**Email Threat Defense** addresses potential gaps in *Microsoft 365* email security by leveraging proven Cisco email security technology to block advanced email threats like ransomware, business email compromise, phishing, spoofing and spam observed from external and lateral (internal East/West traffic) email transmissions.

## **Benefits:**

- Enhance Microsoft 365 security in less than 5 minutes without changing the mail flow
- Get complete visibility to inbound, outbound, and internal messages
- Combat advanced threats using Secure Endpoint, and Secure Malware Analytics.
- Leverage fast API-driven remediation of messages with malicious content.
- Detect and **block more threats** with superior threat intelligence from Cisco Talos™.
- **Simplify mail flow** by protecting your mailboxes without changing MX records.
- No hardware needed, all done through API calls directly to MS Azure.
- Single SKU (CMD-SEC-SUB) includes onboarding help and TAC support (25 users min.)

#### **Use Cases:**

#### **Efficacy Improvement:**

Traditional Secure Email Gateways (SEGs) not only lack visibility into user-to-user traffic, but also the ability to protect it. *Secure Email Threat Defense* extends protection past the perimeter to achieve both and can control internal traffic.

## Protecting organizations of all sizes:

For smaller organizations with limited resources, *Email Threat Defense* simplifies the experience and provides a format that requires little prior knowledge or oversight. Larger organizations can benefit from the increased intelligence provided by *Threat Defense* in combination with their existing SEG; whether Cisco or another solution.

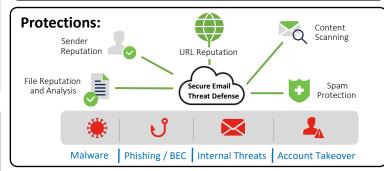
## **Ensuring Compliance and Privacy:**

Using *Email Threat Defense* architecture, full email message content never leaves *Azure*. Only metadata (e.g. sender, recipient, subject, URL's etc.) leaves the *Azure* environment to be searched. This maintains a strict level of compliance and customer privacy.

# **Discovery Questions:**

- Do you use MS365 Cloud?
- How many MS365 tenants/instances?
- Do you use a SEG solution? What vendor?
- Do you use different types of mailboxes? (Exchange Onpremise, Google, Postfix, etc.)
- Do you intend to deploy more than 100,000 seats?
- Do you require multiple Secure Email Threat Defense accounts? (i.e., separate instances are required per MS365 account).
- If so, how many and what is the rationale behind it?

Comparisons:	Threat Defense	Secure Email
Features:	Detelise	
O365 webmail support		
Additional webmail support		<b>✓</b>
On Premise / Hybrid		<b>✓</b>
Inspect Intra-office emails	<b>✓</b>	
Context / Behavioral Analysis	<b>✓</b>	
Spam Protection	✓	<b>✓</b>
File Reputation	✓	<b>✓</b>
File Analysis	<b>✓</b>	<b>✓</b>
Cloud URL Analysis	<b>✓</b>	<b>✓</b>
Data Loss Prevention		<b>✓</b>
Email Encryption		<b>✓</b>
URL Rewriting		<b>✓</b>
Post-Delivery Remediation	<b>✓</b>	<b>✓</b>
Talos Threat Intelligence	<b>✓</b>	<b>✓</b>
Trajectory and Conversation View	<b>✓</b>	
Grey-Mail Detection	<b>✓</b>	<b>✓</b>
No change to email flow	<b>✓</b>	



Resources:Release NotesFAQSalesResourcesUser GuideVideosOrder GuideAt-a-Glance30-day Free TrialData SheetPoV Best PracticesPublic page