The bridge to possible

Cisco Secure Email Gateway (Cloud and On-premises) and Cisco Secure Email and Web Manager

The bridge to possible

Contents

The bridge to possible

Cisco Secure Email

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 Secure Email Gateway 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.

Product overview

Cisco Secure Email Gateway 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 Gateway 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.
- Drop emails with malicious links 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.
- Integrate with Cisco Secure Email Threat Defense for advanced threat detection and protection.

With Cisco Secure Email and Web Manager customers can:

- Access centralized reporting, message tracking, and quarantine
- Streamline management efforts through unified dashboard.

Maximize deployment flexibility with a cloud, on-premises, or hybrid deployment or move to the cloud in phases.

Cisco XDR simplifies security operations, accelerates responses, and empowers Security Operations Center (SOC) teams with AI-driven and proactive threat detection and response. It is designed to address the challenges faced by security analysts and offers a cloud-native, extensible solution that brings data from multiple security tools, and applies machine learning and analytics to arrive at correlated detections. To learn more, visit cisco.com/go/xdr.

The bridge to possible

Cisco Secure Email Gateway (Cloud and On-Premises)

Today's email security threats consist of ransomware, advanced malware, BEC, phishing, and spam. Cisco Secure Email Gateway 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 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. Check out more.
Reputation filtering	Block unwanted email with reputation filtering, which is based on reputation database from Talos. Reputation service is curated for IP addresses, Domains, and Websites. Anything with known bad reputations can be automatically blocked. Reputation filtering stops most 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 Secure Email makes it easy. Cisco Secure Email Gateway 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 Gateway 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 Gateway stops the broadest range of threats with industry-leading accuracy.
Virus defense	By offering a high-performance virus scanning solution integrated at the gateway, Cisco Secure Email Gateway provides a multilayered, multivendor approach to virus filtering.

The bridge to possible

Feature	Benefit
Malware Defense (previously known as AMP and Threat Grid)	Cisco Secure Email Gateway comes with Malware Defense that provides protection from malicious email attachments sent by bad actors. Files are first checked against file reputation (SHA256 lookup) to prevent known malicious files. For new and suspicious files, the gateway can initiate a file analysis (sandboxing) that can provide detailed analysis of any file's behavior within minutes. In case new techniques emerge and new threat intelligence is gathered, with file retrospection alert, IT admins can be notified of change in disposition. With Mailbox Auto-Remediation (Microsoft 365 and Microsoft on-prem Exchange) the gateway is able to automatically remediate infected emails from a user's mailbox and prevent users from accessing the malicious attachments. With Password Protected File Analysis, Cisco Secure Email Gateway can analyze password protected files by extracting the password from the email body or by using an admin provided list of passwords to test. Customers can purchase an additional license to deploy their Malware Analytics system completely on-premises with the Cisco Secure Endpoint Private Cloud. This, along with Cisco Secure Malware Analytics appliance (Threat Grid), brings the entire Malware Analytics offering completely on-premises. See more
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 an 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.

Feature	Benefit
URL filtering and control	Users are protected against malicious URLs with URL filtering, scanning of URLs in emails and attachments. Appropriate policies are applied to the messages based on the reputation or category of the URLs. Cisco Secure Email Gateway also supports analysis of short URLs and open redirect URLs. Rewriting URLs provides click-time-protection for URLs that were benign during initial scan. But with URL retrospection alert, Cisco Secure Email Gateway can utilize Mailbox Auto-Remediation (Microsoft 365 and Microsoft on-prem Exchange) to remediate the emails automatically from end users' mailboxes.
External Threat Feeds	In addition to Cisco Talos, Cisco Secure Email Gateway can pull additional threat intelligence from an external source utilizing STIX over TAXII protocol.
File handling and Macro Detection	Cisco Secure Email Gateway can help protect customers from unwanted email attachment file types and content. Using file metadata analysis, the gateway can precisely recognize file type as well as embedded macro scripts (Microsoft, Adobe, or OLE type macros). With Safe Print action, Cisco Secure Email Gateway can transform an attachment into pdf with original content as a screenshot.
Outbreak filters	Outbreak filters defend against emerging and viral threats, most of which are phishing and scams campaigns. Talos manages an Outbreak ruleset for Cisco Secure Email Gateway to help get a lead time on zero-day phishing and viruses. Outbreak filters can also rewrite URLs linked in suspicious messages. When clicked, the new URLs redirect the recipient through the Cisco Security proxy that would display a block page if site is (on the time of the click) malicious or take a screenshot of the website if it is suspicious. User can choose to be redirected to the web page if they feel it is safe to do so.
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 Gateway. 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.

The bridge to possible

Feature	Benefit
Data security for sensitive content in outgoing emails	Cisco Secure Email offers effective Data Loss Prevention and email end-to-end encryption. **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 library of templates with nearly 200 prebuilt policies covering government, private sector, and company-specific regulations. The predefined DLP policies are included with Cisco Secure Email Gateway 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. Offer encryption not as a mandate but as a service that's easy to use and gives the sender complete control.
Threat Defense Connector	To improve detection of advanced level email attacks, Cisco Secure Email Gateway can integrate with Cisco Secure Email Threat Defense using Threat Defense Connector. Email Threat Defense uses AI/ML based scanning engines to detect malicious emails that might bypass the gateway.

The bridge to possible

Cisco Secure Email and Web Manager

With Secure Email and Web Manager, you can manage updates and settings centrally rather than on the individual appliances. Message tracking aggregates data from multiple Cisco Secure Email Gateways, including data categorized by sender, recipient, message subject, and other parameters. Scanning results, such as spam and virus verdicts, are also displayed, as are policy violations. It also:

- Tracks and reports on message disposition, URLs, and other email attributes.
- Consolidates email security quarantines into a single repository.
- Includes antispam, antivirus, Outbreak Filters, policy quarantines, and more.
- By centralizing the management of multiple appliances, administrators can enforce consistent acceptable use policies across the organization.

Note: While it is not mandatory to deploy Cisco Secure Email and Web Manager, it makes management easier, faster, and more efficient.

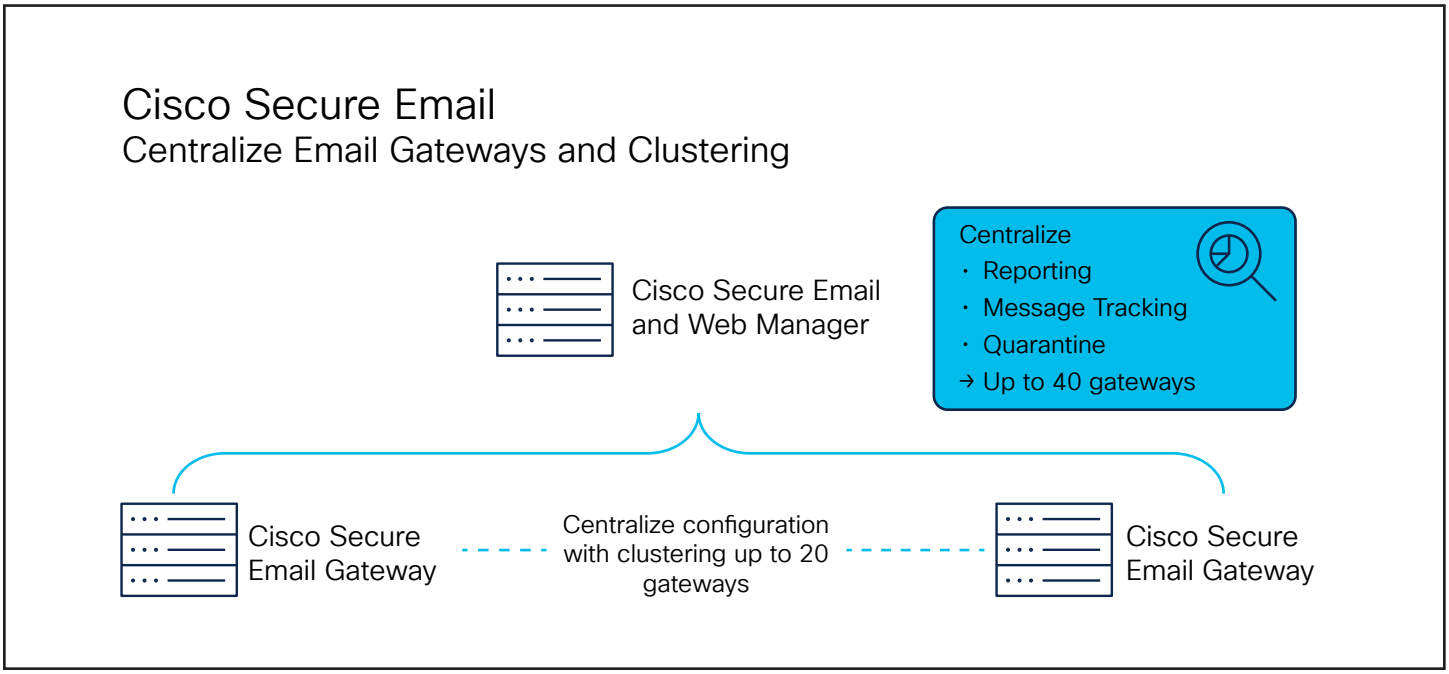


Table 2. Main capabilities

Feature	Benefit
Centralized reporting	The Secure Email and Web Manager simplifies administration by fully integrating reporting from multiple Cisco Secure Email Gateways to be consolidated.
Message tracking	Data is aggregated from multiple Cisco Secure Email Gateways, including data categorized by sender, recipient, message subject, and other parameters. Scanning results display detailed scanning results from each security check and action taken according to policy and configuration.
Spam quarantine	Spam messages can be stored centrally with the easy-to-use self-service Cisco Spam Quarantine solution. Large enterprises with multiple Cisco Secure Email Gateways can offload their spam traffic to one location for easier tracking and provide a single point for employee access.
Policy quarantine	Suspicious and policy violating messages can be stored centrally for admin view and management. Messages can be viewed safely from the dashboard and actioned according to an admin's decision. Multiple Cisco Secure Email Gateways can offload their policy quarantined emails to one single point for admin access.

Cisco Secure Email Software Licenses

There are three email security software bundles: Essentials, Advantage, and Premier; add-on standalone options are also available (see Table 3). Just purchase the appropriate licenses for the number of mailboxes you need to support.

There are three different deployment options for licenses: Cloud, On-Prem, and Hybrid. Each deployment option will give entitlements to run the solution in its respective platform:

- Cloud – Cisco hosted
- On-Prem – Virtual Machines
- Hybrid – Cisco hosted + Virtual Machines.

Comparison of license bundles and add-ons click here.

The bridge to possible

Term and Quantity based Subscription Licenses

Licenses are term-based subscriptions of 1, 3, or 5 years.

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.

For Cisco Partners, please refer to the Ordering guide for more details.

The major components of each software offering are provided in Table 3.

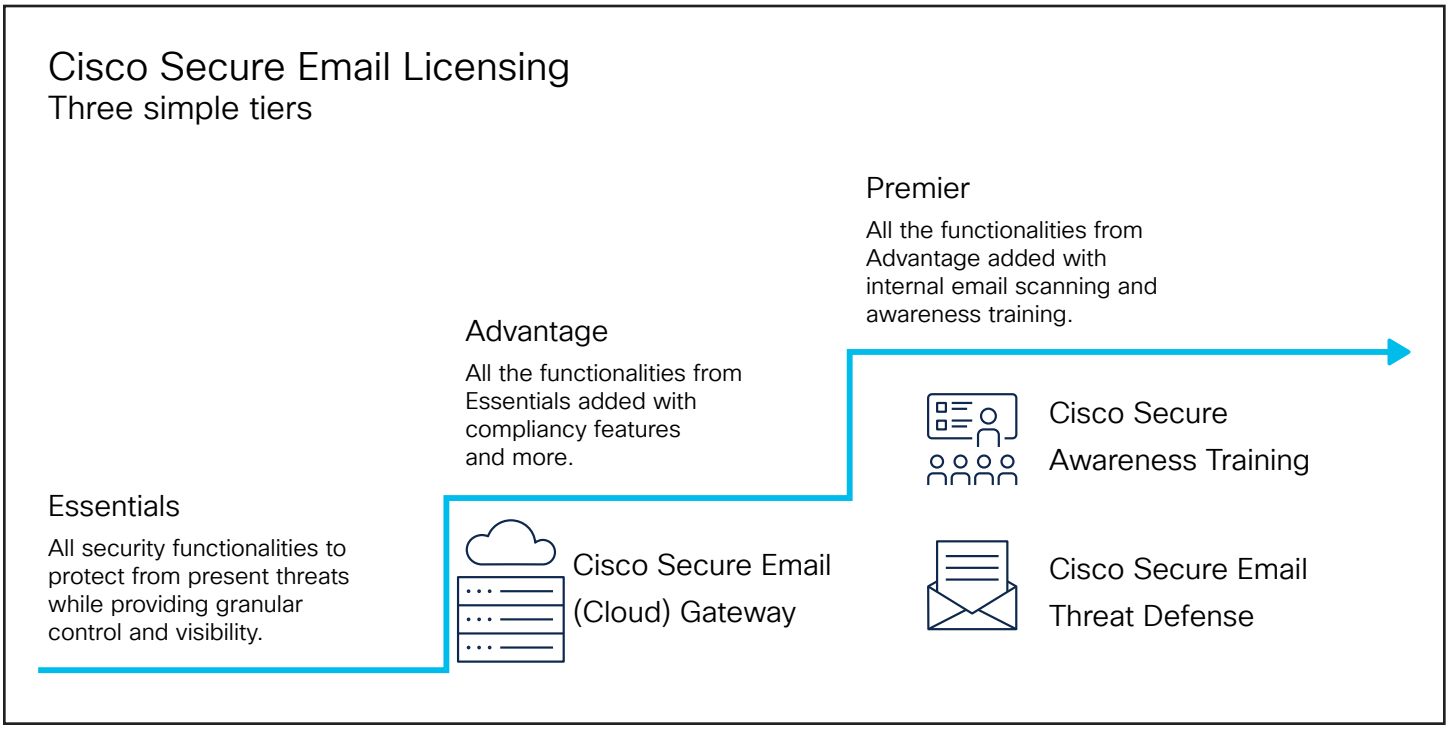


Table 3. Software components

Bundles	Description
Essentials	The Cisco Secure Email Essentials bundle delivers protection against email-based threats and includes Antispam, Sophos antivirus, Malware Defense, Graymail detection, and outbreak filters. Malware Defense includes sandboxing with Malware Analytics solution (formerly Threat Grid) with a limitation on how many files per day are sandboxed.
Advantage	The Cisco Secure Email Advantage bundle includes all features from Essentials plus Data Loss Prevention, Envelope Encryption, and Safe Unsubscribe features. In this bundle Malware Analytics does not have file submission limitation (unlimited).
Premier	The Cisco Secure Email Premier bundle combines three products: • Cisco Secure Email Gateway Advantage bundle • Cisco Secure Email Threat Defense • Cisco Secure Awareness Training

Add-ons	Description
Security Management Appliance (SMA)	The Cisco Secure Email Manager feature allows administrators to centrally report and search messages and quarantines across multiple email gateways at the same time. This add on is only available for on-premises gateway bundles. For cloud gateway bundles, Cisco Secure Cloud Email Manager is included always.
Image Analyzer	Detects illicit content in incoming and outgoing email, allowing customers to identify, monitor, and educate offending users.
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 level.
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.

Add-ons	Description
McAfee Antivirus	Offers McAfee antivirus scanning technology.
Data Loss Prevention	Enables detection of sensitive data in the outbound traffic and various actions based on severity.
Encryption	License to activate Cisco Secure Email Encryption service. This service will provide an option to fully encrypt end-to-end emails that are sensitive.
Secure Email Threat Defense	To improve detection with AI/ML-based engines and for Microsoft 365 customers, internal traffic visibility and protection.

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 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.

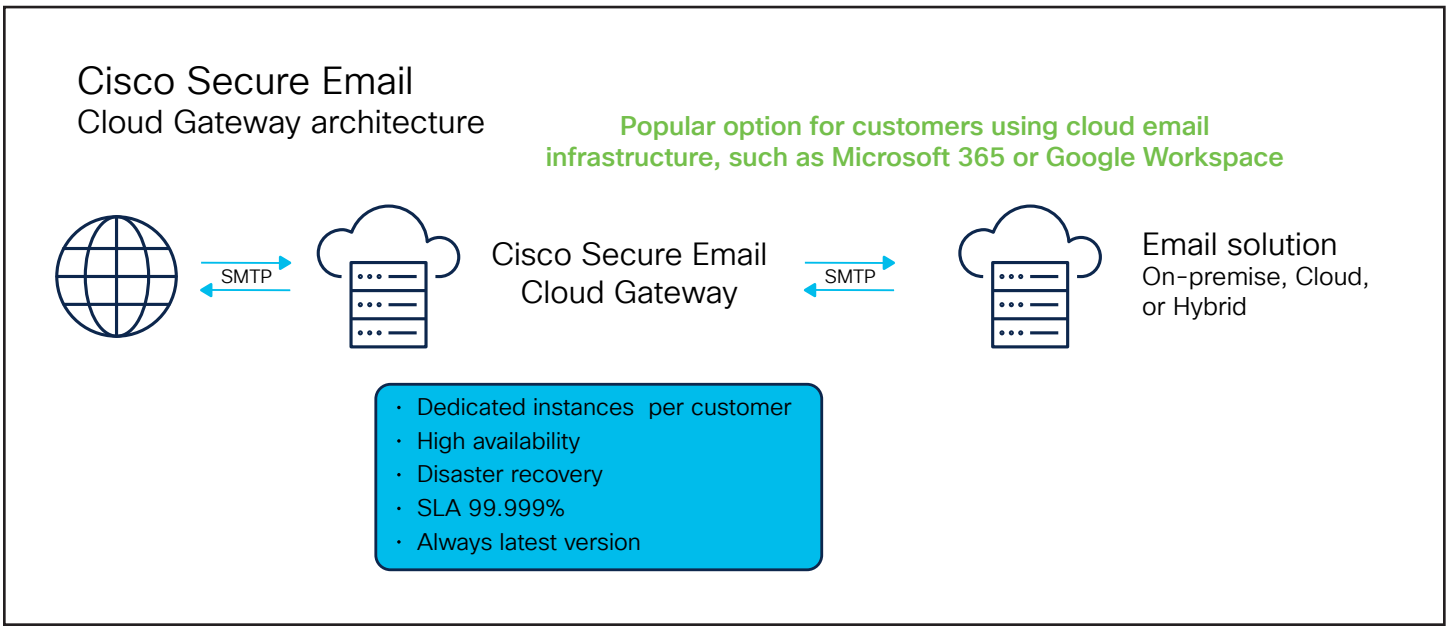
Where to deploy

All Cisco Secure Email deployment 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 and 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.

The bridge to possible

Cloud

Cisco Secure Email Cloud Gateway 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.

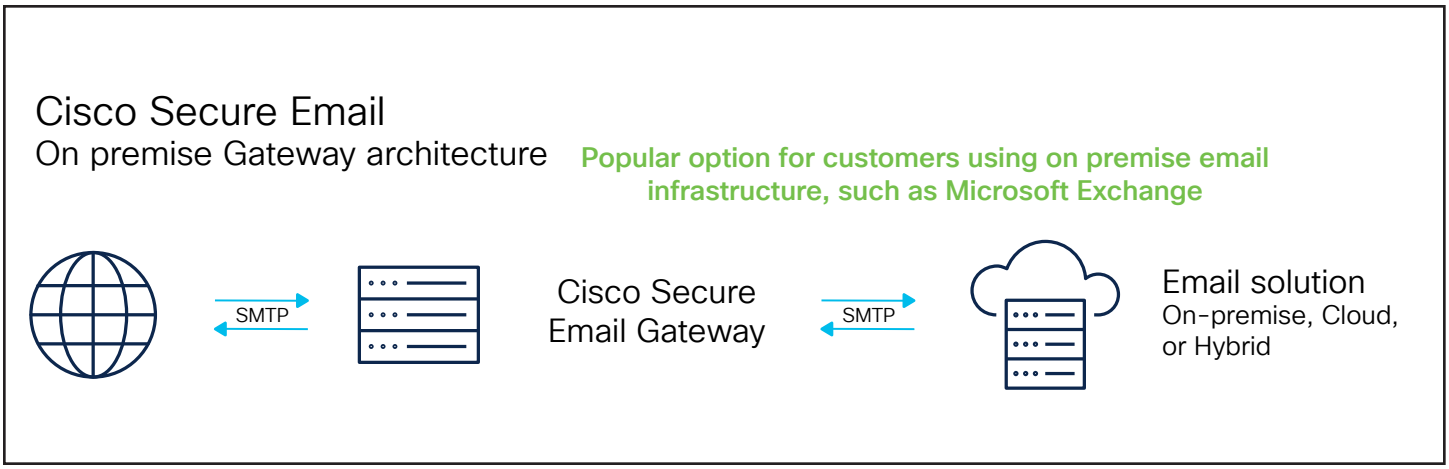


On-Premises – Virtual Machine

The Cisco Secure Email Gateway and Cisco Secure Email and Web Manager virtual appliances 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. Virtual appliances are supported with various hypervisors such as VMware ESXi, Microsoft Hyper-V, Red Hat Virtualization, Amazon AWS, and Microsoft Azure. You receive an unlimited license for the virtual appliance with the purchase of any Cisco Secure Email software core bundles (essentials, advantage, and premier).

With the virtual appliance, you can respond instantly to increasing traffic growth with simplified capacity planning.

The bridge to possible



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 Gateway 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.

Cisco Secure Email specifications

Cisco Secure Email Cloud Gateway is sized automatically based on user license purchased. More details and documentation about Cloud Gateway is available here: https://docs.ces.cisco.com/docs/ces-reference-docs.

Tables 3, 4, and 5 represent the requirements for virtual deployments for different hypervisors and cloud platforms. For accurate sizing, verify your choice by checking with a Cisco content security specialist.

For Cisco Partners, please refer to the Sizing tool for initial sizing specifications.

Please refer for more details on virtual deployments here:

- Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual Appliance Installation Guide.
- Deploying Cisco Secure Email Gateway and Secure Email and Web Manager Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services.
- Deploying Cisco Secure Email Virtual Gateway and Cisco Secure Email and Web Manager Virtual on Microsoft Azure Cloud Platform.

Table 4. Email Security Virtual Appliance requirements for VMware ESXi, Hyper V, and KVM.

Product	Model	Disk	Memory	Cores
Cisco Secure Email Virtual Gateway	C100v*	200 GB	8 GB	2
	C300v*	500 GB	16 GB	4
	C600v	500 GB	16 GB	8
Cisco Secure Email and Web Manager Virtual	M100v*	250 GB	6 to 8 GB	2
	M300v*	1TB	8 to 16 GB	4
	M600v	2TB	16 GB	8

* Only available for VMware ESXi.

Table 5. Email Security Virtual Appliance requirements for Amazon AWS.

Product	Model	Disk	vRAM	vCPU	EC2 instance types
Cisco Secure Email Virtual Gateway	C600v	500 GB	30 GB	16	c4.4xlarge
Cisco Secure Email and Web Manager Virtual	M600v	2TB	15 GB	8	c4.2xlarge

Table 6. Email Security Virtual Appliance requirements for Microsoft Azure.

Product	Model	Disk	Memory	vCPU	Azure VM Size
Cisco Secure Email Virtual Gateway	C600v	500 GB	32 GB	8	Standard D8s v3
Cisco Secure Email and Web Manager Virtual	M600v	1TB	32 GB	8	Standard D8s v3

The bridge to possible

How to evaluate Cisco Secure Email Gateway

- To try our virtual appliance, go to this page and follow the steps noted.
- To try Cisco Secure Email Cloud Gateway, reach out to your Cisco account team or partner to initiate a free 45-day evaluation.

Cisco Security 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.

Learn more

More information about Cisco Secure Email can be found at https://www.cisco.com/go/emailsecurity.

C78-742868-06 06/24