DATASHEET

Email Security Cloud Gateway

Il tuo alleato basato su IA per la sicurezza e la resilienza delle e-mail per M365 e Google Workspace

Il problema

Attacchi di phishing, BEC e tattiche dannose sono alcune delle minacce veicolate dalle e-mail che le organizzazioni devono contrastare. Le soluzioni per la sicurezza e-mail non riescono a tenere il passo, spesso non riconoscono i tentativi avanzati di social engineering, i malware zero-day e i tentativi di spoofing dei domini, esponendo le comunicazioni a potenziali compromissioni. Poiché gli attacchi puntano sempre di più a piattaforme come M365 e Google Workspace, un approccio su più livelli alla sicurezza e-mail è ormai indispensabile.

La soluzione

Basato su cloud, Email Security Cloud Gateway di Mimecast è progettato per proteggere anche gli ambienti di posta elettronica più complessi grazie a funzionalità di ispezione su più livelli potenziate da misure di difesa tradizionali, intelligence sulle minacce e IA avanzata. Questa soluzione completa ispeziona ogni elemento di un'e-mail in tempo reale, bloccando le minacce prima che raggiungano le caselle di posta. Con criteri personalizzabili, controlli granulari e una vasta gamma di soluzioni complementari, Cloud Gateway si integra perfettamente con lo stack di sicurezza esistente, fornendo al contempo funzionalità di correzione automatica che permettono ai team IT e di sicurezza di controllare efficacemente i rischi e ridurre la complessità, per proteggere dagli attacchi e-mail più complessi senza compromettere la continuità aziendale.

2,9 MILIARDI

miliardi di $ di perdite causate da attacchi BEC nel 2023[1]

40%

degli attacchi email dovuto a BEC e pretexting[2]

Il valore di Mimecast

- **Ottieni la protezione migliore**
  Blocca tutte le minacce veicolate dalle e-mail con il rilevamento leader del settore basato su IA, già scelto da 40.000 clienti.
- **Elimina la complessità**
  Gestisci con facilità ambienti e-mail complessi, consolidando e semplificando i servizi di sicurezza.
- **Semplifica le operazioni di sicurezza**
  Riduci il carico di lavoro, informa e responsabilizza il personale.

1 https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
2 https://www.verizon.com/business/resources/reports/dbir/

Funzionalità	Dettagli
BEC	• Protezione da attacchi di social engineering, omografi, omoglifi e impersonificazioni • Analisi della forza delle relazioni tra il mittente e i destinatari nell'organizzazione* • Rilevamento del linguaggio specifico della minaccia nelle e-mail correlate a minacce BEC, come richieste di aiuto in attività, falsi bonifici, urgenza, cambio del canale di comunicazione, truffe con carte regalo, bancarie e finanziarie* • Interpretazione di contesto, sfumature e implicazioni del messaggio per determinarne accuratamente l'intento reale* • Banner di avviso assistiti da IA, visualizzati e aggiornati in tempo reale sui dispositivi in base al livello di rischio*
Minacce interne	• Rilevamento di e-mail con indirizzi errati per la difesa dalle fughe di dati* • Analisi di e-mail interne e in uscita, contro gli utenti interni compromessi, negligenti e malintenzionati
Malware	• Protezione a più livelli contro malware, minacce note e zero-day • Analisi statica dei file e ambiente sandbox per l'emulazione completa • Conversione degli allegati in documenti PDF sicuri e innocui • Portale di decrittografia per la scansione protetta da password di malware e URL
Phishing	• Riscrittura dell'URL di tutti i link nelle e-mail, con scansione al momento del clic • Scansione completa degli URL in più fasi con rilevamento delle minacce basato su apprendimento automatico e protezione delle credenziali • Protezione dei codici QR nelle e-mail e negli allegati con analisi profonda degli URL • I link per il download diretto vengono analizzati attraverso l'analisi statica dei file e il sandboxing
Amministrazione	• Amministrazione centralizzata da un'unica console web • Supporto per M365, Google Workspace, ambienti on-premise, ibridi e altro • Amministrazione avanzata e federata degli account, a supporto delle attività di fusione e acquisizione frequenti • Instradamento intelligente delle e-mail in base a indicatori, destinatari o policy • Sincronizzazione automatica con IAM per i criteri e il controllo degli accessi • Informazioni sulle minacce centralizzate e flussi di lavoro amministrativi ottimizzati • Correzione automatica o manuale di e-mail non sicure, indesiderate o dannose • Ingestione di feed delle minacce specifici per il tenant e delle tendenze delle minacce a livello regionale nei sistemi SIEM, SOAR o TIP • Facile integrazione con fornitori quali Splunk, CrowdStrike, Netskope e altri
Componenti aggiuntivi disponibili	• Cloud Archive • Continuity • DMARC Analyzer • Large File Send • Mimecast Engage • Mimecast Email Incident Response • Messaggistica sicura

*richiede una protezione BEC avanzata

Casi d’uso della sicurezza e-mail

Attacchi di phishing e Business Email Compromise (BEC)

La difesa di Mimecast contro gli attacchi di phishing e BEC sofisticati è strettamente integrata. I feed delle minacce e i protocolli di autenticazione delle e-mail ispezionano le e-mail; quindi l’elaborazione del linguaggio naturale (NLP) estrae il testo e usa il modello di minaccia per analizzare gli indizi di contesto e identificare le minacce senza payload, bloccandole prima che raggiungano le caselle di posta. La tecnologia del grafo sociale crea un grafo di identità delle relazioni tra mittente e destinatario, rilevando le attività anomale con banner dinamici che avvisano gli utenti delle potenziali minacce. Le funzionalità di scansione di allegati e URL della piattaforma, come la protezione dal furto di credenziali e il rilevamento di attacchi a più fasi, analizzano i link per individuare le pagine di phishing.

Minacce malware e ransomware

Il sistema completo di rilevamento delle minacce di Mimecast impiega più livelli di protezione per garantire la massima sicurezza. I file vengono confrontati con il database proprietario di Mimecast, che memorizza un registro dei file già scansionati e si integra con i dati di intelligence sulle minacce specifici del cliente. Per la sicurezza avanzata, vengono utilizzati più motori antivirus per intercettare un numero maggiore di minacce malware. La rapida analisi statica dei file verifica quindi la presenza di caratteristiche sospette come codice nascosto, strutture insolite o connessioni a siti dannosi noti. Infine, i file vengono analizzati in dettaglio in un ambiente sandbox di emulazione che simula un sistema completo. La conversione sicura dei file (facoltativa) consente di eliminare gli eseguibili potenzialmente pericolosi prima della consegna del file.

Contenimento degli attacchi di phishing

In caso di attacco di phishing, gli strumenti di correzione nativi di Mimecast possono gestire e contenere con efficacia le minacce senza affidarsi a sistemi esterni. Con le funzionalità di analisi e risposta, gli analisti identificano la portata della minaccia e cercano altri indicatori di compromissione, semplificando il processo di categorizzazione e risposta alle minacce. La correzione delle minacce semplifica la rimozione delle e-mail colpite direttamente dalla casella di posta degli utenti, riducendo i potenziali danni con risposte rapide. Queste capacità di correzione possono essere utilizzate con strumenti integrati come le piattaforme SOAR o XDR.