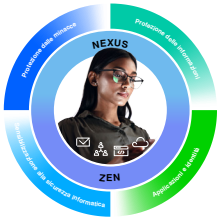
Proofpoint Account Takeover Protection

Rileva e neutralizza i takeover degli account cloud

Vantaggi principali

- Rilevamento degli account Microsoft 365, Google Workspace e Okta compromessi
- Protezione contro i takeover degli account che eludono l'autenticazione a più fattori (MFA)
- Accelerazione delle indagini grazie a una vista centralizzata delle attività successive al takeover degli account
- Riduzione del tempo di permanenza dei criminali informatici grazie alla sospensione degli account e alla reimpostazione forzata delle password
- Annullamento delle modifiche dannose apportate alle regole della casella email e alle configurazioni dell'MFA
- Rimozione delle applicazioni di terze parti sospette

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 Account Takeover Protection (ATO Protection) estende le funzionalità di Proofpoint Targeted Attack Protection (TAP) per rilevare gli cloud account compromessi e proteggere i tuoi ambienti cloud.

Proofpoint ATO Protection estende le funzionalità di Proofpoint Targeted Attack Protection (TAP) per rilevare e proteggere gli account cloud compromessi. Proofpoint ATO Protection sfrutta l'intelligenza artificiale (IA), le informazioni di threat intelligence correlate e l'analisi comportamentale per rilevare le attività sospette in ogni fase della catena d'attacco. Rileva le modifiche effettuate dai criminali informatici dopo la violazione e revoca il loro accesso. Annulla le modifiche dannose apportate alle regole della casella email e ai parametri dell'autenticazione a più fattori (MFA). Inoltre, rimuove le applicazioni di terze parti sospette e mette in quarantena e rimuove i file sospetti.

Proofpoint ATO Protection fornisce report dettagliati che mostrano le connessioni sospette, gli utenti attaccati e i sistemi e i parametri interessati. L'integrazione con Proofpoint Identity Threat Defense ti mostra il potenziale impatto di un takeover degli account su altri account e host con un solo clic. Queste informazioni ti aiutano a bloccare gli attacchi prima che diventino violazioni più gravi che potrebbero danneggiare la tua azienda.

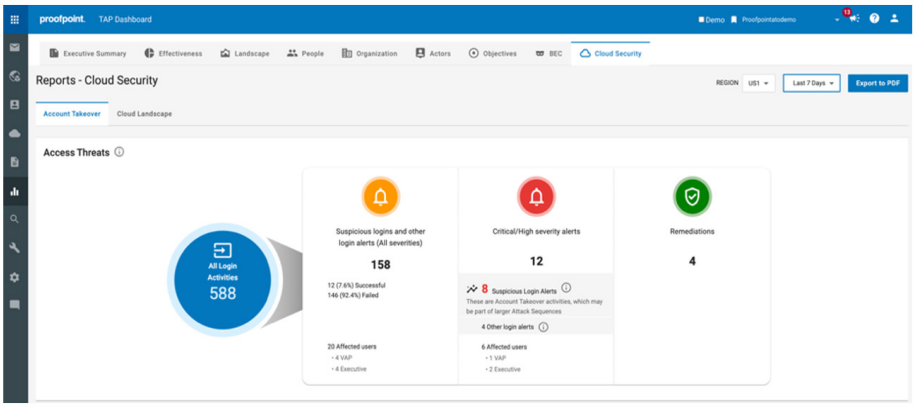


Figura 1. Proofpoint ATO Protection rileva le connessioni sospette, ti fornisce informazioni dettagliate per aiutarti a condurre indagini sulle minacce e annullare le modifiche dannose.

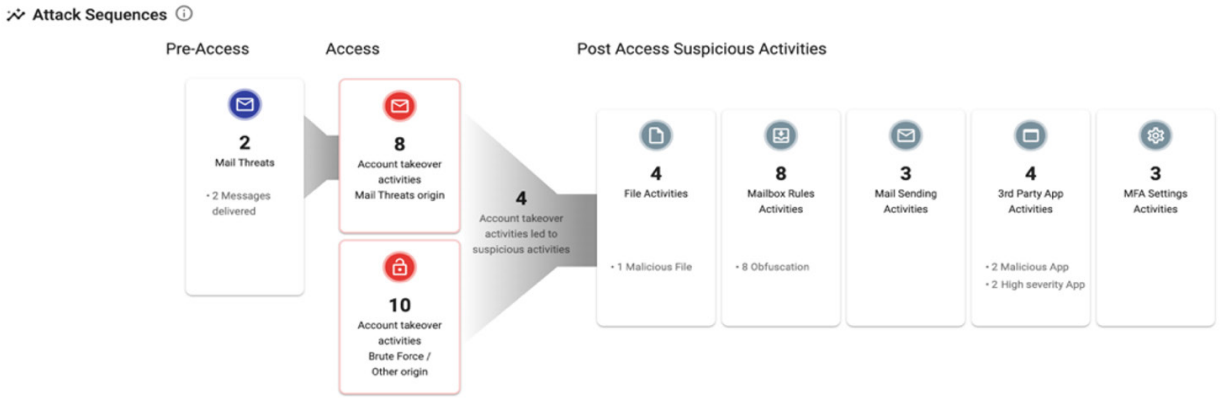


Figura 2. Il report Attack Sequence (Sequenza d'attacco) mostra le attività delle minacce prima e dopo l'accesso per gli account interessati.

Miglioramento del rilevamento e della visibilità

Proofpoint ATO Protection rileva gli account compromessi, le email sospette nonché altre attività dannose nei tuoi ambienti cloud. Utilizza la threat intelligence proveniente da oltre 40 milioni di utenti monitorati in migliaia di aziende. Combina queste informazioni con l'IA e l'analisi comportamentale per rilevare attività insolite nel tuo ambiente. Questa combinazione di tecniche riduce i falsi positivi. Disponi di rilevamenti accurati e di una chiara visione di tutte le attività nei tuoi account attaccati.

Quando un account viene compromesso, Proofpoint ATO Protection aggiunge degli avvisi nella dashboard TAP. Una vista cronologica mostra le attività di takeover degli account, le attività a livello di file e email, le modifiche apportate alle regole della casella email e ai parametri MFA, nonché l'aggiunta di applicazioni di terze parti.

Accelerazione delle indagini

Proofpoint ATO Protection mostra ai tuoi analisti della sicurezza la causa di un takeover degli account e spiega loro come limitare i rischi. Queste informazioni vengono integrate nel sistema e nel processo di indagine di TAP.

In questo modo, ricevi informazioni complementari a quelle fornite da TAP. Una vista cronologia mostra inoltre gli account compromessi e ti permette di fare clic su ogni evento per analizzarlo.

Puoi vedere come è stato attaccato un account e la posizione del criminale informatico. Inoltre puoi identificare gli utenti che sono stati colpiti da minacce simili. Analisi avanzate forniscono viste cronologiche dettagliate delle attività degli utenti, degli indirizzi IP, dei domini e di altri attributi. Questi dati arricchiti ti aiutano a valutare i rischi per la tua azienda.

Automazione della risposta

Proofpoint ATO Protection rileva e annulla le modifiche dannose apportate alle regole della casella email e ai parametri MFA. I criminali informatici spesso modificano le regole della casella email per dissimulare la loro presenza nel tuo sistema e monitorarlo prima di lanciare un attacco di phishing interno o intraprendere altre fasi dell'attacco. Proofpoint ATO Protection rimuove anche le applicazioni di terze parti dannose. Tutte queste azioni limitano i danni alla tua azienda e riducono il tempo necessario per analizzare e neutralizzare le minacce. Se le tue indagini rivelano altre attività dannose, puoi correggere gli account compromessi. Puoi anche rimuovere i file che i criminali informatici hanno aggiunto all'account di un utente.

Proofpoint Account Takeover Protection in precedenza era noto con il nome Proofpoint TAP Account Takover.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito **proofpoint.com/it**.