Libro electrónico

4 requisitos para una sucursal de zero trust



© 2024 Zscaler, Inc. Todos los derechos reservados.

Al implementar un enfoque de zero trust en la sucursal, las empresas no solo 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 enfrentan 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 tradicionales radiales y basadas en cortafuegos eran eficaces a la hora de satisfacer esas necesidades. Sin embargo, a medida que el entorno de trabajo moderno ha evolucionado, estos enfoques tradicionales han empezado a tener dificultades para brindar una protección adecuada contra las amenazas y una experiencia de usuario óptima.

Actualmente, 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 y más. Además, la proliferación del internet de las cosas (IoT) complica aún más el panorama de la seguridad empresarial, ya que los dispositivos IoT/OT plantean un riesgo de seguridad adicional.

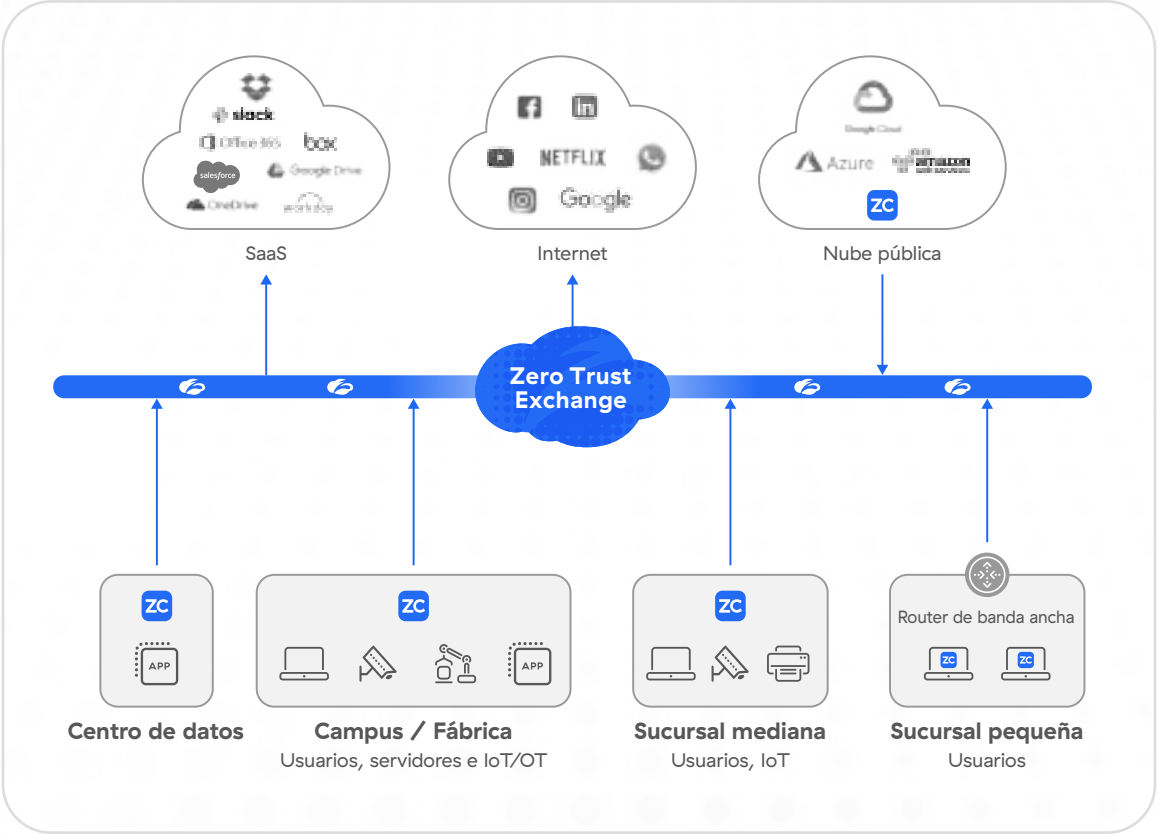

Figura 1: Zero Trust Branch ofrece un enfoque de zero trust para la conectividad de red

© 2024 Zscaler, Inc. Todos los derechos reservados.

Este panorama cambiante está impulsando a las organizaciones hacia un enfoque de zero trust en materia de seguridad. Los principios de zero trust (nunca confiar, siempre verificar y exigir el acceso privilegio mínimo) han permitido a muchas empresas frustrar ataques cibernéticos sofisticados. Con zero trust, 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 zero trust a la conectividad de la red, las organizaciones pueden protegerse mejor contra las amenazas, especialmente las que se originan en las ubicaciones. El despliegue del enfoque de zero trust en la sucursal garantiza una conectividad segura y operaciones simplificadas, superando las complejidades de enrutamiento o una experiencia de usuario en declive, al tiempo que elimina la superficie de ataque y previene el movimiento lateral de amenazas.

La arquitectura de sucursal de zero trust garantiza una seguridad mejorada para todas las ubicaciones, incluidas sucursales, fábricas, estaciones de cómputo y centros de datos. A continuación presentamos cuatro requisitos clave para garantizar una sucursal de zero trust:

Garantice los principios de zero trust para su red 1

Asegure 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 los empleados en la oficina y a distancia 4

© 2024 Zscaler, Inc. Todos los derechos reservados.

La SD-WAN tradicional no es de zero trust

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 las amenazas, permitiendo que los dispositivos comprometidos en ubicaciones remotas se comuniquen fácilmente con las aplicaciones críticas para la empresa en el centro de datos o la nube pública. Las empresas experimentan un mayor riesgo de amenazas laterales y ataques basados en Internet al utilizar SD-WAN heredadas. Un conjunto de parches de dispositivos de seguridad, herramientas y políticas no estándar conducen a un mayor riesgo de seguridad debido a lagunas conocidas y desconocidas en la cobertura de seguridad. Por lo tanto, a la hora de diseñar la conectividad segura de las sucursales, resulta imprescindible centrarse en la implementación de zero trust para reducir la superficie de ataque y evitar el movimiento lateral de las amenazas.

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

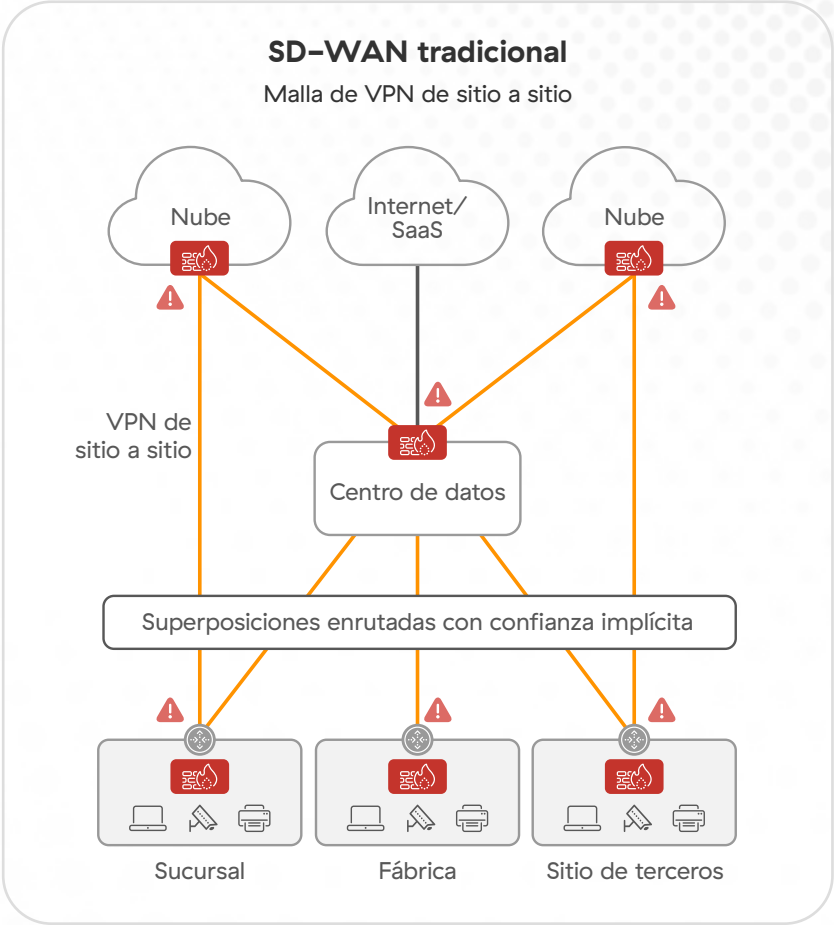

Figura 2: Las SD-WAN tradicionales amplían la superficie de ataque y no protegen contra el movimiento lateral de amenazas.

© 2024 Zscaler, Inc. Todos los derechos reservados.



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

En los últimos 12 meses, ¿ha sufrido su organización algún ataque que aprovecha las vulnerabilidades de seguridad de sus servidores VPN?

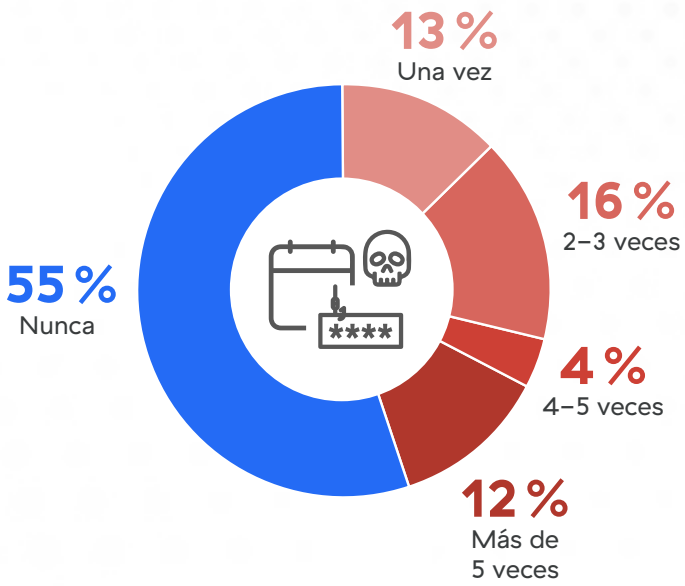

Figura 3: Las organizaciones están experimentando un aumento de los ciberataques debido a las vulnerabilidades en los servidores VPN.

© 2024 Zscaler, Inc. Todos los derechos reservados.

No se puede construir una zero trust 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 convencional de sitio a sitio se vuelve menos viable, ya que el tráfico sigue siendo redirigido al centro de datos, lo que se traduce en una experiencia de usuario degradada y en 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 de las empresas quieren pasar de una red radial a una arquitectura directa a la nube que envíe el tráfico de las aplicaciones a un proveedor de seguridad en la nube, mejorando así el rendimiento de las aplicaciones.

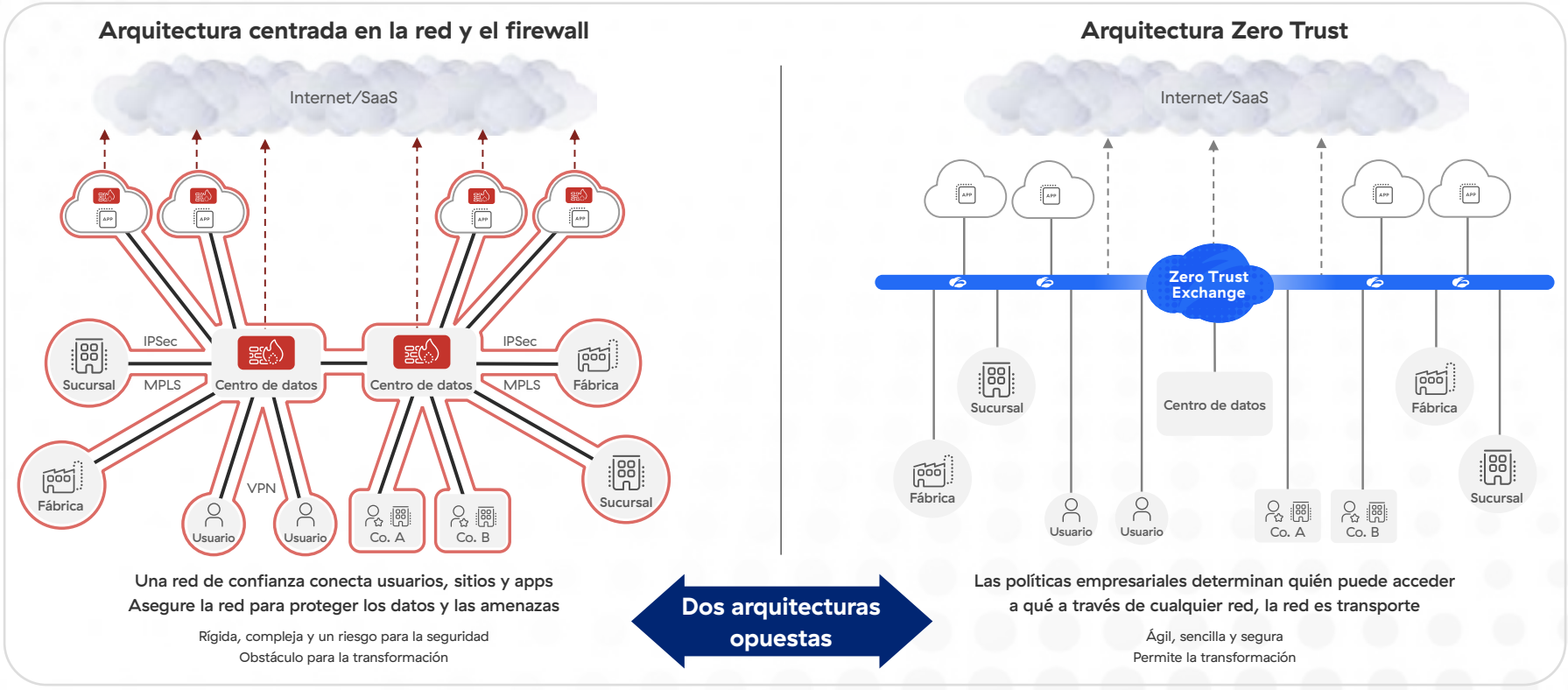

Figura 4: Las redes radiales cuentan con una arquitectura compleja y rígida. En cambio, una arquitectura de confianza cero es ágil, sencilla, segura y permite la transformación.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Cuatro requisitos clave para garantizar una sucursal de zero trust

1 Garantice los principios de zero trust 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 que están fuera de su control directo y permiten los flujos de tráfico de forma implícita, lo que posibilita el movimiento lateral de las amenazas. A diferencia de la segmentación de red tradicional, que divide la red en zonas y es compleja de gestionar, la segmentación de usuario a aplicación y de dispositivo a aplicación proporciona un acceso granular y contextual solo cuando está autorizado. Una base de red construida sobre principios de confianza cero elimina los riesgos inherentes a las redes planas tradicionales y le ayuda a evitar la complejidad de superponer cortafuegos para los controles de seguridad. experiencia 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 de las empresas quieren pasar de una red radial a una arquitectura directa a la nube que envíe el tráfico de las aplicaciones a un proveedor de seguridad en la nube, mejorando así el rendimiento de las aplicaciones.

2 Asegure los dispositivos IoT/OT en sus sucursales o oficinas

Los dispositivos IoT/OT se multiplican en casi todas las organizaciones con el auge de los dispositivos "inteligentes", como impresoras, televisores, cámaras, lectores de tarjetas y sensores. Estos dispositivos ejecutan innumerables sistemas operativos con distintos riesgos de seguridad, por lo que la gestión de parches sigue siendo un reto. Muchos responsables de TI no pueden ver estos dispositivos, y mucho menos disponer de un inventario detallado; sin embargo, a menudo estos dispositivos tienen acceso sin restricciones a las aplicaciones más importantes en sus centros de datos y servicios en la nube. Teniendo en cuenta que los ataques basados en malware IoT han aumentado un 400 %, esto representa un importante vector de amenazas para su organización. Las organizaciones deben asegurar los dispositivos IoT/OT en sucursales o fábricas para proteger sus operaciones empresariales.

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

© 2024 Zscaler, Inc. Todos los derechos reservados.

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

La arquitectura directa a la nube conecta rápidamente a cualquier usuario o dispositivo IoT/OT con cualquier aplicación, esté donde esté ese usuario o dispositivo IoT/OT en el mundo. La implementación de rutas directas a la nube para el SaaS y el tráfico de Internet es crucial para optimizar el rendimiento de la red y garantizar una conectividad sin problemas. Las arquitecturas radiales que devuelven el tráfico a un centro de datos a través de costosos enlaces MPLS degradan el rendimiento de las aplicaciones y dificultan la productividad empresarial. Cuando las aplicaciones se encontraban en el centro de datos, tenía sentido redirigir el tráfico de las aplicaciones a un centro regional. Sin embargo, con el traslado de las aplicaciones a la nube, lo más sensato es enviar el tráfico de los usuarios o de los dispositivos IoT/OT directamente a su destino. 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 muchos beneficios, incluidos ahorros de costos, experiencia de usuario mejorada y simplificación de la red.

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

4 Garantice experiencias de usuario consistentes 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 de trabajo ha puesto de manifiesto un reto 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 genera una nueva serie de preocupaciones que los equipos informáticos 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 a la actividad y disminuye la productividad.

En la actualidad, los líderes empresariales quieren una experiencia tipo cafetería para sus usuarios y equipos de TI, que haga que la conexión a las aplicaciones empresariales sea lo más sencilla posible y que, al mismo tiempo, ofrezca un rendimiento superior de las aplicaciones. Quieren una experiencia en la que los usuarios de empresa puedan acceder a las aplicaciones que necesitan con una experiencia uniforme entre el hogar y la oficina con la misma facilidad de uso, lo que es imposible cuando se conecta a redes a través de VPN. Para seguir siendo relevantes en el competitivo mundo actual, las organizaciones deben garantizar experiencias de usuario consistentes para los empleados en la oficina y a distancia, con el fin de impulsar la productividad de los empleados y fomentar la creatividad.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Aplicar los principios de zero trust a SASE

Secure Access Service Edge (SASE) integra los servicios de red y de seguridad en una solución unificada y en la nube, lo que agiliza las operaciones, reduce la complejidad y permite a las organizaciones aplicar políticas consistentes en todas sus redes. SASE combina redes de zero trust 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 de la SD-WAN tradicional es fragmentaria y rudimentaria, lo que permite que las amenazas se propaguen fácilmente a otros sistemas, con el consiguiente riesgo de colapsar sitios o redes enteras.

El Grupo de Estrategia Empresarial (ESG) de TechTarget encuestó a 390 profesionales de TI y ciberseguridad de varias organizaciones de Norteamérica (EE.UU. y Canadá) para conocer el estado del SASE. Según este estudio, los tres principales casos de uso que conducen 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 zero trust. Las SD-WAN tradicionales conectan varios sitios a través de VPN de sitio a sitio o superposiciones enrutadas, estableciendo una confianza implícita que garantiza un acceso sin restricciones a los recursos empresariales críticos, incluso para las entidades comprometidas. Por otro lado, las SD-WAN diseñadas según los principios de zero trust reducen eficazmente la superficie de ataque y protegen contra el movimiento lateral de amenazas, al tiempo que facilitan la comunicación segura entre usuarios, dispositivos y aplicaciones.



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

© 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 zero trust en la sucursal, las empresas pueden fortificar sus redes contra las amenazas y agilizar la conectividad para los usuarios, los dispositivos IoT/OT y las aplicaciones en diversas ubicaciones. El diseño de una red de sucursales con principios de zero trust 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 detenidamente los cuatro requisitos aquí expuestos a la hora de implementar los principios de zero trust en la sucursal para navegar con eficacia por las complejas y siempre cambiantes demandas de seguridad y conectividad de red.

Referencias:

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

© 2024 Zscaler, Inc. Todos los derechos reservados.



Experience your world, secured.™

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ataques cibernéticos y pérdida de datos al conectar de forma segura usuarios, dispositivos y aplicaciones 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. Obtenga más información en **zscaler.com.mx** 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 registradas listadas en **zscaler.com.mx/legal/trademarks** son (i) marcas registradas o marcas de servicio o (ii) marcas registradas o marcas de servicio de Zscaler, Inc. en Estados Unidos y otros países. Cualquier otra marca comercial pertenece a sus respectivos propietarios.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San José, CA 95134 zscaler.com.mx