Documento técnico

Por qué los responsables de TI deberían considerar una estrategia de acceso a la red de confianza cero

Habilitar el negocio digital a la vez que se protegen los datos

Aunque la tecnología se ha considerado durante mucho tiempo un motor necesario para que la empresa siga avanzando, ahora se reconoce como un verdadero motor empresarial, capaz de crear nuevas eficiencias y oportunidades de ingresos. Del mismo modo, el papel del líder de TI ha evolucionado, con la participación de los CISO, CIO y CTO, que se unen a la suite ejecutiva para centrarse y liderar las iniciativas tecnológicas.

Los principales factores de este cambio han sido el tremendo auge de la adopción de la nube pública empresarial, incluidos Azure, AWS y Google Cloud, y el uso generalizado de dispositivos móviles personales propios de los empleados para el trabajo. Las empresas están aprovechando estas tecnologías para optimizar los procesos empresariales y ofrecer productos y servicios con mayor rapidez y menor coste global.

Pero ¿qué pasa con el riesgo que suponen?

Debido al cambio hacia la nube y la movilidad de los usuarios, ha desaparecido el perímetro de seguridad tradicional que en el pasado protegía a los usuarios y los servicios internos una vez que se encontraban dentro de la red corporativa.

Por ello, al pedir presupuesto para nuevas TI que apoyen la nube y la movilidad, es preciso ayudar a la junta directiva a ver la conexión entre el riesgo y su impacto potencial en los ingresos de la empresa. Es importante comunicar eficazmente el coste que supone una infracción de datos, el coste del tiempo de inactividad de las infraestructuras críticas y el coste de la pérdida de reputación de la marca. Básicamente, TI debe promover una conversación sobre el valor empresarial que los ejecutivos entiendan.

Lo primero que los líderes de TI deben comprender es a qué riesgos se enfrenta su empresa y determinar hasta qué punto la empresa es propensa al riesgo. Sus aplicaciones críticas para el negocio pueden cumplir con SOC1 o ISO 27001 y requerir capas adicionales de seguridad. Estas se consideran una infraestructura crítica. Puede haber ciertos países, como China, que deben aislarse de otros países. Con la infraestructura heredada que necesita una evaluación continua de los parches, una configuración de cortafuegos errónea podría suponer enormes problemas para la empresa.

Los desafíos que deben superar los líderes tecnológicos

A fin de lograr habilitar iniciativas de negocio clave y salvar la distancia entre las necesidades de la empresa y las capacidades de las TI, los líderes de TI deben elegir una tecnología que les ayude a superar sus desafíos y les permita:

1. Facilitar el trabajo y minimizar el estrés para su personal
2. Ofrecer una experiencia de usuario superior para empleados y terceros
3. Reducir los riesgos que pueden amenazar la productividad, la propiedad intelectual y la reputación de la empresa
4. Ser adaptables y ágiles para potenciar un negocio que cambia dinámicamente
5. Acelerar la transformación digital mediante la adopción de la nube pública

Identificar las tecnologías que permitirán alcanzar estos objetivos es una tarea difícil ya que, en ocasiones, los resultados deseados de una solución pueden añadir complejidad a otra. Por ejemplo, la decisión de adoptar servicios en la nube y tecnologías móviles logra el objetivo de una experiencia de usuario optimizada, pero ¿qué ocurre con el objetivo de minimizar el riesgo de un ataque de ciberseguridad? Los responsables de TI deben encontrar un delicado equilibrio entre la aceleración de la adopción de nuevas tecnologías y la garantía de la seguridad de los datos confidenciales. Por lo tanto, es fundamental elegir la tecnología adecuada en el momento adecuado.

El valor de ZTNA para la empresa

Gartner recomienda que los líderes de TI adopten ZTNA como parte de una estrategia de perímetro de servicio de seguridad (SSE) para brindar conectividad flexible y segura al personal híbrido. Los servicios ZTNA proporcionan un acceso seguro a las aplicaciones empresariales privadas para los usuarios remotos y locales sin necesidad de tecnologías VPN tradicionales.

Los servicios ZTNA crean un límite de acceso lógico basado en el contexto y la identidad en torno a una aplicación o un conjunto de aplicaciones. Las aplicaciones se ocultan para no ser descubiertas y el acceso se restringe a un conjunto de entidades designadas a través de un intermediario de confianza. El intermediario verifica la identidad del usuario, el contexto y la adhesión a la política de los participantes especificados antes de permitir la intermediación de la conexión.
Esto evita que los activos de la aplicación sean visibles en Internet y reduce significativamente la superficie de ataque.

Gartner

Para el año 2025, al menos el 70 % de los nuevos despliegues de acceso remoto serán servidos predominantemente por ZTNA en contraposición a los servicios VPN, frente a menos del 10 % a finales de 2021.

Anteriormente se han mencionado los cinco factores clave que los responsables de TI deben tener en cuenta a la hora de adoptar nuevas tecnologías. Echemos un vistazo al papel que desempeña ZTNA en la habilitación de cada uno de ellos:

1. Mejora la productividad:

Tres de cada cuatro empleados a tiempo completo en las oficinas están **planeando renunciar este año,** sumándose a las decenas de millones que ya han dado este paso durante la gran renuncia impulsada por la pandemia. Con la reorganización masiva de la mano de obra, los empresarios se están replanteando cómo fidelizar y atraer el talento, y los responsables de TI pueden utilizar la tecnología para ayudar a cambiar esta tendencia mientras sientan las bases para el futuro del trabajo.
La facilidad de uso de ZTNA ofrece importantes beneficios a los usuarios, ya que elimina los quebraderos de cabeza que supone iniciar un cliente VPN cada vez que el usuario se conecta a la red, lo que mantiene la productividad alta y la frustración al mínimo.
La simplicidad de ZTNA, que se entrega en la nube y es solo software, hace que sea fácil de configurar e implementar. Esta simplicidad permite al departamento de TI adoptar una tecnología de aplicaciones en la nube segura, incluso en dispositivos móviles, al tiempo que se maximiza la productividad del personal de TI y de toda la organización.

2. Proporciona experiencias de usuario superiores:

Hoy en día, los usuarios trabajan desde cualquier lugar: en la oficina, en casa e incluso de viaje. Estos usuarios a menudo son una combinación de empleados y terceros, los cuales esperan un acceso sin fricciones a las aplicaciones independientemente de su dispositivo, ubicación o red. ZTNA garantiza que cada usuario tenga una experiencia rápida y completamente fluida.
También elimina la necesidad de una VPN y los incómodos inicios de sesión, a la vez que admite usuarios de terceros y todo tipo de dispositivos sin necesidad de un agente de punto final.

Además, el ZTNA sin clientes que aprovecha el acceso basado en políticas a las aplicaciones privadas aumenta la productividad, ya que los usuarios pueden conectarse a las aplicaciones desde cualquier dispositivo, independientemente de su ubicación.

3. Reduce el riesgo:

La seguridad sigue siendo una preocupación para la adopción de la nube y el trabajo a distancia, ya que pueden aumentar la probabilidad de un ataque contra las aplicaciones e infraestructuras críticas para la empresa si no se manejan con cuidado. Las tecnologías tradicionales centradas en la red, como las VPN y los cortafuegos, son excesivamente confiadas y deben evitarse. Estas soluciones colocan a los usuarios remotos directamente en la red, lo que requiere que los servidores VPN escuchen las llamadas entrantes de Internet. Es por ello que las VPN se han convertido en caballos de Troya para el ransomware. Esto significa que, tanto si es remoto como local, el usuario tiene acceso lateral a través de la red. Este es el caso tanto de empleados como de terceros que podrían tener prácticas de seguridad más débiles. Los servicios ZTNA utilizan políticas basadas en la confianza cero para brindar conectividad a aplicaciones privadas específicas que se ejecutan en una nube pública, nube privada o centro de datos exclusivamente a usuarios autorizados (basándose en la identidad y en la postura del dispositivo). La reciente evolución de ZTNA, que ha pasado de proporcionar principalmente conectividad a proporcionar una seguridad completamente integrada para proteger las aplicaciones frente a amenazas internas y atacantes avanzados, ayuda a las organizaciones a mejorar su nivel general de seguridad.

4. Agilidad y escala en la nube:

Hoy en día, la cantidad de empleados, dispositivos de usuario, aplicaciones y tráfico sigue creciendo. El proveedor aloja los servicios ZTNA entregados en la nube, por lo que el aumento de la escala ya no es una preocupación para TI. A medida que aumenta la demanda, el servicio ZTNA gestiona la carga adicional automáticamente. No es necesario desplegar dispositivos de hardware adicionales ni cortafuegos virtualizados que ralentizarían los proyectos de adopción de la nube pública. Más agilidad y más escala son fundamentales para el éxito de un líder de TI, y ZTNA lo proporciona.

5. Acelera la transformación digital:

Hoy en día, la nube y la movilidad son prioridades para la mayoría de los equipos empresariales. Sin embargo, si están implementadas las soluciones incorrectas, puede tardar meses o incluso años en aprovechar la nube de forma segura en una base de usuarios global. Esto se debe, en parte, a la complejidad que supone el uso de la tecnología tradicional de redes y seguridad para proporcionar acceso a las aplicaciones en la nube desde dispositivos de usuario no gestionados. ZTNA utiliza software para reducir la complejidad, lo que reduce el tiempo de implementación de meses o años a solo horas. Con ZTNA, las organizaciones pueden obtener rápidamente los beneficios de la nube y mejorar la movilidad.

> “Con los cambios que hemos hecho en nuestro recorrido hacia la nube, confío en que estaremos en una posición sólida para gestionar cualquier eventualidad. Al final, esta experiencia tendrá un impacto duradero y acabará por cambiar la mentalidad heredada. Estamos presentando nuevas formas de trabajar, a la vez que mostramos el impacto de la tecnología y de la resistencia y creatividad de nuestro personal”.
>
> — **Alex Philips,** CIO de National Oilwell & Varco

Más información sobre ZTNA

Los servicios de acceso a la red de confianza cero son una herramienta valiosa para los líderes de TI empresariales. En Zscaler, hemos desarrollado un servicio ZTNA denominado Zscaler Private Access (ZPA). El servicio utiliza nuestra nube global para proporcionar acceso seguro y sin problemas a las aplicaciones internas. Esto es exactamente lo que se necesita para que TI pase de ser el "centro de costes" a convertirse en el héroe de la sala de juntas.

No se olvide de ver la historia de Paychex relatada por Carlo Cong, director sénior de Enterprise Technology Services, acerca de cómo simplificaron y aceleraron sus integraciones de TI de fusiones y adquisiciones con ZTNA.

Vea la historia de CMA-CGN

Haga que su equipo pruebe de forma gratuita durante 7 días la solución ZTNA de Zscaler.

Comience una demostración de ZTNA de 7 días

¿Tiene más preguntas? No dude en ponerse en contacto directamente con nuestros expertos en ZTNA en **sales@zscaler.com.**

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