Cisco Email Security Appliance Keeps Your Critical Business Email Safe

BENEFITS

- **Faster, more comprehensive email protection** often hours or days ahead of the competition
- **The largest network of threat intelligence** with Cisco Talos, built on unmatched collective security analytics
- **Outbound message protection** through effective Data Loss Prevention (DLP) and email encryption
- **Lower total cost of ownership** with a small footprint, easy implementation, and automated administration that yield savings for the long-term

Email is the leading threat vector for cyber attacks. Cisco helps protect your network from inbound threats while helping prevent the loss of business-sensitive data on outbound mail.

Mass spam campaigns and unsafe attachments are no longer your only email security concerns. By scouring social media websites, criminals find information on intended victims and create sophisticated and highly targeted attacks. They use personal information and social engineering tactics that may be tied to global news events to deceive users.

There are more opportunities for attacks than ever before. Employees once checked text-based email from a workstation behind a company firewall. Today they access rich HTML messages from multiple devices, anytime and anywhere. Ubiquitous access creates new network entry points that blur the lines of historically segmented security layers.

It's time to safeguard your network and protect your users' credentials. The Cisco® Email Security portfolio—including the Cisco Email Security Appliance, Cisco Email Security Virtual Appliance, and Cisco Cloud Email Security solutions—delivers inbound protection and outbound threat control through advanced threat intelligence and a layered approach to security. Features include Forged Email Detection to protect against spoofing attacks, antispam and antivirus tools, Outbreak Filters, and Cisco Advanced Malware Protection (AMP).

Protecting a Vital Business Asset

Businesses consider email one of their most important systems. Employees and management are more apt to send email than they are to make a phone call, send a package or fax, or even send a text message. Email is still the number one form of communication, especially for business, And email volume is rising. A solid email security gateway is vital.

Changing Threats

Spammers make a lot of money. Malware companies make a lot of money. Email attacks are a multibillion-dollar business, and they're here to stay.

Targeted attacks, advanced malware, viruses and spam aren't going away anytime soon. Cybercriminals are getting smarter and more sophisticated.

At the same time, it's more important than ever to protect your organization's sensitive data and to meet the compliance regulations for your industry.

> "With Cisco, a substantial reduction in total cost of ownership and the new features to battle viruses and spam [are] a reality."
>
> **- Kenichi Tabata, Komatsu Ltd., Japan**

Cisco Email Security Overview

All Cisco Email Security solutions share a simple approach to implementation. Three Email Security software license bundles are available as well as one standalone offering. These are Cisco Email Security Inbound, Cisco Email Security Outbound, Cisco Email Security Premium, and Advanced Malware Protection, respectively. These licenses are supported physically on our x70, x80, and x90 appliances as well as virtually through VMware's hypervisor appliance.

In addition, we offer a cloud-based solution that is a complete and highly reliable service with software, computing power, and support. The co-managed user interface is identical to that of the hardware and virtual appliances. You get outstanding protection with little administrative overhead and no onsite hardware to monitor and manage. And customers who prefer to transition their email security to the cloud can do so in phases. They can change the number of on-premises versus cloud users at any time throughout the term of their contract, assuming the total number of users does not change. This allows for deployment flexibility as their organization's needs change.

Our hybrid solution gives you advanced outbound control of sensitive messages on site along with the cost-effective convenience of the cloud. On-premises hardware and virtual appliances come ready to plug in. You can choose the model that works best for your environment to protect inbound and outbound messages at your gateway.

Table 1. Software Components

Bundles	Description
Cisco Email Security Inbound Essentials	The Inbound Essentials bundle delivers protection against email-based threats. It includes antispam tools, the Sophos antivirus solution, virus outbreak filters, Forged Email Detection, category- and reputation-based web filtering, and clustering.
Cisco Email Security Outbound Essentials	The Outbound Essentials bundle guards against data loss with DLP compliance, email encryption, and clustering.
Cisco Email Security Premium	The Premium bundle combines both inbound and outbound protections included in the two Essentials licenses noted above, for protection against email-based threats and essential data loss prevention.

Standalone Offerings	Description
Advanced Malware Protection	Advanced Malware Protection can be purchased separately with any Email Security software bundle. AMP is a comprehensive solution that provides malware detection and blocking, continuous analysis, and retrospective alerting. AMP augments the malware detection and blocking capabilities already offered in Email Security with file reputation scoring and blocking, file sandboxing, and file retrospection for a continuous analysis of threats, even after they have traversed the email gateway.
Graymail safe-unsubscribe	Graymail management tags graymail with a “safe-unsubscribe” option. This tag will manage the “unsubscribe” action on behalf of the end user. It will also monitor the different types of graymail and unsubscribe requests. All of these actions can be managed at a policy, LDAP-group level.

Email Security Features

Feature	Description
Threat defense	Effective protection against email-transported threats requires an informed vision of the threat landscape. That means bringing to bear a global threat perspective and an email protection infrastructure that responds rapidly. Cloud-based intelligence, combined with real-time analytics, is essential to generating zero-day responses. Email Security delivers inbound protection and outbound threat control through advanced threat intelligence and a layered approach to security. Features include URL categorization and reputation filtering, antispam and antivirus tools, outbreak filters, and Advanced Malware Protection. Stay protected against the latest threats with Cisco Talos. With a 24-hour view into global traffic activity, Talos analyzes anomalies, uncovers new threats and monitors traffic trends to provide proven zero-day threat defense often well ahead of competitors. Cisco’s broad view of dynamic threats includes: • Over 1.6 million global devices • Historical library of 40,000 threats • 35 percent of global email traffic seen per day • Over 13 billion web requests seen per day • Over 200 parameters tracked • Multivector visibility Talos consists of three pillars to provide proactive email protection: SenderBase, the Threat Operations Center, and dynamic updates. **SenderBase** Encounter fewer false positives with Cisco’s email reputation database. SenderBase, part of Talos, compiles data along more than 200 parameters, including email volume, domain blacklists and safe lists, domain registration dates, and the length of time that domains have been sending email. This information is gathered to create a composite IP reputation score to block email from suspicious senders. **Threat Operations Center** Stay ahead of evolving threats with around-the-clock global coverage that generates new rules using machine-based technology with human ideas behind them. Our Threat Operation Center runs in five centers worldwide, covering 95 percent of Internet languages. Data feeds from email security devices are compiled along with those from Intrusion Prevention System (IPS), firewall and web products. In addition, penetration testing, botnet infiltration, malware reverse engineering, and vulnerability research provide insight into current and future threat trends. Those insights are used to create updates that feed into Email Security. **Dynamic Updates** Receive automatic updates to the antispam, antivirus, and outbreak filter engines of your Email Security solution every 3 to 5 minutes—over eight million rules each day. Reputation updates also provide real-time protection against known bad senders. Automated content updates reduce exposure windows, eliminate processing of most spam messages, and lower security management overhead. Other solutions for threat defense include reputation filtering, category-based web filtering, and antivirus tools. **Reputation Filtering** Block known bad email with reputation filtering, which is based on threat intelligence from Cisco Talos’s database. For each embedded hyperlink, a reputation check is performed to verify the integrity of the source. Websites with known bad reputations are automatically blocked. Reputation filtering stops 90 percent of spam before it even enters your network, allowing the solution to scale by analyzing a much smaller payload. **Category-Based Web Filtering** Administrators can filter specific categories such as gambling and adult sites. If the associated website violates a policy, the URL may be dropped, quarantined, or disarmed accordingly. **Forged Email Detection** 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 and provides detailed logs on all attempts and actions taken. **Antivirus Tools** For multilayer antivirus protection, you can deploy either the Sophos or McAfee antivirus engine, or both. Run both engines to dual-scan messages for the most comprehensive protection. During an attack, use a multilayered antispam approach for comprehensive protection. Cisco combines the outer layer of filtering based on sender reputation and an inner layer of filtering that performs a deep analysis of each message to stop spam from reaching company inboxes.

Feature	Description
	The emails that pass through reputation filtering are scanned with an antispam engine for a greater than 99 percent catch rate and a less than one in one million false positive rate. You can decide to drop, quarantine, or deliver messages suspected of being spam. We also offer optional multiengine spam-scanning technology to catch corner-case spam. Additionally, you can decide whether you want to deliver, quarantine, drop, or bounce marketing messages that typically come from an aggressive marketer: ones that stem from agreeing to the terms on a site that shares your data with affiliate companies. **Advanced Malware Protection** The Email Security Appliance now includes Advanced Malware Protection. It also features file reputation scoring and blocking, file sandboxing, and file retrospection for a continuous analysis of threats. Users can block more attacks, track suspicious files, mitigate the scope of an outbreak, and remediate quickly. Advanced Malware Protection is available to all Email Security Appliance customers as an additionally licensed feature. Also available is Cisco AMP Threat Grid, which supports all the AMP capabilities through an on-premises appliance for organizations that have compliance or policy restrictions on submitting malware samples to the cloud. Customers can also purchase an additional license to deploy their AMP system completely on premises with the AMP private cloud. This, along with the AMP Threat Grid appliance, brings the entire AMP offering completely on-premise. 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. **Graymail Detection** Graymail is categorized as marketing, social networking, and bulk messages. Using a unsubscribe mechanism, end users can indicate to the sender that they want to opt out of receiving such emails. Since mimicking a unsubscribe mechanism is a popular phishing technique, users are wary of clicking the unsubscribe links. The graymail solution provides: • Protection against malicious threats masquerading as unsubscribe links • A uniform interface for managing subscriptions • Better visibility for email administrators and end users into such emails **Outbreak Filters** Outbreak filters defend against emerging threats and blended attacks. They can issue rules on any combination of six parameters, including file type, file name, file size, and URLs in a message. As Talos learns more about an outbreak, it can modify rules and release messages from quarantine accordingly. Outbreak filters can also rewrite URLs linked in suspicious messages. When clicked, the new URLs redirect the recipient through the Web Security proxy. The website content is then actively scanned, and outbreak filters will display a block screen to the user if the site contains malware. **Web Interaction Tracking** Administrators can track the users who click URLs that have been rewritten by the Email Security Appliance. Reports show: • Top users who clicked on malicious URLs • The top malicious URLs clicked by end users • Date and time, rewrite reason, and action taken on the URLs
Data security	Email Security offers effective, accurate DLP policy enforcement and email encryption. Centralized management and reporting simplifies data protection. Scale to meet the demands of your business with your choice of appliance-based, virtual, cloud-based, and hybrid solutions. Hardware and virtual appliances keep sensitive data on the premises. Alternatively, reduce your onsite data center footprint in the cloud. You can let Cisco take care of policy changes for you, or have full access to create policy changes as needed. A hybrid option allows for the benefits of the cloud while controlling sensitive data on site before it leaves your network border. **Data Loss Prevention (DLP)** Protect outbound messages with Cisco Email Security DLP. Comply with industry and government regulations worldwide and prevent confidential data from leaving your network. Choose from an extensive policy library of more than 100 expert policies covering government, private sector, and company-specific regulations. The predefined data loss prevention policies are included with Email Security solutions and simplify the application of content-aware outbound email policy. Remediation choices include encrypting, adding footers and disclaimers, adding Blind Carbon Copies (BCCs), notifying, and quarantining. For companies needing a complex custom policy, the building blocks of the predefined policies are readily available to make the process quick and easy. **Encryption** Give senders control of their content, even after messages have been sent. With email encryption, senders don't fear mistyped recipient addresses, mistakes in content, or time-sensitive emails, because they can always lock a message. The sender of an encrypted message receives a read receipt once a recipient opens a message, and highly secure replies and forwards are automatically encrypted to maintain end-to-end privacy and control. Take advantage of the most advanced cloud-based encryption key service available today. Manage recipient registration, authentication and per-message, per-recipient encryption keys with the Cisco Registered Envelope Service. This highly available managed service provides all user registrations and authentications. There is no additional infrastructure to deploy. For enhanced security, message content goes straight from your gateway to the recipient, and only the encryption key is stored in the cloud.

Feature	Description
	Meet encryption requirements for regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), or the Sarbanes-Oxley Act (SOX)—as well as state privacy regulations and European directives—without burdening the senders, recipients, or email administrators. Offer encryption not as a mandate but as a service that's easy to use and gives the sender complete control. Help the sender manually encrypt a message with a simple feature key requiring no desktop software or additional management. The Registered Envelope Service can also scan the outbound email and automatically encrypt that message. An email containing encryption-required content is automatically enrolled into the key-management system. Once the message has been sent, the sender can log in to the service and activate track, secure, reply, recall, and other commands. The administrator can set configurations so that senders receive automatic read receipts. Facilitate easy yet highly secure access for recipients. The recipient simply needs to open the message, confirm his identity and view the message. If this is the first time a user is asked to register credentials, he will be directed to a site to create an account and establish a password. That password will be used to open this email and all other secure emails sent from the company or from any one of the over 5000 companies using this service. 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 seamlessly with our Cisco Email Security Appliance to automate the protection of your most sensitive email content. Superior Transport Layer Security (TLS) support is simple 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 how sensitive data is delivered. 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 directly to users' in-boxes. Compliance and security officers gain superior visibility through a customizable reporting dashboard. The 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.
Manageability	**Universal Device Support** Make sure all users can access messages when needed, regardless of whether they are on smartphones, tablets, laptops, or desktop computers. Universal device support is designed to ensure that highly secure messages can be read by any recipient, no matter what device is used to open the message. Dedicated plug-in applications offer an enhanced user experience for Microsoft Outlook and on Apple iOS and Google Android smartphones and tablets. **System Overview Dashboard** Monitor and report on outbound messages from a centralized, custom System Overview dashboard. Unified business reporting offers a single view for comprehensive insight across your organization. Get the details of any report for advanced visibility. **Detailed Message Tracking** Track a message by envelope recipient, envelope sender, subject, attachments, and message events including DLP policy or IDs. When you send a message to the Email Security solution, the message tracking database is populated within a minute or two, and you can see what happened to the messages that are crossing the system at every step of processing.

> "We needed an intelligent pre-gateway filtering solution that would make it easier to enforce policies and to protect users, without being overzealous and bringing the business to a grinding halt."
>
> **- Ben Gordon, IT Infrastructure Manager, Noble Foods**

Related Services

Cisco branded services	The Cisco Security Planning and Design Service helps you deploy a strong security solution quickly and cost-effectively. The Cisco Email Security Configuration and Installation Remote Service mitigates security risks by installing, configuring, and testing your solution. The Cisco Security Optimization Service supports an evolving security system to meet new security threats, with design, performance tuning, and support for system changes.
Collaborative and partner services	The Cisco Collaborative Professional Services Network Device Security Assessment Service helps maintain a hardened network environment by identifying security gaps. The Cisco Smart Care Service keeps your business running at its best with proactive monitoring using intelligence from highly secure visibility into a network's performance. Cisco partners also provide a wide range of additional services across the planning, design, implementation, and optimization lifecycle.
Cisco financing	Cisco Capital® can tailor financing solutions to business needs. Acquire Cisco technology faster and see the business benefits sooner.
Cisco Smart Net Total Care™ Service	To get the most value from your technology investment, you can purchase the Cisco Smart Net Total Care Service for use with the Email Security Appliances. The service helps you resolve network problems quickly with direct, anytime access to Cisco experts, self-help support tools, and rapid hardware replacement.

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.

Customer Case Studies

Customer Name: Komatsu

Headquarters: Japan

Business: Worldwide industrial equipment and vehicle manufacturer

Cisco Email Security provided:

- Proactive and reactive threat prevention and management with powerful email security and security management appliances
- An estimated 75 percent increase in the detection of spam within one week of deployment
- Transparent management and updating for low cost of ownership with reduced administrative burdens and downtime

Customer Name: Noble Foods

Headquarters: United Kingdom

Industry: Food production, agriculture, and retail

With Email Security:

- Over two million threats were blocked and 99.3 percent less spam was received in the first six months
- There is now less risk of delay for legitimate email
- Spam- and virus-related IT service desk calls declined by 80 percent, releasing IT staff to focus more on business-enablement projects

Organization: Gobierno de Castilla-La Mancha

Headquarters: Spain

Industry: Government

Email and Web Security:

- Significantly reduced external Internet access malware threats, improving the user experience
- Stabilized email security, dramatically improving performance
- Provided easy-to-deploy and easy-to-manage solutions, freeing up IT staff time to handle other initiatives

Figure 1. Cisco Email Security x90 Appliance

Why Cisco?

Security is a top priority for Cisco. We've backed that focus with over $1 billion spent in dynamic threat research and development. Cisco was cited as a leader in the Gartner Magic Quadrant for email and web security, next-generation IPS, and next-generation firewalls. Our 37,000 content security customers around the world trust Cisco's high catch rate, low false positives, and low solution complexity along with Talos, the industry's largest collection of real-time threat intelligence. Cisco also has over 10 J.D. Power award-winning security support centers to serve customers around the globe and globally dispersed escalation experts, quality assurance, and development staff to meet our customers' needs 24 hours a day, 365 days a year.

Next Steps

Find out more about the Cisco Email Security Appliance at https://www.cisco.com/go/esa. Evaluate how Cisco products will work for you with a Cisco sales representative, channel partner, or systems engineer.

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 **https://www.cisco.com/go/offices**.

Printed in USA C22-733566-05 07/17