DARKTRACE

# Darktrace / SECURE AI™

Proteja su adopción de la IA con una IA adaptativa que ofrece visibilidad y control en tiempo real en prompts, agentes, entornos de desarrollo e IA en la sombra.

**88%**

**de las organizaciones**

utilizan la IA en al menos una función empresarial[1]

**80%**

**de los clientes de Darktrace**

ahora utilizan servicios de IA generativa[2]

**44%**

**de los profesionales de la seguridad**

están muy o extremadamente preocupados por los agentes de IA[3]

## La adopción de la IA está superando el control empresarial

La IA ha entrado en la empresa a un ritmo rápido que no hace más que acelerarse. Mientras la adopción y la innovación avanzan, la seguridad todavía se está poniendo al día. Las organizaciones se enfrentan ahora a un problema de seguridad de la IA, en el que el riesgo se acumula de forma silenciosa en flujos de trabajo, herramientas, datos y decisiones, a menudo sin ninguna visibilidad.

La naturaleza adaptativa e impredecible de la IA hace que una seguridad eficaz exija una comprensión profunda de lo que es «normal» en las personas, los sistemas de IA y los agentes, de modo que los primeros indicios de desviación, uso indebido o vulneración puedan detectarse antes de que se agraven.

## BENEFICIOS EMPRESARIALES

**Visibilidad unificada de la IA**
Vea las interacciones de IA en toda la IA generativa empresarial, los agentes, la actividad de desarrollo y la IA en la sombra a través de una única vista de inteligencia basada en el comportamiento.

**Detección de riesgos en tiempo real**
Detecte el uso indebido sutil, las desviaciones y los riesgos emergentes en los prompts y el comportamiento de los agentes a medida que se producen, sin depender de reglas predefinidas.

**Gobernanza alineada con las políticas**
Vincule la política de su propia organización con la actividad de la IA, de modo que la gobernanza esté alineada con las prioridades del negocio y se evalúe en función de cómo se utiliza realmente la IA.

**Adopción de la IA con confianza a escala**
Amplíe el uso de la IA en toda la empresa con la visibilidad, la comprensión y la supervisión necesarias para gestionar el riesgo a escala.

1: Estado de la IA de McKinsey 2025
2: Investigación de Darktrace
3: Estado de la ciberseguridad de la IA de Darktrace 2026

## Llevar la seguridad basada en el comportamiento a su adopción de la IA

**Impulsado por la IA adaptativa, Darktrace / SECURE AI aplica más de una década de comprensión del comportamiento para proteger el modo en que se utilizan los prompts, los agentes y los sistemas de IA en toda su empresa.**

En lugar de basarse en reglas predefinidas o firmas, aprende los patrones operativos de su organización y saca a la luz el uso indebido, las configuraciones incorrectas y las desviaciones que los controles tradicionales basados en reglas no están diseñados para detectar.

Ofrecido a través de Darktrace Platform Portal, Darktrace / SECURE AI reúne las interacciones de IA en una única vista, lo que ayuda a los equipos a comprender la intención, evaluar el riesgo, proteger los datos confidenciales y aplicar políticas tanto en la actividad humana como en la de los agentes de IA.

### DISEÑADO PARA LA IA EN SU EMPRESA

| | |
|---|---|
| GenAI empresarial | Agentes de IA |
| Low-Code | High-Code / IA en la nube |
| IA en la sombra | SaaS |
| MCP | SASE |

# Cómo protege Darktrace su IA

**La IA adaptativa de Darktrace ya interpreta la ambigüedad, descubre intenciones sutiles y detecta desviaciones antes de que las actividades o los eventos se vuelvan peligrosos en toda su empresa.**

Extender ese mismo enfoque basado en el comportamiento a la IA es el siguiente paso natural, no un salto, y se basa en la Darktrace Behavioral Defense Platform™, que ya protege a las personas y la infraestructura.

## Descubra y controle la IA en la sombra

Darktrace le ayuda a detectar actividad de IA no autorizada o inesperada dondequiera que aparezca, incluida la creación no autorizada de agentes de low-code y la infraestructura agéntica oculta, como los servidores MCP implementados localmente, al combinar la visibilidad nativa de / SECURE AI con fuentes de datos de red, nube, endpoint y SASE. Las políticas y vías de respuesta adecuadas para el entorno ayudan posteriormente a contener la exposición de datos y orientan a los usuarios hacia opciones autorizadas.

## Supervise los prompts que impulsan a los agentes y asistentes de GenAI

Darktrace / SECURE AI proporciona inspección en tiempo real de prompts, sesiones y respuestas en herramientas de IA empresarial como Microsoft Copilot y ChatGPT Enterprise, entornos low-code como Copilot Studio, entornos high-code como Amazon Bedrock y proveedores de SaaS como Salesforce y Microsoft 365. El análisis de comportamiento puede revelar desviaciones sutiles en la actividad de la IA que podrían indicar un riesgo emergente, lo que ayuda a las organizaciones a detectar posibles problemas como la exposición de datos confidenciales, intentos de jailbreak y otros comportamientos inseguros o imprevistos.

## Proteja las identidades de los agentes de IA en tiempo real

Puede descubrir las identidades de los agentes en todos los proveedores y entornos, mapear sus permisos, roles y conexiones, y auditar el comportamiento en SaaS, la nube, la red, el endpoint, la OT y el correo electrónico. Esta vista de auditoría en tiempo real ofrece a las organizaciones una comprensión clara de sus agentes de IA, incluidos el lugar donde están desplegados, cómo se utilizan y qué permisos tienen, lo que ayuda a los equipos a identificar riesgos potenciales y mantener la supervisión a escala.

## Evalúe los riesgos de la IA en el desarrollo y la implementación

Con Darktrace / SECURE AI, obtendrá visibilidad sobre las identidades, los permisos y los accesos que se configuran en herramientas de desarrollo low-code como Copilot Studio, plataformas high-code como Amazon Bedrock y laboratorios internos, con una gestión de la postura que señala configuraciones incorrectas y eventos anómalos de compilación antes de que un agente llegue a producción. / SECURE AI conecta entonces esa visibilidad del momento de compilación con el comportamiento en tiempo de ejecución.

# Elija la protección que necesita

**Darktrace / SECURE AI está disponible en paquetes diseñados para dar soporte a diferentes niveles de madurez en seguridad de la IA, siguiendo la misma ruta de adopción Core, Advanced y Complete que el resto de la Darktrace Behavioral Defense Platform.**

### CORE

Incluye análisis de prompts de IA y gestión integrada de la IA en la sombra para proporcionar visibilidad sobre el uso autorizado de la IA y el riesgo asociado, así como el mapeo de la alineación con las políticas.

### AVANCE

Amplía Core con la gestión profunda de Shadow AI, las identidades y acciones de los agentes y la gestión de riesgos en el desarrollo de agentes de IA para una supervisión más profunda de la actividad de la IA, el comportamiento de los agentes y el riesgo.

De inmediato, tuvimos acceso a la información que nos había faltado todo este tiempo: **quién utiliza qué dentro de nuestra organización** y **qué está haciendo con los datos**

- **Vicepresidente de TI, sector manufacturero de Estados Unidos**

**Acerca de Darktrace** Darktrace es líder mundial en IA para la ciberseguridad que permite a las organizaciones adelantarse cada día al panorama de amenazas en constante evolución. Fundada en 2013 en Cambridge (Reino Unido), Darktrace ofrece la plataforma de ciberseguridad esencial para proteger a las organizaciones frente a amenazas desconocidas mediante una IA que aprende de cada empresa en tiempo real. La plataforma y los servicios de Darktrace cuentan con el respaldo de 2.300 empleados que protegen a cerca de 10.000 clientes en todo el mundo. Para más información, visite darktrace.com.

América del Norte: +1 (415) 229 9100 | Europa: +44 (0) 1223 394 100 | Asia-Pacífico: +65 6804 5010 | América Latina: +55 11 4949 7696

darktrace.com | info@darktrace.com

© 2026 Darktrace Holdings Limited. Todos los derechos reservados.