White paper
Public

single point of contact

Cisco Email Security: Advanced Threat Defense for Microsoft Office 365

Microsoft Office 365 has become the standard productivity platform in organizations large and small around the world. It is a cost-effective solution and provides a basic level of email security through Microsoft Exchange Online Protection. But as more and more companies make the transition to this platform, Office 365 has also become an attractive attack surface for cybercriminals.

Over 90 percent of breaches start with email. According to the Cisco 2017 Midyear Cybersecurity Report, attackers turn to email as the primary vector for spreading ransomware and other malware. This is why no company can afford skimp on email security.

To achieve enterprise-level security, Office 365 customers are enhancing Exchange Online Protection with an additional layer of email security. This additional layer helps ensure that they have the most advanced capabilities to protect their leading attack vector from sophisticated and costly cyberattacks.

Cisco Email Security for Microsoft Office 365

If you are one of the many businesses that has adopted Office 365 for your email solution, it's time to protect your investment and enable secure email use with multiple layers of protection. Cisco® Email Security provides industry-leading protection against malware, ransomware, business email compromise (BEC), URL-based phishing attacks, and spam.

Our solution is built on the same comprehensive platform that has led Gartner's Magic Quadrant for Secure Email Gateways for a decade. Cisco Email Security offers best-in-class differentiating features for Office 365 customers.

Block more threats with comprehensive threat intelligence

Talos™, one of the largest threat-detection teams in the world, provides a massive repository of threat intelligence gathered from a wide range of sources including 600 billion messages, 16 billion web requests, and 1.5 million malware samples daily. In addition, intelligence sharing with other Cisco security products means that if a threat is discovered through another security product, Talos automatically shares this information with Cisco Email Security customers for more effective protection. The volume and diversity of data helps Talos identify email threats as they are emerging and block them faster. Talos updates Cisco Email Security solutions with the latest intelligence every three to five minutes.

Combat the stealthiest malware hidden in files

With Cisco Advanced Malware Protection (AMP), Office 365 customers protect against files with malware that evade point in time detection. AMP first checks the reputation of a file and sends this information to its cloud-based intelligence network for a reputation verdict. An action is taken–to deliver, block, or hold 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. With Mailbox Auto-Remediation for Office 365, you can automatically remove a file that turns malicious once inside your network. This feature removes advanced persistent threats that pass through the Office 365 mailbox. Administrators can configure Cisco Email Security to forward, delete, or simultaneously forward and delete messages that contain malicious attachments, saving your team hours of work.

AMP also provides strong protection against malware in outgoing emails. Such malware can lead to a loss of IP or domain reputation. Now, with the same license, you can enable AMP to monitor both inbound and outbound emails.

> **"Cisco Cloud Email Security with AMP helps me sleep better at night. I don't have to stay up expecting an email from the C-level folks or VP asking 'Is this email legit?' or 'Should I open this attachment?' since CES is managing all that for us."**
>
> **Milind Samant**
> Director of Information Technology Services and Information Security Officer (ISO), SUNY Old Westbury

AMP on Email Security is part of our AMP Everywhere architecture, which shares malware analysis and verdicts from customers globally for superior threat efficacy. It integrates with other Cisco security products to correlate threat information for a fast and synchronized response to threats.

Make decisions faster when defending against malware

If an unknown file enters your environment, Cisco Threat Grid analyzes it in a sandbox or secure environment. Threat Grid helps you detect, analyze, and understand what malware is doing, or attempting to do, and determine how large a threat it poses and how to defend against it. The email is then released to the user, with or without the attachment, or deleted if it is found malicious. With Threat Grid, you can make informed decisions faster, prioritize the threats with the most impact on your organization, and speed up incident investigation.

Block URL-based threats more efficiently with better intelligence

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 are blocked.

Cisco Email Security also includes the following features:

Antispam

To stop spam from reaching users' inboxes, a multilayered defense combines an outer layer of filtering based on the reputation of the sender. It also runs an inner layer of filtering that performs a deep analysis of the message. Together, reputation filtering and our antispam technology block over 99 percent of incoming spam emails with near-zero misclassifications (1 in 1 million). This spam catch rate significantly reduces the administrative burden.

Forged Email Detection

Email forging, or business email compromise (BEC), alters a message to hide the real identity of the sender and make it appear as if the email is coming from someone you know. This feature helps you discover whether an email is coming from an attacker by validating proper use of spoof email. It can create a filter to detect forged or BEC messages and define what to do with those messages.

Graymail Detection

Graymail consists of marketing, social networking, and bulk messages. The graymail detection feature precisely classifies and monitors these types of emails entering your organization. An administrator can then take appropriate action on each category of graymail.

Graymail Safe-Unsubscribe

This feature tags graymail with a safe unsubscribe option. This option safely processes an unsubscribe request on behalf of the end user. It also monitors the various graymail and unsubscribe requests. This feature can be managed at a policy, Lightweight Directory Access Protocol (LDAP) group level.

Antivirus

We offer the choice and flexibility to deploy either Sophos or McAfee antivirus engines. These engines can also run in tandem, providing a layered approach for additional antivirus protection.

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.

Data Loss Prevention

Cisco Data Loss Prevention (DLP) provides an integrated, all-in-one DLP solution. This solution helps ensure compliance with industry and government regulations worldwide and helps prevent confidential data from inadvertently leaving your network.

Email Encryption

Make sending confidential information easy for your users with automatic scanning. Outgoing emails with sensitive information are secured without user action to help ensure compliance. This feature includes Secure/Multipurpose Internet Mail Extension (S/MIME) and Transport Layer Security (TLS) encryption support.

Our unique cloud offering for protecting Office 365 email

Customers can reduce their onsite data center footprint and outsource the management of their email security to trusted security experts. Cisco Email Security provides a dedicated cloud infrastructure in multiple resilient Cisco data centers to help ensure the highest levels of service availability and data protection. Cisco provides you with direct access to your solution for configuration and reporting so you can retain complete visibility of your cloud-based email solution. You’ll also get comprehensive reporting and message tracking capabilities that provide exceptional administrative flexibility.

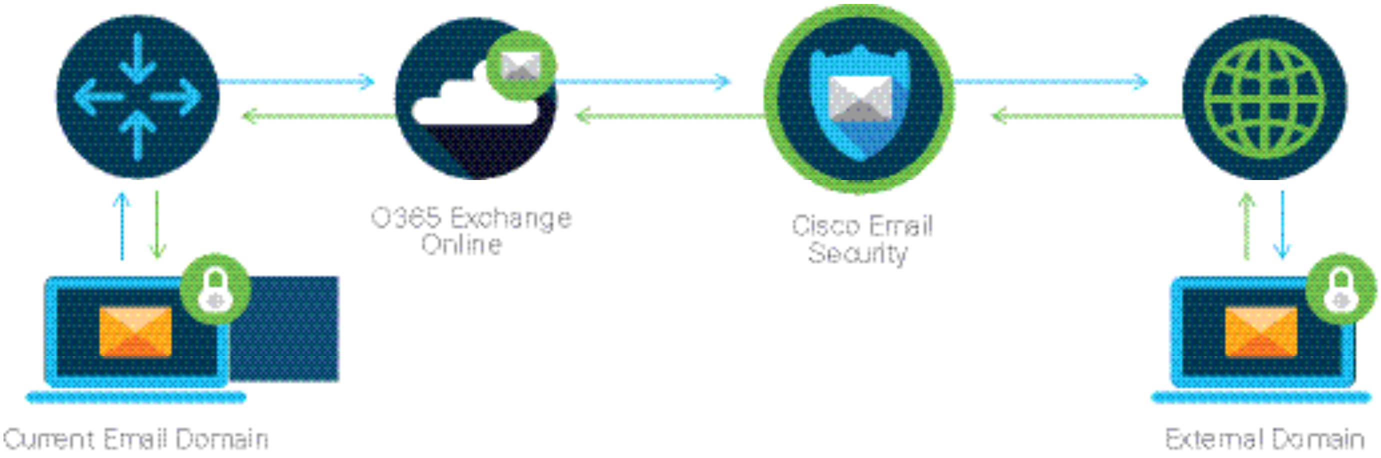
This unique service is all-inclusive, with software, hardware, and support bundled for simplicity. It offers Office 365 customers several differentiating features:

- Dedicated cloud infrastructure: Each customer has a dedicated email security instance that is hosted in multiple Cisco data centers around the world.
- Cloud-capacity assurance: Users are protected and peak performance is maintained regardless of whether spam volumes increase. Additional capacity is included with a simple per-user, per-year pricing model.
- Cloud-availability guarantee: Cloud Email Security guarantees 99.999 percent uptime, so security is available and working for you through multiple data centers.
- Dedicated IP addresses: Customers have dedicated IP addresses, avoiding shared-fate blacklisting. Customers also have financially backed service-level agreements (SLAs).

How Cisco Email Security integrates with Microsoft Office 365

Cisco Email Security in the cloud integrates transparently with Microsoft Office 365 regardless of your setup: whether you have a portion of your mailboxes in the Office 365 cloud or all of them. Simply point your Mail Exchange (MX) records to the Cisco Email Security cloud platform. Configure your Smart Host settings in Office 365 to deliver outbound mail through the Cisco Email Security cloud platform, and our easy-to-use and easy-to-configure DLP and encryption features will control your outbound mail flows, hiding sensitive data from prying eyes (Figure 1).

Figure 1. Cisco Email Security in the cloud for Microsoft Office 365



Single Point of Contact has been consulting businesses with their network and security requirements for almost 20 years. From the cloud to the end point, Single Point of Contact can help with your cloud and network security requirements. Contact us today and our consultants can help guide you through any challenge your firm might be having. Email or call us at 800-791-4300.