Cloudflare Email Security

Fornire protezione autonoma e multicanale per una comunicazione sicura nell'ambiente di lavoro

Proteggiti dagli attacchi mirati di phishing

Blocca e isola facilmente le minacce non rilevate da altre soluzioni

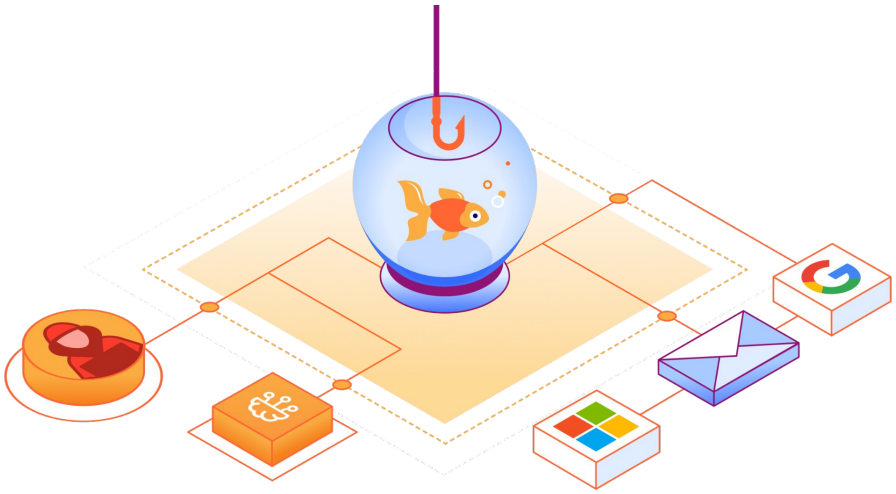
Poiché la posta elettronica rappresenta l'applicazione aziendale più utilizzata e sfruttata, è più importante che mai proteggere gli utenti dagli attacchi di phishing che cercano di manipolare la loro fiducia. Mentre le organizzazioni continuano ad adottare sempre di più i servizi di posta elettronica su cloud tramite Microsoft 365 e Google Workspace per supportare meglio i lavoratori ibridi, gli autori delle minacce si sono concentrati su attacchi più mirati e a basso volume in grado di eludere i tradizionali Secure Email Gateway (SEG) come Proofpoint e Mimecast.

Ecco perché la soluzione di sicurezza e-mail cloud native di Cloudflare è stata progettata appositamente per sfruttare l'intelligence preventiva delle campagne, l'analisi dei contenuti basata su ML e una piattaforma Zero Trust unificata per bloccare le minacce di phishing prima che raggiungano la forza lavoro.

91%
di tutti gli attacchi informatici inizia con un'e-mail di phishing[1]

50 miliardi
in perdite a causa di attacchi BEC nell'ultimo decennio[2]

81%
delle organizzazioni ha subito un attacco multi-canale negli ultimi 12 mesi[3]



Blocca gli attacchi BEC (Business Email Compromise)

Rileva gli account impersonificati e compromessi con un'analisi contestuale a più livelli basata su ML.

Isola gli attacchi differiti e multicanale

Isola gli utenti dai contenuti Web dannosi forniti tramite collegamenti sconosciuti e offuscati.

Blocca ransomware e allegati dannosi

Impedisci ai tentativi di estorsione e al codice dannoso di compromettere la tua organizzazione.

Maggiore protezione e semplicità

Implementa una sicurezza a più livelli che offra una maggiore protezione a una frazione del costo

Mentre gli attacchi di phishing continuano a proliferare, Microsoft e Google hanno continuato a sviluppare funzionalità native che abilitano funzionalità essenziali di protezione dei dati e della posta elettronica, come autenticazione, archiviazione, e crittografia lato client. Tuttavia, gli autori delle minacce hanno sviluppato ulteriormente le loro tattiche per eseguire attacchi più mirati ed evasivi che spesso aggirano i controlli di sicurezza nativi e garantiscono un tasso di successo più elevato.

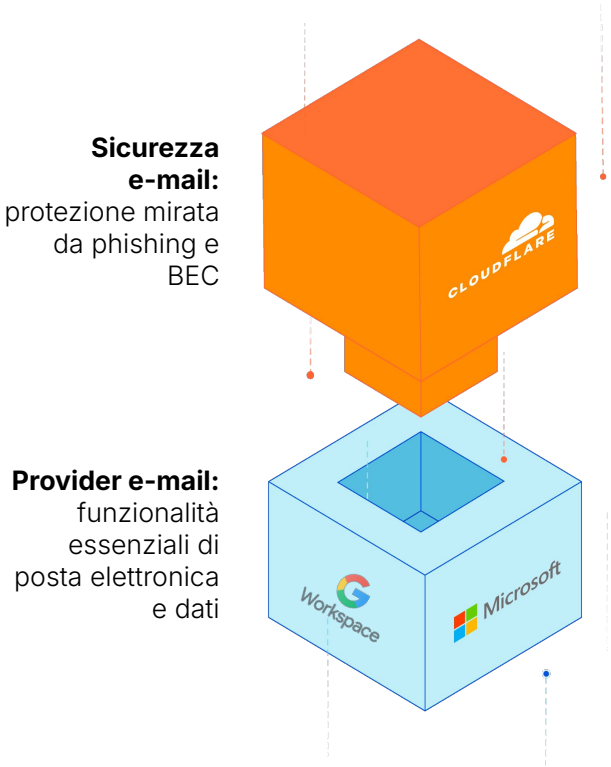
Utilizzando Cloudflare, le organizzazioni possono bloccare o isolare automaticamente attacchi di phishing mirati che sfruttano collegamenti dannosi, allegati e account compromessi per sottrarre informazioni sensibili e commettere frodi finanziarie.

Aumenta i controlli di sicurezza delle e-mail esistenti

La soluzione di sicurezza e-mail cloud native di Cloudflare può essere distribuita in pochi minuti per migliorare le distribuzioni SEG esistenti o integrare le funzionalità di posta elettronica integrate fornite da Microsoft e Google. Con una messa a punto minima o nulla, le organizzazioni possono ottenere una maggiore protezione dal phishing con meno tempo e impegno dedicati alla gestione continua della sicurezza.

"Da quando abbiamo implementato Cloudflare [su M365] abbiamo riscontrato una riduzione del 50% nel numero di e-mail dannose o sospette che i nostri utenti ricevono ogni giorno. In questo modo liberiamo più ore che possiamo reinvestire in altri obiettivi".

Werner Enterprises
(Fortune 1000)



Reinvesti le ore risparmiate grazie alla maggiore automazione

La soluzione automatizzata e leggera di Cloudflare offre un'integrazione perfetta con i flussi di lavoro Microsoft e Google fornendo al contempo un'unica interfaccia utente intuitiva per le attività degli analisti.

Ottieni un'efficacia di rilevamento del 99,997%

La combinazione delle funzionalità native del provider di posta elettronica con la protezione da phishing e BEC di Cloudflare garantisce alle aziende una copertura completa con un rischio minimo.

Realizza maggiore valore a un costo inferiore

La sostituzione di implementazioni obsolete, costose e complesse con la soluzione low-touch di Cloudflare può ridurre i costi operativi, le funzionalità ridondanti e l'eccessiva messa a punto.

Blocca attacchi BEC sofisticati

50 miliardi di dollari di perdite segnalate e in crescita

Considerando che gli attacchi BEC sono responsabili di un'impressionante quantità di perdite nell'ultimo decennio, è sorprendente che alcune organizzazioni non abbiano ancora dato priorità alla lotta contro una forma così efficace di frode finanziaria. Sebbene gli attacchi BEC rappresentino una percentuale molto più piccola delle minacce di phishing, spesso non vengono rilevati dai SEG e dai provider di posta elettronica cloud, con conseguenti maggiori perdite finanziarie. Questi attacchi mirati sono difficili da catturare perché sfruttano account e contesti di conversazione impersonificati o compromessi, mascherandosi da dipendenti o fornitori fidati.

Estendere i principi Zero Trust alla posta elettronica

Sfruttando l'account e-mail di un dipendente o di un fornitore compromesso, gli autori degli attacchi possono eludere i tradizionali controlli di sicurezza che tentano solo di confermare la legittimità dell'account del mittente. Cloudflare fa un ulteriore passo avanti analizzando un'ampia gamma di attributi comportamentali, modelli di scrittura, indicatori di sentiment e cronologia delle conversazioni per determinare l'autenticità del mittente. I modelli di minaccia basati sul machine learning di Cloudflare e l'ampia intelligence di rete forniscono l'arma più efficace contro gli account compromessi utilizzati per estorcere pagamenti fraudolenti.

Figura 1: Analisi del messaggio

Rilevamento del BEC con analisi contestuale basata su ML

L'identificazione accurata degli attacchi BEC richiede molto più della semplice analisi strutturale di un messaggio. Un rilevamento efficace implica anche una comprensione granulare delle variazioni all'interno dello stile e dell'intento conversazionale. L'ampia telemetria di rete di Cloudflare (oltre 3 bilioni di richieste DNS giornaliere) e i modelli ML in evoluzione alimentano il motore di analisi a pattern ridotto che decostruisce ogni aspetto di un messaggio e-mail per valutare pattern di scrittura, sentiment, contesto storico e un'ampia gamma di altre variabili che contribuiscono a scoprire l'autenticità del mittente.

Isola gli attacchi basati su collegamenti

Gli attacchi basati sui link sono diventati il metodo preferito per sottrarre credenziali, caricare malware/ransomware ed estrarre informazioni sensibili. L'utilizzo combinato di e-mail, chat, SMS, social e altre app per distribuire questi collegamenti complica ulteriormente il processo di protezione dei dipendenti e dei dati dagli attacchi di phishing mirati.

Cloudflare risolve gli attacchi di phishing basati su collegamenti eseguendo il rendering di tutto il codice Web in remoto sulla nostra rete cloud globale anziché sul dispositivo locale dell'utente. In questo modo, si riduce il rischio di malware e minacce zero-day al browser, garantendo al contempo un controllo granulare sulle azioni dell'utente (ad esempio, la disabilitazione dell'input da tastiera) per impedire la raccolta di credenziali e le fughe di dati.

Elimina il rischio di phishing senza rallentare la forza lavoro

Grazie all'integrazione di funzionalità di Browser Isolation di nuova generazione basate sulla nostra esclusiva tecnologia Network Vector Rendering (NVR), Cloudflare è in grado di offrire una soluzione fluida, sicura e scalabile per l'isolamento di collegamenti potenzialmente dannosi. A differenza delle tecniche che richiedono molta larghezza di banda, l'NVR trasmette in streaming i comandi di progettazione sicuri al dispositivo, contribuendo a eliminare il rischio di contenuti Web dannosi senza compromettere l'esperienza dell'utente finale. Grazie all'NVR e alla rete a bassa latenza di Cloudflare, le organizzazioni possono isolare le minacce multicanale garantendo al contempo una produttività senza interruzioni per i propri dipendenti.

Indagine e risoluzione rapide

Gestione della sicurezza intuitiva e low-touch

Con una maggiore automazione e una configurazione minima necessaria per ottenere risultati ottimali, Cloudflare riduce significativamente il tempo e l'impegno necessari per la gestione continua della sicurezza della posta elettronica. I team di sicurezza possono ottenere immediatamente una visione completa di tutti i parametri e le tendenze principali all'interno della dashboard, con la possibilità di accedere a dettagli più granulari sui messaggi contrassegnati. L'analisi delle tendenze consente di scoprire rapidamente i tipi di attacchi frequenti, quali dirigenti vengono presi di mira, gli attacchi differiti mitigati e altri punti dati critici.

Tutte le analisi, la telemetria, gli elementi osservabili delle minacce e gli indicatori di compromissione (IOC) sono disponibili tramite un'API estesa per una facile integrazione nei flussi di lavoro degli analisti esistenti e negli strumenti di orchestrazione.

"Dico spesso ai colleghi come Cloudflare sia semplice e facile da usare come soluzione SaaS basata su cloud e discuto di quanto sono soddisfatto del suo elevato livello di precisione".

Japan Airlines

Rilevamento e risposta gestiti (PhishGuard)

Il servizio di sicurezza e-mail gestito di Cloudflare, PhishGuard, integra il tuo team SOC esistente per liberare i cicli di indagine sulla sicurezza e fornire intelligence delle minacce preziosa minacce. PhishGuard può aiutare a neutralizzare le campagne di phishing fornendo assistenza nelle indagini, nella valutazione delle minacce interne, nella rimozione attiva delle frodi e nelle complesse esigenze di riparazione. PhishGuard estende le risorse e le competenze in materia di sicurezza per segnalare attivamente potenziali frodi e minacce interne, effettuando al tempo stesso la caccia alle minacce basata su e-mail.

Caratteristiche e vantaggi di PhishGuard:

- Invii di phishing gestiti e risposta agli incidenti per una risoluzione più rapida.
- BEC proattivo e notifiche di frode in modo che le organizzazioni possano rispondere rapidamente nelle prime fasi del ciclo di vita dell'attacco.
- Risorse dedicate per il monitoraggio in tempo reale, revisioni periodiche degli account e valutazioni continue delle minacce.
- Firme di blocco personalizzate basate su un'analisi delle minacce dell'ambiente gestito.

Oltre 1.100

ore risparmiate ogni anno automatizzando le attività di triage manuale

La soluzione automatizzata di Cloudflare elimina le attività manuali che richiedono molto tempo, migliorando i tempi di risposta e sbloccando cicli aggiuntivi.

50%

di riduzione delle e-mail dannose o sospette consegnate (su M365)

L'integrazione di Cloudflare su Microsoft 365 consente alle organizzazioni di intercettare attacchi mirati e ridurre il numero complessivo di e-mail dannose.

40

ore totali trascorse in sette anni sulla configurazione della sicurezza della posta elettronica

La sicurezza e-mail low-touch di Cloudflare richiede poca configurazione iniziale e messa a punto continua, fornendo immediatamente un'elevata efficacia di rilevamento.

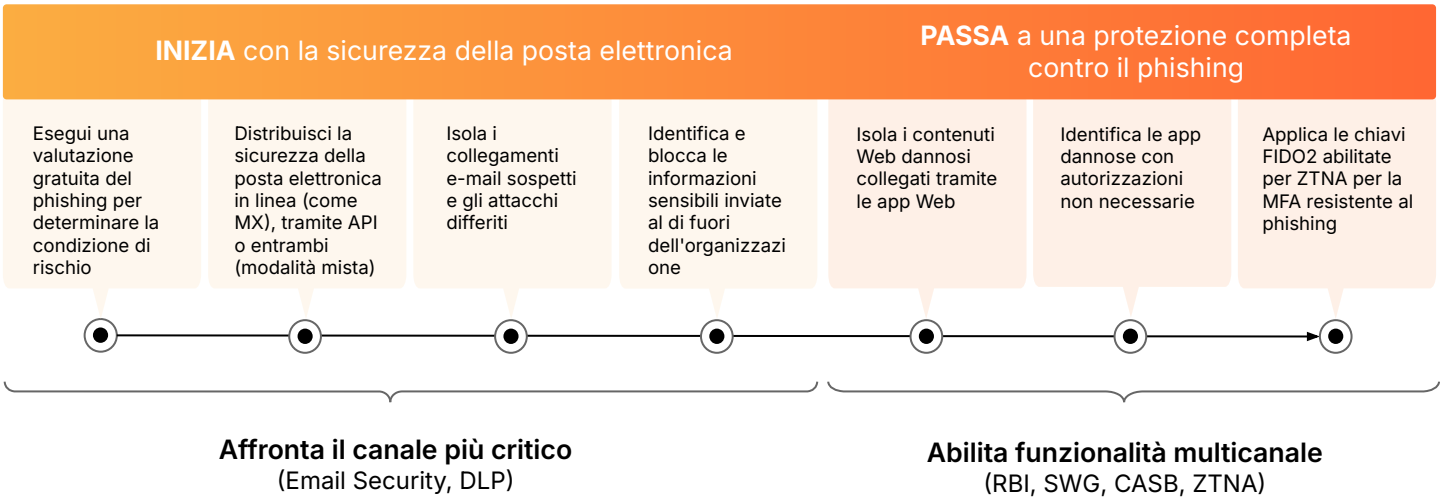
VANTAGGI

Protezione multicanale completa

Poiché le campagne di phishing si stanno rapidamente diffondendo oltre la posta elettronica, ora è più urgente che mai per le organizzazioni implementare una soluzione di phishing che fornisca un percorso semplice e rapido verso una protezione multicanale completa.

Con la piattaforma di sicurezza unificata di Cloudflare, le organizzazioni possono finalmente distribuire la sicurezza della posta elettronica leader del settore per affrontare rapidamente il canale di phishing più critico, quindi abilitare facilmente i servizi Zero Trust per estendere la protezione a tutti i canali, bloccando efficacemente le minacce di phishing note ed emergenti.

- **Protezione low-touch estremamente efficace:** riduci al minimo il rischio di phishing con un'efficacia di rilevamento leader del settore che richiede una messa a punto minima.
- **Maggiore consolidamento, costi inferiori:** riduci la spesa con un'unica piattaforma completamente integrata che risolve tutti i casi d'uso del phishing.
- **Rapida da implementare, facile da gestire:** garantisci una protezione immediata riducendo al contempo il tempo e gli sforzi necessari per la gestione continuativa.



Valuta e confronta

Valuta le tue attuali difese e-mail e scopri quali minacce vengono ignorate

Esegui una scansione retrospettiva gratuita in pochi minuti per scoprire quali minacce di phishing sono sfuggite negli ultimi 14 giorni oppure richiedi una valutazione del rischio di phishing (PRA, Phishing Risk Assessment) per monitorare le caselle di posta in arrivo alla ricerca di messaggi di phishing non appena vengono recapitati. Confronta le opzioni di altri fornitori senza alcuna messa a punto immediata per scoprire quale soluzione di sicurezza della posta elettronica offre la protezione più rapida e semplice.

Esegui una scansione retrospettiva | Richiedi una PRA

1. Ricerca Deloitte 2020: Fonte
2. 2023 FBI IC3 PSA: Fonte
3. Istantanea di 2023 Forrester Opportunity: Fonte

