Brochure

Cisco Email Security: Layered Protection from Blended Threats

Email is the number one threat vector for cyber attacks. The Cisco® Email Security Appliance keeps your critical business email safe and helps eliminate data leakage.

BENEFITS

- Faster, more comprehensive email protection, often hours or days ahead of the competition
- Threat intelligence from 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
- Flexibility for customers who prefer an on-premises and cloud hybrid deployment or who wish to transition to the cloud gradually

The Cisco Email Security portfolio—including the Cisco Email Security Appliance (Figure 1), the Cisco Email Security Virtual Appliance, and Cisco Cloud Email Security—delivers inbound protection and outbound data control. It does so 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 Defense

Advanced Protection

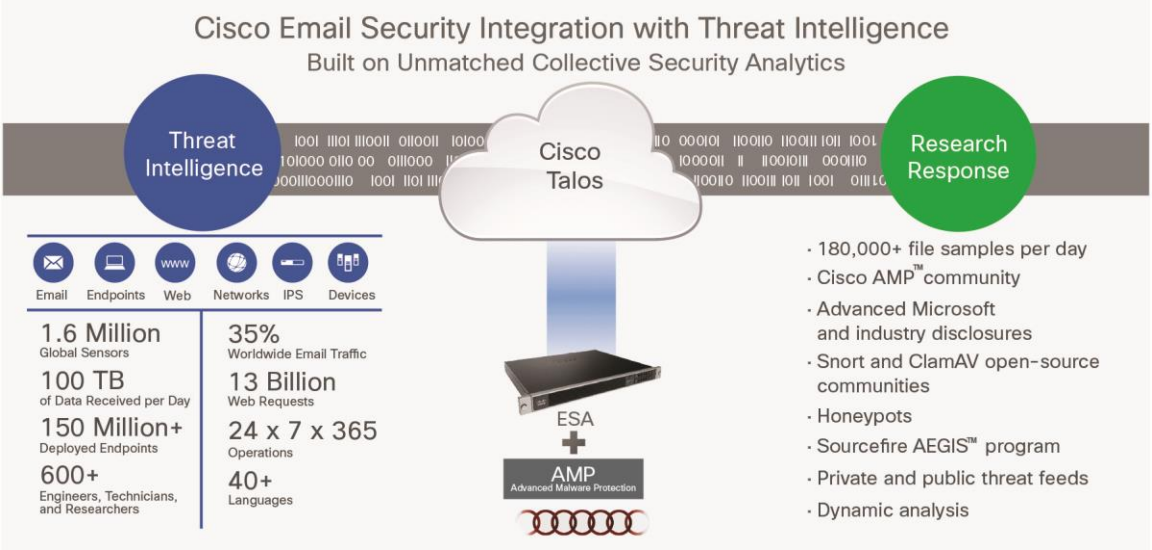
Cisco Email Security is powered by the Cisco Talos Security Intelligence and Research Group (Talos), the industry's largest network of real-time threat intelligence, with the broadest visibility and largest footprint. Talos discovers where threats are hiding by pulling massive amounts of global information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

Our Talos service provides a 24-hour view into global traffic activity. It delivers early-warning intelligence along with threat and vulnerability analysis to help protect organizations against zero-day advanced threats. It continually generates new rules that feed updates to your devices every 3 to 5 minutes, so Cisco Email Security can deliver threat defense hours and even days ahead of competitors. You can analyze anomalies, uncover new threats, and monitor traffic trends.

Figure 2. Cisco Talos Security Intelligence and Research Group



A Multilayered Defense to Tackle Multiple Threats

In addition to the protection that Talos provides, the Email Security Appliance helps you:

- Stop phishing and spoofing attempts as well as 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

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.

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 offer three engine choices. One is an intelligent multiscan (IMS), which uses multiple antispam engines for the best possible catch rate. Recent enhancements help defend against snowshoe campaigns using contextual analysis, enhanced automation, and autoclassification.

Antivirus Protection

For multilayer antivirus protection, you can deploy the Sophos or the McAfee antivirus engine—or both. Run both antivirus engines in tandem to dual-scan messages for the most comprehensive protection. Use the same license for inbound antispam and antivirus scanning to check your outbound messages, with intelligent multiscanning providing the best possible catch rate. Use all these features for the visibility to identify needed remediation and keep your company off blacklists. Use outbreak filters to help stop threats before they manifest themselves as an outbound flood of messages (that is, zero-day outbreaks).

Sandboxing and Continuous Analysis

Advanced Malware Protection (AMP) is an additionally licensed feature available to all Email Security Appliance customers. AMP is a comprehensive malware-defeating solution that provides malware detection and blocking, continuous analysis, and retrospective alerting. 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 Email Security Appliance. It offers enhanced file reputation capabilities, detailed file-behavior reporting, continuous file analysis, and retrospective verdict alerting. 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.

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 based on the AMP retrospective alert that exposes malicious emails.

Exceptional Performance

DLP and Compliance

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

We provide integrated DLP functionality to help ensure compliance with industry and government regulations worldwide and help prevent confidential data from leaving your network.

Encryption

Satisfy compliance requirements with highly secure messaging.

Meet encryption requirements for regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and Gramm-Leach-Bliley Act (GLBA)— as well as state privacy regulations and European directives—without burdening senders, recipients, or email administrators. Offer encryption not as a mandate but as a service that’s easy to use.

Give senders 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 the Cisco Registered Envelope Service.

This highly available managed service handles all user registration and authentication. There's no additional infrastructure to deploy. For enhanced security and reduced risk, message content goes straight from your gateway to the recipient.

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 Email Security Appliance to automate the protection of your most sensitive email content.

Superior 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.

Continuous Innovation

Lower Total Cost of Ownership

The Email Security Appliance 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 more 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 Email Security Virtual Appliance.

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

The Email Security Appliance has a flexible set of deployment options. 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 yourself.

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.

Organizations that prefer an on-premises and cloud hybrid deployment, or who wish to transition to the cloud gradually, can now change their deployment mix (number of on-premises users versus cloud users) at any time.

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

Models and Options Available

Tables 1 and 2 provide performance and hardware specifications for the Email Security Appliance. Table 3 provides specifications for the Email Security Virtual Appliance, and Table 4 describes the software components.

Table 1. 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 2.4GHz, 6C
Large enterprise	ESA C690X	2.4 TB (600 x 8)	Yes (RAID 10)	32 GB DDR4	2 x 2.4GHz, 6C
Large enterprise	ESA C680	1.8 TB (300 x 6)	Yes (RAID 10)	32 GB DDR3	2 x 2.0GHz, 6C
Medium-sized enterprise	ESA C390	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR4	1 x 2.4GHz, 6C
Medium-sized enterprise	ESA C380	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR3	1 x 2.0GHz, 6C
Small to midsize businesses or branch offices	ESA C190	1.2 TB (600 x 2)	Yes (RAID 1)	8 GB DDR4	1 x 1.9GHz, 6C
Small to midsize businesses or branch offices	ESA C170	500 GB (250 x 2)	Yes (RAID 1)	4 GB DDR3	1 x 2.8GHz, 2C

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. Email Security Appliance Hardware Specifications

Model	C690	C690X	C680	C390	C380	C190	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 (NICs), RJ-45	6-port 1GBASE-T copper network interface (NICs), RJ-45	6-port 1GBASE-T copper network interface (NICs), RJ-45	6-port 1GBASE-T copper network interface (NICs), RJ-45	6-port 1GBASE-T copper network interface (NICs), RJ-45	2-port 1GBASE-T copper network interface (NICs), RJ-45	2-port 1GBASE-T copper network interface (NICs), RJ-45

Table 3. Email Security Virtual Appliance Specifications

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 1000)	Cisco ESAV C100v	250 GB (10K RPM SAS)	6 GB	2 (2.7 GHz)
Medium enterprise (up to 5000)	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, 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 (AMP) 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. 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. In addition, the AMP system can be deployed completely on premises with the AMP private cloud license. This is important for customers who have policy requirements that do not allow for a public feed.

Next Steps

Find out more at http://www.cisco.com/go/esa. Evaluate how the Cisco Email Security Appliance 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.

Printed in USA C02-733901-04 06/16