Cisco Email Security Appliance

Each day, more than 100 billion corporate email messages are exchanged. As email use rises, security becomes an ever-greater priority. Cisco® solutions offer high availability email protection against the dynamic, rapidly changing threats affecting your organization.

Features and Benefits

Whether physical, virtual, cloud, or hybrid, our email security solutions are recognized as industry leaders that offer:

- **Fast, comprehensive protection,** often hours or days ahead of the competition
- **One of the largest networks of threat intelligence,** built on extensive collective security analytics from Cisco Talos
- **Outbound message protection** through on-device data loss prevention (DLP), email encryption, and optional integration with the RSA enterprise DLP solution
- **Low total cost of ownership** with a small footprint, easy implementation, and automated administration that yield savings for the long term

Product Overview

Today, spam and malware are part of a complex email security picture that includes inbound threats and outbound risks. The all-in-one Cisco Email Security Appliance offers simple, fast deployment, with few maintenance requirements, low latency, and low operating costs. Our set-and-forget technology frees your staff after the automated policy settings go live. The solution then automatically forwards security updates to Cisco's cloud-based threat intelligence solution. Threat intelligence data is refreshed in the email appliance every 3 to 5 minutes, providing you with an up-to-date threat defense response hours or days before other vendors. Flexible deployment options and smooth integration with your existing infrastructure make this appliance an excellent fit for your business needs.

Virtual Appliance

The Cisco Email Security Virtual Appliance significantly lowers the cost of deploying email security, especially in highly distributed networks. This appliance lets your network manager create instances where and when they are needed, using your existing network infrastructure. A software version of the physical appliance, it runs on top of a VMware ESXi hypervisor and Cisco Unified Computing System™ (Cisco UCS®) servers. You receive an unlimited license for the virtual appliance with the purchase of any Cisco Email Security software bundle.

With the virtual appliance, you can respond instantly to increasing traffic growth with simplified capacity planning. You don't need to buy and ship appliances, so you can support new business opportunities without adding complexity to a data center or having to hire additional staff.

Main Capabilities

You can defend your mission-critical email systems with physical, virtual, cloud, and hybrid solutions. Table 1 summarizes the major capabilities of our email security solutions.

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

Table 1. Main Capabilities

Capability	Description
Global threat intelligence	Get fast, comprehensive email protection backed by one of the largest threat detection networks in the world. Cisco provides broad visibility and a large footprint, including: • 100 terabytes (TB) of security intelligence daily • 1.6 million deployed security devices including firewalls, Cisco IPS sensors, and web and email appliances • 150 million endpoints • 13 billion web requests per day • 35 percent of the world's enterprise email traffic Cisco Talos provides a 24-hour view into global traffic activity. It analyzes anomalies, uncovers new threats, and monitors traffic trends. Talos helps prevent zero-hour attacks by continually generating rules that feed updates to the security appliances. These updates occur every 3 to 5 minutes, delivering industry-leading threat defense.
Spam blocking	Spam is a complex problem that demands a sophisticated solution. Cisco makes it easy. To stop spam from reaching your inbox, a multilayered defense combines an outer layer of filtering based on the reputation of the sender and an inner layer of filtering that performs a deep analysis of the message. With reputation filtering, more than 80 percent of spam is blocked before it even hits your network. Recent enhancements include contextual analysis and enhanced automation, as well as autoclassification, to provide a strong defense against snowshoe campaigns. Customers that experience large volumes of email within short periods will be able to apply filters based on the sender or subject, which will block the associated messages or place them in quarantine.
Graymail detection and safe unsubscribe	Graymail consists of marketing, social networking, and bulk messages. The graymail detection feature helps precisely classify and monitor graymail entering an organization. An administrator can then take appropriate action on each category. Often graymail has an unsubscribe link that lets end users can indicate to the sender that they would like to opt out of receiving such emails. Because mimicking a unsubscribe mechanism is a popular phishing technique, users should be wary of clicking these unsubscribe links. The safe unsubscribe solution provides: • Protection against malicious threats masquerading as unsubscribe links • A uniform interface for managing all subscriptions • Better visibility for email administrators and end users into such emails
Advanced Malware Protection	Cisco Email Security Appliance now includes Cisco Advanced Malware Protection. It offers file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for the continuous analysis of threats, even after they have traversed the email gateway. 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. The Cisco AMP Threat Grid delivers malware protection through an on-premises appliance for organizations that have compliance or policy restrictions on submitting malware samples to the cloud. 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.

Capability	Description
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 Cisco 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	A fully integrated solution allows IT administrators to track the end users who click URLs that have been rewritten by the Email Security Appliance. Reports show: • Top users who clicked malicious URLs • The top malicious URLs clicked by end users • Date and time, rewrite reason, and action taken on the URLs The admin can also trace back to all the messages containing the particular URL.
Outbound message control	Email Security Appliances control outbound messages through DLP, email encryption. This control helps ensure that your most important messages comply with industry standards and are protected in transit. Additionally, outbound antispam and antivirus scanning, along with outbound rate limiting, can be used to keep compromised machines or accounts from getting your company on email blacklists. New: The Email Security Appliance now supports Secure/Multipurpose Internet Mail Extensions (S/MIME) encryption and signing in addition to Transport Layer Security (TLS).
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 with a dedicated content filter. This feature provides detailed logs on all attempts and actions taken.
Excellent performance	The security appliances quickly block new inbound email viruses. Domain delivery queues keep undeliverable emails from causing a backup of critical deliveries to other domains. This solution offers an industry-leading spam catch rate greater than 99.9 percent and false positive rate of less than 1 in 1 million.
DLP	You can use one or more predefined policies (there are more than 100 to choose from) to help prevent confidential data from leaving the network. If you prefer, you can use parts of those predefined policies to create your own custom policies. The built-in RSA email DLP engine uses pretuned data structures along with your own optional data points such as words, phrases, dictionaries, and regular expressions to quickly create accurate policies with few false positives. The DLP engine scores violations by severity, so you can apply different levels of remediation to fit your needs.
Low cost	A small footprint, an easy setup, and the automated management of updates mean savings for the life of your email security solution. Cisco's solution has one of the lowest TCOs available.
Flexible deployment	All Cisco email security solutions share a simple approach to implementation. The system setup wizard can handle even complex environments and will have you up and protected in just minutes, making you safer, fast. Licensing is user based, not device based, so you can apply it per user instead of per device to provide inbound as well as outbound email gateway protection at no additional cost. This capability lets you scan outbound messages with antispam and antivirus engines to fully support your business needs. The virtual appliance offers all the same features as the physical appliance, with the added convenience and cost savings of a virtual deployment model. It offers instant self-service provisioning. With a Cisco Email Security Virtual Appliance license, you can deploy email security gateways in your network without Internet connections. This license has purchased software licenses embedded in it. You can apply licenses at any time to a new virtual image file stored locally. Pristine virtual image files can be cloned if needed, giving you the ability to deploy several email security gateways immediately. You can run hardware and virtual email security solutions in the same deployment. So your small branch offices or remote locations can have the same protection you get at headquarters without the need to install and support hardware at those locations. You can easily manage custom deployments with the Cisco Content Security Management Appliance or Cisco Content Security Management Virtual Appliance.
Solutions that fit your business	Cisco Cloud Email Security is a comprehensive and highly reliable service with software, computing power, and support. The co-managed user interface is identical to that of the Cisco physical and virtual email security appliances. You therefore get outstanding protection with little administrative overhead and no onsite hardware to monitor and manage. Microsoft Office 365 customers can also get the same industry-leading protection with Cloud Email Security for Office 365. This solution is easy to deploy, and you can count on guaranteed reliability through multiple resilient data centers for the highest levels of service availability and data protection. The hybrid solution gives you advanced outbound control of sensitive messages on site while helping you take advantage of the cost-effective convenience of the cloud. You can also 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. 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.

Product Specifications

Table 2 presents the performance specifications for the Email Security Appliance, Table 3 presents the hardware specifications for the appliance, Table 4 presents the specifications for the virtual appliance, and Table 5 presents the specifications for the Security Management Appliance.

Table 2. Email Security Appliance Performance Specifications

Deployment	Model	Disk Space	RAID Mirroring	Memory	CPUs
Large enterprise	ESA C690	2.4 TB (600 x 4)	Yes (RAID 10)	32 GB DDR4	2 x 2.4 GHz, 6 core
Large enterprise	ESA C690X	2.4 TB (600 x 8)	Yes (RAID 10)	32 GB DDR4	2 x 2.4 GHz, 6 core
Large enterprise	ESA C680	1.8 TB (300 x 6)	Yes (RAID 10)	32 GB DDR3	2 x 2.0 GHz, 6 core
Medium-sized enterprise	ESA C390	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR4	1 x 2.4 GHz, 6 core
Medium-sized enterprise	ESA C380	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR3	1 x 2.0 GHz, 6 core
Small to midsize businesses or branch offices	ESA C190	1.2 TB (600 x 2)	Yes (RAID 1)	8 GB DDR4	1 x 1.9 GHz, 6 core
Small to midsize businesses or branch offices	ESA C170	500 GB (250 x 2)	Yes (RAID 1)	4 GB DDR3	1 x 2.8 GHz, dual core

Note: For accurate sizing, verify your choice by checking the peak mail-flow rates and average message size with a Cisco content security specialist.

Table 3. Email Security Appliance Hardware Specifications

Model	ESA C690	ESA C690X	ESA C680	ESA C390	ESA C380	ESA C190	ESA C170
Rack units (RU)	2RU	2RU	2RU	1RU	2RU	1RU	1RU
Dimensions (H x W x D)	3.4 in. x 19 in. x 29 in. (8.6 x 48.3 x 73.7 cm)	3.4 in. x 19 in. x 29 in. (8.6 x 48.3 x 73.7 cm)	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm)	1.7 in. x 19 in. x 31 in. (4.3 x 48.3 x 78.7 cm)	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm)	1.7 in. x 19 in. x 31 in. (4.3 x 48.3 x 78.7 cm)	1.67 in. x 16.9 in. x 15.5 in. (4.24 x 42.9 x 39.4 cm)
DC power option	Yes	Yes	Yes	No	Yes	No	No
Remote power cycling	Yes	Yes	Yes	Yes	Yes	No	No
Redundant power supply	Yes	Yes	Yes	Yes	Yes	Yes, accessory option	No
Hot-swappable hard disk	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ethernet interfaces	6-port 1GBASE-T copper network interface (NIC), RJ-45	6-port 1GBASE-T copper network interface (NIC), RJ-45	4-port 1GBASE-T copper network interface (NIC), RJ-45	6-port 1GBASE-T copper network interface (NIC), RJ-45	4-port 1GBASE-T copper network interface (NIC), RJ-45	2-port 1GBASE-T copper network interface (NIC), RJ-45	2-port 1GBASE-T copper network interface (NIC), RJ-45
Speed (Mbps)	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate
Fiber option	Yes, separate SKUs 4-port 1GBASE-SX Fiber: ESA-C690-1G 4-port 10GBASE-SR Fiber: ESA-C690-10G	Yes, separate SKUs 4-port 1GBASE-SX Fiber: ESA-C690-1G 4-port 10GBASE-SR Fiber: ESA-C690-10G	Yes, separate SKUs 6-port 1GBASE-SX Fiber: ESA-C680-1G 6-port 10GBASE-SR Fiber: ESA-C680-10G	No	No	No	No

Table 4. Email Security Virtual Appliance Specifications

Email Users				
	Model	**Disk**	**Memory**	**Cores**
Evaluations only	ESAV C000v	200 GB (10K RPM SAS)	4 GB	1 (2.7 GHz)
Small enterprise (up to 1000 employees)	ESAV C100v	200 GB (10K RPM SAS)	6 GB	2 (2.7 GHz)
Medium-sized enterprise (up to 5000 employees)	ESAV C300v	500 GB (10K RPM SAS)	8 GB	4 (2.7 GHz)
Large enterprise or service provider	ESAV C600v	500 GB (10K RPM SAS)	8 GB	8 (2.7 GHz)
Servers				
Cisco UCS	VMware ESXi 5.0, 5.1 and 5.5 Hypervisor			

Table 5. Secure Management Appliance M-Series Platform Specifications

Model	SMA M690/690X/680	SMA M390/380	SMA M190/M170
Number of users	10,000 or more	Up to 10,000	Up to 1,000

Where to Deploy

You can deploy our email security solutions:

- **On premises:** The Email Security Appliance is a gateway typically deployed in a network edge outside the firewall (the so-called demilitarized zone). Incoming Simple Mail Transfer Protocol (SMTP) traffic is directed to the appliance's data interface according to specifications set by your mail exchange records. The appliance filters it and redelivers it to your network mail server. Your mail server also directs outgoing mail to the data interface, where it is filtered according to outgoing policies and then delivered to external destinations.
- **Virtual:** With Cisco UCS running in your small branch office, you could host the virtual appliance with other Cisco products such as the Cisco Web Security Virtual Appliance. Together, they provide the same level of protection as their hardware equivalents but save you money on space and power resources. You can centrally manage this custom deployment with the Secure Management Appliance or virtual appliance.

Options for Cloud Security

Cisco Cloud Email Security provides you with a flexible deployment model for email security. It helps you reduce costs with co-management and no onsite email security infrastructure.

Cisco Hybrid Email Security gives you the benefits of Cloud Email Security and provides advanced outbound control of encrypting messages and onsite DLP. This hybrid solution lets you transition to a cloud solution at your own pace.

Cisco Email Security: Physical and Virtual Appliance Licenses

A license for the virtual appliance is included in all email security software bundles: the Cisco Email Security Inbound, Email Security Outbound, and Email Security Premium bundle. This license has the same term as the other software services in the bundle and can be used for as many virtual instances as needed, as long as it conforms with the purchased user count. The Email Security Appliance licenses are included in all email security software bundles. Just purchase the appropriate licenses for the number of mailboxes you need to support, then buy the appropriate on-premises appliances. For virtual appliances, simply order the software licenses to get entitlement.

Term-Based Subscription Licenses

Licenses are term-based subscriptions of 1, 3, or 5 years.

Quantity-Based Subscription Licenses

The Cisco Email Security portfolio uses tiered pricing based on the number of mailboxes. Sales and partner representatives will help you determine the correct customer deployment.

Email Security Software Licenses

Three Email Security software license bundles are available: Cisco Email Security Inbound, Cisco Email Security Outbound, and Cisco Email Security Premium. Advanced Malware Protection can be bought separately. The major components of each software offering are provided in Table 6.

Table 6. Software Components

Bundles	Description
Cisco Email Security Inbound Essentials	The Cisco Email Security Inbound Essentials bundle delivers protection against email-based threats, including antispam with graymail detection, Sophos antivirus solution, virus outbreak filters, Forged Email Detection, and clustering.
Cisco Email Security Outbound Essentials	The Cisco Email Security Outbound Essentials bundle guards against data loss with DLP compliance, email encryption, and clustering.
Cisco Email Security Premium	The Cisco Email Security Premium bundle combines the inbound and outbound protections included in the two Cisco Email Security Essentials licenses noted above, for protection against email-based threats and essential data loss prevention.
Standalone Offering	**Description**
Cisco Advanced Malware Protection	Cisco Advanced Malware Protection can be purchased along with any Cisco Email Security software bundle. AMP is a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis, and retrospective alerting. Advanced Malware Protection augments the antimalware detection and blocking capabilities already offered in the Cisco Email Security Appliances with file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for continuous analysis of threats, even after they have traversed the email gateway. Upon purchase of any necessary hardware, you receive an unlimited license of AMP Threat Grid. And the AMP system, along with the Threat Grid appliance, can now be deployed completely on premises with the AMP private cloud license. This is important for customers who have stringent policy requirements that do not allow for use of the AMP public cloud.
Graymail safe unsubscribe	Graymail now can be tagged with a truly safe “unsubscribe” option. This tag manages a highly secure “unsubscribe” action on behalf of the end user. It also monitors the different graymail unsubscribe requests. All these can be managed at an LDAP group policy level.

Software License Agreements

The Cisco End-User License Agreement and the Web Security Supplemental End-User License Agreement are provided with each software license purchase.

Software Subscription Support

All email security licenses include software subscription support that is essential to keeping business-critical applications available, highly secure, and operating at peak performance. This support entitles you to the services listed below for the full term of the purchased software subscription.

- Software updates and major upgrades keep applications performing at their best, with the most current features.
- The Cisco Technical Assistance Center provides fast, specialized support.
- Online tools build and expand in-house expertise and boost business agility.
- Collaborative learning provides additional knowledge and training opportunities.

Cisco Services

Table 7 summarizes the Cisco Services available for our email security solutions.

Table 7. Cisco Services

Service	Description
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 Support Services

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. For more information, visit http://www.cisco.com/c/en/us/services/support/smart-net-total-care.html.

How to Evaluate the Cisco Email Security Appliances

The best way to understand the benefits of the Cisco Email Security Appliance C-Series and X-Series platforms is to participate in the Try Before You Buy program. To receive a fully functional evaluation appliance to test in your network, free for 45 days, visit this page.

How to Evaluate the Cisco Cloud Email Security Services

The cloud-based solution is a reliable, all-inclusive service that provides a flexible deployment model for email security. It reduces your personal costs with co-management and no onsite email security infrastructure. Your Cisco account team or reseller can assist you in setting up a free 45-day evaluation.

How to Evaluate the Cisco Email Security Virtual Appliance

1. Go to http://www.cisco.com/go/esa.
2. Under "Support" on the right side, click "Software Downloads, Release and General Information." Click "Download Software"; then click the link for any model to see the downloadable virtual machine images available. You will also see a downloadable XML evaluation license. You will need to download one of the images and the XML evaluation license.
3. Download the following documentation from Cisco.com:
   a. Cisco Security Virtual Appliance Installation Guide
   b. Release Notes for Cisco AsyncOS® 9.5 for Email

4. Follow the instructions in the Cisco Security Virtual Appliance Installation Guide to get started. Please note that Cisco Content Security Virtual Appliance evaluations are not covered under the Cisco Smart Net Total Care Service and are therefore unsupported.

Warranty Information

Find warranty information on Cisco.com at the Product Warranties page.

Why Cisco?

Security is more critical to your network than ever before. As threats and risks persist, along with concerns about confidentiality and control, security is necessary for providing business continuity, protecting valuable information, and maintaining brand reputation. Cisco's integrated security solutions embedded in the fabric of your network give you heightened visibility and control to protect your business without disruption. Our market leadership, advanced threat protection before, during, and after an attack, innovative products, and longevity make us the right vendor to serve your security needs.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital financing 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.

For More Information

For further details, visit http://www.cisco.com/go/emailsecurity. Or take advantage of the popular offer, Three Ways to Try Email Security for Free.

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 C78-729751-12 08/16