

Proofpoint Impersonation Protection

Proteggi le tue comunicazioni con partner,
clienti e fornitori di fiducia



Vantaggi principali

- **Protezione delle tue comunicazioni aziendali dalle minacce di furto d'identità**
- **Prevenzione del furto della tua identità o di quella del tuo marchio**
- **Monitoraggio di domini fotocopia dannosi e loro smantellamento**
- **Rilevamento e protezione contro i fornitori a rischio, inclusi gli account di fornitori compromessi**
- **Proteggi le email inviate per tuo conto da applicazioni, dispositivi, piattaforme SaaS e agenti di IA**
- **Basato su Nexus[®] AI, machine learning, LLM e analisi comportamentale**

La maggior parte delle aziende si affida all'email come vettore di comunicazione principale.

Tuttavia gli aggressori hanno capito come dirottare i fidati mezzi di comunicazione delle aziende, mentre l'IA generativa ha reso questi attacchi più rapidi, più convincenti e più facili da scalare. Possono impersonare un'impresa, il suo marchio o i suoi partner commerciali per creare messaggi e siti web credibili in pochi minuti anziché in ore.

Secondo il Centro Segnalazioni Reati di Internet dell'FBI, la violazione dell'email aziendale (BEC) genera costantemente miliardi di dollari di perdite, che continuano ad aumentare di anno in anno. L'FBI ha inoltre iniziato a monitorare l'IA come un fattore di minaccia distinto, attribuendo decine di milioni di dollari di perdite BEC specificamente ad attacchi con una componente IA confermata. Avverte che questa cifra è probabilmente sottostimata rispetto al reale.

Gli attacchi combinano spesso molteplici tattiche di furto d'identità, inclusi domini contraffatti, domini fotocopia e account di fornitori compromessi. Insieme mettono a rischio le comunicazioni con partner, clienti e fornitori di fiducia, rendendo più difficile per i destinatari distinguere i messaggi legittimi da quelli fraudolenti.

Proofpoint adotta un approccio globale e multilivello per proteggere la tua azienda e il tuo marchio dal furto d'identità. Forniamo gli strumenti, la tecnologia e le risorse per autenticare le email generate dagli utenti e dalle applicazioni, per proteggere i messaggi inviati per tuo conto, per identificare account di fornitori rischiosi o potenzialmente compromessi e per monitorare i dannosi domini fotocopia in modo che possano essere rimossi.

Proteggi il tuo marchio dal furto d'identità

Una delle tattiche di furto d'identità più comuni è il domain spoofing. L'IA generativa ha velocizzato la produzione di messaggi contraffatti e reso più difficile distinguerli da quelli autentici. Senza i giusti controlli di sicurezza, i criminali informatici possono facilmente rubare i tuoi domini di fiducia e utilizzare l'IA per creare messaggi altamente convincenti su larga scala. Ciò consente loro di colpire i tuoi clienti, partner e persino i tuoi collaboratori con un livello di velocità e perfezione che fino a un anno fa non esisteva. L'autenticazione delle email è il modo più efficace per bloccarli.

Proofpoint Impersonation Protection semplifica l'implementazione di DMARC, guidandoti attraverso ogni fase, e consente l'autenticazione sia delle email degli utenti che di quelle delle applicazioni. I nostri esperti lavoreranno insieme a te per identificare i tuoi mittenti legittimi. Assicureranno inoltre che tutte le tue email, incluse quelle inviate da mittenti terzi autorizzati, siano debitamente autenticate.

L'integrazione con Proofpoint Threat Protection ti permette di applicare l'autenticazione DMARC per i messaggi in entrata con la massima fiducia. Aggiunge un livello di difesa contro i tentativi di furto d'identità generati dall'IA che falsificano i tuoi domini di fiducia. Ti permette inoltre di derogare alle policy DMARC senza bloccare le email legittime o compromettere la sicurezza con delle liste di autorizzazione. Quest'integrazione ti offre visibilità sul traffico email in entrata che in uscita. Puoi visualizzare tutte le email inviate che utilizzano i tuoi domini di fiducia, incluse quelle spedite da terze parti e, sempre più spesso, da agenti di IA che agiscono per tuo conto.

Proteggiti dagli account di fornitori compromessi

I criminali informatici stanno sfruttando sempre più la supply chain per compromettere le comunicazioni aziendali di fiducia. Spesso utilizzano account di fornitori compromessi per dirottare i thread di email tra di te e i tuoi partner commerciali. L'IA generativa li aiuta a studiare le conversazioni precedenti e a imitare lo stile di scrittura di un fornitore, rendendo i messaggi fraudolenti più difficili da rilevare. E poiché queste email possono provenire da account legittimi senza contenere alcuna carica virale, possono eludere i tradizionali controlli di autenticazione e rilevamento. Il risultato è una significativa perdita economica, il furto dei dati, l'estorsione o il ransomware.

Proofpoint Impersonation Protection ti consente di individuare e contrastare i fornitori a rischio, inclusi gli account potenzialmente compromessi. Utilizza l'IA comportamentale, il machine learning e la threat intelligence provenienti dall'ampia base di clienti di Proofpoint per individuare i segni di compromissione dei fornitori, inclusi gli attacchi in cui l'IA generativa viene impiegata per creare inganni più convincenti. I controlli adattivi, come l'isolamento automatico degli URL, riducono l'esposizione alle minacce provenienti dai mittenti compromessi. L'integrazione con Proofpoint Threat Protection, insieme al contesto sulle relazioni tra mittente e destinatario, aiuta a semplificare la risposta agli incidenti e le indagini condotte da terze parti.

Rileva e rimuovi i siti web dannosi, inclusi i sitgi fotocopia.

I criminali informatici creano siti web appositamente progettati per gli attacchi. Alcuni impersonano altre aziende, marchi o istituzioni per indurre i tuoi dipendenti, clienti o partner a fidarsi. Altri imitano la tua azienda, utilizzando domini e pagine che rispecchiano fedelmente il tuo logo, il layout e l'esperienza del tuo marchio. L'IA generativa ha reso entrambi i tipi di attacchi più facili da produrre, più difficili da individuare e più veloci da scalare. I malintenzionati utilizzano tali siti nel phishing delle credenziali, nel BEC, negli attacchi tramite telefonata (TOAD, Telephone-Oriented Attack Delivery) e in altri schemi che si basano su una presenza digitale convincente.

Con Proofpoint Impersonation Protection monitoriamo continuamente i domini appena registrati che potrebbero impersonare la tua azienda e forniamo il contesto necessario per valutare il rischio potenziale.

Il rilevamento è solo il primo passo. Quando invii un sito sospetto al nostro Takedown Team lo indaghiamo, raccogliamo le prove disponibili e interveniamo per mitigare l'attività dannosa e rimuovere il sito. Manteniamo relazioni in un'ampia rete di fornitori di infrastrutture internet e di partner affidabili, inclusi registrar, fornitori di hosting, fornitori di servizi di posta elettronica, partner della lista di blocco e altri ancora.

I nostri addetti gestiscono il processo di rimozione per tuo conto, così non devi decidere chi contattare o quale documentazione sia necessaria. I nostri servizi di rimozione si estendono oltre i domini fotocopia per supportare la mitigazione di sottodomini e URL dannosi, nonché dei domini non fotocopia.

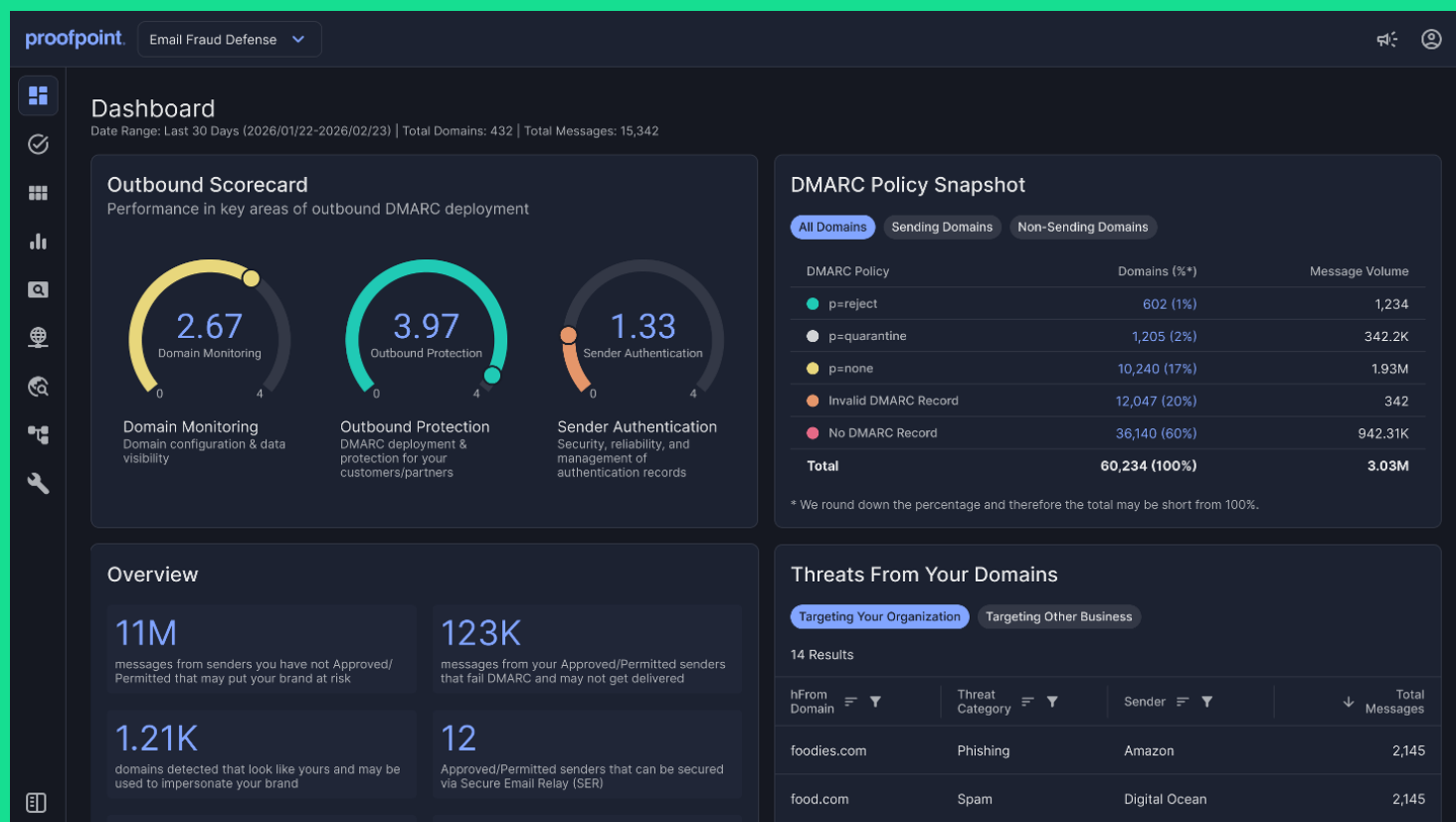


Figura 1. Proofpoint offre visibilità sulle minacce di domain spoofing, sugli ostili domini fotocopia dei tuoi domini e sulle email inviate utilizzando i tuoi domini di fiducia.

Email sicure inviate per tuo conto

Non tutte le email che lasciano il tuo dominio provengono da una persona che scrive un messaggio. Le piattaforme per le risorse umane inviano avvisi sulle buste paga, gli strumenti di relazione con la clientela spediscono ricevute ai clienti, i dispositivi d'ufficio mandano notifiche di scansione via email e fax e anche gli agenti IA stanno iniziando a generare messaggi per tuo conto. Ogni fonte può prestarsi ad abusi. Se un'applicazione, un dispositivo o un servizio di invio viene compromesso, i criminali informatici utilizzano quel canale fidato per inviare email dannose che sembrano provenire da te, superano i controlli di autenticazione. Se poi vengono migliorate con l'IA generativa, appaiono più convincenti che mai.

Proofpoint Impersonation Protection colma questa lacuna con un relay sicuro e dedicato per i mittenti automatizzati che usano i tuoi domini: dalle applicazioni interne ai dispositivi da ufficio, dalle piattaforme SaaS agli agenti di IA. Accetta la posta solo da fonti verificate e autenticate, applica una scansione antispam e antivirus avanzata a ogni messaggio e firma con DKIM la posta autorizzata. Questo aiuta le fonti in uscita a supportare l'allineamento al DMARC e la conformità SPF senza interrompere il flusso di posta legittima. Proofpoint SER isola inoltre questo traffico dietro IP dedicati e affidabili, contribuendo a proteggere l'infrastruttura di invio e la reputazione del marchio dai criminali informatici che potrebbero altrimenti sfruttare la fiducia nel tuo dominio.

Ottieni visibilità, controllo e supporto alla conformità

Proofpoint Impersonation Protection centralizza visibilità e controllo sui servizi di invio ad alto volume, come Amazon SES. Puoi vedere cosa esce in massa dal tuo dominio e risalire all'applicazione, al dispositivo o all'agente di IA che ha inviato tali messaggi. La crittografia opzionale e la prevenzione della perdita di dati aiutano a salvaguardare i dati sensibili, incluse le informazioni di identificazione personale e le informazioni di identificazione sanitaria, nei messaggi transazionali. Questi controlli supportano la conformità a quadri e normative come i requisiti HIPAA, SEC e FINRA.

Proofpoint Impersonation Protection ti aiuta inoltre a soddisfare i principali requisiti del fornitore di posta elettronica riguardanti l'identità dei mittenti e l'integrità dei messaggi per i mittenti di massa. Grazie al supporto per le intestazioni di cancellazione dell'iscrizione e alla gestione centralizzata delle liste, aiuta i messaggi legittimi a raggiungere la casella email.

Per saperne di più

Per maggiori informazioni, visita il nostro sito all'indirizzo [proofpoint.com/it](https://www.proofpoint.com/it).



Informazioni su Proofpoint, Inc. Proofpoint, Inc. è un'azienda leader globale nella cybersecurity incentrata sulle persone e sugli agenti, che protegge il modo in cui persone, dati e agenti IA si connettono tramite email, cloud e strumenti di collaborazione. Proofpoint è il partner di fiducia di oltre 80 aziende della classifica Fortune 100, oltre 10.000 grandi imprese e milioni di aziende più piccole, per contrastare le minacce, prevenire la perdita di dati e rafforzare la resilienza di persone e processi di IA. La piattaforma di collaborazione e sicurezza dei dati di Proofpoint aiuta aziende di tutte le dimensioni a proteggere e responsabilizzare i propri collaboratori in modo che possano adottare l'IA in modo sicuro e con fiducia. Per saperne di più, visita www.proofpoint.com/it.

Seguici: [LinkedIn](#)

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