Proofpoint Secure Email Relay

Soluzione ottimizzata per controllare e proteggere le email transazionali provenienti da applicazioni e partner SaaS

Vantaggi principali

- Protezione delle email transazionali provenienti dalle applicazioni interne e dai fornitori SaaS come Salesforce, ServiceNow e Workday
- Accelerazione dell'implementazione DMARC grazie alla firma DKIM delle email di tutte le fonti prima dell'invio
- Protezione del tuo dominio di fiducia dall'abuso da parte di mittenti compromessi e di fornitori di servizi email vulnerabili i cui indirizzi IP appaiono nei tuoi record SPF
- Protezione dei dati sensibili nelle email inviate dalle vostre applicazioni, come i dati personali e i dati sanitari personali, grazie alla crittografia del payload e alla prevenzione della perdita dei dati (DLP)
- Sostituzione dei relay on premise con un'alternativa sicura basata sul cloud
- Prevenzione dell'interruzione dell'email degli utenti isolandola dalla tua applicazione email

Proofpoint Secure Email Relay (SER) consolida e protegge le email transazionali. Impedisce a mittenti di terze parti compromessi di inviare email dannose utilizzando i tuoi domini e ti aiuta a garantire la conformità DMARC grazie alla firma DKIM. Come soluzione in hosting, Proofpoint SER ti aiuta a raggiungere i tuoi obiettivi di migrazione al cloud.

La migrazione delle applicazioni dai sistemi on premise verso il cloud può ampliare la superficie d'attacco della tua azienda. Le email inviate a tuo nome possono provenire da mittenti che utilizzano applicazioni di terze parti sulle quali tu non hai alcun controllo, facilitando lo spoofing dell'identità. Senza controlli adeguati, i criminali informatici possono facilmente rubare l'identità della tua azienda e poi sfruttare gli ambienti cloud dei mittenti autorizzati. L'invio di email dannose autorizzate a tuo nome diventa quindi semplicissimo. Questi messaggi non vengono rilevati dai protocolli SPF/DKIM/DMARC. Possono essere inviati direttamente ai tuoi clienti, partner e dipendenti.

Proofpoint SER applica i nostri controlli di sicurezza e conformità alle email transazionali che utilizzano la tua identità. Questi tipi di messaggi provengono da applicazioni interne o da partner SaaS di terze parti come Salesforce, ServiceNow e Workday. Includono fatture, codici di autenticazione, conferme, ecc. Possono essere isolati dalle email inviate dagli utenti, ma Proofpoint SER offre loro gli stessi livelli di protezione.

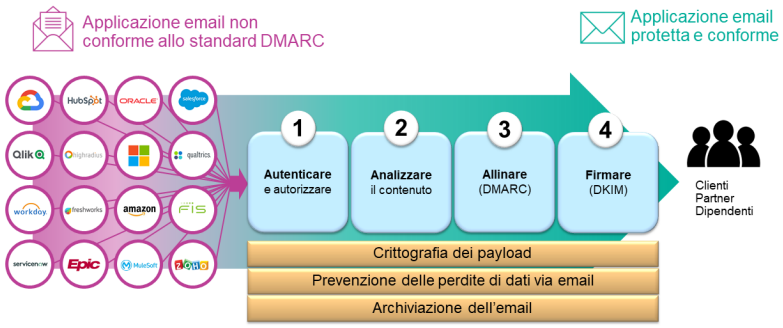

Figura 1. Proofpoint Secure Email Relay protegge le applicazioni cloud che inviano email transazionali a tuo nome e ti permette di applicare controlli di sicurezza (per esempio, crittografia e prevenzione della perdita di dati) alla tua applicazione email.

Altri esempi di email transazionali:

- Notifiche di dichiarazione
- Notifiche di consegna pacchi
- Conferme d'ordine
- Ricevute elettroniche
- Preventivi assicurativi
- Richieste di esperienze o commenti
- Notifiche di attività
- Allarmi IoT o del dispositivo
- Gestione di allarmi/urgenze

Proofpoint SER facilita l'applicazione del protocollo DMARC grazie alla firma DKIM di tutte le email. Analizza le email con una tecnologia antispam/antivirus e protegge i dati sensibili grazie alla crittografia dei payload e alla prevenzione della fuga di dati. Proofpoint SER ti permette di mantenere il controllo dell'identità delle tue email. I tuoi clienti, partner e dipendenti sono certi di ricevere da parte tua solo email autentiche.

Protezione dell'email in ambienti vulnerabili

Le applicazioni email e i fornitori di servizi email possono essere autorizzati a inviare email utilizzando i tuoi domini ma spesso non seguono le best practice di sicurezza. Ti espongono alla violazione dell'account o all'abuso della piattaforma. In entrambi i casi, i criminali informatici possono utilizzare i tuoi domini di fiducia per inviare email dannose che non vengono rilevate dai protocolli di autenticazione.

Proofpoint SER adotta un sistema chiuso nel quale solo le entità commerciali verificate sono autorizzate a utilizzare il nostro servizio di relay dell'email. Gli utenti casuali non possono iscriversi ad account gratuiti sulla nostra piattaforma. Questo permette di ridurre notevolmente il rischio di fornitori di servizi email vulnerabili o compromessi.

Proofpoint SER accetta anche in modo sicuro le email provenienti da applicazioni autorizzate tramite l'autenticazione SMTP e TLS (STARTTLS). Applica le misure antispam e antivirus di Proofpoint a ogni messaggio. Proofpoint SER blocca qualsiasi applicazione email, autorizzata ma compromessa, che cerca di inviare un'email dannosa a tuo nome. Puoi anche proteggere la tua applicazione email con indirizzi IP affidabili. Questi confonderanno i criminali informatici che inviano email utilizzando la tua identità.

Accelerazione dell'implementazione DMARC

Alcune applicazioni e alcuni fornitori SaaS non supportano la firma DKIM. Puoi avere il protocollo DMARC a singolo passaggio basato solo su SPF, ma senza protocollo DKIM le tue email legittime non disporranno dell'autenticazione ridondante richiesta. Non sarai in grado di proteggerti dalle regole di inoltro, per esempio. Proofpoint SER garantisce la conformità DMARC di queste email transazionali grazie alla firma DKIM dei messaggi prima del loro invio. Questo ti permette di attivare più rapidamente policy di rifiuto DMARC sui tuoi domini per impedire ai criminali informatici di effettuarne lo spoofing.

Rispetto della conformità normativa delle applicazioni email

Le aziende stanno migrando verso il cloud e spesso dispongono solo di opzioni per l'email mediocri in termini di conformità alle normative. Alcune instradano le email tramite sistemi on premise esponendosi ad ambienti esterni vulnerabili. Altre mettono insieme soluzioni isolate nel cloud. Ma generalmente non hanno una visione consolidata delle loro attività.

Proofpoint SER ti permette di rispettare gli standard di conformità normativa per la tua applicazione email. Le email provenienti da applicazioni che accedono ai dati personali e ai dati sanitari personali possono utilizzare una connessione crittografata o un payload crittografato. Proofpoint SER permette anche di applicare soluzioni di prevenzione della perdita dei dati (DLP) e di archiviazione alla tua applicazione email al fine di garantire la conformità alle normative della SEC/FINRA.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita la pagina **proofpoint.com/it**.