Cisco Secure Email

Comprehensive Threat Defense against the #1 Attack Vector

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, Cisco's Email Cybersecurity Report found that attackers still turn to email as the primary vector for spreading malware.

Cisco Secure Email (formerly Cloud Email Security) includes advanced threat defense capabilities that detect, block, and remediate threats in incoming email faster. Simultaneously, it protects an organization's brand, prevents data loss, and secures important information in transit with end-to-end encryption.

Benefits

- Detect and block more threats with global threat intelligence from Talos™ and local intelligence from multiple patented machine learning models.
- Combat stealthy malware that evades initial detection and remediate it fast to contain its impact.
- Drop emails with risky links automatically or block access to newly infected sites with realtime URL analysis to protect against phishing.
- Gain a real-time understanding of senders and learn and authenticate email identities and behavioral relationships to protect against BEC attacks.
- Prevent brand abuse from attackers using your domain to carry out phishing campaigns with automation of the Domain-based Message Authentication (DMARC) process.
- Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption.
- Gain maximum flexibility with a cloud, virtual, on-premises, or hybrid deployment or move to the cloud in phases.

"Since phishing is one of the main threat vectors for my industry, [Secure Email] is critical in assisting with weeding out threats before they reach users' inboxes."

Senior IT Architect,
Medium Enterprise Industrial Manufacturing Company

Protect users from threats in incoming emails

Detect and bock more threats with comprehensive threat intelligence

Talos, one of the largest threat detection teams in the world, provides global threat intelligence from a wide range of sources. In addition to Talos, multiple patented machine learning models provide local intelligence that combine identity and relationship modeling with behavior analytics. Talos and the machine learning models provide real-time intelligence updates to detect and prevent attacks.

Combat the stealthiest malware hidden in email attachments

With Cisco Secure Email, customers combat targeted, zero-hour ransomware and malware that evades initial point-in-time detection. Secure Email 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 email with an unknown file comes in Cisco Secure Malware Analytics analyzes the attachment in a sandbox. Secure Malware Analytics helps you determine how large a threat specific malware poses and how to defend against it.

Mailbox Auto-Remediation for Microsoft 365 and Exchange automates removal of emails with files that become malicious after the initial point of inspection. This saves administrators hours of work and helps contain a threat's impact.

Block URL-based threats like phishing

With broad URL intelligence from our industry-leading portfolio of web security products, including Cisco Umbrella™, Secure Email 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 are blocked.

Increase spam catch rates

Cisco Secure Email blocks unwanted emails using a multilayered scanning architecture. Offered as an additional subscription, Intelligent Multi-Scan (IMS) is a multi-layer anti-spam solution consisting of a combination of anti-spam engines, including Cisco Anti-Spam, working together for maximum efficacy.

Protect users from fraudulent senders

Block fraudulent senders to prevent BEC and advanced phishing attacks. With Forged Email Detection you can protect high-value targets via a customized content filter. To further enhance protection, Cisco Advanced Phishing Protection learns and authenticates email identities and behavioral relationships. This intelligence continuously adapts to drive a real-time understanding of senders. Read this at-a-glance to learn more about Cisco Secure Phishing Defense

Protect your brand and sensitive data in outgoing email

Uncontrolled spoof abuse of your domain and data loss greatly reduces your brand reputation and impacts your abilty to easily communicate with your partners and customers. Sensitive data can also fall into the wrong hands when sent in unsecure email. This can lead to compliance violations.

Guard against brand abuse

Cisco Domain Protection identifies and eliminates sources of illegitimate email by automating the process of DMARC email authentication and enforcement. It also gives you visibility into third-party senders who are using your domain to send email on your behalf to protect your brand identity while increasing email marketing effectiveness.
Read the at-a-glance to learn more about Cisco Secure Domain Protection.

Preserve your domain reputation

You can now utilize Cisco Secure Email to guard against malware in outgoing emails. Companies can face loss of IP or domain reputation if malicious content leaves your organization via email. Now you can enable Secure Email to monitor both inbound and outbound emails.

Prevent data loss

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.

Secure important data in outgoing email

Secure Email features the Cisco Secure Encryption Service, a flexible and scalable cloud-based solution that helps organizations meet regulatory compliance demands and secure your sensitive information, like intellectual property, in transit. 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

Secure Email can be deployed in the cloud, virtual, on-premises or hybrid, and organizations can migrate to the cloud in phases, enabling maximum flexibility.

Integration

Cisco Secure Email's integration into the SecureX platform provides enhanced visibility and automation across the entire Cisco Security product suite providing the protection that ensure businesses function securely. The robust platform simplifies your Secure Email experience by coordinating with other components within your infrastructure to expedite time to detect across multiple components. That level of visiblity maximizes the efficiency of Secure Email and the productivity of your teams.

Next steps

Learn more about Cisco Secure Email at www.cisco.com/go/emailsecurity, request a free 45-day trial or speak with your Cisco sales representatives or channel partners.