Informe de riesgos de VPN de 2024 de Zscaler ThreatLabz

Cybersecurity INSIDERS

Explore las tendencias clave en seguridad, riesgos y experiencia de usuario de VPN a medida que la adopción de zero trust toma un impulso decisivo

Índice

Resumen

El entorno de trabajo distribuido y centrado en la nube actual ha provocado un cambio en los métodos de acceso de las redes privadas virtuales (VPN) tradicionales a marcos de seguridad más potentes como zero trust. Tradicionalmente, las VPN proporcionaban capacidades esenciales de acceso remoto para conectar usuarios o sitios de oficina completos. Sin embargo, la creciente sofisticación de las ciberamenazas junto con la expansión de las fuerzas laborales remotas y las tecnologías en la nube han expuesto importantes vulnerabilidades en las VPN. Debido a su arquitectura heredada, las VPN otorgan un acceso a la red demasiado amplio una vez que se verifican las credenciales, lo que aumenta significativamente el riesgo de ciberataques si esas credenciales se ven comprometidas.

Las recientes vulneraciones de alto perfil a dispositivos VPN han puesto de relieve vulnerabilidades críticas (en particular, CVE-2023-46805, CVE-2024-21887 y CVE-2024-21893) que afectan a sectores esenciales, incluida la defensa de Estados Unidos. Estas vulnerabilidades permiten a los atacantes eludir la autenticación, ejecutar comandos con privilegios elevados y persistir después de reiniciar el dispositivo. En respuesta, la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) emitió una directiva de emergencia a las agencias federales para que desconectaran inmediatamente los dispositivos VPN afectados debido a importantes riesgos de seguridad.

A través de la Orden Ejecutiva 14028, el gobierno de EE. UU. exige ahora la adopción de arquitecturas de zero trust para mejorar la ciberseguridad y dejar atrás las VPN tradicionales. Esta directiva, parte de una estrategia integral para fortalecer la ciberseguridad nacional, instruye a las agencias federales a implementar zero trust, que verifica cada solicitud de acceso independientemente de su origen. La Oficina de Administración y Presupuesto (OMB) respalda aún más esta iniciativa con una detallada Estrategia Federal de zero trust, que insiste en el paso de la confianza implícita basada en VPN dentro de los perímetros de la red a la verificación continua de todas y cada una de las solicitudes de acceso. Estas directivas y recomendaciones reflejan un consenso dentro de la comunidad de ciberseguridad de que zero trust proporciona una defensa más sólida contra ciberamenazas complejas y en evolución, una necesidad que han subrayado las recientes vulnerabilidades de las VPN tradicionales.

Como resultado, las organizaciones están adoptando rápidamente modelos de zero trust, que no confían inherentemente en ningún usuario o dispositivo dentro o fuera del perímetro de la red y requieren una verificación granular para cada solicitud de acceso. Este modelo es particularmente eficaz para prevenir el movimiento lateral dentro de las redes, una vulnerabilidad que los atacantes suelen utilizar para profundizar su intrusión después de obtener el acceso inicial.

Basado en una encuesta realizada a 647 profesionales de TI y expertos en ciberseguridad, este informe explora los múltiples desafíos de seguridad y experiencia de usuario de las VPN para dar a conocer la complejidad actual de la gestión de acceso, las vulnerabilidades a diversos ataques cibernéticos y su potencial para perjudicar la postura de seguridad más amplia de las organizaciones. El informe también describe modelos de seguridad más avanzados, en particular el de zero trust, que se ha establecido firmemente como un marco sólido y preparado para el futuro para asegurar y acelerar la transformación digital.

Le damos las gracias a Zscaler por haber contribuido a esta encuesta de riesgo de VPN. Su experiencia en soluciones de acceso seguro y zero trust ha enriquecido significativamente nuestros hallazgos. Estamos seguros de que las conclusiones de este informe serán un recurso esencial para los profesionales de TI y ciberseguridad en su viaje hacia la seguridad zero trust.

Gracias, Holger Schulze, fundador de Cybersecurity Insiders

“Durante el año pasado, numerosas vulnerabilidades críticas de VPN sirvieron como puntos de entrada exitosos para ataques a grandes empresas y entidades federales. Teniendo en cuenta estos resultados, que continúan repitiéndose, es crucial que las empresas anticipen que los actores de amenazas explotarán cada vez más estos activos heredados expuestos a Internet (dispositivos y virtuales) que les permiten moverse fácilmente lateralmente a través de redes planas tradicionales. Es esencial hacer la transición a la arquitectura Zero Trust, que reduce significativamente la superficie de ataque al eliminar tecnologías heredadas como VPN y cortafuegos, aplicar controles de seguridad consistentes con inspección TLS y limitar el radio de explosión con segmentación y engaño para evitar infracciones dañinas”.

DEEPEN DESAI, DIRECTOR DE SEGURIDAD DE ZSCALER

Principales hallazgos

Los ataques a VPN van en aumento.

El 56 % de las organizaciones experimentó uno o más ataques cibernéticos relacionados con VPN en el último año (frente al 45 % el año anterior), lo que destaca la creciente frecuencia y sofisticación de los ataques dirigidos a VPN.

Las VPN no son rival para el ransomware, malware y DDoS.

Los encuestados identificaron el ransomware (42 %), el malware (35 %) y los ataques DDoS (30 %) como las principales amenazas que explotan las vulnerabilidades de las VPN, lo que subraya la amplitud de los riesgos a los que se enfrentan las organizaciones debido a las debilidades inherentes a las arquitecturas de VPN tradicionales.

La gran mayoría se está pasando a zero trust.

El 78 % de las organizaciones planea implementar estrategias de zero trust en los próximos 12 meses. Mientras tanto, el 62 % de las empresas está de acuerdo en que las VPN van en contra de zero trust.

No se puede ignorar el riesgo de movimiento lateral. El 53 % de las empresas afectadas por vulnerabilidades de VPN dicen que los actores de amenazas se movieron lateralmente, lo que demuestra fallas de contención en el punto inicial del compromiso que subrayan los riesgos de las redes planas tradicionales.

La mayoría tiene dudas sobre la seguridad de las VPN.

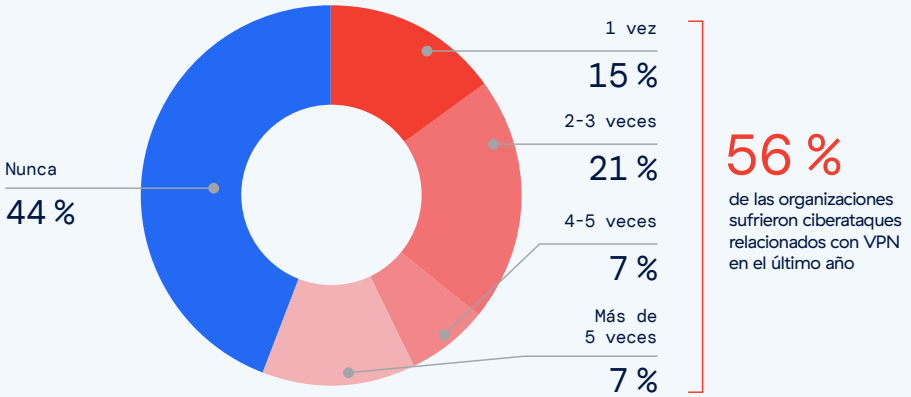
El 91 % de los encuestados expresaron su preocupación por el hecho de que las VPN comprometan su entorno de seguridad de TI, y las recientes infracciones ilustran los riesgos que conllevan las infraestructuras VPN obsoletas o sin revisiones.

Preocupaciones de seguridad con respecto a la VPN

Los ataques a VPN van en aumento

La frecuencia y gravedad de los ataques que aprovechan las vulnerabilidades de las VPN resaltan la ineficacia de las medidas de ciberseguridad convencionales y subrayan los riesgos persistentes que plantea la exposición de la red. Nuestra encuesta revela que el 56 % de las organizaciones sufrieron ciberataques en el último año que aprovecharon las vulnerabilidades de VPN, lo que supone un aumento significativo con respecto al 45 % del año anterior. Un alarmante 41 % de las organizaciones informaron haber sufrido dos o más ataques relacionados con VPN, lo que indica graves brechas de seguridad.

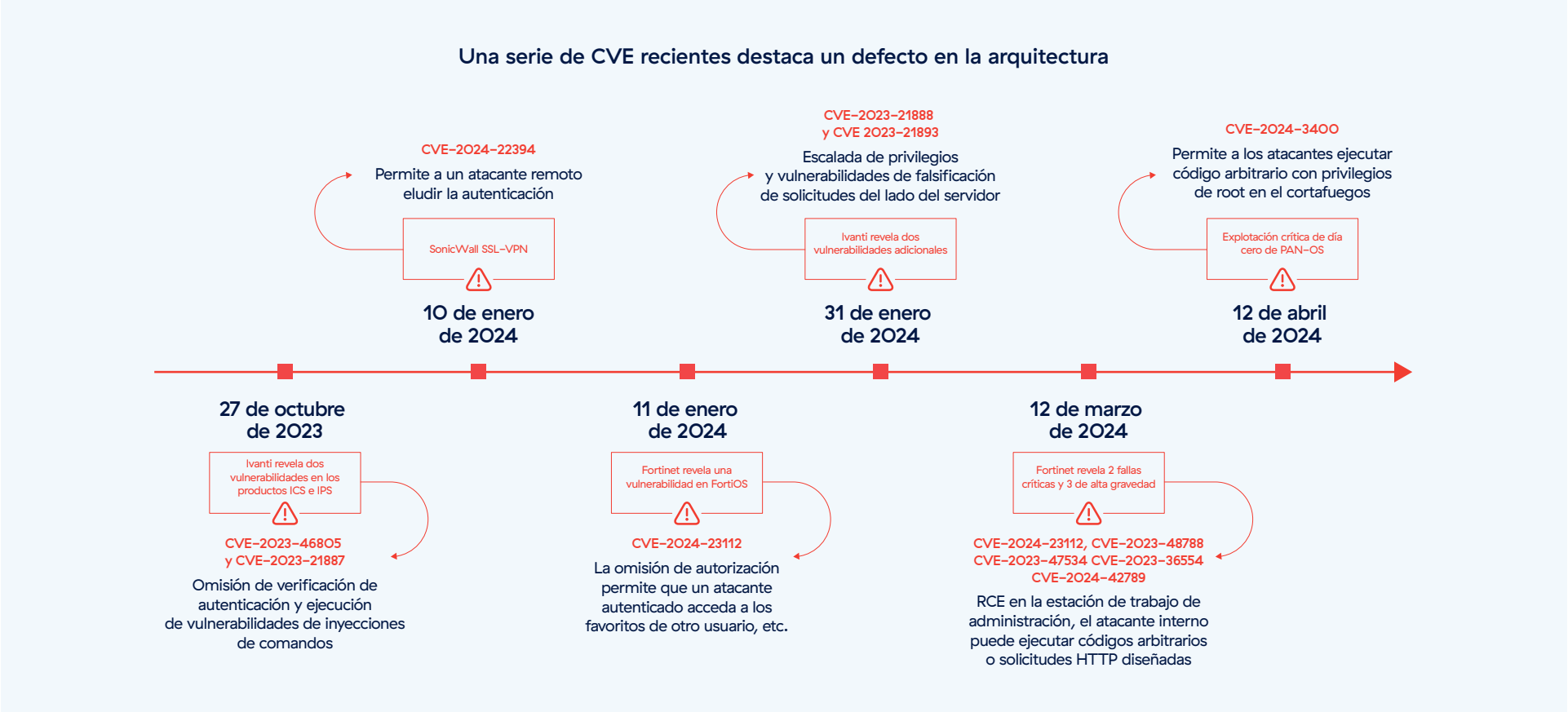
En los últimos 12 meses, ¿con cuánta frecuencia ha experimentado su organización algún ataque que haya aprovechado las vulnerabilidades de seguridad en sus servidores VPN?



Las últimas tendencias confirman que los ataques a las VPN no solo son cada vez más frecuentes, sino también más sofisticados. Por ejemplo, cada vez hay más casos de ransomware que explota fallas de VPN (particularmente después de vulnerabilidades divulgadas públicamente) que ponen de relieve las debilidades críticas inherentes a las VPN tradicionales. Estas vulnerabilidades ofrecen a los atacantes puntos de entrada fáciles para infiltrarse en las redes y facilitar el movimiento lateral, lo que provoca importantes filtraciones de datos e interrupciones operativas.

Principales vulnerabilidades de VPN en el último año

Teniendo en cuenta las recientes series de CVE de alta gravedad que afectan a los productos VPN, no sorprende que las empresas estén reportando más ataques que explotan este tipo de vulnerabilidades. Por supuesto, ningún proveedor ni ninguna tecnología en particular es inmune a las vulnerabilidades del software. En el caso de VPN, el desafío para las empresas es que cada CVE puede representar un único punto de falla de seguridad para la empresa: una cabeza de puente que permite a los atacantes comprometer un activo de VPN, establecer persistencia, moverse lateralmente a través de la red y robar datos. A medida que los CVE de VPN sigan divulgándose a este ritmo, serán un riesgo persistente para las empresas que utilizan VPN para conectividad remota.



Explorando las preocupaciones de seguridad de VPN

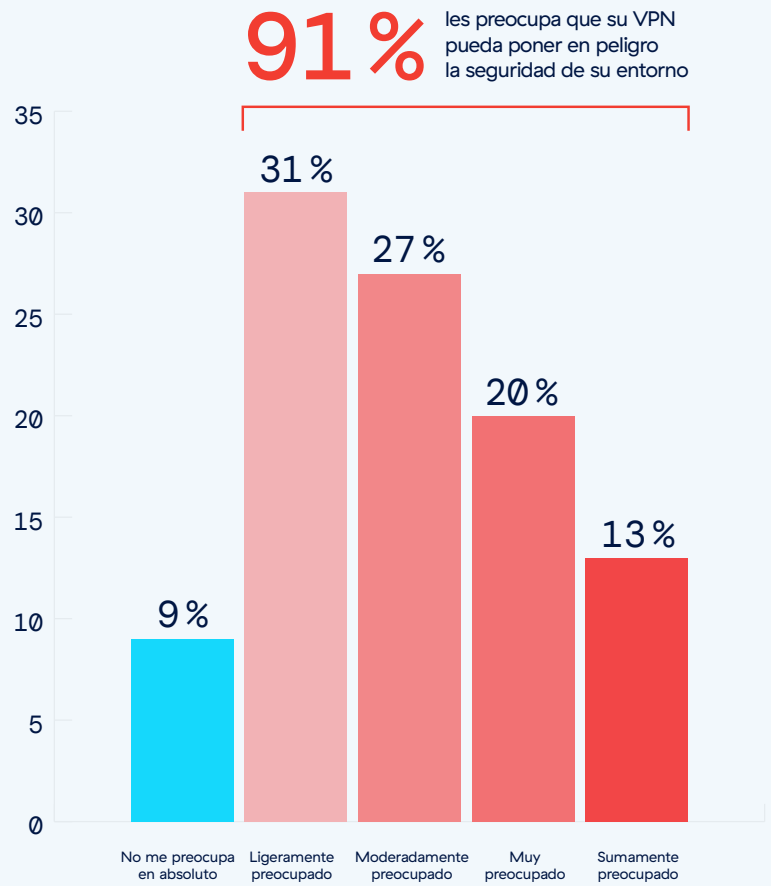
Los resultados de la encuesta reflejan preocupaciones profundamente arraigadas sobre el hecho de que las VPN comprometen los entornos de seguridad, lo cual se hace eco de las tendencias actuales y las crecientes vulnerabilidades en las tecnologías VPN. Una abrumadora mayoría de los encuestados (91 %, frente al 88 % en 2023) expresan su preocupación por el hecho de que las VPN pongan en peligro su seguridad de TI, lo que subraya una mayor conciencia sobre los riesgos relacionados con las VPN entre las organizaciones.

Esta preocupación se justifica por los recientes ataques dirigidos a las VPN de Ivanti, donde los atacantes aprovecharon graves vulnerabilidades para infiltrarse en las redes y exfiltrar datos confidenciales. Estos incidentes, que involucran vulnerabilidades como CVE-2024-21888 y CVE-2024-21893, resaltan los riesgos de mantener y proteger infraestructuras VPN obsoletas o sin revisiones. Además, la arquitectura inherente de las VPN plantea importantes riesgos de seguridad en el panorama digital sin perímetro actual. A medida que las empresas adoptan cada vez más servicios en la nube y los modelos de trabajo remoto evolucionan, las VPN se enfrentan a nuevos desafíos de seguridad, incluida la gestión de los amplios derechos de acceso y la protección de una superficie de ataque en expansión.

Estas vulnerabilidades y limitaciones arquitectónicas subrayan un cambio fundamental en las percepciones de la seguridad de las VPN y se alinean con tendencias de ciberseguridad más amplias que abogan por marcos más dinámicos y resistentes, como zero trust.

Las organizaciones con visión de futuro hacen la transición hacia arquitecturas de zero trust para obtener un control más granular y reducir significativamente la superficie de ataque al no conferir nunca confianza implícita, ya sea dentro o fuera del perímetro de la red. La adopción de una estrategia de este tipo aborda las vulnerabilidades inmediatas de las VPN tradicionales y se alinea con un enfoque proactivo de ciberseguridad, esencial para adaptarse al cambiante panorama de amenazas.

¿Hasta qué punto le preocupa que la VPN pueda poner en peligro su capacidad de mantener la seguridad de su entorno?



Escenarios clave para un acceso seguro

Comprender por qué las organizaciones utilizan las VPN es esencial, ya que refleja cómo priorizan el acceso seguro en diversos escenarios comerciales. También revela qué casos de uso de redes están más expuestos a riesgos de seguridad e indica áreas que requieren estrategias de seguridad de acceso más sólidas e innovadoras.

Un importante 70 % de las organizaciones utilizan VPN principalmente para proteger el acceso de los empleados remotos. Este uso generalizado hace que el acceso remoto sea un objetivo principal para los ciberataques. Después de esto, el 33 % utiliza VPN para conectar varios sitios, lo que presenta riesgos sustanciales, ya que estas conexiones pueden servir como vectores de ataques cibernéticos si no están protegidas adecuadamente. A continuación, el 26 % de las organizaciones destacó el acceso de terceros, lo que complica aún más la seguridad debido a las diferentes posturas de seguridad de las partes interesadas externas y la falta de control sobre las políticas de seguridad. Además, el 20 % de las organizaciones utiliza VPN para el acceso presencial y el 19 % las utiliza para la conectividad de dispositivos IoT/OT.

Las VPN ya no brindan una seguridad adecuada para casos de uso de acceso crítico en el cambiante panorama de ciberamenazas actual porque operan con modelos de confianza obsoletos que otorgan un amplio acceso a la red mediante una simple autenticación del usuario. Este amplio acceso expone a las organizaciones a riesgos importantes al permitir que atacantes potenciales aprovechen un único punto de entrada para moverse y extraer datos confidenciales a través de la red.

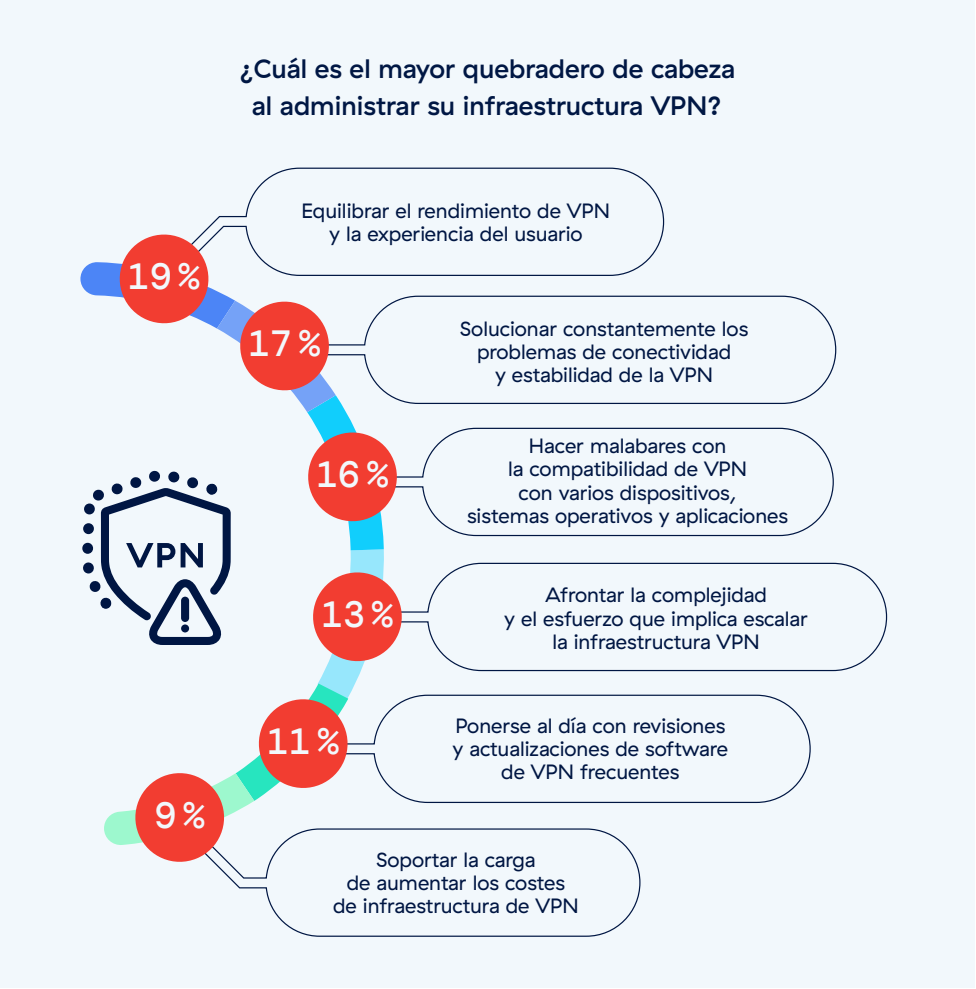
Gestión, rendimiento y experiencia de usuario de VPN

Desafíos en la gestión de VPN

Además de los riesgos de seguridad inherentes, la gestión de infraestructuras VPN presenta desafíos importantes para los equipos de TI a medida que los requisitos de soluciones de acceso sólidas se intensifican en entornos de trabajo dispersos y centrados en la nube. El principal desafío de gestión para los profesionales de TI es equilibrar el rendimiento de VPN y la experiencia del usuario (19 %). Este problema es crucial porque afecta directamente a la productividad: si la VPN ralentiza la red o resulta demasiado complicada de usar, puede provocar una menor satisfacción de los empleados y procesos comerciales lentos e ineficientes.

La siguiente preocupación más común, citada por el 17 % de los encuestados, es la resolución constante de problemas de conectividad y estabilidad de VPN. Estos problemas no solo consumen mucho tiempo para el personal de TI, sino que también causan interrupciones frustrantes para los usuarios. Otros desafíos notables incluyen la falta de compatibilidad de las VPN con una amplia gama de dispositivos, sistemas operativos y aplicaciones, lo que aproximadamente el 16 % de los profesionales de TI considera incómodo. Además, el 13 % de los encuestados lucha con la complejidad y lo trabajoso que es escalar la infraestructura VPN, un problema crítico a medida que las organizaciones crecen y sus necesidades aumentan en medio de una grave escasez de profesionales capacitados en ciberseguridad.

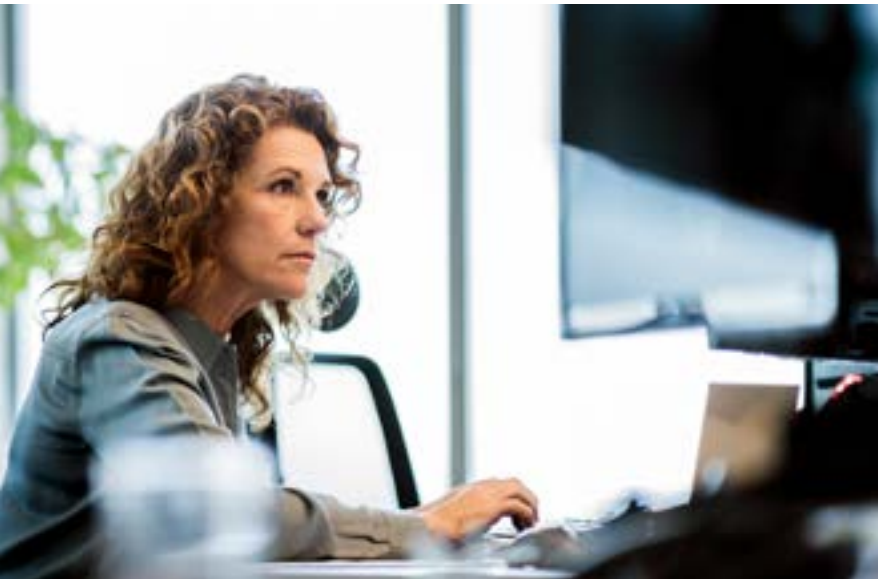
Estos hallazgos reflejan la necesidad de que las organizaciones exploren alternativas más ágiles, fáciles de usar y que requieran menos recursos, como los modelos de acceso a la red zero trust (ZTNA). ZTNA proporciona un control más granular, una escalabilidad mejorada y unos gastos generales de gestión reducidos, lo que la convierte en una opción superior a la VPN tradicional en el dinámico panorama de ciberseguridad actual.

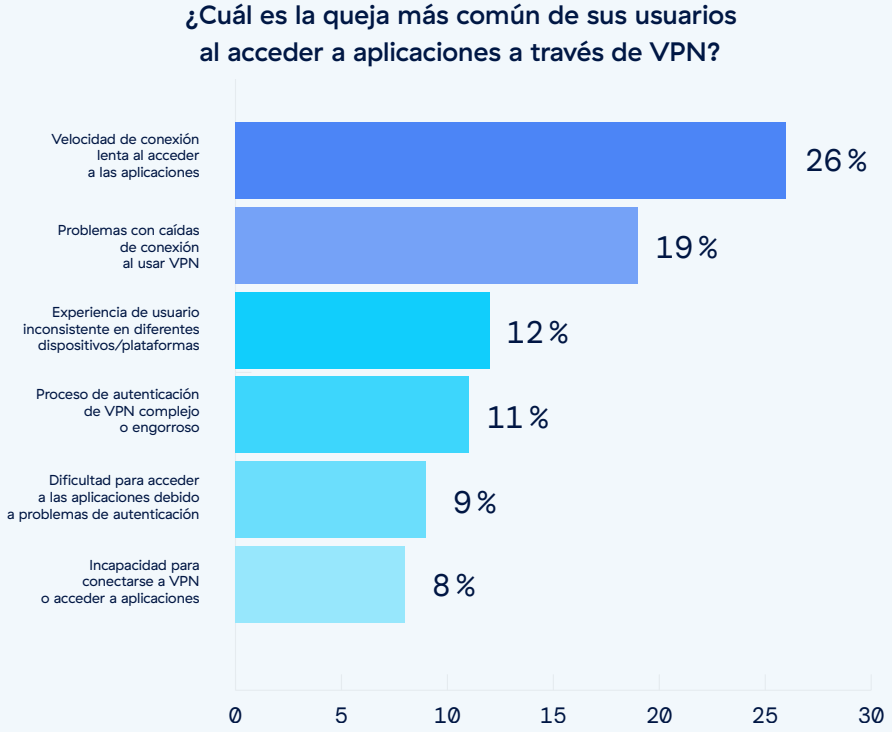


Desafíos comunes para los usuarios de VPN

La queja más frecuente de los usuarios sobre el uso de VPN, según lo señalado por el 26 % de los encuestados, es la baja velocidad de conexión. Esto pone de relieve un problema crítico de productividad y satisfacción del usuario, ya que las velocidades lentas pueden reducir significativamente la eficiencia de las tareas rutinarias y el acceso a los recursos basados en la nube, especialmente en entornos de trabajo desde casa.

Las caídas de la conexión VPN representan el segundo problema más común, citado por el 19 % de los encuestados. Este problema puede interrumpir las tareas y comunicaciones en curso y afectar significativamente la experiencia del usuario y la continuidad operativa. Las experiencias de usuario inconsistentes en diferentes dispositivos y plataformas, reportadas por el 12 % de los usuarios, apuntan a la necesidad de un rendimiento de acceso más uniforme.





Para abordar estas cuestiones, las organizaciones deberían considerar la adopción de soluciones de acceso a la red que ofrezcan más estabilidad y coherencia en varias plataformas. La implementación de una arquitectura zero trust puede resultar particularmente eficaz, ya que mejora la seguridad sin introducir cuellos de botella en el rendimiento. Las redes zero trust garantizan que los problemas de conexión no comprometan la seguridad y que el control de acceso sea estricto y adaptable a diferentes entornos de usuario.

Para contrarrestar estas vulnerabilidades, las organizaciones deben adoptar medidas de seguridad proactivas como un modelo zero trust. Zero trust impone controles de acceso estrictos y una verificación continua de todas las conexiones de red, independientemente de su origen. Esta estrategia mitiga eficazmente los riesgos que plantean una amplia gama de ataques que explotan las debilidades de las VPN, ya que limita el movimiento lateral y refuerza unos controles de acceso ya de por sí sólidos.

Explotación de vulnerabilidades de VPN

La variedad de ciberataques que aprovechan las debilidades de las VPN pone de relieve la amplitud de los riesgos a los que se enfrentan las organizaciones. La encuesta revela que el 42 % de los encuestados identifica los ataques de ransomware como los que tienen más probabilidades de explotar las vulnerabilidades de las VPN, lo que destaca su impacto significativo y la frecuencia con que se dan. A estos les siguen las infecciones de malware, que ha reportado el 35 % de los encuestados, y los ataques DDoS, con un 30 % (que comprometen la disponibilidad así como la confidencialidad e integridad de los sistemas).

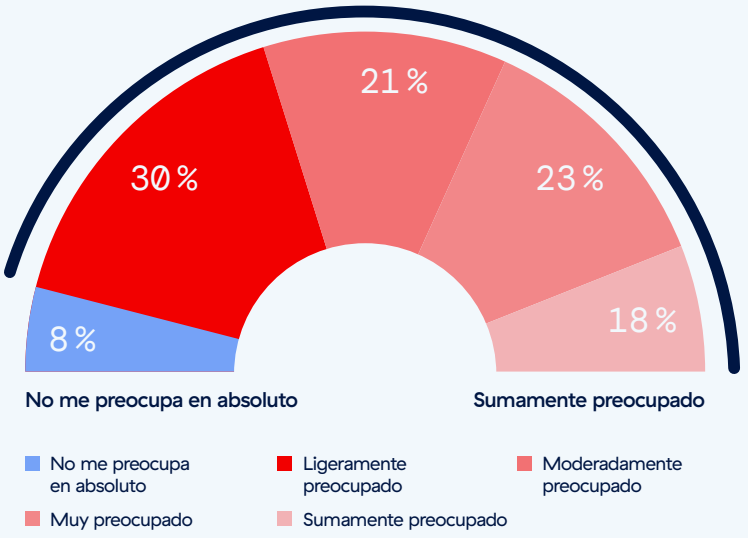
Riesgo de VPN de terceros

La encuesta subraya una importante preocupación en torno al acceso a VPN de terceros como una vulnerabilidad de seguridad de la red. Un notable 92 % de los encuestados expresa temor por este riesgo, lo que supone un ligero aumento con respecto al 90 % de 2023. Este creciente reconocimiento resalta el potencial del acceso de terceros para servir como punto de entrada para las ciberamenazas.

Los nuevos datos sobre las vulnerabilidades y las infracciones relacionadas con las VPN han validado aún más estas preocupaciones. Las VPN tradicionales suelen proporcionar un amplio acceso a la red después de que se validen las credenciales, lo que plantea riesgos si las medidas de seguridad de los proveedores de terceros se ven comprometidas.

¿Hasta qué punto está preocupado por los terceros que actúan como posibles puertas traseras para que los atacantes entren en su red a través de su acceso VPN?

92 % le preocupan los terceros que actúan como puertas traseras potenciales en sus redes a través del acceso VPN



Las organizaciones deberían acelerar su transición de las VPN tradicionales a las arquitecturas zero trust. Este cambio implica implementar sistemas que verifiquen rigurosamente las solicitudes de acceso en función de la identidad y el contexto para que los proveedores externos solo puedan acceder a recursos específicos esenciales para sus tareas.

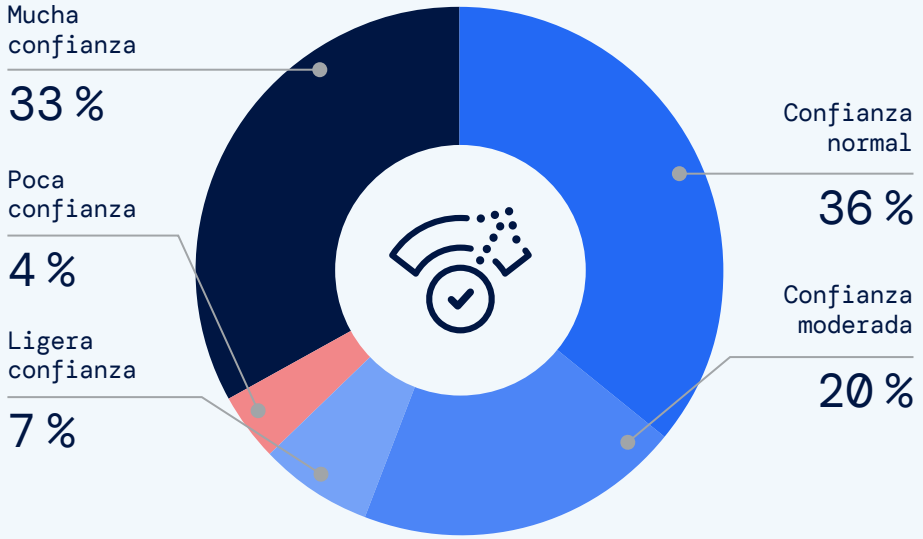
Problemas de seguridad con la infraestructura VPN

Exceso de confianza en la seguridad de VPN

El reciente aumento de las infracciones de VPN pone de relieve una desconexión entre la seguridad percibida y el riesgo real. Las recientes vulneraciones de alta gravedad en productos VPN son un reflejo de que incluso las organizaciones bien preparadas podrían estar subestimando las capacidades de los ciberadversarios, que explotan las vulnerabilidades inherentes a la tecnología VPN. Un significativo 69 % de los encuestados citó una gran confianza en la capacidad de su organización para manejar las vulnerabilidades de VPN, que puede no estar del todo alineada con el creciente panorama de amenazas donde actores sofisticados explotan incluso las debilidades más insignificantes muy rápidamente. El exceso de confianza puede ser particularmente arriesgado dada la complejidad y persistencia de los últimos ataques a VPN, como lo demuestran los incidentes que involucran a grupos patrocinados por el Estado y bandas de ciberdelincuentes que atacan sistemas sin revisiones durante períodos prolongados.

Las organizaciones deben reajustar su postura de seguridad incorporando evaluaciones rigurosas de vulnerabilidad, actualizaciones frecuentes y formación integral de concienciación sobre la seguridad. Es aconsejable adoptar un enfoque de seguridad por capas que no dependa demasiado de las VPN para una protección integral. Este enfoque debe incluir supervisión avanzada, detección de anomalías e integración de principios de zero trust.

¿Qué confianza tiene en la capacidad de su organización para detectar y mitigar las vulnerabilidades de VPN que la exponen a ataques de ciberseguridad?

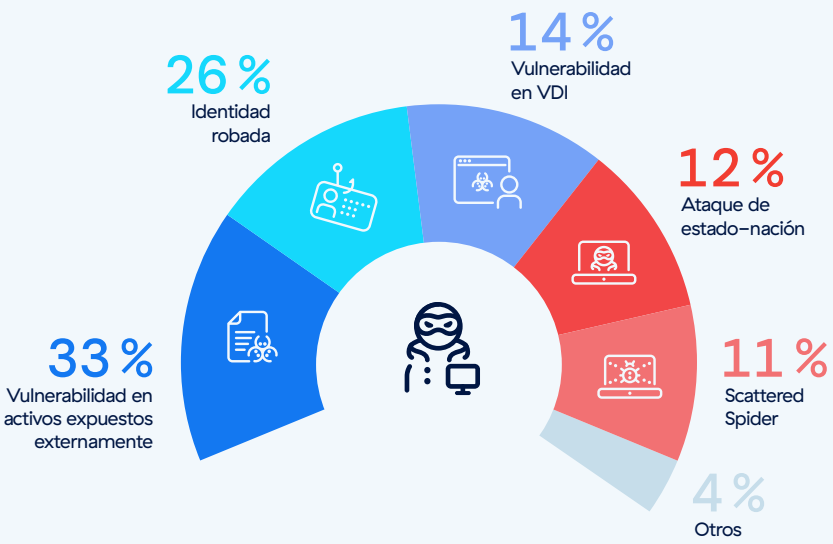


Vectores de ataque de ransomware

La encuesta identifica claramente las vulnerabilidades en los activos expuestos externamente como el vector de ataque potencial de ransomware más preocupante, como señala el 33 % de los encuestados. Esto apunta a un reconocimiento generalizado de los riesgos asociados con los servicios de red o aplicaciones web expuestos, que suelen ser el primer punto de entrada de los ataques de ransomware.

Las identidades robadas le siguen de cerca con un 26 %, lo que subraya el papel que desempeñan las credenciales comprometidas al permitir a los atacantes eludir las medidas de seguridad y obtener acceso para entregar cargas útiles de ransomware. Las preocupaciones sobre las vulnerabilidades en las infraestructuras de escritorios virtuales (VDI) y los ataques de estados-nación, con un 14 % y un 12 % respectivamente, subrayan los diversos orígenes de las amenazas de ransomware contra las que las organizaciones deben defenderse. Scattered Spider (un grupo cibercriminal que utiliza sofisticadas tácticas de ingeniería social, incluido el phishing, los ataques de fatiga de autenticación multifactor y el intercambio de SIM), preocupa al 11 % de los participantes.

¿Qué es lo que más le preocupa como causa principal del ransomware?



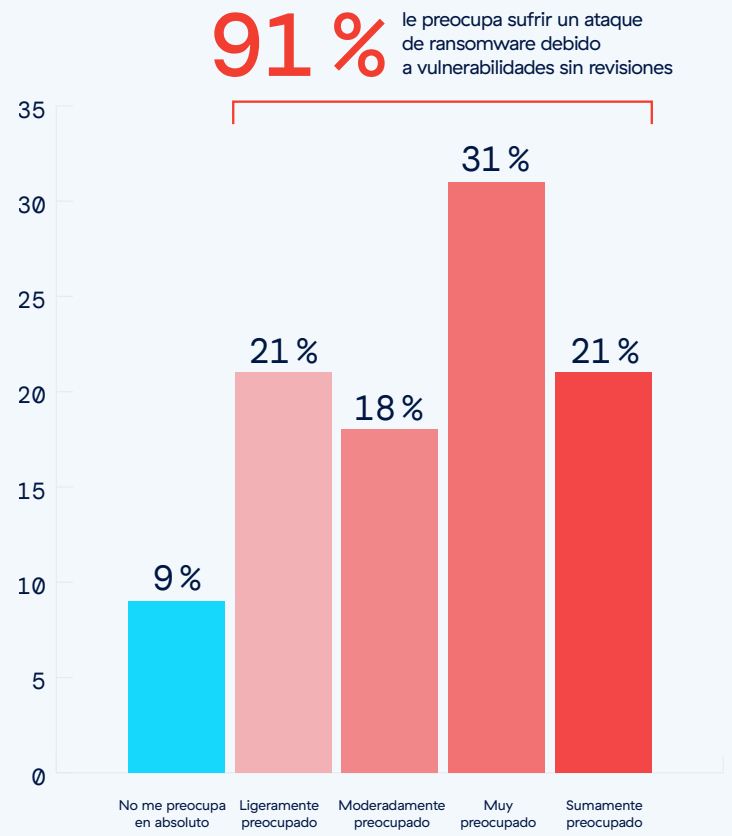
Las organizaciones deben mejorar sus defensas y protocolos de gestión de identidad. La implementación de procesos integrales de gestión de vulnerabilidades y la adopción de un modelo de seguridad zero trust pueden reducir eficazmente el riesgo de ataques de ransomware al negar el acceso a los recursos de la red y la propagación lateral.

Preocupaciones sobre ransomware

Los resultados de la encuesta muestran que el 52 % de los encuestados están muy o extremadamente preocupados por la amenaza del ransomware debido a vulnerabilidades sin revisiones. Esto se justifica porque las vulnerabilidades sin revisiones siguen siendo el principal vector de ataque del ransomware. Análisis recientes muestran que una parte sustancial de los ataques de ransomware aprovechan estas vulnerabilidades y tienen un impacto notablemente grave en comparación con otros tipos de ciberataques.

Los grupos de ransomware se están volviendo más sofisticados y muchos ahora utilizan tácticas avanzadas que pueden explotar rápidamente vulnerabilidades recién descubiertas antes de que las organizaciones puedan revisarlas. Este rápido ciclo de explotación acorta en gran medida el margen para responder a vulnerabilidades críticas, lo que resalta la necesidad urgente de implementar medidas de seguridad avanzadas que reduzcan la superficie de ataque.

¿Cuánto le preocupa sufrir un ataque de ransomware debido a vulnerabilidades sin revisiones?



Movimiento lateral en ataques VPN

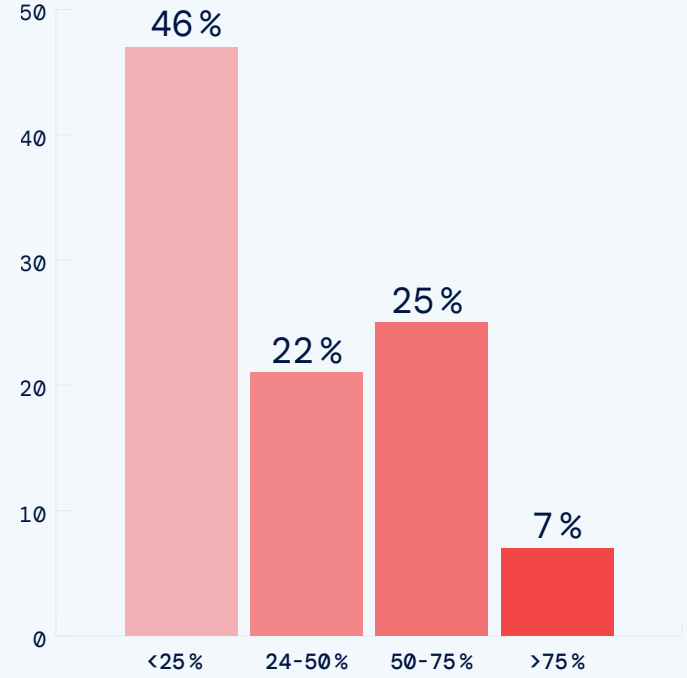
La mayoría de los encuestados (53 %) indican que más del 25 % de los ataques relacionados con VPN involucraron movimientos laterales, lo que demuestra fallas de contención significativas en el punto inicial de compromiso. Casi un tercio (32 %) experimentaron movimientos laterales en más de la mitad de los ataques, lo que indica grandes desafíos para controlar la propagación de amenazas una vez que los adversarios infringen las defensas de la red.

El movimiento lateral es un riesgo importante con las VPN, ya que los atacantes pueden obtener un amplio acceso a la red, similar al de un usuario autenticado. Esto les permite moverse sigilosamente a través de la red y centrarse en áreas sensibles.

De esta manera, las VPN pueden agravar los riesgos y ampliar el alcance de un ataque más allá de su punto de entrada inicial. Resolver esto requiere una segmentación estricta, idealmente con tráfico de usuario a aplicación a través de una arquitectura zero trust, y supervisión continua. Así se reduciría sustancialmente el movimiento lateral y su impacto, porque se permite el acceso granular a un conjunto más pequeño de aplicaciones para cada usuario, mientras que el resto se vuelve invisible.

La creciente sofisticación de los ataques que explotan las vulnerabilidades de las VPN subraya la necesidad de un cambio hacia un marco zero trust. Al aplicar estrictos controles de acceso y verificación continua, el zero trust limita los movimientos laterales no autorizados y mejora la seguridad en entornos digitales en expansión.

De todos los ataques que ha experimentado su organización, ¿qué porcentaje representan las amenazas que se propagaron lateralmente después de obtener acceso a través de VPN?

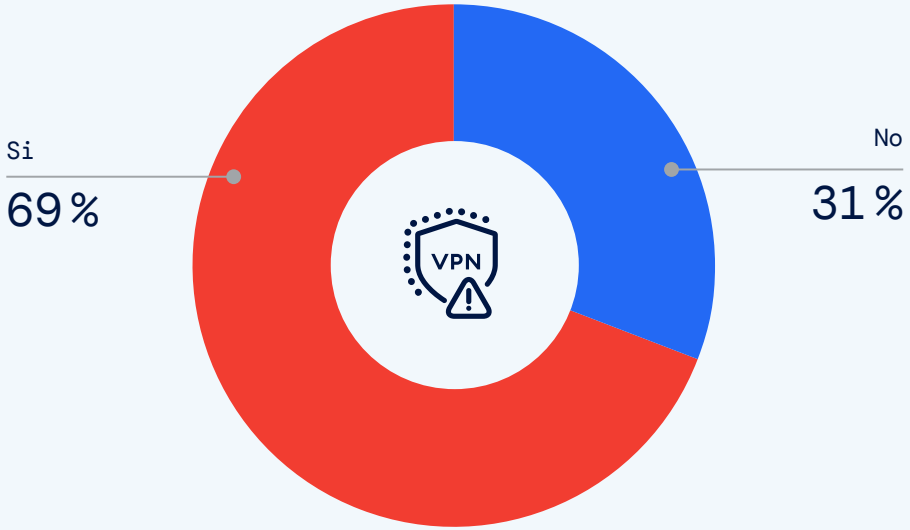


Preocupaciones de seguridad de VPN Tras las fusiones y adquisiciones (M&A)

La preocupación por el impacto de las fusiones y adquisiciones (M&A) en la infraestructura VPN existente destaca las vulnerabilidades potenciales que surgen de los cambios organizacionales y la integración de redes dispares.

Un importante 69 % de los encuestados expresa temor por los ciberataques posteriores a una fusión y adquisición, lo cual refleja que hay una inquietud generalizada por los riesgos de seguridad asociados con estas transformaciones corporativas. Este sentimiento refleja que se sabe claramente que las actividades de M&A pueden desestabilizar los marcos de seguridad existentes y aumentar la exposición a ciberamenazas.

¿Le preocupa convertirse en víctima de un ataque posterior al M&A con su arquitectura actual?



Los períodos de transición durante una M&A son una oportunidad única para que las organizaciones eliminen gradualmente las tecnologías VPN anticuadas y vulnerables en favor de marcos zero trust. Específicamente, las arquitecturas zero trust mejoran la seguridad al proporcionar una segmentación integral del entorno entre usuarios y aplicaciones, cargas de trabajo y cargas de trabajo, sucursales y dispositivos, ya sean administrados, no administrados, IoT o sistemas OT. Este enfoque refuerza significativamente la seguridad durante y después de una transición mediante una verificación rigurosa de todos los usuarios y dispositivos, una segmentación integral y una aplicación estricta de los controles de acceso con menos privilegios.

Adopción empresarial de zero trust

Progreso en la adopción de zero trust

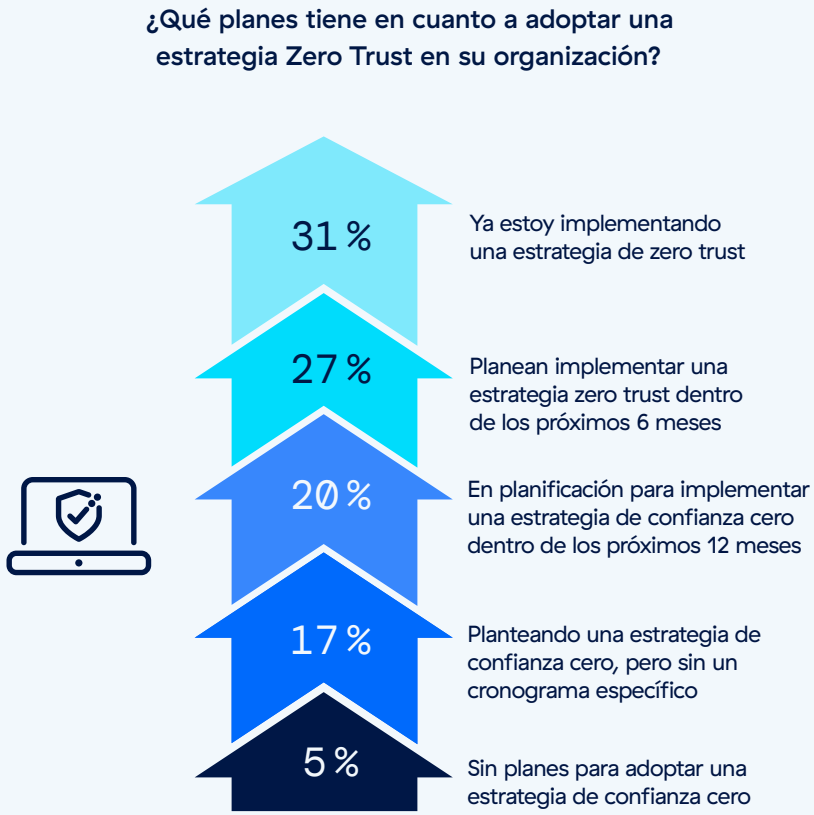
La encuesta refleja una fuerte tendencia hacia la adopción de marcos de seguridad zero trust, lo que subraya el creciente reconocimiento de su importancia para mejorar la ciberseguridad organizacional. Un importante 31 % de los encuestados ya está implementando el zero trust (frente al 27 % en 2023), lo que indica un esfuerzo proactivo cada vez mayor para proteger mejor los recursos de la red.

Además, el 27 % de las organizaciones planea implementar una estrategia de zero trust en los próximos seis meses (frente al 18 % en 2023) y otro 20 % de las organizaciones planea hacer el cambio en los próximos 12 meses, lo que demuestra un compromiso generalizado con la transición hacia el zero trust en un futuro próximo. Esto confirma que más de las tres cuartas partes de los encuestados (78 %) son conscientes de la urgencia y los beneficios del zero trust.

Sin embargo, el 17 % de los encuestados todavía está considerando una estrategia de zero trust y no tiene un cronograma específico (frente al 23 % en 2023), lo que pone de relieve cierta indecisión o posibles desafíos a la hora de planificar o iniciar la transición. Solo una pequeña fracción (5 %) informa de no tener planes para adoptar el zero trust (en comparación con el 8 % en 2023), posiblemente por falta de recursos.

Un análisis por tamaño de empresa indica que las organizaciones más grandes de nuestra encuesta, particularmente aquellas con más de 20 000 empleados, tienen más probabilidades adoptar estrategias de zero trust y lo harán más rápido, y el 33 % ya está en ello. Por el contrario, las empresas más pequeñas con entre 1000 y 5000 empleados muestran una tasa de adopción ligeramente menor, de un 29 %, lo que sugiere que la escala y la disponibilidad de recursos podrían influir en el ritmo y el alcance de la integración de zero trust.

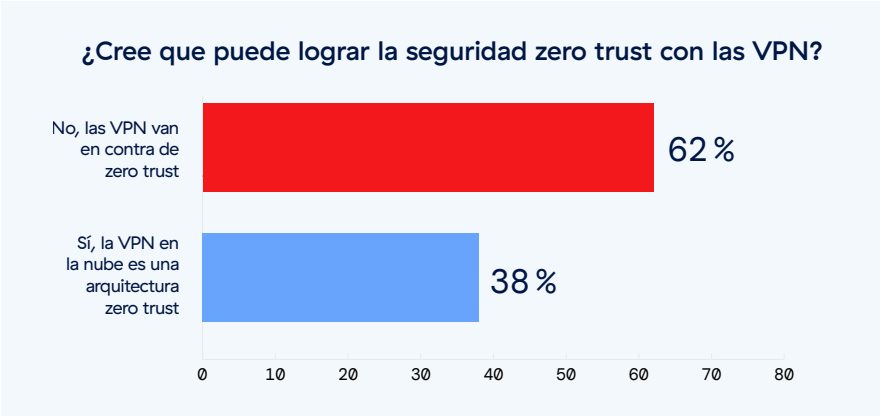
Las organizaciones que aún están indecisas o planean adoptar el zero trust deben comenzar por evaluar su postura de seguridad actual y su arquitectura de red para identificar necesidades específicas y desafíos potenciales.



Las VPN no dan seguridad zero trust

Los resultados de la encuesta reflejan una división significativa en las creencias sobre la compatibilidad de las VPN con marcos de seguridad zero trust. La mayoría (62 %) cree que básicamente las VPN van en contra del zero trust o confianza cero, lo que confirma que las arquitecturas VPN tradicionales no se alinean con los principios de esta. Por el contrario, el 38 % de los encuestados considera que las VPN, especialmente las plataformas basadas en la nube, son compatibles con arquitecturas zero trust.

Si bien esta perspectiva puede deberse a que los proveedores de VPN afirman que sus soluciones basadas en la nube se alinean con los principios de zero trust, es importante examinar estas afirmaciones de manera crítica. El simple hecho de alojar un servicio VPN en la nube, por ejemplo, no confiere automáticamente atributos de zero trust. La seguridad zero trust requiere algo más que un entorno de alojamiento seguro; exige un cambio fundamental de las defensas basadas en el perímetro a un modelo donde la seguridad sea dinámica, granular y esté basada en el contexto.

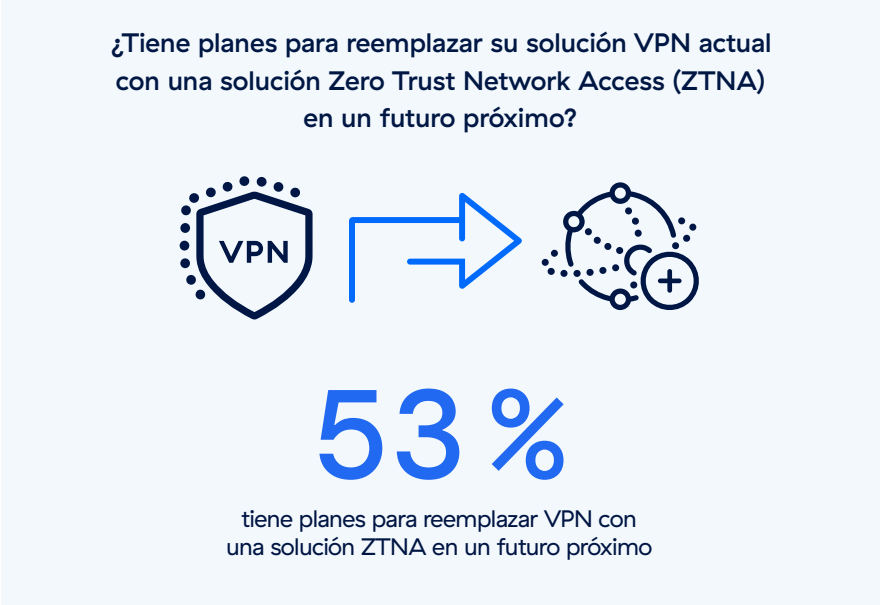


La verdadera seguridad zero trust implica validar continuamente a todos los usuarios y dispositivos, aplicar acceso con privilegios mínimos y segmentar el tráfico para evitar el movimiento lateral, características que las VPN tradicionales, incluso las basadas en la nube, no ofrecen. Por lo tanto, las organizaciones deben asegurarse de que cualquier VPN de “zero trust” realmente incorpora estos principios básicos en lugar de confiar únicamente en las promesas que hace el marketing.

Avanzar de la VPN al acceso a la red zero trust

Los resultados de la encuesta muestran que la mayoría de las organizaciones está haciendo un cambio estratégico, pues un 53 % de los encuestados afirma tener planes para reemplazar sus soluciones VPN existentes con soluciones ZTNA en un futuro próximo. ZTNA ofrece un enfoque más flexible y seguro al aplicar políticas basadas en el contexto del usuario, la ubicación y la seguridad del dispositivo, sin asumir que es confiable por la ubicación de la red. Esto contrasta con las VPN tradicionales, que generalmente otorgan un amplio acceso a una red y a su vez genera vulnerabilidades de seguridad.

Para el 53 % de las organizaciones que avanzan hacia ZTNA, es crucial garantizar una transición sin problemas mediante la planificación de evaluaciones de riesgos integrales, la actualización de las políticas de acceso y la educación de los usuarios sobre los nuevos protocolos. Mientras tanto, el 47 % que aún no tiene pensado hacer este cambio debería evaluar sus desafíos de seguridad actuales y considerar si ZTNA podría abordarlos de manera más efectiva que VPN.

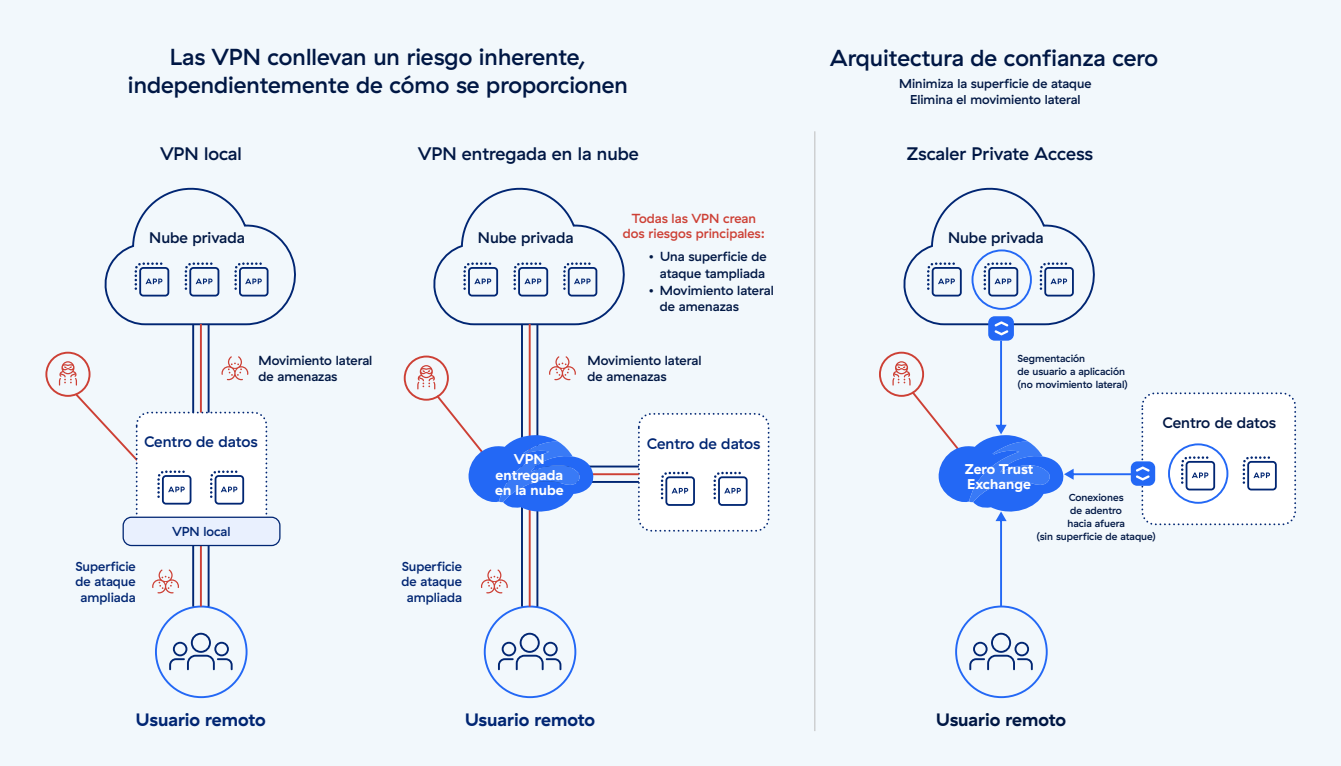


Por qué zero trust es más seguro que una VPN

Desde el punto de vista arquitectónico, zero trust y ZTNA son más seguros que las VPN tradicionales por varias razones, principalmente porque son un marco de seguridad sólido que nunca confía inherentemente en una sola conexión. Las arquitecturas tradicionales basadas en VPN son susceptibles a un único punto de falla. Cuando una VPN o un dispositivo se ve comprometido (por ejemplo, a través de un nuevo CVE), los actores de amenazas pueden explotar la confianza inherente a una red plana para obtener acceso a toda la red, moverse lateralmente, robar datos e implementar ransomware. Por eso los profesionales de la seguridad están cada vez más preocupados por los riesgos de seguridad de las VPN.

Las VPN locales y en la nube presentan vulnerabilidades de seguridad similares. Además, las VPN introducen complejidad, lo que genera sobrecargas innecesarias y tareas que consumen mucho tiempo, como el aprovisionamiento de usuarios, la gestión de tablas de enrutamiento, la resolución de problemas de conectividad, la aplicación de revisiones, la supervisión y la optimización del rendimiento.

En una arquitectura zero trust, nunca se confía en una conexión única. Los usuarios se conectan directamente a las aplicaciones, nunca a la red subyacente. Además, cada conexión finaliza automáticamente, independientemente de su origen, pero primero la verifican siete capas de controles de seguridad zero trust. La arquitectura zero trust permite a las organizaciones segmentar integralmente sus entornos con acceso granular: desde usuarios hasta aplicaciones, desde cargas de trabajo hasta cargas de trabajo, entre sucursales y entre dispositivos, incluidos dispositivos IoT y OT.



Diferencias y ventajas clave

Superficie de ataque significativamente reducida
Una arquitectura zero trust establece una conectividad de dentro hacia afuera que oculta activos críticos, aplicaciones, servidores y más de la Internet pública, al tiempo que elimina la necesidad de tener activos vulnerables como VPN y cortafuegos. Esto permite a las empresas proporcionar conectividad híbrida a su fuerza laboral y al mismo tiempo reducir considerablemente su superficie de ataque. Por el contrario, las arquitecturas basadas en VPN y cortafuegos requieren que las empresas amplíen la superficie de ataque para dar cabida a una mayor conectividad.

Verificación continua
Los modelos zero trust imponen una verificación de seguridad continua de las credenciales y la postura de seguridad antes de otorgar acceso a los recursos, lo que hace mucho más difícil para entidades no autorizadas obtener y mantener el acceso a información y sistemas confidenciales. Mientras tanto, con las VPN, el usuario o dispositivo suele tener un amplio acceso a los recursos de la red una vez que se le concede el acceso.

Acceso con privilegios mínimos
Los principios de zero trust aplican políticas de acceso con privilegios mínimos, lo que garantiza que los usuarios y dispositivos solo tengan acceso a los recursos que necesitan para hacer sus funciones específicas.
Esto minimiza el riesgo de amenazas internas y movimiento lateral dentro de una red, que son vulnerabilidades comunes en las configuraciones de VPN.

Acceso granular y segmentación
Al dividir los recursos de la red en segmentos separados (entre usuarios y aplicaciones, entre cargas de trabajo, entre dispositivos), zero trust aísla las posibles infracciones en zonas más pequeñas, lo que reduce en gran medida el impacto de un ataque. Si bien las organizaciones a menudo intentan segmentar sus entornos de red, es un proceso operativo complejo y caro que, en la práctica, queda incompleto, requiere cientos de reglas de cortafuegos distintas y expone áreas de red más amplias a usuarios autenticados.

Potenciar la fuerza laboral híbrida actual
Zero trust permite ampliar fácilmente el acceso ultrarrápido a aplicaciones privadas a usuarios remotos, además de a quienes están en la sede central, las sucursales y los socios externos.

Experiencia de usuario mejorada y complejidad reducida
Zero trust mejora las experiencias de los usuarios al eliminar la necesidad de que todo el tráfico remoto se enrute a través de un punto de red central, un cuello de botella de rendimiento común en las VPN. Esta arquitectura es más capaz de manejar los requisitos de escala de las redes modernas que incluyen políticas de IoT y BYOD. Además, zero trust reduce los gastos generales de gestión al automatizar los controles de seguridad y simplificar la aplicación de las políticas de seguridad en toda la red.

Estas ventajas arquitectónicas hacen de zero trust una alternativa convincente a las VPN tradicionales, particularmente si se tiene en cuenta que el panorama de amenazas actual es cada vez más sofisticado y distribuido. Para las organizaciones que buscan reforzar sus defensas de ciberseguridad, la adopción de un enfoque zero trust proporciona una infraestructura de seguridad más sólida, flexible y escalable.

Predicciones sobre la VPN para 2024 y más adelante

1 Aumentarán las vulnerabilidades graves de VPN

Dada la frecuencia, gravedad y escala de las vulnerabilidades de VPN reveladas el año pasado, las empresas deberían esperar que esta tendencia continúe. Los actores de amenazas y los investigadores de seguridad son conscientes del mayor riesgo de vulnerabilidades de alta gravedad en los productos VPN. A su vez, buscan activamente más, por lo que es probable que se encuentren nuevos CVE en los próximos meses y años.

2 Los ataques de alto perfil que causa VPN serán el centro de atención

Esta predicción está estrechamente relacionada con la primera. Veremos que más organizaciones grandes revelan infracciones que resultan de vulnerabilidades de VPN explotadas. Esto pasará en parte debido a las nuevas pautas regulatorias de la SEC que requieren que las empresas públicas revelen detalles sobre infracciones con un impacto material. Como hemos visto, los actores de amenazas crean constantemente puertas traseras en los entornos de destino cuando hay vulnerabilidades de VPN con el objetivo único de explotarlas más adelante, incluso después de que estas vulnerabilidades se hayan corregido. A medida que avance el año, se empezarán a desvelar más casos de este tipo en presentaciones públicas de la SEC y aparecerán en las noticias.

3 El aumento de las ofertas de VPN impulsadas por IA suscitará preocupación en cuanto a la seguridad y la privacidad

En medio de los continuos avances en IA, las soluciones VPN impulsadas por IA inundarán el mercado. Sin embargo, las empresas deberían evaluar estas ofertas con cautela. Aunque prometan un mejor rendimiento, la integración de la IA amplifica los riesgos de seguridad y aumenta las oportunidades para que los atacantes aprovechen las vulnerabilidades de las VPN. Además, surgirán preocupaciones sobre la privacidad por el análisis exhaustivo de datos que aumenta el riesgo de que se exponga información confidencial.

4 Los ataques de pulverización de contraseñas a las VPN seguirán creciendo

Los atacantes encontrarán cada vez más formas de explotar las prácticas débiles de gestión de contraseñas y los perfiles de conexión VPN predeterminados no utilizados mediante ataques de pulverización de contraseñas. En estos ataques, los actores de amenazas intentan usar la misma contraseña en muchas cuentas VPN hasta que inician sesión exitosamente y obtienen acceso no autorizado. Dado que numerosas infracciones recientes de VPN de alto perfil aprovechan eficazmente esta técnica, las empresas deberían esperar que sigan dándose ataques similares.

5 El gasto empresarial pasará de concentrarse en las VPN a la conectividad zero trust

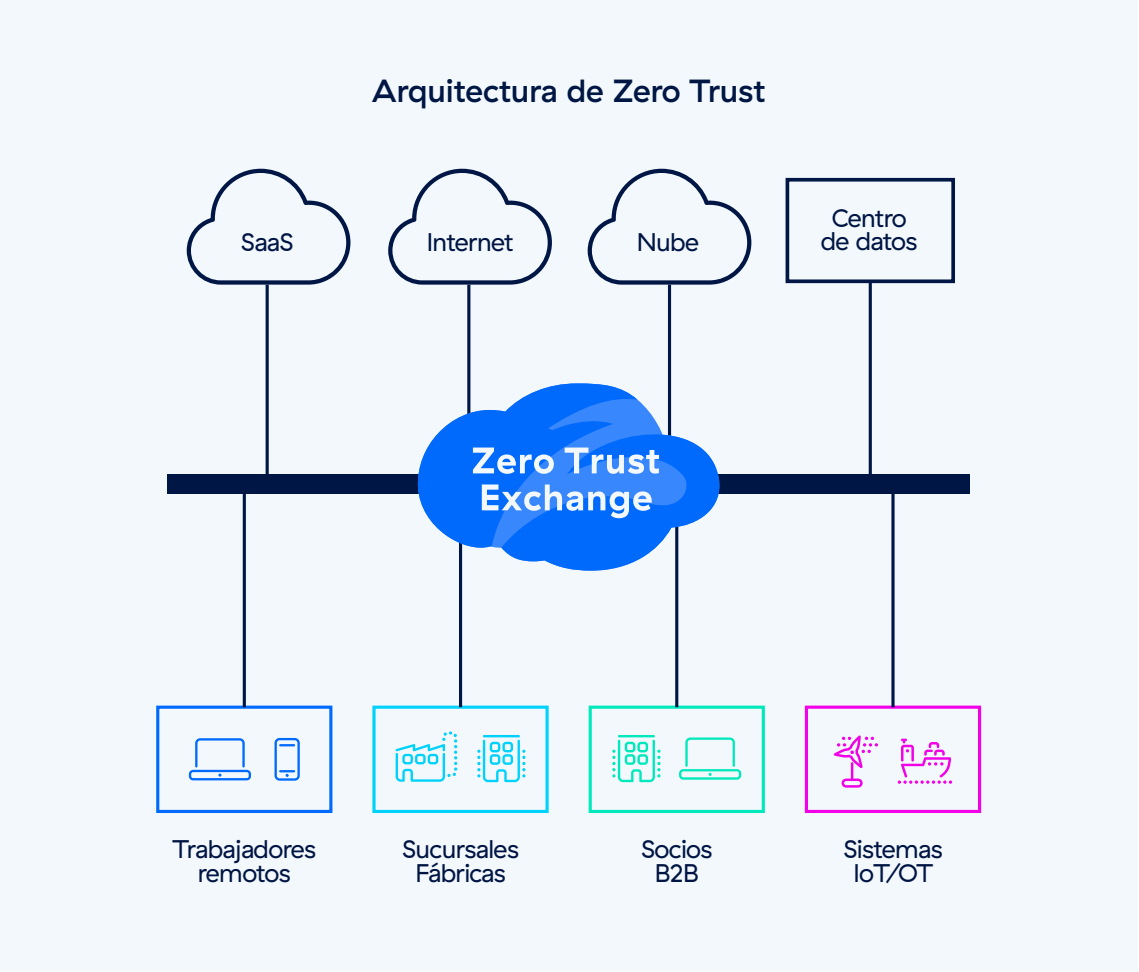
La VPN ha permitido durante mucho tiempo la conectividad remota para las empresas, pero los constantes y crecientes desafíos de seguridad de la tecnología harán que sea más difícil justificar el gasto a largo plazo. A medida que las empresas lleguen a un consenso de que zero trust es la mejor arquitectura para tener seguridad y conectividad, los presupuestos empresariales seguirán orientándose hacia iniciativas de zero trust para proteger a la fuerza laboral remota.

Cómo Zscaler hace posible que se reemplace VPN y se haga una transformación zero trust

Los cortafuegos tradicionales y las VPN crean una superficie de ataque masiva que permite a los atacantes ver y explotar los recursos expuestos. Al colocar a los usuarios en la red y permitirles acceder a cualquier aplicación que aloje, estos enfoques heredados brindan a los atacantes un fácil acceso a datos confidenciales. Hacen que proporcionar acceso o compartir recursos con proveedores externos, contratistas y agencias de forma segura sea un desafío y requiera mucho tiempo. Además de eso, incrementan los costes y la complejidad, y son demasiado lentos para atender al personal remoto actual.

La plataforma Zscaler Zero Trust Exchange™, la nube de seguridad en línea más grande del mundo, conecta de forma segura a usuarios, cargas de trabajo, IoT/OT y socios B2B sin ampliar el acceso a la red.

Zscaler Private Access™ (ZPA™), una parte esencial de Zero Trust Exchange, proporciona acceso directo a aplicaciones privadas que están ocultas detrás de Zero Trust Exchange para minimizar la superficie de ataque, conseguir una segmentación granular 1:1 de usuario a aplicación, eliminar el movimiento lateral y brindar protección de aplicaciones privadas e inspección del tráfico en línea mientras se detienen las amenazas de día cero. En resumen, su postura de seguridad se lleva a otro nivel. Como servicio nativo en la nube, ZPA puede implementarse en cuestión de horas para sustituir a las herramientas de acceso remoto heredadas, como la VPN y VDI.



Redes de confianza cero

ZPA permite un acceso granular y segmentado con conectividad de dentro hacia afuera a aplicaciones y cargas de trabajo privadas. Además, ZPA incluye un conjunto integral de servicios de control de acceso, incluida la segmentación de usuario a aplicación impulsada por IA (con recomendaciones automatizadas para políticas de acceso de usuarios y segmentos de aplicaciones), segmentación de carga de trabajo a carga de trabajo, acceso remoto privilegiado, perímetro de servicio privado o acceso al navegador, entre otros.

Protección contra amenazas cibernéticas

ZPA ofrece capacidades avanzadas de ciberprotección para proteger su organización. Entre ellas, capacidades de protección de aplicaciones que utilizan inspección de seguridad en línea para detener los ataques de aplicaciones más frecuentes y las vulnerabilidades de día cero, así como tecnología de engaño que atrae a los atacantes con aplicaciones señuelo y facilita la detección de amenazas sofisticadas.

Protección de datos

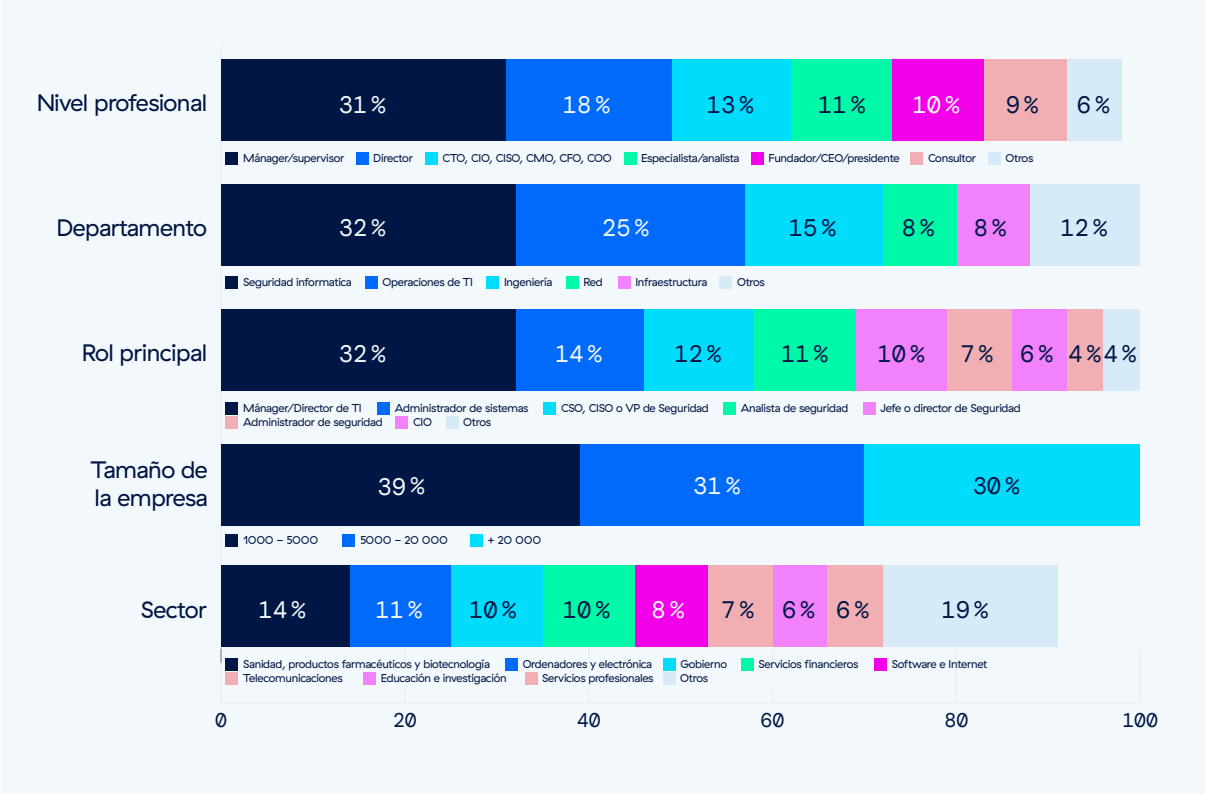
ZPA proporciona protección integral de datos y detiene la pérdida de estos en todos los canales con prevención de pérdida de datos (DLP) web, DLP de puntos finales y aislamiento del navegador, que evita la fuga de datos para usuarios vulnerables y puntos finales de tipo BYOD.

Mejores prácticas para contrarrestar los riesgos de VPN

- **Minimice la superficie de ataque:** proporcione acceso directo a las aplicaciones para garantizar que tanto las aplicaciones como los usuarios sean invisibles para Internet. De esta manera, se evita de manera efectiva que los atacantes los descubran y exploten para obtener acceso inicial.
- **Evite el compromiso inicial:** inspeccione todo el tráfico en línea para detener automáticamente las vulnerabilidades de día cero, el malware y otras amenazas sofisticadas.
- **Bloquee el acceso no autorizado:** utilice una autenticación multifactor (MFA) fuerte, como contraseñas o tókenes de un solo uso, datos biométricos o credenciales FIDO2 para validar las solicitudes de acceso de los usuarios. Por otro lado, la MFA débil a menudo se basa en enfoques que utilizan preguntas para restablecer la contraseña.
- **Aplique el acceso con privilegios mínimos:** restrinja los permisos para usuarios, tráfico, sistemas y aplicaciones según la identidad y el contexto para garantizar que solo los usuarios autorizados puedan acceder a los recursos aprobados (lo que proporciona seguridad adicional en casos de compromiso de MFA o robo de credenciales).
- **Elimine el movimiento lateral:** conecte a los usuarios directamente a las aplicaciones, no a la red, para limitar el radio de explosión de un posible incidente y mitigar el riesgo de movimiento lateral de amenazas.
- **Quite el acceso a los usuarios comprometidos y las amenazas internas:** habilite la inspección y la supervisión en línea para detectar usuarios comprometidos con acceso a su red, aplicaciones privadas y datos.
- **Detenga la pérdida de datos:** inspeccione los datos en movimiento y en reposo para detener el robo de datos activo durante un ataque.
- **Implemente defensas activas:** aproveche la tecnología de engaño y sus señuelos y busque amenazas a diario para frustrar y capturar ataques en tiempo real.
- **Ponga a prueba su postura de seguridad:** haga evaluaciones periódicas de riesgos con terceros y lleve a cabo actividades de purple team para identificar y reforzar las brechas en su programa de seguridad. Solicite a sus proveedores de servicios y socios tecnológicos que hagan lo mismo y comparta los resultados de estos informes con su equipo de seguridad.

Metodología y demografía

Este informe se basa en los resultados de una exhaustiva encuesta en línea realizada a 647 profesionales de la informática y la ciberseguridad, llevada a cabo en abril de 2024, para identificar las últimas tendencias de adopción por parte de las empresas, los retos, las carencias y las preferencias de soluciones relacionadas con el riesgo de las VPN. Entre los encuestados hay desde ejecutivos técnicos hasta profesionales de seguridad de TI, que representan una sección transversal equilibrada de organizaciones de diferentes tamaños en múltiples sectores.



Acerca de Zscaler

Zscaler 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 ubicados 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 línea en la nube del mundo. Si desea más información, visite www.zscaler.es.

Acerca de ThreatLabz

ThreatLabz es la división de investigación de seguridad de Zscaler. Este equipo de clase mundial es responsable de localizar nuevas amenazas y asegurar que las miles de organizaciones que utilizan la plataforma global de Zscaler estén siempre protegidas. Además de investigar el malware y analizar el comportamiento, los miembros del equipo participan en la investigación y el desarrollo de nuevos módulos prototipo para la protección contra amenazas avanzadas en la plataforma Zscaler y realizan regularmente auditorías de seguridad internas para garantizar que los productos y la infraestructura de Zscaler cumplen con los estándares de cumplimiento de seguridad. ThreatLabz publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal, research.zscaler.com.

Acerca de Cybersecurity Insiders

Cybersecurity Insiders reúne a más de 600 000 profesionales de seguridad de TI y proveedores de tecnología de clase mundial para facilitar la resolución inteligente de problemas y la colaboración para abordar los desafíos de ciberseguridad más críticos de la actualidad.

Nuestro enfoque se centra en crear y organizar contenido único que eduque e informe a los profesionales de ciberseguridad sobre las últimas tendencias, soluciones y mejores prácticas de ciberseguridad. Desde estudios de investigación integrales y revisiones imparciales de productos hasta guías electrónicas prácticas, seminarios web atractivos y artículos educativos, estamos comprometidos a proporcionar recursos que brinden respuestas basadas en evidencia a los complejos desafíos de ciberseguridad de la actualidad.

Póngase en contacto con nosotros hoy para saber cómo Cybersecurity Insiders puede ayudarle a destacarse en un mercado saturado y aumentar la demanda, la visibilidad de la marca y la presencia de liderazgo intelectual.

Envíenos un correo electrónico a info@cybersecurity-insiders.com o visite cybersecurity-insiders.com.

Experimente su mundo, protegido.

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 los usuarios, dispositivos y aplicaciones ubicados 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 línea en la nube del mundo. Si desea más información, visite **www.zscaler.es**.

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