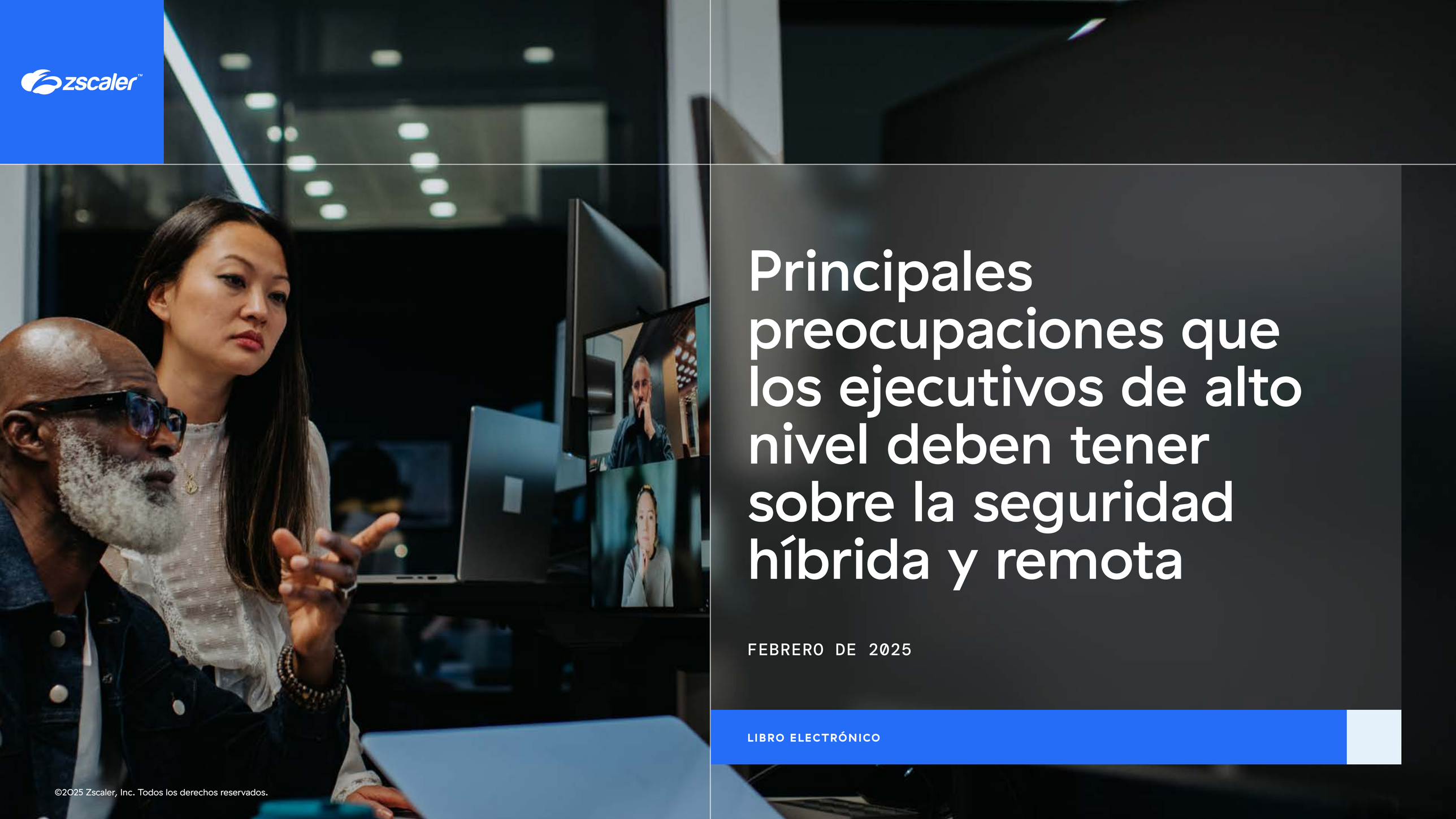


Principales preocupaciones que los ejecutivos de alto nivel deben tener sobre la seguridad híbrida y remota

FEBRERO DE 2025

LIBRO ELECTRÓNICO

©2025 Zscaler, Inc. Todos los derechos reservados.

Índice



Introducción 3

Descripción general de problemas críticos de seguridad de redes y remota 3

El cambiante panorama de la seguridad digital 4

Últimas tendencias en seguridad digital y trabajo remoto 4

Principales preocupaciones de seguridad organizacional para los líderes 5

Protección de datos confidenciales 5

Gestión de amenazas internas 5

Garantizar el cumplimiento de la normativa 5

Estrategias para abordar las preocupaciones de liderazgo 6

Implementación de una gestión potente de identidad y acceso 6

Mejorar 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 cortafuegos a zero trust 9

Un enfoque integral de zero trust 9

Fuentes 9

©2025 Zscaler, Inc. Todos los derechos reservados.

Introducción

Los ciberataques crecieron un asombroso 30 % interanual[1] a nivel mundial en el segundo trimestre de 2024. La mayor 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 ThreatLabz Encrypted Attacks de Zscaler, la nube de Zscaler bloqueó una cifra sin precedentes de 32 100 millones de ataques integrados en tráfico TLS/SSL, y las amenazas cifradas representan el 87,2 % de todos los ataques bloqueados, un aumento interanual del 10,3 %.[2] Estos datos ponen de manifiesto la creciente dependencia del cifrado por parte de los ciberdelincuentes para ocultar sus actividades maliciosas.

Las tecnologías heredadas, como los cortafuegos y las redes privadas virtuales (VPN), ya no son suficientes para proteger los datos, las aplicaciones y las redes de la empresa, lo que genera en las personas encargadas de la toma de decisiones y en los altos cargos una larga lista de preocupaciones cuando se trata de proteger los entornos de trabajo remotos. Los líderes están bajo presión constante para minimizar el riesgo de infracciones, garantizar el cumplimiento de las regulaciones y los estándares del sector, y evitar el robo de datos valiosos como propiedad intelectual o secretos comerciales.

La buena noticia es que las soluciones zero trust basadas en la nube están diseñadas para proteger las redes de las organizaciones que utilizan personal remoto e híbrido. Con la tecnología adecuada, los ejecutivos pueden eliminar estas preocupaciones principales.

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, infracciones 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 anterior a la pandemia, los cortafuegos y las VPN podrían 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 forma en que las organizaciones protegen sus entornos digitales hoy en día.

Últimas tendencias en seguridad digital y trabajo remoto

Los empleados remotos inevitablemente necesitan recursos de la empresa para realizar su trabajo, independientemente de sus ubicaciones, y muchas organizaciones han adoptado aplicaciones de software como servicio (SaaS) basadas en la nube para habilitar 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 e infracciones de seguridad.

Los cibercriminales también han desarrollado tácticas más sofisticadas (como el robo de credenciales y los ataques de día cero), lo que aumenta la apuesta de los directivos en materia de ciberseguridad. De hecho, Estados Unidos sigue siendo el principal objetivo del ransomware, con un 49,95 % de los ataques en general, 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 normas de privacidad y seguridad de los datos, por no mencionar el riesgo financiero.

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

- **Arquitectura zero trust**, que funciona según el principio de “nunca confiar, siempre verificar”. Todos los usuarios y dispositivos, incluidos los dispositivos propios de los usuarios, deben ser verificados.
- **Detección de amenazas impulsada por inteligencia artificial (IA) y aprendizaje automático (ML)**, que ayuda a identificar y mitigar de forma proactiva ciberataques sofisticados.
- **Segmentación de aplicaciones**, que evita el movimiento lateral de amenazas.
- **Seguridad de terminales**, que se centra en proteger los dispositivos que utilizan los empleados remotos. Las soluciones basadas en IA pueden detectar y bloquear amenazas antes de que afecten a los terminales, lo que garantiza una mejor protección para el personal distribuido.

©2025 Zscaler, Inc. Todos los derechos reservados.

Principales preocupaciones de seguridad organizacional para los líderes

Con la prevalencia del trabajo remoto e híbrido y la creciente dependencia de 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:

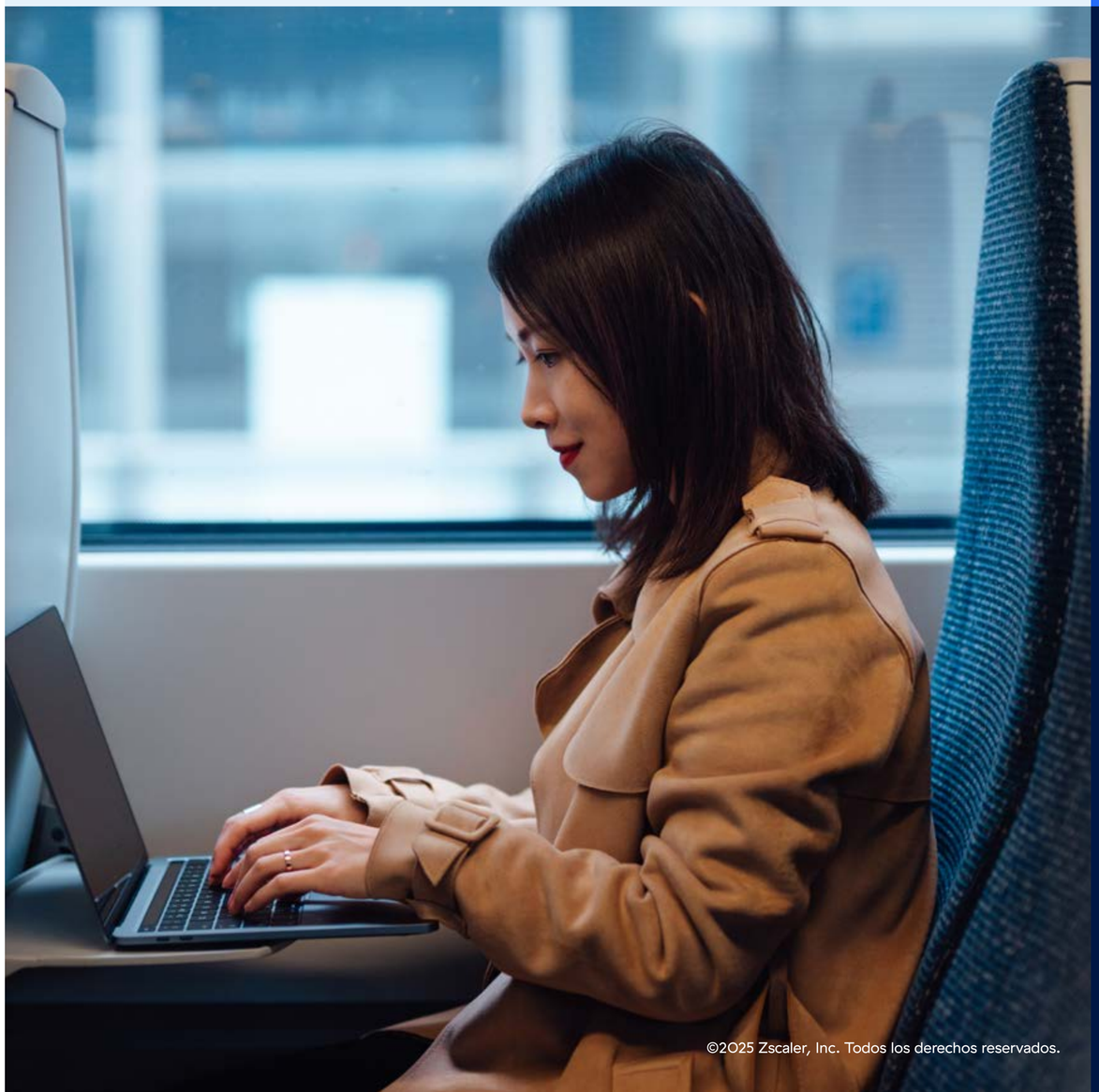
- **Cifrado de extremo a extremo** para proteger datos en reposo y en tránsito, especialmente cuando se transfieren a través de canales no seguros.
- **Gestión de identidad y acceso** para garantizar que sólo los empleados autorizados puedan acceder y utilizar los datos necesarios.
- Técnicas de **prevención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

Gestión de amenazas internas

Las acciones tanto accidentales como 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 implementado 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 del sector, como la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA). En entornos de trabajo remoto, mantener el cumplimiento de estos requisitos reglamentarios implica estrategias de gobernanza exhaustivas.



©2025 Zscaler, Inc. Todos los derechos reservados.

Estrategias para abordar las preocupaciones de liderazgo

Los altos ejecutivos pueden adoptar varias estrategias para abordar los complejos desafíos de seguridad del entorno laboral moderno.

Implementación de una gestión potente 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 sólo 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 perímetro, IAM implica controles de acceso más estrictos independientemente del dispositivo y la ubicación del usuario. Los líderes deberían plantearse implementar una plataforma que admita soluciones IAM flexibles e integración.

Mejorar las capacidades de detección y respuesta ante amenazas

A medida que los ciberdelincuentes evolucionan sus estrategias, los líderes de seguridad también deben actualizar las suyas para frustrar los ataques con detección y respuesta ante amenazas avanzadas. Implementar soluciones que utilicen modelos de IA y ML para supervisar el tráfico de la red y el comportamiento del usuario para detectar desviaciones automáticamente.

La IA y el ML también amplían las soluciones de zero trust que aíslan los dispositivos y archivos comprometidos en tiempo real, lo que permite respuestas rápidas a las amenazas y habilita 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 sólo serán plenamente eficaces si también lo son las personas que las utilizan. Un buen ejemplo es el 80 % de los CISO que creen que la negligencia de los empleados y el riesgo humano serán las principales preocupaciones en materia de ciberseguridad en 2026[4]. Los empleados que trabajan a distancia son especialmente vulnerables porque no siempre pueden comunicarse en persona con los profesionales de seguridad para pedir ayuda, lo que provoca retrasos y daños irreversibles.

Para mitigar estos escenarios, las organizaciones pueden implementar programas de capacitación en seguridad continua que familiaricen a los empleados con las amenazas existentes, emergentes y en evolución, y las mejores prácticas que les permitan mantenerse alerta ante un panorama de amenazas en constante cambio. Forme a su equipo sobre las mejores prácticas de trabajo remoto, higiene de contraseñas y manejo seguro de datos. Además, realice sesiones de capacitación periódicamente para poner al día a los empleados sobre 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.

Aprovechar 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 base para garantizar que los equipos tengan una seguridad integral:

Zscaler Internet Access (ZIA)

Zscaler Internet Access es una solución zero trust, basada en IA y nativa de la nube que ayuda a reforzar la seguridad digital para el personal remoto. Con una arquitectura de proxy zero trust que inspecciona el 100 % del tráfico TLS/SSL a escala y conexiones directas de usuario a aplicación basadas en identidad, contexto y políticas comerciales, ZIA garantiza un acceso seguro y sin inconvenientes a SaaS y aplicaciones basadas en la web con las siguientes capacidades clave:

- **La pasarela web segura nativa de la nube (SWG)** ofrece una experiencia web rápida y segura mientras detecta y previene ataques avanzados con análisis en tiempo real impulsados por inteligencia artificial y filtrado de URL.
- **Prevención de amenazas avanzada basada en IA/ML** para detener amenazas avanzadas como botnets, ransomware, comando y control, uso compartido peligroso, contenido activo malicioso, scripts entre sitios, sitios fraudulentos, etc.
- **El filtrado URL mediante IA** garantiza sesiones de navegación de aplicaciones web seguras para sus usuarios deteniendo amenazas sofisticadas, como phishing y ransomware, y aplicando una política de uso aceptable.
- **Cloud Access Security Broker (CASB)** protege las aplicaciones en la nube, protege los datos, detiene las amenazas y garantiza el cumplimiento en sus entornos SaaS e IaaS con protección integrada.
- **Data Loss Prevention (DLP)** protege los datos en movimiento con una inspección completa en línea, que incluye Exact Data Match (EDM), Indexed Document Matching (IDM) y aprendizaje automático.
- **La política dinámica basada en riesgo** detiene los ataques activos y prepara sus defensas para el futuro con análisis de usuarios, dispositivos, aplicaciones y contenidos que impulsen continuamente una política dinámica de seguridad y acceso.
- **El cortafuegos Zero Trust** habilita conexiones rápidas y seguras dentro y fuera de la red así como accesos locales a Internet para el tráfico de usuarios en todos los puertos y protocolos, sin necesidad de administrar ningún hardware o software
- **El aislamiento del navegador impulsado por IA** hace que las sesiones web sean sólo píxeles en el navegador del usuario, lo que brinda una experiencia web casi nativa sin el riesgo de pérdida de datos o infección del dispositivo.
- **La seguridad DNS** filtra dominios maliciosos y de riesgo, y detiene el uso de túneles DNS para transferir cargas útiles 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 de zero trust (ZTNA) impulsada por IA del sector y es una oferta nativa de la nube que brinda acceso zero trust para todos los usuarios. Al ofrecer conectividad directa a aplicaciones privadas y minimizar la superficie de ataque, ZPA elimina el movimiento lateral de amenazas mediante la segmentación de usuario a aplicación impulsada por IA y protege contra ataques sofisticados con inspección de tráfico integrada y protección de datos y aplicaciones. Algunas de las capacidades clave de ZPA que pueden proteger al personal híbrido incluyen:

- **La segmentación de aplicaciones impulsada por IA** descubre aplicaciones automáticamente y proporciona recomendaciones generadas por IA sobre segmentos y políticas de aplicaciones para reducir su superficie de ataque y evitar el movimiento lateral.
- **La segmentación de carga de trabajo a carga de trabajo** protege las comunicaciones de carga de trabajo en la nube en entornos híbridos y multinube como AWS y Azure.
- **El acceso remoto con privilegios** proporciona a trabajadores remotos y terceros acceso remoto sin cliente a sistemas de producción confidenciales RDP, SSH y VNC.
- **El perímetro de servicio privado** lleva ZTNA a los usuarios locales con acceso directo del usuario a la aplicación y con el mínimo privilegio a aplicaciones privadas.
- **La continuidad de la actividad empresarial** garantiza un acceso ininterrumpido y basado en políticas a aplicaciones de misión crítica durante cortes de conectividad y eventos de cisne negro.
- **El soporte de aplicación extranet** habilita el acceso zero trust a las aplicaciones de socios comerciales y proveedores (aplicación de extranet) alojadas en sus redes.
- **La supervisión de la experiencia digital** permite optimizar sus experiencias digitales para garantizar la productividad de los usuarios al detectar y resolver rápidamente problemas de aplicaciones, redes y dispositivos.

Funciones de seguridad avanzadas

Zscaler ofrece varias funciones avanzadas, entre ellas:

- **Inspección SSL/TLS** a escala para una protección completa de datos e inspección desde el usuario hasta la aplicación.
- **Detección de amenazas en línea impulsada por 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 fortalecer la seguridad de su entorno de trabajo remoto, debe considerar abandonar las soluciones de ciberseguridad tradicionales. La plataforma zero trust Zscaler ofrece varias formas de facilitar la transición.

Transformación de los cortafuegos a zero trust

Los cortafuegos y las VPN son ineficaces en el entorno empresarial moderno porque expanden su red corporativa, lo que brinda a los atacantes más vías de entrada. Por el contrario, Zscaler Zero Trust Exchange™ actúa como una centralita inteligente que inspecciona el tráfico entrante y saliente hacia y desde los dispositivos de los usuarios para detectar y bloquear amenazas, al tiempo que negocia de forma segura las conexiones a aplicaciones y recursos en la nube.

Un enfoque integral de zero trust

Un verdadero enfoque de zero trust para la seguridad 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 sólo los usuarios confiables puedan acceder a recursos específicos, y que esos usuarios y recursos estén designados por los controles establecidos de su empresa. Puede establecer reglas en su marco de seguridad zero trust para otorgar acceso a los usuarios en función de la ubicación, la identidad, la hora/fecha, etc., y Zscaler le guía a través de este proceso para que su organización comience con buen pie con estos controles.

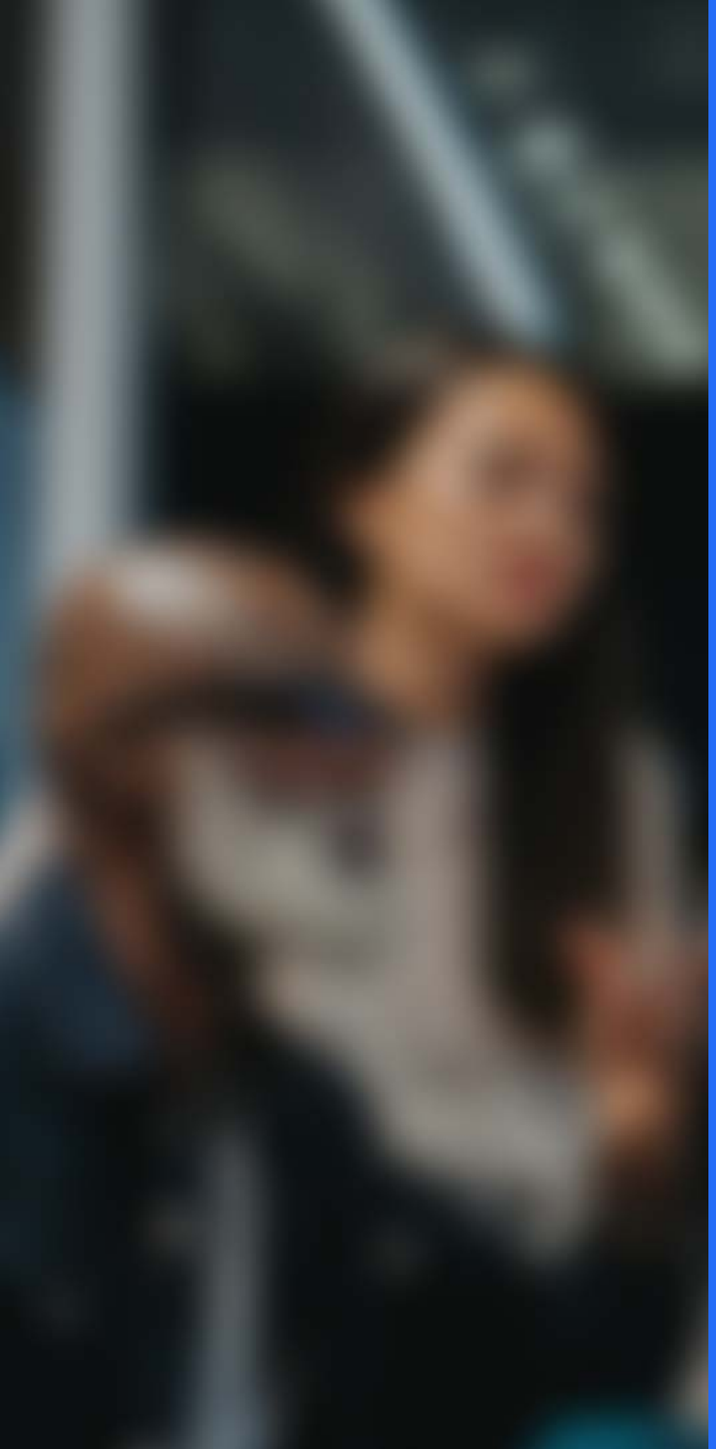
Obtenga más información sobre cómo Zscaler puede ayudarle a transformar su postura de seguridad para proteger a su personal disperso solicitando una demostración.

FUENTES:

1. El CISO inteligente de Check Point Research revela las tendencias de ciberataques del segundo trimestre de 2024, destacando los aumentos globales y en los Emiratos Árabes Unidos, 29 de julio de 2024.
2. Informe sobre el estado de los ataques cifrados de ThreatLabz de Zscaler, 2024.
3. Informe sobre el ransomware de ThreatLabz de Zscaler , 2024.
4. Infosecurity Magazine, El 70 % de los CISO esperan ciberataques el próximo año, según un informe, 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 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.

