Cisco Email Security
Advanced Email Protection

Product Overview

Customers of all sizes face the same daunting challenge: email is simultaneously the most important business communication tool and the leading attack vector for security breaches. Cisco® Email Security enables users to communicate securely and helps organizations combat business email compromise (BEC), ransomware, advanced malware, phishing, spam, and data loss with a multi-layered approach to security.

The Cisco Email Security Difference

Cisco Email Security includes advanced threat protection capabilities to detect, block, and remediate threats faster; prevent data loss; and secure important information in transit with end-to-end encryption.

With Cisco Email Security customers can:

- Detect and block more threats with superior threat intelligence from Talos™, our threat research team.
- Combat ransomware hidden in attachments that evade initial detection with Cisco Advanced Malware Protection (AMP) and Cisco Threat Grid.
- Drop emails with risky links automatically or block access to newly infected sites with real-time URL analysis to protect against phishing and BEC.
- Protect sensitive content in outgoing emails with data loss prevention (DLP) and easy-to-use email encryption, all in one solution.
- Gain maximum deployment flexibility with a cloud, virtual, on-premises, or hybrid deployment or move to the cloud in phases.

Features

Today's email security threats consist of ransomware, advanced malware, business email compromise (BEC), phishing, and spam. Cisco Email Security technology blocks threats so that companies receive only legitimate messages. Cisco uses multiple layers to provide the utmost in comprehensive email security, incorporating preventive and reactive measures to strengthen your defense. Table 1 summarizes the major capabilities of our email security solutions.

Table 1. Main Capabilities

Capability	Description
Global threat intelligence	Get fast, comprehensive email protection backed by Talos, one of the largest threat detection networks in the world. Talos provides broad visibility and a large footprint, including: • 600 billion emails per day • 16 billion web requests per day • 1.5 million malware samples 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 customers' email security solutions. These updates occur every three to five minutes, delivering industry-leading threat defense.
Reputation filtering	Block unwanted email with reputation filtering, which is based on threat intelligence from Talos. 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.

Capability	Description
Spam protection	Spam is a complex problem that demands a sophisticated solution. Cisco makes it easy. Cisco Email Security blocks unwanted emails using a multilayered scanning architecture delivering the highest spam catch rate of greater than 99 percent, with a less than a one-in-one-million false-positive rate. The antispam functionality in Cisco Email Security uses the Cisco Context Adaptive Scanning Engine (CASE). This engine examines the complete context of a message, including what content the message contains, how the message is constructed, who is sending the message, and where the call to action of the message takes you. By combining these elements, Cisco Email Security stops the broadest range of threats with industry-leading accuracy.
Forged Email Detection	Forged Email Detection protects against business email compromise attacks focused on executives, who are considered high-value targets. Forged-email detection helps you block these customized attacks and provides detailed logs on all attempts and actions taken.
Virus Defense	By offering a high-performance virus scanning solution integrated at the gateway, Cisco Email Security provides a multilayered, multivendor approach to virus filtering.
Graymail detection and safe unsubscribe	Graymail consists of marketing, social networking, and bulk messages. The graymail detection feature precisely classifies and monitors graymail entering an organization. An administrator can then take appropriate action on each category. Often graymail has an unsubscribe link where end users can indicate to the sender that they would like to opt out of receiving such emails. Since 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
Cisco Advanced Malware Protection and Cisco Threat Grid	Cisco Advanced Malware Protection (AMP) and Cisco Threat Grid provide file reputation scoring and blocking, file sandboxing, and file retrospection for continuous analysis of threats. Users can block more attacks, track suspicious files, mitigate the scope of an outbreak, and remediate quickly. Mailbox Auto-Remediation for Office 365 customers helps remediate breaches faster and with less effort. Customers simply set their email security solution to take automatic actions on those infected emails. Customers can also purchase an additional license to deploy their AMP system completely on premises with the AMP private cloud. This, along with Threat Grid, brings the entire AMP offering completely on premises.
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	Web interaction tracking is a fully integrated solution that allows IT administrators to track the end users who click on URLs that have been rewritten by Cisco Email Security. 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 for sensitive content in outgoing emails	Cisco Email Security offers effective data loss prevention (DPL) and email encryption. Centralized management and reporting simplifies data protection. **Data Loss Prevention** Protect outbound messages with Cisco Email Security Data Loss Prevention (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 DLP policies are included with Cisco Email Security 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. 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. 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

Capability	Description
	encryption not as a mandate but as a service that's easy to use and gives the sender complete control. 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 Cisco Email Security to automate the protection of your most sensitive email content.
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 Cisco Email Security, 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.

Cisco Email Security Software Licenses

There are three email security software bundles: Cisco Email Security Inbound Essentials, Cisco Email Security Outbound Essentials, and Cisco Email Security Premium; add-on standalone options are also available (see Table 2). Just purchase the appropriate licenses for the number of mailboxes you need to support. For cloud and 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.

The major components of each software offering are provided in Table 2.

Table 2. Software Components

Bundles	Description
Cisco Email Security Inbound Essentials	The Cisco Email Security Inbound Essentials bundle delivers protection against email-based threats and includes antispam, graymail detection, Sophos antivirus solution, Outbreak Filters and Forged Email Detection.
Cisco Email Security Outbound Essentials	The Cisco Email Security Outbound Essentials bundle guards against data loss with DLP compliance and email encryption.
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 DLP and encryption.
Standalone Offerings	**Description**
Cisco Advanced Malware Protection and Cisco Threat Grid	Cisco Advanced Malware Protection (AMP) can be purchased along with any Cisco Email Security software bundle. Threat Grid and AMP augments the malware detection and blocking capabilities already offered in Cisco Email Security with file reputation scoring and blocking, sandboxing, and file retrospection for continuous analysis of threats, even after they have traversed the email gateway. Upon purchase you receive an unlimited license of Cisco Threat Grid. AMP and Threat Grid can now be deployed completely on premises with the Cisco AMP Private Cloud Virtual Appliance. 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 a policy, Lightweight Directory Access Protocol (LDAP) group level.

Software License Agreements

The Cisco End-User License Agreement is 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.

Where to Deploy

All Cisco Email Security deployments options 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 faster. 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.

Cloud

Cisco Email Security in the cloud provides you with a flexible deployment model for email security. It helps you reduce costs with co-management and no onsite email security infrastructure. Dedicated email security deployments in multiple resilient Cisco data centers provide the highest levels of service availability and data protection. Customers retain access to (and visibility of) the cloud infrastructure, and comprehensive reporting and message tracking helps assure administrative flexibility. This service is all-inclusive, with software, computing power, and support bundled for simplicity.

Virtual

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 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.

On-Premises

The Cisco 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.

Hybrid

The hybrid solution provides you with maximum flexibility. You can mix any deployment options to best suit your needs. For example, you can take advantage of Cisco Email Security in the cloud to protect against threats in incoming messages while deploying outbound control of sensitive messages onsite. You can also choose to deploy inbound threat protection on-premises and in the cloud to transition to the cloud at your own pace.

You can also run on-premises and virtual Cisco Email Security 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.

Cisco Email Security Specifications

Table 3 presents the performance specifications for Cisco Email Security while Table 4 presents the hardware specifications, and Table 5 presents the specifications for a virtual deployment. Table 6 presents specifications for the Secure Management Appliance M-Series Platform.

Table 3. Cisco Email Security 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	4.8 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, 2 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 4. Cisco Email Security 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 (930W)	Yes (930W)	Yes (930W)	No	Yes (930W)	No	No
Remote power cycling	Yes	Yes	Yes	Yes	Yes	Yes	No
Redundant power supply	Yes	Yes	Yes	Yes	Yes	Yes, accessory option	No
Hot-swappable hard disk	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Power Consumption	2216.5 BTU/hr	2216.5 BTU/hr	2216.5 BTU/hr	2626 BTU/hr	2216.5 BTU/hr	2626 BTU/hr	1364 BTU/hr
Power Supply	650W	650W	650W	770W	650W	770W	400W

Model	ESA C690	ESA C690X	ESA C680	ESA C390	ESA C380	ESA C190	ESA C170
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 2-port 1GBASE-SX Fiber: ESA-C690-1G 2-port 10GBASE-SR Fiber: ESA-C690-10G	Yes, separate SKUs 2-port 1GBASE-SX Fiber: ESA-C690-1G 2-port 10GBASE - SR Fiber: ESA-C690-10G	Yes, separate SKUs 2-port 1GBASE-SX Fiber: ESA-C680-1G 2-port 10GBASE - SR Fiber: ESA-C680-10G	No	No	No	No
HD Size	Four 600 GB hard disk drives (2.5" 10K SAS 4Kn) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	Eight 600 GB hard disk drives (2.5" 10K SAS 4Kn) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	Cisco C680 Email Security appliance includes six (6) 300 G HDDs	Two 600 GB hard disk drives (2.5" 10K SAS 4Kn) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	Cisco C380 Email Security appliance includes two (2) 600 G HDDs	Two 600 GB hard disk drives (2.5" 10K SAS 4Kn) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	250 GB, RAID 1
CPU	Two E5-2620 v3 processor	Two E5-2620 v3 processor	Two Intel Xeon E5-2620 Series processors (2.0 G, 6C)	One E5-2620 v3 processor	One Intel Xeon ES-2620 Series processors (2.0 G, 6C)	One E5-2609 v3 processor	1x2 (1 Dual Core)
RAM	Four 8GB DDR4-2133 DIMM1	Four 8GB DDR4-2133 DIMM1	Eight (8) 4 GB DDR3-1600-MHz RDIMM DRAM	Two 8GB DDR4-2133 DIMM1	Four (4) 4 GB DDR3-1600-MHz RDIMM DRAM	One 8GB DDR4-2133 DIMM1	4 GB

Table 5. Cisco Email Security Virtual 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 6. 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

How to Evaluate Cisco Email Security

- To try Cisco Email Security in the cloud, request a free 45-day trial at www.cisco.com/go/emailsecurity.

  To try our virtual appliance, go to https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.html#anc6 and follow the steps noted.

- To understand the benefits of the Cisco Email Security C-Series and X-Series appliances visit https://www.cisco.com/c/en/us/partners/sell-integrate-consult/promotions/try-buy-program.html for a 45-day trial.

Cisco Services

- **Advisory Services:** Our experts align risk, compliance, security, and threat management with your business goals.
- **Implementation Services:** With expertise and best practices working with thousands of customers across all industries around with the world, we'll help you more quickly realize and increase the benefits of your investment in advanced security solutions, including email security.
- **Managed Services:** Our expert investigators proactively monitor customer networks 24x7 from our global network of state-of-the-art security operations centers, providing constant vigilance and in-depth analysis as a comprehensive security solution.
- **Technical Services:** We provide proactive, pre-emptive technical services for hardware, software, multivendor solutions, and network environments. Our global team enhances IT operations, helping to ensure your IT works simply, consistently, and securely to keep your business running smoothly.

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 Cisco Emai Security. 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 https://www.cisco.com/c/en/us/services/technical/smart-net-total-care.html

Warranty information

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

For more information

More information about Cisco Email Security can be found at www.cisco.com/go/emailsecurity, where you can request a free 45-day trial.

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 C22-739910-00 10/17