Proceso de sustitución de las VPN:

Conoce cuándo y cómo las empresas sustituyen sus VPN obsoletas

Conectividad segura, ágil y preparada para el futuro

74% de las organizaciones reducirán el hardware reemplazando la VPN por ZTNA

Las VPN enfrentan cada vez más vulnerabilidades, y las organizaciones tienen dificultades con respecto a tres desafíos principales:

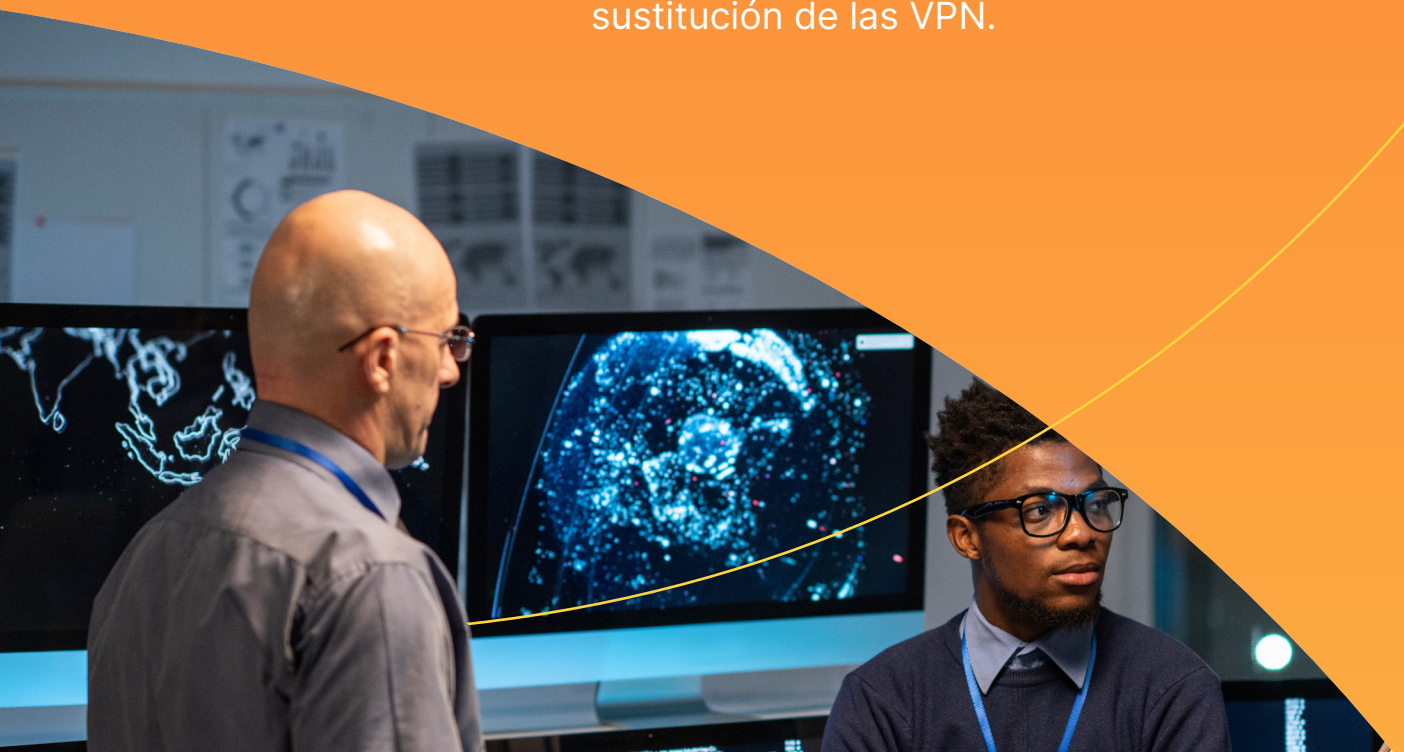
44% de los empleados a tiempo completo son usuarios híbridos o remotos.

27% de los usuarios que acceden a los recursos internos son usuarios de terceros.

50% de los empleados acceden a los recursos internos desde dispositivos no administrados.

Fuente: Enterprise Strategy Group custom research commissioned by Cloudflare, "Considerations for Implementing Zero Trust for the Workforce," julio de 2024.

Si bien las vulnerabilidades de las VPN son bien conocidas, aún hay un exceso de confianza a la hora de adoptar una alternativa Zero Trust. Sin embargo, debido al riesgo cada vez mayor para la seguridad y que la experiencia del usuario final sufre más que nunca las consecuencias, ha llegado el momento de establecer una alineación interna y de definir un plan para la sustitución de las VPN.



Introducción

Las VPN operan muy por encima de su capacidad original. Además, representan un riesgo para la seguridad y causan mayores ineficiencias para las empresas, desde las PYMES hasta las grandes empresas. Ante los cambios de los hábitos de trabajo y la proliferación de aplicaciones y dispositivos, ahora los empleados trabajan mucho más allá de los límites del perímetro de red tradicional. Eso supone complicaciones constantes para los integrantes de los equipos que se encargan de la seguridad y la conectividad (donde los roles pueden abarcar diversas responsabilidades, desde la informática hasta las redes y la infraestructura).

Las VPN dificultan las tareas a los equipos de seguridad que deben garantizar el cumplimiento de los principios de una arquitectura moderna, pero también evitar los ciberataques, responder a ellos y solucionarlos de la forma adecuada. Además, las VPN limitan la agilidad empresarial y la productividad de los equipos responsables de la informática, las redes y la infraestructura, lo que aumenta la complejidad del proceso de incorporación de nuevos empleados y contribuye a una experiencia de usuario deficiente.

La sustitución de la VPN está en la agenda de los responsables de TI y la adopción de un servicio de acceso a la red Zero Trust (ZTNA) es un excelente primer paso que permitirá a los equipos de red y de seguridad reforzar su estado de seguridad, reducir las incidencias informáticas y mejorar la productividad de los equipos.

Sin embargo, prevalece un exceso de confianza en el mercado y una ralentización del cambio. A menudo la razón es la falta de claridad acerca de por dónde empezar a eliminar la dependencia de la VPN, qué hacer y en qué orden. Sin embargo, debido a los problemas de seguridad y las continuas experiencias deficientes de los usuarios es necesario terminar con esta tendencia y priorizar el inicio inmediato de ese proceso.

Esta guía explica a los responsables de la informática y la seguridad qué deben tener en cuenta para decidir por dónde empezar, y ofrece pasos claros para ayudarles con la transición a ZTNA, así como ejemplos de cómo otras organizaciones han llevado a cabo este cambio fundamental.

Contenido

Costos de una demora

La sustitución de la VPN suele estar en la categoría de tareas a realizar "algún día". Sin embargo, puedes hacer algunos cálculos sencillos para cuantificar los verdaderos costos de demorar lo inevitable e iniciar el proceso de cambio.

Para empezar, esta calculadora es útil para comprender la rentabilidad de la modernización de distintos componentes de tu pila de soluciones de seguridad. A continuación, también encontrarás algunas ideas sobre costos implicados, que puedes adoptar y aplicar a tu empresa en particular.

Riesgo de las fugas de seguridad

En febrero de 2024, la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de EE. UU., junto con otros organismos del Reino Unido, Canadá, Australia y Nueva Zelanda, publicaron un documento de información conjunto sobre la explotación de las vulnerabilidades de Ivanti por parte de ciberdelincuentes. Su recomendación era limitar las conexiones de salida de Internet de los dispositivos VPN SSL a fin de restringir el acceso al servicio necesario, y limitar las conexiones de VPN SSL a las cuentas sin privilegios.[1]

Un reconocido experto lanzó una advertencia a todas las organizaciones del mundo en la publicación especializada SecurityInfoWatch.com, instándolas a reevaluar sus políticas de acceso remoto seguro.[2]

Más allá de los costos evidentes de las fugas de datos y los daños a la reputación, afecta también a los ciberseguros, que no solo son cada vez más costosos, sino también más difíciles de conseguir.

En los últimos años, el costo de los ciberseguros se ha disparado. Y si bien este costo ha empezado a estabilizarse, la lista de exclusiones sigue aumentado.[3]

La aseguradora Munich Re indicó en un informe reciente que "las aseguradoras y los modeladores de riesgos continúan analizando los límites y las posibilidades de la asegurabilidad".[4]

"Ante un panorama de amenazas sumamente dinámico, donde los factores estresantes geopolíticos y tecnológicos definen las nuevas prioridades, es fundamental abordar los desafíos relacionados con la asegurabilidad y gestionar el riesgo acumulativo para lograr una sostenibilidad a largo plazo y una funcionalidad en un mercado que aún está en un proceso de maduración", indica el informe.

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b
2. https://www.securityinfowatch.com/cybersecurity/article/55019571/vpns-no-more-new-cisa-advisory-signals-need-for-secure-remote-access-amid-china-sponsored-attacks
3. https://professional.ft.com/en-gb/blog/cyber-insurance-rate-hikes-slow-but-exclusions-expand/
4. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

Experiencia del usuario e incorporación deficientes

La tecnología ineficiente puede contribuir al abandono de los empleados. En el séptimo informe sobre la situación laboral de Workfront, el 49 % de los trabajadores encuestados de EE. UU. afirmaron que estarían dispuestos a dejar su trabajo en caso de tener frustraciones relacionadas con la tecnología[5].

Gallup[6] estima que el costo de la sustitución de un empleado puede representar desde la mitad hasta el doble del salario anual del empleado. Por lo tanto, vale la pena considerar si una mala experiencia de los usuarios de la VPN puede afectar la satisfacción del personal.

Esta afirmación es especialmente cierta en el caso de los empleados cuyas atribuciones incluyen el manejo de información confidencial a la que se accede de forma remota (por ejemplo, los contables), donde el estudio muestra que algunas de las principales frustraciones están relacionadas con la experiencia del usuario y una integración adecuada de los sistemas [7]. Lo mismo sucede con los empleados que deben acceder continuamente a distintos sistemas, como los desarrolladores de software. Si el acceso es lento o ineficiente, puede tener un impacto cuantificable en su productividad.

Eficiencias empresariales y otros costos empresariales

En cambio, la adopción de una arquitectura Zero Trust puede resultar eficiente en el ámbito empresarial. Por ejemplo, la incorporación manual puede crear trabajo adicional y aumentar el tiempo necesario para que los nuevos empleados y proveedores sean plenamente productivos, ya que deben esperar el envío de hardware por correo postal y la conexión manual a aplicaciones y programas. De hecho, una empresa declaró una **reducción del 60 % del tiempo de incorporación tras la implementación de una herramienta ZTNA.**[8]

Otros costos empresariales que se pueden reducir son, entre otros, el aumento del ancho de banda debido a costos de redimensionamiento, y el incremento del hardware.

5. https://www.zdnet.com/article/nearly-half-of-workers-will-quit-their-job-if-their-workplace-technology-is-not-up-to-scratch/
6. https://www.gallup.com/workplace/247391/fixable-problem-costs-businesses-trillion.aspx
7. https://www.icaew.com/technical/technology/technology-and-the-profession/mastering-mid-tier-technology/icaews-mid-tier-research-highlights-shifts-in-technology-adoption
8. https://www.cloudflare.com/case-studies/eteacher-group/

Costos estratégicos de una demora

Las redes y los sistemas afectan a una gran parte de la estrategia empresarial, como las fusiones y adquisiciones.

Por ejemplo, un informe de Deloitte[9] estimó que aproximadamente el 60 % de las organizaciones considerarán el estado de ciberseguridad en su proceso de diligencia debida como un factor crítico durante cualquier operación de fusión y adquisición.

"La tecnología también desempeña un rol importante, no solo porque posibilita la integración, sino también porque impulsa el nuevo modelo operativo de las empresas. Puede dar lugar a una amplia variedad de ciberataques, y un estado de ciberseguridad deficiente puede ralentizar el proceso de adquisición de la empresa y, en algunos casos, incluso ser un factor decisivo que impida alcanzar un acuerdo", explica Deloitte.

En un informe reciente de Enterprise Strategy Group, *Considerations for Implementing Zero Trust for the Workforce*, el 78 % de los directivos de TI encuestados coincidían en que la actividad de fusiones y adquisiciones impulsa la necesidad de acelerar la integración informática de los distintos proveedores de identidad y redes.[10]

Estos costos estratégicos también pueden incluir demoras en el lanzamiento de nuevas aplicaciones, e incluso la pérdida de certificaciones de cumplimiento normativo.

Costos personales de una demora

Una vulneración de la ciberseguridad puede dañar la reputación de aquellos implicados, desde los directores de una empresa hasta los profesionales de la seguridad responsables de impedir los ataques. Investigadores de la universidad de Oxford han estudiado las repercusiones de los ciberataques (entre otras, desde el punto de vista psicológico y de los daños a la reputación), e identificaron aspectos como el abandono del personal y el daño a las relaciones con los clientes.[11]

No solo eso, los directores pueden ser (y son) declarados personalmente responsables en muchas jurisdicciones de todo el mundo[12].

Una VPN ineficiente aumenta la carga de trabajo para el personal de TI, tanto en términos de ineficiencias de los usuarios como del incremento de incidencias informáticas.

9. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-cybersecurity-for-mergers-and-acquisitions-noexp.pdf
10. https://cfl.re/esg-zero-trust-workforce-ebook-2024
11. https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks
12. https://www.whitecase.com/insight-alert/director-liability-cyber-breaches-transatlantic-warning-signs, https://www.allens.com.au/insights-news/insights/2022/04/cyber-risks-resilience-and-responsibilities/

Cómo garantizar la alineación interna

La sustitución de la VPN es un proyecto multifuncional, por lo tanto, es fundamental garantizar la alineación interna para una implementación eficaz y en el momento oportuno.

Los proyectos de sustitución de la VPN los pueden iniciar tanto el equipo de seguridad como los equipos de informática/redes/infraestructura, según las necesidades de cada empresa. Lo que es imprescindible es que estos equipos trabajen en forma conjunta para que haya una alineación en términos de la propiedad y la implementación. Un buen punto de partida es comprender todos los grupos que probablemente participen en una colaboración, y establecer la alineación de las distintas dinámicas empresariales que afectan la necesidad de impulsar el cambio.

El apoyo de la dirección también es fundamental para ayudar con la alineación de los equipos, si es necesario.

Un taller gratuito sobre arquitectura, de pizarra compartida, con el equipo de especialistas en seguridad de Cloudflare también puede ayudarte. Puedes reservar uno aquí.

Desafíos de la seguridad heredada

Las VPN están limitadas al perímetro corporativo. Por lo tanto, es más difícil evitar los incidentes de seguridad, responder a ellos y solucionarlos debido a la falta de disponibilidad y a la incapacidad de restringir el movimiento lateral y los permisos de acceso.

Como resultado, se aplican soluciones temporales que son ineficaces de gestionar, y políticas excesivamente restrictivas para cumplir con las obligaciones de seguridad. El incumplimiento normativo puede incluso dar lugar a sanciones, a la imposibilidad de firmar un acuerdo y a incurrir en responsabilidades a nivel personal.

13. https://cfl.re/esg-zero-trust-workforce-ebook-2024

Desafíos de la conectividad heredada

Mientras tanto, para las funciones relacionadas con la conectividad (que pueden incluir responsabilidades en materia de informática, de red y de infraestructura), una VPN afecta a los equipos encargados de las operaciones empresariales, y limita su agilidad operativa, especialmente en periodos de crecimiento.

En primer lugar, les hace perder tiempo de distintas formas (por ejemplo, deben incorporar a los nuevos empleados mediante complejos procesos manuales, responder a un número excesivo de incidencias y quejas de los usuarios finales y configurar complejas políticas de firewall para segmentar la red).

Además, el tiempo necesario hasta que los nuevos empleados sean totalmente productivos, la pérdida de productividad de los usuarios finales y los largos periodos de mantenimiento afectan su reputación y pueden ser un motivo de frustración para los directivos de alto nivel.

Consulta a continuación para obtener más información.

Podrías tener que colaborar con:

ARQUITECTOS DE CONECTIVIDAD

Los arquitectos de conectividad podrían tener que colaborar con los arquitectos de seguridad, los equipos responsables de las operaciones de seguridad o los equipos responsables de las operaciones de conectividad.

ARQUITECTOS DE SEGURIDAD

Los arquitectos de seguridad podrían tener que colaborar con los equipos responsables de las operaciones de seguridad, los arquitectos de seguridad o los equipos responsables de las operaciones de seguridad.

RESPONSABLE EMPRESARIAL

Los responsables empresariales podrían tener que garantizar la alineación entre los arquitectos de seguridad, los equipos encargados de las operaciones de seguridad, los arquitectos de conectividad y los equipos responsables de las operaciones de conectividad.

OPERACIONES DE CONECTIVIDAD

Los equipos responsables de las operaciones de conectividad podrían tener que colaborar con los arquitectos de seguridad, los equipos responsables de las operaciones de seguridad o los arquitectos de conectividad.

OPERACIONES DE SEGURIDAD

Los equipos responsables de las operaciones de seguridad podrían tener que colaborar con los arquitectos de seguridad, los arquitectos de conectividad o los equipos responsables de las operaciones de conectividad.

	Por qué deben dejar atrás la VPN	Valor que aporta la sustitución de la VPN
 **Arquitecto de seguridad**	Para los arquitectos de seguridad, las arquitecturas de seguridad heredadas fragmentadas suponen una mayor complejidad, potenciales vulnerabilidades y más dificultades para cumplir con los requisitos normativos.	La adopción de ZTNA brinda a los arquitectos de seguridad una gestión centralizada de todos sus recursos clave. También simplifica las pruebas y les permite entender la conectividad y el acceso en todo su entorno.
 **Operaciones de seguridad**	Las VPN tradicionales dejan expuesta un área demasiado amplia de la red, especialmente cuando las credenciales de usuario están en riesgo. Son menos escalables y eficientes. El número cada vez mayor de conexiones dificulta la inspección del tráfico al equipo responsable de las operaciones de seguridad. Además, es difícil actualizar y revisar las redes domésticas y los dispositivos de propiedad privada, lo que crea potenciales brechas de seguridad.	Con la adopción de ZTNA, los equipos responsables de las operaciones de seguridad pueden limitar la exposición de la red y proteger los datos confidenciales, incluso si las credenciales de usuario están en riesgo. También brinda una seguridad uniforme tanto en las redes corporativas como en las redes domésticas, sin necesidad de gestionar dispositivos privados. Además, ofrece una eficiente escalabilidad con cargas de trabajo alojadas en la nube y la capacidad de gestionar la inspección del tráfico con más eficacia.
 **Arquitectos de conectividad**	La utilización de las VPN implica inconsistencias entre los sistemas informáticos remotos y de las oficinas. Es posible que los arquitectos de conectividad compaginen varias configuraciones y redundancias en sus VPN (o incluso varios proveedores de VPN) para adaptarse a los distintos departamentos, regiones y empresas subsidiarias. El hardware heredado también causa problemas, especialmente cuando no está alineado con la agilidad que requieren las empresas modernas.	El abandono de las VPN implica la adopción de una arquitectura escalable, flexible, moderna, ágil, fiable y resiliente. Esta migración también mejora la seguridad y el cumplimiento, y genera eficiencias tanto a nivel de costos como de las operaciones. Además, un servicio ZTNA ofrece una mayor compatibilidad y una integración más fácil con las tecnologías existentes
 **Operaciones de conectividad**	Los equipos responsables de las operaciones de conectividad, cuando utilizan las VPN, suelen compaginar varios agentes de dispositivo y distintos proveedores de protección de puntos finales y de identidad, y además deben abordar la cuestión de los dispositivos privados no administrados. También deben gestionar VPN configuradas manualmente que requieren mucho tiempo y que generan incidencias de los usuarios. Además, son responsables de gestionar el ancho de banda y los cuellos de botella del tráfico. A menudo se los culpabiliza de los problemas de rendimiento y de las interrupciones, y cada vez con más frecuencia se los considera responsables de suministrar las aplicaciones a los empleados.	El abandono de las VPN significa que el equipo responsable de las operaciones de conectividad debe gestionar menos herramientas e integraciones. Además, reduce su carga de trabajo, ya que pueden automatizar los flujos de trabajo lo máximo posible y permitir gestionar a los usuarios finales sus solicitudes informáticas en modo autoservicio. Una buena experiencia del usuario final también mejora la reputación de los equipos (que ofrecen un servicio rápido y fiable que no solo no entorpece la productividad, sino que la mejora).

Por dónde empezar

Una vez que los equipos internos están alineados, el siguiente paso es trazar un plan claro de la estrategia de implementación de ZTNA.

Un reciente estudio de Enterprise Strategy Group encargado por Cloudflare, *Considerations for Implementing Zero Trust for the Workforce*,[13] encuestó a responsables de la toma de decisiones en seguridad informática de Norteamérica y Europa.

Una de las principales conclusiones recomendaba llevar a cabo el proceso de adopción de ZTNA por fases debido a la gran variedad de usuarios y aplicaciones.

Para simplificar, la encuesta dividió el proceso en tres fases: fase 1 (despliegue inicial), fase 2 (expansión) y fase 3 (progresión). En la práctica, no hay ningún número "correcto" de fases o de maneras de abordar la estrategia de implementación de ZTNA. Es posible que algunas organizaciones nunca logren un índice de sustitución del 100 %, ya sea por su posición especializada, por los recursos heredados o por preocupaciones más generales relacionadas con la gestión del cambio. La clave es empezar a pequeña escala y generar una dinámica que favorezca la modernización a un ritmo adecuado.

Lanzamiento inicial

En la primera fase, la organización identifica las prioridades clave y luego aborda un conjunto limitado de casos de uso o funciones antes de un despliegue más amplio.

Las organizaciones deben intentar encontrar proyectos que aporten alto valor en relación con el tiempo invertido. Esto ayudará a generar una dinámica y garantizará que el proyecto siga avanzando.

Expansión

En la fase 2, la organización pone la solución a disposición de un número mayor de empleados, aumenta la cobertura a un conjunto más amplio de aplicaciones, o se beneficia de funciones o capacidades adicionales.

Avance

En la fase 3 y posteriores, la organización implementa a nivel general la iniciativa para la mayoría de los empleados y las aplicaciones, utiliza funciones avanzadas, y se asegura de que el proyecto cumpla con los objetivos generales.

Si quieres que te ayudemos a trazar tu propio plan, puedes reservar un taller gratuito sobre arquitectura, de pizarra compartida, con el equipo de especialistas en seguridad de Cloudflare aquí.

13. https://cfl.re/esg-zero-trust-workforce-ebook-2024

Porcentaje promedio de usuarios y aplicaciones cubiertos durante el lanzamiento inicial

25 %
Lanzamiento inicial

Grupos de usuarios más habituales
- Equipos de ventas
- TI
- Directivos de alto nivel

Tipos de aplicaciones más habituales
- ERP
- Comunicación y colaboración
- Almacenamiento e intercambio de archivos

Ventajas de la implementación sin agente

Casi tres cuartas partes (el 71 %) de los encuestados indicaron que sus herramientas ZTNA actuales eran compatibles con la implementación sin agente, y el 84 % afirmaron que la facilidad de implementación les ayudó considerablemente a acelerar la adopción de Zero Trust.

Los encuestados también coinciden en que ZTNA sin agente abordó eficazmente los casos de uso, los usuarios y las aplicaciones que querían cubrir, por lo que pudieron ampliar la cobertura sin necesidad de implementar más herramientas que utilizaran agentes.

Ventajas de la implementación sin agente

~84 %
de los encuestados

- **Implementación simplificada, con la consiguiente reducción de la carga administrativa y de los puntos de falla**
- **Aceleración significativa de la adopción de Zero Trust**
- **Fácil escalabilidad gracias a la eliminación de las instalaciones de agentes individuales en cada dispositivo**
- **Eficaz cobertura de nuestros casos de uso y la escalabilidad deseada para el número de usuarios y aplicaciones que queremos**

Cómo otros clientes han adoptado Zero Trust

Como ya he mencionado, los equipos encargados de la seguridad y de la conectividad tienen sus propias razones para la sustitución de las VPN. Tanto unos como otros pueden iniciar este proceso, y posteriormente ampliarlo e integrar más colaboradores. No existe ninguna forma establecida para ello, ya que la propiedad del proyecto varía según las empresas.

Para darte una idea sobre cómo podría ser este proceso, aquí te mostramos algunas historias de clientes que destacan los principales catalizadores y el valor que han conseguido con la sustitución de la VPN, desde el punto de vista de la seguridad y de la conectividad (arquitectos y operaciones), aunque hay algunas coincidencias. Estas historias de clientes analizan la manera en que las empresas han avanzado desde su punto de partida a la transición propiamente dicha, y destacan los principales resultados para la organización.

CASO PRÁCTICO

Arquitecto de seguridad

Conglomerado de empresas de medios de comunicación y publicidad protege a más de 50 000 empleados del conocimiento

Una necesidad urgente de abordar las vulnerabilidades de seguridad llevó al cambio a largo plazo

En 2022, un conglomerado de empresas de medios de comunicación y publicidad decidió retirar sus operaciones de Rusia tras la invasión de Ucrania. Poco después, empezaron a sufrir intentos de ataque a sus sitios web públicos. La preocupación sobre estas amenazas (entre otras, era un objetivo de atacantes respaldados por el estado) alcanzó tal punto que la empresa cerró todas sus propiedades web y varias aplicaciones internas críticas un domingo por la tarde.

Solución

Cloudflare, en colaboración con uno de sus principales socios de implementación, inició una rápida respuesta para mitigar las amenazas dirigidas a los sitios web externos. Como siguiente paso, la empresa desplegó el servicio de acceso a la red Zero Trust (ZTNA) de Cloudflare, con el fin de proteger algunas aplicaciones críticas basadas en web que se habían visto gravemente interrumpidas para miles de usuarios.

En tan solo 48 horas, la empresa pudo reanudar sus operaciones empresariales críticas. Y en apenas unos días, desplegó ZTNA en varios miles de empleados adicionales.

Una vez restablecida la estabilidad de las operaciones empresariales, la empresa empezó a reconsiderar su enfoque a largo plazo de la protección del acceso. La migración de la aplicación de las políticas de acceso a una red en la nube distribuida globalmente ofrecía una oportunidad de brindar una experiencia más uniforme para los empleados, que trabajan en muchos países, tanto en ubicaciones remotas como en las oficinas.

Durante los meses siguientes, la empresa amplió sus políticas basadas en la identidad y en grupos para cientos de aplicaciones adicionales y miles de usuarios. En mayo de 2022, casi 50 000 usuarios utilizaban Cloudflare para la autenticación en sus aplicaciones más utilizadas, lo que descargaba la mayor parte del tráfico de las VPN existentes de la empresa.

Resultados

La empresa estima que la modernización de su seguridad con Cloudflare Zero Trust en toda su organización puede reducir potencialmente los costos en más de 5 millones de dólares al año, gracias al ahorro de tiempo en la administración de TI, la mejora de la productividad para los usuarios finales, la reducción del gasto en la VPN y en otras herramientas heredadas, y la menor probabilidad y la reducción de las potenciales repercusiones de una fuga de datos.

CASO PRÁCTICO

Operaciones de seguridad

EQT protege a más de 2000 empleados del conocimiento

EQT

El rápido incremento del número de empleados presentaba un desafío para la seguridad

EQT, empresa de inversión con sede central en Suecia, había expandido su presencia global y regional y ampliado rápidamente su cantidad de empleados, y había hecho una migración importante a la nube. La combinación de cambios complicó el trabajo al equipo central de informática y de seguridad responsable de la protección de sus empleados e inversores, así como de garantizar la seguridad de las empresas de su cartera.

Anteriormente, EQT dependía de herramientas tradicionales como Active Directory local de Microsoft para establecer políticas de acceso para sus aplicaciones locales. Para complicar aún más la situación, poco después de su migración a la nube, EQT dependía de una combinación de sus propios proxies personalizados y de una VPN local, cuyo mantenimiento era complejo y no siempre garantizaba la seguridad.

Al mismo tiempo, EQT estaba centrada en el desarrollo de sus propias aplicaciones internas para impulsar el crecimiento empresarial y, a su vez, en la contratación de más desarrolladores, que requerían un acceso sencillo y seguro. La empresa tenía más de 20 aplicaciones web propias que un número cada vez mayor de usuarios utilizaban a diario para tareas importantes.

Solución

Actualmente, EQT protege el acceso a todas las aplicaciones autoalojadas para todos los empleados y proveedores que utilizan el servicio de acceso a la red Zero Trust (ZTNA) de Cloudflare. Mediante un enfoque Zero Trust, Cloudflare autentica una solicitud enviada a una aplicación solo después de verificar la identidad de un usuario (en este caso, mediante la integración con el proveedor de identidad de EQT, Okta).

EQT también ha podido automatizar la mayor parte del proceso de configuración de políticas mediante la integración de Cloudflare con Terraform, la herramienta de infraestructura como código.

Resultados

Un proceso que antes requería toda una semana, ahora lleva tan solo cinco minutos

Los equipos de seguridad de EQT valoran poder reforzar la seguridad con políticas de negación por defecto y privilegio mínimo coherentes con las prácticas recomendadas Zero Trust, al mismo tiempo que simplifican la experiencia para sus empleados.

Antes de Cloudflare, el proceso de modificación o creación de políticas de acceso a las aplicaciones podía llevar hasta una semana, mientras que ahora apenas requiere cinco minutos.

CASO PRÁCTICO

Arquitectos de conectividad

Canva conecta más de 7000 empleados del conocimiento

Canva

La expansión requería mayor agilidad y simplificación

La plataforma de diseño de gráficos de Canva la utilizan millones de usuarios en todo el mundo. A medida que la empresa crecía, contrataba más empleados y externalizaba más tareas a desarrolladores de terceros, los administradores de TI debían encontrar una mejor forma de hacer las cosas para autenticar a los usuarios y hacer un seguimiento del uso de las aplicaciones.

Solución

Canva necesitaba una solución que le permitiera continuar su escala global y garantizar un alto rendimiento sin sacrificar la seguridad.

Para mejorar la seguridad y la eficiencia, Canva adoptó Cloudflare, que brinda un acceso seguro a las aplicaciones internas. Tras una exitosa prueba piloto con CanvaWorld, una plataforma de redes sociales interna, Canva amplió su uso de ZTNA a su flujo de trabajo de desarrollo de pruebas internas y de front-end.

Resultados

Eliminación de las ineficiencias causadas por las contraseñas compartidas

Cloudflare Zero Trust no solo ha eliminado las ineficiencias causadas por las contraseñas compartidas. También ha mejorado significativamente la seguridad de las aplicaciones internas de Canva y ha ahorrado a Canva la tarea de desarrollar su propio sistema de gestión de identidad y acceso (IAM).

Además, esto significaba que Canva no tenía que integrar funciones de permisos de usuario en las aplicaciones que protege ZTNA. Por ejemplo, la empresa quería dar a los empleados diferentes niveles de permisos en CanvaWorld, algo que permite ZTNA.

ZTNA también simplifica los procesos de incorporación y salida de empleados, y mejora su seguridad. Esto significa que Canva puede agregar o eliminar cuentas en función de las incorporaciones o bajas. No es necesario cambiar una contraseña común, guardarla en un archivo y notificarlo a todo el mundo.

CASO PRÁCTICO

Operaciones de conectividad

Delivery Hero conecta más de 40 000 empleados del conocimiento

Delivery Hero

La rápida expansión requería una simplificación del proceso de incorporación y una reducción de los problemas de conectividad

Entre 2016 y 2020, la plataforma de entrega de pedidos de comida Delivery Hero amplió su alcance global y su plantilla creció aproximadamente de 9000 a 30 000 empleados. Los equipos de informática y seguridad de la empresa tenían dificultades para seguir el ritmo de la incorporación de nuevos usuarios y de la integración de nuevas empresas que tenían distintas pilas de soluciones tecnológicas. La adopción del trabajo remoto en 2020 aumentó aún más la carga de trabajo del equipo de seguridad, ya que Delivery Hero debía gestionar una superficie de ataque ampliada.

Delivery Hero dependía de una solución de VPN, que era ineficiente de gestionar y lenta para los usuarios finales.

Solución

En primer lugar, Delivery Hero protegió el acceso a las aplicaciones internas utilizando Cloudflare One, una plataforma de perímetro de servicio de acceso seguro (SASE) que incluye un servicio ZTNA para proteger el acceso remoto.

Para empezar, se centraron en aplicar comprobaciones basadas en identidad para las aplicaciones web (un caso de uso inicial habitual que no requiere la implementación de ningún software de cliente en dispositivo).

Tras proteger el acceso a los recursos internos con Cloudflare, Delivery Hero inició un proceso similar para la seguridad en todos sus recursos accesibles públicamente, como sitios web, aplicaciones para clientes de dispositivos móviles y de escritorio, y portales administrativos disponibles para los proveedores.

Resultados

Escalar de forma más eficiente simplificando el proceso

En la actualidad, Delivery Hero usa Cloudflare para proteger el acceso de más de 40 000 empleados a todas las aplicaciones en entornos autoalojados, SaaS y no web. Aplicar comprobaciones de identidad en inicios de sesión únicos ayudó a Delivery Hero a mejorar su estrategia de seguridad (gracias a las prácticas recomendadas Zero Trust) y a agilizar la experiencia de los usuarios finales.

La adopción de Cloudflare ayudó a Delivery Hero a escalar de forma más eficiente, ya que pudo simplificar la incorporación de nuevos usuarios y consolidar las políticas de acceso en una única plataforma. De esta manera, liberamos tiempo y energía para que el personal técnico de Delivery Hero se centre en la innovación, y no en tareas administrativas.

Cómo elegir un proveedor

Si bien muchos proveedores de seguridad ofrecen una capacidad similar para crear políticas de acceso Zero Trust, no todos son iguales.

La solución de Cloudflare, por ejemplo, es más rápida y más fácil de implementar, ya que utiliza una sencilla configuración de implementación sin agente con operaciones uniformes para la expansión eficaz a más accesos y servicios en línea.

Luego de implementar la solución, Cloudflare brinda una mejor experiencia del usuario final y con latencia baja, donde los servicios de seguridad se brindan cerca de los usuarios finales, y están disponibles en cualquier lugar para cualquier usuario a escala global.

También ofrece resiliencia y conectividad fiable de un extremo a otro, y una red troncal privada con enrutamiento del tráfico y equilibrio de carga automatizado como código, así como información sobre amenazas integrada. La arquitectura de red Anycast de Cloudflare ofrece un SLA del 100 % para los planes de pago.

Además, con los servicios modulares de Cloudflare disponibles en todo el mundo, puedes continuar fácilmente con la implementación del resto de una estrategia SSE o SASE cuando estés preparado.
La sustitución de la VPN con la conectividad cloud de Cloudflare genera la dinámica necesaria para una modernización y consolidación más general de tus recursos informáticos y de seguridad.

Próximos pasos

Es imprescindible superar el exceso de confianza y dejar atrás las VPN. Posponer lo que es inevitable solo costará tiempo y dinero, y aumentará el riesgo y la posibilidad de incurrir en responsabilidades empresariales.

Para obtener más información sobre la implementación de ZTNA con Cloudflare, da un vistazo a nuestras guías de implementación para el acceso web sin cliente y la sustitución de tu VPN.

Si quieres reservar un taller gratuito sobre arquitectura, de pizarra compartida, con nuestro equipo de especialistas en seguridad, puedes hacerlo aquí.

Si tienes alguna pregunta o quieres comentar este tema con más detalle, ponte en contacto con nosotros.

Reserva un taller sobre arquitectura, de pizarra compartida, para conocer más

Acerca de Cloudflare

Cloudflare, Inc. (NYSE: NET) es una plataforma unificada e inteligente de servicios nativos de nube programables que ofrece una seguridad inigualable para proteger a los usuarios, las aplicaciones y las redes, y que permite a las organizaciones recuperar el control, reducir los costos y disminuir los riesgos de la protección de un entorno de red ampliado.

Visita cloudflare.com/connectivity-cloud para saber más sobre Cloudflare y radar.cloudflare.com para conocer las últimas tendencias y estadísticas más recientes sobre Internet.

Síguenos en: Blog | X | LinkedIn | Facebook | Instagram

Contacto

Teléfono: +55 (11) 3230 4523
www.cloudflare.com/es-la

CLOUDFLARE