proofpoint.

GUIDA ALLA PIANIFICAZIONE

Passaggio da un gateway di posta tradizionale a Proofpoint

I gateway email sicuri (SEG) tradizionali sono stati concepiti per bloccare lo spam e il malware noti. Tuttavia, attualmente i criminali informatici utilizzano minacce sofisticate e tecniche multi-vettore, come la violazione dell'email aziendale (BEC, Business Email Compromise), il takeover degli account (ATO, Account Takeover), il phishing tramite codice QR e l'elusione dell'autenticazione a più fattori. Tutte minacce che questi strumenti di vecchia generazione non sono stati progettati per contrastare. Pertanto, se utilizzi un gateway di questo tipo, la tua azienda corre un rischio maggiore di subire una violazione e vedere aumentare i costi.

Se desideri passare a Proofpoint per rafforzare la tua sicurezza, questa guida alla pianificazione ti aiuterà a preparare il tuo percorso di migrazione. È concepita per i clienti di Barracuda, Cisco (IronPort), Forcepoint (Websense), Symantec Email Security.cloud (MessageLabs), Trellix (FireEye/McAfee) e Trend Micro.

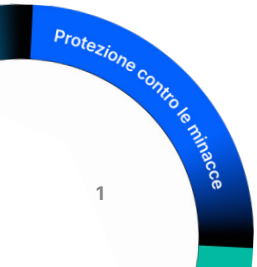
Queste istruzioni dettagliate ti aiuteranno a valutare l'efficacia del tuo gateway di vecchia generazione, a misurarne i costi e a definire le tempistiche per la migrazione. Proofpoint offre opzioni di distribuzione flessibili - migrazione completa del gateway, implementazione di un'API o approccio graduale - in modo che tu possa scegliere ciò che si adatta meglio al tuo ambiente. Per semplificare questo processo, il tuo team Proofpoint può fornirti strumenti gratuiti (valutazione rapida dei rischi, report sulle discrepanze, valutazione del valore aggiunto) per quantificare la riduzione dei rischi e il ritorno sull'investimento.

Fase 1. Quantificare l'efficacia della tua protezione attuale

Inizia con la visibilità. Misura l'efficacia delle tue difese attuali, e cosa non rilevano, per stabilire una chiara base di riferimento.

- Esamina i report dei falsi negativi, che si trovano nei registri di amministrazione e nei ticket SIEM/IR. Queste informazioni possono aiutarti a comprendere l'entità e la portata dei rilevamenti mancati.
- Documenta la percentuale di email segnalate dagli utenti confermate come veri positivi, perché questi dati numerici ti aiuteranno a quantificare il tempo impiegato dagli analisti per risolvere i falsi positivi.
- Identifica gli incidenti di takeover degli account (ATO) rilevati da altri sistemi. Tra gli esempi rientrano l'uso improprio delle regole della casella di posta, gli avvisi relativi all'impossibilità di spostarsi o alla geolocalizzazione, nonché l'elusione dell'autenticazione a più fattori.
- Esamina i tentativi di phishing interno o laterale rilevati da altri sistemi o segnalati dagli utenti.
- Effettua una valutazione rapida dei rischi legati all'email di Proofpoint. Questo servizio ti fornirà visibilità basata sui dati relativi alle minacce che il tuo gateway esistente o il tuo sistema Microsoft 365 potrebbero non rilevare.

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



Fase 2. Calcolare il costo dello status quo

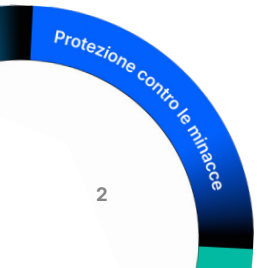
La sicurezza non si misura solo in termini di elementi bloccati, ma anche in termini di efficienza operativa. Valuta il tempo, gli sforzi e il livello di attenzione richiesti agli analisti per il triage manuale, i falsi positivi e i flussi di lavoro frammentati, per mettere in evidenza il costo reale della manutenzione del tuo gateway di vecchia generazione.

- Documenta il numero di clic e di minuti/ore necessarie ai tuoi analisti per indagare su un singolo incidente di phishing (Non è insolito che gli analisti impieghino più di 12 clic e diverse ore per risolvere ogni incidente). Inoltre, identifica dove si verificano solitamente i ritardi.
- Tieni traccia delle ore dedicate dagli analisti al triage della casella di posta per gli abusi. Calcola quanto tempo gli analisti dedicano ogni settimana alla disamina delle email segnalate dagli utenti. Scopri inoltre quale percentuale di questi messaggi si rivela una minaccia reale rispetto ai falsi allarmi.
- Calcola il tempo che il tuo team dedica alla preparazione dei report. Annota il tempo impiegato dal tuo team a compilare e formattare le metriche di sicurezza necessarie per redigere i report destinati alla dirigenza o al consiglio di amministrazione. Quest'attività spesso richiede esportazioni di dati manuali e operazioni nei fogli di calcolo.
- Parla con gli analisti della sicurezza e documenta i loro punti di frustrazione. Quali sono i problemi che si presentano più frequentemente? Tra gli esempi rientrano rumore, falsi positivi e la proliferazione delle console.

Fase 3. Scegliere il tuo percorso di migrazione

Il tuo ambiente e le tue priorità evolveranno e la sicurezza della tua email dovrebbe fare lo stesso. Proofpoint ti offre una flessibilità che i fornitori a modello unico non possono garantire. Ci distinguiamo perché offriamo tre percorsi di migrazione:

- **Opzione 1: rafforzamento della protezione basata su API.** Quest'opzione richiede poco sforzo e ha un impatto elevato. Integra l'API Proofpoint Core Email Protection con Microsoft 365 per una protezione immediata contro minacce come la violazione dell'email aziendale (BEC), il takeover degli account (ATO) e il phishing. Questo modello supporta anche il passaggio da un gateway email tradizionale a un modello Microsoft + Proofpoint, garantendo una protezione continua durante e dopo la migrazione.
- **Opzione 2: implementazione dell'API, seguita dalla migrazione del gateway.** Quest'opzione richiede uno sforzo moderato, ma ha un impatto maggiore. Inizia a implementare l'API Proofpoint per ottenere rapidi vantaggi operativi e ridurre i rischi. Successivamente, effettua una transizione graduale al gateway email sicuro di Proofpoint per ottenere il controllo del routing, rispondere alle mutevoli esigenze di conformità o garantire una difesa avanzata a più livelli.
- **Opzione 3: sostituzione completa del gateway.** Elimina completamente il tuo gateway email di vecchia generazione e migra i tuoi record MX sulla soluzione Proofpoint per il massimo controllo e una protezione completa dell'email prima della consegna.



Fase 4. Pianificare la migrazione e lanciare un progetto pilota

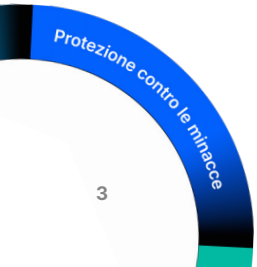
Convalida i risultati prima dell'implementazione completa. Un progetto pilota controllato ti consente di testare Proofpoint insieme al tuo gateway esistente, confermare un rilevamento più efficace e una risposta più rapida, e rafforzare la fiducia della dirigenza grazie a dati concreti.

- Definisci fin da subito i tuoi criteri di successo. Quali risultati desideri ottenere? Per esempio: un miglior rilevamento delle minacce, una riduzione dei falsi positivi, una risoluzione più rapida e la prevenzione dei takeover degli account (ATO).
- Osserva i potenziali miglioramenti del rilevamento eseguendo la protezione dell'email di Proofpoint in modalità silenziosa.
- Stabilisci se il tuo progetto pilota offre i seguenti risultati:
  - Un confronto chiaro che mostra le minacce rilevate da Proofpoint e quelle che il tuo gateway email tradizionale non ha rilevato
  - Una sintesi di facile lettura delle lacune identificate nella protezione offerta dal gateway
  - Un report sul valore aggiunto che quantifica, in euro, il tempo risparmiato dal tuo team e la riduzione dei rischi per la tua azienda

Fase 5. Stabilire le tue tempistiche

Pianifica una transizione graduale che sia in linea con i cicli di rinnovo, il tuo personale e la tua tolleranza a rischi. Con il supporto alla migrazione di Proofpoint, puoi modernizzare la protezione senza interruzioni di servizio.

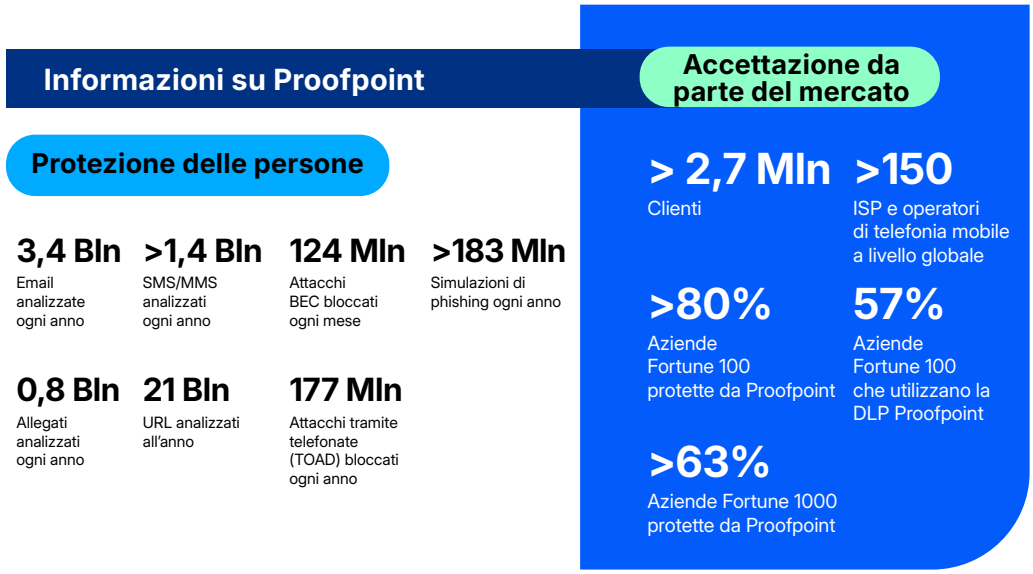
- Crea un piano in 3 fasi:
  1. Progetto pilota
  2. Esecuzione in parallelo
  3. Trasferimento finale
- Esamina le tue tempistiche di rinnovo della licenza e i cicli di budget. Se necessario, cerca opportunità di acquisto contrattuale.
- Esegui il tuo vecchio sistema in parallelo come misura di sicurezza aggiuntiva finché la nuova implementazione non avrà ricevuto l'approvazione della direzione.
- Utilizza i Servizi Premium di Proofpoint per un'esperienza di migrazione di alto livello. I nostri team dei servizi Proofpoint Advisory e Applied forniscono competenze pratiche per ottimizzare le configurazioni, accelerare l'implementazione e garantire una protezione continua durante la transizione.



Conclusione

Quando scegli Proofpoint, ti supportiamo durante la fase di transizione. Forniamo manuali di migrazione, modelli di progetto pilota e storie di successo di clienti per accompagnarti nel tuo percorso. Che tu abbia scelto l'implementazione iniziale dell'API, una transizione graduale o la sostituzione completa del tuo gateway email tradizionale, ti aiutiamo a migrare con sicurezza e a ottenere risultati misurabili.

Perché scegliere Proofpoint?



proofpoint.

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 un partner di fiducia per 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 ulteriori informazioni, visitare il sito www.proofpoint.com/it.

Seguici: LinkedIn

SCOPRI LA PIATTAFORMA PROOFPOINT →