

# Fai uscire l'IA dall'ombra.

## Adotta e usa l'IA con fiducia.

Le organizzazioni stanno adottando l'IA più velocemente di quanto riescano a gestirla. Dati sensibili vengono condivisi, gli agenti operano senza visibilità e i team di sicurezza spesso mancano di informazioni su quali strumenti vengano utilizzati. Basato su Sophos Fusion, Sophos AI Defense ti aiuta a scoprire, comprendere e controllare l'uso dell'IA nel tuo intero ambiente.

69%

delle aziende sospetta o dispone di prove che i dipendenti utilizzino servizi pubblici di IA non autorizzati<sup>1</sup>

82%

Percentuale di organizzazioni che hanno rilevato strumenti o flussi di lavoro di IA sconosciuti<sup>2</sup>

90%

Percentuale di IT Manager che esprimono preoccupazioni sul rischio della shadow AI<sup>3</sup>

1,3Mld

Numero previsto di agenti IA entro il 2028<sup>4</sup>

## COSA OFFRE SOPHOS

### Vedi l'IA. Controlla l'IA. Proteggi l'IA.

#### Vedi cosa sta facendo davvero l'IA.

La visibilità inizia da ciò che accade realmente,, non solo da ciò che è approvato.

- Rileva l'uso dell'IA tra dipendenti, strumenti e flussi di lavoro
- Convalida gli strumenti approvati e rileva eventuali utilizzi non autorizzati
- Ottieni visibilità continua sui punti di interazione a livello di browser, endpoint e rete

#### Individua i comportamenti dell'IA che contano davvero.

Non tutte le attività dell'IA introducono esposizione a rischi, ma senza contesto i team non sono in grado di distinguere tra un uso approvato e comportamenti che richiedono un intervento.

- Valuta l'uso dell'IA includendo identità, comportamento e contesto dei dati
- Distingui tra uso accettabile e attività non gestite, con privilegi eccessivi o a rischio
- Concentrati sulla reale esposizione al rischio, invece di reagire a eventi isolati o a basso impatto

#### Trasforma le policy sull'IA in controllo.

Man mano che l'adozione dell'IA aumenta, le policy statiche diventano inefficaci. L'implementazione deve essere continua e concreta.

- Applica barriere protettive sulle modalità reali di utilizzo dell'IA, non solo su ciò che è definito nelle policy.
- Implementa controlli nei punti chiave di interazione per allineare l'uso dell'IA e la condivisione dei dati alle policy e alle normative
- Riduci la shadow AI guidando gli utenti verso strumenti approvati

#### Integra l'IA nelle operazioni di sicurezza.

L'IA amplia la superficie di attacco, introducendo nuovi rischi legati a prompt, dati e azioni guidate da agenti che richiedono una gestione attiva.

- Evidenzia usi impropri, abusi e compromissioni dell'IA nei flussi di lavoro di rilevamento e indagine
- Integra l'attività dell'IA nella telemetria di sicurezza più estesa
- Applica gli stessi playbook, strumenti e percorsi di escalation utilizzati per le minacce standard

## SOPHOS AI DEFENSE IN SINTESI

- Rileva l'uso dell'IA tra dipendenti, strumenti e flussi di lavoro, inclusa la shadow AI
- Identifica i comportamenti rischiosi con informazioni su identità, esposizione dei dati e contesto di utilizzo
- Applica barriere protettive nei punti di interazione a livello di browser, endpoint e rete
- Previene la condivisione di dati sensibili con gli strumenti di IA ispezionando prompt, caricamenti e interazioni con l'IA in tempo reale
- Integra il rischio legato all'IA nei flussi di lavoro delle operazioni di sicurezza

## A CHI SI RIVOLGE SOPHOS AI DEFENSE

- Cybersecurity Manager che hanno bisogno di visibilità e controllo sull'uso dell'IA
- Team di Security Operations incaricati di individuare e rispondere ai rischi derivanti dall'IA
- Organizzazioni che desiderano adottare e distribuire strumenti di IA in modo sicuro
- Aziende che vogliono valorizzare gli investimenti di sicurezza esistenti per gestire il rischio legato all'IA

## PRIORITÀ PER I RISCHI REALI DELL'IA

### Sicurezza pratica per l'IA, progettata per il modo in cui viene utilizzata realmente.

#### Risolvi i rischi legati all'IA del presente, non le ipotesi future.

La maggior parte delle soluzioni protegge i modelli o le applicazioni. Sophos AI Defense affronta ciò che ti mette effettivamente a rischio oggi:

- Uso non gestito dell'IA da parte del personale
- Visibilità limitata su strumenti, agenti e flussi di lavoro
- Dati sensibili condivisi con strumenti di IA esterni tramite prompt e flussi di lavoro automatizzati

#### Estendi la sicurezza che hai già.

Sophos AI Defense si basa sui controlli già esistenti, coordinandoli per fornire risultati immediati e pratici.

- Valorizza il tuo investimento in Sophos Workspace Protection, EDR, Firewall, XDR e MDR
- Connette i punti di controllo in un framework unificato di policy sull'IA
- Offre valore immediato, senza bisogno di nuove implementazioni o risorse extra

#### Converti la visibilità in risultati, non solo in ulteriori dati.

La visibilità, da sola, non basta. Sophos AI Defense trasforma le informazioni in azione:

- Combina visibilità, analisi del contesto e implementazione in un unico sistema, monitorando l'uso dell'IA, i movimenti dei dati e l'attività degli agenti
- Applica policy, assegna priorità ai problemi e rispondi all'interno degli stessi flussi di lavoro
- Garantisce risultati controllati, non semplicemente altre dashboard

## RICONOSCIMENTI UFFICIALI DEGLI ESPERTI DI SETTORE

### Riconosciuto ufficialmente dagli analisti e dalle organizzazioni più autorevoli.

#### GARTNER 2026

Leader, Endpoint Protection

#### VALUTAZIONI DI MITRE ATT&CK

100% di copertura del rilevamento

#### G2 SUMMER 2026

N°1 per le soluzioni XDR e MDR

#### GARTNER PEER INSIGHTS

Una delle "Customers' Choice" per XDR e MDR

### Un unico sistema. Tutti i punti di controllo. Che proteggono come una singola entità.

Sophos AI Defense fa parte di Sophos Fusion, il più completo sistema di cyber difesa al mondo. Protegge le organizzazioni dalle minacce basate sull'IA che si propagano più velocemente di quanto i team di sicurezza siano in grado di rispondere.

[sophos.it/ai-defense](https://sophos.it/ai-defense) →

<sup>1</sup> Gartner, Shadow AI Demands Stricter Endpoint Application Control, 25 maggio 2026. <sup>2</sup> CSA, The Shadow AI Agent Problem in Enterprise Environments, 2025. <sup>3</sup> Indagine Komprise IT: AI, dati e rischio aziendale. AI, Data & Enterprise Risk. <sup>4</sup> IDC Info Snapshot, sponsorizzato da Microsoft, 1,3 miliardi di agenti IA entro il 2028, #US53361825, maggio 2025.

I contenuti di Gartner Peer Insights sono una raccolta delle opinioni di utenti finali individuali, basate sulle relative esperienze; non devono essere interpretati come affermazioni di fatto, né come rappresentazione delle opinioni di Gartner o dei suoi affiliati. Gartner non appoggia alcun fornitore, produttore o servizio citato nei suoi contenuti, né fornisce alcuna garanzia, espressa o implicita, in riferimento a tali contenuti, alla loro accuratezza o completezza, inclusa qualsivoglia garanzia sulla commerciabilità o sull'idoneità a un particolare scopo. GARTNER è un marchio registrato e un marchio di servizio di Gartner, Inc. e/o dei suoi affiliati negli U.S.A. e a livello internazionale, PEER INSIGHTS è un marchio registrato di Gartner Inc. e/o dei suoi affiliati e viene qui adoperato con la dovuta autorizzazione. Tutti i diritti riservati. Gartner®, Peer Insights™, Voice of the Customer for Extended Detection and Response, Peer Contributors, 23 maggio 2025. Gartner®, Peer Insights™, Voice of the Customer for Managed Detection and Response, con il contributo di professionisti del settore, 31 marzo 2026.