proofpoint.

PANORAMICA SULLA SOLUZIONE

Proofpoint User Protection

Responsabilizza i tuoi collaboratori
e estendi la protezione contro il takeover
degli account e il phishing oltre le email

Vantaggi principali

- **Estensione della protezione contro il phishing** oltre le email
- **Rafforzamento della tua protezione** con la threat intelligence integrata di Proofpoint
- **Supporto dei tuoi collaboratori** affinché facciano scelte più sicure di fronte alle minacce
- **Automazione della risposta** ai takeover degli account

I criminali informatici continuano a utilizzare il social engineering per colpire i tuoi collaboratori. Queste tattiche ingannano o minacciano gli utenti per spingerli a condividere le loro credenziali d'accesso o eseguire un codice dannoso. L'email resta il principale vettore di attacco per tali attacchi. Tuttavia, i criminali informatici ora sfruttano molti altri canali digitali, tra cui strumenti di collaborazione e comunicazione come Slack, Microsoft Teams, LinkedIn, Zoom. Questi attacchi mirano a violare gli account degli utenti e prenderne il controllo. In base a ricerche condotte da Proofpoint nel 2024, il 99% delle aziende viene regolarmente preso di mira da tentativi di takeover degli account. Circa il 62% sono vittime di tali attacchi[1]. Questi dati mostrano che le aziende hanno bisogno di un approccio globale per proteggere i loro collaboratori e ridurre i rischi di violazione degli account.

Proofpoint User Protection offre ai tuoi utenti un livello di protezione aggiuntivo oltre le email. La soluzione automatizza l'apprendimento basato sui rischi per i collaboratori che si lasciano più ingannare e i VAP (Very Attacked People, ovvero le persone più attaccate). Grazie a un'esperienza utente fluida, blocca gli URL dannosi trasmessi tramite applicazioni di messaggistica e collaborazione. Utilizza anche funzioni di rilevamento basato sull'IA e automatizza l'applicazione di misure correttive per prevenire il takeover degli account, accelerando così la risposta alle minacce.

1. Ricerche condotte da Proofpoint, dimensione del campione n > 5.000 aziende, 2024

©Proofpoint, Inc. 2025

Protezione rafforzata grazie a una migliore visibilità

Con Proofpoint User Protection, puoi sfruttare tutto il potenziale della piattaforma Human-Centric Security di Proofpoint. Grazie alla nostra threat intelligence integrata e alle informazioni sui rischi, disponi di una protezione rafforzata e di una visibilità approfondita sulle persone ad alto rischio e sulle attività dannose.

Proofpoint User Protection è ottimizzato da Proofpoint Nexus®, una piattaforma di threat intelligence alimentata da IA, machine learning e threat intelligence in tempo reale. Proofpoint User Protection estende questo stack di rilevamento delle minacce all'avanguardia per bloccare tutti gli URL dannosi, in qualsiasi modo siano distribuiti. Identifica in modo preciso i takeover degli account in strumenti come Microsoft 365, Google Workspace e Okta.

Proofpoint User Protection ti aiuta anche a individuare i tuoi utenti ad alto rischio analizzando i comportamenti dei tuoi utenti e le loro prestazioni nell'ambito della formazione sulla sicurezza informatica e delle simulazioni delle minacce. Quest'analisi dei rischi considera anche gli indicatori di violazioni di account attivi.

Grazie a questa maggior visibilità sui rischi legati agli utenti, puoi applicare controlli di sicurezza adattivi agli utenti con profili di rischio variabili. Per esempio, puoi attribuire automaticamente corsi di formazione sulla sicurezza informatica personalizzata ai tuoi VAP, ai collaboratori più inclini a farsi ingannare o agli obiettivi imminenti. Puoi anche applicare misure correttive automatiche dopo il takeover di un account: revoca dell'accesso, reimpostazione delle password, messa in quarantena degli account, ecc. Puoi anche revocare l'accesso alle applicazioni di terze parti e annullare le modifiche dannose apportate alle regole della casella email.

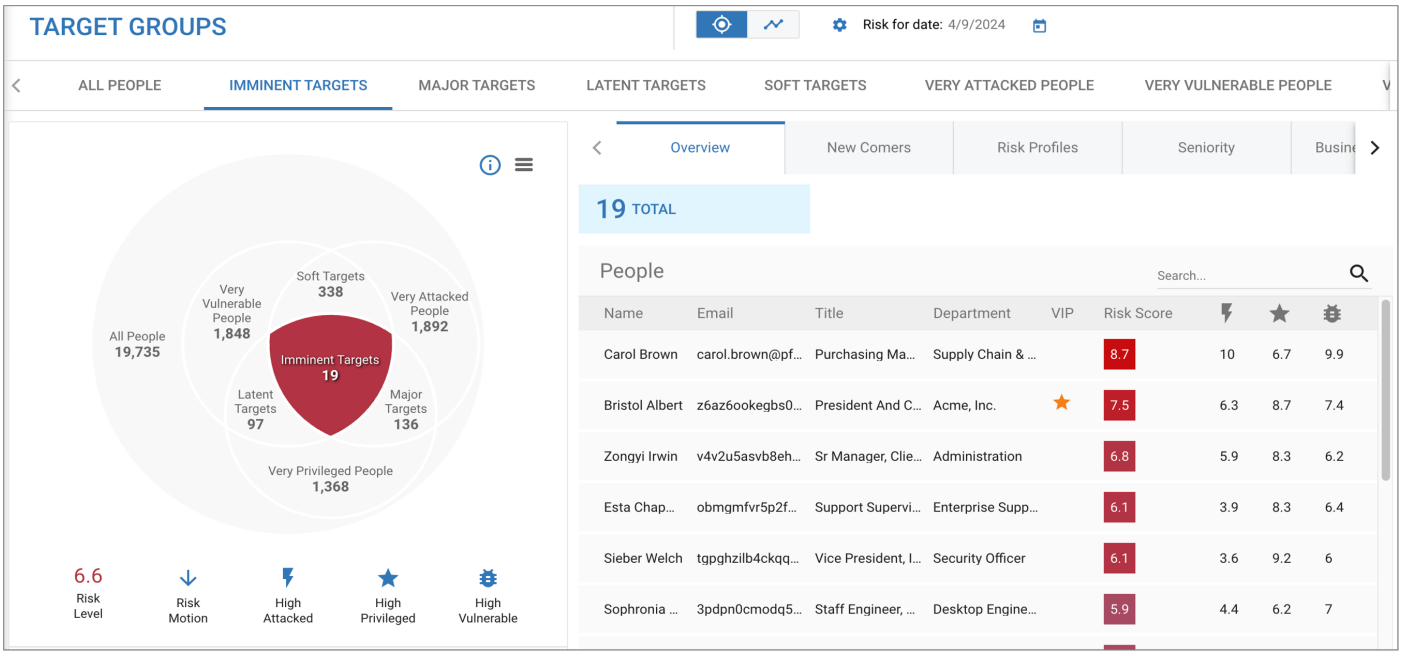

Figura 1. Proofpoint User Protection identifica i tuoi utenti a alto rischio grazie a un punteggio migliorato dei rischi legati agli utenti. Questa visibilità migliorata ti consente di dare priorità alle attività di sicurezza, applicare controlli di sicurezza adattivi e fornire formazione aggiuntiva agli utenti più a rischio.

©Proofpoint, Inc. 2025

Aiuta gli utenti a rafforzare la resilienza contro le minacce emergenti

Proofpoint User Protection offre ai tuoi collaboratori gli strumenti, le conoscenze e le motivazioni per rafforzare la loro resilienza contro le mutevoli tattiche di social engineering.

Sfruttando la threat intelligence globale di Proofpoint, la nostra soluzione ti offre informazioni in tempo reale sul panorama delle minacce in costante evoluzione. Con queste informazioni, puoi formare i tuoi utenti sulle tendenze delle minacce e le minacce emergenti. Puoi così fornire ai tuoi VAP un'istruzione mirata, inclusa la formazione, le simulazioni delle minacce e le notifiche, in merito alle minacce specifiche che si trovano a affrontare. Puoi anche personalizzare la formazione per adattarla ai ruoli, comportamenti e profili di rischio unici degli utenti.

Le funzionalità Adaptive Groups e Pathways ti permettono di iscrivere automaticamente i tuoi utenti a alto rischio a campagne mirate. In questo modo risparmi tempo e energie nella creazione di un programma efficace di cambiamento dei comportamenti. Inoltre, i tuoi collaboratori imparano a fare scelte più sicure di fronte alle minacce.

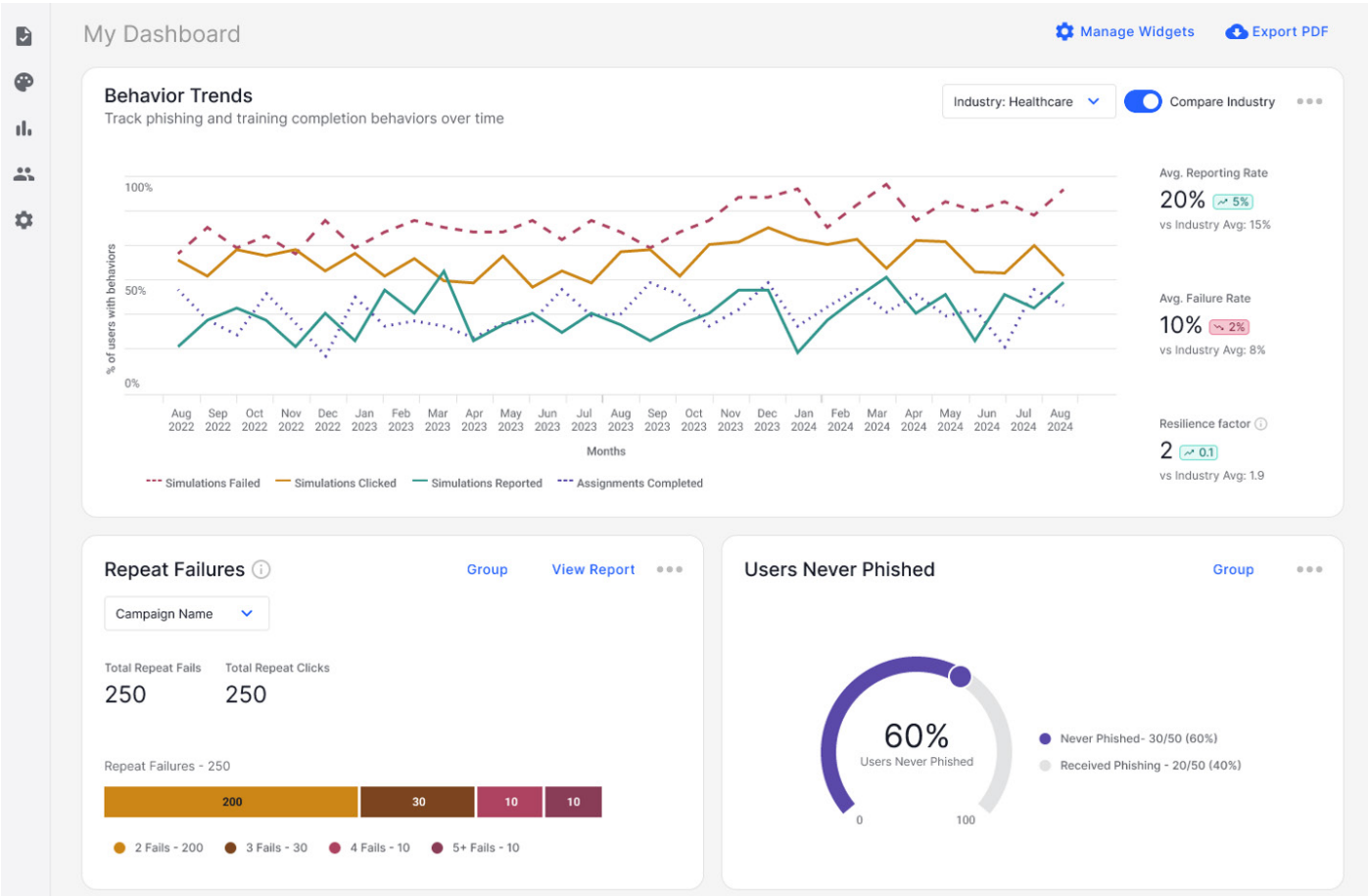

Figura 2. Proofpoint User Protection è alimentata dalla threat intelligence globale di Proofpoint. Ti fornisce informazioni fruibili sul panorama delle minacce in costante evoluzione. Puoi formare i tuoi utenti sulle nuove minacce e al contempo acquisire le tendenze comportamentali nel tempo.

©Proofpoint, Inc. 2025

Blocca i link dannosi su molteplici piattaforme

I criminali informatici oggi sfruttano altri canali digitali oltre all'email, tra cui Microsoft Teams, Zoom, Slack, LinkedIn e altre piattaforme dei social media. Proofpoint User Protection ti offre una protezione estesa bloccando gli URL dannosi su tutti questi canali.

Proofpoint User Protection è ottimizzato da Proofpoint Nexus, che analizza oltre 21 bilioni di URL. Grazie a queste informazioni, esegue un'ispezione della reputazione degli URL e analizza tutti gli URL nel browser. Quando un collaboratore cerca di accedere a un link in uno strumento di messaggistica o collaborazione, Proofpoint User Protection analizza l'URL in tempo reale e lo blocca se è dannoso. In questo modo, i tuoi utenti rimangono protetti contro i siti web e i contenuti dannosi.

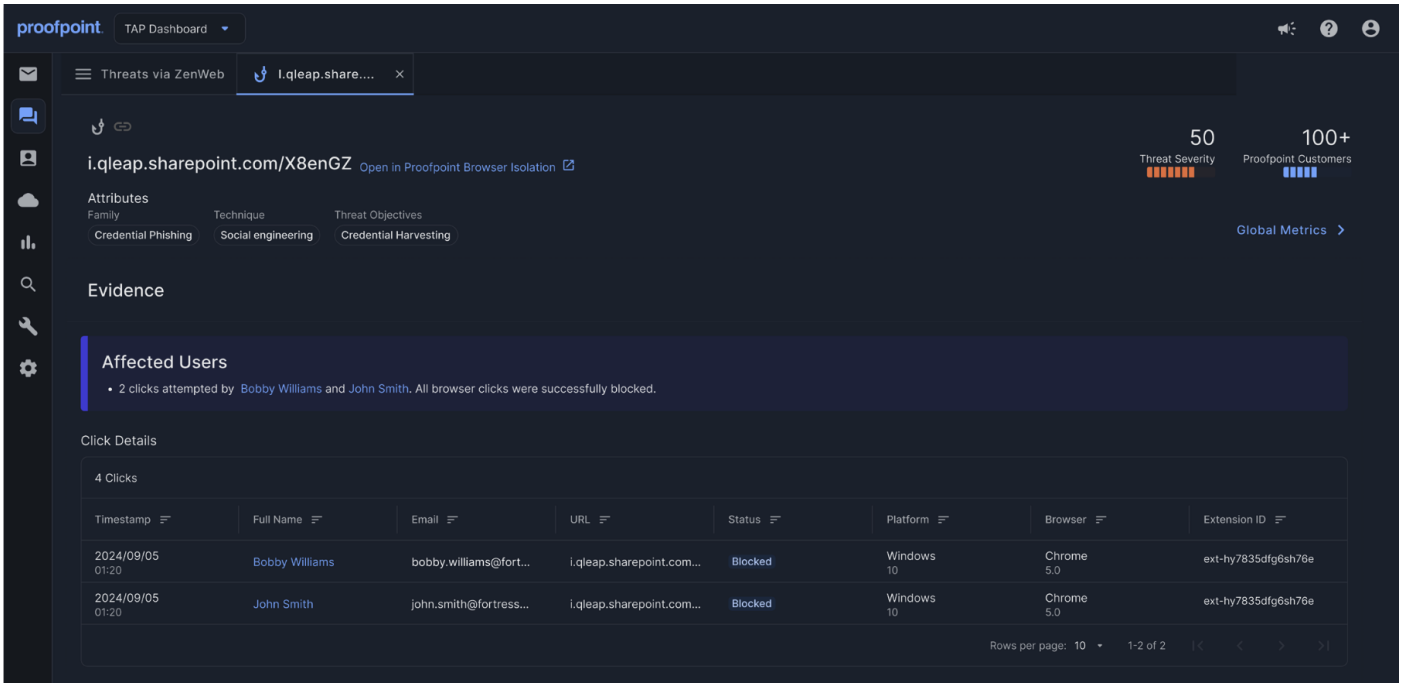

Figura 3. Proofpoint estende la protezione contro il phishing oltre le email. Blocca anche gli URL dannosi condivisi tramite piattaforme di messaggistica, collaborazione e comunicazione.

©Proofpoint, Inc. 2025

Rileva e neutralizza rapidamente gli account compromessi

Proofpoint User Protection ti offre la massima tranquillità in caso di violazione dell'account di uno dei tuoi collaboratori in uno strumento come Microsoft 365, Google Workspace o Okta. Rileva e neutralizza l'incidente prima che causi dei danni. Utilizzando l'IA, il machine learning, l'analisi comportamentale e la threat intelligence di Nexus, Proofpoint User Protection rileva le attività sospette sugli account cloud. Le correla con le minacce trasmesse via email per identificare in modo più preciso i takeover degli account e porvi fine.

Le soluzioni della concorrenza hanno capacità limitate per neutralizzare le attività che si verificano dopo il takeover degli account. Per contro, Proofpoint velocizza la tua risposta alle minacce dopo aver rilevato un takeover degli account. Identifica le modifiche apportate dai criminali informatici e revoca il loro accesso. Forza la reimpostazione delle password, annulla le modifiche apportate alle regole della casella email e ai parametri dell'autenticazione a più fattori (MFA) e interrompe i collegamenti con le applicazioni di terze parti dannose. Inoltre mette in quarantena i file che sono stati caricati dal criminale informatico e li rimuove.

Con Proofpoint User Protection puoi automatizzare tutte queste azioni. Dedichi meno tempo all'analisi e neutralizzazione dei takeover degli account e riduci i danni potenziali per la tua azienda.

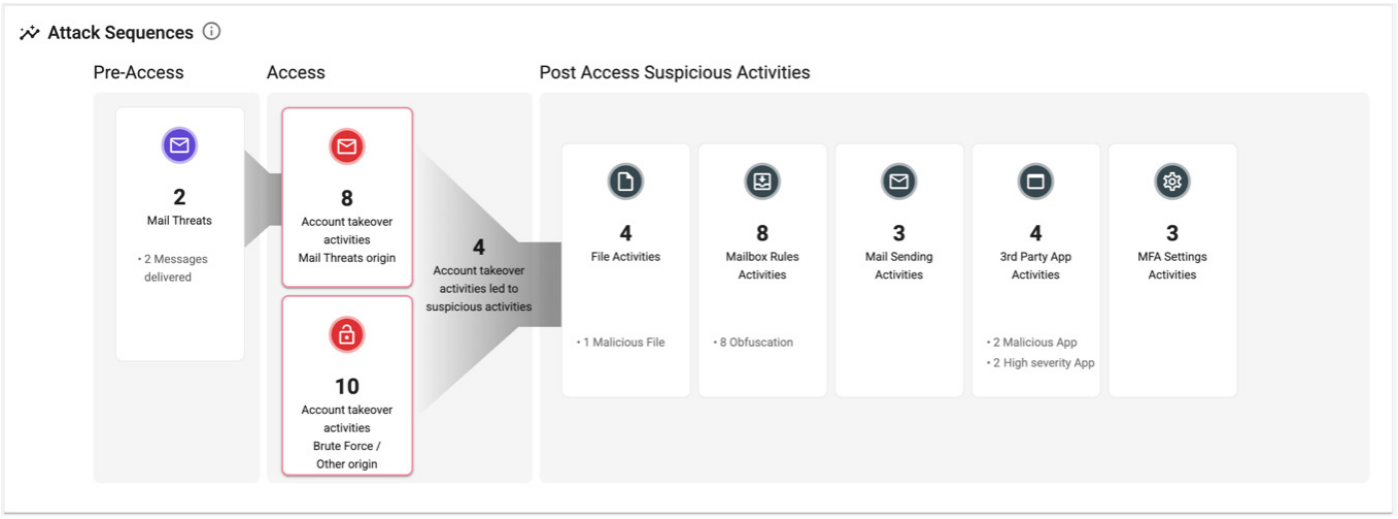

Figura 4. Proofpoint User Protection mostra le attività dannose prima e dopo l'accesso per gli account interessati.

©Proofpoint, Inc. 2025

Sfrutta la nostra competenza, ottimizza il tuo programma di sicurezza

La tecnologia è fondamentale per la protezione contro le minacce, ma un approccio moderno deve anche tenere conto di persone e processi. Con le giuste competenze, soluzioni ottimizzate e una cultura di sicurezza solida, le aziende possono adattarsi a un panorama delle minacce in costante evoluzione.

Combinando i servizi Premium di Proofpoint con le soluzioni di Proofpoint, ottieni accesso a un team di esperti che ti aiuta a implementare e gestire una strategia di protezione contro le minacce completa e incentrata sulle persone. Dai consigli alla gestione pratica di sistemi e programmi, il team dei servizi Premium di Proofpoint ti permette di rafforzare la tua sicurezza e accelerare la valorizzazione.

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 l'85% 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.

Seguici: X | LinkedIn | Facebook | YouTube

Proofpoint è un marchio registrato di Proofpoint, Inc. negli Stati Uniti e/o negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari. ©Proofpoint, Inc. 2025

SCOPRI LA PIATTAFORMA PROOFPOINT →