5

PASOS PARA UNA EXITOSA

MIGRACIÓN DE VPN A ZTNA

Las empresas se dan cuenta de que es hora de aumentar o reemplazar sus redes privadas neutrales (VPN). Esta tecnología de hace décadas no está diseñada para lidiar con los desafíos de seguridad de hoy en día de una mano de obra distribuida internacionalmente y un ecosistema de amenazas en aumento. Zero Trust Network Access (ZTNA) es el estándar de la industria moderna para el acceso seguro a lo que sea desde donde sea y por quien sea. Aunque muchas empresas entienden su valor, la realidad de migrar de la tecnología VPN puede parecer abrumadora. Este eBook brinda una guía sobre los cinco pasos que las organizaciones pueden adoptar para hacer una transición exitosa de VPN a ZTNA, incluyendo las prácticas óptimas para minimizar la perturbación de las operaciones.

TABLA DE CONTENIDOS

Introducción

Los equipos de TI y seguridad se dan cuenta de que es hora de potenciar las estrategias de acceso remoto aumentando o reemplazando su VPN. Este cambio de mentalidad surge de la necesidad de abordar un aumento significativo de trabajadores remotos, iniciativas de transformación digital aceleradas y un panorama avanzado de amenazas. Las VPN son cada vez más deficientes e inmanejables en el ecosistema TI actual, lo que resulta en mayores riesgos y complejidades. ZTNA es una solución óptima para combatir estos defectos inherentes a la VPN. Sin embargo, abandonar la VPN puede parecer abrumador, ya que las grandes inversiones a lo largo de los años la han arraigado profundamente a la estrategia de seguridad.

Este eBook explica cómo migrar sin problemas de VPN a ZTNA con un enfoque incremental de cinco pasos que no interrumpe las operaciones comerciales, reduce el riesgo y lo prepara para el éxito a largo plazo:

1. Comprenda su ecosistema VPN
2. Desarrolle su hoja de ruta ZTNA
3. Comience
4. Implemente su primer caso de uso
5. Amplíe su implementación de ZTNA

Este enfoque gradual de ZTNA fortalece y simplifica los controles de acceso sin interrumpir sus operaciones comerciales.

Limitaciones de las VPN: No aptas para los desafíos de seguridad modernos

Introducida a mediados de los 90 como una solución de acceso remoto, la arquitectura VPN ya quedó anticuada. Varias agencias del gobierno de EE. UU., incluyendo la Agencia de Seguridad Nacional (NSA), ha emitido advertencias sobre vulnerabilidades de VPN. Nunca fueron diseñadas para usarse con una infraestructura TI híbrida y con una mano de obra dispersada internacionalmente.

INTRÍNSECAMENTE INSEGURA

Uno de los problemas de seguridad más graves de VPN se centra en torno a los puertos abiertos. Sin excepción, cada concentrador VPN se despliega de tal manera que tiene una presencia en Internet con un puerto abierto de escucha continua. Los agentes maliciosos buscan e ingresan en las redes a través de estos puertos abiertos, inevitablemente moviéndose lateralmente para alcanzar y explotar a sus objetivos.

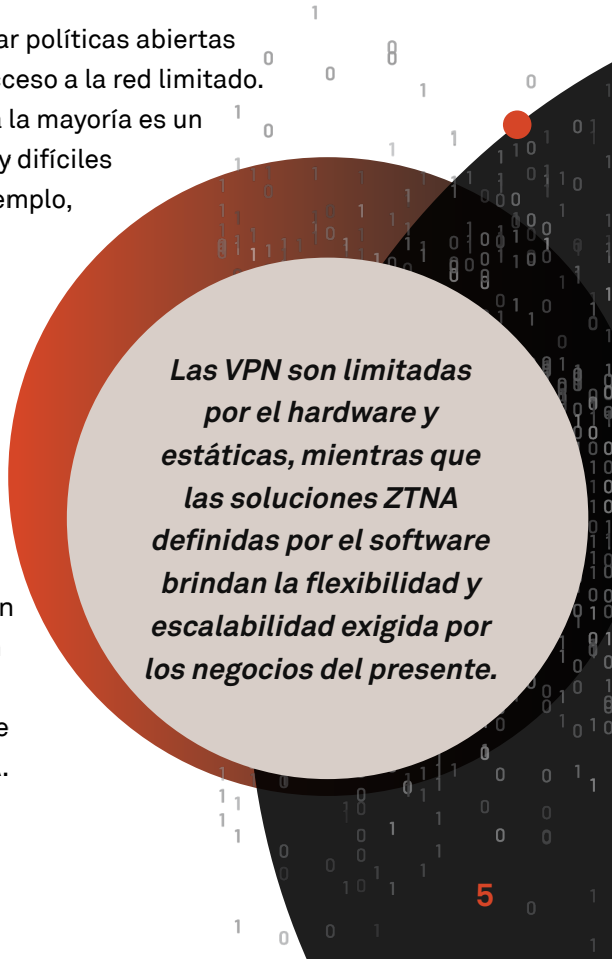
El método de autenticación TCP/IP utilizado por las VPN es otra zona de debilidad. La mayoría de las VPN basan el acceso "confiable" en la dirección IP del usuario. Es sencillo obtener/adquirir un conjunto válido de credenciales de acceso a través de la ingeniería social, phishing, smishing, sitios web falsos... la lista sigue. Incluso los códigos de verificación de autenticación de dos factores son sencillos de capturar. Hay millones de credenciales de acceso robadas en venta al mayor postor en la Dark Web. Una y otra vez, este enfoque heredado a la autenticación es fácilmente manipulado por agentes maliciosos y es un error absoluto considerando la enorme cantidad de datos contextuales disponibles para validad la identidad de usuarios.

PROBLEMAS DE COMPLEJIDAD

Los administradores VPN están obligados a tomar una decisión crucial: crear políticas abiertas para el acceso a la red generalizado o crear políticas restrictivas para un acceso a la red limitado. Esto es intrínsecamente problemático porque la decisión más sencilla para la mayoría es un acceso generalizado vs. políticas restrictivas complejas propensas al error y difíciles de gestionardada la velocidad para cambiar que requiere el negocio (por ejemplo, agilidad y transformación digital).

Todas estas cuestiones son exacerbadas por un aumento de mano de obra distribuida y la creación IP dinámica inherente al trabajo en la nube. Es realmente demasiado para gestionar eficazmente y mantener una postura de seguridad robusta a la vez.

Además, las VPN son soluciones limitadas por el hardware y compartimentadas que solo resuelven el acceso remoto. Esto las vuelve engorrosas y costosas a la hora de escalarlas mientras se inhabilita la capacidad de automatizar procesos e integrarlas con otras soluciones. Al fin y al cabo, las VPN son una solución exclusiva para el acceso remoto. Fueron diseñadas para hacer una cosa y no pueden hacerla con seguridad. Estas limitaciones técnicas y fallas en el diseño solo son una pequeña muestra de por qué usted debería considerar seriamente una migración de VPN a ZTNA.



10 RAZONES PARA DESHACERSE DE SU VPN

1. El modelo de autenticación centrado en IP de VPN es débil y carece de sensibilidad de identidad y contexto.
2. El enfoque “confiar, luego verificar” de las VPN da como resultado un ingreso a la red sencillo de hallar.
3. Las VPN fomentan el movimiento lateral dentro de una red plana, aumentando el “radio de explosión” de un ataque.
4. Las VPN carecen de la capacidad de realizar una comprobación de la postura del dispositivo como criterio para verificar la confiabilidad.
5. Los concentradores de VPN crean cuellos de botella, dando como resultado un mal desempeño y trabajadores frustrados.
6. Las VPN crean complejidades de gestión de políticas y cortafuegos.
7. Las VPN carecen de interoperabilidad con sistemas de TI, seguridad y comerciales.
8. Las VPN son caras y requieren mucho tiempo para escalar.
9. Los usuarios deben cambiar de VPN para acceder a flujos de trabajo distribuidos y heterogéneos.
10. Las VPN solo ofrecen configuraciones active-activo o activo-pasivo para redundancia, lo que limita significativamente la productividad y la escalabilidad.

“Las VPN son anticuadas, y aunque puede que tengan algún valor para un ‘arreglo’ inmediato, hay que eliminarlas.

Son recopiladores de vulnerabilidades y un blanco perfecto para ser explotados”.

Dr. Chase Cunningham, Dr. Zero Trust

ZTNA vs. VPN

ZTNA impone el acceso de "principio de mínimo privilegio" a la red que es un mandato líder de la industria. ZTNA está diseñado para las realidades de la TI de hoy en vez de las de la década de 1990. Ofrece beneficios significativos por sobre las VPN. Es como comparar el motor a vapor con el motor a combustión. Uno sirvió en su época, mientras que el otro reinó supremo porque fue diseñado con más adaptabilidad para todos los tiempos.

Estas son las diferencias clave que ZTNA tiene para ofrecer por sobre la VPN:

- **Reducción de superficie de ataque:**
  Mientras que los puertos abiertos de la VPN son fáciles de encontrar y explotar, la arquitectura ZTNA utiliza la tecnología Single Packet Authorization (SPA) para hacer que los recursos sean 100% invisibles salvo que se los autentique o se los considere una identidad confiable.

- **Autenticación centrada en la identidad:**
  ZTNA utiliza las direcciones IP como criterio para autenticar, pero llega mucho más lejos a la hora de verificar la identidad. Lo hace combinando información de cualquier repositorio de identidades e incorporando capas de variables contextuales como horario, fecha, ubicación y postura de seguridad del dispositivo.

- **Acceso de mínimo privilegio:**
  Se les otorga acceso confiable pero limitado a los usuarios y máquinas exclusivamente a los recursos necesarios para hacer sus trabajos. Y con la tecnología SPA y la microsegmentación minuciosa, los agentes maliciosos o dispositivos infectados no pueden moverse lateralmente por la red.

- **APIs programables:**
  A diferencia de la naturaleza compartimentada de la VPN, las soluciones ZTNA se integran a través de los sistemas comerciales, de TI y de seguridad para obtener una visibilidad de red aumentada y capacidades de automatización. La naturaleza definida por software de las soluciones ZTNA garantiza un escalamiento sin fisuras y simultáneo con infraestructuras dinámicas.

ZTNA y SDP

El modelo ZTNA originalmente se conocía como perímetro definido por software (SDP). Los nombres se pueden usar indistintamente y hacen referencia a una postura de seguridad de acceso a la red renovada y más robusta.

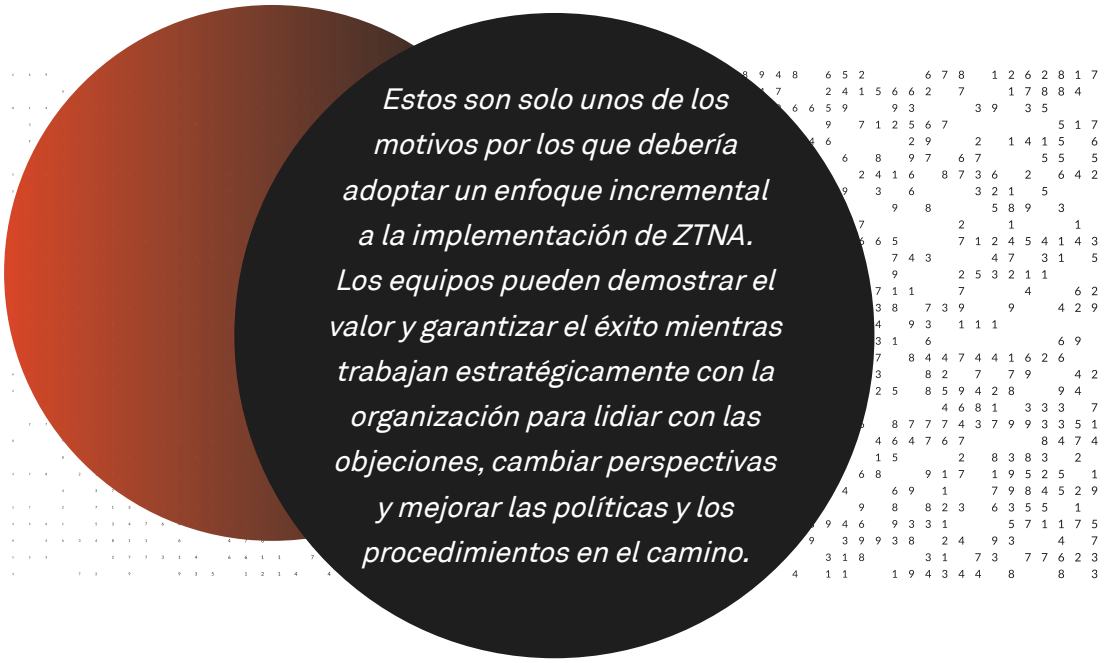
¿QUIERE SABER MÁS?

Lea *Zero Trust Network Access: Todo lo que necesita saber*

DESCÁRGUELO AHORA

LIMITACIONES DE VPN VS. VENTAJAS DE ZTNA

VPN	ZTNA
Centrado en la res: Modelo “confiar, luego verificar” basado en una relación IP-a-puerto simple.	**Centrado en la identidad:** Modelo “verificar, luego confiar” basado en la identidad, el contexto y los perfiles multidimensionales.
Puertos abiertos: Acceso de usuario típicamente generalizado a la red autenticada, permitiendo movimiento lateral sin control.	**Infraestructura oculta:** Los usuarios autorizados acceden solamente a recursos aprobados, ocultando todo lo demás para evitar el movimiento lateral.
Limitado por hardware: Engorroso de implementar; estático y difícil de escalar a medida que cambiar la infraestructura.	**Definido por software:** Elástico y escalable por todos los ambientes híbridos a través de integraciones API.
Cambiar de VPN: El acceso de los usuarios a múltiples recursos suele requerir cambiar de una VPN a otra construida sobre plíticas complejas proclives al error.	**Conexiones simultáneas:** Les permite a los usuarios accede a múltiples segmentos de red y recursos digitales a través de un solo puerto de conexión.
Compartimentado y estático: Solo aplicable a acceso de usuarios remotos: incapaz de asegurar a usuarios o redes in situ.	**Flexible y dinámico:** Versátil y ampliable, trascendiendo los usuarios remotos para brindar un acceso unificado y seguro para todos.



Superando las objeciones contra migrar a ZTNA

El deseo de proteger las inversiones y decisiones existentes suele ser una fuerza motriz detrás de por qué las organizaciones no quieren avanzar con un plan de migración a ZTNA. La realidad es que no hace falta hervir el océano de una vez. Se puede mejorar la avejentada tecnología de seguridad y hacer un plan de migración por etapas que brinde mejoras a lo largo del tiempo.

GASTOS IRRECUPERABLES

Las VPN están arraigadas a las estructuras tecnológicas en todo el mundo, así que la resistencia al cambio es común. Para muchos, la mayor objeción es simplemente que ya se hizo la inversión en la tecnología actual. Típicamente, las VPN representan una gran cantidad de gastos irrecuperables, y sus departamentos de IT/seguridad probablemente estén reticentes a tener discusiones de "arrancar y reemplazar" a gran escala. De hecho, en una encuesta reciente que realizamos a más de 500 profesionales de "infosec", el mayor factor detrás de la toma de decisiones era el deseo de sentirse seguros respecto a las inversiones previas en tecnología. A la vez, ponderaron a una tecnología que cree conexiones rápidas y seguras entre usuarios y aplicaciones como el criterio más importante a la hora de adquirir tecnología. Lamentablemente, las VPN fallan en esa área.

Recomendamos una estrategia de migración de VPN a ZTNA incremental que resuelve ambos factores. Para empezar, desvíe el presupuesto destinado a las nuevas iniciativas de acceso seguro de las VPN – u otras tecnologías avejentadas – a una solución ZTNA. Otro camino es reemplazar las VPN que requieren una actualización de hardware onerosa.

LO CONOCIDO VS. LO DESCONOCIDO

Las VPN son elementos conocidos, y los usuarios finales están acostumbrados a trabajar con y a pesar de ellas. Recapacitar al personal y recibir llamadas de servicio técnico pueden ser objeciones iniciales a adoptar ZTNA, pero son efímeras comparadas con los beneficios, que incluyen una complejidad reducida, una experiencia de usuario mejorada y beneficios en el rendimiento. Surgido de una filosofía de seguridad Zero Trust, hay un argumento claro a favor de los beneficios operativos conseguidos a través de las soluciones ZTNA.

SOBRECARGA DE SOLUCIONES

Hay una objeción natural que los agregados a la estrategia de seguridad podrían crear un exceso vs. consolidación. Pero el ZTNA de hecho reduce la dependencia en las soluciones VPN, NAC y cortafuegos sin requerir un "arrancar y reemplazar". Eso es debido a la extensibilidad de una superposición de plataforma de acceso privada única con un motor de políticas centralizadas que resuelven las limitaciones de acceso seguro de estas herramientas heredadas. Así que se puede reducir el número de reglas de cortafuegos para gestionar; acabar con las nuevas inversiones en soluciones VPN y reducir los cuellos de botella de los concentradores VPN; y eliminar futuras instalaciones complejas y caras de NAC. Estos beneficios operativos significan que sus sobrecargados equipos de seguridad e TI pueden concentrarse en iniciativas comerciales relevantes en vez de en tareas mundanas de gestión de políticas intrínsecas a las herramientas de seguridad de red heredadas.

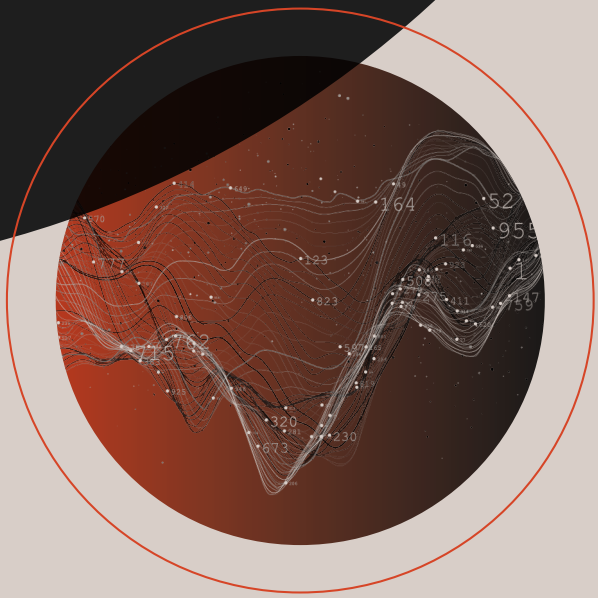
STATUS QUO VS. CHANGE

Otras posibles objeciones incluyen una falta de conciencia sobre los ciber-riesgos asociados con las VPN y el miedo de perturbar el negocio con la implementación de nueva tecnología. Puede contrarrestarlas gugleando "CPN CVE" para encontrar los últimos titulares relacionados a las vulnerabilidades críticas de VPN, o encuestando a su equipo TI o a los empleados en general con respecto a las solicitudes de asistencia técnica y los problemas de gestión de políticas relacionadas a la gestión de VPN. La perturbación ya está allí y debe ser erradicada para alcanzar una mayor eficiencia y una postura de seguridad más robusta y flexible.

Pasos de migración de VPN a ZTNA

Empezar puede ser la parte más difícil del camino al Zero Trust. Pero si usted empieza de a poco, piensa en grande y escala en el camino, el proceso se vuelve más manejable. Empiece entendiendo su ecosistema VPN actual, luego evalúelo en función de las metas de la empresa y las áreas de riesgo grave. Cuando emerja la hoja de ruta, los equipos pueden identificar y priorizar los casos de uso. A partir de allí, un plan por etapas puede surgir tan rápida y metódicamente como lo desee su organización.

1. Entienda su ecosistema VPN
2. Desarrolle su hoja de ruta ZTNA
3. Comience
4. Implemente su primer caso de uso
5. Amplíe su implementación de ZTNA



1

ENTIENDA SU ECOSISTEMA VPN

Su evaluación de base de la VPN le ofrece una imagen complete de cómo funcionan las VPN dentro de su organización mientras consideran todas las influencias técnicas, organizativas y económicas.

Cada organización tiene su propia configuración e implementación de VPN única. Antes de considerar la migración ZTNA, debe tener una noción clara de su ecosistema VPN existente. Si no existe un mapa de su estructura VPN, este es un excelente momento para crearlo para ver dónde se usan los VPN... por aplicación, segmento de red y grupo de usuarios.

Una evaluación de base de la VPN debería detallar cómo se integran sus VPN a su estrategia de tecnología. Define qué activos digitales deben ser asegurados y cómo hacerlo, y considera los requisitos tecnológicos, organizativos y económicas.

En paralelo, es aconsejable determinar qué grupos de usuarios tienen acceso a los datos más sensibles y representan el mayor riesgo a su compañía si se ven comprometidos. Esto ayuda a identificar puntos débiles y cómo lidiar con ellos antes de que se vuelvan un problema mayor. Por ejemplo, en vez de realizar una implementación ZTNA total para todos los trabajadores remotos a la vez, es prudente probar ZTNA con un grupo de usuarios menor que representen un riesgo de seguridad alto. Luego de tener éxito y reducir la postura de riesgo dentro de ese grupo, puede ampliarlo a la población de usuarios general.

2 DESARROLLE SU HOJA DE RUTA ZTNA

El siguiente paso es determinar su destino final y desarrollar la hoja de ruta ZTNA para llegar a él. Es fundamental considerar el estado final de seguridad Zero Trust que desea su organización, incluyendo la estrategia a largo plazo. Recuerde que el ZTNA es mucho más extensible que la VPN – y es solo un punto de partida natural. Su hoja de ruta puede extenderse más allá de simplemente resolver el acceso remoto para englobar el panorama de acceso de red general. En definitiva, usted puede brindarles acceso seguro a todos los usuarios, dispositivos y flujos de trabajo independientemente de dónde residan.

ZTNA admite muchos otros casos de uso más allá del acceso remoto, así que las prioridades dependen completamente de los objetivos, riesgos y posturas de seguridad deseadas de su organización.

OTROS CASOS DE USO COMUNES DE ZTNA:

- **MIgración en la nube:**
  Mudar aplicaciones y datos a la nube – o múltiples nubes – efectivamente transforma a todos los usuarios en usuarios remotos, pero con algunas diferencias claves. ZTNA escala automáticamente con las resoluciones dinámicas de las IP asociadas con los flujos de trabajo en la nube, resultando en derechos de acceso dinámicos a través de ambientes multinube sin intervención manual.

- **Accesos DevOps seguros:**
  Los equipos DevOps requieren acceso remoto a activos digitales sensibles alojados en ambientes multinube e in situ, lo que puede generar fricción y riesgo dentro de las capacidades limitadas de la VPN. ZTNA puede liberar a los DevOps de esas limitaciones brindando acceso simultáneo a varios ambientes de nube acompañados por el ancho de banda y rendimiento que los desarrolladores necesitan para hacer su trabajo. Esto también brinda una oportunidad una oportunidad única para explorar las capacidades de automatización usando las prestaciones de metadatos e integración (por ejemplo, con gestión de servicios TI.

- **Acceso de terceros:**
  Los terceros, como los proveedores, contratistas y socios comerciales, pueden exponer fácilmente a su empresa a los riesgos asociados con el acceso sobre privilegiado. Los terceros son invariablemente de naturaleza remota, así que muchas organizaciones dependen de las VPN para gestionar su acceso. ZTNA puede otorgar acceso confiable a usuarios externos sin arriesgarse a exponerlos a recursos no autorizados.

- **Máquina a máquina (M2M):**
  Las soluciones ZTNA más robustas pueden utilizar los mismos principios Zero Trust aplicados a los usuarios a las conexiones M2M. Esta es solo otra forma que tiene el ZTNA de reducir la superficie de ataque, porque frustra el movimiento lateral si una máquina se ve comprometida.

- **Interconexión estilo café:**
  Este es el objetivo final de ZTNA... una amalgama de todos los casos de uso que dé como resultado un modelo de política unificada para todos los usuarios, redes, flujos de trabajo y dispositivos. Básicamente elimina la necesidad de tener diversos modelos de acceso al trabajar remotamente o en una oficina independientemente de conectarse a la nube o flujos de trabajo in situ.

Al utilizar API enriquecidas, ZTNA puede integrarse y automatizarse con los sistemas comerciales, de seguridad y de TI existentes, lo que la convierte en una solución ideal para todos sus casos de uso de acceso a la red. Estas capacidades deben tenerse en cuenta en la hoja de ruta, ya que la automatización y la eficiencia operativa probablemente se convertirán en demandas comerciales estratégicas.

3 COMIENCE

Ahora solo queda el detalle de elegir un proveedor ZTNA para poder abordar su primer caso de uso ZTNA. Debe considerar varias arquitecturas y funciones que cumplan con los requisitos actuales y futuros para evitar un cambio de proveedor en el camino o la incorporación de una segunda solución ZTNA a una estrategia tecnológica ya abarrotada.

Los factores clave para elegir un proveedor ZTNA incluyen:

- Capacidad de gestionar todos los protocolos, no solo las aplicaciones web
- Dependencias de latencia, cumplimiento y seguridad para ambientes de nube multiusuario
- Capaz de funcionar en ambientes heterogéneos
- Flexibilidad para escoger opciones de implementación, como ZTNA como-servicio o auto-alojado
- Capacidad para proteger el tráfico de red este-oeste y norte-sur
- Prestaciones de integración para automatizaciones futuras
- Capaz de gestionar repositorios de identidades múltiples y variables
- Capacidad para brindar un modelo de políticas unificado que incluye IoT y sucursales seguras

Cuando haya elegido su solución ZTNA ideal, es hora de implementarla:

- **Selección de infraestructura – escoja entre:**
  - Soluciones ZTNA autoalojadas que requieren una implementación ligera para portales y controladores (motor de políticas unificado); o
  - Soluciones ZTNA “como-servicio” que pueden implementarse rápidamente y reducir la necesidad de soporte técnico completo al depender del hosting en la nube del proveedor
- **Creación de políticas:**
  - Su repositorio de identidades debe estar unificado para grupos de usuarios debido al enfoque centrado en la identidad de ZTNA para la creación de políticas. Entonces, su proveedor ZTNA debe soportar múltiples y distintos proveedores de identidades. Entonces usted puede establecer unas pocas políticas simples que pueden incluir contexto basado en riesgo como hora, fecha, ubicación, MFA, etc.
- **Incorporación de usuarios:**
  - Su primer caso de uso y grupo de usuarios determinará si necesita un cliente instalado para la comprobación de postura de dispositivos y soporte de protocolo o un acceso por navegador para las aplicaciones web. Una solución ZTNA que pueda manejar ambas es ideal, así puede elegir en casos futuros.
- **Automatización:**
  - Decida dónde la automatización reducirá la complejidad, mejorará la agilidad y facilitará las tareas administrativas, que pueden incluir automatizar la integración con un sistema ITSM, MFA o de soporte comercial.

También es importante planificar para medir el éxito. Considere rastrear las tasas satisfacción y adopción de los usuarios, la disminución de llamados de soporte y otros puntos para validad cómo ZTNA apoya sus metas comerciales. Otros parámetros pueden incluir beneficios de productividad de los usuarios y TI, reducción de reglas de puertos abiertos y cortafuegos, o la comparación de tiempo de instalación de ZTNA vs VPN. Medir y reportar los resultados de los primeros casos de uso a las partes interesadas claves despejará el camino para el paso final.

4 IMPLEMENTE SU PRIMER CASO DE USO

Comience tomando un trozo pequeño de su primer caso de uso más natural, que, como ya se dijo, es la migración de VPN a ZTNA. Aunque no hay ningún punto de lanzamiento "correcto" o predefinido, estos son algunos puntos a considerar al actualizar su acceso remoto de seguridad con ZTNA:

- **Mitigación de riesgos:**
  Una pregunta natural es "¿Dónde reside el mayor riesgo asociado con el acceso VPN?". Podría ser un subconjunto de usuarios privilegiados que tocan recursos sensibles regularmente. Este caso se trata de implementar medidas preventivas y cómo evitar la naturaleza costosa de una vulneración, que promedia en $1,52 millones por incidente, según el Informe 2020 de costos por vulneración de datos de Ponemon.

- **Beneficios de productividad:**
  Otro punto lógico para empezar a entender dónde puede ganar eficiencia operativa. Puede ser un gran subconjunto de usuarios frustrados sufriendo las fallas de VPN, como cuellos de botella y problemas de rendimiento, dando como resultado un aumento en llamados al servicio técnico y cargas administrativas. Y luego están sus desarrolladores y DevOps, que requieren el acceso correcto a recursos híbridos en el momento justo para cumplir en un entorno de aplicaciones aceleradas.

- **Ciclo presupuestario:**
  Este es un excelente momento para comenzar su migración de VPN a ZTNA. Una actualización importante de hardware VPN planeada en un ciclo presupuestario presenta una oportunidad para un diálogo de acceso seguro de "reemplazo vs actualización". Las renovaciones de software VPN y su expiración de mantenimiento ofrecen una oportunidad atractiva similar para reevaluarlo.

- **Nuevas iniciativas:**
  Las nuevas iniciativas de transformación digital o proyectos de migración a la nube también son una oportunidad primordial para adoptar ZTNA. Asociarse con unidades empresariales para acelerar estas iniciativas – sin sacrificar, sino más bien fortaleciendo la seguridad – transforma a ZTNA en un catalizador para la transformación digital.

5 AMPLÍE SU IMPLEMENTACIÓN ZTNA

Luego de que el primer caso de uso haya demostrado su éxito, puede ampliar la implementación ZTNA en empresas más grandes. Debido a que la solución está definida por el software, es sencillo seguir la hoja de ruta con todos los usuarios y flujos de trabajo. Simplemente agregue más portales, define nuevas políticas e incorpore a más usuarios.

Idealmente, el proceso de ampliación se moverá horizontal y verticalmente. La ampliación horizontal agrega más usuarios. La ampliación vertical cubre nuevos casos de uso e incorpora integración y automatización. Cómo se haga y cuán rápido se complete dependerá de su hoja de ruta. Las soluciones ZTNA pueden moverse tan rápido o tan lento como usted requiera.

La ampliación puede englobar casos como DevOps, migración a nube, servidor-a-servidor (por ejemplo, tráfico este-oeste), dispositivos IoT o una red tipo café a toda máquina. Una ampliación exitosa depende de mantener unificado y centralizado el motor de políticas. Las soluciones ZTNA que ofrecen una implementación y opciones de acceso flexibles le permite mantener un enfoque unificado, realizando pequeños ajustes estructurales para cumplir con todos los casos de uso. Por ejemplo, los proveedores externos tal vez no permitan la instalación de un cliente en sus terminales. Sin embargo, una solución ZTNA multifunción habilitará permisos mínimos desde navegadores externos sin requerir una nueva solución o una Interfaz gráfica de usuario para gestionar políticas.

Finalmente, a medida que madure su implementación, puede destrabar más funciones para su solución, que pueden incluir:

- **Políticas automatizadas:**
  Aproveche los datos de los sistemas de identidad y de directorio y metadatos ambientales para crear o extender políticas y derechos de acceso de forma dinámica

- **Infraestructura automatizada:**
  Controle, construya y gestione la infraestructura- como-código con terraform, el operador GitGub SDP

- **Orqueste flujos de trabajo:**
  Intégrelo con los sistemas de operación empresarial o de soporte comercial existentes, como las plataformas de gestión de servicio TI o servicio técnico

- **Potencie la comprobación de posturas:**
  Intégrelo con soluciones para puntos de conexión para garantizar un análisis de “dispositivo confiable” o comportamiento de usuarios para garantizar un criterio de acceso de “usuario confiable” como riesgo

- **Haga que los datos trabajen:**
  Lleve la actividad detallada de registro de acceso a otras herramientas y extraiga la inteligencia como criterio de acceso de otras herramientas, como TIP, SIEM y UEBA

Simplifique la migración con la solución ZTNA de Appgate

Appgate ha ayudado a cientos de clientes a hacer el cambio de VPN a ZTNA. Somos reconocidos por nuestra experiencia líder del sector en hacer que las empresas hagan la transición sin problemas al SDP de Appgate, la mejor solución en s clase que ha pasado la prueba de la migración de VPN a ZTNA muchas veces.

LA SDP de Appgate brinda una gama complete de funcionalidades de seguridad ZTNA para todos los usuarios, dispositivos y cargas de trabajo híbridas:

- **Superficie de ataque reducida** al ocultar puertos, flujos de trabajo y aplicaciones salvo que el usuario esté autorizado a accederlos.
- **Permisos de acceso condicionales** para verificar la identidad del usuario basados en indicadores específicos del contexto como fecha, puesto, ubicación, postura del dispositivo, etc.
- **Microsegmentación avanzada** que limita la autorización a la redes o flujos de trabajo protegidos y está definida por derechos de acceso dinámicos que se ajustan a medida que el contexto del usuario y el dispositivo cambia.
- **Gestión de políticas mejorada** al reducir la complejidad con una sola estructura para todos los usuarios, dispositivos, redes e infraestructuras para tener una experiencia de acceso unificada con una configuración consistente entre TI heterogéneas.
- **Conexiones simultáneas** que potencian la experiencia del usuario y que soportan accesos directos simultáneos para todos los recursos de nube, SaaS e in situ autorizados.

"La arquitectura Zero Trust de Appgate les permitió a todos nuestros empleados trabajar de forma remota desde la seguridad de sus casas manteniendo el mayor nivel de seguridad exigido por nuestros clientes".

– Chris Edwards, Fundador y CEO, The Third Floor

"La SDP de Appgate nos simplifica un montón de cosas... Pudimos rebajar nuestras políticas de cortafuegos de unas 50 políticas a las actuales dos o tres".

– Deryk Motietall, Gerente general de infraestructura, WW

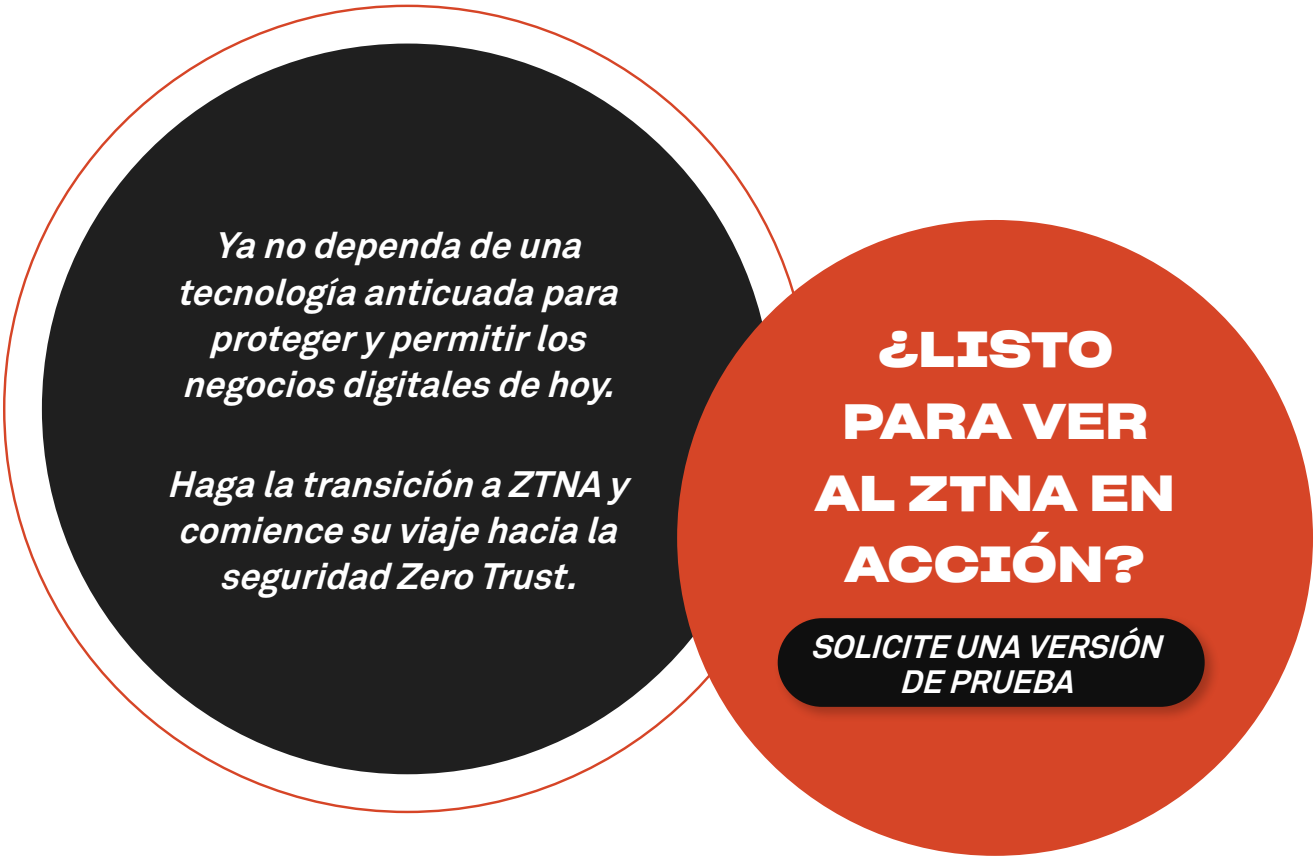
"Como proveedor de servicios gestionados, nuestros clientes confían en nosotros para proteger sus datos. Siempre estamos en busca de mejorar nuestra postura de seguridad. El SDP de Appgate nos ayudó a alcanzar esa meta".

– Matthew Staver, CTO, Verdant Services

Haga la transición a ZTNA

Llegó la hora de reemplazar o aumentar su VPN heredado con la supremacía de seguridad moderna de ZTNA. El panorama de ciberamenazas cada vez más sofisticadas – combinado con los modelos de negocios trabaja-desde-donde-sea – hace que sea fundamental.

Comience de a poco pero piense en grande en términos de metas de seguridad a largo plazo. Al comenzar con un caso de uso ZTNA abarcable, sus equipos de TI y seguridad pueden aprovechar su conocimiento y experiencia para una implementación incremental en toda la empresa. Esto garantiza el apoyo de las partes interesadas, mayor adaptación de los usuarios y una mínima interrupción de las operaciones.



Acerca de Appgate

La SDP de Appgate es una solución de Acceso de Red Zero Trust líder que simplifica y fortalece los accesos de control para todos los usuarios, dispositivos y flujos de trabajo. Nosotros les brindamos acceso seguro a empresas complejas e híbridas, frustrando amenazas complejas, reduciendo costos y potenciando la eficiencia operativa.

El conjunto completo de las soluciones y servicios Appgate protege a más de 650 organizaciones entre empresas del gobierno, Fortune 50 e internacionales. Comience su viaje de acceso seguro con seguridad visitando **www.appgate.com**.