Proofpoint Email Fraud Defense

Vantaggi principali

- Semplificazione dell'implementazione di DMARC grazie al supporto in ogni fase del processo
- Protezione del tuo marchio evitando contro le frodi via email, senza bloccare i messaggi legittimi
- Identificazione automatica dei fornitori e dei rischi a loro associati
- Visibilità su tutte le email inviate utilizzando i tuoi domini di fiducia e domini fotocopia
- Hosting affidabile dei record SPF, DKIM e DMARC grazie ai servizi di autenticazione in hosting di Proofpoint
- Integrazione con l'avanzato gateway email di Proofpoint per un'autenticazione DMARC flessibile e sicura
- Visualizzazione dei tassi di successo DMARC per i domini dell'azienda gestiti nell'ambiente Microsoft 365

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a mitigare le quattro principali categorie di rischi legati agli utenti.

Proofpoint Email Fraud Defense ottimizza l'implementazione dell'autenticazione DMARC grazie a flussi di lavoro guidati e al supporto di consulenti esperti. La soluzione protegge la reputazione della tua azienda dalle frodi via email. Permette di visualizzare le fonti delle email inviate tramite i tuoi domini e domini fotocopia. Limita anche i rischi legati ai fornitori identificando i tuoi fornitori e i domini fotocopia registrati da terze parti.

Proofpoint Email Fraud Defense ti guida nell'intero processo di implementazione di DMARC. La soluzione ti aiuta a proteggere i tuoi clienti, partner commerciali e collaboratori dalle truffe di violazione dell'email aziendale (BEC, Business Email Compromise). Con Email Fraud Defense, Proofpoint protegge il tuo marchio impedendo che venga sfruttato in frodi via email e riduce i rischi di impostori nel traffico in entrata. Autentichiamo anche tutte le email inviate da o verso la tua azienda, senza bloccare le email legittime.

Facilità d'uso

Consulenti dedicati e consigli degli esperti

Per aiutarti a configurare l'autenticazione delle email, Proofpoint crea un piano del progetto per tuo conto. Il piano include flussi di lavoro guidati che semplificano il processo di configurazione. I nostri consulenti ti assisteranno in ogni fase di implementazione del piano. In collaborazione con i tuoi team, identifichiamo tutti i mittenti legittimi, comprese le terze parti e le applicazioni Shadow IT, per assicurare una corretta autenticazione. Analizziamo anche il tuo ambiente email per aiutarti ad assegnare le priorità alle attività in base alle esigenze specifiche della tua azienda, come il volume dei messaggi e i principali mittenti.

Servizi di autenticazione in hosting

Proofpoint Email Fraud Defense include i servizi SPF in hosting, DKIM in hosting e DMARC in hosting di Proofpoint. Questi servizi in hosting ti aiutano a configurare e gestire le regole per le policy SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) e DMARC. Distribuiti a livello geografico e fault-tolerant, questi servizi garantiscono l'affidabilità.

SPF in hosting

- Superamento dei limiti della ricerca DNS (10) imposti da SPF
- Riduzione del carico di lavoro associato alla modifica dei record SPF
- Aggiornamento dei record in tempo reale, con validazione della sintassi
- Rafforzamento della sicurezza SPF tramite l'offuscamento dell'infrastruttura di invio
- Semplificazione della gestione di invii in blocco da diversi domini che utilizzano la stessa infrastruttura di invio

DKIM in hosting

- Semplificazione della configurazione e della gestione dei selettori e delle chiavi DKIM
- Opzioni flessibili di hosting per i selettori DKIM (delegati o non)
- Supporto del protocollo DNSSEC (DNS Security Extensions)
- Semplice importazione dei selettori e delle chiavi pubbliche DKIM

DMARC in hosting

- Configurazione e gestione semplificata dei record DMARC per i tuoi domini
- Supporto del protocollo DNSSEC
- Semplice importazione dei record DMARC esistenti

Protezione completa del marchio

Per proteggere il tuo marchio, Proofpoint Email Fraud Defense blocca l'invio di email fraudolente tramite i tuoi domini approvati.

Identificazione dei domini fotocopia

Proofpoint Email Fraud Defense utilizza le informazioni di registrazione di Proofpoint Domain Discover. La soluzione rileva i domini che abusano dell'identità del tuo marchio, che si tratti di attacchi email o siti web di phishing. Proofpoint analizza milioni di domini e correla i dati di registrazione con i suoi dati sugli scambi via email e sugli attacchi. La soluzione mostra i domini sospetti e come i criminali informatici abusano del tuo marchio. Invia anche degli avvisi quando i domini sospetti diventano attivi.

Il componente aggiuntivo Proofpoint Takedown riduce l'esposizione dei tuoi consumatori, partner commerciali e collaboratori ai domini fotocopia. Puoi richiedere la rimozione di un dominio dannoso al registrar del dominio, alla rete di distribuzione dei contenuti o (CDN) o al fornitore dei servizi email. Puoi anche esportare i domini da bloccare a livello del gateway di posta di Proofpoint.

Visibilità a 360° sull'intero ecosistema email

Proofpoint Email Fraud Defense mostra tutte le email inviate tramite i tuoi domini approvati, comprese le email inviate alle caselle email dei consumatori, ai gateway delle aziende e al tuo gateway.

La nostra dashboard mostra i domini della tua azienda che i criminali informatici hanno cercato di violare e il tasso di abuso per ciascun dominio. Mostra i mittenti autorizzati e i loro record DMARC, nonché le tue policy e i tassi di successo per SPF, DKIM e DMARC.

Proofpoint Email Fraud Defense ti offre informazioni fruibili e suggerimenti. Non devi così preoccuparti di fallire nell'autenticazione DMARC né di bloccare traffico legittimo, neutralizzando i criminali informatici.

Visibilità sui rischi associati ai fornitori

Proofpoint Email Fraud Defense va oltre di DMARC per offrirti visibilità anche sui rischi posti dai tuoi fornitori. Il modulo Nexus Supplier Risk Explorer identifica i tuoi fornitori, verifica i loro record DMARC e mostra i rischi associati. La soluzione mostra i messaggi recapitati da domini fotocopia. Dando priorità agli avvisi in base ai livelli di rischio, ti aiutiamo a concentrarti sugli incidenti più gravi.

Integrazione con il gateway email di Proofpoint

Proofpoint Email Fraud Defense opera di concerto con il gateway email Proofpoint per applicare l'autenticazione DMARC sui messaggi in entrata. La soluzione ti aiuta a verificare la reputazione DMARC di un dominio, in modo che il tuo gateway non blocchi i messaggi legittimi che non superano l'autenticazione DMARC. Inoltre ti aiuta a creare policy di override per le email legittime senza indebolire la tua sicurezza.

Visibilità DMARC per Microsoft 365

Se utilizzi Microsoft 365 con i tuoi record MX (Mail eXchange) che puntano verso i server in ingresso di Microsoft, Proofpoint Email Fraud Defense può comunque mostrare la conformità dei tuoi domini a DMARC. Questa visibilità ti aiuta ad applicare DMARC sul traffico in entrata dai tuoi domini con fiducia.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il nostro sito all'indirizzo **proofpoint.com/it**.