Cisco Secure Email Advanced Email Protection

May 2021

Contents

The Cisco Secure Email Difference

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 multilayered approach to security.

Product overview

Cisco Secure Email 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 Secure Email 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 Secure Email Malware Defense 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.
- Prevent brand abuse and sophisticated identity-based email attacks with Cisco Secure Email Domain Protection and Cisco Secure Email Phishing Defense services.
- Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.
- Provide user behavior training with Cisco Secure Awareness Training to help users work smarter and safer.
- Maximize deployment flexibility with a cloud, virtual, on-premises, or hybrid deployment or move to the cloud in phases.
- Integrate across a growing number of Cisco Security products and accelerate key security operations functions like visibility, detection, automation, investigation, and remediation with SecureX.

Features and benefits

Today's email security threats consist of ransomware, advanced malware, BEC, phishing, and spam. Cisco Secure Email 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

Feature	Benefit
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.
Spam protection	Spam is a complex problem that demands a sophisticated solution. Cisco makes it easy. Cisco Secure Email blocks unwanted emails using a multilayered scanning architecture delivering the highest spam catch rate of greater than 99 percent, with a false-positive rate of a less than a one in one million. The antispam functionality in Cisco Secure Email 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 Secure Email stops the broadest range of threats with industry-leading accuracy.
Forged email detection	Forged email detection protects against BEC 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.
Cisco Secure Email Phishing Defense	CAPP stops identity deception–based attacks such as social engineering, imposters, and BEC by combining global Cisco Talos threat intelligence with local email intelligence and advanced machine learning techniques to model trusted email behavior on the Internet, within organizations and between individuals. • Integrates machine learning techniques to drive daily model updates, maintaining a real- time understanding of email behavior to stop identity deception. • Combines rapid Domain Message Authentication Reporting and Conformance (DMARC), advanced display name protection, and look-alike domain imposter–driven detection to stop BEC attacks. • Models account takeover threat behavior to block attacks originating from compromised email accounts. • Deploys as a lightweight sensor via the cloud or on-premises in the customer's environment as a hosted Virtual Machine (VM) of choice or bare-metal installs. Please refer to Table 7 for virtual machine hardware specifications. A cloud-based sensor is provisioned as part of Cisco Cloud Email Security deployment. • Supports dual-delivery mode. In this mode, the sensor accepts copies of email messages over Simple Mail Transfer Protocol (SMTP) and extracts metadata in a streaming fashion.

Feature	Benefit
Cisco Secure Email Domain Protection	CDP for external email helps prevent phishing emails from being sent using a customer domain(s). It automates the process of implementing the DMARC email authentication standard to better protect employees, customers, and suppliers from phishing attacks using a customer domain(s). This protects the customers' brand identity as well as increases email marketing effectiveness by reducing phishing messages from reaching inboxes.
Virus defense	By offering a high-performance virus scanning solution integrated at the gateway, Cisco Secure Email 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.
Malware Defense and Cisco Threat Grid	Malware Defense and 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. Cisco Secure Email also integrates with Malware Defense for Endpoints. Malware Defense for Endpoints shares threat intelligence across a customer's entire environment, unifying security across endpoints, network, email, the cloud, and the web. Through these integrations, Malware Defense automatically correlates files, telemetry data, behavior, and activity to proactively defend against advanced threats across all possible vectors. Mailbox Auto-Remediation for Microsoft 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 purchase an additional license to deploy their Malware Defense system completely on-premises with the Malware Defense private cloud. This, along with Threat Grid, brings the entire Malware Defense offering completely on-premises.
SecureX	Our architectural approach to integrated security products means effective threat intelligence sharing and more. SecureX threat response provides a faster, more synchronized response across the entire portfolio.
URL-related protection and control	Users are protected against malicious URLs with URL filtering, scanning of URLs in attachments, and managed (shortened) URLs. Appropriate policies are applied to the messages based on the reputation or category of the URLs.
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.

Feature	Benefit
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 Secure Email. 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 Secure Email offers effective DPL and email encryption. Centralized management and reporting simplifies data protection. **DLP** Protect outbound messages with Cisco Secure Email 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 Secure Email 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 encryption not as a mandate but as a service that's easy to use and gives the sender complete control.

Feature	Benefit
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 Secure Email, 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.
Secure Awareness Training	Provides flexibility and support to effectively deploy phishing simulations and awareness training, as well as measure and report results. It focuses on user behavior training to make long-term changes and empowers the security operations team with the ability to address real-time threats. **High-quality content** that includes a course builder with 150+ learning modules to choose from, role-based learning, and highly interactive content with gamification to keep users engaged. **Intuitive phishing simulator** that provides out-of-the-box phishing scenarios that reflect real-life cyber and phishing threats, which are integrated with training for just-in-time feedback. **Multilingual content and platform** with support for 40+ languages (narration and text) to make security awareness programs available globally. **Communications and reinforcement materials** provided by large libraries of predesigned content and templates for internal campaign promotion and content reinforcement (including videos, posters, and newsletters). **Consultative approach** with unique offerings, including CISO coaching, managed services, and content customization, to help organizations develop and optimize a security awareness strategy.

Cisco Secure Email Software Licenses

There are three email security software bundles: Cisco Secure Email Inbound Essentials, Cisco Secure Email Outbound Essentials, and Cisco Secure Email 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 Secure Email 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 Secure Email Inbound Essentials	The Cisco Secure Email Inbound Essentials bundle delivers protection against email-based threats and includes antispam, graymail detection, Sophos antivirus solution, outbreak filters, and forged email detection.
Microsoft 365 Cisco Secure Email Inbound Essentials	The Cisco Secure Email Inbound Essentials bundle delivers protection against email-based threats and includes antispam, graymail detection, outbreak filters, and forged email detection.
Cisco Secure Email Inbound Essentials plus Malware Defense and Cisco Threat Grid	The Cisco Secure Email Inbound Essentials bundle delivers protection against email-based threats and includes antispam, graymail detection, Sophos antivirus solution, outbreak filters, and forged email detection. Malware Defense can be purchased along with any Cisco Secure Email software bundle. Threat Grid and Malware Defense augments the malware detection and blocking capabilities already offered in Cisco Secure Email with file reputation scoring and blocking, sandboxing, and file retrospection for continuous analysis of threats, even after they have traversed the email gateway. Malware Defense and Threat Grid can now be deployed completely on-premises with Malware Defense Private Cloud Virtual Appliance. This is important for customers who have stringent policy requirements that do not allow for use of the Malware Defense public cloud.
Cisco Secure Email Outbound Essentials	The Cisco Secure Email Outbound Essentials bundle guards against data loss with DLP compliance and email encryption.
Cisco Secure Email Premium	The Cisco Secure Email Premium bundle combines the inbound and outbound protections included in the Cisco Secure Email Inbound and Outbound Essentials licenses noted above for protection against email-based threats and essential DLP and encryption.

Bundles	Description
Microsoft 365 Cisco Secure Email Premium	The Cisco Secure Email Premium bundle combines the inbound and outbound protections included in the Office 365 Cisco Secure Email Inbound and Cisco Secure Email Outbound Essentials licenses noted above for protection against email-based threats and essential DLP and encryption.
Cisco Secure Email Premium plus Malware Defense and Cisco Threat Grid	The Cisco Secure Email Premium bundle combines the inbound and outbound protections included in the Cisco Secure Email Inbound and Outbound Essentials licenses noted above for protection against email-based threats and essential DLP and encryption. Malware Defense can be purchased along with any Cisco Secure Email software bundle. Threat Grid and Malware Defense augment the malware detection and blocking capabilities already offered in Cisco Secure Email with file reputation scoring and blocking, sandboxing, and file retrospection for continuous analysis of threats, even after they have traversed the email gateway. Malware Defense and Threat Grid can now be deployed completely on-premises with Malware Defense Private Cloud Virtual Appliance. This is important for customers who have stringent policy requirements that do not allow for use of the Malware Defense public cloud.
Malware Defense and Cisco Threat Grid	Malware Defense can be purchased along with any Cisco Secure Email software bundle. Threat Grid and Malware Defense augments the malware detection and blocking capabilities already offered in Cisco Secure Email with file reputation scoring and blocking, sandboxing, and file retrospection for continuous analysis of threats, even after they have traversed the email gateway. Malware Defense and Threat Grid can now be deployed completely on-premises with Malware Defense Private Cloud Virtual Appliance. This is important for customers who have stringent policy requirements that do not allow for use of the Malware Defense public cloud.
Intelligent Multi-Scan	Intelligent Multi-Scan (IMS) is a high performant multi-layer anti-spam solution that uses a combination of anti-spam engines, including Cisco Anti-Spam, to increase spam catch rates. You cannot configure the order of the scanning engines used in Cisco Intelligent Multi-Scan; Cisco Anti-Spam will always be the last to scan a message and Cisco Intelligent Multi-Scan will not skip it if a third-party engine determines that a message is spam. Using Cisco Intelligent Multi-Scan can lead to reduced system throughput. Please contact your Cisco support representative for more information. To use the updated IMS engine, you must add the IMS feature key and accept the license in your appliance. For the existing IMS users, all the mail policies for IMS are migrated to work seamlessly with the updated IMS engine.
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.
Cisco Secure Email Phishing Defense	CAPP can be purchased along with any Cisco Secure Email software bundles. CAPP stops identity deception–based attacks such as social engineering, imposters, and BEC. It provides local email intelligence and advanced machine learning techniques to model trusted email behavior on the Internet, within organizations and between individuals. CAPP also integrates machine learning techniques to drive daily model updates, maintaining a real-time understanding of email behavior to stop identity deception. Offered only for one and three year subscriptions.

Bundles	Description
Cisco Secure Email Domain Protection	CDP can be purchased along with any Cisco Secure Email software bundle. CDP for external email helps prevent phishing emails from being sent using a customer domain(s). The CDP service automates the process of implementing the email authentication standard DMARC to better protect employees, customers, and suppliers from phishing attacks using a customer domain(s). This protects the customers' brand identity as well as increases email marketing effectiveness by reducing phishing messages from reaching inboxes. Offered only for one and three year subscriptions.
Image Analyzer	Detects illicit content in incoming and outgoing email, allowing customers to identify, monitor, and educate offending users.
McAfee AntiVirus	Offers McAfee antivirus scanning technology.
Cisco Secure Awareness Training	Cisco Secure Awareness Training can be purchased along with any Cisco Secure Email software bundles. It is designed to help promote and apply effective cybersecurity common sense by modifying end-user behavior and empower employees to work smarter and safer. This cloud-delivered subscription provides comprehensive simulation, training, and reporting so employee progress can be continually monitored and tracked. It helps organizations remain safe with engaging and relevant computer-based content with various simulated attack methods and empowers the people in your organization to play a critical role in its overall security with Cisco Secure Awareness Training.

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 Secure Email 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 unique user based, not device based, so you can apply it per unique user instead of per device to provide inbound as well as outbound email gateway protection at no additional cost.

Cloud

Cisco Secure Email 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 Secure Email 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 Secure Email 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 Secure Email Appliance is a gateway typically deployed in a network edge outside the firewall (the so-called demilitarized zone). Incoming 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 Secure Email 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 Secure Email 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 Secure Email and Web Manager or Cisco Secure Email and Web Manager Virtual.

Cisco Secure Email specifications

Table 3 presents the performance specifications for Cisco Secure Email 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 7 includes information on the virtual machine hardware requirements for the Cisco Secure Email Phishing Defense on-premises sensor deployment.

Table 3. Cisco Secure Email performance specifications

	Model	Disk Space	Raid Mirroring	Memory	CPUs
Large enterprise	ESA C695	4.8 TB (600 x 8)	Yes (RAID 10)	32 GB DDR4	1 x 2.6 GHz, 12 core
Large enterprise	ESA C690	2.4 TB (600 x 4)	Yes (RAID 10)	32 GB DDR4	2 x 2.4 GHz, 12 core
Medium-sized enterprise	ESA C395	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR4	1 x 2.1 GHz, 12 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

	Model	Disk Space	Raid Mirroring	Memory	CPUs
Small to midsize businesses or branch offices	ESA C195	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR4	1 x 2.1 GHz, 8 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

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 Secure Email Hardware specifications

Model	ESA C695	ESA C690	ESA C395	ESA C390	ESA C195	ESA C190
Rack Units (RU)	1RU	2RU	1RU	1RU	1RU	1RU
Dimensions including handles (H x W x D)	1.7 x 16.89 x 29.8 in. (4.32 x 43.0 x 75.6 cm)	3.4 in. x 19 in. x 29 in (8.6 x 48.3 x 73.7 cm)	1.7 x 16.89 x 29.8 in. (4.32 x 43.0 x 75.6 cm)	1.7 x 16.89 x 29.8 in. (4.32 x 43.0 x 75.6 cm)	1.7 x 16.89 x 29.8 in. (4.32 x 43.0 x 75.6 cm)	1.7 x 16.89 x 29.8 in. (4.32 x 43.0 x 75.6 cm)
DC power option	No	Yes (930W)	No	No	No	No
Remote power cycling	Yes	Yes	Yes	Yes	Yes	Yes
DC Power Option	No	Yes (930W)	No	No	No	No
Remote power cycling	Yes	Yes	Yes	Yes	Yes	Yes

Model	ESA C695	ESA C690	ESA C395	ESA C390	ESA C195	ESA C190
Redundant power supply	Yes	Yes	Yes	Yes	Yes, accessory option	Yes, accessory option
Hot-swappable hard disk	Yes	Yes	Yes	Yes	Yes	Yes
Power Consumption	2626 BTU/hr	2216.5 BTU/hr	2626 BTU/hr	2626 BTU/hr	2626 BTU/hr	2626 BTU/hr
Power Supply	770W	650W	770W	770W	770W	770W
Ethernet interfaces	6-port 1GBASE-T copper network interface (NIC), RJ-45	6-port 1GBASE-T copper network interface (NIC), RJ-45	6-port 1GBASE-T copper network interface (NIC), RJ-45	6-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, auto negotiate	10/100/1000, auto negotiate	10/100/1000, auto negotiate	10/100/1000, auto negotiate	10/100/1000, auto negotiate	10/100/1000, auto negotiate
Fiber option	Yes, separate SKU, 2-port 1GBASE-SX Fiber or 10GBASESR Fiber selectable upon ordering (modules included): ESA-C695F	Yes, separate SKUs, 2-port 1GBASE-SX Fiber: ESA-C690-1G 2-port 10GBASESR Fiber: ESAC690-10G	No	No	No	No
HD Size	Eight 600 GB hard disk drives (2.5” 12G SAS 10K RPM) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	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	Two 600 GB hard disk drives (2.5” 12G SAS 10K RPM) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	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	Two 600 GB hard disk drives (2.5” 12G SAS 10K RPM) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	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
CPU	One 2.6GHz 12c 2666MHz processor	Two E5-2620 v3 processor	One 2.1GHz 12c 2400MHz processor	One E5-2620 v3 processor	One 2.1GHz 8c 2400MHz processor	One E5-2609 v3 processor
RAM	Two 16GB DDR4-2666 DIMM1	Four 8GB DDR4-2133 DIMM1	One 16GB DDR4-2666 DIMM1	Two 8GB DDR4-2133 DIMM1	One 16GB DDR4-2666 DIMM1	One 8GB DDR4-2133 DIMM1

Table 5. Email Security Virtual Appliance specifications

	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 Cisco UCS	VMware ESXi 6.0 and 6.5 Hypervisor			

Table 6. Secure Management Appliance M-Series Platform specifications

Model	SMA M695/690	SMA M395/390	SMA M195/190
Number of unique users	10,000 or more	Up to 10,000	Up to 1000

Table 7. Virtual machine hardware requirements for Cisco Secure Email Phishing Defense on-premises sensor deployment

Operating system	CPU	Memory	Disk	Network	Docker
Modern, 64-bit Linux: • Red Hat Enterprise Linux 7.4 or later • CentOS 7.4 or later • Ubuntu 16 or later	Intel or AMD x 86_64 8 cores	16 GB minimum 32 GB Recommended	The following minimum allocations: • /var/opt/agari/: 100 GB • /opt/agari/: 20 GB • /var/lib/docker: 20 GB	1 Gbit/sec recommended	17.06 or later

How to evaluate Cisco Secure Email

- To try Cisco Secure Email in the cloud, request a free 45-day trial at https://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 Secure Email 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.
- 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 Secure Email. 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.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

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

2451451 05/21

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 **https://www.cisco.com/go/offices**.