Sin ataduras: Cómo los CIO y CISO allanan el camino para el nuevo personal híbrido

En este informe de investigación a fondo, descubra técnicas efectivas para hacer la transición de una infraestructura heredada expuesta a una estrategia efectiva de confianza cero.

UN INFORME DE INVESTIGACIÓN DE HMG STRATEGY IMPULSADO POR ZSCALER

HMG STRATEGY

zscaler™

RESUMEN EJECUTIVO

A medida que avanzamos hacia una nueva fase de la pandemia mundial, muchas empresas están luchando por hacer regresar a sus empleados después de más de dos años sin trabajar en la oficina. Encuesta tras encuesta muestra que la mayoría de las personas quieren adecuaciones de trabajo híbridos, una combinación de presencial y remota, y se van en busca de nuevas oportunidades cuando no se les brinda la libertad de decidir cuándo y dónde trabajar.

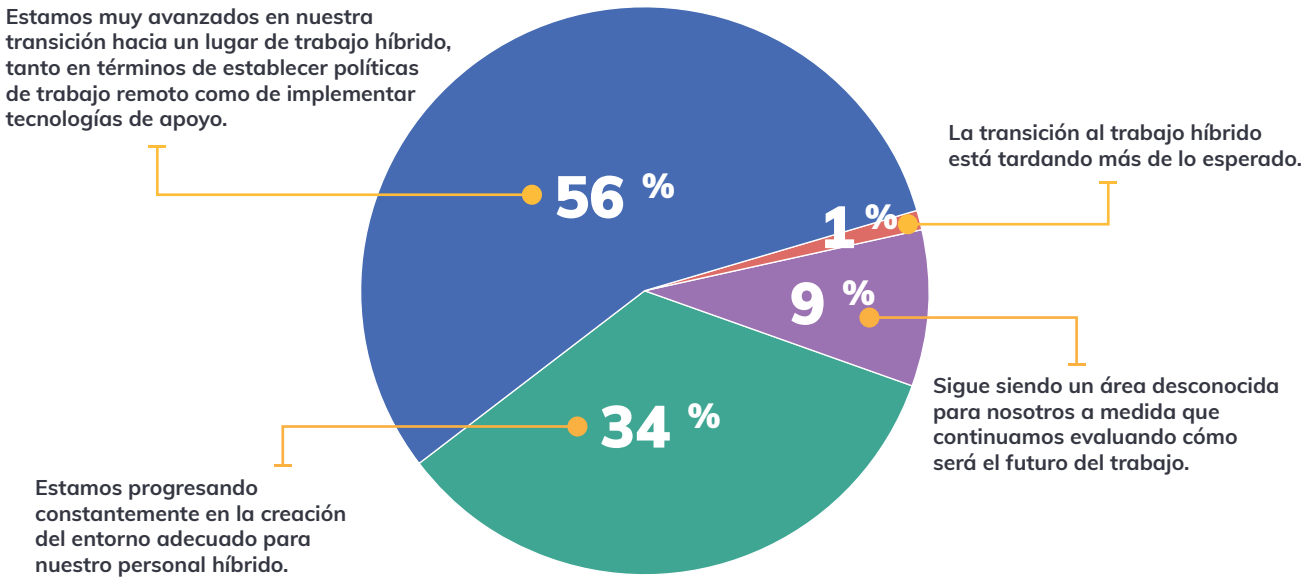
Así que ¿cómo hacemos una transición exitosa de la empresa al futuro del trabajo híbrido? ¿Y cómo pueden los CIO y CISO trabajar en consonancia con otros miembros ejecutivos de nivel C para ofrecer un entorno de trabajo ágil y productivo mientras protegen adecuadamente a la empresa?

Una encuesta reciente de 138 CIO, CISO y líderes tecnológicos corporativos realizada por HMG Strategy, patrocinada por Zscaler, revela que, mientras el 56 % de los encuestados informan que sus organizaciones están "muy avanzadas" en su transición hacia un lugar de trabajo híbrido (tanto en términos de configuración políticas de trabajo remoto e implementación de tecnologías de apoyo), casi la mitad (44 %) de los ejecutivos definen su transición de sus organizaciones a un lugar de trabajo híbrido como una tarea en progreso.

De hecho, entre ese 44 %, casi uno de cada cinco encuestados dice que la transición hacia ser un lugar de trabajo híbrido "todavía es un área bastante desconocida para nosotros ya que seguimos evaluando cómo será el futuro del trabajo".

Adaptarse al lugar de trabajo híbrido

¿Cómo definiría la transición de su organización del trabajo remoto al trabajo híbrido?



Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

“La mayoría de las organizaciones sobreviven a sus transiciones del trabajo remoto al híbrido, pero no están prosperando”, dijo **Bryan Green**, CISO de América, Zscaler. Por ejemplo, desde el comienzo de la pandemia, la mayoría de las empresas han realizado inversiones temporales a corto plazo para expandir el uso de tecnologías VPN o saltarse aplicaciones confidenciales de gran ancho de banda, como los sistemas de videoconferencia, para abordar el cambio hacia el trabajo remoto. “Aunque no necesariamente están tomando las decisiones correctas de seguridad a largo plazo”, agregó Green.

Como "agentes de cambio" en época de pandemia, los líderes tecnológicos están bien posicionados para ayudar a sus organizaciones en la próxima fase del lugar de trabajo en evolución, asegurándose de implementar las tecnologías adecuadas para satisfacer las necesidades de los trabajadores híbridos mientras crean un entorno flexible, productivo y seguro. para trabajadores en la oficina y remotos por igual. Pero como indica la investigación, se necesita más trabajo para hacer realidad este concepto.

HMG Strategy se ha asociado con Zscaler para comprender mejor los desafíos y oportunidades a los que se enfrentan las empresas en su transición a un entorno de trabajo híbrido, incluidas las barreras tecnológicas y culturales para lograr un lugar de trabajo híbrido seguro y flexible. En este informe de investigación, descubrirá:

- Las dificultades técnicas para lograr un lugar de trabajo híbrido seguro y flexible, incluidas las deficiencias de la infraestructura heredada, como las tecnologías VPN.
- Los riesgos que afrontan las organizaciones al asegurar el acceso a las aplicaciones para un personal híbrido
- Los desafíos de seguridad asociados a dar acceso a aplicaciones privadas para trabajadores remotos y en la oficina
- Una arquitectura sólida como solución a los escollos de seguridad del entorno de trabajo híbrido con confianza cero

Los medios para acceder a las aplicaciones

¿Qué formas de tecnologías de acceso a aplicaciones está utilizando actualmente?

41%
Red privada virtual

29%
Servicios de red privada virtual/escritorio remoto

19%
Red privada virtual/infraestructura de escritorio virtual

11%
Red privada virtual/Infraestructura de escritorio virtual/Servicios de escritorio remoto

Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

“La mayoría de las organizaciones sobreviven a sus transiciones del trabajo remoto al híbrido, pero no están prosperando”.

BRYAN GREEN
CISO América
Zscaler

Superando las barreras para ser un lugar de trabajo híbrido flexible y seguro

Si bien las empresas han seguido adoptando el software como servicio (SaaS) y los servicios de nube pública en los últimos años, muchas organizaciones todavía siguen inmersas en el proceso de migración a la nube. Durante el próximo año, el 63 % de las empresas planea cambiar la mayor parte o la totalidad de su infraestructura de TI a la nube, frente a la cifra actual del 41 %, según un estudio de Foundry.

Y aunque la adopción de la nube avanza rápidamente, las empresas aún tienen una gran inversión en centros de datos e infraestructura local.

“A pesar del hecho de que han pasado 16 años desde que AWS comenzó a lanzar infraestructura de nube pública y privada, la COVID solo comenzó a acelerar el impulso masivo hacia el trabajo remoto hace dos años”, dijo Green, “por lo que aún hay un largo recorrido durante el que las empresas deben abordar la desafíos asociados con las complejidades de las personas, los procesos y las tecnologías en sus organizaciones”.

La dinámica del liderazgo es otro tema complejo asociado con el cambio al trabajo híbrido. Dadas las enormes inversiones inmobiliarias que las empresas han realizado en espacios de oficinas propios o alquilados, muchos altos ejecutivos quieren asegurarse de que el espacio de oficinas se utilice de manera eficaz. En algunos casos, los administradores senior exigen que los empleados trabajen dos o tres días a la semana en una oficina dedicada, aunque muchos empleados continúan rechazando estos lineamientos.

En la primera semana posterior al Día del Trabajo de 2022, el uso de oficinas en 10 áreas metropolitanas importantes de EE. UU. se acercó al 50 % de la asistencia previa a la pandemia de 2020, según un estudio compilado por Kastle Systems, una empresa de seguridad administrada que supervisa las entradas a los edificios de oficinas. La asistencia a la oficina sigue siendo más baja que antes de la pandemia, aunque varios estudios han mostrado un aumento en los últimos meses.

“La directivas de muchas organizaciones se enfrentan a la realidad de que tienen esas inversiones masivas en bienes raíces”, dijo Green. “Quieren que la gente esté allí para colaborar, así que es un desafío muy difícil”.

Abordar los desafíos de la ciberseguridad

Cuando las empresas dieron el giro hacia el trabajo remoto en marzo de 2020, quedaron de manifiesto una serie de deficiencias en su enfoque para supervisar y proteger al personal remoto. Para empezar, muchas organizaciones han confiado en las redes privadas virtuales (VPN) para que los empleados envíen y reciban datos a través de redes públicas o compartidas. Esto expuso una serie de vulnerabilidades con las VPN:

- Cada puerta de enlace de VPN tiene un oyente de entrada que la convierte en una superficie de ataque expuesta en sí misma.
- La puerta de enlace VPN se convierte en un punto de partida para ataques más sofisticados de piratas informáticos.
- La naturaleza de una VPN es intrínsecamente abierta, lo que obliga a los equipos de seguridad a bloquear explícitamente el acceso de los empleados a aplicaciones y sistemas a los que no tienen o no deberían tener derechos de acceso.

Modernización del lugar de trabajo híbrido

Muchos de los desafíos asociados con lograr un lugar de trabajo híbrido seguro y ágil están relacionados con una infraestructura obsoleta, combinada con la falta de herramientas necesarias para evitar la pérdida de datos y el acceso no autorizado a las aplicaciones.

Las principales barreras para un lugar de trabajo híbrido seguro y flexible

30 %

Aunque habilitamos activamente un sistema de uso de dispositivos personales, no contamos con las herramientas necesarias para minimizar el riesgo de pérdida de datos y acceso no autorizado a los recursos internos.

20 %

Nuestra infraestructura de VPN ralentiza notablemente la conectividad a Internet y afecta negativamente a la productividad de los empleados

22 %

Nuestro negocio depende de socios y contratistas externos, pero es un desafío brindarles acceso seguro a las aplicaciones internas.

16 %

La latencia de nuestra red VDI frustra a los empleados y hace que incluso las tareas más simples sean imposibles en los escritorios virtuales

7 %

Aunque habilitamos activamente un sistema de uso de dispositivos personales, no contamos con las herramientas necesarias para minimizar el riesgo de pérdida de datos y acceso no autorizado a los recursos internos; nuestro negocio depende de socios y contratistas externos, pero es un desafío brindarles acceso seguro a las aplicaciones internas.

5 %

La latencia de nuestra red VDI frustra a los empleados y hace que incluso las tareas más simples sean imposibles en los escritorios virtuales; nuestro negocio depende de socios y contratistas externos, pero es un desafío brindarles acceso seguro a las aplicaciones internas.

Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

"Si tiene alguna combinación de VPN de acceso remoto y VPN de sitio a sitio, termina con esta enorme superficie de ataque donde los usuarios o ciberdelincuentes pueden potencialmente enumerar su infraestructura".

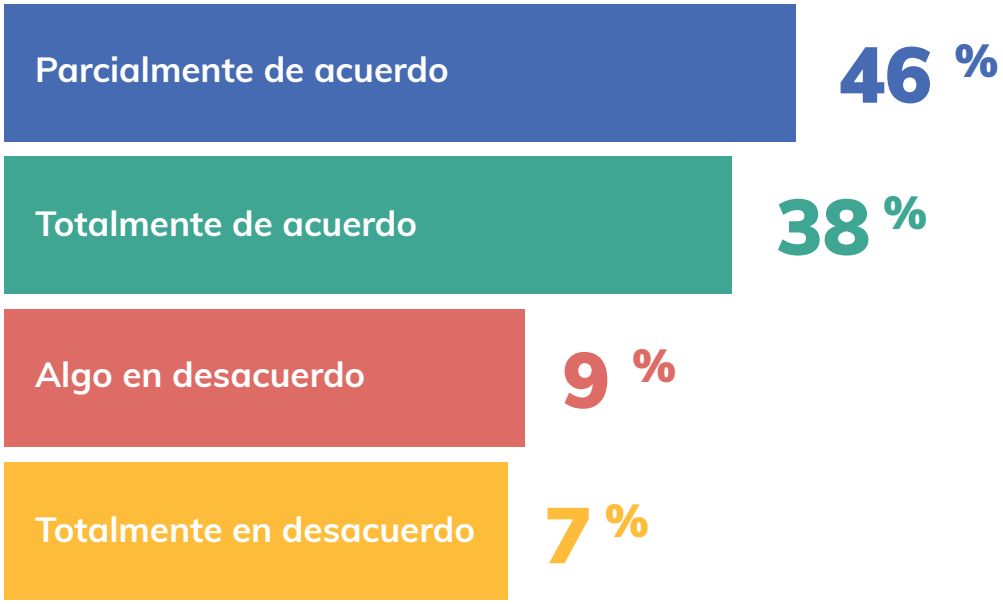
BRYAN GREEN
CISO América
Zscaler

“Cuando crea una conexión VPN, está extendiendo efectivamente la red corporativa a varias ubicaciones”, dijo Green, quien trabajó en los concentradores VPN de Cisco desde 2003. “Si tiene alguna combinación de VPN de acceso remoto y VPN de sitio a sitio, termina con esta enorme superficie de ataque donde los usuarios o ciberdelincuentes pueden potencialmente enumerar su infraestructura. A menos que haya ciertos tipos de cortafuegos o ciertos tipos de segmentación, realmente tienen carta blanca para acceder a la infraestructura”.

Un ladrón de productividad

El uso de acceso remoto y VPN de sitio a sitio no solo expande exponencialmente la superficie de ataque de una organización, sino que también estanca la productividad de los empleados híbridos.

¿Hasta qué punto está de acuerdo con que el rendimiento frustrantemente lento de las VPN afecta negativamente a la productividad de los empleados híbridos?



Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

Las vulnerabilidades inherentes asociadas con el uso de VPN son solo algunas de las razones por las que las organizaciones deben hacer la transición a una arquitectura de confianza cero para salvaguardar el lugar de trabajo híbrido. Una arquitectura de confianza cero no solo puede aislar a las organizaciones de infracciones costosas, sino que también brinda a las empresas una complejidad reducida, una protección de datos más sólida y una mejor experiencia para los empleados a la vez que elimina la superficie de ataque.

En las siguientes secciones del informe, exploraremos los desafíos de seguridad asociados con el acceso con privilegios excesivos junto con los beneficios operativos y comerciales de adoptar una estrategia de confianza cero.

Eliminación del acceso con privilegios excesivos para un entorno híbrido seguro

Aunque muchas organizaciones han tenido subconjuntos de empleados remotos durante años, el giro digital generalizado que las empresas se vieron obligadas a realizar en marzo de 2020 expandió exponencialmente la huella digital de cada organización, así como su superficie de ataque.

A medida que las empresas continúan expandiendo su adopción de nubes públicas, esto también aumenta el riesgo de acceso con privilegios excesivos y la exposición de datos críticos.

La exposición al riesgo de la mano de obra híbrida

Las infraestructuras heredadas aplicadas a un lugar de trabajo híbrido crean múltiples exposiciones con las que los equipos de seguridad deben lidiar, incluido el acceso a aplicaciones con privilegios excesivos para empleados y contratistas, así como usuarios vulnerados que acceden a los recursos de la red.

¿Qué riesgos enfrenta cuando protege el acceso a las aplicaciones para un personal híbrido?

31%
Acceso con privilegios excesivos para empleados o proveedores externos

26%
Usuarios vulnerados que acceden a los recursos de la red

18%
Pérdida de datos accidental y/o malintencionada

15%
Dispositivos de alto riesgo que acceden a los recursos de la red (p. ej., desconocidos, que no cumplen las normativas)

10%
Ataques de aplicaciones (p. ej., denegación de servicio, secuencias de comandos entre sitios, inyección)

Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

“El acceso con privilegios excesivos es un tremendo problema de seguridad al que nos enfrentamos, y es uno que nos ha costado abordar como sector”, dijo Green. Green hace una analogía con las interacciones de los clientes en una sucursal bancaria. En una sucursal bancaria, un cliente no da a cada cajero o empleado del banco una llave de su caja de seguridad. Pero cuando se trata de dar a los empleados y usuarios acceso lógico a diferentes tipos de aplicaciones en función de sus roles, "es mucho más difícil de implementar en comparación con el acceso físico", dijo Green.

Afortunadamente, las herramientas modernas, como la administración de derechos de infraestructura en la nube (CIEM), abordan los riesgos asociados con el acceso con privilegios excesivos al visibilizar profundamente los derechos de la nube y los riesgos de acceso, al tiempo que permiten a las organizaciones adoptar una estrategia de privilegios mínimos.

En la sección final del informe de investigación, compartiremos los factores que están impulsando a los líderes de seguridad y tecnología a adoptar estrategias de seguridad de confianza cero, junto con los beneficios operativos y comerciales de aplicar un modelo de confianza cero.

Falta de confianza en las herramientas de seguridad existentes

Solo un tercio de los líderes de seguridad y tecnología expresaron una gran confianza en que las herramientas de seguridad existentes de su organización podrían identificar a un usuario vulnerado o una amenaza interna que acceda a los recursos de la red.

¿Qué confianza tiene en que sus herramientas de seguridad existentes podrían identificar a un usuario vulnerado o una amenaza interna que accede a los recursos de la red?

34 %

Mucha confianza

62 %

Cierta confianza

4 %

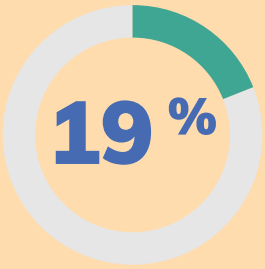
Ninguna confianza

Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

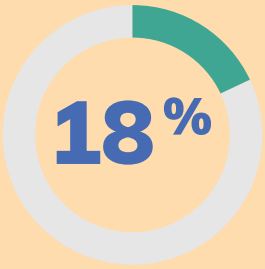
Las deficiencias de seguridad del acceso a aplicaciones privadas

No son solo las aplicaciones públicas las que están expuestas a vulnerabilidades de seguridad. Las aplicaciones privadas que están disponibles a través de las puertas de enlace de Internet también pueden ser vulnerables a los ataques.

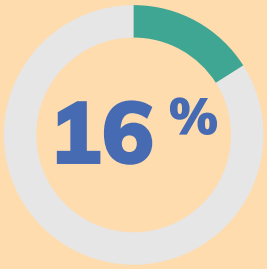
¿Cuál de los siguientes escenarios ha encontrado al dar acceso a aplicaciones privadas para trabajadores remotos y en la oficina?



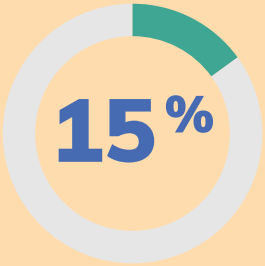
Los usuarios experimentan frustración debido a políticas de acceso inconsistentes y problemas de conectividad



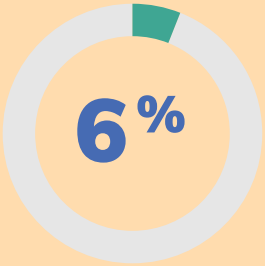
Las aplicaciones privadas están expuestas a Internet para dar acceso, lo que las hace vulnerables a los ataques.



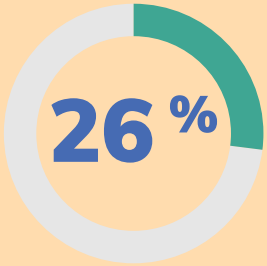
Los empleados y los usuarios externos tienen acceso completo a la red corporativa, lo que aumenta los riesgos de movimiento lateral



Llevamos a los usuarios remotos a nuestros centros de datos para acceder a aplicaciones privadas, lo que ralentiza su conexión a Internet.



Conectamos a los usuarios de la oficina/sucursal a nuestro centro de datos para acceder a aplicaciones privadas, lo que afecta negativamente el rendimiento



No hemos vivido ninguno de estos escenarios.

Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

El viaje hacia una estrategia de confianza cero

Con el aumento de las preocupaciones de seguridad asociadas con los dispositivos personales no administrados en un entorno de trabajo desde el hogar, la continua dependencia de las redes privadas virtuales (VPN) ha dejado expuestas a demasiadas organizaciones. Agregue a esto las vulnerabilidades asociadas con el acceso a aplicaciones con privilegios excesivos, y está claro que la infraestructura heredada que muchas organizaciones tienen para respaldar a su personal híbrido es simplemente una situación insostenible.

Estos son solo algunos de los motivos por los que la mayoría de los CISO y los líderes de seguridad de las empresas están adoptando arquitecturas modernas de confianza cero para apuntalar sus defensas y salvaguardar la organización de extremo a extremo.

"En primer lugar, una solución de acceso a la red de confianza cero mejora los resultados de seguridad en términos de una superficie de ataque reducida", dijo Green. "Además, ZTNA mejora drásticamente la experiencia y el rendimiento del usuario".

Los ejecutivos de tecnología de nivel C están considerando seriamente alternativas a la arquitectura heredada a medida que el trabajo híbrido se implementa más ampliamente. El fortalecimiento de la seguridad aumentando al mismo tiempo la productividad ha sido el motor para que la mayoría de las organizaciones adopten ZTNA. Todas las organizaciones que han adoptado la confianza cero han visto una reducción significativa en el coste y la complejidad, lo que lleva a un mayor enfoque en el negocio.

Los elementos detrás de la adopción de la confianza cero

Más del 35 % de los encuestados están considerando adoptar la confianza cero en vez de las soluciones heredadas para proteger su pila tecnológica y a los empleados en el entorno de trabajo híbrido.

¿Qué llevó a su organización a adoptar una estrategia de seguridad de confianza cero?

29 %

Actualmente estamos considerando una transición a la seguridad de confianza cero, pero aún no hemos tomado una decisión.

Reconocimos que los cortafuegos tradicionales y las VPN son más fáciles de eludir por los atacantes y que permitían el movimiento lateral libre. **21 %**

Hemos hecho la transición a una estrategia de confianza cero para permitir la conectividad segura y flexible del personal **20 %**

Reconocemos que los cortafuegos tradicionales y las VPN creaban una superficie importante para los ataques. **15 %**

Actualmente no planeamos adoptar una estrategia de seguridad de confianza cero. **15 %**

Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

“Digamos que un actor malicioso establece un punto de apoyo o vulnera alguna infraestructura dentro de su entorno. Desde la perspectiva de la cadena de eliminación, quiere poder asegurarse de que no puedan continuar moviéndose lateralmente por toda su organización”, dijo Green. “Lo más importante es que no puedan filtrar ninguno de esos datos de su entorno para que no puedan robar propiedad intelectual confidencial, secretos comerciales o datos de clientes. Creo que la combinación de esas tres cosas es realmente una de las razones más convincentes para avanzar hacia una solución basada en acceso de confianza cero”.

Una estrategia de confianza cero también ofrece beneficios adicionales en un mercado laboral ajustado. **El ochenta y cuatro por ciento** de los ejecutivos de tecnología que participaron en el estudio de investigación de HMG Strategy creen que habilitar un modelo de trabajo híbrido flexible y seguro ha contribuido a la capacidad de su organización para atraer y retener talento.

“Creo que el alto porcentaje de ejecutivos que ven esta conexión refleja la flexibilidad y la libertad con la que los empleados eligen trabajar”, dijo Green.

El 55 % de los encuestados en el estudio de investigación de HMG Strategy indican que el cambio al trabajo híbrido ha llevado a sus organizaciones a reevaluar su infraestructura de acceso remoto heredada.

Mientras tanto, dado que muchos equipos ejecutivos se han centrado en los costes, la transición de los controles heredados anticuados y costosos a una infraestructura moderna de confianza cero permite a las empresas responder a las condiciones cambiantes del mercado de manera rápida y flexible, al tiempo que reduce los costes y los riesgos para la empresa.

Al reemplazar los controles heredados dispares, una arquitectura de confianza cero también permite a los equipos de seguridad optimizar y administrar sus controles de seguridad generales de manera más efectiva. “Avanzar hacia un modelo de confianza cero realmente le permite plasmar gran parte del control en el plano de cumplimiento, de modo que realmente puede tener un solo panel para implementar muchos de estos controles de seguridad”, señaló Green.

Desde el punto de inflexión del lugar de trabajo digital en marzo de 2020, los empleados han demostrado no solo cuán productivos pueden ser mientras trabajan de forma remota, sino cuánto anhelan más flexibilidad en sus vidas personales y profesionales. Cada vez es más evidente que el entorno tradicional de oficina de nueve a cinco es cosa del pasado. Claramente, las tecnologías heredadas, como las VPN, no brindan la flexibilidad ni la protección para salvaguardar los datos confidenciales en un lugar de trabajo híbrido. Se necesita un enfoque nuevo y más eficaz.

Green dijo: "La confianza cero es una oportunidad fantástica para que las organizaciones mejoren la forma en que pueden operar en un entorno de trabajo híbrido".

Las tecnologías de confianza cero que protegen el trabajo híbrido

¿Cuál de las siguientes tecnologías de confianza cero utiliza actualmente su organización para habilitar el trabajo híbrido seguro?

19 %
Autenticación multifactor

16 %
Seguridad de puntos finales

14 %
Cortafuegos en la nube

10 %
Prevención de pérdida de datos (DLP)

9 %
Pasarela web segura

32 %
Otras entradas

Fuente: Encuesta de lugar de trabajo híbrido seguro 2022 de HMG Strategy, 138 CIO, CISO y ejecutivos de tecnología, realizada en el segundo y tercer trimestre de 2022.

Acerca de HMG Strategy

HMG Strategy es la plataforma digital líder del mundo para conectar a los ejecutivos de tecnología para reimaginar la empresa y remodelar el mundo de los negocios. La red global de HMG Strategy consta de más de 400 000 CIO, CTO, CISO, CDO, ejecutivos senior de tecnología comercial, ejecutivos de la industria de búsqueda, capitalistas de riesgo, expertos del sector y líderes de pensamiento de clase mundial.

Acerca de Zscaler

Zscaler acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zero Trust Exchange de Zscaler protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de los usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la mayor plataforma de seguridad en línea en la nube del mundo.