PRODUCT BRIEF

CHALLENGE

Cybercriminals continuously refine their ransomware tactics, using phishing, zero-day exploits, and compromised accounts to bypass traditional security defenses.

OPPORTUNITY

Implementing a multi-layered email security solution like Symantec® ESS can help organizations proactively detect and block ransomware threats before they reach users.

BENEFITS

ESS enhances email security with advanced threat detection, real-time link analysis, and behavioral monitoring; reducing the risk of ransomware infections and minimizing costly business disruptions.

Defending Against Ransomware

How Symantec® Email Security.cloud (ESS) Stops Email-Based Attacks

Overview

Ransomware remains one of organizations' most significant cyber threats, with email serving as a primary attack vector. According to the 2024 Verizon Data Breach Investigations Report, email is the leading method for distributing ransomware and the second most common vector in breaches. Ransomware encrypts files or locks users out of systems, demanding payment for restoration. In 2023, ransomware payments exceeded $1 billion, as reported by Chain Analysis, highlighting the financial toll of these attacks. The Verizon report also found that nearly one-third of all breaches involved ransomware or extortion tactics, affecting 92 percent of industries. Additionally, the 2024 IBM Cost of a Data Breach Report noted that ransomware-related breaches grew by 41 percent in the past year and took significantly longer to identify and contain.

Despite recent law enforcement efforts, including arrests of key players in the LockBit ransomware group, attack volumes remain unchanged. Ransomware's persistence underscores the need for robust cybersecurity defenses.

The Ransomware Challenges

Preventing email-based ransomware attacks presents several challenges, but the following four challenges are the most significant:

Sophisticated Social Engineering Tactics

Attackers use highly convincing phishing emails to trick users into opening malicious attachments or clicking on harmful links. These emails often impersonate trusted contacts, exploit urgent business requests, or use psychological manipulation to bypass user skepticism. Even well-trained employees can fall victim to these evolving tactics, making human error a persistent challenge.

Evasive Malware and Zero-Day Threats

Cybercriminals continuously develop new ransomware strains that evade traditional security measures. Many attacks leverage zero-day vulnerabilities or use polymorphic malware, which changes its code to avoid detection by signature-based security solutions. Organizations struggle to identify and block these evolving threats without advanced threat detection techniques before infiltrating systems.

Increasing Use of Compromised Accounts

Attackers often hijack legitimate email accounts through credential theft or phishing, allowing them to distribute ransomware from trusted sources. Since these emails come from known contacts, they easily bypass security filters and raise less suspicion among recipients. Detecting compromised accounts requires advanced behavioral analysis and real-time monitoring to identify unusual activity before damage occurs.

Use of Complex Attack Chains to Obfuscate the Threat from Legacy Email Hygiene Solutions

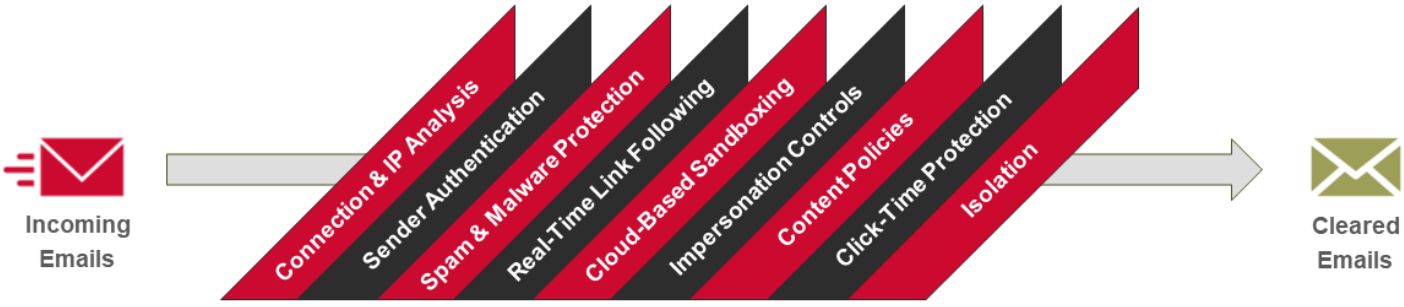
Malware is no longer delivered as an attachment to an email but instead as a web based download. These downloads are commonly obfuscated at the end of long attack chains which may include multiple redirectors, legitimate document sharing sites, and different file downloads. Unless an email security solution has the ability to follow these links before they are delivered and also at the time the user clicks the link, they are at risk from the attack.

To combat these challenges, organizations need a multi-layered email security strategy that includes advanced threat detection, user training, and proactive monitoring to stay ahead of attackers. This document will explore how Symantec ESS delivers these essential protections to help organizations prevent email-based ransomware attacks.

The Symantec Approach

Symantec ESS is an advanced, intelligent email security platform designed to enhance the native security of email systems while minimizing false positives. Symantec ESS leverages cutting-edge technologies, including real-time link analysis, cloud-based sandboxing, click-time protection, and isolation; all powered by telemetry from the Symantec Global Intelligence Network. These capabilities enable Symantec ESS to block sophisticated email threats such as ransomware, spear phishing, and business email compromise (BEC).

Figure 1: Multi-layered Defenses Delivered by Symantec ESS



As shown in Figure 1, Symantec ESS provides multi-layered defenses to protect your email communications. The following sections will explore these defenses in greater detail.

Connection and IP Analysis

The first line of defense provided by Symantec ESS is connection-level protection. Many email attacks leverage botnets which behave differently from legitimate email servers. Symantec ESS evaluates SMTP connections in real time, identifying and dropping those connections originating from non-email servers. Simultaneously, Symantec ESS inspects the sender's IP address and enforces DNS blocking for any blacklisted sources. These two filtering layers prevent approximately 44% (based on internal data from Symantec ESS) of malicious email traffic from ever reaching users.

Sender Authentication

Cybercriminals frequently use impersonation tactics to make malicious emails appear legitimate. To counter this tactic, Symantec ESS verifies whether an email originates from an authorized system or domain based on published authentication records (SPF, DKIM, DMARC). If the email fails authentication, it is convicted before reaching the recipient. Symantec ESS prevents attackers from tricking employees into opening malicious emails or sharing sensitive information by detecting spoofed emails that mimic trusted senders.

Spam and Malware Protection

Symantec ESS leverages reputation analysis, antivirus engines, and antispam signatures to detect and block malicious attachments and links. While traditional signature-based detection is highly effective against known threats, modern ransomware attacks often use weaponized URLs instead of attachments to evade these filters. To counter this tactic, Symantec ESS incorporates heuristic-based detection, analyzing email patterns and behaviors to identify previously unseen threats before they can cause harm.

Real-Time Link Following

To help address obfuscated downloads, one of Symantec ESS's most critical defenses, real-time link following, proactively scans and evaluates embedded URLs in incoming emails. Before an email is even delivered, Symantec ESS follows each link to its ultimate destination, even if the attacker attempts to obfuscate the true URL through redirection or shortening services.

For example, in April 2024, a spam campaign known as TA547 targeted German organizations by delivering the Rhadamanthys information stealer through variants of the following attack chain and later targeting Australia with banking and ransomware payloads:

1. An email containing a password protected ZIP attachment is sent to the targeted organization.
2. The receiver, extracting the ZIP archive, finds a link file.
3. Clicking on that link results in downloading a PowerShell script which delivers the malware.

This type of attack can only be uncovered by activating all of the steps to determine the final outcome. In this case, Symantec ESS would simulate the user actions by unzipping the file, discovering the link, and then following the link to determine where it leads. If a URL is determined to be malicious, the email is blocked. If uncertain, Symantec ESS assigns a risk score based on various factors, such as site registration details and traffic patterns. Organizations can set risk thresholds to block high-risk emails before they automatically reach users. By scanning links in real time before delivery, Symantec ESS helps neutralize sophisticated ransomware campaigns that rely on stealthy or newly created malicious URLs.

Cloud-Based Sandboxing

Symantec ESS includes cloud-based sandboxing to detect malicious scripts and executables. Suspicious attachments are executed in a virtual environment where Symantec ESS monitors their behavior. Symantec ESS determines whether the attachments pose a threat. While most ransomware attacks do not rely on traditional executable attachments, this capability helps catch unconventional or emerging threats that do.

Impersonation Controls

Symantec ESS employs a sophisticated impersonation engine to detect and block emails that mimic legitimate users, executives, or trusted domains. This protection is crucial for stopping ransomware and BEC attacks, which frequently rely on CEO fraud and fake supplier emails to deceive recipients into downloading malware or transferring funds. By identifying fraudulent emails that attempt to exploit trust, Symantec ESS protects users from falling victim to ransomware-laced phishing scams.

Content Policies

Symantec ESS allows organizations to create custom file-blocking rules to prevent high-risk attachments from being received or sent. If an organization does not use certain file types (such as .exe, .scr, or macro-enabled Office documents), it can configure Symantec ESS to reduce their attack surface by blocking emails containing those file types automatically. For example, an organization could block JavaScript and VBScript files which are commonly used in email-based ransomware attacks. Customers can also create bespoke policies around other aspects of the email, including how long ago a domain was registered and the category or risk level of URLs contained in the email body and attachments.

Click-Time Protection

Another common strategy that attackers use is to change the destination of a malicious link shortly after it is sent. This tactic might allow the email to bypass the scan-time protections and reach the recipient's inbox. To address these scenarios, click-time protection acts as a second line of defense. When a user clicks a link, Symantec ESS re-evaluates the link in real-time, following redirects and scanning the destination for threats. Symantec ESS blocks access immediately if the link leads to a known malicious site. If the site is suspicious but not confirmed as malicious, the link is opened in an isolated environment to prevent potential harm. Since cybercriminals frequently update malicious URLs after email delivery, click-time protection ensures that even delayed attacks are neutralized before execution. This behavior is applied automatically to known malicious URLs, and customers can create their own click time policies to prohibit unwanted URLs based on over 64 pre-build categories.

Isolation

Symantec ESS employs email threat isolation to shield users from advanced phishing and ransomware attacks. If a user clicks on a suspicious link, Symantec ESS renders the webpage remotely, preventing malicious scripts from executing on the user's device. Additionally, potentially dangerous downloads are scanned before being delivered. By isolating unknown or high-risk URLs, Symantec ESS ensures that users cannot interact directly with ransomware-laden sites, reducing the risk of infection.

Why Broadcom

Ransomware remains a top cyber threat, with email serving as its primary entry point. Symantec ESS provides a powerful, multi-layered defense against these evolving attacks by combining real-time link analysis, advanced threat detection, and behavioral monitoring to stop ransomware before it reaches users. With capabilities like sender authentication, sandboxing, impersonation controls, and click-time protection, Symantec ESS effectively blocks phishing attempts, malicious attachments, and compromised accounts. Risk is minimized and costly disruptions are prevented. As ransomware tactics grow more sophisticated, organizations need proactive email security that adapts to emerging threats, and Symantec ESS delivers the intelligence and protection necessary to stay ahead of attackers.

For more information, please visit www.broadcom.com/products/cybersecurity/email.

BROADCOM®
connecting everything®

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

DAR-ESS-PB100 February 25, 2025