

Proofpoint Email Fraud Defense

VANTAGGI PRINCIPALI

- Semplificazione dell'implementazione di DMARC grazie al supporto in ogni fase del processo
- Protezione del tuo marchio in caso di email fraudolente senza bloccare i messaggi legittimi
- Identificazione automatica dei fornitori e dei rischi associati
- Visibilità sui domini cugini e sulle email inviate tramite i tuoi domini approvati
- Integrazione con l'avanzato gateway di Proofpoint per un'autenticazione DMARC flessibile e sicura

Proofpoint Email Fraud Defense ottimizza l'implementazione dell'autenticazione DMARC grazie a un flusso di lavoro guidato e al supporto di consulenti dedicati. La soluzione protegge la reputazione della tua azienda dalle frodi via email. Inoltre, fornisce piena visibilità su domini cugini e messaggi inviati tramite il tuo dominio, inclusi i mittenti di terze parti. Email Fraud Defense permette anche di mitigare i rischi posti dai fornitori identificando automaticamente i tuoi fornitori e i domini cugini registrati da terzi.

Dal 2016, numerose aziende di ogni dimensione e settore hanno perso più di 26 miliardi di dollari a causa di frodi via email. I criminali informatici utilizzano una varietà di tattiche di furto dell'identità, come lo spoofing dei domini e i domini cugini, per invogliare le loro vittime a effettuare bonifici bancari fraudolenti. E tra i vari tipi di truffe via email, le frodi delle fatture dei fornitori comportano spesso le perdite finanziarie più cospicue, dato l'elevato volume di pagamenti effettuati tra le aziende.

L'implementazione dell'autenticazione dell'email aiuta a proteggere contro le minacce fraudolente. Tuttavia, l'implementazione di DMARC (Domain-based Message Authentication, Reporting and Conformance) può rivelarsi un processo lungo e complesso. Inoltre, c'è il rischio di bloccare il flusso delle email legittime.

Email Fraud Defense semplifica l'implementazione DMARC fornendo supporto per l'intera durata del processo. Autenticiamo tutte le email inviate da o verso la tua azienda senza bloccare le email legittime. Proteggiamo il tuo marchio dalle frodi via email e limitiamo i rischi posti dalle minacce fraudolente in entrata. Email Fraud Defense ti permette di proteggere meglio i tuoi clienti, partner commerciali e i tuoi dipendenti dagli attacchi di violazione dell'email aziendale (BEC, Business Email Compromise) e di riconquistare la loro fiducia nell'affidabilità delle tue comunicazioni.

Facilità d'uso

Consulenti dedicati e un flusso di lavoro guidato

In qualità di cliente di Email Fraud Defense, hai a disposizione una soluzione all'avanguardia e un'assistenza di prim'ordine. Fin dal primo giorno, creiamo per te un progetto con un flusso di lavoro guidato. I nostri consulenti, spesso elogiati per le loro elevate valutazioni NPS (Net Promoter Score)¹, sono a tua disposizione per aiutarti in ogni fase dell'implementazione.

In collaborazione con il tuo team, identifichiamo tutti i mittenti legittimi, comprese le terze parti, per garantire una corretta autenticazione. I nostri consulenti ti offrono delle raccomandazioni per aiutarti ad assegnare le priorità alle attività in base alle tue esigenze e ai criteri della tua azienda, come il volume dei messaggi e i principali mittenti, analizzando la specificità del tuo ambiente email. Grazie al nostro collaudato piano di implementazione, puoi distribuire il sistema di autenticazione dell'email su larga scala senza problemi. Inoltre, puoi ottenere più rapidamente valore dal tuo investimento nella soluzione Proofpoint.

¹ NPS è l'indice di riferimento per misurare la soddisfazione e la fedeltà dei clienti. Sulla base di dati di riferimento a livello mondiale, il punteggio medio NPS equivale a +32. I consulenti di Proofpoint Email Fraud Defense ottengono un punteggio NPS di +90.

SPF hosted

Email Fraud Defense include il servizio SPF hosted che ti consente di aggirare il tradizionale limite della ricerca SPF (pari a 10) e di ridurre il carico di lavoro tipicamente associato alla modifica dei record SPF. Invece del consueto ritardo di 72 ore, il servizio SPF hosted assicura l'aggiornamento dei record in tempo reale. Anche la sicurezza SPF viene migliorata, poiché i criminali informatici non sono più in grado di utilizzare i tuoi record SPF disponibili pubblicamente per abusare del tuo dominio.

Protezione completa del marchio

Lo spoofing delle email e i domini cugini sono due tattiche comuni degli attacchi BEC. I criminali informatici sfruttano il marchio di un'azienda per rubare denaro o informazioni sensibili alle vittime. Email Fraud Defense impedisce l'invio di email fraudolente tramite i tuoi domini approvati. Proteggiamo il tuo marchio e la reputazione della tua azienda dalle frodi via email.

Identificazione dei domini simili al tuo

Sfruttando le informazioni di Proofpoint Domain Discover, Email Fraud Defense identifica automaticamente i domini simili al tuo. Rileviamo dinamicamente i nuovi domini registrati che abusano dell'identità del tuo marchio, che si tratti di attacchi email o siti web di phishing. Analizziamo milioni di domini e correliamo i dati di registrazione con i nostri dati sugli scambi via email e sugli attacchi attivi. In questo modo forniamo una visibilità completa sui domini sospetti. Ti mostriamo come i criminali informatici abusano del tuo marchio. Ricevi avvisi immediati quando i domini sospetti precedentemente dormienti diventano attivi.

Con il modulo aggiuntivo Virtual Takedown, puoi ridurre rapidamente l'esposizione dei consumatori, dei partner commerciali e dei dipendenti a domini cugini dannosi. Inoltre, puoi richiedere la cancellazione del dominio al Registro dei domini o al fornitore del servizio di hosting. Puoi anche esportare i domini da bloccare a livello del gateway di posta di Proofpoint.

Visibilità a 360° sull'intero ecosistema email

Email Fraud Defense ti offre una visibilità senza pari su tutte le email inviate attraverso i tuoi domini approvati, compresi quelli per le caselle email dei consumatori, i gateway delle aziende e il tuo. Nessun altro strumento di sicurezza o fonte di dati pubblici è in grado di offrire un tale livello di visibilità.

La nostra dashboard completa fornisce le seguenti informazioni:

- Domini della tua azienda che i criminali informatici hanno cercato di violare
- Tasso di abuso di ogni dominio
- Le tue policy e le percentuali di successo dell'autenticazione DMARC, SPF e DKIM
- Mittenti autorizzati e i loro record DMARC

A differenza di altre soluzioni le cui dashboard mostrano solo numeri, Email Fraud Defense ti offre informazioni fruibili e raccomandazioni. Puoi così beneficiare di una tracciabilità e di una gestione migliorate e puoi gestire le attività aperte. Con Email Fraud Defense, non dovrai più preoccuparti di non riuscire a implementare DMARC o di bloccare il traffico email legittimo, pur avendo la certezza che nessun criminale informatico potrà abusare dei tuoi domini.

Visibilità sui rischi associati ai fornitori

Email Fraud Defense va oltre l'implementazione di DMARC per offrirti visibilità sui rischi posti dai tuoi fornitori. La funzione Nexus Supplier Risk Explorer identifica automaticamente i tuoi fornitori, convalida i loro record DMARC e determina i rischi che rappresentano per la tua azienda, in termini di minacce fraudolente, phishing, malware e spam. Indichiamo il volume dei messaggi e i messaggi consegnati da domini cugini di quelli dei tuoi fornitori. Inoltre, è possibile indagare ulteriormente su qualsiasi potenziale minaccia. Dando priorità al livello di rischio del dominio di ogni fornitore, ti aiutiamo a concentrarti sugli incidenti più critici.

Stretta integrazione con il gateway di posta di Proofpoint

Proofpoint è l'unico fornitore di sicurezza ad offrire una reale integrazione tra l'autenticazione dell'email e un gateway di posta sicuro. Quando la soluzione Email Fraud Defense è associata all'avanzato gateway di posta di Proofpoint, puoi ridurre efficacemente il rischio di minacce fraudolente applicando DMARC al traffico in entrata in modo sicuro e flessibile. Ti aiutiamo a verificare la reputazione DMARC di un dominio specifico, in modo che il tuo gateway non blocchi i messaggi legittimi che non superano l'autenticazione DMARC per qualsiasi motivo. Inoltre ti aiutiamo a creare policy di override per le email legittime senza mettere a repentaglio la tua sicurezza. Insieme, ci assicuriamo che i tuoi dipendenti siano meglio protetti dalle frodi via email.

APPROFONDISCI

Per maggiori informazioni, visita proofpoint.com/it/products/email-fraud-defense.

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: www.proofpoint.com/it.

©Proofpoint, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.