Experiencias de Cliente

Explore historias de transformación del mundo real, impulsadas por Zscaler Zero Trust + IA.

Descubra cómo las empresas han elevado sus posturas de seguridad, fomentando experiencias de usuario excepcionales y simplificando las fusiones y adquisiciones y mucho más con Zero Trust + IA.

La obsesión por el cliente es uno de nuestros valores fundamentales en Zscaler, y como tal, estamos comprometidos a ofrecer lo mejor en innovación Zero Trust para ayudar a su organización a alcanzar sus objetivos. Con las capacidades básicas que ofrece nuestra plataforma Zero Trust Exchange, impulsada por la IA, hemos ayudado a más de 5000 empresas de todo el mundo a reducir costos y complejidad, simplificar sus arquitecturas de red, asegurar a sus usuarios y protegerse de las ciberamenazas en constante evolución. En este libro electrónico, se adentrará en los casos prácticos de algunas de las organizaciones más exitosas del mundo y en cómo han transformado sus redes, seguridad y operaciones con Zscaler.

Con más de 15 años como pionero en Zero Trust, Zscaler mantiene su compromiso de ayudar a organizaciones de todos los tamaños e industrias a alcanzar y superar sus objetivos Zero Trust. La única constante que conocemos en tecnología es el “cambio”, y con nuestra plataforma Zero Trust Exchange, las empresas pueden estar preparadas para lo que venga, sin dejar de innovar y transformar su infraestructura informática.

Mike Rich
CRO y Presidente de ventas globales

Contenido

Explore las experiencias de éxito de nuestros clientes por vertical del sector

01 Construcción

58 John Holland

02 Educación

28 Departamento de Educación de la Ciudad de Nueva York

03 Energía, petróleo, gas y minería

70 Maxeon
30 Southwest Gas

04 Entretenimiento y hospitalidad

22 MGM Resorts International

05 Ámbito federal y Gobierno

14 Gobierno de D.C.
38 State Capital Magdeburg

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
Sector sanitario y farmacéutico

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

AMS

Explore las historias de éxito de nuestros clientes por región

8 AMN Healthcare

10 ATN International

12 Cox Automotive

14 Gobierno de D.C.

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

VISIÓN GENERAL DE AMN HEALTHCARE

Ofrecer a los clientes soluciones relativas al personal sanitario para mejorar la atención a los pacientes

- Sector sanitario y farmacéutico
- Dallas, Texas, Estados Unidos
- Más de 10,000 clientes en 24 ubicaciones

1.2 mil millones

de transacciones web procesadas mensualmente

7 M

de amenazas bloqueadas en tres meses

Horas

para implementar un perímetro seguro en cualquier lugar

Problemas

- La infraestructura de seguridad heredada ya no era compatible con el ecosistema operativo en evolución de la empresa, que priorizaba la nube.
- Las VPN tradicionales no podían hacer frente a las crecientes necesidades de acceso remoto, dejando 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 etapas

1. **Se proporcionó acceso directo a Internet seguro**, lo que garantizaría un trabajo flexible desde cualquier lugar para una fuerza de trabajo dispersa globalmente
2. **Se introdujo el acceso a aplicaciones privadas microsegmentado y Zero Trust**, que ofrecería una alternativa segura a las VPN heredadas
3. **Se racionalizó la pila de supervisión y se aprovechó la visibilidad integral de extremo a extremo para** mejorar la resolución de problemas de los usuarios

Resultados

- **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 costos de tecnología** para lograr una postura de seguridad más sólida con menos gastos generales

El enfoque de Zscaler está alineado con nuestra filosofía general Zero Trust, y la plataforma Zero Trust Exchange fue la materialización 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 asegura 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 las VPN y garantiza una integración y una incorporación más seguras de las fusiones y adquisiciones.

VISIÓN GENERAL DE ATN INTERNATIONAL

Ofrece infraestructura y servicios de comunicaciones con experiencia en mercados remotos

- Telecomunicaciones
- Beverly, Massachusetts, Estados Unidos
- 750,000 clientes a nivel internacional

100 %
eliminación de las VPN y tickets de soporte de VPN

Todos
los empleados protegidos por Zscaler

Minutos
vs. horas para mitigar problemas de los usuarios

Problemas

- La infraestructura de seguridad local no podía respaldar de manera eficaz las operaciones empresariales orientadas a la nube ni los futuros objetivos de fusiones y adquisiciones
- Los dispositivos VPN heredados tuvieron dificultades para escalar con un aumento del trabajo a distancia, lo que provocó experiencias de usuario deficientes y un mayor riesgo
- Las soluciones de seguridad tradicionales no ofrecían las integraciones críticas en la nube para permitir la mitigación proactiva de los problemas de los usuarios

Proceso por etapas

1. **Se proporcionó acceso directo a Internet,** aprovechando las funciones de registro e inspección de tráfico para evitar violaciones de políticas
2. **Se sustituyeron los dispositivos VPN por un acceso Zero Trust y con privilegios mínimos** a las aplicaciones y recursos privados
3. **Se aprovecharon las funciones de Zscaler potenciadas por IA y la integración exhaustiva con Microsoft** para identificar y resolver los problemas de los usuarios con mayor rapidez

Resultados

- **Se mejoró la experiencia de trabajo remoto para más de 2500 usuarios** y se eliminaron los problemas de los usuarios relacionados con las VPN: los tickets de servicio se redujeron en un 100 %
- **Se aceleraron los plazos de las fusiones y adquisiciones y se garantizó una incorporación más segura** de las empresas adquiridas con una arquitectura de seguridad Zero Trust
- **Se redujo a solo unos minutos el tiempo necesario para identificar y resolver los problemas gracias** a las sólidas funciones de elaboración de informes y supervisión

Una de las cosas que busco en las herramientas de infraestructura y seguridad es que nos ayuden a ser más eficientes operativamente y aumenten la seguridad. Zscaler cumple ambas condiciones.

Richard Casselberry
Vicepresidente de seguridad informática, arquitectura y cumplimiento,
ATN International

Ver historia de éxito

COX AUTOMOTIVE

Cox Automotive implementa Zero Trust en etapas 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.

VISIÓN GENERAL DE COX AUTOMOTIVE

El proveedor de servicios y tecnología automotriz más grande del mundo

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

Más de 30 mil
miembros del equipo protegidos

Más de 40 mil
clientes de concesionarios de automóviles respaldados

1
plataforma única reduce la complejidad

Problemas

- Se buscaba una plataforma compatible con la nube que pudiera servir como base para una arquitectura de seguridad Zero Trust integral
- Los dispositivos de firewall tradicionales tenían dificultades para inspeccionar el tráfico de Internet a escala para un grupo de usuarios disperso por todo el mundo
- Las VPN heredadas no admitían políticas de control de acceso basadas en la identidad, lo que exponía las aplicaciones y los datos privados a un mayor riesgo

Proceso por etapas

1. **Se implementó una plataforma Zero Trust multiusuario 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 privilegios mínimos para aplicaciones privadas

Resultados

- **Protege a un equipo que trabaja en los cinco continentes,** proporcionando flexibilidad para trabajar desde cualquier lugar y mejorando la experiencia de los usuarios
- **Protege las aplicaciones y los recursos privados críticos**, incluidos los datos sobre millones de clientes, de una manera más rentable
- **Retira las soluciones de seguridad heredadas, incluidos firewalls y VPN,** para agilizar los procesos de TI y acelerar la

Una vez que los agentes estén instalados en todos los dispositivos, será fácil integrar otras capacidades de Zscaler en nuestra arquitectura. Será solo cuestión de "encender el interruptor".

Jon Mahes
Gerente sénior de ciberseguridad
Cox Automotive

Ver historia de éxito

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

Zscaler sustituye los dispositivos VPN heredados para racionalizar la arquitectura de seguridad, refuerza el conocimiento de los riesgos en tiempo real y protege a 15,000 usuarios

VISIÓN GENERAL DEL GOBIERNO DE D.C.

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

- Ámbito federal y Gobierno
- Washington, D.C., EE. UU.
- Más de 15,000 empleados

15K
empleados del gobierno asegurados

~3 mil millones
de transacciones procesadas por mes

Más de 200 mil
amenazas de seguridad bloqueadas por mes

Problemas

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

Proceso por etapas

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 uniformes para los recursos privados.
3. **Se aprovecharon los datos y las perspectivas impulsados por la IA para reforzar el conocimiento de los riesgos** y mitigar las amenazas potenciales en tiempo real, a escala.

Resultados

- **La arquitectura Zero Trust mejora la postura de seguridad** procesa alrededor de 3 mil millones de transacciones y bloquea más de 200 mil amenazas al mes
- **Mejora la experiencia remota para 15,000 usuarios**y se integra perfectamente con las soluciones de identidad existentes
- **Permite un enfoque más exhaustivo de la gestión de riesgos**, propiciado por una mejor comprensión de los factores de riesgo y la postura de seguridad

La asociación con Zscaler ha sido invaluable para nosotros. Implementamos la plataforma a una velocidad récord, incorporamos usuarios de manera más eficaz y mejoramos la experiencia del usuario.

Suneel Cherukuri
CISO, Gobierno del Distrito de Columbia

Ver historia de éxito

DMI implementa BYOD a gran escala, mejorando la protección de datos y descubriendo importantes ahorros de costos

Zscaler proporciona conectividad Zero Trust para toda la fuerza de trabajo y permite a los empleados trabajar de manera segura desde el dispositivo de su elección

VISIÓN GENERAL 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 mil dólares
ahorro anual

>2
semanas para implementar

3 %
Resolución de SLA más rápida después de la implementación

Problemas

- La instalación de nuevo hardware en un entorno heredado generó tiempos de inactividad, provocó interrupciones y requirió actualizaciones periódicas
- Exigir a los usuarios que trabajaran desde dispositivos DMI hizo que los empleados fueran menos productivos e impactó negativamente en la huella de carbono global de la organización

Proceso por etapas

1. **Se aseguró el acceso a Internet y conectividad Zero Trust real** para empleados, contratistas y terceros, sin necesidad de configurar manualmente los dispositivos, lo que consumía mucho tiempo
2. **Se implementó la iniciativa "traiga su propio dispositivo" (BYOD) respaldada por el aislamiento del navegador,** lo que permitió a los empleados trabajar en el dispositivo de su elección

Resultados

- **Se implementó Zero Trust en 2 semanas** sin impacto para los usuarios y sin tiempo de inactividad
- **Se ahorran 700,000 dólares anuales, se** mejoran las experiencias de incorporación y desconexión y se acorta el tiempo de instalación de nuevas oficinas y dispositivos

Con el proyecto BYOD, pudimos ahorrar dinero al no tener que comprar laptops para personas que no las necesitaban. Esto supuso un ahorro anual de más de 700,000 dólares para DMI, ¡lo cual es increíble!

Mauricio Mendoza
Vicepresidente de TI global y Seguridad, DMI

Ver historia de éxito

Eaton asegura operaciones globales con segmentación impulsada por la IA

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

VISIÓN GENERAL DE EATON

Fabricante mundial de equipos eléctricos para la industria aeroespacial y otras industrias.

Fabricación

Cleveland, Ohio, Estados Unidos

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

4M

de amenazas bloqueadas en un mes

90 mil

Los empleados de todo el mundo se conectan a Internet y a aplicaciones privadas a través de Zero Trust

Múltiples

socios estratégicos de la alianza se integran sin problemas

Problemas

- Las VPN y firewalls heredados obstaculizaron el crecimiento y fueron incapaces de dar soporte a los más de 30,000 empleados de la fábrica durante la pandemia y posteriormente
- La arquitectura de seguridad tradicional basada en el perímetro era incompatible con la estrategia basada en la nube y las necesidades de segmentación de la empresa
- La falta de visibilidad limitó el descubrimiento de amenazas y ralentizó el tiempo de solución

Proceso por etapas

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. **Se mejoró la concientización de los ataques** con detección y respuesta preventiva y predictiva a las violaciones

Resultados

- **Se ofreció una experiencia de usuario más segura, confiable y regulada** para empleados y terceros
- **Se aprovechó el poder de la IA para la detección de amenazas**, la prevención de pérdida de datos, la remediación, la visibilidad del uso de ChatGPT y la segmentación de aplicaciones
- **Se fortaleció el control de acceso** a través de la segmentación Zero Trust y la integración con herramientas EDR, CDR y NDR

Zscaler fue fácil de usar y sus capacidades están integradas en un agente de punto final. Hemos podido implementar Zscaler en nuestro entorno global rápidamente y ampliar sus capacidades con pocos recursos necesarios por nuestra parte.

Jason Koler
CISO, Eaton Corporation

Ver historia de éxito

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

Zscaler sustituye al hardware de seguridad, ofreciendo una resistencia superior; seguridad siempre activa y una superficie de ataque reducida

VISIÓN GENERAL DE GUARANTEED RATE

El segundo líder en hipotecas minoristas más grande de los EE. UU., con más de 500 sucursales en 50 estados

Servicios financieros y seguros

Chicago, Illinois, Estados Unidos

más de 6000 empleados

97 %
de tráfico cifrado inspeccionado

2.5 millones
amenazas bloqueadas en 3 meses

2–3x
acceso más rápido a aplicaciones

Problemas

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

Proceso por etapas

1. **Se aseguró el acceso a Internet y SaaS desde la nube:** no más conexiones de retorno desde más de 500 sucursales
2. **Se sustituyó la VPN**, ofreciendo a los usuarios un acceso rápido y confiable a más de 500 aplicaciones privadas en el centro de datos y en la nube
3. **Se optimizó la experiencia del usuario** al identificar y resolver problemas de rendimiento de manera más rápida y eficiente.

Resultados

- **Se minimizó la superficie de ataque** al brindar a los usuarios acceso directo y con privilegios mínimos al tiempo que mejoró la detección y la respuesta
- **Se redujo el riesgo de compromiso** con la supervisión en línea del tráfico TLS/SSL y la protección contra amenazas avanzadas impulsada por la IA
- **Se evitó el movimiento lateral** con tecnología del engaño para alejar a los atacantes de los recursos confidenciales y contener las amenazas en tiempo real

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

Darin Hurd
CISO de Guaranteed Rate

Ver historia de éxito

MGM Resorts International redobla su apuesta por una arquitectura Zero Trust nativa de la nube

Zscaler ofrece un tiempo de obtención de valor inigualable con segmentación Zero Trust, protección contra la pérdida de datos y profundos conocimientos procesables en toda la empresa.

VISIÓN GENERAL 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 mil
amenazas bloqueadas cada mes

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

Problemas

- La seguridad de castle-and-moat aumentó 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 experiencia de usuario deficiente.
- Las herramientas de seguridad heredadas ofrecían información limitada sobre la actividad de navegación de toda la base de usuarios

Proceso por etapas

1. **Se remplazaron las VPN y se implementó la segmentación Zero Trust** en toda la fuerza de trabajo
2. **Se implementaron rápidamente** un conjunto de soluciones de acceso privado, experiencia digital y protección de datos
3. **Se adoptó tecnología del engaño** para protegerse contra ataques activos

Resultados

- **Se mejoró la experiencia de los empleados** con un rendimiento más rápido y conectividad en todo el entorno.
- **Nos mantuvimos a la vanguardia de las amenazas emergentes** con DLP integral, acceso privado y segmentación Zero Trust
- **Se fortaleció la postura de seguridad empresarial** al tiempo que se ayudó a acelerar la actividad con un enfoque centrado en la nube

Logramos la segmentación Zero Trust en toda nuestra fuerza de trabajo 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
CISO, MGM Resorts International

Ver historia de éxito

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

Zscaler ofrece integraciones sin fisuras y funciones de IA para respaldar un trabajo remoto más seguro desde cualquier lugar y proteger los datos financieros confidenciales frente a las amenazas

VISIÓN GENERAL 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 los tickets de soporte de TI

0
tiempo de inactividad debido al malware

Problemas

- Las soluciones de seguridad tradicionales no permitían una inspección completa del tráfico en línea, lo que impedía la detección y prevención de amenazas
- Las VPN tradicionales eran incompatibles con las necesidades de priorizar la nube de una fuerza de trabajo distribuida, lo que generaba experiencias de usuario deficientes.
- La escasez de datos sobre la actividad de los usuarios y la postura de los dispositivos dificultaba el diagnóstico y la resolución de problemas para una plantilla remota

Proceso por etapas

1. **Se aseguró la contectividad directa a a internet segura**, utilizando funciones de contención de amenazas impulsadas por la 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 sólidos de los usuarios** para aliviar la sobrecarga administrativa sin aumentar el riesgo

Resultados

- **Se redujo la superficie de ataque:** cero tiempo de inactividad causado por malware o ransomware desde la implementación de Zscaler
- **Se limitó el movimiento lateral y se redujo el radio de alcance** en caso de que una amenaza ingresara a la pila de seguridad, lo que garantizó una remediación más rápida
- **Las integraciones con AWS, Crowdstrike y Okta optimizaron la infraestructura de seguridad** y reforzaron el cumplimiento normativo

Consideramos a Zscaler como líder en este espacio porque es integral y cubre todas las facetas de Zero Trust. Para conseguir la misma funcionalidad que obtenemos de Zscaler en otros lugares, tendríamos que implementar soluciones de varios proveedores.

Arjun Thusu
Director de información,
Mercury Financial

Ver historia de éxito

Molson Coors ofrece una excelente experiencia de usuario con Zscaler Zero Trust Exchange

Zscaler elimina la necesidad de dispositivos VPN, asegura la conectividad de una plantilla global y proporciona información que resuelve los problemas con mayor rapidez.

VISIÓN GENERAL DE MOLSON COORS

Tercera cervecera mundial e innovadora global en la industria de bebidas

Alimentos, bebidas y tabaco

Chicago, Illinois, Estados Unidos

más de 17,000 empleados
más de 42 cervecerías

17 mil
usuarios protegidos por Zero Trust

96 %
resolución más rápida de problemas de los usuarios

Millones
de amenazas bloqueadas diariamente

Problemas

- Los dispositivos de firewall no podían escalar 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 creó un entorno de red plano y una superficie de ataque más amplia

Proceso por etapas

1. **Se aseguró el acceso directo a Internet provisto con funciones avanzadas de detección de amenazas** para mantener seguros a los usuarios remotos y externos
2. **Se aprovechó 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 remplazaron las VPN tradicionales con acceso Zero Trust para aplicaciones privadas** para 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 solo desde Zscaler? Siempre son cientos de miles o millones, dependiendo del día. Es simple y fácil de usar. Podrá capacitar inmediantamente. No hay limitaciones

Jeremy Bauer
Director sénior de seguridad de la información (CISO), Molson Coors Beverage Company

Ver historia de éxito

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

VISIÓN GENERAL 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 Estados Unidos y uno de los mayores del mundo. Atiende a más de un millón de alumnos desde el jardín de infancia hasta el 12º grado con una plantilla 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 en ataques

40 %

más amenazas bloqueadas

Problemas

- La infraestructura heredada no pudo escalar para brindar experiencias seguras y uniformes para más de 1 millón de usuarios
- El enfoque tradicional de VPN y firewall fue ineficaz para bloquear ciberamenazas avanzadas
- La escasa visibilidad de los puntos finales dificultó el mantenimiento y la supervisión de los dispositivos de aprendizaje remoto del departamento

Proceso por etapas

1. **Se aseguró el acceso a Internet y SaaS** con una arquitectura proxy Zero Trust 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. **Se mejoró la visibilidad** 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 facilitar 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 entender lo que estamos haciendo con la IA y ayudarnos a actuar más rápido cuando se trata de responder a incidentes y encontrar esa aguja en el pajar.

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

Ver historia de éxito

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

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

VISIÓN GENERAL 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 exhaustiva Zero Trust

95 %

de casos de uso cumplidos

1

plataforma de un solo proveedor para mayor simplicidad

Problemas

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

Proceso por etapas

1. **Se implementó una plataforma Zero Trust multiusuario**, agilizando la pila de seguridad y optimizando los entornos de trabajo remotos
2. **Se suministró acceso directo a Internet y a las aplicaciones SaaS** con una protección uniforme frente a las amenazas, independientemente de su ubicación
3. **Se sustituyeron las VPN por un acceso Zero Trust para** las aplicaciones privadas con el 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 los usuarios y los datos en 50 oficinas de campo
- **Permite políticas de control de acceso microsegmentadas y con privilegios mínimos** 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 asistencia técnica.

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

David Petroski
Arquitecto sénior de infraestructuras, Southwest Gas

Ver historia de éxito

United Airlines detecta y bloquea amenazas en constante evolución con Zscaler 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

VISIÓN GENERAL 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 a Zero Trust

1PB
del tráfico TLS inspeccionado

más de 3 millones de dólares
de ahorro de costos en comparación con las soluciones tradicionales

Problemas

- Una arquitectura tradicional basada en perímetros y dependiente de centros de datos no podría respaldar una transformación digital acelerada
- Los firewalls y VPN heredados carecían de la agilidad necesaria para escalar con un aumento del trabajo remoto, lo que ponía en peligro a los usuarios y los datos
- Los anteriores productos de puntos de seguridad carecían de capacidades avanzadas de detección de amenazas, lo que dejaba al descubierto una mayor superficie de ataque

Proceso por etapas

1. **Proporcionó conectividad segura y directa a Internet y aplicaciones SaaS** para garantizar una protección uniforme para los usuarios en cualquier lugar
2. **Remplazó las VPN con políticas de acceso Zero Trust y con privilegios mínimos** para proteger las aplicaciones y los datos privados de posibles vulneraciones
3. **Aprovechó 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 manera segura desde cualquier ubicación** y protege el acceso remoto a más de 2000 aplicaciones privadas críticas
- **Reduce la complejidad y los costos de la arquitectura:** no se necesitan firewalls 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

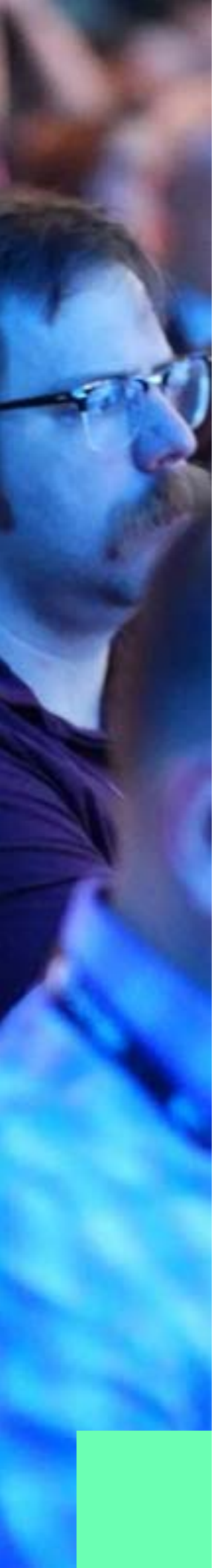
Zscaler nos da la tranquilidad de que el tráfico será seguro, independientemente de la red subyacente, para nuestros empleados, clientes y socios.

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

Ver historia de éxito

EMEA

Explore las historias de éxito de nuestros clientes por región



01
Austria
36 Raiffeisen Bank

02
Alemania
38 State Capital Magdeburg

03
Italia
40 Cisalfa Sports

04
Noruega
42 Hydro

05
Sudáfrica
44 Capitec

06
España
46 Noatum
48 Sanitas

07
United Kingdom
50 Colt
52 Primetals Technologies
54 Unilever

Raiffeisen Bank International

Raiffeisen Bank International transforma la seguridad con Zscaler Zero Trust Exchange

Zscaler sustituye a los dispositivos heredados para proporcionar una protección completa contra las amenazas, permitir la flexibilidad del trabajo desde cualquier lugar y reducir los costos de seguridad

VISIÓN GENERAL DE 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 mil

empleados protegidos por Zero Trust

18.6 millones

de clientes que disfrutan de una banca segura

1

plataforma que ofrece zero trust total

Problemas

- 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 permitía el acceso basado en identidad para aplicaciones privadas, lo que generaba políticas inconsistentes y una superficie de ataque más amplia

Proceso por etapas

1. **Implementó una plataforma Zero Trust integral**, aprovechando los servicios públicos y privados para proteger a los usuarios en cualquier ubicación.
2. **Proporcionó conectividad directa a Internet segura sin tráfico de retorno** para garantizar experiencias de usuario uniformes para una fuerza de trabajo híbrida
3. **Remplazó 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 una fuerza de trabajo híbrida**, brindando protección uniforme 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 manera 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 costos 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 Zscaler Zero Trust Exchange

La capital del estado alemán reemplaza los dispositivos VPN y potencia una fuerza de trabajo híbrida al tiempo que sienta las bases para una evolución digital continua con Zscaler

VISIÓN GENERAL DE LA CAPITAL DEL ESTADO, MAGDEBURGO

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

Ámbito federal y Gobierno

Magdeburgo, Alemania

2500 empleados

2.5 mil
empleados híbridos protegidos

230 mil
residentes de la ciudad respaldados

1
Solución de un proveedor único para simplificar la seguridad

Problemas

- 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 firewall heredadas no podían ampliarse para asegurar la conectividad a Internet de una fuerza de trabajo cada vez más híbrida
- 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 etapas

1. **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. **Se aseguró el acceso a aplicaciones privadas con controles Zero Trust basados en la identidad**, lo que garantiza una protección uniforme para datos críticos

Resultados

- **Mejora las experiencias de los usuarios para una fuerza de trabajo híbrida** y permite el trabajo remoto seguro para hasta 1500 usuarios por mes
- **Reduce los costos 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 ejemplo a seguir para otros municipios y animarles a evaluar y aplicar buenas soluciones para la empresa, del mismo modo en que lo hicimos con una solución de seguridad basada en la nube.

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

Ver historia de éxito

Cisalfa Sport fortalece su estrategia 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.

VISIÓN GENERAL 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 en toda la empresa implementación de Zscaler

más de 130
socios y contratistas externos acceden de manera segura a aplicaciones privadas e infraestructura local

70 %
de usuarios incorporados dentro de 2 semanas de implementación

Problemas

- La VPN permitía a todos los empleados y a terceros el acceso no segmentado a toda la red corporativa, lo que aumentaba el riesgo y el radio de explosión de posibles ataques
- Dos soluciones VPN heredadas tenían políticas y configuraciones contradictorias, lo que provocaba una seguridad incoherente y problemas de gestión de la seguridad
- Acceder a las aplicaciones a través de una VPN provocaba un rendimiento lento y un alto volumen de tickets de soporte de usuarios internos y externos

Proceso por etapas

1. **Se redujo la superficie de ataque** al reemplazar 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 uniformes
- **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 suministrada a través del punto de presencia más cercano

Zscaler Zero Trust Exchange... cubre todas las bases: acceso más rápido y seguro a las aplicaciones sin necesidad de VPN, reducción de riesgos en todo el entorno y una ruta clara hacia la expansión de Zero Trust.

Fabio Freti
Operaciones de TI e infraestructura
Director de Cisalfa Sport

Ver historia de éxito

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

Zscaler reduce la superficie de ataque y la huella de carbono mientras que el proveedor de energía renovable aspira a retirar el hardware heredado y volverse 100 % orientado a la nube

VISIÓN GENERAL DE HYDRO

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

Fabricación

Oslo, Noruega

31,000 empleados

33 mil
empleados protegidos por Zero Trust

1
enfoque del proveedor para reducir costos y complejidad

100 %
de operaciones de la nube como objetivo

Problemas

- La infraestructura y el hardware de seguridad heredados consumían mucha energía y no se ajustaban a los objetivos de sustentabilidad corporativos
- Una red MPLS de bajo ancho de banda no podría 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 etapas

1. **Conectividad segura y directa a Internet**, lo que elimina el tráfico de retorno y mejora la confiabilidad del acceso
2. **Ofreció una conectividad segura y directa** a Internet, eliminando el retorno del tráfico y mejorando la confiabilidad del acceso
3. **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 multiusuario nativa de la nube
- **Aumenta el rendimiento de las aplicaciones SaaS**, mejorando las experiencias de los usuarios para 33,000 empleados en 140 ubicaciones
- **Reduce los costos y la complejidad de la gestión al tiempo que mejora la postura de seguridad** mediante una solución de proveedor único de Zero Trust

Con Zscaler Private Access, los usuarios ya no necesitan conectarse a la red para utilizar nuestras aplicaciones privadas. Ahora, a medida que seguimos desarrollando nuestro lugar de trabajo moderno, avanzamos hacia la retirada de las VPN.

Armin Auth
Jefe de programas estratégicos de integración y prueba

Ver historia de éxito

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

El banco más grande de Sudáfrica implementa seguridad Zero Trust en tres meses, protegiendo a 17,000 usuarios y bloqueando 745,000 amenazas en Zero Trust Exchange

VISIÓN GENERAL DE CAPITEC

El mayor banco de Sudáfrica, con 21 millones de clientes y el número 1 en satisfacción del cliente

Servicios financieros y seguros

Ciudad del Cabo, Sudáfrica

15,450 empleados en 860 sucursales

3

segundos para migrar aplicaciones privadas a AWS

125 millones

violaciones de políticas prevenidas en un año

3

meses para implementar de manera integral Zero Trust

Problemas

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

Proceso por etapas

1. **Aseguró la conectividad directa a Internet y a las aplicaciones SaaS**, aprovechando la inspección del tráfico para evitar que los datos se vieran comprometidos
2. **Desplazó a los dispositivos VPN heredados, introduciendo un acceso Zero Trust** para aplicaciones privadas y datos financieros confidenciales
3. **Aprovechó las capacidades avanzadas de experiencia digital y los conocimientos prácticos** para resolver problemas persistentes 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 violaciones 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:** solo se necesitan unos segundos para migrar aplicaciones a AWS sin tiempo de inactividad ni fallas de seguridad

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

Andrew Baker
CTO, Capitec

Ver historia de éxito

Noatum implementa un conjunto de tecnologías de 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.

VISIÓN GENERAL 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

0
dependencia de VPN y firewalls

360
grados de cuantificación del riesgo

Problemas

- Las VPN tradicionales dejaban a la organización demasiado expuesta a ciberataques cuando los usuarios accedían a Internet.
- La seguridad heredada, como los firewalls, impedía a la organización inspeccionar el tráfico cifrado
- Las arquitecturas basadas en el perímetro hicieron que la incorporación de las fusiones y adquisiciones tardara mucho más de lo debido

Proceso por etapas

1. **Sustituyó las VPN** por una plataforma en la nube que permite el acceso seguro a Internet y a aplicaciones privadas
2. **Creó un centro de supervisión de experiencias único y basado en la nube** con ZDX
3. **Evaluó el riesgo empresarial** de manera 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 fue realmente el catalizador para que buscáramos una solución como Zscaler.

Josep Pou
CISO, 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 sin importar dónde se encuentren

VISIÓN GENERAL DE SANITAS

Sanitas, una gran compañía de seguros médicos de alto crecimiento

Sector sanitario y farmacéutico

Madrid, España

Más de 11,700 empleados en España, Europa y América Latina

2.5
meses para implementar para todos los usuarios

12–15 mil
de usuarios protegidos por nuestra plataforma

0
necesidad de conectarse a un centro de datos

Problemas

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

Proceso por etapas

1. Implemente un modelo Zero Trust homogéneo y basado en la nube para asegurar toda la organización a escala
2. Reemplazó las VPN con un modelo Zero Trust para mejorar la conectividad de todos los usuarios independientemente de su ubicación
3. Ofreció acceso seguro y sin inconvenientes a las aplicaciones para todos los usuarios, incluidos los socios

Resultados

- Protege entre 12,000 y 15,000 usuarios en 2.5 meses con Zscaler Internet Access
- Permite trabajar desde cualquier lugar, posibilitando negocios flexibles y ágiles con una experiencia similar a la de una oficina
- Ofrece un acceso seguro a las cargas de trabajo y las aplicaciones

Actualmente, los empleados pueden trabajar desde casa, igual que lo hacen desde la oficina, de manera transparente, flexible, muy ágil y sin esas barreras que solíamos tener con otras soluciones.

Antonio Cerezo
Responsable de ciberseguridad, Europa y LATAM

Ver historia de éxito

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

Al asociarse con Zscaler para implementar una arquitectura Zero Trust en tres meses, la empresa puede ayudar a otras compañías a lograr la transformación de la seguridad

VISIÓN GENERAL 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

5 MIL

empleados híbridos protegidos

83 %

implementación más rápida que las soluciones tradicionales

100 millones

de violaciones de políticas evitadas trimestralmente

Problemas

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

Proceso por etapas

1. **Implementó una arquitectura de seguridad Zero Trust nativa de la nube** para respaldar las operaciones comerciales basadas en la nube y el trabajo híbrido.
2. **Suministró un acceso seguro y directo a Internet**, inspeccionando todo el tráfico cifrado para detener las amenazas y la pérdida de datos
3. **Sustituyó a los dispositivos VPN heredados con un acceso Zero Trust para aplicaciones privadas**, facilitando y haciendo más seguro el trabajo a distancia

Resultados

- **Ofrece experiencias digitales excepcionales a 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 Zscaler nativa de la nube protege a nuestros empleados independientemente de dónde trabajen y de los dispositivos que utilicen.

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

VISIÓN GENERAL DE PRIMETALS TECHNOLOGIES

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

Alta tecnología

Londres, Reino Unido

Más de 7500 empleados

7.5 mil
usuarios protegidos por Zero Trust

Hasta un 35 %
en reducción de costos de infraestructura

4.53/5
índice de satisfacción de los empleados

Problemas

- Una pila de seguridad tradicional construida en torno a los centros de datos no podía escalar para respaldar la transformación digital que da prioridad a la nube
- Los dispositivos de seguridad heredados, incluidos los firewalls y las VPN, no eran lo suficientemente ágiles para sustentar un nuevo rediseño de la red SD-WAN
- Los dispositivos VPN obsoletos no protegían eficazmente la conectividad remota para una fuerza de trabajo híbrida y dispersa globalmente

Proceso por etapas

1. **Implementó conectividad directa a Internet compatible con SD-WAN** para optimizar la infraestructura y mejorar el rendimiento
2. **VPN desplazadas con acceso Zero Trust para aplicaciones privadas** que permiten trabajar desde cualquier lugar de manera segura a usuarios de todo el mundo
3. **Aprovechó 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 costos generales de infraestructura
- **Garantiza una conectividad entrante y saliente fluida** para un grupo de usuarios híbrido, el 25 % de los cuales trabaja de manera totalmente remota
- **Reduce el volumen de tickets de asistencia técnica y resuelve problemas más rápidamente**, mejorando la experiencia del usuario final y aliviando la sobrecarga administrativa.

En el transcurso de 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 un acceso controlado 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

VISIÓN GENERAL DE UNILEVER

Una 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 3 mil millones

Detalle de transacciones aseguradas semanalmente

99.9 %

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

Más de 1500

Aplicaciones administradas con acceso Zero Trust controlado

Problemas

- Las VPN heredadas tenían una flexibilidad limitada y no podían escalar con la estrategia de nube global de Unilever
- El modelo de seguridad tradicional aumenta el riesgo debido a un control de acceso y una visibilidad insuficientes
- La creciente demanda de acceso remoto puso a prueba la infraestructura VPN, lo que afectó a la experiencia de los usuarios

Proceso por etapas

1. **Habilitó el acceso seguro de los usuarios a Internet y SaaS** con inspección completa del tráfico TLS/SSL y protección avanzada contra amenazas
2. **Remplazó las VPN** con acceso Zero Trust a aplicaciones privadas
3. **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 la fuerza de trabajo de Unilever

El enfoque Zero Trust de Zscaler ha transformado la seguridad en Unilever. La eliminación de los cuellos de botella de VPN permite a nuestra fuerza de trabajo global acceder de manera 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

APJ

Explore las historias de éxito de nuestros 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 costos de red en un 50 % utilizando Zero Trust Exchange

Zscaler facilita la transición a SD-WAN y permite el desplazamiento de cientos de firewalls, mejorando la eficiencia operativa y la postura de seguridad

VISIÓN GENERAL DE JOHN HOLLAND

Una empresa de infraestructuras integradas, construcción, ferrocarril y transporte multimodal

Construcción

Melbourne, Victoria, Australia

Más de 5000 empleados en más de 120 ubicaciones

1 semana
para el implementación de Zero Trust

6,000
de empleados y contratistas protegidos

122 mil
amenazas bloqueadas en tres meses

Problemas

- Una arquitectura de seguridad tradicional y perimetral no podía escalar para dar soporte a unas operaciones empresariales cada vez más orientadas a 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 costos
- Los dispositivos de firewall heredados carecían de la agilidad necesaria para inspeccionar el tráfico cifrado en línea, lo que aumentaba la vulnerabilidad ante las amenazas

Proceso por etapas

1. **Implementó una plataforma de seguridad Zero Trust integral nativa de la nube** para crear un entorno de TI más ágil y escalable
2. **Redujo la dependencia de los dispositivos de firewall y de los costos de red** con un acceso seguro y directo a Internet y a las aplicaciones SaaS
3. **Aprovechó las funciones avanzadas de detección de amenazas para agilizar el ecosistema** de seguridad y eliminar el riesgo de que los datos se vean comprometidos

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 firewall heredados con conectividad Zero Trust**, consiguiendo una reducción del 50 % en los costos de red
- **Asegura la conectividad de los usuarios**, procesa 400 TB de tráfico y previene 98 millones de violaciones de políticas trimestralmente

Zscaler proporciona el resto de nuestra seguridad que simplificó nuestros procesos y, a través de esa simplificación, fortaleció la seguridad.

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 en Zscaler 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 fuerte perímetro de seguridad.

VISIÓN GENERAL DE PROBE CX

Uno de los mayores subcontratistas australianos de experiencia del cliente y procesos empresariales

Servicios

Melbourne, Victoria, Australia

19,000 empleados, operaciones en 32 puntos de entrega

100 %
de VPN retiradas

8.1 mil millones
de transacciones procesadas en un trimestre

3.1 millones
amenazas bloqueadas en tres meses

Problemas

- Una arquitectura de seguridad tradicional no podía escalar con una fuerza de trabajo en rápido crecimiento o un enfoque en evolución que le da prioridad a 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 del rendimiento de la aplicación hacía que mitigar los problemas fuera complicado y llevara mucho tiempo

Proceso por etapas

1. **Garantizó una conexión directa segura a Internet y a las aplicaciones SaaS**, inspeccionando el tráfico en línea, sin tráfico de retorno
2. **Sustituyó las VPN por un acceso Zero Trust para las aplicaciones** privadas con el fin de proteger mejor la propiedad intelectual y los datos críticos
3. **Aprovechó 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 uniformes y minimizando la superficie de ataque
- **Simplifica la gestión de la seguridad con una plataforma multiusuario** que ofrece seguridad Zero Trust con un costo total de propiedad más bajo

Algunos de los principales beneficios que hemos obtenido al implementar esta tecnología ahora ha sido poder deshacernos del 100 % de esas VPN dentro del entorno.

Rohan Khanna
Director de tecnología, Probe CX

Ver historia de éxito

Persistent

Persistent aumenta la seguridad a la vez que ahorra 2 millones de dólares en costos de capital y operaciones año tras año

Zero Trust protege los datos confidenciales de los clientes y la propiedad intelectual, permite la innovación, reduce la complejidad y cumple con los objetivos medioambientales, sociales y de gobernanza (ESG)

VISIÓN GENERAL 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

Problemas

- Proporciona a los trabajadores remotos de 21 países una conectividad rápida y una experiencia de usuario más productiva
- Protege la propiedad intelectual y los datos confidenciales de los clientes en el entorno de la nube
- Simplifica una infraestructura compleja
- Reduce los costos operativos y de hardware en todo el entorno
- Encuentra un socio Zero Trust a largo plazo con una solución escalable que fomenta una rápida expansión
- Minimiza el impacto ambiental reduciendo la huella de carbono

Proceso por etapas

1. **Mejoró la postura de seguridad** con conexiones seguras y directas a Internet, SaaS y aplicaciones privadas
2. **Redujo la latencia, disminuyó los costos y mejoró la experiencia del usuario** al eliminar VPN y firewalls poco confiables y no seguros
3. **Protegió la valiosa propiedad intelectual y los datos de los clientes con** tecnología avanzada de prevención de pérdida de datos (DLP) y engaño

Resultados

- **Mejora y acelera** 4 veces el acceso remoto para 23,000 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

El centro médico Keiju transforma la atención digital al paciente con Zscaler 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 la experiencia de los pacientes

VISIÓN GENERAL DEL CENTRO MÉDICO KEIJU

El único hospital de asistencia médica de la región de Noto, reconocido como líder digital

Sector sanitario y farmacéutico

Ciudad de Nanao, Prefectura de Ishikawa, Japón

más de 800 empleados para más de 400 camas

800
empleados médicos protegidos

100
de dispositivos móviles conectados de manera segura

1
plataforma para seguridad zero trust

Problemas

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

Proceso por etapas

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 permitió 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 para proteger el acceso remoto a los datos de EMR

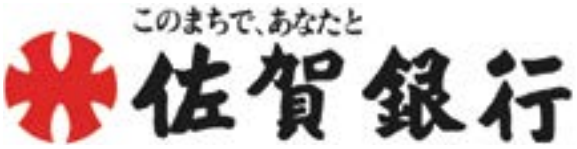
Resultados

- **Permite la flexibilidad del trabajo desde cualquier lugar para el personal médico** y amplía la oferta de contratación de médicos de calidad
- **Protege los registros confidenciales de pacientes contra amenazas** cuando se accede a ellos de manera remota: más de 500 dispositivos móviles se conectan de manera 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... así que necesitábamos un entorno de acceso remoto seguro y fácil de usar.

Sr. Masahiro Kamino
Presidente del Consejo de Administración, Keiju Medical Center

Ver historia de éxito



The Bank of Saga apoya la transformación digital con Zscaler 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

VISIÓN GENERAL 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 1200 empleados

alrededor del 33 %
menores costos de comunicación

1.8 mil
usuarios protegidos por Zero Trust

1
inicio de sesión único aumenta la productividad

Problemas

- Una arquitectura de seguridad tradicional basada en el perímetro no respaldaría 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 etapas

1. **Implementó una plataforma Zero Trust integral y nativa de la nube** para aplicar políticas de seguridad uniformes en toda la empresa
2. **Introdujo la conectividad directa a Internet** y aprovechó la inspección de tráfico en línea para proteger el acceso a las aplicaciones SaaS públicas
3. **Reemplazó 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 uniformes independientemente de la ubicación
- **Protege las aplicaciones de banca privada y los datos críticos contra riesgos**, asegurando y mejorando las experiencias de los clientes
- **Optimiza la pila de seguridad y reemplaza los dispositivos heredados**, simplificando la gestión de políticas y reduciendo costos

La transición a la nube es necesaria para la transformación digital. ... [Sin embargo,] la seguridad perimetral convencional no permite aprovechar plenamente la comodidad del SaaS y de los servicios web. La seguridad Zero Trust fue 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 fuerza de trabajo híbrida 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

VISIÓN GENERAL DE CEBU PACIFIC AIR

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

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

234 millones

de violaciones de políticas evitadas trimestralmente

90 %

de aumento de la satisfacción del usuario

2

semanas para implementar el acceso remoto a aplicaciones Zero Trust

Problemas

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

Proceso por etapas

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 una fuerza de trabajo híbrida
3. **Se reemplazaron los dispositivos VPN tradicionales con acceso Zero Trust** para aplicar controles de acceso granulares a aplicaciones privadas

Resultados

- **Asegura la conectividad de trabajo desde cualquier lugar para 3900 usuarios con una alternativa a la VPN segura**, mejorando la satisfacción del usuario en un 90 %
- **Optimiza la pila de seguridad y al mismo tiempo proporciona una protección sólida:** procesa 733 millones de transacciones al año
- **Previene 234 millones de violaciones 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
CIO, 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

VISIÓN GENERAL DE MAXEON

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

Energía, petróleo, gas y minería

Singapur

5000 empleados en 40 ubicaciones

134 %
más tráfico procesado trimestralmente

31 millones
violaciones de la política evitadas en un trimestre

2.9 millones
amenazas bloqueadas en tres meses

Problemas

- La seguridad perimetral tradicional construida alrededor de los centros de datos no sería compatible con una infraestructura en evolución basada en la nube
- Los firewalls heredados no podían escalar con las crecientes necesidades de acceso remoto, lo que provocaba un rendimiento deficiente y un mayor riesgo
- Las soluciones DLP anteriores eran difíciles de gestionar, lo que ponía en peligro la propiedad intelectual y los activos críticos

Proceso por etapas

1. **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. **Implementó una solución de supervisión de experiencias diseñada específicamente para Zero Trust** para agilizar los procesos de incorporación y concesión de licencias
3. **Introdujo una solución DLP integrada** para salvaguardar la información crítica, garantizar el cumplimiento y prevenir violaciones de datos

Resultados

- **Acelera la transformación digital:** todos los centros de datos han sido 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 los datos de PI de misión crítica, incluidas más de 1400 patentes,** mejorando la postura de seguridad y garantizando la continuidad empresarial

Aunque evaluamos a varios proveedores reconocidos, Zscaler resultó ser un claro ganador por su posición de liderazgo en el Magic Quadrant de Gartner® y sus capacidades comprobadas.

Stephen Gani
CISO, Maxeon Solar Technologies

Ver historia de éxito