proofpoint

PANORAMICA SULLA SOLUZIONE

SSO Password Guard

Rileva le esposizioni delle password prima che si trasformino in un takeover degli account

Vantaggi principali

- **Rileva le password aziendali inserite su siti non approvati e segnala l'esposizione delle credenziali d'accesso prima che i criminali informatici possano utilizzarle.**
- **Fornisce suggerimenti in tempo reale all'interno del browser quando gli utenti riutilizzano la loro password aziendale, in modo da favorire una correzione rapida e ridurre le esposizione ripetute.**
- **Riduce le violazioni legate alle credenziali d'accesso, con una conseguente diminuzione degli incidenti di takeover degli account, indagini e reimpostazioni delle password.**

Panoramica

I takeover degli account sono il risultato dell'esposizione delle credenziali d'accesso. Possono verificarsi a seguito di attacchi che eludono i controlli di prevenzione o a causa dei comportamenti quotidiani degli utenti che violano le policy aziendali.

I collaboratori spesso riutilizzano le password aziendali in applicazioni SaaS, strumenti di IA e siti web esterni, estendendo il rischio ben oltre il controllo dell'azienda. Una volta esposte, queste credenziali d'accesso consentono ai criminali informatici di connettersi come utenti legittimi e di eludere facilmente le difese tradizionali. I controlli di sicurezza tradizionali si concentrano sul blocco delle minacce prima che si verifichino o sulla segnalazione di attività insolite dopo una violazione. Tale approccio lascia una lacuna critica nel momento in cui le credenziali vengono inserite su siti non approvati o dannosi.

SSO Password Guard aiuta a colmare tale lacuna.

Operando direttamente nel browser, rileva qualsiasi riutilizzo delle password aziendali al punto di accesso e guida gli utenti a modificare le loro abitudini non sicure. Questo strumento, che fa parte di Proofpoint Collaboration Security Prime, estende la protezione a tutti i canali e le fasi di attacco per ridurre il rischio di takeover degli account e il carico di lavoro del tuo team.

Proteggersi dall'esposizione delle credenziali d'accesso al momento del rischio

SSO Password Guard interviene in un punto critico della catena di attacco: dopo che una minaccia ha raggiunto l'utente, ma prima che si verifichi un takeover degli account.

Quando gli utenti inseriscono password aziendali su siti non approvati o dannosi, Proofpoint rileva tale comportamento in tempo reale. Fornisce quindi suggerimenti immediati all'interno del browser sia al momento della registrazione che dell'accesso. L'esposizione delle credenziali viene così gestita quando si verifica, prima che le password possano essere riutilizzate o sfruttate altrove.

Riducendo l'uso improprio delle password al punto di accesso, le aziende bloccano uno dei percorsi più affidabili utilizzati dai criminali informatici per ottenere l'accesso. Ciò riduce il rischio di takeover degli account prima che si trasformi in un incidente.

Applicare le policy relative alle credenziali d'accesso e promuovere un cambiamento del comportamento

Le policy aziendali da sole non sono sufficienti a impedire agli utenti di riutilizzare le password aziendali.

SSO Password Guard rafforza i comportamenti sicuri intervenendo nel momento esatto in cui gli utenti eseguono azioni non sicure. I suggerimenti nel browser in tempo reale collegano direttamente il comportamento dell'utente al rischio, trasformando le azioni non sicure in momenti di apprendimento immediati.

Allo stesso tempo, i team della sicurezza ottengono visibilità sui trasgressori recidivi e sugli schemi di esposizione. Ciò consente loro di implementare programmi di sensibilizzazione mirati e basati su prove. Le aziende passano così da una formazione generale a un'azione mirata in grado di ridurre il rischio di recidiva nel tempo.

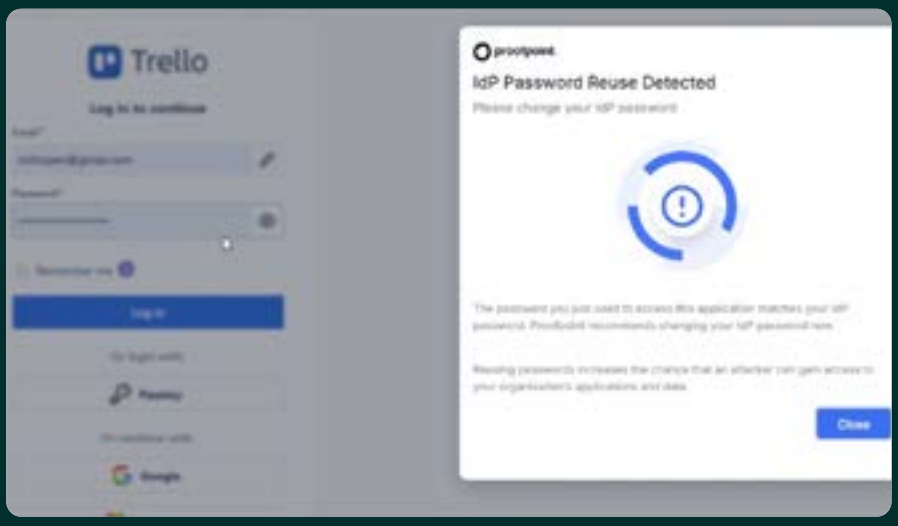

Figura 1. Esempio di avviso di SSO Password Guard rivolto a un utente finale

Ridurre il carico operativo e la complessità

La maggior parte dei team della sicurezza è costretta a indagare sugli incidenti di takeover degli account a seguito dell'esposizione delle credenziali d'accesso. Spesso non dispongono di informazioni chiare sul luogo in cui si è verificata l'esposizione o sugli utenti all'origine dei rischi.

SSO Password Guard riduce il carico di lavoro mettendo fine alle esposizioni delle password evitabili prima che si trasformino in incidenti, fornendo al contempo informazioni estremamente precise sul riutilizzo delle credenziali d'accesso. I team della sicurezza possono vedere su quali siti web vengono utilizzate le password aziendali. Possono valutare i rischi associati a tali siti e identificare gli utenti che espongono ripetutamente le loro credenziali d'accesso e rappresentano il rischio maggiore.

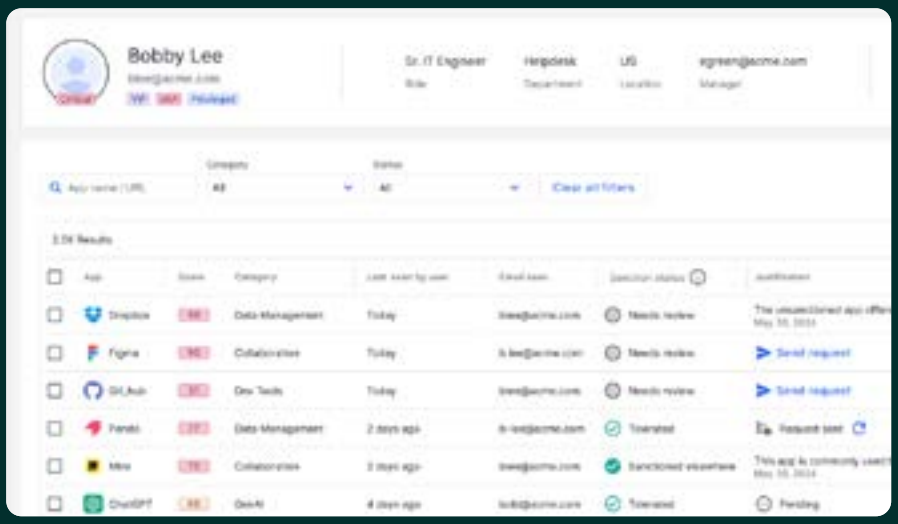

Figura 2. Informazioni sull'esposizione delle password in SSO Password Guard

Ciò si traduce in una diminuzione dei takeover degli account nonché in una riduzione del tempo dedicato alle indagini, alla reimpostazione delle password e alla pulizia. Quando si verifica un'esposizione, i team dispongono del contesto necessario per rispondere immediatamente, senza congetture.

Essendo integrato in Proofpoint Collaboration Security Prime, SSO Password Guard riduce anche la dipendenza da stack di rilevamento complessi e basati su segnali. I team della sicurezza traggono vantaggio da una visibilità centralizzata, segnali estremamente affidabilità e una risposta semplificata. Questo contribuisce a ridurre il costo totale di possesso migliorando al contempo i risultati relativi alla sicurezza.

proofpoint.