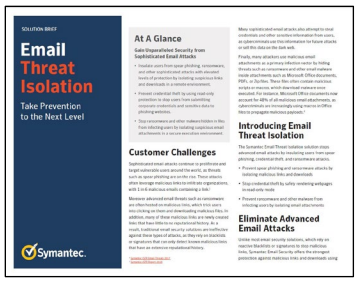


Email Threat Isolation

Take Prevention to the Next Level

Thank you for downloading this Symantec solution brief. Carahsoft is the distributor for Broadcom Cybersecurity solutions available via 'Educational Software Solutions and Services – OMNIA Partners, Public Sector', 'Cobb County GA Technology Products, Solutions and Related Services – OMNIA Partners, Public Sector,' 'Texas DIR-TSO04288,' and other contract vehicles.

To learn how to take the next step toward acquiring Symantec's solutions, please check out the following resources and information:

For additional resources:
carah.io/broadcomresources

For upcoming events:
carah.io/broadcomevents

For additional Broadcom solutions:
carah.io/broadcomsolutions

For additional cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
Broadcom@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/broadcomcontracts

For more information, contact Carahsoft or our reseller partners:
Broadcom@carahsoft.com | 888-662-2724

SOLUTION BRIEF

Email Threat Isolation

Take Prevention to the Next Level

Symantec™

At A Glance

Gain Unparalleled Security from Sophisticated Email Attacks

- Insulate users from spear phishing, ransomware, and other sophisticated attacks with elevated levels of protection by isolating suspicious links and downloads in a remote environment.
- Prevent credential theft by using read-only protection to stop users from submitting corporate credentials and sensitive data to phishing websites.
- Stop ransomware and other malware hidden in files from infecting users by isolating suspicious email attachments in a secure execution environment.

Customer Challenges

Sophisticated email attacks continue to proliferate and target vulnerable users around the world, as threats such as spear phishing are on the rise. These attacks often leverage malicious links to infiltrate organizations, with 1 in 6 malicious emails containing a link.[1]

Moreover advanced email threats such as ransomware are often hosted on malicious links, which trick users into clicking on them and downloading malicious files. In addition, many of these malicious links are newly created links that have little to no reputational history. As a result, traditional email security solutions are ineffective against these types of attacks, as they rely on blacklists or signatures that can only detect known malicious links that have an extensive reputational history.

[1] Symantec ISTR Email Threats 2017
[2] Symantec ISTR Report 2019

Many sophisticated email attacks also attempt to steal credentials and other sensitive information from users, as cybercriminals use this information for future attacks or sell this data on the dark web.

Finally, many attackers use malicious email attachments as a primary infection vector by hiding threats such as ransomware and other email malware inside attachments such as Microsoft Office documents, PDFs, or Zip files. These files often contain malicious scripts or macros, which download malware once executed. For instance, Microsoft Office documents now account for 48% of all malicious email attachments, as cybercriminals are increasingly using macros in Office files to propagate malicious payloads.[2]

Introducing Email Threat Isolation

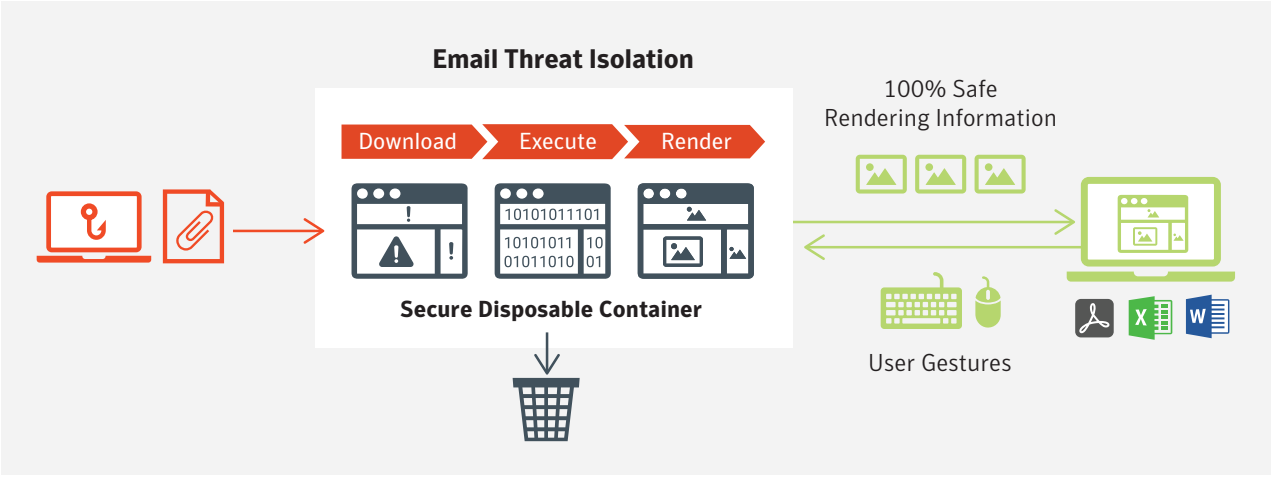
The Symantec Email Threat Isolation solution stops advanced email attacks by insulating users from spear phishing, credential theft, and ransomware attacks.

- Prevent spear phishing and ransomware attacks by isolating malicious links and downloads
- Stop credential theft by safely rendering webpages in read-only mode
- Prevent ransomware and other malware from infecting users by isolating email attachments

Eliminate Advanced Email Attacks

Unlike most email security solutions, which rely on reactive blacklists or signatures to stop malicious links, Symantec Email Security offers the strongest protection against malicious links and downloads using

Email Threat Isolation gives you elevated levels of protection and strong isolation.



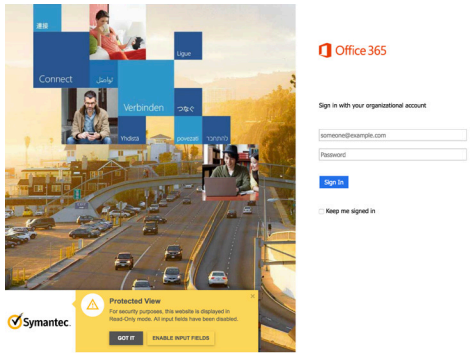
Email Threat Isolation to contain sophisticated email threats such as spear phishing and ransomware.

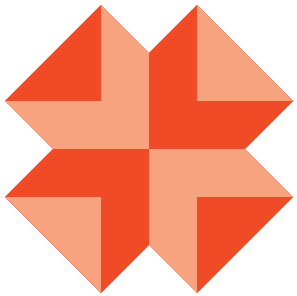
Symantec does this by virtualizing browsers in a highly-scalable and secure, disposable container, which creates a secure execution environment between users and the links in their email. This remote environment confines all malicious activity by executing web sessions from suspicious links in real-time and guarantees that only safe rendering resources are sent to users. In addition, advanced malware such as ransomware is blocked since email links that host potentially infected downloads are scanned before delivery. As a result, Symantec stops threats that contain malicious links or downloads from reaching users, as suspicious links are executed remotely, away from users and their devices. This protects users even after they have clicked on a suspicious link and opened a phishing website.

Email Threat Isolation takes prevention to the next level by making email links to malicious websites harmless. When isolated, these links cannot deliver their spear phishing, ransomware, and other advanced threats to email recipients. All of this is done without frustrating users, as Symantec provides a seamless user experience through the native browser, which is indistinguishable from opening links directly to the web.

Protect Your Users from Tricky Credential Theft

Many phishing emails also link to highly crafted webpages that look identical to well-known, authentic websites. As a result, attackers are able to use these webpages to steal corporate credentials and other confidential information from users, who mistake these webpages for legitimate websites.





Symantec gives customers strong isolation and protection against advanced email attacks through the industry's first isolation solution.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's
Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Email Threat Isolation defends against these credential theft attacks with read-only protection for potential phishing websites. Suspected phishing websites opened via email links are rendered in read-only mode, which disables input fields such as text boxes. This stops credential theft by blocking users from submitting corporate passwords and sensitive data to malicious websites, which use social engineering to trick users into entering their credentials and other confidential information.

Stop Ransomware From Infecting Your Users

Cybercriminals often hide threats inside email attachments, which unsuspecting users can easily mistake for legitimate documents. After they're downloaded, these files typically call malicious scripts or macros that execute dangerous malware such as ransomware, which infects user devices.

Email Threat Isolation prevents these advanced attacks that hide ransomware and other malware within files by isolating suspicious email attachments. Potentially risky attachments are rendered as HTML5 documents, which are executed in a remote container. This secure execution environment confines all malicious activity by creating a virtual 'air gap' between users and their devices.

Thus, ransomware and other advanced attacks that hide malware in email attachments cannot infect users, since these threats are isolated in a remote environment which keeps these attacks away from user devices. This protects users from advanced attacks, even if they've opened a suspicious attachment that contains ransomware or other email malware.

Deployment Models

Email Threat Isolation can be deployed as either a cloud-based service or on-premises appliance. Additionally, Email Threat Isolation is available both as a standalone service and as an add-on to the Symantec Email Security solution. When deployed as a standalone service, Email Threat Isolation adds an additional layer of protection and isolation to third-party email security solutions.

When deployed as an add-on to the Symantec Email Security solution, Email Threat Isolation is part of the Symantec Integrated Cyber Defense platform that covers endpoint and web security, threat analytics, security orchestration and automation, and more. Symantec takes an integrated approach to security that results in complete, multi-channel protection across endpoints, web, and messaging apps.

Symantec gives customers strong isolation and protection against advanced email attacks through the industry's first isolation solution. When combined with the market-leading defenses of Symantec Email Security solutions, this solution gives organizations unparalleled security from sophisticated email attacks. No other vendor offers this level of protection against advanced email attacks such as spear phishing, credential phishing, and ransomware.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

20A243111_SB_EMAIL_THEAT_ISOLATION_EN