EBOOK

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

Introducción

A medida que los desafíos de seguridad siguen aumentando, las arquitecturas de red no han evolucionado para seguir su ritmo. Según el informe sobre ransomware de Zscaler ThreatLabz 2024, los pagos de rescates han sido mayores que nunca y se ha producido un aumento interanual del 58 % en el número de empresas extorsionadas. El ransomware se propaga rápidamente por las organizaciones por una sencilla razón: las redes heredadas confían implícitamente en todo lo que está conectado a ellas, lo que permite que el ransomware se mueva libremente desde los dispositivos infectados en las sucursales remotas hasta las aplicaciones joya de la corona.

En el pasado, las organizaciones dependían de un modelo de seguridad castle-and-moat, donde todo el tráfico dentro de la red se consideraba seguro por defecto y los controles de seguridad se aplicaban solo 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 y confiables en las que los atacantes pueden moverse lateralmente, a pesar de la multitud de firewalls implementados en todas partes.

Mientras tanto, las redes incluyen un número cada vez mayor de dispositivos IoT. Se calcula que 55,700 millones de estos dispositivos estarán conectados a las redes empresariales en 2025, generando 80,000 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 la seguridad basados en el perímetro sean cada vez más insostenibles. Como resultado, año tras año, el número (y el coste) de las violaciones de datos sigue aumentando y la actividad del ransomware sigue creciendo.

Para proteger su infraestructura contra estas amenazas crecientes, las organizaciones de todas las industrias 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]

En 2024 se informó de un pago récord de 75 millones de dólares por un ataque de ransomware.[2]

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

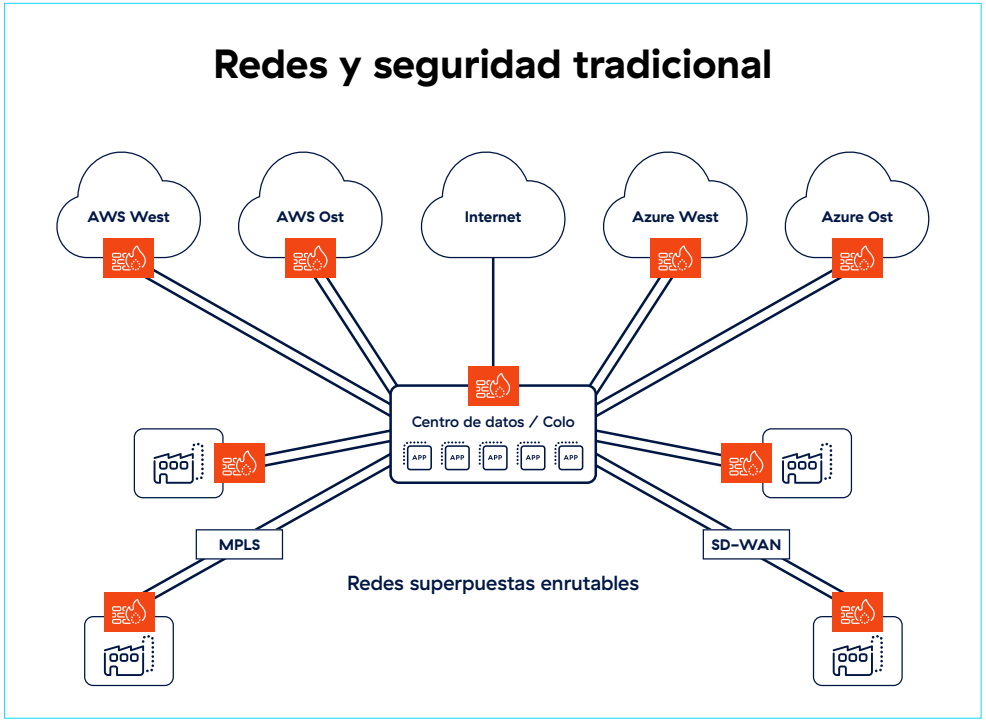
El costo promedio global de una violación de datos alcanzó un máximo histórico de 4.88 **millones** en 2024.[4]

1: IDC Research, Future of Industry Ecosystems: Shared Data and Insights, 2021.
2: Zscaler ThreatLabz 2024 Ransomware Report.
3: Identity Theft Resource Center, H1 2024 Data Breach Analysis.
4: IBM, Cost of a Data Breach Report 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 varios servicios e infraestructuras de transporte de red. Los protocolos de enrutamiento que tienen en cuenta a las aplicaciones mejoran el rendimiento de éstas priorizando 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. Diseñado para simplificar la conectividad, SD-WAN permite 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 contra el 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 costos, la complejidad y los tiempos de implementación.

SD-WAN fue diseñado para mejorar la conectividad, haciendo que sea más rápido y fácil para los usuarios acceder a los recursos. Pero la conectividad no es igual a seguridad. En cambio, Zero Trust requiere que se verifiquen 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 firewalls, VPN de malla y otras herramientas como el control de acceso a la red (NAC), soluciones de seguridad DNS, etc. Esta arquitectura es compleja y su gestión consume excesivos recursos presupuestarios y de personal.

> De hecho, cuando la conectividad se consigue a través de la confianza por defecto, se contradice con el modelo Zero Trust".

¿Qué es Zero Trust?

La confianza cero es una estrategia de seguridad que afirma que no se debe confiar en ninguna entidad (usuario, aplicación, servicio o dispositivo) de manera 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 luego se reevalúa continuamente para cada nueva conexión, incluso si la entidad se autenticó antes.

Primeros pasos con Zero Trust

Empezar con una red abierta y plana y agregar puntos de aplicación 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. ¿Y si pudiera empezar al revés? ¿Y si sus sucursales pudieran ser como cafeterías, sin una red enrutable que las conectara a las aplicaciones de la organización en la nube?

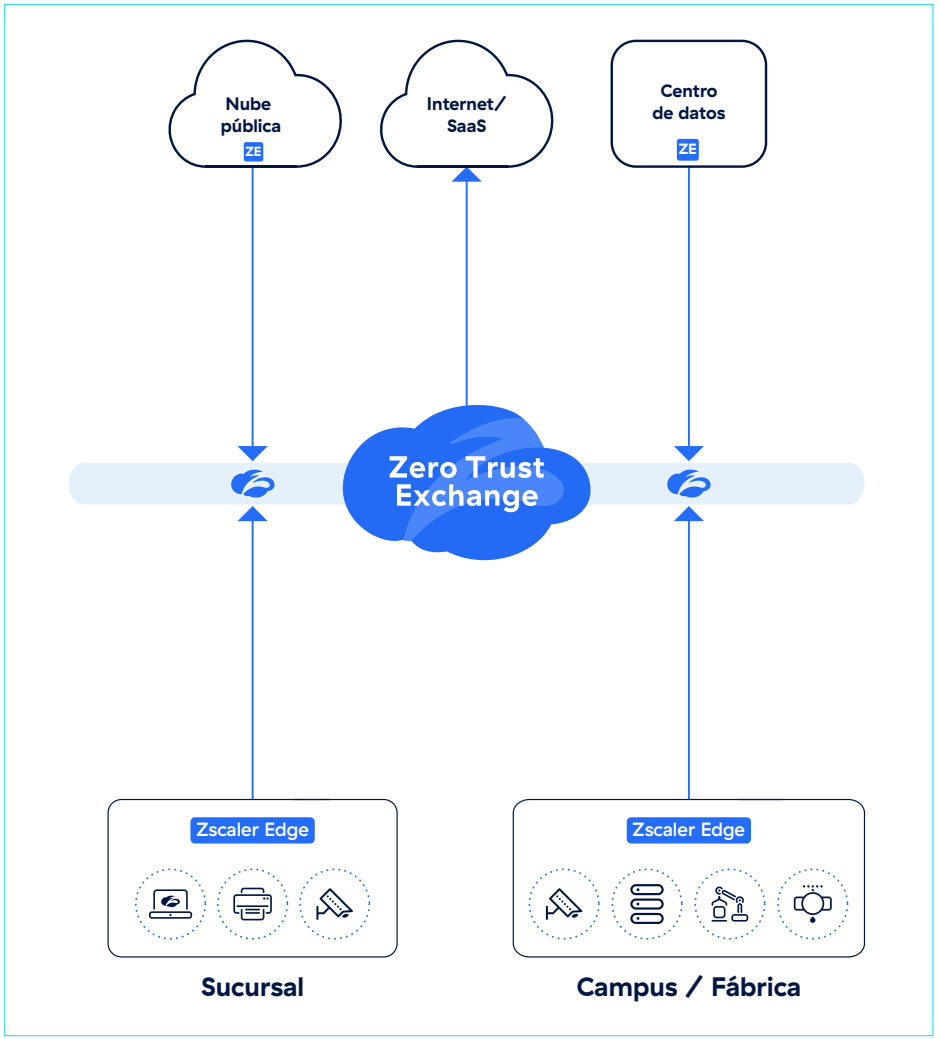
Conecta usuarios y dispositivos a aplicaciones en función de políticas, no de la presencia en la red, lo que proporciona seguridad sólida y simplicidad operativa.

Este es un enfoque Zero Trust nativo 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 contra ciberamenazas con sólidos controles de acceso basados en identidad y contexto.

> “Zero Trust SD-WAN es una nueva manera 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 impulsar 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 costos y la complejidad.**
  Este enfoque elimina la necesidad de contar con múltiples firewalls, 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 basarse en el Zero Trust Exchange para conectar de manera 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	Sí	No
Reduce la complejidad de los firewalls y de las reglas de ACL	Sí	No
Elimina las disyuntivas entre seguridad y rendimiento.	Sí	No
Elimina la necesidad de firewalls en la sucursal.	Sí	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 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 Zero Trust nativa que reduzca la complejidad y elimine la necesidad de firewalls 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 costo 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. Zero Trust Exchange™ protege a miles de clientes contra ciberataques y pérdida de datos al conectar usuarios, dispositivos y aplicaciones de manera segura en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange, basado en SASE, es la plataforma de seguridad en la nube en línea más grande del mundo. Para obtener más información, visite **www.zscaler.com/mx.**

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134

zscaler.com/mx