Proofpoint Advanced Email Security

Contrasta le minacce avanzate veicolate tramite email, semplifica le operazioni e ottieni una visibilità fruibile sui rischi legati agli utenti e sul tuo panorama delle minacce

Prodotti

- Proofpoint Email Protection
- Proofpoint TAP
- Proofpoint TRAP
- Proofpoint Email Isolation
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Email Fraud Defense
- Proofpoint Internal Mail Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

Vantaggi principali

- Blocco dei tentativi di frode via email e dei messaggi che contengono URL pericolosi, allegati dannosi e ransomware
- Neutralizzazione automatica dei messaggi segnalati dagli utenti o attivati dopo la consegna grazie a flussi di lavoro integrati
- Visibilità ineguagliata sui tuoi dipendenti, sulle minacce e sui rischi legati al cloud e ai fornitori
- Semplice implementazione delle policy DMARC e applicazione rapida e sicura per bloccare le email fraudolente che imitano domini autorizzati
- Formazione e responsabilizzazione dei tuoi utenti per trasformarli in una solida linea di difesa contro le minacce informatiche

L'email è un elemento fondamentale dell'attività delle aziende moderne, ma è anche il principale vettore delle minacce. Inoltre, gli attacchi via email - dal phishing alla violazione dell'email aziendale (BEC, Business Email Compromise), passando per gli attacchi alla supply chain, il ransomware e la violazione degli account cloud - sono in costante evoluzione. Pertanto, proteggere in modo efficace questo vettore dalle minacce è un compito difficile, anche per le aziende più grandi e più complesse. Fortunatamente, Proofpoint può aiutarti.

La nostra soluzione di protezione avanzata dell'email è distribuita in un numero di aziende delle classifiche Fortune 100, Fortune 1000 e Global 2000 superiore a quello di qualsiasi altro fornitore. Per affrontare questa sfida, adotta un approccio in linea e basato su API. Questo garantisce piena protezione di tutti i messaggi in entrata e in uscita. Non si focalizza solo sulle email che le soluzioni di sicurezza tradizionali non rilevano. Il nostro approccio integrato a più livelli riduce il rischio di attacchi andati a buon fine rilevando le minacce in modo più rapido e preciso. Le nostre avanzate funzionalità di rilevamento e la nostra piattaforma scalabile ti consentono di migliorare l'efficacia operativa. Grazie alle informazioni fruibili fornite da Proofpoint, puoi comprendere meglio i rischi, agire proattivamente e rispondere alle minacce in modo più rapido ed efficace.

Rilevamento e blocco delle minacce avanzate

Un'efficacia affidabile

La threat intelligence e le funzionalità di rilevamento delle minacce di Proofpoint offrono una solida difesa contro le minacce sofisticate, riducendo i falsi positivi.

Sfruttiamo strumenti di analisi della reputazione, riscrittura degli URL e sandboxing predittivo e al momento del clic per rilevare i payload dannosi, come quelli che vengono recapitati tramite allegati e URL. Integriamo il rilevamento delle tecniche di elusione e offuscamento come i CAPTCHA e dei link protetti da password, dei siti estremamente renderizzati, dei reindirizzatori e dei siti di condivisione dei file.

Utilizziamo anche modelli di intelligenza artificiale e di machine learning del grafico delle minacce Nexus per rilevare gli attacchi senza payload, come gli attacchi BEC.

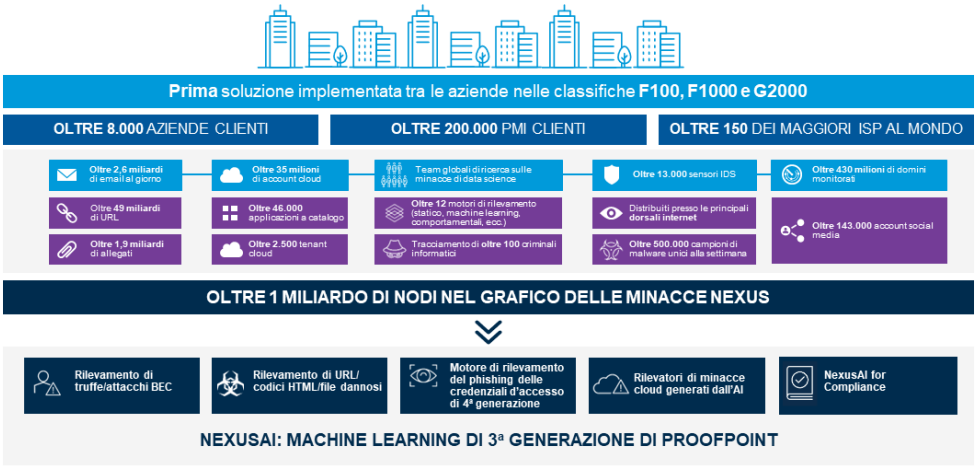

Figura 1. Grafico delle minacce Nexus.

Nell'odierno panorama delle minacce incentrato sulle persone, i tuoi collaboratori sono il tuo bene più prezioso, ma anche il tuo rischio più grande.

Questi modelli valutano segnali come il rischio legato ai fornitori, segnali legati agli utenti provenienti dalle suite di collaborazione, l'elaborazione del linguaggio naturale dei contenuti, le relazioni con i destinatari e l'intento. I dati di riferimento e contestuali ci permettono di individuare rapidamente le email potenzialmente dannose. Si tratta di un ottimo complemento per la nostra threat intelligence e altri motori di rilevamento mirati, che permette di minimizzare i falsi positivi.

Analizziamo le email tramite strumenti di analisi dei contenuti, analisi della reputazione e sandboxing. Questo ci permette di bloccare con successo le minacce avanzate trasmesse tramite email, tra cui il malware polimorfico e il ransomware, prima che colpiscano i tuoi utenti. Inoltre, ti offriamo funzionalità di sandboxing predittivo degli URL al momento del clic per rilevare e bloccare gli URL dannosi. La riscrittura degli URL protegge i tuoi utenti su qualsiasi rete e dispositivo. Permette anche di rilevare se un messaggio è stato reso "dannoso" dopo la consegna

Clic in sicurezza grazie all'isolamento dell'email e del browser

Proofpoint Browser Isolation e Proofpoint Email Isolation offrono un ambiente sicuro nel quale i tuoi utenti possono consultare in modo sicuro i siti web, la loro webmail personale e la loro email aziendale. I criminali informatici utilizzano diverse tattiche e vettori di minaccia per cercare di accedere ai tuoi sistemi, come la violazione degli account del fornitore. Possono, per esempio, prendere di mira i tuoi utenti tramite la loro email personale o canali non protetti. Grazie all'isolamento, puoi disabilitare upload e download. Puoi anche limitare l'inserimento dei dati durante l'analisi in tempo reale di un sito web. Sono sufficienti pochi secondi. La tecnologia aggiunge un livello di protezione ulteriore per prevenire il furto delle credenziali di accesso, il malware e il ransomware. È particolarmente utile contro le email di phishing che contengono URL che innescano attività dannose dopo la consegna.

Prevenzione delle frodi via email grazie all'autenticazione delle email

L'autenticazione delle email aggiunge un ulteriore livello di protezione. La sua efficacia nel bloccare le minacce di impostori privi di malware, come gli attacchi BEC è ben nota. Tuttavia, le aziende esitano ad adottare e applicare gli standard DMARC per paura di bloccare le email legittime.

Proofpoint ti aiuta a distribuire e applicare l'autenticazione DMARC in tutta sicurezza, senza bloccare il flusso di email legittime. L'autenticazione DMARC ti protegge dallo spoofing dei domini e dalle email fraudolente che utilizzano i tuoi domini affidabili. Blocca i messaggi fraudolenti a livello del gateway Proofpoint, proteggendo al contempo l'identità delle email della tua azienda. Inoltre, puoi visualizzare in modo centralizzato tutte le minacce fraudolente, compresi i domini fotocopia dannosi.

Questa visibilità è possibile indipendentemente dalla tattica utilizzata o dalla persona presa di mira. Con il nostro servizio Proofpoint Virtual Takedown, puoi prevenire proattivamente gli attacchi tramite email che utilizzano domini fotocopia prima che colpiscano. Semplifichiamo l'implementazione DMARC mettendo a tua disposizione un consulente esperto che ti assisterà durante tutto il processo di implementazione. In collaborazione con il tuo team, identifichiamo tutti i mittenti affidabili, comprese le terze parti, per garantire una corretta autenticazione. Proofpoint ha aiutato oltre un terzo delle aziende Fortune 1000 durante questo processo. Siamo in grado di lavorare con le configurazioni più sofisticate.

Protezione delle email interne e rapida neutralizzazione delle minacce

Proteggere le email interne è fondamentale tanto quanto proteggere la posta in arrivo. I criminali informatici utilizzano account compromessi per inviare email di phishing, lanciare attacchi BEC o diffondere malware. Analizziamo le email interne alla ricerca di contenuti dannosi inclusi URL e allegati. Quando viene rilevata un'email interna dannosa, puoi estrarla e metterla in quarantena automaticamente, anche se altri utenti l'hanno già ricevuta e inoltrata. Forniamo anche report che mostrano tutti gli account che potrebbero essere stati compromessi, in modo da poter intervenire rapidamente su tali account.

Visibilità sugli attacchi e sulla superficie d'attacco costituita dai tuoi dipendenti

Per meglio mitigare i rischi e portarli all'attenzione del tuo management e del consiglio di amministrazione, devi essere in grado di identificare:

- Gli utenti più a rischio e le tecniche di attacco utilizzate
- Il panorama delle minacce, gli obiettivi, i criminali informatici e le tendenze
- Altri segnali come i rischi legati ai fornitori e al cloud

Proofpoint ti fornisce tutte queste informazioni e altro ancora. Grazie al nostro approccio basato su una piattaforma, ottieni una comprensione completa dei rischi incentrati sulle persone, senza frammentazione dei dati. Ti aiutiamo a essere più proattivo nella gestione delle minacce sofisticate.

Riduzione dei rischi con informazioni incentrate sulle persone

Nel panorama odierno delle minacce incentrato sulle persone, i tuoi dipendenti sono il tuo bene più prezioso, ma anche il tuo rischio principale. Ti offriamo visibilità ineguagliata sugli attacchi mirati e sulla superficie d'attacco costituita dai tuoi collaboratori.

Identifichiamo inoltre gli utenti che rappresentano il rischio maggiore per la tua azienda e ne spieghiamo il motivo. Il nostro report sui VAP (Very Attacked People™ ovvero le persone più attaccate) elenca gli utenti più colpiti. Il nostro report sugli utenti che si lasciano ingannare più facilmente identifica gli utenti che hanno fatto cli su messaggi dannosi. Puoi tracciare i VIP tramite la dashboard. Una volta ottenute queste informazioni, puoi implementare controlli adattivi per i tuoi utenti vulnerabili, in modo da poter definire le priorità e ridurre i rischi. Questi controlli possono includere una formazione mirata di sensibilizzazione alla sicurezza, l'isolamento del browser e l'autenticazione a più fattori.

Informazioni incentrate sulle minacce a fini di contestualizzazione

Forniamo informazioni forensi dettagliate su minacce e campagne in tempo reale. La nostra analisi approfondita delle minacce fornisce tutte le informazioni necessarie, tra cui l'obiettivo dell'attacco, l'origine dell'attacco e le modalità. Stabiliamo anche il fine dell'attacco (Per esempio, possiamo stabilire se lo scopo è quello di esfiltrare i dati, installare ransomware, perpetrare azioni fraudolente, ecc.). Correliamo gli attacchi email con i tentativi di connessione sospetti per aiutarti a rilevare e bloccare le violazioni degli account in modo più efficace. La nostra piattaforma ti permette di confrontare tutti i tipi di minacce e gli obiettivi dei criminali informatici che ti prendono di mira con quelli che colpiscono tuoi omologhi.

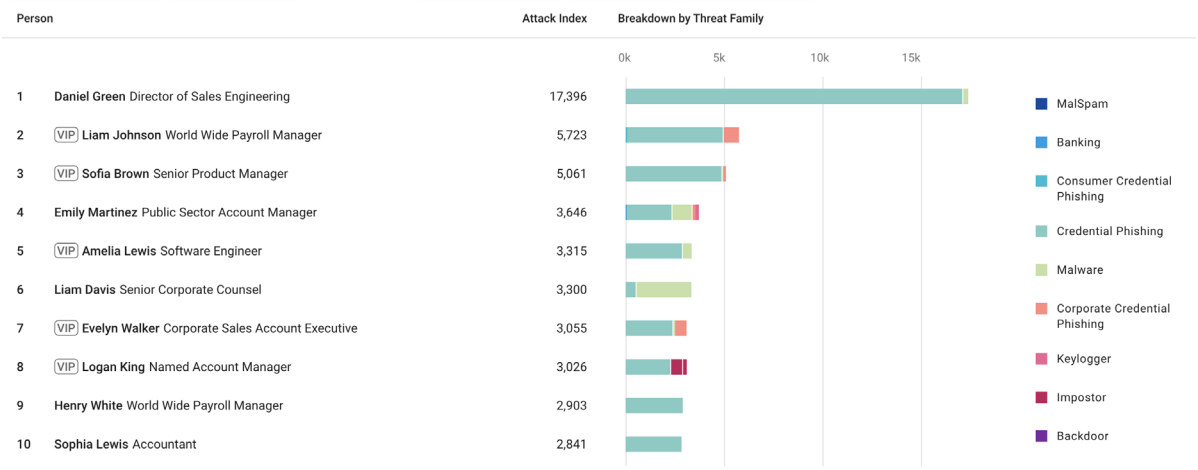

Figura 2. Report sui VAP di Proofpoint che mostra gli utenti più a rischio e i tipi di minaccia.

Figura 3. Soluzione Proofpoint Closed-Loop Email Analysis and Response (CLEAR) con casella di posta per gli abusi automatizzata.

Integrazione delle informazioni sui rischi di violazione degli account cloud e su quelli legati ai fornitori

Ti offriamo visibilità sui rischi di violazione e sui rischi legati ai fornitori. Inoltre, questa visibilità ti permette di sradicare completamente gli attacchi complessi. Nexus Supplier Risk Explorer ci permette di identificare automaticamente i fornitori potenzialmente compromessi e i domini che utilizzano per inviare email ai tuoi utenti. Grazie alla nostra funzionalità SaaS Defense integrata puoi ottenere informazioni sugli utenti potenzialmente compromessi, sui file dannosi o esposti e sulle applicazioni di terze parti a rischio.

Miglioramento dell'efficacia operativa

Molti team della sicurezza sono sotto organico o sovraccarichi di lavoro. Spesso si trovano a dover gestire più fornitori e prodotti di sicurezza aziendale, raramente compatibili tra di loro. Ti offriamo una soluzione integrata che si concentra sulle minacce più importanti e ne automatizza il rilevamento e la neutralizzazione. Puoi così risparmiare denaro e tempo prezioso, poiché i team della sicurezza possono dedicare meno risorse interne alla neutralizzazione delle email rispetto all'utilizzo di soluzioni concorrenti.

Estrazione automatica delle email dannose

La nostra soluzione permette anche di eliminare il lavoro manuale e le ipotesi dalle attività di risposta agli eventi. Puoi così neutralizzare le minacce in modo più rapido ed efficiente. Eliminiamo le email di phishing che contengono URL la cui attività dannosa viene attivata dopo la consegna. Inoltre, possiamo eliminare - con un clic o automaticamente - le email indesiderate dagli account interni compromessi, anche se sono state inoltrate o ricevute da altri utenti. Oltre a ciò, il nostro grafico delle minacce Nexus genera avvisi e acquisisce e confronta automaticamente i dati forensi, in modo da ottenere una visione fruibile delle minacce. Grazie a questo approccio puoi ridurre fino al 90% il tempo dedicato alla neutralizzazione delle email.

Ottimizzazione della procedura di segnalazione degli abusi tramite la casella email dedicata

Ti aiutiamo a ottimizzare la procedura di segnalazione degli abusi tramite la casella email dedicata e a ridurre il carico di lavoro del tuo team IT. Gli utenti possono segnalare le email sospette con **un clic** direttamente da un avviso o tramite il componente aggiuntivo PhishAlarm®. Se il messaggio segnalato risulta essere dannoso, può essere messo automaticamente in quarantena, così come tutte le sue copie. Gli utenti ricevono un'email personalizzata che li informa che si tratta di un messaggio dannoso. Un tale approccio li incoraggia a segnalare messaggi simili in futuro. Gli amministratori possono ottenere report dettagliati sul comportamento degli utenti e confrontare la precisione della segnalazione dei messaggi dannosi con quella di altre aziende del settore.

Cambiamento dei comportamenti grazie alla formazione incentrata sulle minacce

Le minacce odierne trasmesse via email richiedono generalmente una qualche forma di attivazione da parte dell'utente. Ma i tuoi dipendenti non devono essere l'anello debole dalla tua strategia di sicurezza informatica. Una forza lavoro consapevole della sicurezza informatica può rappresentare una solida linea di difesa contro gli attacchi informatici.

Proofpoint consente di intervenire sui VAP o sui dipendenti che si lasciano ingannare più facilmente. I dati raccolti su di loro vengono automaticamente integrati nella nostra piattaforma di sensibilizzazione alla sicurezza informatica. La piattaforma utilizza questi dati per sviluppare un programma di formazione più mirato ed efficace. Ti permette di utilizzare delle simulazioni di attacchi di phishing realistiche basate sulla threat intelligence di Proofpoint per creare esperienze di formazione pertinenti. Gli utenti che cadono nella trappola di una simulazione ricevono indicazioni puntuali e possono poi essere iscritti automaticamente a una formazione specifica. Forniamo inoltre agli utenti avvisi in caso di email sospette compreso un tasto "Report Suspicious" (Segnala come sospetto). Questi avvisi includono brevi descrizioni e immagini personalizzabili dei rischi associati a una particolare email e consentono agli utenti di segnalare i messaggi direttamente dall'avviso. Questo permette ai tuoi utenti di prendere decisioni più informate. Queste funzioni sono compatibili con tutti i dispositivi e con tutte le applicazioni.

Protezione dalle perdite di dati via email

L'email è il vettore delle minacce per eccellenza sia per le minacce in entrata che per le perdite di dati in uscita. Devi quindi proteggere i tuoi dati sensibili e prevenire la perdita di dati via email. Ti forniamo la visibilità e le regole preconfigurate necessarie per prevenire la perdita di dati accidentale o intenzionale durante gli scambi di email. La prevenzione della perdita dei dati (DLP) e la crittografia sono strettamente integrate e possono essere gestite a livello centrale nella piattaforma Proofpoint Information and Cloud Security. Grazie al nuovo gestore unificato degli avvisi, puoi personalizzare le analisi dei dati preconfigurate per rilevare e segnalare le violazioni DLP di tuo interesse. Semplifica le tue operazioni grazie a flussi di lavoro ottimizzati e a funzionalità di neutralizzazione delle email. Analizziamo le informazioni riservate all'interno di dati strutturati e non strutturati. Inoltre, ti forniamo policy ottimizzate e dizionari predefiniti. Questi identificano automaticamente i dati soggetti alla conformità normativa e alla legislazione sulla privacy dei dati. Ti aiutano inoltre a rispettare le normative sulla protezione dei dati di una vasta gamma di settori industriali - tra cui PCI DSS, SOX, HIPAA, GDPR e altri - riducendo al contempo le attività manuali. In combinazione con la crittografia, puoi definire e personalizzare policy univoche per crittografare automaticamente i dati nell'email. Un tale approccio semplifica la gestione e la sicurezza degli scambi di dati sensibili.

In breve

Proofpoint Advanced Email Security offre una protezione ineguagliata contro le minacce che prendono di mira l'email. Fornisce una visibilità fruibile sugli attacchi e sulle persone più attaccate. I benefici della soluzione sono molteplici:

- Blocco delle minacce avanzate prima che vengano distribuite
- Visibilità ineguagliata sui rischi legati ai dipendenti, sulle minacce e altre informazioni
- Miglioramento dell'efficacia operativa grazie all'automazione della risposta alle minacce
- Formazione e responsabilizzazione degli utenti per trasformarli in una solida ultima linea di difesa
- Protezione dalle perdite di dati via email

PER SAPERNE DI PIÙ

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

INFORMAZIONI SU PROOFPOINT

Proofpoint 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 il 75% delle Fortune 100, 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**.