proofpoint.

PANORAMICA SULLA SOLUZIONE

Sicurezza dei dati per l'IA generativa

Assicura un utilizzo sicuro dell'IA generativa

Vantaggi principali

- Conseguimento di visibilità sull'utilizzo non autorizzato di strumenti di IA generativa
- Prevenzione dell'esposizione di dati sensibili attraverso gli strumenti di IA generativa aziendali e sviluppo utilizzando gli LLM
- Applicazione di policy di utilizzo accettabile dell'IA generativa nel cloud e sugli endpoint
- Monitoraggio delle minacce interne grazie a policy dinamiche che permettono di rilevare gli utilizzi pericolosi dell'IA
- Formazione dei collaboratori sull'utilizzo accettabile degli strumenti di IA generativa

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a mitigare le quattro principali categorie di rischi legati agli utenti.

L'IA generativa (GenAI) offre un potenziale immenso, stimolando la produttività, l'innovazione e le informazioni sui dati. Tuttavia, la sua adozione pone delle sfide, in particolare in termini di sicurezza dei dati, privacy e conformità. Quando utilizzano strumenti pubblici di IA generativa, gli utenti rischiano di esporre dati sensibili e elementi di proprietà intellettuale. Inoltre, una scarsa governance può portare a un accesso non autorizzato ai dati da parte di strumenti aziendali come Microsoft 365 Copilot e alla classificazione errata dei risultati. I modelli linguistici di grandi dimensioni (LLM) personalizzati addestrati con i dati dei clienti possono divulgare dati a carattere personale, aumentando i rischi di non conformità a normative come il GDPR e le leggi HIPAA e CCPA. Senza una solida governance, le aziende rischiano di incorrere in violazioni della sicurezza e in multe dovute alla mancanta conformità con le normative.

Proofpoint assicura un utilizzo accettabile degli strumenti e modelli di IA generativa grazie a un approccio completo e incentrato sulle persone che riunisce visibilità, controllo e formazione. Proofpoint Data Loss Prevention (DLP) monitora l'utilizzo dell'IA generativa sugli endpoint, fornendo informazioni sulle interazioni degli utenti e identificando gli strumenti non autorizzati. Per prevenire la perdita di dati, Proofpoint applica policy che bloccano o oscurano i dati sensibili inseriti nei prompt dell'IA generativa. Proofpoint Data Security Posture Management (DSPM) previene l'esposizione di dati tramite gli strumenti di IA generativa e LLM classificando i dati sensibili e proteggendoli da accessi non autorizzati. Inoltre, Proofpoint Zenguide offre formazione di sensibilizzazione alla sicurezza informatica personalizzata per spiegare agli utenti come utilizzare in modo sicuro l'IA generativa, promuovendo una cultura di utilizzo responsabile. Integrando queste strategie, Proofpoint protegge i dati sensibili delle aziende nel panorama in costante evoluzione dell'IA generativa.

Ottieni visibilità sull'utilizzo non autorizzato degli strumenti di IA generativa

Proofpoint aiuta le aziende a identificare chi utilizza quali strumenti di IA generativa e se i dati sensibili trapelano attraverso questi strumenti o LLM personalizzati. Il nostro report della sicurezza dei dati in un contesto di utilizzo dell'IA mette in evidenza i tipi di dati inviati agli strumenti pubblici di IA generativa, gli utenti più attivi, i principali siti per attività e altro ancora (Figura1).

Grazie a API cloud, puoi identificare le autorizzazioni di applicazioni IA di terze parti, come OpenAI e generare degli avvisi. Puoi anche identificare le implementazioni di IA in AWS Bedrock e Azure OpenAI che utilizzano dati sensibili.

Vantaggi principali

- Prevenzione dell'esposizione di dati sensibili attraverso gli strumenti di IA generativa aziendali e sviluppo utilizzando gli LLM

Previeni l'esposizione di dati sensibili attraverso gli strumenti di IA generativa e gli LLM

Proofpoint DSPM identifica e classifica i dati sensibili nei flussi di lavoro IA, in modo da prevenire l'esposizione che potrebbe portare a delle violazioni. Protegge inoltre i dati a cui accede Microsoft Copilot applicando etichette Microsoft Information Protection (MIP), che vengono utilizzate per implementare policy di protezione come la crittografia e i controlli d'accesso.

Protegge LLM personalizzati e applicazioni di IA su piattaforme come AWS Bedrock e Azure OpenAI i rilevando i dati sensibili immessi nei modelli di base o personalizzati nonché i flussi di lavoro RAG (Retrieval-Augmented Generation).

Proofpoint offre API specializzate per la sicurezza degli LLM, permettendo un'analisi in tempo reale della sensibilità dei dati che fluiscono da e verso gli LLM. Queste API offrono governance e visibilità complete sull'utilizzo dei dati con un'integrazione fluida nei flussi di lavoro dei clienti per un'implementazione efficace.

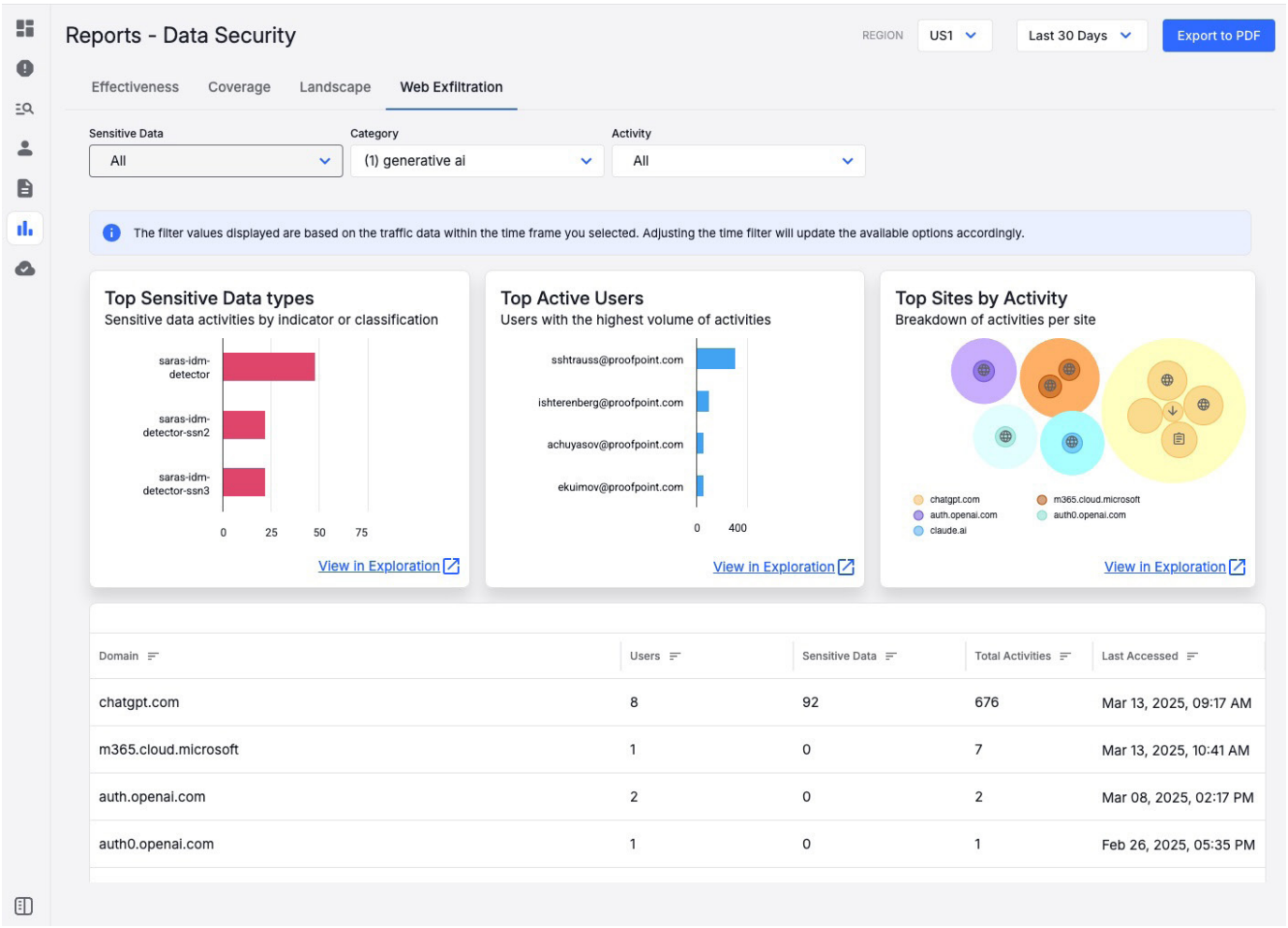

Figura 1. Report che evidenzia i principali rischi di esfiltrazione dei dati attraverso l'IA generativa

Vantaggi principali

- Applicazione di policy di utilizzo accettabile dell'IA generativa nel cloud e sugli endpoint
- Monitoraggio delle minacce interne grazie a policy dinamiche che permettono di rilevare gli utilizzi pericolosi dell'IA
- Formazione dei collaboratori sull'utilizzo accettabile degli strumenti di IA generativa

Previeni la perdita di dati e le minacce interne associate all'utilizzo dell'IA generativa

Sugli endpoint, puoi monitorare gli utenti che navigano sui siti di IA generativa utilizzando la categorizzazione dei web o generare avvisi in caso di installazione di applicazioni di IA non autorizzate. Le nostre policy dinamiche possono rafforzare il monitoraggio degli endpoint per gli utenti che presentano comportamenti a rischio. Per esempio, puoi acquisire metadati e schermate prima e dopo l'invio da parte degli utenti di contenuti sensibili a siti di IA generativa non autorizzati. Ciò ti aiuta a dedicare meno tempo all'analisi delle interazioni degli utenti con gli strumenti di IA generativa.

Con Proofpoint DLP, puoi applicare policy DLP a livello di endpoint per oltre 600 strumenti di IA generativa per utente, gruppo o dipartimento e bloccare gli upload su piattaforme di IA generativa o mascherare i dati sensibili inseriti nei prompt. Per preservare la produttività degli utenti, la nostra soluzione può anche incoraggiarli a rispettare le policy di utilizzo dell'IA generativa o chiedere loro una giustificazione invece di applicare policy di prevenzione.

Tramite API cloud, offriamo visibilità sui file condivisi in modo eccessivo esposti a Microsoft 365 Copilot e avvisiamo il tuo team della sicurezza quando gli utenti utilizzano in modo improprio Copilot per localizzare i file che contengono informazioni sensibili.

Per esempio, Proofpoint rileva quando un utente interno a rischio utilizza Copilot per accedere a molti file che contengono dati sensibili in un breve periodo. Inoltre, la nostra soluzione classifica, etichetta e protegge i contenuti generati dall'IA nelle applicazioni cloud. Inoltre, revoca o blocca le autorizzazioni di applicazioni di IA di terze parti non approvate.

Forma i collaboratori sull'utilizzo accettabile degli strumenti di IA generativa

Proofpoint educa gli utenti all'utilizzo sicuro dell'IA generativa nella tua azienda. ZenGuide forma gli utenti con video, poster, moduli interattivi e newsletter sulla gestione sicura dei dati. Ti consente di sfruttare le informazioni sui tuoi utenti a alto rischio e automatizzare l'apprendimento personalizzato basato sul livello di rischio per gruppi mirati, come gli sviluppatori, o per gli utenti più a rischio.

Le attività di formazione stimolano comportamenti positivi attraverso valutazioni, avvisi personalizzati e esperienze di coaching. Tali attività includono valutazioni delle conoscenze, assegnazioni dei corsi di formazione, notifiche e accettazione delle policy, tutte concepite per migliorare la sensibilizzazione e incoraggiare un utilizzo sicuro e accettabile degli strumenti di IA generativa.

Potenzia la tua azienda grazie all'utilizzo sicuro dell'IA generativa

Proofpoint propone una soluzione incentrata sulle persone per rispondere alle moderne sfide di sicurezza dei dati. Forniamo informazioni sui rischi di esposizione dei dati e di fuoriuscita degli stessi legati agli strumenti di IA generativa e agli LLM.

Con Proofpoint, puoi trovare facilmente il giusto equilibrio tra produttività dell'utente e sicurezza dei dati adottando strategie che permettono agli utenti di accedere a strumenti e modelli di IA generativa grazie alla formazione, un monitoraggio rafforzato e i giusti controlli sui dati.

proofpoint.

Proofpoint 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 →

0207-017-05-01 03/25