proofpoint.

PANORAMICA SULLA SOLUZIONE

Proofpoint Collaboration Security Prime

Protezione contro gli attacchi ottimizzati dall'IA rivolti all'email e altri canali

Vantaggi principali

- Blocca la più ampia gamma di minacce con un'efficacia del 99,999%
- Estende la protezione agli utenti tramite email e su altri canali
- Rafforza la resilienza degli utenti grazie a informazioni e consigli basati sui rischi
- Riduce l'impatto delle violazioni degli account interni e dei fornitori
- Semplifica le operazioni grazie a una piattaforma unificata che automatizza i flussi di lavoro
- Elimina i costi e la complessità delle soluzioni frammentate grazie al consolidamento

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a proteggere persone e dati nell'ambiente di lavoro agentico.

Panoramica

Con l'ingresso nell'era dell'IA agentica, le aziende adottano strumenti e assistenti ottimizzati dall'IA per aiutare i loro collaboratori a lavorare in modo più efficace. Questi agenti IA diventano parte integrante della forza lavoro estesa, interagendo con collaboratori, applicazioni e altri agenti tramite email, piattaforme di messaggistica, applicazioni cloud e altro ancora. Con l'espansione dell'area di lavoro, aumenta anche la superficie d'attacco e i criminali informatici non hanno tardato a sfruttare questi canali di comunicazione affidabili.

In risposta, numerose aziende sono costrette ad adottare un approccio frammentato alla sicurezza, basato su prodotti isolati. Ciò crea ulteriori lacune nelle loro difese, isola i team e aumenta la complessità operativa.

Per difendersi dagli attacchi su larga scala ottimizzati dall'IA, che si verificano su più canali e in diverse fasi, nonché per proteggere le interazioni affidabili - che si tratti di interazioni tra esseri umani, tra esseri umani e assistenti IA, o tra esseri umani e applicazioni cloud - le aziende hanno bisogno di un approccio più completo. Proofpoint Collaboration Security Prime può aiutarle. Proofpoint Prime unifica rilevamento e neutralizzazione delle minacce nell'intero ambiente di lavoro agentico.

In questo modo puoi:

- Proteggerti dagli attacchi multicanale in più fasi con una precisione senza pari
- Ridurre al minimo l'impatto delle violazioni degli account interni e dei fornitori
- Proteggere le comunicazioni aziendali di fiducia con fornitori, partner e clienti
- Rafforzare la resilienza umana con una formazione mirata incentrata sui rischi e sulle persone
- Ottimizzare le operazioni di sicurezza attraverso l'automazione

Protezione delle persone tutti i canali di collaborazione, inclusa l'email

Con il progredire della migrazione verso spazi di lavoro più connessi e assistiti dall'IA, Proofpoint Collaboration Security Prime protegge i collaboratori ovunque lavorino. Blocca gli attacchi multicanale tramite email e strumenti di collaborazione e messaggistica, come Microsoft Teams, Slack, i social media e le applicazioni cloud, senza interferire con i metodi di lavoro.

Proofpoint Prime protegge i collaboratori in questo ambiente di lavoro esteso contro un'ampia gamma di minacce, tra cui:

- Phishing avanzato
- Violazione dell'email aziendale (BEC)
- Attacchi tramite telefonate (TOAD)
- Invio in massa di email
- Ransomware
- Takeover degli account
- Attacchi generati dall'IA e tecniche di exploit dell'IA, come l'iniezione di prompt

Inoltre, blocca gli attacchi in tutte le fasi del ciclo di vita delle minacce: prima della consegna, dopo la consegna, al momento del clic al momento dell'accesso.

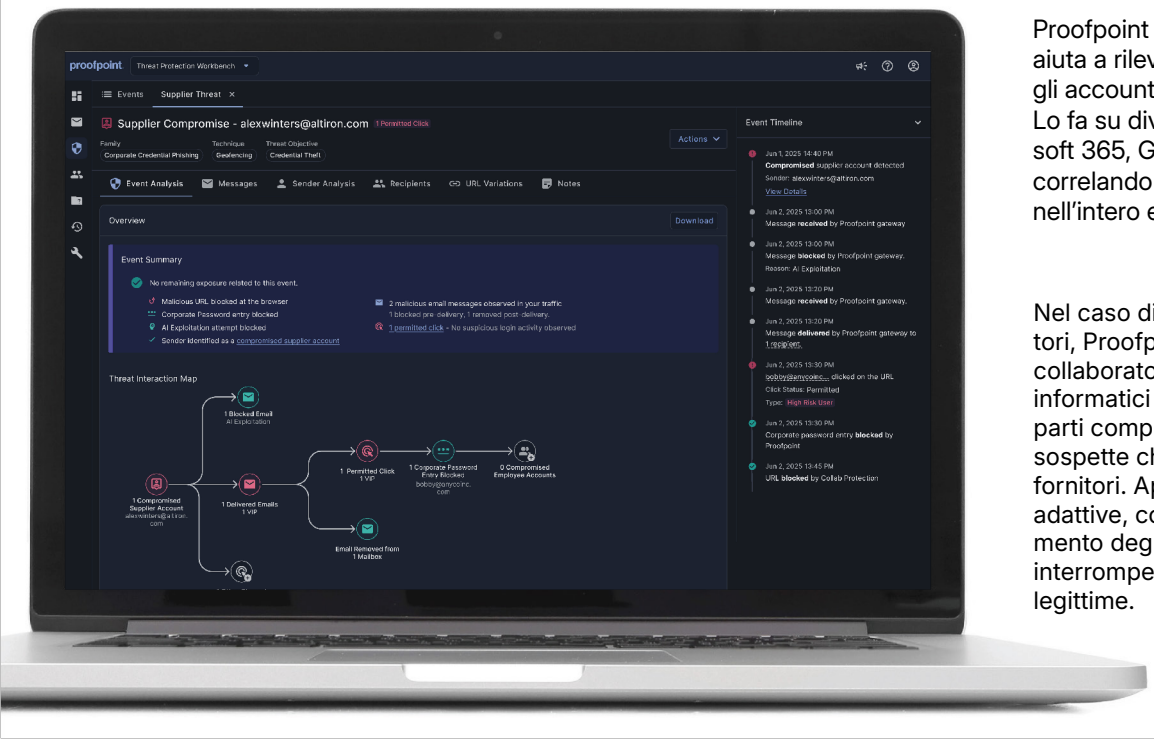

Figura 1. Proofpoint Collaboration Security Prime blocca e correla le minacce a livello di email, messaggistica e collaborazione, cloud e canali dei fornitori.

Alimentato dalla nostra tecnologia Proofpoint Nexus® AI, Proofpoint Prime offre una protezione senza pari contro le minacce con un'efficacia del 99,999%. Combina la nostra ricca threat intelligence, modelli linguistici avanzati, grafici delle relazioni, machine learning, analisi comportamentale e computer vision. Tutte queste tecnologie lavorano di concerto per rilevare e bloccare le minacce prima che causino danni.

I modelli Nexus® AI sono addestrati con uno dei set di dati più vasti e diversificati del settore della sicurezza informatica.

Protezione contro la violazione degli account

I criminali informatici utilizzano identità compromesse per accedere ad account legittimi e lanciare attacchi in più fasi. Sfruttano gli account compromessi dei tuoi collaboratori e dei tuoi fornitori di fiducia. In un ambiente di lavoro guidato dalla collaborazione e assistito da agenti, è fondamentale ridurre al minimo l'impatto di queste minacce.

Proofpoint Collaboration Security Prime ti aiuta a rilevare, analizzare e neutralizzare gli account dei collaboratori compromessi. Lo fa su diverse piattaforme come Microsoft 365, Google Workspace, Okta, ecc., correlando i segnali di identità e di attività nell'intero ecosistema Proofpoint.

Nel caso di minacce provenienti dai fornitori, Proofpoint Prime impedisce che i tuoi collaboratori vengano sfruttati da criminali informatici che utilizzano account di terze parti compromessi. Identifica le attività sospette che provengono da account di fornitori. Applica inoltre misure di protezione adattive, come segnali di allarme e isolamento degli URL, per ridurre i rischi senza interrompere le comunicazioni aziendali legittime.

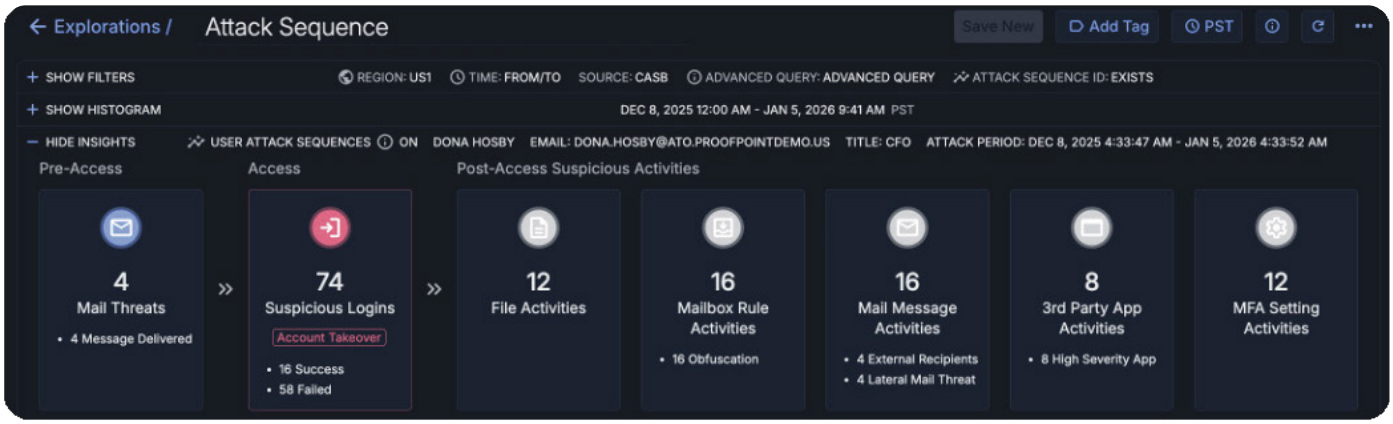

Figura 2. Proofpoint Collaboration Security Prime offre visibilità sulle sequenze di attacco e automatizza il

Protezione delle tue comunicazioni aziendali affidabili

I criminali informatici spesso utilizzano tattiche di furto dell'identità per inserirsi in comunicazioni aziendali affidabili. Il furto d'identità della tua azienda - attraverso lo spoofing diretto dei domini o la registrazione di domini fotocopia - mette i tuoi collaboratori, i tuoi clienti e i tuoi partner in pericolo e può causare gravi danni al tuo marchio.

Proofpoint Collaboration Security Prime può aiutarti a ridurre in modo proattivo questi rischi di furto d'identità. Ti offre una visibilità completa su tutte le email in uscita inviate utilizzando i tuoi domini di fiducia, incluse quelle inviate da terze parti. Hai accesso non solo a potenti strumenti, ma anche a consulenti esperti che ti guideranno attraverso ogni fase dell'implementazione dell'autenticazione delle email. Ciò ti aiuta a conseguire la piena conformità DMARC e a impedire ai criminali informatici di violare i tuoi domini.

La nostra protezione va oltre le email generate dagli utenti e include un ambiente dedicato sicuro per l'inoltro di messaggi generati dalle applicazioni e le email inviate da fornitori SaaS terzi per tuo conto.

Proofpoint Prime fornisce inoltre funzionalità avanzate di rilevamento di domini fotocopia. Monitora Internet in modo dinamico alla ricerca di domini che assomigliano molto ai tuoi. Fornisce anche informazioni dettagliate sulla loro registrazione e sul loro possibile uso improprio.

Non ci limitiamo al rilevamento. Possiamo operare per tuo conto per smantellare i domini e gli URL dannosi grazie alle nostre solide relazioni con gli enti di registrazione, fornitori di servizi di hosting e di domini di primo livello. I nostri professionisti gestiscono l'intero processo, permettendo ai tuoi team di concentrarsi sulle operazioni aziendali strategiche.

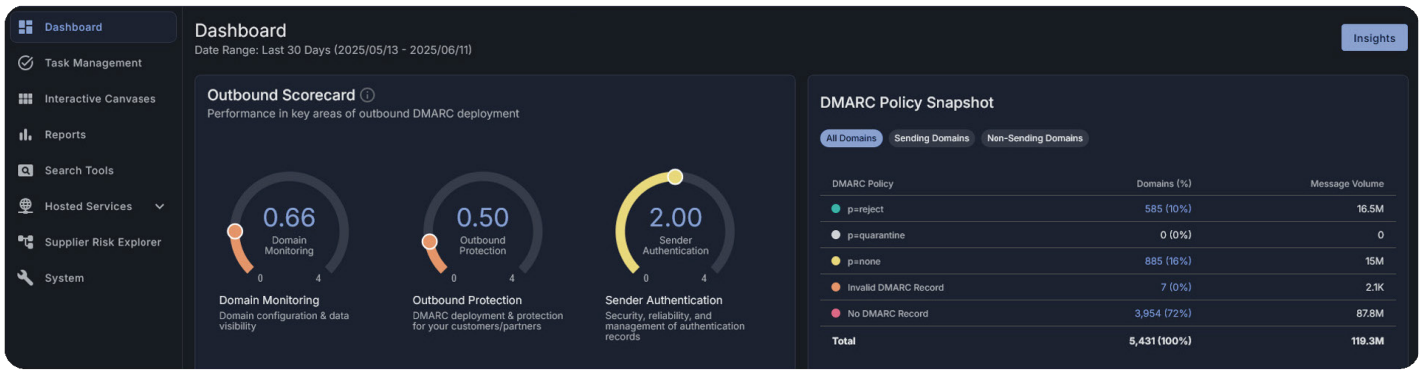

Figura 3. Proofpoint Collaboration Security Prime offre visibilità sulle minacce di furto d'identità, come lo spoofing del dominio e i domini fotocopia dannosi.

Rafforzamento della resilienza degli utenti grazie a consigli basati sui rischi

Con il lavoro che diventa sempre più collaborativo e dinamico, è fondamentale che i collaboratori dimostrino una maggior resilienza nei confronti degli attacchi informatici. Perciò è necessario andare oltre una formazione incentra sulla conformità per includere la gestione dei rischi legati agli utenti — una

Proofpoint Collaboration Security Prime aiuta la tua azienda a compiere questo cambiamento incoraggiando i tuoi collaboratori a compiere scelte più sicure. Fornisce una formazione automatizzata, mirata e basata sui rischi legati alle persone, personalizzato in base al comportamento, al ruolo, all'esposizione agli attacchi e al profilo di rischio unico di ciascun utente. Grazie all'IA, Proofpoint Prime converte le minacce del mondo reale in simulazioni istantanee con un solo clic. La formazione è così allineata ai segnali di rischio attivi per promuovere cambiamenti di comportamento misurabili e duraturi.

I moduli di apprendimento non solo si adattano ai singoli segnali di rischio, ma sono erogati attraverso esperienze di apprendimento ludiche e coinvolgenti. Questo incentiva la partecipazione degli utenti e consolida nel tempo comportamenti più sicuri. Gli utenti possono seguire facilmente i loro progressi tramite una dashboard intuitiva, che li tiene informati e garantisce che si assumano le loro responsabilità.

Allo stesso tempo, gli amministratori possono facilmente personalizzare i programmi per allinearli alle priorità in termini rischi dell'azienda. I risultati parlano da soli: maggiore coinvolgimento, cambiamento dei comportamenti misurabile e cultura della sicurezza più solida nella tua azienda.

Figura 4. Proofpoint Collaboration Security Prime fornisce visibilità sul comportamento reale degli utenti, che permette di fornire formazione mirata e basata sui rischi.

Semplificazione delle operazioni di sicurezza

Con l'estendersi delle minacce oltre le email per colpire strumenti di collaborazione, piattaforme cloud ed ecosistemi dei fornitori, i team della sicurezza sono chiamati a fare sempre di più con meno risorse. In questo contesto, soluzioni isolate scollegate non facilitano loro il compito. Non solo aumentano la complessità, ma rallentano anche i tempi di risposta e aumentano i costi operativi. Tutto ciò rende più difficile ridurre i rischi su larga scala.

Proofpoint Collaboration Security Prime semplifica le operazioni di sicurezza unificando il rilevamento e l'analisi delle minacce e automatizzando i flussi di lavoro e la risposta. Grazie a integrazioni native, Threat Protection Workbench utilizza integrazioni native per riunire informazioni relative al rilevamento e analisi dettagliate degli attacchi provenienti da email, messaggi, piattaforme di collaborazione, account cloud ed ecosistemi dei fornitori. I team possono così indagare sugli incidenti e intraprendere azioni decisive, il tutto da un unico spazio di lavoro unificato per la massima efficienza.

Proofpoint Prime aiuta inoltre i team a stabilire le priorità in modo efficace. La Threat Interaction Map correla le minacce e gli eventi di sicurezza nei punti di controllo e fornisce una mappa visiva dei percorsi di attacco. Questo consente agli analisti di identificare rapidamente gli incidenti più critici. In parallelo, ispeziona automaticamente i messaggi segnalati dagli utenti, neutralizza i contenuti dannosi e fornisce un feedback agli utenti. Ciò permette di ridurre gli interventi manuali e di rafforzare i comportamenti sicuri degli utenti.

Il risultato? Una risposta più rapida e una minore complessità operativa. Inoltre, il tuo team della sicurezza può fare di più con meno, senza sacrificare la protezione.

Scelta del giusto livello di protezione

Proofpoint Collaboration Security Prime è disponibile in diversi livelli, consentendoti di scegliere una protezione in base al profilo di rischio e alle esigenze operative della tua azienda. Ogni livello si base su quello precedente. La copertura va dalle minacce email di base ai canali di collaborazione, alla violazione degli account, alla riduzione dei rischi legati alle persone fino alla protezione avanzata del marchio.

Scopri le funzionalità disponibili nella pagina seguente.

	Funzionalità disponibili	Proofpoint Core Email Protection	Proofpoint Collaboration Security Tier 2	Proofpoint Collaboration Security Tier 3	Proofpoint Collaboration Security Prime
Sicurezza dell'email	Protezione contro attacchi BEC, phishing, phishing di callback e malware	●	●	●	●
	Stack di rilevamento multilivello ottimizzato da Nexus AI	●	●	●	●
	Dati senza pari sulle minacce provenienti da oltre 2,8 milioni di clienti	●	●	●	●
	Sandboxing di allegati e URL	●	●	●	●
	Riscrittura di URL e sandboxing al momento del clic	SEG	SEG	SEG	SEG
	Isolamento dei clic sospetti sugli URL riscritti	VAP*	Tutti gli utenti*	Tutti gli utenti*	Tutti gli utenti*
	Antispam e rilevamento di graymail	●	●	●	●
	Visualizzazione di avvisi contestuali per le email sospette	●	●	●	●
	Strumenti adattivi di integrità dell'email con apprendimento automatico in base al comportamento degli utenti	●	●	●	●
	Policy di instradamento delle email configurabili	SEG	SEG	SEG	SEG
	Correzione automatica dei messaggi	●	●	●	●
	Automazione della casella di posta per gli abusi	●	●	●	●
	Persone più attaccate (VAP)™, criminali informatici e threat intelligence mondiale	●	●	●	●
Protezione contro le minacce multicanale e in più fasi	Rilevamento e correzione degli account cloud compromessi		●	●	●
	Blocco degli URL dannosi inviati tramite applicazioni di messaggistica e collaborazione		●	●	●
	Protezione contro gli account fornitori compromessi		●	●	●
Resilienza umana e sensibilizzazione alla sicurezza informatica	Automazione della formazione basata sul livello di rischio			●	●
	Rafforzamento della sensibilizzazione dei collaboratori tramite simulazioni basate su minacce reali			●	●
	Conversione delle minacce attive in simulazioni sicure			●	●
Protezione contro il furto d'identità	Prevenzione degli usi impropri del marchio tramite l'autenticazione delle email				●
	Rilevamento e neutralizzazione dei domini fotocopia dannosi				●
	Relay sicuro delle email generate dalle applicazioni (250 GB)				●

SEG = distribuzione solo di un gateway email sicuro

***Disponibile solo per implementazioni SEG.