proofpoint.

L'IA in Proofpoint

L'IA offre soluzioni nuove e innovative per aiutare le persone a svolgere il proprio lavoro. Allo stesso tempo, aiuta anche i criminali informatici a incrementare la loro produttività. Le loro tattiche, tecniche e procedure (TTP) sono oggi rafforzate dall'IA, che consente loro 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.

Ma 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. È qui che entra in gioco l'IA. Permette di monitorare il flusso di dati e identificare i comportamenti a rischio nel contesto, riducendo in modo significativo il carico di lavoro dei team del centro 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 giocano d'anticipo sui criminali informatici,

94%

Proofpoint ha osservato un aumento del 94% delle minacce tramite email contro i suoi clienti nel 2025.

Come i criminali informatici utilizzano l'IAper scalare gli attacchi

Proofpoint ha osservato in prima persona le conseguenze dell'IA quando viene utilizzata dai criminali informatici. Nel 2025, Proofpoint ha rilevato un aumento del 94% del numero delle minacce tramite email contro i clienti rispetto all'anno precedente. Ciò si traduce in un panorama delle minacce più sofisticato che include l'iniezione di prompt, l'invio in massa di email e attacchi di abuso di servizi legittimi.

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

- **Moltiplicatore di forza.** L'IA consente ai criminali informatici di lanciare attacchi più sofisticati su una superficie più ampia. Quest'anno, abbiamo osservato migliaia di email volte a indurre gli agenti IA ad agire per conto del criminale informatico.

- **Barriera ridotta all'ingresso.** L'IA può 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, i criminali informatici si affidavano a modelli prevedibili e generici per i loro attacchi. Grazie all'IA, possono creare attacchi personalizzati per ogni vittima. Quest'anno abbiamo assistito a un aumento degli attacchi personalizzati che abusano di 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.

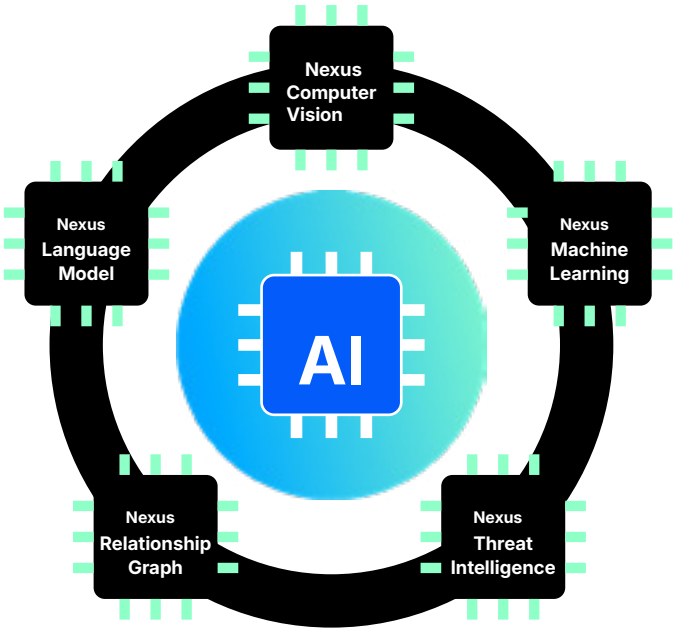
Proofpoint Nexus AI per proteggere la collaborazione

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

L'IA per rilevare e bloccare le minacce

Proofpoint Nexus è un insieme di motori ottimizzati dall'IA che operano di concerto per offrire un'efficacia del rilevamento del 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 Proofpoint Nexus AI elaborano 2,3bilioni di email all'anno, supportati da un team di threat intelligence che monitora oltre 100 gruppi unici di criminali informatici e oltre 8.400 campagne di minacce attive.



N exus 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 cambiamenti comportamentali sottili nelle comunicazioni degli utenti, rilevando deviazioni rispetto al normale comportamento degli utenti, cambiamenti nei volumi e condivisione di dati aziendali sensibili per ridurre il rischio di attacchi basati sul 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 di apprendimento non supervisionato per rilevare le anomalie sconosciute.

Proofpoint Nexus AI per la sicurezza e la governance dei dati

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

L'IA per prevenire la perdita di dati

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) impara a identificare i tipi di documenti professionali reali della tua azienda, come i documenti per le trattative, le previsioni o i design 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) analizza le relazioni tra i dati per prevenire la perdita accidentale e intenzionale di dati a causa di email indirizzate al destinatario errato e scenari di sottrazione di dati.

Nexus TI™ (Threat Intelligence) protegge dagli account compromessi che inviano email di phishing sia internamente che esternamente.

Nexus CV™ (Computer Vision) rileva i contenuti sensibili nelle immagini all'interno di email e documenti.

Nexus ML™ (Machine Learning) offre visibilità end-to-end su come i file vengono creati, copiati, rinominati, condivisi e spostati tra repository e destinazioni. Collega tale attività a uno storico tracciabile che permette di accelerare le indagini, implementare controlli basati sull'origine e fornire prove pronte ad essere presentare in occasione delle verifiche relative ai programmi di protezione dei dati.

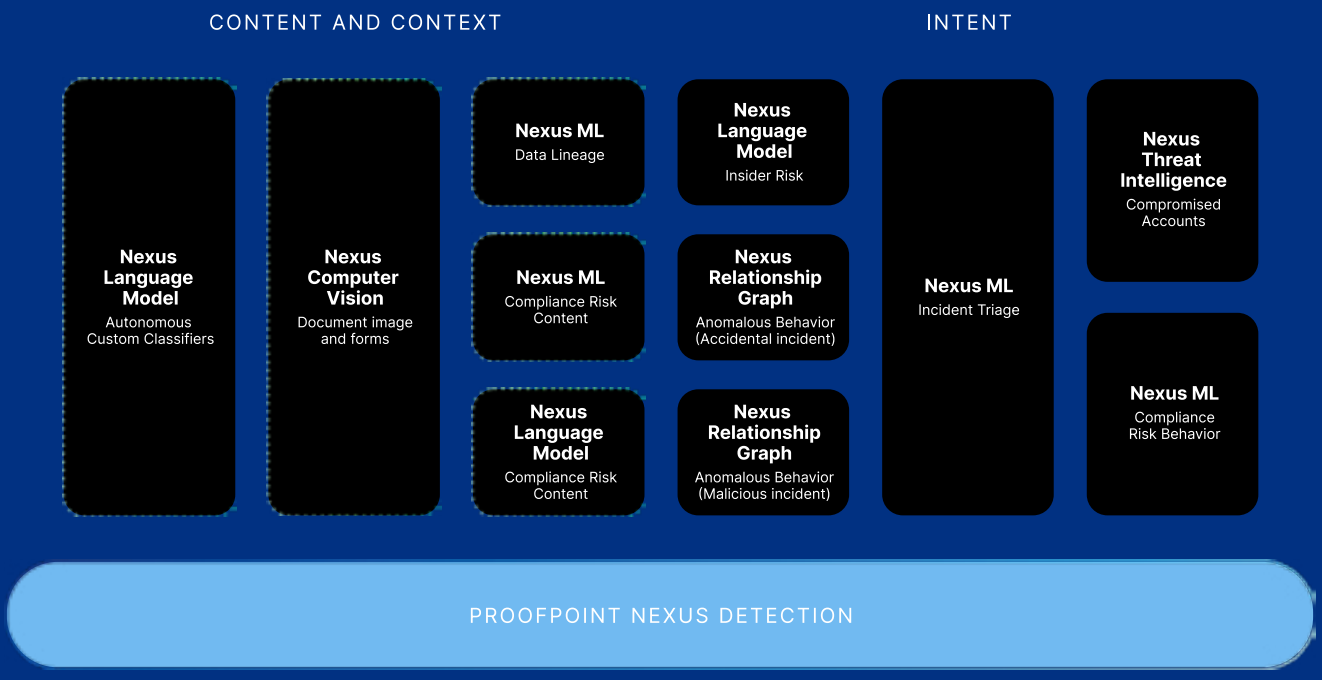


Figura 1. Nexus ottimizza le soluzioni di sicurezza e governance dei dati.

L'IA agentica in Proofpoint

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

1. Proofpoint Satori™ Agents

Sviluppiamo agenti 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 mes-saggi segnalati. Ciò riduce il carico di lavoro del SOC con il compito di distinguere tra minacce reali ed email inoffensive.
- **D LP Triage Agent** gestisce gli avvisi e il monitoraggio delle atti-vità della tua soluzione di prevenzione della perdita di dati (DLP).
- **Phishing Simulation Agent** utilizza l'automazione basata sull'IA per rendere operativi i tuoi programmi di sensibilizzazione alla sicurezza informatica e rafforzare la resilienza umana.

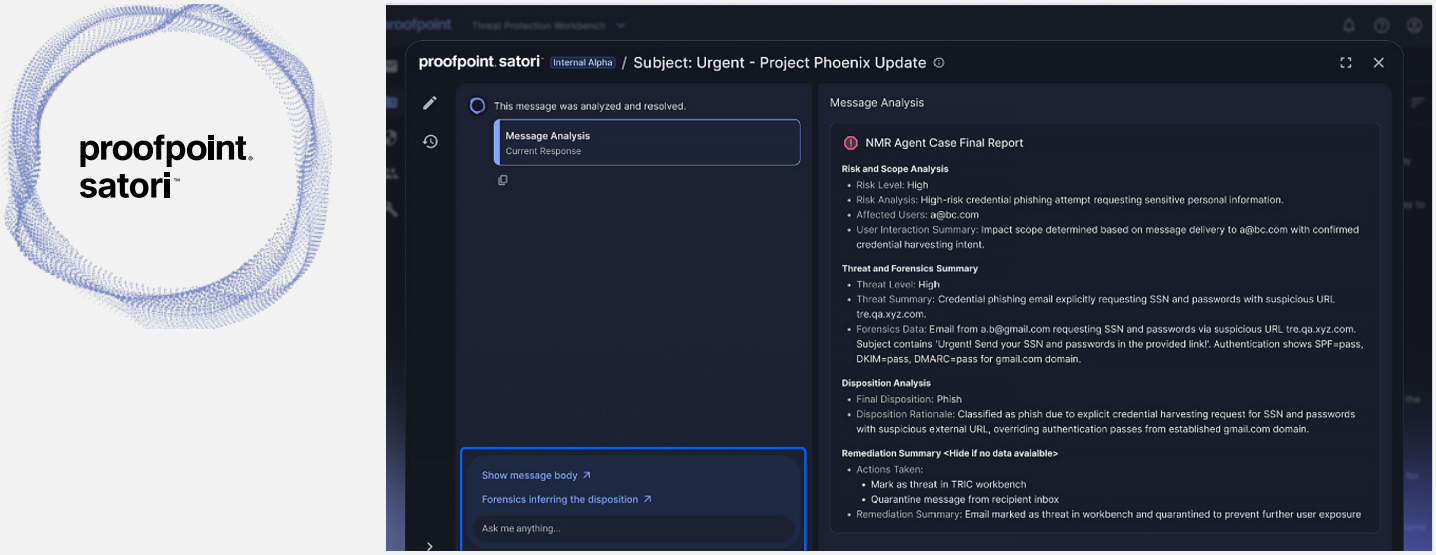


Figura 2. Proofpoint Satori Abuse Mailbox Agent in azione

2. Proofpoint Secure Agent Gateway

Siamo consapevoli delle lacune di sicurezza intrinseche all'implementazione di flussi di lavoro di IA agentica all'interno della tua azienda. Per questo motivo estendiamo la nostra piattaforma Human-Centric Security per proteggere anche tutti i tuoi agenti.

Proofpoint Secure Agent Gateway protegge i flussi di lavoro agentici esistenti e unifica i controlli agentici di tutti gli agenti del tuo ambiente.

- **Protegge le informazioni sensibili in entrata e in uscita da ogni** flusso di lavoro agentico
- **È ottimizzato dalla nostra tecnologia MCP** (Model Context Protocol)
- **Controlla l'accesso ai dati sensibili** utilizzati dagli agenti