

Forcepoint AI Data Security

Protege la IA. Empieza por los datos.

Desafío:

- › Los agentes de IA autónomos actúan sin supervisión y heredan permisos de usuario para consultar, agregar y transmitir datos sensibles a velocidad de máquina, sin intervención humana
- › La organización promedio tiene 37 agentes de IA en uso, la mayoría desconocidos para TI, que se propagan tan rápido como una extensión de navegador
- › Cada prompt enviado a un LLM público o a Copilot es una posible transferencia de datos que saca PII, código fuente y datos financieros del control de la empresa al instante

Soluciones:

- › Gobierna a los agentes autónomos en el punto de acción aplicando acceso de mínimo privilegio y controles basados en la identidad, de modo que cada acción quede atribuida y controlada
- › Descubre y controla la Shadow AI identificando de forma continua las herramientas no autorizadas y aplicando políticas de acceso antes de que se conviertan en una exposición sin gestionar
- › Extiende la protección de datos a cada prompt aplicando las políticas de clasificación y DLP existentes a prompts, respuestas y cargas de archivos en las plataformas de IA autorizadas

Resultados:

- › Adopta la IA con confianza y mantén una protección de datos coherente
- › Extiende las inversiones existentes en seguridad de datos a la IA sin tener que reconstruir las políticas
- › Demuestra una gobernanza de IA responsable con evidencia clara y auditable

La IA ha transformado el panorama de la seguridad de datos y ha abierto nuevas vías de riesgo que las herramientas de seguridad tradicionales no pueden bloquear. Los empleados comparten información sensible mediante prompts en lugar de archivos. Las herramientas de Shadow AI se propagan más rápido de lo que TI puede rastrear. Los agentes autónomos consultan y transmiten datos empresariales sin revisión humana. Lo que exige este momento es una seguridad que gobierne a qué puede acceder la IA antes de que lo alcance.

Gobierna cada interacción de IA desde una sola plataforma

Forcepoint AI Data Security extiende a cada interacción de IA la misma protección en la que ya se confía para otros canales.

Aplica automáticamente tu política de protección de datos existente a los prompts de IA, las respuestas de los agentes y el tráfico entre agentes y aplicaciones, sin necesidad de reclasificar.

Visualiza la IA autorizada, la Shadow AI y los agentes en una sola consola

Una consola unificada gobierna todas las superficies de IA: las plataformas autorizadas que los empleados usan a diario, las herramientas de Shadow AI que nunca pasaron por revisión y los agentes autónomos que actúan sobre datos empresariales sin supervisión humana. No se requiere ninguna herramienta ni política independiente.

Aplica las políticas en todas las superficies de IA

Forcepoint AI Data Security actúa sobre el riesgo en lugar de limitarse a reportarlo: remedia prompts y respuestas sensibles, revoca accesos compartidos en exceso y retiene las acciones de agentes de alto riesgo hasta su aprobación. Un único marco de políticas dirige cada respuesta, de modo que la protección se mantiene coherente sin importar dónde surja el riesgo.

Logra una IA gobernada en minutos, no en meses

Forcepoint ARIA, el asistente de IA integrado, lleva a los administradores desde el primer inicio de sesión hasta un entorno de IA gobernado, sin necesidad de servicios profesionales. Recomienda una configuración de políticas inicial según la región, el sector y la sensibilidad de los datos, y ofrece orientación en lenguaje sencillo.

Obtén pruebas de gobernanza para los reguladores y tu junta directiva

Cada interacción de IA y cada acción de los agentes se registra en una única pista de auditoría inmutable que respalda los requisitos de EU AI Act, NIST AI RMF, GDPR, DORA, NIS2, LFPDPPP y SEC. Ahora puedes demostrar la gobernanza cuando la necesites, en lugar de hacerlo después de los hechos.

Cómo funciona: conocer, adaptar, proteger

Conocer

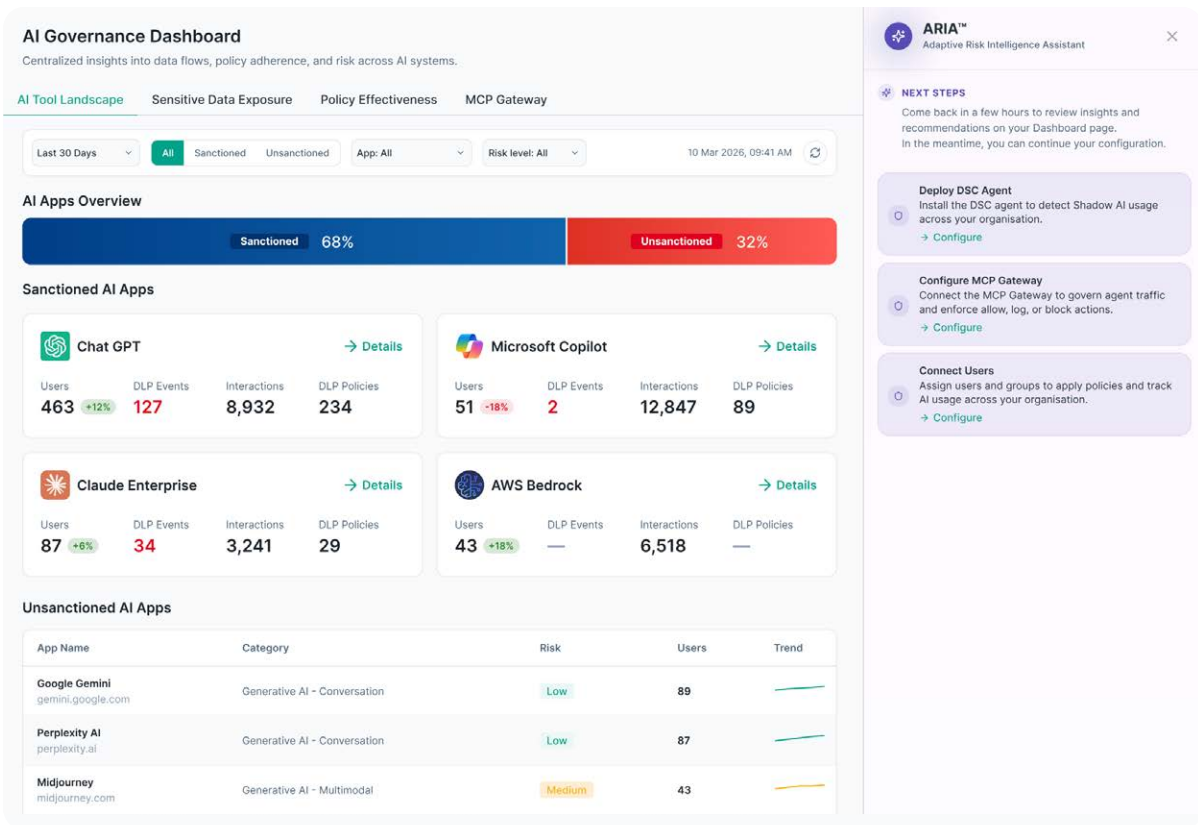
Comprende el riesgo de la IA a medida que se forma

Forcepoint AI Data Security ofrece una visión continuamente actualizada del entorno de IA de la empresa:

- Un inventario centralizado de plataformas de IA autorizadas, herramientas de Shadow AI y agentes de IA
- Visibilidad basada en API de los servicios de IA empresariales, incluida la actividad histórica al conectarse

- Visibilidad de endpoints para detectar aplicaciones de IA no aprobadas y agentes que se ejecutan localmente
- Clasificación previa de datos sensibles en fuentes estructuradas y no estructuradas, que hace que las interacciones de IA reconozcan los datos desde el principio
- Atribución completa de cada interacción de IA al usuario humano, al agente de IA o al par agente-usuario involucrado

Los equipos de seguridad obtienen una vista operativa única de dónde existe el riesgo de IA y quién es responsable de él.



Adaptar

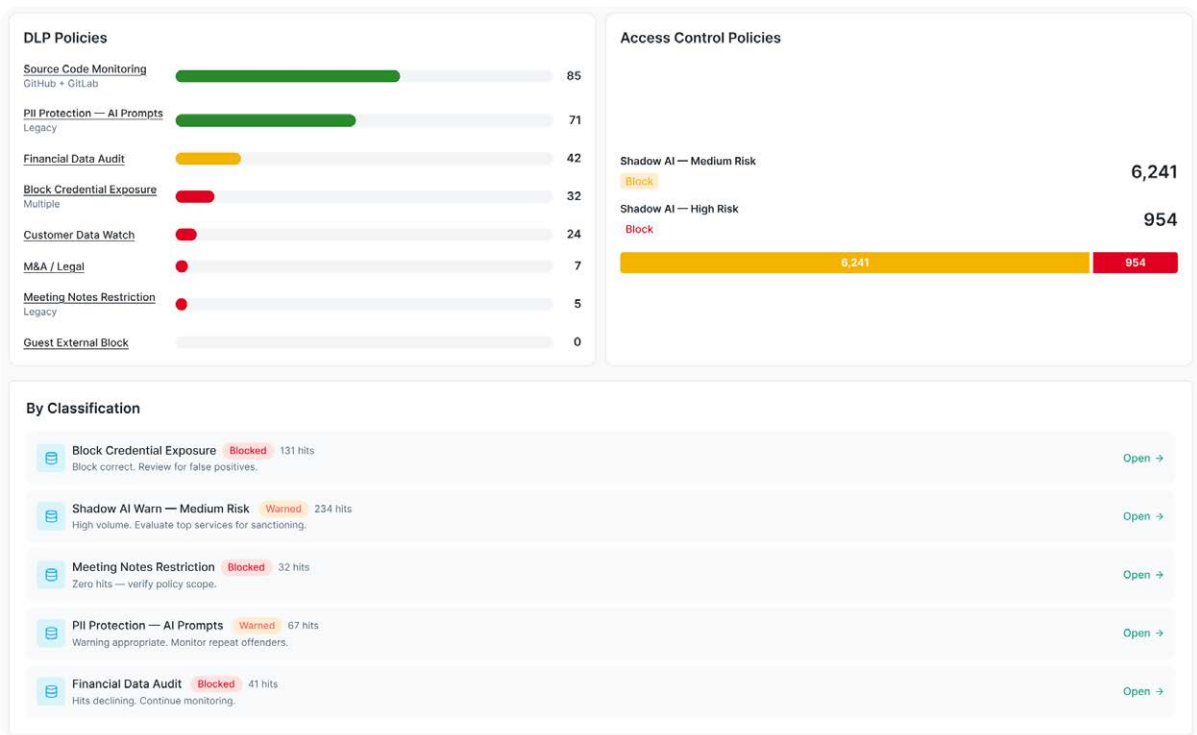
Convierte la información en acción a la velocidad de la IA

La visibilidad por sí sola no basta si la aplicación de las políticas no puede seguir el ritmo. Forcepoint AI Data Security adapta la protección automáticamente a medida que evoluciona el uso de la IA:

- Las políticas de seguridad de datos existentes se extienden a los prompts de IA, las respuestas, las cargas de archivos y las acciones de los agentes sin reconstruir políticas ni reclasificar
- Un único marco de políticas gobierna el correo electrónico, la web, los endpoints, SaaS y la IA para una protección coherente dondequiera que fluyan los datos

- Forcepoint ARIA guía a los administradores desde el primer inicio de sesión hasta un entorno de IA gobernado, sin necesidad de servicios profesionales
- Los controles de remediación permiten a los equipos orientar a los usuarios, restringir acciones, exigir aprobación para la ejecución de agentes o bloquear la actividad de alto riesgo
- Los agentes autónomos se restringen al mínimo privilegio, lo que evita los excesos por permisos heredados y por inyección de prompts antes de que comiencen

Este enfoque permite a las organizaciones gobernar la adopción de la IA sin frenar la productividad.



Proteger

Aplica una protección coherente dondequiera que la IA interactúe con los datos

Forcepoint AI Data Security aplica la protección en el punto de interacción, no después de que ocurra la exposición:

- La aplicación basada en API se conecta directamente a las plataformas de IA autorizadas para inspeccionar prompts, respuestas y acciones de los agentes sin necesidad de proxies, extensiones de navegador ni cambios en la red
- La aplicación en endpoints extiende la protección a la actividad de IA que ocurre localmente en los dispositivos, incluidos los agentes que se ejecutan localmente y las herramientas de IA basadas en el navegador
- AI Agent Gateway gestiona las credenciales de los agentes autónomos que llaman a aplicaciones empresariales como Salesforce y Microsoft 365, inspecciona cada respuesta a nivel de campo y retiene las acciones de alto riesgo hasta su

aprobación

- Las barreras de acceso a los datos evitan que los asistentes de IA expongan datos compartidos en exceso o mal clasificados, al remediar el acceso antes de la exposición
- Casi 2000 plantillas, políticas y clasificadores cubren 80 o más regiones regulatorias desde el primer momento y bloquean pegados, cargas y recursos compartidos riesgosos sin paralizar a los empleados
- Cada acción de aplicación se registra con atribución completa de identidad para crear un registro auditable

Esto ofrece una protección inmediata y coherente tanto para la actividad de IA dirigida por personas como para la autónoma.

Policy

Access Control

Data Security

Content Inspection Policies

Inspect and control what data users share with AI tools. Define allow/block rules for sensitive data categories like PII, PHI, source code, and financial data.

Search policies...

Filters

On-prem DLP policies are managed in FSM

Name	Classifier	Action	Status
Australia PII Government-issued travel document identifiers	PII	Audit	☒
Biometric Files Biometric Files	PII	Audit	☒
Business and Technical Drawings Files State and national driving license identifiers	Identity	Alert	☒
Call Detail Records Fingerprints, facial recognition, retinal scans	Identity	Alert High	☒
Credit Card Magnetic Strips Personal and corporate email identifiers	PII	Alert	☒
Financial Information Bank accounts, transaction records, payment information	Financial	Alert	☒
HIPAA The Health Insurance Portability and Accountability Act	PII	Audit	☒
India PHI Policy for detection of protected health information	Identity	Audit	☒
Japan PII Policy for detection of Japanese private information.	Identity	Audit	☐
Location coordinates Policy for detection of location coordinates.	Financial	Alert	☐

4

Capacidades clave

Protección de datos en todas las interacciones de IA

Inspecciona prompts, respuestas y cargas de IA con las mismas clasificaciones de datos que ya protegen el correo electrónico, la web y los endpoints.

Descubrimiento y control de Shadow AI

Descubre y administra las herramientas de IA no autorizadas desde un único panel, con puntuación de riesgo y políticas de control de acceso aplicadas por aplicación.

Controles de acceso a datos para IA autorizada

Identifica y remedia los datos compartidos en exceso o mal clasificados antes de que asistentes de IA como Copilot puedan mostrar contenido sensible.

Monitoreo y gobernanza de agentes de IA personalizados

Captura registros de actividad detallados de los agentes de IA, incluido quién los activó, a qué datos accedieron y qué acciones realizaron.

AI Agent Gateway: control y aplicación en tiempo de ejecución

Gestiona las credenciales de los agentes y aplica protección de datos a nivel de campo en cada transacción entre agente y aplicación, con aprobación humana para las acciones de alto riesgo.

Una plataforma, cada interacción de IA

La plataforma Forcepoint AI Data Security protege los datos en ambos lados de la IA: gobierna los datos para que sea seguro usarlos con la IA y los protege de los riesgos que esta introduce. La misma protección acompaña a los datos dondequiera que estén: en una laptop administrada o un navegador personal, en una aplicación autorizada o una herramienta no autorizada, en la oficina o en un teléfono en casa.

Forcepoint es la única empresa que protege cualquier dato, estructurado o no estructurado, local y en la nube, en cada canal por el que se mueve, incluida la IA. Otros proveedores agregan la seguridad de IA como una herramienta independiente. Forcepoint extiende la seguridad de datos en la que las organizaciones ya confían a la puerta de entrada de la IA.

