Solution Brief

Treat Every Inbox as an AI-Targeted Attack Surface

How to Help Stop AI-Enhanced Phishing, Impersonation, and Malicious Content before They Become Incidents

Challenge

AI makes phishing, impersonation, business email compromise, malicious links, and weaponized attachments far more convincing, scalable, and difficult to distinguish from legitimate communications.

Opportunity

Apply layered email security that blocks threats before delivery, protects users at interaction, streamlines investigation and response, and aligns with deployment requirements.

Benefits

Reduce email-borne risk, safeguard sensitive communications, heighten threat visibility, and maintain deployment flexibility without sacrificing security or compliance.

AI Turns Email into a More Effective Attack Surface

Email remains a primary gateway for attackers targeting enterprise users, high-value accounts, and critical business processes. AI escalates this risk by enabling adversaries to craft polished phishing messages, imitate trusted brands, generate convincing impersonations, and scale malicious campaigns faster than ever. Malicious links, attachments, credential-harvesting portals, and business email compromise (BEC) schemes now look far more credible and evolve too quickly for static filters or user awareness alone to reliably stop.

Filtering more messages is only part of the solution. Security teams require layered controls that neutralize threats predelivery, inspect suspicious links and files, protect users during risky interactions, identify coordinated campaigns, and safeguard sensitive data from disclosure; all while aligning seamlessly with the organization's cloud, on-premises, or hybrid email architecture.

Symantec® Email Security helps organizations address this challenge with two complementary solutions. Symantec Email Security.cloud delivers SaaS-based protection for Microsoft 365 and Google Workspace environments. Symantec Messaging Gateway delivers appliance-based inbound and outbound security for organizations that need to retain direct control of email infrastructure. Together, they provide layered protection, visibility, and policy enforcement across the email environments enterprises operate today.

The Human Trust Challenge

AI-enhanced social engineering exploits a difficult security reality: email is designed to be trusted, urgent, and easy to act on. A message that appears to come from an executive, supplier, customer, or internal colleague can trigger a payment, credential submission, file download, or disclosure of sensitive information before traditional security controls can intervene. These risks extend beyond generic phishing to include business email compromise, executive impersonation, ransomware delivery, credential theft, malicious links, and attacks that change after initial delivery.

While baseline controls remain essential, targeted campaigns and postdelivery weaponization require full lifecycle protection: evaluating messages predelivery, inspecting risky content at click, isolating suspicious interactions, and providing actionable telemetry for investigation and response.

Protect the Full Email Lifecycle

Modern email attacks rarely rely on a single obvious attachment. Attackers often conceal malware behind shortened URLs, document-sharing services, password-protected archives, scripts, or web downloads. Furthermore, a link that appears benign at delivery can later be redirected to a malicious destination.

To counter these evasive tactics, effective email security must operate throughout the attack lifecycle: blocking known threats and impersonation attempts predelivery, inspecting URLs and files, re-evaluating links upon click, and isolating suspicious interactions. This layered approach prevents a single convincing message from escalating into credential theft, malware execution, or ransomware delivery.

Choose the Correct Control Model

Enterprise email architectures vary significantly based on organizational needs. While cloud environments like Microsoft 365 or Google Workspace benefit from cloud-delivered security that extends native controls, other organizations must maintain control over email infrastructure to fulfill regulatory, data-residency, or architectural requirements.

Symantec Email Security accommodates both deployment choices. Symantec Email Security.cloud delivers SaaS-based protection, whereas Symantec Messaging Gateway offers physical or virtual appliance-based security for on-premises and private-cloud environments. Both options provide comprehensive inbound and outbound protection for threats, sensitive data, and targeted attacks while seamlessly aligning with your operational governance.

Protect Modern Cloud Email with Symantec Email Security.cloud

Symantec Email Security.cloud enhances Microsoft 365 and Google Workspace with layered, cloud-delivered protection beyond native email controls. It stops malware, spam, phishing, and impersonation attempts before they reach inboxes while providing security teams with full visibility and policy control across inbound and outbound email.

Core capabilities include advanced malware and spam filtering, phishing and spoofing protection, real-time and click-time URL and attachment inspection, threat isolation for suspicious content, and campaign analytics with automated response workflows.

To counter evasive campaigns that hide behind redirects, shortened URLs, password-protected files, or postdelivery weaponization, Symantec Email Security.cloud inspects links and attachments predelivery, re-evaluates URLs at click time, and isolates suspicious content to block zero-day exploits, credential harvesting, and ransomware.

For advanced requirements, Symantec Email Security.cloud seamlessly extends with Symantec Email Threat Detection Response and Isolation for cloud sandboxing, click-time protection, automated message clawback, deeper analytics, and response workflows. Organizations can also integrate Symantec Data Loss Prevention (DLP) and Symantec PGP® Encryption Service for Email to enforce compliance and secure sensitive outbound communications.

Retain Infrastructure Control with Symantec Messaging Gateway

Symantec Messaging Gateway provides comprehensive, appliance-based security for organizations managing email infrastructure on-premises, or in private or public clouds (such as Azure and GCP). Available in physical or virtual form factors, it protects inbound and outbound mail while giving teams direct operational control over their email security environment.

Symantec Messaging Gateway defends against malware, spam, phishing, executive impersonation, business email compromise, ransomware, and data exposure. It combines multilayered detection, flexible content filtering, malicious link protection, domain intelligence, built-in data loss prevention, and detailed auditing to block threats predelivery, prevent compromised internal accounts from sending outbound spam, and enforce policy on critical data.

For deeper data protection and threat inspection, Symantec Messaging Gateway can be expanded with Symantec DLP, Symantec PGP Encryption, and Symantec Content Analysis. These add-ons deliver advanced file analysis (including static inspection, machine learning, risk scoring, and sandboxing) and policy-driven encryption without requiring changes to the existing infrastructure model.

A Layered Email Protection Model

A message is not safe simply because it reached the inbox. Effective security must defend against threats before delivery, at the point of click, and post-discovery.

Email Lifecycle Stage	Email Security.cloud	Messaging Gateway	Security Value
Before delivery: Block suspicious senders and messages	Cloud-delivered malware and spam filtering, phishing and impersonation protection, and policy controls.	Appliance-based multilayer detection, reputation analysis, heuristics, sender intelligence, and BEC controls.	Prevents malicious messages, spoofed senders, and known threats from reaching users.
Before delivery: Inspect links and files	Real-time URL and attachment inspection, policy enforcement, and threat isolation.	URL reputation filtering, spear-phishing and ransomware defense, and optional Content Analysis.	Uncovers weaponized links, evasive files, and multistage delivery chains before user engagement.
After delivery: Protect at the point of click	Click-time URL analysis, re-evaluation, threat isolation, and automated response options.	Gateway controls block threats predelivery; advanced inspection modules strengthen file analysis.	Blocks postdelivery weaponized links and limits exposure during interactions with suspicious content.
After detection: Investigate and respond	Campaign visibility, email threat detection and response analytics, sandboxing, automated clawback, and response integrations.	Message tracking, interactive dashboards, reporting, auditing, and SIEM integration.	Enables teams to identify affected users, investigate related activity, and coordinate remediation.
Protect sensitive communications	Built-in policy controls; optional Symantec DLP and PGP Encryption Service for Email.	Built-in DLP, SMTP over TLS, and optional DLP and PGP email encryption services.	Reduces data loss risk while supporting regulatory compliance and governance requirements.
Align to deployment requirements	SaaS-based deployment.	Physical or virtual appliance deployment.	Allows organizations to choose the deployment model that best fits their infrastructure and control needs.

Priority Use Cases

Use Case	Description
Stop AI-enhanced phishing and impersonation	Apply layered defenses (including malware, spam, phishing, BEC, and impersonation controls) to keep sophisticated social-engineering campaigns from reaching users or high-value accounts.
Protect against malicious links and attachments	Inspect URLs and files predelivery and at click time, isolate suspicious content, and apply deep sandboxing to mitigate ransomware, malware, and credential theft risks.
Investigate targeted campaigns faster	Leverage campaign tracking, threat intelligence, message auditing, and SIEM integrations to quickly pinpoint affected users and coordinate response.
Secure cloud email beyond native controls	Enhance Microsoft 365 and Google Workspace with SaaS-based threat inspection, isolation, automated response, and data loss prevention.
Address data residency requirements	Deploy appliance-based inbound and outbound protection, policy enforcement, auditing, and DLP while maintaining direct control over infrastructure.
Protect sensitive outbound communications	Enforce policy-driven DLP, content controls, and automated encryption to prevent unauthorized data disclosure and ensure compliance.

Get Started

Identify high-risk email workflows, key user groups, and critical business processes vulnerable to targeted social engineering. Focus initial efforts on high-value roles, such as executives, finance, privileged administrators, customer-facing staff, and employees handling sensitive data or systems.

Evaluate current capabilities against these core operational questions:

- Are defenses specifically equipped to stop AI-driven phishing, impersonation, and business email compromise rather than basic spam?
- Can security controls inspect and isolate weaponized links and attachments at click time or postdelivery?
- Can security operations trace active campaigns across users and automatically coordinate incident response?
- Does the security model align with existing cloud, on-premises, private-cloud, and compliance requirements?

Use these findings to prioritize threat prevention, content isolation, automated detection and response, and the deployment model best suited to your organization.

Business Outcomes

- Prevent phishing, BEC, impersonation, and weaponized content from turning into business-impacting security incidents.
- Strengthen protection for high-value targets and sensitive processes frequently targeted by social engineering.
- Isolate suspicious links and attachments before user engagement leads to credential theft or malware deployment.
- Enhance threat visibility and streamline investigation across email and wider SecOps workflows.
- Protect sensitive outbound data using policy-driven DLP and automated encryption.
- Choose cloud-delivered or appliance-based protection to match operational governance and architecture demands.

Why Broadcom

Broadcom delivers flexible enterprise email security aligned with modern infrastructure needs. Symantec Email Security.cloud enhances Microsoft 365 and Google Workspace with cloud-native filtering, inspection, isolation, and response. Symantec Messaging Gateway provides appliance-based protection for organizations retaining direct operational control over email security infrastructure.

Both options move organizations beyond static filtering to enforce layered protection against advanced phishing, BEC, ransomware, and data loss. As threats evolve, Symantec seamlessly extends protection with cloud sandboxing, DLP, encryption, threat analytics, and SIEM integration; transforming email security into a unified, proactive defensive asset.

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.

TEI-AAS-SB100 September 29, 2026