SOLUTION BRIEF

Isolate Advanced Email Attacks

Take Prevention to the Next Level

Symantec™

At A Glance

Gain Unparalleled Security from Sophisticated Email Attacks

- Insulate users from spear phishing and other sophisticated attacks with elevated levels of protection by isolating suspicious links 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 advanced email attacks by blocking weaponized attachments from performing suspicious behavior

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 in 2017.[1] Suspicious links are tough for traditional email security solutions to stop, as these links use techniques such as multiple redirects, shortened URLs, or time-based delays to evade detection. 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.

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. For instance, 81% of data breaches involved stolen or weak credentials[2] and 12.4 million credentials were stolen via phishing attacks last year.[3]

Finally, advanced email threats such as ransomware often leverage malicious attachments to breach organizations, as 74% of malicious emails contained attachments in 2017.[1] Many of these threats use fileless attack techniques that 'live off the land' by using malicious scripts and other active content to weaponize attachments such as Office documents or PDF files. These techniques make identifying these attacks difficult, as traditional file-based detection methods are ineffective at spotting these types of threats.

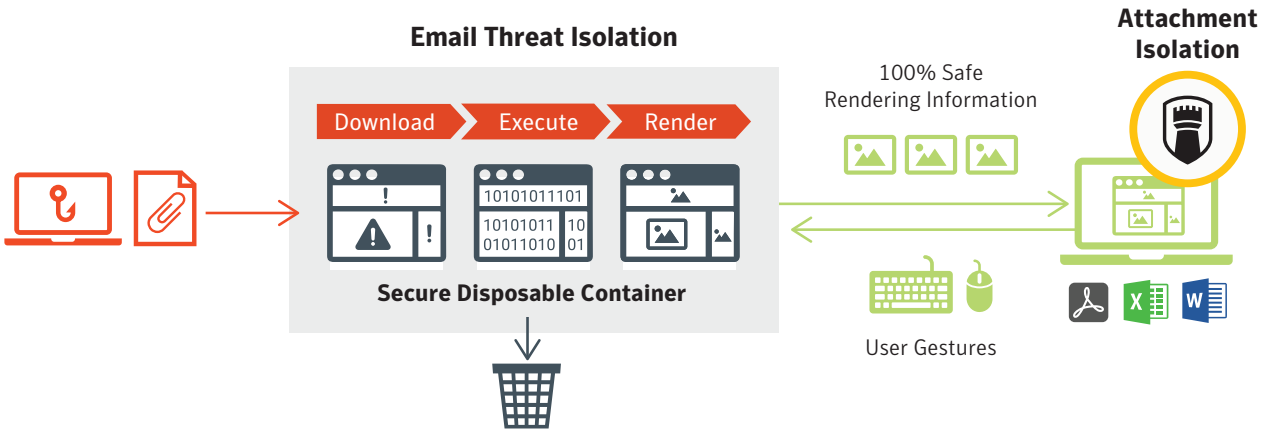
Introducing Email Threat Isolation

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

- Prevent spear phishing attacks by isolating malicious links
- Stop credential theft by safely rendering webpages in read-only mode
- Shut down ransomware by shielding trusted applications from weaponized attachments

[1] Symantec ISTR Email Threats 2017
[2] Verizon Data Breach Investigations 2017 Report
[3] Google Stolen Credentials 2017 Report

Email Threat Isolation adds elevated levels of protection and strong isolation to Symantec Email Security.



Eliminate Advanced Spear Phishing Attacks

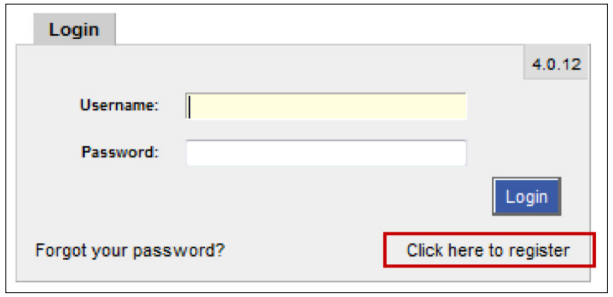
Unlike most email security solutions, which rely on reactive blacklists or signatures to stop malicious links, Symantec Email Security offers the strongest protection against malicious links using Email Threat Isolation to contain sophisticated email threats such as spear phishing.

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 suspicious links in real-time and guarantees that only safe rendering resources are sent to users. As a result, Symantec stops any threats that contain malicious links from reaching users, as every link it receives is treated as malicious and executed remotely, away from users and their devices.

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.



Attachment isolation works in tandem with behavior analysis, sandboxing, and machine learning technologies in Symantec Email Security.

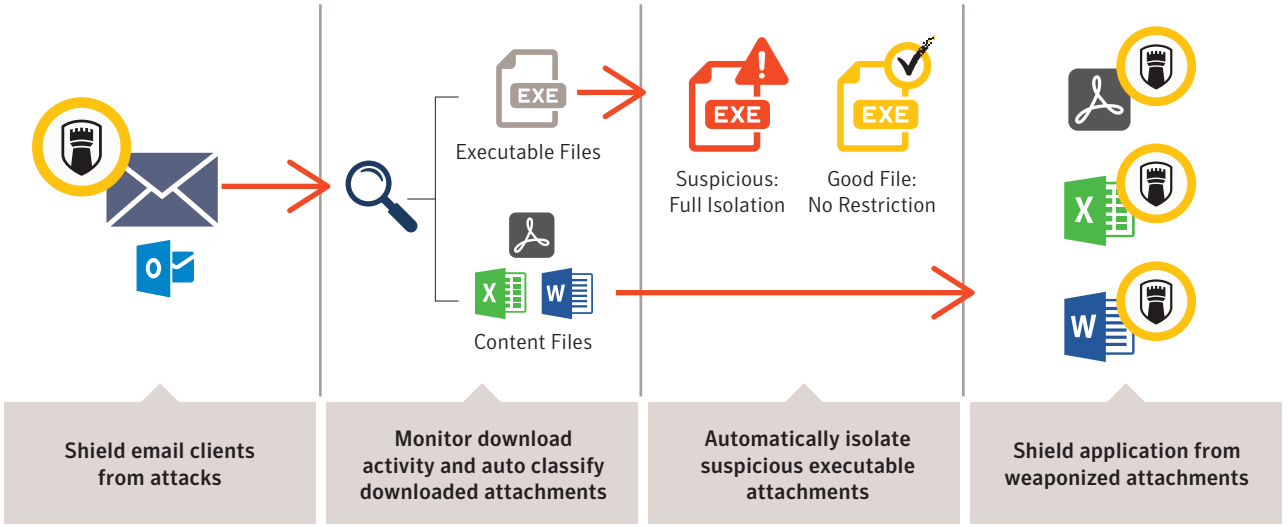
Email Threat Isolation defends against these credential theft attacks with read-only protection for potential phishing websites. Suspected phishing websites opened via email links are rendered in read-only mode, which disables input fields such as text boxes. This stops credential theft by blocking users 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.

Defend Your Business from Ransomware

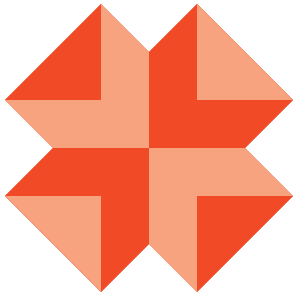
Symantec shields trusted applications from ransomware and other advanced email attacks that leverage weaponized documents through attachment isolation, which is available through the Symantec Endpoint Protection Hardening add-on.

These capabilities run trusted applications such as Microsoft Word, Adobe PDF, Microsoft Excel, and more in "castle mode," to prevent weaponized documents from performing suspicious behavior. Weaponized attachments will be given limited access rights and cannot execute privileged operations such as installing new software, modifying registry keys, changing the system settings, or modifying other processes or resources. This solution restricts the behavior of weaponized attachments and blocks any suspicious operations. Outside of alerting users about malicious activity, this process is transparent to users and preserves productivity.

Attachment isolation works in tandem with behavior analysis, sandboxing, and machine learning technologies in Symantec Email Security to analyze email attachments for malicious behavior. As a result, ransomware and other advanced email attacks that deliver weaponized attachments to users are stopped from doing any damage to organizations.



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



Gain Integrated Cyber Defense from a Single Vendor

The Email Threat Isolation solution 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. All of this is powered by insights from the Symantec Global Intelligence Network, the world's largest civilian global intelligence network that leverages telemetry from over 175 million endpoints, 80 million web proxy users, and 57 million attack sensors in 157 countries.

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.

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 or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

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

18D156055_SB_ISOLATE_ADVANCED_EMAIL_ATTACKS_FOR_SMG_EN