PRODUCT BRIEF

Email Threat Detection Response and Isolation

Add-on Module for Symantec® Email Security.cloud

AT A GLANCE

ETDRI integrates with Symantec® Email Security.cloud to deliver a comprehensive solution for combating targeted and advanced email threats.

KEY BENEFITS

- Advanced detection of sophisticated threats
- Comprehensive visibility and analytics
- Seamless integration with SOCs
- Accelerated response and remediation

KEY FEATURES

- Cloud-based sandboxing
- Click-time URL protection
- Email threat isolation
- Security awareness training

Overview

Email remains one of the most common attack vectors for cyber criminals. Four primary challenges are presented by these targets and advanced email attacks:

- **Evolving threat landscape:** Cyber criminals employ increasingly sophisticated techniques such as time-based URL weaponization, virtual machine-aware malware, and multi-stage attacks.
- **Limited visibility:** Traditional solutions often fail to provide detailed insights into targeted attack campaigns or contextual data about clean and malicious emails.
- **Delayed response:** Manual processes for identifying and blacklisting indicators of compromise (IOCs) slow down response times and overburden security teams.
- **User vulnerabilities:** Employees often fall victim to phishing attacks, underscoring the need for effective security awareness training.

Addressing these challenges requires robust detection, swift response, and comprehensive visibility into email-based attacks.

Introducing Symantec Email Threat Detection Response and Isolation (ETDRI)

Symantec ETDRI, a cloud-based service, enhances email security by integrating advanced detection technologies such as cloud-based sandboxing, click-time URL protection, Office365 clawback, and web browser isolation into the Symantec Email Security.cloud platform. ETDRI delivers a robust solution to detect, prioritize, and remediate advanced email threats while reducing risks through user education.

Advanced Detection and Protection

Cloud-Based Sandboxing

ETDRI employs advanced machine learning, behavior analysis, and network traffic evaluation to detect and prioritize sophisticated email attacks. Stealthy and persistent threats are detected using both virtual and physical hardware techniques. Furthermore, the service integrates with the Symantec Global Intelligence Network (GIN), leveraging data from 175 million endpoints and 8 billion daily security requests for unmatched visibility. Detailed insights into malicious files and execution actions streamline investigation and remediation.

Click-Time URL Protection

This feature blocks malicious links in real time, safeguarding users against spear phishing attacks. Deep link evaluation is used to identify threats even with techniques like URL redirection or time-based weaponization. This includes following the 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. The proactive protection extends beyond reactive blacklists or signature-based defenses.

Web Browser Isolation

ETDRI isolates risky links and attachments, shielding users from attacks like credential theft and ransomware. These suspicious links are rendered in a secure environment, neutralizing malicious content. Additionally, potentially risky attachments are executed in a virtual air gap environment to prevent malware infection. Finally, phishing websites are displayed in read-only mode to block credential theft.

Office365 Clawback

ETDRI can automatically move any delivered email that is later found to contain malware out of end-user inboxes using the Office365 clawback feature.

Comprehensive Analytics and Security Operations Center (SOC) Integration

Advanced Email Security Analytics

As shown in Figure 1, ETDRI provides unparalleled visibility into email attack campaigns with more than 60 data points, including indicators of compromise (IOCs) such as URLs, file hashes, and attack sources. Threat categorization and severity levels are determined to prioritize responses. Detailed reporting on both clean and malicious emails are developed and available for full-spectrum visibility.

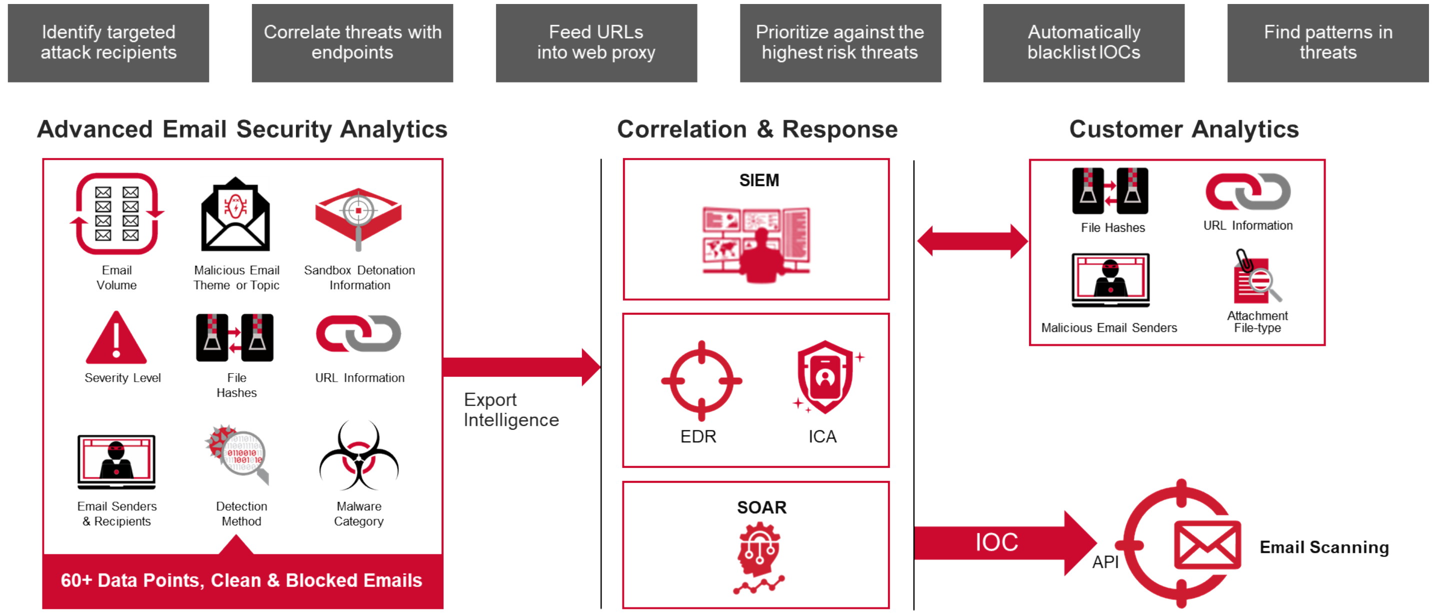
SOC Integration

ETDRI integrates seamlessly with third-party Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems to enhance threat intelligence and streamline SOC workflows. Granular, API-driven data feeds are provided for rapid threat correlation, and prebuilt apps for Splunk and QRadar visualize threats, track high-risk users, and analyze attack timelines.

Consolidated Threat View

ETDRI integrates with Symantec Endpoint Detection and Response (EDR) and the Secure Web Gateway family via Symantec Information Centric Analytics (ICA), enabling cross-control point correlation powered by the Symantec GIN. This enables unified threat insights to detect advanced threats that evade individual point products.

Figure 1: The Deepest Visibility Into Advanced Email Attacks


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
Advanced Email Security Analytics
Correlation & Response
Customer 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
SIEM
EDR
ICA
SOAR
File Hashes
URL Information
Malicious Email Senders
Attachment File-type
IOC
API
Email Scanning

Rapid Response and Remediation

Automated Remediation

ETDRI automates the blacklisting of IOCs, such as file hashes and IP addresses, to accelerate response times and reduce manual workloads. This allows the service to remove malicious emails from Office 365 inboxes before user interaction and strengthens the overall security posture while enhancing security team productivity. While an API is provided for speed, the service also supports adding via the console for convenience.

Security Awareness Training

ETDRI includes integrated security awareness training to reduce user susceptibility to phishing. This allows organizations to simulate phishing attacks to evaluate employee readiness. Detailed reporting and executive dashboards are available to identify the most vulnerable users. Furthermore, ongoing training and repeat assessments can be scheduled to improve resilience against emerging phishing threats.

Summary

Symantec ETDRI is a comprehensive solution for combating targeted and advanced email threats. By combining state-of-the-art detection, automated remediation, and user education, ETDRI ensures that organizations stay ahead of evolving cyber risks. With its integration into broader security ecosystems, ETDRI empowers security teams to respond quickly and effectively while enhancing the organization's overall security posture.

BROADCOM®
connecting everything®

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