Advanced Threat Protection for Microsoft 365

Summary

While Microsoft E3 provides only basic phishing and spam filtering, E5 offers some advanced email threat detection. Microsoft customers currently using E3 may be moving away from secure email gateways and are often mistakenly under the impression that E3 capabilities are robust enough for complete email protection.

The AI-powered protections in Cisco® Secure Email Threat Defense are a key differentiator, providing a more complete level of defense. Microsoft customers considering moving to E5 to achieve broader and more advanced protections from that platform will find even more robust protections from the combination of Cisco User and Cisco Breach Protection Suites.

Secure Email Threat Defense is a key part of both the Cisco User Protection and Cisco Breach Protection Suites, which provide a comprehensive, network-led SaaS solution with built-in detections from email, network and endpoints. Unified within Cisco XDR, these detections provide analytics that empower quick and accurate detection, investigation and response. In addition, users are protected on any device, anywhere they work.

Product highlights

Secure Email Threat Defense maximizes an organization's email security investment by augmenting Microsoft 365 with comprehensive, AI-powered advanced threat protection. Deployed in minutes, Email Threat Defense sits behind any email gateway to detect and block dangerous and damaging threats.

Features:

- Complete visibility of inbound, outbound, and internal messages.
- Using numerous AI models, it:
  - Uncovers known, emerging, and targeted threats with advanced threat detection capabilities.
  - Identifies malicious techniques and gains context for specific business risks.
  - Rapidly searches for dangerous threats and remediates all threat instances in real time.
  - Utilizes searchable threat telemetry to categorize threats, and understands which parts of your organization are most vulnerable to attack.
  - Detects malicious QR codes, account takeover, and Business Email Compromise (BEC).
  - Cisco Extended Detection and Response (XDR) natively integrates telemetry from Secure Email Threat Defense and utilizes user accounts as an asset for correlation. All threat verdicts from Email Threat Defense are a part of Cisco XDR's incident attack chains.

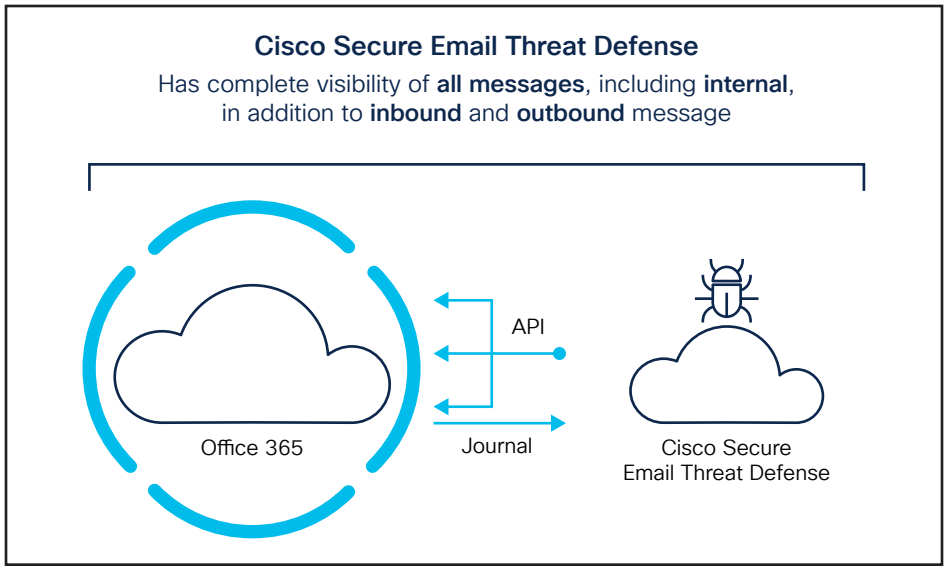

Figure 1. Expanded visibility for better threat detection

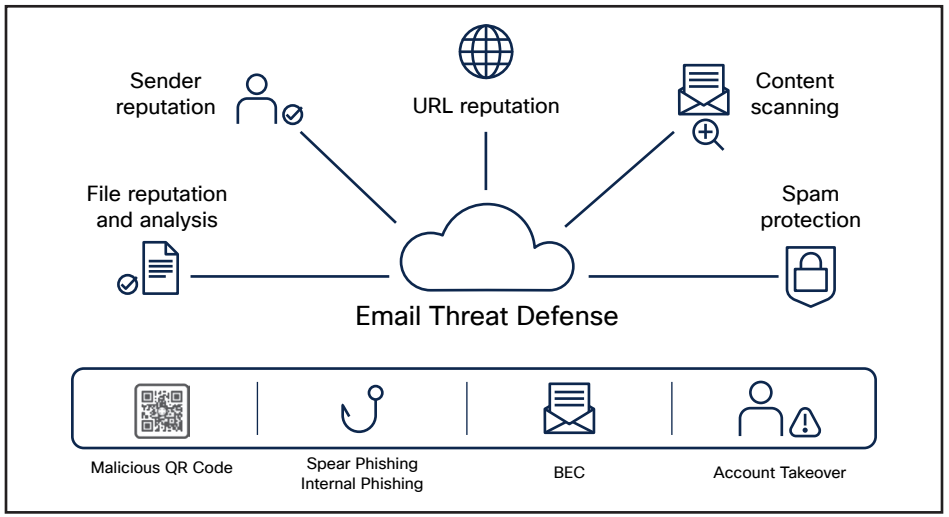

Figure 2. Comprehensive attack protection

Powerful AI detections that catch the widest array of threats

Email Threat Defense bolsters your existing Microsoft investment by:

- Providing AI-powered detections including:
  - Natural Language Processing (NLP)
  - Image processing
  - Computer vision
  - Large Language Models (LLMs)
  - Social Graph (SG) analysis and
  - Sender reputation/verification
- Evolving AI tools to uncover existing and emerging threats
- Utilizing over 200 Machine Learning–based detectors that evaluate signals to determine intent of the email
- Providing instantaneous searchable threat telemetry that empowers more informed responses
- Surfacing the highest value targets in your organization to understand where you are most vulnerable to attack
- Remediating threats across the entire organization in only a few clicks

AI capabilities within Email Threat Defense

Type of Threat	How Email Threat Defense leverages AI and other techniques to address it
Business Email Compromise (BEC)	• Social graphing of relationships determine new or rare senders • Detectors for non-payload emails, like initial lure or direct deposit requests • Deriving unparalleled context for specific business risks by correlating key markers of malicious intent, including sense of urgency, calls to action, and sentiment
Advanced phishing/spear phishing	• Embedding AI technology that extracts and analyzes the content of image-only emails that aim to evade text-based detections • Identifying malicious techniques used in advanced attacks targeting your organization • Detects behavioral analysis and anomalies of URL payloads using reputation, crawling, and static analysis techniques
Image analysis and obfuscation	• Utilizes Optical Character Recognition (OCR) detection that leverages Long Short-Term Memory (LSTM) neural networks for content extraction • Recognition of scripting, encoding, and embedding techniques like QR codes, HTML smuggling, and JavaScript used to obfuscate URL and file payloads
Account takeover	• Monitoring internal and outbound mail to quickly alert your team to potentially compromised accounts
User impersonation	• Applying behavioral models to VIPs and targeted personnel to identify impersonation attempts on names, email address, and even job titles
Unwanted email	• Categorizes emails as spam and graymail using a combination of Bayesian, heuristics, and Machine Learning–generated rules
File reputation and analysis	• Secure Hash Algorithm (SHA)-based blocking of known malware and unlimited analysis of files against 2,500+ behavioral indicators using Cisco Secure Malware Analytics

Feature comparison: Email Threat Defense and Microsoft E3 and E5

	Feature	Cisco Email Threat Defence	Microsoft 365 E3	Microsoft 365 E5
Basic (Core) Email Security				
1	SPAM Detection	Yes	Yes	Yes
2	Malware Detection (AV)	Yes	Yes	Yes
3	Malware Behavioral Analysis (Sandboxing)	Yes	No	No
4	Malicious URLs Detection	Yes	No	Yes
5	Malicious URLs Sandboxing	Yes	No	No
6	Anti-Phishing Policies	Yes	No	Yes
7	Phishing Detection	Yes	No	Yes
Advanced Threats				
1	Advanced Threat Analytics	Yes	No	Yes
2	Obfuscated URLs, QR Codes and File Detection	Yes	No	Yes
3	Scam Detection	Yes	No	Yes
4	Business Email Compromise Detection	Yes	No	Yes
5	User Impersonation Detection	Yes	No	Yes
AI and Machine Learning				
	ML Models for Advanced Detections			
1	Natural Language Processing (NLP)	Yes	No	Yes
2	Behavioral Analysis Models	Yes	No	Yes
3	Phishing Detection Models	Yes	No	Yes
4	Impersonation Detection Models	Yes	No	Yes
5	Relationship Graphs	Yes	No	Yes
Threat Response				
1	Manual Message Remediation	Yes	No	No
2	Automated Investigation and Response	Yes (Cisco XDR)	No	Yes

Enhanced protection across the full Microsoft suite

Our integration with Microsoft Sentinel and the use of the Security Graph API enables Secure Email Threat Defense to identify unique Incidents of Compromise (IoCs) that can be used to enhance protection across the full Microsoft suite.

Secure Email Threat Defense is constantly learning and evolving to adopt new detection techniques that add increased value to Microsoft environments. Start a free trial today to quickly see why it is a natural complement to your existing infrastructure and investment.

Ease of deployment to quickly elevate your email security

- Leveraging Microsoft Graph API to effectively enforce your mail policy and protect your users from threats
- Deploying quickly and simply without altering MX records
- **Demonstrating quick and impactful time to value**

Analyst accolades

Frost Radar: Email Security Recognition

In July 2024 Frost & Sullivan published The Frost Radar™: Email Security, 2024. It recognizes Secure Email Threat Defense as the Growth leader for its incredible market growth, significant advances in AI, and global expansion efforts.

> "Cisco is the Growth leader on this Frost Radar. Cisco's Email Threat Defense solution has had remarkable growth with an astonishing 182.6% CAGR for 2020–2023. Cisco has made significant advancements in AI, global expansion efforts, and innovating its cloud email platform over the past three years. These aspects have all contributed significantly to its growth achievements."

C22-5124603-00 05/25