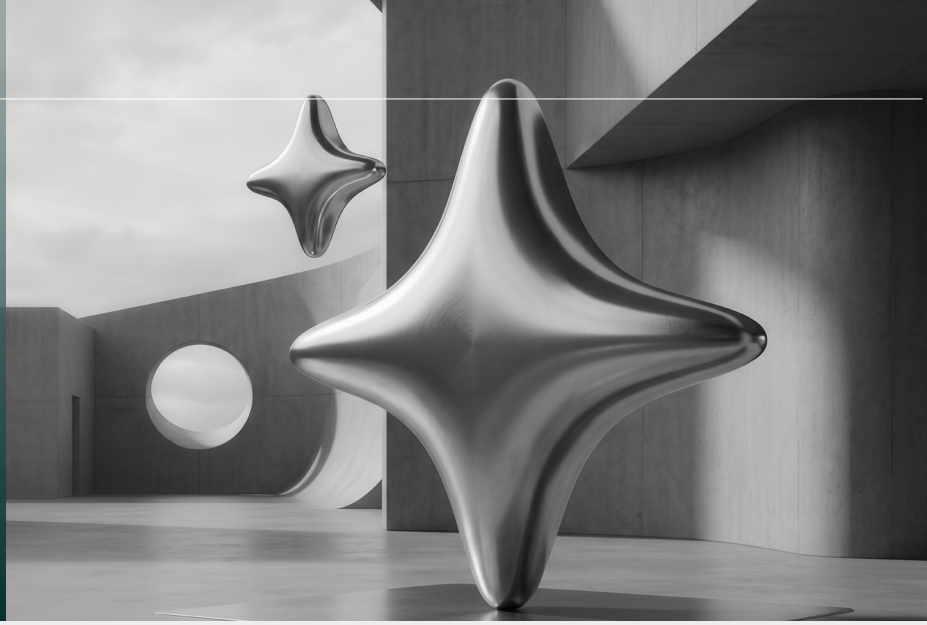
proofpoint.



PANORAMICA SULLA SOLUZIONE

L'IA in Proofpoint

L'IA offre nuove e innovative soluzioni per aiutare le persone a svolgere il proprio lavoro. Allo stesso tempo però, l'IA aiuta anche i malintenzionati a incrementare la propria produttività. Le loro tattiche, tecniche e procedure (TTP) sono oggi rafforzate dall'IA, che consente di condurre attacchi su più canali e in più fasi su scala mondiale. Queste minacce spesso eludono le tradizionali difese di sicurezza e sono più difficili da rilevare per gli utenti.

Tuttavia, i rischi non sono solo il frutto di attacchi esterni. Le esposizioni di dati derivano sempre più dal comportamento quotidiano degli utenti all'interno dell'azienda. L'IA contribuisce a monitorare il flusso di dati e a identificare i comportamenti a rischio nel contesto. Ciò può ridurre significativamente il carico sui team dei centri delle operazioni di sicurezza (SOC).

Mentre l'impatto dell'IA sul mondo del lavoro continua a evolversi, Proofpoint si conferma all'avanguardia del settore in termini di utilizzo dell'IA per proteggere i suoi clienti. Combinando l'innovazione continua basata sull'IA con una threat intelligence senza pari, le nostre soluzioni superano i criminali informatici, proteggono i dati sensibili e aiutano le aziende a rimanere al sicuro in un mondo sempre più alimentato dall'IA.

Nel 2025 Proofpoint ha osservato un aumento del

94%

del numero di minacce email contro i clienti rispetto all'anno precedente.

Come i criminali informatici utilizzano l'IA per scalare gli attacchi

Proofpoint ha osservato in prima persona le conseguenze dell'IA quando viene utilizzata dai malintenzionati. Nel 2025 ha riscontrato un aumento del 94% nel numero di minacce email contro i propri clienti rispetto all'anno precedente. Ciò significa un panorama delle minacce più sofisticato che include l'iniezione di prompt per l'IA, il bombardamento di email e gli attacchi di abuso di servizi legittimi.

I criminali informatici sfruttano l'IA per guadagnare terreno in diversi modi:

- **Moltiplicatore di forza.** L'IA consente di lanciare attacchi più sofisticati su una superficie d'attacco più ampia. Quest'anno abbiamo osservato migliaia di email volte a indurre gli agenti di IA ad agire per conto dei pirati informatici.
- **Soglia di ingresso più bassa.** L'IA permette di automatizzare l'80-90% della catena di attacco. I criminali informatici dispongono così di più tempo da dedicare ad attacchi più complessi. Abbiamo osservato un aumento degli attacchi in più fasi e su più canali che coinvolgono migliaia di messaggi indesiderati.
- **Targetizzazione avanzata.** Prima dell'IA, per i loro attacchi i malintenzionati si affidavano a modelli prevedibili e generici. Con l'IA possono creare attacchi personalizzati per ogni vittima.

Quest'anno, abbiamo osservato un aumento degli attacchi personalizzati che abusano dei servizi legittimi.

Tutti questi sviluppi hanno reso più difficile l'identificazione accurata delle minacce tramite email.

L'analisi semantica e altri metodi basati su modelli linguistici di grandi dimensioni possono essere d'aiuto.

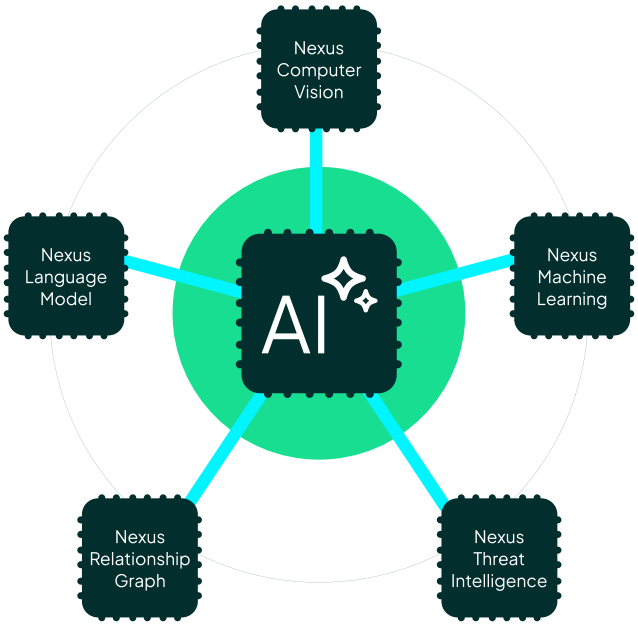
L'IA di Proofpoint Nexus per la sicurezza della collaborazione

Le soluzioni Proofpoint Collaboration Security Prime sfruttano la nostra piattaforma di IA Nexus™ che utilizza un approccio multilivello al rilevamento delle minacce.

Come i criminali informatici utilizzano l'IA per scalare gli attacchi

Nexus è un insieme di motori alimentati dall'IA che operano di concerto per offrire un'efficacia di rilevamento pari al 99,999%. Combina machine learning, computer vision, grafici delle relazioni, threat intelligence e modelli linguistici per rilevare e bloccare con precisione gli attacchi.

I modelli di IA di Proofpoint Nexus elaborano **2100 miliardi di email** all'anno, supportati da un team di threat intelligence che monitora oltre **100 diversi gruppi di malintenzionati** e più di **8900 campagne di minacce**.



Nexus LM™ (Language Model) rileva gli attacchi BEC e le minacce di phishing sofisticate, sfruttando un'analisi linguistica avanzata (tra cui linguaggio transazionale, urgenza, contesto e intento) per scoprire le minacce nascoste e i rischi sconosciuti per i dati.

Nexus RG™ (Relationship Graph) identifica i sottili cambiamenti di comportamento nelle comunicazioni dei tuoi utenti, rilevando deviazioni rispetto al normale comportamento, variazioni nei volumi e la condivisione di dati aziendali sensibili. Riduce così i rischi di perdite di dati e ti protegge contro i rischi informatici legati al comportamento.

Nexus TI™ (Threat Intelligence) analizza le tattiche dei criminali informatici e protegge in modo proattivo dalle nuove minacce informatiche sfruttando dati in tempo reale per identificare le nuove tattiche dei criminali informatici e le vulnerabilità di sistema, nonché attivare l'emulazione in sandbox per gli URL e gli allegati sospetti.

Nexus CV™ (Computer Vision) identifica e neutralizza le minacce basate sulla visione. Grazie a una tecnologia di computer vision avanzata, Nexus CV rileva le minacce nascoste negli elementi visivi, come siti di phishing, codici QR, allegati dannosi e email falsificate.

Nexus ML™ (Machine Learning) utilizza tecniche di apprendimento dinamiche e adattive, come l'apprendimento supervisionato, l'apprendimento non supervisionato e i metodi d'insieme. Combina queste tecniche con funzionalità di rilevamento predittivo delle minacce per mappare i comportamenti di attacco noti e con tecniche non supervisionate per rilevare le anomalie sconosciute.

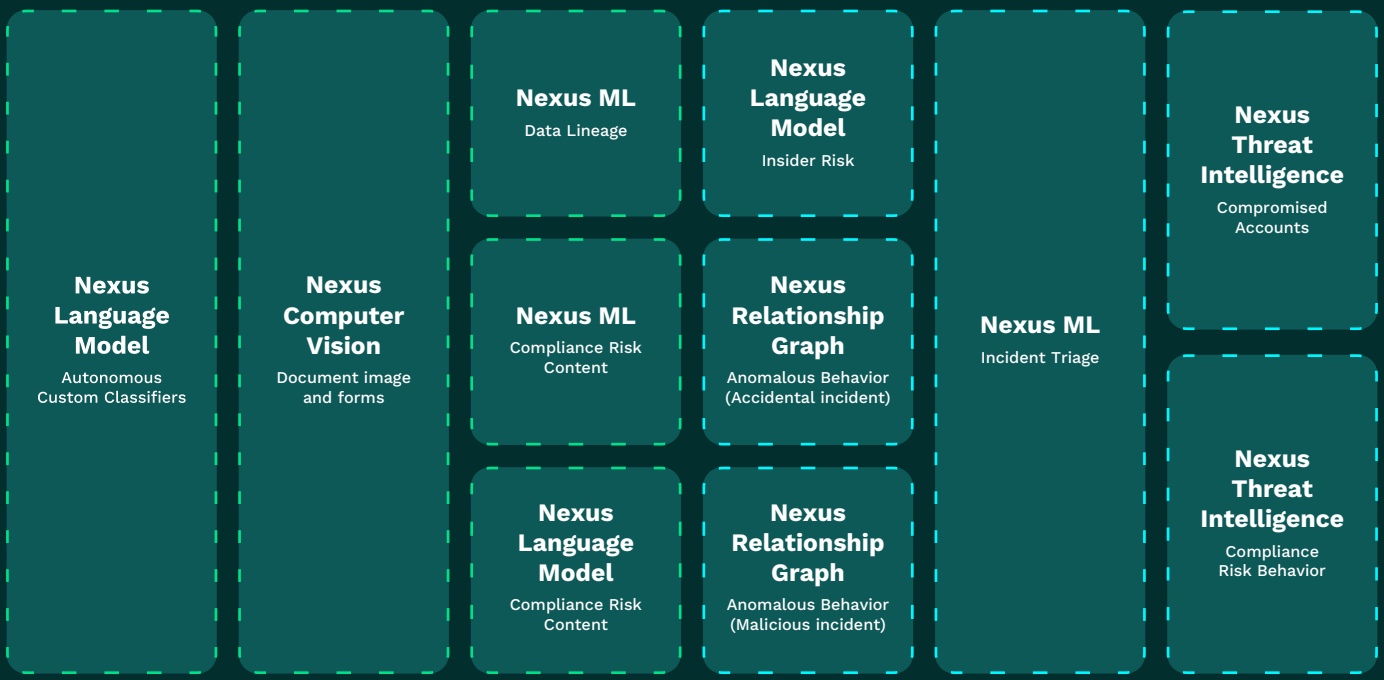
Proofpoint Nexus AI per la sicurezza e la governance dei dati

Proofpoint utilizza gli stessi motori Nexus, potenti e all'avanguardia, per ottimizzare le sue soluzioni di sicurezza e governance dei dati.

L'IA per prevenire la perdita di dati

Proofpoint Nexus classifica e traccia il percorso dei dati e il loro flusso. Non importa se i destinatari fanno parte dell'azienda o sono esterni.

- **Nexus LM™ (Language Model, modello linguistico)** impara a identificare i tipi di documenti professionali reali dell'azienda, come i documenti per le trattative, le previsioni o i progetti dei prodotti. Trasforma queste classi apprese in un contesto di policy fruibili per scoprire, assegnare le priorità e proteggere rapidamente i dati sensibili senza intervento manuale.
- **Nexus RG™ (Relationship Graph, grafico delle relazioni)** capisce le relazioni per prevenire la perdita accidentale e intenzionale di dati dovuta a destinatari errati delle email e alle sottrazioni di dati.
- **Nexus TI™ (Threat Intelligence, informazioni sulle minacce)** protegge dagli account compromessi che inviano email di phishing sia internamente sia esternamente.
- **Nexus CV™ (Computer Vision)** rileva i contenuti sensibili nelle immagini incluse in email e documenti.
- **Nexus ML™ (Machine Learning, apprendimento automatico) offre visibilità end-to-end su come i file vengono creati, copiati,** rinominati, condivisi e spostati tra archivi e destinazioni. Collega tale attività a uno storico tracciabile che consente.



L'IA agentica in Proofpoint

Per quanto riguarda l'ambiente di lavoro basato sull'IA agentica, Proofpoint investe in due aree chiave.

1. Proofpoint Satori™ Agents

Sviluppiamo agenti di IA da integrare nelle soluzioni Proofpoint esistenti. I Proofpoint Satori Agents automatizzano le attività e riducono il carico di lavoro manuale dei tuoi team SOC.

- **Abuse Mailbox Agent** automatizza la revisione manuale dei messaggi segnalati. Ciò riduce il carico di lavoro del SOC con il compito di distinguere tra minacce reali e email inoffensive.
- **DLP Triage Agent** gestisce gli avvisi e il monitoraggio delle attività della tua soluzione di prevenzione della perdita di dati (DLP).
- **Phishing Simulation Agent** utilizza l'automazione basata sull'IA per rendere operativi i programmi di sensibilizzazione alla sicurezza informatica e per rafforzare la resilienza umana.

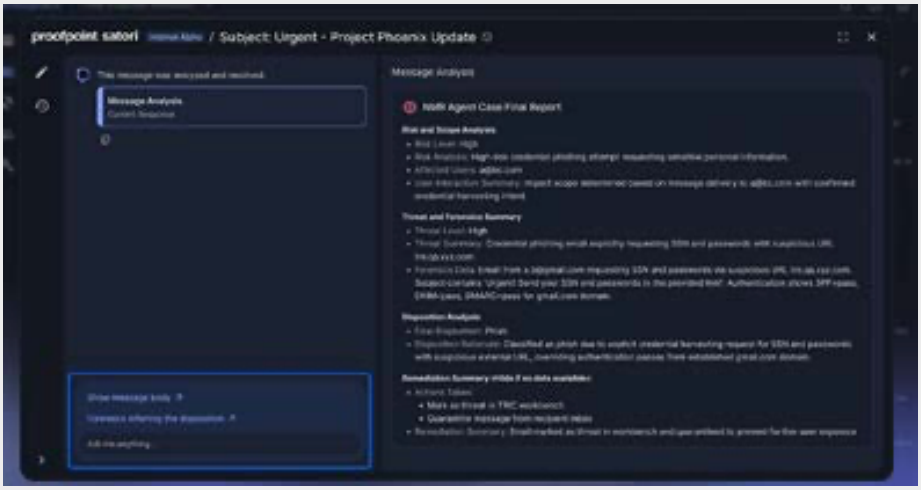


Figura 2. Proofpoint Satori Abuse Mailbox Agent in azione

2. Proofpoint AI Security

Siamo consapevoli dei rischi per la sicurezza introdotti dalla rapida adozione dell'IA a livello di utenti, agenti e sistemi aziendali. Per questo motivo abbiamo esteso la nostra piattaforma Human-Centric Security per proteggere e governare lo spazio di lavoro agentico nel suo complesso.

Proofpoint AI Security offre visibilità unificata, controllo e protezione per tutte le interazioni dell'IA, assicurando un utilizzo sicuro e conforme delle tecnologie di IA.

- **Protegge il modo in cui utenti, agenti e sistemi interagiscono con l'IA** in tutta l'azienda.
- **Offre visibilità e governance end-to-end** a livello di utilizzo dell'IA, agenti e interazioni con i modelli.
- **Previene la fuga di dati, l'uso improprio degli strumenti e le eccessive autorizzazioni d'accesso** nei flussi di lavoro dell'IA.

proofpoint.