Zero trust, governance, innovazione

# La formula di Zscaler IT per la sicurezza dell'AI



©2026 Zscaler, Inc. Tutti i diritti riservati.

WHITE PAPER

# Introduzione

Nell'attuale panorama digitale in rapida evoluzione, l'intelligenza artificiale (AI) è un'arma a doppio taglio: offre opportunità di trasformazione, ma introduce anche complessità senza precedenti in termini di sicurezza, governance e gestione dei rischi. Man mano che le aziende adottano l'intelligenza artificiale per favorire innovazione, agilità ed efficienza, si trovano di fronte a una sfida cruciale: come possono proteggere l'AI per tutelare i dati sensibili, garantire la conformità e sviluppare fiducia, sia all'interno che all'esterno dell'organizzazione?

Questa sfida è al centro della strategia IT di Zscaler. In qualità di leader globale nella sicurezza cloud, abbiamo adottato un approccio proattivo all'integrazione dell'AI nelle operazioni aziendali, mantenendo al contempo rigorose misure di controllo e governance. Questo impegno riflette non solo la nostra posizione di leadership nel settore della sicurezza informatica, ma anche la consapevolezza dell'importanza di proteggere l'AI per le aziende di ogni settore. In questo white paper, illustriamo **l'approccio di Zscaler IT all'adozione sicura dell'AI e analizziamo i principi fondamentali che le aziende devono seguire per bilanciare la potenza dell'AI con la necessità di mitigare i rischi.**


©2026 Zscaler, Inc. Tutti i diritti riservati.

# Affrontare le complesse sfide dell'AI

Le opportunità offerte dall'AI si accompagnano inevitabilmente a rischi che le aziende devono affrontare per adottarla con successo. Dalla **possibile esposizione dei dati dovuta alla compromissione dei modelli, ai pericoli legati a bias, usi impropri o output generati senza adeguati controlli, le aziende si trovano a navigare in un campo minato di criticità relative a sicurezza, conformità e governance.** Nel ricorrere all'AI per trasformare le proprie attività, le organizzazioni devono gestire questi rischi senza frenare l'innovazione. Per riuscirsi, servono strategie proattive e solidi framework per la sicurezza dell'AI.

In assenza di misure di protezione complete, le aziende si espongono a rischi significativi, tra cui la compromissione della proprietà intellettuale, la perdita di fiducia dei clienti e potenziali violazioni normative. Le organizzazioni devono non solo impedire l'utilizzo non autorizzato dell'AI, ma anche garantire una rigorosa governance dei modelli e degli output per preservare fiducia e affidabilità. In qualità di leader nel campo dell'innovazione della sicurezza, **Zscaler IT si è assunta questa responsabilità, sviluppando un framework completo per la sicurezza e la governance dell'AI, basato sui principi dello zero trust e conforme a standard internazionali come il NIST AI Risk Management Framework.** Il nostro approccio a più livelli affronta le sfide specifiche introdotte dall'AI, garantendo la sicurezza dei dati sensibili e preservando la resilienza dell'organizzazione.

La posta in gioco è alta e, nell'era dell'AI, mitigare i rischi richiede l'adozione di soluzioni che rafforzino la fiducia e, al contempo, proteggano le attività aziendali. Solo attraverso una governance scrupolosa, framework progettati con attenzione e tecnologie all'avanguardia le imprese possono affrontare con sicurezza il futuro dell'adozione dell'intelligenza artificiale. In Zscaler, l'approccio rigoroso e basato sulla governance alla sicurezza dell'AI rappresenta un requisito fondamentale e obbligatorio per tutte le attività aziendali, non una semplice scelta discrezionale.

# Framework e processi di governance dell'AI in Zscaler

La sicurezza dell'AI parte dalla governance e dai processi. In Zscaler, la governance dell'AI si basa su principi fondamentali e solide policy aziendali, tra cui la policy sull'utilizzo dell'intelligenza artificiale generativa e gli standard interni di due diligence. L'obiettivo fondamentale del framework per la sicurezza dell'AI è proteggere i dati, sia dei clienti che dell'azienda, da rischi come la fuoriuscita di informazioni dai modelli, le allucinazioni e l'utilizzo improprio.

## I principi fondamentali dell'AI e adozione delle policy

L'approccio di Zscaler all'intelligenza artificiale si basa su quattro principi fondamentali: responsabilità, equità, trasparenza, sicurezza e conformità.

Il nostro documento sugli standard di sicurezza dell'AI generativa si basa sul NIST AI Risk Management Framework e sulle best practice del settore. I principali requisiti che tutti i dipendenti e i collaboratori esterni devono rispettare includono:


©2026 Zscaler, Inc. Tutti i diritti riservati.

- **Limitazione dell'accesso a determinati strumenti di AI generativa pubblici (GenAI):** i modelli di AI e gli LLM non autorizzati o provenienti da Paesi considerati ad alto rischio vengono bloccati. L'accesso limitato può essere concesso solo previa approvazione di una deroga da parte del team di sicurezza, per specifici casi d'uso aziendali, come la ricerca e sviluppo o l'innovazione.

- **AI pubblica protetta:** qualsiasi utilizzo di strumenti AI pubblici deve avvenire attraverso controlli di sicurezza approvati, tra cui le policy DLP e i controlli di AI Guard, per garantire la protezione dei dati e una governance adeguata. Queste misure sono progettate per definire regole chiare e monitorare le interazioni con gli strumenti di AI pubblici, nel rispetto dei requisiti di sicurezza di Zscaler.

- **Restrizioni sui dati:** gli utenti non devono inserire negli strumenti di AI generativa dati personali o informazioni rilevanti non pubbliche (ad esempio, aziende potenzialmente oggetto di acquisizione o roadmap di prodotto non ancora annunciate). È inoltre vietato inserire informazioni riservate (come report sulla sicurezza, dettagli tecnici e tecnologici e dati dei clienti).

- **Obbligo di revisione umana:** gli output degli strumenti di AI generativa devono essere sottoposti a revisione umana. È vietato utilizzare questi strumenti per prendere decisioni automatizzate senza l'intervento o la supervisione di una persona.

- **Restrizioni sull'utilizzo degli strumenti AI nelle risorse umane:** è espressamente vietato utilizzare strumenti di AI/ML per finalità legate al rapporto di lavoro, come la valutazione dei candidati, le decisioni di assunzione o la definizione dei termini e delle condizioni di impiego, senza la preventiva revisione e approvazione dei reparti delle risorse umane e degli affari legali specializzati.

## Piattaforme di AI interne autorizzate

Zscaler mantiene un elenco degli strumenti, delle piattaforme e degli LLM di AI generativa autorizzati. È espressamente vietato utilizzare modelli, strumenti o servizi di AI associati a Paesi soggetti a sanzioni o considerati ad alto rischio, inclusi gli LLM cinesi come DeepSeek e Qwen, per finalità legate ai prodotti, alla ricerca e sviluppo o alle attività aziendali.

| Ambito | Piattaforma/strumento approvato | Sicurezza e mitigazione dei rischi |
|---|---|---|
| **Utilizzo generale da parte dei dipendenti** | **ZChat** (approvato dall'azienda e ospitato su un tenant Zscaler dedicato). **ChatGPT** e **Gemini** (strumenti pubblici approvati). | Richiede controlli del profilo di sicurezza tramite ZPA o l'ispezione SSL tramite ZIA, oltre ad AI Guard e alla disattivazione obbligatoria del monitoraggio dell'uso improprio effettuato dalle piattaforme di AI generativa di terze parti. |
| **Ingegneria/ Sviluppo prodotti** | Microsoft Azure AI, Google Vertex AI, Amazon AWS AI Services, Z-Llama (Gateway LLM interno). | Richiede l'utilizzo di ZIA DLP, chiavi di crittografia CMEK (Customer Managed Encryption Key) per le applicazioni SaaS, connettività ZPA per l'accesso ai sistemi che ospitano le risorse più critiche (come Bitbucket) e strumenti di sicurezza SAST/SCA per analizzare il codice generato. |
| **Sviluppo software** | Gli strumenti autorizzati possono generare suggerimenti o frammenti di codice per i prodotti destinati ai clienti oppure codice per test interni o applicazioni aziendali (ad esempio, uno script per automatizzare l'elaborazione degli stipendi). | Tutto il codice generato deve rispettare gli standard di Zscaler per il ciclo di vita dello sviluppo software, che prevedono la revisione del codice da parte di altri sviluppatori, test unitari e valutazioni delle vulnerabilità di sicurezza. |


©2026 Zscaler, Inc. Tutti i diritti riservati.

## Processo di procurement e due diligence per le soluzioni AI di fornitori esterni:

Prima di acquistare qualsiasi prodotto o servizio di AI da fornitori esterni, abbiamo reso obbligatorio un rigoroso processo di approvazione interna che coinvolge i team di sicurezza, privacy e affari legali. Questo sistema è progettato per gestire il rischio associato all'utilizzo di strumenti di intelligenza artificiale esterni.

Il processo inizia con il responsabile aziendale, che deve verificare che sia stato firmato un accordo di riservatezza (NDA) con il fornitore e presentare un modulo di richiesta debitamente compilato.

La valutazione interna della sicurezza richiede al fornitore di presentare una documentazione completa:

- **Questionario di sicurezza del fornitore (VSQ):** deve essere compilato in ogni sua parte.
- **Report SOC 2 Tipo 2:** è necessario presentare un report valido o una bridge letter relativa al periodo non coperto dal report.
- **Risultati dei penetration test:** è necessario presentare i risultati di test condotti negli ultimi due anni che dimostrino l'assenza di vulnerabilità critiche o di gravità elevata ancora irrisolte negli ambienti di produzione oppure forniscano indicazioni chiare e tempistiche definite per la loro mitigazione.

## Sicurezza dei dati e standard per l'hosting dei modelli:

Zscaler valuta l'architettura dell'AI e i flussi di dati utilizzando il framework Five Safes per la valutazione dei rischi dell'AI e richiede l'adozione di pratiche sicure per la gestione dei dati sensibili, tra cui anonimizzazione, mascheramento e tokenizzazione.

I criteri di accettazione dipendono da dove è ospitato il modello di intelligenza artificiale e dal tipo di dati elaborati (pubblici, riservati o confidenziali):

- **Modelli ospitati da fornitori di quarta parte (ad es. API di OpenAI):** per i dati pubblici o ad accesso limitato, si prediligono nettamente una politica di conservazione zero dei dati (zero data retention) e la disattivazione dei processi di monitoraggio degli utilizzi impropri da parte del fornitore. Per i dati riservati, il fornitore deve garantire l'isolamento degli utenti e dei tenant, l'assenza di conservazione dei dati da parte del fornitore di quarta parte e la garanzia che i dipendenti di quest'ultimo non accedano mai ai dati riservati di Zscaler.
- **Restrizioni sul training dei modelli:** i dati dei clienti non vengono mai utilizzati per addestrare modelli di AI interni o esterni. Per maggiori informazioni, consulta l'articolo "Zscaler's Commitment to Responsible AI" sul nostro sito web. Zscaler vieta l'utilizzo dei propri dati interni per addestrare i modelli generici dei fornitori. Se per il training vengono utilizzati dati interni ad accesso limitato o riservati, questi devono essere sottoposti a rigorose procedure di deidentificazione o aggregazione, oppure il modello deve essere addestrato e utilizzato esclusivamente per Zscaler. Inoltre, è assolutamente vietato ai fornitori di quarta parte addestrare i propri modelli utilizzando qualsiasi dato di Zscaler.


©2026 Zscaler, Inc. Tutti i diritti riservati.

## Garanzie legali e contrattuali:

Il team legale addetto al procurement inserisce nei contratti con i fornitori clausole che limitano fortemente l'utilizzo dei dati di Zscaler. Le clausole contrattuali standard vietano espressamente ai fornitori di accedere ai dati di Zscaler, raccoglierli o utilizzarli per:

- **Addestrare, mettere a disposizione o migliorare** i modelli di AI o ML del fornitore o di terze parti.
- **Generare output o fornire servizi** di qualsiasi tipo a proprio vantaggio, a vantaggio delle proprie affiliate o di terze parti.

Se un fornitore richiede dati Zscaler per il training AI/ML, l'ufficio legale deve richiedere **un'eccezione.** In caso di approvazione, vengono redatte clausole contrattuali specifiche per limitare i rischi per Zscaler, tra cui la restrizione dell'utilizzo a **un'istanza dedicata esclusivamente a Zscaler** e la garanzia che Zscaler detenga tutti i diritti di proprietà intellettuale sui propri dati e sugli output generati.

# Profilo di sicurezza AI: i prodotti Zscaler in azione

Una volta completati tutti i processi di governance, definizione del framework e onboarding dei fornitori, il passo successivo fondamentale è garantire la sicurezza dell'AI utilizzando i prodotti di Zscaler. Gli strumenti e le strategie di Zscaler per proteggere l'AI durante la sua evoluzione si concentrano sulla tutela dei dati sensibili e della privacy e sulla prevenzione dell'utilizzo improprio attraverso policy contestuali avanzate e una moderna architettura zero trust.

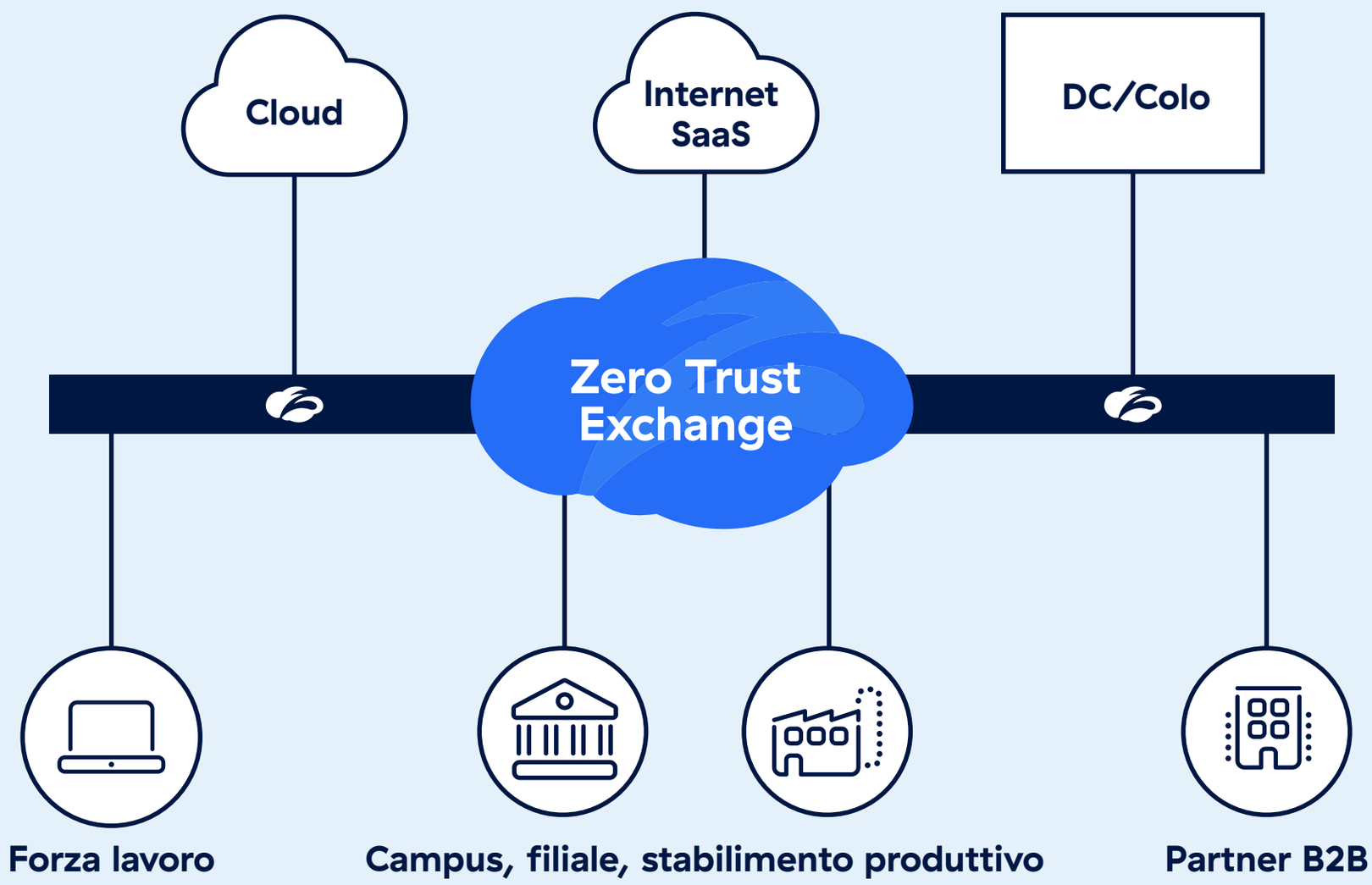



**FIGURA 1:** l'architettura Zscaler per la rete e la sicurezza elimina complessità e rischi.


©2026 Zscaler, Inc. Tutti i diritti riservati.

## Fondamenti zero trust e sicurezza della rete

La strategia di sicurezza di Zscaler si basa sui principi zero trust, garantendo connessioni sicure e un rigoroso controllo degli accessi.

- **Zscaler Internet Access (ZIA) per la sicurezza Internet:** tutto il traffico Internet degli utenti viene instradato su Zscaler Internet Access per l'applicazione delle policy prima di consentire l'accesso. Le policy includono: ispezione SSL, rilevamento avanzato delle minacce, sandboxing e policy DLP. Gli ambienti cloud vengono dotati di Cloud Connector per proteggere l'accesso dei workload cloud a Internet.

- **Zscaler Private Access (ZPA) per applicazioni interne:** l'accesso a tutte le applicazioni interne avviene tramite ZPA e richiede il superamento dei controlli del profilo di sicurezza prima di essere autorizzato. Gli ambienti cloud dispongono di app connector che forniscono un accesso sicuro e senza interruzioni alle applicazioni cloud ospitate privatamente.

- **Zscaler AI Guard** offre protezione in fase di esecuzione per le applicazioni AI gestite dall'azienda, garantendo sicurezza e conformità nelle operazioni AI.

- **Zero Trust Branch(ZTB):** tutti gli uffici di Zscaler sono passati a un modello di rete simile a quello delle reti Wi-Fi pubbliche, eliminando costosi firewall e dispositivi di routing. Le appliance ZTB installate nelle sedi combinano sicurezza perimetrale della rete, SD-WAN e microsegmentazione, isolando ogni utente, visitatore e dispositivo IoT in una rete individuale. Questo impedisce qualsiasi movimento laterale delle minacce all'interno delle sedi aziendali.

## Proteggere l'utilizzo degli strumenti AI pubblici

Le piattaforme AI pubbliche (ad es. ChatGPT, Perplexity, CoPiliot, Grok, ecc.) sono utili per accelerare i flussi di lavoro, risolvere problemi complessi ed elaborare i dati. Tuttavia, il loro utilizzo può esporre involontariamente dati sensibili, aprire la strada alla diffusione di malware e amplificare i rischi legati a modalità di utilizzo non sicure. Zscaler affronta queste sfide implementando difese a più livelli.

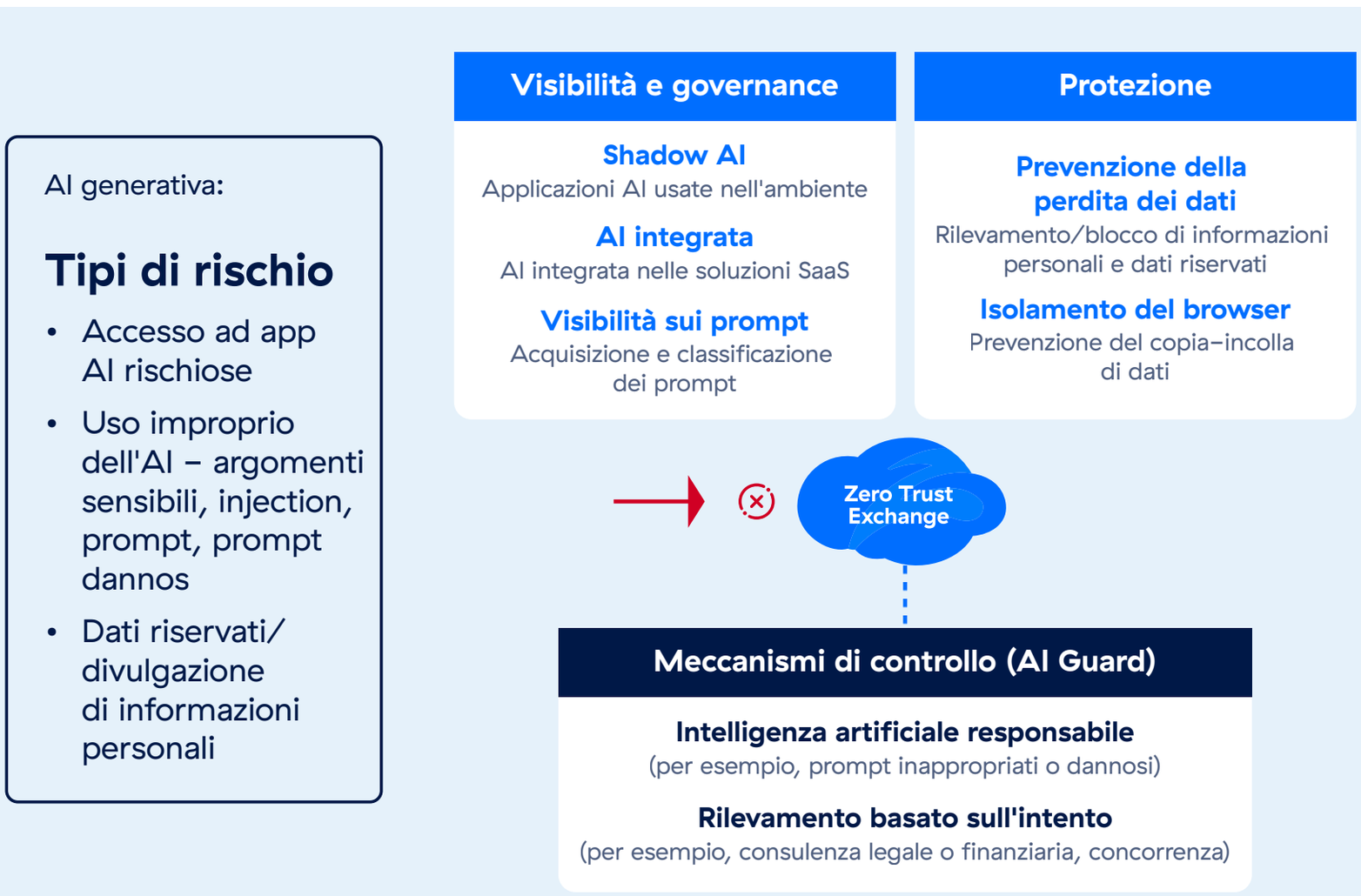



**FIGURA 2:** Zscaler garantisce la sicurezza dell'utilizzo dell'AI generativa pubblica e privata.


©2026 Zscaler, Inc. Tutti i diritti riservati.

- **Blocco degli URL AI indesiderati e delle app cloud di shadow AI** Utilizzando il filtro URL e le policy per le applicazioni cloud di Zscaler Internet Access, è possibile bloccare l'accesso non autorizzato a determinate piattaforme e applicazioni cloud AI utilizzate per l'AI generativa.

- **Isolamento di categorie di URL AI/ML per limitare la condivisione dei dati** Sfruttando anche la categorizzazione degli URL AI/ML di Zscaler Internet Access, consentiamo l'accesso agli strumenti di AI/ML generici, ma solo all'interno di una sessione del browser isolata. Tutto il traffico diretto a questa categoria che non è stato esplicitamente bloccato dalla policy viene reindirizzato su Zscaler Zero Trust Browser. Impedire agli utenti finali di incollare dati sensibili o riservati consente di ridurre il rischio di violazioni della sicurezza o l'uso improprio dell'AI senza ostacolare l'innovazione.

- **Ispezione DLP inline** Monitoraggio in tempo reale di tutto il traffico Internet, comprese le interazioni con l'AI, per impedire che i dati sensibili vengano inseriti nei prompt o esfiltrati.

- **Sicurezza della GenAI** Tutto il traffico AI consentito viene registrato e analizzato dal prodotto GenAI Security. Questo report è attualmente attivo in ZIA, con l'acquisizione dei prompt abilitata. Fornisce al team della sicurezza aziendale e al CISO report dettagliati su:

  - Quali strumenti GenAI vengono utilizzati (consentiti o bloccati).
  - Chi utilizza questi strumenti.
  - Categorizzazione dei prompt

- **AI Guard per l'AI pubblica (meccanismi di controllo per gli LLM)** Controlli di sicurezza sui prompt e sulle risposte tramite AI Guard, che introduce ulteriori misure di protezione per analizzare sia i prompt inviati alle piattaforme AI pubbliche autorizzate sia le relative risposte. Questi controlli includono:

  - Blocco dell'invio di informazioni personali all'LLM.
  - Prevenzione di richieste e risposte tossiche o inappropriate.
  - Blocco della prompt injection e dei tentativi di jailbreaking per aggirare i controlli, che vengono continuamente aggiornati man mano che emergono nuovi vettori di attacco specifici dell'AI.

Queste misure di sicurezza assicurano che gli utenti interagiscano in modo responsabile con gli strumenti di intelligenza artificiale senza esporre dati aziendali sensibili. Inoltre, si limitano i contenuti restituiti dagli LLM per proteggere gli utenti e l'azienda.

## Creazione di una piattaforma di GenAI privata e sicura

Zscaler IT ha creato una piattaforma privata di intelligenza artificiale generativa per consentire a tutti i dipendenti di adottare l'AI in modo sicuro.  Il modello di sicurezza di ZChat si basa sui principi zero trust di Zscaler, sfruttando tutte le funzionalità di AI e ZPA della piattaforma Zscaler, integrate con Okta per la gestione delle identità e il controllo degli accessi basato sui ruoli (RBAC).  Dettagli di ZChat:

- **Hosting interno:** Hosting nell'ambiente AWS di Zscaler: ZChat è ospitato su Amazon Web Services (AWS) e utilizza l'architettura nativa del cloud di Zscaler. Questo consente una distribuzione scalabile e resiliente, sfruttando le funzionalità di sicurezza native di AWS.


©2026 Zscaler, Inc. Tutti i diritti riservati.

- **Autenticazione degli utenti:** ZChat è integrato con Okta per l'autenticazione, in modo che solo gli utenti autorizzati, ovvero quelli registrati e gestiti tramite Okta, possano accedervi.

- **Controllo degli accessi basato sui ruoli (RBAC):** l'accesso a ZChat è ulteriormente limitato tramite controlli degli accessi basati sui ruoli all'interno dell'applicazione. Questo garantisce che gli utenti abbiano accesso solo alle funzionalità e ai dati appropriati al loro ruolo.

- **Comunicazione con i servizi OpenAI di Zscaler su Azure:** ZChat comunica in modo sicuro con i servizi OpenAI di Zscaler ospitati su Microsoft Azure.

- **Controllo degli accessi tramite ZPA:** Zscaler Private Access offre un accesso sicuro alle applicazioni AI private segmentando l'accesso degli utenti tramite perimetri definiti da software. In questo modo, impedisce il movimento laterale, riduce le superfici di attacco e garantisce che solo gli utenti autenticati e autorizzati possano interagire con sistemi di intelligenza artificiale che elaborano grandi quantità di dati.

- **Profilo di sicurezza del dispositivo:** per stabilire una connessione alle applicazioni private protette da ZPA, è obbligatorio che tutti i dispositivi siano completamente gestiti e conformi ai requisiti di sicurezza.

- **AI Guard per gli strumenti AI privati:** come per l'AI pubblica, Zscaler implementa negli strumenti di AI privata controlli di sicurezza sui prompt e sulle risposte che bloccano attività come la condivisione di dati personali, gli utilizzi impropri o i tentativi di sfruttamento tramite istruzioni dannose (ad esempio, i tentativi di jailbreaking). Integrando queste protezioni nelle applicazioni private, possiamo applicare rigorose policy sull'utilizzo dell'AI, sfruttandone al contempo tutte le potenzialità.

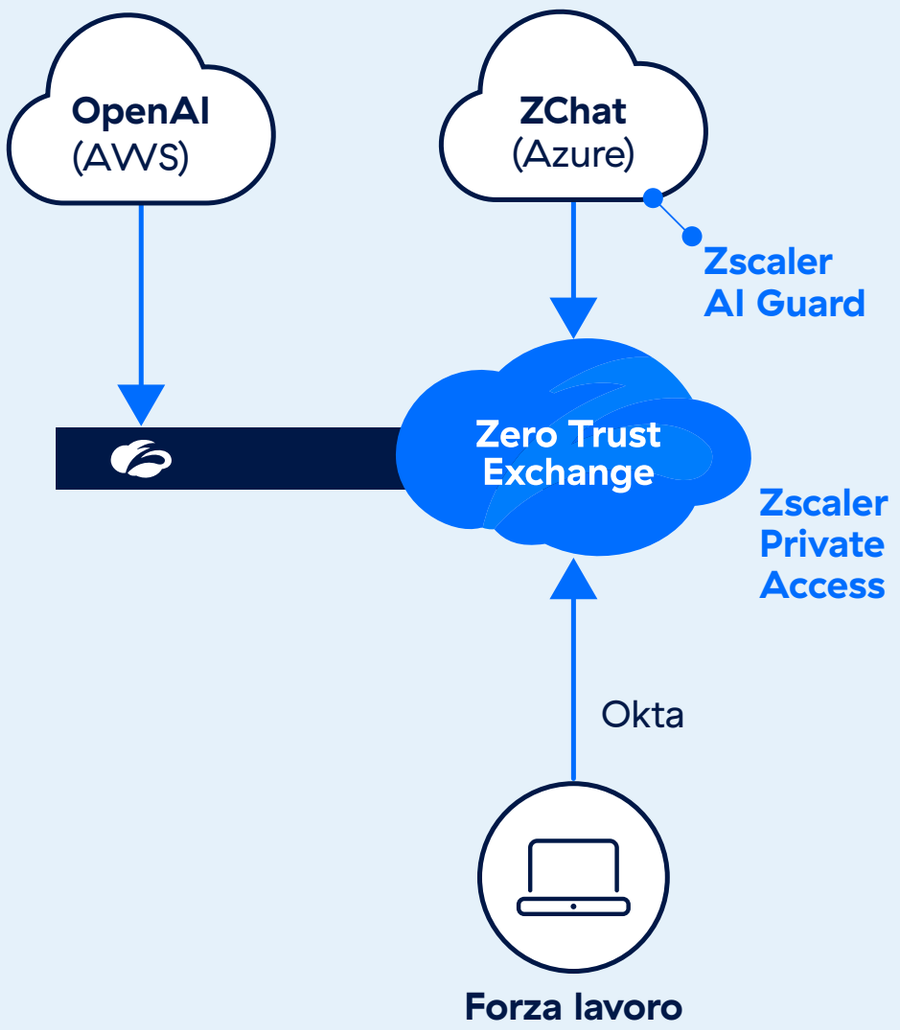



**FIGURA 3:** Zscaler Private Access (ZPA) fornisce ai dipendenti un accesso sicuro all'applicazione privata ZChat (in esecuzione su AWS). ZPA protegge anche la comunicazione backend tra ZChat e i servizi OpenAI di Zscaler ospitati in Microsoft Azure. Tutte le interazioni private con la GenAI (prompt e risposte) all'interno di ZChat sono protette da Zscaler AI Guard


©2026 Zscaler, Inc. Tutti i diritti riservati.

# AI sicura:
# una protezione completa per le aziende

## I vantaggi per la sicurezza

- **Architettura zero trust:** Zscaler applica i principi del privilegio minimo e della sicurezza fin dalla progettazione agli accessi di tutti gli utenti, i dispositivi e le applicazioni, riducendo al minimo la superficie di attacco e impedendo il movimento laterale delle minacce nei diversi ambienti.

- **Governance completa:** tutte le iniziative legate all'intelligenza artificiale sono regolamentate da rigorose policy interne e sono in linea con framework come il NIST AI Risk Management Framework.

- **Solida protezione dei dati:** i dati sensibili (ad esempio, dati personali e informazioni aziendali riservate) sono protetti attraverso rigorosi controlli sui dati in ingresso e in uscita, DLP inline e isolamento del browser, per prevenire la fuoriuscita accidentale di dati e l'uso improprio.

- **Monitoraggio continuo delle attività AI:** il report di sicurezza sulla GenAI offre funzionalità avanzate di supervisione e reportistica, consentendo il monitoraggio in tempo reale dell'utilizzo degli strumenti e garantendo la conformità alle policy di utilizzo.

- **Meccanismi di controllo a più livelli:** Zscaler AI Guard aggiunge il monitoraggio di prompt e risposte, bloccando i tentativi di condivisione di dati sensibili, impedendo gli attacchi di jailbreaking e prevenendo richieste tossiche o non autorizzate, sia per l'AI generativa pubblica che per l'AI interna o privata.

- **Mitigazione del rischio associato ai fornitori:** tutti gli strumenti di AI di terze parti sono sottoposti a rigorose procedure di due diligence, che includono valutazioni della sicurezza, penetration test e garanzie legali e contrattuali per la protezione dei dati (ad esempio, il divieto di utilizzare i dati per addestrare modelli di AI esterni).

## Aumento della produttività dei dipendenti

- **Implementazione sicura dell'AI:** fornendo un accesso sicuro a strumenti di AI sia privati che pubblici, Zscaler consente ai dipendenti di utilizzare l'intelligenza artificiale in modo sicuro per la ricerca, la pro-grammazione e l'automazione dei flussi di lavoro, favorendo l'innovazione senza rischi di esposizione.

- **Processo decisionale più rapido:** i dipendenti possono utilizzare l'AI in tutta sicurezza per ricavare informazioni utili, riepilogare dati e automatizzare le attività, sapendo di poter contare su misure di protezione e controlli di conformità che eliminano i colli di bottiglia.

- **Sviluppo rapido:** gli ingegneri sfruttano strumenti di GenAI e di suggerimento del codice sicuri e approvati preventivamente (protetti da revisione del codice e controlli di sicurezza), riducendo i tempi del ciclo di sviluppo senza compromettere gli elevati standard qualitativi.


©2026 Zscaler, Inc. Tutti i diritti riservati.

## Valore generato per l’azienda

- **Maggiore fiducia e conformità:** grazie all’allineamento agli standard internazionali e all’adozione proattiva di misure di governance dell’AI, Zscaler riduce i rischi normativi, rafforza la fiducia dei clienti e tutela la reputazione aziendale.

- **Riduzione dell’esposizione al rischio informatico:** una segmentazione rigorosa, l’ispezione del traffico e l’applicazione delle policy riducono drasticamente il rischio di violazioni dei dati, violazioni della conformità e perdita di proprietà intellettuale, con conseguenti risparmi sui costi.

- **Maggiore agilità e innovazione:** i framework sicuri di Zscaler consentono all’organizzazione di esplorare il potenziale dell’AI con rapidità e sicurezza, favorendo lo sviluppo di modelli di business differenziati e accelerando il Time to Market di nuovi prodotti e servizi.

- **Leadership e differenziazione sul mercato:** adottando l’utilizzo dei propri prodotti e documentando in modo trasparente i risultati ottenuti, Zscaler dimostra la propria leadership nella sicurezza dell’AI, offrendo un esempio ai clienti e rafforzando la propria posizione competitiva.

# Conclusione: un’AI affidabile e scalabile in un mondo zero trust

Zscaler IT dimostra che è possibile puntare sull’innovazione nell’AI senza compromettere la sicurezza, la privacy e la conformità normativa. Implementando un quadro di governance completo, integrando policy rigorose e sfruttando la potenza della piattaforma Zero Trust Exchange, Zscaler si è affermata come leader nell’adozione sicura dell’intelligenza artificiale. Strumenti come Zscaler Internet Access, con la funzionalità di acquisizione dei prompt AI, AI Guard e la DLP integrata, garantiscono un utilizzo dell’AI non solo scalabile, ma anche trasparente e soggetto a rigorosi controlli di governance. Queste pratiche permettono a Zscaler di mitigare le minacce informatiche, proteggere i dati sensibili e rispettare i requisiti normativi, il tutto migliorando l’efficienza operativa e favorendo l’innovazione.

L’approccio di Zscaler alla sicurezza dell’AI dimostra che le aziende possono sfruttare con fiducia il potenziale trasformativo dell’intelligenza artificiale, preservando al contempo la fiducia e la resilienza aziendale. Promuovendo un’innovazione più rapida e responsabile e stabilendo nuovi standard per una governance sicura dell’AI, Zscaler continua a essere un punto di riferimento per l’adozione dell’AI su larga scala, in modo sicuro e affidabile.

**Informazioni su Zscaler**
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **www.zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler**.

© 2026 Zscaler, Inc. Tutti i diritti riservati. Zscaler™ e gli altri marchi commerciali presenti su **zscaler.com/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. Eventuali altri marchi commerciali appartengono ai rispettivi proprietari.

**+1 408.533.0288** **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/it**

zscaler™

**Act Fast.**
**Stay Secure.**