance while protecting users. When spam volumes increase, organizations typically have to purchase new hardware to maintain protection. Cisco alleviates the worry about 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: Customers can share management responsibility with Cisco. This single interface provides the following benefits:

- Access to the 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 Talos: Cisco Talos 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 that are automatically delivered to Cisco security devices, along with best-practice recommendations

Summary

Cisco Hybrid Email Security is a “best of both worlds” service, providing leading email security in a unique form factor. It provides 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 highly secure on premises.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Next Steps

The best way to understand the benefits of Cisco Cloud Email Security is to participate in the Try Before You Buy evaluation program. For additional information, please visit: http://www.cisco.com/go/cloudemail

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 C78-734189-01 06/16