ZSCALER AI RED TEAMING

Detección y gestión de activos de IA

DE-UN-VISTAZO

Detecte y proteja automáticamente todos los activos de IA (LLM, flujos de trabajo, servidores MCP y protecciones) para lograr una visibilidad completa de la postura.

¿Por qué gestionar activos con IA?

A medida que las empresas aceleran la adopción de tecnología de IA, se construyen e implementan más LLM, flujos de trabajo y sistemas de IA (como servidores MCP y protecciones de IA) en todos los departamentos a un ritmo sin precedentes. Esto supone un desafío crítico para los líderes de seguridad: la mayoría de las organizaciones no saben cuántos componentes de IA están en uso, dónde están implementados, si es seguro usarlos o cuáles son los riesgos de seguridad que conllevan.

Para las grandes empresas, la escala es asombrosa: se pueden utilizar cientos o incluso miles de modelos de IA en diferentes unidades de negocio, a menudo fuera de la línea de visión de la seguridad. Sin un inventario centralizado, los CISO y sus equipos carecen de la visibilidad necesaria para evaluar riesgos, garantizar el cumplimiento o evitar que los componentes de IA inseguros lleguen a producción.

La gestión de activos de IA de la plataforma Zscaler AI Red Teaming resuelve esta brecha crítica de transparencia y visibilidad. AI unificar la detección de cada LLM, flujo de trabajo, servidor MCP y protección en una única AI-BOM, Zscaler AI Red Teaming brinda a los ejecutivos de seguridad la claridad para ver exactamente qué está en uso, analizar vulnerabilidades y decidir qué es adecuado para la implementación, al mismo tiempo que cumple con los crecientes requisitos de políticas de IA para que la IA sea transparente y explicable. Esta visión unificada es la base para proteger la IA a escala empresarial.

INVENTARIO DE IA UNIFICADO

Una única fuente de verdad para cada LLM, flujo de trabajo, servidor MCP y protección utilizados en las organizaciones.

AI-SPM AGILIZADA

Combine la detección de IA, las pruebas de seguridad, la protección en tiempo de ejecución y el mapeo de cumplimiento en una sola herramienta.

VISIBILIDAD A ESCALA EMPRESARIAL

Obtenga claridad en miles de modelos y flujos de trabajo y sepa qué es seguro para implementar.

Visibilidad completa de su pila de IA con una lista de materiales de IA unificada

DETECTE Y APRUEBE TODOS LOS MODELOS DE IA

Cada LLM utilizado o implementado en su organización se detecta automáticamente y se mapea a los puntos de referencia confiables de Zscaler AI Red Teaming. Los equipos de seguridad pueden evaluar riesgos, comparar puntuaciones de seguridad e identificar rápidamente modelos inseguros. Cada modelo se puede aprobar o bloquear, lo que brinda a los CISO control total sobre el uso y la implementación empresarial.



ESCANEE SERVIDORES DE PROTOCOLO DE CONTENIDO DE MODELOS (MCP) Y ENCUENTRE SUS DEBILIDADES

Los servidores MCP actúan como capas de orquestación críticas en las pilas de IA, pero a menudo no se supervisan. La plataforma de equipos rojos Zscaler AI Red Teaming los detecta y escanea automáticamente en busca de vulnerabilidades y configuraciones erróneas que los atacantes podrían explotar. Al integrar la visibilidad de MCP en una lista de materiales de IA unificada (AI-BOM), los equipos de seguridad pueden remediar los puntos débiles y mantenerse seguros.



VISUALICE FLUJOS DE TRABAJO DE IA Y EJECUTE PRUEBAS DE SEGURIDAD

Los repositorios de código fuente se escanean continuamente para detectar y mapear los flujos de trabajo de IA, revelando cada agente, herramienta y servidor MCP en su interior. Las evaluaciones de riesgos automatizadas indican configuraciones incorrectas y posibles vulnerabilidades, lo que ayuda a los equipos de seguridad de IA a proteger los flujos de trabajo y reducir la exposición al riesgo antes de que puedan ser explotados.

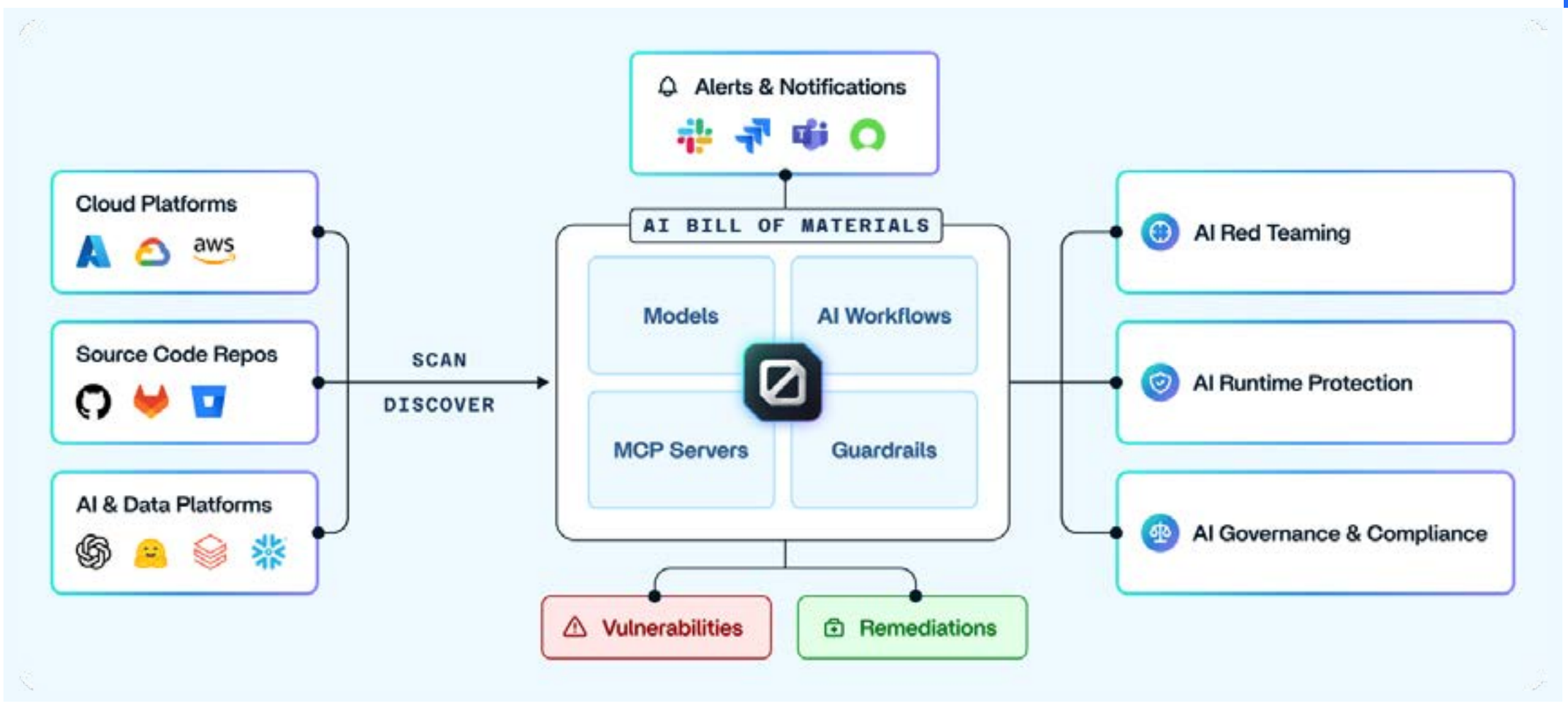


INTEGRE SU PILA PARA OBTENER UNA VISIBILIDAD COMPLETA DE LA IA

La plataforma Zscaler AI Red Teaming se conecta con los principales proveedores de nube, repositorios de código fuente, plataformas de AI/ML y sistemas de datos para ofrecer una detección completa de activos de IA en toda la empresa. Miles de entornos se unifican en una única AI-BOM, lo que elimina los puntos ciegos y brinda a los líderes de seguridad la visibilidad y la preparación para el cumplimiento requeridas a escala empresarial.



© 2025 Zscaler, Inc. Todos los derechos reservados.



Gestión de la postura de seguridad de la IA (AI-SPM)?

Obtenga visibilidad completa y control de su postura de seguridad de IA

Reúna todos los componentes de IA en un único inventario y proteja los sistemas de IA de su organización a escala.

AGENDAR UNA DEMO



Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales listadas en **zscaler.com/mx/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca comercial es propiedad de sus respectivos propietarios.

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134 zscaler.com/mx

zscaler™

Zero Trust Everywhere