eBook

Cuatro razones por las que los firewalls y las VPN exponen a las organizaciones a violaciones

Las soluciones de ayer son los problemas de hoy

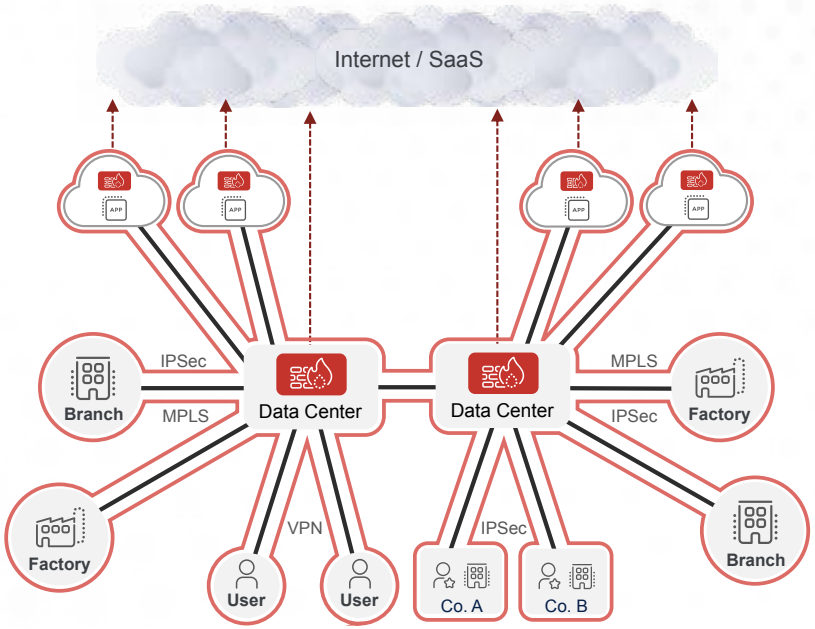
Los firewalls y las VPN están exponiendo a las organizaciones a las violaciones. Puede parecer contraintuitivo debido a que ambas han sido herramientas de seguridad imprescindibles durante décadas, pero ahí radica el problema. Se diseñaron para una época en la que el trabajo se realizaba de una manera muy diferente a la actual. En el pasado, los usuarios y las aplicaciones residían en las instalaciones (ya fuera 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 "hub-and-spoke" estaba defendida por un modelo de seguridad "castle-and-moat".

Este enfoque recibe múltiples nombres, como arquitectura basada en el perímetro, arquitectura centrada en la red y arquitectura tradicional o heredada. Independientemente de cómo se denomine, implica intrínsecamente el uso de herramientas como firewalls y VPN, que se implementan para intentar proteger la red; concretamente, manteniendo lo malo afuera y lo bueno adentro.

Las organizaciones evolucionaron rápidamente en los últimos años, en gran parte debido a la pandemia del COVID-19. Para seguir siendo productivos en 2020, tuvieron que acelerar sus plazos de transformación digital, convirtiendo las aplicaciones en la nube y el trabajo a distancia en la nueva norma. Sin embargo, esta evolución era incompatible con los firewalls, las VPN y las arquitecturas basadas en el perímetro que las herramientas daban por supuestas. Esto se debe a que es inviable construir un perímetro de seguridad alrededor de una red que se extiende sin cesar a cada vez más usuarios, dispositivos, aplicaciones y nubes fuera de las instalaciones.

Para las organizaciones que mantienen la arquitectura heredada en medio de la transformación digital, esto crea numerosos desafíos en torno a la complejidad, la rigidez, el costo y la productividad. Además, y lo que es más importante, aumenta el ciberriesgo y expone a las organizaciones a violaciones de cuatro maneras clave que se explican en las próximas páginas.

Arquitectura centrada en firewalls y VPN



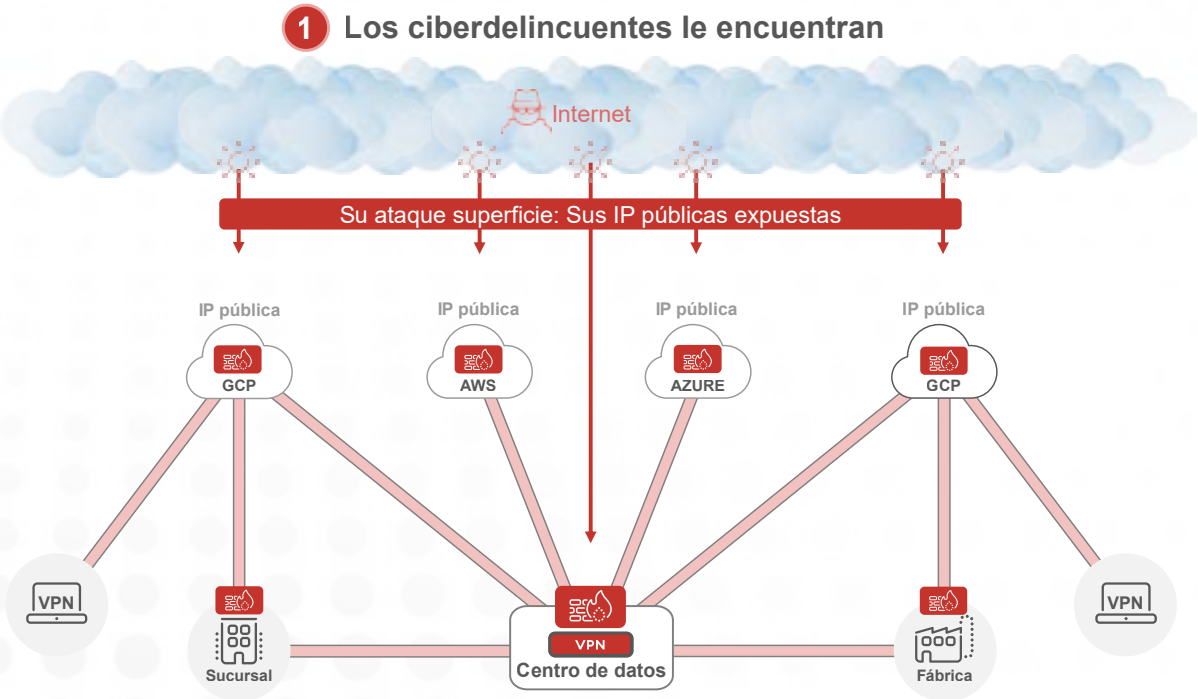
Una red confiable conecta usuarios, sitios y aplicaciones. Las amenazas y la protección de datos se centran en asegurar la red.

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

Los ciberdelincuentes buscan constantemente objetivos que puedan atacar para penetrar en las defensas de las organizaciones y ejecutar sus planes malintencionados. Lamentablemente, con el modo de trabajar actual, las arquitecturas basadas en el perímetro amplían la superficie de ataque y ayudan inadvertidamente a los malintencionados en sus esfuerzos por identificar objetivos atractivos.

Como se ha mencionado anteriormente, seguir utilizando una red hub-and-spoke en el mundo moderno implica ampliar continuamente esa red a cada vez más usuarios remotos, dispositivos, recursos basados en la nube, sucursales y mucho más. Esto significa efectivamente que una red plana en expansión es un tesoro de recursos interconectados en expansión, y que hay muchas vías (aplicaciones en la nube, usuarios remotos, etc.) que los ciberdelincuentes pueden explotar como puntos de entrada en dicha red. En pocas palabras, una red en constante expansión implica una superficie de ataque cada vez mayor.

Cómo la arquitectura centrada en firewalls y VPN aumenta el riesgo



Lamentablemente, los problemas de superficie de ataque de las arquitecturas basadas en perímetro van mucho más allá de lo anterior, y eso se debe a los firewalls y las VPN. Estas herramientas son los medios con los que se supone que los modelos de seguridad castle-and-moat defienden las redes hub-and-spoke, pero su uso tiene consecuencias imprevistas.

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

En otras palabras, los firewalls 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 firewalls y VPN adicionales para escalar y mejorar la seguridad en realidad exacerba aún más el problema de la superficie de ataque.

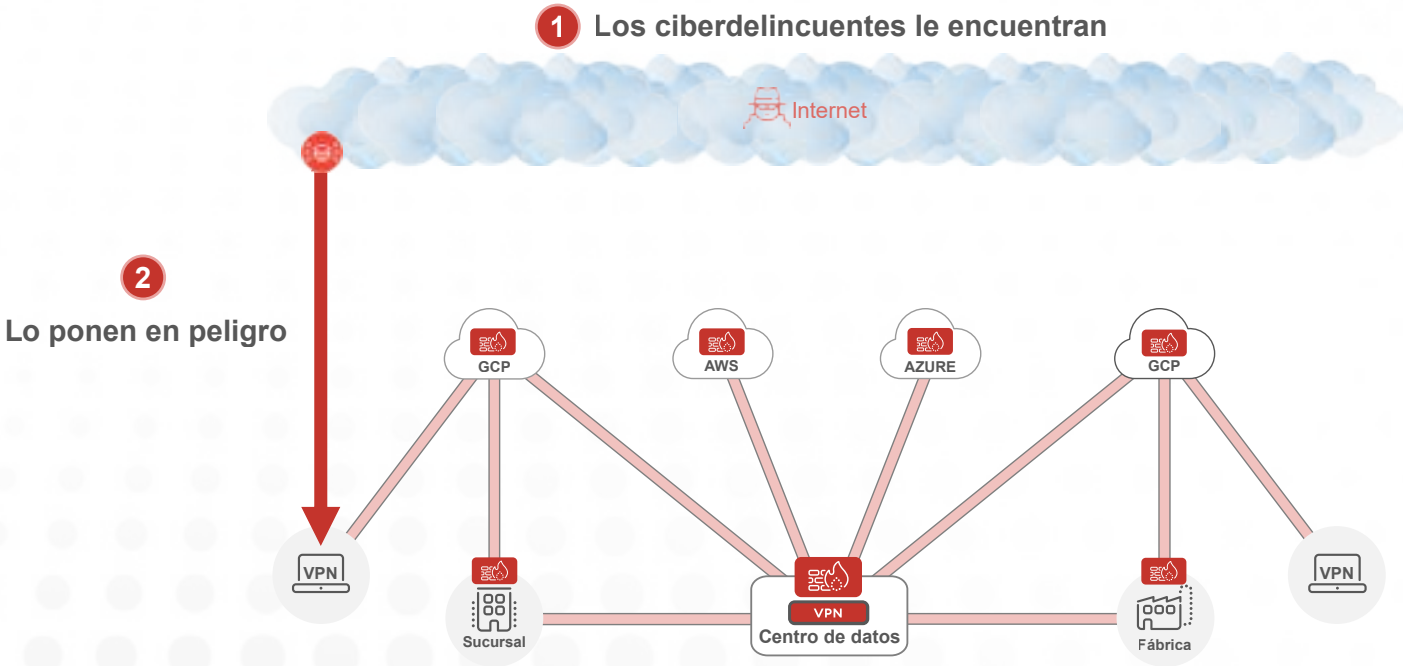
#2 Los firewalls y las VPN no logran evitar el riesgo

Una vez que los ciberdelincuentes han identificado con éxito un objetivo atractivo, lanzan sus ciberataques para infiltrar las defensas de la organización. Lamentablemente, una vez más, las herramientas tradicionales como firewalls y VPN no son adecuadas para proteger esta etapa de la cadena de ataque.

Para evitar el peligro es necesario emplear políticas de seguridad en línea que detengan las amenazas en tiempo real, antes de que puedan entrar en el entorno de una organización y empezar a causar daños.

Esto, a su vez, significa que las organizaciones deben ser capaces de inspeccionar todo el tráfico a través de sus operaciones para que puedan identificar cualquier amenaza potencial. Para lograrlo, la capacidad de inspeccionar el tráfico cifrado es increíblemente importante, y ello se debe a que la gran mayoría del tráfico web actual está cifrado (más del 95 %). Pero aquí es donde se manifiesta otra debilidad clave de la arquitectura basada en firewalls y VPN.

Cómo la arquitectura centrada en firewalls 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. Lamentablemente, los dispositivos de seguridad como los firewalls tienen dificultades para funcionar según sea necesario para lograr esto, ya sea que se implementen como dispositivos de hardware en las instalaciones o 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 confían en las herramientas y arquitecturas tradicionales se quedan con una inspección incompleta del tráfico cifrado, en el mejor de los casos, y ninguna inspección del tráfico cifrado, en el peor.

Al no inspeccionar el tráfico cifrado a escala, 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 ello y han empezado a utilizar el tráfico cifrado como medio preferido para ejecutar sus ataques. En la actualidad, 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 consigue detener a la gran mayoría de las amenazas que intentan traspasar sus defensas. En pocas palabras, las arquitecturas de firewalls y VPN no consiguen evitar el compromiso.

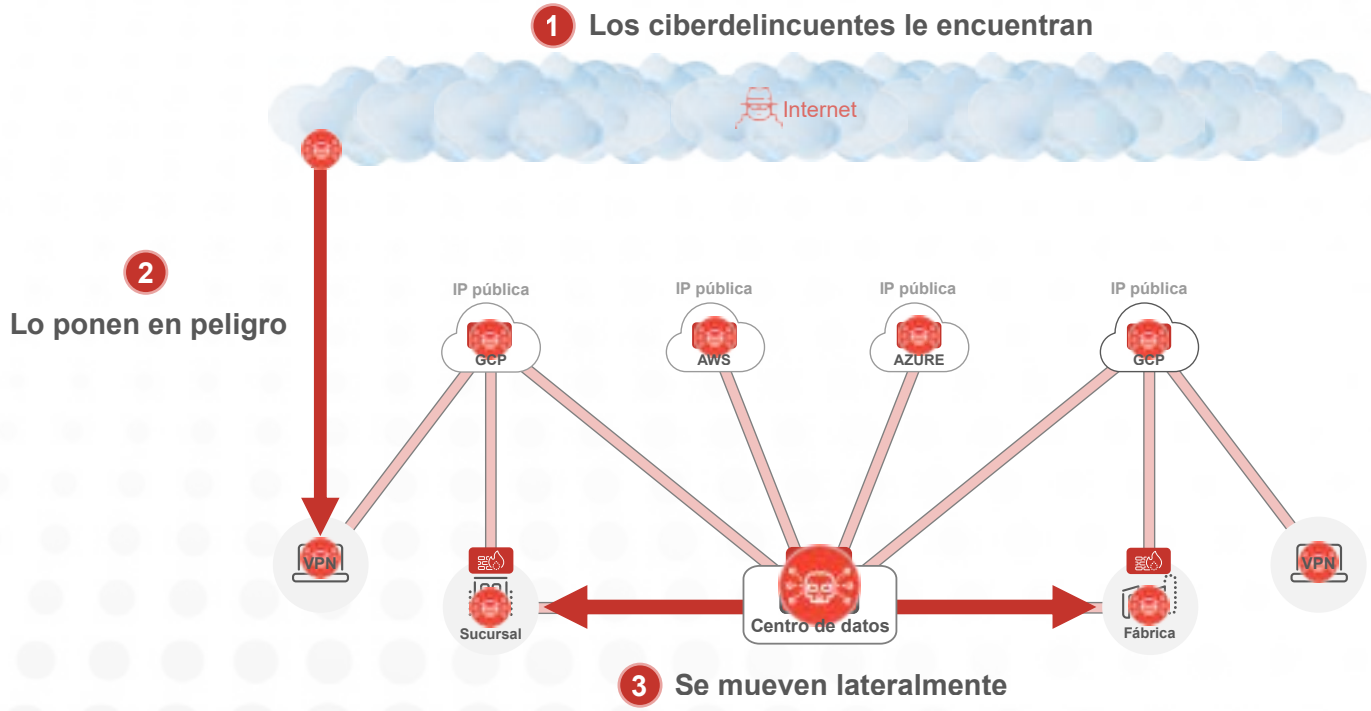
#3 Los firewalls y las VPN permiten el movimiento lateral de amenazas

Una vez que se ha producido el compromiso y una ciberamenaza ha superado las defensas de una organización, las debilidades de los firewalls y las VPN quedan a la vista. El movimiento lateral de amenazas, también conocido como propagación lateral, se refiere a la manera 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 viola el perímetro de una organización.

Para comprender cómo puede ocurrir el movimiento lateral de amenazas, solo es necesario considerar la analogía contenida en la frase “seguridad de tipo castle-and-moat”.

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

Cómo la arquitectura centrada en firewalls y VPN aumenta el riesgo



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

La debilidad mencionada anteriormente de castillos y fosos también está presente cuando se utilizan firewalls y VPN. Esto se debe a la naturaleza altamente interconectada de las redes hub-and-spoke en las que algunas organizaciones todavía confían, así como a la manera en que los modelos de seguridad castle-and-moat centran los esfuerzos de protección contra amenazas en defender el acceso a la red como un todo.

Simplemente piense en los firewalls como el "foso", las VPN como el "puente levadizo" y la propia red como el "castillo". Una vez que una ciberamenaza prevalece sobre el "foso" y entra en el "castillo", el malintencionado puede pasar fácilmente de un recurso conectado a otro, accediendo a las distintas "habitaciones" del "castillo".

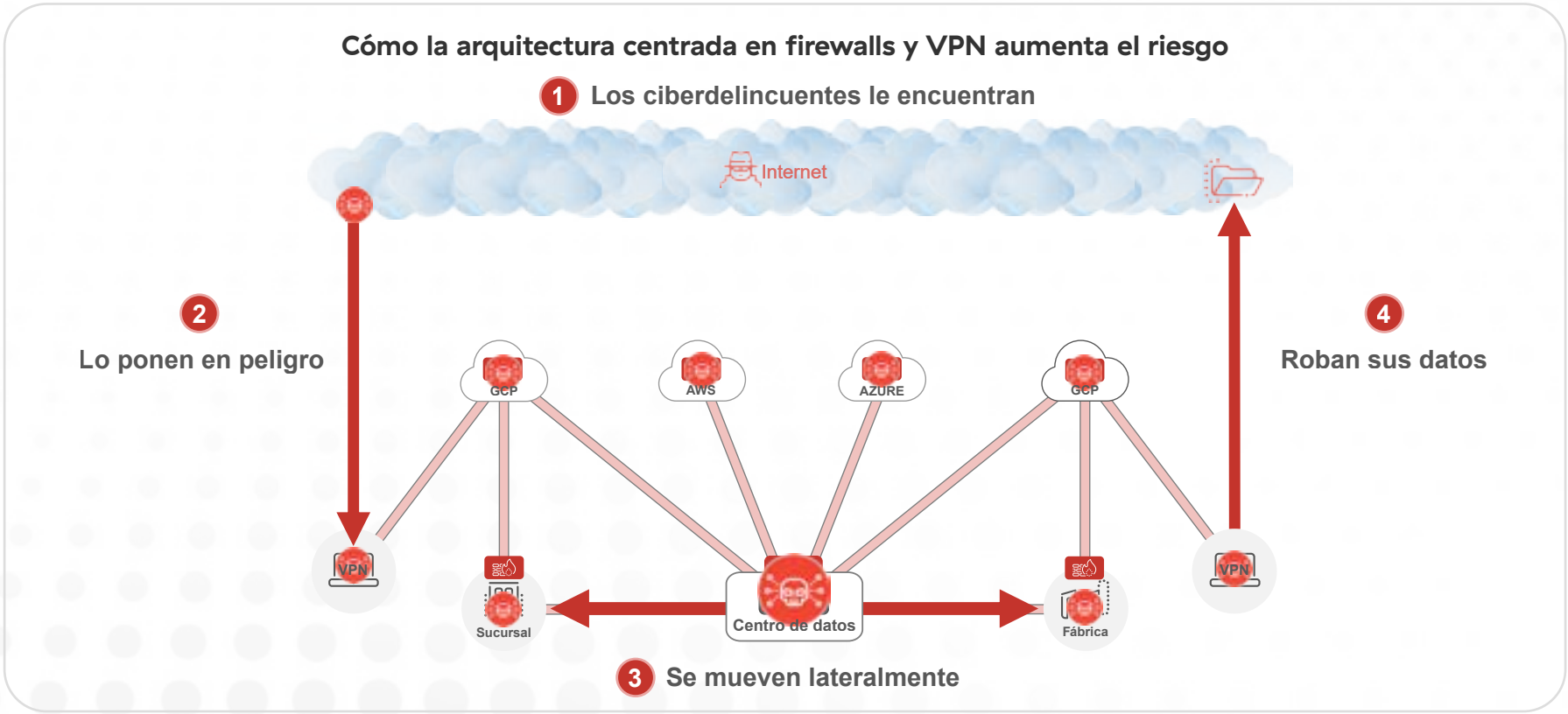
En palabras más explícitas, los firewalls y las VPN permiten el movimiento lateral de las amenazas y hacen posible que los ciberdelincuentes amplíen el alcance de sus violaciones a través de la red, causando daños, trastornos y costos masivos. Hacer concesiones en cualquier área significa efectivamente hacer concesiones en todas las áreas. Si bien la segmentación de la red a menudo se presenta como la solución a este problema, esta táctica inevitablemente se traduce en comprar más y más firewalls, lo que no permite abordar los problemas arquitectónicos subyacentes inherentes a las herramientas basadas en los perímetros del pasado.

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

En la gran mayoría de los ciberataques, los malintencionados no buscan vulnerar las organizaciones simplemente por diversión 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 como palanca en un ataque de ransomware de doble extorsión para obligar a una organización a pagar un rescate. 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 son facilitados por firewalls y VPN), buscarán la mayor cantidad de datos posible en toda la red, priorizando información particularmente confidencial o regulada. Naturalmente, a esto le sigue la exfiltración de datos.

Confiar en las herramientas tradicionales para detener este último eslabón de la cadena de ataque genera de nuevo resultados arriesgados y permite la pérdida de datos.



Como ya se ha mencionado, más del 95 % del tráfico web actual está cifrado. La inspección del tráfico cifrado requiere una gran potencia de cálculo y los dispositivos estáticos son incapaces de escalar lo necesario para procesar los volúmenes masivos de tráfico cifrado que generan las organizaciones en crecimiento. Este desafío (tanto para el hardware como para los dispositivos virtuales) influye no solo en el compromiso, sino también en 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 no es solo por los desafíos de escalabilidad que herramientas como los firewalls no pueden detener la exfiltración de datos. Las tecnologías del ayer fueron diseñadas para el mundo del ayer, antes de la aparición de las aplicaciones en la nube y los trabajadores remotos. Por ello, no pueden asegurar las vías modernas de fuga de datos; por ejemplo, la funcionalidad de compartir integrada en aplicaciones SaaS como Google Drive, Box, Microsoft OneDrive y otras. Del mismo modo, los recursos en la nube configurados erróneamente, como los buckets S3 de AWS configurados por error como "públicos", exponen los datos pero no pueden remediarse con firewalls, VPN o incluso herramientas convencionales de prevención de pérdida de datos (DLP).

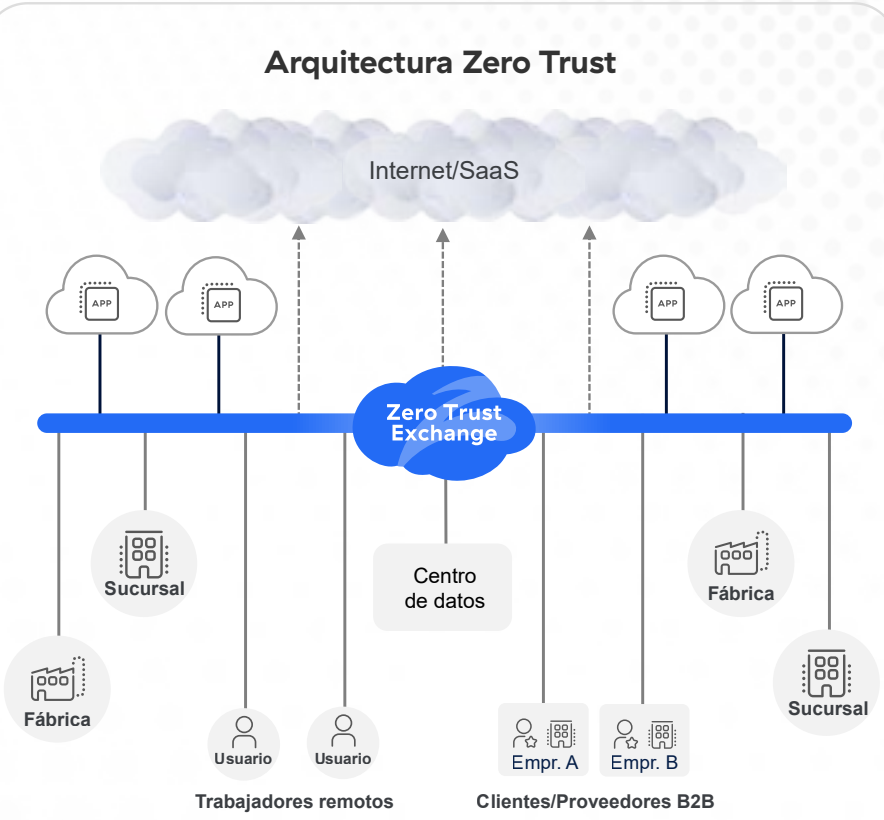
Los atacantes externos buscan utilizar estos y otros medios modernos para robar información confidencial; sin embargo, es fundamental tener en cuenta que no son la única amenaza para los datos. Las organizaciones deben enfrentarse a la realidad de que personas malintencionadas y descuidadas con información privilegiada también pueden fugar información confidencial de las maneras mencionadas. Independientemente del atacante, la seguridad debe evolucionar si se quiere mantener a salvo los datos.

Cómo la arquitectura 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 alivie los problemas de las arquitecturas basadas en perímetros sin resolver realmente sus causas subyacentes. Más bien, Zero Trust es una arquitectura distinta que se basa en el principio de acceso con privilegios mínimos; es inherentemente diferente de una arquitectura estándar basada en firewalls y VPN.

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

Con Zero Trust, la seguridad y la conectividad se desvinculan con éxito de la red, y las arquitecturas basadas en el perímetro se convierten en cosa del pasado.



Las políticas empresariales determinan quién puede acceder a qué a través de cualquier red. La red es solo el transporte.

Con esta arquitectura moderna, las organizaciones pueden poner fin a las cuatro maneras en que los firewalls y las VPN las exponen a las violaciones:

- **Minimice la superficie de ataque:** Aproveche Zero Trust para detener la expansión interminable de la red, elimine los firewalls, las VPN y sus IP públicas, impida las conexiones entrantes y oculte las aplicaciones tras una nube Zero Trust.
- **Detenga el compromiso:** Inspeccione todo el tráfico, incluido el cifrado a escala, a través de una nube Zero Trust de alto rendimiento que identifica las amenazas y aplica las políticas de seguridad en tiempo real.
- **Evite el movimiento lateral de las amenazas:** Conecte usuarios, cargas de trabajo y dispositivos directamente a las aplicaciones en lugar de a la red en su conjunto, manteniendo el principio del acceso con privilegios mínimos.
- **Bloquee la pérdida de datos:** Detenga la pérdida de datos en el tráfico cifrado y en todas las demás vías de fuga de datos, incluidos los datos en reposo en la nube y los datos en uso en los dispositivos de punto final de los empleados.

Además de reducir el riesgo de violaciones, una arquitectura Zero Trust reduce la complejidad, aumenta la productividad de los usuarios, ahorra dinero y mejora el dinamismo de la organización, resolviendo una serie de problemas que afectan a las arquitecturas basadas en firewalls y VPN.

Resumen

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

Más de 150
Centros de datos globales

Más de 360 mil millones
Transacciones aseguradas diariamente

Más de 500 billones
Señales de telemetría diarias

Más de 70
Puntuación de Net Promoter

40 %
De Fortune 500 son clientes

Líder
En el Gartner® MQ para SSE

Para más información, inscríbase en nuestro seminario web mensual "Empiece aquí: Una introducción a Zero Trust". En el seminario web, hablamos de la arquitectura Zero Trust desde los primeros niveles (además de compartir más información sobre Zscaler) para que cualquiera pueda comenzar su experiencia Zero Trust con confianza.

zscaler™ | 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 ciberataques y pérdida de datos al conectar de manera 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**.

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