



El estado de la transformación a zero trust 2023

DE LA PREVENCIÓN A LA HABILITACIÓN:

*cómo aprovechar todo el potencial de zero trust para las
empresas con gran movilidad y centradas en la nube*



Contenido

03.

[Resumen ejecutivo](#)
05.

[Estado de zero trust: Algunos datos](#)
06.

[Sección I: El contexto de la nube detrás de zero trust](#)
13.

[Sección II: Asegurar argumentos a favor de zero trust](#)
Punto de vista regional: La voz de América
22.

[Sección III: La elección de zero trust para ofrecer opciones de trabajo híbrido](#)
Punto de vista regional: La voz de APAC
30.

[Sección IV: Adopción de un modelo zero trust para integrar las tecnologías emergentes](#)
Punto de vista regional: La voz de EMEA
35.

[Sección V: El camino para aprovechar todo el potencial de zero trust](#)
38.

[Acerca de Zscaler y Zscaler Zero Trust Exchange](#)
40.

[Metodología](#)



Resumen ejecutivo

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

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



Y los líderes de TI de todo el mundo se están dando cuenta de esto, a medida que zero trust se vuelve más popular, desbaratando décadas de principios de red y seguridad heredados.

Más del 90 % de los líderes de TI que han iniciado su migración a la nube ya han implementado, o están en proceso de implementar, una estrategia de seguridad zero trust el año que

viene. Esto es según los resultados de nuestra última encuesta global, que recopiló información de más de 1,900 CIO, CISO, CDO, CTO y jefes de infraestructura, de organizaciones que ya han comenzado a migrar aplicaciones y servicios a la nube.

Esto constituye un buen avance, y las razones que lo sustentan muestran un optimismo continuado respecto a la implementación de una arquitectura zero trust más allá de los próximos 12 meses.



22 %

Con solo un 22 % de confianza en que su organización está aprovechando todo el potencial de su infraestructura en la nube, los resultados indican que, para el futuro, es necesario pensar más allá de la seguridad.

De hecho, a medida que avanzan sus trayectorias hacia la nube, los argumentos de seguridad a favor de zero trust son 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 zero trust tiene claras ventajas sobre los firewalls y las VPN tradicionales cuando se trata de proteger el acceso remoto a las aplicaciones.

Sin embargo, con solo un 22 % de confianza en que su organización está aprovechando todo el potencial de su infraestructura en la nube, los resultados

indican que, para el futuro, es necesario pensar más allá de la seguridad. Cuando se considera desde un punto de vista holístico de TI, zero trust 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 costos tangibles.

A medida que las organizaciones luchan por ofrecer una nueva clase de lugar de trabajo moderno, de modelo híbrido y que

depende de toda una serie de tecnologías emergentes como IoT/OT, 5G e incluso el metaverso, deben ampliar la lente a través de la cual observan tanto zero trust como la transformación dig. Una plataforma zero trust tiene el poder de rediseñar los requisitos de las infraestructuras empresariales y organizativas, para convertirse en un verdadero motor empresarial que no solo permita a las empresas ofrecer el modelo de trabajo híbrido que exigen los empleados, sino convertirse en organizaciones 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 a zero trust en las organizaciones. Lo que descubrimos es prometedor: sólidas tasas de implementación. Pero los motivos de la implementación podrían ser más ambiciosos. Existe una oportunidad increíble para que los responsables de TI eduquen a los responsables de la toma de decisiones empresariales sobre el modelo zero trust y lo pongan sobre la mesa como un motor empresarial de alto valor: es el eslabón perdido que ayuda a las empresas a capacitarse y prepararse para las tecnologías del futuro, hoy mismo..



ESTADO DE ZERO TRUST

90 % Más del 90 % de las organizaciones que han iniciado su migración a la nube ya han implementado, o están en proceso de implementar, una estrategia de seguridad zero trust en los próximos doce meses.

88 % El 88 % de los líderes de TI de todo el mundo tiene cierto nivel de confianza en que su organización aprovecha el potencial de la infraestructura de la nube, pero solo el 22 % tiene plena confianza.

EN LA REGIÓN, LA PLENA CONFIANZA PARA APROVECHAR EL POTENCIAL DE LA INFRAESTRUCTURA DE LA NUBE SE SITÚA EN:



Nº 1 ZTNA es la prioridad n.º 1 para la inversión en tecnología zero trust 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 aceptan que la transformación segura a la nube es imposible con la infraestructura de seguridad de red heredada o que el acceso a la red zero trust (ZTNA) tiene claras ventajas sobre los firewalls y las VPN tradicionales cuando se trata de proteger el acceso remoto a las aplicaciones.

54 % de los líderes de TI indicó que creían que tanto las VPN como los firewalls perimetrales eran ineficaces para proteger contra ciberataques o proporcionar visibilidad de los ataques y el tráfico de aplicaciones.

PRINCIPALES OBSTÁCULOS PARA APROVECHAR TODO EL POTENCIAL DE LA NUBE:

- 45 %** Desafíos para proteger los datos en la nube y los problemas de privacidad de los datos
- 42 %** Complejidad de la red y hardware de seguridad difícil de escalar
- 40 %** Acceso remoto y de terceros a IoT y OT
- 33 %** Conectividad que no es uniforme y experiencia de acceso remoto deficiente para los usuarios

DEJANDO DE LADO LA SEGURIDAD, EL ACCESO Y LA COMPLEJIDAD, LOS IMPULSORES EMPRESARIALES ESTRATÉGICOS NO SE DESTACAN DENTRO DE LAS PRINCIPALES RAZONES PARA IMPLEMENTAR UNA ARQUITECTURA ZERO TRUST:

- 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 una conectividad segura para una fuerza de trabajo híbrida
- 24 %** Reducir el costo y la complejidad de la seguridad de red heredada



Sección I

El contexto de la nube detrás de la adopción de zero trust

Cuando en esta encuesta nos referimos a la "nube", estamos hablando de aplicaciones, datos y cargas de trabajo que se proporcionan como servicios alojados a través de Internet, en lugar de 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 adentrarnos en los pormenores de zero trust, quisimos establecer el contexto de su adopción, examinar lo que está ocurriendo en el panorama general de la TI sobre este tema y, concretamente, en qué punto se encuentran las organizaciones en su proceso hacia la nube.

No hay duda de que los eventos de los últimos años han acelerado el traslado

a la nube. En muchas organizaciones, el proceso ya está en marcha, si es que ya no ha terminado.

Entrevistamos a más de 1,900 CIO, CISO, CDO, CTO y jefes de infraestructura, de organizaciones de todo el mundo que ya han comenzado a migrar aplicaciones y servicios a la nube. De ellos, casi la mitad (46 %) afirmó que el proceso de migración

se había completado al 100 %.

Pero mientras que el 88 % de los líderes de TI tienen cierto nivel de confianza en que están haciendo el mejor uso de su proceso hacia la nube, solo el 22 % está completamente seguro de que su organización está aprovechando todo el potencial de la infraestructura de la nube actual.

ENCUESTADOS QUE TIENEN MUCHA CONFIANZA EN QUE SU ORGANIZACIÓN ESTÁ APROVECHANDO TODO EL POTENCIAL DE LA INFRAESTRUCTURA DE LA NUBE ACTUAL

22 % Total

14 % Europa

42 % América

24 % APAC



% DE ENCUESTADOS TIENEN MUCHA CONFIANZA EN QUE SU ORGANIZACIÓN ESTÁ APROVECHANDO TODO EL POTENCIAL DE LA INFRAESTRUCTURA DE LA NUBE ACTUAL

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

Europa:

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

América:

- 41 % EE. UU.
- 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 la nube, y solo un 14 % expresa plena confianza. Sin embargo, en América, esta cifra se eleva al 42 %.

Aunque no existe una causa única y clara de esta disparidad, las diferencias interculturales en la velocidad de adopción de tecnologías innovadoras, puede ser una posible razón, ya que Europa adopta tradicionalmente un modelo más cauteloso y presta más atención a la privacidad de los datos. Además, con la infraestructura de conectividad bien establecida de Europa y el sólido modelo en la fabricación, el estímulo para adoptar innovaciones como 5G inmediatamente es menor, y cambiar los procesos empresariales ya establecidos lleva más tiempo. Como analizaremos más a fondo en otra sección, las organizaciones en 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 para que la infraestructura de nube sea compatible con casos de uso más sofisticados.

Pero, en términos más generales, ¿por qué las organizaciones tenían dificultades para aprovechar todo el potencial de la nube?

En la superficie, la seguridad aparece como el obstáculo principal, y los líderes de TI seleccionan dos motivos relacionados con la seguridad como principales respuestas a esta pregunta:

PRINCIPALES OBSTÁCULOS PARA APROVECHAR TODO EL POTENCIAL DE LA NUBE

- 45 %** Problemas y desafíos de privacidad de datos para proteger los datos en la nube
- 42 %** La red es muy compleja para adaptar y la seguridad de red resulta difícil de escalar
- 40 %** Desafíos para permitir el acceso remoto y de terceros a los sistemas IoT y OT
- 33 %** Conectividad que no es uniforme y experiencia de acceso remoto deficiente para los usuarios



LOS PRINCIPALES OBSTÁCULOS PARA APROVECHAR TODO EL POTENCIAL DE LA NUBE, POR PAÍS



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

En toda Europa y APAC, las preocupaciones por la privacidad son más marcadas en:

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

En América, las organizaciones están luchando con los desafíos que presenta la protección de datos en la nube:

- 44 % Brasil
- 30 % EE. UU.

Mientras tanto, Singapur y Japón, en particular, tienen dificultades para escalar el hardware de seguridad de red:

- 41 % Singapur
- 30 % Japón



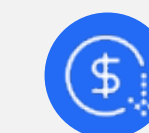


En un entorno basado en la nube, la superficie de ataque aumenta exponencialmente, ya que cada servicio, usuario y dispositivo conectado a Internet se convierte en un posible punto de entrada, una puerta de entrada vulnerable que debe protegerse contra las amenazas.

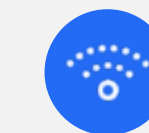
Y las preocupaciones de las organizaciones están bien justificadas. En un entorno basado en la nube, la superficie de ataque aumenta exponencialmente, ya que cada servicio, usuario y dispositivo conectado a Internet se convierte en un posible punto de entrada, una puerta de entrada vulnerable que debe protegerse contra las amenazas. En la próxima sección hablaremos más sobre este tema.

Pero un vistazo a las motivaciones generales detrás de las migraciones a la nube apunta a un obstáculo mucho más básico en la manera en que los responsables de TI consideran la nube, y que sin duda afecta su uso efectivo. Cuando se les preguntó por los factores principales que impulsan los proyectos de transformación digital en sus organizaciones, se destacaron tres: reducir los costos, facilitar la innovación tecnológica y controlar los riesgos cibernéticos.

FACTORES PRINCIPALES QUE IMPULSAN LOS PROYECTOS DE TRANSFORMACIÓN DIGITAL SEGÚN LOS LÍDERES MUNDIALES DE TI:



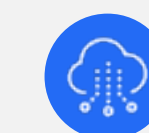
Reducir los costos de **infraestructura de TI**



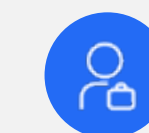
Facilitar innovaciones tales como **5G y Edge Computing**



Mitigar los riesgos **cibernéticos de seguridad**



Administrar los **entornos multinube**



Mejorar la capacidad de atraer y retener a los **mejores talentos**



FACTORES PRINCIPALES QUE IMPULSAN LOS PROYECTOS DE TRANSFORMACIÓN DIGITAL POR PAÍS



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

Brasil coincidió con el consenso mundial, y la mayoría de las organizaciones citaron la reducción de los costos de infraestructura de TI como el motor principal.

Sin embargo, en algunos países europeos se daba otra situación. En **Francia**, las organizaciones estaban más preocupadas por permitir el trabajo híbrido, mientras que la prioridad principal en **Suecia** era la experiencia del usuario.

Facilitar innovaciones como 5G y Edge Computing fue más importante en los países más vanguardistas, como **Japón**, **México** y **Singapur**. En Singapur se dio una importancia similar al crecimiento de los ingresos.

La optimización de los procesos empresariales también estuvo entre los 3 principales en **Brasil** y **España**.



Todo muy práctico, y todo impulsado por TI. De hecho, la gran importancia de reducir los costos, aunque sea entendible en el momento actual, indica que todavía puede existir una clara falta de comprensión

de las principales ventajas de la nube. Y esto, a su vez, podría estar afectando el modelo y el uso de las tecnologías que se están utilizando para apoyarla. **zero trust a escena.**

**No hay duda de que
los eventos de los últimos
años han acelerado el
traslado a la nube.**



Sección II

Asegurar argumentos a favor de zero trust

Zero trust es un modelo holístico para proteger a las organizaciones modernas. Se basa en el acceso con privilegios mínimos y el principio de que no se debe confiar inherentemente en ningún usuario ni aplicación. Comienza con la suposición de que todo es hostil, y solo establece confianza según la identidad del usuario y el contexto, utilizando políticas como un guardián en cada paso del proceso. En los Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) define el principio subyacente de una arquitectura zero trust como "no se concede confianza implícita alguna a los activos o cuentas de usuarios únicamente sobre la base de su ubicación física o de red (es decir, redes de área local vs. Internet) o sobre la base de la propiedad de activos (empresariales o personales). Es una revisión del antiguo proverbio, "Nunca confíe. Siempre verifique".

Teniendo en cuenta que la seguridad, el acceso y la complejidad son las principales preocupaciones de los responsables de TI en relación con la nube, no es de extrañar que cada vez más organizaciones se interesen por zero trust como medio para superar estos obstáculos. Las respuestas mostraron que

las organizaciones están desarrollando una buena base de comprensión de las ventajas de la seguridad que otorga zero trust en comparación con los modelos 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 indicó que creían que tanto las VPN como los firewalls perimetrales son ineficaces para proteger contra ciberataques o proporcionar visibilidad de los ataques y el tráfico de aplicaciones. Otro 68 % reconoció que, cuando se trata de asegurar el acceso

remoto a las aplicaciones, el acceso a la red zero trust (ZTNA) tiene claras ventajas sobre los firewalls y las VPN tradicionales, o que la transformación segura a la nube no se puede lograr con una infraestructura de seguridad de red heredada.



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

Encuestados que están de acuerdo con que la transformación segura de la nube es imposible con la infraestructura de seguridad de red heredada, y que el acceso a la red zero trust tiene claras ventajas sobre los firewalls y VPN tradicionales cuando se trata de proteger el acceso remoto a las aplicaciones:

- 85 % India
- 81 % EE. UU.
- 75 % Brasil
- 75 % Singapur
- 73 % Suecia

Encuestados que concuerdan en que tanto las VPN como los firewalls perimetrales son ineficaces para proteger contra ciberataques o proporcionar visibilidad de los ataques y el tráfico de aplicaciones:

- 72 % India
- 65 % Singapur
- 64 % Japón
- 57 % Alemania
- 56 % EE. UU.

Encuestados que concuerdan 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 % EE. UU.
- 56 % Singapur
- 51 % España
- 50 % Japón





90 %

Más del 90 % de los encuestados que han iniciado su migración a la nube ya han implementado, o están en proceso de implementar, una estrategia de seguridad zero trust en los próximos doce meses.



Más allá de este conocimiento, lo que demuestra ser más prometedor es que actúan en consecuencia. Más del 90 % de los encuestados que han iniciado su migración a la nube ya han implementado, o están en proceso de implementar, una estrategia de seguridad zero trust en los próximos doce meses.

Italia y la India lideran el camino a la hora de implementar una estrategia de seguridad zero trust, con el 97 % de las organizaciones italianas y el 96 % de las organizaciones de la India que confirman que ya la tienen implementada o están en vías de hacerlo.



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

Porcentaje de organizaciones que ya disponen de seguridad zero trust, que la están implementando o que están en etapa de planificación estratégica para implementarla:

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





Zero trust se sigue considerando predominantemente como una solución (de seguridad) aislada y centrada en la TI ... pero zero trust podría ofrecer muchísimo más a las organizaciones.

Pero, lamentablemente, disponer de un sistema de seguridad zero trust, o tener planes para implementarlo, no indica en absoluto que se esté aprovechando todo su potencial como activo clave de la empresa.

De hecho, los resultados indican que zero trust se sigue considerando predominantemente como una solución (de seguridad) aislada y centrada en la TI, lo que significa que se resuelven los desafíos inmediatos en materia de seguridad y se obtienen ventajas tácticas, pero zero trust podría ofrecer muchísimo más a las organizaciones.

PRINCIPALES MOTIVOS PARA IMPLEMENTAR UNA ARQUITECTURA ZERO TRUST PARA UNA FUERZA DE TRABAJO HÍBRIDA

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 una conectividad segura para una fuerza de trabajo híbrida

24 % Reducir el costo y la complejidad de la seguridad de red heredada



PRINCIPALES RAZONES PARA IMPLEMENTAR UNA INFRAESTRUCTURA ZERO TRUST EN TODO EL MUNDO:

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

Para mejorar la detección de amenazas avanzadas:

- 52 % India
- 42 % Singapur
- 41 % EE. UU.
- 39 % Italia
- 35 % España
- 30 % Francia
- 26 % Reino Unido

Para mejorar la detección de ataques a aplicaciones web:

- 44 % Brasil
- 35 % México

Para ampliar la seguridad y proteger los datos confidenciales:

- 44 % Brasil

Para proporcionar acceso remoto seguro a proveedores, socios y contratistas:

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





Este modelo que lleva a zero trust, utilizarlo solo para la seguridad al principio de un proceso de transformación, limita significativamente su potencial, en un momento en el cual hay mucho que depende de la capacidad que tengan una organización de digitalizarse e innovar, rápidamente y a escala. Cuando se entiende correctamente y no se ve como una mera tecnología o producto, le permite a las empresas simplificar su infraestructura, replantearse su manera de hacer negocios y transformarse en una empresa totalmente digitalizada. Por ejemplo, las empresas que han implementado zero trust tendrían 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 los procesos, reducir los costos, eliminar el hardware heredado y mejorar la eficiencia. Pero para lograr estos beneficios estratégicos, el mensaje en torno a zero trust debe poder traspasar el directorio y convertirse en parte de la estrategia empresarial más amplia. Está claro que hoy sigue habiendo incertidumbre y probablemente un déficit de competencias en cuanto a lo que significa zero trust y su impacto en la empresa. La tarea urgente que tenemos delante es ayudar a los líderes empresariales, incluidos los

CIO, a comprender que el objetivo de zero trust es introducir simplicidad en la infraestructura general, eliminando el hardware que requiere un alto nivel de administración para que pueda ofrecer más fácilmente los resultados empresariales exactos que necesita una organización, todo ello manteniendo una seguridad de máximo nivel. Si observamos las tecnologías zero trust en las cuales las organizaciones están priorizando invertir en los próximos doce meses, algunas pruebas indican que esta comprensión de las ventajas empresariales está evolucionando, pero a un ritmo notablemente diferente en las distintas regiones del mundo y con un amplio margen de mejora.

PRINCIPALES TECNOLOGÍAS
ZERO TRUST EN LAS
QUE INVIERTEN LAS
ORGANIZACIONES

30 %

zero trust Network Access (ZTNA)

29 %

Cloud Firewall

27 %

Prevención de la pérdida de datos (DLP)



PUNTO DE VISTA REGIONAL: LA VOZ DE AMÉRICA

Amit Chaudhry, director sénior de Marketing de Producto



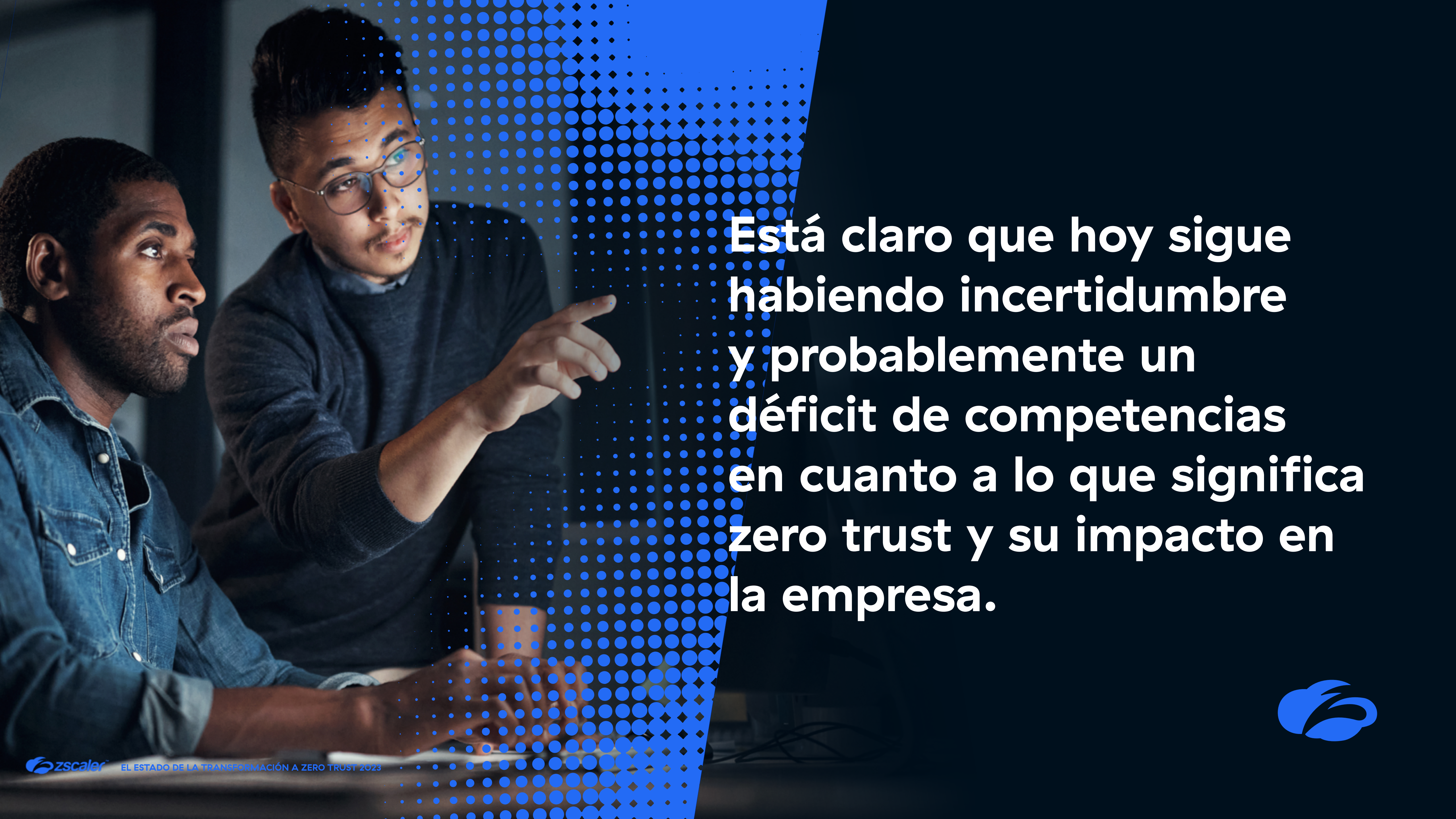
Las organizaciones de hoy están adoptando las tecnologías de nube, movilidad, IA, IoT y OT para que las empresas sean más ágiles y competitivas. Los usuarios están en todas partes, y sus datos también. Pero naturalmente, para una colaboración rápida y productiva, quieren tener acceso directo a las aplicaciones desde cualquier sitio y en cualquier momento.

Este ritmo explosivo de transformación digital ha brindado a los delincuentes

oportunidades para aprovecharse de las arquitecturas de red y seguridad con décadas de antigüedad. La cantidad de ataques se ha vuelto incomparable, especialmente los ataques de ransomware y a la cadena de suministro. Y dado que estos se vuelven más sofisticados, la seguridad perimetral de las VPN y los firewalls no puede proteger la red ni ofrecer una buena experiencia de usuario.

Para materializar la visión de un lugar de trabajo híbrido seguro, las organizaciones

se están trasladando rápidamente de los firewalls y las VPN hacia la arquitectura zero trust, lo que asegura un acceso rápido y directo a las aplicaciones desde cualquier sitio y en cualquier momento. Diseñada sobre el principio del acceso con privilegios mínimos, en el que la conexión se realiza en función de la identidad y el contexto, zero trust podría ser el modelo más sencillo y a la vez la más importante en relación con la manera de proteger los datos.

A photograph of two men in an office environment. The man on the left, who is Black, is wearing a blue denim shirt and looking towards the right. The man on the right, who is Asian, is wearing glasses and a dark sweater, pointing his right index finger towards a screen that is out of frame. The background is dark and out of focus. A large blue graphic with a white dot pattern is overlaid on the right side of the image, containing the text.

**Está claro que hoy sigue
habiendo incertidumbre
y probablemente un
déficit de competencias
en cuanto a lo que significa
zero trust y su impacto en
la empresa.**





Sección III

La elección de zero trust para ofrecer opciones de trabajo híbrido

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

Cuando los primeros confinamientos hicieron que las organizaciones se desesperaran para establecer el trabajo desde casa para sus empleados, poco podíamos imaginar que esta "medida temporal" abriría la puerta a una manera de trabajar totalmente nueva y que, de hecho, el trabajo en sí ya no volvería a ser lo mismo que antes.

En cambio, la fuerza de trabajo de hoy en día tiene opciones: trabajar desde

casa, la oficina o cualquier otra ubicación, y tiene (debería tener) la tecnología para hacerlo posible.

Los encuestados prevén que, en los próximos 12 meses, sus fuerzas de trabajo seguirán adoptando plenamente las distintas opciones a su disposición y que están 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.

Mientras que casi dos tercios (62 %) de los líderes de TI afirman que sus organizaciones adoptan el mundo híbrido u ofrecen a su personal la plena flexibilidad para trabajar a distancia, el hecho de que más de un tercio (38 %) estima que volverán a la oficina a tiempo completo es sorprendente y hasta preocupante. Aunque esto puede ser entendible para determinados sectores

que dependen de las interacciones en persona (como el sector sanitario y la hotelería), en condiciones de mercado favorables, también podría dificultar la atracción y retención de talento para muchas organizaciones si no pueden ofrecer el entorno de trabajo flexible que los empleados se han acostumbrado a tener durante los últimos años.



19 %

Solo el 19 % de los responsables de la toma de decisiones en TI encuestados globalmente indicaron que ya disponen de una infraestructura basada en zero trust específica para el trabajo híbrido.

PORCENTAJE DE LA FUERZA DE TRABAJO QUE SE ESPERA QUE TRABAJE A TIEMPO COMPLETO A DISTANCIA, EN LA OFICINA O DE MANERA HÍBRIDA EN LOS PRÓXIMOS 12 MESES.

38 % Personal de oficina a tiempo completo

35 % Totalmente a distancia

27 % Híbrido

Dejando de lado la intención, el hecho de que su infraestructura de TI y seguridad esté o no totalmente equipada para implementar esta combinación que se viene dando, es una cuestión totalmente distinta. Solo el 19 % de los responsables de la toma de decisiones en TI encuestados globalmente indicaron que ya disponen de una infraestructura basada en zero trust específica para el trabajo híbrido, lo que pone de

manifiesto que las organizaciones no están totalmente preparadas para manejar este entorno de trabajo altamente distribuido a gran escala. Junto a los que ya han actualizado su infraestructura, otro 50 % está en proceso de implementar o está planificando una estrategia híbrida basada en zero trust.

Y entre aquellos que implementan o están planificando implementar zero trust para proporcionar acceso remoto seguro a proveedores,

socios, contratistas u operadores de fábrica y equipos, es decir, aquellos que por su naturaleza trabajan en un entorno híbrido, hay una indicación clara de que el acceso a la red zero trust es un área de inversión principal para los próximos 12 meses. Esto sugiere que existe una gran necesidad de resolver los problemas inmediatos que plantea el cambio en curso a un entorno de trabajo híbrido.



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

La aplicación de una estrategia basada en zero trust es una prioridad en:

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

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

- 34 % México
- 27 % EE. UU.
- 27 % Francia
- 25 % Suecia

En general, el Reino Unido parece ser el más reacio a adoptar estrategias híbridas basadas en zero trust, con el 21 % de las organizaciones que dicen que actualmente no tienen planes de implementar una infraestructura híbrida y un 20 % que prefiere seguir con sus tecnologías de acceso remoto tradicionales.





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 ESTÁN CAMBIANDO AL TRABAJO HÍBRIDO:

- 54 %** tanto sistemas de tecnología operativa (OT) como 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 los objetos y acceso remoto a Internet

Pero es importante tener en cuenta que estos resultados muestran que la seguridad en un entorno de trabajo híbrido no solo se trata de mantener alejadas a las amenazas, sino también de cómo puede proporcionar acceso a la infraestructura de manera segura a una gran variedad de usuarios, desde empleados a proveedores externos y socios comerciales.

Partiendo de esta base, a pesar de la comprensible importancia que tiene la seguridad, las razones aducidas por quienes implementan o planifican una infraestructura de trabajo híbrido basada en zero trust también empiezan a aludir al impacto empresarial más amplio de las soluciones zero trust, ya que tiene consecuencias también para la experiencia y la productividad de los empleados.

RAZONES PARA IMPLEMENTAR O PLANIFICAR LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE TRABAJO HÍBRIDA BASADA EN ZERO TRUST

- 52 %** Los empleados tienen experiencias de acceso a aplicaciones y datos en las instalaciones y en la nube que no son uniformes.
- 46 %** Los empleados experimentan pérdidas de productividad debido a 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 en más detalle.

Países que mencionan más casos de experiencia de acceso que no es uniforme:

- 70 % Japón
- 68 % India
- 64 % EE. UU.
- 62 % Singapur

En Europa, solo alrededor de la mitad de las organizaciones encuestadas declararon sufrir la misma falta de uniformidad, con:

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

Se mencionaron pérdidas de productividad por problemas de acceso a la red como el motivo predominante para pasar a una nueva infraestructura en:

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





Aquellos encuestados cuyas organizaciones utilizan una infraestructura de trabajo híbrida tradicional basada en VPN declararon que seguían lidiando con algunos problemas fundamentales en el trabajo a distancia.

La experiencia del usuario es vital para la productividad en los entornos de trabajo híbridos: esa es una de las principales conclusiones del año pasado. Y nuestros resultados indican que las regiones han reaccionado a diferentes velocidades en lo que hace a la modernización de su infraestructura para abordar los problemas de experiencia hasta la fecha.

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

y la congestión. Las organizaciones deben tener en cuenta la movilidad del empleado híbrido moderno, que debe dirigirse dinámicamente hacia la aplicación requerida desde cualquier lugar con un ancho de banda optimizado, ya sea que trabaje desde casa, en la oficina o en la carretera. Además, si un empleado no está satisfecho con la forma en la que tiene acceso a sus aplicaciones comerciales críticas, también podría buscar maneras de evitar los controles de seguridad, lo que aumentaría aún más la posibilidad de un impacto negativo.

En comparación, aquellos encuestados cuyas organizaciones utilizan una infraestructura de trabajo híbrida tradicional basada en VPN declararon que seguían lidiando con algunos problemas fundamentales en el trabajo a distancia. Entre ellos se incluyen la complejidad de administrar diferentes infraestructuras de seguridad para los empleados que trabajan en las instalaciones y los empleados remotos (47 %), los empleados que experimentan un rendimiento lento de las aplicaciones (39 %) y la dificultad de TI para supervisar y resolver los problemas de experiencia de los usuarios remotos (37 %).

Si bien todavía quedan muchas preocupaciones de seguridad relacionadas con el cambio al trabajo híbrido, las respuestas como estas reflejan un problema mucho más amplio que el que las distintas opciones de trabajo híbrido presentan a las organizaciones, un problema que incluye el acceso, la experiencia y el rendimiento. Cuando se comprende correctamente, zero trust proporciona una respuesta a todos ellos, lo que ofrece una simplicidad que permite a los departamentos de TI centrar su atención en responder a las expectativas y requisitos empresariales que cambian constantemente.



PUNTO DE VISTA REGIONAL: LA VOZ DE APAC

Heng Mok, CISO, APJ



La región Asia-Pacífico (APAC) es un gran ejemplo de que "una misma solución no sirve para todos". Esta región es un crisol de culturas y estilos de vida en el que todos y cada uno de los mercados tiene una forma distinta de trabajar. Incluso antes de la pandemia, hemos observado diferencias significativas, con mercados como Japón y Singapur con una estructura más jerárquica, mientras que Australia e India tenían un modelo de trabajo más relajado.

Dado que la región APAC incluye algunas de las ciudades que tuvieron los confinamientos más estrictos del mundo, estos matices son aún más pronunciados ahora que dejamos los confinamientos atrás. Entre los encuestados, la mayoría de los responsables de la toma de decisiones de TI de Japón y Singapur esperaba que su fuerza de trabajo volviera a la oficina a tiempo completo, lo cual constituye una marcada diferencia con respecto a los encuestados en Australia e India, que esperaban la modalidad de trabajo a distancia.

Sin embargo, esperamos ver que aún más organizaciones redoblen su apuesta a largo plazo a los modelos de trabajo híbrido. Muchas organizaciones con las que he hablado prefieren la modalidad de trabajo híbrido para aprovechar los beneficios intangibles de atraer y retener talento. Dada la mayor competencia para atraer a un grupo limitado de talento, no es una sorpresa que muchos adopten políticas similares y analicen un conjunto de tecnologías para respaldar esta transición con muchísimos menos problemas.



La experiencia del usuario es vital para la productividad en los entornos de trabajo híbridos: esa es una de las principales conclusiones del año pasado.



Sección IV

Adopción de un modelo zero trust para integrar las tecnologías emergentes

Las tecnologías emergentes se refieren a tecnologías nuevas o en rápido desarrollo, con aplicaciones prácticas que, en gran parte, aún no se han materializado, pero se espera que tengan un impacto significativo en las empresas e impulsen la ventaja competitiva.

Por supuesto, las soluciones digitales para permitir el trabajo a distancia no son las únicas tecnologías que las organizaciones están intentando adoptar. En la era digital actual, la tecnología operativa desempeña un papel cada vez más importante. Este segmento del modelo empresarial de una organización, que históricamente ha dependido mucho de sistemas y procesos heredados, experimentará un cambio transformador fundamental hacia tecnologías nuevas y emergentes, cada una con su propio conjunto

atractivo de posibilidades para lograr más simplificación y automatización en los procesos empresariales.

Pero las organizaciones deben pensar aún más allá, teniendo en cuenta también los próximos avances tecnológicos adicionales para tomar decisiones de infraestructura preparadas para el futuro. Los responsables de la toma de decisiones de TI deben responsabilizarse de las distintas direcciones hacia las que puede dirigirse la empresa, basándose en las innovaciones,

y tener una mentalidad abierta sobre cómo las tecnologías emergentes pueden apoyar sus funciones empresariales de manera eficaz. Zero trust puede ser el eslabón perdido, y ayudar a las empresas a adquirir la capacidad y prepararse para las tecnologías futuras hoy mismo.

Paralelamente a las motivaciones que respaldan la migración a la nube y la transformación digital en general, nuestros resultados mostraron que la falta de atención a los resultados estratégicos

más amplios está presente el modo en que las organizaciones planifican los proyectos tecnológicos emergentes.

Cuando se preguntó sobre el único aspecto más problemático de la implementación de proyectos tecnológicos emergentes, el 30 % mencionó una seguridad adecuada, seguida de los requisitos presupuestarios para una mayor digitalización (23 %). Sin embargo, solo el 19 % citó la dependencia de las decisiones empresariales estratégicas como un problema.



EL ASPECTO MÁS PROBLEMÁTICO DE LA IMPLEMENTACIÓN DE PROYECTOS TECNOLÓGICOS EMERGENTES, POR REGIÓN

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

Los siguientes países plantearon que el mayor problema son las preocupaciones por la seguridad:

- 54 % Brasil
- 41 % Japón
- 37 % India
- 37 % Italia
- 35 % España
- 31 % EE. UU.

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

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

La falta de visión parece ser el obstáculo principal entre las organizaciones y las tecnologías emergentes.

- 24 % Países Bajos

El único país donde la mayoría de las empresas señalaron la dependencia de las decisiones empresariales estratégicas como el mayor obstáculo.

- 28 % Suecia





Aunque las preocupaciones presupuestarias son predecibles, es interesante la atención que se presta a la protección de la red mientras que se ignora la alineación empresarial estratégica. Las organizaciones le prestan más atención a la seguridad sin comprender plenamente la ventaja empresarial de la seguridad, una prueba más de que zero trust todavía no se considera un activo clave de la empresa.

Mientras que 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 también se convierte en una preocupación. Esto es especialmente cierto en América, donde el interés por las tecnologías emergentes en los próximos tres años es también especialmente alto.

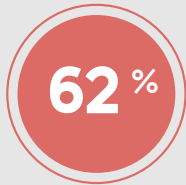
RELEVANCIA DEL ACCESO A APLICACIONES DE BAJA LATENCIA Y ALTO RENDIMIENTO EN LOS PRÓXIMOS TRES AÑOS



Europa



América



APAC

TECNOLOGÍAS DE MAYOR PRIORIDAD PARA 2025	GLOBAL	EUROPA	AMÉRICA	APAC
Acceso basado en la nube a tecnología operativa y sistemas de control industrial	34 %	29 %	40 %	38 %
Implementación de la tecnología 5G para mejorar la conectividad	32 %	29 %	39 %	32 %
Reducción de 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 en más detalle.

Organizaciones que se centran en el acceso basado en la nube a OT y control industrial:

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

Organizaciones que priorizan la implementación de tecnologías 5G:

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

Organizaciones que declaran que la reducción de la huella de carbono es la prioridad n.º 1:

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

Solo las organizaciones de los Países Bajos consideran que la expansión de la computación perimetral es lo más importante (29 %), mientras que los EE. UU. se centran más específicamente en implementar proyectos de inteligencia artificial y aprendizaje automático (43 %).





Ya podemos empezar a ver cómo otorgarle prioridad a estas tecnologías emergentes podría ser el camino para obtener resultados empresariales más amplios. Sin embargo, nuestros resultados aún sugieren que falta una visión más amplia en las organizaciones. Debe existir un consenso mucho más consciente en la empresa acerca de las ventajas competitivas que se obtienen gracias al empleo 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 haya sido la cuna de la revolución industrial con los inventos mecánicos, la región ha sido superada hace tiempo en lo que se refiere a la adopción de la tecnología digital. La región de Asia-Pacífico se ha convertido en el centro de la tecnología en torno a la fabricación de chips y el conocimiento para innovar reúne a personas de todo el mundo para desarrollar tecnologías transformadoras en Silicon Valley.

En este contexto, no sorprende que Asia ya haya reconocido el poder de 5G para ir más allá de la conexión inalámbrica hacia el próximo tipo de conectividad como base para la digitalización. Mientras que América se encuentra en un punto intermedio, Europa sigue sin saber cómo pasar a 5G para sus esfuerzos de digitalización. Sin embargo, Europa está lista para crecer significativamente en la nube digital y las tecnologías emergentes, ya que el cambio en las tendencias geopolíticas, tales como la escasez de chips y los problemas de la cadena de suministro, requiere que los países establezcan centros de excelencia locales en la región.



Sección V

El camino para aprovechar todo el potencial de zero trust

En base a estos hallazgos, ¿cómo deben las organizaciones dirigir sus trayectorias hacia zero trust?

Los problemas causados por las arquitecturas heredadas de red y seguridad son generalizados, de larga duración y requieren un replanteamiento de cómo se autoriza la conectividad en el mundo moderno. Aquí es donde debe aprovecharse la arquitectura zero trust, una arquitectura en la que no se confía en ningún usuario o aplicación de manera predeterminada. Zero trust se basa en el acceso con privilegios mínimos, que asegura que solo se confía luego de verificarse la identidad y el contexto y de hacer cumplir las políticas.

Este modelo trata todas las comunicaciones de red como hostiles; las comunicaciones entre usuarios y cargas de trabajo, o entre las propias cargas de trabajo, se bloquean hasta ser validadas por políticas basadas en la identidad. Esto impide efectivamente el acceso inapropiado y el movimiento lateral. Esta validación se expande a cualquier entorno de red, donde la ubicación de la red de una entidad ya no es un factor y no depende de una segmentación de red rígida.

Zero trust comenzó como una nueva manera 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 consideró el tráfico en función de su relación con una red, en lugar de eliminar la red por completo. Hoy, las organizaciones deben conocer todo el potencial de zero trust para proteger las aplicaciones SaaS, el tráfico hacia y desde las nubes públicas e incluso, a los usuarios cuando tienen acceso a la red de Internet pública. Y los originadores de ese tráfico pueden ser tanto cargas de trabajo como usuarios. Se puede tener acceso independientemente del transporte, con tráfico que fluye a través de cualquier enrutador y que llega a través de cualquier red, cableada o inalámbrica, 4G o 5G, y las extensiones que surjan en el futuro.

Ya es hora de aplicar los principios de zero trust a todo el tráfico, independientemente del origen y del destino. Ahora es el momento de dejar de pensar en qué entidad se está conectando a qué red y, en su lugar, utilizar zero trust para conectar las entidades correctas entre sí utilizando políticas empresariales. En la era de la nube, Internet es la nueva red corporativa y todo el tráfico es válido para conectarse a la entidad correcta utilizando políticas empresariales.



¿Qué medidas pueden tomar hoy las organizaciones para asegurarse de que podrán transformarse en las empresas seguras, ágiles, flexibles y eficientes que necesitan ser para lidiar tanto con los entornos macroeconómicos actuales como con los requisitos tecnológicos emergentes?

Existen tres recomendaciones clave:

1

Las organizaciones deben reconsiderar lo que entienden por zero trust y darse cuenta de que este modelo es un activo clave de la transformación digital segura y de los resultados empresariales.

Con sus mayores niveles de visibilidad y control, una arquitectura basada en zero trust elimina la complejidad de las TI modernas 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 menores costos.

2

Se necesita más educación para disipar el miedo, la incertidumbre y las dudas en torno a lo que significa zero trust y todas sus consecuencias para la empresa.

El CIO y el CISO tienen un papel fundamental que desempeñar aquí para comunicar el mensaje ampliado de zero trust al directorio, poniendo su atención en que es acorde con la estrategia empresarial.

3

Las tecnologías emergentes deben considerarse una ventaja empresarial competitiva y hoy, las infraestructuras zero trust sientan las bases del futuro.

La decisión acerca de cuáles son las tecnologías emergentes que se deben seguir debe basarse en la visión empresarial global y las necesidades actuales y futuras de la organización, no en las tendencias o en la moda. El objetivo de zero trust es apoyar los requisitos de conectividad segura y eficaz de las tendencias emergentes.

Por lo tanto, una vez que la mentalidad haya cambiado para reconocer que zero trust es un verdadero activo clave de la empresa, ¿cómo deben las organizaciones garantizar una arquitectura zero trust que logre estos resultados empresariales con éxito?



Zscaler ha implementado zero trust como componente central de la arquitectura de Zero Trust Exchange, y se expande a través de cada elemento del marco SSE. Esto incluye un modelo zero trust para los usuarios que tienen acceso a cualquier aplicación (interna o externa), conectividad IoT/OT y cargas de trabajo que tienen acceso a recursos en un entorno multinube o en Internet. Los principios de zero trust permiten un trabajo híbrido seguro desde cualquier sitio como estrategia empresarial, lo cual a su vez, permite a los empleados, socios comerciales y clientes trabajar desde la ubicación más adecuada para su productividad, un requisito clave para la continuidad empresarial, adquisición de talento remoto y distribución de entornos de trabajo híbridos cada vez más conocidos.

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

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



Verificar

La arquitectura Zero trust comienza por cortar la conexión y establecer:

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



Control

La arquitectura zero trust apunta a:

- 4. Evalúa el riesgo
- 5. Evita el peligro
- 6. Previene la pérdida de datos



Hacer cumplir

Antes de establecer finalmente una conexión, la arquitectura zero trust hará lo siguiente:

- 7. Hace cumplir la política

Tener en cuenta estos elementos será la base para que las organizaciones que dan prioridad a la nube aceleren la transformación digital y evolucionen para convertirse en organizaciones listas para lo que se presente el futuro.



Acerca de Zscaler y Zscaler zero trust Exchange

Zscaler es líder en zero trust con reconocimiento mundial, gracias a la plataforma zero trust de mayor envergadura, la más fácil de usar y la más madura.

Puede confiar en la plataforma nativa de la nube Zscaler Zero Trust Exchange para su trayectoria hacia zero trust. A diferencia de los productos de redes y seguridad heredados, Zero Trust Exchange es una plataforma especialmente diseñada para la nube. Su seguridad comienza con la terminación de 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 tienen acceso, como Microsoft 365 y AWS. Asimismo, garantiza el camino más corto entre los usuarios y sus destinos, proporcionando una seguridad integral y una experiencia de usuario sorprendente.

Puede obtener más información sobre nuestra plataforma fácil de usar [aquí](#).

A man with a beard, wearing a high-visibility yellow safety jacket over a green shirt and a black safety harness, is looking down at a tablet computer. He is standing in a field of tall, dry grass. In the background, there are several large white wind turbines under a clear sky. A blue dotted pattern is overlaid on the right side of the image.

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



Metodología

ATOMIK Research encuestó a 1,908 responsables sénior de la toma de decisiones (CIO/CISO/CDO/directores de arquitectura de red) en EMEA (Reino Unido, Alemania, Francia, Países Bajos, Suecia, Italia, España), AMS (EE. UU., México, Brasil) y APAC (Japón, India, Australia, Singapur). La investigación se llevó a cabo entre el 31 de mayo y el 28 de junio de 2022. La muestra incluyó un 43 % de organizaciones de hasta 4,999 empleados, un 32 % de 5,000 a 9,999 empleados y un 25 % de 10,000 o más empleados.