SICUREZZA INCENTRATA SULLE PERSONE

Adottare una sicurezza incentrata sulle persone nel panorama digitale moderno

Come la piattaforma di protezione multilivello completa di Proofpoint implementa una sicurezza incentrata sulle persone nell'era della trasformazione digitale

proofpoint®

Sintesi

Il panorama digitale moderno ha cambiato sostanzialmente i metodi di lavoro. Le aziende hanno adottato il cloud e i team ora collaborano tramite un insieme di ambienti diversi, tra cui email, strumenti di messaggistica e collaborazione, piattaforme dei social media, applicazioni SaaS, modelli linguistici di grandi dimensioni (LLM), servizi di condivisione di file, ecc.

Questa transizione ha velocizzato l'innovazione e portato una maggior flessibilità. Ma ha anche introdotto numerose nuove superfici d'attacco che i criminali informatici possono sfruttare. Gli operatori della conoscenza ora generano, archiviano e consultano dati in modi che sfuggono alle strategie di sicurezza tradizionali, incentrate sulla protezione delle reti e degli endpoint. Questi cambiamenti richiedono un'architettura moderna allineata al modo in cui le aziende e il personale lavorano. Un'architettura che tenga conto del fatto che oggi sono gli utenti, e non l'infrastruttura, gli obiettivi principali delle minacce informatiche.

Questo white paper si concentra su un importante contributo di Proofpoint a questa nuova realtà: la piattaforma Human-Centric Security, prima nel suo genere in questo settore, che mette le persone al centro della strategia di difesa moderna.

Questo white paper:

- **Spiega perché la protezione delle persone è più importante** che mai nell'attuale ambiente di lavoro digitale
- **Descrive i problemi incentrati sulle persone** che la piattaforma Proofpoint risolve
- **Esamina le principali tecnologie** alla base di un'architettura concepita per rilevare proattivamente le minacce, guidare e proteggere gli utenti in tempo reale e ottimizzare le indagini e la risposta agli incidenti

I collaboratori, il nuovo perimetro di sicurezza: perché la sicurezza incentrata sulle persone è essenziale

L'essere umano è al centro della sfida della sicurezza informatica attuale. Le minacce incentrate sulle persone, tra cui phishing, takeover degli account, rischi interni e sottrazione dei dati, ora rappresentano la maggior parte delle violazioni. La maggior parte degli attacchi moderni non sfrutta perciò le vulnerabilità tecniche, ma il comportamento umano. Che sia attraverso l'inganno, la distrazione o la manipolazione, i criminali informatici prendono di mira gli utenti all'interno di ambienti di lavoro digitali sempre più complessi.

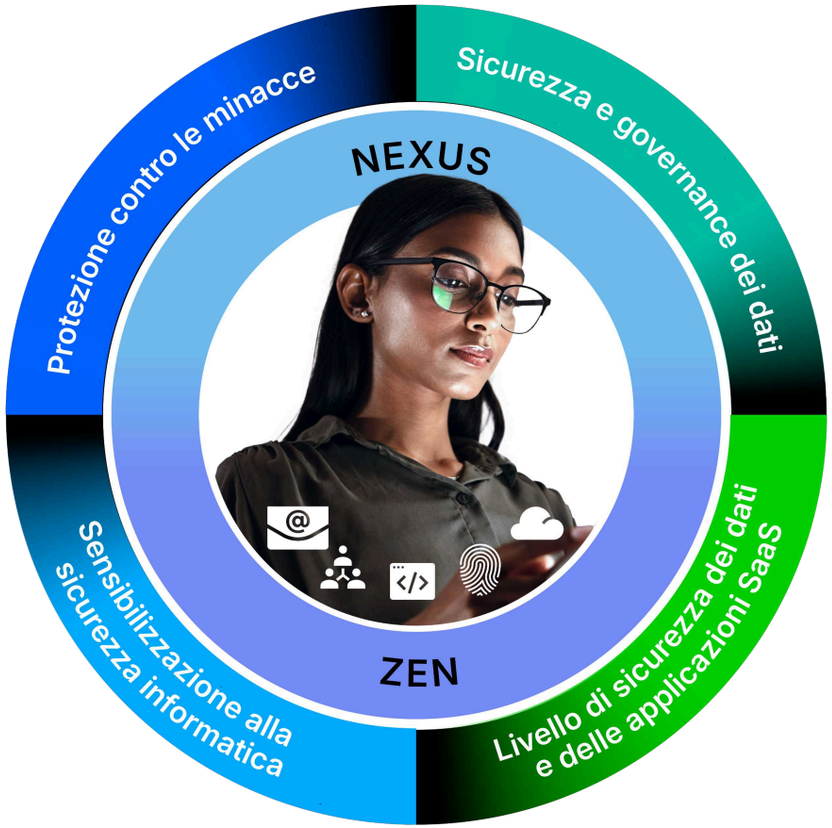
I modelli di sicurezza tradizionali si concentrano sulla protezione di reti e endpoint, ma le minacce moderne prendono di mira le vulnerabilità della natura umana. Grazie alla piattaforma di sicurezza informatica di Proofpoint, le aziende possono proteggere gli utenti e i dati grazie a un approccio incentrato sulle persone. La nostra piattaforma propone soluzioni avanzate per rispondere a quattro problematiche critiche: blocco delle minacce, protezione delle informazioni, sensibilizzazione degli utenti e rafforzamento del livello di sicurezza dei dati e delle applicazioni SaaS.

PROTEZIONE CONTRO LE MINACCE

Blocco delle minacce che prendono di mira i tuoi collaboratori

SENSIBILIZZAZIONE ALLA SICUREZZA INFORMATICA

Formazione continua per i tuoi collaboratori



SICUREZZA E GOVERNANCE DEI DATI

Prevenzione della perdita di dati e governance delle comunicazioni

LIVELLO DI SICUREZZA DEI DATI E DELLE APPLICAZIONI SAAS

Correzione dell'esposizione dei dati e delle applicazioni SaaS

Figura 1. La piattaforma Proofpoint Human-Centric Security offre soluzioni all'avanguardia in quattro aree chiave.

Una piattaforma completa e multilivello

La piattaforma completa di Proofpoint si basa su un'architettura multilivello che:

- **Rileva proattivamente le minacce** nell'intero ambiente di lavoro digitale grazie a funzionalità come l'IA avanzata, il machine learning e la threat intelligence in tempo reale
- **Fornisce un'ampia gamma di punti di controllo a livello dell'utente finale** per proteggere persone e dati, ovunque si trovino
- **Avvisa gli utenti, li guida e gli fornisce gli strumenti appropriati** per assicurare la loro resilienza contro gli attacchi che li prendono di mira
- **Semplifica le indagini e la risposta agli incidenti**

Queste funzionalità si basano su tre tecnologie fondamentali: Proofpoint Nexus, Zen e Threat Protection Workbench. Nelle sezioni seguenti prendiamo in esame queste tecnologie.

Proofpoint Nexus

Rilevamento assistito dall'IA e dalla threat intelligence

Proofpoint Nexus® è il livello di rilevamento dell'architettura Proofpoint. È un framework di rilevamento unificato ottimizzato da IA, machine learning e threat intelligence in tempo reale.

Proofpoint Nexus integra diversi tipi di modelli di IA, ciascuno dei quali è studiato per analizzare segnali di rischio specifici associati alle modalità di lavoro degli utenti, tra cui email, applicazioni cloud, strumenti di collaborazione e browser.

Principali componenti del framework di rilevamento Proofpoint Nexus

Nexus Threat Intelligence (TI) acquisisce continuamente i segnali associati a criminali informatici, campagne e infrastrutture, sia noti che sconosciuti, per fornire alle soluzioni Proofpoint rilevamenti contestualizzati e la capacità di adattarsi all'evoluzione delle tecniche di attacco.

Nexus Language Model (LM) sfrutta la potenza dei modelli linguistici dell'intelligenza artificiale avanzata per valutare il tono, l'enfasi e la struttura linguistica dei messaggi utilizzati negli attacchi di social engineering, come la violazione dell'email aziendale (BEC, Business Email Compromise).

Nexus Relationship Graph (RG) correla l'attività degli utenti, lo storico dei loro comportamenti e il livello di sensibilità del ruolo per valutare la probabilità di comportamenti dannosi o attacchi mirati contro collaboratori ad alto rischio.

Nexus Machine Learning (ML) rileva i comportamenti insoliti dell'utente negli strumenti di comunicazione e collaborazione, identificando segnali sottili ma significativi che rivelano la violazione di account o utilizzi impropri da parte di utenti interni.

Nexus Computer Vision (CV) identifica le tattiche di furto d'identità e di frode visiva analizzando la struttura, il posizionamento dei loghi o l'impaginazione alla ricerca di imitazioni fraudolente. Utilizzando una tecnologia di computer vision avanzata, rileva le minacce nascoste negli elementi visivi, come siti di phishing, codici QR, allegati dannosi e email falsificate.

Proofpoint Nexus rileva gli attacchi di phishing avanzati, il furto delle credenziali, i tentativi di furto d'identità e le campagne di ransomware. A titolo d'esempio, Proofpoint Nexus ha identificato una frode delle fatture rivolta contro un dipartimento finanziario specifico, scaturita dalla violazione di un fornitore. Ha bloccato l'attacco prima che potesse svolgersi identificando incoerenze negli elementi visivi e nel linguaggio utilizzato e basandosi su una threat intelligence globale.

Proofpoint Nexus offre un'eccellente protezione dei dati. In un altro caso reale, Proofpoint Nexus ha rilevato un'attività anomala a livello di dati sensibili quando un collaboratore ha incollato i dati di un cliente in uno strumento di IA generativa non autorizzato: ha alzato il punteggio di rischio e bloccato l'azione.

Nexus analizza più di **2,6 miliardi di email al giorno, analizza oltre 450 milioni di URL quotidianamente** e correla i segnali provenienti da centinaia di criminali informatici. Questo enorme volume di dati rafforza sia l'accuratezza che la reattività nell'intero panorama delle minacce.

proofpoint.

Proofpoint Zen

Punti di controllo e consigli contestuali per gli utenti

Proofpoint Zen™ è il livello di applicazione delle misure di sicurezza e assistenza agli utenti dell'architettura Proofpoint. Applica le policy di sicurezza proprio dove gli utenti svolgono le loro attività. I punti di controllo della suite Proofpoint Zen convertono la threat intelligence in protezione in tempo reale e generano messaggi per gli utenti in linea con le policy definite. Tali avvisi aiutano gli utenti a prendere decisioni più informate senza rallentare la loro produttività.

Principali componenti della suite Proofpoint Zen

Zen for Outlook trasforma gli utenti in difensori in prima linea, integrando gli strumenti di sicurezza nei flussi di lavoro delle email. Utilizzando la threat intelligence in tempo reale di Proofpoint Nexus, la soluzione mostra agli utenti avvisi contestuali quando ricevono email sospette e facilita la segnalazione. Evidenzia intelligentemente i comportamenti a rischio e invia un avviso in caso di presenza di dati sensibili nelle email in uscita.

ZenWeb è un'estensione leggera per i browser Chromium che protegge le attività web sugli strumenti SaaS, di condivisione di file e di IA generativa e protegge gli utenti contro i siti di phishing. Grazie a rilevamenti in diretta basati sui modelli delle minacce di Nexus, ZenWeb rileva e previene le minacce in tempo reale senza impattare sulla produttività dell'utente.

Zen Endpoint DLP/Insider Threat Management assicura la protezione dei dispositivi contro la perdita di dati e le minacce interne monitorando il comportamento degli utenti sull'endpoint. Questo componente monitora l'utilizzo delle porte USB, la clipboard, le operazioni di sincronizzazione di file e il comportamento delle applicazioni. Acquisisce le schermate delle azioni sospette degli utenti e registra la cronologia delle attività dell'utente.

Zen Cloud API Connectors estende la sicurezza alle piattaforme SaaS nel cloud come Microsoft 365, Google Drive, Slack e Box. Monitora il caricamento di file e rileva i comportamenti insoliti come la condivisione eccessiva di file. Consente inoltre di creare flussi di lavoro personalizzati in Okta e negli strumenti di orchestrazione, automazione e risposta della sicurezza (SOAR).

Zen Communications Connectors acquisisce le comunicazioni in piattaforme regolamentate, come Microsoft Teams, Zoom e Slack, per l'archiviazione e la supervisione. Questo componente riceve i messaggi da vari canali e li trasforma in un formato di archiviazione unificato e si integra con strumenti di supervisione dei flussi di lavoro degli uffici legali e delle risorse umane.

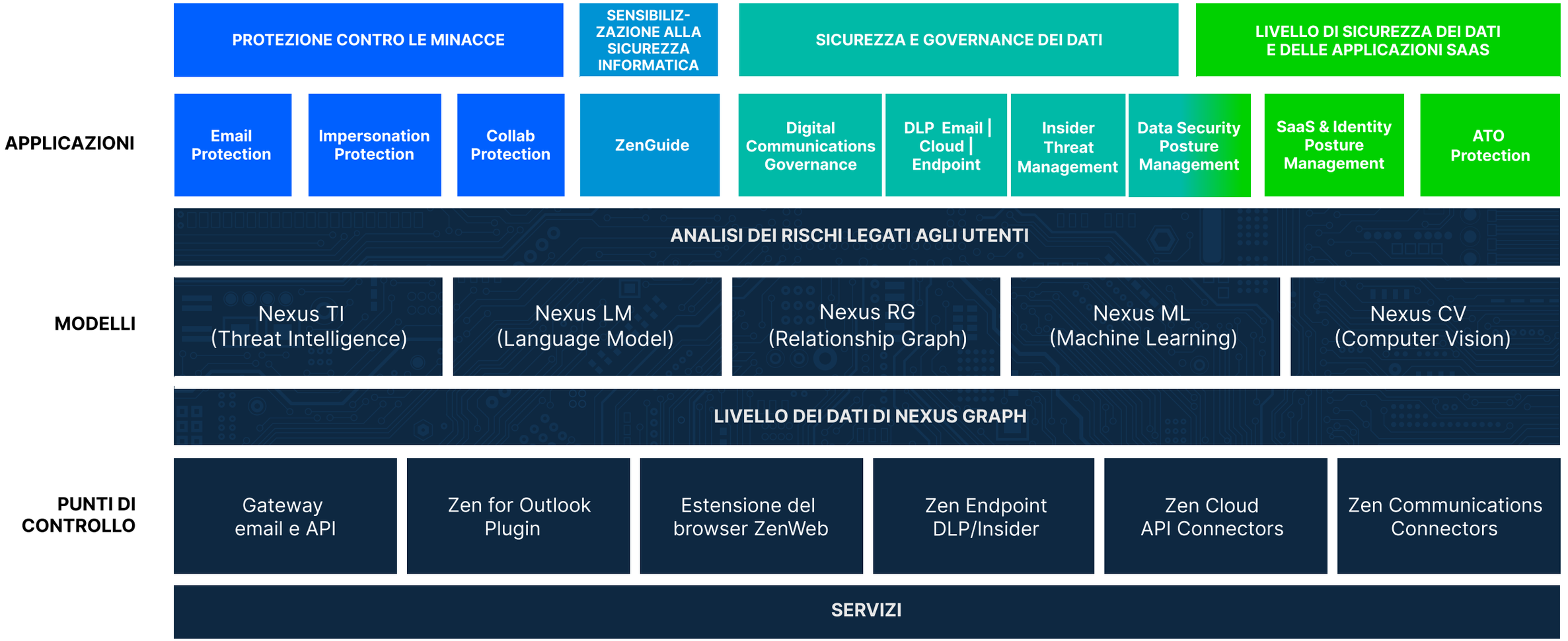


Figura 2. La piattaforma Human-Centric Security di Proofpoint si basa su un'architettura multilivello. Le soluzioni Proofpoint (nelle nostre aree di soluzioni fondamentali che sono la protezione contro le minacce, la sensibilizzazione alla sicurezza informatica, la sicurezza e la governance dei dati e il livello di sicurezza dei dati e delle applicazioni SaaS) utilizzano direttamente le funzionalità delle nostre tecnologie di base Proofpoint Nexus e Proofpoint Zen.

Proofpoint Threat Protection Workbench

Indagini rapide e remediation automatica

Quando viene rilevata una minaccia o viene segnalata una violazione alla policy, velocità e trasparenza diventano un fattore critico. Per i team SOC, molteplici console, un numero eccessivo di clic e la dipendenza da altri team rallentano i tempi di risposta e aumentano il rischio che gli attacchi vadano a buon fine.

Proofpoint Threat Protection Workbench è il livello di indagine e automazione dell'architettura Proofpoint. Fornendo al SOC una console centralizzata intuitiva, semplifica le indagini sulle minacce e le attività di remediation. Consente ai team della sicurezza di classificare, analizzare e rispondere alle minacce senza i ritardi causati dal passare da uno strumento all'altro o dalla frammentazione dei dati.

I team della sicurezza utilizzano Proofpoint Threat Protection Workbench per elaborare le segnalazioni alla casella di posta per gli abusi, scalare i segnali relativi a utenti a alto rischio e esaminare le campagne d'attacco. Correlando la threat intelligence di Proofpoint Nexus con i comportamento degli utenti e gli attivatori delle policy, Proofpoint Threat Protection Workbench genera degli avvisi ad alta fedeltà, limitando i falsi positivi.

Esempi di casi d'uso di Proofpoint Threat Protection Workbench

- Risposte automatiche per le indagini su possibili takeover degli account
- Visualizzazioni della sequenza di clic degli utenti presi di mira dagli attacchi
- Sintesi delle minacce multicanale complesse

Tutte queste funzionalità riducono il carico di lavoro degli analisti e il tempo di permanenza delle minacce. Per rispondere alle minacce, gli analisti possono attivare direttamente l'esecuzione di procedure predefinite o utilizzare API per scalare l'informazione a altri componenti integrati nei loro stack di sicurezza più estesi.

Conclusione

Un’architettura dedicata per una sicurezza incentrata sulle persone

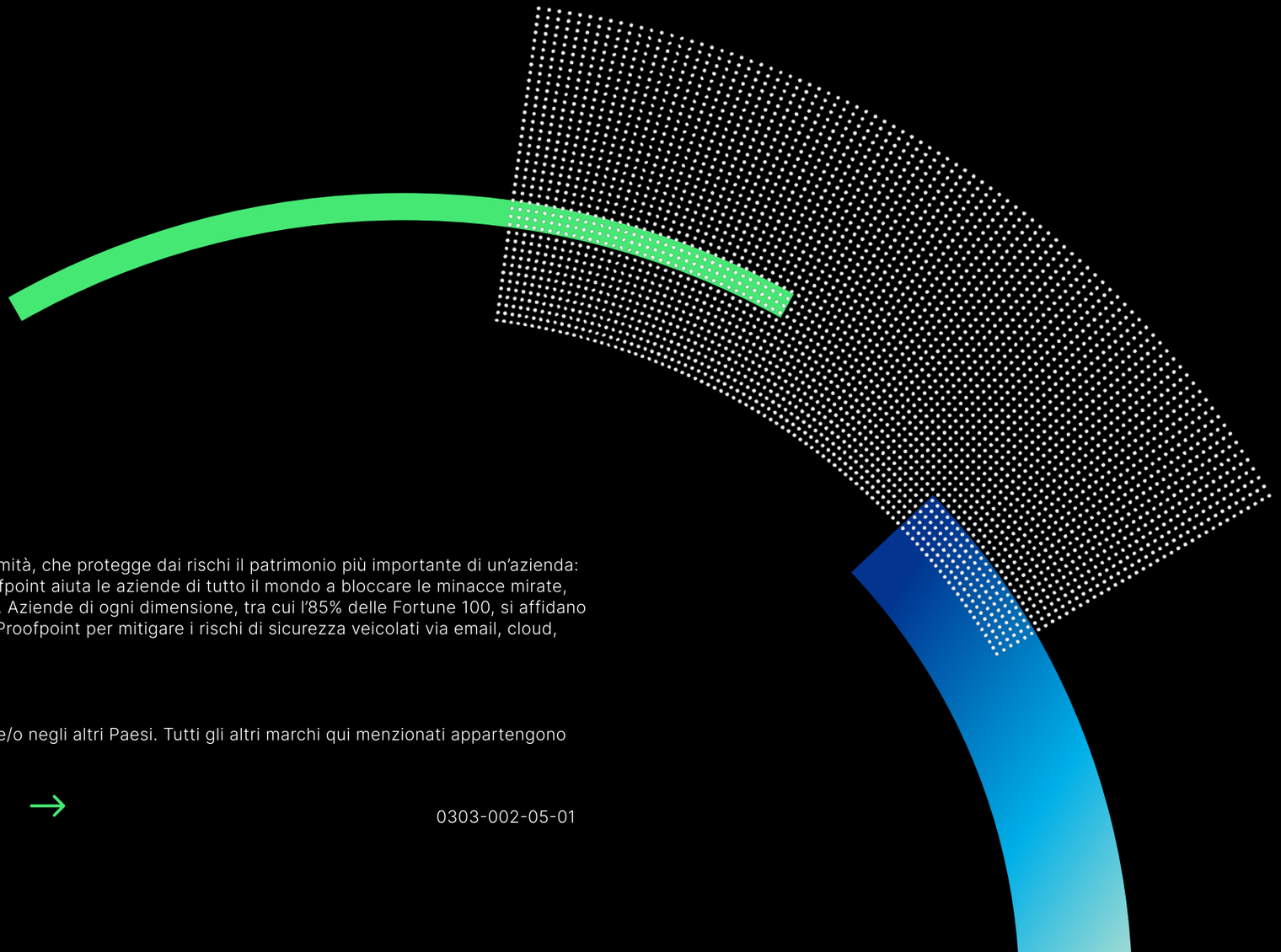
La natura dei rischi informatici è cambiata. Le minacce non prendono più di mira solo i sistemi, colpiscono le persone. La complessità dell’ambiente di lavoro digitale ha superato le difese concepite per proteggerlo. Gli utenti utilizzano ormai indifferentemente email, browser, strumenti di collaborazione e applicazioni cloud, perciò il vecchio approccio alla sicurezza, basato su perimetri statici e soluzioni universali, non è più efficace.

La piattaforma di Proofpoint risolve questa sfida allineando la sua architettura di sicurezza con le nuove modalità di lavoro. Con Proofpoint Nexus, le aziende ottengono una visibilità guidata dall’IA sulle minacce incentrate sulle persone, che si basa su una threat intelligence ineguagliata e l’analisi comportamentale. Con Proofpoint Zen, la nostra piattaforma protegge e consiglia gli utenti in tempo reale, senza attrito. E con Proofpoint Threat Protection Workbench, i team della sicurezza possono reagire più velocemente, con informazioni più chiare e un minor carico operativo.

Non si tratta solo di vantaggi teorici. La nostra piattaforma offre un’architettura comprovata che riduce i rischi e crea una resilienza di lungo periodo. Le aziende possono proteggere i flussi di lavoro attuali e prepararsi per la prossima evoluzione dei rischi incentrati sulle persone.

Combinando rilevamento avanzato, controlli comportamentali incorporati e risposta rapida e integrata, possiamo aiutare la tua azienda a ridurre i rischi dove è più importante: dove si incrociano le persone, i dati e le minacce.

proofpoint.



proofpoint.

Proofpoint, Inc. 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 →

0303-002-05-01