LIBRO ELECTRÓNICO

Cómo las SD-WAN tradicionales posibilitan los ataques de ransomware y cómo detenerlos

Introducción

Los desafíos de seguridad continúan aumentando pero las arquitecturas de red no evolucionan al mismo ritmo. Según el informe sobre ransomware 2024 de ThreatLabz de Zscaler, se realizaron los pagos de rescate más grandes que nunca y hubo un aumento interanual del 58 % en la cantidad de empresas extorsionadas. El ransomware se propaga rápidamente a través de las organizaciones por una sencilla razón: las redes tradicionales confían implícitamente en todo lo que está conectado a ellas, lo que permite que el ransomware se mueva libremente desde dispositivos infectados en sucursales remotas hasta aplicaciones clave.

En el pasado, las organizaciones dependían de un modelo de seguridad de "castillo y foso", donde todo el tráfico dentro de la red se consideraba seguro de forma predeterminada y los controles de seguridad se aplicaban únicamente en el perímetro. A medida que se volvieron más distribuidas y centradas en la nube, las organizaciones simplemente extendieron sus redes privadas a sucursales y nubes, utilizando redes de área amplia definidas por software (SD-WAN) y VPN de sitio a sitio. Esto creó redes grandes, planas y confiables en las que los atacantes pueden moverse lateralmente, a pesar de la multitud de cortafuegos que se implementaron.

Mientras tanto, las redes incluyen una cantidad cada vez mayor de dispositivos IoT. Se estima que 55,7 mil millones de estos dispositivos estarán conectados a redes empresariales para 2025, generando 80 mil millones de zettabytes de datos cada año.[1] Esta expansión del perímetro crea una superficie de ataque cada vez mayor, lo que hace que las organizaciones sean más vulnerables. Todas estas tendencias hacen que los enfoques de seguridad basados en el perímetro sean cada vez más insostenibles. Como resultado, año tras año, la cantidad (y el coste) de las infracciones de datos continúa aumentando y la actividad de ransomware sigue creciendo.

Para proteger su infraestructura contra estas amenazas crecientes, las organizaciones de todos los sectores recurren cada vez más a un enfoque zero trust para la ciberseguridad.

Aumento del 17,8% en los ataques de ransomware entre 2023 y 2024.[2]

Se informó de un pago récord de **75 millones de dólares** por ataques de ransomware en 2024.[2]

Aumento del 104 % en el número de víctimas de infracciones de datos entre 2023 y 2024.[3]

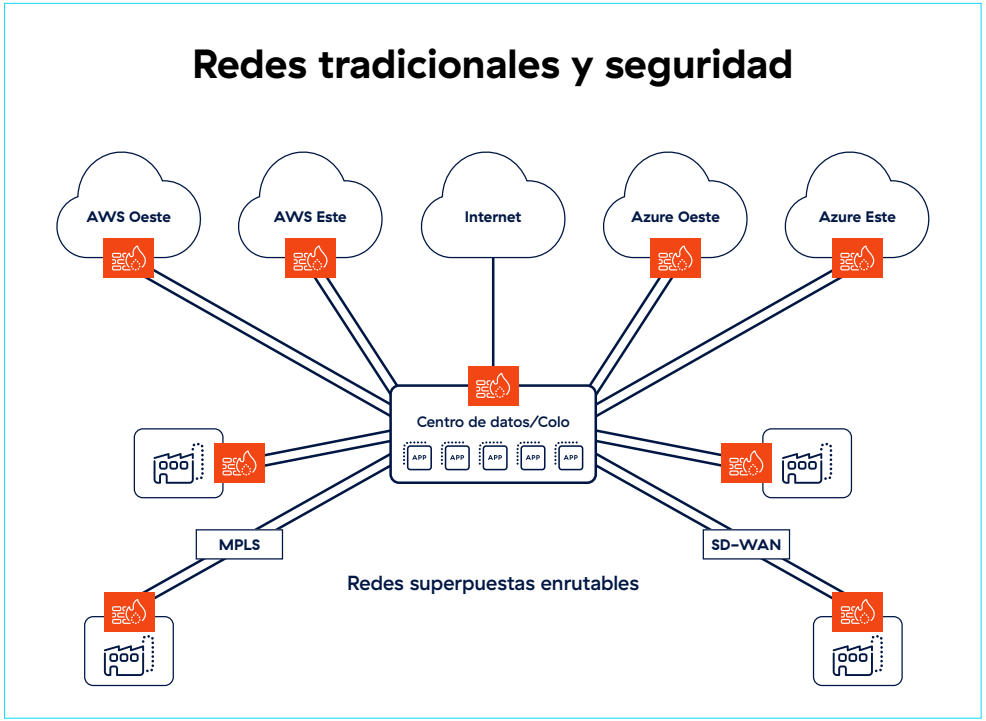
El coste promedio global de una filtración de datos alcanzó el máximo histórico de 4,88 millones de dólares estadounidenses en 2024.[4]

1: IDC Research, El futuro de los ecosistemas industriales: datos y conocimientos compartidos, 2021.
2: Informe sobre ransomware Zscaler ThreatLabz 2024.
3: Centro de recursos sobre robo de identidad, análisis de infracciones de datos del primer semestre de 2024.
4: IBM, Informe sobre el coste de una infracción de datos en 2024.

¿Qué es y qué no es la SD-WAN tradicional?

SD-WAN aprovecha la automatización para dirigir el tráfico de red hacia la ruta más eficiente a través de diversos servicios e infraestructuras de transporte de red. Los protocolos de enrutamiento conscientes de las aplicaciones mejoran el rendimiento de las aplicaciones al priorizar el tráfico entre aplicaciones críticas.

Las soluciones SD-WAN tradicionales simplemente extienden la red de la organización a las sucursales y los centros de datos. Diseñadas para simplificar la conectividad, SD-WAN permiten que los dispositivos en todas partes (incluidas sucursales, fábricas y sitios de terceros) se comuniquen con aplicaciones en el centro de datos o la nube pública. Estas arquitecturas, que comprenden una red de dispositivos y VPN de sitio a sitio, ofrecen poca o ninguna protección frente al movimiento lateral de amenazas y el ransomware.



Permite el movimiento lateral de amenazas y facilita los ataques de ransomware.

Amplía la superficie de ataque a sucursales, fábricas y nubes.

Aumenta los costes, la complejidad y los tiempos de implementación.

SD-WAN se diseñó para mejorar la conectividad, haciendo que sea más rápido y fácil para los usuarios acceder a los recursos. Pero conectividad no es igual a seguridad. En cambio, zero trust requiere que se verifique la identidad y la postura de seguridad antes de permitir la conectividad. La confianza implícita incorporada en las redes tradicionales solo las hace más difíciles de proteger y facilita la rápida propagación del ransomware.

Para lograr zero trust en una SD-WAN tradicional, una organización necesita agregar dispositivos de seguridad, herramientas y puntos de aplicación de políticas adicionales. El resultado es un mosaico de cortafuegos, VPN en malla y otras herramientas como control de acceso a la red (NAC), soluciones de seguridad DNS, etc. Esta arquitectura es compleja y su gestión consume un presupuesto y recursos de personal excesivos.

> “De hecho, cuando la conectividad se logra a través de la confianza por defecto, está en desacuerdo con el modelo zero trust”.

¿Qué es la confianza cero?

La confianza cero es una estrategia de seguridad que afirma que no se debe confiar en ninguna entidad (usuario, aplicación, servicio o dispositivo) de forma predeterminada. Siguiendo el principio de acceso con privilegios mínimos, antes de permitir cualquier conexión, se establece la confianza en función del contexto y la postura de seguridad de la entidad, y se sigue reevaluando continuamente para cada nueva conexión, incluso si la entidad ya se había autenticado antes.

Empezando con Zero Trust

Comenzar con una red abierta y plana, y agregar puntos de cumplimiento y controles de seguridad para lograr zero trust es operativamente complejo y costoso. Los proyectos de segmentación de red a menudo duran meses o incluso años, y los requisitos suelen cambiar antes de que estos proyectos finalicen. ¿Qué pasaría si pudiese empezar al revés? ¿Qué pasaría si sus sucursales pudieran ser como cafeterías, sin una red enrutable que las conectara a las aplicaciones de la organización en la nube?

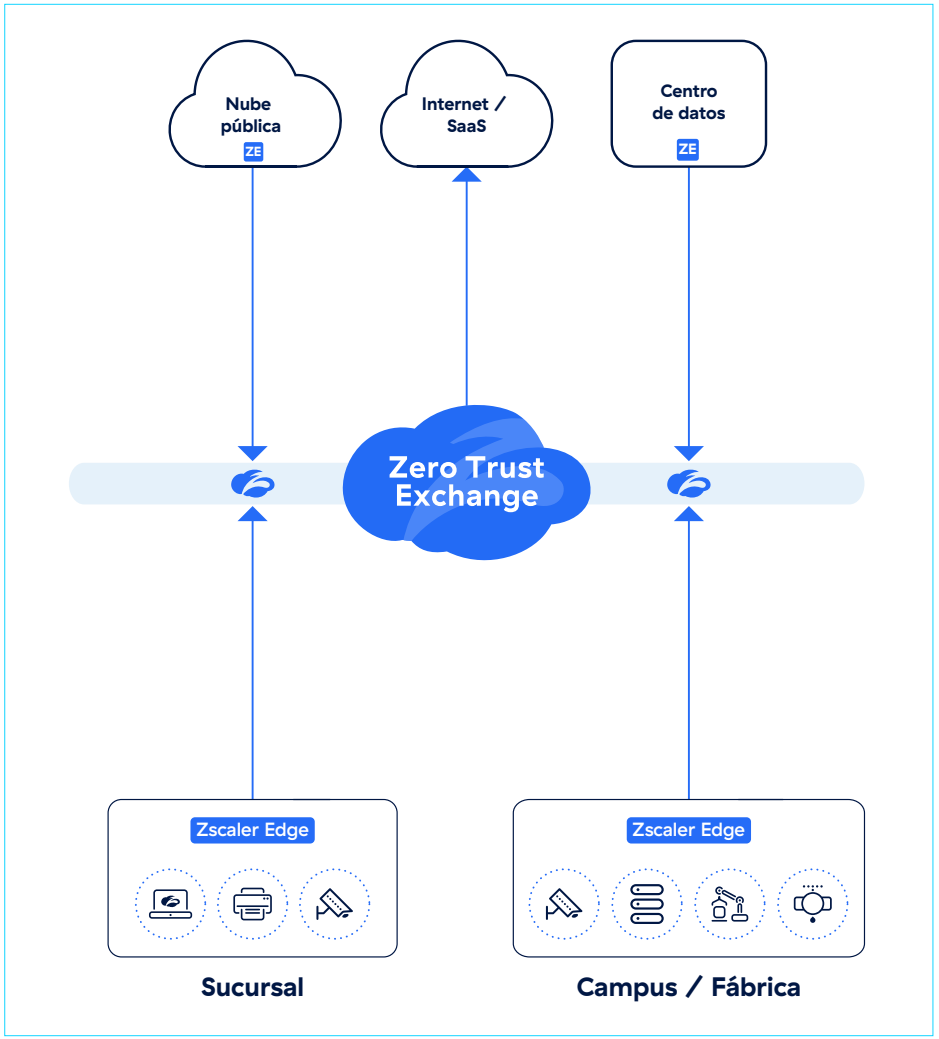
Conecta usuarios y dispositivos a aplicaciones en función de políticas, no de la presencia en la red, lo que proporciona seguridad sólida y simplicidad operativa.

Este es un enfoque nativo de zero trust que hace imposible el movimiento lateral, ya que los usuarios y los dispositivos (incluidos los dispositivos de Internet de las cosas (IoT) y de tecnología operativa (OT)) nunca están conectados directamente a las aplicaciones. En cambio, se comunican a través de la plataforma Zscaler Zero Trust Exchange™, que facilita la protección total de datos y frente a ciberamenazas con sólidos controles de acceso basados en identidad y contexto.

> “Zero Trust SD-WAN es una nueva forma de brindar a las sucursales y centros de datos un acceso rápido y confiable a Internet, aplicaciones privadas y servicios en la nube sin extender la red corporativa a todas partes”.

Este enfoque zero trust:

- **Mejora el rendimiento de las aplicaciones.**
  Las empresas pueden reemplazar las complejas VPN de sitio a sitio por una arquitectura sencilla de conexión directa a la nube que ofrece un rendimiento rápido y constante para respaldar la productividad.
- **Minimiza la superficie de ataque de Internet.**
  Las soluciones WAN tradicionales exponen los puertos VPN a la Internet pública, lo que deja la red vulnerable a los ataques. Con Zero Trust SD-WAN, las aplicaciones privadas se encuentran detrás de Zero Trust Exchange, donde no pueden ser descubiertas ni atacadas desde Internet.
- **Previene el movimiento lateral de amenazas.**
  Las VPN de sitio a sitio crean una gran red enrutable donde una infección de malware puede transmitirse desde un solo dispositivo a todos los dispositivos de la red. Con Zero Trust SD-WAN, las conexiones se realizan directamente a las aplicaciones, no a la red. Esto hace imposible el movimiento lateral.
- **Reduce los costes y la complejidad.**
  Este enfoque elimina la necesidad de contar con múltiples cortafuegos, VPN, NAC y otras soluciones en capas. El resultado es una arquitectura más simple, menos costosa y mucho más fácil de configurar y mantener.



Zscaler resuelve los desafíos de la SD-WAN tradicional

Al confiar en Zero Trust Exchange para conectar de forma segura sucursales, fábricas y centros de datos, Zscaler garantiza un acceso zero trust uniforme y consistente para todos los usuarios, dispositivos IoT/OT y aplicaciones.

	Zero Trust SD-WAN	SD-WAN tradicional
Reduce la superficie de ataque y detiene el movimiento lateral de amenazas	Si	No
Reduce la complejidad de las reglas de ACL y cortafuegos	Si	No
Elimina las disyuntivas entre seguridad y rendimiento	Si	No
Elimina la necesidad de cortafuegos en la sucursal	Si	No

Zscaler Zero Trust SD-WAN es lo suficientemente flexible como para admitir múltiples opciones de implementación que no requieren un reemplazo completo. Puede funcionar junto con la infraestructura SD-WAN de su sucursal existente y crear superposiciones de zero trust para Zero Trust Exchange. Esto garantizará un acceso seguro y de alto rendimiento desde los dispositivos de su sucursal a aplicaciones privadas en otros sitios y en la nube sin permitir el movimiento lateral de amenazas.

Si está adoptando un nuevo enfoque para las necesidades de conectividad de su organización, comience con una arquitectura nativa zero trust que reduzca la complejidad y elimine la necesidad de cortafuegos adicionales en todas partes. Zscaler Zero Trust SD-WAN puede administrar las conexiones de su ISP y dirigir de manera inteligente el tráfico de aplicaciones para brindar una experiencia de sucursal segura, similar a una cafetería, a sus usuarios y, al mismo tiempo, mantener a su organización a salvo de ataques de ransomware.

Detenga los ataques de ransomware con zero trust

Zero trust es fundamental para enfrentar los desafíos de seguridad actuales y reducir el riesgo de ataques de ransomware. Con Zscaler Zero Trust SD-WAN, su organización puede proteger todas las comunicaciones y eliminar la posibilidad de movimiento lateral de amenazas sin el coste y la complejidad operativa de los enfoques tradicionales. Además, las experiencias digitales excepcionales mantendrán a los clientes, empleados y otros usuarios finales productivos y satisfechos.

zscaler™ | Experience your world, secured.™

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 los ciberataques y la pérdida de datos mediante la conexión segura de los 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 SASE es la mayor plataforma de seguridad en línea en la nube del mundo. Si desea más información, visite **www.zscaler.com/es.**

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