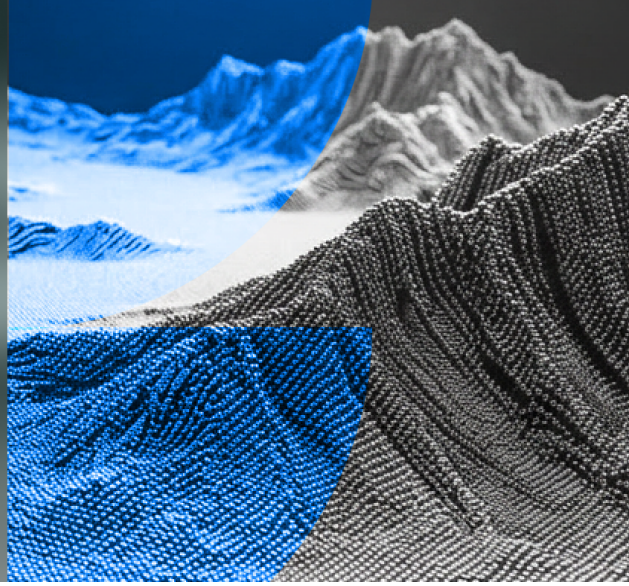
proofpoint.

PANORAMICA SULLA SOLUZIONE

Proofpoint Core Email Protection

Blocca le minacce trasmesse via email ottimizzate dall'IA grazie a una protezione completa e continua lungo l'intero ciclo di vita delle email



Vantaggi principali:

- **Blocco delle minacce trasmesse via email ottimizzate dall'IA prima della consegna**
- **Rilevamento delle minacce con una percentuale di efficacia del 99,999%**
- **Implementazione in 24 ore tramite API o gateway email sicuro**
- **Copertura completa prima della consegna, dopo la consegna e al momento del clic**
- **Threat Protection Workbench unificato per indagini più rapide**
- **Integrazioni con ecosistemi avanzati**

La sfida: le minacce trasmesse via email ottimizzate dall'IA

I criminali informatici lanciano attacchi alla velocità delle macchine. L'IA avanzata ha rimosso i vincoli che un tempo limitavano la rapidità con cui i criminali informatici potevano creare esche di phishing, attacchi BEC (Business Email Compromise) e campagne di social engineering. Una singola campagna genera ora infinite varianti altamente mirate e personalizzate per ogni destinatario.

Queste minacce generate dall'IA arrivano tramite l'email e i canali di collaborazione senza refusi, senza modelli riutilizzati e senza impronte digitali familiari. Le difese tradizionali basate su liste di reputazione e firme statiche non riescono a tenere il passo. Contemporaneamente, il 94% degli attacchi informatici che prendono di mira le persone inizia ancora con un'email[1].

Questi attacchi sfruttano le lacune di sicurezza: protezioni mancanti prima della consegna, punti ciechi nel rilevamento delle violazioni dei fornitori, ambienti cloud e di collaborazione isolati e mancanza di controlli volti a impedire i takeover degli account.

L'IA come moltiplicatore di forza

Attività che richiedevano 16 ore a un criminale informatico ora richiedono solo 5 minuti. Il phishing generato dall'IA produce esche impeccabili e personalizzate, senza errori rivelatori.

Varianti infinite
Ogni esca è diversa

Velocità delle macchine
Creazione di campagne in pochi minuti

Multicanale
Email, voce e video

[1] Fonte: ricerche sulle minacce condotte da Proofpoint

La soluzione: Proofpoint Core Email Protection

Proofpoint Core Email Protection blocca un'ampia gamma di minacce trasmesse via email ottimizzate dall'IA grazie a una protezione completa e continua lungo l'intero ciclo di vita delle email. Implementabile tramite gateway email sicuro o API, offre un'efficacia di rilevamento delle minacce del 99,999%, senza pari nel settore.

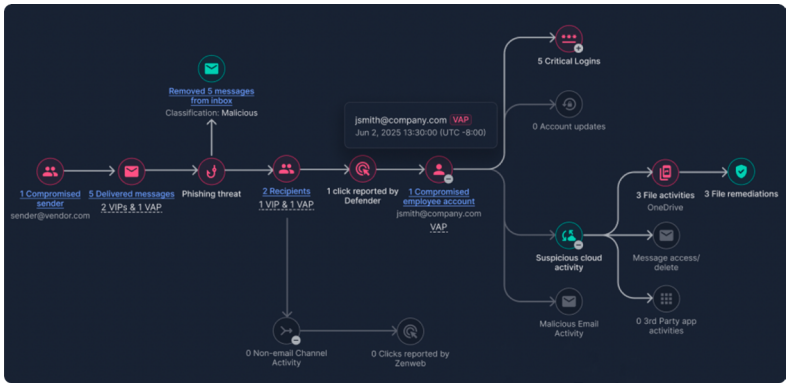


Figura 1. Threat Protection Workbench mappa le minacce end-to-end.

Funzionalità essenziali:

Rilevamento ottimizzato da Proofpoint Nexus AI

Proofpoint Nexus utilizza modelli linguistici, grafici relazionali, machine learning, threat intelligence e computer vision per rilevare un'ampia gamma di minacce avanzate trasmesse via email con rilevamenti basati sull'intento dell'IA.

Proofpoint Nexus AI

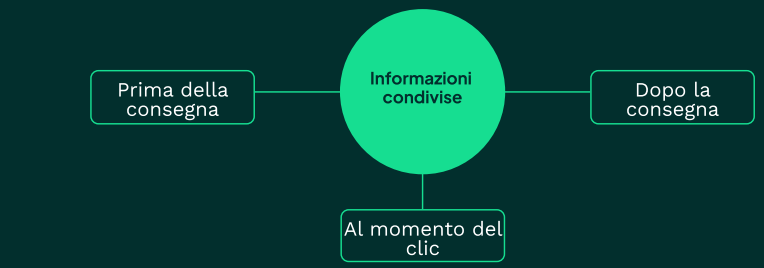
- **LM** — Modelli linguistici
- **GR** — Grafico delle relazioni
- **ML** — Machine Learning
- **IM** — Informazioni sulle minacce
- **CV** — Computer vision

Dati sulle minacce senza eguali

- **2,1 trl** di email
- **20,4 trl** di URL
- **8900** campagne
- **>100** malintenzionati

Protezione completa e continua

Proofpoint Core Email Protection offre una difesa coordinata prima della consegna, dopo la consegna e al momento del clic. Le informazioni vengono condivise tra i controlli in tempo reale, in modo che una minaccia emersa dopo la consegna permetta di affinare la decisione successiva prima della consegna.



Informazioni condivise fra i controlli in tempo reale

Componenti aggiuntivi opzionali:

- Takeover degli account
- Messaggistica
- Fornitore
- Momento dell'accesso

Implementazione unificata basata su gateway email sicuro e API

Proofpoint unifica le sue avanzate implementazioni basate su gateway email sicuro e API in un'unica architettura integrata. Il nostro gateway email sicuro aiuta a bloccare le minacce in entrata e in uscita a livello del gateway email, mentre la nostra protezione basata su API estende la visibilità e la risposta alle minacce via email interne e dopo la consegna.

Un'unica console, un unico flusso di lavoro per le indagini e un unico set di policy sostituiscono la frammentazione operativa associata alla gestione di strumenti separati. Le aziende che scelgono l'implementazione tramite API possono farlo in sole 24 ore, oppure possono scegliere di combinare gateway email sicuro e API per la massima copertura.

Operazioni di sicurezza efficienti

Con il 99,999% delle minacce bloccate automaticamente, i team della sicurezza possono concentrarsi sulle indagini a più alta priorità. Threat Protection Workbench fornisce una ricostruzione visiva, end-to-end, della catena di attacco, collegando messaggi, utenti, clic e azioni correttive in un'unica vista. Flussi di lavoro automatizzati, ricerca integrata e triage basato sugli avvisi riducono il tempo medio di applicazione delle misure correttive.

Impatto operativo

Ecco cosa puoi aspettarti con Proofpoint

Efficacia del rilevamento senza pari

Rilevamento delle minacce con una percentuale di efficacia del 99,999%, con solo un falso positivo ogni 19,7 milioni di messaggi e un falso negativo ogni 5,3 milioni di messaggi.

Valorizzazione più rapida

Le implementazioni tramite API sono operative in 24 ore. Le implementazioni che combinano gateway email sicuro e API offrono una difesa in profondità.

Riduzione del carico di lavoro del SOC

I flussi di lavoro automatici e le indagini visive della catena di attacco riducono il tempo dedicato dagli analisti alla correlazione manuale.

Copertura più ampia delle minacce

Ottieni una protezione contro le minacce esterne, le violazioni dopo la consegna, il phishing interno e gli invii diretti.

Architettura a prova di futuro

Una piattaforma integrata offre protezione automatica contro le nuove minacce rilevate e i criminali informatici emergenti.

Integrazioni avanzate

Integrazioni con gli ecosistemi CrowdStrike, Okta, Palo Alto Networks, Microsoft Defender, Splunk e Sentinel.

Per saperne di più, visita il sito **proofpoint.com/it**

proofpoint.