

Libro electrónico

4 requisitos para una sucursal de confianza cero

© 2024 Zscaler, Inc. Todos los derechos reservados.

Al implementar un enfoque de confianza cero en la sucursal, las empresas no sólo pueden fortalecer sus redes contra amenazas, sino también optimizar la conectividad para usuarios, dispositivos y aplicaciones en diversas ubicaciones.

En el dinámico panorama empresarial actual, muchas empresas afrontan desafíos para garantizar la seguridad de sus usuarios, dispositivos y aplicaciones. En el pasado, cuando las aplicaciones residían en centros de datos y los usuarios se conectaban principalmente desde oficinas, los requisitos de conectividad eran relativamente sencillos. Las arquitecturas radiales tradicionales basadas en cortafuegos eran eficaces para satisfacer esas necesidades. Sin embargo, a medida que el entorno de trabajo moderno ha ido evolucionado, estos enfoques tradicionales experimentan dificultades para brindar una protección adecuada contra las amenazas y una experiencia de usuario óptima.

Hoy en día, los usuarios ya no se conectan exclusiva-mente desde sus espacios de oficina, sino desde una gran cantidad de ubicaciones, incluidos sus hogares, cafeterías, aeropuertos, etc. Además, la proliferación del Internet de las cosas (IoT) complica aún más el panorama de la seguridad empresarial, ya que los dispositivos IoT/OT suponen un riesgo de seguridad adicional.

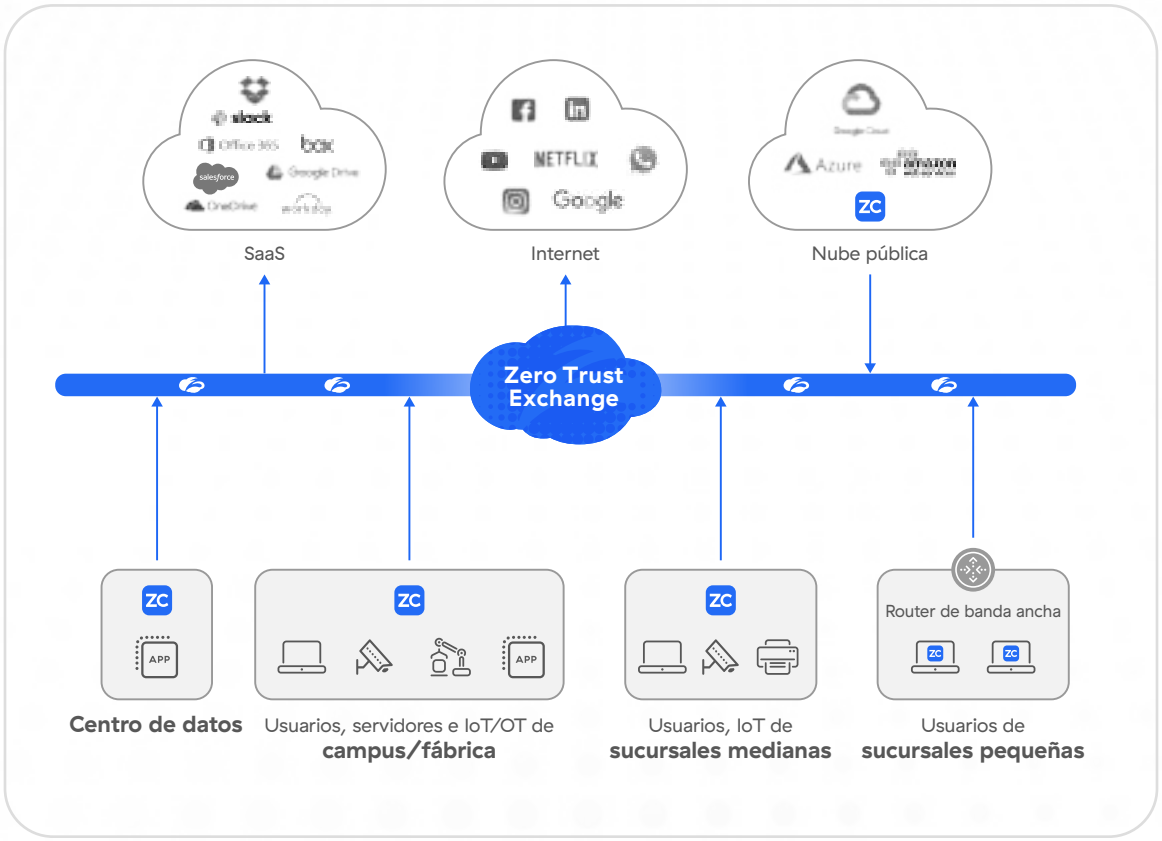

Figura 1: La sucursal de confianza cero ofrece un enfoque de confianza cero para la conectividad de red

© 2024 Zscaler, Inc. Todos los derechos reservados.

El panorama cambiante está impulsando a las organizaciones hacia un enfoque de confianza cero en materia de seguridad. Los principios de confianza cero (nunca confiar, siempre verificar y exigir el acceso menos privilegiado) han permitido a muchas empresas frustrar ataques cibernéticos sofisticados. Con confianza cero, los usuarios solo obtienen acceso a las aplicaciones que necesitan, a diferencia de las VPN, que colocan a los usuarios en la red y les brindan acceso sin restricciones. Al aplicar principios de confianza cero a la conectividad de la red, las organizaciones pueden protegerse mejor contra las amenazas, especialmente las que se originan en sus instalaciones. La implementación del enfoque de confianza cero en la sucursal garantiza una conectividad segura y operaciones simplificadas, superando las complejidades de enrutamiento o una experiencia de usuario degradada, al tiempo que elimina la superficie de ataque y previene el movimiento lateral de amenazas.

Una arquitectura de sucursal de confianza cero garantiza una seguridad mejorada para todas las ubicaciones, incluidas sucursales, fábricas, quioscos y centros de datos. He aquí cuatro requisitos clave para garantizar una sucursal de confianza cero:

Garantice los principios de confianza cero para su red 1

Proteja los dispositivos IoT/OT en sus sucursales 2

Garantice rutas directas a la nube para el tráfico SaaS/Internet 3

Garantice una experiencia de usuario consistente para empleados que trabajan desde la oficina y empleados remotos 4

© 2024 Zscaler, Inc. Todos los derechos reservados.

La SD-WAN tradicional no es de confianza cero

Los dispositivos SD-WAN tradicionales simplemente extienden la red corporativa a sucursales remotas, ampliando la superficie de ataque empresarial. Ofrecen una protección deficiente contra el movimiento lateral de amenazas, lo que permite que los dispositivos comprometidos en ubicaciones remotas se comuniquen fácilmente con aplicaciones críticas para el negocio en el centro de datos o la nube pública. Las empresas experimentan un mayor riesgo de sufrir amenazas laterales y ataques basados en Internet al utilizar SD-WAN heredada. Una amalgama de dispositivos de seguridad, herramientas y políticas no estándar conducen a un mayor riesgo de seguridad debido a brechas conocidas y desconocidas en la cobertura de seguridad. Por lo tanto, al diseñar una conectividad segura de las sucursales, resulta imperativo centrarse en implementar la confianza cero para reducir la superficie de ataque y evitar el movimiento lateral de las amenazas.

Un informe de riesgos de VPN de 2023 elaborado por Cybersecurity Insiders que encuestó a 382 profesionales de TI y expertos en ciberseguridad encontró que las VPN plantean riesgos de seguridad, y el 88 % de las organizaciones expresaron una preocupación leve a extrema de que las VPN puedan poner en peligro la seguridad de su organización.

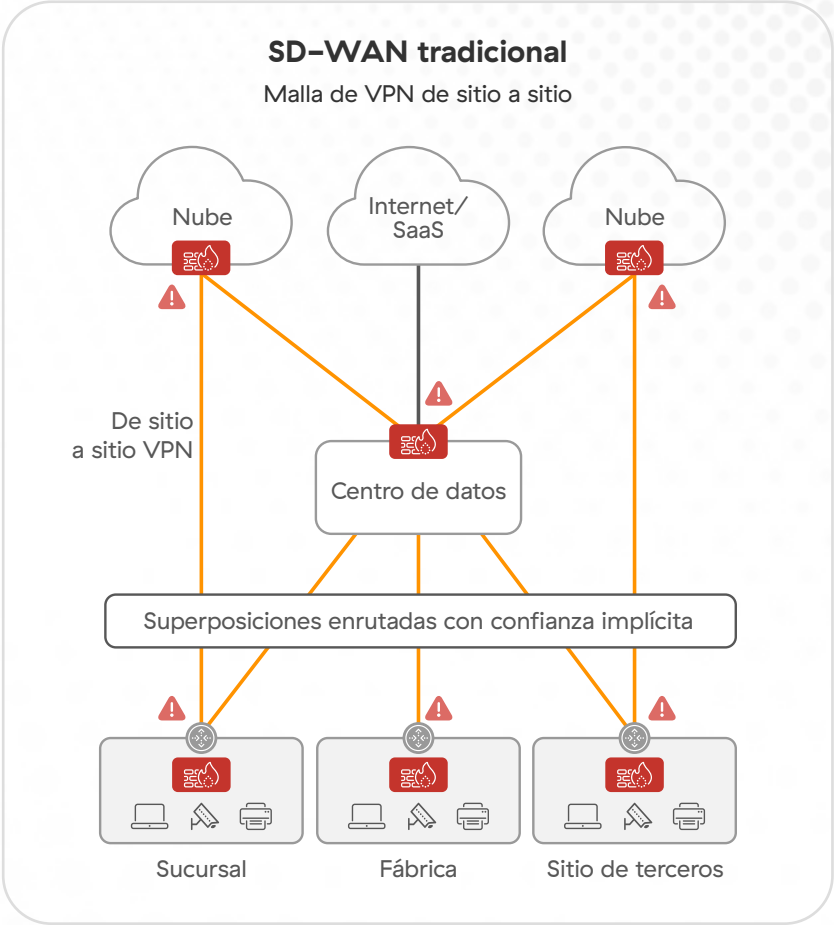

Figura 2: Las SD-WAN tradicionales amplían la superficie de ataque y no protegen contra el movimiento lateral de amenazas.

© 2024 Zscaler, Inc. Todos los derechos reservados.



Además, el 45 % de las organizaciones confirmaron que habían experimentado al menos un ataque que aprovechó las vulnerabilidades de VPN en los últimos 12 meses; una de cada tres fue víctima de ataques de ransomware relacionados con VPN. La creciente amenaza de ciberataques que aprovechen las vulnerabilidades relacionadas con las VPN subraya la necesidad urgente de abordar la seguridad de las arquitecturas actuales.

En los últimos 12 meses, ¿su organización ha experimentado algún ataque que haya aprovechado las vulnerabilidades de seguridad en sus servidores VPN?

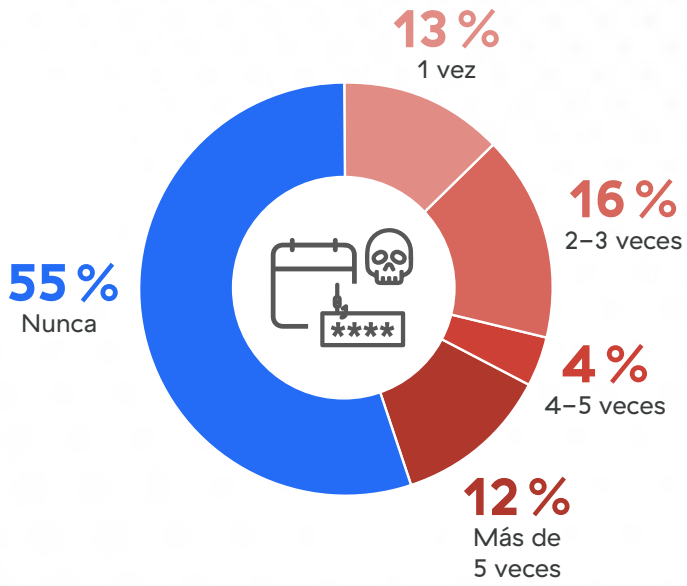

Figura 3: Las organizaciones están experimentando un aumento de los ciberataques debido a las vulnerabilidades en los servidores VPN.

© 2024 Zscaler, Inc. Todos los derechos reservados.

No se puede generar confianza cero con cortafuegos y VPN

Tradicionalmente, las empresas implementaban VPN de sitio a sitio para garantizar la conectividad a aplicaciones críticas alojadas en el centro de datos. Sin embargo, a medida que estas aplicaciones migran a la nube, la arquitectura VPN de sitio a sitio convencional se vuelve menos viable ya que el tráfico aún retorna al centro de datos, lo que resulta en una experiencia de usuario degradada y problemas de rendimiento.

También introduce complejidad operativa, ya que los túneles VPN requieren administración y configuración del sitio de forma individual. En consecuencia, los equipos de TI empresariales quieren hacer la transición de una red radial a una arquitectura directa a la nube que envíe el tráfico de aplicaciones a un proveedor de seguridad en la nube, mejorando el rendimiento de las aplicaciones.

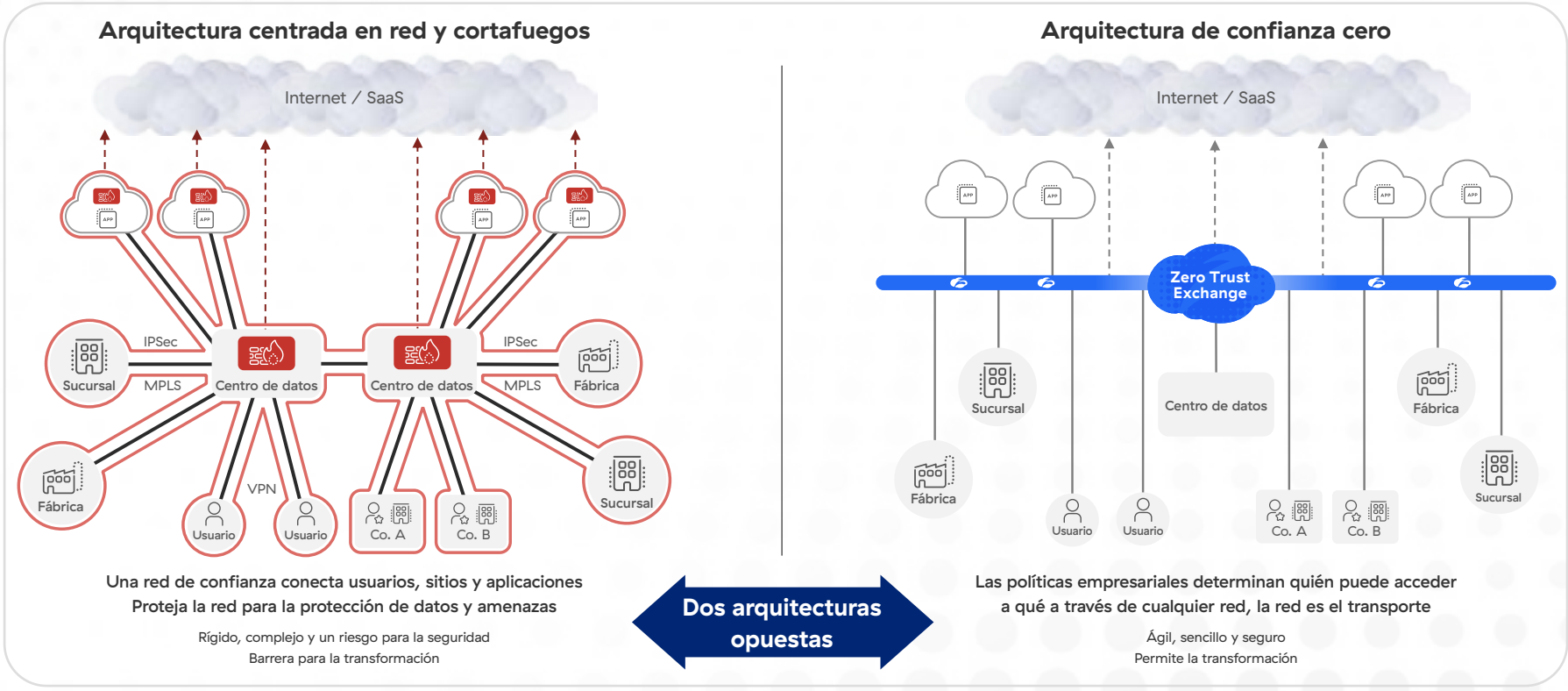

Figura 4: Las redes radiales tienen una arquitectura rígida y compleja. Por el contrario, una arquitectura de confianza cero es ágil, sencilla, segura y permite la transformación.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Cuatro requisitos clave para garantizar una sucursal de confianza cero

1 Garantice los principios de confianza cero para su red

Las VPN de sitio a sitio extienden su red corporativa a sucursales, centros de datos, regiones de nube y terceros. Las redes tradicionales amplían su superficie de ataque a entidades más allá de su control directo y permiten flujos de tráfico implícitos, lo que facilita el movimiento lateral de amenazas. A diferencia de la segmentación de red tradicional, que divide la red en zonas y es compleja de administrar, la segmentación de usuario a aplicación y de dispositivo a aplicación proporciona acceso contextual granular sólo cuando está autorizado. Una fundación de red basada en principios de confianza cero elimina los riesgos inherentes a las redes planas tradicionales y le ayuda a evitar la complejidad de superponer cortafuegos para controles de seguridad, y a prevenir problemas de experiencia y rendimiento. También introduce complejidad operativa, ya que los túneles VPN requieren administración y configuración del sitio de forma individual. En consecuencia, los equipos de TI empresariales quieren hacer la transición de una red radial a una arquitectura directa a la nube que envíe el tráfico de aplicaciones a un proveedor de seguridad en la nube, mejorando el rendimiento de las aplicaciones.

2 Proteja los dispositivos IoT/OT en sus sucursales

Los dispositivos IoT/OT están proliferando en casi todas las organizaciones con el aumento de elementos “inteligentes” como impresoras, televisores, cámaras, lectores de tarjetas y sensores. Estos dispositivos ejecutan una gran variedad de sistemas operativos con distintos riesgos de seguridad, y la gestión de parches sigue siendo un desafío como tal. Muchos líderes de TI no tienen visibilidad de estos dispositivos, y mucho menos un inventario detallado; sin embargo, estos dispositivos a menudo tienen acceso sin restricciones a sus aplicaciones más importantes en sus centros de datos y servicios en la nube. Con un aumento de los ataques IoT basados en malware del 400 %[1], esto representa un importante vector de amenazas para su organización. Las organizaciones deben proteger los dispositivos IoT/OT en sucursales o fábricas para proteger sus operaciones comerciales.

Los ataques de malware basados en IoT y OT han aumentado un 400 % desde 2022, lo que representa un importante vector de amenaza.

© 2024 Zscaler, Inc. Todos los derechos reservados.

3 Garantice rutas directas a la nube para SaaS y tráfico de Internet

La arquitectura directa a la nube conecta rápidamente a cualquier usuario o dispositivo IoT/OT a cualquier aplicación, dondequiera que ese usuario o dispositivo IoT/OT esté. La implementación de rutas directas a la nube para SaaS y el tráfico de Internet es crucial para optimizar el rendimiento de la red y garantizar una conectividad perfecta. Las arquitecturas radiales que redirigen el tráfico a un centro de datos a través de costosos enlaces MPLS degradan el rendimiento de las aplicaciones y obstaculizan la productividad empresarial. Cuando las aplicaciones residían en el centro de datos, tenía sentido redirigir el tráfico de aplicaciones a un centro regional. Sin embargo, con las aplicaciones migrando a la nube, el envío del tráfico de usuarios o dispositivos IoT/OT directamente a su destino tiene más sentido.
Una arquitectura directa a la nube permite que las aplicaciones SaaS y el tráfico de Internet tomen las rutas más eficientes y directas hacia sus destinos. Esto tiene numerosos beneficios, como el ahorro de costes, una experiencia de usuario mejorada y la simplificación de la red.

Hoy en día, los líderes empresariales quieren una experiencia similar a la de una cafetería para sus usuarios y equipos de TI que haga que la conexión a aplicaciones empresariales sea lo más sencilla posible y, al mismo tiempo, ofrezca un rendimiento superior de las aplicaciones.

4 Garantice experiencias de usuario uniformes para empleados remotos y en la oficina

Muchos empleados trabajan de forma remota o dividen su tiempo entre trabajar desde casa y en la oficina. Este cambio en la dinámica laboral ha puesto de manifiesto un desafío importante. Es decir, los usuarios frecuentemente expresan insatisfacción con la calidad de la conectividad en la oficina en comparación con su entorno de trabajo en casa. Esta situación introduce un nuevo conjunto de preocupaciones que los equipos de TI deben abordar. Las tecnologías VPN que devuelven el tráfico a un centro de datos dan como resultado una experiencia de usuario deficiente e inconsistente, lo que impacta negativamente en el negocio y disminuye la productividad.

Hoy en día, los líderes empresariales quieren una experiencia similar a la de una cafetería para sus usuarios y equipos de TI que haga que la conexión a aplicaciones empresariales sea lo más sencilla posible y al mismo tiempo ofrezca un rendimiento superior de las aplicaciones. Quieren una experiencia en la que los usuarios empresariales puedan acceder a las aplicaciones que necesitan con una consistencia uniforme de experiencia entre el hogar y la oficina con la misma facilidad de uso, lo cual es imposible cuando se conectan a redes a través de VPN. Para seguir siendo relevantes en el mundo competitivo de hoy, las organizaciones deben garantizar experiencias de usuario uniformes para los empleados remotos y en la oficina, a fin de impulsar la productividad de los empleados y su creatividad.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Aplicación de los principios de confianza cero a SASE

Secure Access Service Edge (SASE) integra servicios de redes y seguridad en una solución unificada entregada en la nube, agilizando las operaciones, reduciendo la complejidad y permitiendo a las organizaciones aplicar políticas consistentes en sus redes. SASE combina redes de confianza cero con servicios de seguridad esenciales proporcionados en la nube como SWG, CASB, FWaaS y ZTNA. Es fundamental reconocer que las soluciones SASE basadas en SD-WAN tradicional ofrecen una protección inadecuada, lo que aumenta la superficie de ataque empresarial y expone las aplicaciones críticas a diversas amenazas de Internet.

Además, la capacidad de segmentación en la SD-WAN tradicional es fragmentada y tosca, lo que permite que las amenazas se propaguen fácilmente a otros sistemas; esto supone un riesgo de caída de redes o sitios enteros.

El Enterprise Strategy Group (ESG) de TechTarget encuestó a 390 profesionales de TI y ciberseguridad en varias organizaciones de América del Norte (EE. UU. y Canadá) para comprender el estado de SASE. Según este estudio, los tres casos de uso principales que impulsan a las organizaciones hacia SASE son:

1. Alinear las políticas de red y seguridad
2. Reducir o eliminar la superficie de ataque de Internet
3. Mejorar la seguridad de los usuarios remotos

Los tres casos de uso de SASE resaltan la importancia de proporcionar conectividad segura para usuarios, dispositivos y aplicaciones al establecer un marco SASE resistente. Las organizaciones que se embarcan en la implementación de SASE deben priorizar soluciones que cumplan con los principios de confianza cero. Conectan varios sitios a través de VPN de sitio a sitio o superposiciones enrutadas, estableciendo una confianza implícita que otorga acceso sin restricciones a recursos comerciales críticos, incluso para entidades comprometidas. Por otro lado, las SD-WAN basadas en principios de confianza cero reducen eficazmente la superficie de ataque y protegen frente al movimiento lateral de amenazas, al tiempo que facilitan una comunicación segura entre el usuario y la aplicación, el dispositivo a la aplicación y la aplicación a la aplicación.



Figura 5: Conclusiones de la encuesta sobre ESG acerca de los casos de uso de SASE iniciales actuales o previstos.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Conclusión

Las arquitecturas de redes de sucursales tradicionales se basan en la confianza implícita, lo que expande la superficie de ataque hasta la ubicación de sucursal más lejana y permite que las ciberamenazas se muevan lateralmente por toda la organización. Al adoptar un enfoque de confianza cero en la sucursal, las empresas pueden fortalecer sus redes contra amenazas y optimizar la conectividad de usuarios, dispositivos IoT/OT y aplicaciones en diversas ubicaciones. El diseño de una red de sucursales con principios de confianza cero mejora la postura de seguridad empresarial al eliminar la superficie de ataque y prevenir el movimiento lateral de amenazas, al tiempo que se superan las complejidades del enrutamiento. Es importante que las organizaciones consideren cuidadosamente los cuatro requisitos descritos aquí al implementar principios de confianza cero en la sucursal para navegar de manera efectiva las demandas complejas y en constante cambio de seguridad y conectividad de red.

Referencias

1. zscaler.es/press/zscaler-threatlabz-finds-400-increase-iot-and-ot-malware-attacks-year-over-year-underscoring
2. info.zscaler.com/2023-vpn-risk-report-es
3. zscaler.es/resources/industry-reports/esg-sse-leads-the-way-to-sase.pdf

© 2024 Zscaler, Inc. Todos los derechos reservados.

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 usuarios, dispositivos y aplicaciones 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 la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

© 2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience y ZDX™ y otras marcas comerciales mencionadas en **zscaler.es/legal/trademarks** son (i) marcas comerciales o marcas de servicio registradas o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/o en otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.

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