

Cisco Secure Email Cloud Mailbox

Supplemental cloud email protection for
Microsoft Office 365



The bridge to possible

Contents

Mailboxes shift to the cloud	3
Security challenges with cloud-based email	3
Cloud Mailbox-Solution components and differentiators	4
Why choose Cloud Mailbox?	5

Mailboxes shift to the cloud

The migration of email infrastructure from on-premises to the cloud has accelerated to the extent that by 2021, 70% of public and private organizations will use cloud email services (**Gartner, Market Guide for Email Security, 2019.**) Microsoft 365 is the predominant office suite. Because email is vulnerable to advanced threats, Gartner recommends adding cloud email supplemental security to protect cloud mailboxes with layered security and diversified threat intelligence. Cisco Secure Email Cloud Mailbox (Cloud Mailbox)–integrated email security for Microsoft 365, protects your organization against the number one threat vector: Email.

Product Overview

Cloud Mailbox augments native Microsoft 365 security and provides complete visibility to inbound, outbound, and internal user-to-user messages.

With Cloud Mailbox customers can:

- Detect and block threats with superior threat intelligence from Cisco Talos, one of the largest threat research and efficacy teams
- Combat advanced threats using Secure Endpoint, and Secure Malware Analytics
- Get complete visibility to inbound, outbound, and internal messages
- Leverage fast API-driven remediation of messages with malicious content
- Use an integrated dashboard for search, reporting and tracking, including conversation view and message trajectory
- Enhance Microsoft 365 security in less than 5 minutes without changing the mail flow

Security challenges with cloud-based email

Security administrators need to be aware of the increased security risks inherent in moving mailboxes to the cloud. Native cloud email security can leave you exposed.

Native cloud email security can leave you exposed

With all of your organization's email data hosted in the cloud, it makes sense to bolster your security defenses with innovative enterprise-grade security and diversified threat intelligence.

Unknown and dynamic threats

Unknown and dynamic threats can be missed and continue to linger in cloud mailboxes. Faster, automated detection and remediation tools are needed to mitigate the spread of email-borne threats inside your organization.

Targeted platform wide attacks

The broad-based adoption of cloud email opens up organizations to new threat vectors. Attackers have increasingly targeted cloud mailboxes for takeover to launch attacks against the overall organization. Cloud email platforms are among the most impersonated domains. A successful credential phish can expand the attack surface to include the full office suite, with options to launch insider or spearphishing attacks.

Sophisticated attacks using advanced threats

Advanced threats like ransomware, Business Email Compromise (BEC) and targeted phishing attacks such as spearfishing, can breach the native security defenses of cloud email platforms.

Perimeter security lacks complete visibility into email traffic

Cloud email platforms are susceptible to threats emanating from within the office suite. A credential phish can lead to an account takeover, giving access to internal communications, and creating a launch pad for internal phishing and business email compromise attacks.

Since perimeter security is unaware of insider threats, it is important to scan every mail entering or leaving each cloud mailbox. Continuous mailbox analysis is the key to protect against insider threats.

Cloud Mailbox–Solution components and differentiators

Cloud Mailbox is a cloud native solution leveraging superior threat intelligence from Cisco, an API enabled architecture for faster response times, complete email visibility including internal emails, a conversation view for better contextual information, and tools for auto or manual remediation of threats lurking in Microsoft 365 mailboxes.

Secure Email Gateway vs. CESS



Talos: Visibility, Intelligence and Response

Immense visibility and telemetry on a global scale enables Talos to stop more spam, malicious attachments and URLs, and phishing.

As the largest global provider of cutting-edge security research and intelligence, Talos delivers high-impact, actionable security content and tools–giving customers a uniquely comprehensive and proactive approach to stopping more threats with greater accuracy and efficacy.

Cisco Secure Endpoint and Cisco Secure Malware Analytics

Cisco Secure Endpoint (formerly Cisco AMP) and Cisco Secure Malware Analytics (formerly Threat Grid) provide file reputation scoring and blocking, file sandboxing, and file retrospection for continuous analysis of threats. Customers can block more attacks, track suspicious files, mitigate the scope of an outbreak, and remediate quickly. Secure Endpoint (formerly Cisco AMP) shares threat intelligence across Cisco security devices, thereby unifying security across endpoints, networks, email, the cloud, and the web.

API enabled architecture

Cloud Mailbox uses the Microsoft Graph API to communicate with Microsoft 365, enabling very fast detection and remediation. The solution is RESTful API capable, allowing easy and flexible integration with other security tools.

Unified user interface

Cloud Mailbox has a single interface for reporting, configuration and tracking. Cloud Mailbox provides full conversation and message trajectory views with full email traffic visibility in your Microsoft 365 mailboxes, thereby providing better contextual information to make an appropriate judgement.

Cloud-native

Cloud Mailbox scanning engines run within Microsoft Azure, ensuring that email messages do not exit regional Azure boundaries. The scanning engines generate and push only the verdicts and email metadata to the Cloud Mailbox platform for policy, search, remediation, and reporting.

Why choose Cloud Mailbox?

Cloud Mailbox addresses potential gaps in Microsoft 365 email security by leveraging proven Cisco email security technology to block spam and advanced email threats like ransomware, business email compromise, and phishing attacks.

Augment native Microsoft 365 security

Cloud Mailbox adds an additional layer of security to native Microsoft 365 email security by using industry-leading threat intelligence from Cisco Talos, AMP, and Secure Malware Analytics—including vast cross-vector threat intelligence from web, network, and endpoint-based sources.

Protect against sophisticated and targeted attacks

Cloud Mailbox protects against phishing, business email compromise, and account takeover attacks by continuously analyzing emails entering or leaving mailboxes. A security layer that is always ON and remediating threats irrespective of the timeline of identification.

Configure and deploy instantly

Cloud Mailbox exemplifies simplicity. Protection is activated with an easy one-time configuration without any changes to mail exchanger (MX) records. This avoids any risk associated with altering mail flow and adds no latency to mail delivery. The solution can:

- Conduct instant Proof of Value (PoV) with a quick setup wizard
- Monitor Microsoft 365 mailboxes in audit mode, or remediate threats with enforcement mode
- Be fully configured in less than 5 minutes
- Convert a Proof-of-Value (PoV) to production deployment instantly

Leverage a cloud native solution

Cloud Mailbox is a cloud-native solution with high availability, optimization for performance, faster detection, and response times—a true API-driven cloud solution that automatically scales resources based on demand and can be deployed quickly across regions for global scale.

Get complete email visibility, including internal user-to-user email

Be it internal or external emails, every message entering or leaving a mailbox should be treated with the same level of scrutiny. Doing so will minimize the spread of insider threats whether it is a malicious actor inside the organization, or a compromised Microsoft 365 mailbox. Cloud Mailbox scans all messages in the mailbox in all directions—inbound, outbound, or internal. It allows administrators to search messages across all mailboxes.

Performing threat analysis with Cisco SecureX threat response casebooks

Cloud Mailbox is pre-integrated with the Cisco SecureX threat response casebook to record, organize, and share a set of observables of interest, during an investigation and threat analysis across multiple products.

Improved data protection and data privacy

Cloud Mailbox security engines run in the Microsoft Azure cloud and send only the verdicts and email metadata to the Cisco Cloud Mailbox platform for reporting and policy-based action. This ensures improved data privacy as email messages never leave the data boundaries of the Microsoft 365 Azure region.

Simplified Ordering and Support

Ordering Cloud Mailbox is easy. A single subscription SKU is used to select the number of seats (minimum 25) and subscription term (1, 3, or 5 years.) High-Value Support Services is included by default.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)