AI Pulse Survey, Vol. 4: la visibilità sull'AI come abilitatore di sicurezza

Il contesto: una doppia realtà nel panorama cyber

Il 2026 si sta confermando come l'anno in cui l'intelligenza artificiale ha smesso di essere un tema di sola innovazione per diventare, a tutti gli effetti, una variabile centrale della postura di cybersecurity aziendale. Attori state-sponsored e gruppi criminali stanno utilizzando l'AI per accelerare e scalare gli attacchi, sfruttando le debolezze nelle catene di fornitura software, nelle applicazioni SaaS e nei processi di terze parti. Le frodi tramite deepfake, in particolare, rappresentano oggi la minaccia di social engineering a maggiore crescita per le imprese.

In questo scenario, la quarta edizione dell'AI Pulse Survey di Protiviti, dedicata a cybersecurity e resilienza, restituisce un'istantanea preoccupante: l'IT e la sicurezza operativa percepiscono un'escalation significativa delle minacce derivate dall'AI, mentre la C-suite e i Board ne hanno una lettura più moderata. È questa disconnessione che dà il titolo al report: senza visibilità non può esserci fiducia. E senza fiducia fondata su evidenze, ogni decisione di investimento sui controlli rischia di poggiare su informazioni obsolete.

1. Un blind spot strutturale: il vero utilizzo degli strumenti AI

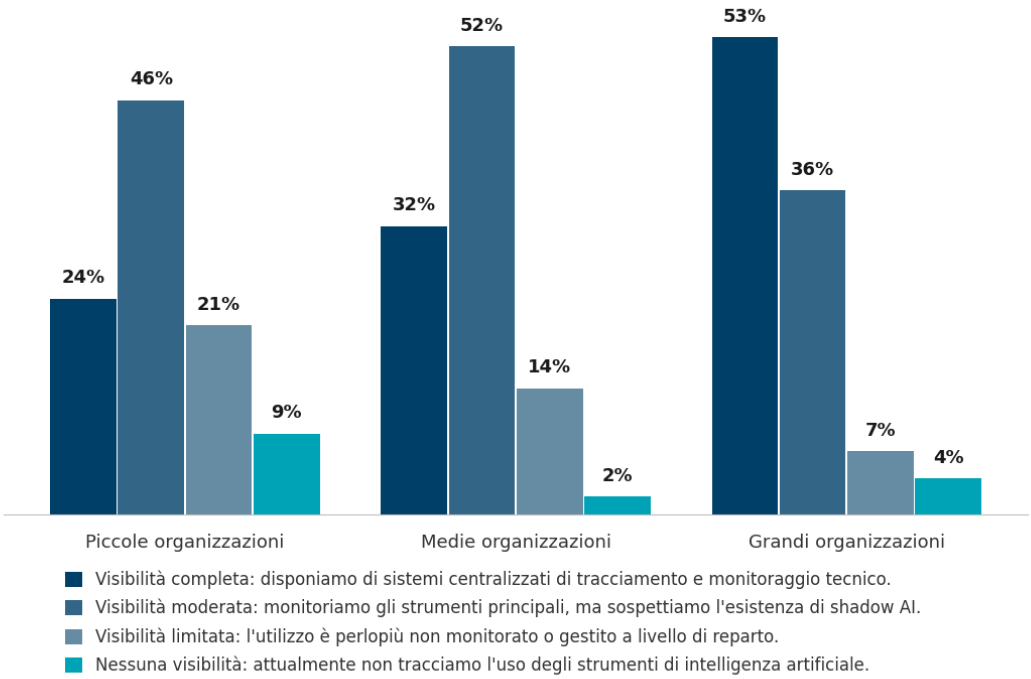
Il primo dato che colpisce è la diffusione dello "Shadow AI", ovvero l'utilizzo di strumenti, modelli o funzionalità basate su intelligenza artificiale all'interno dell'organizzazione senza approvazione formale, visibilità o controlli di governance, tipicamente al di fuori del perimetro di IT e security.

La piena visibilità sull'uso degli strumenti AI da parte dei dipendenti rappresenta oggi l'eccezione, non la norma. Anche tra le grandi organizzazioni (con oltre 5 miliardi di dollari di fatturato), soltanto il 53% dichiara di avere visibilità completa, il 47% non ha piena consapevolezza dei rischi associati. Il dato peggiora sensibilmente per le aziende di fascia media (tra 100 milioni e 5 miliardi di fatturato), dove il 68% ammette di avere visibilità solo parziale o nulla.

Le cause sono strutturali: piattaforme tecnologiche ridondanti, controlli applicati in modo disomogeneo tra unità di business, geografie diverse e processi di compliance normativa frammentati a seguito di operazioni di M&A.

Nelle realtà più piccole, dove le capacità di discovery sono meno sofisticate e le procedure di approvazione meno rigorose, lo Shadow AI prolifera e passa inosservato. Pertanto, le conseguenze sono evidenti. Strumenti, applicazioni e plug-in non autorizzati sono utilizzati liberamente, meccanismi di governance risultano incoerenti e ciò produce un indebolimento progressivo della protezione del dato. Quando il vertice non vede i propri punti ciechi, non condivide l'urgenza di rilevare le minacce. **E ciò che non si vede non si può difendere.**

Figura 2: **Come descriveresti la visibilità della tua organizzazione sugli specifici strumenti di intelligenza artificiale (sia autorizzati sia non autorizzati) attualmente utilizzati dai dipendenti?**

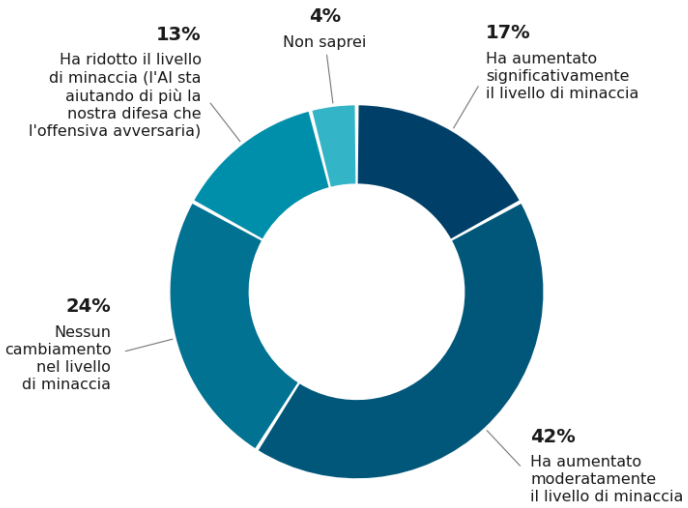


2. Il divario della percezione del pericolo: vertice e prima linea vedono due rischi diversi

Il secondo dato di interesse tocca un nervo scoperto della governance. La percezione delle minacce AI cambia radicalmente a seconda del livello gerarchico osservato. Il 45% dei responsabili di IT e Security Operations ritiene che l'AI abbia aumentato significativamente il livello di minaccia cyber. Tra C-suite e membri del Board, la stessa percezione si ferma al 30%.

Questo scarto non è un dettaglio di nomenclatura. Storicamente, simili disallineamenti venivano attribuiti al fisiologico ritardo con cui le nuove tecnologie vengono assorbite dalle organizzazioni e con cui le evidenze di rischio risalgono dalla linea operativa al management. Ma nell'attuale panorama di minacce AI-enabled, questi ritardi sono pericolosi e si traducono in priorità definite con valutazioni incoerenti, controlli/mitigazione senza sufficienti investimenti e decisioni di governance basate su una fotografia che non corrisponde più al presente.

Figura 1: **Valutazione complessiva del livello di minaccia — risultati totali**



Le ricadute concrete del divario di percezione

- **Rallentamenti decisionali**: contro deepfake e attacchi AI-driven, in cui ogni minuto di ritardo nel contenimento e nella comunicazione conta, una governance lenta è una vulnerabilità a tutti gli effetti.
- **Overconfidence nei controlli:** la sicurezza percepita ai vertici può tradursi in una sottostima di processi e controlli specifici per l'AI, con il rischio che l'adozione corra più veloce della capacità di mitigare le insidie.
- **Erosione del supporto del Board:** se le minacce vengono sottovalutate, anche i budget per la cyber-resilienza rischiano di non garantire sufficiente supporto alla realizzazione delle mitigazioni necessarie.

3. La fiducia nei controlli non è universale

Il terzo dato mette in dubbio il tono rassicurante che spesso accompagna le comunicazioni interne sulla cybersecurity. La maggioranza dei leader intervistati dichiara fiducia nella capacità dei propri controlli di tenere il passo con le minacce AI-driven. Ma quasi un dirigente su tre (il 30%) non esprime un grado di assurance, forte del fatto che i presidi attuali siano effettivamente all'altezza.

Anche qui, il dato si stratifica in modo significativo. Tra le grandi organizzazioni, la quota di chi si dichiara meno fiducioso scende al 21%, segno di processi e dotazioni più strutturate. Tra le piccole imprese, invece, sale al 39%: oltre un terzo riconosce esplicitamente di non avere solide garanzie. E in ogni dimensione, la fiducia cala via via che ci si allontana dalla C-suite per avvicinarsi ai team

operativi, i quali gestiscono in prima persona gli incidenti e ne osservano da vicino la complessità crescente.

Il messaggio per Board e Top Management è esplicito: la fiducia espressa al vertice non sostituisce l'evidenza osservate delle linee operative. Chi opera ogni giorno sui sistemi sta segnalando che il livello di sicurezza va consolidato con investimenti specifici, non rassicurazioni di principio.

4. Formalizzazione di framework di AI Governance

Se le prime tre evidenze descrivono un problema, la quarta inizia a indicare una soluzione concreta. Quattro organizzazioni su dieci (41%) dichiarano oggi di avere un framework formale di AI governance, mentre un ulteriore 43% è in fase di implementazione. La diffusione cresce significativamente con la dimensione aziendale: si passa dal 30% delle piccole imprese al 39% delle medie, fino al 64% delle grandi.

Il dato più rilevante, però, non riguarda l'adozione in sé, bensì la sua correlazione con altri indicatori di maturità. L'intervista evidenzia chiaramente che dove esiste un framework formale, cresce anche la visibilità sugli strumenti AI utilizzati, aumenta la confidenza nei controlli e si riducono i casi di leader meno fiduciosi delle proprie difese. In altre parole, il framework non è un esercizio documentale: è il meccanismo che converte l'intenzione di governare l'AI in evidenze misurabili.

Un framework di AI governance non ferma gli attacchi e non elimina le minacce esterne. Ma affronta una sfida diversa e altrettanto critica legata a regolare con chiarezza ruoli, responsabilità e coerenza. Oltre a ciò, definisce la proprietà dei processi, fissa standard di uso accettabile, stabilisce aspettative di monitoraggio sui sistemi AI in produzione. Per il Board e la C-suite, è il modo più efficace per smettere di governare il rischio AI sulla base di assunzioni e iniziare a farlo sulla base di evidenze documentate.

Tabella 1: **Più framework formalizzati, controlli più solidi**

Lente di analisi	Framework formale adottato	Visibilità completa sugli strumenti AI	Bassa fiducia nei controlli di sicurezza
Totale campione	41%	35%	30%
Grandi organizzazioni	64%	53%	21%
Medie organizzazioni	39%	32%	26%
Piccole organizzazioni	30%	24%	39%

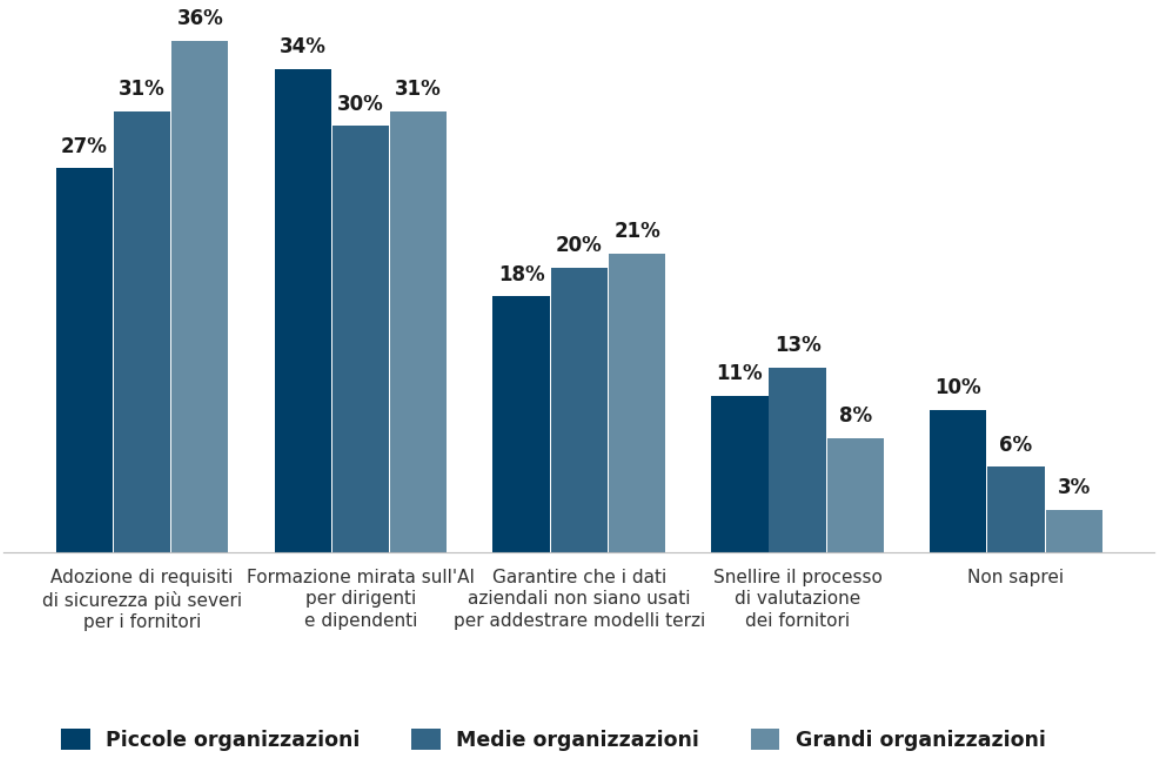
5. AI nei software di terzi

L'ultimo grande tema affrontato dalla ricerca riguarda l'intelligenza artificiale che i fornitori stanno integrando, spesso senza troppo clamore, dentro i software che le aziende usano ogni giorno. La velocità con cui questa integrazione sta avvenendo nelle suite gestionali, nelle piattaforme in cloud, negli strumenti di produttività, ha aperto un nuovo punto cieco. Si tratta di funzionalità di AI gestite dal fornitore, attive nei processi interni dell'azienda, ma spesso sono prive di una vera supervisione e con perimetri d'uso poco definiti.

Alla domanda su quale sia la leva più importante per gestire questo rischio, i dirigenti hanno indicato in prima posizione l'adozione di requisiti di sicurezza più severi nei confronti dei fornitori: lo dichiara il 32% del campione complessivo, percentuale che sale al 36% tra le grandi organizzazioni. Subito dopo, con valori molto simili, compare la formazione mirata sull'intelligenza artificiale rivolta sia ai dirigenti sia ai dipendenti. È un dato che merita attenzione, perché conferma quanto le aziende, soprattutto quelle più strutturate, riconoscano l'importanza del giudizio umano nelle approvazioni e nelle decisioni di tutti i giorni.

Particolarmente rilevante, infine, è il peso crescente di una richiesta che le aziende stanno mettendo nero su bianco nei contratti, ovvero la garanzia che i propri dati non vengano usati per addestrare i modelli di intelligenza artificiale dei fornitori. È il segnale di una nuova consapevolezza su come le informazioni aziendali vengono raccolte, conservate e, in alcuni casi, riutilizzate. E indica un'evoluzione delle clausole contrattuali nella direzione di una maggiore tracciabilità e verificabilità.

Figura 3: **Qual è la priorità principale della tua organizzazione nel gestire i rischi legati all'AI integrata nei software dei fornitori?**



** L'1% delle grandi organizzazioni ha selezionato "altro"*

Le cinque leve abilitanti

Le organizzazioni che si dichiarano più fiduciose nella gestione dei rischi AI sono quelle che hanno investito di più in capacità concrete in grado di trasformare l'intenzione ("prendiamo il rischio AI sul serio") in evidenza ("lo vediamo, lo governiamo, lo difendiamo").

Il report identifica cinque leve abilitanti su cui investire:

- **Framework formale di AI governance:** definire con chiarezza cosa è consentito e cosa no, a chi spetta la responsabilità delle decisioni e quali limiti non possono essere superati, in modo che la diffusione dell'AI non vada più veloce della capacità dell'azienda di tenerla sotto controllo.
- **Monitoraggio degli strumenti AI:** investire in sistemi capaci di rilevare quali strumenti di AI vengono effettivamente utilizzati dai dipendenti, così da intercettare per tempo gli usi non autorizzati e dimostrare, con dati alla mano, che i controlli aziendali stanno funzionando.
- **Readiness e resilienza organizzativa:** ridurre il rischio di errori umani e costruire un modo coerente di lavorare con l'intelligenza artificiale in tutta l'azienda, perché la tecnologia da sola non basta se le persone non sanno come usarla.
- **L'intelligenza artificiale al servizio della difesa:** integrare strumenti di intelligenza artificiale all'interno dei sistemi di sicurezza aziendali consente di individuare gli attacchi più rapidamente, riconoscere meglio gli schemi sospetti e rispondere con maggiore efficacia a minacce che, a loro volta, sono accelerate dall'AI.
- **Presìdi sui fornitori per l'AI integrata:** chiudere il punto cieco che si sta allargando con la diffusione di funzionalità di intelligenza artificiale all'interno delle piattaforme in cloud e degli strumenti forniti da terze parti, dove l'AI lavora di fatto in modo invisibile all'interno dei sistemi aziendali.

Metodologia

L'AI Pulse Survey, Vol. 4 è stata condotta da Protiviti nel febbraio 2026 su un campione di 863 partecipanti, di cui 150 tra Board member e C-suite. Per garantire l'accuratezza dell'analisi, le risposte di leader tecnici, operativi ed esecutivi sono state isolate. Tra i C-suite: i CEO rappresentano la quota maggiore (37%), seguiti da CTO (19%), CIO (13%), CFO (11%) e COO (10%). I responsabili IT pesano per circa un terzo del campione complessivo (31%). I rispondenti provengono da una pluralità di settori, guidati da: Technology (10%), Pubblica Amministrazione (8%), Retail (8%), Manufacturing (7%) e Aerospace & Defence (6%), e da una base geografica internazionale: Stati Uniti (41%), India (14%), Regno Unito (12%), Australia (10%) e Canada (9%).

Contatti

Emma Marcandalli
Managing Director
emma.marcandalli@protiviti.com

Luca Risi
Managing Director
luca.risi@protiviti.com

Enrico Ferretti
Managing Director
enrico.ferretti@protiviti.com

Nicola Dalla Benetta
Director
nicola.dallabenetta@protiviti.com