Libro electrónico

¿Quiere proteger a su personal híbrido con ZTNA?

Busque estas diez capacidades imprescindibles

Índice

Introducción 3

¿Qué es Zero Trust Network Access (ZTNA)? 4

N.º 1: Eliminar la superficie de ataque haciendo que las aplicaciones sean invisibles para el Internet público 5

N.º 2: Habilitar la conectividad perfecta desde cualquier lugar 6

N.º 3: Aplicar el acceso con privilegios mínimos 7

N.º 4: Mantener la productividad de los usuarios detectando y resolviendo rápidamente problemas de aplicaciones, redes y dispositivos 8

N.º 5: Prevenir el movimiento lateral a través de la microsegmentación de la aplicación 9

N.º 6: Admitir el acceso seguro para dispositivos propios de los usuarios y dispositivos corporativos 10

N.º 7: Detener los ataques y bloquear las amenazas con una inspección de contenido en línea completa 11

N.º 8: Integrarse perfectamente con una amplia gama de proveedores y soluciones de identidad 12

N.º 9: Incorporar tecnología de engaño integrada para frustrar a los atacantes 13

N.º 10: Permitir una implementación rápida y sencilla 14

Vea usted mismo por qué Zscaler Private Access es la plataforma ZTNA más implementada del mundo 15

Introducción

El mundo laboral está cambiando. El modo y el lugar en el que los empleados son más productivos es diferente de lo que era hace unos pocos años. A medida que un número cada vez mayor de organizaciones adoptan el trabajo híbrido y remoto, trasladan un número cada vez mayor de aplicaciones de misión crítica a la nube para poder aprovechar al máximo la flexibilidad, la escalabilidad y la eficiencia que ofrece.

Sin embargo, mientras se van transformando los ecosistemas de TI, se crean nuevos desafíos de seguridad. La adopción a gran escala del trabajo híbrido y remoto, junto con un mayor uso de la nube y un mayor acceso móvil, puede expandir la superficie de ataque, especialmente si estos cambios no van acompañados de un distanciamiento de las soluciones de seguridad heredadas (como las VPN y los cortafuegos) y enfoques obsoletos. Además de la expansión de la superficie de ataque, esta situación limita la visibilidad de los equipos de seguridad, lo que dificulta la investigación de incidentes y la resolución de problemas.

Lo que se necesita es un nuevo modelo para proteger los entornos tecnológicos, uno que se adapte mejor a las necesidades actuales de seguridad y conectividad. La confianza cero proporciona exactamente esto y actualmente está experimentando una rápida adopción en todos los sectores y ámbitos geográficos.

Cada vez más organizaciones eligen el acceso a la red de confianza cero o Zero Trust Network Access (ZTNA) para fortalecer su postura de seguridad para el trabajo híbrido. ZTNA proporciona un marco claro y bien definido para seguir el camino hacia la confianza cero. La firma analista Gartner informa que el mercado de ZTNA se está expandiendo a una velocidad vertiginosa. Actualmente está experimentando un crecimiento superior al 60 % interanual.

Las organizaciones citan el reemplazo de VPN como su principal motivación para implementar ZTNA.

¿Qué es Zero Trust Network Access (ZTNA)?

ZTNA es un conjunto de tecnologías y funcionalidades que permiten el acceso seguro a aplicaciones internas y/o privadas para usuarios remotos.

ZTNA opera de acuerdo con un modelo de confianza adaptativo, en el que la confianza nunca es implícita y en el que el acceso se otorga sólo en función de la necesidad de saber, con los privilegios mínimos definidos por políticas granulares.

A medida que un número creciente de organizaciones adopta infraestructuras y aplicaciones en la nube, muchas buscan unificar sus servicios de seguridad con una única plataforma en la nube. Esto se conoce como perímetro de servicio de seguridad o Security Service Edge (SSE), que comprende la puerta de enlace web segura (SWG), el agente de seguridad de acceso a la nube (CASB) y las capacidades de ZTNA. Gartner recomienda que los líderes de gestión de riesgos y seguridad comiencen sus estrategias de adopción de SSE adoptando ZTNA. En este sentido, ZTNA suele ser un primer paso clave en el camino hacia la seguridad en la nube.

Muchas organizaciones recurren a ZTNA para reemplazar las infraestructuras VPN que no funcionan bien a escala o exponen a la organización a un mayor riesgo de seguridad porque su presencia amplía la superficie de ataque. Pero ZTNA es mucho más que un sustituto de la VPN: ofrece a las organizaciones la oportunidad de eliminar los dispositivos heredados (junto con la sobrecarga de administración), brinda a los usuarios acceso rápido y directo a las aplicaciones, escala sin esfuerzo y mejora el control administrativo y la visibilidad.

Sin embargo, no todos los productos o soluciones de ZTNA del mercado son iguales. Para lograr todos estos beneficios y más, busque uno que pueda hacer las siguientes diez cosas.

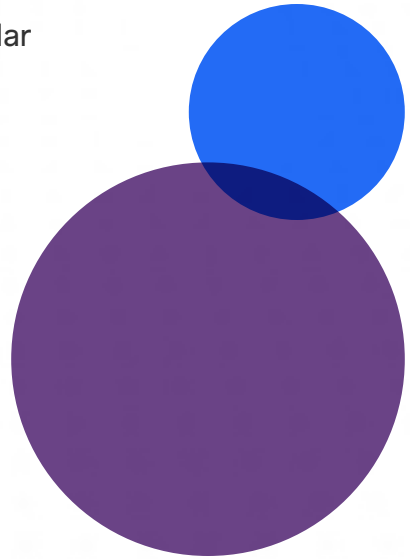
N.º 1: Eliminar la superficie de ataque haciendo que las aplicaciones sean invisibles para el Internet público

En las arquitecturas de red radiales tradicionales, cualquier atacante que pueda violar el perímetro de seguridad puede encontrar fácilmente las aplicaciones.

Una vez que los ciberdelincuentes están dentro de la red, las aplicaciones y otros recursos se pueden descubrir fácilmente a través de una simple búsqueda.

Con una verdadera solución ZTNA, el acceso a la aplicación se otorga de uno en uno a través de la segmentación. Esto hace que sea imposible descubrir otras aplicaciones en su entorno, incluso si un atacante obtiene acceso a una.

Todas las aplicaciones están ocultas detrás de la plataforma ZTNA, que intermedia la conectividad directa. Debido a que los atacantes no pueden dirigirse a lo que no pueden ver, una solución ZTNA debe ocultar las identidades de origen ofuscando sus direcciones IP. Básicamente, estas conexiones de adentro hacia afuera hacen que todo su ecosistema de aplicaciones sea invisible. De esta forma, los atacantes no pueden lanzar ataques dirigidos contra aplicaciones individuales.



N.º 2: Habilitar la conectividad perfecta desde cualquier lugar

El 77 % de las organizaciones actuales han adoptado o buscan habilitar el trabajo híbrido.

Las arquitecturas de red heredadas se basan en costosos enlaces MPLS entre las sucursales y el centro de datos central y conectan a los usuarios remotos a través de VPN. A medida que el trabajo híbrido y remoto se generaliza, el uso de VPN crea desafíos de rendimiento porque las VPN no pueden escalar.

Por el contrario, ZTNA aísla por completo el acceso a las aplicaciones del acceso a la red, por lo que elimina la necesidad de enlaces MPLS y VPN. Busque ZTNA que se ofrece como un servicio entregado en la nube, ya que esto elimina la necesidad de enviar el tráfico al centro de datos corporativo. En su lugar, los usuarios obtienen acceso rápido y directo a las aplicaciones que necesitan para mantenerse productivos.

Tenga en cuenta que un proveedor de ZTNA con una presencia global ampliada (en cuanto a centros de datos) podrá encontrar la ruta de conectividad más corta entre los usuarios y las aplicaciones. El empleo de conexiones lo más cerca posible del perímetro garantiza que los empleados disfruten de experiencias de usuario de primer nivel.

N.º 3: Aplicar el acceso con privilegios mínimos

El acceso con privilegios mínimos es un principio clave dentro de la filosofía de confianza cero. Su definición es simple: a los usuarios se les otorga sólo el nivel mínimo de acceso necesario para realizar sus tareas laborales, y nada más.

Construir una arquitectura de seguridad que pueda soportar este enfoque puede ser todo un desafío sin la solución ZTNA adecuada. La solución debe incorporar mecanismos sólidos de autenticación de la identidad del usuario, comprender el contexto del dispositivo y tener la capacidad de imponer una segmentación muy granular de usuario a aplicación en sus controles. Para lograr esto, ZTNA debe ofrecer integraciones profundas con todas las principales plataformas de proveedores de identidad (IdP).

Busque una solución ZTNA que pueda hacer cumplir las políticas comerciales y de TI conectando a los usuarios verificados sólo a las aplicaciones que están autorizados a usar, no a la red. Este acceso debe extenderse por igual a usuarios remotos y locales, independientemente de su ubicación, y los controles de seguridad deben ser idénticos para todos los usuarios, en todas partes.

Zscaler habilitó el trabajo remoto seguro para 18 000 empleados de la Ciudad de Los Ángeles.

N.º 4: Mantener la productividad de los usuarios detectando y resolviendo rápidamente problemas de aplicaciones, redes y dispositivos.

Careem mejoró el tiempo medio de respuesta (MTTR) en un 62 % con Zscaler Digital Experience Monitoring.

La adopción de la confianza cero, especialmente si los equipos intentan implementarla mediante VPN heredadas, requiere una segmentación granular de la red.

Desde una perspectiva de ingeniería, esta no es una tarea fácil. Sin embargo, cuando se trata de la experiencia del usuario, existen obstáculos adicionales. Cuando las redes están segmentadas de esta manera, es difícil, si no imposible, que los equipos de la red y del servicio de atención al cliente estén informados sobre el rendimiento de las aplicaciones y los dispositivos de los usuarios finales que necesitan para garantizar excelentes experiencias para los usuarios finales.

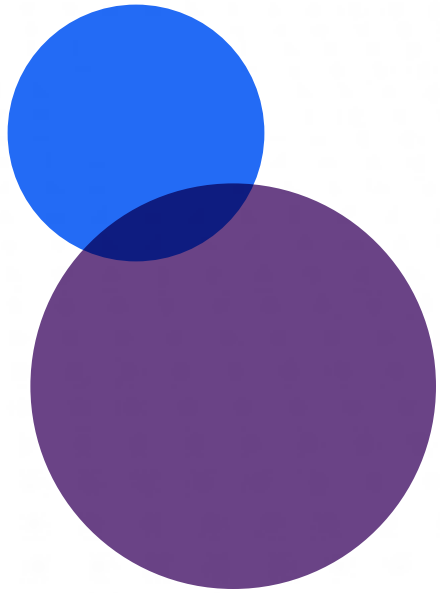
Una solución ZTNA debe proporcionar capacidades clave que ayuden a los equipos a superar este desafío. Debe recopilar métricas sobre el estado del dispositivo del usuario final, el rendimiento de la red y la disponibilidad de la aplicación, y debe presentarlas en un panel de control fácil de supervisar que haga posible que los equipos de soporte al usuario identifiquen y solucionen los problemas antes de que los usuarios finales los experimenten.

N.º 5: Prevenir el movimiento lateral a través de la microsegmentación de la aplicación

Una solución ZTNA debe proteger sus datos, flujos de trabajo, servicios y recursos a través de la microsegmentación definida por software. Esto significa que los usuarios deben conectarse directamente a las aplicaciones, no a la red.

Si se sigue este enfoque, los equipos de seguridad ya no necesitarán preocuparse por el movimiento lateral a través de la red. En caso de que se viole una sola cuenta de usuario o aplicación, no hay forma de que el atacante pueda ir más allá para comprometer otros recursos de la empresa.

Con ZTNA, establecer una conexión a una sola aplicación o recurso nunca debería significar que se le otorga automáticamente acceso a otros.



N.º 6: Admitir el acceso seguro para dispositivos propios de los usuarios y dispositivos corporativos

Careem mejoró el tiempo medio de respuesta (MTTR) en un 62 % con Zscaler Digital Experience Monitoring.

Busque una solución ZTNA que admita el acceso con y sin agente para empleados y terceros.

Busque una solución ZTNA que admita el acceso con y sin agente para empleados y terceros. De esta manera, ZTNA puede permitir que los socios y proveedores accedan sin problemas a sus recursos, al tiempo que hace posible que los empleados usen sus propios dispositivos (incluidos los dispositivos móviles) para fines laborales y hacerlo de manera segura.

A medida que el uso de dispositivos no administrados se vuelve cada vez más habitual, también es importante que su solución ZTNA pueda admitir el acceso sin clientes. De lo contrario, sólo podrá proteger a sus propios empleados en dispositivos corporativos. En el mundo moderno centrado en las comunicaciones móviles, esta es una limitación importante.

N.º 7: Detener los ataques y bloquear las amenazas con una inspección de contenido en línea completa

Para obtener la visibilidad completa que se necesita para bloquear todas las amenazas, una solución ZTNA debería poder realizar una inspección de contenido en línea integral.

Esto significa que el servicio podrá inspeccionar todo el tráfico (incluido el tráfico cifrado con SSL, que se utiliza para enmascarar la transmisión de contenido peligroso como ransomware, spyware y virus), y sólo permitirá el paso de comunicaciones legítimas conocidas. Esta inspección en línea debe tener como base una inteligencia de amenazas cultivada a partir de una amplia gama de señales globales para garantizar que pueda detener el ransomware, el phishing y las amenazas de día cero que prevalecen actualmente, así como los ataques avanzados.

¿Quiere saber contra qué amenazas ZTNA debería poder protegerse? El OWASP Top 10 representa un amplio consenso de expertos sobre los riesgos de seguridad más críticos para las aplicaciones web. Una solución ZTNA debe proporcionar una cobertura integral de las técnicas de ataque más comúnmente empleadas, incluida la inyección de SQL, las secuencias de comandos entre sitios, los escáneres de puertos y entornos, y el envenenamiento de cookies.

Zscaler permite bloquear los riesgos enumerados en el OWASP Top 10 y otros riesgos de seguridad de aplicaciones web conocidos, incluida la inyección de SQL y las secuencias de comandos entre sitios.

N.º 8: Integrarse perfectamente con una amplia gama de proveedores y soluciones de identidad

Zscaler tiene integraciones profundas con proveedores de identidad como Microsoft y Okta, y plataformas de detección y respuesta de punto final (EDR) como CrowdStrike.

Lo primero que hace la seguridad de confianza cero es verificar la identidad del usuario que intenta obtener acceso a una aplicación u otro recurso.

A medida que un número creciente de organizaciones adoptan estrategias que dan prioridad a la nube para respaldar los entornos actuales de trabajo desde cualquier lugar, recurren a una amplia gama de socios de gestión de identidad y acceso (IAM) y gobernanza y administración de identidad (IGA) para respaldar su capacidad de gestionar la autenticación y las identidades de los usuarios a lo largo de su ciclo de vida.

Por supuesto, una solución ZTNA debe integrarse con sus socios actuales de IAM e IGA. Pero debe buscar un proveedor que haya establecido alianzas sólidas con todos los mejores proveedores de soluciones tecnológicas del sector si desea preparar su identidad y su estrategia de autenticación para el futuro.

N.º 9: Incorporar tecnología de engaño integrada para frustrar a los atacantes

La tecnología de engaño es una nueva categoría de solución de ciberseguridad.

El uso de la tecnología de engaño hace posible detectar amenazas del mundo real rápidamente con tasas de falsos positivos muy bajas. Esta tecnología implementa señuelos realistas (por ejemplo, dominios, bases de datos, directorios, servidores, aplicaciones, archivos, credenciales, enlaces) en una red junto con activos reales para actuar como señuelos. En el momento en que un atacante interactúa con un señuelo, la tecnología comienza a recopilar información que utiliza para generar alertas de alta fidelidad.

Aprovechar la tecnología de engaño puede mejorar la capacidad de su equipo de seguridad para detectar amenazas, generar mejores conocimientos sobre los riesgos a los que se enfrenta su negocio, en tiempo real, y permitirle cubrir mejor lo que de otro modo serían puntos ciegos en su entorno. Los señuelos de engaño actúan como trampas en un entorno de confianza cero, detectando cuentas de usuario comprometidas o intentos de moverse lateralmente a través de la red.

Debido a que esta es una tecnología emergente, algunos proveedores de ZTNA aún tienen que integrar plataformas de engaño, pero los líderes del sector ya han hecho este avance.

KuppingerCole denominó a Zscaler un líder en plataformas distribuidas de engaño.

N.º 10: Permitir una implementación rápida y sencilla

A diferencia de otras soluciones tecnológicas que pueden tardar semanas o meses en implementarse, ZTNA, líder en el sector, se puede implementar desde cualquier lugar en cuestión de días.

Zscaler permitió a la Ciudad de Los Ángeles brindar acceso seguro al trabajo desde cualquier lugar a 18 000 empleados en menos de dos semanas.

Vea usted mismo por qué Zscaler Private Access es la plataforma ZTNA más implementada del mundo

Zscaler Private Access (ZPA) hace todo esto y más. Basado en la arquitectura de confianza cero única de Zscaler, ZPA aplica el principio de privilegio mínimo para brindar a los usuarios conexiones seguras y directas a aplicaciones privadas al tiempo que elimina el acceso no autorizado y el movimiento lateral. Debido a que ZPA es un servicio entregado en la nube, se puede implementar en cuestión de horas y reemplaza las VPN y las herramientas de acceso remoto heredadas con una plataforma de confianza cero moderna y holística.

Zscaler Private Access ofrece:

- **Seguridad incomparable, que va mucho más allá de lo que pueden lograr las VPN y los cortafuegos heredados:** los usuarios se conectan directamente a las aplicaciones, no a la red, lo que minimiza la superficie de ataque y elimina la posibilidad de movimiento lateral.
- **El fin del riesgo para las aplicaciones privadas:** la mejor protección de aplicaciones de su clase, con prevención en línea, engaño y aislamiento de amenazas, minimiza el riesgo que plantea el compromiso de las cuentas de usuario.
- **Productividad superior para el personal híbrido de hoy:** acceso ultrarrápido a aplicaciones privadas que se extiende sin problemas a usuarios remotos, oficinas corporativas y sucursales, y socios externos.
- **ZTNA unificado para usuarios, cargas de trabajo y dispositivos:** los empleados y socios pueden conectarse de forma segura a aplicaciones, servicios y dispositivos OT/IoT privados con la plataforma ZTNA más completa.

¿Quiere más información? Solicite una demostración gratuita hoy.

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. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada 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