



Mimecast E-Mail-Sicherheit Cloud-Gateway

- Einfache Sicherung komplexer E-Mail-Umgebungen
- Integrieren und erweitern Sie Ihr Sicherheits-Ökosystem
- Erhalten Sie erstklassige E-Mail Sicherheitseffizienz
- Passen Sie Richtlinien an Ihre Anforderungen an



Ihr unverzichtbarer Begleiter für KI-gestützte E-Mail- und Ausfallsicherheit für M365 und Google Workspace

Cyber-Bedrohungen per E-Mail sind nach wie vor eines der größten Risiken für Unternehmen. Von Phishing und Ransomware bis hin zu Credential und Zero-Day-Angriffen, das Volumen und die Raffinesse der Bedrohungen, die auf Ihr wichtigstes Kommunikationsmittel zielen, nehmen weiter zu. Ihre Arbeitsoberfläche ist jetzt auch Ihre Risikooberfläche.

Sichern Sie selbst die komplexesten E-Mail Umgebungen, passen Sie Richtlinien an Ihre Bedürfnisse an und erweitern Sie den Schutz durch eine Reihe von ergänzenden Lösungen mit Mimecast Email Security, Cloud Gateway (CG). Ein Secure Email Gateway in der Cloud, das KI-gestützte Erkennung zur Verteidigung gegen Angriffe nutzt und sich nahtlos mit M365 und Google Workspace integrieren lässt, um die Abwehr zu verstärken und einen vollständigen Schutz zu erzielen.

Wichtigste Vorteile:

- Sichern Sie jede Art von E-Mail-Umgebung: M365, Google Workspace, Vor-Ort, Cloud, Hybrid
- Blockieren Sie die gefährlichsten Bedrohungen mit KI-gestützter Erkennung
- Passen Sie Richtlinien an Ihre spezifischen Anforderungen an
- Einfaches Verwalten großer und komplexer E-Mail-Umgebungen: AAA, FAA, häufige M&A
- Erweitern und vereinfachen Sie den E-Mail Schutz mit vollständig integrierten, ergänzenden Lösungen
- Integrieren Sie Mimecast ganz einfach in Ihr größeres Sicherheits-Ökosystem

Blockieren Sie alle E-Mail-basierten Bedrohungen

Mimecast ist seit 20 Jahren führend im Bereich E-Mail-Sicherheit und bietet branchenführende Erkennung und erstklassige Effizienz, auf die 42.000 Kunden weltweit vertrauen. Durch den Einsatz der richtigen Erkennungsfunktionen zur richtigen Zeit, umgibt Email Security CG Ihre Kommunikation mit kontinuierlichem Schutz und blockiert Bedrohungen, von Phishing und Ransomware bis hin zum Diebstahl von Zugangsdaten und Zero-Day-Bedrohungen. Die branchenweit zuverlässigste Übersicht über die E-Mail-Bedrohungslandschaft - abgeleitet aus der Prüfung von 1,3 Milliarden E-Mails täglich durch Mimecast - ermöglicht die sofortige Blockierung der überwiegenden Mehrheit der E-Mail-basierten Angriffe, während die neueste KI und das maschinelle Lernen eine intelligente Erkennung neuer und unbekannter Bedrohungstypen liefert.

Marken weltweit vertrauen Mimecast

42.000

E-Mail-Sicherheit Kunden in aller Welt

1.3 Milliarden

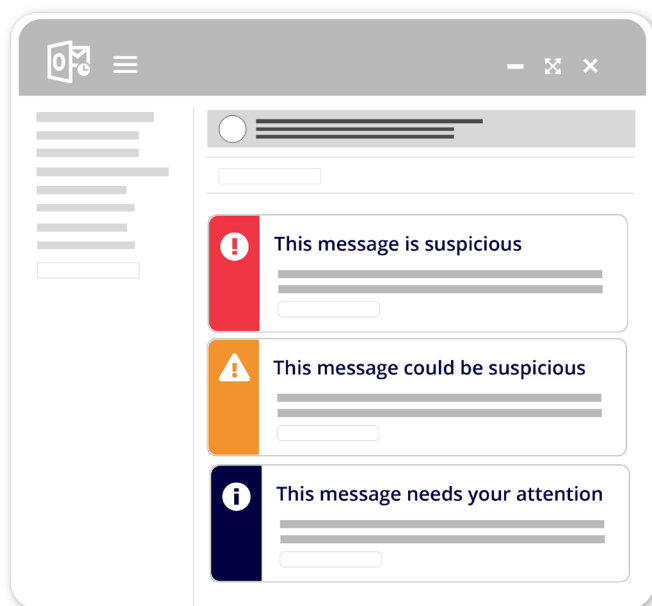
Die von Mimecast täglich geprüft werden, geben uns den branchenweit zuverlässigsten Überblick über die E-Mail-Bedrohungslandschaft

“Unsere globale Plattform verändert sich häufig durch Fusionen und Übernahmen. Wir brauchen Partner, die mit uns skalieren können und flexibel bleiben.”

Erik Hart, Chief Information Security Officer
Cushman & Wakefield

Begrenzen Sie die Erkundung durch Angreifer und befähigen Sie Ihre Mitarbeiter durch KI-gesteuerte Warnbanner

Email Security CG schützt Mitarbeiter bis zum Punkt des Risikos und nutzt Social Graphing, um Kommunikationsmuster abzubilden, Anomalien zu identifizieren und Angriffe zu erkennen, die Techniken wie dateilose Malware und Social Engineering nutzen. KI-gestützte Warnbanner werden dann nur auf E-Mails angewendet, die sie rechtfertigen und in Echtzeit auf allen Geräten aktualisiert, wenn sich die Risikostufe ändert. Die Lösung erkennt auch und warnt Mitarbeiter vor potenziell falsch adressierten E-Mails und entfernt eingebettete E-Mail-Tracker die Details wie den Standort des Benutzers preisgeben, die für gezielte Angriffe genutzt werden können.



Sichern Sie selbst die komplexesten E-Mail-Umgebungen

Komplexe Organisationen haben oft auch komplexe E-Mail-Sicherheitsanforderungen - hybride E-Mail Einsätze, regionale und globale Unterschiede, AAA oder FAA, häufige M&A-Aktivitäten und vieles mehr. Email Security CG bietet flexible und effektive Tools für die Verwaltung großer oder komplexer E-Mail-Infrastrukturen, wobei Domänen oder Abteilungen, die eine Segmentierung oder eine Trennung der administrativen Aufgaben erfordern ebenfalls eingerichtet werden können, während die Kontrolle bei den Top-Level-Administratoren bleibt. Flexible Richtlinienvererbung stellt sicher, dass Richtlinien auf Gruppen- oder Unternehmensebene bis hinunter zu regionalen oder abteilungsspezifische Geschäftskonten übertragen wird.

Einfache Integration von Mimecast in Ihr größeres Sicherheits-Ökosystem

Email Security CG beschleunigt und vereinfacht die Integration mit anderen Sicherheitstechnologien, wie SIEM, SOAR, TIP, XDR, und mehr. Die Integration von Mimecast mit Ihren anderen Lösungen und die gemeinsame Nutzung von Informationen aus dem Angriffsvektor - E-Mail - ist schnell und einfach und eröffnet unendlich viele Möglichkeiten, die Erkennung und Reaktion zu beschleunigen, den manuellen Aufwand zu reduzieren und Investitionen zu optimieren.



Anpassen von E-Mail-Sicherheitsrichtlinien für Ihre spezifischen Anforderungen

Email Security CG bietet Schutzmaßnahmen, die bei der Bereitstellung optimiert sind und gleichzeitig Richtlinienanpassung und granulare Kontrollen unterstützt, die viele IT- und Sicherheitsteams benötigen, von Benutzersegmentierung und Quarantäne-Einstellungen, Spam-Filterung, Anpassung von Aufklärungs- und Warnbanner und vieles mehr.

Der Zugriff auf die globale Policy Engine der Lösung erfolgt über eine intuitive, einheitliche Verwaltungskonsole, die sowohl Benutzerfreundlichkeit als auch Übersichtlichkeit bietet.

Umfassender Schutz für M365 und Google Workspace

Die Massenkonsolidierung auf M365 und Google Workspace hat den Fokus der Angreifer auf diese kritischen Produktivitätsplattformen, wobei immer mehr und mehr Bedrohungen, die speziell darauf ihre Verteidigung zu umgehen. Email Security CG integriert sich nahtlos in diese Umgebungen und nutzt KI-gestützte Erkennung, um Angriffe abzuwehren, die etablierte E-Mail-Anbieter übersehen.

Verbessern Sie den Schutz mit vollständig integrierten, sich ergänzenden Lösungen

Ein Angriffsvektor, ein Problem - was wäre, wenn das alles wäre, was Sie zu lösen hätten? Meistens sind es aber doch mehrere Angriffsvektoren und auch mehr Probleme. Unsere vollständig integrierten, sich ergänzenden Lösungen können Ihnen helfen eine breite Palette von Herausforderungen einfach, effektiv und erschwinglich zu beheben.

DMARC-Verwaltung

Erhalten Sie volle Transparenz und Kontrolle darüber, wer E-Mails in Ihrem Namen versendet durch Beschleunigung und Vereinfachung der Implementierung des DMARC-Protokolls

Schutz vor Insider-Risiken

Verhindern Sie, dass sich Angriffe intern und in Ihrer Lieferkette ausbreiten, indem Sie Best-Practice-Prüfungen für interne und ausgehende E-Mails nutzen

Kontinuität

Halten Sie den E-Mail-Verkehr aufrecht, auch bei geplanten oder ungeplanten Ausfallzeiten mit einfach zu verwaltenden, intuitiven Kontinuitätsfunktionen

Verschlüsselung von Nachrichten

Ermöglichen Sie Ihren Anwendern den sicheren Versand vertraulicher Informationen mit Nachrichtenverschlüsselung, die für alle Nutzer einfach zu bedienen und für Sie einfach zu verwalten ist

