Asegure la IA que se utiliza, diseña y ejecuta en todas partes.

RESUMEN DE LA SOLUCIÓN DE SEGURIDAD DE LA IA

La inteligencia artificial está transformando el funcionamiento de las organizaciones, pero también introduce una nueva y compleja superficie de ataque. Desde el uso no gestionado de la IA hasta la fuga de datos y la manipulación de modelos, las herramientas de seguridad tradicionales son incapaces de detectar los riesgos que conlleva la IA. Los equipos de seguridad deben adaptarse para proteger los datos confidenciales, garantizar el cumplimiento normativo y proteger contra las nuevas amenazas impulsadas por la inteligencia artificial.

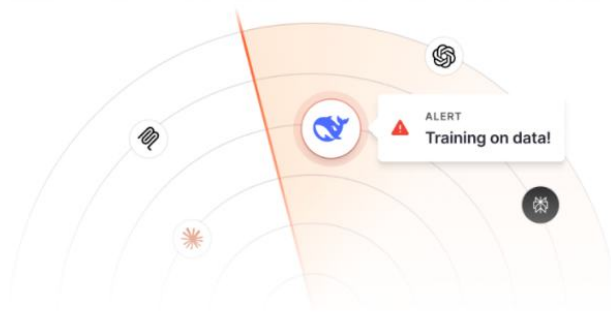
INTRODUCCIÓN

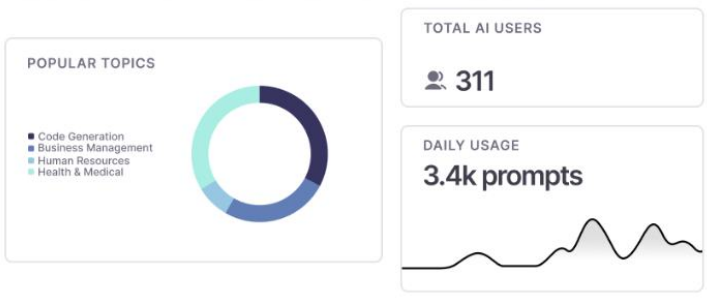
Una solución completa para asegurar cada interacción con la IA

Proteja todas las interacciones con la IA, desde el uso de IA de terceros hasta las aplicaciones y agentes de IA propios. Esta oferta aprovecha el motor de detección de IA más avanzado del sector y se integra fácilmente en cualquier entorno empresarial.

Descubra la Shadow IA

Identifique todas las aplicaciones y modelos de IA utilizados en su organización, junto con los riesgos asociados a ellos. Obtenga visibilidad sobre el uso oculto o no autorizado de la IA para evitar la exposición de datos y los riesgos de cumplimiento normativo.



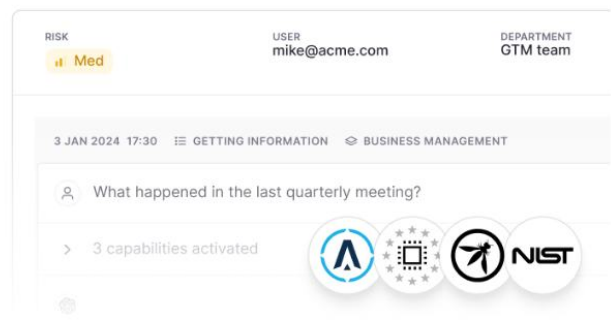


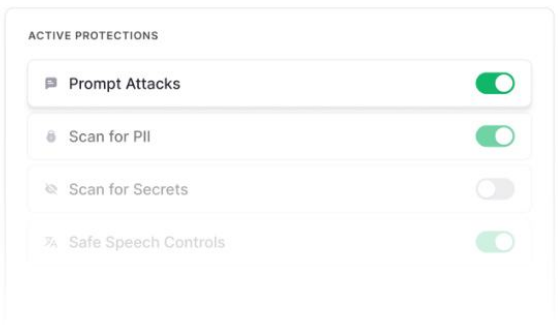
Gobierne y asegure las interacciones con la IA

Supervise y controle las indicaciones de los empleados y las interacciones del sistema con los servicios de IA. Aplique políticas de seguridad y gobernanza de datos para evitar el intercambio de información confidencial o el uso indebido de los resultados de la IA.

Asegure el ciclo de vida de los desarrollos de IA

Evalúe y fortalezca continuamente sus ciclos de desarrollo de IA. Descubra las vulnerabilidades debidas a configuraciones incorrectas en los modelos y los procesos antes de que lleguen a la fase de producción.



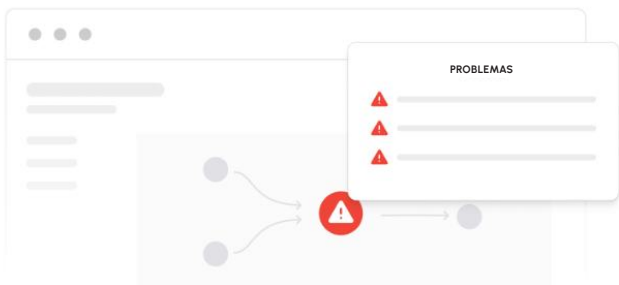


Proteja las aplicaciones de IA de producción propia

Detecte y bloquee ataques como la inyección de comandos, la exfiltración de datos y las cargas maliciosas con protecciones avanzadas en tiempo de ejecución, lo que garantiza que sus aplicaciones de IA propias sigan siendo fiables, conformes y resistentes durante todo el funcionamiento.

Proteja los agentes de IA que crea y ejecuta

Descubra y evalúe los riesgos en sus sistemas y aplicaciones de inteligencia artificial y despliegue medidas de protección de vanguardia en tiempo de ejecución para protegerlos contra la inyección de comandos, el envenenamiento de datos y el acceso no autorizado.



"La solución proporciona un valor inmenso a múltiples partes interesadas en nuestra organización, en los equipos de seguridad, comerciales y legales. Me encanta el hecho de que garantice todo el alcance de nuestro uso de la IA generativa, independientemente de dónde se aplique".

Drew Robertson, CISO — FINANCE of AMERICA

Gartner COOL VENDOR 2025 FOR AGENTIC AI TRISM

Aim Security, ahora parte de Cato Networks, reconocida como proveedor destacado por Gartner en gestión de riesgos de agentes. Gartner, Cool Vendors in Agentic AI TRiSM, 2 de septiembre de 2025.

Contacto