Product Brief

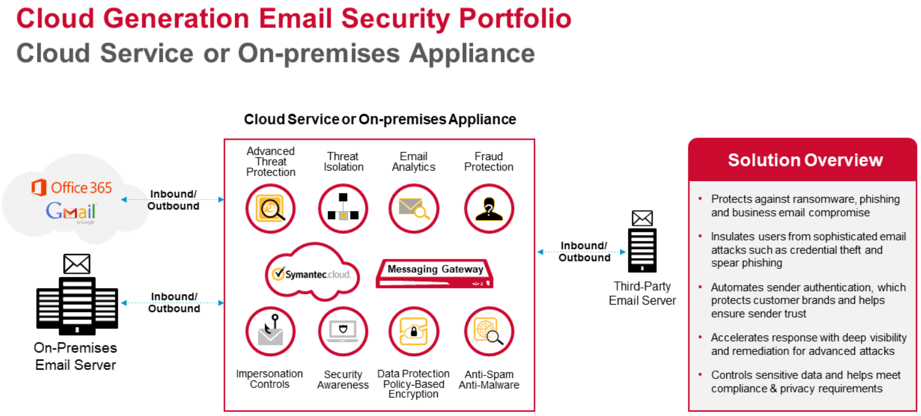
Email Security for the Enterprise

Multilayered Email Defense for the Cloud Generation

Table of Contents

Cloud Generation Email Security Portfolio

Figure 1: Advanced Policy Based Encryption



Cloud Generation Email Security Portfolio

Cloud Service or On-premises Appliance

Solution Overview

- Protects against ransomware, phishing and business email compromise
- Insulates users from sophisticated email attacks such as credential theft and spear phishing
- Automates sender authentication, which protects customer brands and helps ensure sender trust
- Accelerates response with deep visibility and remediation for advanced attacks
- Controls sensitive data and helps meet compliance & privacy requirements

Facing the Challenges of Securing the Cloud Generation

Intelligent, across-the-board email security—whether for on-premises, cloud-based, or hybrid email systems—begins with a clear, realistic understanding of what you're up against. Email is the most common way for cyber criminals to launch and distribute threats. According to the 2020 Data Breach Investigations Report, Verizon, most malware is delivered through email, with 46% of organizations getting almost all their malware this way. The 2019 Internet Crime Report, FBI shows that Business Email Compromise (BEC) accounted for half the reported losses experienced from all cyber crime ($1.77Bn).

As the volume of these attacks has increased, so has the level of sophistication. Advanced and zero-day threats are much more difficult to detect and stop than traditional malware, while standard signature-based antimalware tools have proven largely ineffective against them. Attackers now favor targeted spear phishing, especially in the form of business email compromise (BEC) scams. These elusive and dangerous targeted attacks use sophisticated methods including domain spoofing and obfuscation of malicious links embedded in email messages.

The losses from these attacks amounted to $26Bn in July 2019, over double the losses reported in May 2018.[1]

High-value targets, such as executives or finance teams, are most at risk as they typically have access to sensitive data and systems. Moreover, users unaware of email threats are susceptible to advanced attacks, which increases security risks for their organization.

The rapid adoption of Microsoft Office 365 and Google G Suite is transforming the way IT departments deliver messaging services to their organizations. Compared to traditional on-premises email, such cloud-based email services cut costs significantly by lowering operational overhead. And both providers point out that their email comes with included malware and spam protection. But how complete and effective are these built-in capabilities? What security issues should you consider as your organization prepares to migrate to cloud-based email?

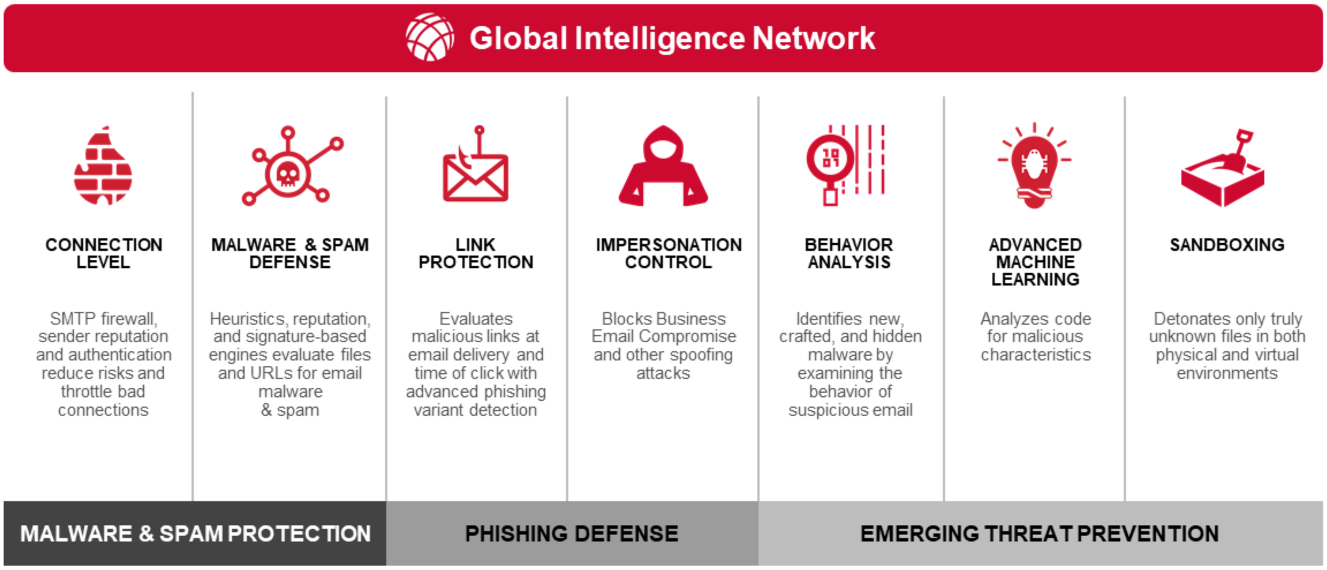
Organizations are having a hard time piecing together a complete, integrated email security solution out of multiple point products that solve only a portion of the email security problem. Worse, most email security solutions do not integrate with the rest of your security infrastructure (such as endpoint security, network security, SIEMs, and SOCs), leaving the burden of a complex integration to IT security teams. All the above, combined with a shortage of trained IT security talent, leaves organizations with operational complexity, gaps in their security architecture—and vulnerable to sophisticated multivector attacks.

Finally, organizations are struggling to prevent sensitive data from being exposed as users share sensitive information over email. This data must be kept secure and private to meet security, legal, and compliance requirements. Exposure can result in damaged brands and reputations, regulatory fines, and, ultimately, financial losses.

Gain the Most Complete Protection in the Industry

The Symantec™ Enterprise Division provides the industry's most complete cloud and on-premises email security portfolio. This protection comprises multiple layers of security technologies. And it is powered by insights from the world's largest civilian threat intelligence network, the Symantec™ Global Intelligence Network (GIN), which offers visibility into the threat landscape worldwide. The GIN helps ensure better security outcomes through telemetry distilled from over 175 million endpoints, 80 million Web proxy users, and 57 million attack sensors in 157 countries and by analyzing 8 billion threats every day. Symantec email security is part of our Integrated Cyber Defense Platform, covering and integrating Web, endpoint, and email security, threat analytics, security orchestration and automation, and more.

Figure 2: Worldwide Visibility into the Threat Landscape

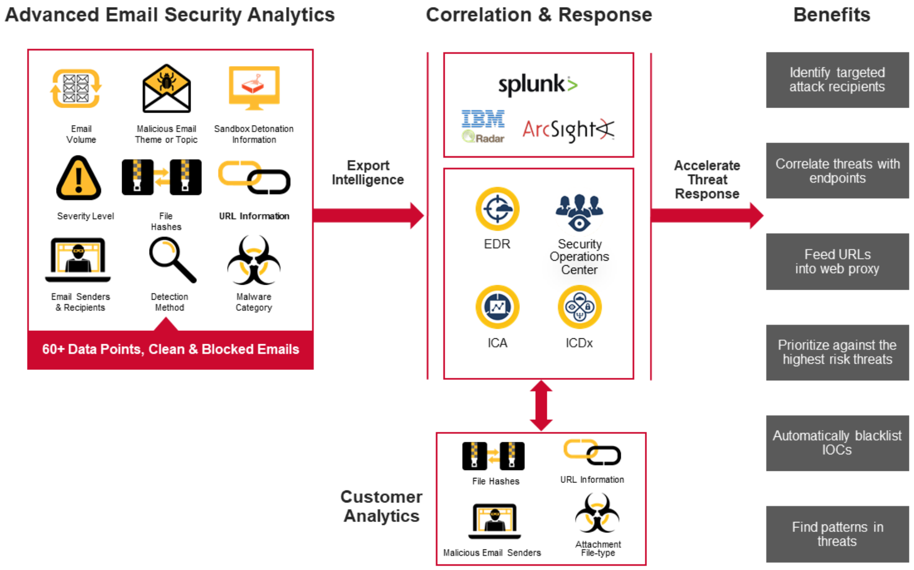

Global Intelligence Network
CONNECTION LEVEL
SMTP firewall, sender reputation and authentication reduce risks and throttle bad connections
MALWARE & SPAM DEFENSE
Heuristics, reputation, and signature-based engines evaluate files and URLs for email malware & spam
LINK PROTECTION
Evaluates malicious links at email delivery and time of click with advanced phishing variant detection
IMPERSONATION CONTROL
Blocks Business Email Compromise and other spoofing attacks
BEHAVIOR ANALYSIS
Identifies new, crafted, and hidden malware by examining the behavior of suspicious email
ADVANCED MACHINE LEARNING
Analyzes code for malicious characteristics
SANDBOXING
Detonates only truly unknown files in both physical and virtual environments
MALWARE & SPAM PROTECTION
PHISHING DEFENSE
EMERGING THREAT PREVENTION

Symantec™ Email Security Capabilities

The Symantec email security portfolio enables you to:

- **Prevent evolving and zero-day threats**
  - Block spam, malware, and advanced email threats such as spear phishing, ransomware, and business email compromise by leveraging multilayered defense that includes machine learning, behavioral analysis, and impersonation controls. Multiple scanning engines stop unwanted email such as spam, newsletters, and marketing emails.
  - Prevent the most complex, persistent email threats with virtual machineaware sandboxing and payload detonation powered by advanced machine learning, network traffic analysis, and behavioral analysis.
  - Block advanced phishing attacks, which weaponize a link after an email is delivered. Link protection probes and evaluates links in real time, both before email delivery and at the time of click. Link protection follows links to their final destination, even when attackers try to bypass detection with sophisticated techniques. Moreover, because cyber criminals often reuse code in new attacks, we use advanced phishing variant detection to sniff out and block spear phishing links that are similar to known phishing attacks.
- **Isolate email links and attachments for the ultimate protection**
  - Defend users from spear phishing and advanced attacks with the industry's first email threat isolation technology; remotely execute and render suspicious Web links in a secure execution environment while scanning downloads from these sites before they're delivered to the user's device.
  - Prevent credential theft by rendering suspicious websites in read-only mode, which stops users from submitting sensitive data such as corporate passwords.
  - Stop ransomware and other malware hidden in files from infecting users by isolating suspicious email attachments in a secure remote environment.
- **Respond quickly to security threats**
  - Act on the deepest visibility into targeted and advanced email attacks with detailed reporting on every incoming malicious and clean email scanned: 60+ data points such as URLs, file hashes, sender/recipient data, and targeted attack information.
  - Accelerate response to targeted and advanced attacks with rich threat intelligence exported to your Security Operations Center through API integration with third-party SIEMs, Symantec Information Centric Symantec Information Centric Analytics or Symantec Integrated Cyber Defense Exchange.
  - Correlate email, endpoint, Web and other security control points alongside user behavior to fully understand the highest risks you face in order to prioritize the right response.

Figure 3: Quick Response to Security Threats


Advanced Email Security Analytics
Email Volume
Malicious Email Theme or Topic
Sandbox Detonation Information
Severity Level
File Hashes
URL Information
Email Senders & Recipients
Detection Method
Malware Category
60+ Data Points, Clean & Blocked Emails
Export Intelligence
Correlation & Response
splunk>
IBM Radar
ArcSight
EDR
Security Operations Center
ICA
ICDx
Customer Analytics
File Hashes
URL Information
Malicious Email Senders
Attachment File-type
Accelerate Threat Response
Benefits
Identify targeted attack recipients
Correlate threats with endpoints
Feed URLs into web proxy
Prioritize against the highest risk threats
Automatically blacklist IOCs
Find patterns in threats

- **Prepare users to avoid threats with security awareness and training**
  - Evaluate employee readiness to detect phishing attacks with security assessments that mimic real-world threats; assessments can be customized to meet the needs of your organization, and match the evolving threat landscape.
  - Track progress of employee security awareness over time with repeated assessments and detailed reporting.
  - Create user risk profiles by combining assessment results with email security analytics.
- **Protect sensitive data in email**
  - Protect sensitive data and address legal and compliance requirements with built-in data loss prevention controls; enforce regulatory compliance and prevent data leakage by choosing from an extensive list of prebuilt, easily customizable templates.
  - Safeguard the security and privacy of confidential email with policy-based encryption controls that automatically encrypt specific outbound email.
- **Integrate with Symantec and IT security ecosystem**
  - Symantec Email Security is an integral part of the Symantec Integrated Cyber Defense Platform, which delivers complete multichannel protection—threat analysis, blocking, remediation, and more—across Web, endpoint, email, and cloud apps; backed by the Symantec GIN telemetry feeds aggregated and distilled from Symantec products.
  - Tight integration with Symantec Data Loss Prevention provides an email channel enforcement point for data protection policies.
  - Extensive API library enables integration with third-party SIEM and IT ticketing tools, enhancing security operation processes for maximum efficiency and an orchestrated response.

Symantec™ Email Security Products

Symantec Email Security.cloud

Symantec Email Security.cloud is a complete email security solution that safeguards cloud email, such as Microsoft Office 365 and Google Gmail, as well as on-premises email such as Microsoft Exchange.

It blocks new and sophisticated email threats such as ransomware, spear phishing, and business email compromise through a multilayered defense and insights distilled from the world's largest civilian threat intelligence network. When combined with Symantec Email Threat Isolation and Email Threat Detection and Response, it offers the strongest protection against spear phishing attacks with comprehensive defense that includes link protection, isolation, threat visibility, and user awareness training. Moreover, Symantec Email Fraud Protection enables organizations to automate Sender Authentication using DMARC, protecting all recipients from impersonation attacks.

In addition, advanced email security analytics provides deep visibility into targeted attack campaigns, with further context available when integrated into Symantec ICDx. Integrated DLP and encryption controls keep your business email secure and confidential.

In our testing, Symantec Email Security.cloud offers the highest effectiveness and accuracy of any email security on the market today—it blocks the most threats with the fewest false positives.[2]

Learn more about Symantec Email Security.cloud.

Symantec Messaging Gateway

On-premises messaging isn't going away any time soon thanks to strict industry regulations, data sovereignty, and company mandates to retain complete control over email infrastructure. For many organizations, security solutions for on-premises email are just as important as they are for cloud-delivered email.

Symantec Messaging Gateway provides inbound and outbound on-premises messaging security that includes powerful protection against the latest messaging threats and built-in data protection capabilities to keep your email secure and confidential. It catches 99+ percent of spam, registers fewer than 1 in 1 million false positives, and effectively responds to new messaging threats with real-time automatic antispam and antimalware updates. Messaging Gateway integrates with Symantec Content Analysis to deliver advanced protection against malicious files, and with Symantec Web Isolation for additional levels of link and attachment protection.

Learn more about Symantec Messaging Gateway.

Symantec Email Fraud Protection

Symantec Email Fraud Protection is a cloud-based service that provides additional protection against Business Email Compromise and other fraudulent email attacks. The service simplifies and automates compliance with email sender authentication standards, helping you achieve DMARC enforcement and protecting your email brand(s) from being used fraudulently.

Learn more about Symantec Email Fraud Protection

Symantec Email Threat Detection and Response

Symantec Email Threat Detection and Response adds advanced detection technologies such as cloud-based sandboxing and click-time URL protection to the Symantec Email Security.cloud service. In addition, it supplies Email Security Analytics on over 60+ data points for both clean and malicious email to equip security teams to proactively find threats and remediate them faster. With the included Symantec Phishing Readiness module you can assess and educate your staff about the risks of email attacks.

Advanced Threat protection capabilities can also be added to the Symantec Messaging Gateway by integrating it with Symantec Content Analysis System.

Learn more about Symantec Email Threat Detection and Response

Symantec Email Threat Isolation

Symantec Email Threat Isolation insulates users who click on email links to risky or uncategorized Web pages. By isolation such Web pages, ransomware and other malware attacks are prevented, and read-only protection stops spear phishing and credential theft. Risk email attachments can also be opened in an isolated container to reduce malware risk. Email Threat Isolation is simple to administer as security policies are set using Symantec threat intelligence and this capability is available for both cloud and on-premises solutions.

Learn more about Symantec Email Threat Isolation

Symantec Policy Based Encryption Advanced

Symantec Policy Based Encryption Advanced (PBE Advanced) extends the Data Protection policies available in Symantec Email Security.cloud or Symantec Messaging Gateway. Using PBE Advanced, your organization's email can be analyzed, and based on your policies certain email messages will be encrypted (for example based on key words or credit card information). Several delivery methods are available that enable recipients to read encrypted emails.

Learn more about Symantec Policy Based Encryption Advanced

To learn more about Symantec's email security solutions, visit
www.broadcom.com/products/cyber-security/network/messaging-security

About Symantec Enterprise Division

Broadcom's Symantec Enterprise Division, the global leader in cyber security, helps organizations and governments secure identities and information wherever they live. Organizations across the world look to Broadcom's Symantec Enterprise Division for strategic, integrated solutions to defend against sophisticated attacks across endpoints, identities, and infrastructure, whether on-premises, in the cloud, or both. For additional information please visit www.broadcom.com/symantec or subscribe to our blogs.

[1] FBI, Public Service Announcement,Alert Number: I-071218-PSA, https://www.ic3.gov/Media/Y2018/PSA180712, July 2018, and FBI, Public Service Announcement, Alert Number: I-091019-PSA, https://www.ic3.gov/Media/Y2019/PSA190910, September 2019

[2] Symantec Blog: "Independent Tests Prove Effectiveness of Symantec's Email Security" February 19, 2019

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

Symantec
A Division of Broadcom

Product Brief

Symantec™ Email Threat Detection and Response

Stop targeted and advanced email attacks with powerful protection that includes complete visibility, prioritized response, and automated remediation.

Key Features

- Detect complex and stealthy advanced attacks with cloud-based sandboxing capabilities.
- Stop malicious links weaponized after email delivery with Click-Time URL Protection, which helps provide the strongest protection against spear phishing, targeted attacks, and other advanced threats.
- Accelerate response to targeted and advanced attacks through advanced email security analytics that provide the deepest visibility into email attack campaigns with more than 60 data points on every clean and malicious email.
- Quickly correlate and respond to threats by exporting advanced email security analytics to your Security Operations Center through integration with third-party SIEMs, Symantec Information Centric Analytics (ICA), and Symantec Integrated Cyber Defense Exchange (ICDx).
- Decrease remediation time while preventing newly discovered threats with automatic blacklisting of IOCs found in your security environment.
- Reduce the risk of phishing with security awareness training that prepares your users for phishing attacks and helps you prioritize protection for the most vulnerable users in your organization.
- Correlate suspicious activity across all control points to identify and prioritize security events that pose the most risk.

Prevent the Most Advanced Email Attacks

Symantec™ Email Threat Detection and Response (ETDR) is a cloud-based service that uncovers and prioritizes advanced attacks entering your organization through email by adding advanced detection technologies such as cloud-based sandboxing and Click-Time URL Protection to the Symantec Email Security.cloud service. In addition, it helps accelerate your response to targeted and advanced threats with advanced email security analytics that provide the deepest visibility into targeted and advanced attack campaigns. This intelligence includes insights into both clean and malicious emails as well as more Indicators of Compromise (IOCs) than any other vendor, with more than 60 data points such as URLs, file hashes, and targeted attack information.

You can export this data to your Security Operations Center (SOC) to quickly determine the severity and scope of any targeted or advanced attack. Furthermore, you can quickly remediate email attacks by automatically blacklisting IOCs found while hunting threats. Moreover, ETDR reduces the risk of phishing by preparing your users to recognize the latest phishing attacks with built-in security awareness training. Finally, when used alongside Symantec Endpoint Detection and Response and the Symantec Secure Web Gateway family to detect advanced threats, you can automatically correlate events across all control points.

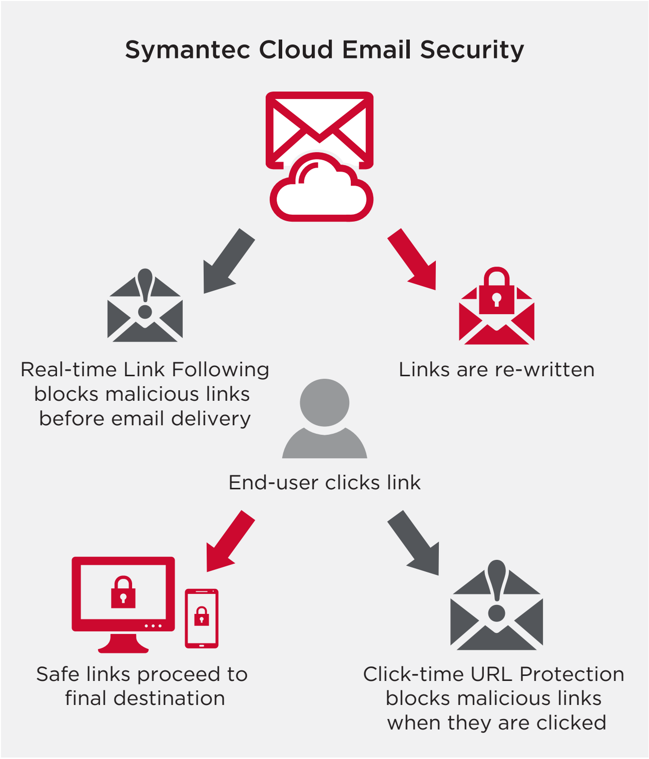
Cloud-Based Sandboxing

ETDR customers can leverage cloud-based sandboxing capabilities to discover and prioritize today's most complex targeted and advanced attacks. This service uses advanced machine learning, network traffic analysis, and behavior analysis to detect even the most stealthy and persistent threats. In addition, it's infused with security telemetry from the Symantec Global Intelligence Network, the world's largest civilian threat intelligence network. The Symantec Global Intelligence Network provides comprehensive visibility into the threat landscape and delivers better security outcomes by collecting and analyzing security telemetry from more than 175 million endpoints, 80 million web proxy users, and 8 billion daily security requests across 157 countries. Our cloud-based sandboxing also provides you the details of malicious files and their execution actions, so that all relevant attack components can be quickly investigated and remediated. Today, many advanced attacks are *virtual machine-aware*, which means they don't reveal suspicious behavior when run in typical sandboxing systems. To combat this, we employ techniques to mimic human behavior and execute suspicious files both virtually and on physical hardware to uncover attacks that evade detection by traditional sandboxing technologies.

Click-Time URL Protection

Click-Time URL Protection blocks malicious links by analyzing them when they are clicked by end-users to protect against spear phishing attacks that weaponize a link after an email is delivered. This complements Real-Time Link Following technology in Email Security.cloud, which blocks malicious links used in spear phishing attacks before an email is delivered. Unlike other solutions that rely on reactive blacklists or signatures to stop spear phishing attacks, we proactively stop both new and known spear phishing attacks that employ malicious links by performing deep evaluation of links in real-time. This deep evaluation follows links to their final destination, even when attackers use sophisticated techniques such as multiple redirects, shortened URLs, hijacked URLs, and time-based delays that bypass detection by traditional security solutions. Any files found at the destination URL are downloaded and deep heuristic analysis is performed to determine whether they are malware. This deep link evaluation powers both Click-Time URL Protection and Real-Time Link Following, which enables us to provide the most effective protection against spear phishing, targeted attacks, and other advanced threats that contain malicious links.

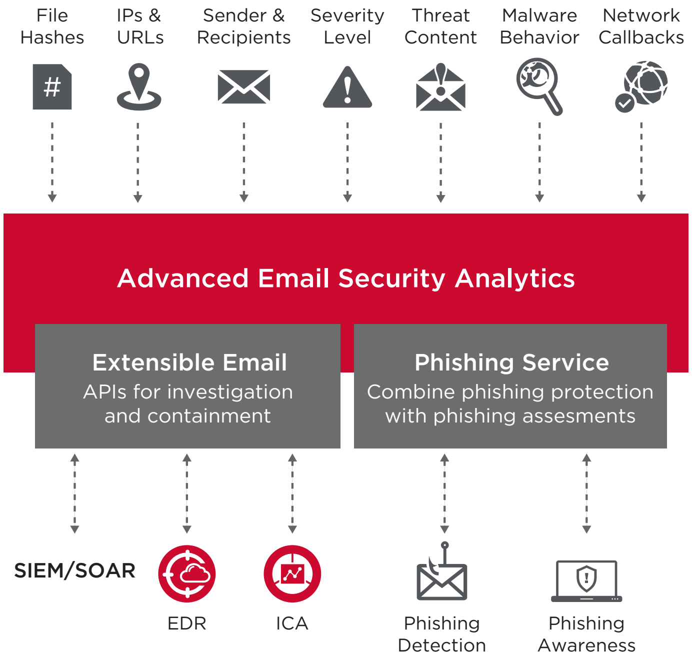
Figure 1: Block Malicious Links with Click-Time URL Protection


Symantec Cloud Email Security
Real-time Link Following blocks malicious links before email delivery
Links are re-written
End-user clicks link
Safe links proceed to final destination
Click-time URL Protection blocks malicious links when they are clicked

Advanced Email Security Analytics

ETDR helps accelerate your response to targeted and advanced threats with advanced email security analytics that provide the deepest visibility into email attack campaigns. This rich intelligence includes detailed reporting on every clean and malicious email entering your organization. These reports include more than 60 data points including IOCs such as the source URLs of an attack, targeted attack information, malware categorization, sender and recipient information, method of detection, clicked re-written URLs, and detailed information about file hashes. Each attack is assigned a threat category, such as Trojan or Infostealer, and a severity level of low, medium, or high to indicate the level of sophistication of an attack. You can even search and find detailed information about blocked emails, including both the original link in an email and the final destination link containing malware as determined by Real-Time Link Following. These advanced analytics give comprehensive insights into targeted and advanced threats against your organization by offering more IOCs than any other email vendor.

Figure 2: Deep Visibility into Email Attack Campaigns with Email Threat Detection and Response



Security Operations Center Integration

ETDR enables you to easily export the advanced email security analytics on clean and malicious emails to your SOC through integration with third-party SIEMs such as Splunk, IBM QRadar, HPE ArcSight, and more. Threat intelligence data is streamed directly to your SIEM through a granular, API-driven feed to give your security team rapid visibility into threats. Security analysts can leverage this data to quickly correlate and analyze threats when investigating and responding to threats. You can easily respond to email threats with a free Splunk or IBM QRadar app, which allows you to export the advanced email security analytics directly to Splunk or QRadar. These apps provide deep visibility into the threat landscape with data points such as malicious URLs and file hashes, information such as high-risk users, a geographical view of incoming attacks, and a timeline of email malware.

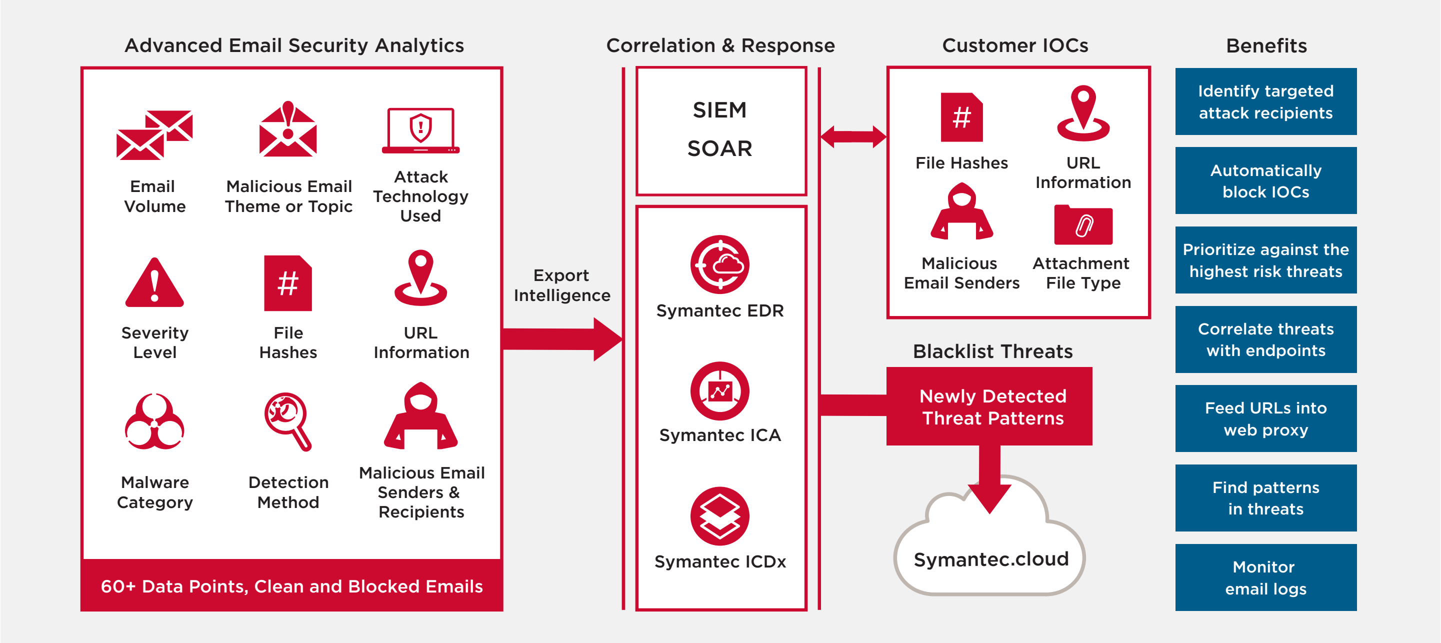
You can speed-up detection and response of targeted and advanced threats by exporting our advanced email security analytics to ICA or ICDx. ICA helps you understand and prioritize the riskiest threats to your organization by correlating email analytics with broader security and user behavior analytics. ICDx streamlines threat response by collecting, filtering, and forwarding security analytics across your environment to your SOC.

Automated Remediation

Security teams frequently come across IOCs when responding to an attack or while correlating and hunting threats in your environment. However, remediation is often slow and cumbersome even after these threats are discovered since IOCs are typically blacklisted manually. This manual process delays response time and increases remediation workloads, which can be critical for security teams dealing with hundreds or even thousands of incidents at a time.

ETDR allows you to quickly respond to targeted and advanced attacks by automatically remediating email threats. These capabilities speed incident response by automatically blacklisting IOCs such as file hashes, IP addresses, and sender and recipient information through an API. Furthermore, security teams can blacklist threats through the admin console. Blacklisting these IOCs protects your organization from newly discovered threats, decreases the time to remediate attacks, and improves your overall security posture while increasing the productivity of your security team. In case any threats get through our defenses, ETDR automatically removes these emails from Office 365 inboxes before your users can open them.

Figure 3: Symantec Security Operations Center Integration



Security Awareness Training

ETDR includes security awareness training, which reduces the risk of phishing by evaluating user readiness to phishing threats while helping you identify and train the most vulnerable users in your organization on phishing attacks. Customizable security assessments enable you to assess user readiness to phishing attacks by simulating the latest real-world phishing threats across your organization. After simulating an attack, detailed reporting and executive dashboards help you benchmark employee readiness and pinpoint the most susceptible users. Finally, you can improve user readiness to phishing threats by using training notifications to educate users on new and emerging phishing attacks and performing repeat assessments to track readiness over time.

Consolidated View Across Control Points

ETDR integrates with Endpoint Detection and Response and works alongside the Secure Web Gateway family to detect advanced threats that evade individual point products. This is powered by the massive Symantec Global Intelligence Network, and includes the ability to automatically correlate threats across all control points through Endpoint Detection and Response.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

Product Brief

Email Security.cloud

Complete Email Security for the Cloud Generation

Critical and Challenging Role of Email Security

Why is email today's No. 1 threat vector? Email is the most common way for cyber criminals to launch and distribute threats. According to the 2020 Data Breach Investigations Report, Verizon, most malware is delivered through email, with 46% of organizations getting almost all their malware this way. In the 2019 Internet Crime Report, the FBI shows that business email compromise (BEC) accounted for half the reported losses experienced from all cyber crime ($1.77B).[1]

As the volume of these attacks has increased, so has the level of sophistication. Advanced and zero-day threats are much more difficult to detect and stop than traditional malware, while standard signature-based antimalware tools have proven largely ineffective against them. Attackers now favor targeted spear phishing, especially in the form of BEC scams. These elusive and dangerous targeted attacks use sophisticated methods including domain spoofing and obfuscation of malicious links embedded in email messages. The losses from these attacks amounted to $26B in July 2019, over double the losses reported in May 2018.

At the same time, businesses are migrating their email from on-premises servers to cloud-based systems such as Microsoft Office 365 and Google G Suite. Unfortunately, the basic, built-in security of these systems cannot fully protect against email threats. Traditional email security solutions do not work either. Their rudimentary defenses fail to block new and sophisticated attacks, and their siloed approach to security allows advanced threats to slip through the cracks. Both types of security give organizations limited visibility and provide only basic analytics, which makes it harder to respond to threats.

Further complicating the landscape, vendors offer myriad point products that address only part of the security problem. These disjointed products—for email security, data loss prevention (DLP), endpoint protection, web security, and more—require costly, custom integrations and high management overhead. And again, a patchwork defense is leaky. Add in a shortage of trained IT security personnel and organizations end up with increased operational complexity and greater vulnerability.

Finally, as users increasingly share sensitive information over email, organizations are struggling to keep confidential data from being exposed. Data leakage undermines an organization's ability to meet its legal and compliance requirements. And it can result in damaged brand reputations, regulatory fines, and ultimately, financial losses.

At A Glance

- **Accurately defend against ransomware, BEC and emerging threats.** Stop new and sophisticated threats such as ransomware, spear phishing, and business email compromise with the most effective and accurate email security.
- **Stop spear phishing with comprehensive defense.** Shield your organization from spear phishing through a comprehensive defense that includes multiple layers of protection, strong isolation, deep visibility, and dynamic security awareness.
- **Accelerate your threat response with Integrated Cyber Defense.** Contain attacks and orchestrate response across endpoint security and web gateways by remediating attacks, block-listing threats, and correlating security analytics.
- **Ensure safe cloud adoption with the industry's strongest controls.** Fully secure Office 365 and G Suite through Symantec Email Security.cloud, Cloud Access Security Broker (CASB), and Data Loss Prevention solutions.

[1] FBI, Public Service Announcement,Alert Number: I-071218-PSA, https://www.ic3.gov/Media/Y2018/PSA180712, July 2018, and FBI, Public Service Announcement, Alert Number: I-091019-PSA, https://www.ic3.gov/Media/Y2019/PSA190910, September 2019

Shut Down the No. 1 Threat Vector

Symantec™ Email Security.cloud is a complete email security solution that safeguards cloud email such as Office 365 and G Suite and on-premises email such as Microsoft Exchange. It blocks new and sophisticated email threats such as ransomware, spear phishing, and BEC with a multilayered defense and insights from the world's largest civilian global intelligence network.

Email Security.cloud repels spear phishing attacks with comprehensive defense that includes protection, isolation, visibility, sender authentication and user awareness. It also accelerates attack response with analytics that provide deep visibility into targeted attack campaigns. Symantec Information Centric Analytics correlates email, other security streams, and user behavior analytics to give even deeper visibility.

Finally, Email Security.cloud is part of the Symantec Integrated Cyber Defense Platform, which covers endpoint and web security, threat analytics, security orchestration and automation, and more.

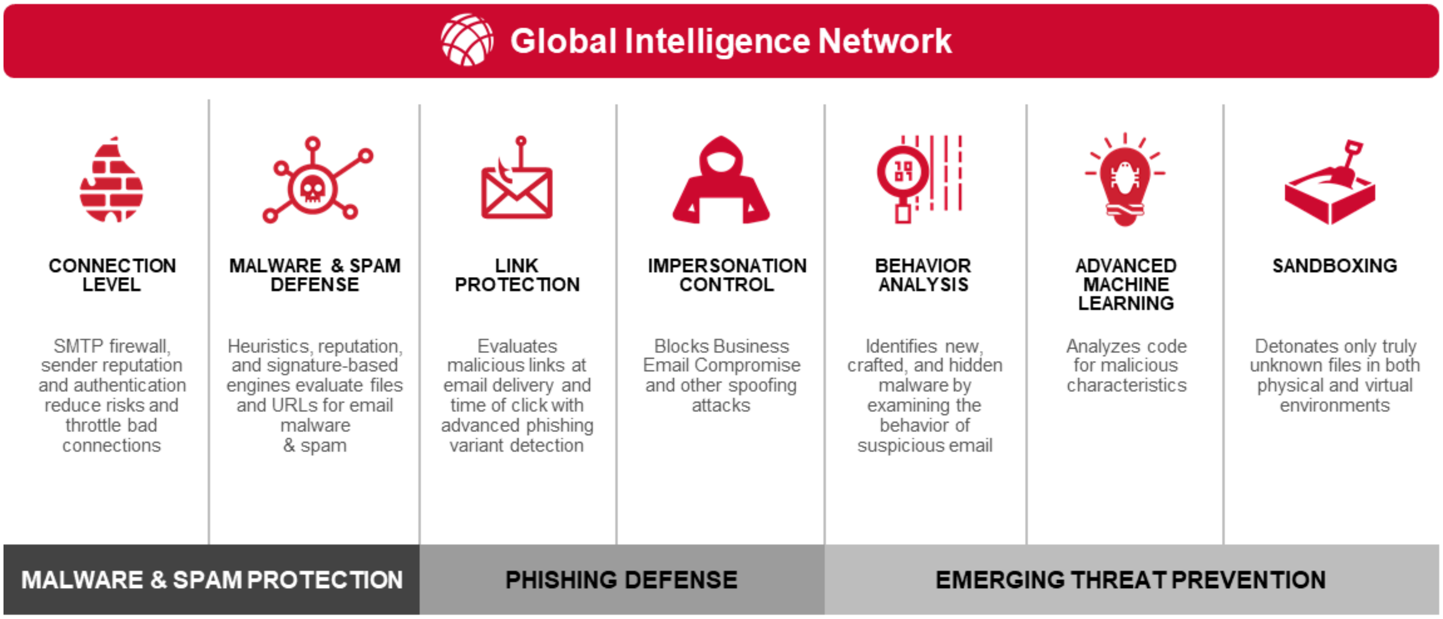
Prevent

Email Security.cloud supercharges the built-in security of cloud and on-premises email systems by preventing the most malware and email threats with the fewest false positives. This cloud-based solution repels sophisticated email attacks such as ransomware, spear phishing, and BEC with multiple, advanced detection technologies and telemetry from the Symantec Global Intelligence Network. It also improves user productivity by blocking spam and other unwanted email such as newsletters and marketing emails.

Emerging Threat Prevention

- **Sandboxing** uncovers targeted and advanced attacks by executing unknown files in physical and virtual environments. This helps catch 'virtual machine-aware' attacks, which are threats that do not exhibit suspicious behavior in virtual environments. The Symantec sandbox mimics human behavior to draw out attacks that appear malicious only in the presence of humans. In addition, our sandbox uses machine learning to detect stealthy, persistent threats by analyzing code for suspicious characteristics. And it utilizes network traffic analysis to identify malware that call command-and-control servers.
- **Behavior analysis** blocks new, crafted, and hidden ransomware by examining all email characteristics including delivery behavior, message attributes, attachments, and social engineering tricks. It also blocks new ransomware variants by determining if an email contains reused malicious code. Finally, it uses file decomposition techniques to spot and extract hidden ransomware within attachments.

Figure 1: The Most Complete Protection In The Industry



Global Intelligence Network

CONNECTION LEVEL

SMTP firewall, sender reputation and authentication reduce risks and throttle bad connections

MALWARE & SPAM DEFENSE

Heuristics, reputation, and signature-based engines evaluate files and URLs for email malware & spam

LINK PROTECTION

Evaluates malicious links at email delivery and time of click with advanced phishing variant detection

IMPERSONATION CONTROL

Blocks Business Email Compromise and other spoofing attacks

BEHAVIOR ANALYSIS

Identifies new, crafted, and hidden malware by examining the behavior of suspicious email

ADVANCED MACHINE LEARNING

Analyzes code for malicious characteristics

SANDBOXING

Detonates only truly unknown files in both physical and virtual environments

MALWARE & SPAM PROTECTION

PHISHING DEFENSE

EMERGING THREAT PREVENTION

Phishing Defense

- **Link protection** probes and evaluates links in real time before email delivery and again at the time of click—unlike traditional email security solutions that rely on reactive block lists or signatures to block only known spear phishing links. Link protection follows links to their final destination, even when attackers try to bypass detection with sophisticated techniques. Moreover, because cyber criminals often reuse code in new attacks, we use advanced phishing variant detection to sniff out and block spear phishing links that are similar to known phishing attacks.
- **Impersonation controls** provide the strongest protection against BEC and other spoofing attacks by using a sophisticated impersonation engine to block threats that masquerade as a specific user or legitimate email domain in your organization.
- **Threat isolation** opens risky or unknown website links in read-only mode to keep users safe from phishing attacks.
- **Fraud protection** automates sender authentication by ensuring that your email domain can not be impersonated, in turn eliminating the risk of fraud for internal and external recipients.

Malware and Spam Protection

- **Malware and spam defense** stops spam and malware by inspecting links and attachments with technologies such as reputation analysis, antivirus engines, and antispam signatures.
- **Connection-level protection** reduces the risk of spam and malware by slowing and dropping anomalous SMTP connections.
- **Threat Isolation** prevents ransomware and other malware from infecting users by isolating suspicious email attachments. This technology also isolates risky or unknown email links which host malware, keeping users and devices safe from infected downloads.

Symantec Global Intelligence Network

Threat Intelligence from the world's largest civilian network provides global visibility into the threat landscape and helps ensure better security outcomes. The GIN helps ensure better security outcomes through telemetry distilled from over 175 million endpoints, 80 million Web proxy users, and 57 million attack sensors in 157 countries and by analyzing 8 billion threats every day.

Isolate

Symantec Email Threat Isolation shields users from advanced email attacks such as spear phishing, credential theft, and ransomware by isolating suspicious links and attachments while stopping credential theft by safely rendering risky web pages. Email threat isolation takes prevention up a notch by creating an insulated execution environment between users and their email links, rendering suspicious links remotely and showing only inoculated web content to users, while scanning potentially infected downloads before delivery. Therefore attacks meant to be delivered via malicious links are simply neutralized.

Credential phishing attacks are also stopped with Symantec Email Threat Isolation. When a suspected phishing website is opened via an email link, the site is rendered in read-only mode, which prevents users from entering sensitive information such as corporate passwords.

Thirdly, advanced attacks that use attachments which link to ransomware and other malware are stopped from infecting users by isolating email attachments. When a potentially risky attachment is found, email threat isolation capabilities render these documents in a secure remote environment, which creates a virtual 'air gap' between files and user devices. As a result, ransomware and other advanced attacks that hide malware in email attachments cannot infect users.

- Prevent spear phishing 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

Respond

Email Security.cloud accelerates attack response with analytics that provide the deepest visibility into targeted and advanced attack campaigns. This intelligence includes insights into both clean and malicious emails, and provides more Indicators of Compromise (60+ data points including URLs, file hashes, and targeted attack information) than any other vendor. This can all be streamed to your Security Operations Center through API integration with third-party Security Information and Event Management (SIEM) systems,Symantec Information Centric Analytics or Symantec Integrated Cyber Defense Exchange.

Respond (cont.)

This enables you to hunt for threats across your environment and quickly determine an attack's severity and scope. When used alongside Symantec Endpoint Detection and Response and the Secure Web Gateway family to detect advanced threats, you can automatically correlate events across all control points. You can then remediate threats and orchestrate response by containing attacks and block-listing attacks across your security environment.

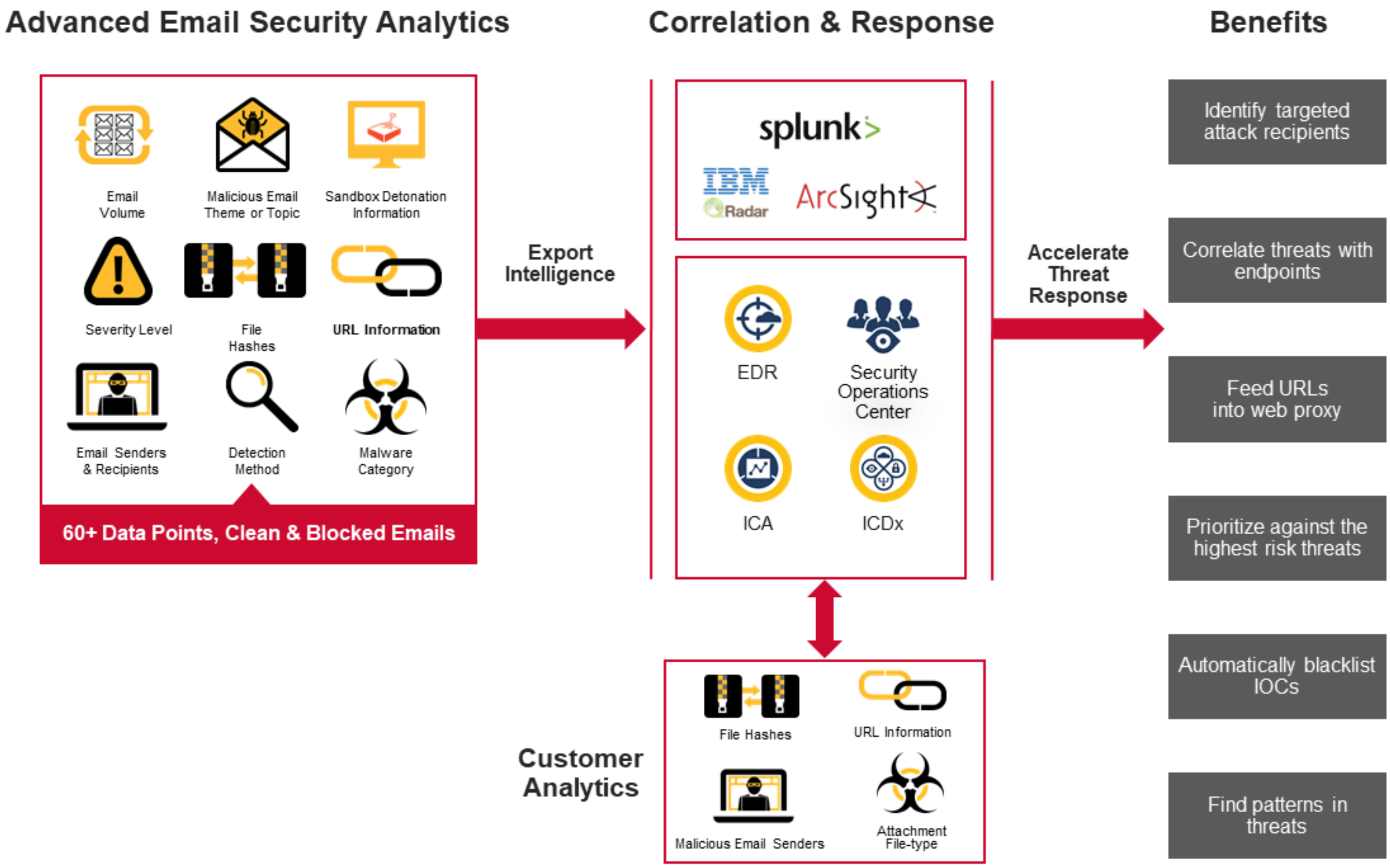
- Accelerate your attack response
- Hunt threats across your environment
- Remediate threats and orchestrate your response

Prepare

Email Security.cloud provides broad security awareness and education capabilities that reduce business risks by preparing users to recognize phishing attacks and helping organizations prioritize protection for the most vulnerable users. Evaluate employee readiness with security assessments that mimic real-world threats, which can be easily customized to meet the needs of your organization. Executive dashboards and detailed reporting help benchmark your organization's security awareness by giving visibility into user behavior and repeat assessments identify key trends by comparing results to previous evaluations. Admins can even develop user risk profiles and prioritize risky users by combining these insights with Symantec email security analytics or correlating user behaviour using Information Centric Analytics. This security awareness and education prepares employees to recognize and report email attacks with training notifications that teach users to spot the latest, sophisticated email attacks.

- Assess employee readiness with real-world simulations
- Track progress with repeat assessments and detailed reporting
- Educate users to recognize email attacks

Figure 2: The Deepest Visibility Into Advanced Email Attacks


Advanced Email Security Analytics
Correlation & Response
Benefits
Email Volume
Malicious Email Theme or Topic
Sandbox Detonation Information
Severity Level
File Hashes
URL Information
Email Senders & Recipients
Detection Method
Malware Category
60+ Data Points, Clean & Blocked Emails
Export Intelligence
splunk>
IBM Radar
ArcSight
EDR
Security Operations Center
ICA
ICDx
Accelerate Threat Response
Identify targeted attack recipients
Correlate threats with endpoints
Feed URLs into web proxy
Prioritize against the highest risk threats
Automatically blacklist IOCs
Find patterns in threats
Customer Analytics
File Hashes
URL Information
Malicious Email Senders
Attachment File-type

Integrate

Simplify your security stack and increase return on investment by integrating email security with the rest of your security infrastructure, including DLP and encryption controls as well as endpoint, network, and cloud security.

Email Security.cloud prevents data leakage and helps meet compliance and privacy requirements with built-in DLP and policy-based encryption controls. Flexible DLP policies identify and control sensitive emails with over 100 pre-defined lists of keyword dictionaries, regular expression, and MIME type lists. Policy-based encryption controls keep confidential emails private by automatically encrypting emails via a password-protected PDF for a mobile-friendly "push" encryption experience.

Email Security.cloud is a part of the Symantec Integrated Cyber Defense Platform, so its built-in DLP controls are strengthened through integration with Symantec Data Loss Prevention, which prevents data loss across your entire environment—email, endpoint, network, cloud, mobile, and storage systems. Moreover, you can meet advanced encryption needs and get customizable branding with Symantec Policy-Based Encryption Advanced, a cloud-based add-on service.

Email Security.cloud also integrates with other Symantec products to protect endpoints, web, and messaging apps, which strengthen your overall security posture. Use it with Symantec Endpoint Security to accelerate your response to emerging threats. For example, intelligence gathered from threats in the email channel can be pushed out as block lists to all endpoints, preventing infection across your environment. This extends protection to the latest collaboration and messaging apps—in the cloud and on premises—such as Slack, Salesforce, and Box.

Add-Ons to Symantec Email Security.cloud

The core Symantec Email Security.cloud offers enhanced protection through the following add-ons:

- **Email Threat Detection and Response:** Protects against advanced threats while providing deep visibility and rapid response to targeted attack campaigns. This also includes Phishing Readiness security awareness training capabilities.
- **Email Threat Isolation:** Opens suspicious email links and attachments in an isolated container, allowing users to interact with potentially risky websites, files, and downloads while blocking malware or phishing attacks.
- **Email Fraud Protection:** Simplifies the process of achieving and maintaining sender authentication enforcement by using automation to support various standards (for example, DMARC, DKIM, SPF).

Gain High Operational Efficiency at a Low TCO

Email Security.cloud is easy to deploy and operate, and scales quickly as messaging volume grows. When you add up its high effectiveness and accuracy, strong SLAs, and the Symantec Integrated Cyber Defense Platform, your organization will decrease operational complexity, enjoy a lower total cost of ownership, and get unmatched protection from even the most sophisticated email attacks.

Symantec™
A Division of **Broadcom**

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-email-security-cloud-PB100 November 24, 2020