



IA generativa: consentine un utilizzo sicuro e riduci i rischi per i dati

Zscaler fornisce massima visibilità e controllo sull'IA generativa, consentendo all'organizzazione di farne uso senza mai perdere di vista la sicurezza dei dati sensibili.

Rischi e vantaggi dell'uso di IA generativa

Gli strumenti di IA stanno rappresentando per molte organizzazioni la nuova frontiera della produttività. Tuttavia, essi generano anche rischi per i dati sensibili, i quali possono risultare esposti se questi strumenti vengono utilizzati in modo improprio. Con Zscaler, le organizzazioni possono personalizzare l'uso di particolari applicazioni di IA in base alle proprie esigenze, garantendo così una protezione completa dei dati e una piena visibilità sull'utilizzo di queste soluzioni.

Problemi dell'IA generativa per la sicurezza

- Chi utilizza le app di IA?
- È possibile controllare l'accesso di ogni singolo utente?
- Si dispone di un controllo granulare su app specifiche?
- Quali sono i livelli di rischio delle app di IA?
- È possibile proteggere i dati sensibili sulle app di IA?
- È possibile controllare le query effettuate all'IA in tutta l'organizzazione?

Funzionalità principali



Controlli di utilizzo dell'IA basati sul rischio

Consenti solo l'uso delle applicazioni IA appropriate, in base al rischio, sfruttando controlli di utilizzo granulari, con un livello di dettaglio che arriva ai singoli team e utenti.



Visibilità sull'IA

Comprendi chi utilizza l'IA all'interno dell'organizzazione e ottieni la piena visibilità su tutte le richieste e le query su ChatGPT.



Protezione dati per l'IA

Previene le potenziali fughe di dati attraverso le applicazioni di IA con una protezione DLP completa che tutela i dati dall'esfiltrazione nei prompt destinati all'IA.



Previene le azioni rischiose

Incorpora misure di sicurezza aggiuntive, come l'isolamento del browser, per impedire download, upload di dati e utilizzo degli appunti, impedendo l'esfiltrazione di grandi quantitativi di dati potenzialmente sensibili attraverso i prompt.

Vantaggi principali



Stimola l'innovazione con l'IA

Utilizza con sicurezza l'IA per potenziare i tuoi team e innovare.



Ottimizza l'uso dell'IA e mitiga i rischi

Gestisci i rischi e le spese consentendo solo l'utilizzo delle app di IA appropriate e utili per l'organizzazione, riducendo così rischi e spese.



Informazioni continue sull'AI

Grazie alla visibilità continua sull'utilizzo e sui prompt impiegati, l'organizzazione è in grado di comprendere, controllare e perfezionare costantemente l'uso e le attività legate all'IA.



Codice sorgente interno



Confidenzialità dei contenuti creati



Analisi dei dati sensibili

Controllo degli accessi

Policy di filtraggio degli URL
Controllo delle app cloud
Navigazione sicura (isolamento)

Blocco della perdita dei dati

Ispezione DLP inline

Zero Trust Exchange



IA generativa

Visibilità sull'IA

Dettagli sull'utilizzo delle app (ZIA)
Violazioni delle policy (DLP)

Logging SIEM

Zscaler Nanolog Streaming

Con Zscaler, l'organizzazione può potenziare la sicurezza dell'IA generativa e i controlli dei dati grazie a una sola piattaforma unificata.

Oltre a metterne in sicurezza l'utilizzo, Zscaler si avvale da anni dell'intelligenza artificiale per ottimizzare il livello di sicurezza dei team di IT e security.



Segmentazione basata sull'IA

Riduci al minimo la superficie di attacco interna individuando in automatico i segmenti delle applicazioni per creare le giuste policy di accesso zero trust e ridurre i rischi per la sicurezza.



Una protezione dei dati più rapida

Proteggi i dati in modo istantaneo con la classificazione automatica basata sul machine learning, senza bisogno di configurazione, e accelera i programmi di protezione dati dell'azienda.



Analisi delle cause radice basata sull'IA

Identifica le cause alla radice delle esperienze scadenti 180 volte più velocemente e aiuta gli utenti a tornare al lavoro in pochi secondi, accelera l'MTTR e consenti all'IT di evitare di ricorrere a laboriose analisi e procedure di risoluzione dei problemi.



Verdetti di sandboxing basati sull'IA

Evita le infezioni da paziente zero grazie all'IA, che ti consente di stabilire istantaneamente se un nuovo file è dannoso e di bloccarne l'ingresso nell'organizzazione senza aspettare un verdetto della sandbox.



Experience your world, secured.™

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata su SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su zscaler.it o seguici su X (precedentemente Twitter) sull'[@zscaler](https://twitter.com/zscaler).

© 2023 Zscaler, Inc. Tutti i diritti riservati. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ e gli altri marchi commerciali elencati all'indirizzo zscaler.it/legal/trademarks sono (i) marchi commerciali o marchi di servizio registrati o (ii) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Qualsiasi altro marchio commerciale è di proprietà dei rispettivi titolari.