Libro electrónico

¿Quiere proteger su personal híbrido con ZTNA?

Busque estas 10 capacidades imprescindibles

Libro electrónico

Contenido

Introducción

El mundo laboral está cambiando. La forma y el lugar en que los empleados son más productivos no son los mismos que hace unos pocos años. A medida que cada vez más organizaciones adoptan el trabajo híbrido y remoto, también trasladan un número creciente de aplicaciones de misión crítica a la nube para poder aprovechar al máximo la flexibilidad, escalabilidad y eficiencia que ofrece.

Sin embargo, a medida que los ecosistemas informáticos se transforman, surgen nuevos problemas en materia 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,—pueden ampliar la superficie de ataque, especialmente si no se dejan de lado las soluciones de seguridad heredadas (como las VPN y los firewalls) y los modelos anticuados. 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.

Se necesita un nuevo modelo para asegurar los entornos tecnológicos,—uno que se adapte mejor a las necesidades actuales de seguridad y conectividad. Esto es precisamente lo que ofrece la confianza cero, y en la actualidad está siendo adoptada rápidamente por todas las industrias de diferentes zonas geográficas.

Cada vez son más las organizaciones que eligen el Zero Trust Network Access (ZTNA) para reforzar su postura de seguridad en el trabajo híbrido. El ZTNA ofrece un esquema claro y bien definido para la confianza cero. La empresa de análisis Gartner informa que el mercado de ZTNA se está expandiendo a gran velocidad. Actualmente registra un crecimiento interanual superior al 60 %.

Las organizaciones señalan la sustitución de las VPN como su principal razón para implantar el ZTNA.

¿Qué es Zero Trust Network Access (ZTNA)?

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

El ZTNA funciona con un modelo de confianza adaptable, en el que la confianza nunca se da por sentada, y en el que elacceso solo se concede en función de la "necesidad de conocer", con privilegios mínimos que se definen mediante políticas granulares.

A medida que aumenta el número de organizaciones que adoptan aplicaciones e infraestructuras en la nube, muchas buscan unificar sus servicios de seguridad con una única plataforma en la nube. Esto se conoce como Security Service Edge (SSE)—, que incluye la pasarela web segura (SWG), el agente de seguridad de acceso a la nube (CASB) y las capacidades de ZTNA. Gartner recomienda que los responsables de la seguridad y el control de riesgos inicien sus estrategias de implementación de SSE adoptando el ZTNA. En este sentido, el ZTNA suele ser un primer paso clave en el camino hacia la seguridad en la nube.

Muchas organizaciones están recurriendo al ZTNA para sustituir infraestructuras de VPN que no funcionan bien a escala o que exponen a la organización a un mayor riesgo de seguridad debido a que su presencia amplía la superficie de ataque. Pero el ZTNA es mucho más que un sustituto de las VPN ya queofrece a las organizaciones la oportunidad de eliminar los dispositivos heredados (junto con sus gastos generales de gestión), proporciona a los usuarios un acceso rápido y directo a las aplicaciones, se 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 conseguir todos estos beneficios y muchos más, debe encontrar un producto que le permita tener todas estas características.

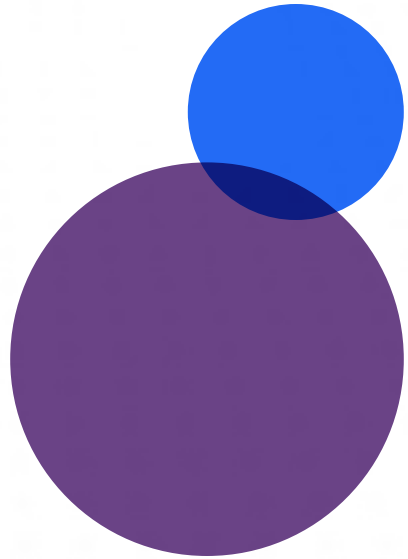
N.° 1: Elimina la superficie de ataque haciendo que las aplicaciones sean invisibles a la Internet pública.

En las arquitecturas de red radiales tradicionales, un atacante capaz de vulnerar el perímetro de seguridad puede encontrar fácilmente las aplicaciones.

Una vez que los agentes maliciosos están dentro de la red, las aplicaciones y otros recursos se pueden descubrir con facilidad mediante una simple búsqueda.

Con una verdadera solución de ZTNA, el acceso a las aplicaciones se concede de forma individualizada mediante la segmentación. Esto hace que sea imposible descubrir otras aplicaciones en su entorno, incluso si un atacante consigue acceder a una de ellas.

Todas las aplicaciones se ocultan tras la plataforma de ZTNA, que actúa como intermediaria para la conectividad directa. Dado que los atacantes no pueden atacar lo que no pueden ver, una solución de ZTNA debe ocultar las identidades de origen ofuscando sus direcciones IP. Básicamente, estas conexiones internas hacen invisible todo su ecosistema de aplicaciones. De este modo, los atacantes no pueden realizar ataques dirigidos contra aplicaciones individuales.



N.° 2: Permite una conectividad sin interrupciones desde cualquier lugar.

El 77 % de las organizaciones actuales han adoptado o están estudiando la posibilidad de permitir 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 se impone el trabajo híbrido y remoto, el uso de las VPN genera problemas de rendimiento porque estas no pueden escalarse.

Por el contrario, ZTNA aísla completamente el acceso a las aplicaciones del acceso a la red, eliminando la necesidad de enlaces MPLS y VPN. Busque un ZTNA que se ofrezca como un servicio en la nube, ya que de esta forma no se necesita retransmitir el tráfico al centro de datos corporativo. En su lugar, los usuarios obtienen un acceso rápido y directo a las aplicaciones que necesitan para seguir siendo productivos.

Tenga en cuenta que un proveedor de ZTNA con una amplia presencia mundial —(en lo que respecta a los centros de datos)— podrá encontrar la ruta de conectividad más corta entre los usuarios y las aplicaciones. La intermediación de conexiones lo más cerca posible del perímetro garantiza que los empleados tengan experiencias de usuario de primera categoría.

N.° 3: Posibilita el acceso con menos privilegios.

El acceso con menos privilegios es un principio clave en la filosofía de la confianza cero. Su definición es sencilla: a los usuarios solo se les concede el nivel mínimo de acceso necesario para realizar sus funciones, y nada más.

Desarrollar una arquitectura de seguridad con este modelo puede ser un verdadero problema si no se cuenta con la solución de ZTNA adecuada. La solución debe incorporar mecanismos sólidos de autenticación de identidad del usuario, comprender el contexto del dispositivo y garantizar una segmentación muy granular de usuario a aplicación en sus controles. Para lograrlo, el ZTNA debe ofrecer integraciones profundas con las principales plataformas de proveedores de identidad (IdP por sus siglas en inglés).

Busque una solución de ZTNA que pueda hacer cumplir las políticas empresariales y de TI conectando a los usuarios verificados solo a las aplicaciones que están autorizados a utilizar, y no a la red. Este acceso debe extenderse igualmente a los usuarios remotos y locales, independientemente de su ubicación y los controles de seguridad, deben ser idénticos para todos los usuarios, en cualquier lugar.

Zscaler permitió trabajar de forma segura y remota a 18,000 empleados de la ciudad de Los Ángeles.

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

N.° 4: Mantiene la productividad de los usuarios detectando y resolviendo rápidamente los problemas de las aplicaciones, la red y los dispositivos.

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

Desde una perspectiva de ingeniería, no es tarea fácil. Sin embargo, cuando se trata de la experiencia del usuario, existen otros obstáculos. Cuando las redes están segmentadas de esta forma, es difícil, por no decir imposible, que los equipos de la red y del servicio de asistencia obtengan la información sobre el rendimiento de los dispositivos y las aplicaciones de los usuarios finales que necesitan para garantizarles una gran experiencia.

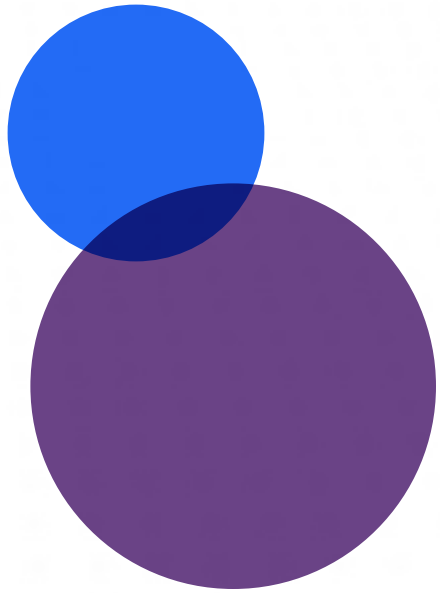
Una solución de ZTNA debe contar con capacidades clave que ayuden a los equipos a superar este reto. Debe recopilar métricas sobre el estado de los dispositivos de los usuarios finales, el rendimiento de la red y la disponibilidad de las aplicaciones, y presentarlas en un panel de control fácil de supervisar que permita a los equipos de asistencia al usuario identificar y solucionar los problemas antes de que los usuarios finales los detecten.

N.° 5: Evita el movimiento lateral gracias a la microsegmentación de las aplicaciones.

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

Si se sigue este modelo, los equipos de seguridad ya no tendrán que preocuparse por el movimiento lateral en la red. Cuando una sola cuenta de usuario o aplicación sea vulnerada, no hay forma de que el atacante pueda llegar más lejos y comprometer otros recursos de la empresa.

Con el ZTNA, el establecimiento de una conexión con una sola aplicación o recurso nunca debe implicar que se le conceda automáticamente el acceso a otras aplicaciones o recursos.



N.° 6: Admite el acceso seguro tanto para BYOD como para dispositivos que pertenecen a la empresa

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

Encuentre una solución de ZTNA que permita tanto el acceso con agente como sin agente para empleados y terceros.

Encuentre una solución de ZTNA que permita tanto el acceso con agente como sin agente para empleados y terceros. De este modo, el ZTNA hace posible que sus socios y proveedores accedan sin problemas a sus recursos, al tiempo que permite que los empleados utilicen sus propios dispositivos (incluidos los dispositivos móviles) con fines laborales, y que lo hagan de forma segura.

Dado que los dispositivos no controlados son cada vez más frecuentes, también es importante que su solución de ZTNA pueda permitir el acceso sin cliente. De lo contrario, solo podrá proteger a sus propios empleados cuando usen dispositivos facilitados por la empresa. En un mundo moderno en donde todo gira en torno a los dispositivos móviles, esta es una limitación importante.

N.° 7: Detiene los ataques y bloquea las amenazas con una inspección exhaustiva de los contenidos en línea.

Para obtener la visibilidad completa que se necesita para bloquear todas las amenazas, una solución de ZTNA debe ser capaz de realizar una inspección completa del contenido en línea.

Esto significa que el servicio podrá inspeccionar todo el tráfico (incluido el cifrado SSL, que se utiliza para ocultar la transmisión de contenidos peligrosos como ransomware, spyware y virus) y solo permitirá el paso de las comunicaciones reales conocidas. Esta inspección en línea debe basarse en la información sobre amenazas obtenida a partir de una amplia variedad de señales globales para garantizar que pueda detener el ransomware, el phishing y las amenazas de día cero más frecuentes en la actualidad, así como los ataques avanzados.

¿Quiere saber contra qué amenazas debería brindar protección el ZTNA? El Top 10 de OWASP incluye la opinión de varios expertos sobre los riesgos de seguridad más importantes para las aplicaciones web. Una solución de ZTNA debería abarcar completamente las técnicas de ataque más utilizadas, como la inyección SQL, las secuencias de comandos entre sitios, los escáneres de entornos y puertos y el envenenamiento de cookies.

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

N.° 8: Se integra perfectamente con una amplia variedad de proveedores de identidad y soluciones.

Zscaler cuenta con integraciones sólidas con proveedores de identidad como Microsoft y Okta, y plataformas de detección y respuesta de puntos finales (EDR) como CrowdStrike.

La seguridad de confianza cero comienza con la verificación de la identidad del usuario que intenta acceder a una aplicación o a otro recurso.

A medida que cada vez más organizaciones adoptan estrategias que dan prioridad a la nube para brindar soporte a los entornos de trabajo actuales desde cualquier lugar, empiezan arecurrir a una amplia variedad de socios de control de identidades y accesos (IAM) y de administración y gobernanza de identidades (IGA) para respaldar su capacidad de controlar la autenticación y las identidades de los usuarios durante su ciclo de vida.

Por supuesto, una solución de ZTNA debe integrarse con sus socios actuales de IAM e IGA. Pero usted debe buscar un proveedor que haya forjado alianzas fuertes con los mejores proveedores de soluciones tecnológicas del sector si desea que su estrategia de identidad y autenticación se adapte al futuro.

N.° 9: Incorpora tecnología de disuasión integrada para frustrar a los atacantes.

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

El uso de la tecnología del engaño permite detectar rápidamente las amenazas del mundo real con índices muy bajos de falsos positivos. Esto consiste en implantar señuelos realistas (por ejemplo, dominios, bases de datos, directorios, servidores, aplicaciones, archivos, credenciales, rutas de navegación) en su red junto a los activos reales para actuar como cebos. En el momento en que un atacante interactúa con un señuelo, la tecnología comienza a recopilar información que utiliza para generar alertas de alta fiabilidad.

La tecnología del engaño puede ayudarle a mejorar la capacidad de su equipo de seguridad para detectar amenazas, generar mejores datos sobre los riesgos a los que se enfrenta su empresa en tiempo real y permitirle abarcar mejor lo que de otra forma serían puntos ciegos en su entorno. Los señuelos actúan como trampas en un entorno de confianza cero, detectando cuentas de usuario comprometidas o intentos de desplazarse lateralmente por la red.

Al tratarse de una tecnología emergente, pocos proveedores de ZTNA han integrado las plataformas de engaño hasta ahora, pero los líderes del sector ya han conseguido este avance.

KuppingerCole mencionó que Zscaler es el líder en Plataformas Distribuidas de Engaño

N.° 10: Permite un despliegue rápido y sencillo

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

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

Compruebe usted mismo por qué Zscaler Private Access es la plataforma ZTNA más utilizada en el mundo

Zscaler Private Access (ZPA) hace todo esto y mucho más. Creado sobre la exclusiva arquitectura de confianza cero de Zscaler, ZPA aplica el principio del menor privilegio para ofrecer a los usuarios conexiones seguras y directas a aplicaciones privadas, al tiempo que elimina el acceso no autorizado y el movimiento lateral. Dado que la ZPA es un servicio prestado en la nube, puede implementarse en cuestión de horas, sustituyendo las VPN y las herramientas de acceso remoto heredadas por una plataforma de confianza cero moderna e integral.

Zscaler Private Access:

- **Ofrece seguridad sin igual, mucho mejor que la que pueden conseguir las VPN y los firewalls 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.
- **Elimina el peligro de las aplicaciones privadas:** La mejor protección de aplicaciones de su clase, con prevención en línea, engaño y aislamiento de amenazas, minimiza el riesgo de las cuentas de usuario.
- **Ofrece más productividad para el personal híbrido de hoy en día:** Un acceso ultrarrápido a aplicaciones privadas que se extiende en forma continua entre usuarios remotos, oficinas corporativas y sucursales, y socios de terceros.
- **Ofrece ZTNA unificada para usuarios, cargas de trabajo y dispositivos:** los empleados y socios pueden conectarse de forma segura a aplicaciones, servicios y dispositivos OT/IoT privados en la plataforma ZTNA más completa de la industria.

¿Desea más información? Solicite hoy mismo una demostración gratuita.

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 al conectar de manera segura a los usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com.mx** o síganos en Twitter **@zscaler.**

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com.mx