El estado de la transformación de confianza cero 2023

DE LA PREVENCIÓN A LA HABILITACIÓN:
aprovechar todo el potencial de la confianza cero para las empresas altamente móviles y centradas en la nube.

Índice

Resumen ejecutivo

Nathan Howe | Vicepresidente de Tecnología Emergente y 5G de Zscaler

En un contexto de rápida transformación digital, la confianza cero ha surgido como el marco ideal para proteger a los usuarios, las cargas de trabajo y los dispositivos empresariales en su nube altamente distribuida y su mundo centrado en los dispositivos móviles.

Los responsables de TI de todo el mundo se están dando cuenta de ello, a medida que la confianza cero se va imponiendo y altera décadas de principios de seguridad y redes heredadas.

Más del 90 % de los responsables de TI que han iniciado su migración a la nube han implementado, o están en proceso de implementar, una estrategia de seguridad de confianza cero en el próximo año. Eso se desprende de los resultados de nuestra última encuesta mundial, que recabó la opinión de más de 1900 directores de sistemas de información, directores de seguridad de la información, directores de datos, directores de tecnología y responsables de infraestructuras de organizaciones que ya han empezado a migrar aplicaciones y servicios a la nube.

Esta evolución es correcta, y las razones de dicho desarrollo evidencian un optimismo continuo en cuanto a la implementación de una arquitectura de confianza cero más allá de los próximos 12 meses.

22 %

Solo el 22 % confía plenamente en que su organización está aprovechando todo el potencial de su infraestructura en la nube, por lo que los resultados indican la necesidad de ir más allá de la mera seguridad.

De hecho, a medida que continúan sus recorridos en la nube, los argumentos a favor de la confianza cero parecen claros. Más de dos tercios (68 %) de los responsables de TI están de acuerdo en que la transformación segura de la nube es imposible con la infraestructura de seguridad de red heredada o en que el acceso a la red de confianza cero tiene claras ventajas sobre los cortafuegos tradicionales y las VPN cuando se trata de proteger el acceso remoto a las aplicaciones.

Sin embargo, solo el 22 % confía plenamente en que su organización está aprovechando todo el potencial de su infraestructura en la nube, por lo que los resultados indican la necesidad de ir más allá de la mera seguridad. Cuando se enfoca desde una perspectiva de TI global, la confianza cero tiene el potencial de desbloquear una gran cantidad de oportunidades en un proceso general de digitalización: sí, puede prevenir ataques de ciberseguridad a gran escala, pero también puede hacer mucho más, desde impulsar una mayor innovación hasta apoyar un mejor compromiso de los empleados o proporcionar eficiencias de costes tangibles.

A medida que las organizaciones se enfrentan a una nueva clase de entorno laboral moderno enfocado en lo híbrido y que depende de todo un conjunto de tecnologías emergentes como IoT/OT, 5G e incluso el metaverso de la transformación digital, deben ampliar la lente a través de la cual ven confianza cero y transformación digital. Una plataforma de confianza cero tiene el poder de rediseñar los requisitos de las infraestructuras empresariales y organizativas: puede convertirse en un verdadero motor empresarial que no solo permita a las empresas ofrecer el modelo de trabajo híbrido que exigen los empleados, sino hacer que las organizaciones estén totalmente digitalizadas con todas las ventajas que ello conlleva, desde agilidad y eficiencia hasta infraestructuras preparadas para el futuro.

Encargamos esta investigación para descubrir el estado actual de la transformación de confianza cero en las organizaciones. Lo que descubrimos es prometedor: las tasas de implementación son importantes. Pero las razones de esa implementación podrían ser más ambiciosas. Los líderes de TI tienen una oportunidad increíble para informar a los responsables de la toma de decisiones empresariales sobre la confianza cero y llevarla a la mesa como impulsor empresarial de alto valor, ya que es el vínculo que falta para ayudar a las empresas a que actualmente se empoderen y se preparen para futuras tecnologías.

ESTADO DE CONFIANZA CERO

90 % Más del 90 % de las organizaciones que han iniciado su migración a la nube han implementado o están en proceso de implementar una estrategia de seguridad de confianza cero en los próximos 12 meses.

88 % A nivel mundial, el 88 % de los responsables de TI confía en que su organización está aprovechando el potencial de la infraestructura en la nube, pero solo el 22 % tiene confianza plena.

REGIONALMENTE, LA CONFIANZA PLENA EN EL APROVECHAMIENTO DEL POTENCIAL DE LA INFRAESTRUCTURA EN LA NUBE SE SITÚA EN:

Número 1 ZTNA es la prioridad número uno para la inversión en tecnología de confianza cero en los próximos 12 meses, lo que indica la importancia del acceso remoto para el lugar de trabajo híbrido.

68 % Más de dos tercios (68 %) de los líderes de TI están de acuerdo en que la transformación segura de la nube es imposible con la infraestructura de seguridad de red heredada o en que el acceso a la red de confianza cero tiene claras ventajas sobre los cortafuegos tradicionales y las VPN cuando se trata de proteger el acceso remoto a las aplicaciones.

54 % de los responsables de TI indicaron que, en su opinión, tanto las VPN como los cortafuegos perimetrales son ineficaces a la hora de proteger contra los ciberataques o de proporcionar visibilidad sobre el tráfico de aplicaciones y los ataques.

LAS PRINCIPALES BARRERAS QUE IMPIDEN APROVECHAR TODO EL POTENCIAL DE LA NUBE:

45 % Las dificultades de proteger los datos en la nube y de garantizar la privacidad de la información

42 % Dificultad de escalar la complejidad de la red y el hardware de seguridad

40 % Acceso remoto y de terceros a IoT y OT

33 % Conectividad incoherente y mala experiencia de acceso remoto para los usuarios.

APARTE DE LA SEGURIDAD, EL ACCESO Y LA COMPLEJIDAD, ENTRE LAS PRINCIPALES RAZONES PARA IMPLEMENTAR UNA ARQUITECTURA DE CONFIANZA CERO NO SE INCLUYEN FACTORES ESTRATÉGICOS DE PROMOCIÓN EMPRESARIAL:

65 % Mejorar la detección de amenazas avanzadas o ataques a aplicaciones web, y ampliar la seguridad de los datos confidenciales

44 % Proteger el acceso remoto para proveedores, socios y tecnología operativa

27 % Mejorar la conectividad segura para una plantilla híbrida

24 % Reducir el coste y la complejidad de la seguridad de las redes heredadas

Sección I

El contexto de la nube que subyace a la adopción de la confianza cero

Cuando nos referimos a la "nube" en esta encuesta, estamos hablando de aplicaciones, datos y cargas de trabajo que se proporcionan como servicios alojados a través de Internet, en lugar de en un centro de datos local dentro de una red corporativa. Algunos ejemplos son el software como servicio (SaaS), la infraestructura como servicio (IaaS), la plataforma como servicio (PaaS) o las aplicaciones privadas creadas o alojadas en la nube.

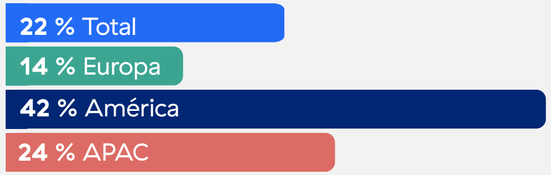
Antes de profundizar en los aspectos específicos de la confianza cero, queríamos establecer el contexto detrás de su adopción. De esta manera, examinamos lo que está sucediendo en el panorama de TI más amplio que la rodea y específicamente en qué punto de sus recorridos en la nube se encuentran las organizaciones.

No cabe duda de que los acontecimientos de los últimos años han acelerado el paso a la nube. En muchas organizaciones, el proceso ya está muy avanzado o incluso ya ha finalizado.

Entrevistamos a más de 1900 CIO, CISO, CDO, CTO y jefes de infraestructura de todo el mundo que trabajan en organizaciones que ya han empezado a migrar aplicaciones y servicios a la nube. De ellos, casi la mitad (46 %) afirmaron que el proceso de migración se había completado al 100 %.

Sin embargo, mientras que el 88 % de los líderes de TI tienen cierto nivel de confianza en que están aprovechando al máximo su viaje a la nube, solo el 22 % está completamente seguro de que su organización está aprovechando todo el potencial de la infraestructura de la nube en la actualidad.

LOS ENCUESTADOS CONFÍAN MUCHO EN QUE SU ORGANIZACIÓN ESTÁ APROVECHANDO TODO EL POTENCIAL DE LA INFRAESTRUCTURA EN LA NUBE HOY EN DÍA.



PORCENTAJE DE ENCUESTADOS MUY SEGUROS DE QUE SU ORGANIZACIÓN ESTÁ APROVECHANDO TODO EL POTENCIAL DE LA INFRAESTRUCTURA EN LA NUBE EN LA ACTUALIDAD

Pase el cursor por encima de los países para ver más detalles.

Europa:

- 9 % Alemania
- 11 % Francia
- 11 % España
- 19 % Reino Unido

América:

- 41 % Estados Unidos
- 51 % Brasil

APAC:

- 16 % Singapur
- 55 % India

Si examinamos las diferencias regionales, los responsables de TI europeos son los que muestran más dudas en su uso de la infraestructura en nube, pues solo un 14 % expresa total confianza. En América, sin embargo, esta cifra se eleva al 42 %.

Aunque no hay una única causa clara para esta disparidad, una posible razón puede ser las diferencias culturales en la velocidad de adopción de tecnologías innovadoras, pues Europa tradicionalmente adopta un enfoque más conservador y, además, se centra más en la privacidad de los datos. Asimismo, con la afianzada infraestructura de conectividad y el cuidado en la fabricación característicos en Europa, la motivación para adoptar de inmediato innovaciones como el 5G es menor, y se tarda más en cambiar los procesos empresariales. Como exploraremos más adelante, las organizaciones de América se centran más en las tecnologías emergentes, como la inteligencia artificial, el aprendizaje automático y la realidad aumentada, lo que sugiere que ya existen planes de infraestructura en la nube para respaldar casos de uso más sofisticados.

Pero, en términos generales, ¿por qué a las organizaciones les está costando aprovechar todo el potencial de la nube?

A primera vista, la seguridad aparece como la principal barrera y los líderes de TI seleccionan dos razones relacionadas con la seguridad para responder a esta pregunta:

PRINCIPALES BARRERAS QUE IMPIDEN APROVECHAR TODO EL POTENCIAL DE LA NUBE:

45 % Preocupaciones y desafíos en cuanto a la privacidad de los datos al proteger los datos en la nube.

42 % La adaptación de la red es un proceso complejo, y su seguridad es difícil de escalar.

40 % Desafíos para permitir el acceso de terceros y el acceso remoto a los sistemas IoT y OT.

33 % Conectividad incoherente y mala experiencia de acceso remoto para los usuarios

PRINCIPALES BARRERAS QUE IMPIDEN APROVECHAR TODO EL POTENCIAL DE LA NUBE, POR PAÍSES

Pase el cursor por encima de los países para ver más detalles.

En toda Europa y APAC predominan las preocupaciones sobre la privacidad de datos:

- 36 % España
- 34 % India
- 33 % Italia
- 32 % Australia
- 28 % Francia

En América, las organizaciones se enfrentan a desafíos para proteger los datos en la nube:

- 44 % Brasil
- 30 % Estados Unidos

Mientras tanto, Singapur y Japón, en particular, luchan por ampliar el hardware de seguridad de las redes:

- 41 % Singapur
- 30 % Japón

En un entorno basado en la nube, la superficie de ataque aumenta exponencialmente y cada servicio, usuario y dispositivo orientado a Internet se convierte en un posible punto de entrada, en una puerta delantera vulnerable que debe protegerse contra amenazas.

Las organizaciones tienen buenas razones para estar preocupadas. En un entorno basado en la nube, la superficie de ataque aumenta exponencialmente y cada servicio, usuario y dispositivo orientado a Internet se convierte en un posible punto de entrada, en una puerta delantera vulnerable que debe protegerse contra amenazas. Abordaremos este tema con más profundidad en la próxima sección.

Pero un vistazo a las motivaciones generales que subyacen a las migraciones a la nube apunta a una barrera mucho más fundamental en la forma en la que los responsables de TI ven la nube y que sin duda afecta a su uso efectivo. Cuando se preguntó sobre los principales factores que impulsan los proyectos de transformación digital en sus organizaciones, tres factores se posicionaron en los primeros lugares: reducir los costes, facilitar la innovación tecnológica y gestionar el ciberriesgo.

LOS PRINCIPALES FACTORES QUE IMPULSAN LOS PROYECTOS DE TRANSFORMACIÓN DIGITAL DE ACUERDO CON LOS LÍDERES DE TI GLOBALES SON:

- Reducir los costes de la **infraestructura** de TI.
- Facilitar innovaciones como la tecnología **5G y la informática en el perímetro.**
- Mitigar **el riesgo** de ciberseguridad.
- Gestionar **entornos multinube.**
- Mejorar la capacidad de atraer y retener **al mejor talento.**

LOS PRINCIPALES FACTORES QUE IMPULSAN LOS PROYECTOS DE TRANSFORMACIÓN DIGITAL POR PAÍS

Pase el cursor por encima de los países para ver más detalles.

Brasil se alineó con el consenso global; la mayoría de las organizaciones mencionaron reducir los costes de infraestructura de TI como el principal impulsor.

Sin embargo, en algunos países europeos sucedió algo diferente. En Francia, las organizaciones estaban más preocupadas por habilitar el trabajo híbrido, mientras que la principal prioridad en Suecia era la experiencia del usuario.

Facilitar innovaciones como la tecnología 5G y la informática perimetral fue más importante en los países que miran más al futuro, como Japón, México y Singapur. En Singapur, el crecimiento de los ingresos fue igual de importante.

La optimización de los procesos empresariales también fue uno de los tres factores más importantes en Brasil y España.

Todo muy práctico y todo impulsado por las TI. De hecho, la gran importancia que se concede a la reducción de costes, aunque comprensible en el clima actual, indica que todavía puede haber una clara falta de comprensión de las principales ventajas de la nube. Y esto, a su vez, podría estar influyendo en el enfoque y el uso de las tecnologías que se están introduciendo para apoyarla. **Entra en juego la confianza cero.**

No cabe duda de que los acontecimientos de los últimos años han acelerado el paso a la nube.

Sección II

Argumentos a favor de la confianza cero

La confianza cero es un enfoque global de la seguridad de las organizaciones modernas basado en el acceso con menos privilegios y en el principio de que ningún usuario o aplicación debe ser intrínsecamente confiable. Comienza con la suposición de que todo es hostil y solo establece la confianza basándose en la identidad y el contexto del usuario, sirviendo la política como guardián en cada paso del camino. En los Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) define el principio subyacente de una arquitectura de confianza cero de esta forma: "No se concede confianza implícita a activos o cuentas de usuario basándose únicamente en su ubicación física o en la red (es decir, redes de área local frente a Internet) o en de quién sea el activo (empresarial o personal)". Es una nueva versión del viejo refrán "nunca confíe, siempre verifique".

Con la seguridad, el acceso y la complejidad como principales preocupaciones relacionadas con la nube de los líderes de TI, no resulta sorprendente que cada vez más organizaciones se interesen en la confianza cero como medio para superar estos obstáculos. Las respuestas mostraron que las organizaciones están desarrollando un buen entendimiento básico de las ventajas de seguridad de la confianza cero frente a enfoques más tradicionales en este nuevo entorno operativo.

Cuando se preguntó sobre la infraestructura tradicional de red y seguridad, el 54 % de los líderes de TI indicaron que creían que las VPN o los cortafuegos perimetrales son ineficaces para protegerse contra ciberataques o proporcionar visibilidad del tráfico de aplicaciones y de los ataques. Otro 68 % reconoció que, en cuanto al acceso remoto seguro a aplicaciones, el acceso a la red de confianza cero (ZTNA) tiene claras ventajas sobre los cortafuegos y las VPN tradicionales, o que la transformación segura de la nube no puede lograrse con la infraestructura de seguridad de red heredada.

Pase el cursor por encima de los países para ver más detalles.

Encuestados que están de acuerdo en que la transformación segura de la nube es imposible con una infraestructura de seguridad de red heredada y en que el acceso a la red de confianza cero tiene claras ventajas sobre los cortafuegos y VPN tradicionales cuando hay que proteger el acceso remoto a las aplicaciones.

- 85 % India
- 81 % Estados Unidos
- 75 % Brasil
- 75 % Singapur
- 73 % Suecia

Encuestados que están de acuerdo en que las VPN y los cortafuegos perimetrales son ineficaces en la protección contra ciberataques o proporcionan poca visibilidad del tráfico de aplicaciones y de los ataques:

- 72 % India
- 65 % Singapur
- 64 % Japón
- 57 % Alemania
- 56 % Estados Unidos

Encuestados que están de acuerdo en que, además de la seguridad, los equipos de TI necesitan herramientas integradas para analizar, solucionar y resolver eficazmente los problemas de la experiencia del usuario:

- 70 % India
- 63 % México
- 62 % Estados Unidos
- 56 % Singapur
- 51 % España
- 50 % Japón

90 %

Más del 90 % de los encuestados que han iniciado su migración a la nube han implementado o están en proceso de implementar una estrategia de seguridad de confianza cero en los próximos 12 meses.

Si miramos más allá de esta toma de conciencia, lo más prometedor es que actúan en consecuencia. Más del 90 % de los encuestados que han iniciado su migración a la nube han implementado o están en proceso de implementar una estrategia de seguridad de confianza cero en los próximos 12 meses.

Italia e India lideran el camino a la hora de implementar una estrategia de seguridad de confianza cero; el 97 % de las organizaciones italianas y el 96 % de las organizaciones indias confirman que tienen una o están en proceso de implementarla.

Pase el cursor por encima de los países para ver más detalles.

Porcentaje de organizaciones que ya disponen de seguridad de confianza cero, que la están implantando o que están en proceso de planificación estratégica para implantarla:

- 97 % Italia
- 96 % India
- 95 % Reino Unido
- 95 % Estados Unidos
- 94 % Japón
- 93 % Brasil
- 93 % Singapur
- 92 % Alemania
- 91 % México
- 90 % Países Bajos
- 89 % España
- 89 % Francia
- 88 % Australia
- 85 % Suecia

La confianza cero sigue considerándose predominantemente una solución de seguridad aislada centrada en las TI... pero la confianza cero podría ofrecer a las organizaciones mucho más que eso.

Desafortunadamente, tener un sistema de seguridad de confianza cero implantado o tener planes de implementar uno no son evidencias suficientes de que se está aprovechando todo su potencial para habilitar las actividades empresariales.

De hecho, las conclusiones indican que la confianza cero sigue considerándose predominantemente una solución de seguridad aislada centrada en las TI, lo que significa que se están abordando los retos de seguridad inmediatos y se están logrando beneficios tácticos. No obstante, la confianza cero podría ofrecer a las organizaciones mucho más que eso.

PRINCIPALES RAZONES PARA IMPLANTAR UNA ARQUITECTURA DE CONFIANZA CERO

65 % Mejorar la detección de amenazas avanzadas o ataques a aplicaciones web, y ampliar la seguridad de los datos confidenciales

44 % Proteger el acceso remoto para proveedores, socios y tecnología operativa

27 % Mejorar la conectividad segura para una plantilla híbrida

24 % Reducir el coste y la complejidad de la seguridad de las redes heredadas

RAZONES PRINCIPALES PARA IMPLANTAR UNA INFRAESTRUCTURA DE CONFIANZA CERO EN TODO EL MUNDO:

Pase el cursor por encima de los países para ver más detalles.

Mejorar la detección de amenazas avanzadas.

- 52 % India
- 42 % Singapur
- 41 % Estados Unidos
- 39 % Italia
- 35 % España
- 30 % Francia
- 26 % Reino Unido

Mejorar la detección de ataques a aplicaciones web:

- 44 % Brasil
- 35 % México

Ampliar la seguridad a fin de proteger los datos confidenciales:

- 44 % Brasil

Proporcionar acceso remoto seguro a proveedores, socios y contratistas:

- 33 % Australia
- 32 % Japón
- 24 % Países Bajos

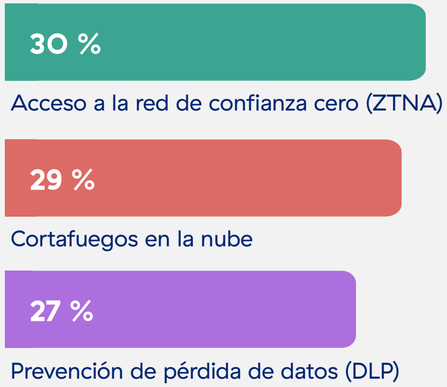
Este enfoque de la confianza cero (utilizarla con fines de seguridad solo al principio de un viaje de transformación) limita significativamente su potencial, en un momento en que tantos factores influencian la capacidad de una organización para digitalizarse e innovar, a velocidad y a escala.

Cuando se entiende correctamente y no se considera simplemente una tecnología o un producto, permite a las empresas simplificar su infraestructura, replantearse su forma de hacer negocios y posibilita la transformación de una organización en una empresa totalmente digitalizada. Por ejemplo, las empresas que han logrado la confianza cero tienen un inventario completo y preciso de todas sus aplicaciones y de todo lo que tienen dentro de su organización. A partir de este inventario, pueden tomar decisiones estratégicas sobre cómo optimizar procesos, reducir costes, eliminar hardware heredado y mejorar la eficiencia.

Pero para lograr estos beneficios estratégicos, el mensaje sobre la confianza cero debe ser capaz de entrar en la sala de juntas y convertirse en parte de la estrategia empresarial más amplia. Hoy en día, está claro que todavía hay incertidumbre y probablemente una carencia de habilidades en torno a lo que significa la confianza cero y su impacto en la empresa. La tarea urgente que tenemos entre manos es ayudar a los líderes empresariales, incluidos los directores de sistemas de información, a comprender que el objetivo de la confianza cero es introducir simplicidad en la infraestructura general eliminando el hardware de administración intensiva para que pueda ofrecer más fácilmente los resultados empresariales precisos que necesita una organización, todo ello manteniendo la seguridad de máximo nivel.

Si observamos las tecnologías de confianza cero a las que las organizaciones van a dar prioridad de inversión en los próximos doce meses, hay pruebas de que esta comprensión de los beneficios empresariales está evolucionando, pero a un ritmo notablemente diferente en las distintas regiones del mundo y con un amplio margen de mejora.

PRINCIPALES TECNOLOGÍAS DE CONFIANZA CERO EN LAS QUE LAS ORGANIZACIONES ESTÁN INVIRTIENDO:



PUNTO DE VISTA REGIONAL: LA VOZ DE AMÉRICA

Amit Chaudhry, director sénior de Marketing de Productos

Hoy en día, las organizaciones están adoptando tecnologías de nube, movilidad, IA, IoT y OT para hacer que los negocios sean más ágiles y competitivos. Los usuarios están en todas partes, y también lo están sus datos. Pero, naturalmente, para una colaboración rápida y productiva, quieren acceso directo a las aplicaciones desde cualquier lugar y en cualquier momento.

Este ritmo explosivo de transformación digital ha brindado a los delincuentes la oportunidad de aprovecharse de arquitecturas de red y seguridad con décadas de antigüedad. Las cifras de ataques se han vuelto incomparables, especialmente las de ataques de ransomware y a la cadena de suministro. A medida que estos se vuelven más sofisticados, la seguridad basada en el perímetro mediante VPN y cortafuegos no protege la red suficientemente, ni ofrece una buena experiencia de usuario.

Para conseguir un lugar de trabajo híbrido seguro, las organizaciones se están alejando rápidamente de los cortafuegos y las VPN para acercarse a la arquitectura de confianza cero, que garantiza un acceso rápido y directo a las aplicaciones desde cualquier lugar y en cualquier momento. Basada en el principio del acceso con privilegios mínimos en el que la conexión se realiza en función de la identidad y el contexto, la confianza cero es quizás la idea más simple pero más importante relacionada con la forma en que se protegen los datos.

Hoy en día, está claro que todavía hay incertidumbre y probablemente una carencia de habilidades en torno a lo que significa la confianza cero y su impacto en la empresa.

Sección III

Adoptar la confianza cero para ofrecer formas híbridas de trabajar

Por infraestructura de trabajo híbrido se entiende una infraestructura que permite a los empleados cambiar de entorno de trabajo sin problemas, alternando entre ubicaciones físicas y remotas, sin limitaciones ni complejidad administrativa.

Cuando los primeros confinamientos obligaron a las organizaciones a establecer apresuradamente a los empleados para que trabajasen casa, no teníamos ni idea de que esta "medida temporal" abriría las puertas a una forma completamente nueva de trabajar ni de que, de hecho, el propio trabajo nunca volvería a ser lo mismo.

Ahora, los trabajadores de hoy tienen varias opciones: trabajar desde casa, la oficina o cualquier otro lugar, y deberían disponer de la tecnología para hacerlo posible.

Los encuestados prevén que, en los próximos 12 meses, sus plantillas sigan adoptando plenamente las distintas opciones a su disposición, divididas entre trabajadores de oficina a tiempo completo (38 %), totalmente a distancia (35 %) e híbridos (27 %). Estas cifras son relativamente uniformes en todo el mundo.

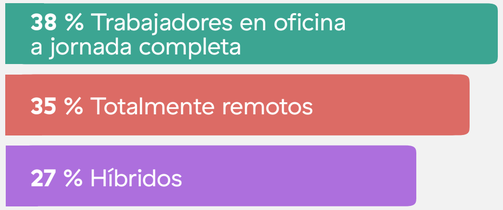
Aunque casi dos tercios (el 62 %) de los líderes de TI dicen que sus organizaciones adoptan el mundo híbrido u ofrecen a su personal la flexibilidad total de trabajar a distancia, el hecho de que más de un tercio (38 %) prediga que van a volver a estar en la oficina a tiempo completo es preocupante y, a la vez, sorprendente.

Aunque esto puede ser comprensible para ciertos sectores que dependen de interacciones cara a cara (como la atención sanitaria y la hostelería), en condiciones favorables del mercado también podría llevar a muchas organizaciones a tener dificultades para atraer y retener talento si no pueden ofrecer el entorno de trabajo flexible que los trabajadores esperan desde hace unos años.

19 %

A nivel mundial, solo el 19 % de los responsables de la toma de decisiones de TI encuestados indicaron que ya tienen una infraestructura híbrida basada en la confianza cero específica para el trabajo.

PORCENTAJE DE LA PLANTILLA QUE SE ESPERA QUE TRABAJE A TIEMPO COMPLETO A DISTANCIA, A TIEMPO COMPLETO EN LA OFICINA O DE FORMA HÍBRIDA EN LOS PRÓXIMOS 12 MESES:



Dejando a un lado la intención, si su infraestructura informática y de seguridad está totalmente equipada para gestionar esta combinación en evolución es otra cuestión totalmente distinta. A nivel mundial, solo el 19 % de los responsables de la toma de decisiones de TI indicaron que ya tienen una infraestructura híbrida basada en la confianza cero específica para el trabajo, lo que pone de manifiesto que las organizaciones no están totalmente preparadas para gestionar este entorno de trabajo altamente distribuido a gran escala. Junto a los que ya han actualizado su infraestructura, otro 50 % está en proceso de implantarla o planea una estrategia híbrida basada en la confianza cero.

Entre los que implantan o planean implantar la confianza cero para proporcionar un acceso remoto seguro a proveedores, socios, contratistas u operadores de fábricas y equipos (es decir, los que por su naturaleza trabajan en un entorno híbrido), se ha identificado claramente que el acceso a la red de confianza cero es un área de inversión prioritaria para los próximos 12 meses. Esto sugiere que hay un gran interés para superar los desafíos inmediatos del cambio actual a un entorno de trabajo híbrido.

Pase el cursor por encima de los países para ver más detalles.

Aplicar una estrategia híbrida basada en la confianza cero es una prioridad para:

- 37 % India
- 36 % Singapur
- 33 % Japón
- 29 % Alemania
- 29 % Países Bajos

Mientras tanto, los siguientes países están todavía en fase de planificación:

- 34 % México
- 27 % Estados Unidos
- 27 % Francia
- 25 % Suecia

En general, el Reino Unido parece ser el país más reacio a adoptar estrategias híbridas basadas en la confianza cero, con un 21 % de organizaciones que afirman no tener planes actualmente para implantar una infraestructura híbrida y otro 20 % que prefiere seguir con sus tecnologías tradicionales de acceso remoto.

Naturalmente, la seguridad es una de las principales preocupaciones de las organizaciones, cada vez más híbridas.

PRINCIPALES PREOCUPACIONES EN MATERIA DE SEGURIDAD PARA LAS ORGANIZACIONES QUE CAMBIAN AL TRABAJO HÍBRIDO:

54 % Tanto los sistemas de tecnología operativa (OT) como el acceso a Internet.

53 % Aplicaciones privadas en las instalaciones o aplicaciones privadas y cargas de trabajo en la nube (en IaaS, PaaS)

32 % Internet de las cosas y acceso remoto a Internet

Pero es importante señalar que estos resultados demuestran que la seguridad en un entorno de trabajo híbrido no consiste solo en mantener alejadas las amenazas, sino también en cómo se puede proporcionar acceso seguro a la infraestructura a una amplia gama de usuarios, desde empleados a proveedores externos y socios comerciales.

Partiendo de esta base, a pesar del comprensible énfasis en la seguridad, las razones aducidas por quienes implantan o planifican una infraestructura de trabajo híbrida basada en la confianza cero también empiezan a aludir al impacto empresarial más amplio de las soluciones de confianza cero, con implicaciones para la experiencia y la productividad de los empleados.

MOTIVOS PARA IMPLEMENTAR O PLANIFICAR LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE TRABAJO HÍBRIDO BASADA EN LA CONFIANZA CERO

52 % Los empleados se enfrentan a experiencias de acceso desiguales para aplicaciones y datos locales y en la nube.

46 % Los empleados pierden productividad por problemas de acceso a la red.

39 % Los empleados no pueden acceder a aplicaciones y datos desde dispositivos personales.

Pase el cursor por encima de los países para ver más detalles.

Los países que informaron de una mayor cantidad de experiencias de acceso inconsistentes fueron:

- 70 % Japón
- 68 % India
- 64 % Estados Unidos
- 62 % Singapur

En Europa, solo alrededor de la mitad de las organizaciones que respondieron informaron que sufrían la misma inconsistencia:

- 52 % Suecia
- 49 % Países Bajos
- 47 % Francia
- 45 % Alemania

Las pérdidas de productividad debidas a problemas de acceso a la red figuraron como la razón principal para pasar a una nueva infraestructura en los siguientes países:

- 55 % México
- 48 % España
- 47 % Reino Unido

Aquellos encuestados cuyas organizaciones utilizan una infraestructura de trabajo híbrida tradicional basada en VPN indicaron que seguían enfrentándose a algunos problemas más fundamentales del trabajo remoto.

La experiencia del usuario es esencial para la productividad en los entornos de trabajo híbridos: esa es una de las principales conclusiones que sacamos del último año. Nuestros resultados indican que, hasta la fecha, las regiones han reaccionado con diferente rapidez a la hora de modernizar sus infraestructuras para hacer frente a los problemas de experiencia.

Para ofrecer experiencias de usuario óptimas en el entorno empresarial actual, cada vez más disperso, el tráfico de usuario debe dirigirse a la aplicación por la ruta más corta posible para evitar latencia y congestión.

Las organizaciones deben tener en cuenta la movilidad del empleado híbrido moderno, que debe ser dirigido dinámicamente a la aplicación requerida desde cualquier ubicación con un ancho de banda optimizado, tanto si trabaja desde casa como en la oficina o de viaje. Dejando a un lado la experiencia, si un empleado no está satisfecho con el rendimiento del acceso a sus aplicaciones críticas para la empresa, también podría buscar formas de evitar los controles de seguridad, lo que agravaría aún más el posible impacto negativo.

En comparación, aquellos encuestados cuyas organizaciones utilizan una infraestructura de trabajo híbrida tradicional basada en VPN indicaron que seguían enfrentándose a algunos problemas más fundamentales del trabajo remoto. Entre ellos figura la complejidad de administrar diferentes infraestructuras de seguridad para empleados locales y remotos (47 %), el rendimiento lento de las aplicaciones que los empleados experimentan (39 %) y la dificultad para TI para supervisar y solucionar los problemas de la experiencia de los usuarios remotos (37 %).

Aunque sigue habiendo mucha preocupación en materia de seguridad en torno al paso al trabajo híbrido, respuestas como estas reflejan el desafío mucho más amplio que las formas híbridas de trabajar plantean a las organizaciones, un reto que abarca el acceso, la experiencia y el rendimiento.

La confianza cero, cuando se entiende correctamente, ofrece una respuesta a estas cuestiones, proporcionando una simplicidad que permite a TI centrar su atención en responder a unas expectativas y requisitos empresariales en constante cambio.

PUNTO DE VISTA REGIONAL: LA VOZ DE APAC

Heng Mok, CISO, APJ

Asia Pacífico (APAC) es un gran ejemplo de cómo no se puede aplicar el mismo enfoque en todos los casos. Crisol de culturas y estilos de vida, todos y cada uno de los mercados de esta región tienen un enfoque diferente del trabajo. Incluso antes de la pandemia, ya veníamos observando diferencias significativas: mercados como Japón y Singapur seguían una estructura más jerárquica, mientras que Australia e India tenían un modelo de trabajo más relajado.

Dado que la región APAC comprende algunas de las ciudades con mayores niveles de reclusión de todo el mundo, estos matices son aún más pronunciados a medida que emergemos de los confinamientos. Entre los encuestados, la mayoría de los responsables de la toma de decisiones de TI de Japón y Singapur esperaban que su plantilla acudiera a la oficina a tiempo completo, un marcado contraste con los encuestados de Australia e India, que esperaban que su plantilla fuera totalmente remota.

Sin embargo, esperamos que a largo plazo sean aún más las organizaciones que apuesten por modelos de trabajo híbridos. Muchas organizaciones con las que he hablado optan por prácticas de trabajo híbridas para aprovechar los beneficios intangibles de atraer y retener talento. Con una mayor competencia para contratar el limitado número de trabajadores, no es sorprendente que muchos incorporen políticas similares y recurran a las pilas tecnológicas para respaldar esta transición de una forma mucho más fluida.

La experiencia del usuario es esencial para la productividad en los entornos de trabajo híbridos: esa es una de las principales conclusiones que sacamos del último año.

Sección IV

Adoptar un enfoque de confianza cero para integrar tecnologías emergentes

Por tecnologías emergentes se entienden tecnologías nuevas o en rápido desarrollo, cuyas aplicaciones prácticas aún no se han realizado en gran medida, pero que se espera tengan un impacto significativo en las empresas e impulsen ventajas competitivas.

Por supuesto, las soluciones digitales para permitir el trabajo a distancia no son las únicas tecnologías a las que las organizaciones están intentando recurrir. En la era digital actual, la tecnología operativa juega un papel cada vez mayor. Este segmento del modelo de negocio de una organización, que históricamente ha dependido mucho de sistemas y procesos heredados, verá un cambio transformador fundamental hacia nuevas tecnologías emergentes, cada una de las cuales aporta su propio conjunto de increíbles posibilidades para una mayor simplificación y automatización de los procesos empresariales.

Sin embargo, las organizaciones deben pensar aún más en el porvenir, y tener en cuenta también los próximos avances tecnológicos adicionales para tomar decisiones sobre una infraestructura a prueba de futuro. Los responsables de la toma de decisiones de TI deben asumir las diversas direcciones en las que la empresa puede dirigirse debido a las innovaciones, y tener una mentalidad abierta sobre cómo las tecnologías emergentes pueden respaldar sus funciones empresariales de manera efectiva. La confianza cero puede ser el vínculo que falta para ayudar a las empresas a que se empoderen y se preparen para las tecnologías futuras.

En consonancia con las motivaciones que subyacen a la migración a la nube y la transformación digital en general, nuestros resultados mostraron que centrarse en resultados estratégicos más amplios es algo que parece faltar en la planificación de proyectos tecnológicos emergentes.

Cuando se preguntó por el aspecto más difícil de implantar proyectos tecnológicos emergentes, el 30 % indicó que era garantizar la seguridad adecuada, seguido de los requisitos presupuestarios para una mayor digitalización (23 %). Sin embargo, solo el 19 % mencionó la dependencia de las decisiones empresariales estratégicas como un reto.

EL ASPECTO MÁS COMPLEJO DE LA IMPLANTACIÓN DE PROYECTOS TECNOLÓGICOS EMERGENTES, POR REGIÓN

Pase el cursor por encima de los países para ver más detalles.

Los problemas de seguridad plantearon el mayor desafío para los siguientes países:

- 54 % Brasil
- 41 % Japón
- 37 % India
- 37 % Italia
- 35 % España
- 31 % Estados Unidos

Mientras tanto, los siguientes países tienen dificultades predominantemente con los requisitos presupuestarios:

- 27 % Singapur
- 27 % Francia
- 23 % Reino Unido

La falta de visión parece ser el principal obstáculo que se interpone entre las organizaciones y las tecnologías emergentes en estos países:

- 24 % Países Bajos

El único país en el que la mayoría de las empresas identificaron la dependencia de decisiones empresariales estratégicas como el mayor obstáculo es el siguiente:

- 28 % Suecia

Aunque las preocupaciones presupuestarias son predecibles, centrarse en proteger la red a la vez que se ignora la alineación estratégica del negocio es una estrategia interesante. Las organizaciones se centran en la seguridad sin comprender plenamente el beneficio empresarial de la seguridad, una prueba más de que la confianza cero aún no se entiende como un elemento para facilitar las actividades empresariales.

A medida que se planifican casos de uso de tecnologías emergentes como la realidad aumentada, los gemelos digitales y la construcción virtual, el acceso a aplicaciones de baja latencia y alto rendimiento gana relevancia. Esto es especialmente cierto en América, donde el interés en las tecnologías emergentes durante los próximos tres años también es particularmente alto.

RELEVANCIA DEL ACCESO A APLICACIONES DE ALTO RENDIMIENTO Y BAJA LATENCIA EN LOS PRÓXIMOS TRES AÑOS

TECNOLOGÍAS PRIORITARIAS EN 2025	GLOBAL	EUROPA	AMÉRICA	APAC
Acceso basado en la nube a tecnología operativa y sistemas de control industrial	34 %	29 %	40 %	38 %
Implantación de la tecnología 5G para mejorar la conectividad	32 %	29 %	39 %	32 %
Reducir la huella de carbono de la empresa	29 %	28 %	28 %	30 %
Implementación de proyectos de inteligencia artificial/ aprendizaje automático	27 %	22 %	39 %	28 %

Pase el cursor por encima de los países para ver más detalles.

Organizaciones centradas en el acceso basado en la nube a OT y el control industrial:

- 46 % México
- 45 % India
- 44 % Singapur
- 36 % Australia
- 33 % Francia

Organizaciones que priorizan la implantación de tecnologías 5G:

- 47 % Brasil
- 45 % India
- 41 % Italia
- 36 % España
- 28 % Reino Unido

Las organizaciones que declaran que la reducción de la huella de carbono es la prioridad número 1:

- 41 % Italia
- 28 % Alemania
- 32 % Suecia

Solo las organizaciones de los Países Bajos consideran más importante la expansión de la informática perimetral (29 %), mientras que los Estados Unidos se centran abiertamente en la implantación de proyectos de IA y ML (43 %).

Ya podemos empezar a ver cómo estas tecnologías emergentes priorizadas podrían mejorar los resultados empresariales. Sin embargo, nuestros resultados aún sugieren que falta de una visión más amplia dentro de las organizaciones. Debe haber una alineación mucho más deliberada dentro de la empresa sobre las ventajas competitivas que se obtienen a través de las tecnologías emergentes y su implementación estratégica, que por supuesto incluye cómo se protegen.

PUNTO DE VISTA REGIONAL: LA VOZ DE EMEA

Nathan Howe, vicepresidente de Tecnología Emergente

Es menos probable que las organizaciones europeas sean las primeras en adaptarse a las tecnologías nuevas o emergentes. Aunque Europa ha sido la cuna de la revolución industrial con el desarrollo de sistemas mecánicos, la región fue superada hace tiempo en lo que respecta a la adopción de la tecnología digital. APJ se ha convertido en el centro de gravedad de la tecnología en torno a la fabricación de chips, y el conocimiento para innovar reúne a las personas de todo el mundo para desarrollar tecnologías transformadoras en Silicon Valley.

En este contexto, no es sorprendente que Asia ya haya reconocido el poder del 5G para ir más allá de la conexión inalámbrica a una siguiente forma de conectividad como base para la digitalización. Mientras que América se encuentra en un punto intermedio, Europa sigue sin saber cómo pasar a la tecnología 5G para fomentar la digitalización. No obstante, Europa está lista para crecer exponencialmente en la nube digital y las tecnologías emergentes debido a que el cambio de las tendencias geopolíticas, como la escasez de chips y los problemas de la cadena de suministro, requiere que los países establezcan centros de excelencia en la región.

SECCIÓN V

La ruta para hacer realidad todo el potencial de la confianza cero

A partir de estas conclusiones, ¿cómo deberían enfocar las organizaciones el paso a la confianza cero?

Los retos que han causado las arquitecturas de red y seguridad heredadas son omnipresentes y de larga duración, y exigen un replanteamiento del modo en que se concede la conectividad en el mundo moderno. En este punto es donde se debe aprovechar la arquitectura de confianza cero, una arquitectura en la que no se confía de forma predeterminada en ningún usuario o aplicación. La confianza cero se basa en un acceso con privilegios mínimos, lo que garantiza que la confianza solo se conceda una vez que se verifiquen la identidad y el contexto, y se apliquen las verificaciones de políticas correspondientes.

Este enfoque considera hostiles todas las comunicaciones de red. Las comunicaciones entre los usuarios y las cargas de trabajo o entre las propias cargas de trabajo se bloquean hasta que son validadas por las políticas basadas en la identidad. De este modo, se evita el acceso inadecuado y el movimiento lateral. Esta validación sirve en cualquier entorno de red, pues la ubicación en una red de una entidad ya no es un factor a tener en cuenta y no depende de una segmentación rígida de la red.

La confianza cero surgió como una nueva forma de proteger las redes. Con el tiempo, se expandió más allá de las redes locales, pero seguía centrándose principalmente en proteger el tráfico de aplicaciones privadas. Durante demasiado tiempo se ha considerado el tráfico en función de su relación con una red, en lugar de eliminar la red por completo. Hoy en día, las organizaciones deben conocer todo el potencial de la confianza cero para proteger las aplicaciones SaaS, el tráfico hacia y desde nubes públicas, e incluso a los usuarios cuando acceden a la Internet pública. El origen de ese tráfico pueden ser cargas de trabajo, así como usuarios. Se puede acceder independientemente del transporte, ya sea con tráfico que fluye a través de cualquier enrutador y que llega a través de cualquier red, por cable o inalámbrica, 4G, 5G o ampliaciones futuras.

Ya es hora de aplicar los principios de confianza cero a todo el tráfico, independientemente de su origen y su destino. Ha llegado el momento de dejar de pensar en qué entidad se está conectando a qué red y, en su lugar, utilizar la confianza cero para conectar a todas las entidades directamente utilizando políticas empresariales. En la era de la nube, Internet es la nueva red corporativa, y se deben poder establecer las conexiones entre las entidades correctas directamente mediante políticas empresariales.

¿Qué pasos pueden empezar a dar hoy las organizaciones para asegurarse de que pueden transformarse en las empresas seguras, ágiles, flexibles y eficientes que necesitan ser para hacer frente no solo a los entornos macroeconómicos actuales, sino también a los requisitos tecnológicos emergentes?

Hay tres recomendaciones clave:

1

Las organizaciones tienen que reconsiderar su forma de entender la confianza cero y considerarla un facilitador de la transformación digital segura y un impulsor de los resultados empresariales.

Con sus mayores niveles de visibilidad y control, una arquitectura basada en la confianza cero elimina la complejidad de la TI moderna y permite a las organizaciones centrarse en obtener los resultados que necesitan de su tecnología, desde un alto rendimiento y una experiencia de usuario mejorada hasta una reducción de costes.

2

Es necesaria una mayor formación para disipar el miedo, la incertidumbre y las dudas sobre el significado de la confianza cero y su impacto en las empresas.

El CIO y el CISO desempeñan un papel fundamental, ya que pueden proporcionar más información sobre la confianza cero en la sala de juntas y mostrar cómo se alinea con la estrategia empresarial.

3

La tecnología emergente debe considerarse una ventaja competitiva para las empresas. Las infraestructuras de confianza cero sientan hoy las bases del futuro.

La decisión sobre qué tecnologías emergentes implantar debe estar impulsada por la visión general del negocio y las necesidades actuales y futuras de la organización, no por las tendencias y la popularidad. La confianza cero tiene como objetivo dar apoyo a los requisitos de conectividad de seguridad y rendimiento de las tendencias emergentes.

Así pues, una vez que se ha cambiado la mentalidad para reconocer que la confianza cero es un verdadero facilitador empresarial, ¿cómo deben proceder las organizaciones para garantizar una arquitectura de confianza cero que logre con éxito estos resultados empresariales?

Zscaler ha implementado la confianza cero como componente arquitectónico central de Zero Trust Exchange e impregna cada elemento del marco SSE. Esto incluye un enfoque de confianza cero para los usuarios que acceden a cualquier aplicación (interna o externa), la conectividad IoT/OT y las cargas de trabajo que acceden a los recursos en un entorno multinube o en la propia Internet. Los principios de confianza cero habilitan el trabajo híbrido seguro desde cualquier lugar como estrategia empresarial, lo que permite a empleados, socios comerciales y clientes trabajar desde la ubicación más adecuada para su productividad, un requisito clave para la continuidad empresarial, la adquisición de talento a distancia y la oferta de los cada vez más populares entornos de trabajo híbridos.

Zscaler Zero Trust Exchange es un servicio nativo en la nube que proporciona a empleados, socios y clientes un acceso rápido, directo y seguro a aplicaciones externas e internas, independientemente de su ubicación, dispositivo o red.

También incorpora los siete elementos esenciales de la arquitectura de confianza cero, que se agrupan en las tres categorías siguientes:

Verificación

La arquitectura de confianza cero termina primero la conexión y establece lo siguiente:

1. ¿Quién se está conectando?
2. ¿Cuál es el contexto de acceso?
3. ¿Hacia dónde va la conexión?

Control

La arquitectura de confianza cero pretende entonces:

4. Evaluar el riesgo
5. Prevenir riesgos
6. Prevenir la pérdida de datos

Aplicación

Antes de establecer finalmente una conexión, la arquitectura de confianza cero:

7. Aplicar las políticas

Tener en cuenta estos elementos será la base para que las organizaciones que priorizan la nube aceleren la transformación digital y evolucionen hacia organizaciones preparadas para lo que les depare el futuro.

Acerca de Zscaler y Zscaler Zero Trust Exchange

Zscaler es reconocido universalmente como líder en confianza cero, con la plataforma de confianza cero más grande, fácil de usar y madura.

Puede confiar en Zscaler Zero Trust Exchange, nuestra plataforma nativa en la nube, para su paso a la confianza cero. A diferencia de los productos de redes y seguridad heredados, Zero Trust Exchange es una plataforma especialmente diseñada para la nube. Lo primero que hace para garantizar la seguridad es terminar cada conexión, lo que permite una inspección profunda del contenido y la verificación de los derechos de acceso en función de la identidad y el contexto.

Zero Trust Exchange se ejecuta en 150 centros de datos en todo el mundo, lo que garantiza que el servicio esté cerca de sus usuarios, junto con los proveedores de la nube y las aplicaciones a las que acceden, como Microsoft 365 y AWS. Asimismo, garantiza el camino más corto entre sus usuarios y sus destinos, proporcionando así una seguridad integral y una experiencia de usuario sorprendente.

Puede obtener más información sobre nuestra plataforma de fácil uso aquí.

Zero Trust Exchange opera en 150 centros de datos de todo el mundo

Metodología

ATOMIK Research encuestó a 1908 altos responsables de la toma de decisiones (CIO / CISO / CDO / director de arquitectura de red) en EMEA (Reino Unido, Alemania, Francia, Países Bajos, Suecia, Italia, España), AMÉRICA (EE. UU., México, Brasil) y APAC (Japón, India, Australia, Singapur). El estudio se llevó a cabo entre el 31 de mayo y el 28 de junio de 2022. La muestra comprende un 43 % de organizaciones de hasta 4999 empleados, un 32 % de empresas de entre 5000 y 9999 empleados y un 25 % de empresas de más de 10 000 empleados.