

L'IA corre, la sicurezza delle identità resta indietro: cosa dice davvero il rapporto SailPoint

I dati sugli agenti di intelligenza artificiale, confrontati con il comunicato originale

di **Alex Trizio** · 9 ottobre 2026 · lettura 8 min

Il 9 ottobre 2026 The Hacker News ha pubblicato un pezzo su un presunto «paradosso della velocità»: le aziende adottano agenti di intelligenza artificiale a ritmo di macchina, ma ne governano gli accessi con metodi pensati per le persone. I numeri vengono da un rapporto di SailPoint, azienda che vende software per la sicurezza delle identità. Questo dossier ricostruisce i dati, li confronta con il comunicato originale e separa ciò che il rapporto misura da ciò che serve a promuovere una soluzione.

In questo dossier

01 La fonte

Un rapporto firmato da chi vende la soluzione

02 I numeri

Un mercato fermo ai blocchi di partenza

03 Il confronto

Due maturità a velocità diverse

04 Il problema

Perché i controlli pensati per le persone non reggono con gli agenti

05 Il divario

Fiducia alta, capacità bassa

06 La soluzione

Il «bilanciamento» e la strada indicata da SailPoint

07 Cosa manca

Cosa resta da verificare

08 Fonti

Le fonti del dossier

Un rapporto firmato da chi vende la soluzione

L'articolo di The Hacker News reca in calce un'avvertenza: è un contributo di un partner della testata. I link nel testo rinviano alla pagina del rapporto sul sito di SailPoint, con parametri di tracciamento. Non è una cronaca indipendente, ma la presentazione di uno studio realizzato e diffuso da un'azienda.

SailPoint è quotata al Nasdaq con la sigla SAIL e vende software per la gestione delle identità digitali. Il rapporto è uscito il 6 ottobre 2026 dalla conferenza Navigate, ad Austin. Lo stesso giorno l'azienda ha annunciato nuovi prodotti dedicati agli agenti di IA, tra cui Autonomous Agents e Agentic Fabric Security.

Questo non toglie valore ai dati. Conviene però leggerli sapendo chi li ha raccolti e che cosa vende.

Come si misura la maturità

Il rapporto è alla quinta edizione. Si basa su un sondaggio globale tra 340 responsabili di identità, informatica, sicurezza e rischio. SailPoint colloca

ogni organizzazione su una scala di cinque «Horizon»: dal primo, senza alcun programma formale, al quinto, integrato nell'ecosistema.

Il giudizio considera strategia, modello operativo, personale, fiducia tecnica e capacità tecniche. Secondo la ricostruzione di The Hacker News, il secondo livello indica processi manuali assistiti da strumenti.

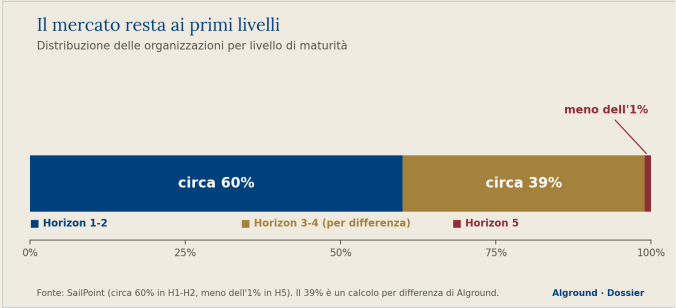
La classificazione è definita e applicata da SailPoint, non da un ente terzo. Il campione, inoltre, cambia da un anno all'altro: l'edizione 2025-2026 si basava su 375 decisori intervistati a giugno 2025.

I numeri

Un mercato fermo ai blocchi di partenza

Il primo dato riguarda tutto il mercato. Circa il 60% delle organizzazioni resta nei primi due Horizon, cioè senza programma formale o con controlli manuali assistiti da strumenti. Meno dell'1% ha raggiunto il quinto.

Per differenza resterebbe circa il 39% nei livelli intermedi, il terzo e il quarto. È un calcolo di questo dossier: il comunicato non pubblica la ripartizione completa.



Secondo SailPoint il ritardo dipende soprattutto dalle identità non umane. L'87% giudica capaci o migliori le proprie funzioni di gestione degli accessi per le persone. Solo il 43% dichiara processi maturi per l'accesso degli agenti.

The Hacker News ne ricava che il problema non sia l'impegno, ma un limite di architettura. I metodi nati per i dipendenti faticherebbero a governare agenti che eseguono migliaia di operazioni al minuto. È una lettura dell'articolo, non un risultato misurato dal sondaggio.

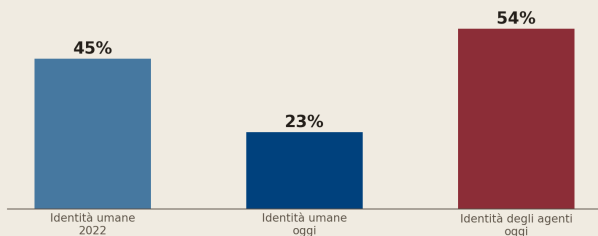
Due maturità a velocità diverse

Per le identità delle persone il quadro migliora. Nel 2022 il 45% delle organizzazioni era al primo Horizon. Oggi è il 23%: quasi la metà.

Per gli agenti di IA si parte molto più indietro. Il 54% delle organizzazioni è oggi al primo Horizon per l'identità degli agenti, una posizione peggiore di quella delle identità umane al punto di partenza.

Organizzazioni ferme al primo Horizon

Quota senza alcun programma formale di sicurezza delle identità



Fonte: SailPoint, Horizons of Identity Security 2026 (comunicato del 6 ottobre 2026). Ricostruzione di Alground.

Alground · Dossier

Gli agenti pesano già. Rappresentano il 22% di tutti gli account non umani, mentre l'85% delle organizzazioni continua a usare strumenti d'identità tradizionali, non pensati per loro.

SailPoint ne trae una conclusione: le aziende non hanno cinque anni di tempo e devono comprimere in una curva che per le persone ne ha richiesti circa cinque. La frase è di Wendy Wu, direttrice marketing dell'azienda, ed è contenuta in un comunicato aziendale.

Un dettaglio sulle date

L'articolo di The Hacker News scrive che «cinque anni fa» il dato era il 45%. Il comunicato SailPoint indica invece il 2022, cioè quattro anni prima del 2026. Il dossier usa la data del comunicato.

Il problema

Perché i controlli pensati per le persone non reggono con gli agenti

Secondo il rapporto, le organizzazioni di livello intermedio hanno digitalizzato bene i processi umani, come l'ingresso dei dipendenti e le verifiche periodiche degli accessi. The Hacker News chiama «trappola della digitalizzazione» il tentativo di replicare le stesse scadenze sulle identità delle macchine.

Molte identità di agenti durano minuti o secondi. Una revisione trimestrale arriverebbe quando l'identità non esiste più. Per l'articolo diventa un costo operativo senza utilità.

La direzione indicata è l'abbandono dei permessi permanenti e delle richieste a ticket. Al loro posto ci sarebbero regole continue, contestuali e automatiche, applicate alla velocità delle macchine. La formula tecnica è «zero standing privilege»: nessun privilegio fisso.

Il direttore tecnico di SailPoint, Chandra Gnanasambandam, ha definito irrealistica l'idea che un amministratore approvi gli accessi di agenti che fanno circa 10.000 chiamate a strumenti al secondo. La frase, pronunciata a Navigate, è riportata da un articolo di Yahoo Finance.

Il ritardo operativo ha un numero: solo il 15% delle organizzazioni può assegnare accessi non umani in tempo reale.

Resta una distinzione utile. Che i controlli periodici siano inadatti agli agenti è un argomento tecnico plausibile. Che il rimedio sia il prodotto di chi lo propone è un'altra affermazione. Vanno valutate separatamente.

Fiducia alta, capacità bassa

Il dato più citato è il divario fra adozione e protezione. Il 79% delle organizzazioni usa già agenti di IA in produzione. Solo il 2% adotta strumenti d'identità progettati apposta per governarli. Da qui il rapporto di 40 a 1.

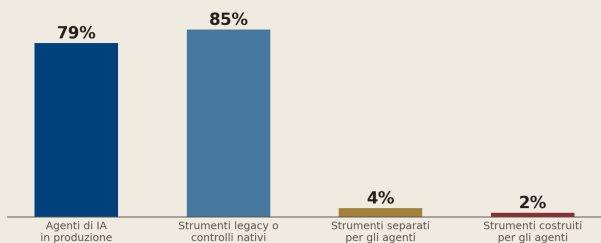
40
A
1

Quel 2% ha una definizione precisa: tecnologia costruita su misura per gli agenti. Un ulteriore 4% usa strumenti separati per le loro identità. L'85% si affida a strumenti generici o ai controlli nativi delle piattaforme. Non significa che non abbia alcun controllo.

Il 65% ha messo gli agenti a disposizione di oltre un quarto del personale. Solo il 23% dichiara uno stack d'identità pienamente moderno.

79% usa agenti, 2% li protegge con strumenti dedicati

Il divario di 40 a 1 tra adozione e protezione specifica



Fonte: SailPoint 2026, comunicato e Channel Insider (7 ottobre 2026). Le categorie non si escludono a vicenda.

Alground · Dossier

Quanto ci si sente pronti e quanto lo si è

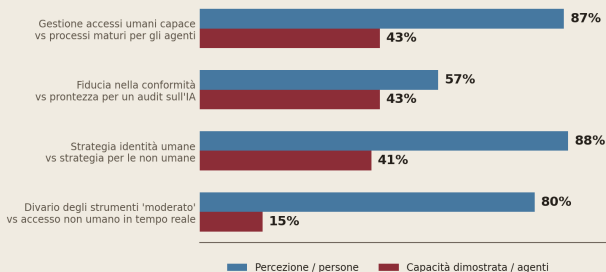
Il rapporto misura anche la distanza fra sicurezza percepita e capacità dimostrabile. Il 57% si dice fiducioso di rispettare gli obblighi normativi, ma solo il 43% si sente molto pronto a produrre prove in un audit legato all'IA.

L'88% considera la strategia per le identità umane una priorità o un fattore strategico. Solo il 41% ha una strategia per le identità non umane allineata ai piani aziendali sull'IA.

L'80% dei leader ritiene il divario degli strumenti moderato o minore. In tempo reale, però, solo il 15% riesce ad assegnare accessi non umani.

Fiducia alta, capacità bassa

Quanto ci si sente pronti e quanto lo si è davvero



Fonte: SailPoint 2026 (comunicato e Channel Insider).

L'80% è attribuito al 'leader' dal comunicato, al settore tecnologico da Channel Insider.

Alground · Dossier

La soluzione

Il «bilanciamento» e la strada indicata da SailPoint

Davanti alla scelta fra velocità e sicurezza, secondo The Hacker News il 49% dice di bilanciarle in egual misura. Il dato compare nell'articolo, ma non è presente nel comunicato né nelle altre sintesi consultate per questo dossier.

L'articolo lo definisce un falso compromesso. Un equilibrio dichiarato, senza la capacità di farlo rispettare, sarebbe una stasi. È un giudizio dell'articolo, non una misura del sondaggio.

La soluzione proposta

La conclusione del rapporto è che non serve ricostruire tutto da zero. Basta estendere alle identità non umane le regole di governo già mature per le persone, in un'unica struttura. Il 64% delle organizzazioni governa già le identità di macchine e agenti con piattaforme centralizzate.

Il rapporto articola l'architettura in quattro pilastri: accesso, governo, dati e sicurezza. E il percorso in tre tappe: scoprire, governare, proteggere. La prima chiede un inventario di account di servizio, token, script e agenti, con un responsabile per ciascuno e l'individuazione dell'IA non autorizzata.

Le tappe successive portano all'automazione di assegnazione, modifica e revoca dei privilegi, alla rotazione delle credenziali e, infine, ad autorizzazioni dinamiche con accessi temporanei e contenimento automatico.

I benefici dichiarati

Il rapporto lega la maturità ai risultati. Il 62% di chi ha investito nella sicurezza delle identità non umane riferisce guadagni di produttività

misurabili. Il 46% parla di rilasci dell'IA più rapidi e sicuri. Il 76% si aspetta che una governance più forte migliori l'accesso alle polizze cyber o le loro condizioni.

Sono risposte dichiarate dagli intervistati, non verifiche indipendenti. Le indicazioni di fondo sono di buon senso, ma coincidono con la linea commerciale di SailPoint, che lo stesso giorno ha presentato prodotti pensati per gli agenti di IA.

Cosa manca

Cosa resta da verificare

Il rapporto completo 2026-2027 non è stato consultato per intero. Il dossier si fonda sul comunicato ufficiale e su articoli che lo riprendono. Le percentuali non pubblicate, come la ripartizione fra tutti e cinque gli Horizon, restano da controllare sul documento originale.

Il campione è di 340 intervistati e le risposte sono autovalutazioni. Le definizioni dei livelli e del 2% di strumenti «costruiti su misura» sono di SailPoint.

Due punti sono ambigui. Il comunicato attribuisce all'«80% dei leader» la fiducia nel proprio livello di strumenti, mentre Channel Insider la riferisce ai leader del settore tecnologico. Il dato del 49% sul bilanciamento è presente solo nell'articolo di The Hacker News.

Fonti

Le fonti del dossier

- The Hacker News, «The AI Velocity Paradox: Why Security Is Decades Behind AI Ambition», 9 ottobre 2026, contributo di un partner: thehackernews.com
- SailPoint, comunicato sul rapporto Horizons of Identity Security 2026, 6 ottobre 2026: globenewswire.com
- Channel Insider, «SailPoint Finds AI Agent Adoption Far Outpacing Identity Security», 7 ottobre 2026: channelinsider.com
- Yahoo Finance, «SailPoint's 40x Gap», sulla conferenza Navigate 2026: finance.yahoo.com
- SailPoint, «From chaos to control», annuncio dei prodotti per l'identità degli agenti: sailpoint.com

- SailPoint, comunicato sull'edizione 2025-2026 (375 intervistati): nasdaq.com
-

- Il passaggio decisivo è la lettura del rapporto completo 2026-2027, che permetterà di controllare definizioni dei livelli e percentuali non pubblicate.

© Alground · 9 ottobre 2026 · Versione PDF del dossier pubblicato su alground.com