zscaler™

E-BOOK

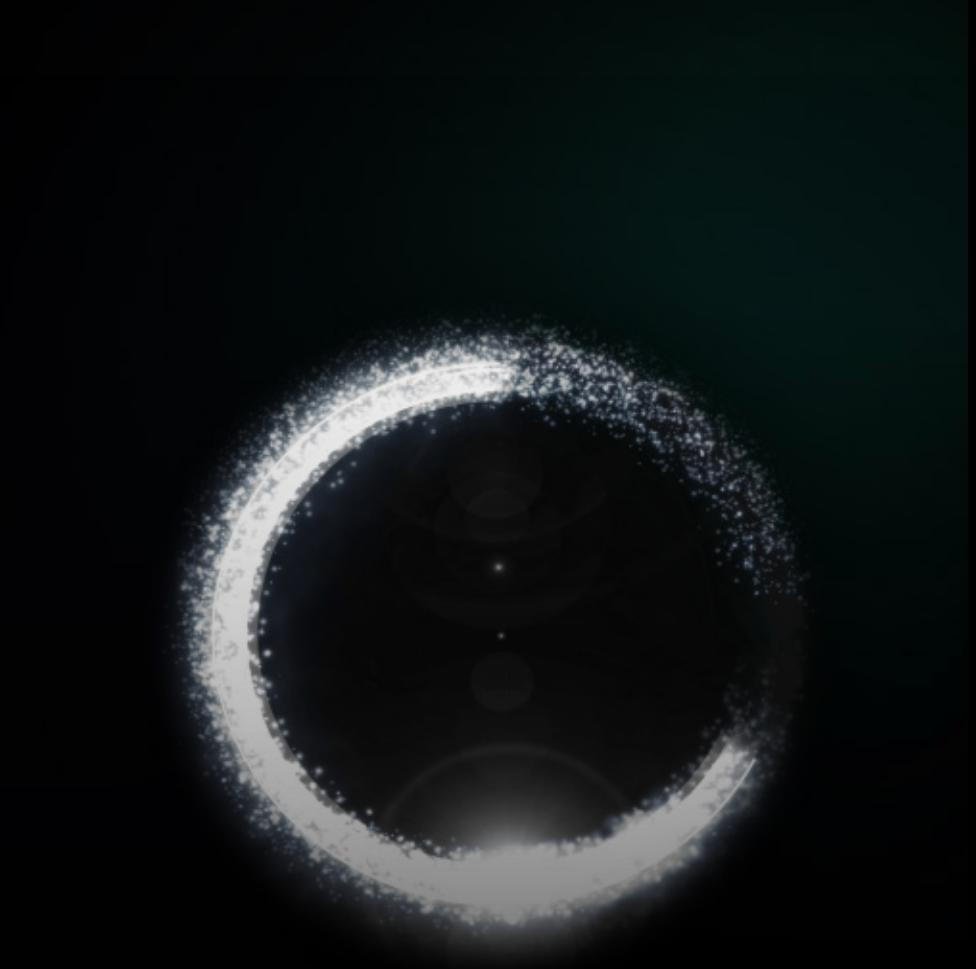
Las tres claves para la transformación Zero Trust: **plataforma, personas y proceso**

INTRODUCCIÓN

El camino hacia el modelo Zero Trust

La transformación digital ha cambiado fundamentalmente la forma de operar de las empresas modernas. Sus **empleados pasan ahora más tiempo en Internet que en la red corporativa,** accediendo a aplicaciones y datos desde cualquier lugar. Los datos empresariales sensibles se han distribuido más, ya que residen fuera del perímetro corporativo en aplicaciones SaaS, como Microsoft 365, y aplicaciones privadas en AWS, Azure y Google Cloud Platform.

El proceso de transformación digital mejora la agilidad empresarial y el flujo de información, pero amplía drásticamente la superficie de ataque y expone a su empresa a nuevas amenazas. Las arquitecturas de seguridad tradicionales, que se centraban en la protección de la red, ya no son eficaces en esta nueva realidad. Proteger su empresa y conservar las ventajas de la **transformación digital requiere migrar a un modelo de seguridad de confianza cero suministrado a través de la nube,** más cercano a donde se encuentran ahora sus usuarios y activos empresariales.



DEFINICIÓN

¿Pero qué es la confianza cero?

El concepto de confianza cero existe desde hace más de una década, pero ha habido mucha confusión acerca del significado real del término. No es simplemente una tecnología única.

Zero Trust es un enfoque holístico para asegurar 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 del usuario y el contexto,** siendo la política el guardián en cada paso del camino.

DEFINICIÓN

Zero Trust en la práctica

La confianza cero aborda los retos más difíciles de hoy en día, que abarcan la seguridad, las redes y la habilitación del lugar de trabajo moderno:

SEGURIDAD

Evite las amenazas cibernéticas:
la confianza cero ofrece protección contra amenazas cibernéticas no solo para los usuarios, sino también para las cargas de trabajo en la nube, para los servidores y para las aplicaciones SaaS.

Evite la pérdida de datos:
Zero Trust proporciona un enfoque holístico para garantizar que los datos no puedan filtrarse o perderse, ya sea accidental o intencionadamente, por parte de los usuarios o de las cargas de trabajo en la nube.

NETWORKING

Simplifique la conectividad de usuarios y sucursales:
la confianza cero permite a las organizaciones transformar las redes radiales heredadas, permitiendo a las sucursales y a los usuarios remotos conectarse de forma segura a cualquier destino directamente a través de Internet, independientemente de dónde se conecte el usuario.

Asegure la conectividad en la nube:
en lugar de ampliar las VPN tradicionales de sitio a sitio a la nube, lo que conlleva el riesgo de movimiento lateral, la confianza cero permite que las cargas de trabajo se conecten de forma segura a otras cargas de trabajo.

HABILITAR EL ESPACIO DE TRABAJO MODERNO

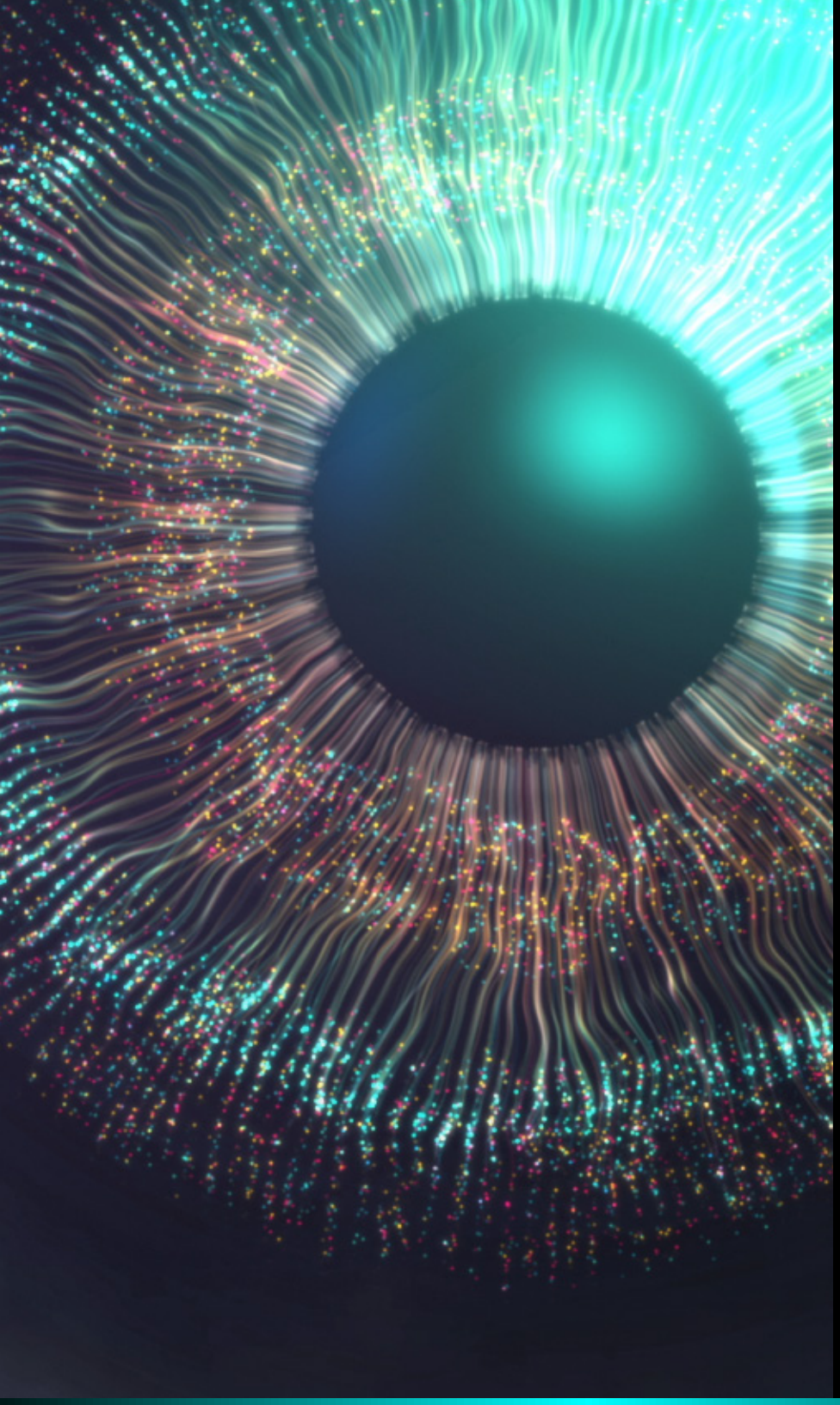
Asegure el trabajo desde cualquier lugar:
una verdadera solución de confianza cero debería permitir que sus empleados trabajen de forma segura y sin problemas desde cualquier lugar, sin tener que preocuparse por la red o por si necesitan activar o no una VPN.

Optimice las experiencias de usuario:
al garantizar que usted entiende la experiencia de cada empleado para cada aplicación, Zero Trust permite a las organizaciones ofrecer de manera consistente una excelente experiencia de usuario.

Planificar el éxito de la confianza cero

A medida que Internet se convierte en su nueva red corporativa, la confianza cero proporciona el camino para **un acceso rápido, fluido y seguro** en todo su ecosistema empresarial.

Pero la implantación de un modelo de seguridad de confianza cero no es solo una función de TI, sino que afecta a todas las áreas de su empresa y va más allá de los límites tradicionales de su organización. Para implantar con éxito el modelo Zero Trust se requiere una estrategia detallada que aborde los retos y las oportunidades de **las personas, los procesos y las plataformas tecnológicas.** →



LA BASE DE LA CONFIANZA CERO

Plataforma

La confianza cero no implica simplemente una única tecnología como la identidad o la segmentación de aplicaciones. Zero Trust es una estrategia, **una base sobre la cual construir su ecosistema de seguridad.** Conecta de forma segura a los usuarios con las aplicaciones mediante políticas empresariales a través de Internet. En esencia, se trata de una plataforma tecnológica de confianza cero guiada por tres principios clave:

1. Conectividad basada en **identidad y política**
2. Hacer **que las aplicaciones sean invisibles**
3. **Arquitectura basada en proxy** para conectarse a las aplicaciones e inspeccionar el tráfico

LA BASE DE LA CONFIANZA CERO

Plataforma

1 Conectividad basada en identidad y contexto

Las VPN y los cortafuegos tradicionales ponen a los usuarios en la red para que accedan a las aplicaciones. Una vez en la red, la confianza inherente que se deposita en el usuario aumenta el riesgo de movimiento lateral por amenazas o posibles atacantes. Por el contrario, la confianza cero utiliza la identidad y las políticas basadas en el contexto para conectar de forma segura a los usuarios autentificados exclusivamente con una aplicación específica autorizada, basándose en políticas granulares de acceso y seguridad, sin colocar nunca a los usuarios en la red corporativa. Limitar el acceso impide el movimiento lateral y reduce el riesgo empresarial. Y dado que no es necesario exponer a Internet ningún recurso de la red en ningún momento, puede protegerse de ataques dirigidos y DDoS.

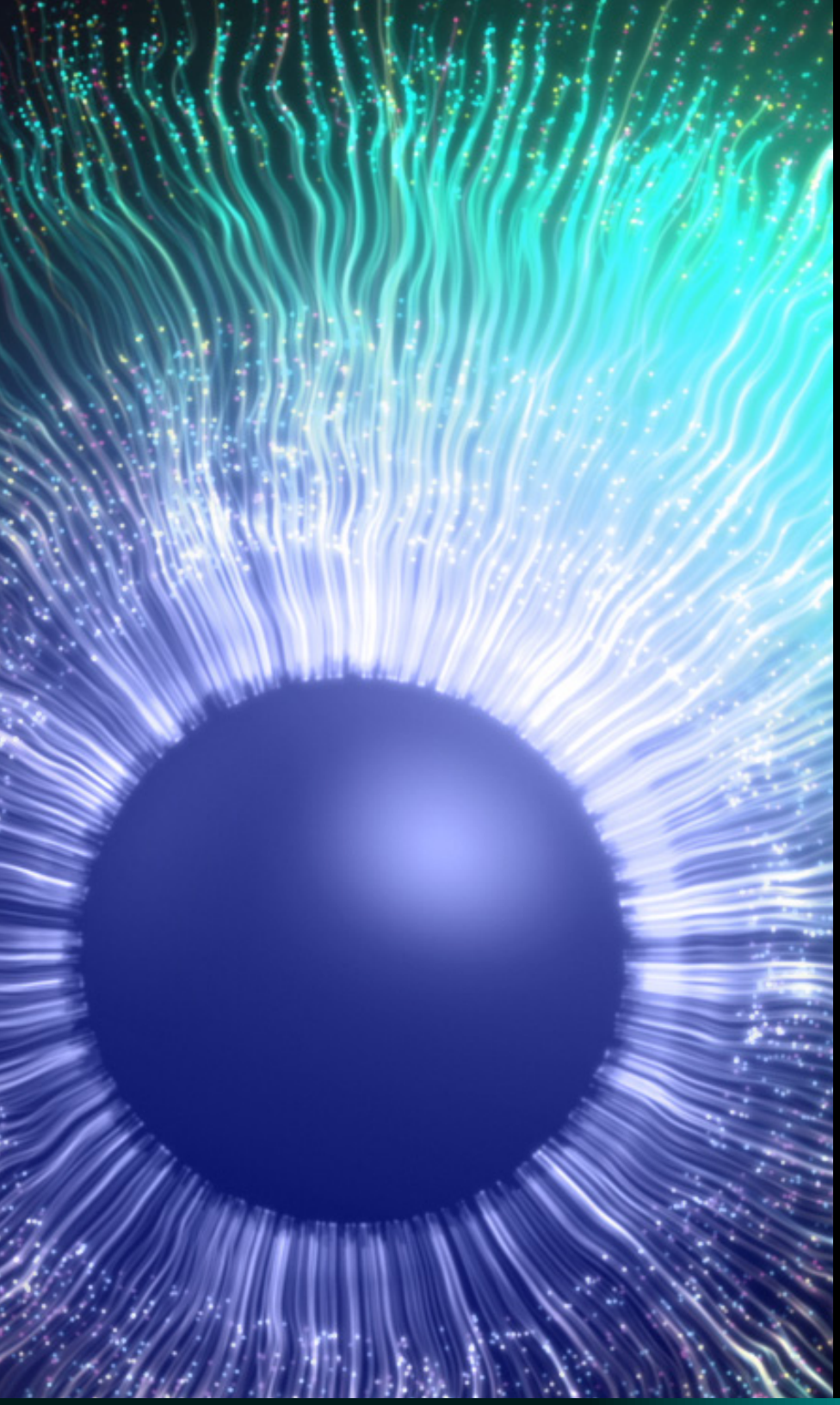
2 Hacer que las aplicaciones sean invisibles

La migración de aplicaciones a la nube amplía en gran medida la superficie de ataque. Los cortafuegos tradicionales publican sus aplicaciones en Internet, lo que significa que los usuarios y los hackers informáticos pueden encontrarlas fácilmente. Un enfoque de confianza cero debe evitar exponer la red corporativa a Internet ocultando las identidades de las fuentes y las direcciones IP. Al hacer que las aplicaciones sean invisibles para los adversarios y que solo puedan acceder a ellas los usuarios autorizados, se reduce la superficie de ataque y el acceso a las aplicaciones (en Internet, en SaaS o en nubes públicas o privadas) es siempre seguro.

3 Arquitectura basada en proxy para conectarse a las aplicaciones e inspeccionar el tráfico

Los cortafuegos de última generación tienen serias dificultades para inspeccionar el tráfico cifrado. En consecuencia, las organizaciones a menudo terminan omitiendo la inspección del tráfico cifrado, aumentando el riesgo de amenazas cibernéticas y pérdida de datos. Además, los cortafuegos utilizan un enfoque "de paso", lo que permite que el contenido desconocido alcance su destino antes de que se complete cualquier análisis. Si se detecta una amenaza, se envía una alerta, pero puede ser demasiado tarde. En su lugar, la protección eficaz contra amenazas y la prevención integral contra la pérdida de datos requieren una arquitectura proxy diseñada para inspeccionar las sesiones SSL, analizar el contenido de las transacciones y tomar decisiones sobre política y seguridad en tiempo real antes de permitir que el tráfico llegue a su destino. Y debe hacer todo esto a escala, sin afectar el rendimiento y sin importar dónde se conecten sus usuarios.

Acción recomendada: evalúe una plataforma de confianza cero como Zscaler Zero Trust Exchange™



UN CAMBIO CULTURAL

Personas

La adopción satisfactoria de la confianza cero comienza con la plataforma correcta, pero depende de que la organización **desarrolle nuevas habilidades y adopte una nueva mentalidad cultural.** Desde los líderes de TI que se enfrentan a la necesidad de transformarse de manera rápida y segura, hasta los profesionales de TI sobre el terreno que implementan la confianza cero, todos, desde su equipo ejecutivo hasta sus usuarios finales y ecosistema ampliado, deben estar incluidos para garantizar el éxito.

UN CAMBIO CULTURAL

Personas

Líderes de TI

Como líder de TI, debe ser tanto un innovador como un estratega. Su viaje hacia la Zero Trust requiere que alinee las prioridades de negocio y de TI, que rompa los silos y que aplique las tecnologías y la arquitectura adecuadas para impulsar la transformación y lograr los resultados deseados para su negocio. En su viaje hacia la confianza cero, esto es lo que necesitará hacer:

- **Comprender las mejores prácticas y estrategias** para la transformación de los compañeros y organizar la empresa para aplicar esos cambios
- **Ayudar a sus profesionales de TI a desarrollar las habilidades y conocimientos** necesarios para pasar con éxito de una arquitectura centrada en la red a una arquitectura de confianza cero
- Hacer que la confianza cero **sea invisible para sus usuarios finales**

Acción recomendada:
conecte con innovadores con la misma visión de la confianza cero y las mejores prácticas de transformación digital en un foro como **Zero Trust REvolutionaries**

UN CAMBIO CULTURAL

Personas

Encargados de TI

Sus equipos de TI son expertos en redes y seguridad y están acostumbrados a trabajar con hardware y a establecer políticas basadas en 30 años de principios de seguridad y redes de TI. La migración a la confianza cero **afecta directamente a sus profesionales de TI.** Muchas de las habilidades en las que han confiado en el pasado tendrán que ser actualizadas y deberán desarrollar nuevas habilidades para la transformación digital, pero el resultado será que tendrán un impacto mucho mayor en la organización y un cúmulo de conocimientos más valioso y orientado al futuro.

El éxito depende de proporcionar **formación avanzada para la transición de su personal de TI,** asegurándose de que entienden los nuevos procesos de negocio, así como las mejores prácticas y procedimientos para utilizar los servicios de confianza cero. Al mismo tiempo, puede demostrarles cómo el modelo Zero Trust **les ahorrará tiempo** y les permitirá **ofrecer más valor** a la organización.

Acción recomendada:
ayude a sus profesionales de TI a ponerse al día sobre la confianza cero con un programa de formación certificado, el Zscaler™ Zero Trust Academy

UN CAMBIO CULTURAL

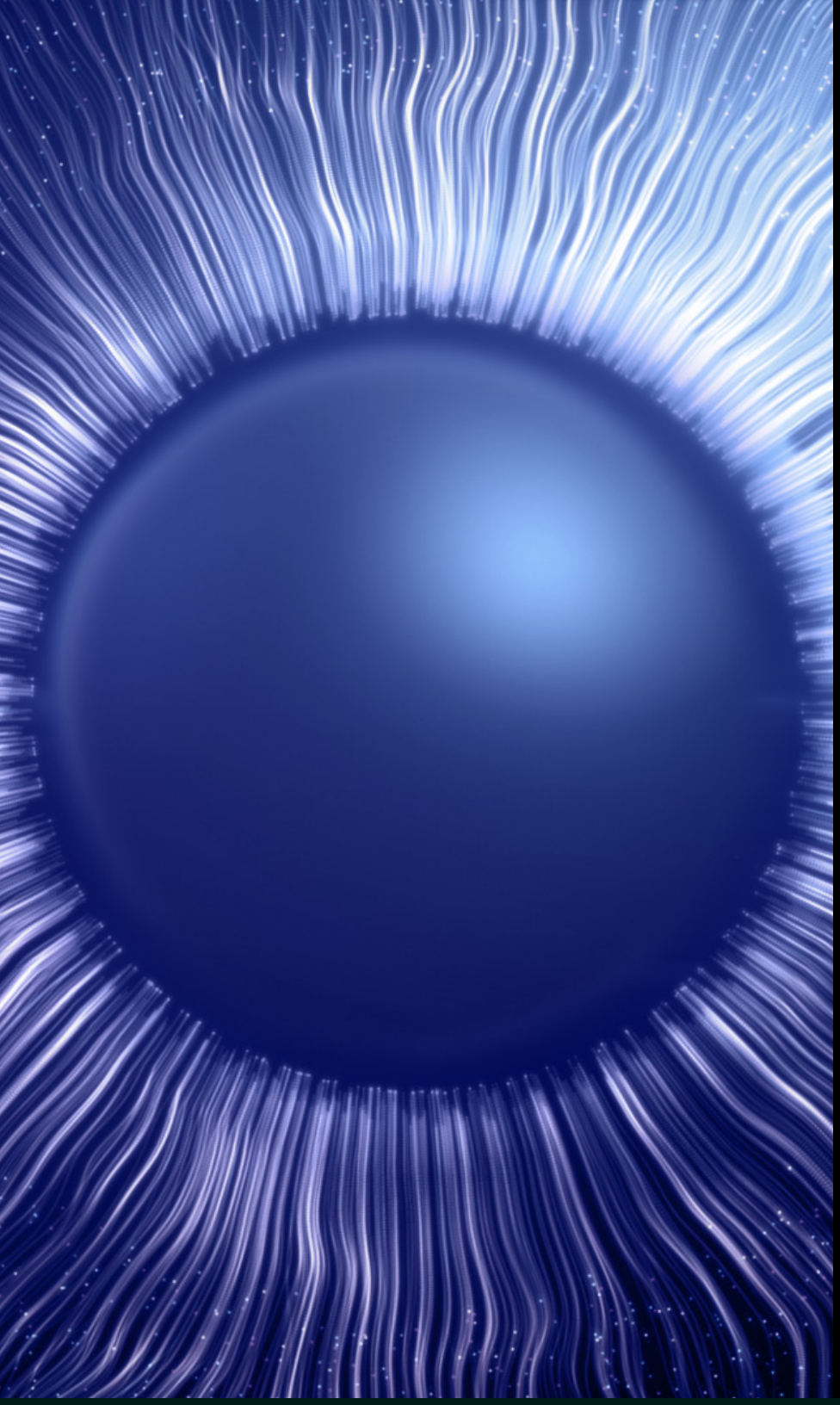
Personas

Sus usuarios

Si se hace correctamente, la confianza cero es un habilitador invisible para sus usuarios finales, que permite a los empleados trabajar desde cualquier lugar en cualquier dispositivo. Dado que el acceso Zero Trust se basa siempre en las políticas de identidad y de negocio y que el servicio en la nube conecta automáticamente a los usuarios con las aplicaciones a través de la ruta de acceso más rápida, la ubicación física del usuario ya no importa. Un usuario que trabaja en la oficina tiene la **misma experiencia de acceso rápido y consistente** cuando trabaja desde casa o desde cualquier otro lugar.

Al mismo tiempo, una solución sólida de confianza cero permite a las organizaciones **reducir drásticamente el riesgo sin bloquear el acceso a las aplicaciones** para los usuarios. Por ejemplo, la tecnología de aislamiento del navegador en la nube puede proporcionar un acceso seguro al contenido activo mediante la entrega de páginas web como píxeles renderizados en un entorno aislado sin afectar a la experiencia del usuario. También puede aprovecharse para limitar la capacidad de copiar y pegar datos, impedir la descarga de archivos o confinar las descargas al contenedor de aislamiento para proteger los dispositivos endpoint del ransomware y otras amenazas sofisticadas. De este modo, la confianza cero aprovecha la tecnología para limitar el riesgo en función del contexto.

Acción recomendada:
aproveche las arquitecturas de confianza cero que incluyen herramientas que garantizan a sus usuarios una gran experiencia, como Zscaler Digital Experience



UNA VÍA PROGRAMÁTICA

Proceso

¿Cuáles son los pasos para llegar a la confianza cero y cómo puede acelerar la transformación de su negocio? Saber por dónde empezar puede ser la parte más difícil de este viaje, pero no tiene por qué ser así. Zero Trust comienza con una plataforma y debe extenderse para **abarcar datos, personas, dispositivos y cargas de trabajo.**

Por lo tanto, la integración sólida de productos con su proveedor de identidades, la solución de seguridad de endpoints y la solución SIEM son piezas esenciales del rompecabezas de la confianza cero para añadir un contexto adicional y simplificar la adopción.

UNA VÍA PROGRAMÁTICA

Proceso

En vista de la necesidad de integración, recomendamos una **plataforma de confianza cero y un ecosistema de socios tecnológicos** que proporcionen las siguientes herramientas para informar su diseño y potenciar su adopción de la confianza cero:

- **Modelos de soluciones** que proporcionan arquitecturas de referencia de casos prácticos
- **Guías de diseño** que comparten los principios de diseño y las mejores prácticas de integración
- **Guías de implantación** que proporcionan orientación sobre la configuración a medida que se activan las integraciones para la prueba de valor (POV) y la implantación en producción

La implantación de una solución holística de confianza cero resulta mucho más fácil con el proyecto adecuado. Busque proveedores con arquitecturas de referencia validadas conjuntamente y diseñadas para abordar un conjunto específico de casos de uso y una guía de diseño prescriptiva para los arquitectos de seguridad sobre el uso conjunto de estas plataformas basada en las mejores prácticas.

Dicha guía proporciona un marco más estructurado que simplifica la implantación, garantiza operaciones eficientes y la mejor experiencia de usuario a la vez, que permite la aplicación de una seguridad óptima. Todo ello le permitirá acelerar la adopción de la confianza cero en toda su organización.

Acción recomendada: aproveche las soluciones con una mayor integración de socios que proporcionan diseños y proyectos validados, como los que se encuentran en el ecosistema de confianza cero de Zscaler

Aproveche su momento Zero Trust

La transformación digital hace que las empresas sean más ágiles y eficientes, pero requiere que replantee sus arquitecturas de red y seguridad. Zero Trust proporciona **la base para que las organizaciones que priorizan la nube aceleren la transformación digital** y capaciten a los empleados para que trabajen de manera productiva y segura desde cualquier lugar. Al comenzar su viaje, desarrollar una estrategia que incorpore la plataforma, las personas y los procesos adecuados ayudará a garantizar el éxito.

Seleccione una plataforma que utilice la identidad y la política empresarial para establecer la confianza y que conecte a los usuarios con los recursos sin colocarlos en la red corporativa. Proteja las aplicaciones haciéndolas invisibles a los adversarios y accesibles exclusivamente a los usuarios autorizados. Asimismo, utilice una arquitectura proxy en lugar de un cortafuegos passthrough o "de paso" para proteger sus datos y garantizar una protección eficaz contra amenazas cibernéticas.

Logre que sus colegas se acojan a las mejores prácticas y estrategias para la transformación. Alinee a su organización para adoptar una nueva mentalidad cultural y desarrollar las habilidades necesarias para implementar y gestionar una arquitectura Zero Trust, a la vez que garantiza que la confianza cero sea invisible y fluida para sus usuarios finales. Todo esto se hace más fácil con el proyecto correcto. Aproveche **una plataforma de Zero Trust con integraciones sólidas de socios que proporcionan arquitecturas de referencia validadas conjuntamente y orientación de diseño prescriptivo** para usar estas plataformas conjuntamente.

Mantener estos elementos en mente le ayudará a **aprovechar su momento de Zero Trust, acelerar su transformación digital y hacer de TI un verdadero habilitador de negocio.**

Explore las innumerables ventajas de **una auténtica plataforma de Zero Trust.**

Comience su viaje

zscaler™