Product Brief

Email Threat Detection and Response

Comprehensive Email Security for the Modern Threat Landscape

At A Glance

- Detect and respond to advanced email attacks with sandboxing, click-time protection, isolation, and integrated threat analytics.

Business Outcomes

- Reduce risk from email-borne attacks.
- Improve operational efficiency for SecOps and email teams.
- Strengthen governance and compliance for sensitive communications.

Solution Capabilities

- Advanced Detection and Protection
- Visibility and Response
- User Preparedness
- Interoperability and Integration

Overview

Email remains the primary vector for enterprise attacks—delivering phishing, business email compromise (BEC), ransomware, malicious links, and other evasive threats through a channel employees rely on every day. While native protections in cloud email platforms provide an important first layer of defense, many organizations need stronger detection, deep visibility into targeted attacks, and automated response capabilities when malicious emails reach the inbox or weaponize post-delivery.

Modern email attacks increasingly rely on techniques designed to bypass traditional defenses, including time-based URL weaponization, evasive malware, multi-stage campaigns, and social engineering aimed at both general users and high-value targets. As a result, security teams need more than basic filtering—they need deep inspection, rich threat context, and integrated response capabilities to rapidly identify, prioritize, and remediate advanced attacks.

Symantec® Email Threat Detection and Response (ETDR) extends Symantec Email Security.cloud with advanced detection, analytics, response, and user preparedness capabilities that help organizations strengthen protection against targeted and evolving email attacks. By combining cloud-based sandboxing, click-time URL protection, post-delivery response, threat isolation, security analytics, and user-focused awareness capabilities, ETDR helps security teams move beyond basic detection toward a more operational and resilient approach to email threat defense.

Introducing Symantec Threat Detection and Response

Symantec ETDR extends Symantec Email Security.cloud with advanced capabilities for detecting, analyzing, and responding to targeted and evolving email threats. As a cloud-based add-on module, ETDR helps organizations strengthen protection against attacks that evade initial filtering or change after delivery, including malicious links, suspicious attachments, and multi-stage phishing campaigns.

By combining cloud-based sandboxing, click-time URL protection, Microsoft 365 clawback, threat isolation, advanced analytics, and user preparedness capabilities, ETDR helps security teams identify high-risk activity, investigate campaigns more effectively, and take action more quickly. The result is an operational approach to email security that improves visibility, accelerates remediation, and maximizes the value of the Email Security.cloud platform.

Advanced Detection and Protection

ETDR helps organizations strengthen protection against advanced email attacks that evade initial filtering or weaponize after delivery. As an add-on to Email Security.cloud, it provides deeper inspection and post-delivery controls that help security teams address malicious links, suspicious attachments, and multi-stage phishing attacks with confidence.

Core capabilities include cloud-based sandboxing to uncover evasive files, click-time URL protection for links weaponized after delivery, Microsoft 365 clawback to remove newly identified malicious messages from user inboxes, and threat isolation to reduce exposure to dangerous web content and downloads. Together, these controls bridge the critical gap between message delivery and user interaction—mitigating the risk of ransomware, credential theft, and business email compromise.

By extending Email Security.cloud with more advanced detection and protection controls, ETDR helps organizations move beyond basic email filtering toward a more resilient defense model for evolving threats.

Visibility and Response

ETDR provides deeper visibility into targeted and advanced email attacks, equipping security teams with the context needed to investigate threats and act decisively. By analyzing both clean and malicious email activity, ETDR surfaces actionable threat intelligence—including indicators of compromise such as URLs, file hashes, and campaign patterns—to help teams identify affected users, understand attack patterns, and prioritize response.

ETDR seamlessly translates intelligence into action. Its analytics integrate directly into Security Operations Center (SOC) workflows and connect with Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) platforms, enabling teams to correlate email events with endpoint and web activity, accelerate remediation, and strengthen threat response across multiple control points.

User Preparedness

ETDR strengthens the human element of email security through integrated awareness and assessment tools. Built-in phishing simulations, reporting, and user risk profiling help security teams evaluate employee readiness, identify high-risk users, and build lasting resilience against social engineering attacks.

By combining user-focused awareness capabilities with detection and response intelligence, ETDR delivers a comprehensive approach to email security. This helps organizations reduce user-driven risk while making security awareness a more measurable and actionable part of the broader email defense strategy.

Interoperability and Integration

Email Security.cloud is designed to operate as part of a broader security ecosystem rather than as a standalone email control. Through integration with SOC workflows, SIEM and SOAR platforms, and related endpoint, web, data protection, and encryption solutions, organizations can extend email security insights into wider detection, investigation, and response processes.

This connected approach helps reduce operational silos, improve policy consistency, and strengthen protection across multiple digital touchpoints. For organizations with broader governance and data protection requirements, Email Security.cloud seamlessly extends with Symantec DLP and Symantec PGP® Encryption Service for Email to align email security with compliance, privacy, and secure collaboration objectives.

Summary

Symantec Email Security.cloud helps organizations go beyond basic email filtering with a layered, cloud-delivered approach to prevention, isolation, visibility, response, user preparedness, and data protection. By combining core email protection with advanced capabilities from ETDR and optional extensions for DLP and encryption, Symantec provides a complete and extensible architecture for defending against modern email threats.

The result is stronger protection against phishing, ransomware, business email compromise, and sensitive data exposure, alongside deeper operational visibility and a unified approach to enterprise email security.

BROADCOM®

For more information, visit our website at: www.broadcom.com

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

SED-ETDR-PB103 August 4, 2026