CISCO
SECURE

Data sheet
Cisco public

Cisco Secure Email Threat Defense

Contents

Advanced threat detection capabilities to protect against the most advanced and pervasive threats

Today's organizations face a daunting challenge. Email is simultaneously the most important business communication tool and the leading attack vector for security breaches.

Losses caused by ransomware and Business Email Compromise (BEC) are staggering and continue to increase. In 2021, the FBI IC3 received 19,954 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses of nearly $2.4 billion, Phishing incidents up 40% YOY, Ransomware incidents cost up 120% in 2021, and number of victims up 85%.

According to the 2022 Verizon Data Breach Investigations Report (DBIR), this year, Ransomware has continued its upward trend with an almost 13% increase – a rise as big as the last five years combined (for a total of 25% this year).

The adoption of cloud-based email like Microsoft 365 continues to increase. Cloud email security is less costly and more scalable compared to on-premises appliances and this trend is driving growth in the SaaS email security market. Because email is vulnerable to advanced threats, Gartner has been recommending in the last two years for adding cloud email supplemental security to protect your cloud mailbox with layered security and diversified threat intelligence. Cisco Secure Email Threat Defense protects your organization against the number one threat vector: Email.

Product Overview

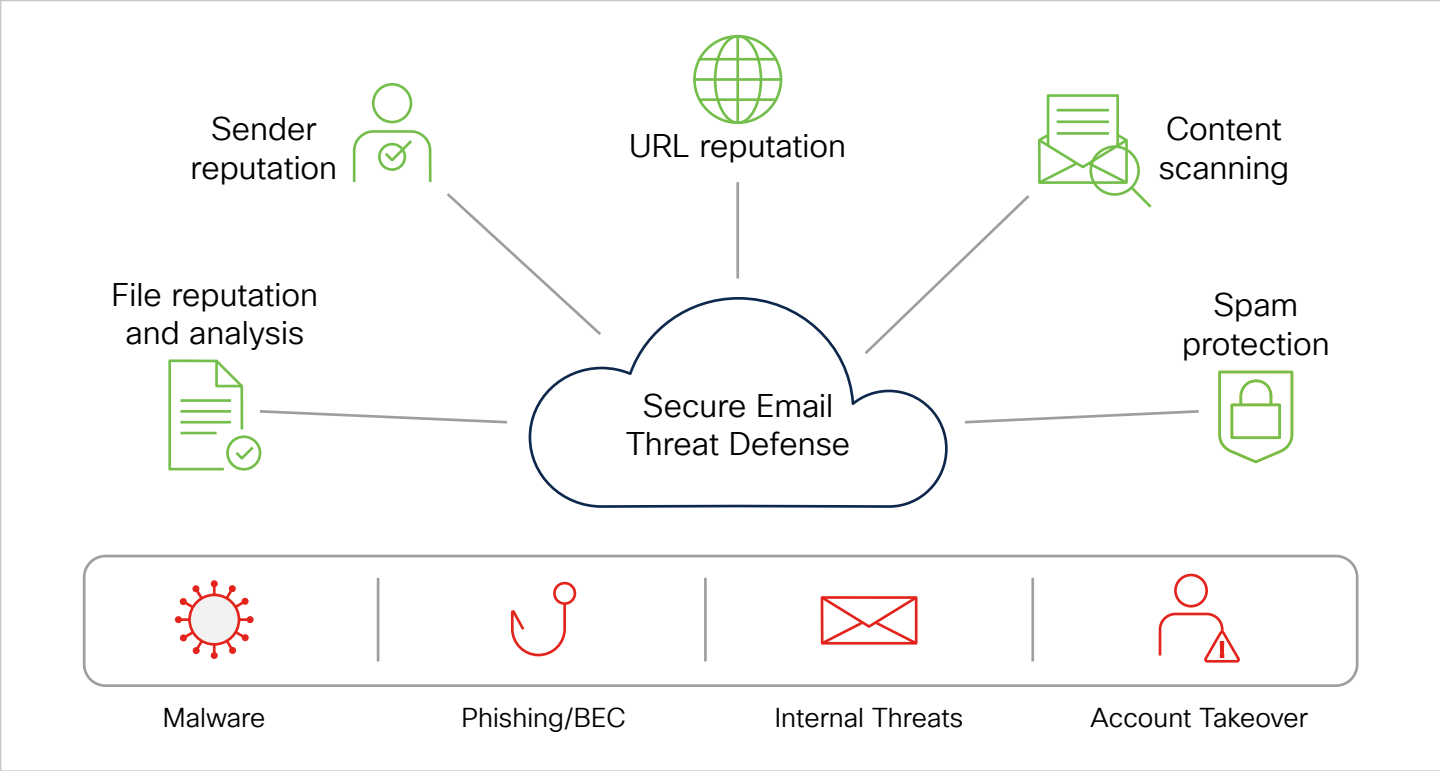
Email Threat Defense augments native Microsoft 365 security and provides complete visibility to inbound, outbound, and internal user-to-user messages.

With Email Threat Defense 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

Email Threat Defense – Solution components and differentiators

Email Threat Defense is a cloud-native solution leveraging superior threat intelligence from Cisco Talos. It has 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.



Advanced threat defense techniques and detectors

Cisco Secure Email combats phishing using sender authentication and BEC detection capabilities. It integrates machine learning and Artificial Intelligence engines that combine local identity and relationship modeling with real-time behavior analytics to protect against identity deception-based threats. It models trusted email behavior within organizations and between individuals. Among other key features, Email Threat Defense will provide the following benefits:

- Uncover known, emerging and targeted threats with advanced threat detection capabilities
- Identify malicious techniques and gain context for specific business risks
- Rapidly search for dangerous threats and remediate them in real-time
- Utilize searchable threat telemetry to categorize threats and understand which parts of your organization are most vulnerable to attack

Talos: Visibility, Intelligence and Response

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 threat analysis. 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

Email Threat Defense 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

Email Threat Defense has a single interface for reporting, configuration and tracking. Email Threat Defense 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 judgment.

Why choose Email Threat Defense?

Email Threat Defense leverages 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

Email Threat Defense adds an additional layer of security to native Microsoft 365 email security by using industry-leading threat intelligence from Cisco Talos, Cisco Secure Endpoint(AMP), and Secure Malware Analytics–including vast cross-vector threat intelligence from web, network, and endpoint-based sources.

Protect against sophisticated and targeted attacks

Email Threat Defense 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 remediates threats irrespective of the timeline of identification.

Enhance your Extended Detection and Response (XDR) strategy

As an important part of a larger Extended Detection and Response strategy, Secure Email defends against critical threats with industry-leading threat intelligence, advanced threat detection capabilities and vital telemetry that informs strategic threat protection. In combination with numerous third-party integration partners and the larger Cisco Secure portfolio of products, this provides the visibility, efficiency, simplicity and telemetry that empower your team to act quickly.

Configure and deploy instantly

Email Threat Defense 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

Email Threat Defense 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 a global scale.

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

Whether 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. Email Threat Defense scans all messages in the mailbox in all directions – inbound, outbound, or internal. It allows administrators to search messages across all mailboxes.

Powerful Reporting

Cisco Secure Email Threat Defense provides comprehensive reporting capabilities to help understand what the most common attack vectors are aimed at your organization, the top targeted users, the business risks, and the techniques used. With these reporting capabilities, we will be more prepared to decide on additional security policies, end-user training, etc.

Performing threat analysis with Cisco SecureX threat response casebooks

Email Threat Defense is 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.

Technical details

Deployment options

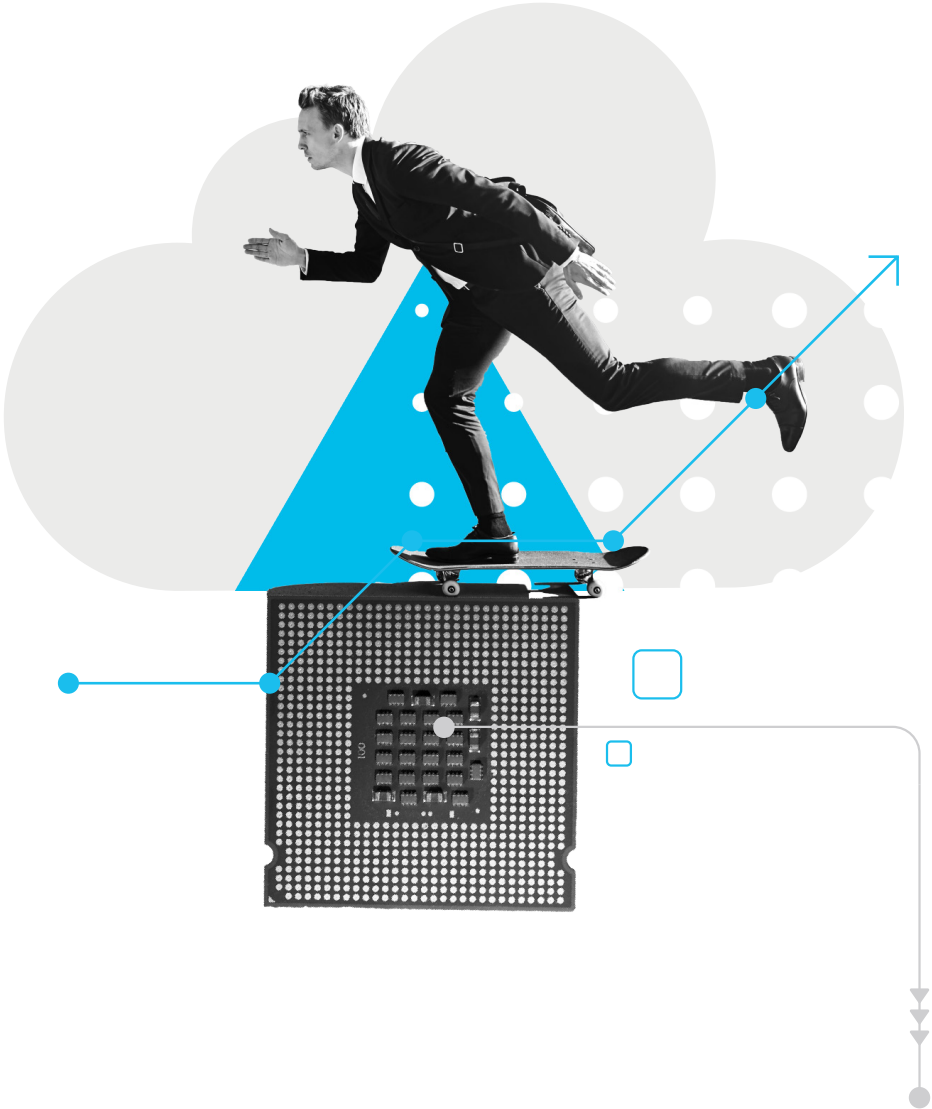
- Audit
- Audit with Enforcement

Enforcement actions

- Move to Trash
- Move to Junk
- Move to Inbox
- Move to Quarantine
- Delete
- No action

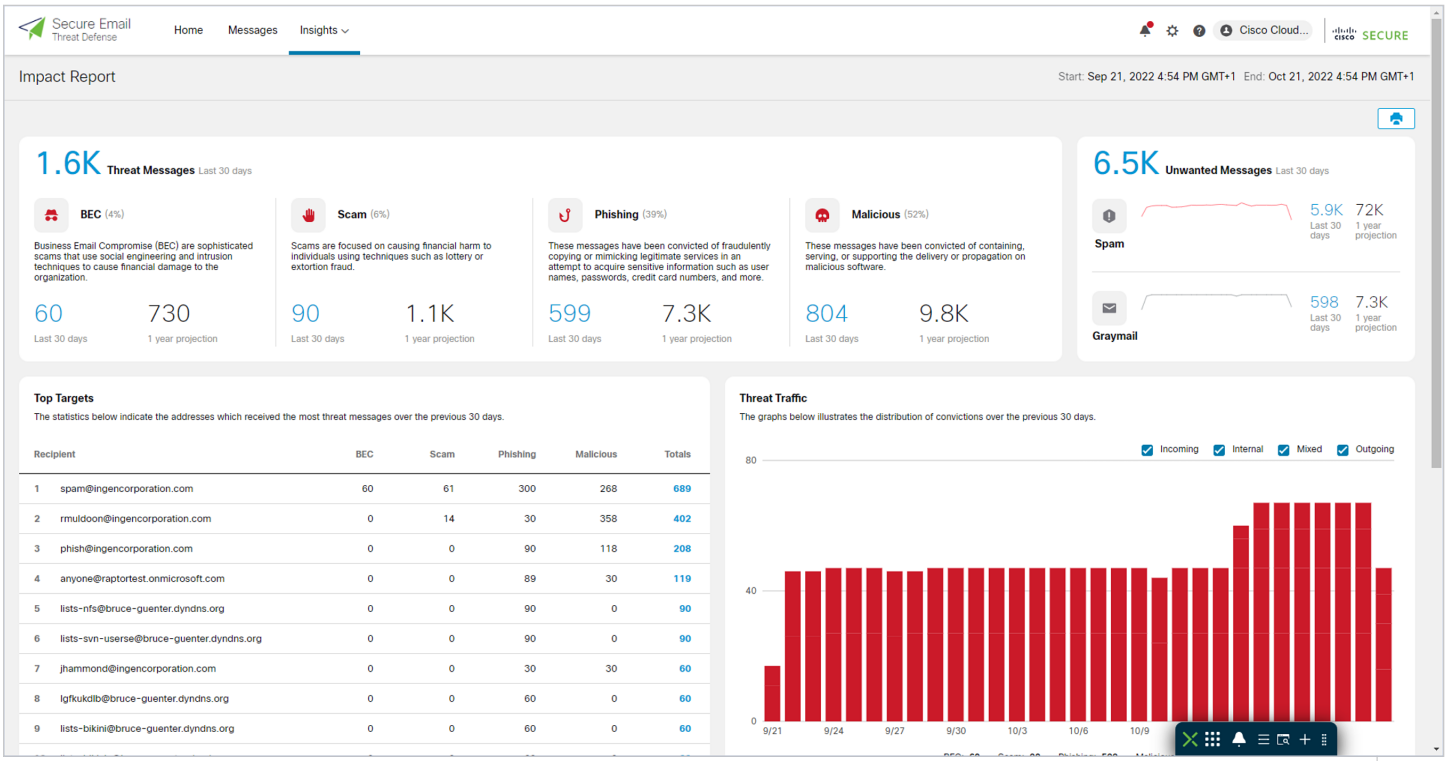
Verdicts supported:

- BEC
- Scam
- Phishing
- Malicious
- Spam
- Graymail
- Neutral



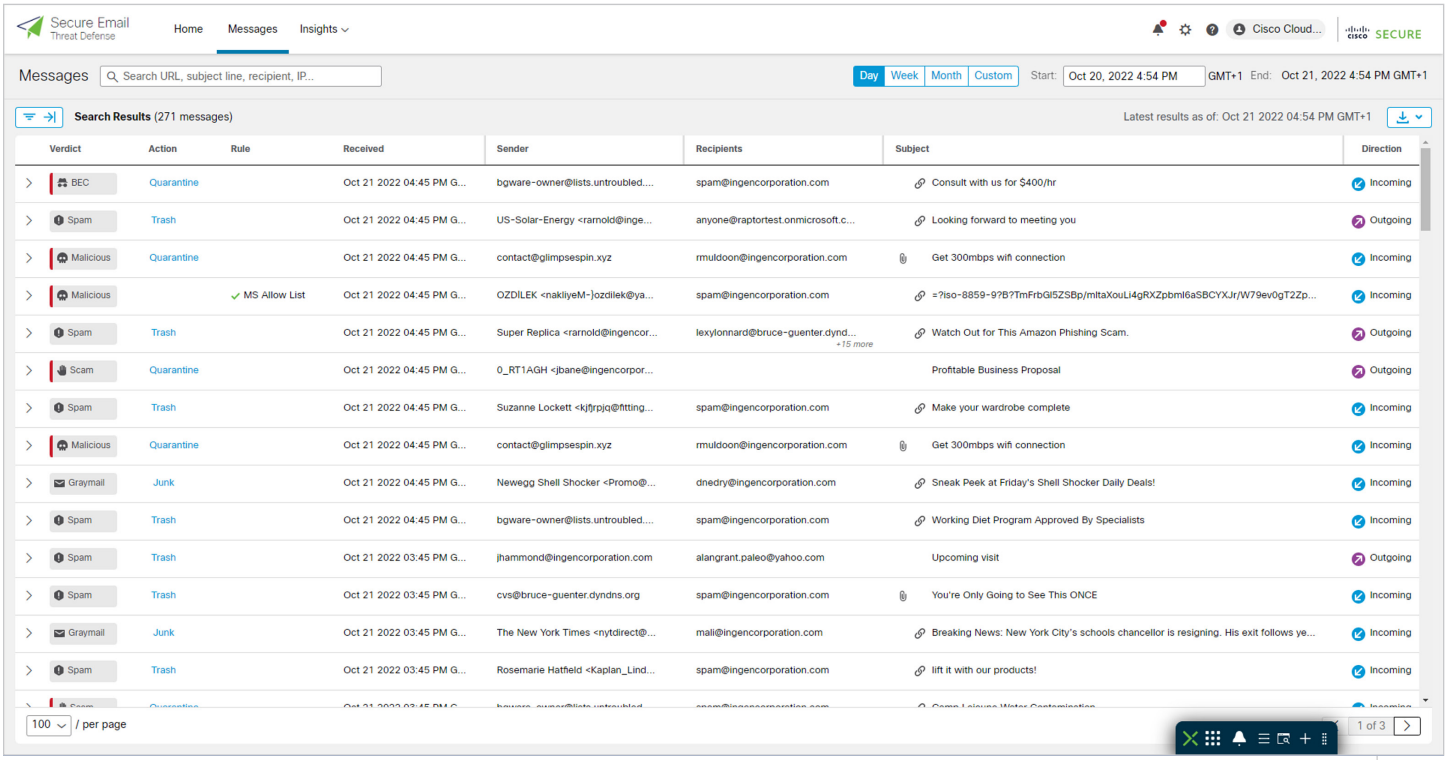
Reporting

- Trend Report
- Impact Report
  - Metrics and 12-month Projections about:
    - BEC
    - Scam
    - Phishing
    - Malicious
    - Spam and Graymail (unwanted messages)
  - Top targets – indicate the addresses which received the most threat messages, per type of threat
  - Threat Traffic per origin (internal, incoming, outgoing, mixed)
  - Potentially Compromised Accounts – The internal addresses listed here were seen sending threat messages from within the organization
  - Protection by Email Threat Defense – metrics about the protection Email Threat Defense provided to recipient mailboxes in your environment



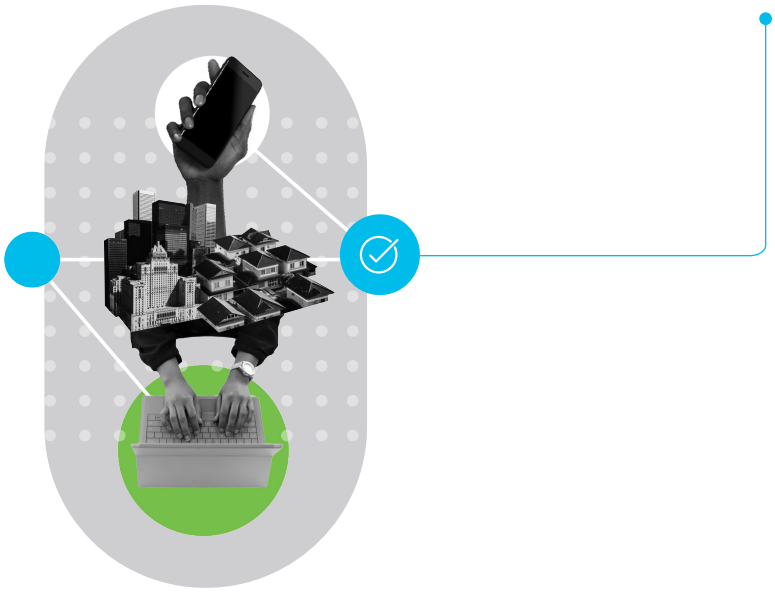
Dashboard

- Total Messages scanned (internal, incoming, outgoing, mixed)
- Threat Traffic
- Spam Traffic
- Graymail Traffic
- Message details with Verdict, Sender and Recipient details, Attachment information, included URL
- Conviction details (why was that message convicted, which detectors were used, what evidence was found)
- Conversation view – To whom the email was sent
- Timeline view – From receiving, convicting, etc.



Search capabilities

- Sender
- Recipient
- Subject
- Envelope From address
- Reply To
- SMTP Server IP
- SMTP Client IP
- X-Originating IP
- Organization-BCC
- URL
- Attachment name
- MS Message ID



Simplified Ordering and Support

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

Use the CMD-SEC-SUB top-level part number in CCW to order Secure Email Threat Defense.

C78-3274733-00 11/22