

# Email Security.cloud

## Umfassende E-Mail-Sicherheit für die moderne Bedrohungslandschaft

### Übersicht

Umfassende E-Mail-Sicherheit für die moderne Bedrohungslandschaft

E-Mail ist nach wie vor ein Hauptziel für Cyberangriffe, die von Kriminellen für die Verbreitung von Bedrohungen wie Ransomware, Business Email Compromise (BEC) und Phishing ausgenutzt werden. Laut dem Verizon Data Breach Investigations Report 2024 ist die E-Mail die wichtigste Methode zur Verbreitung von Ransomware und der zweithäufigste Vektor bei Sicherheitsverletzungen. Der IBM 2023 Security Breach Report zeigt die enormen Kosten von E-Mail-basierten Angriffen auf: durchschnittlich 4,67 Millionen Dollar für BEC, 4,76 Millionen Dollar für Phishing und 4,55 Millionen Dollar für Social Engineering-Angriffe.

Angreifer setzen zunehmend ausgefeilte Taktiken wie Spear-Phishing, Domain-Spoofing und verschleierte Links ein, um herkömmliche E-Mail-Abwehrmechanismen zu umgehen. Unternehmen, die zu Cloud-basierten E-Mail-Systemen wie Microsoft Office 365 und Google Workspace migrieren, sehen sich mit erhöhten Schwachstellen konfrontiert, da die integrierte Sicherheit oft nicht ausreicht. Veraltete E-Mail-Sicherheitslösungen, die durch unzureichende Analysen und isolierte Abläufe eingeschränkt sind, können die Anforderungen der heutigen komplexen Bedrohungslandschaft nur schwer erfüllen. Dies führt zu Lücken im Schutz, betrieblicher Komplexität und einem steigenden Risiko von Datenverlusten, Verstößen gegen die Compliance und finanziellen Verlusten. Robuste, integrierte E-Mail-Sicherheit ist jetzt eine Notwendigkeit.

### Einführung von Symantec® Email Security.cloud Service (ESS)

Symantec ESS bietet eine umfassende Lösung zum Schutz von Cloud-basierten E-Mail-Plattformen (Office 365, Google Workspace) und lokalen Systemen (Microsoft Exchange). Symantec ESS nutzt einen mehrschichtigen Schutz und blockiert fortschrittliche Bedrohungen wie Ransomware, Spear-Phishing und BEC. Gleichzeitig wird die Transparenz von Angriffskampagnen durch fortschrittliche Analysen und die Integration mit dem Symantec Global Intelligence Network (GIN) verbessert.

Abbildung 1: Der umfassendste Schutz in der Branche



Diese umfassende E-Mail-Sicherheitslösung bietet End-to-End-Schutz, beginnend mit Prävention, Isolierung und Reaktion. Sie legt außerdem Wert auf die Vorbereitung der Benutzer, Interoperabilität und Kompatibilität, um den Sicherheitsstapel zu optimieren und die Investitionsrentabilität zu maximieren.

## Produktbeschreibung

### auf einen Blick

Symantec® Email Security.cloud bietet eine umfassende Lösung für den Schutz Cloud-basierter E-Mail-Plattformen.

### Vorteile

- Verbesserter Schutz vor fortgeschrittenen Bedrohungen
- Verbesserte betriebliche Effizienz
- Kostengünstige Sicherheitslösung
- Stärkere Einhaltung von Vorschriften und Datenschutz
- Gestärktes Benutzerbewusstsein

### KEY FEATURES

- Erweiterte Erkennung und Prävention
- Funktionen zur Isolierung von Bedrohungen
- Umfassende Bedrohungsdaten
- Integrierte Benutzerschulung und Analysen
- Nahtlose Integration in Sicherheits-Ökosysteme

## Prävention: Die erste Verteidigungslinie

Der Eckpfeiler der E-Mail-Sicherheit ist die Prävention. Symantec ESS verbessert die systemeigene Sicherheit von E-Mail-Systemen, indem es Malware und E-Mail-Bedrohungen mit minimalen Fehlalarmen wirksam verhindert. Fortschrittliche Erkennungstechnologien und Telemetriedaten aus dem GIN blockieren ausgefeilte Angriffe wie Ransomware, Spear Phishing und BEC. Durch die Filterung von Spam und unerwünschten E-Mails wie Newslettern und Marketing-Nachrichten steigert Symantec ESS die Benutzerproduktivität und bietet gleichzeitig einen zuverlässigen Schutz.

### Malware & Spam Schutz

- **Schutz vor Malware und Spam:** Nutzen Sie Reputationsanalysen, Antivirus-Engines und Antispam-Signaturen, um Links und Anhänge zu prüfen und so Spam und Malware effektiv zu blockieren.
- **Schutz auf Verbindungsebene:** Verringern Sie Spam- und Malware-Risiken, indem Sie anormale SMTP-Verbindungen verlangsamen und unterbrechen.
- **Isolierung von Bedrohungen:** Verhindern Sie die Infektion von Benutzern mit Ransomware und anderer Malware, indem Sie verdächtige E-Mail-Anhänge isolieren. Diese Technologie isoliert auch riskante oder unbekannte E-Mail-Links, die Malware enthalten, und schützt so Benutzer und Geräte vor infizierten Downloads.

### Phishing-Abwehr

- **Link-Schutz:** Scannen Sie Links in Echtzeit vor der E-Mail-Zustellung und erneut zum Zeitpunkt des Klicks und verfolgen Sie sie bis zu ihrem endgültigen Ziel - selbst wenn Angreifer fortschrittliche Umgehungstechniken verwenden. Die erweiterte Erkennung von Phishing-Varianten identifiziert und blockiert Links, die bekannten Phishing-Angriffen ähneln.
- **Impersonation-Kontrollen:** Starker Schutz vor BEC und Spoofing durch den Einsatz einer ausgeklügelten Impersonation-Engine zur Blockierung von Bedrohungen, die legitime Benutzer oder Domänen imitieren.
- **Isolierung von Bedrohungen:** Öffnen Sie riskante oder unbekannte Website-Links im schreibgeschützten Modus, um die Benutzer vor Phishing-Angriffen zu schützen.

Symantec ESS nutzt globale Bedrohungsdaten aus dem weltweit größten zivilen globalen Netzwerk, um einen unvergleichlichen Einblick in die Bedrohungslandschaft zu erhalten. Telemetriedaten von über 175 Millionen Endgeräten, 80 Millionen Web-Proxy-Benutzern und 57 Millionen Angriffssensoren in 157 Ländern ermöglichen die Analyse von täglich 8 Milliarden Bedrohungen und sorgen für bessere Sicherheitsergebnisse und proaktive Abwehrstrategien.

## Isolierung: Verbessern Sie die Prävention mit der Erkennung neu auftretender Bedrohungen

Symantec Email Threat Detection Response and Isolation (ETDRI), ein Cloud-basierter Service, erweitert die Fähigkeiten von Symantec Email Security durch die Integration fortschrittlicher Technologien zur Neutralisierung von E-Mail-basierten Angriffen, bevor sie Benutzern oder Systemen schaden können.

### Schlüsselkompetenzen

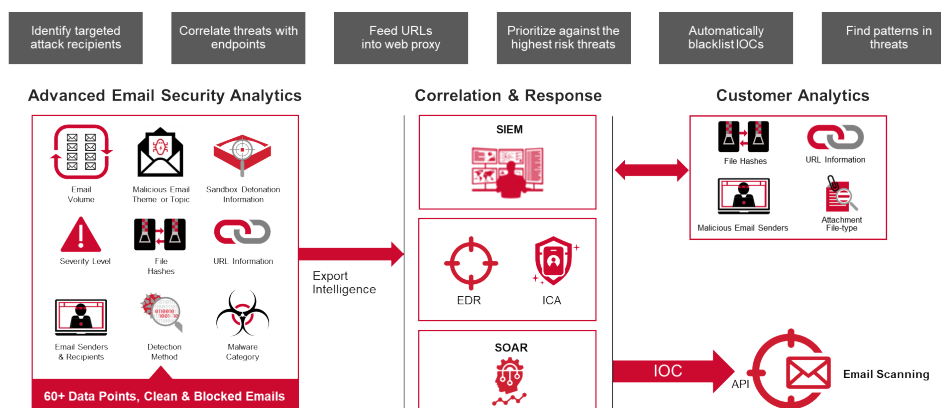
- **Cloud-basiertes Sandboxing:** Entdecken Sie komplexe und fortgeschrittene Angriffe mit unserer Cloud-basierten Sandbox-Umgebung. Dieser Service nutzt Techniken, um menschliches Verhalten zu imitieren und verdächtige Dateien sowohl virtuell als auch auf physischer Hardware auszuführen, um Angriffe zu entdecken, die sich der Erkennung durch herkömmliche Sandboxing-Technologien entziehen.
- **URL-Schutz mit Klickzeit:** Bösartige Links werden blockiert, wenn sie angeklickt werden, um Benutzer vor Angriffen zu schützen, die einen Link nach der Zustellung einer E-Mail als Waffe einsetzen. Dies ergänzt die Echtzeit-Linkverfolgung in ESS.
- **Office 365-Rückforderung:** Verschieben Sie zugestellte E-Mails, bei denen sich später herausstellt, dass sie Malware enthalten, aus dem Posteingang des Endbenutzers.

- **Webbrowser-Isolierung:** Benutzer werden vor fortschrittlichen E-Mail-Angriffen wie Spear-Phishing, Diebstahl von Anmeldedaten und Ransomware geschützt, indem eine isolierte Ausführungsumgebung zwischen Benutzern und E-Mail-Links geschaffen wird, die verdächtige Inhalte per Fernzugriff rendert und potenziell infizierte Downloads scannt, bevor sie ausgeliefert werden.

## Reagieren: Verbesserte Sichtbarkeit und schnellere Reaktion

Wirksame E-Mail-Sicherheit geht über Prävention und Isolierung hinaus, indem sie Unternehmen mit den Tools und Erkenntnissen ausstattet, die sie benötigen, um auf E-Mail-basierte Angriffskampagnen zu reagieren. Symantec ETDRI unterstützt diese Fähigkeit, indem es einen umfassenden Einblick und Analysen bietet und so schnellere und effektivere Reaktionen auf gezielte und hochentwickelte Bedrohungen ermöglicht.

Wie in Abbildung 2 dargestellt, liefert Symantec ETDRI unübertroffene Informationen, indem es sowohl saubere als auch bösartige E-Mails analysiert und über 60 Indikatoren für eine Gefährdung (Indicators of Compromise, IoCs), einschließlich URLs, Datei-Hashes und gezielte Angriffsdetails, bereitstellt.



Dieser umfangreiche Datenstrom kann über APIs nahtlos in ein Security Operations Center (SOC) integriert werden, was die Kompatibilität mit Security Information and Event Management (SIEM) und Security Orchestration, Automation, and Response (SOAR) Systemen von Drittanbietern ermöglicht.

Mit dieser Integrationsebene können Unternehmen Folgendes erreichen:

- **Jagen Sie nach Bedrohungen:** Analysieren Sie Ihre Umgebung, um potenzielle Risiken zu erkennen und die Schwere und den Umfang von Angriffen zu bewerten.
- **Korrelieren von Ereignissen:** Kombinieren von Erkenntnissen aus Symantec Endpoint Detection and Response (EDR) und Secure Web Gateway-Lösungen, um fortschrittliche Bedrohungen an mehreren Kontrollpunkten zu erkennen.
- **Abhilfe schaffen und Reaktionen orchestrieren:** Eindämmen von Bedrohungen durch Blockieren von Angriffen und Automatisieren von Reaktionen im gesamten Sicherheitsökosystem.

Durch die Integration von Symantec ETDRI in ein umfassenderes Sicherheits-Framework erhalten Sie einen einheitlichen Ansatz für die Identifizierung, Analyse und Neutralisierung von Bedrohungen, der sicherstellt, dass Ihr Unternehmen gegen sich entwickelnde E-Mail-basierte Angriffe gewappnet ist.

## Vorbereitung der Benutzer: Das menschliche Element stärken

In jeder Sicherheitsstrategie ist das menschliche Element oft das schwächste Glied. Angreifer verstehen sich hervorragend auf Social Engineering, so dass es für Benutzer schwierig ist, Bedrohungen zu erkennen, bevor es zu spät ist. Symantec ETDRI stellt sich dieser Herausforderung, indem es robuste Funktionen für die Sicherheitsaufklärung und -schulung bereitstellt, die darauf ausgelegt sind, Risiken zu reduzieren und Benutzer in die Lage zu versetzen, E-Mail-Bedrohungen effektiv zu erkennen und darauf zu reagieren. Symantec ETDRI unterstützt Unternehmen wie folgt:

- **Bewerten Sie die Bereitschaft:** Simulieren Sie reale Phishing-Bedrohungen mit anpassbaren Sicherheitsbewertungen, die auf die Bedürfnisse Ihres Unternehmens zugeschnitten sind.
- **Verfolgen und bewerten Sie den Fortschritt:** Mit Hilfe von Dashboards und detaillierten Berichten erhalten Sie Einblick in das Benutzerverhalten. Wiederholte Bewertungen helfen, Trends zu erkennen und Verbesserungen im Laufe der Zeit zu messen.
- **Priorisieren Sie den Schutz:** Entwickeln von Risikoprofilen für Benutzer durch Kombination von Erkenntnissen aus Symantec-E-Mail-Sicherheitsanalysen mit Information Centric Analytics, so dass sich Administratoren auf die am stärksten gefährdeten Benutzer konzentrieren können.

Schulungsbenachrichtigungen und Lerninhalte bereiten Mitarbeiter darauf vor, ausgeklügelte E-Mail-Angriffe zu erkennen und zu melden. Indem Symantec ETDRI Benutzer mit dem Wissen und den Fähigkeiten ausstattet, Phishing-Versuche zu erkennen, wird eine Kultur des Sicherheitsbewusstseins geschaffen, die die Wahrscheinlichkeit erfolgreicher Angriffe verringert und die allgemeine Widerstandsfähigkeit des Unternehmens erhöht.

## Interoperabilität und Kompatibilität: Nahtlose Integration für mehr Sicherheit

Durch die Integration von Symantec ESS in eine umfassendere Sicherheitsinfrastruktur, einschließlich Data Loss Prevention (DLP), Verschlüsselungskontrollen sowie Endgeräte-, Netzwerk- und Cloud-Sicherheitslösungen, können Unternehmen ihre Sicherheitsabläufe optimieren und die Investitionsrendite maximieren.

Symantec ESS verbessert die Einhaltung von Richtlinien und den Datenschutz durch integrierte DLP- und richtlinienbasierte Verschlüsselungskontrollen:

- **Schutz vor Datenverlust (DLP):** Flexible Richtlinien identifizieren und kontrollieren sensible E-Mails mithilfe von über 100 vordefinierten Schlüsselwort-Wörterbüchern, regulären Ausdrücken und MIME-Typ-Listen.
- **Richtlinienbasierte Verschlüsselung:** Vertrauliche E-Mails werden vertraulich behandelt, indem Nachrichten automatisch in passwortgeschützte PDFs verschlüsselt werden, um eine mobilfreundliche Push-Verschlüsselung zu ermöglichen.

Als Teil der Symantec Integrated Cyber Defense Platform erweitert Symantec ESS seine DLP-Funktionen durch die Integration mit Symantec Data Loss Prevention und ermöglicht so einen umfassenden Schutz von Daten über E-Mail-, Endgeräte-, Netzwerk-, Cloud-, Mobil- und Speichersysteme hinweg. Erweiterte Verschlüsselungsanforderungen werden mit Symantec Policy-Based Encryption Advanced erfüllt, einem anpassbaren Cloud-basierten Zusatzdienst, der es Administratoren ermöglicht, flexible, richtliniengesteuerte Verschlüsselungsregeln zum Schutz von Informationen in Übereinstimmung mit den Compliance-Anforderungen des Unternehmens festzulegen. Mit dieser gehosteten Lösung können Unternehmen schnell robuste Verschlüsselungsfunktionen zum Schutz vertraulicher Daten implementieren, die per E-Mail ausgetauscht werden, ohne dass die Verwaltung digitaler Zertifikate oder Verschlüsselungsschlüssel kompliziert ist.

Die Lösung lässt sich außerdem nahtlos in andere Symantec-Produkte integrieren, um die Sicherheit auf Endgeräten, im Internet und in Messaging-Anwendungen zu erhöhen. In Verbindung mit Symantec Endpoint Security können E-Mail-Informationen, die von neuen Bedrohungen gesammelt wurden, als Blocklisten an Endgeräte verteilt werden, um Folgendes zu verhindern

Infektionen in einem Unternehmen. Diese Kompatibilität dehnt den Schutz auf moderne Collaboration- und Messaging-Plattformen aus - sowohl Cloud-basiert als auch vor Ort -, darunter Slack, Salesforce und Box, und gewährleistet so eine zusammenhängende und verstärkte Sicherheitslage.

Durch die Verknüpfung von E-Mail-Sicherheit mit dem bestehenden Sicherheits-Ökosystem vereinfacht Symantec ESS die Verwaltung, verbessert die Reaktion auf Bedrohungen und stärkt den Schutz über alle digitalen Berührungspunkte hinweg.

### Zusammenfassung

Symantec ESS bietet unvergleichlichen Schutz vor hochentwickelten E-Mail-Bedrohungen durch die Integration von fortschrittlicher Erkennung, Isolierung, Analyse und Benutzerschulung. Diese Lösung versetzt Unternehmen in die Lage, den sich entwickelnden Cyber-Risiken einen Schritt voraus zu sein und sich gleichzeitig nahtlos in breitere Sicherheits-Ökosysteme

zu integrieren, um die Compliance zu verbessern, die betriebliche Komplexität zu reduzieren und die allgemeine Sicherheitslage zu stärken.

Symantec ESS zeichnet sich durch hohe Effektivität, hohe Genauigkeit und branchenführende SLAs aus und lässt sich bei wachsendem Messaging-Volumen einfach implementieren, betreiben und skalieren. Unterstützt von der Symantec Integrated Cyber Defense Platform bietet die Lösung unübertroffenen Schutz, betriebliche Effizienz und niedrige Gesamtbetriebskosten und ist damit die ideale Wahl für den Schutz der E-Mail-Infrastruktur selbst vor den fortschrittlichsten Angriffen.