CISCO
SECURE

How to Protect Your Business with Enhanced Email Security

Mailboxes shift to the cloud

Native Microsoft 365 security leaves businesses vulnerable

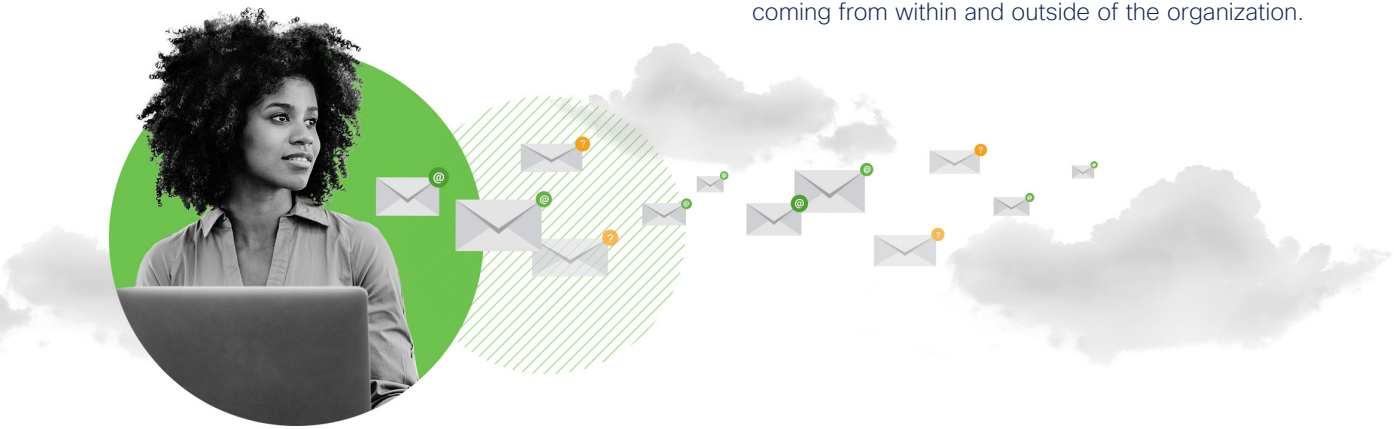
As email infrastructure moves from on-premises to the cloud, organizations reap the benefits of increased collaboration capabilities, streamlined workflows, and centralized project management. At the same time, widespread cloud email adoption also opens organizations to new threats.

Attackers increasingly target cloud mailboxes for takeover in order to launch attacks against the entire organization. Cloud email platforms are among the most impersonated domains and a successful credential phish can expand the attack surface to include the full office suite. Detecting threats as quickly as possible to mitigate exposure is critical to keeping businesses secure.

© 2021 Cisco and/or its affiliates. All rights reserved.

With over 90% of data breaches starting with email[1] and Microsoft 365 surpassing 200 million monthly users[2], native Microsoft 365 protections often aren't sufficient. Companies using Microsoft 365 need to deploy additional cloud email security tools to defend against advanced threats that could cost them billions[3].

Cisco Secure Email Cloud Mailbox (Cloud Mailbox) provides your organization with a necessary layer of extra protection to stop threats before and after they reach your inbox.



Protect Inboxes Across Your Organization with Cloud Mailbox

Cloud Mailbox adds that additional layer of security to native Microsoft 365 email by using proven Cisco Secure Email technology, industry-leading threat intelligence from Cisco Talos, Cisco Secure Malware Defense, and Cisco Secure Malware Analytics to protect organizations against phishing, business email compromise (BEC) and account takeover attacks.

Cloud Mailbox is a security layer that remediates threats coming from within and outside of the organization.

Leading Threat Intelligence as the Foundation

Cloud Mailbox leverages the full force of Cisco Talos, one of the largest and most trusted providers of global cutting-edge security research. With Talos, users are able to:

- Access the work of hundreds of full-time threat researchers who track new and emerging threats.
- Gain insight into the data Cisco Security products and services use to take action.
- Act on intelligence gathered from a wide range of sources, including other Cisco security products, which is then shared with Cisco Secure Email customers for more effective protection.
- See a threat once and block it everywhere. With best-in-class protection and safeguards against blended attacks, Talos addresses and blocks threats as they are emerging.

© 2021 Cisco and/or its affiliates. All rights reserved.

Key Cloud Mailbox Features

Configure and deploy instantly

Cloud Mailbox can be deployed with no prior email security experience. Users can get up and running with an easy, one-time configuration, without altering mail flow or slowing down message delivery.

Ease the burden on administrators

Our robust AI-driven threat detection paired with our advanced search and remediation tools allow administrators to quickly discover and remediate threats, allowing them to focus on other business-critical issues.

Leverage a cloud native solution

As a cloud-native solution, Cloud Mailbox is built to automatically scale resources based on demand, provide a highly available resilient service, and optimize for maximum performance, faster detections and response times.

Analyze every message

Cloud Mailbox scans every message with the same level of scrutiny – inbound, outbound, or internal. It enables administrators to search messages across all mailboxes and take immediate action if they discover a threat.

Lower overhead costs

Cloud Mailbox requires minimal configuration and the interface so intuitive that administrators don't need any specialised training and can immediately start triaging and remediating threats.

Protect against account takeover attacks

Because Cloud Mailbox scans and remediates against internal messages, it can spot lateral movement and internal malware propagation that can occur after an account takeover. Outbound malware and spam are given the highest priority and administrators are alerted immediately when this type of behavior is detected.

Prioritize data protection and privacy

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

Simplified ordering and support

Becoming a Cloud Mailbox customer 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 are included by default.

[1] Over 90% of breaches start with email - https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-security-o365-whitepaper.pdf

[2] Office 365 Hits 200 Million Monthly Users - https://office365itpros.com/2019/10/24/office-365-hits-200-million-monthly-active-users/

[3] BEC breaches cost companies more than $1.7 billion in 2019 - https://www.fbi.gov/ news/stories/2019-internet-crime-report-released-021120

© 2021 Cisco and/or its affiliates. All rights reserved.

Ready to get serious about email security?

Relying solely on native Microsoft 365 email security tools leaves inboxes (and therefore businesses) vulnerable. To see Cloud Mailbox in action, check out this on-demand demo or sign up for a free 30-day trial.

© 2021 Cisco and/or its affiliates. All rights reserved. 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: 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. 04/21