Zscaler AI Security de un vistazo

DE UN VISTAZO

Ventajas de la seguridad de la IA

DESCUBRA LOS ACTIVOS Y RIESGOS DE IA
Descubra y cartografíe todo su ecosistema de IA, desde la IA en la sombra y las aplicaciones de riesgo hasta los modelos y canalizaciones de IA, entre otros elementos.

DETECTE LAS VULNERABILIDADES DE LA IA
Someta los sistemas de IA a pruebas de equipo rojo para detectar vulnerabilidades y riesgos mediante pruebas continuas y automáticas.

ACCESO SEGURO A LA IA
Aproveche las medidas de protección de IA en línea para aplicar protecciones en tiempo real contra amenazas y pérdidas de datos, y garantizar un uso seguro.

GESTIONE EL CUMPLIMIENTO NORMATIVO DE LA IA
Gestione su presencia e implementaciones de IA mediante marcos de IA para mantener el cumplimiento normativo y controlar los riesgos

Seguridad de IA de extremo a extremo con Zscaler

Zscaler ofrece soluciones basadas en IA diseñadas para ayudar a las empresas a aprovechar el poder transformador de la inteligencia artificial, al tiempo que gestionan los riesgos asociados.

Con funcionalidades que abarcan desde la identificación del uso arriesgado de la IA hasta la garantía de un desarrollo seguro y la protección de desarrollos sensibles mediante defensas avanzadas en línea.

Zscaler redefine lo que significa proteger la innovación en IA. Libere el potencial de la IA con confianza e impulse el progreso sin temor con Zscaler.



¿Por qué Zscaler para la seguridad de la IA?

CICLO DE VIDA COMPLETO DE LA IA
Seguridad de la IA desde el descubrimiento hasta la implementación

PLATAFORMA UNIFICADA
Plataforma de eficacia demostrada que integra la seguridad de la IA con Zero Trust

SOCIO DE CONFIANZA
Experiencia en el éxito y la transformación de los clientes

Descubrimiento de activos con AI SPM

Determinar su presencia en el ámbito de la IA supone un reto en el acelerado entorno actual de la IA. Sin una visibilidad clara de la IA en la sombra, los modelos, los servicios, los servidores MCP y las canalizaciones, las organizaciones tienen dificultades para detectar los riesgos y responder a ellos eficazmente.

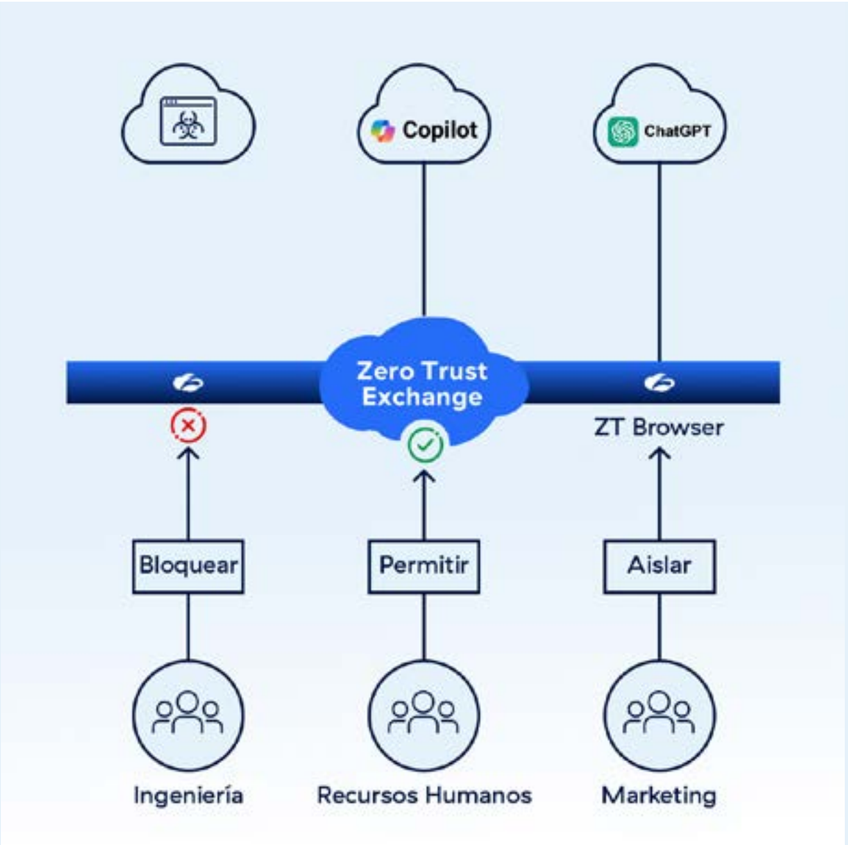
Con Zscaler AI SPM, las organizaciones obtienen una visibilidad integral de sus ecosistemas de IA. Proporciona información sobre su presencia en aplicaciones de IA generativa, LLM, modelos, servidores MCP y canalizaciones, lo que le ayuda a identificar exposiciones de riesgo y vulnerabilidades que podrían poner en peligro sus datos y su negocio.



Seguridad de acceso mediante IA

Controlar el acceso y garantizar la seguridad de las aplicaciones SaaS de IA generativa es cada vez más complejo. Ante la propagación descontrolada de la IA en la sombra y los crecientes riesgos de pérdida de datos o uso no conforme, las organizaciones necesitan soluciones eficaces para hacer frente a estas amenazas.

Con la solución de seguridad de acceso a la IA de Zscaler, puede garantizar el uso seguro, conforme a las normativas y responsable de las aplicaciones de IA. Aplique controles de acceso detallados para determinar qué usuarios o aplicaciones pueden interactuar con las herramientas de IA.
Aproveche la protección DLP o el aislamiento para evitar la pérdida de datos a través de instrucciones, y aplique la moderación de contenido para garantizar el cumplimiento de las políticas corporativas de uso aceptable.



©2026 Zscaler, Inc. Todos los derechos reservados.

Pruebas automatizadas de equipo rojo

Probar los sistemas de IA para detectar vulnerabilidades suele ser un proceso complejo y que requiere mucho tiempo. Para las organizaciones que no cuentan con recursos específicos de equipo rojo, realizar evaluaciones exhaustivas puede parecer prácticamente imposible.

La solución de Zscaler para pruebas de equipo rojo automáticas y continuas aborda estos desafíos con un innovador motor de pruebas de equipo rojo automatizado. Con más de 25 pruebas predefinidas, además de compatibilidad con pruebas totalmente personalizadas y la carga de conjuntos de datos, SPLX permite a las organizaciones adaptar los escenarios de prueba a sus ámbitos específicos, entornos normativos y casos de uso.



Protección en línea con AI Guard

Los LLM se han convertido rápidamente en un nuevo y peligroso vector de amenazas y pérdida de datos. Sin una inspección en línea de alto rendimiento de estas conexiones, las organizaciones son vulnerables a la exposición de datos, a sistemas de IA comprometidos y a amenazas maliciosas.

Con Zscaler AI Guard, las organizaciones pueden ofrecer una inspección en línea de alto rendimiento de las instrucciones e interacciones de la IA. Detecte amenazas como las inyecciones de instrucciones y el jailbreaking, evite la pérdida de datos confidenciales y modere el contenido para garantizar un uso seguro y aplicar las políticas de uso aceptable. Basándose en su experiencia como líder de confianza en la inspección en línea, Zscaler garantiza una protección sólida para su tráfico crítico de IA.



©2026 Zscaler, Inc. Todos los derechos reservados.

Gobernanza de la IA con AI SPM

Garantizar el cumplimiento normativo y la gobernanza de los sistemas de IA resulta cada vez más complejo a medida que las organizaciones adoptan la IA a gran escala. Sin una supervisión adecuada del cumplimiento de las políticas y los marcos de IA, las empresas se arriesgan a sufrir daños legales, financieros y de reputación.

Con el enfoque de Zscaler para la gobernanza de la IA, puede automatizar la supervisión del cumplimiento y optimizar los procesos de elaboración de informes. Supervise continuamente los sistemas de IA para garantizar su conformidad con las políticas internas y las normas reglamentarias, y proporcione las pruebas necesarias para respaldar las auditorías y cumplir los requisitos. Asegúrese de que el uso de la IA cumpla con los marcos de gobernanza, lo que ayudará a su organización a mitigar los riesgos y mantener la integridad operativa.



Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo , Zero Trust Exchange™ basada en SSE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite **zscaler.com/es** o síganos en Twitter **@zscaler**.

© 2026 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales enumeradas en **zscaler.com/es/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 registrada es propiedad de sus respectivos dueños.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/es**

zscaler™

Zero Trust Everywhere