Email is the most important business communication tool—and simultaneously, the most used for cyber attacks. In fact, according to the Cisco’s Annual Cybersecurity Report, attackers turn to email as the primary vector for spreading malware. Attackers also use social engineering to create sophisticated and highly targeted Business Email Compromise (BEC) and phishing campaigns.

Cisco Email Security provides the first layer of defense against cyber threats and protects sensitive outbound data. It guards against spam, fraudulent senders, infected files—whenever they become malicious—and blocks risky URLs to prevent attacks. It also prevents data loss and secures sensitive data in transit to ensure compliance.

**Benefits**

- Block more threats with global threat intelligence from Talos and local intelligence from patented machine learning models.
- Combat stealthy malware that evades initial detection and remediate it fast to contain the impact of a threat.
- Drop emails with risky links automatically or block access to newly infected sites with real-time URL analysis to protect against phishing.
- Gain a real-time understanding of senders, 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 deployment flexibility with a cloud, virtual, on-premises, or hybrid deployment or move to the cloud in phases.

**Advanced email protection for inbound email**

**Comprehensive threat intelligence**

Talos, one of the largest threat detection teams in the world, provides global threat intelligence from a wide range of sources, including 600 billion messages, 16 billion web requests, and 1.5 million malware samples daily. 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.
Reputation filtering

Block unwanted email with reputation filtering, which is based on threat intelligence from Talos. For each embedded hyperlink, a reputation check is performed to verify the integrity of the source. Websites with known bad reputations are automatically blocked. Reputation filtering stops 90 percent of spam before it even enters your network, allowing the solution to scale by analyzing a much smaller payload.

Antispam filtering

The emails that pass through reputation filtering are scanned with an antispam engine for a catch rate of greater than 99 percent and a false-positive rate of less than one in one million. You can decide to drop, quarantine, or deliver messages suspected of being spam. We also offer optional multiengine spam-scanning technology to catch corner-case spam.

Forged Email Detection

Forged Email Detection protects against business email compromise attacks focused on executives who are considered high-value targets. Forged email detection helps you block these customized attacks and provides detailed logs on all attempts and actions taken.

Cisco Advanced Phishing Protection

Cisco Advanced Phishing Protection stops deception–based attacks such as social engineering, BEC, and phishing with local email intelligence and advanced machine learning techniques that models trusted email behavior on the Internet, within organizations and between individuals. This intelligence continuously adapts to drive a real-time understanding of senders and prevent attacks. Learn more about Cisco Advanced Phishing Protection on this at-a-glance.

Antivirus tools

For multilayered antivirus protection, you can deploy either the Sophos or McAfee antivirus engine, or both. Run both engines to dual scan messages for the most comprehensive protection.

Advanced Malware Protection (AMP)

AMP and Threat Grid provide file reputation scoring and blocking, file sandboxing, and file retrospection for continuous analysis of threats. Users can block more attacks, track suspicious files, mitigate the scope of an outbreak, and remediate quickly.

Mailbox Auto-Remediation is an AMP feature that helps Microsoft Office 365 customers automatically remove emails with files that become malicious after the initial point of inspection. Administrators can configure Cisco Email Security to forward, delete, or simultaneously forward and delete messages that contain malicious attachments, saving administrators hours of work and containing the impact of a threat.

Customers can also purchase an additional license to deploy their AMP system completely on-premises with the AMP private cloud. This, along with Threat Grid, brings the entire AMP offering completely on-premises.

Graymail management

The graymail management solution includes two features - Graymail Detection and Safe Unsubscribe. Graymail detection helps to precisely classify and monitor graymail entering your organization. An administrator can then take appropriate action for each category of graymail. The Safe Unsubscribe feature automatically presents recipients with a safe way to unsubscribe via a real-time analysis of the sender’s unsubscribe method that provides feedback one and a half seconds later.
The graymail solution provides:

- Protection against malicious threats masquerading as unsubscribe links.
- A uniform interface for managing subscriptions.
- Better visibility for email administrators and end users into such emails.

**Outbreak Filters**

Outbreak Filters defend against emerging threats and blended attacks. They can issue rules on any combination of six parameters, including file type, file name, file size, and URLs in a message. As Talos learns more about an outbreak, it can modify rules and release messages from quarantine accordingly. Outbreak Filters can also rewrite URLs linked in suspicious messages.

When clicked, the new URLs redirect the recipient through the web security proxy. The website content is then actively scanned, and Outbreak Filters will display a block screen to the user if the site contains malware.

---

**“Cisco Email Security stops everything thrown at it, it has been bullet-proof in stopping all email threats! Couple that with Cisco TAC support and you can’t go wrong!”**

Steven Wujek
Senior IT Architect
Technology Concepts & Design

---

**Brand and data protection for outbound email**

Cisco Email Security offers effective brand protection, accurate DLP policy enforcement and email encryption.

**Cisco Domain Protection**

Through automation of the DMARC standard, Cisco Domain Protection gives you visibility into internal and third-party senders who are using your domain to send email on your behalf. This helps you identify and eliminate sources of illegitimate email to preserve your brand identity. It automatically correlates information into an easy-to-read report that gives you visibility into which third-party senders are sending email on your behalf and whether they are DMARC compliant. It also provides guidance on how to block unauthorized senders and set up DMARC protection to reduce the likelihood of your domain being used to send fraudulent emails. Learn more about [Cisco Domain Protection](#) on this at-a-glance.

**Advanced Malware Protection**

You can use AMP to guard against malware in outgoing emails. Your company can face loss of IP or domain reputation if malicious content leaves your organization via email. Now with the same AMP license, you can enable AMP to monitor both inbound and outbound emails.

**DLP**

Protect outbound messages with Cisco Email Security DLP. Comply with industry and government regulations worldwide and prevent confidential data from leaving your network. Choose from an extensive policy library of more than 100 expert policies covering government-, private sector-, and company-specific regulations. Remediation choices include encrypting, adding footers and disclaimers, adding Blind Carbon Copies (BCCs), notifying, and quarantining. For companies needing a complex custom policy, the building blocks of the predefined policies are readily available to make the process quick and easy.
Encryption

Give senders control of their content, even after messages have been sent. With email encryption, senders don’t fear mistyped recipient addresses, mistakes in content, or time-sensitive emails because they can always lock a message. The sender of an encrypted message receives a read receipt once a recipient opens a message, and highly secure replies and forwards are automatically encrypted to maintain end-to-end privacy and control. There is no additional infrastructure to deploy. For enhanced security, message content goes straight from your gateway to the recipient, and only the encryption key is stored in the cloud.

Meet encryption requirements for regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), or the Sarbanes-Oxley Act (SOX)—as well as state privacy regulations and European directives—without burdening the senders, recipients, or email administrators. Offer encryption not as a mandate but as a service that is easy to use and gives the sender complete control.

Manageability

System overview dashboard

Monitor and report on messages from a centralized dashboard. A new and simplified interface offers a single view for comprehensive insight across your organization. Get the details of any email for advanced visibility.

Detailed message tracking

When you send a message to Cisco Email Security, the message tracking database is populated within a minute or two, and you can easily see what happened to the messages that are crossing the system at every step of processing.

Where to Deploy

Cisco Email Security can be deployed in the cloud, virtual, on-premise or hybrid. You also get access to all features across any deployment option—cloud, virtual, on-premises, or hybrid. The user interface is identical no matter which deployment option you choose. Organizations can also transition to the cloud in phases. This allows for maximum deployment flexibility as your organization’s needs change.

Take advantage of Cisco Services

- **Advisory services**: Our experts align risk, compliance, security, and threat management with your business goals.
- **Implementation services**: With expertise and best practices working alongside thousands of customers across all industries around the world, we’ll help you more quickly realize and increase the benefits of your investment in advanced security solutions, including email security.
- **Managed services**: Our expert investigators proactively monitor customer networks 24/7 from our global network of state-of-the-art security operations centers, providing constant vigilance and in-depth analysis as a comprehensive security solution.
• **Technical services:** We provide proactive, pre-emptive technical services for hardware, software, multivendor solutions, and network environments. Our global team enhances IT operations, helping to ensure your IT works simply, consistently, and securely to keep your business running smoothly.

**Cisco Capital**

**Financing to help you achieve your objectives**

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.]

**Next steps**

Learn more about Cisco Email Security at [https://www.cisco.com/go/emailsecurity](https://www.cisco.com/go/emailsecurity) request a free 45-day trial or speak with your Cisco sales representatives or channel partners.