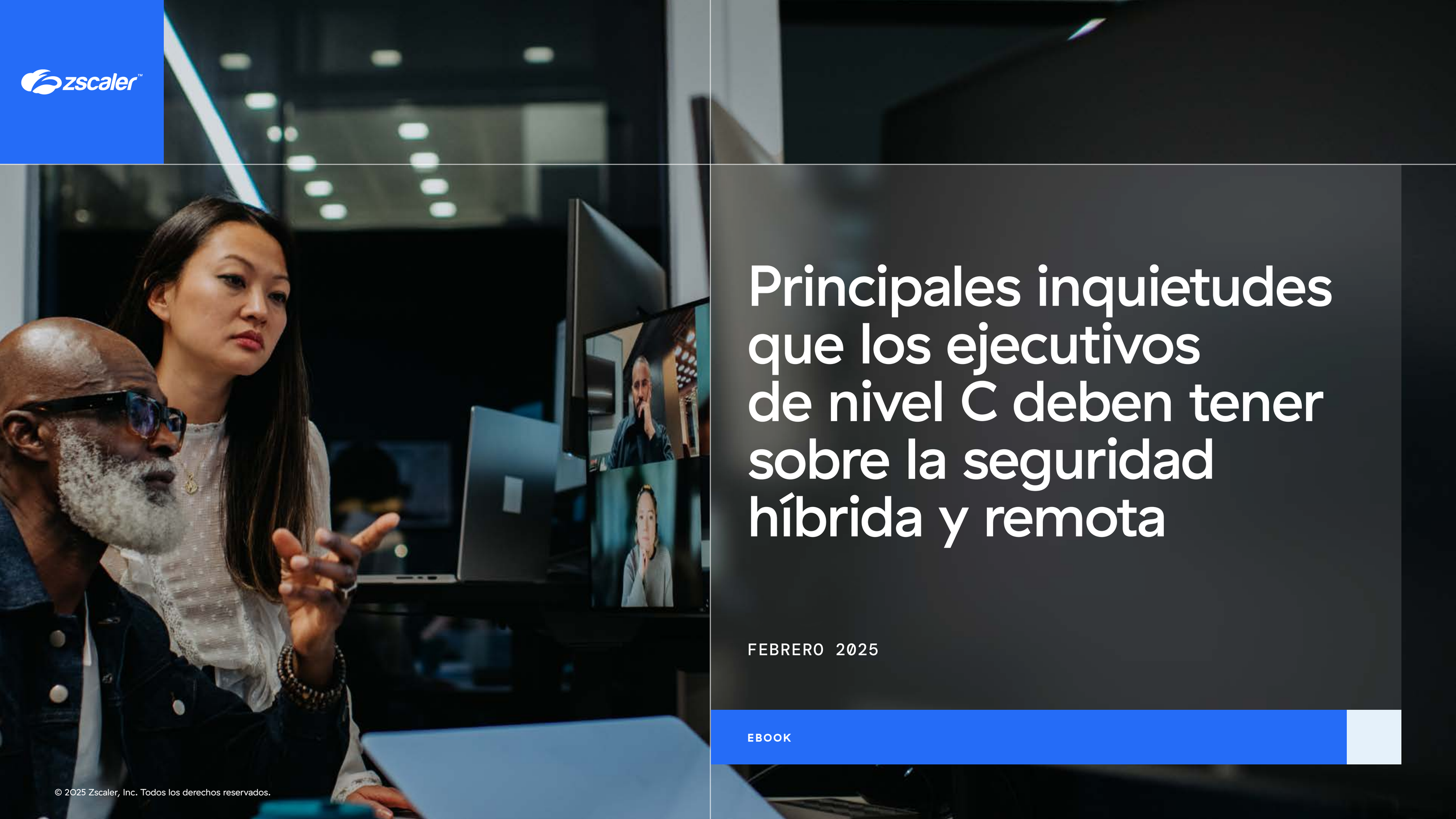


Principales inquietudes que los ejecutivos de nivel C deben tener sobre la seguridad híbrida y remota

FEBRERO 2025

EBOOK

© 2025 Zscaler, Inc. Todos los derechos reservados.

Índice



Introducción 3

Visión general de los problemas críticos de seguridad en redes y a distancia 3

El cambiante panorama de la seguridad digital 4

Últimas tendencias en seguridad digital y trabajo remoto 4

Principales preocupaciones en materia de seguridad organizativa para los directivos 5

Protección de datos confidenciales 5

Gestión de amenazas internas 5

Garantizar el cumplimiento de la normativa 5

Estrategias para abordar las cuestiones de liderazgo 6

Implementación de una gestión robusta de identidad y acceso 6

Mejora de las capacidades de detección y respuesta ante amenazas 6

Programas regulares de capacitación y concientización sobre seguridad 6

Aprovechamiento de las soluciones Zscaler para la seguridad en la oficina, híbrida y remota 7

Zscaler Internet Access (ZIA) 7

Zscaler Private Access (ZPA) 8

Funciones de seguridad avanzadas 8

Cómo proteger a su equipo con Zscaler 9

Transformación de los firewalls a Zero Trust 9

Un enfoque Zero Trust integral 9

Fuentes 9

© 2025 Zscaler, Inc. Todos los derechos reservados.

Introducción

Los ciberataques aumentaron nada menos que un 30 % interanual[1] en todo el mundo en el segundo trimestre de 2024. La creciente adopción del trabajo remoto ha ampliado la superficie de ataque y ha dejado a las organizaciones vulnerables a una amplia gama de amenazas. Según el Informe de Ataques Cifrados ThreatLabz de Zscaler, la nube de Zscaler bloqueó una cifra sin precedentes de 32.1 mil millones de ataques incrustados en el tráfico TLS/SSL, donde las amenazas cifradas representaron el 87.2 % de todos los ataques bloqueados, un aumento interanual del 10.3 %.[2] Estos datos ponen de relieve la creciente dependencia del cifrado por parte de los malintencionados para ocultar sus actividades maliciosas.

Las tecnologías heredadas, como los firewalls y las redes privadas virtuales (VPN), ya no bastan para proteger los datos, las aplicaciones y las redes de la empresa, por lo que los responsables de la toma de decisiones y los altos cargos tienen una larga lista de preocupaciones cuando se trata de proteger los entornos de trabajo remotos. Los líderes están sometidos a una presión constante para minimizar el riesgo de violaciones, garantizar el cumplimiento de los reglamentos y las normas del sector y evitar el robo de datos valiosos como la propiedad intelectual o los secretos comerciales.

La buena noticia es que las soluciones Zero Trust basadas en la nube están diseñadas para salvaguardar las redes de las organizaciones que cuentan con fuerzas de trabajo remotas e híbridas. Con la tecnología adecuada, los ejecutivos pueden eliminar estas inquietudes comunes.

Descripción general de problemas críticos de seguridad de redes y remotas

Las operaciones de trabajo remoto pueden debilitar el control de las empresas sobre los datos y la integridad de su arquitectura de seguridad. Los empleados pueden usar dispositivos no administrados que pueden no tener software de seguridad instalado o no ser supervisados activamente para acceder a los recursos de la empresa, incluidas aplicaciones críticas.

Además, los profesionales de seguridad no tienen visibilidad completa sobre cómo los empleados remotos manejan los datos confidenciales y si los eliminan después de su uso. Los empleados pueden almacenar datos en sus dispositivos personales, lo que los hace vulnerables a ataques de ransomware, violaciones de datos y otras amenazas.

El cambio a aplicaciones basadas en la nube amplía aún más la superficie de ataque, complicando la seguridad de su infraestructura digital.



©2025 Zscaler, Inc. Todos los derechos reservados.



El cambiante panorama de la seguridad digital

En el mundo previo a la pandemia, los firewalls y las VPN podían haber sido suficientes para proteger las redes y los datos confidenciales de una empresa. Sin embargo, el trabajo remoto e híbrido ha impulsado la necesidad de una transformación completa en la manera en que las organizaciones salvaguardan sus entornos digitales en la actualidad.

Últimas tendencias en seguridad digital y trabajo remoto

Los empleados remotos necesitan inevitablemente los recursos de la empresa para realizar su trabajo, independientemente de su ubicación, y muchas organizaciones han adoptado aplicaciones de software como servicio (SaaS) basadas en la nube para permitir el trabajo remoto y mejorar la productividad. La implementación de SaaS en una red dispersa de empleados genera una superficie de ataque más amplia y aumenta el riesgo de acceso no autorizado y violaciones de seguridad.

Los ciberdelincuentes también han desarrollado tácticas más sofisticadas (entre ellas el relleno de credenciales y los ataques de día cero) aumentando la presión sobre los directivos en lo que respecta a la ciberseguridad. De hecho, Estados Unidos sigue siendo el principal objetivo del ransomware, con el 49.95 % de los ataques totales, seguido del Reino Unido, Alemania, Canadá y Francia.[3] Además de erosionar la reputación de la marca y la confianza de los clientes, estos ataques ponen a su empresa en riesgo de incumplimiento de las normativas sobre privacidad y seguridad de los datos, por no hablar del peligro financiero.

A la luz de estas tendencias, los altos ejecutivos y los responsables de seguridad están adoptando nuevas medidas de seguridad, como:

- **Arquitectura Zero Trust**, que se basa en el principio de "nunca confiar, siempre verificar". Todos los usuarios y dispositivos, incluidos los dispositivos personales (BYOD), deben ser verificados.
- **Detección de amenazas impulsada por inteligencia artificial (IA) y aprendizaje automático (ML)**, que ayuda a identificar y mitigar de manera proactiva ciberataques sofisticados.
- **Segmentación de aplicaciones**, que evita el movimiento lateral de amenazas.
- **La seguridad de los puntos finales**, que se centra en salvaguardar los dispositivos utilizados por los empleados remotos. Las soluciones basadas en IA pueden detectar y bloquear las amenazas antes de que afecten a los puntos finales, garantizando una mejor protección de las fuerzas de trabajo distribuidas.

© 2025 Zscaler, Inc. Todos los derechos reservados.

Principales preocupaciones en materia de seguridad organizativa para los directivos

Con la prevalencia del trabajo remoto e híbrido y la creciente dependencia de las soluciones basadas en la nube, los líderes empresariales y los CISO deben pensar más allá de la seguridad basada en el perímetro.

Protección de datos confidenciales

Cuando los empleados acceden a datos comerciales a través de redes no seguras y los guardan en dispositivos personales, se aumenta el riesgo de acceso no autorizado y de manejo indebido de datos. La protección de datos confidenciales en entornos de trabajo remoto implica:

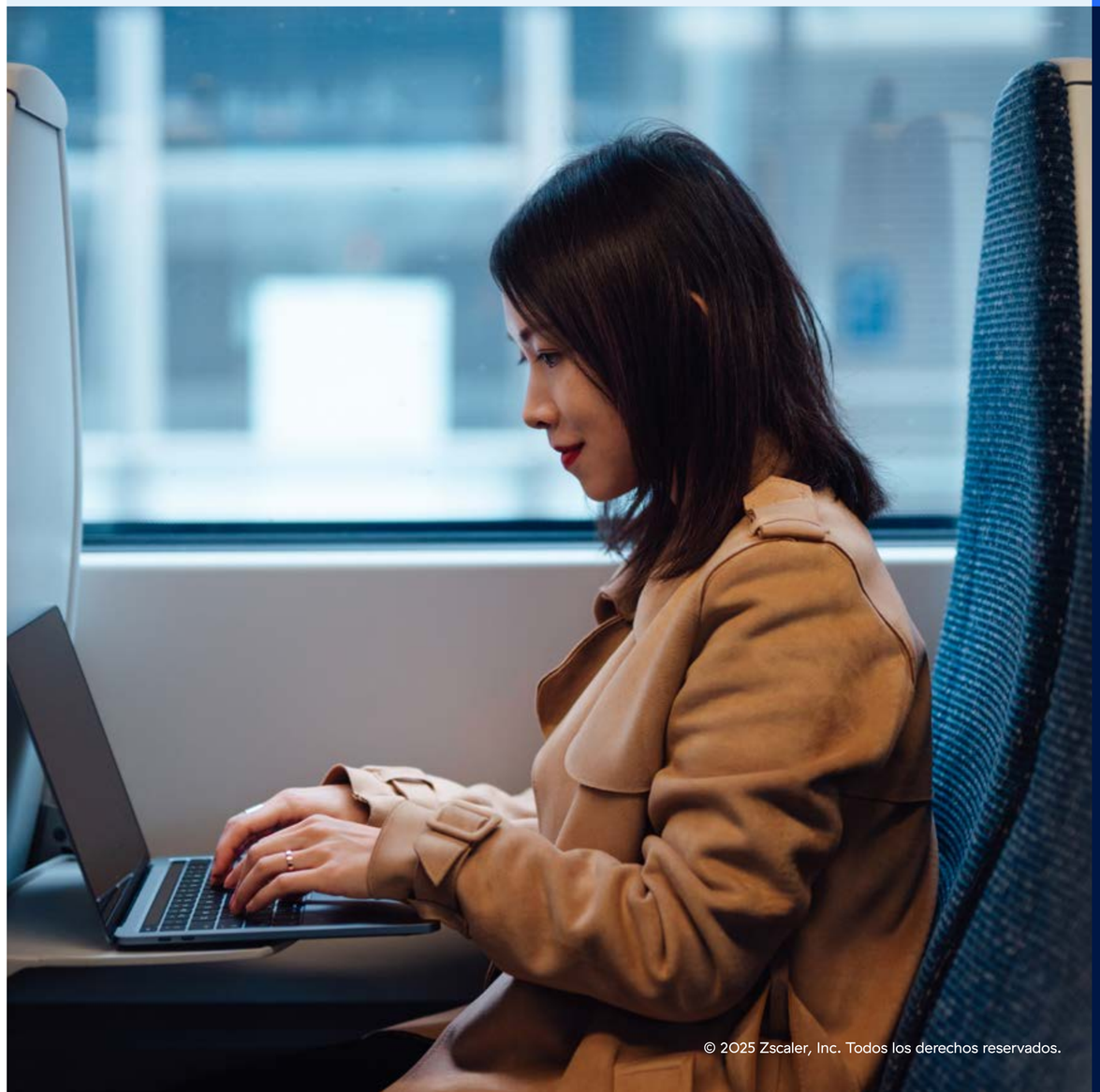
- **Cifrado de extremo a extremo** para proteger datos en reposo y en tránsito, especialmente cuando se transfieren a través de canales no seguros.
- **Gestión de identidad y acceso** para garantizar que solo los empleados autorizados puedan acceder y utilizar los datos necesarios.
- **Técnicas de prevención de pérdida de datos** para mitigar la exposición accidental de datos y las violaciones de seguridad.

Gestión de amenazas internas

Las acciones accidentales e intencionales de empleados locales y remotos pueden comprometer la seguridad del sistema. Por ejemplo, un empleado nuevo podría ser víctima de una estafa de phishing o un empleado descontento puede hacer un mal uso de datos confidenciales de la empresa. El control de acceso basado en roles, las políticas de acceso con privilegios mínimos y el análisis de comportamiento pueden ayudar a minimizar el riesgo de amenazas internas.

Garantizar el cumplimiento de la normativa

Decenas de gobiernos han puesto en marcha leyes de protección de datos y privacidad para proteger la información personal de los consumidores, como el Reglamento General de Protección de Datos (RGPD) y la Ley de Privacidad del Consumidor de California (CCPA). Además, existen regulaciones específicas de la industria, como la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA). En los entornos de trabajo remotos, mantener el cumplimiento de estos requisitos normativos requiere estrategias de gobernanza exhaustivas.



© 2025 Zscaler, Inc. Todos los derechos reservados.

Estrategias para abordar las cuestiones de liderazgo

Los ejecutivos de alto nivel pueden adoptar varias estrategias para hacer frente a los complejos desafíos de seguridad del entorno laboral moderno.

Implementación de una gestión robusta de identidad y acceso

La gestión de identidad y acceso (IAM) es un método eficaz para evitar el acceso no autorizado a la red y los sistemas de su organización. Garantiza que solo las personas adecuadas tengan acceso a las aplicaciones y los datos que necesitan para realizar su trabajo.

IAM minimiza la superficie de ataque, reduciendo la exposición innecesaria a datos confidenciales. A diferencia de los métodos de seguridad basados en el perímetro, IAM implica controles de acceso más estrictos independientemente del dispositivo y la ubicación del usuario. Los líderes deberían considerar implementar una plataforma que admita soluciones IAM flexibles e integración.

Mejora de las capacidades de detección y respuesta ante amenazas

A medida que los ciberdelincuentes desarrollan sus estrategias, los responsables de la seguridad deben actualizar también las suyas para frustrar los ataques con una detección y respuesta avanzadas a las amenazas. Implemente soluciones que utilicen modelos de IA y ML para supervisar el tráfico de la red y el comportamiento de los usuarios con el fin de detectar desviaciones de manera automática.

La IA y el ML también refuerzan las soluciones Zero Trust que aíslan los dispositivos y archivos comprometidos en tiempo real, permitiendo respuestas rápidas a las amenazas y favoreciendo un enfoque de ciberseguridad más proactivo. Los algoritmos de ML también pueden resaltar vulnerabilidades potenciales al tiempo que identifican y bloquean amenazas emergentes.

Programas regulares de capacitación y concientización sobre seguridad

Las políticas y herramientas de seguridad son tan eficaces como las personas que las utilizan.

Un ejemplo: el 80 % de los CISO creen que la negligencia de los empleados y el riesgo humano serán las principales amenazas para la ciberseguridad en 2026[4]. Los empleados en entornos de trabajo remotos son especialmente vulnerables porque no siempre pueden acudir a los profesionales de la seguridad en persona para pedir ayuda, lo que provoca retrasos y daños irreversibles.

Para mitigar estos escenarios, las organizaciones pueden poner en marcha programas de capacitación continua en seguridad que familiaricen a los empleados con las amenazas existentes, emergentes y en evolución, así como con las mejores prácticas que les capaciten para mantenerse alerta ante un panorama de amenazas en constante cambio. Instruya a su equipo sobre las mejores prácticas de trabajo a distancia, la higiene de las contraseñas y el tratamiento seguro de los datos. Además, organice sesiones de capacitación periódicas para repasar con los empleados los protocolos de ciberseguridad de toda la empresa y los recursos disponibles sobre qué hacer si sus dispositivos, datos y acceso a las aplicaciones se ven comprometidos.

© 2025 Zscaler, Inc. Todos los derechos reservados.

Aprovechamiento de las soluciones Zscaler para la seguridad en la oficina, híbrida y remota

Las soluciones Zero Trust basadas en la nube de Zscaler están diseñadas para ayudar a los líderes empresariales a proteger cualquier entorno de trabajo hoy y en el futuro a medida que evolucionan las amenazas. Zscaler Zero Trust Exchange™ incluye las siguientes soluciones básicas para garantizar que los equipos cuenten con una seguridad integral:

Zscaler Internet Access (ZIA)

Zscaler Internet Access es una solución Zero Trust nativa en la nube e impulsada por la IA que ayuda a reforzar la seguridad digital de las fuerzas de trabajo remotas. Mediante una arquitectura de proxy Zero Trust que inspecciona el 100 % del tráfico TLS/SSL a escala, con conexiones directas de usuario a aplicación basadas en la identidad, el contexto y las políticas empresariales, ZIA garantiza un acceso seguro y sin problemas a SaaS y aplicaciones basadas en web con las siguientes capacidades clave:

- **La Secure Web Gateway (SWG) nativa de la nube** ofrece una experiencia web segura y rápida, al tiempo que detecta y previene los ataques avanzados con análisis y filtrado de URL en tiempo real y potenciados por IA.
- **Prevención avanzada de amenazas basada en IA/ML** para detener amenazas avanzadas como botnets, ransomware, comando y control, intercambio de archivos riesgosos, contenido activo malicioso, secuencias de comandos en sitios cruzados, sitios fraudulentos, etc.
- **El filtrado de URL potenciado por IA** garantiza a sus usuarios sesiones seguras de navegación por aplicaciones web, deteniendo amenazas avanzadas (como el phishing y el ransomware) y aplicando una política de uso aceptable.
- **Cloud Access Security Broker (CASB)** asegura las aplicaciones en la nube, protege los datos, detiene las amenazas y garantiza el cumplimiento en todos sus entornos SaaS e IaaS con una protección integrada.
- **Data Loss Prevention (DLP)** protege los datos en movimiento con una inspección completa en línea, que incluye la coincidencia exacta de datos (EDM), la coincidencia indexada de documentos (IDM) y el aprendizaje automático.
- **La política dinámica basada en riesgos** detiene los ataques activos y prepara sus defensas para el futuro con un análisis continuo de los riesgos de usuarios, dispositivos, aplicaciones y contenidos que alimenta los controles de acceso dinámicos.
- **Zero Trust Firewall** permite conexiones rápidas y seguras dentro y fuera de la red, así como conexiones locales a Internet para el tráfico de los usuarios a través de todos los puertos y protocolos, sin necesidad de actualizaciones de hardware o software.
- **Browser Isolation, potenciado por IA,** renderiza las sesiones web como píxeles en el navegador del usuario, ofreciendo una experiencia web casi nativa sin riesgo de pérdida de datos o infección del dispositivo.
- **DNS Security** filtra los dominios riesgosos y maliciosos y detiene el uso de túneles DNS para transferir cargas maliciosas y datos confidenciales.



©2025 Zscaler, Inc. Todos los derechos reservados.

Zscaler Private Access (ZPA)

Zscaler Private Access es la primera solución de acceso a la red Zero Trust (ZTNA) potenciada por IA del sector y es una oferta nativa en la nube que ofrece acceso Zero Trust para todos los usuarios. Al ofrecer conectividad directa a las aplicaciones privadas al tiempo que minimiza la superficie de ataque, ZPA elimina el movimiento lateral de amenazas mediante la segmentación de usuario a aplicación impulsada por la IA y protege contra ataques sofisticados con inspección de tráfico integrada y protección de aplicaciones y datos. Algunas de las capacidades clave de ZPA que pueden asegurar la fuerza de trabajo híbrida incluyen:

- **AI-Powered App Segmentation** descubre aplicaciones automáticamente y proporciona recomendaciones generadas por IA sobre segmentos de aplicaciones y políticas para reducir su superficie de ataque y evitar el movimiento lateral.
- **Workload-to-Workload Segmentation** asegura las comunicaciones de carga de trabajo en la nube a través de entornos híbridos y multinube como AWS y Azure.
- **Privileged Remote Access** proporciona acceso remoto sin cliente a trabajadores remotos y terceros a sistemas de producción confidenciales RDP, SSH y VNC.
- **Private Service Edge** lleva la ZTNA a los usuarios locales con acceso directo de usuario a aplicación, con privilegios mínimos, a las aplicaciones privadas.
- **Business Continuity** garantiza un acceso ininterrumpido y basado en políticas a las aplicaciones de misión crítica durante los cortes de conectividad y los eventos de cisne negro.
- **Extranet Application Support** permite el acceso Zero Trust a las aplicaciones de socios comerciales y proveedores alojadas en sus redes.
- **Digital Experience Monitoring** optimiza sus experiencias digitales para mantener la productividad de los usuarios detectando y resolviendo rápidamente los problemas de las aplicaciones, la red y los dispositivos.

Funciones de seguridad avanzadas

Zscaler ofrece varias funciones avanzadas, entre ellas:

- **InspecciónSSL/TLS** a escala para una protección completa de los datos y una inspección de usuario a aplicación.
- **Detección de amenazas en línea impulsada por la IA** para detener los vectores de ataque antes de que alcancen su objetivo.
- **Risk360™** para visualizaciones de riesgos intuitivas, factores, detalles e informes para que pueda tomar medidas inmediatas para mitigar los riesgos.

© 2025 Zscaler, Inc. Todos los derechos reservados.

Cómo proteger a su equipo con Zscaler

Si desea reforzar la seguridad de su entorno de trabajo a distancia, debe considerar la posibilidad de alejarse de las soluciones de ciberseguridad heredadas. La plataforma Zero Trust de Zscaler ofrece varias formas de facilitar la transición.

Transformación de los firewalls a Zero Trust

Los firewalls y las VPN son ineficaces en el entorno empresarial moderno porque amplían su red corporativa, ofreciendo a los atacantes más vías de entrada. Por el contrario, el Zscaler Zero Trust Exchange™ actúa como una centralita inteligente, inspeccionando el tráfico entrante y saliente hacia y desde los dispositivos de los usuarios para detectar y bloquear las amenazas mientras intermedia de manera segura en las conexiones con las aplicaciones y los recursos en la nube.

Un enfoque Zero Trust integral

Un verdadero enfoque de la seguridad basado en la Zero Trust requiere políticas de acceso centradas en la identidad y conscientes del contexto que se adapten a cada usuario, dispositivo y aplicación. El objetivo es garantizar que solo los usuarios de confianza puedan acceder a recursos específicos, y que esos usuarios y recursos estén designados por los controles establecidos por su empresa. Puede establecer reglas en su marco de seguridad Zero Trust para conceder acceso a los usuarios en función de la ubicación, la identidad, la hora/fecha y más, y Zscaler le guía a través de este proceso para que su organización empiece a aplicar estos controles con el pie derecho.

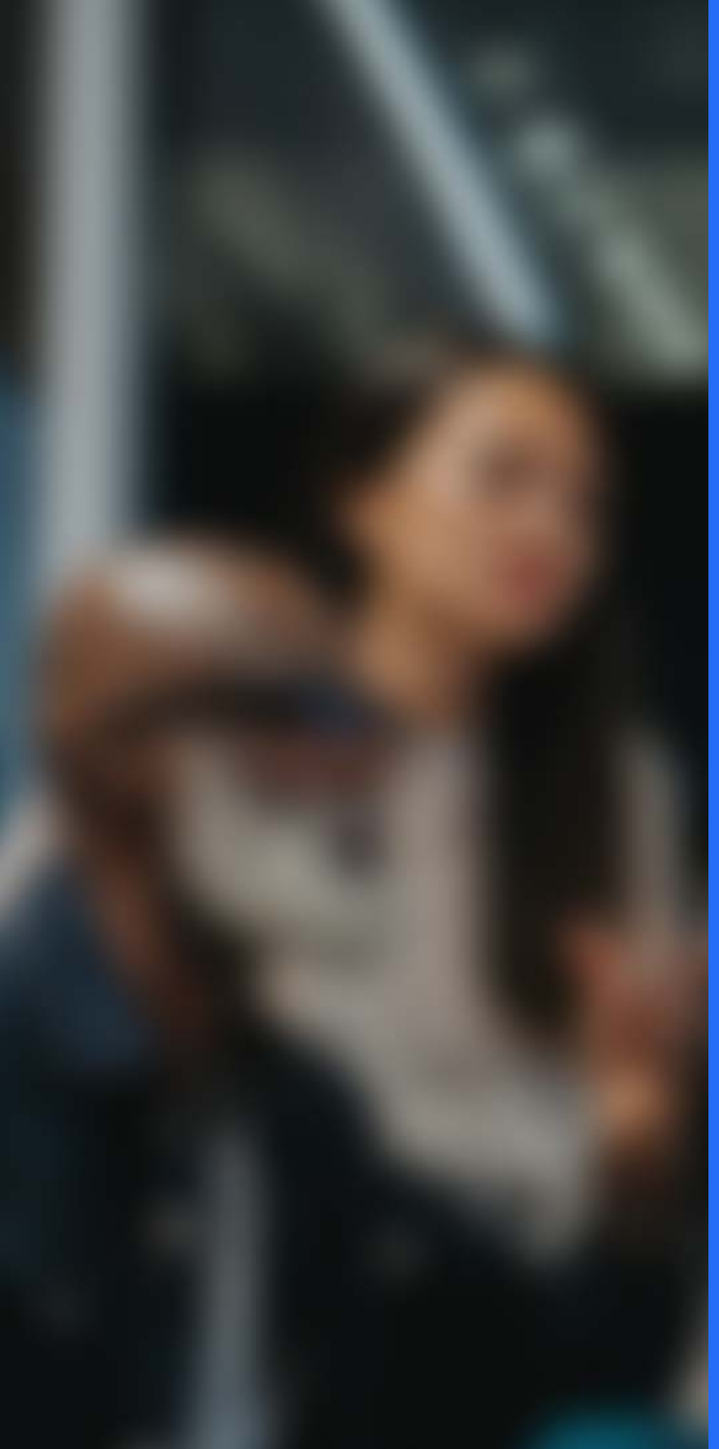
Obtenga más información sobre cómo Zscaler puede ayudarle a transformar su postura de seguridad para proteger a su fuerza de trabajo dispersa solicitando una demostración.

FUENTES:

1. Intelligent CISO, Check Point Research unveils Q2 2024 cyberattack trends, highlighting global and UAE increases, 29 de julio de 2024.
2. Informe sobre el estado de los ataques cifrados de Zscaler ThreatLabz 2024, 2024
3. Informe sobre el ransomware de Zscaler ThreatLabz 2024, 2024.
4. Infosecurity Magazine, 70% of CISOs Expect Cyber-Attacks in Next Year, Report Finds, 21 de mayo de 2024.



©2025 Zscaler, Inc. Todos los derechos reservados.



zscaler™ | Experience your world, secured.™

© 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.

