Libro electrónico

Cuatro razones por las que los cortafuegos y las VPN exponen a las organizaciones a infracciones

Las soluciones de ayer son los problemas de hoy

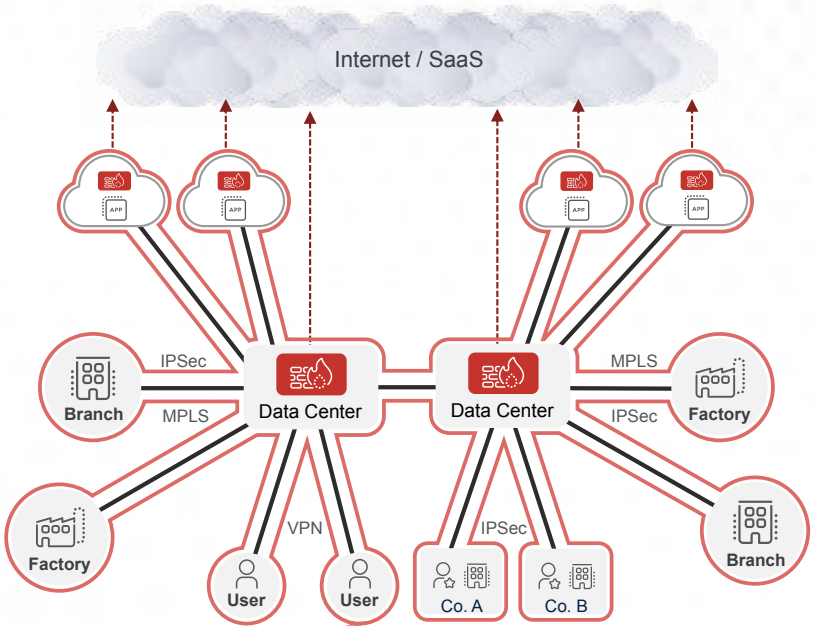
Los cortafuegos y las VPN exponen a las organizaciones a infracciones. Puede parecer contradictorio debido al hecho de que ambas han sido herramientas de seguridad de referencia durante décadas, pero ahí radica el problema. Fueron diseñados para una época en la que el trabajo se hacía de manera muy diferente a como se hace hoy. En el pasado, los usuarios y las aplicaciones residían en las instalaciones (ya sea en la oficina principal o en una sucursal) y los esfuerzos de seguridad se centraban en establecer un perímetro alrededor de la red que los conectaba. En otras palabras, una red radial estaba defendida por un modelo de seguridad de castillo y foso.

Este enfoque recibe varios nombres, incluida arquitectura basada en perímetro, arquitectura centrada en red y arquitectura tradicional o heredada. Independientemente de cómo se llame, implica inherentemente el uso de herramientas como cortafuegos y VPN, que se implementan en un intento de proteger la red, específicamente manteniendo los elementos negativos fuera y los positivos dentro.

En los últimos años las organizaciones han evolucionado rápidamente, en gran parte debido a la pandemia de COVID-19. Para seguir siendo productivos en 2020, tuvieron que acelerar sus cronogramas de transformación digital, haciendo de las aplicaciones en la nube y el trabajo remoto la nueva norma. Sin embargo, esta evolución era incompatible con los cortafuegos, las VPN y las arquitecturas basadas en perímetros que utilizaban las herramientas. Esto se debe a que no es factible construir un perímetro de seguridad alrededor de una red que se extiende infinitamente a cada vez más usuarios, dispositivos, aplicaciones y nubes fuera de las instalaciones.

Para las organizaciones que siguen utilizando arquitecturas heredadas en medio de la transformación digital, esto crea numerosos desafíos en torno a la complejidad, la rigidez, el coste y la productividad. Además, y lo más importante, aumenta el riesgo cibernético y expone a las organizaciones a infracciones de cuatro formas clave que se explican a lo largo de las páginas siguientes.

Arquitectura centrada en cortafuegos y VPN



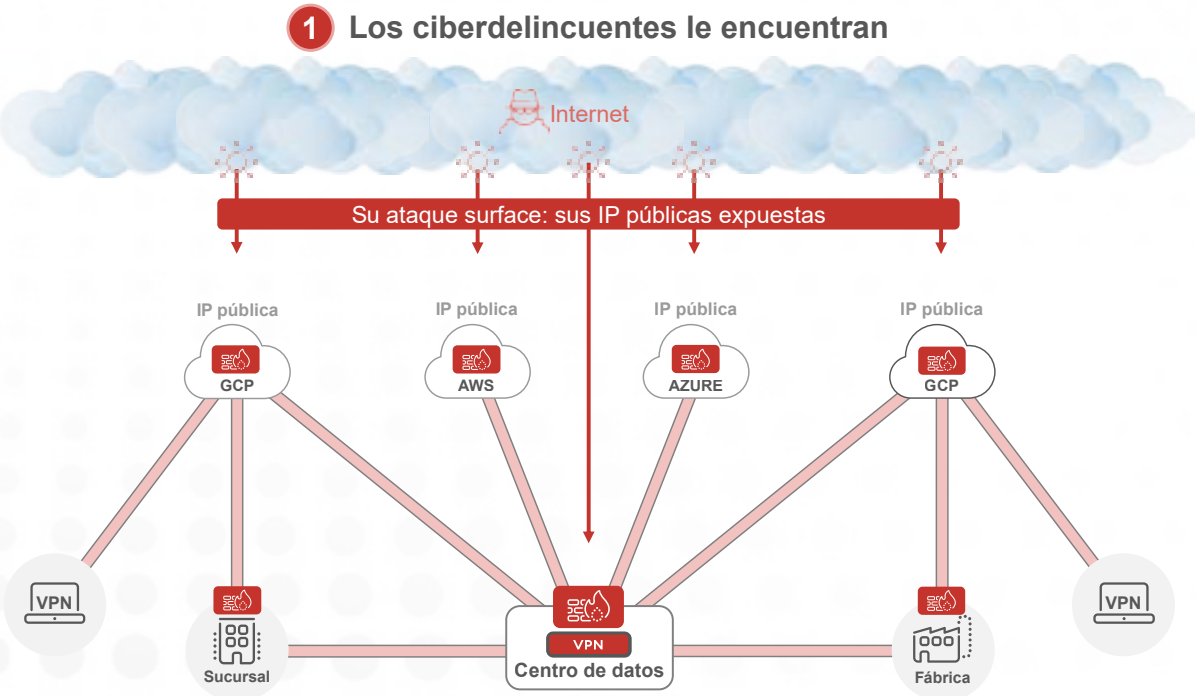
Una red confiable conecta usuarios, sitios y aplicaciones. La protección de datos y amenazas se centra en proteger la red.

#1 Los cortafuegos y las VPN amplían la superficie de ataque

Los ciberdelincuentes buscan constantemente objetivos a los que atacar para penetrar las defensas de las organizaciones y ejecutar sus diseños mal intencionados. Desafortunadamente, con la forma en que se hace el trabajo hoy en día, las arquitecturas basadas en el perímetro amplían la superficie de ataque y, sin darse cuenta, ayudan a los actores maliciosos en sus esfuerzos por identificar objetivos atractivos.

Como se ha mencionado anteriormente, continuar utilizando una red radial en el mundo moderno implica extender continuamente esa red a cada vez más usuarios, dispositivos, recursos basados en la nube, sucursales remotos. En la práctica, esto significa que una red plana en expansión es un creciente tesoro de recursos interconectados, y que existen muchas vías (aplicaciones en la nube, usuarios remotos, etc.) que los ciberdelincuentes pueden explotar como puntos de entrada a dicha red. En pocas palabras, una red en constante expansión significa una superficie de ataque en constante expansión.

Cómo la arquitectura centrada en cortafuegos y VPN aumenta el riesgo



Desafortunadamente, los problemas de superficie de ataque de las arquitecturas basadas en el perímetro van mucho más allá de lo anterior, y eso se debe a los cortafuegos y VPN. Estas herramientas son los medios mediante los cuales se supone que los modelos de seguridad de castillo y foso defienden las redes radiales, pero su uso tiene consecuencias no deseadas.

Los cortafuegos y las VPN tienen direcciones IP públicas que se pueden encontrar en la Internet pública. Esto es así para que los usuarios legítimos y autorizados puedan acceder a la red a través de la web, interactuar con los recursos conectados allí y hacer su trabajo. Sin embargo, también los ciberdelincuentes que buscan objetivos que atacar pueden encontrar estas direcciones IP públicas para obtener acceso a la red.

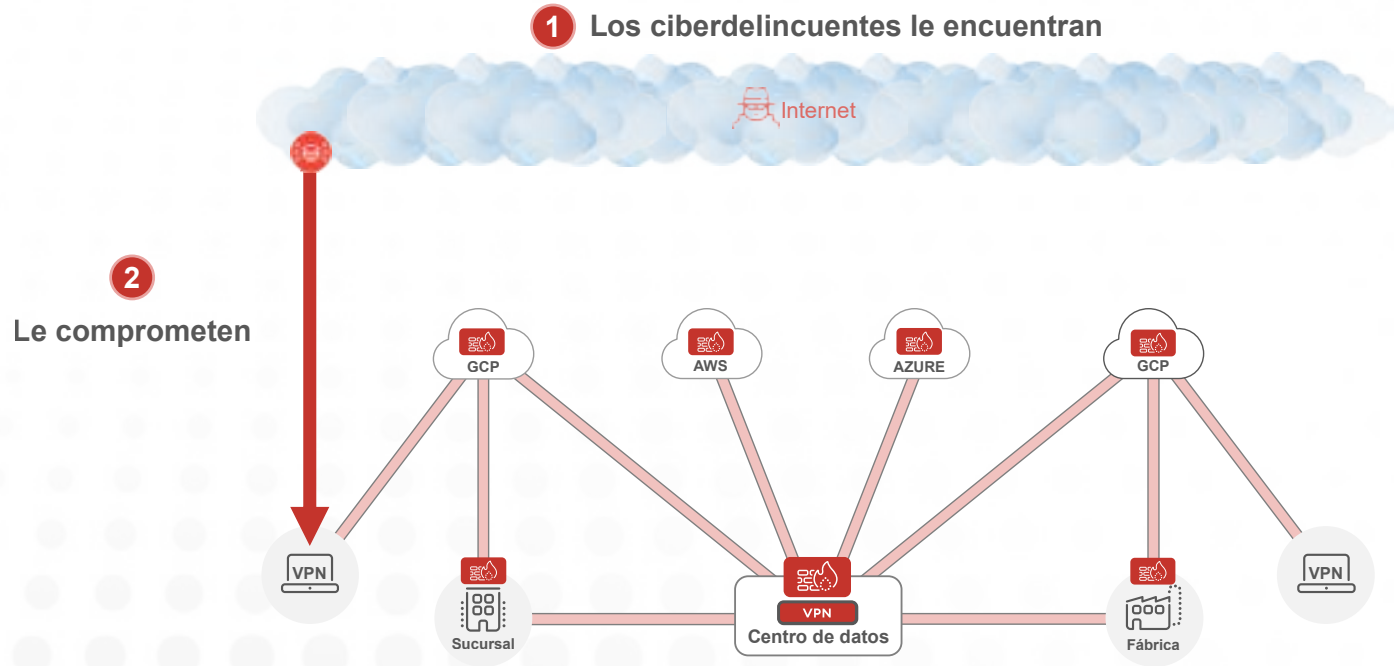
En otras palabras, los cortafuegos y las VPN brindan a los ciberdelincuentes más vectores de ataque al expandir la superficie de ataque de la organización. Irónicamente, esto significa que la estrategia estándar de implementar cortafuegos y VPN adicionales para escalar y mejorar la seguridad en realidad exacerba aún más el problema de la superficie de ataque.

#2 Los cortafuegos y las VPN no logran evitar el riesgo

Una vez que los ciberdelincuentes han identificado con éxito un objetivo atractivo, desatan sus ciberataques en un intento de penetrar las defensas de la organización. Desafortunadamente, una vez más, las herramientas tradicionales como cortafuegos y VPN no son adecuadas para proteger esta etapa de la cadena de ataques.

Prevenir el compromiso requiere el uso de políticas de seguridad en línea que detengan las amenazas en tiempo real, antes de que puedan acceder al entorno de una organización y comenzar a causar daños. Esto, a su vez, significa que las organizaciones deben poder inspeccionar todo el tráfico en sus operaciones para poder identificar cualquier amenaza potencial. Para lograrlo, la capacidad de inspeccionar el tráfico cifrado es increíblemente importante, y eso se debe a que la gran mayoría del tráfico web actual está cifrado: más del 95 %. Pero aquí es donde se hace evidente otra debilidad clave de la arquitectura basada en cortafuegos y VPN.

Cómo la arquitectura centrada en cortafuegos y VPN aumenta el riesgo



La inspección del tráfico cifrado es un proceso que consume muchos recursos, lo que significa que se necesita una gran cantidad de potencia informática para descifrar, examinar y volver a cifrar el tráfico. Desafortunadamente, los dispositivos de seguridad como los cortafuegos tienen dificultades para actuar del modo necesario para lograr este objetivo, tanto si se implementan como dispositivos de hardware en las instalaciones o¡como si lo hacen como dispositivos virtuales en una instancia de la nube.

Esto se debe a que los dispositivos tienen capacidades fijas para brindar un determinado nivel de servicio. No pueden ampliarse indefinidamente para satisfacer los requisitos cada vez mayores de una organización en materia de inspección del tráfico en tiempo real, especialmente cuando se trata de tráfico cifrado.
Como resultado, las organizaciones que dependen de herramientas y arquitecturas tradicionales se quedan con una inspección incompleta del tráfico cifrado, en el mejor de los casos, y, en el peor, sin inspección del tráfico cifrado.

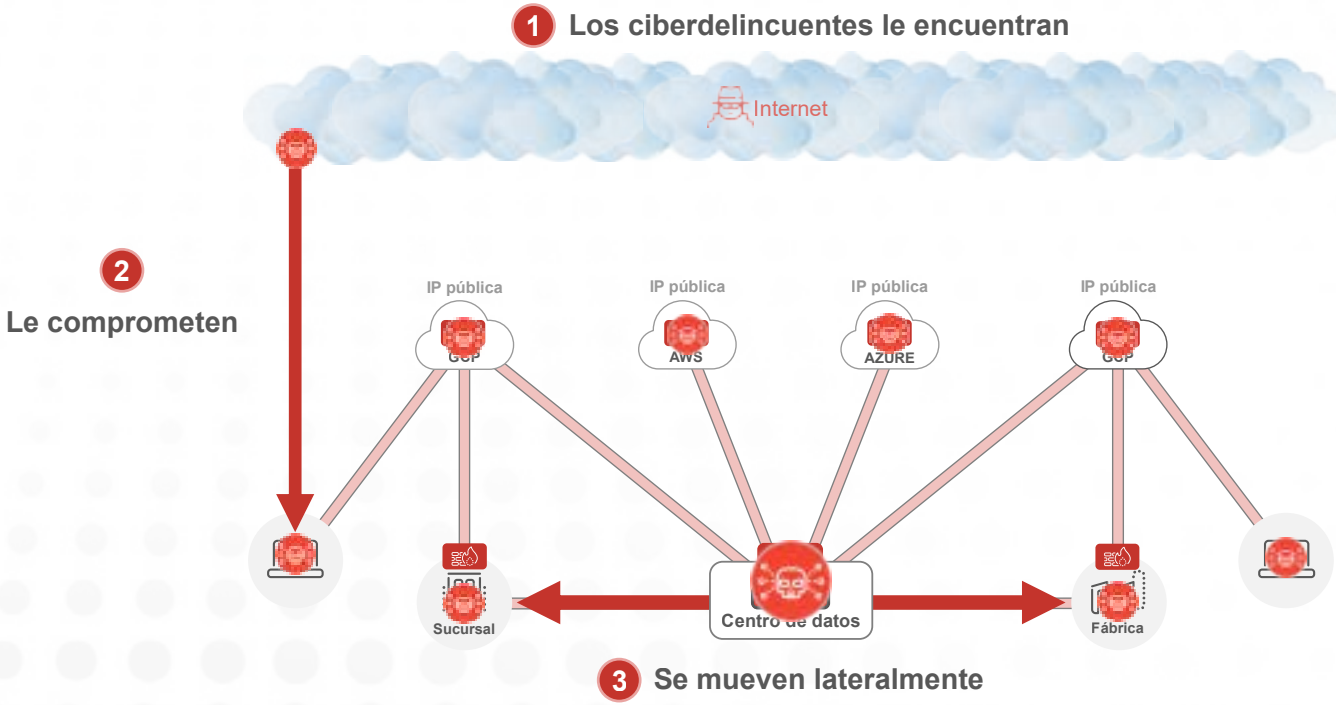
No inspeccionar el tráfico cifrado a escala implica que las amenazas pueden atravesar las defensas sin ser detectadas, lo que permite a los atacantes llevar a cabo sus planes. Lamentablemente, parece que los ciberdelincuentes se han dado cuenta de este hecho y han comenzado a utilizar el tráfico cifrado como medio preferido para ejecutar sus ataques. Hoy en día, aproximadamente el **86 %** de los ciberataques se producen a través de tráfico cifrado. Por lo tanto, si una organización no inspecciona su tráfico cifrado, no podrá detener la gran mayoría de las amenazas que intentan vulnerar sus defensas. En pocas palabras, las arquitecturas de cortafuegos y VPN no logran evitar el compromiso.

#3 Los cortafuegos y las VPN permiten el movimiento lateral de amenazas

Una vez que se ha producido el compromiso y una ciberamenaza ha superado las defensas de una organización, las debilidades de los cortafuegos y las VPN quedan a la vista. El movimiento lateral de amenazas, también conocido como propagación lateral, se refiere a la forma en que las amenazas en la red pueden acceder a los diversos recursos de la organización, ya sean aplicaciones locales, cargas de trabajo en nubes privadas o instancias de aplicaciones SaaS. Rara vez es una sola aplicación la que se ve comprometida cuando una amenaza traspasa el perímetro de una organización. Para comprender cómo se puede producir el movimiento lateral de amenazas, sólo es necesario considerar la analogía contenida en la frase “seguridad de castillo y foso”.

Se utiliza un foso para defender un castillo; específicamente, impidiendo que los atacantes accedan al castillo. Esto se hace para proteger todo lo que hay de importancia y a las personas dentro de la fortaleza. Sin embargo, si los atacantes lograran pasar el foso, el principal mecanismo de defensa de un castillo quedaría inútil.

Cómo la arquitectura centrada en cortafuegos y VPN aumenta el riesgo



En ese caso, quedaría poca protección para evitar que los enemigos saquearan todo el castillo.

La debilidad mencionada anteriormente en el caso de castillos y fosos también está presente cuando se utilizan cortafuegos y VPN. Esto se debe a la naturaleza altamente interconectada de las redes radiales en las que algunas organizaciones todavía optan por confiar, así como a la forma en que los modelos de seguridad de castillo y foso centran los esfuerzos de protección contra amenazas en defender el acceso a la red como un entero.

Simplemente imagine que los cortafuegos son el “foso”, las VPN el “puente levadizo” y la red misma el “castillo”. Una vez que una ciberamenaza prevalece sobre el “foso” y entra en el “castillo”, el ciberdelincuente puede pasar fácilmente de un recurso conectado a otro, accediendo a las distintas “salas” del “castillo”.

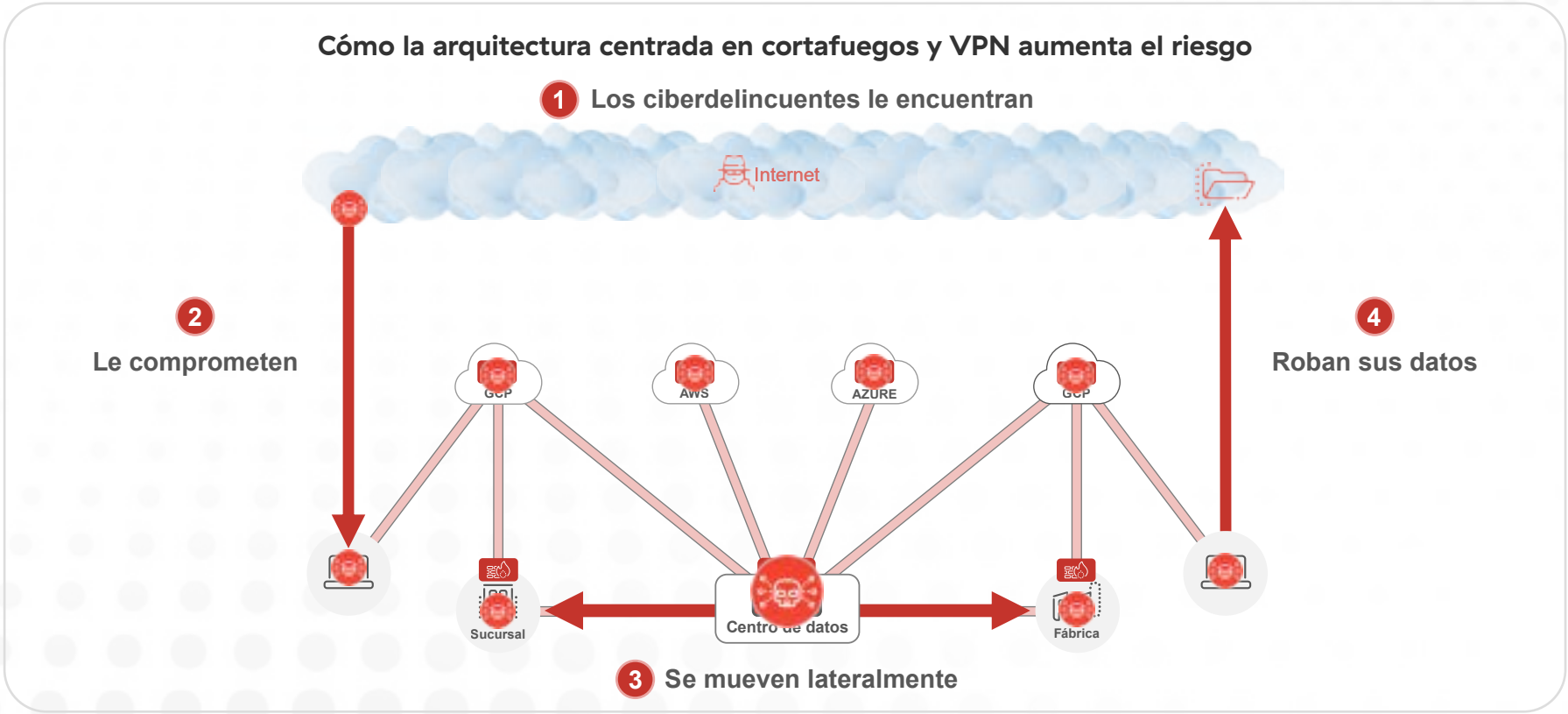
En pocas palabras, los cortafuegos y las VPN permiten el movimiento lateral de amenazas y permiten a los ciberdelincuentes expandir el alcance de sus infracciones a través de la red, causando daños, interrupciones y costes masivos. Hacer concesiones en cualquier lugar significa de hecho hacer concesiones en todas partes. Si bien la segmentación de la red a menudo se presenta como la solución a este problema, esta táctica inevitablemente equivale a adquirir más y más cortafuegos, lo que no logra resolver los problemas arquitectónicos subyacentes inherentes a las herramientas basadas en perímetros del pasado.

#4 Los cortafuegos y las VPN permiten la pérdida de datos

En la gran mayoría de los ciberataques, los ciberdelincuentes no buscan atacar las organizaciones simplemente por la emoción de hacerlo. Más bien, tienen un objetivo específico en mente, y ese objetivo es robar información confidencial. Esto se debe a que los datos robados pueden venderse en la web oscura para obtener ganancias significativas o usarse para presionar a una organización a pagar un rescate en un esquema de ransomware de doble extorsión. De cualquier manera, las repercusiones pueden ser catastróficas para cualquier organización.

Entonces, una vez que los ciberdelincuentes han encontrado una superficie de ataque, han comprometido las defensas y han comenzado el movimiento lateral (todos ellos facilitados por cortafuegos y VPN), buscarán la mayor cantidad de datos posible en toda la red, priorizando información particularmente sensible o regulada. Naturalmente, a esto le sigue la exfiltración de datos.

Depender de herramientas tradicionales para detener este eslabón final de la cadena de ataque produce una vez más resultados arriesgados y permite la pérdida de datos.



Como se mencionó anteriormente, hoy en día más del 95 % del tráfico web está cifrado, la inspección del tráfico cifrado requiere una gran potencia informática y los dispositivos estáticos no se pueden ajustar para procesar los enormes volúmenes de tráfico cifrado generados por organizaciones en crecimiento. Este desafío (tanto para el hardware como para los dispositivos virtuales) es relevante no sólo en lo referente a infracciones, sino también para la pérdida de datos. Los ciberdelincuentes son conscientes de que es más probable que las organizaciones tengan puntos ciegos donde el tráfico está cifrado y están utilizando este tráfico como vía preferida para la exfiltración de datos.

Pero los desafíos de escalabilidad no son el único motivo por el que herramientas como los cortafuegos no pueden detener la filtración de datos. Las tecnologías del pasado fueron diseñadas para el mundo de ayer, antes de las aplicaciones en la nube y los trabajadores remotos. Como resultado, no pueden proteger las rutas modernas de filtración de datos; por ejemplo, la funcionalidad para compartir integrada en aplicaciones SaaS como Google Drive, Box, Microsoft OneDrive y otras. De manera similar, los recursos de la nube mal configurados, como los depósitos de AWS S3 configurados por error como “públicos”, exponen los datos, pero no pueden remediarse con cortafuegos, VPN o incluso herramientas convencionales de prevención de pérdida de datos (DLP).

Los atacantes externos están ansiosos por utilizar estos y otros medios modernos para robar información confidencial; sin embargo, es fundamental señalar que no son la única amenaza a los datos. Las organizaciones deben lidiar con la realidad de que personas internas maliciosas y descuidadas también pueden filtrar información confidencial de las formas anteriormente mencionadas. Independientemente de quién sea el culpable, la seguridad debe evolucionar si se quiere mantener los datos seguros.

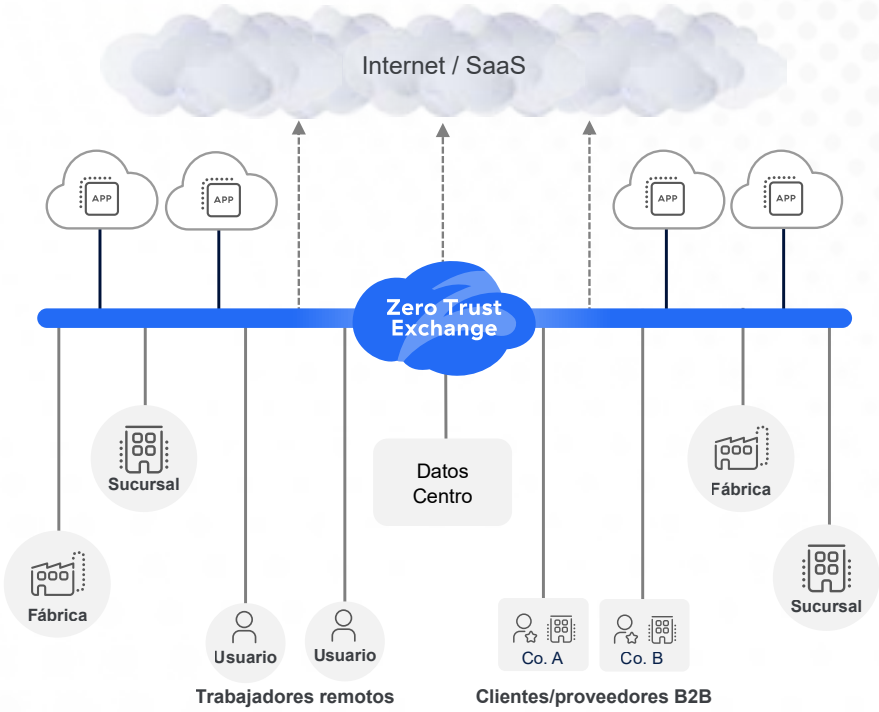
Cómo la arquitectura de Zero Trust resuelve estos problemas

Zero Trust no es simplemente otra herramienta más para agregar al status quo existente centrado en la red. No es algo que simplemente disminuya los problemas de las arquitecturas basadas en perímetros sin resolver realmente sus causas subyacentes. Más bien, la confianza cero es una arquitectura distinta que se basa en el principio de acceso con privilegios mínimos; es inherentemente diferente de una arquitectura estándar basada en cortafuegos y VPN.

Cuando existe una arquitectura de Zero Trust, las organizaciones se benefician de una nube de seguridad global que actúa como una centralita inteligente, conectando de forma segura a usuarios, cargas de trabajo, dispositivos IoT/OT y socios B2B, sin extender la red a nadie ni a nada. Al mismo tiempo, la nube de confianza cero debería ofrecer conjuntos completos de soluciones (como ciberamenazas y protección de datos) que se entreguen como un servicio en el perímetro, lo más cerca posible del usuario final.

Con Zero Trust, la seguridad y la conectividad se desacoplan con éxito de la red y las arquitecturas basadas en el perímetro pasan a ser cosa del pasado.

Arquitectura de Zero Trust



Las políticas empresariales determinan quién puede acceder a qué a través de cualquier red; la red es simplemente el transporte.

Con esta arquitectura moderna, las organizaciones pueden poner fin a las cuatro formas en que los cortafuegos y las VPN las exponen a infracciones:

- **Minimice la superficie de ataque:** aproveche Zero Trust para detener la expansión interminable de la red, elimine cortafuegos, VPN y sus IP públicas, evite conexiones entrantes y oculte aplicaciones detrás de una nube de Zero Trust.
- **Detenga el riesgo:** inspeccione todo el tráfico, incluido el tráfico cifrado a escala, a través de una nube de confianza cero de alto rendimiento que identifica amenazas y aplica políticas de seguridad en tiempo real.
- **Evite el movimiento lateral de amenazas:** conecte usuarios, cargas de trabajo y dispositivos directamente a las aplicaciones en lugar de a la red en su conjunto, manteniendo el principio de acceso con privilegios mínimos.
- **Bloquee la pérdida de datos:** detenga la pérdida de datos en el tráfico cifrado y en todas las demás rutas de filtración de datos, incluidos los datos en reposo en la nube y los datos en uso en los dispositivos terminales de los empleados.

Además de reducir el riesgo de infracciones, una arquitectura de Zero Trust reduce la complejidad, aumenta la productividad del usuario, ahorra dinero y mejora el dinamismo organizacional, resolviendo una variedad de problemas que afectan a las arquitecturas basadas en cortafuegos y VPN.

Recapitulación

Para aquellos que necesitan una arquitectura de Zero Trust, Zscaler Zero Trust Exchange impulsado por IA es la plataforma elegida. Como la mayor nube de seguridad en línea y la más implementada del mundo, su escala y éxito hablan por sí solos:

Más de 150
Centros de datos globales

+ 360 000 millones
Transacciones aseguradas diariamente

500T+
Señales de telemetría diarias

70+
Net Promoter Score

40 %
De las Fortune 500 son clientes

Líder
En el Gartner MQ para SSE

Para obtener más información, regístrese en nuestro seminario web mensual, "Empiece aquí: Introducción a Zero Trust".” En el seminario web, analizamos la arquitectura de Zero Trust desde una perspectiva básica (y compartimos más información sobre Zscaler) para que cualquiera pueda comenzar un viaje de Zero Trust con confianza.

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**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.es