

Saque la IA de las sombras.

Adopte y utilice la IA con confianza.

Las organizaciones están adoptando la IA a un ritmo más rápido del que pueden gestionar. Se comparten datos confidenciales, los agentes operan sin visibilidad y, a menudo, los equipos de seguridad carecen de información sobre qué herramientas se están utilizando. Basado en Sophos Fusion, Sophos AI Defense le ayuda a detectar, comprender y controlar el uso de la IA en todo su entorno.

69%

de organizaciones que sospechan o tienen evidencia de que sus empleados están utilizando servicios públicos de IA prohibidos¹

82%

de las organizaciones identificaron herramientas o flujos de trabajo de IA que desconocían²

90 %

de los responsables de TI expresan su preocupación por el riesgo de la IA en la sombra³

1,3 mil millones

Número previsto de agentes de IA para 2028⁴

QUÉ OFRECE SOPHOS

Vea la IA. Controle la IA. Proteja la IA.

Vea lo que hace la IA realmente.

La visibilidad comienza por lo que ocurre realmente, no solo por lo que está autorizado.

- Sepa cómo se utiliza la IA entre sus empleados, herramientas y flujos de trabajo
- Valide las herramientas autorizadas y detecte los usos no autorizados
- Obtenga una visibilidad continua en los puntos de interacción del navegador, los endpoints y la red

Identifique el comportamiento de la IA que más importa.

No todas las actividades relacionadas con la IA suponen un riesgo, pero sin contexto, los equipos no pueden distinguir entre un uso autorizado y un comportamiento que justifique tomar medidas.

- Evalúe el uso de la IA, incluyendo la identidad, el comportamiento y el contexto de los datos
- Distinga entre el uso aceptable y las actividades no gestionadas, con privilegios excesivos o de riesgo
- Céntrese en una exposición significativa en lugar de reaccionar ante incidentes aislados o de bajo impacto

Convierta la política en materia de IA en un mecanismo de control.

A medida que se generaliza la adopción de la IA, las políticas estáticas dejan de ser eficaces. Su aplicación debe ser continua y exigible.

- Establezca medidas de protección en torno al uso de la IA, y no solo a su definición en las políticas
- Aplique controles en los puntos de interacción clave para que el uso de la IA y el intercambio de datos se ajusten a las políticas y normativas
- Reduzca el uso de la IA en la sombra orientando a los usuarios hacia herramientas autorizadas

Integre la IA en las operaciones de seguridad.

La IA amplía la superficie de ataque, con nuevos riesgos relacionados con los prompts, los datos y las acciones impulsadas por los agentes que requieren una gestión activa.

- Haga aflorar los usos indebidos, las prácticas malintencionadas y las vulnerabilidades relacionadas con la IA en los flujos de trabajo de detección e investigación
- Integre la actividad de la IA en la telemetría de seguridad más amplia
- Aplique los mismos manuales de procedimientos, herramientas y vías de derivación que se utilizan para las amenazas habituales

SOPHOS AI DEFENSE DE UN VISTAZO

- Sepa cómo se utiliza la IA entre sus empleados, herramientas y flujos de trabajo, incluida la IA en la sombra
- Identifique los comportamientos de riesgo basándose en la identidad, la exposición de datos y el contexto de uso
- Implemente medidas de protección en los puntos de interacción del navegador, los endpoints y la red
- Evite que se compartan datos confidenciales con las herramientas de IA mediante la supervisión en tiempo real de los prompts, las cargas de archivos y las interacciones con la IA
- Integre los riesgos relacionados con la IA en los flujos de trabajo de las operaciones de seguridad

A QUIÉN VA DIRIGIDO SOPHOS AI DEFENSE

- Responsables de seguridad que necesitan visibilidad y control sobre el uso de la IA
- Equipos de operaciones de seguridad encargados de identificar y dar respuesta a los riesgos derivados de la IA
- Organizaciones que desean adoptar e implementar herramientas de IA de forma segura
- Empresas que desean ampliar sus inversiones actuales en seguridad para gestionar los riesgos relacionados con la IA

EL ENFOQUE EN LOS RIESGOS REALES DE LA IA

Seguridad práctica para la IA, diseñada teniendo en cuenta el uso real que se le da.

Resolver los riesgos actuales de la IA, no las hipótesis futuras.

La mayoría de las soluciones protegen modelos o aplicaciones. Sophos AI Defense aborda lo que realmente supone un riesgo hoy en día:

- El uso no controlado de la IA por parte de los empleados
- La visibilidad limitada sobre las herramientas, los agentes y los flujos de trabajo
- El intercambio de datos confidenciales con herramientas de IA externas a través de prompts y flujos de trabajo automatizados

Extender la seguridad que ya tiene.

Sophos AI Defense se basa en sus controles actuales y los coordina para ofrecer resultados inmediatos y prácticos.

- Amplía su inversión en Sophos Workspace Protection, EDR, Firewall, XDR y MDR.
- Conecta los puntos de control en un marco unificado de políticas de IA
- Ofrece valor inmediato: no requiere desplegar nada ni recursos adicionales

Transformar la visibilidad en resultados, no solo en más datos.

La visibilidad por sí sola no es suficiente. Sophos AI Defense convierte la información en acción:

- Combine la visibilidad, el contexto y la aplicación de medidas en un único sistema que abarque el uso de la IA, la transferencia de datos y la actividad de los agentes
- Aplique políticas, priorice los problemas y responda sin salir de los mismos flujos de trabajo
- Ofrezca resultados controlados, no solo más paneles de control.

RECONOCIMIENTO DEL SECTOR

Reconocido oficialmente por los analistas y las organizaciones más prestigiosas.

GARTNER 2026

Líder, Endpoint Protection

G2 DE VERANO 2026

Soluciones n.º 1 en materia de XDR y MDR

EVALUACIONES MITRE ATT&CK

100% de cobertura de detección

GARTNER PEER INSIGHTS

Distinción "Customers' Choice" para XDR y MDR

Un único sistema. Todos los puntos de control. Una defensa coordinada.

Sophos AI Defense forma parte de Sophos Fusion, el sistema de ciberdefensa más completo del mercado. Protege a las organizaciones frente a las amenazas optimizadas por IA, capaces de actuar más rápido que los equipos de defensa.

sophos.com/ai-defense →

¹ Gartner, Shadow AI Demands Stricter Endpoint Application Control, 25 de mayo de 2026. ² CSA, "The Shadow AI Agent Problem in Enterprise Environments", 2025. ³ Komprise IT Survey: AI, Data & Enterprise Risk. ⁴ IDC Info Snapshot, patrocinado por Microsoft, 1.300 millones de agentes de IA para 2028, #US53361825, mayo de 2025.

El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias; no deben considerarse declaraciones de hecho, ni representan las opiniones de Gartner ni de sus afiliados. Gartner no apoya a ningún proveedor, producto o servicio descrito en este contenido ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comercialización o conveniencia para fines particulares. GARTNER es una marca de servicio y marca registrada de Gartner, Inc. y/o asociados en EE. UU. y en otros países, y PEER INSIGHTS es una marca registrada de Gartner, Inc. y/o asociados y se utiliza aquí con su permiso. Reservados todos los derechos. Gartner®, Peer Insights™, Voice of the Customer for Extended Detection and Response, Peer Contributors, 23 de mayo de 2025. Gartner®, Peer Insights™ Voice of the Customer for Managed Detection and Response¹ Peer Contributors, 31 de marzo de 2026.