Cisco Email Security: Layered Protection from Blended Threats

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 on-device Data Loss Prevention (DLP), email encryption, and optional integration with RSA's Enterprise DLP solution
- **Lower total cost of ownership** with a small footprint, easy implementation, and automated administration that yield savings for the long term

Email is the number one threat vector for cyberattacks, according to the 2015 Cisco Annual Security Report. The Cisco® Email Security Appliance keeps your critical business email safe and helps eliminate data leakage.

The Cisco Email Security portfolio–including the Cisco Email Security Appliance (ESA; see Figure 1), Cisco Email Security Virtual Appliance (ESAV), and Cisco Cloud Email Security (CES) solutions–delivers inbound protection and outbound data control through advanced threat intelligence and a layered approach to security. This approach comprises URL categorization and reputation filtering, antispam and antivirus filters, Outbreak Filters, and Advanced Malware Protection (AMP).

Figure 1. Cisco Email Security Appliance

Threat-focused

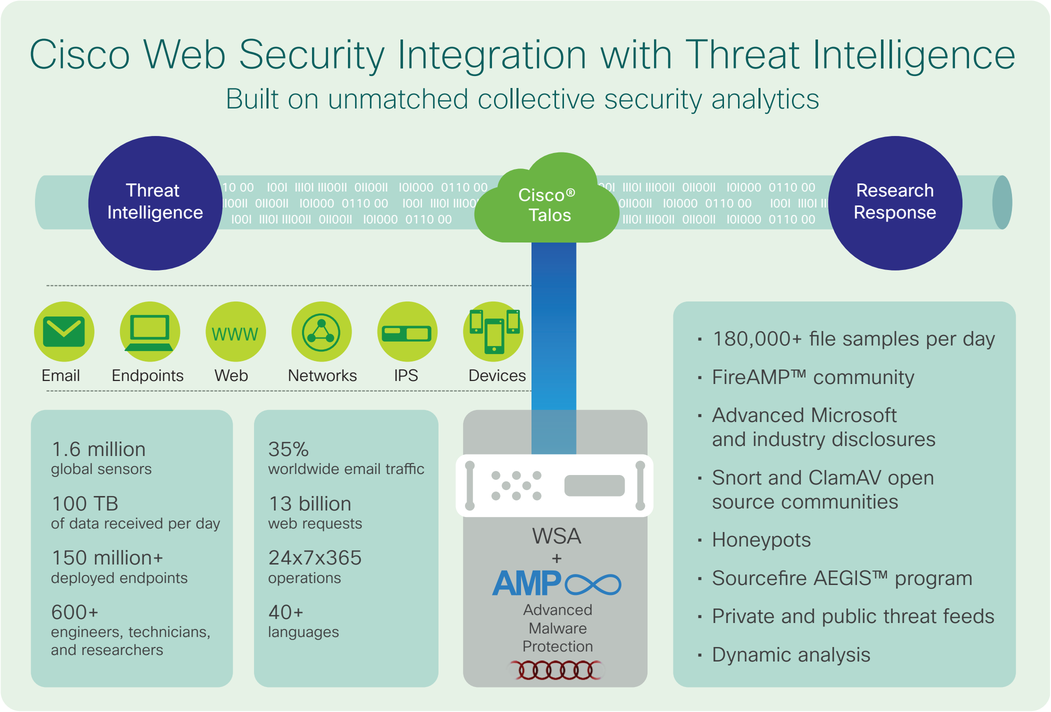
Advanced Threat Defense

Cisco Email Security is powered by Cisco Talos Security Intelligence and Research Group (Talos), the industry's largest collection of real-time threat intelligence, with the broadest visibility and largest footprint. Talos discovers where threats are hiding by pulling massive amounts of global information across multiple attack vectors (see Figure 2). This information gathering encompasses:

- 100 TB of security intelligence daily
- 1.6 million deployed security devices including firewall, intrusion prevention system (IPS), web, and email appliances
- 150 million endpoints
- 13 billion web requests per day
- Hundreds of applications and 150,000 microapplications
- 35 percent of the world's enterprise email traffic

Talos delivers early-warning intelligence, threat and vulnerability analysis to help protect organizations against zero-day advanced threats. It continually generates new rules that feed updates every three to five minutes, so that Cisco Email Security can deliver industry-leading threat defense hours and even days ahead of competitors.

Figure 2. Cisco Talos Security Intelligence and Research Group



Cisco Web Security Integration with Threat Intelligence

Built on unmatched collective security analytics

1.6 million global sensors

100 TB of data received per day

150 million+ deployed endpoints

600+ engineers, technicians, and researchers

35% worldwide email traffic

13 billion web requests

24x7x365 operations

40+ languages

- 180,000+ file samples per day
- FireAMP™ community
- Advanced Microsoft and industry disclosures
- Snort and ClamAV open source communities
- Honeypots
- Sourcefire AEGIS™ program
- Private and public threat feeds
- Dynamic analysis

A Multilayered Defense to Tackle Multiple Threats

Integrated into the Cisco ESA is our Cisco Talos service, which provides a 24-hour view into global traffic activity (see Figure 4). You can analyze anomalies, uncover new threats, and monitor traffic trends. Automatic policy updates are pushed to network devices every three to five minutes.

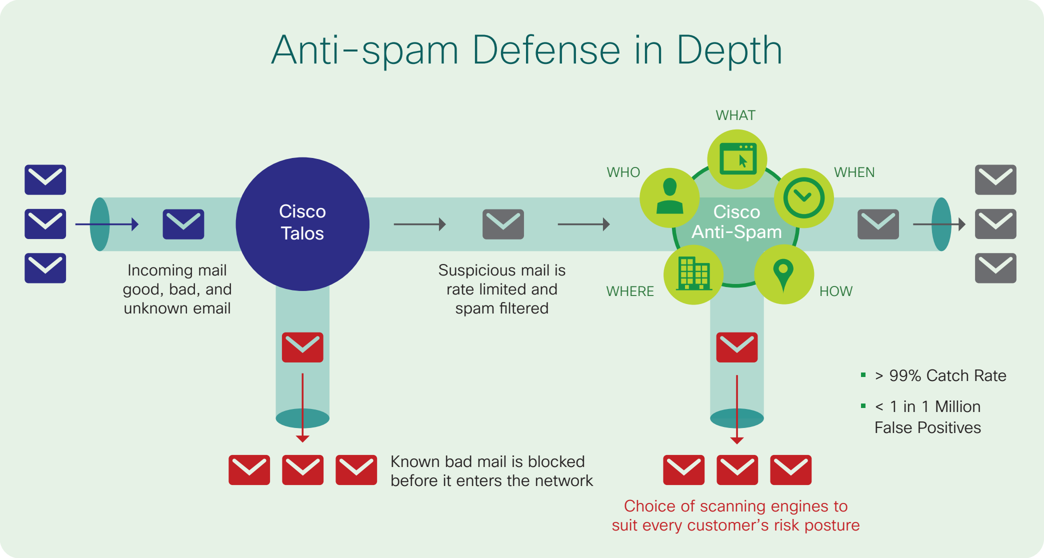
With Cisco ESA you can also:

- Stop phishing attempts and blended threats
- Satisfy requirements for highly secure messaging with dependable encryption
- Comply with industry and government data loss prevention regulations
- Defend against advanced threats and targeted attacks
- Set and enforce detailed email policies

Advanced Spam Defense

We make it easy to stop spam from reaching your inbox. A multilayered defense combines an outer layer of filtering based on the reputation and validity of the sender and an inner layer of filtering that performs a deep analysis of the message. We have 3 engine choices, one of which is IMS that uses multiple anti-spam engines for the best possible catch rate. And recent enhancements help defend against snowshoe campaigns using contextual analysis, enhanced automation, and autoclassification (see Figure 3).

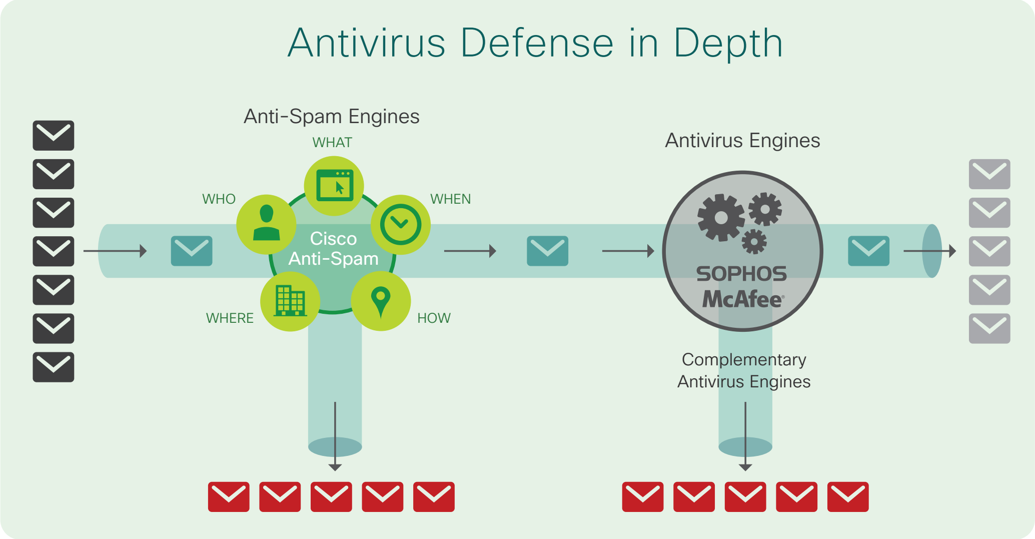
Figure 3. Cisco ESA's SPAM Protection


Anti-spam Defense in Depth
WHAT
WHO
WHEN
WHERE
HOW
Cisco Talos
Cisco Anti-Spam
Incoming mail good, bad, and unknown email
Suspicious mail is rate limited and spam filtered
Known bad mail is blocked before it enters the network
> 99% Catch Rate
< 1 in 1 Million False Positives
Choice of scanning engines to suit every customer's risk posture

Anti-virus

For multi-layer anti-virus protection, choose to deploy either Sophos or McAfee anti-virus engines—or both. Run both antivirus engines in tandem to dual-scan messages for the most comprehensive protection. Use the same license for inbound anti-spam and anti-virus scanning to check your outbound messages, with intelligent multi-scanning providing the best possible catch rate. Use all of these features for the visibility to identify needed remediation and keep your company off of blacklists. Combine this with Outbreak Filters to help stop the threats before they manifest themselves as an outbound flood of messages (i.e. zero-day outbreaks).

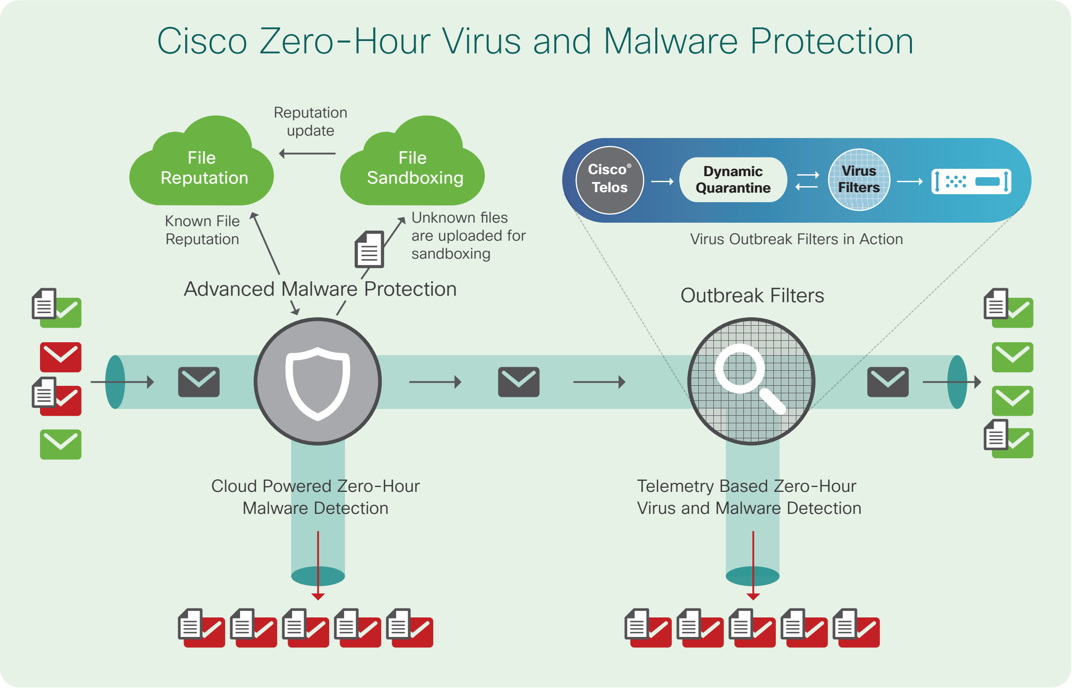
Figure 4. Cisco ESA's Threat Protection



Sandboxing and Continuous Analysis

Advanced Malware Protection (AMP) is an additionally licensed feature available to all Cisco ESA customers. AMP is a comprehensive malware-defeating solution that provides malware detection and blocking, continuous analysis, and retrospective alerting (see Figure 5). It takes advantage of the vast cloud security intelligence networks of both Cisco and Sourcefire (now part of Cisco). AMP augments the malware detection and blocking capabilities already offered in the Cisco ESA with enhanced file reputation capabilities, detailed file-behavior reporting, continuous file analysis, and retrospective verdict alerting. New: Customers now have the ability to sandbox PDF and Microsoft Office files, and archive/compressed files in addition to EXE files supported in the first AMP release.

Figure 5. Cisco Zero-Hour Virus and Malware Protection


Cisco Zero-Hour Virus and Malware Protection
Reputation update
File Reputation
File Sandboxing
Known File Reputation
Unknown files are uploaded for sandboxing
Advanced Malware Protection
Cisco® Telos
Dynamic Quarantine
Virus Filters
Virus Outbreak Filters in Action
Outbreak Filters
Cloud Powered Zero-Hour Malware Detection
Telemetry Based Zero-Hour Virus and Malware Detection

Best Performance

DLP and Compliance

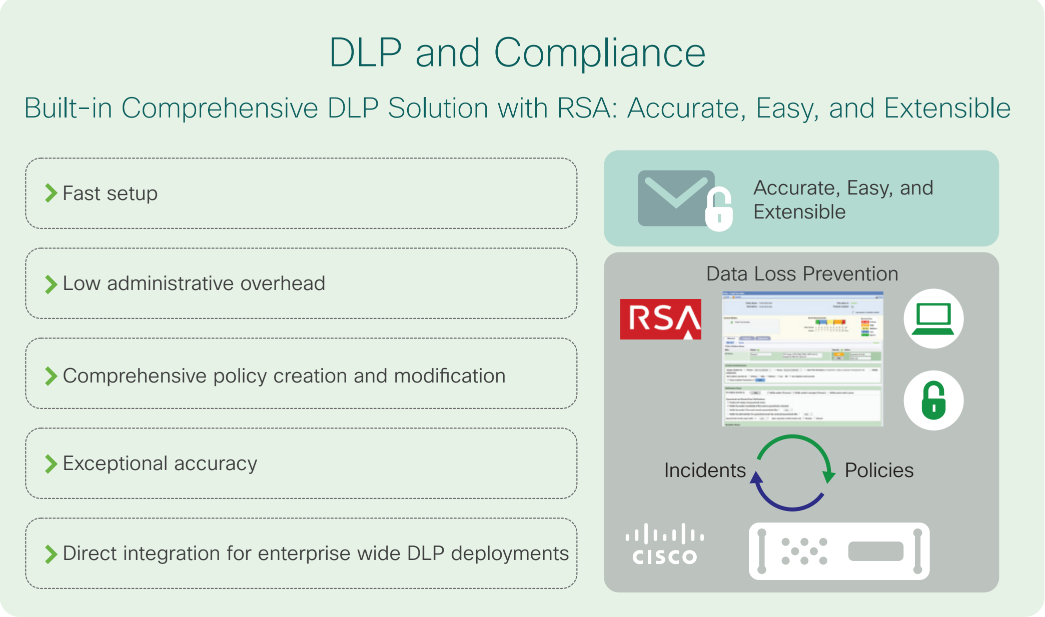
Data loss prevention and compliance are a key part of the Cisco Email Security technology. In fact, your outbound data loss prevention filters are already onboard your Cisco Email Security solution.

We partner with RSA, the leader in DLP technology, to provide integrated DLP functionality to help ensure compliance with industry and government regulations worldwide and help prevent confidential data from leaving your network.

Instead of Cisco reinventing all of these DLP libraries, we partner with a proven vendor and build its compliance libraries and lexicons into all of our email security solutions (see Figure 6).

If you are looking to expand beyond email to protect sensitive data in other threat vectors such as web, endpoints, data center, and so on, we offer direct integration with DLP Enterprise Manager, the overarching management console for the RSA DLP Suite. With this integration, RSA Enterprise Manager is your single pane of glass for setting common rules, policies, and remediation measures across your organization, not just your email.

Figure 6. Cisco ESA’s DLP Model



DLP and Compliance

Built-in Comprehensive DLP Solution with RSA: Accurate, Easy, and Extensible

- Fast setup
- Low administrative overhead
- Comprehensive policy creation and modification
- Exceptional accuracy
- Direct integration for enterprise wide DLP deployments

Encryption

Satisfy compliance requirements with secure messaging.

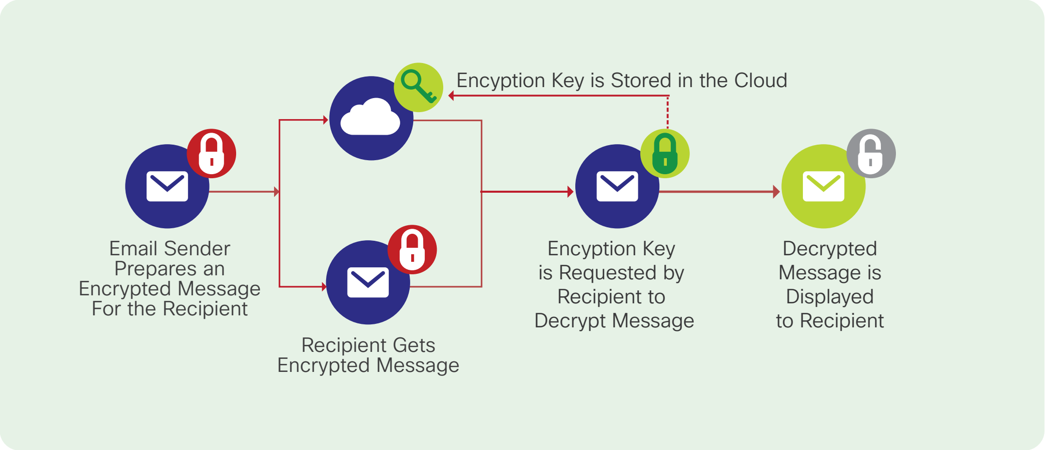
Meet encryption requirements for regulatory requirements such as PCI, HIPAA, SOX, and GLBA–as well as state privacy regulations and European directives–without burdening the senders, recipients, or email administrators. Offer encryption not as a mandate, but as a service that’s easy to use.

Give the sender complete control of their content, even after it’s been sent. With Cisco’s email encryption, senders don’t fear mistyped recipient addresses, mistakes in content, or time-sensitive emails because the sender always has the option to lock the message.

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 Cisco Registered Envelope Service.

Cisco Registered Envelope Service provides all user registration and authentication as a highly available managed service. There’s no additional infrastructure to deploy. For enhanced security and reduced risk, message content goes straight from your gateway to the recipient.

Figure 7. Cisco Registered Envelope Service


Encyption Key is Stored in the Cloud
Email Sender Prepares an Encrypted Message For the Recipient
Recipient Gets Encrypted Message
Encyption Key is Requested by Recipient to Decrypt Message
Decrypted Message is Displayed to Recipient

Continuous Innovation

Lower Total Cost of Ownership

The Cisco ESA delivers a consolidated solution in a single appliance, unlike other solutions that often require additional devices for new features and functions. You spend less time troubleshooting. You save time with automatic updates from Talos and stay tuned against the latest threats without intervention. Lastly, you can use your existing VMware infrastructure in an unlimited number of deployments of the Cisco Email Security Virtual Appliance (ESAV).

Flexible Deployments: On Premises, in the Cloud, Hybrid, and Virtual

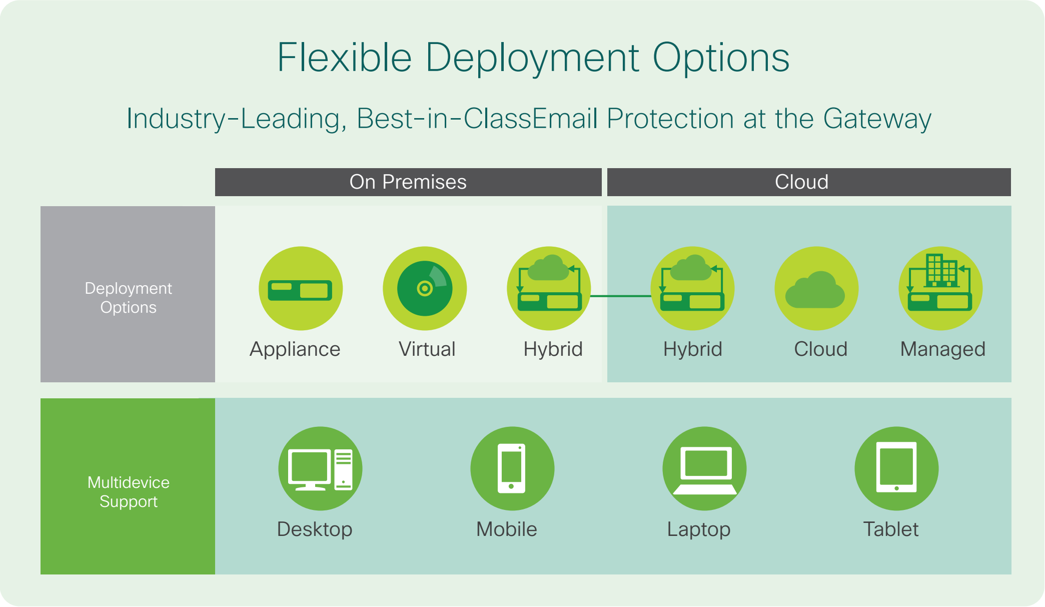
The Cisco ESA has a flexible set of deployment options (see Figure 8). You can deploy it on premises with an appliance or a clustered group of appliances, either hardware or virtual. You can do multiple clusters if needed. You can have some in certain data centers and others in other data centers for redundancy or for hot or cold standby.

And then we have a cloud approach and a hybrid approach. You can handle all your inbound and outbound security in the cloud if you don't want the appliance on premises or if you simply want someone else to handle it. In the cloud you can have us make changes to policies. Or you can have full access to the cloud to create the policy changes.

The hybrid approach has a similar co-management situation. You can clean the messages coming into the cloud but do the control outbound on premises to stop those messages before they leave your gateway or network border.

We offer these options with support across multiple devices, including desktops, mobile phones, laptops, and tablets, and for Android, iOS, Mac, PC, and Linux.

Figure 8. Cisco ESA Deployment Options



Models and Options Available

Tables 1 and 2 provide performance and hardware specifications for the Cisco ESA. Table 3 provides specifications for the Cisco ESAV, and Table 4 describes the software components.

Table 1. Cisco ESA Performance Specifications

Deployment	Model	Disk Space	RAID Mirroring	Memory	CPUs
Large enterprise	Cisco ESA C680	1.8 TB (3 x 600 GB)	Yes (RAID 10)	32 GB	2 x 6 (2 hexa cores)
Medium-sized enterprise	Cisco ESA C380	1.2 TB (2 x 600 GB)	Yes (RAID 1)	16 GB	1 x 6 (1 hexa core)
Small to midsize businesses or branch offices	Cisco ESA C170	500 GB (2 x 250 GB)	Yes (RAID 1)	4 GB	1 x 2 (1 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 2. Cisco ESA Hardware Specifications

Model	Cisco ESA C680	Cisco ESA C380	Cisco ESA C170
Rack units (RU)	2RU	2RU	1RU

Model	Cisco ESA C680	Cisco ESA C380	Cisco ESA C170
Dimensions (H x W x D)	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.)	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	No
Remote power cycling	Yes	Yes	No
Redundant power supply	Yes	Yes	No
Hot-swappable hard disk	Yes	Yes	Yes
Ethernet interfaces	4 Gigabit network interface cards (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 Gigabit Ethernet fiber option	Yes (accessory)	NNo	

Table 3. Cisco ESAVSpecifications

Email Users				
Email users	Model	Disk	Memory	Cores
Evaluations only	Cisco ESAV C000v	250 GB (10K RPM SAS)	4 GB	1 (2.7 GHz)
Small enterprise (up to 1K)	Cisco ESAV C100v	250 GB (10K RPM SAS)	6 GB	2 (2.7 GHz)
Medium enterprise (up to 5K)	Cisco ESAV C300v	1024 GB (10K RPM SAS)	8 GB	4 (2.7 GHz)
Large enterprise or service provider	Cisco ESAV C600v	2032 GB (10K RPM SAS)	8 GB	8 (2.7 GHz)
Servers				
Cisco UCS	VMware ESXi 5.0, 5.1 and 5.5 Hypervisor			

Table 4. Software Components

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 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.
A la Carte Offerings	**Description**
Cisco Advanced Malware Protection	Cisco 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.

Next Steps

Find out more at http://www.cisco.com/go/esa. Evaluate how the Cisco ESA 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 **www.cisco.com/go/offices.**