Symantec by Broadcom

Email Threat Isolation

PRODUCT BRIEF

KEY BENEFITS

- Prevents spear phishing and ransomware
- Stops credential theft
- Neutralizes malicious attachments
- Seamless user experience
- Industry-leading email security

KEY FEATURES

- Virtualized browsers for link isolation
- Read-only web page rendering
- Attachment isolation and safe viewing
- Ransomware and malware blocking

Overview

Sophisticated email attacks are growing in volume and complexity, targeting vulnerable users worldwide. Threats such as spear phishing, ransomware, and credential theft exploit human vulnerabilities and traditional security shortcomings and often leverage the following methods:

- Use malicious links to deliver ransomware or steal sensitive information.
- Employ newly created URLs with little or no reputational history, bypassing deny lists and signature-based defenses.
- Disguise malware within email attachments, including Microsoft Office documents, PDFs, or ZIP files, which execute harmful scripts or macros upon opening.

Traditional email security solutions struggle to detect and block these evolving threats, exposing organizations.

Introducing Email Threat Isolation

Symantec® Email Threat Isolation protects users from advanced email attacks by insulating them from spear phishing, credential theft, and ransomware. Key benefits include the following:

- **Prevent spear phishing and ransomware:** Isolate malicious links and downloads to stop attacks before they reach users.
- **Stop credential theft:** Render web pages in read-only mode, blocking users from entering sensitive information into phishing sites.
- **Neutralize malicious attachments:** Isolate and securely execute potentially harmful email attachments.

How Symantec Email Threat Isolation Works

Eliminate Advanced Email Attacks

Unlike reactive solutions that depend on blacklists or signatures, Symantec Email Threat Isolation proactively protects users:

- **Virtualize browsers:** Email links are executed in a disposable, secure container, ensuring malicious activities remain isolated from user devices.
- **Block advanced malware:** Links hosting ransomware or other malware are scanned and contained before delivery.
- **Neutralize phishing websites:** Suspicious links lead to isolated environments where potential threats are rendered harmless without disrupting the user experience.

This approach ensures that the threats are contained and neutralized even when users interact with malicious links or phishing sites, providing seamless and secure browsing.

HOW SYMANTEC EMAIL THREAT ISOLATION WORKS

- Eliminate advanced email attacks
- Protect users from credential theft
- Stop ransomware hidden in attachments
- Flexible deployment models

Protect Users from Credential Theft

Phishing emails often mimic legitimate websites to trick users into entering credentials. The Symantec solution defends against this tactic:

- **Read-only rendering:** Potential phishing websites opened via email links are displayed in read-only mode, disabling input fields such as text boxes.
- **Block data submission:** Prevents users from entering corporate passwords or sensitive data into phishing websites.

By halting credential theft at the source, Symantec solutions reduce the risk of data breaches and future attacks.

Stop Ransomware Hidden in Attachments

Email attachments are a common vector for ransomware and malware. Symantec Email Threat Isolation takes precautions to protect users:

- **Isolate attachments:** Suspicious files are executed in a secure, remote container rendered as HTML5 documents.
- **Create a virtual air gap:** Malicious scripts or macros are contained within the isolated environment, preventing them from infecting user devices.

Even if a user opens a suspicious attachment, the threat is neutralized in the isolated environment, ensuring complete protection.

Flexible Deployment Models

Symantec Email Threat Isolation can be deployed to meet diverse organizational needs:

- **Cloud-based service:** For scalable, on-demand protection.
- **Stand-alone or integrated deployment:** As a stand-alone service, it adds an isolation layer to third-party email security solutions. As an add-on to Symantec Email Security, it integrates with the Symantec Integrated Cyber Defense platform for comprehensive multi-channel protection.

Summary

Symantec Email Threat Isolation, included with Symantec Email Threat Detection Response and Isolation, is the industry's first solution to provide robust isolation against advanced email attacks. When combined with Symantec Email Security's market-leading defenses, organizations realize the following benefits:

- **Unparalleled protection:** Against spear phishing, credential theft, ransomware, and other sophisticated email threats.
- **Integrated cyber defense:** Covering endpoints, web, messaging apps, and more.
- **Seamless user experience:** A native browser experience indistinguishable from direct web access.

No other vendor offers this level of proactive protection, making Symantec solutions the choice for organizations seeking to defend against the most sophisticated email attacks.

BROADCOM®
connecting everything®

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

SYM-ETI-PB100 March 14, 2025