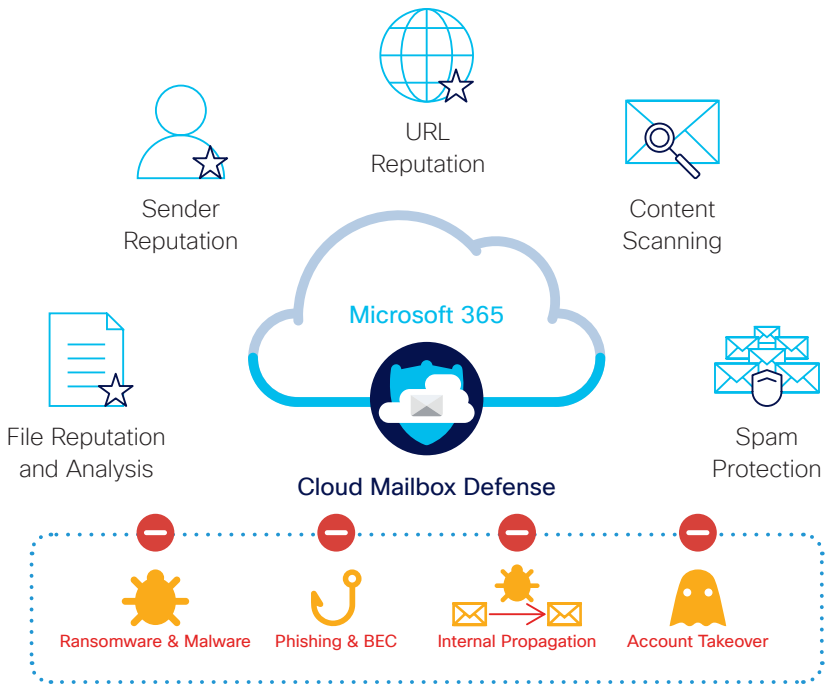
Cisco Cloud Mailbox Defense NEW

Integrated Cloud-Native Security Solution for Microsoft 365

The **Cisco Cloud Mailbox Defense (CMD)** is an integrated cloud-native security solution for Microsoft 365 that focuses on simple deployment, easy attack remediation, superior visibility and best-in-class efficacy from Cisco Talos. CMD addresses gaps in Microsoft 365 security by blocking advanced email threats like ransomware, BEC (Business Email Compromise), phishing, spoofing, and spam by leveraging proven Cisco Email Security technologies.
Full conversation and message trajectory views allow insight into email traffic within your Microsoft 365 mailboxes, thereby providing better contextual information needed to make an appropriate judgement. CMD can quickly remediate threats —either automatically or manually— using the most modern and effective tools available without interrupting the regular delivery of messages.



Highlights

Cisco Cloud Mailbox Defense (CMD) provides simplified and effective security with:

- **Lower Total Cost of Ownership and Higher SOC Productivity**
  CMD is designed with simplicity in mind. Because there are no required changes to mail flow, it can be deployed without the administrative overhead of altering MX records or email architecture. Because the configuration is minimal and the interface so intuitive, no specialized training is required, and operations can immediately triage and remediate threats.
- **Protection against Account Takeover Attacks**
  Because CMD scans and remediates against internal messages, we 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.
- **Direct Integration with Microsoft's Cloud**
  CMD allows organizations to augment native Microsoft 365 security controls by leveraging the industry-leading security intelligence of Cisco Talos. By integrating directly with Microsoft's cloud, we can bring Cisco security as close to the mailbox as possible. Further integration with Cisco SecureX provides visibility across the entire Cisco Security portfolio and increases automation.*1
- **Improved Efficacy**
  Integration into the Cisco SecureX platform provides enhanced visibility and automation across the entire Cisco Security product suite providing coordination with other components across a Customer's infrastructure and expediting time to detect across multiple components.*1

*1 SecureX integration will be available in Q2FY21.

© 2020 Cisco and/or its affiliates. All rights reserved.

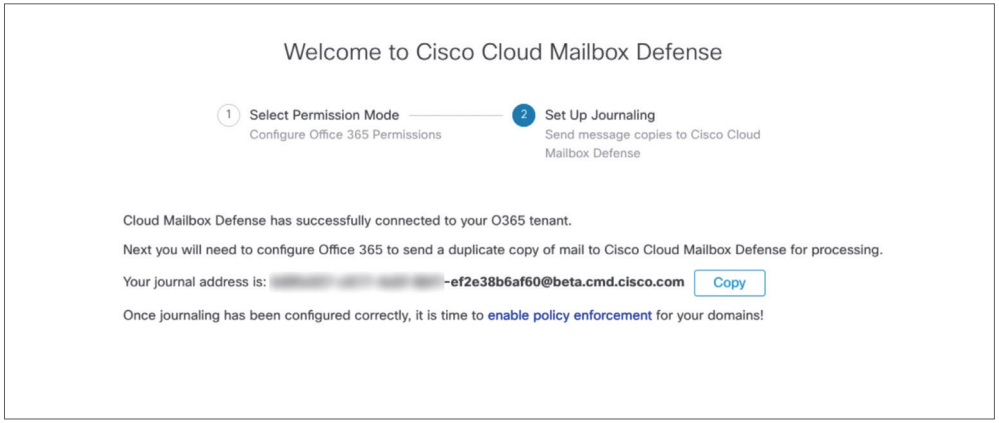
Cisco Cloud Mailbox Defense NEW

Features

Cisco Cloud Mailbox Defense (CMD) 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**
  CMD adds an additional layer of security to native Microsoft 365 email security by using industry-leading threat intelligence from Cisco Talos, Cisco AMP, and Cisco Threat Grid — including vast cross-vector threat intelligence from web, network, and endpoint-based sources.
- **Protect against Sophisticated and Targeted Attacks**
  CMD 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**
  CMD 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**
  CMD 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.

Quick setup wizard (two-step deployment)



© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud Mailbox Defense NEW

- **Unified User Interface**

  CMD has a single interface for reporting, configuration, and tracking. CMD 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.

- **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. CMD scans all messages in the mailbox in all directions — inbound, outbound, or internal. It allows administrators to search messages across all mailboxes.

- **Cisco Talos: Visibility, Intelligence and Response**

  Immense visibility and telemetry on a global scale enable Cisco 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 Advanced Malware Protection (AMP) and Cisco Threat Grid**

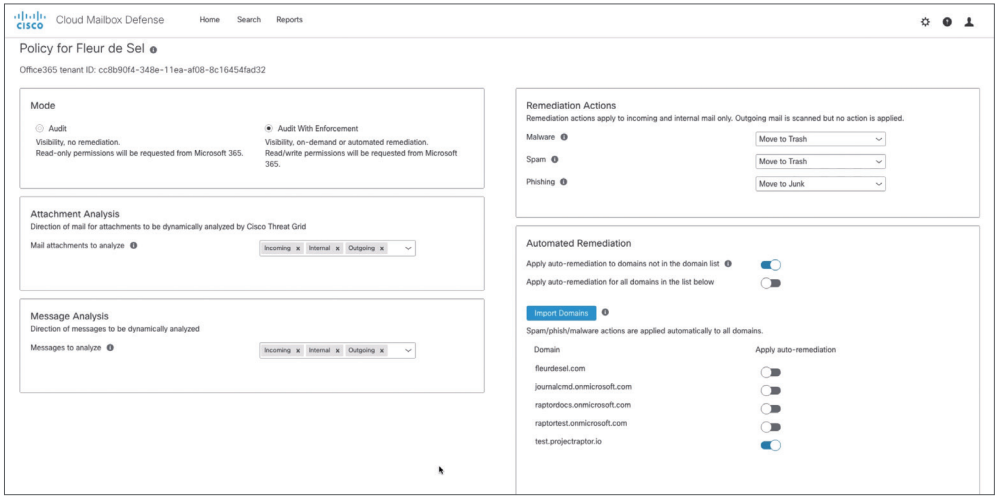
  Cisco AMP and Cisco Threat Grid provide file reputation scoring and blocking, file sandboxing, and file retrospection for continuous analysis of threats. Customers can block more attacks, track suspicious files, mitigate the scope of an outbreak, and remediate quickly. AMP shares threat intelligence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

- **Performing Threat Analysis with Cisco Threat Response Casebooks**

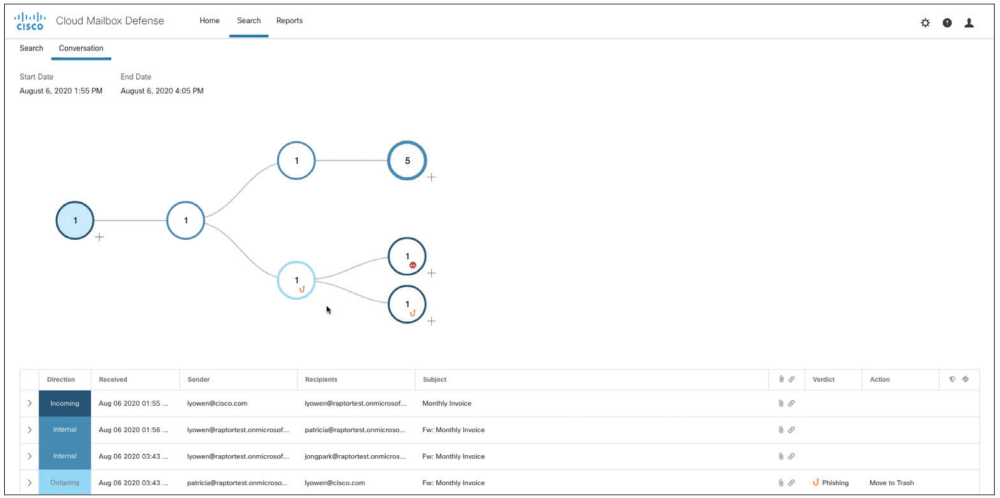
  CMD is pre-integrated with the Cisco Threat Response (CTR) casebook to record, organize, and share a set of observables of interest, during an investigation and threat analysis across multiple products.

- **Improved Data Protection and Data Privacy**

  CMD security engines run in the Microsoft Azure cloud, and send only the verdicts and email metadata to the CMD 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.



Simple policy configuration



Full conversation and message trajectory views

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud Mailbox Defense NEW

Cisco Cloud Mailbox Defense License

Product SKU*1	Description
CMD-ESS-LIC	Cloud Mailbox Defense Essential per Seat License (25~ seats)

*1 CMD-SEC-SUB is required in CCW. See Ordering Guide for details.

Cisco Cloud Mailbox Defense Enhanced Support

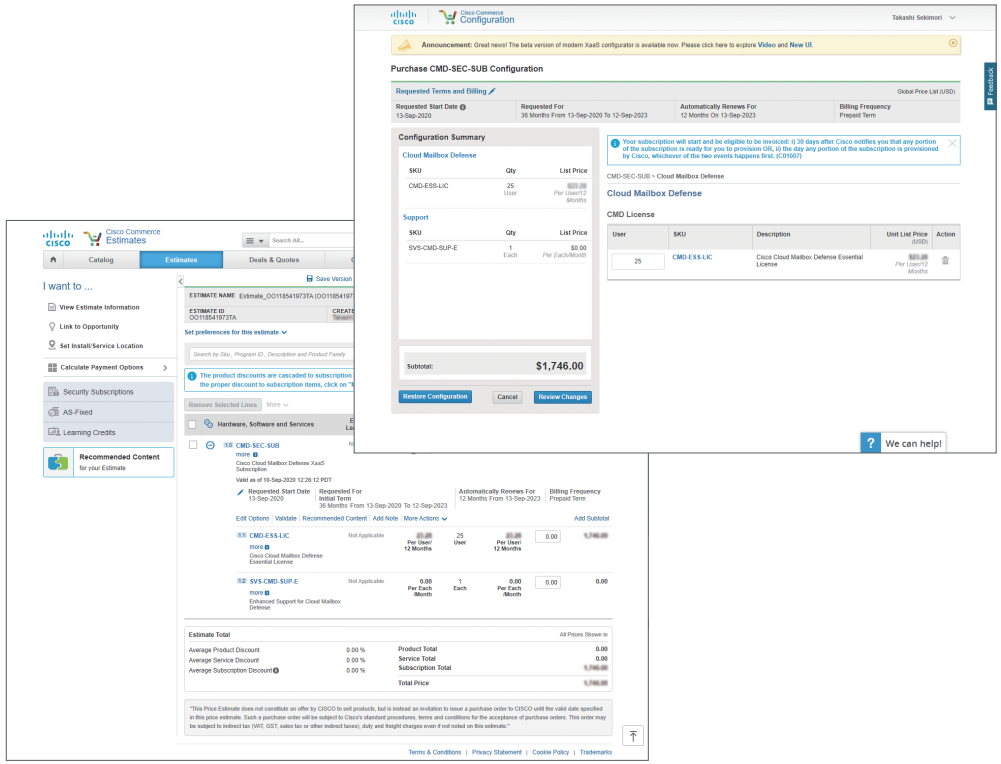
Product SKU*1	Description
SVS-CMD-SUP-E	Cloud Mailbox Defense Enhanced Support*2

*1 CMD-SEC-SUB is required in CCW. See Ordering Guide for details.
*2 Included with the purchase of CMD subscription.

Ordering and Licensing Guide

Cisco Cloud Mailbox Defense (CMD) is licensed on a subscription basis. Each end customer has only one subscription (per Azure region). The subscription is available for standard term lengths of 12, 36, and 60 months. Enhanced support services from Cisco are included by default.

CMD is licensed per seat. A seat is defined as a Microsoft 365 user. The number of seats ordered should match the number of Microsoft 365 users, who will be protected by CMD. Seat counts are independent of the number of devices or mailboxes that the user may have. The seat-based license follows a tiered-pricing model: pricing depends on the seat count and the term of the subscription. Sales and partner representatives should determine the correct number of users for each customer deployment so that the appropriate seat count is selected. Cisco Commerce Workspace (CCW) will dynamically determine the correct price associated with the seat count entered.



Cisco Cloud Mailbox Defense Licensing Summary

Licensing Model Element	Cloud Mailbox Defense
License Type	Subscription
Licensing Unit	Seats with bands
Minimum Units	25
Licensing Terms	12, 36, or 60 months
Billing Frequency	Prepaid term, annual billing
Renewal Terms	12 months
Renewal Type	Automatic renewal
Support Model	Enhanced Support (by default)

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud Mailbox Defense NEW

Cloud Email Needs Cloud Security

1. Email is Moving to the Cloud — But So are Threats

Cloud email platforms offer a number of unique advantages:

- Improved productivity
- Easier roaming and remote work
- Access to the latest features

But they're also creating new vulnerabilities for users, devices, and businesses.

Microsoft 365 phishing takeover is 1 of the 3 most common email threats.*1
By 2020, 50% of organizations using Microsoft 365 will rely on non-Microsoft tools to maintain consistent security.*2

2. Email Continues to be the #1 Threat Vector*3

Because email is the most widely used form of business communication, it's a major target for attacks.

- Common Email Threats
  - Ransomware
  - Phishing
  - Malware
  - Spam
  - Domain Compromise
  - Account Takeover
  - Internal Threats
  - Spoofing

of breaches occur via email, and cloud email platforms like Microsoft 365 don't necessarily have security that can keep up.*4

3. Built-in Email Security isn't Enough

Microsoft 365 provides basic email security, but its native controls can leave you susceptible to more advanced threats. In particular, Microsoft 365 lacks visibility into internal emails sent back and forth across your business.

4. Layer Your Security

To secure your Microsoft 365 mailboxes, you need to augment its native security with additional protection. This supplemental security solution should include:

- **Multiple security elements** to identify all the destructive elements of an email
- **Continual mailbox analysis** for proactive protection anywhere
- **Automated detection and remediation tools** to mitigate the spread of email-borne threats both inside and outside your organization

The solution is Cloud Email Security Supplements (CESS); Cisco Cloud Mailbox Defense.

*1 Source: Gartner, Market Guide for Email Security, Peter Firstbrook, Neil Wynne, June 6, 2019. *2 Source: Gartner, How to Enhance the Security of Office 365, 2017.
*3 Source: FBI IDC Report, 2019. *4 Source: Verizon 2019 Data Breach Investigations Report.

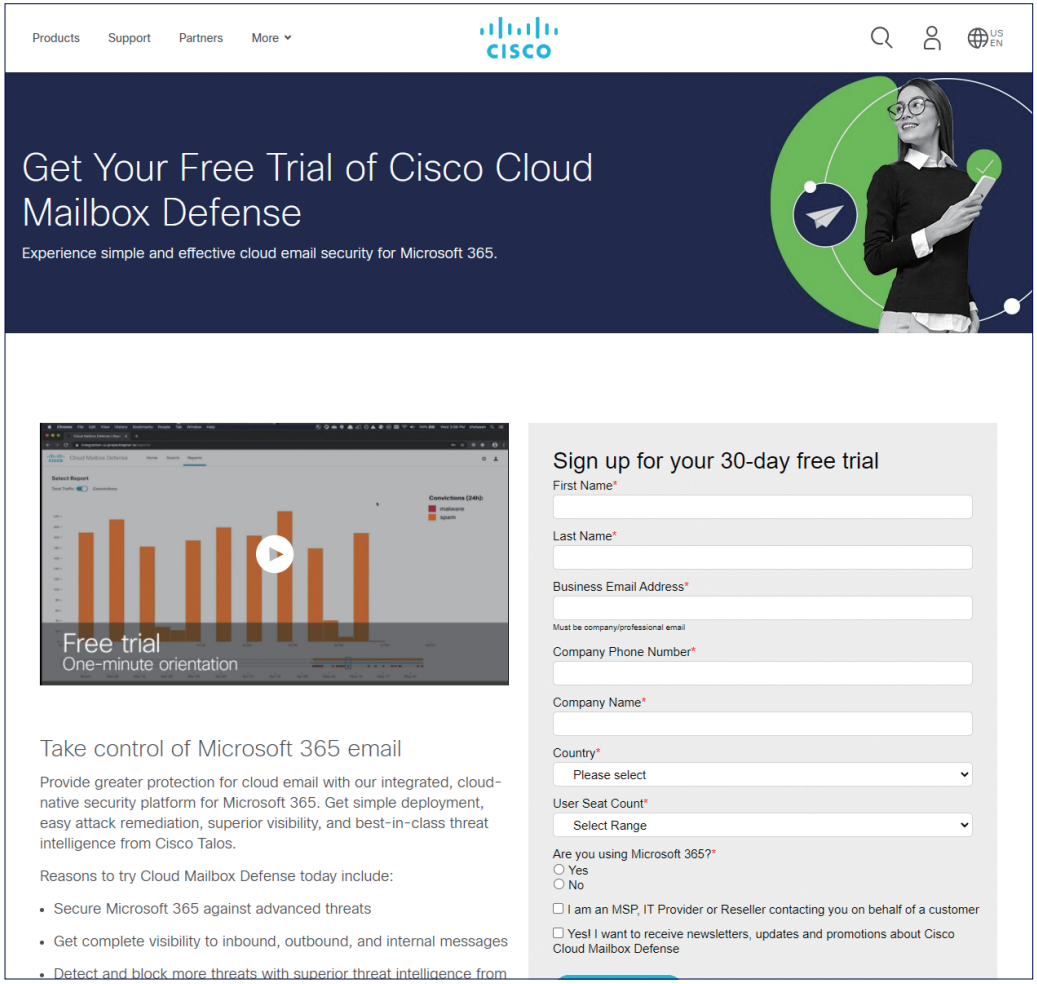
© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud Mailbox Defense NEW

Get Your Free Trial of Cisco Cloud Mailbox Defense

Sign up for a free 30-day trial and experience simple and effective cloud email security for Microsoft 365.

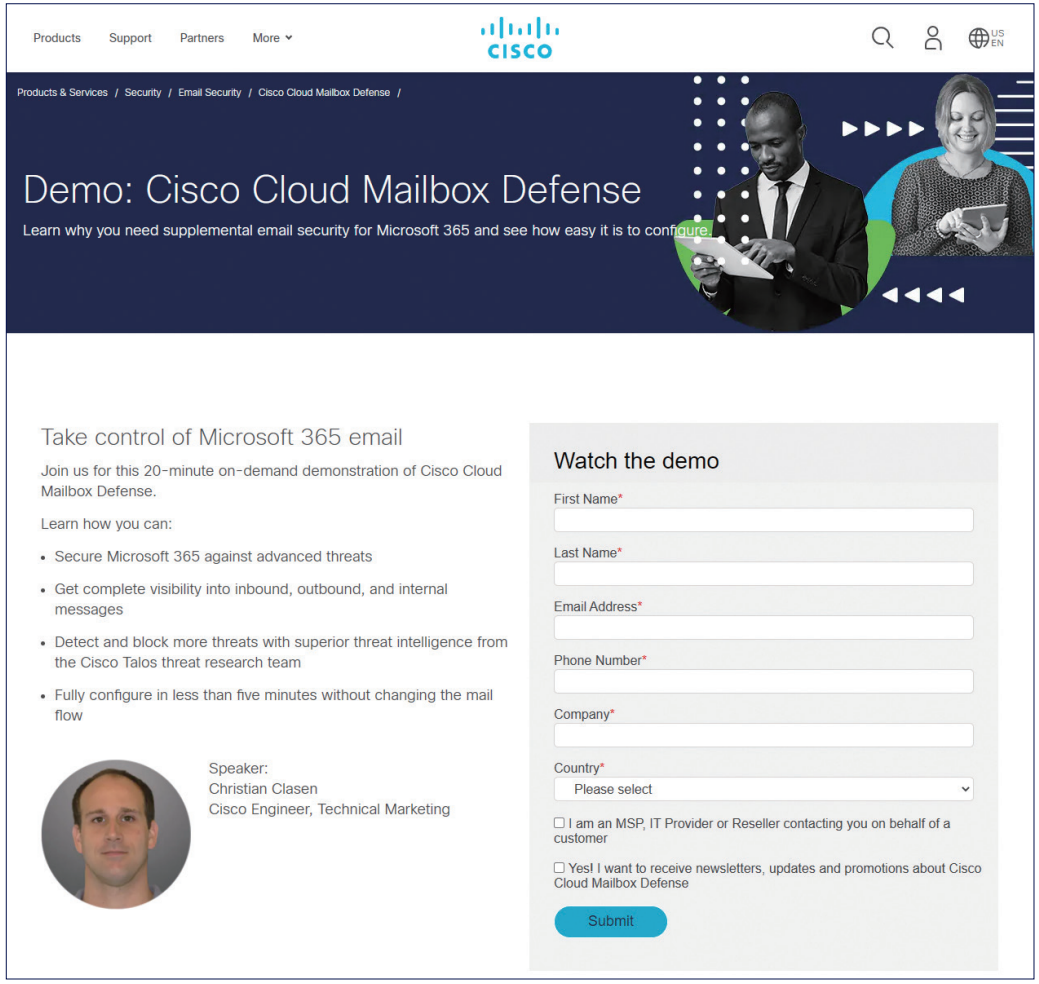
www.cisco.com/c/en/us/products/security/cloud-mailbox-defense/freetrial.html



Demo: Cisco Cloud Mailbox Defense

Learn why you need supplemental email security for Microsoft 365 and see how easy it is to configure.

www.cisco.com/c/en/us/products/security/cloud-mailbox-defense/demo.html



© 2020 Cisco and/or its affiliates. All rights reserved.