Cisco Email Security

Protect Your Leading Attack Vector from Security Breaches

Today's organizations face a daunting challenge. Email is simultaneously the most important business communication tool and the leading attack vector for security breaches. In fact, according to the Cisco 2017 Midyear Cybersecurity Report, attackers turn to email as the primary vector for spreading ransomware and other malware.

Cisco® Email Security enables users to communicate securely. It helps organizations combat business email compromise (BEC), ransomware, advanced malware, phishing, spam, and data loss with a multilayered approach to security.

Benefits

- Detect and block threats faster with superior threat intelligence from Talos, our threat research team. Talos automatically sends intelligence updates every five minutes.
- Combat ransomware and advanced malware hidden in files that evade point-in-time detection with Cisco Advanced Malware Protection (AMP) 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.
- Protect sensitive content in outgoing emails with data loss prevention (DLP) and easy-to-use email encryption, all in one solution.
- Gain maximum deployment flexibility with a cloud, virtual, on-premises, or hybrid deployment, or move to the cloud in phases.

The Cisco Email Security Advantage

Cisco Email Security includes advanced threat protection capabilities that detect, block, and remediate threats faster; prevent data loss; and secure important information in transit with end-to-end encryption.

Block more threats with comprehensive threat intelligence

Talos, one of the largest threat-detection teams in the world, provides comprehensive threat intelligence from a wide range of sources including 600 billion messages, 16 billion web requests, and 1.5 million malware samples daily. Talos provides real-time intelligence updates to Cisco Email Security solutions every three to five minutes.

Combat the stealthiest malware hidden in email attachments

With AMP, customers combat ransomware and malware that evades point-in-time detection. AMP first checks the reputation of a file and delivers, blocks, or holds the message—based on the verdict. If a file becomes malicious after it has passed the initial inspection, you can see where the file traveled in your environment to remediate it quickly. If an unknown file enters your environment, then Threat Grid analyzes it in a sandbox. Threat Grid also helps you determine how large a threat specific malware poses and how to defend against it. AMP also provides strong protection against malware in outgoing emails to protect against a loss of IP or domain reputation.

With Mailbox Auto-Remediation, you can automate the removal of files that become malicious after initial inspection. Administrators can configure Cisco Email Security to forward, delete, or simultaneously forward and delete messages that contain malicious attachments, saving hours of work.

Block URL-based threats to prevent BEC and phishing attacks

With broad URL intelligence from our industry-leading portfolio of web security products, including Cisco Umbrella™, Cisco Email Security uses deep knowledge of web-based attacks and methods to prevent attacks from infected links. Using real-time click-time analysis, even websites that change to a malicious behavior will be blocked.

With Cisco Email Security you can also:

- Stop unwanted emails with better reputation intelligence and effective anti-spam protection.
- Block fraudulent senders with multiple layers of authentication and Forged Email Detection.
- Identify graymail and tag with “safe unsubscribe” option.
- Set and enforce detailed email policies.
- Respond to critical calls within minutes if an incident occurs with real-time message tracking.

Protecting Data in Outgoing Emails

When confidential information leaves your network, either intentionally or inadvertently, it has the potential to fall into the wrong hands. This can lead to compliance violations, data compromise, and reputation damage.

Data Loss Prevention

Email is the leading vector for data loss. To help companies address this risk more effectively, Cisco provides customers with comprehensive regulatory compliance, best-in-class accuracy for identifying sensitive data and comprehensive remediation options.

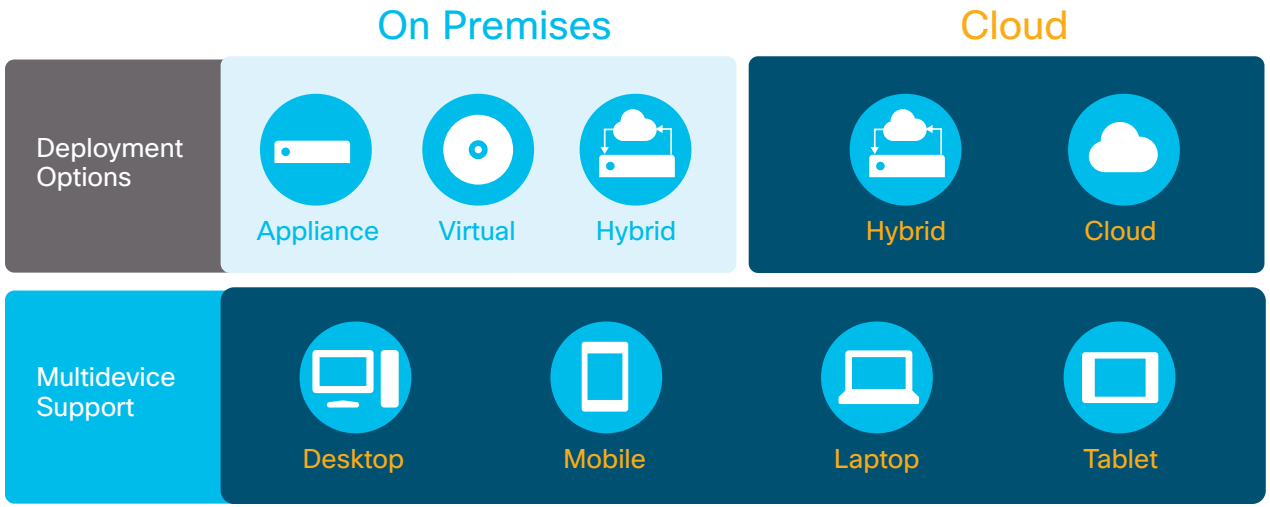
End-to-End Email Encryption

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

Deployment Options

Cisco Email Security can be deployed in the cloud, on-premise, or in a hybrid configuration and organizations can migrate to the cloud in phases enabling maximum flexibility. Figure 1 illustrates these deployment options.

Figure 1. Flexible Email Security Deployments



For more information

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