

Proofpoint Data Security for AI

Monitora e controlla l'utilizzo dei dati sensibili nelle applicazioni di IA approvate e non approvate

Vantaggi principali

- **Riduzione dei rischi indotti dall'IA che gravano sui dati**
- **Miglioramento della visibilità sull'attività dell'IA in azienda**
- **Monitoraggio e governance dell'utilizzo delle applicazioni di IA non approvate**
- **Protezione dei dati sensibili nei prompt e negli upload**
- **Accelerazione dell'adozione sicura dell'IA**
- **Supporto della conformità e della preparazione alle verifiche**

La sfida: l'esposizione dei dati indotta dall'IA

Le applicazioni di IA generativa (GenAI) stanno trasformando le aziende, aiutando i collaboratori a lavorare in modo più rapido ed efficiente. Ma le aziende incontrano anche difficoltà a controllare come i dati sensibili vengono condivisi con gli strumenti di IA, i copiloti e le applicazioni ottimizzate dall'IA.

I collaboratori spesso caricano file e inviano richieste contenenti informazioni aziendali sensibili a strumenti di IA approvati e non approvati. Le tecnologie tradizionali di sicurezza dei dati non sono state concepite per monitorare i prompt, i caricamenti e le risposte dell'IA in tempo reale. Le aziende hanno così una visibilità limitata sulle modalità con cui i sistemi di IA accedono ai dati sensibili e li espongono.

Anche gli utenti interni possono utilizzare in modo improprio gli strumenti di IA — intenzionalmente o meno — per individuare, sintetizzare, riscrivere o sottrarre informazioni sensibili, tra cui documenti riservati, codice proprietario e elementi di proprietà intellettuale. Gli utenti interni malintenzionati possono utilizzare gli strumenti di IA per accelerare il furto di dati, eludere i controlli tradizionali o automatizzare l'estrazione di dati sensibili su larga scala.

Senza i controlli adeguati, le aziende rischiano di subire fughe di dati, violazioni della conformità e la divulgazione non autorizzata di informazioni soggette a regolamentazione o riservate. I team della sicurezza hanno bisogno di una visibilità costante sull'utilizzo e l'esposizione dei dati da parte dell'IA, di un'applicazione più rigorosa delle policy e di una verificabilità completa per sostenere un'adozione sicura dell'IA.

La soluzione: Proofpoint Data Security for AI

Proofpoint aiuta le aziende a adottare l'IA in modo sicuro grazie alla visibilità sull'utilizzo dei dati da parte delle applicazioni di IA approvate e non approvate. Unifica il monitoraggio, i controlli dei dati specifici per l'IA e le informazioni sull'attività dell'IA per ridurre i rischi e favorire un'adozione sicura e scalabile dell'IA.

Funzionalità essenziali

Visibilità sull'utilizzo dei dati da parte dell'IA e sul livello di sicurezza delle applicazioni di IA

Proofpoint offre visibilità su come i collaboratori e l'IA interagiscono con i dati aziendali. I team della sicurezza possono così identificare gli utenti ad alto rischio, rilevare le interazioni non sicure con l'IA e capire quali dati e documenti sensibili sono esposti a causa di un utilizzo di applicazioni di IA approvate e non approvate.

I classificatori personalizzati autonomi della soluzione identificano i dati sensibili specifici dell'azienda condivisi tramite prompt dell'IA, upload e risposte generate dall'IA, tra cui la proprietà intellettuale, il codice sorgente, i dati finanziari e i documenti strategici. Questo contesto permette di rilevare, mascherare e proteggere i dati in modo più preciso nelle applicazioni di IA approvate e non approvate.

Proofpoint monitora costantemente gli ambienti di IA e SaaS per rilevare configurazioni errate, autorizzazioni eccessive a livello di sito e integrazioni non sicure. L'identificazione dei diritti di accesso eccessivi e delle lacune nella configurazione consente alle aziende di mitigare i rischi, ridurre la superficie di attacco ed evitare che i dati sensibili vengano esposti agli utenti e alle applicazioni di IA.

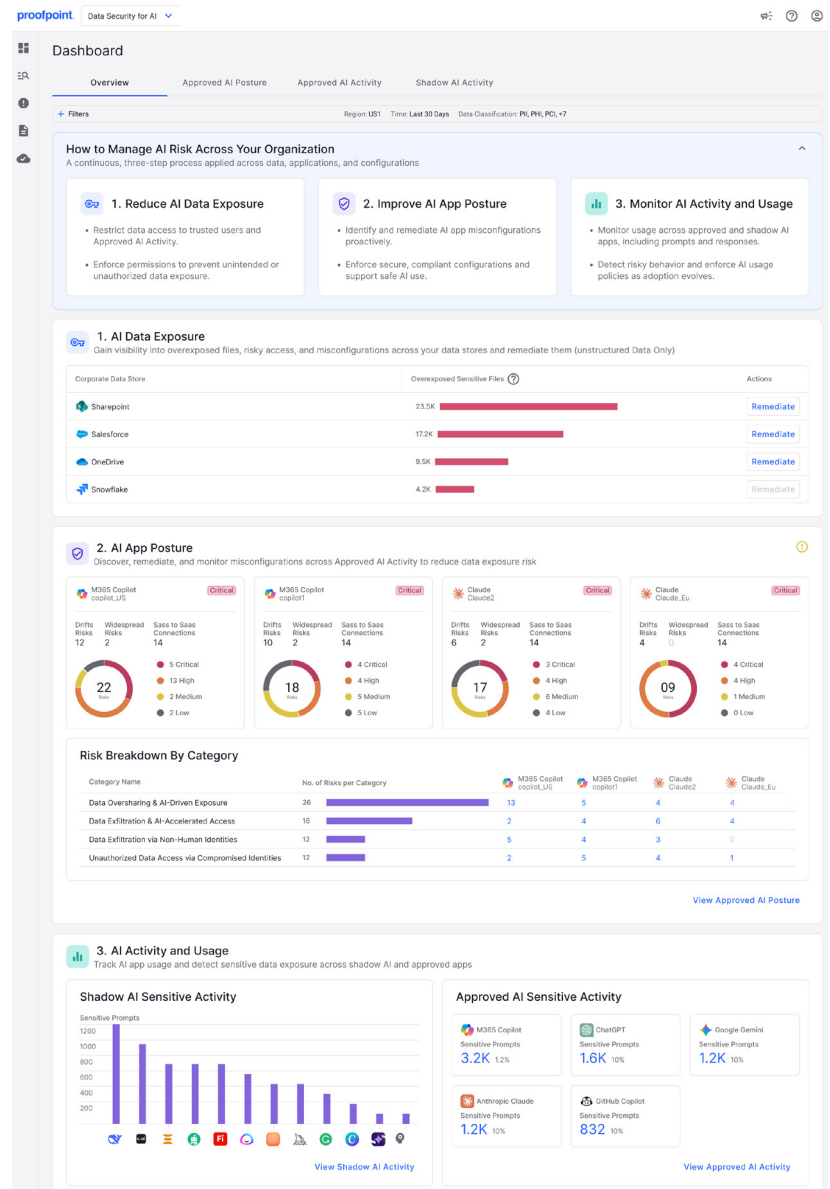


Figura 1. Proofpoint offre ai team della sicurezza una visibilità approfondita sul modo in cui i collaboratori e gli strumenti di IA interagiscono con i dati sensibili.

Monitoraggio delle applicazioni di IA approvate e applicazione di misure correttive

Proofpoint monitora costantemente i prompt, gli upload e le risposte generate dall'IA all'interno delle applicazioni di IA approvate al fine di identificare l'esposizione di dati sensibili e le attività insolite da parte degli utenti interni, tra cui un numero eccessivo di prompt o l'upload di grandi volumi di dati. L'acquisizione completa dei prompt e delle risposte facilita le indagini e la preparazione alle verifiche. I flussi di lavoro di applicazione di misure correttive integrati aiutano gli amministratori e i proprietari dei file a intervenire rapidamente in caso di condivisione eccessiva dei dati.

Sicurezza dei dati delle applicazioni di IA non approvate

Le aziende possono ridurre l'esposizione dei dati da parte dell'IA monitorando e controllando il loro utilizzo da parte di applicazioni di IA web e desktop non approvate. Proofpoint aiuta a prevenire la perdita di dati tramite i prompt, l'upload di file e le azioni di incollaggio. Inoltre, maschera i dati sensibili presenti nei prompt prima che vengano condivisi con gli strumenti di IA. Le aziende possono così estendere l'adozione dell'IA in modo sicuro senza bloccare del tutto le applicazioni di IA.

Impatto operativo

Riduzione della perdita di dati indotta dall'IA

Previene l'esposizione di dati sensibili nelle applicazioni di IA approvate e non approvate.

Miglioramento della visibilità e della governance dell'IA

Ottieni una visibilità centralizzata su come i collaboratori e gli strumenti di IA interagiscono con i dati aziendali.

Adozione più sicura dell'IA in azienda

Autorizza un utilizzo produttivo dell'IA generativa mantenendo al contempo i controlli relativi a sicurezza, governance e conformità.

Accelerazione delle indagini e delle risposte

Acquisisci l'attività dell'IA, i prompt e le risposte per facilitare le indagini, l'applicazione di misure correttive e la preparazione alle verifiche.

Rafforzamento del livello di conformità

Adattati all'evoluzione dei requisiti in materia di IA, privacy e protezione dei dati applicando policy alle informazioni regolamentate, riservate e proprietarie utilizzate con gli strumenti di IA.

Riduzione dei rischi legati alle applicazioni di IA non approvate

Identifica e governa l'utilizzo delle applicazioni di IA non approvate e i comportamenti a rischio degli utenti, riducendo al minimo l'impatto sulla produttività aziendale.

Per saperne di più

Per maggiori informazioni, visita il nostro sito all'indirizzo [proofpoint.com/it](https://www.proofpoint.com/it).

Informazioni su Proofpoint. Inc. Proofpoint, Inc. è un'azienda leader globale nella cybersecurity incentrata sulle persone e sugli agenti, che protegge il modo in cui persone, dati e agenti IA si connettono tramite email, cloud e strumenti di collaborazione. Proofpoint è un partner di fiducia per oltre 80 aziende della classifica Fortune 100, oltre 10.000 grandi imprese e milioni di aziende più piccole, per contrastare le minacce, prevenire la perdita di dati e rafforzare la resilienza di persone e processi di IA. La piattaforma di collaborazione e sicurezza dei dati di Proofpoint aiuta aziende di tutte le dimensioni a proteggere e responsabilizzare i propri collaboratori in modo che possano adottare l'IA in modo sicuro e con fiducia. Per saperne di più, visita www.proofpoint.com/it.

Seguici: [LinkedIn](#)

Proofpoint è un marchio registrato o nome commerciale di Proofpoint, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.