Libro electrónico

Una empresa segura comienza desde la confianza cero

Acelere la transformación de su empresa

Haga de la seguridad la base de una transformación exitosa

La transformación digital solo puede ayudar a su empresa a alcanzar sus objetivos estratégicos (ventaja competitiva sostenible, liderazgo en el mercado, nuevos modelos de negocio, oportunidades de ingresos y muchos más), si tiene una base segura.

Sin embargo, las tecnologías que hacen posible la transformación (la nube, la movilidad, SaaS, Internet de las cosas [IoT], etc.) también pueden aumentar significativamente el riesgo de graves ciberataques. El perímetro corporativo tradicional sencillamente no puede mantener segura su organización en un mundo que da prioridad a la nube, donde los usuarios, las aplicaciones y los datos están en todas partes, lo que aumenta exponencialmente su superficie de ataque. Los enfoques de seguridad heredados no son adecuados en los entornos de nube modernos, lo que da lugar a una mayor complejidad, costes y gastos operativos iniciales que a su vez generan obstáculos y baches que retrasan la transformación.

Es por ello que las empresas deben transformar la seguridad y convertirla en la base de la transformación digital de su empresa. El éxito comienza con la seguridad y la seguridad comienza con la confianza cero.

Le mostraremos cómo.

Despídase del foso

El enfoque de seguridad tradicional (conocido como arquitectura de castillo y foso) se basaba en la defensa del perímetro (el foso) para proteger a la organización (el castillo) de los ataques externos. Las defensas perimetrales protegían la red y daban por sentado que todo lo que operaba dentro de la red y de las cuatro paredes del centro de datos era seguro y de confianza.

El mundo ha cambiado:

- **El nuestro es un mundo que da prioridad a la nube:** los negocios se hacen en la nube, lo que la convierte (a la nube, no al centro de datos) en el nuevo centro de gravedad de la empresa. La modernización de las aplicaciones en la nube está muy avanzada y el uso de SaaS sigue creciendo. Por lo tanto, ¿cómo pueden las empresas proteger su actividad en la nube si no se realiza dentro del castillo ni está protegida por el foso?
- **Ya no se puede confiar en el tráfico interno:** hace tiempo que desapareció el perímetro, como han demostrado el uso de dispositivos propios, la movilidad y el trabajo remoto. Los ciberataques dañinos se aprovechan de la confianza implícita en las defensas perimetrales defectuosas. Las redes planas heredadas permiten el movimiento lateral sin restricciones de adversarios cada vez más sofisticados. Los atacantes pasan de un usuario infectado a una máquina (o controlador de dominio, servidor o carga de trabajo) tras otra. Toda la red está en peligro.
- **Los enfoques de seguridad heredados están obsoletos:** a pesar de su nombre, los cortafuegos de próxima generación (NGFW) y otras soluciones de seguridad de red heredadas no están diseñados para la arquitectura de TI moderna y la transformación de la nube. No son compatibles con la confianza cero, el modelo de seguridad basado en el contexto más recomendado que elimina la confianza implícita para hacer que los usuarios, los dispositivos, las aplicaciones y los datos estén seguros, sin importar dónde estén. Los NGFW y otras soluciones heredadas son demasiado frágiles, complejos y costosos para dar soporte a los principios de la confianza cero de manera efectiva para reducir el riesgo y proteger mejor a la empresa.

ESTADÍSTICAS DE DATOS

El estado de la seguridad en la nube

80%

ataques principales explotaron los servicios expuestos a Internet[1]

26%

de servidores exponen sus puertos Secure Shell (SSH) a Internet[2]

20%

de servidores exponen puertos de protocolo de escritorio remoto (RDP) a Internet[3]

#1

la principal preocupación de los directores generales en Estados Unidos son las ciberamenazas[4]

63%

de las transformaciones de la ciberseguridad van a la zaga de la digitalización o solo mantienen el ritmo[5]

Fuentes: 1. NSA 2020; 2–3. Zscaler, "El estado de la (in)seguridad en la nube en 2020"; 4–5. PwC, "Cyber-ready – Today and for Tomorrow", junio de 2021

Comprenda las limitaciones de la seguridad tradicional en la nube

Hacer extensivos los enfoques de seguridad tradicionales, como los NGFW, a un entorno moderno de nube, híbrido o multinube da lugar a muchos más problemas que beneficios, incluida una superficie de ataque ampliada que pone a su empresa en un riesgo aún mayor que antes.

Las organizaciones utilizan dos enfoques principales para adaptar su infraestructura de seguridad heredada a la nube: extender la red y la infraestructura de seguridad a la nube o ampliar el perímetro para incluir la nube. Ninguno de estos enfoques ofrece la base segura que las empresas necesitan para acelerar con confianza la transformación digital.

USO DE LA SEGURIDAD TRADICIONAL EN UN MUNDO DE LA NUBE

ENFOQUE N.º 1:

Hacer extensiva la red heredada y la seguridad a la nube

- Hacer extensiva la red a la nube a través de VPN de sitio a sitio
- Hacer extensiva la red a todos los usuarios mediante VPN
- Hacer extensiva la red a las sucursales mediante MPLS

DESAFÍOS

Mala experiencia de usuario.
El tráfico de retorno introduce latencia e impacta en el rendimiento de la aplicación.

Riesgo de movimiento lateral de amenazas.
La ampliación de la WAN aumenta el riesgo. Un solo usuario infectado puede propagar el malware a toda la red corporativa.

Alto costo y sobrecarga operativa.
A medida que la red y la pila de seguridad proliferan, también lo hacen los costos.

ENFOQUE Nº 2:

Ampliar el perímetro para incluir la nube

- Hacer extensiva la red a la nube a través de VPN de sitio a sitio
- Hacer extensiva la red a los usuarios a través de VPN a cortafuegos de nube virtual
- Hacer extensiva la red a las sucursales a través de VPN de sitio a sitio

DESAFÍOS

Gran superficie de ataque.
Cada cortafuegos y aplicación orientados a Internet se pueden descubrir y explotar potencialmente.

Riesgo de movimiento lateral de amenazas.
El perímetro se vuelve extremadamente grande y, una vez dentro, no hay modo de detener a un atacante.

Alta sobrecarga operativa y costos.
Si bien este enfoque puede reducir los costos de MPLS, la administración de un número de cortafuegos que crece rápidamente y la gran cantidad de alarmas de cortafuegos aumenta la sobrecarga operativa y los costos.

Comience desde la confianza cero para transformar la seguridad

La transformación segura requiere un nuevo enfoque que reinvente fundamentalmente la seguridad como base para toda la transformación. Esa base comienza con la confianza cero.

La confianza cero es un enfoque moderno de la seguridad basado en los principios de acceso con el menor privilegio posible y en que, por defecto, no se debe confiar en ningún usuario o aplicación. Una arquitectura de confianza cero implementa estos principios para conectar de forma segura a usuarios, dispositivos y aplicaciones utilizando políticas empresariales.

Con una base segura fundamentada en la confianza cero, obtendrá la seguridad y la confianza que su empresa necesita para acelerar la transformación. Para conseguir una arquitectura de confianza cero que sea ágil, transparente, escalable y sencilla, no se pueden utilizar los NGFW, dispositivos de seguridad ni enfoques de red tradicionales. Necesita una solución moderna y nativa de la nube.

Una arquitectura de confianza cero

- Protege frente a ciberamenazas sofisticadas
- Previene la pérdida de datos
- Evita el movimiento lateral de las amenazas
- Proporciona una gran experiencia de usuario
- Reduce los costos y la complejidad

Cree una base segura con Zscaler

Las empresas más transformadoras del mundo dependen de la plataforma de seguridad más transformadora del mundo para acelerar su transformación digital segura. Zscaler Zero Trust Exchange™ acelera la transformación empresarial haciendo que la nube sea segura. Protege a los usuarios y las aplicaciones, independientemente de su ubicación, mediante la aplicación de políticas e identidad basada en contexto.

A diferencia de los NGFW tradicionales y los productos específicos de seguridad, Zero Trust Exchange está diseñado para proteger al personal de hoy en día híbrido, que prioriza la nube, con una seguridad altamente proactiva, inteligente y radicalmente simple que reduce enormemente el riesgo empresarial.

Hemos creado la única verdadera plataforma de confianza cero del mundo, rompiendo con décadas de enfoques heredados al abstraer la seguridad de la red subyacente para conectar de forma segura a los usuarios y los dispositivos directamente con las aplicaciones. Nos aseguramos de encontrar y contener las amenazas y los intentos de robo de datos para que usted pueda llevar su negocio adelante con confianza.

Zero Trust Exchange se basa en tres principios que lo hacen superior a los enfoques tradicionales:

ZERO TRUST EXCHANGE DE ZSCALER

1. **Cero acceso a la red.**
   Conecta a los usuarios a las aplicaciones, no a las redes corporativas, para evitar el movimiento lateral.

2. **Cero superficie de ataque.**
   Hace que las aplicaciones sean invisibles para que no las puedan atacar.

3. **Cero conexiones de paso.**
   Deniega todos los privilegios utilizando nuestra arquitectura de proxy, para mejorar la protección de los datos y frente a las ciberamenazas.

ENFOQUE DE CASTILLO Y FOSO/ BASADO EN EL PERÍMETRO

Acceso a la red.
Conecta a los usuarios a las redes para acceder a las aplicaciones.

Superficie de ataque aumentada.
Las aplicaciones se publican en Internet, aumentando con ello la superficie de ataque.

Conexiones de paso.
La arquitectura de cortafuegos de paso ofrece una capacidad limitada para inspeccionar el tráfico y proteger los datos.

¿POR QUÉ ZSCALER?

Reduzca su riesgo con nuestra arquitectura de proxy

Zero Trust Exchange utiliza una arquitectura basada en proxy que puede inspeccionar las sesiones SSL, analizar el contenido de las transacciones y tomar decisiones sobre política y seguridad en tiempo real. Este enfoque proxy finaliza completamente la conexión y luego la restablece.

En comparación, un enfoque tradicional de seguridad de red o cortafuegos utiliza una conexión de paso que no puede realizar una inspección adecuada para la seguridad y la protección de datos, y permite que las amenazas de día cero infecten las organizaciones.

PRINCIPIO N.º 1

Evite el peligro bloqueando las amenazas antes de que lleguen a usted

En lugar de ampliar su superficie de ataque a medida que se transforma y se expande a la nube, Zero Trust Exchange elimina la superficie de ataque de Internet al hacer que las aplicaciones sean invisibles. Al mismo tiempo, puede proteger a los usuarios, servidores, aplicaciones y sistemas IoT/OT con una plataforma que ofrece todos los controles de seguridad empresariales críticos como un servicio perimetral, cerca de cada usuario.

Con Zscaler, puede evitar riesgos ya que hace lo siguiente:

- Detectar, prevenir y contener al instante los ataques más sofisticados y los intentos de ransomware en línea, en todo el tráfico, incluido el SSL, con los mejores servicios de seguridad basados en IA
- Detener los ataques con políticas autónomas de confianza cero que se adaptan continuamente al cambiante panorama de amenazas, impulsadas por los expertos de ThreatLabz de primer nivel y la inteligencia sobre amenazas de la nube de seguridad más grande del mundo
- Evitar que los atacantes descubran, exploten o infecten a los usuarios y las aplicaciones haciéndolos invisibles a Internet y accesibles exclusivamente a los usuarios o dispositivos autorizados a través de Zero Trust Exchange
- Supervisar, validar y resolver automáticamente las deficiencias en los derechos, la política de seguridad y el cumplimiento de la normativa causadas por configuraciones erróneas y un acceso demasiado permisivo en todos los entornos de la nube

PRINCIPIO N.º 2

Evite el movimiento lateral y detenga la propagación

Uno de los mayores riesgos de seguridad de las redes corporativas tradicionales es el movimiento lateral. Una vez que el malware entra en la red, puede propagarse libremente por la organización, provocando daños generalizados.

Con Zscaler, usted elimina el riesgo de movimiento lateral al conectar directamente a los usuarios y los dispositivos a las aplicaciones, no a la red. Con Zscaler, su organización puede hacer lo siguiente:

- Mitigar el potencial de daño de cualquier usuario o dispositivo comprometido con nuestra capacidad integrada de acceso a la red de confianza cero (ZTNA) para usuarios remotos y en las instalaciones
- Ampliar la prevención del movimiento lateral basada en la confianza cero a las cargas de trabajo en la nube y a los centros de datos con una innovadora microsegmentación basada en la identidad que permite o bloquea las comunicaciones de las cargas de trabajo en entornos híbridos y en la nube
- Detectar, atrapar y analizar ataques con aplicaciones y señuelos proactivos que generan alertas de alta confianza y proporcionan información estratégica crítica sobre secuencias de ataque

PRINCIPIO N.º 3

Prevenir la pérdida de datos

Detenga la pérdida de datos causada por la exposición accidental o la extracción maliciosa con nuestras capacidades globales de protección de datos que abarcan dispositivos administrados y no administrados, servidores, nube pública y aplicaciones en la nube. Con la plataforma Zscaler, su organización puede hacer lo siguiente:

- Controlar las aplicaciones en la nube autorizadas y no autorizadas, a la vez que protege los datos confidenciales en reposo del robo o la exposición accidental con las mejores capacidades integradas de CASB
- Proteger los datos confidenciales en movimiento con controles DLP granulares que identifican y bloquean la filtración o el robo de datos en todo el tráfico en línea y SSL en tiempo real
- Extender los controles DLP a dispositivos no gestionados y propios con la tecnología única e integrada de aislamiento del navegador en la nube
- Identificar y corregir errores de configuración peligrosos en SaaS y en las nubes públicas para evitar infracciones de seguridad y pérdida de datos en la nube

La transformación de la seguridad comienza con la confianza cero

Acelere su traslado a la nube con toda confianza con Zscaler Zero Trust Exchange.

Más información

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

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