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.

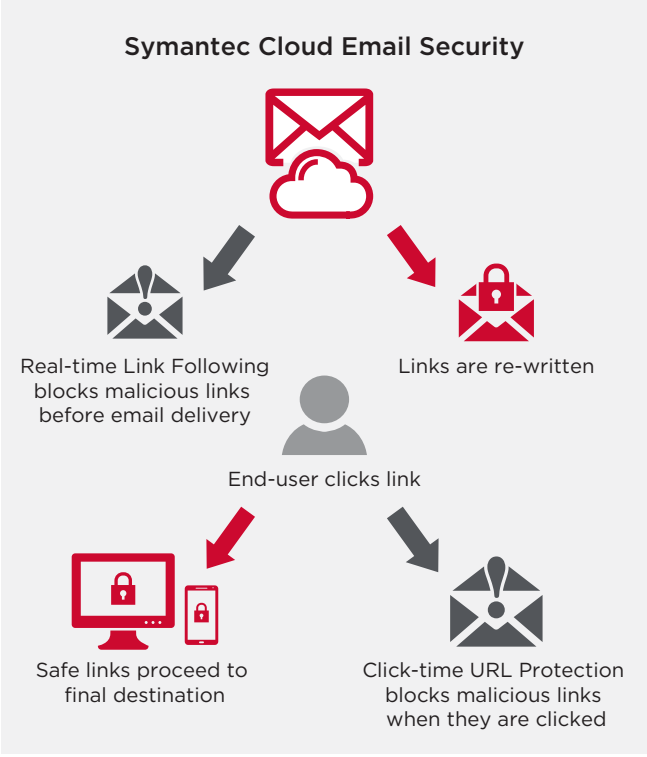
Cloud-Based Sandboxing

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.

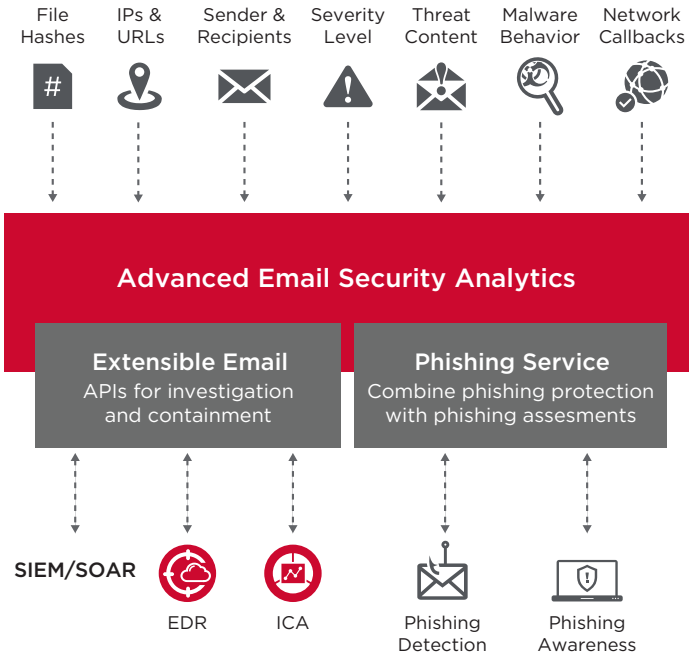
Figure 1: Block Malicious Links with Click-Time URL Protection



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.

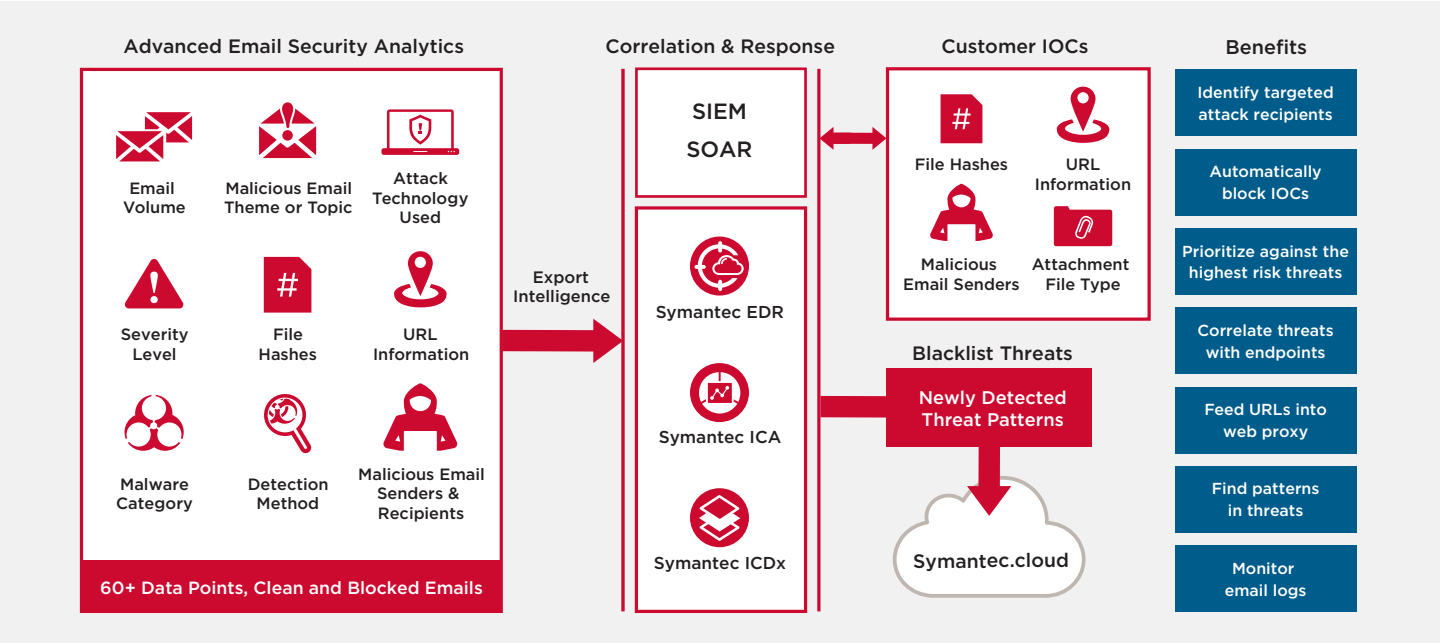
You can speed-up detection and response of targeted and advanced threats by exporting our advanced email security analytics to ICA or ICDx. ICA helps you understand and prioritize the riskiest threats to your organization by correlating email analytics with broader security and user behavior analytics.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

SED-ETDR-PB100 January 11, 2021