PUBLICACIÓN: culturaemprende.com
PAÍS: ESP
TIPO: Web
AVE: €54.00
AUDIENCIA:
AUTOR:
URL: www.culturaemprende.com
> 17 de junio de 2026 a las 14:55
> Versión en línea

Zscaler presenta nuevas innovaciones para proteger la IA agéntica

Madrid, 17 de junio de 2026 – Zscaler, Inc . (NASDAQ: ZS), la plataforma de ciberseguridad para la era de la IA, anunció hoy importantes innovaciones para ampliar la plataforma Zscaler Zero Trust Exchange™ con el fin de proteger los agentes de IA : cómo se conectan, acceden a los datos y se ejecutan en los dispositivos. Con estas innovaciones, Zscaler ofrece la primera plataforma Zero Trust integral del sector para la IA agéntica.

Actualmente, la seguridad empresarial está experimentando una transición desde los usuarios humanos hacia los agentes autónomos. Las herramientas de seguridad tradicionales se diseñaron en torno a identidades humanas conocidas y patrones de acceso predecibles . Los agentes autónomos de IA cambian este modelo. Operan tanto en nombre de un usuario como de forma autónoma y a velocidad de máquina, creando identidades efímeras, generando subagentes y tareas, y ejerciendo permisos de formas que las herramientas de seguridad tradicionales no pueden ver ni controlar por completo.

Aunque pueden aportar importantes ganancias de eficiencia, los agentes de IA también introducen nuevas brechas de visibilidad, acceso y gobernanza , dificultando la identificación de riesgos asociados a los agentes y el seguimiento de los flujos de datos a gran escala. A medida que la IA se integra más profundamente en el desarrollo de software, los endpoints también están cada vez más expuestos a agentes maliciosos, herramientas y complementos que muchas soluciones tradicionales de seguridad para endpoints no fueron diseñadas para detectar.

Para ayudar a las empresas a adoptar la IA agéntica de forma más segura, Zscaler presenta la siguiente evolución de su Zero Trust Exchange con nuevas soluciones que amplían la protección a

PUBLICACIÓN: culturaemprende.com
PAÍS: ESP
TIPO: Web
AVE: €54.00
AUDIENCIA:
AUTOR:
URL: www.culturaemprende.com
> 17 de junio de 2026 a las 14:55
> Versión en línea

todo el ecosistema de IA, ayudando a las empresas a poner en marcha la IA agéntica con mayor seguridad y confianza.

Estas incluyen dos avances clave:

Zscaler AI Broker

ayuda a proteger las comunicaciones agénticas a través de brokers MCP y A2A. Con un Agent Registry integrado, ayuda a las empresas a comprender a qué puede acceder cada agente y a aplicar controles de acceso granulares sobre los agentes de IA empresariales.

Zscaler Endpoint AI Security

ayuda a los clientes a identificar y detener amenazas relacionadas con la IA en los dispositivos de los empleados, incluidos riesgos ocultos en navegadores, plugins, extensiones y herramientas locales de IA. Esta capacidad se adentra en las capas de navegador, extensiones y plugins que las herramientas tradicionales de seguridad para endpoints no alcanzan. Ahora Zscaler puede aplicar políticas para proteger la IA en cualquier lugar, incluidos los endpoints y la nube.

Presentación de Zscaler AI Access Graph: conectando la trazabilidad de datos e identidades con IA para mejorar la seguridad y la gobernanza de la IA agéntica

Un elemento importante de la seguridad agéntica es comprender qué agentes, usuarios e identidades se comunican con qué modelos, aplicaciones y fuentes de datos. Impulsado por la reciente adquisición de Symmetry Systems por parte de Zscaler, Zscaler AI Access Graph cartografía cómo se conectan las identidades, aplicaciones y otras fuentes de datos en toda la empresa. La integración de esta tecnología con Zscaler Zero Trust Exchange permite a las empresas comprender y posteriormente aplicar políticas, reducir accesos innecesarios y riesgos, y rastrear la trazabilidad de los datos en tiempo real a través de todos los canales.

Basándose en Zscaler AI Protect, lanzado en enero de 2026, Zscaler también incorpora importantes mejoras en los tres casos de uso principales de AI Protect:

AI Asset Management

(visibilidad sobre activos de IA, uso y riesgo) incorpora nuevas capacidades para descubrir IA integrada en aplicaciones SaaS y tráfico de Internet, identificar agentes de IA y servidores MCP en entornos de nube pública, detectar riesgos en bases de código agénticas mediante análisis de código y ampliar la visibilidad de la actividad de IA en endpoints.

Secure Access to AI

(acceso seguro y gobernado a herramientas de IA autorizadas) amplía los controles sobre las interacciones con IA mediante extracción de prompts en más de 250 aplicaciones de IA generativa y añade vistas completas de conversaciones, compatibilidad con las API de cumplimiento de

PUBLICACIÓN: culturaemprende.com
PAÍS: ESP
TIPO: Web
AVE: €54.00
AUDIENCIA:
AUTOR:
URL: www.culturaemprende.com
> 17 de junio de 2026 a las 14:55
> Versión en línea

Anthropic y OpenAI, así como salvaguardas basadas en intención para conversaciones de múltiples interacciones.

Secure AI Infrastructure and Apps

(protección para aplicaciones de IA a lo largo de todo su ciclo de vida de desarrollo y ejecución) introduce ejercicios de AI Red Teaming para servidores MCP, un servicio independiente de refuerzo de prompts (prompt hardening) y mapas de calor de cumplimiento para fortalecer la gobernanza de la IA.

“La seguridad tradicional nunca fue diseñada para millones de agentes autónomos que actúan y acceden a datos sensibles a velocidad de máquina. Fuimos pioneros con Zero Trust Exchange para proteger usuarios, sucursales y cargas de trabajo en la nube, y ahora estamos innovando para extender la seguridad Zero Trust a los agentes de IA. Ahora las empresas ya no tienen que verse limitadas a la hora de desplegar agentes por toda la organización”, asegura Jay Chaudhry, presidente y CEO de Zscaler.

“Gestionar la seguridad de los datos ya no consiste únicamente en construir muros más altos; se trata de escalar la visibilidad y tratar los datos como un activo estratégico altamente dinámico”, afirma John Israel, Global CISO de KPMG , quien participó como ponente invitado de Zscaler para analizar este lanzamiento. “A medida que las empresas amplían el uso de agentes de IA para optimizar operaciones, disponer de un marco unificado basado en Zero Trust para rastrear la trazabilidad de los datos y gobernar las interacciones entre agentes es fundamental para mantener la confianza, el cumplimiento normativo y la ventaja competitiva”.

En conjunto, estas innovaciones proporcionan un marco integral para proteger la IA agéntica, construido sobre la plataforma Zscaler Zero Trust Exchange para proteger a las empresas tanto hoy como en el futuro . Al proteger los agentes mediante controles de seguridad integrales, las organizaciones pueden acelerar con confianza la adopción de la IA.

Contacto

Llámanos:

C/ Velázquez 105 - 4ta Planta

28006 Madrid

info@culturaemprende.com

Redes sociales