mimecast®

DATASHEET

Mimecast Advanced Security

Cloudbasierte Email-Security-Lösungen, die Ihr Unternehmen vor neuartigen Email-Bedrohungen wie Spear-Phishing und Identitätsbetrug schützen.

Mimecast Advanced Security umfasst mehrere Cloud-Services, die Unternehmen dabei unterstützen, sich gegen neuartige Email-basierte Bedrohungsformen zu verteidigen. Die Mimecast- Services wehren neben Spam und Viren Email-basierte neue Bedrohungsformen wie Identitätsbetrug, bösartige URLs und Anhänge sowie unternehmensinterne Bedrohungen ab.

Zu den Mimecast-Services gehören:

1. **Mimecast Targeted Threat Protection (TTP).** Inspektion eingehender, ausgehender und interner Emails, um Phishing-Versuche, Ransomware, Identitätsbetrugsversuche, bösartige URLs und Anhänge zu entdecken und zu bekämpfen. Zu TTP gehören URL Protect, Attachment Protect, Impersonation Protect und Internal Email Protect.

2. Inhaltskontrolle und der Schutz vor Datendiebstahl (**Data Leak Prevention, DLP**). Schutz vor dem Verlust geistigen Eigentums, von Kundendaten oder anderen sensiblen Informationen. Die Regeln für Email-Inhalte und sichere Kommunikation werden in Echtzeit auf den eingehenden, ausgehenden und internen Email-Verkehr angewandt.

3. **Spam- und Virenschutz.** Hält infizierte Emails zum Schutz der Mitarbeiterproduktivität aus dem Firmennetz fern. Mimecast garantiert SLAs von 100% bei Viren und 99% bei Spam. Bedrohungen werden in der Cloud abgefangen, bevor sie Ihr Netz erreichen.

So funktionieren die Mimecast-Services

Einfache Implementierung, einfaches Management

- Schalten Sie Ihre MX-Records auf die Mimecast-Cloud-Plattform um.
- Leiten Sie allen eingehenden, ausgehenden oder internen Mail-Verkehr durch die Mimecast-Services.
- Dort prüfen diverse signaturbasierte Inspektionsschritte die Email auf Schadsoftware und Spam.
- Nachrichten mit Spam oder Schadsoftware werden automatisch zurückgewiesen oder gelöscht.
- Nach organisationsspezifischen Regeln werden Email-Inhalte, Anhänge oder Bilder gefiltert.
- Alle eingehenden URLs werden überschrieben und bei Anklicken in Echtzeit überprüft.
- Sandboxing und sofortige Voransicht von Dateianhängen schützen gegen gefährliche Anhänge.
- Blockiert oder kennzeichnet Versuche von Identitätsbetrug.

KEY BENEFITS:

- Schützt gegen das Risiko von Speer-Phishing und fortgeschrittenen Bedrohungen in Emails
- Blockiert Spam und Viren
- Schützt die Mitarbeiter vor Social Engineering und Identitätsbetrugs- Angriffen
- Neutralisiert Bedrohungen durch Malware-Anhänge und verseuchte URLs
- Beseitigt die Graymail-Belastung für Endbenutzer
- Ermöglicht automatisierte E-Mail-Verschlüsselung und sichere Nachrichtenübermittlung
- Microsoft Outlook Tab für verbesserte User Experience
- Unterstützt die Aufmerksamkeit der User auf mögliche Bedrohungen zu richten
- Eliminiert die Notwendigkeit, E-Mail-Sicherheits Software und Hardware zu verwalten
- Erkennt und blockiert Angriffe von externen und internen Bedrohungsakteuren
- Nutzung der Cloud, sofortige Verfügbarkeit der aktuellsten E-Mail-Sicherheitsschutz

- Graymail (legitime Massen-E-Mail) wird gekennzeichnet und außerhalb des Posteingangs der Anwender verwaltet.

Ununterbrochen sicher

Der Schutz vor Viren, Spam und Datenverlusten, die URL-Überschreibung, der Schutz vor Identitätsbetrug, das Blockieren von Schadsoftware, die interne Überwachung und die Kontrolle von Graymail bilden eine einheitliche Lösung. Mimecasts Expertenteam ist auf die Gefahrenabwehr und den Einsatz neuartiger Sicherheitstechnologien spezialisiert. Dies stellt sicher, dass Sie gegen jede aktuelle Angriffsform geschützt sind. Einmal installiert, sichert Mimecast die Posteingangsfächer Ihrer Anwender, schützt Sie vor Spear-Phishing (gezieltem E-Mail-Betrug mit dem Ziel, auf Daten zuzugreifen) und verwaltet Ihre Graymail. Sie können sich auf Ihr Kerngeschäft konzentrieren.

Abwehr neuartiger Bedrohungen

Basis der massiv skalierbaren Email-Sicherheitsdienste von Mimecast ist die selbst entwickelte MimeOS-Cloudplattform. Email-basierte Bedrohungen wie Schadsoftware, Spam, Attacken mittels Spear-Phishing und andere Angriffsformen werden gestoppt, bevor sie Ihr Email-System erreichen. Das senkt die Risiken, denen Mitarbeiter ausgesetzt sind und verbessert die Leistungsfähigkeit des Email-Systems.

Mimecast Targeted Threat Protection (TTP) schützt vor Spear-Phishing und anderen gezielten Angriffsformen per Email. Jede URL in eingehenden Emails wird umgeschrieben und verweist anschließend auf die Mimecast Cloud zur intelligenten Bedrohngsanalyse. Das schützt Anwender, die versehentlich bösartige oder Spearphishing-Sites anklicken könnten, davor, auf potentiell zerstörerische Inhalte zuzugreifen oder ihre Systeme mit Schadsoftware zu verseuchen.

Email-Anhänge können vorbeugend in einer abgeschotteten Umgebung gescannt und in harmlose Dateiformate umgewandelt werden, um so vor schadhaften Anhängen, Macros oder bösartigen Inhalten zu schützen. Endanwender werden zudem vor Social Engineering und Angriffen durch Identitätsbetrug per Email bewahrt. Eine Reihe ausgefeilter Sicherheitsüberprüfungen schützen gegen Spoofing und betrügerische Anfragen. Endanwender werden auf verdächtige Email aufmerksam gemacht, um Datenverluste zu verhindern.

Service für Endanwender

Sollte gelegentlich eine unschädliche Email in Quarantäne geraten, können Endanwender direkt aus Outlook oder über mobile Apps die betroffenen Mails einfach finden. Das verringert den Aufwand für das Helpdesk. Selbstlernende Technologie und persönliche Blockier- und Erlaubnislisten stellen sicher, dass ähnliche Nachrichten zukünftig richtig behandelt werden.

Mimecast Email Security – wichtige Funktionen

MimeOS Cloud-Sicherheitsplattform
Zentrale Verwaltung über eine einzige Web-basierte Administrationskonsole
Endanwenderzugriff über Mimecast Personal Portal
Skalierbare, mandantenfähige Cloud-Infrastruktur mit 100%-SLA
Automatische Synchronisierung mit dem Active Directory für Regel- und Zugangskontrolle
Überwachungs-Dashboard für Email-Warteschlangen und -Dienste mit Benachrichtigung über Email und SMS
Neuartige Routingfunktionen mit Echtzeitansicht aller SMTP-Verbindungen und abgewiesener Verbindungsversuche
Detaillierte Übertragungsdaten für jede Email, die von Mimecast verarbeitet wird
Schutz vor neuartigen Angriffsformen
Mehrschicht-Schutz vor neuartiger und bereits bekannter Schadsoftware
Alle URLs in Emails werden überschrieben, auf Anklicken erfolgt eine Überprüfung, um Endanwender vor bösartigen URLs zu schützen.
Vorbeugende Abschottung von Email-Anhängen, um vor schadhaften Anhängen zu schützen
Sofortige Voransicht von Dateianhängen - aktiver Code wird entfernt, um Makro-Bedrohungen zu neutralisieren
Abwehr vor Social Engineering und Angriffen durch Identitätsbetrug mittels ausgefeilter Schutzmechanismen
Sicherheitsinspektion eingehender, ausgehender und interner Emails
Umfassender verbindungs- und inhaltsbasierter Schutz vor Spam und Phishing
Persönliche Erlaubnis- und Verbotslisten, um das individuelle Quarantäne-Management von Spam und Endanwender-Email fein zu differenzieren
SLAs: 100% Schutz vor Viren, 99% Schutz vor Spam, 0,0001% falsch-positive Spam- Identifikationen.