SICUREZZA INCENTRATA SULLE PERSONE

Un moltiplicatore di forze nelle architetture di sicurezza informatica moderne

Perché una sicurezza incentrata sulle persone è un elemento essenziale di qualsiasi strategia di difesa moderna, che si adatta ai tuoi investimenti in sicurezza informatica esistenti, vi si collega e li ottimizza.

proofpoint®

Sintesi

Una responsabilità chiave dei CISO moderni è stabilire gli investimenti strategici da effettuare nell'architettura di sicurezza informatica della loro azienda. Ci sono anche alcuni pilastri di sicurezza ben noti - come il SASE (Secure Access Service Edge), il rilevamento e risposta avanzata agli incidenti (XDR) e l'identità - che devono essere al centro della strategia di difesa di un'azienda. Questi pilastri non possono funzionare in modo indipendente, ma devono operare di concerto per assicurare che l'architettura sia pronta per affrontare le minacce attuali e future che prendono di mira l'azienda. Sebbene ciascuno di questi pilastri sia un componente fondamentale di ogni strategia di difesa, nessuno tiene conto della minaccia più grande di tutte: le persone e le loro azioni.

Una sicurezza incentrata sulle persone permette di chiudere il cerchio: dalla casella email all'endpoint, dall'identità alle minacce interne. Di fatto, dietro ogni violazione si nasconde una persona negligente, malintenzionata o il cui account è stato compromesso.

Questo white paper spiega perché una sicurezza incentrata sulle persone è un l'elemento essenziale, e trasformazionale, delle architetture di sicurezza informatica moderne.

Questo white paper:

- **Spiega il ruolo cruciale della sicurezza incentrata sulle persone** nella tua architettura complessiva, eliminando i punti ciechi nella protezione esistente e rilevando i rischi legati agli utenti negli attuali ambienti di lavoro digitale.
- **Presenta la piattaforma Human-Centric Security di Proofpoint.** Questo white paper descrive come Proofpoint funge da piano di controllo strategico ottimizzando i tuoi investimenti in sicurezza e proteggendo la tua azienda dalle minacce incentrate sulle persone.

Oltre i perimetri e i prodotti isolati: la falla

Numerosi CISO continuano a contrastare le minacce moderne con modelli di vecchia generazione, ovvero controlli compartimentati, informazioni frammentate e strumenti che non sono in grado di adattarsi abbastanza velocemente. Inoltre, la superficie d'attacco è cambiata e altrettanto deve fare la nostra risposta.

La nuova realtà è la seguente: i criminali informatici oggi prendono di mira le persone e non le porte. Con l'ampliamento degli ambienti di lavoro digitali, i criminali informatici prendono di mire le persone attraverso l'email e diversi altri canali digitali, tra cui strumenti di messaggistica e collaborazione, piattaforme dei social media, applicazioni cloud, modelli linguistici di grandi dimensioni (LLM) e servizi di condivisione di file. I criminali informatici possono anche violare comunicazioni aziendali affidabili, danneggiando le relazioni con fornitori e clienti.

Allo stesso tempo, le perdite di dati non avvengono per magia. Dietro ogni incidente si nascondono delle azioni umane. Gli utenti negligenti gestiscono in modo inadeguato dati sensibili o critici. Gli utenti malintenzionati li portano con loro.

Gli hacker violano gli account utente per rubarli. I collaboratori che rifiutano le regole ne fanno un uso improprio.

Anche se scegliere i migliori strumenti è importante, i CISO devono anche focalizzarsi sulla creazione di un'architettura coesa e intelligente, che evolva con il panorama delle minacce e assicuri che questi strumenti lavorino insieme per offrire una difesa efficace.

Proofpoint ha creato qualcosa di unico nel settore: una piattaforma completa di sicurezza incentrata sulle persone che funge da moltiplicatore di forze, ottimizzando i tuoi investimenti in sicurezza a livello di email, identità, dati e accessi.

Non ci limitiamo a colmare le lacune della sicurezza. Attraverso le strette integrazioni con partner come CrowdStrike, Okta, Zscaler, Microsoft, Palo Alto Networks e altri, riduciamo il tempo di permanenza dei criminali informatici, neutralizziamo ancor prima gli attacchi e alleggeriamo il carico di lavoro del tuo team della sicurezza.

Se utilizzi solo la nostra soluzione di protezione dell'email, non conosci ancora tutti i nostri punti di forza. Scopri la nostra piattaforma.

proofpoint.

I pilastri fondamentali di un'architettura di sicurezza informatica moderna

Tutti i CISO li conoscono. Sono i noti pilastri fondamentali di un'architettura di sicurezza informatica moderna: **SASE, XDR, identità nonché SecOps e automazione.** Come descritto di seguito, ciascuno di questi pilastri è essenziale e risolve un'importante gamma di preoccupazioni legati ai rischi. Tuttavia, nessuno di loro tiene conto del rischio più grande nell'attuale panorama della sicurezza: le persone. **Questo è il motivo per cui una sicurezza incentrata sulle persone rappresenta oggi il pilastro più importante di tutti.**

SecOps e automazione Razionalizzano il rilevamento, l'analisi e la neutralizzazione delle minacce eliminando le attività manuali e i flussi di lavoro compartimentati. Riducono i tempi di risposta, il calo di concentrazione a fronte di un elevato numero di allarmi e le inefficienze operative. Proofpoint automatizza la prioritizzazione delle minacce e l'applicazione delle policy grazie a strategie integrate, informazioni arricchite sui rischi legati agli utenti e API flessibili. Ciò permette ai team del centro delle operazioni di sicurezza (SOC) di agire più rapidamente e con maggior precisione.

SASE

Offre un accesso sicuro e ottimizzato a applicazioni e dati, indipendentemente dalla posizione o dal dispositivo dell'utente. Si occupa della forza lavoro distribuita, dell'accesso al cloud e dell'applicazione coerente di policy negli ambienti remoti. Quando viene alimentato con segnali di rischio incentrati sulle persone, il SASE può dare priorità alla protezione per gli utenti o i comportamenti a alto rischio.

Sicurezza incentrata sulle persone

Pone le persone al centro della protezione tenendo conto del fatto che oggi sono gli utenti, e non l'infrastruttura, gli obiettivi principali delle minacce informatiche. La piattaforma Human-Centric Security di Proofpoint contrasta gli attacchi di phishing, la perdita di dati e le violazioni degli account combinando il rilevamento delle minacce basato sull'IA con formazione in tempo reale degli utenti. Per ridurre i rischi incentrati sulle persone, le nostre tecnologie Nexus e Zen identificano in modo unico e preciso gli utenti, i comportamenti e le esposizioni ai rischi.

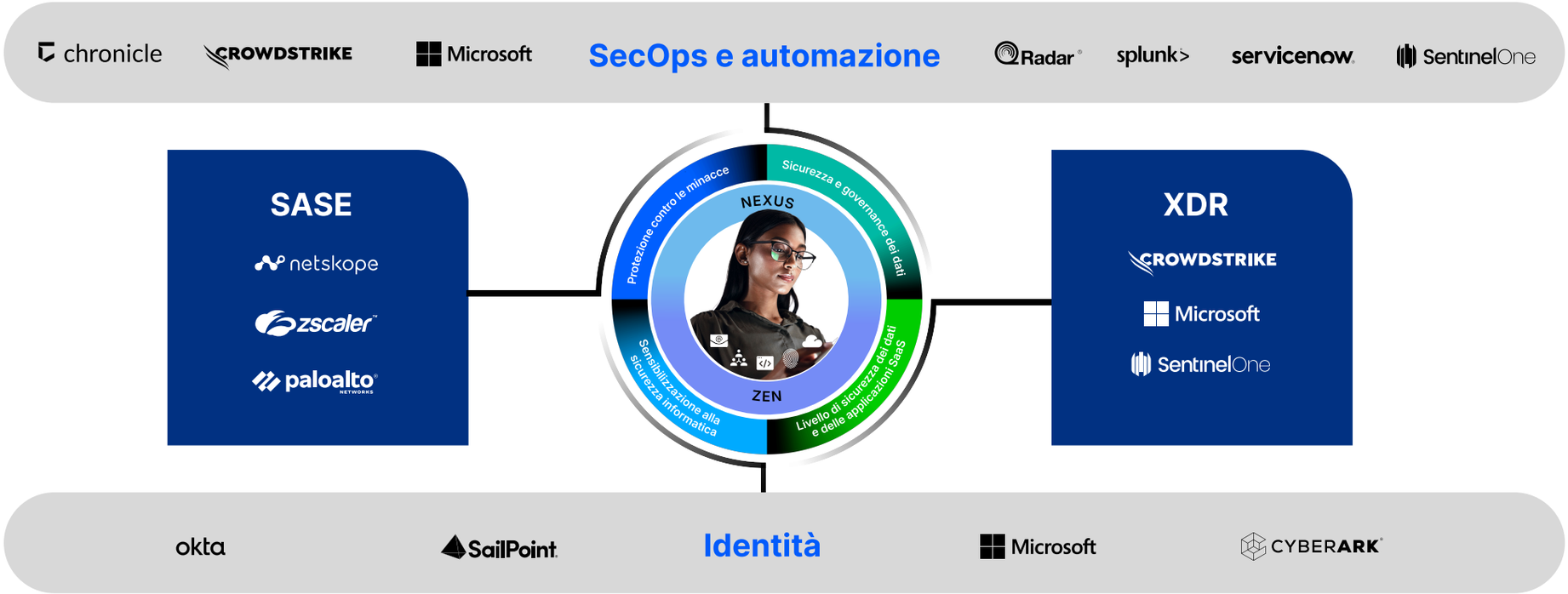
XDR

Unifica i dati di telemetria a livello di email, endpoint, cloud e reti per razionalizzare il rilevamento delle minacce, le analisi e la neutralizzazione delle minacce. Riduce i problemi di silos di visibilità e di tempi di risposta lunghi. I dati di telemetria incentrati sulle persone di Proofpoint, ovvero le informazioni sulle persone prese di mira e a rischio, possono ottimizzare l'XDR grazie a informazioni contestuali anticipate e fruibili.

Identità Protegge le identità e gli accessi degli utenti a livello di cloud e in ambienti on premise rilevando il takeover degli account, l'utilizzo improprio delle credenziali d'accesso e gli errori di configurazione delle applicazioni SaaS. Riduce i rischi di attacchi contro le identità e di accesso non autorizzato grazie al monitoraggio continuo delle autorizzazioni, ai comportamenti di collegamento e alle configurazioni di applicazioni a rischio. Grazie alla visibilità di Proofpoint su chi ha accesso a quali risorse e perché, i team della sicurezza possono prevenire gli spostamenti laterali e applicare il principio del privilegio minimo.

proofpoint.

La sicurezza incentrata sulle persone, un moltiplicatore di forze



La piattaforma Human-Centric Security di Proofpoint funge da piano di controllo strategico nella tua architettura di sicurezza informatica. Si integra con i tuoi investimenti in sicurezza esistenti fornendo segnali di rischi incentrati sulle persone che migliorano la loro efficacia.

La nostra piattaforma si basa sulla comprensione della classificazione dei dati, dell'intenzione degli utenti e del contesto delle minacce. Utilizza IA, machine learning e threat intelligence in tempo reale per estrarre informazioni rilevanti e permettere di prendere decisioni automatizzate sulle policy.

Ecco alcuni dei molti modi in cui la **piattaforma Human-Centric Security di Proofpoint** si integra con gli altri pilastri della tua architettura per trasformare la tua protezione complessiva:

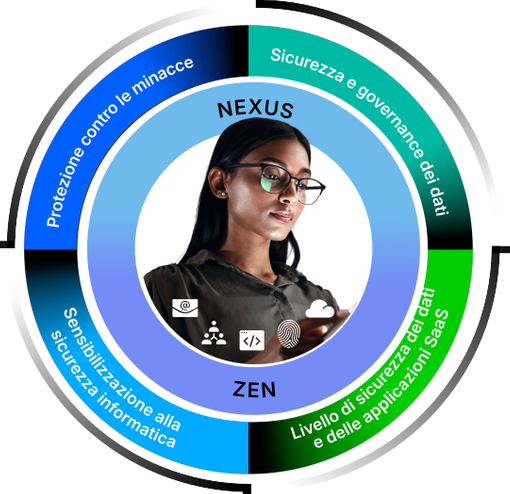
SASE e controlli adattivi degli accessi

In collaborazione con partner come Zscaler e Palo Alto Networks, Proofpoint integra threat intelligence e informazioni sui comportamenti che influenzano le policy d'accesso in tempo reale. Gli utenti interessati sono soggetti a un'autenticazione rafforzata o al blocco dell'accesso tramite Zscaler o Palo Alto Prisma Access. Le attività dannose attivano l'applicazione immediata delle policy.

Si tratta di un'architettura SASE informata da persone, non solo da pacchetti.

Risposta accelerata e automatizzata

Proofpoint si integra con i sistemi di gestione degli eventi e delle informazioni di sicurezza (SIEM) e di risposta agli incidenti di sicurezza (SOAR) per ridurre il tempo medio di rilevamento, analisi e neutralizzazione delle minacce, grazie all'attivazione di avvisi incentrati sulle persone e all'automazione delle azioni di risposta. I segnali di rischi di Proofpoint attivano, in Cortex SOAR o Splunk SOAR, strategie automatizzate che mettono gli utenti in quarantena o reimpostano le credenziali d'accesso. Gli avvisi arricchiti disponibili in Splunk o Microsoft Sentinel riducono i falsi positivi e accelerano la classificazione. I dati sulle minacce e i dati di telemetria sui comportamenti degli utenti di Proofpoint vengono condivisi tra i sistemi per garantire flussi di lavoro unificati.



Un XDR che si applica fin dal punto di ingresso

Il phishing è ancora il principale punto d'ingresso. La nostra collaborazione con CrowdStrike, Microsoft Sentinel e SentinelOne ci permette di chiudere il cerchio. La segnalazione di un'email attiva l'isolamento dell'endpoint in CrowdStrike o SentinelOne in soli pochi secondi, non ore. L'attribuzione di un punteggio di rischio agli utenti e le informazioni contestuali mirati sulle minacce di Proofpoint arricchiscono gli avvisi in Microsoft Sentinel.

Proofpoint fornisce visibilità sul punto d'ingresso, in modo che la tua soluzione XDR goda di informazioni esaustive.

Protezione delle identità e degli accessi con privilegi

Condividiamo il contesto dei rischi con Okta, CyberArk e SailPoint per influenzare dinamicamente il controllo degli accessi. Identifichiamo i tuoi utenti più a rischio e condividiamo tali informazioni con i nostri partner. Un comportamento sospetto? Applichiamo un'autenticazione a più fattori. Un utente ad alto rischio? Applichiamo policy e controlli adattivi. Un account compromesso? Revochiamo l'accesso. Insieme, diamo vita a Zero Trust grazie a un'implementazione adattativa che tiene contro dell'identità.

proofpoint.

Le tue prossime azioni: strategiche, non tattiche

Il punto non è sapere qual è il prossimo strumento da utilizzare, ma è come creare una piattaforma in grado di adattarsi ai tuoi investimenti esistenti, collegarvisi e ottimizzarli.

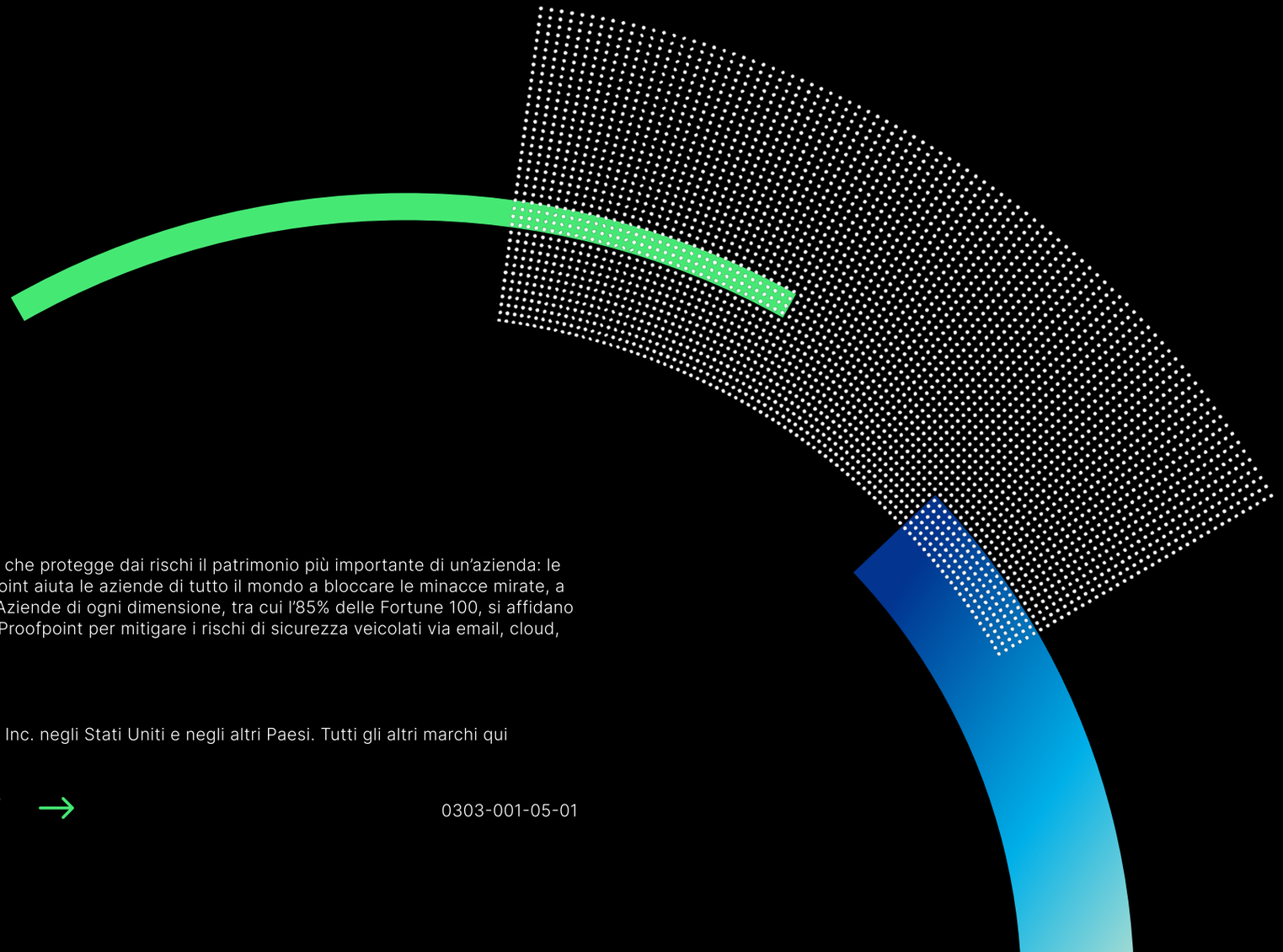
Scopri di più sulle nostre integrazioni

Scopri altri casi d'uso di integrazione tra Proofpoint e altri componenti della tua architettura di sicurezza informatica.
Visita il sito proofpoint.com/use/partners/technology-alliance-partners.

Entra in contatto con Proofpoint

- **Valuta** se la tua architettura di sicurezza è pronta a gestire le minacce incentrate sulle persone.
- **Stabilisci** come i tuoi investimenti esistenti (XDR, SASE e identità) possono essere ottimizzati grazie alle nostre informazioni unificate sui rischi legati agli utenti.
- **Scopri** come si configura una sicurezza basata su una piattaforma e i primi passi per adottarla. Ti mostreremo come convertire informazioni incentrate sulle persone in una sicurezza trasformazionale.

proofpoint.



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: LinkedIn

SCOPRI LA PIATTAFORMA PROOFPOINT →

0303-001-05-01