Experiencias de Cliente

Explore historias de transformación del mundo real, impulsadas por zero trust de Zscaler + AI.

Vea cómo las empresas han mejorado sus posturas de seguridad, fomentado experiencias de usuario excepcionales y simplificado fusiones y adquisiciones, etc. con zero trust + AI.

Centrarse en los clientes es uno de nuestros valores fundamentales en Zscaler y, como tal, estamos comprometidos a ofrecer lo mejor en innovación de zero trust para ayudar a su organización a alcanzar sus objetivos. Con las capacidades centrales aprovechadas por nuestra plataforma Zero Trust Exchange, impulsada por IA, hemos ayudado a más de 5000 empresas en todo el mundo a reducir costes y complejidad, simplificar sus arquitecturas de red, proteger a sus usuarios y protegerse de las ciberamenazas en evolución. En este libro electrónico se analizarán los estudios de casos de algunas de las organizaciones más exitosas del mundo y cómo han transformado sus redes, seguridad y operaciones con Zscaler.

Con más de 15 años de experiencia en el ámbito de zero trust, Zscaler mantiene su compromiso de ayudar a organizaciones de todos los tamaños y sectores a alcanzar y superar sus objetivos de zero trust. La única constante que conocemos en la tecnología es el “cambio”, y con nuestra plataforma Zero Trust Exchange, las empresas pueden estar preparadas para lo que se les presente, mientras continúan innovando y transformando su infraestructura de TI.

Mike Rich
CRO y presidente de Ventas Globales

Índice

Explore las historias de éxito de nuestros clientes por vertical

01 Construcción

58 John Holland

02 Educación

28 Departamento de Educación de la Ciudad de Nueva York

03 Energía, petroleo, gas y minería

70 Maxeon
30 Southwest Gas

04 Entretenimiento y hospitalidad

22 MGM Resorts International

05 Federal y Gobierno

14 Gobierno del Distrito de Columbia
38 Capital del estado: Magdeburgo

06
Servicios financieros y seguros

44 Capitec
20 Guaranteed Rate
24 Mercury Financial
36 Raiffeisen Bank International
66 The Bank of Saga

07
Comida, bebida y tabaco

26 Molson Coors

08
Sanidad y farmacia

8 AMN Healthcare
64 Keiju Medical Center
48 Sanitas

09
Alta tecnología

16 DMI
62 Persistent Systems
52 Primetals Technologies

10
Fabricación

18 Eaton
42 Hydro
54 Unilever

11
Venta minorista y mayorista

12 Cox Automotive
40 Cisalfa Sports

12
Servicios

60 Probe CX

13
Telecomunicaciones

10 ATN International
50 Colt

14
Servicios de transporte

68 Cebu Pacific Air
46 Noatum
32 United Airlines

Región AMS

Explore las historias de éxito de los clientes por región

8 AMN Healthcare

10 ATN International

12 Cox Automotive

14 Gobierno del Distrito de Columbia

16 DMI

18 Eaton

20 Guaranteed Rate

22 MGM Resorts International

24 Mercury Financial

26 Molson Coors

28 Departamento de Educación de la Ciudad de Nueva York

30 Southwest Gas

32 United Airlines

AMN Healthcare protege a los usuarios y los datos a nivel mundial con Zscaler Zero Trust Exchange

Zscaler protege la experiencia de trabajo remoto de más de 5000 usuarios y los datos de los pacientes frente a las crecientes ciberamenazas dirigidas al sector sanitario

INSTANTÁNEA DE AMN HEALTHCARE

Brindando a los clientes soluciones de personal sanitario para mejorar los resultados de los pacientes

- Sanidad y farmacia
- Dallas, Texas, Estados Unidos
- Más de 10 000 clientes en 24 ubicaciones

1200 millones
de transacciones web procesadas mensualmente

7 millones
de amenazas bloqueadas en tres meses

Horas
para implementar un perímetro seguro en cualquier lugar

Desafíos

- Una infraestructura de seguridad heredada ya no era compatible con el ecosistema operativo en constante evolución de la empresa, que priorizaba la nube
- Las VPN tradicionales no podían soportar las crecientes necesidades de acceso remoto, lo que dejaba a los recursos privados más vulnerables a las ciberamenazas
- Una arquitectura de seguridad compleja con múltiples soluciones puntuales hizo que la visibilidad y resolución de problemas fuera difícil de gestionar

Proceso por fases

1. **Se proporcionó acceso directo a Internet seguro**, lo que garantiza un trabajo flexible desde cualquier lugar para un personal disperso globalmente
2. **Se introdujo el acceso privado a aplicaciones zero trust y microsegmentadas**, lo que proporciona un reemplazo seguro para las VPN tradicionales
3. **Se optimizó la pila de supervisión y se aprovechó la visibilidad integral de extremo a extremo** para mejorar la resolución de problemas de los usuarios

Resultados

- **Se asegura la conectividad entrante y saliente para más de 5000 usuarios**, mejorando las capacidades y la eficiencia del trabajo remoto global
- **Aplica políticas de acceso zero trust para aplicaciones privadas y productos digitales** utilizados por más de 10 000 clientes en todo el mundo
- **Simplifica la arquitectura y reduce los costes de tecnología** para lograr una postura de seguridad más potente con menos gastos generales

El enfoque de Zscaler está alineado con nuestra filosofía general de zero trust, y la plataforma Zero Trust Exchange fue la encarnación de nuestra visión de una arquitectura zero trust en AMN Healthcare.

Mani Masood
Jefe de Seguridad de la Información, AMN Healthcare

Ver historia de éxito

ATN International protege sus operaciones y mejora su eficiencia con Zscaler Zero Trust Exchange

Zscaler mejora las capacidades de trabajo remoto para más de 2500 empleados, elimina los problemas de los usuarios relacionados con VPN y garantiza una integración de fusiones y adquisiciones y una incorporación más seguras

INSTANTÁNEA DE ATN INTERNATIONAL

Proporciona infraestructura y servicios de comunicaciones con experiencia en mercados remotos

Telecomunicaciones

Beverly, Massachusetts, Estados Unidos

750 000 clientes en todo el mundo

El 100 %
eliminación de las VPN y tickets de ayuda de VPN

Todos
los empleados protegidos con Zscaler

Minutos
frente a horas para mitigar problemas de los usuarios

Desafíos

- La infraestructura de seguridad local no podía respaldar de manera eficiente las operaciones comerciales basadas en la nube o los objetivos de futuras fusiones y adquisiciones
- Los dispositivos VPN heredados tenían dificultades para ajustarse, debido al aumento del trabajo remoto, lo que generó malas experiencias de usuario y un mayor riesgo.
- Las soluciones de seguridad tradicionales no ofrecían integraciones críticas en la nube para permitir la mitigación proactiva de problemas de los usuarios.

Proceso por fases

1. **Se proporcionó acceso directo a Internet,** aprovechando las funciones de registro e inspección de tráfico para evitar infracciones de políticas
2. **Se reemplazaron los dispositivos VPN con acceso con mínimo privilegio zero trust** a aplicaciones y recursos privados
3. **Se aprovecharon las funciones de Zscaler impulsadas por IA y la profunda integración con Microsoft** para identificar y resolver los problemas de los usuarios más rápido

Resultados

- **Mejora la experiencia de trabajo remoto para más de 2500 usuarios** y elimina los problemas de los usuarios relacionados con VPN: los tickets de servicio se reducen en un 100 %
- **Se acelera el cronograma de fusiones y adquisiciones, y se garantiza una incorporación más segura** de las empresas adquiridas con una arquitectura de seguridad zero trust
- **Reduce el tiempo necesario para identificar y resolver problemas** a solo unos minutos con funciones potentes de generación de informes y supervisión.

Uno de los elementos que busco en las herramientas de infraestructura y seguridad es que te ayuden a ser más eficiente operativamente y te protejan mejor. Zscaler cumple ambos requisitos.

Richard Casselberry
Vicepresidente de Seguridad Informática, Arquitectura y Cumplimiento,
ATN International

Ver historia de éxito

COX AUTOMOTIVE

Cox Automotive implementa Zero Trust en fases con Zscaler Zero Trust Exchange

Zscaler optimiza la arquitectura de seguridad, asegura la conectividad de los usuarios en los cinco continentes y protege los datos de millones de compradores de automóviles en línea.

INSTANTÁNEA DE COX AUTOMOTIVE

El mayor proveedor de servicios y tecnología automotriz del mundo

- Venta minorista y mayorista
- Atlanta, Georgia, Estados Unidos
- 2300 millones de interacciones en línea al año

Más de 30 000
miembros del equipo Protegido

40 000
clientes concesionarios de automóviles apoyados

Una
plataforma única reduce la complejidad

Desafíos

- Se buscaba una plataforma compatible con la nube que pudiera servir como base para una arquitectura zero trust de seguridad integral.
- Los dispositivos de cortafuegos tradicionales tenían dificultades para inspeccionar el tráfico de Internet a gran escala para un grupo de usuarios disperso globalmente.
- Las VPN tradicionales no admitían políticas de control de acceso basadas en identidad, lo que ponía en mayor riesgo las aplicaciones y los datos privados

Proceso por fases

1. **Se implementó una plataforma zero trust multiinquilino nativa de la nube** diseñada específicamente para integrarse fácilmente con otras soluciones en la nube
2. **Conectividad segura y directa a Internet y aplicaciones SaaS**, aprovechando las capacidades de inspección de tráfico en línea
3. **Se reemplazaron las VPN con acceso zero trust** para establecer políticas de seguridad microsegmentadas y con mínimos privilegios para aplicaciones privadas

Resultados

- **Asegura un equipo que trabaja en cinco continentes,** brindando flexibilidad para trabajar desde cualquier lugar y mejorando las experiencias de los usuarios.
- **Protege aplicaciones y recursos privados críticos**, incluidos datos sobre millones de clientes, de una manera más rentable
- **Retira las soluciones de seguridad heredadas, incluidos los cortafuegos y las VPN,** para optimizar los procesos de TI y acelerar la incorporación en fusiones y adquisiciones

Una vez que los agentes estén instalados en los dispositivos de todos los empleados, será fácil integrar otras capacidades de Zscaler en nuestra arquitectura. Será sólo cuestión de pulsar el interruptor de “encendido”.

Jon Mahes
Gerente sénior de Ciberseguridad
Cox Automotive

Ver historia de éxito

El Gobierno del Distrito de Columbia consolida la seguridad con Zero Trust Exchange

Zscaler reemplaza los dispositivos VPN heredados para optimizar la arquitectura de seguridad, reforzar el conocimiento de los riesgos en tiempo real y proteger a 15 000 usuarios

INSTANTÁNEA DEL GOBIERNO DE D.C.

Supervisa y administra todos los servicios críticos para los residentes del Distrito de Columbia.

Federal y Gobierno

Washington, D.C., EE. UU.

Más de 15 000 empleados

15 000
empleados del gobierno protegidos

~3000 millones
transacciones procesadas por mes

Más de 200 000
amenazas de seguridad bloqueadas por mes

Desafíos

- Una infraestructura de seguridad obsoleta no podía soportar el trabajo remoto y contribuía a ineficiencias operativas
- Los dispositivos VPN tradicionales ampliaban la red corporativa a los dispositivos de los usuarios finales, poniendo en riesgo los datos confidenciales.
- Los productos puntuales de seguridad heredados limitaban la visibilidad en torno a las amenazas, lo que dificultaba la evaluación y mitigación de riesgos

Proceso por fases

1. **Se proporcionó conectividad segura y directa a Internet y aplicaciones SaaS**, lo que permitió la flexibilidad de trabajar desde cualquier lugar.
2. **Se reemplazaron las VPN heredadas con acceso zero trust microsegmentado** para aplicar políticas de seguridad consistentes para los recursos privados.
3. **Se aprovecharon los datos y conocimientos impulsados por IA para reforzar la conciencia de los riesgos** y mitigar las amenazas potenciales en tiempo real y a escala.

Resultados

La arquitectura zero trust mejora la postura de seguridad. Procesa aproximadamente 3000 millones de transacciones y bloquea más de 200 000 amenazas mensuales

Mejora la experiencia del usuario remoto para 15 000 usuarios y se integra perfectamente con las soluciones de identidad existentes

Permite un enfoque más integral en la gestión de riesgos, impulsado por mejores conocimientos sobre los factores de riesgo y la postura de seguridad

La asociación con Zscaler ha sido inestimable para nosotros. Implementamos la plataforma a velocidades récord, integramos usuarios de manera más efectiva y mejoramos la experiencia del usuario.

Suneel Cherukuri
CISO, Gobierno de DC

Ver historia de éxito

DMI permite el uso de dispositivos propios del usuario a gran escala, mejorando la protección de datos y poniendo de manifiesto importantes ahorros de costes

Zscaler proporciona conectividad zero trust para todo el personal y permite a los empleados trabajar de forma segura desde el dispositivo de su elección

INSTANTÁNEA DE DMI

DMI es un proveedor líder mundial de servicios digitales que trabaja en la intersección de los sectores público y privado.

Alta tecnología

McLean, Virginia, Estados Unidos

Más de 2100 empleados en 80 países

Más de 700 000 dólares estadounidenses
ahorro anual

2.
semanas para implementar

3 %
resolución de SLA más rápida después de la implementación

Desafíos

- La instalación de nuevo hardware en un entorno heredado generaba tiempos de inactividad, provocaba interrupciones y requería actualizaciones periódicas.
- Exigir a los usuarios que trabajen desde dispositivos DMI hizo que los empleados fueran menos productivos y afectó negativamente la huella de carbono global de la organización.

Proceso por fases

1. **Acceso seguro a Internet y verdadera conectividad zero trust** para empleados, contratistas y terceros sin necesidad de realizar configuraciones manuales de dispositivos que requieran mucho tiempo
2. **Se implementó la iniciativa "traiga su propio dispositivo" respaldada por el aislamiento del navegador,** lo que permite a los empleados trabajar en el dispositivo de su elección

Resultados

- **Implementa zero trust en 2 semanas** sin impacto para los usuarios y sin tiempo de inactividad
- **Ahorra 700 000 dólares estadounidenses anualmente,** mejora las experiencias de incorporación y salida, y acorta el tiempo para configurar nuevas oficinas y dispositivos

Con el proyecto de uso de dispositivos propios del usuario pudimos ahorrar dinero al no tener que comprar ordenadores portátiles para personas que no los necesitaban. En realidad, esto nos supuso un ahorro anual de más de 700 000 dólares estadounidenses para DMI: una cantidad enorme.

Mauricio Mendoza
Vicepresidente de TI global y Seguridad, DMI

Ver historia de éxito

Eaton asegura operaciones globales con segmentación impulsada por IA

Zscaler ayuda a los fabricantes globales a migrar a la nube con protección avanzada frente a amenazas, reducción del riesgo de infracciones y mayor visibilidad a través de integraciones con socios

INSTANTÁNEA DE EATON

Fabricante mundial de equipos eléctricos para la industria aeroespacial y otros sectores

Fabricación

Cleveland, Ohio, Estados Unidos

Más de 90 000 empleados y usuarios en 170 países de todo el mundo

4 millones

amenazas bloqueadas en un mes

90 000

empleados de todo el mundo se conectan a Internet y a aplicaciones privadas a través de zero trust

Varios

socios de alianza estratégica se integran sin problemas

Desafíos

- Las VPN y los cortafuegos heredados obstaculizaban el crecimiento y no podían brindar soporte a más de 30 000 empleados de planta durante la pandemia y más allá
- La arquitectura de seguridad tradicional basada en perímetro era incompatible con la estrategia de nube prioritaria de la empresa y las necesidades de segmentación.
- La falta de visibilidad limitaba la detección de amenazas y ralentizaba la solución

Proceso por fases

1. **Se reemplazaron las herramientas de seguridad** y acceso con conectividad zero trust a Internet y aplicaciones privadas
2. **Se adoptaron innovaciones de IA** para descubrir y combatir amenazas basadas en IA y brindar segmentación para los sitios de fabricación
3. **Conciencia mejorada sobre ataques** con detección y respuesta preventivas y predictivas ante infracciones

Resultados

- **Proporciona una experiencia de usuario más segura, confiable y regulada** para empleados y terceros
- **Aprovecha el poder de la IA para la detección de amenazas**, la prevención de pérdida de datos, la corrección, la visibilidad del uso de ChatGPT y la segmentación de aplicaciones
- **Fortalece el control de acceso** a través de la segmentación zero trust y la integración con herramientas EDR, CDR y NDR

Zscaler es fácil de usar y sus capacidades están integradas en un agente de terminal. Hemos podido implementar Zscaler en nuestro entorno global rápidamente y expandir sus capacidades con pocos recursos necesarios de nuestra parte.

Jason Koler
Director de Seguridad de la Información de Eaton Corporation

Ver historia de éxito

Guaranteed Rate bloquea millones de amenazas y acelera la integración de fusiones y adquisiciones de meses a días

Zscaler reemplaza el hardware de seguridad y ofrece una resiliencia superior, seguridad siempre activa y una superficie de ataque reducida

INSTANTÁNEA DE GUARANTEED RATE

La segunda mayor empresa del sector de las hipotecas minoristas de EE. UU., con más de 500 sucursales en 50 estados

Servicios financieros y seguros

Chicago, Illinois, Estados Unidos

más de 6000 empleados

97 %
del tráfico cifrado inspeccionado

2,5 millones
de amenazas bloqueadas en 3 meses

2–3x
acceso más rápido a Aplicaciones

Desafíos

- El uso de VPN para conectarse a cientos de aplicaciones privadas locales y en AWS abría la superficie de ataque
- El tráfico de retorno desde más de 500 sucursales al centro de datos obstaculizaba el rendimiento y la productividad
- El cortafuegos heredado no podía detectar amenazas de día cero que ingresaban a la red desde Internet y se movían lateralmente

Proceso por fases

1. **Acceso seguro a Internet y SaaS desde la nube:** no más conexiones de retorno desde más de 500 sucursales
2. **Reemplazó la VPN**, brindando a los usuarios acceso rápido y confiable a más de 500 aplicaciones privadas en el centro de datos y la nube
3. **Optimizó la experiencia del usuario** al identificar y resolver problemas de rendimiento de forma más rápida y eficiente

Resultados

- **Minimiza la superficie de ataque** al brindar a los usuarios acceso directo y con menos privilegios al tiempo que mejora la detección y la respuesta
- **Reduce el riesgo de compromiso** con supervisión de tráfico TLS/SSL en línea y protección avanzada contra amenazas impulsada por IA
- **Previene el movimiento lateral** con tecnología de engaño para alejar a los atacantes de recursos confidenciales y contener amenazas en tiempo real

Con Risk360, podemos obtener visibilidad de los puntos ciegos del riesgo cibernético. Esta visibilidad nos permite centrarnos más en dónde pasamos nuestro tiempo para abordar y reducir los riesgos cibernéticos más urgentes.

Darin Hurd
CISO en Guaranteed Rate

Ver historia de éxito

MGM Resorts
La comunidad internacional apuesta por una arquitectura Zero Trust

Zscaler ofrece una rentabilidad inigualable con segmentación zero trust, protección contra pérdida de datos y conocimientos prácticos y profundos en toda la empresa

INSTANTÁNEA DE MGM RESORTS INTERNATIONAL

Líder en juegos, entretenimiento y hospitalidad con 31 destinos turísticos a nivel mundial

Hotelería y Entretenimiento

Las Vegas, Nevada, Estados Unidos

70 000 empleados en todo el mundo

Día 1
valor inmediato desde la plataforma

Más de 275 000
amenazas bloqueadas cada mes

50 %
uso más eficiente de los dispositivos por parte del personal

Desafíos

- La seguridad de castillo y foso aumentaba el riesgo de movimiento lateral al brindar a los usuarios un amplio acceso a la red
- Las puertas de enlace VPN tradicionales creaban cuellos de botella en el tráfico, lo que generaba una mala experiencia del usuario.
- Las herramientas de seguridad heredadas ofrecían información limitada sobre la actividad de navegación de toda la base de usuarios

Proceso por fases

1. **Se reemplazaron las VPN y se implementó la segmentación zero trust** con todo el personal
2. **Se implementó rápidamente** un conjunto de soluciones de acceso privado, experiencia digital y protección de datos
3. **Se adoptó tecnología de engaño** para protegerse contra ataques activos

Resultados

- **Mejora la experiencia de los empleados** con un rendimiento más rápido y conectividad en todo el entorno
- **Se mantiene a la vanguardia de las amenazas emergentes** con DLP integral, acceso privado y segmentación zero trust
- **Fortalece la postura de seguridad empresarial** al tiempo que ayuda a acelerar el negocio con un enfoque centrado en la nube

Logramos la segmentación zero trust en todo nuestro personal en un tiempo récord y el mantenimiento diario de la solución con protección contra pérdida de datos con información sobre nuestras aplicaciones. Desde nuestra perspectiva, estas fueron victorias realmente rápidas y fáciles.

Stephen Harrison
Director de Seguridad de la Información, MGM Resorts International

Ver historia de éxito

Mercury Financial mejora la seguridad y la eficiencia con el Zero Trust Exchange

Zscaler ofrece integraciones perfectas y funciones de inteligencia artificial para respaldar un trabajo remoto más seguro desde cualquier ubicación y proteger los datos financieros confidenciales de las amenazas

INSTANTÁNEA DE MERCURY FINANCIAL

Una empresa de servicios financieros no bancarios que ayuda a los clientes a crear y gestionar el crédito

- Servicios financieros y seguros
- Austin, Texas, Estados Unidos
- Más de 500 empleados

100 %
experiencia perfecta para trabajadores remotos

76 %
reducción de tickets de soporte de TI

Cero
tiempo de inactividad debido al malware

Desafíos

- Las soluciones de seguridad tradicionales no permitían la inspección completa del tráfico en línea, lo que inhibía la detección y prevención de amenazas.
- Las VPN tradicionales eran incompatibles con las necesidades de priorizar la nube de un personal distribuido, lo que generaba malas experiencias de usuario.
- Los datos limitados sobre la actividad del usuario y la postura del dispositivo dificultaron el diagnóstico y la resolución de problemas para un personal remoto

Proceso por fases

1. **Conectividad directa a Internet segura**, utilizando funciones de contención de amenazas impulsadas por IA para evitar la vulneración de datos
2. **Se reemplazaron las VPN con acceso zero trust microsegmentado** para aplicaciones privadas para garantizar que las conexiones remotas estén controladas y sean seguras
3. **Se aprovecharon las integraciones clave y los conocimientos de los usuarios más potentes** para aliviar la sobrecarga administrativa sin aumentar el riesgo

Resultados

- **Reduce la superficie de ataque:** cero tiempo de inactividad causado por malware o ransomware desde la implementación de Zscaler
- **Limita el movimiento lateral y reduce el radio de explosión** si una amenaza accede a la pila de seguridad, lo que garantiza una solución del problema más rápida
- **Las integraciones con AWS, Crowdstrike y Okta optimizan la infraestructura de seguridad** y refuerzan el cumplimiento normativo

Consideramos a Zscaler como líder en este área porque ofrece cobertura integral y cubre todas las facetas de zero trust. Para obtener la misma funcionalidad que obtenemos de Zscaler en otros lugares, tendríamos que implementar varias soluciones de proveedores.

Arjun Thusu
Director de Información
Mercury Financial

Ver historia de éxito

Molson Coors ofrece una excelente experiencia de usuario con Zero Trust Exhange

Zscaler elimina la necesidad de dispositivos VPN, asegura la conectividad para un personal global y proporciona información que resuelve los problemas más rápidamente.

INSTANTÁNEA DE MOLSON COORS

La tercera cervecera más grande del mundo y un innovador global en el sector de bebidas.

Alimentación, bebidas y tabaco

Chicago, Illinois, Estados Unidos

Más de 17 000 empleados
Más de 42 cervecerías

17 000
usuarios protegidos con zero trust

96 %
resolución más rápida de problemas de los usuarios

Millones
de amenazas bloqueadas diariamente

Desafíos

- Los dispositivos de cortafuegos no se podían ajustar con la demanda de acceso remoto a Internet y tenían dificultades para inspeccionar el tráfico en línea.
- La falta de visibilidad en torno a la actividad del usuario y la postura del dispositivo dificultaron la identificación y la solución de problemas de rendimiento.
- Una arquitectura de seguridad heredada que dependía de dispositivos VPN creaba un entorno de red plano y una superficie de ataque más amplia

Proceso por fases

1. **Acceso directo a Internet provisto con funciones avanzadas de detección de amenazas** para mantener seguros a los usuarios remotos y de terceros
2. **Se aprovecha la visibilidad de extremo a extremo entre usuarios y dispositivos** para simplificar la gestión de la seguridad y resolver los problemas de los usuarios más rápidamente
3. **Se reemplazaron las VPN tradicionales con acceso zero trust para aplicaciones privadas** a fin de proteger los recursos y mejorar la experiencia del usuario

Resultados

- **Garantiza una excelente experiencia de usuario para los empleados** que trabajan en 42 cervecerías en todo el mundo, así como para socios externos
- **Mejora el tiempo medio de resolución de problemas del usuario** al identificar las causas fundamentales y automatizar la mitigación en minutos, no en horas
- **Bloquea amenazas avanzadas** y elimina el movimiento lateral para mantener más seguras las aplicaciones privadas y los datos corporativos confidenciales

¿Cuántas amenazas fueron bloqueadas sólo desde Zscaler? Siempre son cientos de miles o millones, según el día. Es simple y fácil de usar. Podrá ponerlo en marcha inmediatamente. Sin límites.

Jeremy Bauer
Director sénior de Seguridad de la Información (CISO), Molson Coors Beverage Company

Ver historia de éxito

NYC Department of Education

El Departamento de Educación de la Ciudad de Nueva York migra de VPN a Zero Trust

Zscaler ayuda a proteger el acceso a Internet y a aplicaciones privadas para más de 1 millón de usuarios y más de 2 millones de dispositivos

INSTANTÁNEA DEL DEPARTAMENTO DE EDUCACIÓN DE LA CIUDAD DE NUEVA YORK

El Departamento de Educación de la Ciudad de Nueva York (NYC DOE) es el mayor sistema escolar de los Estados Unidos y uno de los mayores del mundo. Atiende a más de 1 millón de estudiantes desde educación infantil hasta el 12.º grado con un personal de más de 150 000 profesores y administradores en los cinco distritos de Nueva York.

Educación

Ciudad de Nueva York, Nueva York, Estados Unidos

Más de 1 millón de usuarios y más de 2 millones de dispositivos

Más de 2 millones
de dispositivos de estudiantes y empleados protegidos

15 %
de disminución de ataques

40 %
más amenazas bloqueadas

Desafíos

- La infraestructura heredada no se podía ajustar para brindar experiencias seguras y consistentes para más de 1 millón de usuarios
- El enfoque tradicional de VPN y cortafuegos era ineficaz para bloquear ciberamenazas avanzadas
- La escasa visibilidad de los terminales dificultaba el mantenimiento y la supervisión de los dispositivos de aprendizaje remoto del departamento

Proceso por fases

1. **Acceso seguro a Internet y SaaS** con una arquitectura zero trust de proxy que inspecciona el 100 % del tráfico TLS/SSL a escala
2. **Se reemplazó la VPN con acceso a la red zero trust (ZTNA)** para una conectividad de usuario rápida y sin inconvenientes
3. **Visibilidad mejorada** en redes y dispositivos con supervisión de experiencia digital de extremo a extremo

Resultados

- **Extiende el acceso rápido, confiable y seguro** a las aplicaciones de aprendizaje para estudiantes y empleados en cualquier lugar y en cualquier dispositivo
- **Filtra el tráfico en función del contenido**, más allá del simple bloqueo de URL, para respaldar el cumplimiento de CIPA en los dispositivos de aprendizaje
- **Mejora el rendimiento de la red** al encontrar y resolver problemas de red y DNS en el entorno

Creo que Zscaler puede ser un buen socio para ayudarnos a comprender lo que estamos haciendo con la IA y ayudarnos a avanzar más rápido en la respuesta a incidentes y en encontrar esa aguja en el pajar.

Demond Waters
CISO, Departamento de Educación de la Ciudad de Nueva York

Ver historia de éxito

Southwest Gas aprovecha Zero Trust Exchange de Zscaler para optimizar una experiencia de usuario segura

Zscaler elimina la dependencia de las soluciones de seguridad tradicionales para brindar una conectividad más rápida y confiable para 2300 empleados híbridos y 50 oficinas de campo

INSTANTÁNEA DE SOUTHWEST GAS

Compañía energética que brinda servicio de gas natural en Arizona, Nevada y California

Energía, petróleo, gas y minería

Las Vegas, Nevada, Estados Unidos

2 millones de clientes

4–6

semanas para implementar de manera integral zero trust

95 %

de casos de uso cumplidos

Una

plataforma de un solo proveedor para simplificar

Desafíos

- Una infraestructura de seguridad tradicional no se podía ajustar para soportar la transformación a la nube o el cambio al trabajo híbrido
- Proporcionar conectividad a Internet rápida y confiable era todo un desafío para las oficinas de campo y los empleados remotos en áreas rurales
- Las VPN tradicionales no permitían políticas de acceso basadas en identidad, lo que dejaba a las aplicaciones y datos privados más vulnerables a las amenazas.

Proceso por fases

1. **Se implementó una plataforma zero trust multiinquilino**, agilizando la pila de seguridad y optimizando los entornos de trabajo remotos
2. **Se proporcionó acceso directo a Internet y aplicaciones SaaS** con protección constante frente a amenazas, independientemente de la ubicación
3. **Se reemplazaron las VPN con acceso zero trust para aplicaciones privadas** a fin de reducir la superficie de ataque y eliminar la pérdida de datos

Resultados

- **Garantiza la flexibilidad de trabajar desde cualquier lugar para 2300 empleados híbridos** y protege a usuarios y datos en 50 oficinas de campo
- **Permite políticas de control de acceso microsegmentadas y con menos privilegios** para aplicaciones privadas, manteniendo seguros los datos críticos
- **Acelera la adopción de zero trust**, elimina la complejidad de la gestión de seguridad y reduce las solicitudes de soporte técnico

Después de realizar una prueba de valor (PoV), seleccionamos Zscaler por su arquitectura moderna, que nos permitía poner nuestra pila de seguridad en la nube y optimizar una fuerza de trabajo remota.

David Petroski
Arquitecto senior de Infraestructura, Southwest Gas

Ver historia de éxito

United Airlines detecta y bloquea amenazas en constante cambio con Zero Trust Exchange

Zscaler elimina un 40 % más de amenazas que las soluciones anteriores para proteger a 80 000 usuarios globales y ofrecer viajes más seguros a 143 millones de pasajeros

INSTANTÁNEA DE UNITED AIRLINES

Compañía de aviación estadounidense y tercera aerolínea más grande del mundo, que opera en 48 países

- Servicios de transporte
- Chicago, Illinois, Estados Unidos
- Más de 80 000 empleados en más de 350 ubicaciones

6

meses para la transformación zero trust

1PB

del tráfico TLS inspeccionado

Más de 3 millones de dólares estadounidenses

ahorro de costes en comparación con las soluciones tradicionales

Desafíos

- Una arquitectura tradicional basada en perímetros y dependiente de centros de datos no podía soportar una transformación digital acelerada
- Los cortafuegos y VPN tradicionales carecían de la agilidad para escalar con el aumento del trabajo remoto, lo que ponía en riesgo a los usuarios y los datos.
- Los productos de seguridad puntuales anteriores carecían de capacidades avanzadas de detección de amenazas, lo que exponía una superficie de ataque más amplia

Proceso por fases

1. **Se proporcionó conectividad segura y directa a Internet y aplicaciones SaaS** para garantizar una protección constante para los usuarios en cualquier lugar
2. **Se reemplazaron las VPN con políticas de acceso zero trust y con el mínimo privilegio** para proteger aplicaciones y datos privados de posibles vulneraciones
3. **Se aprovecharon las integraciones en la nube y las funciones de supervisión de experiencias** para aumentar la visibilidad en tiempo real de las amenazas

Resultados

- **Permite que 80 000 empleados trabajen de forma segura desde cualquier ubicación** y protege el acceso remoto a más de 2000 aplicaciones privadas críticas
- **Reduce la complejidad y los costes de la arquitectura:** no se necesitan cortafuegos en los aeropuertos y se eliminan seis productos de seguridad puntuales
- **Unifica el ecosistema de seguridad y aplica dinámicamente políticas** para bloquear un 40 % más de amenazas y mejorar la postura de seguridad

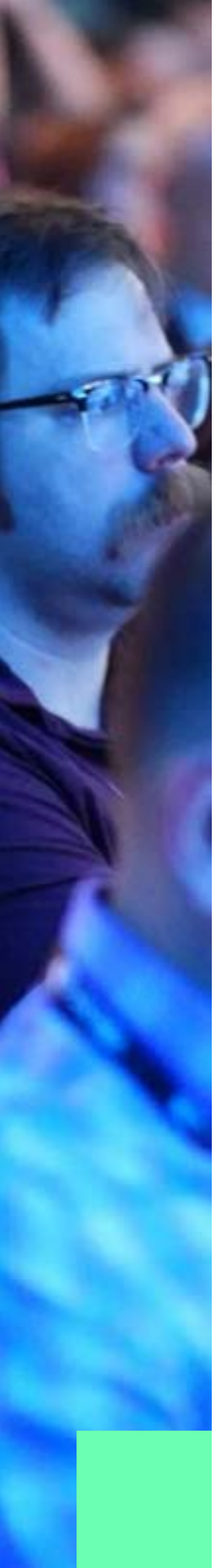
Zscaler nos brinda la tranquilidad de que el tráfico será seguro, independientemente de la red subyacente, para nuestros empleados, clientes y socios.

Deneen DeFiore
Vicepresidente y director de información
Oficial de seguridad, United Airlines

Ver historia de éxito

Región EMEA

Explore las historias de éxito de los clientes por región



01
Austria
36 Raiffeisen Bank

02
Alemania
38 Capital del estado: Magdeburgo

03
Italia
40 Cisalfa Sports

04
Noruega
42 Hydro

05
Sudáfrica
44 Capitec

06
España
46 Noatum
48 Sanitas

07
Unido Reino
50 Colt
52 Primetals Technologies
54 Unilever

Raiffeisen Bank International

Raiffeisen Bank International transforma la seguridad con Zero Trust Exchange

Zscaler reemplaza los dispositivos heredados para brindar protección integral frente a amenazas, permitir la flexibilidad de trabajar desde cualquier lugar y reducir los costes de seguridad

INSTANTÁNEA DEL RAIFFEISEN BANK

Uno de los principales bancos corporativos y de inversión de Austria

Servicios financieros y seguros

Viena, Austria

Millones de clientes en 12 mercados

44 000
empleados protegidos por zero trust

18,6 millones
clientes disfrutan de una banca segura

Una
plataforma ofrece zero trust total

Desafíos

- Una infraestructura de seguridad tradicional no era compatible con un enfoque centrado en la nube, lo que ponía en riesgo a los usuarios y las cargas de trabajo
- Los dispositivos de seguridad heredados no admitían la flexibilidad de trabajar desde cualquier lugar, lo que generaba latencia y un rendimiento deficiente
- Las VPN no permitieron el acceso basado en identidad para aplicaciones privadas, lo que generaba políticas inconsistentes y una superficie de ataque más amplia

Proceso por fases

1. **Se implementó una plataforma zero trust integral**, aprovechando los servicios públicos y privados para proteger a los usuarios en cualquier ubicación
2. **Conectividad directa a Internet segura sin retorno** para garantizar experiencias de usuario consistentes para un personal híbrido
3. **Se reemplazaron los dispositivos VPN con acceso zero trust para aplicaciones privadas** y se perfeccionaron las políticas de acceso basadas en identidad

Resultados

- **Asegura la conectividad entrante y saliente para un personal híbrido**, brindando protección consistente en cada ubicación
- **Reduce la latencia y mejora el rendimiento de aplicaciones privadas y SaaS** para mejorar las experiencias de los usuarios en la oficina y de forma remota
- **Optimiza la arquitectura de seguridad y ofrece protección integral contra amenazas** al tiempo que reduce el gasto en seguridad

La asociación con Zscaler nos brindó mayor seguridad, menores costes y una mejor experiencia de usuario al aplicar nuestros principios zero trust.

Peter Gerdenitsch
Director de Seguridad de la Información del Grupo, Raiffeisen Bank International

Ver historia de éxito

El Ayuntamiento de Magdeburgo asegura su transformación digital con Zero Trust Exchange

La capital del estado alemán reemplaza los dispositivos VPN y potencia un personal híbrido al tiempo que sienta las bases para una evolución digital continua con Zscaler

INSTANTÁNEA DE LA CAPITAL DEL ESTADO DE MAGDEBURGO

Proporciona servicios administrativos a los residentes de la capital de Sajonia-Anhalt

Federal y Gobierno

Magdeburgo, Alemania

2500 empleados

2500
empleados híbridos protegidos

230 000
residentes de la ciudad atendidos

Una
solución de un solo proveedor para simplificar la seguridad

Desafíos

- Una arquitectura de seguridad tradicional basada en hardware no era lo suficientemente ágil para respaldar los objetivos de transformación digital
- Las soluciones de proxy y cortafuegos heredadas no se podían ajustar para garantizar la conectividad a Internet para un personal cada vez más híbrido
- Las VPN no permitían un control de acceso granular, lo que ponía en mayor riesgo las aplicaciones privadas y limitaba las capacidades de trabajo remoto

Proceso por fases

1. **Se implementó una plataforma zero trust nativa de la nube** para modernizar la arquitectura de seguridad y permitir una mayor transformación digital
2. **Se introdujo una conectividad a Internet segura y directa**, aprovechando la funcionalidad de inspección de tráfico incorporada para gestionar las amenazas
3. **Acceso seguro a aplicaciones privadas con controles zero trust basados en identidad**, lo que garantiza una protección constante para datos críticos

Resultados

- **Mejora las experiencias de los usuarios para un personal híbrido** y permite el trabajo remoto seguro para hasta 1500 usuarios por mes
- **Reduce los costes de seguridad y la complejidad de la gestión** con una arquitectura que retira los productos puntuales de seguridad heredados
- **Acelera los futuros esfuerzos de transformación digital** con una arquitectura de seguridad zero trust integral y escalable

Queríamos ser un faro para otros municipios y animarles a evaluar e implementar buenas soluciones para la empresa, tal como hicimos con una solución de seguridad basada en la nube.

Dr. Tim Hoppe
Oficina de Estadísticas, Elecciones y Digitalización, Ciudad de Magdeburgo

Ver historia de éxito

Cisalfa Sport fortalece su postura de seguridad al acelerar la implementación de Zscaler en menos de tres meses

La plataforma zero trust reduce la superficie de ataque y garantiza una experiencia de usuario perfecta para empleados y usuarios externos

INSTANTÁNEA DE CISALFA SPORT

El minorista deportivo omnicanal líder de Italia

- Venta minorista y mayorista
- Curno (BG), Italia
- Más de 3600 empleados

2,5
meses para implementar Zscaler en toda la empresa

Más de 130
socios y contratistas externos de forma segura acceden a aplicaciones privadas e infraestructura local

70 %
de usuarios incorporados en el plazo de 2 semanas desde el despliegue

Desafíos

- La VPN permitía a todos los empleados y terceros tener acceso no segmentado a toda la red corporativa, aumentando el riesgo y el radio de explosión de posibles ataques
- Dos soluciones VPN heredadas tenían políticas y configuraciones conflictivas, lo que generaba problemas inconsistentes de seguridad y gestión de seguridad
- El acceso a las aplicaciones a través de VPN generaba un rendimiento lento y un gran volumen de tickets de soporte técnico de usuarios internos y externos

Proceso por fases

1. **Se redujo la superficie de ataque** reemplazando las VPN vulnerables con acceso directo del usuario a la aplicación privada
2. **Se evitó el movimiento lateral de amenazas** mediante la aplicación de políticas de acceso con privilegios mínimos para todos los usuarios
3. **Se mejoró la experiencia del usuario** con un mejor rendimiento y confiabilidad de la aplicación: no más interrupciones ni múltiples inicios de sesión de VPN para acceder a los recursos

Resultados

- **Mejora la postura de seguridad general** al brindar acceso directo de usuario a la aplicación a todos los usuarios y una aplicación de políticas consistente
- **Permite un acceso sin inconvenientes, transparente y sin cliente** a aplicaciones y datos privados para socios y contratistas
- **Reduce los tickets de soporte técnico relacionados con la latencia** con una conectividad ultrarrápida entregada a través del punto de presencia más cercano

Zero Trust Exchange de Zscaler cubre todas las bases: acceso más rápido y seguro a las aplicaciones sin necesidad de VPN, reducción de riesgos en todo el entorno y un camino explícito hacia la expansión de zero trust.

Fabio Freti
Operaciones e infraestructura de TI
Gerente de Cisalfa Sport

Ver historia de éxito

Hydro refuerza su postura de seguridad y sus esfuerzos de sostenibilidad con Zero Trust Exchange

Zscaler reduce la superficie de ataque y la huella de carbono mientras el proveedor de energía renovable busca retirar el hardware heredado y convertirse en un proveedor 100 % de nube

INSTANTÁNEA DE HIDRO

Una de las mayores empresas de energía renovable del mundo, con presencia en 40 países.

Fabricación

Oslo, Noruega

31 000 empleados

33 000
empleados protegidos con zero trust

Uno
enfoque del proveedor para reducir costes y complejidad

100 %
Operaciones de la nube objetivo

Desafíos

- La infraestructura y el hardware de seguridad heredados consumían mucha energía y no se alineaban con los objetivos de sostenibilidad corporativa
- Una red MPLS de bajo ancho de banda no podía escalar para soportar un aumento en el tráfico de datos vinculados a la nube, lo que genera un rendimiento deficiente
- Las VPN tradicionales con políticas de acceso de todo o nada ponen en riesgo la red, lo que resulta en un costoso ataque de ransomware

Proceso por fases

1. **Se aprovisionó una conectividad segura y directa a Internet**, lo que elimina el tráfico de retorno y mejora la confiabilidad del acceso
2. **Se reemplazaron las VPN heredadas con acceso zero trust basado en políticas** para aplicaciones privadas a fin de proteger los datos de ciberataques
3. **Se implementó una solución de supervisión de experiencias diseñada específicamente para el tráfico en la nube** para permitir una resolución más rápida de los problemas de los usuarios

Resultados

- **Elimina la dependencia de productos puntuales heredados** y reduce la huella de carbono con una plataforma de seguridad multiinquilino nativa de la nube
- **Mejora el rendimiento de las aplicaciones SaaS**, mejorando las experiencias de los usuarios para 33 000 empleados en 140 ubicaciones
- **Reduce los costes y la complejidad de la gestión al tiempo que mejora la postura de seguridad** mediante una solución de proveedor único para zero trust

Con Zscaler Private Access, los usuarios ya no necesitaban conectarse a la red para usar nuestras aplicaciones privadas. Ahora, a medida que continuamos evolucionando nuestro lugar de trabajo moderno, avanzamos hacia la retirada definitiva de la VPN.

Armin Auth
Director de Programas Estratégicos de I&T

Ver historia de éxito

Capitec acelera la transformación digital y protege los datos financieros con Zscaler

El mayor banco de Sudáfrica implementa seguridad Zero Trust en tres meses, protegiendo a 17 OOO usuarios y bloqueando 745 OOO amenazas en Zero Trust Exchange

INSTANTÁNEA DE CAPITEC

El mayor banco de Sudáfrica, que atiende a 21 millones de personas y está clasificado en el primer puesto en satisfacción del cliente

- Servicios financieros y seguros
- Ciudad del Cabo, Sudáfrica
- 15 45O empleados en 86O sucursales

3
segundos para migrar aplicaciones privadas a AWS

125 millones
infracciones de políticas prevenidas en un año

3
meses para implementar de manera integral confianza cero

Desafíos

- La arquitectura de seguridad basada en el perímetro no podía proteger eficazmente los datos financieros de alto valor contra el riesgo y la pérdida
- Los dispositivos de seguridad heredados, como los cortafuegos y las VPN, eran complejos de administrar y la productividad de los usuarios se veía afectada
- La visibilidad limitada sobre la experiencia del usuario impedía un enfoque proactivo para la identificación y resolución de problemas

Proceso por fases

1. **Se aseguró la conectividad directa a Internet y aplicaciones SaaS**, aprovechando la inspección del tráfico para evitar la vulneración de datos
2. **Se retiraron dispositivos VPN heredados, introduciendo acceso zero trust** para aplicaciones privadas y datos financieros confidenciales
3. **Se aprovecharon capacidades avanzadas de experiencia digital y conocimientos prácticos** para resolver problemas duraderos de experiencia del usuario

Resultados

- **Protege el acceso a Internet y a las aplicaciones en la nube para 17 000 usuarios**, evitando 125 millones de infracciones de políticas al año
- **Protege una aplicación de banca privada a la que acceden más de 11 millones de clientes** con acceso zero trust basado en políticas
- **Permite una transformación digital más rápida:** sólo se necesitan unos segundos para migrar aplicaciones a AWS sin tiempo de inactividad ni fallos de seguridad

Incorporamos Zero Trust Exchange a nuestro entorno y nuestros agentes de software de seguridad zero trust se implementaron para todos nuestros usuarios en tres meses.

Andrew Baker
Director de Tecnología, Capitec

Ver historia de éxito

Noatum implementa un conjunto de tecnologías Zscaler para respaldar una variedad de casos de uso

Incluye Internet seguro, SaaS y acceso a aplicaciones privadas, detección mejorada de ciberamenazas y experiencias de usuario optimizadas

INSTANTÁNEA DE NOATUM

Noatum es un grupo multinacional líder en servicios de transporte y logística

Servicios de transporte

Barcelona, España

Más de 4300 empleados

Día 1
Valor inmediato de la plataforma

Sin
dependencia de VPN y cortafuegos

360
grados de cuantificación del riesgo

Desafíos

- Las VPN tradicionales dejaban a la organización demasiado expuesta a ciberataques cuando los usuarios accedían a Internet
- La seguridad heredada, como los cortafuegos, dejaba a la organización sin poder inspeccionar el tráfico cifrado
- las arquitecturas basadas en perímetros hacían que la incorporación de fusiones y adquisiciones tardara mucho más de lo que debería

Proceso por fases

1. **Se reemplazaron las VPN** por una plataforma en la nube permiten un acceso seguro a Internet y a aplicaciones privadas
2. **Se creó un centro de supervisión de experiencias único basado en la nube** con ZDX
3. **Evalúa el riesgo empresarial** de forma integral con Zscaler Risk360

Resultados

- **Permite trabajar desde cualquier lugar** con confianza con un acceso de usuario seguro y sin inconvenientes
- **Minimiza los incidentes de los usuarios** y mejora el análisis de la causa raíz, brindando conocimiento y agilidad
- **Mejora la evaluación de riesgos** y la defensa contra amenazas al ocultar sistemas y aplicaciones de Internet

La VPN tradicional era el problema, la exposición que teníamos en los servicios de Internet y el riesgo de recibir ataques constantemente; este fue realmente el catalizador para que buscáramos una solución como Zscaler.

Josep Pou
Director de Seguridad de la Información de Noatum

Ver historia de éxito

Sanitas
Parte de Bupa

Sanitas ofrece conectividad segura y sin interrupciones con Zscaler Internet Access

Implementación de protecciones para Internet, SaaS y aplicaciones privadas para más de 12 000 usuarios, donde sea que trabajen

INSTANTÁNEA DE SANITAS

Sanitas Una gran compañía de seguros médicos de alto crecimiento

Sanidad y farmacia

Madrid, España

Más de 11 700 empleados en España, Europa y Latinoamérica

2,5
meses para desplegar en todos los usuarios

12000 – 15000
usuarios protegidos por nuestra plataforma

Sin
necesidad de conectar a un centro de datos

Desafíos

- Las unidades de negocio separadas implicaban medios de seguridad separados sin un modelo basado en la nube
- Las VPN creaban un proceso tedioso de autenticación de usuarios con una seguridad mediocre
- Las oficinas asociadas no podían conectarse a los centros de datos y no podían acceder a las aplicaciones

Proceso por fases

1. Implementa zero trust homogénea basada en la nube para proteger toda la organización a escala
2. Se reemplazaron las VPN con un modelo zero trust para mejorar la conectividad de todos los usuarios independientemente de su ubicación
3. Ofrece acceso seguro y sin inconvenientes a las aplicaciones para todos los usuarios, incluidos los socios

Resultados

- Protege entre 12000 y 15000 usuarios en 2,5 meses con Zscaler Internet Access
- Permite trabajar desde cualquier lugar, lo que posibilita una actividad empresarial flexible y ágil con una experiencia similar a la de una oficina
- Proporciona acceso seguro a cargas de trabajo y aplicaciones

Hoy en día, los empleados pueden trabajar desde casa, igual que trabajan desde la oficina, de forma transparente, flexible, súper ágil y sin esas barreras que solíamos tener con otras soluciones.

Antonio Cerezo
Responsable de Ciberseguridad para Europa y Latinoamérica

Ver historia de éxito

Colt Technology Services mejora la seguridad y la experiencia digital con Zero Trust Exchange

La asociación con Zscaler para implementar una arquitectura zero trust en tres meses permite a la empresa ayudar a otras empresas a lograr la transformación de la seguridad

INSTANTÁNEA DE COLT TECHNOLOGY SERVICES

Proporciona servicios de red, voz y centro de datos a más de 25 000 empresas en todo el mundo

Telecomunicaciones

Londres, Reino Unido

Más de 5000 empleados en 60 oficinas en todo el mundo

5000
empleados híbridos protegidos

83 %
implementación más rápida que las soluciones tradicionales

100 millones
infracciones de políticas evitadas trimestralmente

Desafíos

- La aceleración de la migración a la nube para respaldar un entorno de trabajo híbrido aumentaba la superficie de ataque y el riesgo de vulneración
- Una solución de proxy obsoleta no podía gestionar la inspección en línea del tráfico cifrado, lo que generaba puntos ciegos de malware
- Los dispositivos VPN heredados no permitían políticas dinámicas de acceso a aplicaciones privadas, lo que dificultaba mantener el trabajo remoto

Proceso por fases

1. **Implementó una arquitectura de seguridad zero trust nativa de la nube** para respaldar las operaciones comerciales prioritarias en la nube y el trabajo híbrido
2. **Se procuró acceso seguro y directo a Internet**, inspeccionando todo el tráfico cifrado para detener las amenazas y la pérdida de datos
3. **Se sustituyeron los dispositivos VPN heredados para implantar acceso zero trust a aplicaciones privadas**, lo que hace que el trabajo remoto sea más fácil y seguro

Resultados

- **Proporciona experiencias digitales excepcionales para más de 5000 empleados híbridos** al tiempo que protege el tráfico entrante y saliente
- **Inspecciona el tráfico de Internet a gran escala**, procesa 6700 millones de transacciones y bloquea 476 000 amenazas de seguridad trimestralmente
- **Admite políticas de acceso a aplicaciones privadas basadas en políticas y microsegmentadas** que no son posibles con las VPN tradicionales

Zscaler nos ayuda a lograr tanto la experiencia del usuario como la seguridad. La plataforma nativa de la nube Zscaler protege a nuestros empleados sin importar dónde trabajen ni los dispositivos que usen.

Ash Surti
Director de Información y Tecnología Digital, Colt Technology Services

Ver historia de éxito

Primetals Technologies crea un lugar de trabajo híbrido seguro con Zscaler Zero Trust Exchange

El líder mundial en producción de metales abandona los centros de datos y consolida una pila de seguridad heredada para acelerar la transformación digital con Zscaler

INSTANTÁNEA DE PRIMETALS TECHNOLOGIES

Líder mundial en soluciones para plantas metalúrgicas, especializado en producción de acero

Alta tecnología

Londres, Reino Unido

Más de 7500 empleados

7500
usuarios protegidos con zero trust

Hasta un 35 %
de reducción de costes de infraestructura

4,53/5
índice de satisfacción de los empleados

Desafíos

- Una pila de seguridad tradicional construida alrededor de centros de datos no se podía ajustar para soportar la transformación digital que prioriza la nube
- Los dispositivos de seguridad heredados, incluidos los cortafuegos y las VPN, no eran lo suficientemente ágiles para soportar un nuevo rediseño de la red SD-WAN
- Los dispositivos VPN obsoletos no protegían eficazmente la conectividad remota para un personal híbrido y disperso globalmente

Proceso por fases

1. **Se implementó conectividad directa a Internet compatible con SD-WAN** para optimizar la infraestructura y mejorar el rendimiento
2. **Se sustituyeron las VPN por acceso zero trust para aplicaciones privadas** que permiten trabajar desde cualquier lugar de forma segura para usuarios de todo el mundo
3. **Se aprovecharon las funciones avanzadas de supervisión de la experiencia del usuario** para garantizar que las herramientas de colaboración del personal funcionen de manera óptima

Resultados

- **Simplifica la pila de seguridad**, reduce la dependencia de los centros de datos y disminuye el gasto en costes generales de infraestructura
- **Garantiza una conectividad entrante y saliente fluida** para un grupo de usuarios híbrido, el 25 % de los cuales trabaja de forma totalmente remota
- **Reduce el volumen de tickets de soporte técnico y resuelve problemas más rápidamente**, mejorando la experiencia del usuario final y aliviando la sobrecarga administrativa

Durante la transición a la nube, fue necesario modernizar la pila de seguridad. Zscaler Zero Trust Exchange desempeñó un papel fundamental para hacer realidad esa visión.

Ralph Deleja-Hotko
Responsable de Soluciones de back-end y de la nube, Primetals Technologies

Ver historia de éxito

Unilever mejora la seguridad global y logra el acceso idóneo a las aplicaciones con Zero Trust

Zscaler permite a Unilever eliminar las VPN, brindar a los usuarios una conectividad directa segura a las aplicaciones e Internet y agilizar las operaciones en 190 países

INSTANTÁNEA DE UNILEVER

Compañía global de bienes de consumo cuyos productos son utilizados diariamente por 3400 millones de personas

Fabricación

Londres, Reino Unido

Ventas en 190 países

Más de 3000 millones

transacciones detalladas protegidas semanalmente

99.9 %

tiempo de actividad durante el procesamiento de 220 TB de datos en dos meses

Más de 1500

aplicaciones administradas con el acceso zero trust necesario

Desafíos

- Las VPN tradicionales tenían una flexibilidad limitada y no podían escalar con la estrategia de nube global de Unilever
- El modelo de seguridad tradicional aumentaba el riesgo debido al control de acceso y la visibilidad insuficientes
- La creciente demanda de acceso remoto sobrecargaba la infraestructura de VPN, lo que afectaba a la experiencia del usuario

Proceso por fases

1. **Se habilitó acceso seguro a los usuarios a Internet y a SaaS** con inspección completa del tráfico TLS/SSL y protección avanzada contra amenazas
2. **Se reemplazó laVPN** por acceso zero trust a aplicaciones privadas
3. **Se mejoró la experiencia del usuario** al brindar supervisión de la experiencia digital para identificar y resolver problemas de rendimiento rápidamente

Resultados

- **Reduce el riesgo** con acceso seguro y directo a las aplicaciones y sin las limitaciones y vulnerabilidades de las VPN
- **Mejora la eficiencia operativa** al procesar el tráfico de datos a gran escala con un tiempo de actividad del 99,99 %
- **Apoya la estrategia global de la nube** al brindar acceso remoto seguro en 190 países y mantener la flexibilidad para el personal de Unilever

El enfoque zero trust de Zscaler ha transformado la seguridad en Unilever. La eliminación de los cuellos de botella de las VPN permite a nuestro personal global acceder de forma segura a las aplicaciones, lo que mejora el rendimiento, la flexibilidad y la resiliencia.

Richard Mardling
Director de Acceso
y Conectividad, Unilever

Ver historia de éxito

Región APJ

Explore las historias de éxito de los clientes por región

01
Australia

58 John Holland
60 Probe CX

02
India

62 Persistent Systems

03
Japón

64 Keiju Medical Center
66 The Bank of Saga

04
Filipinas

68 Cebu Pacific Air

05
Singapur

70 Maxeon

John Holland reduce los costes de red en un 50 % utilizando Zero Trust Exchange

Zscaler facilita la transición a SD-WAN y permite el reemplazo de cientos de cortafuegos, lo que mejora la eficiencia operativa y la postura de seguridad

INSTANTÁNEA DE JOHN HOLLAND

Empresa integrada de infraestructuras, edificación, ferrocarril y transporte multimodal

Construcción

Melbourne, Victoria, Australia

Más de 5000 empleados en más de 120 ubicaciones

1 semana
para la puesta en marcha confianza cero

6000
personal y contratistas protegidos

122 000
amenazas bloqueadas en tres meses

Desafíos

- Una arquitectura de seguridad perimetral tradicional no podría escalar para soportar operaciones comerciales cada vez más centradas en la nube
- Una red MPLS obsoleta dependía de un importante retorno de tráfico, lo que reducía la velocidad de los servicios de TI y aumentaba los costes
- Los dispositivos de cortafuegos heredados carecían de la agilidad para inspeccionar el tráfico cifrado en línea, lo que aumentaba la vulnerabilidad a las amenazas

Proceso por fases

1. **Se implementó una plataforma de seguridad integral zero trust nativa de la nube** para crear un entorno de TI más ágil y escalable
2. **Menor dependencia de dispositivos de cortafuegos y costes de red** con acceso directo y seguro a Internet y aplicaciones SaaS
3. **Se aprovecharon las funciones avanzadas de detección de amenazas para optimizar el ecosistema de seguridad** y eliminar el riesgo de vulneración de datos

Resultados

- **Migra el 100 % de los usuarios a zero trust en una semana** y permite un acceso más rápido a la red en más de 120 sitios de proyectos
- **Retira cientos de dispositivos de cortafuegos heredados con conectividad zero trust**, lo que permite una reducción del 50 % en los costes de red
- **Asegura la conectividad de los usuarios,** procesa 400 TB de tráfico y previene 98 millones de infracciones de políticas trimestralmente

Zscaler proporciona el resto de nuestra seguridad que ha simplificado nuestros procesos y, a través de esa simplificación, nos ha hecho mucho más seguros.

Kier Morrison
John Holland, director general de Operaciones de Tecnología de TI

Ver historia de éxito

Probe CX elimina progresivamente las VPN para proteger a 7600 empleados y aplicaciones críticas con Zero Trust Exchange

Zscaler optimiza la pila de seguridad, simplifica la gestión de políticas y reduce el gasto en tecnología al tiempo que mantiene un gran nivel protección

INSTANTÁNEA DE PROBE CX

Uno de los mayores subcontratistas de procesos comerciales y de experiencia del cliente de Australia

Servicios

Melbourne, Victoria, Australia

19 000 empleados, operaciones en 32 lugares de entrega

100 %
de las VPN siendo retiradas

8100 millones
transacciones procesadas en un trimestre

3,1 millones
Amenazas bloqueadas en tres meses

Desafíos

- Una arquitectura de seguridad tradicional no se podía ajustar con un personal en rápido crecimiento o un enfoque en evolución que priorice la nube
- Las VPN tradicionales no permitían políticas de control de acceso microsegmentadas, lo que ponía en mayor riesgo las aplicaciones privadas
- La visibilidad limitada de la experiencia del usuario y el rendimiento de la aplicación hizo que mitigar los problemas fuera complicado y llevara mucho tiempo

Proceso por fases

1. **Se protegió la conectividad directa a Internet y aplicaciones SaaS**, inspeccionando el tráfico en línea, sin necesidad de retorno
2. **Se reemplazaron las VPN con acceso zero trust para aplicaciones privadas** a fin de proteger mejor la propiedad intelectual y los datos críticos
3. **Se aprovecharon las capacidades avanzadas de experiencia del usuario** para resolver problemas más rápido y permitir una experiencia de trabajo remoto fluida.

Resultados

- **Proporciona flexibilidad para trabajar desde cualquier lugar respaldada por principios zero trust** para 7600 usuarios en cinco países
- **Procesa aproximadamente 285 TB de tráfico por trimestre**, aplicando políticas de seguridad consistentes y minimizando la superficie de ataque
- **Simplifica la gestión de la seguridad con una plataforma multiinquilino** que ofrece seguridad zero trust a un menor TCO

Algunas de las ventajas clave que hemos obtenido al implementar esta tecnología es que hemos podido deshacernos del 100 % de esas VPN en el entorno.

Rohan Khanna
Director de Tecnología, Probe CX

Ver historia de éxito

Persistent

Persistent aumenta la seguridad mientras ahorra 2 millones de dólares estadounidenses en costes Capex/Opex interanuales

Zero trust protege los datos confidenciales de los clientes y de la propiedad intelectual, permite la innovación, reduce la complejidad y respalda los objetivos ambientales, sociales y de gobernanza (ESG)

INSTANTÁNEA DE PERSISTENT

Un socio global de ingeniería digital y modernización empresarial que ayuda a las empresas a avanzar en la innovación

Alta tecnología

Pune, India

23 000 empleados en 21 países

85 %

Mejora de la postura de seguridad mediante la eliminación de VPN

más de 80

ataques de alta prioridad interceptados en 90 días con engaño

4X

acceso más rápido a aplicaciones privadas que con VPN

Desafíos

- Proporcionar a los trabajadores remotos en 21 países una conectividad rápida y una experiencia de usuario más productiva
- Protección de la propiedad intelectual y los datos confidenciales de los clientes en el entorno de la nube
- Simplificando una infraestructura compleja
- Reducción de los costes operativos y de hardware en todo el entorno
- Encontrar un socio de zero trust a largo plazo con una solución escalable que fomente una rápida expansión
- Minimizar el impacto ambiental reduciendo la huella de carbono

Proceso por fases

1. **Se mejoró la postura de seguridad** con conexiones seguras y directas a Internet, SaaS y aplicaciones privadas
2. **Se redujo la latencia, se redujeron los costes y se mejoró la experiencia del usuario** eliminando VPN y cortafuegos poco confiables y no seguros
3. **Se protegieron la valiosa propiedad intelectual y los datos de sus clientes con** tecnología avanzada de prevención de pérdida de datos (DLP) y detección de engaño

Resultados

- **Mejora y acelera por 4 el acceso remoto** para 23 OOO trabajadores distribuidos globalmente
- **Elimina la complejidad** y mejora la eficacia y eficiencia de la seguridad
- **Acelera la detección y la respuesta** mediante la integración con CrowdStrike, Microsoft Entra ID y Securonix
- **Amplía la cartera** de ofertas de la empresa con una práctica de seguridad centrada en Zscaler para sus propios clientes

Zscaler DLP brinda al equipo de seguridad una vista granular del uso de aplicaciones de inteligencia artificial generativa en la sombra, incluidas las solicitudes de entrada, y aplica el bloqueo de DLP y el aislamiento de aplicaciones en tiempo real.

Debashis Singh
Director de Información, Persistent

Ver historia de éxito

社会医療法人財団善仙会
恵寿総合病院
Keiju Medical Center

Keiju Medical Center transforma la atención digital al paciente con Zero Trust Exchange

Zscaler proporciona una solución para el acceso móvil seguro a los datos del EMR, permite a los médicos colaborar desde cualquier lugar y mejora las experiencias de los pacientes

INSTANTÁNEA DE KEIJU MEDICAL CENTER

El único hospital de apoyo médico de la región de Noto, reconocido como líder digital

Sanidad y farmacia

Ciudad de Nanao, Prefectura de Ishikawa, Japón

Más de 800 empleados para más de 400 camas

800
personal médico protegido

100s
de dispositivos móviles conectados de forma segura

Una
plataforma de seguridad zero trust

Desafíos

- Una arquitectura de seguridad perimetral no podía adaptarse a la creciente necesidad de atención al paciente digital y telemedicina
- Los cortafuegos heredados no podían proteger la conectividad a Internet de forma remota, lo que limitaba la contratación de médicos a una pequeña área local
- Las VPN tradicionales ponían en mayor riesgo de vulnerabilidad las aplicaciones y los recursos privados, incluidos los datos confidenciales de los pacientes

Proceso por fases

1. **Se implementó una arquitectura de seguridad zero trust nativa de la nube** para respaldar formas alternativas de brindar atención digital al paciente
2. **Se introdujo una conectividad segura y directa a Internet**, lo que permite al personal médico trabajar de manera flexible y segura desde cualquier ubicación
3. **Se eliminaron los dispositivos VPN y se adoptó el acceso zero trust** para aplicaciones privadas a fin de proteger el acceso remoto a los datos de EMR

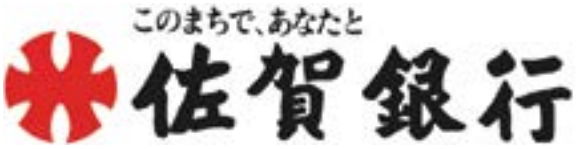
Resultados

- **Permite la flexibilidad de trabajar desde cualquier lugar para el personal médico** y amplía la contratación de médicos de calidad
- **Protege los registros confidenciales de pacientes frente a amenazas** cuando se accede a ellos de forma remota: más de 500 dispositivos móviles se conectan de forma segura a los datos del EMR
- **Elimina la necesidad de dispositivos de seguridad heredados** y mejora la eficiencia operativa, lo que conduce a una mejor atención al paciente

La transformación digital es esencial para garantizar que el personal pueda trabajar eficientemente con recursos limitados. Muchos médicos viven más lejos, por lo que necesitábamos un entorno de acceso remoto seguro y fácil de usar.

Señor Masahiro Kamino
Presidente del Consejo de Administración, Keiju Medical Center

Ver historia de éxito



The Saga Bank apoya la transformación digital en Zero Trust Exchange

Zscaler optimiza la infraestructura y reduce la dependencia de soluciones heredadas, y fortalece la postura de seguridad a medida que las operaciones bancarias migran a la nube

INSTANTÁNEA DE THE BANK OF SAGA

Proveedor de servicios financieros centrado en la comunidad que trabaja para mejorar la comodidad del cliente

- Servicios financieros y seguros
- Ciudad de Saga, prefectura de Saga, Japón
- Más de 1,200 empleados

~33 %
menores costes de comunicación

18 000
usuarios protegidos con zero trust

Un
inicio de sesión único aumenta la productividad

Desafíos

- Una arquitectura de seguridad tradicional basada en perímetro no respaldaba los continuos esfuerzos de migración a la nube del banco
- Los dispositivos de seguridad tradicionales carecían de la agilidad para escalar ante las crecientes necesidades de conectividad a Internet directa y confiable
- Las VPN eran costosas de mantener y aumentaban la superficie de ataque, dejando las aplicaciones y los datos privados vulnerables a las amenazas.

Proceso por fases

1. **Se implementó una plataforma zero trust integral y nativa de la nube** para aplicar políticas de seguridad consistentes en toda la empresa
2. **Se introdujo la conectividad directa a Internet** y se aprovechó la inspección de tráfico en línea para proteger el acceso a las aplicaciones SaaS públicas
3. **Se reemplazaron las VPN con acceso zero trust para aplicaciones privadas**, aprovechando opciones de configuración granular para proteger datos críticos

Resultados

- **Asegura la conectividad entrante y saliente para los empleados**, aplicando políticas de acceso consistentes independientemente de la ubicación
- **Protege las aplicaciones de banca privada y los datos críticos contra riesgos**, asegurando y mejorando las experiencias del cliente
- **Optimiza la pila de seguridad y reemplaza los dispositivos heredados**, simplificando la gestión de políticas y reduciendo costes

La transición a la nube es necesaria para la transformación digital. ... [No obstante,] la seguridad de límites convencional no permite aprovechar al máximo la comodidad de los servicios web y SaaS. La seguridad zero trust era esencial.

Sr. Hiroaki Hayashida
Director Adjunto, Grupo de Planificación y Desarrollo de Sistemas, Departamento de Sistemas, Sede de Gestión Empresarial, The Bank of Saga

Ver historia de éxito

Cebu Pacific Air protege su personal híbrido con Zero Trust Exchange

Zscaler mejora la experiencia de trabajo remoto para 3900 empleados y protege las operaciones comerciales críticas en siete centros estratégicos en Asia

INSTANTÁNEA DE CEBU PACIFIC AIR

Aerolínea líder en Filipinas, que opera vuelos a más de 60 destinos.

- Servicios de transporte
- Metro Manila, Filipinas
- 3900 empleados en siete centros estratégicos

234 millones
infracciones de políticas evitadas trimestralmente

90 %
aumento de la satisfacción del usuario

2
semanas para implementar el acceso zero trust remoto a aplicaciones

Desafíos

- Una infraestructura de seguridad heredada ralentizaba los esfuerzos de transformación digital y aumentaba la vulneración y las amenazas
- Los dispositivos de seguridad tradicionales no podían proteger adecuadamente los recursos privados críticos para las operaciones comerciales
- Los dispositivos VPN tenían problemas de rendimiento y conectividad, lo que hacía que el trabajo remoto fuera más difícil y menos seguro

Proceso por fases

1. **Se retiró una arquitectura de seguridad heredada obsoleta** y, en su lugar, se implementó una plataforma zero trust integral y nativa de la nube
2. **Se proporcionó acceso directo y seguro a Internet con funciones avanzadas de protección contra amenazas** para brindar un mejor soporte a un personal híbrido
3. **Se reemplazaron los dispositivos VPN tradicionales con acceso zero trust** para aplicar controles de acceso a aplicaciones privadas granulares

Resultados

- **Asegura la conectividad de trabajo desde cualquier lugar para 3900 usuarios con una alternativa VPN segura**, mejorando la satisfacción del usuario en un 90 %
- **Optimiza la pila de seguridad y al mismo tiempo proporciona una protección potente:** procesa 733 millones de transacciones al año
- **Previene 234 millones de infracciones de políticas y bloquea 45 000 amenazas de seguridad en un solo trimestre**, mejorando la postura de seguridad

Nuestro entorno de trabajo es dinámico y con Zscaler, los empleados pueden continuar trabajando productivamente sin obstaculizar su capacidad para conectarse a los recursos que necesitan sin comprometer la seguridad.

Laureen Cansana
Director de Información, Cebu Pacific Air

Ver historia de éxito

maxeon

Maxeon Solar Technologies logra la transformación digital con Zscaler tras una desinversión

El líder en energía solar elimina los centros de datos para mejorar la seguridad y las experiencias de trabajo remoto para 5000 usuarios globales con Zero Trust Exchange

INSTANTÁNEA DE MAXEON

Fabricante líder mundial de paneles solares con presencia comercial en más de 100 países

- Energía, petróleo, gas y minería
- Singapur
- 5000 empleados en 40 ubicaciones

134 %
más tráfico procesado trimestralmente

31 millones
infracciones de políticas evitadas en un trimestre

2,9 millones
amenazas bloqueadas en tres meses

Desafíos

- La seguridad perimetral tradicional construida alrededor de los centros de datos no era compatible con una infraestructura en evolución que prioriza la nube
- Los cortafuegos tradicionales no podían escalar con las crecientes necesidades de acceso remoto, lo que generaba un rendimiento deficiente y un mayor riesgo.
- Las soluciones DLP anteriores eran difíciles de gestionar y dejaban en riesgo la propiedad intelectual y los activos críticos.

Proceso por fases

1. **Se aseguró la conectividad directa a Internet con inspección de tráfico en línea** para proteger a los usuarios en cualquier lugar donde necesiten acceso en línea
2. **Se implementó una solución de supervisión de experiencias diseñada específicamente para zero trust** para agilizar los procesos de incorporación y concesión de licencias
3. **Se introdujo una solución DLP integrada** para salvaguardar la información crítica, garantizar el cumplimiento y prevenir infracciones de datos

Resultados

- **Acelera la transformación digital:** todos los centros de datos están desmantelados y el 70 % de las cargas de trabajo han migrado a la nube
- **Proporciona flexibilidad segura para trabajar desde cualquier lugar** para un grupo de usuarios dispersos geográficamente que trabajan en 16 países
- **Protege datos de propiedad intelectual esenciales, como más de 1400 patentes**, lo que mejora la postura de seguridad y garantiza la continuidad del negocio

Si bien evaluamos a varios proveedores de renombre, Zscaler resultó ser un claro ganador debido a su posición de liderazgo en el Cuadrante Mágico de Gartner y sus capacidades comprobadas.

Stephen Gani
Director de Seguridad de la Información, Maxeon Solar Technologies

Ver historia de éxito