Cisco Secure Email Threat Defense

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Product overview 4

ETD Essentials **5**

ETD Advantage **5**

Cisco Secure Email Threat Defense – solution components and differentiators 6

ETD Essentials **6**

ETD Advantage **7**

Advanced threat defense techniques and detectors 7

AI- and ML-powered detection for modern email attacks Error! Bookmark not defined.

Talos: visibility, intelligence, and response **9**

Cisco Secure Endpoint and Cisco Secure Malware Analytics **9**

Flexible architecture **9**

Unified user interface **10**

Why choose Cisco Secure Email Threat Defense? 10

Augment native Microsoft 365 security **10**

Gateway mode and support for any email server **10**

Protect against sophisticated and targeted attacks **10**

Enhance user awareness with subject tagging **10**

URL allow lists **10**

Enhance your Extended Detection and Response (XDR) strategy **11**

Simplify deployment **11**

Leverage a cloud-native solution **11**

Get complete email visibility **11**

Powerful reporting **11**

Extend ETD with MCP-based integrations (*limited availability) **11**

Technical details 12

Deployment Models **12**

ETD Advantage **12**

Enforcement actions **12**

Verdicts supported **12**

High Impact Personnel list **13**

Reporting **13**

Metrics and projections **14**

© 2026 Cisco and/or its affiliates. All rights reserved.

Message search 15
Policies 16
Connection handling: block and allow rules 16
Message downloads 16
REST APIs 16
Simplified ordering and support 17
ETD Essentials 17
ETD Advantage 17
Third-party validation and accolades 17
Email Threat Defense achieves SE Labs AAA rating 17
2025 KuppingerCole Leadership Compass for Email Security 17

© 2026 Cisco and/or its affiliates. All rights reserved.

Advanced threat detection to protect against pervasive and sophisticated 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) remain staggering and continue to reach record highs. In 2025, the FBI IC3 reported that Business Email Compromise losses surpassed $3 billion, making it one of the most financially damaging categories of cybercrime. Additionally, ransomware incidents rose to 3,611 complaints, representing a 14.4% increase from 2024.

The migration to cloud-native email environments, including Microsoft 365 and Google Workspace, remains a dominant architectural trend. While these platforms offer inherent scalability and cost efficiencies compared to legacy on-premises appliances, they often leave organizations exposed to sophisticated, non-malware-based threats. Consequently, there is a critical industry consensus on the necessity of implementing supplemental, API-integrated security layers. This approach ensures robust protection for cloud mailboxes by providing advanced threat detection, behavioral analysis, and the diversified threat intelligence required to mitigate complex, email-borne attack vectors.

Cisco Secure Email Threat Defense (ETD) protects organizations against the number one threat vector: email.

Product overview

Cisco Secure Email Threat Defense is a cloud-native, full-featured email security solution that provides visibility into inbound, outbound, and internal email traffic.

Cisco ETD is available as:

- supplemental Microsoft 365 protection
- gateway-based protection for diverse email environments including Google Workspace and MS Exchange

With Cisco Secure Email Threat Defense, organizations can:

- Detect, block, and remediate threats across supported deployment models with superior threat intelligence from Cisco Talos, one of the largest threat research and efficacy teams in the industry
- Combat advanced threats using Cisco Malware Defense and Cisco Secure Malware Analytics
- Easily integrate with Cisco XDR and other SOC threat analysis and automation platforms
- Gain complete visibility into inbound, outbound, and internal messages
- Search, report on, and track messages using an integrated dashboard with conversation view and message trajectory
- Receive retrospective verdicts on messages that were not initially identified as malicious
- Protect users from modern email-based attacks such as QR code phishing, brand impersonation, user impersonation, and more

© 2026 Cisco and/or its affiliates. All rights reserved.

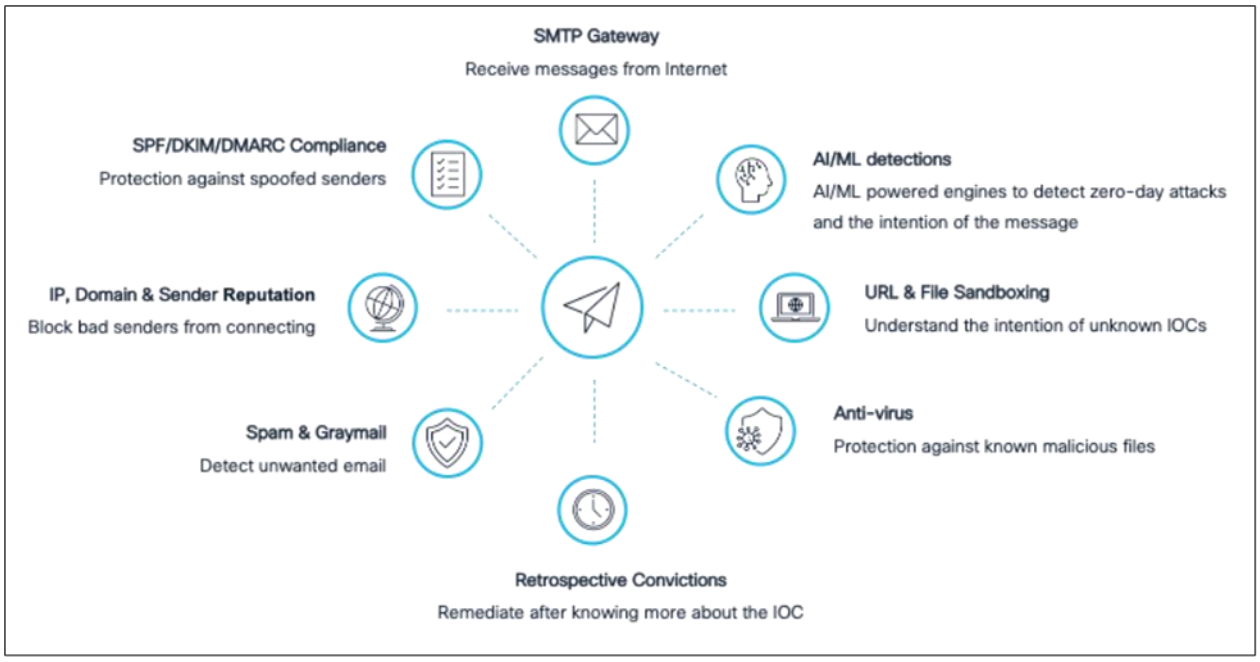
Cisco Secure Email Threat Defense is available in two license-aligned deployment options:

ETD Essentials

- Designed for organizations using Microsoft 365 that want to add a supplemental layer of protection. ETD Essentials uses journaling to provide additional visibility and threat detection for Microsoft 365 environments.

ETD Advantage

- Designed for organizations that require a gateway deployment. ETD Advantage performs pre-delivery inspection to stop threats before they reach the mailbox. It supports any mail server, including Microsoft 365, Google Workspace, and Microsoft Exchange on-premises. For Microsoft 365 environments, ETD Advantage can also leverage Microsoft APIs to enable extended capabilities.



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Email Threat Defense – solution components and differentiators

Cisco Secure Email Threat Defense is a cloud-native, full-featured email security solution designed to provide broad visibility and protection across inbound, outbound, and internal email traffic. By leveraging industry-leading threat intelligence from Cisco Talos, ETD helps defend against advanced threats including Ransomware, Business Email Compromise, Phishing, and Account Takeover attacks.

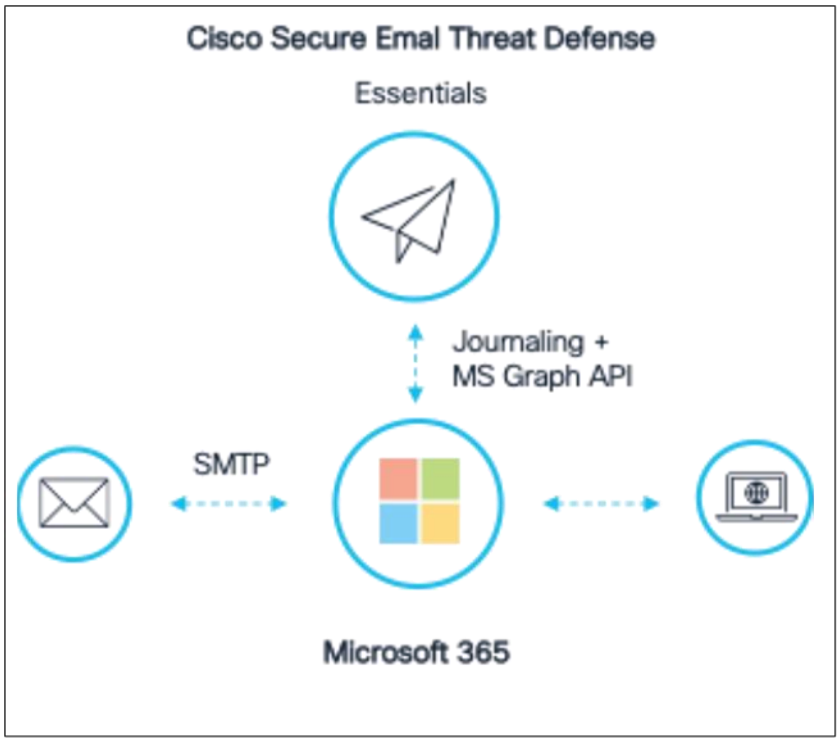
License options: ETD Essentials vs. ETD Advantage

Feature	ETD Essentials	ETD Advantage
License / deployment model	Supplemental Microsoft 365 protection using journaling	Gateway deployment & Supplemental Microsoft 365 protection using journaling for internal messages
Message Directions	Inbound, Internal, Outbound(visibility-only)	Inbound, Internal, Outbound
Supported platforms	Microsoft 365	Microsoft 365, Google Workspace, Microsoft Exchange on-premises, and other mail servers
Mail flow	No inline gateway change required	Inline / pre-delivery inspection in the mail flow
Inspection approach	Supplemental visibility and threat detection for Microsoft 365	Gateway blocking, policy enforcement, pre-delivery protection, Supplemental Microsoft 365 protection
Microsoft 365 extended capabilities	Supported through Microsoft APIs	Supported through Microsoft APIs
Best fit	Organizations augmenting native Microsoft 365 protection	Organizations requiring gateway security and broad platform compatibility
DLP support	Not available	Integrates with Cisco Secure Access DLP (additional licensing is required)

ETD Essentials

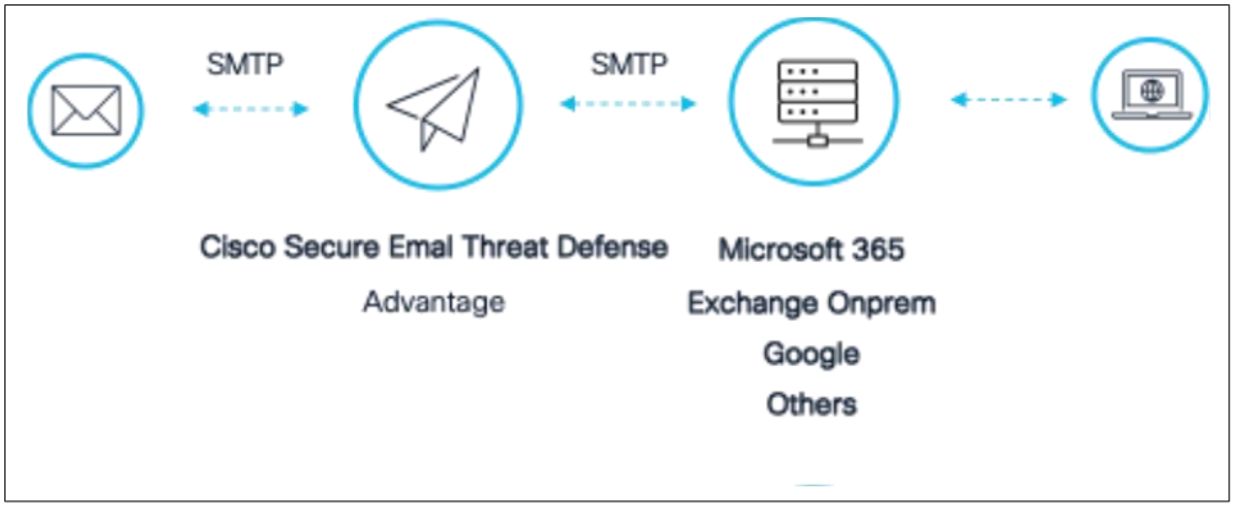
- ETD Essentials is designed for organizations using Microsoft 365 that want to strengthen native email security with an additional layer of protection. ETD Essentials uses journaling for supplemental message visibility and threat detection in Microsoft 365 environments and can use Microsoft APIs for supported visibility and remediation workflows.

© 2026 Cisco and/or its affiliates. All rights reserved.



ETD Advantage

- ETD Advantage is designed for organizations that require gateway-based protection. It sits in the mail flow and performs pre-delivery inspection to stop threats before they reach user mailboxes. ETD Advantage supports any email server solution, including Google Workspace and Microsoft Exchange on-premises. In Microsoft 365 environments, ETD Advantage can also use Microsoft APIs to enable extended capabilities.



Advanced threat defense techniques and detectors

Cisco Secure Email Threat Defense combats phishing through sender authentication and Business Email Compromise detection capabilities. It integrates machine learning and artificial intelligence engines that combine local identity and relationship modeling with real-time behavioral analytics to defend against identity deception-based threats. It models trusted email behavior within organizations and between individuals.

© 2026 Cisco and/or its affiliates. All rights reserved.

Among its key benefits, Cisco Secure Email Threat Defense helps organizations:

- 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
- Use searchable threat telemetry to categorize threats and understand which parts of the organization are most vulnerable to attack

AI- and ML-powered detection for modern email attacks

Modern email attacks increasingly rely on deception, business context, and social engineering to evade traditional reputation- and signature-based controls. Cisco Secure Email Threat Defense uses machine learning and artificial intelligence as a foundational layer in its detection stack, combining **local identity and relationship modeling with real-time behavioral analytics** to understand what trusted communication looks like within the organization and between individuals.

© 2026 Cisco and/or its affiliates. All rights reserved.

This behavioral approach helps ETD identify anomalies that may indicate phishing, Business Email Compromise, account takeover, and impersonation attempts—even when a message does not contain a known malicious attachment, URL, or previously seen indicator. By analyzing sender behavior, communication patterns, and message context, ETD helps detect sophisticated and previously unseen attacks, including threats that depend on manipulation rather than malware.

Examples include:

- **Brand impersonation**, where attackers imitate trusted companies or services to influence user action
- **User impersonation**, where messages appear to come from executives, employees, or other known contacts
- **Urgency-based social engineering**, such as messages designed to pressure recipients into acting quickly
- **Unusual calls to action**, including requests that deviate from expected communication or business processes
- **Suspicious reply-chain or conversation-style attacks**, where a message attempts to appear as part of a legitimate ongoing exchange

When combined with **sender authentication, Cisco Talos threat intelligence, Cisco Secure Endpoint**, and **Cisco Secure Malware Analytics**, ETD provides a layered approach to uncovering known, emerging, and targeted threats. **Retrospective verdicts** further strengthen protection by allowing ETD to reassess messages as new intelligence becomes available, helping organizations respond to threats that were not initially identified as malicious.

Talos: visibility, intelligence, and response

As one of the largest global providers of cutting-edge security research and intelligence, Cisco Talos delivers high-impact, actionable security content and tools. This gives 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 shares threat intelligence across Cisco security devices, helping unify security across endpoints, networks, email, the cloud, and the web.

Flexible architecture

Cisco Secure Email Threat Defense supports flexible deployment models based on the selected license:

- ETD Essentials provides supplemental threat visibility and protection for Microsoft 365 using journaling, or using a connector from the Cisco Secure Email Gateway and Cisco Secure Email Cloud Gateway
- ETD Advantage provides gateway-based pre-delivery protection and, in Microsoft 365 environments, can also use journaling to extend visibility into internal messages, and can leverage Microsoft APIs for extended visibility and post-delivery remediation.

© 2026 Cisco and/or its affiliates. All rights reserved.

- ETD Advantage can be used with a broad range of email environments, including Google Workspace and Microsoft Exchange on-premises
- In addition, ETD offers RESTful APIs to enable flexible integration with other security tools and operational workflows.

Unified user interface

Cisco Secure Email Threat Defense provides a single interface for reporting, configuration, investigation, and tracking. It includes conversation view and message trajectory visibility to help administrators understand the context of email activity and make more informed decisions.

Why choose Cisco Secure Email Threat Defense?

Augment native Microsoft 365 security

ETD Essentials adds a supplemental layer of protection to native Microsoft 365 email security using industry-leading threat intelligence from Cisco Talos, Cisco Secure Endpoint, and Cisco Secure Malware Analytics.

Gateway mode and support for any email server

ETD Advantage provides gateway-based protection for organizations that require pre-delivery inspection and supports any email server solution, including Google Workspace and Microsoft Exchange on-premises. For Microsoft 365, ETD Advantage also supports extended functionality through Microsoft APIs.

Protect against sophisticated and targeted attacks

Cisco Secure Email Threat Defense helps protect against phishing, Business Email Compromise, malicious QR codes, ransomware, and account takeover attacks by continuously analyzing messages and applying a layer of security that becomes increasingly effective even as new intelligence becomes available.

Enhance user awareness with subject tagging

For ETD Advantage gateway deployments handling SMTP/inline incoming messages, administrators can configure subject line modifications as part of the Base Policy. This gives users immediate context about the email they are receiving and increases vigilance against potential threats. Supported tags include:

[Spam]

[Graymail]

[Marketing]

[Bulk]

[External]

[Malicious]

[Potentially harmful]

URL allow lists

Cisco Secure Email Threat Defense allows administrators to create allow lists for specific URLs. When a URL is included in this list, it is bypassed during analysis so that its reputation does not trigger threat detection.

© 2026 Cisco and/or its affiliates. All rights reserved.

Enhance your Extended Detection and Response (XDR) strategy

As an important part of a broader Extended Detection and Response strategy, Cisco Secure Email Threat Defense helps defend against critical threats with advanced detection capabilities and telemetry that informs strategic threat protection. In combination with third-party integrations and the wider Cisco Security portfolio, this provides the visibility, efficiency, simplicity, and telemetry that help teams act quickly. Cisco Secure Email Threat Defense integrates with Cisco XDR Threat Response casebooks to record, organize, and share observables of interest during investigations across multiple products.

Simplify deployment

Cisco Secure Email Threat Defense supports fast deployment based on the chosen model:

- ETD Essentials can be deployed quickly for Microsoft 365 as a supplemental journaling-based solution
- ETD Essentials can be deployed easily for threat visibility in conjunction with existing Cisco Secure Email Gateway and Cisco Secure Email Cloud Gateway, without requiring M365 integration
- ETD Advantage can be deployed as a gateway for inline inspection and broader email platform coverage
- In Microsoft 365 environments, ETD Advantage can also use Microsoft APIs to extend capabilities

Leverage a cloud-native solution

Cisco Secure Email Threat Defense is a cloud-native solution designed for high availability, optimized performance, and faster detection and response. It automatically scales resources based on demand and can be deployed quickly across regions for global organizations.

Get complete email visibility

Whether internal or external, every message entering or leaving a mailbox should be treated with the right level of scrutiny. ETD helps organizations minimize the spread of insider threats and the impact of compromised accounts by providing visibility into message activity across the environment.

Powerful reporting

Cisco Secure Email Threat Defense provides comprehensive reporting to help organizations understand the most common attack vectors targeting them, the users most frequently targeted, the associated business risks, and the techniques being used. These insights can help guide security policy decisions and end-user training initiatives.

Extend ETD with MCP-based integrations (*limited availability)

An MCP server for Cisco Secure Email Threat Defense can make ETD data and actions more accessible to AI assistants, automation platforms, and operational workflows through a standardized interface. Because ETD already provides secure REST APIs for message search, reporting, status, event logs, and remediation, an MCP layer can help teams connect those capabilities to investigation and response workflows faster and with less custom integration effort.

This gives security teams a more efficient way to work with ETD telemetry and controls. Analysts can retrieve message context, verdicts, evidence, and reporting data more quickly, then use approved workflows to support search, reclassification, and remediation actions. The result is faster investigations, more consistent operations, and better use of ETD within broader security and AI-driven workflows.

© 2026 Cisco and/or its affiliates. All rights reserved.

Technical details

Deployment Models

ETD Essentials

Supplemental protection for Microsoft 365 using journaling-based deployment model

Where Microsoft API-based capabilities are used, configurations can support:

- Read-Write: integration with Microsoft 365 for visibility and remediation
- Read: integration with Microsoft 365 for visibility only

Threat visibility using connector integration with Cisco Secure Email gateways, independent of downstream mailbox platform

ETD Advantage

Gateway-based deployment supporting a broad range of email server environments, including:

- Microsoft 365
- Google Workspace
- Microsoft Exchange on-premises

Microsoft 365 extended capabilities with ETD Advantage for Microsoft 365 environments, ETD Advantage can also leverage Microsoft APIs to enable extended capabilities such as enhanced visibility and supported remediation workflows.

Where Microsoft API-based capabilities are used, configurations can support:

- Read-Write: integration with Microsoft 365 for visibility and remediation
- Read: integration with Microsoft 365 for visibility only

For non-Microsoft environments, no Microsoft authentication is required.

Enforcement actions

Supported enforcement actions include:

- Move to Trash
- Move to Junk
- Move to Inbox
- Move to Quarantine
- Delete
- Drop / Deliver (for gateway deployments)
- No action

Verdicts supported

- BEC
- Scam
- Phishing

© 2026 Cisco and/or its affiliates. All rights reserved.

- Malicious
- Spam
- Graymail
- Neutral

High Impact Personnel list

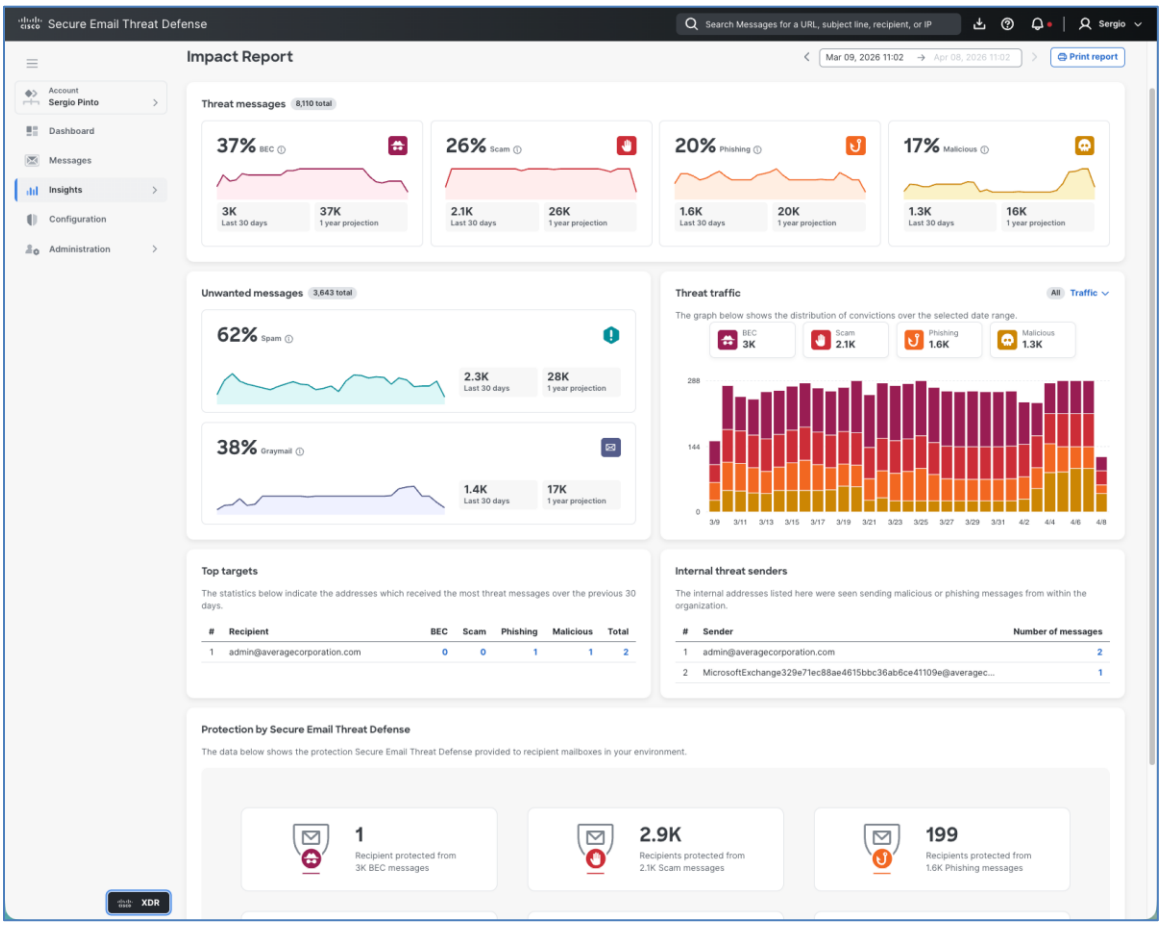
Important personnel, such as members of executive leadership teams, are often at higher risk of impersonation. The High Impact Personnel list helps Secure Email Threat Defense defend the organization from impersonation attacks.

Administrators can create a list of up to 500 people to be sent to Cisco Talos for higher scrutiny on display name and sender email address. Deviations from the configured information for an individual can be identified as a technique in the Verdict Details panel of detected threats.

Reporting

Available Reports

- Trend Report
- Blocked Connections Logs (when deployed in gateway mode)
- Impact Report



© 2026 Cisco and/or its affiliates. All rights reserved.

Metrics and projections

Reporting includes metrics and 12-month projections for:

- BEC
- Scam
- Phishing
- Malicious
- Spam and Graymail

Additional reporting includes:

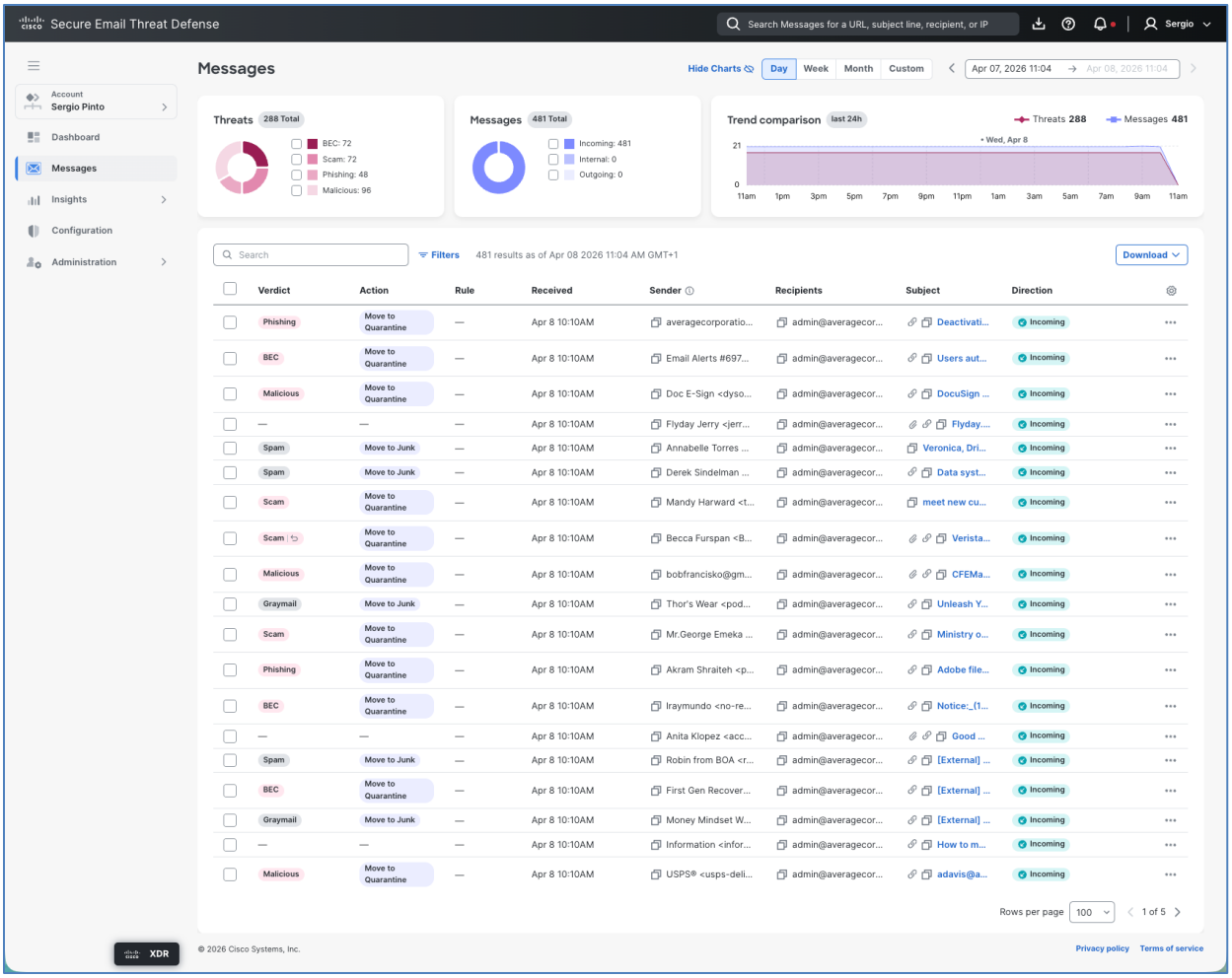
- Top targets: addresses that received the most threat messages, by threat type
- Threat traffic per origin: internal, incoming, outgoing, and mixed
- Potentially compromised accounts: internal addresses observed sending threat messages from within the organization
- Protection by Cisco Secure Email Threat Defense: metrics about the protection provided to recipient mailboxes

Dashboard

The dashboard includes:

- Total messages scanned (internal, incoming, outgoing, mixed)
- Threat traffic
- Spam traffic
- Graymail traffic
- Message details with verdict, sender and recipient details, attachment information, and URLs
- Conviction details, including detectors used and evidence found
- Conversation view
- Timeline view from receipt through conviction and action

© 2026 Cisco and/or its affiliates. All rights reserved.



Message search

Search capabilities

Administrators can search using:

- Sender
- Recipient
- Subject
- Envelope From address
- Reply-To
- SMTP server IP
- SMTP client IP
- X-Originating IP
- Organization-BCC
- URL
- Attachment name
- Microsoft Message ID

© 2026 Cisco and/or its affiliates. All rights reserved.

Policies

The Base Policy defines default remediation actions. Administrators can indicate different actions for different message types such as threats, spam, and graymail, as well as by message direction.

Policy exception rules can be created by:

- Senders (all message sources)
- Recipients (SMTP message sources)
- Rules are applied in ranked order and can be reordered as needed.
- Supported rule criteria
- Sender rules
- Email addresses
- Domains
- IP addresses
- CIDR blocks
- Recipient rules
- Email address
- Domain
- Supported Microsoft Groups

Connection handling: block and allow rules

When ETD is deployed in gateway mode, administrators can define which IP addresses are allowed to communicate with the solution. By using hostnames/FQDNs and IP addresses, allow and block lists can be created. Additional information about blocked connections is available in the Blocked Connections Logs report.

Message downloads

From the Messages page, administrators can download filtered data or longer-duration search results as a CSV file.

Super-admin and admin users can also request EML downloads (copies of the message) from the expanded message view.

REST APIs

Cisco Secure Email Threat Defense APIs allow partners and customers to programmatically access and consume data in a secure and scalable manner. These APIs can be used to create custom reports and dashboards and to better manage operational workflows.

Available APIs include:

- Authentication API
- Message Search API
- Reclassification and Remediation API
- Status API

© 2026 Cisco and/or its affiliates. All rights reserved.

- Reporting API
- Message Events Logs API
- Connection Logs API

For more information, see the API documentation: https://developer.cisco.com/docs/message-search-api/

Simplified ordering and support

Ordering Cisco Secure Email Threat Defense is straightforward. ETD is available in two options:

ETD Essentials

Supplemental Microsoft 365 protection using journaling. It can be ordered under ETD-SEC-SUB, and under CSEMAIL-SEC-SUB as an addon for existing ESA/CES gateway customers. ETD Essentials is also available under User and Breach Suites.

ETD Advantage

Gateway deployment for any email server, including Microsoft 365, Google Workspace, and Microsoft Exchange on-premises. In Microsoft 365 environments, ETD Advantage also supports extended capabilities through Microsoft APIs. It can be ordered under ETD-SEC-SUB

Cisco Secure Email Threat Defense is available as a subscription offering with 1-, 3-, or 5-year terms. High-Value Support Services are included by default.

Third-party validation and accolades

Email Threat Defense achieves SE Labs AAA rating

SE LABS tested Cisco Secure Email Threat Defense, against a mixture of targeted attacks using well-established techniques and public attacks that were found to be live on the internet at the time of the test. The results indicate how effectively the service detected and/or protected against those threats in real time and shortly after the attacks took place. ETD earned the highest rating.

2025 KuppingerCole Leadership Compass for Email Security

“It is a flexible and powerful tool for email protection. We use it throughout the organization and have had no problems since. The performance of this tool is high, and it has advanced security features that ensure the protection of internal and cloud-based emails from any external cyber threats. Another amazing quality is the ease with which it integrates with Office 365; such integration has been helpful in the organization. Secure Email Threat Defense has once again set itself apart from its competition in the KuppingerCole Leadership Compass, with top rankings in four different categories. This report provides an overview of the email security market and a compass to help customers find a solution that best meets their needs.

In 2025 report, Secure Email Threat Defense is ranked as an Overall, Product, Innovation, and Market Leader.”

© 2026 Cisco and/or its affiliates. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

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: https://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. (1110R)

Printed in USA C78-3274733-02 05/26

© 2026 Cisco and/or its affiliates. All rights reserved.