

Cisco Cloud Mailbox Defense

The Cloud Mailbox Migration Journey

Your business has spent time and effort migrating your mailboxes from on-premise Exchange servers to Microsoft 365. The convenience and scalability of this migration are paying off, but you have new questions and challenges about how best to secure your new cloud environment.

Your Secure Email Gateway appliance continues to enforce perimeter security policy, but you're concerned that you aren't seeing the whole picture. Are you adequately protected from insider threats, account takeover, and business email compromise without controlling your internal mail?

What's more, you have had some turnover in your operations and wonder how quickly you can train your new engineers to manage your increasingly complex mail flow policies. Can you leverage the newer cloud-native APIs that are available in Microsoft 365?



Benefits

- Stop threats to Microsoft 365 from both internal and external senders
- Increase visibility into your cloud mailbox environment including internal-to-internal messages
- Reduce administrative overhead by providing your operators with a simple and powerful tool
- Empower incident responders with fast search and triage

Take Command of Your Mailbox

Supplement your existing mail security and gain unprecedented visibility without altering your mail flow or spending time and energy on in-depth technical training. By journaling messages from Microsoft 365, Cisco Cloud Mailbox Defense can see all your mail, internal and external, without requiring changes to your MX records or interrupting the regular delivery of messages.

The industry-leading efficacy of Cisco Talos can now be leveraged directly inside Azure, bringing the technology behind powerful tools like Cisco Secure Malware Defense file reputation and Cisco Secure Malware Analytics file analysis as close to the mailbox as possible.

By taking action using native Microsoft 365 APIs, Cloud Mailbox Defense can quickly remediate threats using the most modern and effective tools available.

With Audit and Enforcement mode, security analysts can investigate and triage threats to your users with minimal required training. Our Conversation feature tells the entire story of an email attack, going beyond the perimeter and focusing on timeline and message propagation. With Enforcement enabled, administrators can set policy to move or delete messages based on their malware or spam disposition, taking into account the attachments, embedded URLs, and even message content.



Find out how Cloud Mailbox Defense can secure your Microsoft 365 environment:

Go to: cisco.com/go/cmd