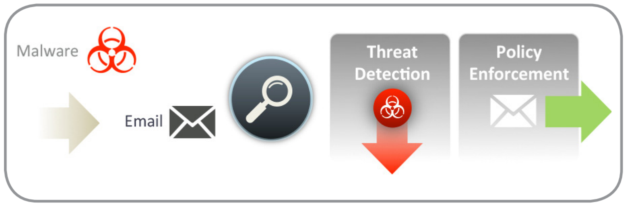
Cisco Email Security

What Is the Value of Cisco Email Security?

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, so they can accelerate their business safely and inspire more productive user communities. This industry-leading solution, like all Cisco security products, is powered by Cisco Security Intelligence Operations (SIO), a cloud-based service for threat defense.

Figure 1. Cisco Email Security Defends Against Advanced Threats While Enforcing DLP and Encryption Policy



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 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, outbound traffic has become a more frequent avenue of vulnerability for organizations since organizations may have difficulty enforcing email policy on smartphones and other personal mobile devices.

With Cisco Email Security, organizations have a simple but powerful way to continually monitor for threats and help users to comply with acceptable use and DLP policies. Available in multiple form factors–from appliances to the cloud–and providing support for mobile, BYOD, and IPv6, Cisco Email Security helps organizations stay ahead of market transitions and gives them the flexibility to better protect users wherever they are and however they are accessing email.

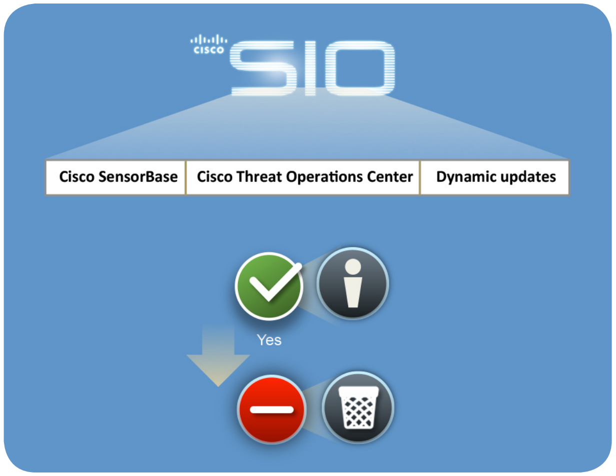
The Best Email Security–Inbound and Outbound

Cisco Email Security is based on the same technology that protects 50 percent of the Fortune 1000, more than 20 percent of the world's largest enterprises, and eight of the 10 largest ISPs. Regardless of deployment method, Cisco Email Security delivers unmatched threat protection for both inbound and outbound traffic.

Unmatched Malware Prevention

Cisco Email Security uses information collected from Cisco SIO, which sees 35 percent of the world's email traffic and 75 TB of web data per day.

Figure 2. Leverage Cisco Security Intelligence Operations' Zero-Day Architecture



Cisco Email Security works in conjunction with Cisco Outbreak Filters, the latest email security innovation for next-generation threat prevention for hard-to-detect threats. Cisco provides the industry's first custom-built engine dedicated to blocking targeted attacks utilizing three major elements: targeted attack heuristics, dynamic quarantine, and cloud web redirect.

Cisco Outbreak Filters scan URLs embedded in emails before they get to users, mitigating damage from infected links. Cisco Outbreak Filters deliver effective outbreak prevention by bridging the gap between the time that a new outbreak occurs and when its anti-malware signature is available, helping organizations to potentially avoid loss or destruction of data.

Cisco Email Security offers multiple anti-malware and anti-spam scanning engines from Sophos, McAfee, and Cloudmark. Administrators can run these scanning engines to enable greater protection against malware threats–with little to no performance degradation.

Flexible Deployment–Appliance to the Cloud

For organizations that require sensitive data to remain physically on-premise and are especially concerned about the risk of performance degradation, dedicated, easy-to-manage Cisco Email Security Appliances are appropriately sized to plug into your environment.

Table 1. Cisco Appliances Are Appropriately Sized For Your Environment

Models	Cisco X1070	Cisco C670	Cisco C370	Cisco C170
Number of users (mailboxes)*	<20,000	10,000+	<10,000	<2000
Clustering	Yes	Yes	Yes	Yes

*When determining sizing, please work with a Cisco content security specialist to consider peak mail flow rates and average message size so that your solution will meet your current and projected future needs.

Organizations that need to reduce their onsite data footprint and total cost of ownership can utilize the Cisco cloud infrastructure, which provides a flexible deployment model for anytime, anywhere email security. The Cisco cloud infrastructure is built on high-availability and high-performance data centers spread throughout the globe. This infrastructure has a proven track record for availability, and provides visibility and security without the need for on-premise devices.

The Right Security Services for Your Needs

Cisco Email Security is a full solution with comprehensive threat protection capability–including encryption and precision DLP–across multiple form factors for inbound and outbound enterprise management and reporting. To help eliminate a diverse range of known and emerging email threats, Cisco Email Security also features industry-leading, high-performance virus scanning, as well as conventional antispam techniques and innovative context-sensitive detection technology.

Table 2. Inbond And Outbound Software Subscriptions Offer Flexible Options For Defense

Security Software Subscription Offerings	Description
Cisco Email Security Inbound	Protects an organization's mailboxes against spam, viruses, and targeted attacks. **(Outbreak Filters + Antivirus + Antispam)**
Cisco Email Security Outbound	Helps satisfy compliance requirements by providing easy-to-use encryption and data loss prevention solutions. **(Data Loss Prevention + Encryption)**
Cisco Email Security Premium	Combines inbound and outbound protection to provide a complete email security solution. **(Inbound + Outbound)**

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 your 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 placed Cisco in the Leader quadrant for Secure Email Gateway.

Why Cisco?

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 to test in your network, free for 30 days, visit http://www.cisco.com/go/esa.

Cisco Email Security: FAQs

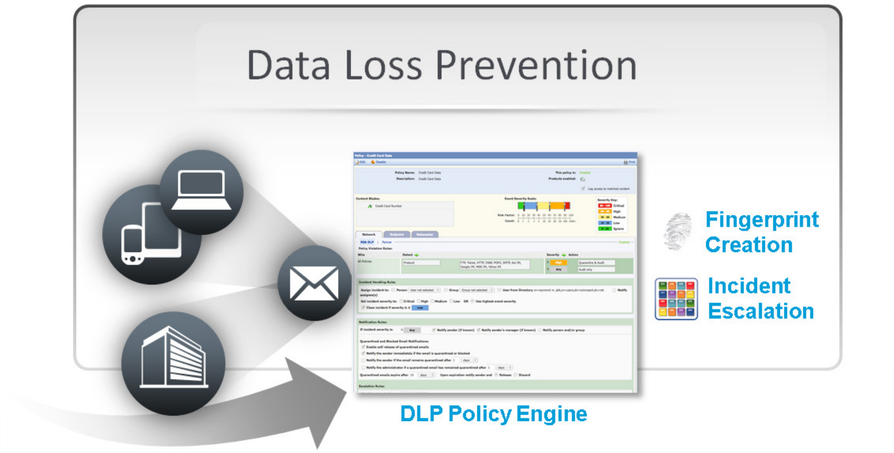
Q. Is reporting and message tracking available with Cisco Email Security?

A. Yes. The Cisco Content 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 DLP work?

A. DLP filters simplify the application of content-aware outbound email policy as part of an overall DLP architecture from RSA. Cisco is working with partners like RSA to form a leading DLP ecosystem that establishes a common classification and policy management platform across enterprises. Cisco has been incorporating RSA DLP technology into its email security solutions since 2009, providing customers with comprehensive global regulatory compliance coverage; best-in-class accuracy for identifying sensitive, data-comprehensive remediation options, including universal message-based encryption; and comprehensive remediation options.

Figure 3. Consistent enforcement of email DLP policy



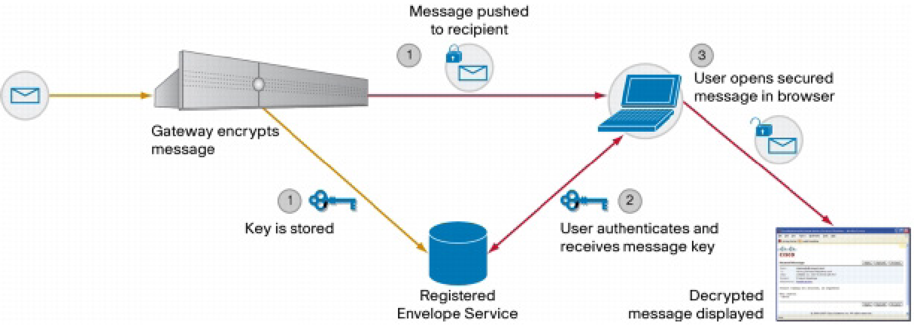
Q. How does Cisco Registered Envelope Service work?

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.

Q. How does Cisco Business-Class Email work?

A. Business-Class Email is a free mobile app that customers can download to their smartphones and use with the Cisco Email Security Outbound bundle with encryption services. Customers experience end-to-end encryption all the way to the inbox on their mobile phones. Cisco Business-Class Email removes the complexity of encryption and key management, enabling users to send and receive secure messages easily. It also changes the sender's experience by providing more control, including read receipts, email recall, email expiration, and control over forward/reply capabilities.

Figure 4. Cisco Encryption Business-Class Email Path


Message pushed to recipient
1
Gateway encrypts message
1
Key is stored
Registered Envelope Service
3
User opens secured message in browser
2
User authenticates and receives message key
Decrypted message displayed