At-a-Glance

Cisco Cloud Email Security

What Is the Value of Cisco Cloud Email Security?

Cisco® Cloud Email Security provides cloud-based email protection, helping organizations reduce their onsite data center footprint and reduce costs. The solution is built on the same comprehensive platform that protects the email infrastructure for 40 percent of the Fortune 1000 and eight of the 10 largest ISPs. Microsoft Office 365 customers can also get the same industry-leading protection with Cloud Email Security for Office 365.

How Is the Cisco Cloud Offering Unique?

Cisco Cloud Email Security delivers several differentiating cloud features:

- **Dedicated cloud infrastructure:** Each cloud customer has a dedicated email security instance, which is hosted in multiple Cisco data centers.
- **Cloud capacity assurance:** Users are protected, and peak performance is maintained, regardless of whether spam volumes increase. Additional capacity is always included with a simple per-user, per-year pricing model.
- **Cloud availability guarantee:** Cisco Cloud Email Security guarantees 99.999 percent uptime, so security is always available and working for you through multiple data centers. Cisco has multiple cloud data centers worldwide.

What Problems Does Cisco Cloud Email Security Help Solve?

Cloud Email Security monitors and filters all inbound and outbound email traffic using effective policy-based data loss prevention and encryption. Its sophisticated filter strategy blocks targeted attacks using reputation, malware, and outbreak filters.

Cisco Talos

Cloud Email Security uses the power of Cisco Security Talos, the largest threat detection network in the world, to provide proven, zero-day threat protection to all users wherever they are. It monitors and detects threats from:

- More than 75 TB of web data per day
- More than 1.6 million deployed devices
- More than 150 million endpoints
- More than 13 billion web requests per day
- More than 35 percent of the world's email traffic

Why Is Email Security So Challenging for Today's Enterprises?

Targeted attacks use social engineering that can trick even the most discriminating user into opening an email and clicking a malicious link. Email is a platform for known and emerging threats such as:

- Blended attacks that use web links to phishing sites
- Advanced malware that is difficult to detect
- Highly targeted attacks using social engineering
- Insider threats and outbound attacks that put intellectual property and customer assets at risk

The Email User Evolution

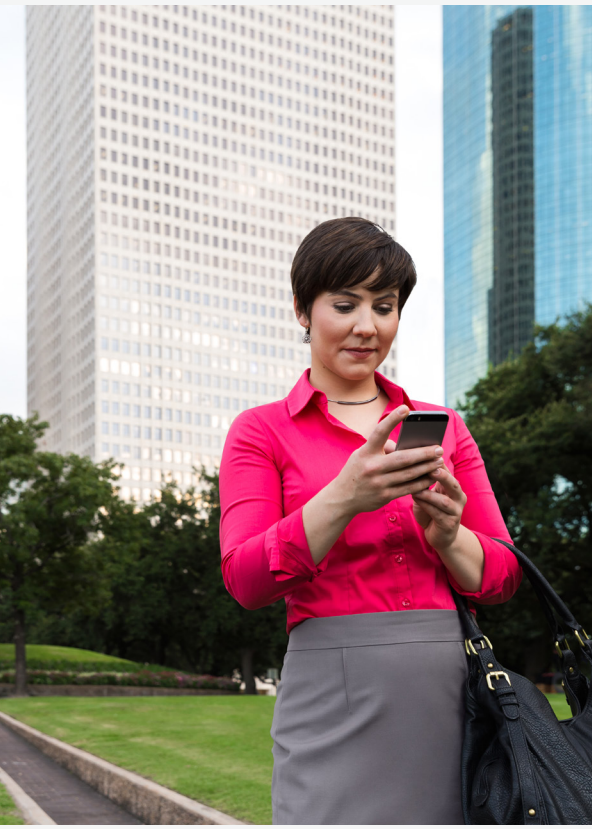
Another challenge to email security is that today's users are not checking text-based messages from a workstation behind the company firewall. Instead, they are accessing rich HTML email through multiple devices—anytime, anywhere—and not always through company-supported devices. According to Cisco's Connected World Technology Report, three in every four employees around the world have multiple devices, and many of these workers use more than one device for work.

The adoption of cloud-based hosted email solutions increases the need for advanced protections not provided by consumer-oriented, one-size-fits-all security. These hosted mailboxes need the security features provided by Cisco solutions.

What Are the Deployment Options for Cisco Cloud Email Security?

Cisco Cloud Email Security: This is a cloud-based software-as-a service (SaaS) offering that requires no onsite hardware because it resides in highly secure Cisco data centers. For organizations that require sensitive data to remain on premises and are especially concerned about the risk of performance degradation, Cisco offers additional solutions.

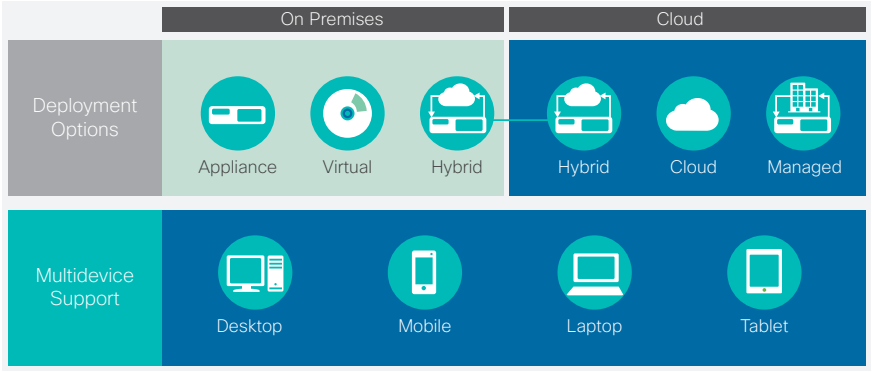
Cisco Hybrid Email Security: This service bundles features for the on-premises and cloud deployments of email security. It divides control between your organization's site and Cisco's cloud-based SaaS offering. Like Cisco Cloud Email Security, the hybrid service provides dedicated email security instances in Cisco data centers, but you retain access to, and visibility into, both on-premises and cloud infrastructures. On-premises appliances add the ability to deliver advanced outbound control with encryption, data loss prevention, and onsite Lightweight Directory Access Protocol (LDAP) integration. In addition, if you are transitioning from on-premises to the cloud, you can do so in phases. You can change the number of on-premises versus cloud users at any time throughout the term of their contract, assuming the total number of users does not change. This provides deployment flexibility as your organization's needs change.



Cisco Managed Email Security: This customized email service stops spam and viruses to help secure the email infrastructure while reducing the burden on IT. It uses a combination of high-performance appliances and expert monitoring and management to comprehensively protect complex email infrastructures. Designed to flexibly manage a growing email infrastructure, Cisco Managed Email Security features a structured implementation model with well-defined phases: evaluation, system design, system implementation, service activation, and product implementation.

Figure 1 illustrates these deployment options.

Figure 1. Flexible Email Security Deployments



The Cisco Cloud Email Security Advantage

Cloud Email Security includes threat-protection capabilities to help eliminate a diverse range of known and emerging threats. It features high-performance virus scanning, outbreak filters, advanced antispam techniques, and innovative context-sensitive detection technology, encryption, and data loss prevention. Advantages include a data loss prevention architecture and end-to-end encryption.

Data Loss Prevention Architecture with RSA

Email is the leading vector for data loss. To help companies address this risk more effectively, Cisco began integrating data loss prevention technology into its email security solutions in 2009. Through this integration, Cisco provides customers with comprehensive global regulatory compliance coverage; best-in-class accuracy for identifying sensitive, data-comprehensive remediation options; and ease of deployment and management.

End-to-End Email Encryption

Cloud Email Security features the Cisco Registered Envelope Service, a flexible and scalable cloud-based solution that helps organizations support their security requirements—including meeting regulatory compliance demands and protecting intellectual property— without having to invest in additional hardware. It also eliminates the complexity of encryption and key management, so users can send and receive highly secure messages as easily as unencrypted emails.

How Is Cisco Cloud Email Security Managed?

Cloud Email Security is complemented by Cisco M-Series Content Security Management Appliances. These flexible tools centralize and consolidate policy and runtime data, providing a single management interface for email and web security.

Why Cisco?

Security is more critical to your network than ever. As threats and risks persist, along with concerns about confidentiality and control, security is necessary for providing business continuity, protecting valuable information, maintaining brand reputation, and adopting new technology.

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 organization's security needs.

Where Should I Go for More Information?

The best way to understand the benefits of Cisco Cloud Email Security is to participate in the Try Before You Buy program. To receive a fully functional virtual appliance to test in your network, free for 45 days, visit http://www.cisco.com/go/cloudemail.

C45-734182-01 06/16