Cisco Email Security Appliances

Product Overview

Over the past 20 years, email has evolved from a tool used primarily by technical and research professionals to become the backbone of corporate communications. Each day, more than 100 billion corporate email messages are exchanged. As the level of use rises, security becomes a greater priority. Mass spam campaigns are no longer the only concern. Today, spam and malware are just part of a complex picture that includes inbound threats and outbound risks.

Cisco® Email Security solutions defend mission-critical email systems with appliance, virtual, cloud, and hybrid solutions. The industry leader in email security solutions, according to an Infonetics Research 2013 study, Cisco delivers:

- Fast, comprehensive email protection that blocks spam, malware and other threats while providing protection before, during, and after an attack
- Flexible cloud, virtual, and physical deployment options to meet your ever-changing business needs
- Outbound message control through on-device data loss prevention (DLP), email encryption, and optional integration with the RSA enterprise DLP solution
- One of the lowest total cost of ownership (TCO) email security solutions available

Cisco's all-in-one solution 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. This threat intelligence data is pulled by the Cisco Email Security Appliances (ESAs) every three to five minutes, providing you with industry-leading threat defense hours or days before other vendors. Flexible deployment options and smooth integration with your existing security infrastructure make Cisco Email Security an excellent fit for your business needs.

Virtual Appliance

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

With the Cisco ESAV, 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.

Features and Benefits

Cisco Email Security defends your mission-critical email systems with appliance, virtual, cloud, and hybrid solutions. Cisco Email Security is recognized by third parties as the best source of email security. Table 1 summarizes the main features and benefits of Cisco Email Security solutions.

Table 1. Features and Benefits

Feature	Benefit
Global threat intelligence	Get fast, complete email protection backed by one of the largest threat detection networks in the world. Cisco Email Security provides broad visibility and a large footprint, including: • 100 terabytes (TB) of security intelligence daily • 1.6 million deployed security devices including firewalls, Cisco Intrusion Prevention System (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 SIO provides a 24-hour view into global traffic activity. It analyzes anomalies, uncovers new threats, and monitors traffic trends. Cisco SIO helps prevent zero-hour attacks by continually generating new rules that feed updates to the Cisco ESAs. These updates occur every three to five minutes, providing 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, over 80 percent of spam is blocked before it even hits your network. 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.
Advanced malware protection	Cisco ESAs now include the Advanced Malware Protection (AMP), a malware defeating solution that takes advantage of the vast cloud security intelligence network of Sourcefire (now a part of Cisco). It delivers protection across the attack continuum: before, during and after an attack. It also features file reputation scoring and blocking, file sandboxing, and file retrospection for 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 faster. AMP is available to all Cisco ESA customers as an additionally licensed feature.
Outbound message control	Cisco ESAs control outbound messages through DLP, email encryption, and optional integration with the RSA Enterprise Manager. This control helps ensure that your most important messages comply with industry standards and are protected in transit. Additionally, outbound antispam and antivirus, along with outbound rate limiting, can be used to keep compromised machines or accounts from getting your company on email blacklists.
Excellent performance	Cisco ESAs quickly block new inbound email viruses. Domain delivery queues keep undeliverable emails from causing a backup of critical deliveries to other domains.
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 a minimum of 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 Cisco Email Security solution. Cisco's solution has one of the lowest TCOs available.

Feature	Benefit
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 Cisco ESAV offers all the same features as the Cisco ESA, with the added convenience and cost savings of a virtual deployment model. The Cisco ESAV offers instant self-service provisioning. With a Cisco ESAV license, you can deploy email security virtual gateways in your network without Internet connections. The Cisco ESAV license has purchased software licenses embedded on it. You can apply licenses at any time to a new Cisco ESAV 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 Cisco 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 that location. You can easily manage custom deployments with the Cisco Content Security Management Appliance (SMA).
Solutions that fit your business	The cloud-based solution is a complete and highly reliable service with software, computing power, and support. The co-managed user interface is identical to that of the Cisco ESA and ESAV. You therefore get outstanding protection with little administrative overhead and no onsite hardware to monitor and manage. The hybrid solution gives you advanced outbound control of sensitive messages onsite while enabling you to take advantage of 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.

Product Specifications

Table 2 presents the performance specifications for the Cisco ESA, Table 3 presents the hardware specifications for the Cisco ESA, Table 4 presents the specifications for the Cisco ESAV, and Table 5 presents the specifications for the Cisco SMA.

Table 2. Cisco ESA Performance Specifications

Deployment*	Model	Disk Space	RAID Mirroring	Memory	CPUs
Large enterprise	Cisco ESA X1070	1.8 TB (300 x 6)	Yes (RAID 10)	4 GB	2 x 4 (2 quad cores)
	Cisco ESA C680	1.8 TB (300 x 6)	Yes (RAID 10)	32 GB	2 x 6 (2 hexa cores)
Medium-sized enterprise	Cisco ESA C670	1.2 TB (300 x 4)	Yes (RAID 10)	4 GB	2 x 4 (2 quad cores)
	Cisco ESA C380	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB	1 x 6 (1 hexa core)
Small-to-midsize businesses or branch offices	Cisco ESA C370	600 GB (300 x 2)	Yes (RAID 1)	4 GB	1 x 4 (1 quad core)
	Cisco ESA C170	500 GB (250 x 2)	Yes (RAID 1)	4 GB	1 x 2 (1 dual core)

* 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. Cisco ESA Hardware Specifications

Model	Cisco ESA X1070	Cisco ESA C680	Cisco ESA C380	Cisco ESA C370	Cisco ESA C170
Rack units (RU)	2RU	2RU	2RU	2RU	1RU
Dimensions (H x W x D)	3.5 in. x 17.5 in. x 26.8 in. (8.9 x 44.5 x 68.1 cm)	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm.)	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm.)	3.5 in. x 17.5 in. x 26.8 in. (8.9 x 44.5 x 68.1 cm)	1.67 in. x 16.9 in. x 15.5 in. (4.24 x 42.9 x 39.4 cm)
DC power option	No	Yes	Yes	No	No
Remote power cycling	No	Yes	Yes	No	No
Redundant power supply	Yes	Yes	Yes	Yes	No
Hot-swappable hard disk	Yes	Yes	Yes	Yes	Yes
Ethernet interfaces	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	2 Gigabit NICs, 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 Gigabit Ethernet fiber option	No	Yes (accessory)	No	No	No

Table 4. Cisco ESAV Specifications

Email Users				
Email users	**Model**	**Disk**	**Memory**	**Cores**
Evaluations only	Cisco ESAV C000v	200 GB	4 GB	1
Up to 1000	Cisco ESAV C100v	200 GB	6 GB	2
1000 to 4999	Cisco ESAV C300v	500 GB	8 GB	4
Enterprise	Cisco ESAV C300v	500 GB	8 GB	4
Large enterprise or service provider	Cisco ESAV C600v	500 GB	8 GB	8
Servers				
Cisco UCS	VMware ESXi 4.0 X 5.0 Hypervisor			

Table 5. Cisco SMA M-Series Platform Specifications

Model	Cisco SMA M1070	Cisco SMA M680	Cisco SMA M380	Cisco SMA M170
Number of users	10,000 or more	10,000 or more	Up to 10,000	Up to 1000

Where to Deploy

You can deploy Cisco Email Security solutions:

- **On premises:** The Cisco ESA is an email gateway typically deployed in a firewall demilitarized zone. Incoming Simple Mail Transfer Protocol (SMTP) traffic is directed to the Cisco ESA data interface according to specifications set by your mail exchange records. The Cisco ESA filters it and redelivers it to your network mail server. Your mail server also directs outgoing mail to the Cisco ESA 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 Cisco ESAV with other Cisco products such as the Cisco Web Security Virtual Appliance (WSAV). 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 Cisco SMA.

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 Cisco 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 Cisco ESAV license is included for all Cisco Email Security software bundles: the Cisco Email Security Inbound, Cisco Email Security Outbound, or Cisco 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 you stick to the purchased user count. The Cisco ESA licenses are included in all Cisco 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 one, three, or five 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 to determine the correct customer deployment.

Email Security Software Licenses

Three Cisco Email Security software license bundles are available, as well as one à la carte offering: Cisco Email Security Inbound, Cisco Email Security Outbound, Cisco Email Security Premium, and Advanced Malware Protection. The major components of each software offering are provided below.

Bundles	Description
Cisco Email Security Inbound Essentials	The Cisco Email Security Inbound Essentials bundle delivers protection against email-based threats, including antispam, Sophos antivirus solution, virus outbreak filters, 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 both 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.
A la Carte Offerings	**Description**
Advanced Malware Protection	Advanced Malware Protection (AMP) can be purchased à la carte 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. AMP augments the antimalware detection and blocking capabilities already offered in Cisco Email Security with file reputation scoring and blocking, file sandboxing, and file retrospection for continuous analysis of threats, even after they have traversed the email gateway.

Software License Agreements

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

Software Subscription Support

All Cisco Email Security licenses include software subscription support 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 (TAC) 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 6 summarizes the Cisco Services available for Cisco Email Security solutions.

Table 6. Cisco Services for Cisco Email Security Solutions

Service	Description
Cisco branded services	• The Cisco Security Planning and Design Service enables you to 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 SMARTnet Support Services

To get the most value from your technology investment, you can purchase the Cisco SMARTnet® Service for use with Cisco ESAs. The Cisco SMARTnet 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/go/smartnet.

How to Evaluate the Cisco ESAs

The best way to understand the benefits of the Cisco ESA 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 30 days, visit http://www.cisco.com/go/esa.

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 30-day evaluation.

How to Evaluate the Cisco ESAV

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. Documentation for Cisco IronPort® Manufacturing - AsyncOS 7.7.5

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 SMARTnet 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 unmatched 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.

For More Information

http://www.cisco.com/go/emailsecurity.

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 C78-729751-04 03/14