Product Brief

Email Security.cloud

Comprehensive Email Security for the Modern Threat Landscape

At A Glance

Protect email from phishing, ransomware, and impersonation using layered defenses, isolation, and policy controls.

Business Outcomes

- Reduce risk from email-borne attacks.
- Improve operational efficiency for SecOps and email teams.
- Strengthen governance and compliance for sensitive communications.
- Enhance user resilience without sacrificing productivity.

Solution Capabilities

- Malware and spam defense
- Phishing and impersonation protection
- Advanced link and attachment inspection
- Threat isolation for risky content
- Campaign visibility and response workflows
- Integrated basic data protection

Overview

Email remains the primary entry point for enterprise cyberattacks through phishing, ransomware, and impersonation. Native cloud controls offer basic protection, but modern organizations require stronger defense-in-depth, campaign visibility, and precise policy enforcement for data protection and governance.

Symantec® Email Security.cloud delivers SaaS-based protection for modern email environments, enhancing Microsoft 365 and Google Workspace. It combines advanced filtering, anti-phishing controls, and real-time link and attachment isolation to neutralize threats before they reach devices. The platform easily expands to include advanced threat detection, DLP, and encryption—aligning email security with enterprise risk strategies without disrupting mail flow.

Why You Need to Go Beyond Basic Email Security

Email remains the easiest entry point for threat actors, who combine phishing, ransomware, Business Email Compromise (BEC), and impersonation to bypass basic security. While native email controls provide essential baseline hygiene, they struggle to stop highly targeted attacks, dynamic links, and sophisticated social engineering aimed at specific teams or executives.

Relying on baseline protections alone leaves critical gaps in defense, visibility, and governance. Sophisticated attacks easily bypass static filters through post-delivery weaponization and stealthy social engineering. Security teams require layered controls that provide deeper inspection, threat isolation, policy enforcement, and coordinated response to align email security with enterprise risk goals.

Introducing the Symantec Email Security.cloud Service

Symantec Email Security.cloud helps organizations protect modern email environments with layered, cloud-delivered defenses that go beyond basic native controls. It strengthens Microsoft 365 and Google Workspace with advanced protection against malware, spam, phishing, impersonation, and other user-targeted threats—while giving security teams greater visibility and control across both inbound and outbound mail.

Symantec Email Security.cloud includes these key capabilities:

- **Malware and spam defense:** Block malicious attachments, weaponized links, and unwanted bulk email before messages reach user inboxes.
- **Phishing and impersonation protection:** Detect and neutralize credential harvesting, domain spoofing, and executive impersonation attacks targeting high-value users.
- **Advanced link and attachment inspection:** Analyze URLs and files in real time—and at click-time—to catch evasive threats.
- **Threat isolation for risky content:** Render suspicious links and attachments in a remote, read-only isolated environment to keep users safe.

- **Campaign visibility and response workflows:** Trace attacks across users, campaigns, and Indicators of Compromise (IoCs) to drive faster, coordinated remediation.
- **Integrated basic data protection:** Enforce content, compliance, and encryption policies on sensitive email traffic to minimize data leakage risk.

Advanced Detection, Response, and Data Protection Modules

For organizations with more advanced requirements, Symantec Email Security.cloud can be extended with add-on modules that expand detection, response, data protection, and encryption capabilities—without disrupting the underlying email environment:

- **Advanced Detection and Response:** Symantec Email Threat Detection, Response, and Isolation extends Email Security.cloud with cloud sandboxing, click-time URL protection, automated clawback, advanced isolation, and deeper analytics to help security teams detect, investigate, and remediate targeted attacks more effectively.
- **Advanced DLP for Complex Policies:** Symantec Data Loss Prevention (DLP) extends built-in email protection with richer policy controls, broader workflows, and seamless integration across email, endpoint, network, and cloud environments for stronger governance and compliance.
- **Advanced Email Encryption Services:** Symantec PGP® Encryption Service for Email adds advanced encryption options for organizations with specialized privacy, regulatory, or partner communication requirements.

Business Outcomes

Symantec Email Security.cloud strengthens your security posture and operations in the following ways:

- **Reduces risk from email-borne attacks.** Lower the likelihood that phishing, ransomware, and impersonation campaigns turn into business-impacting incidents by adding layered controls beyond native email security. Security teams gain stronger protection across everyday users and high-value accounts, helping organizations close common attack paths without disrupting mail flow.
- **Improves operational efficiency for SecOps and email teams.** Simplify how security and messaging teams manage email defenses by consolidating advanced filtering, isolation, analytics, and policy enforcement into a single, cloud-delivered service. This reduces the overhead of managing multiple point solutions and helps teams investigate, respond, and tune controls more quickly.
- **Strengthens governance and compliance for sensitive communications.** Enforce consistent policies on sensitive outbound email with integrated data protection and encryption controls, extending to advanced DLP and encryption modules as requirements grow more complex. This supports regulatory compliance, internal governance standards, and audit readiness without forcing a change to the underlying email platform.
- **Enhances user resilience without sacrificing productivity.** Give users room to work safely by isolating risky content, filtering unwanted bulk mail, and reducing noise from suspicious messages. Employees stay focused on their jobs while security teams use visibility and response workflows to handle threats behind the scenes, improving both security posture and day-to-day productivity.

Why Symantec

Symantec brings long-standing experience in protecting large, complex environments where email remains a primary attack vector. Symantec Email Security.cloud goes beyond basic filtering with layered protection against malware, phishing, impersonation, isolation, and policy-based data protection—helping organizations reduce risk while supporting governance and operational efficiency.

When requirements grow, Symantec extends Email Security.cloud with advanced detection and response, DLP, and encryption capabilities that integrate seamlessly with broader endpoint, web, and data protection strategies. Powered by the Symantec Integrated Cyber Defense Platform and our Global Intelligence Network, our solution leverages threat intelligence correlated across endpoint, network, and DLP solutions. Symantec helps security teams treat email as a fully integrated component of their enterprise security architecture rather than an isolated point solution.

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-email-security-cloud-PB103 August 18, 2026