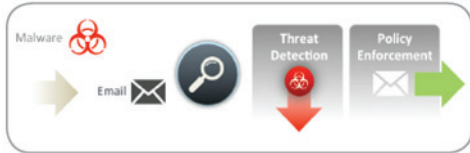# Cisco Email Security Appliances

What Is the Value of Cisco Email Security Appliances?

Email communication is critical to today's businesses— and downtime or compromised email can impact the bottom line. Cisco® Email Security, with content-aware, policy-based data loss prevention (DLP) and encryption, helps businesses detect and manage risks in both inbound and outbound email.

Figure 1. Cisco Email Enforces DLP and Encryption Policy Security While Defending Against Advanced Threats

What Problems Does Cisco Email Security Solve?

Email, while vital to doing business, exposes organizations to an ongoing stream of rapidly evolving and increasingly sophisticated threats, including emerging IPv6 challenges and targeted attacks such as spearphishing and advanced persistent threats (APTs). And as email systems are stretched to handle new architectures, compliance issues, and mobile trends such as "bring your own device" (BYOD) initiatives, policy enforcement for outbound traffic has become increasingly important.

What Models Are Available?

Cisco X-Series and C-Series Email Security Appliances come ready to plug in and install in the right size for your environment. The appliances are built on the same comprehensive platform that protects email infrastructures of major Forbes Global 2000 companies. Regardless of the model you choose, Cisco provides high-availability email protection against the constant, dynamic, rapidly changing threats affecting email today.

- **Cisco X1070**—The Cisco X1070 delivers high-performance, comprehensive security at the network gateway for service providers and large-scale enterprise email systems.
- **Cisco C670**—Made for midsize organizations, the Cisco C670 offers the same email security features and functionality as the Cisco X1070.
- **Cisco C370**—This model is built to meet email security needs for small-to-midsize companies and branches with 1000 to 10,000 users.
- **Cisco C370D**—For outbound delivery, the Cisco C370D provides optimum email deliverability with identity and reputation protection, delivering up to 800,000 messages per hour for authenticated email, investor updates, and marketing newsletters.
- **Cisco C170**—The Cisco C170 provides cost-effective email security designed for small businesses, branch offices, and organizations with fewer than 2000 users.

The Right Security Services for Your Needs

Cisco Email Security is a full solution that includes threat protection capability to help eliminate a diverse range of known and emerging email threats, featuring high-performance virus scanning, outbreak filters, advanced anti-spam techniques, and innovative context-sensitive detection technology, encryption, and DLP.

Security Software Subscription Offerings	Descrption
Cisco Email Security Inbound	Protects an organization's mailboxes against spam, viruses, and targeted attacks. **(Outbreak Filters + Anti-Virus + Anti-Spam)**
Cisco Email Security Outbound	Helps satisfy compliance requirements by providing easy-to-use encryption and DLP solutions. **(DLP + Encryption)**
Cisco Email Security Premium	Combines inbound and outbound protection to provide a complete email security solution. **(Inbound + Outbound)**
A La Carte	Provides the option to chose individual features like alternate anti-virus and anti-spam technologies on top of standard inbound or outbound offerings

Models	Cisco X1070	Cisco C670	Cisco C370*	Cisco C170
Image				
Usage Scenario				
Number of users (mailboxes) per appliance**	Up to 20,000	10,000+	Up to 10,000	Up to 2000
Clustering	Yes	Yes	Yes	Yes
Chassis				
Form factor	2 RU	2 RU	2 RU	1 RU
Dimensions (H x W x D)	3.5 in. x 17.5 in. x 26.8 in. (8.9 x 44.5 x 68.1 cm)	3.5 in. x 17.5 in. x 26.8 in. (8.9 x 44.5 x 68.1 cm)	3.5 in. x 17.5 in. x 26.8 in. (8.9 x 44.5 x 68.1 cm)	1.67 in. x 16.9 in. x 15.5 in. (4.24 x 42.9 x 39.4 cm)
Total weight (lbs.)	57.5	52.2	49	26.96
Power supply	870W, 100/240V	870W, 100/240V	870W, 100/240V	400W, 100/240V
Processor, Memory, and Disks				
CPUs	2x4 (2 quad cores)	2x4 (2 quad cores)	1x4 (1 quad core)	1x2 (1 dual core)
Memory	4 GB	4 GB	4 GB	4 GB
Disk space and count	1.8 TB (300 * 6)	1.2 TB (300 * 4)	600 GB (300 * 2)	500 GB (250 * 2)
RAID level and controller	RAID 10, hardware	RAID 10, hardware	RAID 1, hardware	RAID 1, hardware

* The Cisco C370D is another version of this model that provides maximum email deliverability with identity and reputation protection, delivering up to 800,000 messages per hour for authenticated email, investor updates, and marketing newsletters.

** Please confirm sizing guidance with a Cisco content security specialist to ensure your solution will meet your current and projected future needs.

CISCO

Cisco Email Security Appliance: FAQs

Q. How Easy Are the Appliances to Install?

A. The System Setup Wizard starts automatically when you first log in using the web-based interface to guide you through the process. Appliances install at the perimeter, so you assign at least one IP address that can access the Internet. Depending on your network configuration, your firewall may need to be configured to allow access. An optional Active Directory Wizard is available to configure an LDAP server profile.

Q. Are the Appliances Easy to Manage?

A. The Email Security Monitor and Centralized Management features a System Overview that serves as a system dashboard, providing details about the appliance including system and work queue status, quarantine status, and outbreak activity. An intuitive web-based interface simplifies daily operations.

Q. Is reporting and message tracking available?

A. Yes. The Cisco Security Management Appliance has centralized reporting and runtime data for message tracking in a single management interface for Cisco Email and Web Security Appliances.

Q. How Does Cisco Registered Envelope Service Work?

A. Cisco Registered Envelope Service (CRES) helps companies secure their email communications. This service allows businesses to send encrypted messages via registered "envelopes"—encrypted emails that also may be password-protected.

The Cisco Email Security Appliance Advantage

Cisco Email Security allows organizations to accelerate their business safely and inspire more productive communities within their organization. Users can communicate more quickly and safely exchange information, which helps to enhance collaboration and innovation.

Getting the Most from Your Cisco Network

The best way to enhance the investment in Cisco data centers, networks, and branches is by making security integral to your network architecture. When email is a critical part of your operations, make sure it's secure. Cisco Email Security provides best-in-class protection against the widest variety of email threats—and Gartner named it the leading Secure Email Gateway.

Why Cisco Security?

Security is more critical to your network than ever before. As threats and risks persist, security is necessary for providing business continuity, protecting valuable information, maintaining brand reputation, and adopting new technology. A secure network enables your employees to embrace mobility and securely connect to the right information. It also allows your customers and partners to conduct business with you more easily.

No organization understands network security like Cisco. Our market leadership, unmatched threat protection and prevention, innovative products, and longevity make us the right vendor for your security needs.

Where Should I Go for More Information?

The best way to understand the benefits of Cisco Email Security products is to participate in the Try Before You Buy program. To receive a fully functional evaluation appliance to test in your network, free for 30 days, visit www.cisco.com/go/esa.