zscaler™

ZSCALER

CÓMO LAS EMPRESAS FARMACÉUTICAS PUEDEN APROVECHAR TODO EL POTENCIAL DE LA NUBE

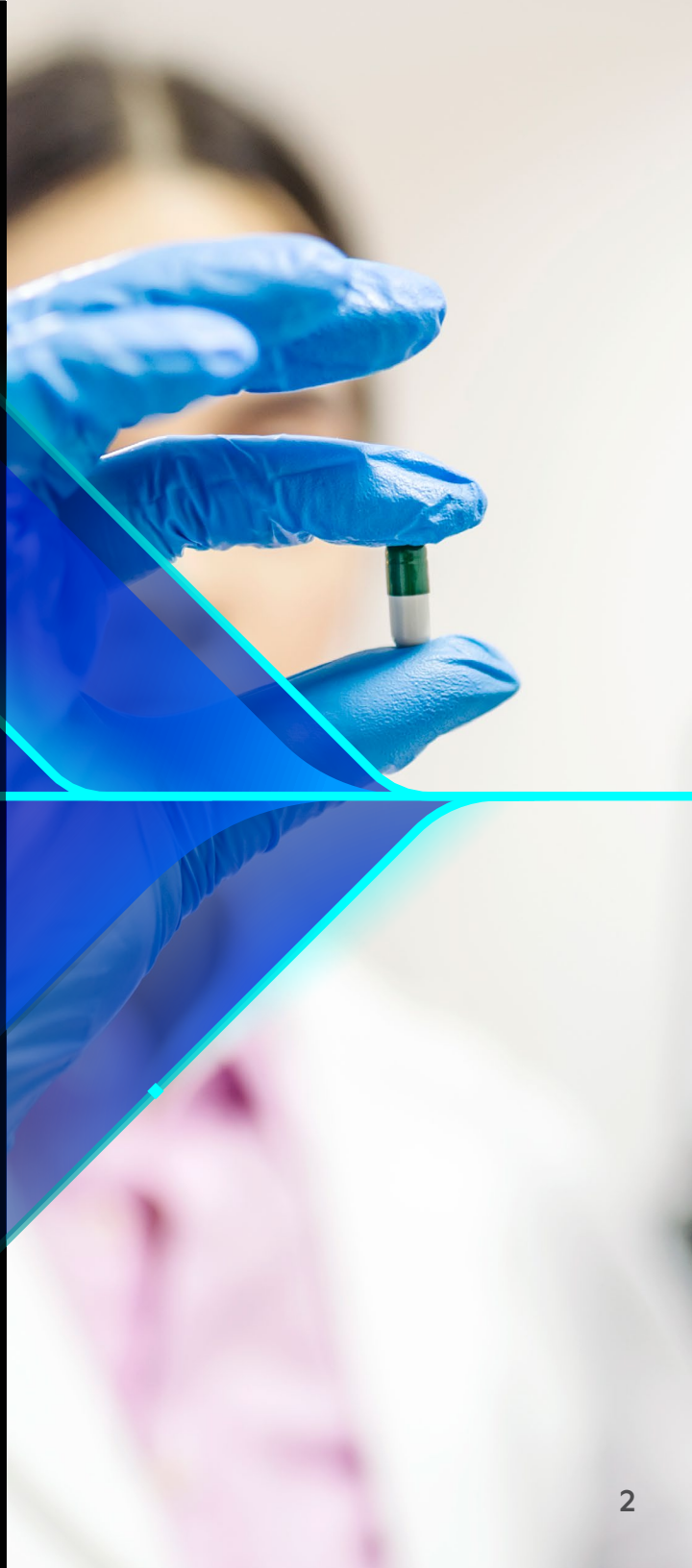
Mantenga e incremente la competitividad en el sector farmacéutico con el modelo de confianza cero y una plataforma de seguridad basada en la nube.

En el sector farmacéutico actual, es vital lanzar medicamentos, vacunas y otros nuevos productos farmacéuticos lo más rápidamente posible. Las empresas farmacéuticas necesitan innovar constantemente para tener éxito en un entorno altamente competitivo. Debido a esto, este sector está en la parte superior de la curva de innovación.

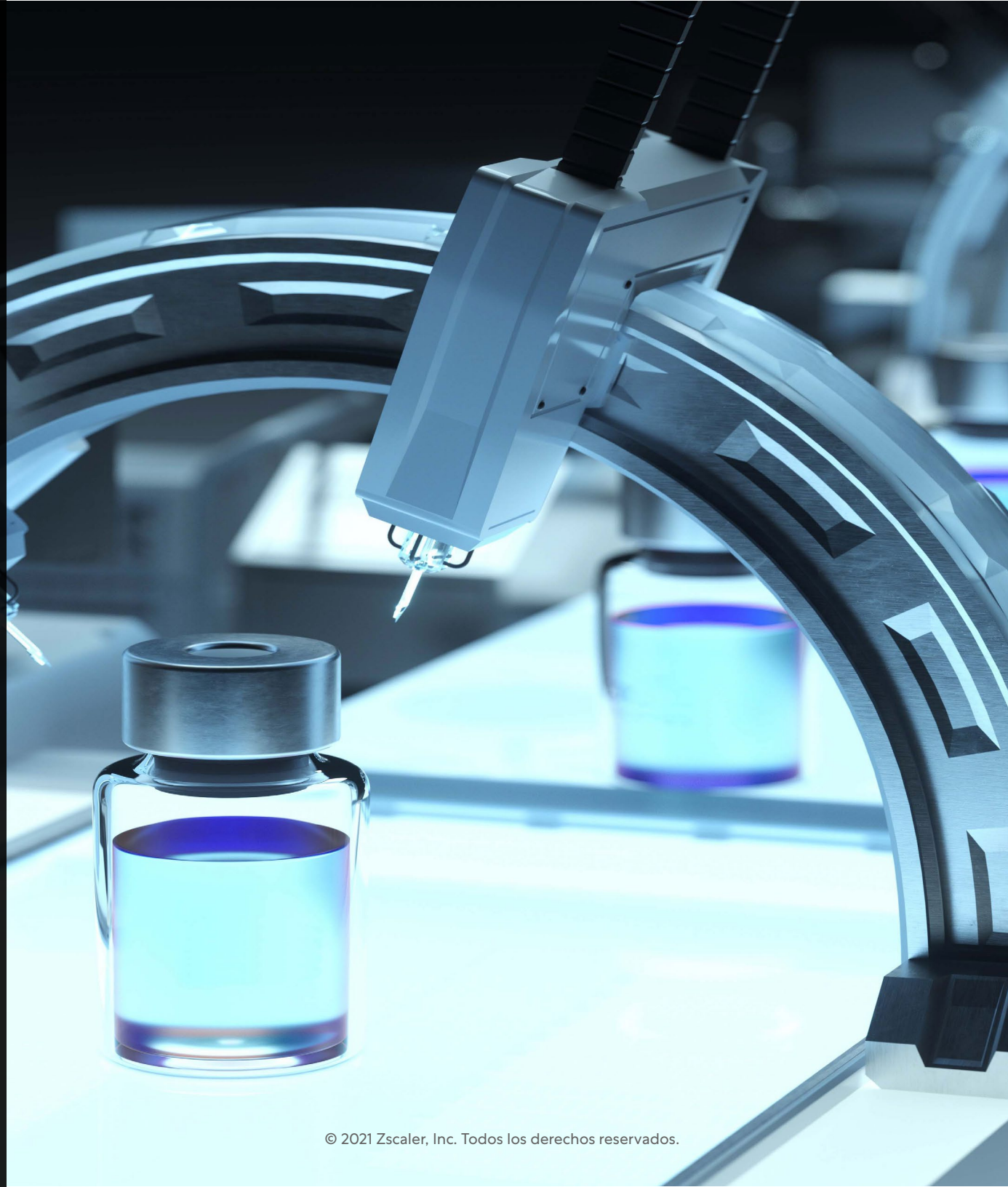
En busca de excelencia innovadora, nuevos modelos de negocio y ventajas competitivas, las empresas farmacéuticas están adoptando modelos colaborativos que están firmemente anclados en el ADN del sector. La nube desempeña un papel fundamental, ya que permite la colaboración entre empresas. Por un lado, las empresas están forjando asociaciones con instituciones externas como clínicas, laboratorios y centros de investigación. Por otro lado, están invirtiendo mucho en fusiones y adquisiciones. Las fusiones y adquisiciones impulsan el crecimiento, permiten aprovechar rápidamente el potencial de innovación y cumplir mejor los crecientes requisitos normativos.

Pero este tipo de modelos de colaboración también dan lugar a complejas infraestructuras informáticas que plantean nuevos retos de seguridad para las empresas farmacéuticas y sus departamentos de TI. Los líderes del mercado en el sector farmacéutico en particular, suelen estar expuestos involuntariamente a ciberamenazas. El coste medio de los daños causados por una violación de seguridad asciende a 5,06 millones de dólares, lo que sitúa al sector farmacéutico a la cabeza si se compara con el resto de sectores.

Ahora veremos las tendencias tecnológicas que han surgido con los modelos de colaboración y la transformación digital hacia la nube, así como los retos que plantean para la seguridad informática en las empresas farmacéuticas. Los ejemplos de mejores prácticas muestran cómo las empresas farmacéuticas consiguen aprovechar todo el potencial de la nube en materia de seguridad informática adoptando un enfoque de confianza cero y convirtiéndolo en una ventaja empresarial.



ÍNDICE



1 NUEVAS **TENDENCIAS TECNOLÓGICAS** EN ALZA

Las tecnologías de la nube se utilizan cada vez más en las empresas farmacéuticas

La transformación digital, el establecimiento de nuevos modelos de negocio basados en la digitalización, gana velocidad a medida que surgen nuevas tecnologías, y el número de dispositivos y redes que las empresas farmacéuticas utilizan para sus procesos de negocio crece de forma espectacular. La inteligencia artificial y el aprendizaje automático ya se están utilizando ampliamente en las empresas farmacéuticas para estructurar el Big Data. La red 5G, que funciona como la columna vertebral de la infraestructura para el Internet de las cosas, permite que innumerables dispositivos dentro de las líneas de producción farmacéutica se conecten y colaboren a alta velocidad.

Las operaciones tradicionales de los centros de datos cada vez cobran menos importancia. Los procesos de trabajo están cambiando cada vez más a la nube, y las tecnologías en la nube se están conectando a la infraestructura de TI existente, por lo que ya no se trata solo de proteger su red con un perímetro seguro. La seguridad de red tradicional tenía sentido siempre y cuando todas las aplicaciones estuvieran alojadas en el centro de datos y todos los usuarios estuvieran en la red. La tecnología de red privada virtual (VPN) heredada no fue diseñada para gestionar miles de accesos remotos; sufre problemas de latencia y seguridad.

Ante el repentino aumento de usuarios que trabajan desde casa, muchas empresas inicialmente lograron proporcionar a sus empleados acceso remoto seguro a la red corporativa central basado en la nube. El número de personas que trabajan desde casa se multiplicó por seis debido a la pandemia de COVID-19. En general, se prevé que esta tendencia al trabajo a distancia se intensificará en el futuro y que muchas personas que trabajan desde casa optarán por un modelo de trabajo híbrido. Estos desarrollos plantean numerosas preguntas: ¿sigue necesitando una red de oficina clásica en estas condiciones? ¿Cómo debe adaptarse la infraestructura de TI para apoyar al personal híbrido a largo plazo?

2 POR QUÉ LAS **EMPRESAS FARMACÉUTICAS** DEBEN ACTUAR AHORA

Las colaboraciones como modelos de negocio farmacéutico establecidos

Las fusiones y adquisiciones son una estrategia de crecimiento frecuente para las empresas farmacéuticas con el fin de mantenerse por delante de la competencia y desarrollar nuevos modelos de negocio así como los conocimientos técnicos necesarios. En 2018, el volumen de transacciones en el sector farmacéutico global fue de cerca de 150 mil millones de dólares. Sin embargo, estas actividades de fusiones y adquisiciones deben implementarse rápidamente para acelerar las sinergias y garantizar una monetización rápida. Aquí es exactamente donde la fusión de redes demuestra ser un obstáculo para la velocidad ya que requiere mucho tiempo. Además, la apertura mutua de las redes debe estar protegida. Por lo tanto, las actividades de fusiones y adquisiciones a menudo se prolongan durante meses y, en ocasiones, incluso años.

La colaboración con terceros proveedores es un reto permanente. Dichos proveedores deben poder acceder a los sistemas centrales de manera rápida y segura a fin de permitir una asociación efectiva. Sin embargo, los expertos en TI generalmente carecen de transparencia sobre quién tiene acceso a qué datos y herramientas bajo qué parámetros de seguridad. Como resultado, las empresas se exponen involuntariamente a un riesgo de seguridad. ¿Cómo puede el departamento de TI controlar con qué terceros trabaja la empresa? ¿Cómo pueden garantizar que solo puedan acceder a las aplicaciones necesarias sin afectar a toda la red? Hay una serie de preocupaciones normativas cuando se trabaja en la nube, especialmente cuando se trata de trabajar con socios. Todos los entornos de trabajo deben verificarse y la información debe estar protegida frente al acceso no autorizado.

La estricta normativa de Internet en China también supone un reto adicional para el sector. La correspondencia comercial electrónica se ve considerablemente ralentizada, si no bloqueada, por el “Gran cortafuegos”. A las empresas farmacéuticas que utilizan los servicios de Google les resulta difícil llevar a cabo negocios sin inconvenientes con sus centros de producción en China y tienen dificultades para conectarse con los usuarios remotos.

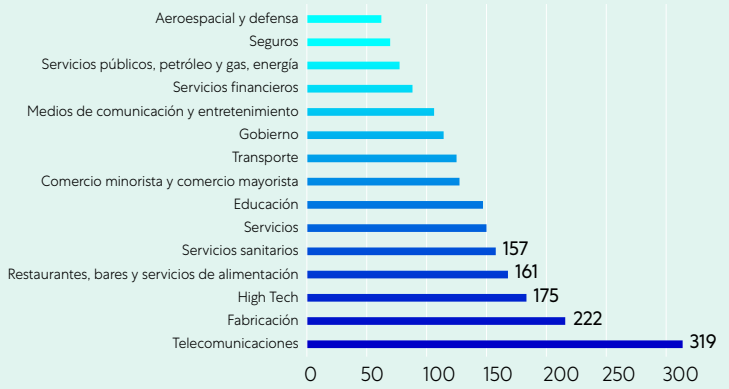
Tecnología de la información obsoleta y mayor complejidad de la red

En sus décadas de existencia, las principales empresas farmacéuticas de todo el mundo han pasado por innumerables modelos de negocio, han introducido modelos nuevos y han dejado otros atrás. Con el tiempo, esto ha dado lugar a un entorno de TI complejo que es difícil de administrar, lo que genera problemas de seguridad.

En la búsqueda de soluciones rápidas, muchos empleados han instalado soluciones por su cuenta, pasando por encima de la TI y creando una "TI en la sombra", evadiendo así el control central.

Esto se ve exacerbado por la escasez global de expertos cualificados en seguridad que podrían abordar los problemas de seguridad de la red existente. Un tercio de las empresas afirman tener problemas para encontrar expertos en TI y se tarda un promedio de seis meses antes en cubrir un puesto de TI. Si bien la escasez de habilidades ya era un problema antes de la pandemia, la batalla por el talento se ha intensificado debido al aumento de las tareas necesarias para gestionar entornos de TI complejos.

Los 15 sectores potencialmente más vulnerables a CVE



Aumento de la ciberdelincuencia debido a la digitalización

La digitalización presenta una plétora de problemas de seguridad que suponen una amenaza potencial para todos los sectores de la economía. Las tecnologías de digitalización se están desarrollando rápidamente, pero los métodos y las herramientas utilizados por los ciberdelincuentes también se están volviendo cada vez más sofisticados. Las industrias farmacéutica y sanitaria se encuentran entre los objetivos más comunes, como evidencian numerosos ejemplos recientes (Informe de superficie de ataque de Zscaler 2020).

Las consecuencias de un ciberataque incluyen el deterioro de la reputación de la marca y la pérdida de la propiedad intelectual, el retraso en la comercialización y los elevados costes de defensa o eliminación de los daños.

En resumen:

la modernización de las TI no se trata realmente de una opción sino de una prioridad para que las empresas farmacéuticas eviten los ciberataques. Un concepto de seguridad de confianza cero no solo protege frente a los problemas de seguridad, sino que debería formar parte de una estrategia de transformación holística para fortalecer la innovación del sector farmacéutico.

Más información sobre Cibercrimen

3 CÓMO PUEDE LA **CONFIANZA CERO** AYUDAR A SUPERAR LOS RETOS DE LA SEGURIDAD INFORMÁTICA

La confianza cero

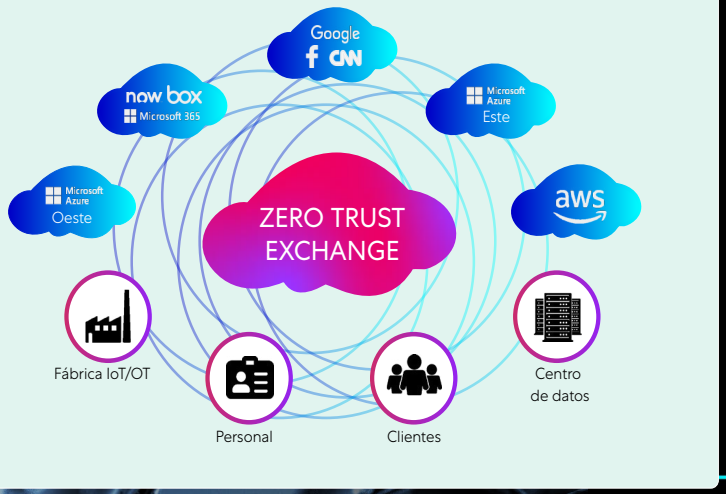
es un enfoque holístico para proteger a las empresas en la era de la digitalización. Se basa en el principio de derechos de acceso mínimos y en el concepto de que ningún usuario o aplicación debe ser inherentemente confiable. En consecuencia, la confianza solo se establece en función de la identidad y el contexto del usuario, con políticas que sirven como guardianes en cada paso.

Las empresas farmacéuticas deben estar preparadas para establecer sus mecanismos de defensa y control allí donde se establecen las conexiones: en Internet. Para garantizar que sean rápidas y seguras, independientemente de cómo o dónde se conecten los usuarios y accedan a sus aplicaciones, es preciso un nuevo concepto: el "enfoque de confianza cero".

El concepto de seguridad de confianza cero se basa en el principio de no confiar en ningún dispositivo, usuario o servicio dentro o fuera de la red. Para implementar este enfoque, se deben tomar amplias medidas para analizar y autenticar el tráfico de red. El riesgo para las redes y aplicaciones corporativas se minimiza al proporcionar visibilidad a todos los derechos de acceso basados en políticas y tráfico a Internet y a las aplicaciones en entornos multinube o en el centro de datos.

Con la introducción de una **plataforma de seguridad de confianza cero** basada en la nube, las empresas farmacéuticas pueden resolver sus problemas informáticos actuales. Se trata de una reestructuración holística que combina aplicaciones, aspectos de seguridad, conectividad y una nueva arquitectura de red. Basándose en esto, las empresas pueden abordar su viaje de transformación digital de forma estratégica.

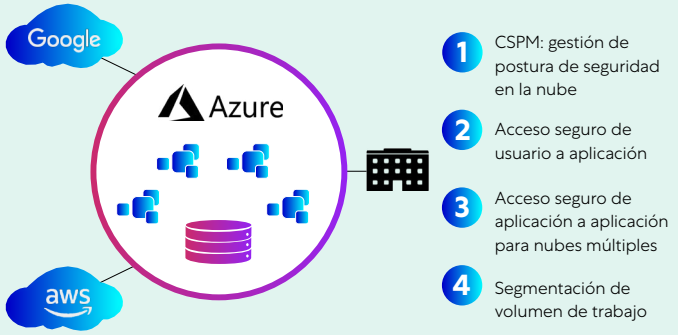
Más información sobre
Zscaler Zero Trust Exchange



La complejidad de la red en entornos multinube

El Zero Trust Exchange de Zscaler permite a los empleados con conexiones rápidas y seguras acceder a las aplicaciones desde cualquier lugar, lo que permite efectivamente que Internet actúe como una red corporativa. El acceso individual de los usuarios se segmenta granularmente a nivel de aplicación, incluido el acceso remoto al centro de datos y las aplicaciones en entornos en la nube. Zero Trust Exchange protege a miles de clientes de ciberataques y violaciones de datos al conectar de forma segura a usuarios, dispositivos y aplicaciones desde cualquier ubicación a través de un microtúnel cifrado basándose en la política.

Los cuatro elementos de ZCP



1. CSPM: gestión de postura de seguridad en la nube
2. Acceso seguro de usuario a aplicación
3. Acceso seguro de aplicación a aplicación para nubes múltiples
4. Segmentación de volumen de trabajo

Zscaler Cloud Protection (ZCP) utiliza la plataforma Zero Trust Exchange no solo para mitigar el riesgo asociado con la migración a la nube, sino también para reducir la complejidad operativa. ZCP identifica cargas de trabajo en la nube y garantiza una sólida postura de seguridad, lo que permite un acceso seguro a las aplicaciones solo para usuarios autorizados y un acceso seguro para cargas de trabajo a otras nubes, centros de datos e Internet. También tiene como objetivo mitigar los riesgos de ataque evitando el movimiento lateral de los atacantes.

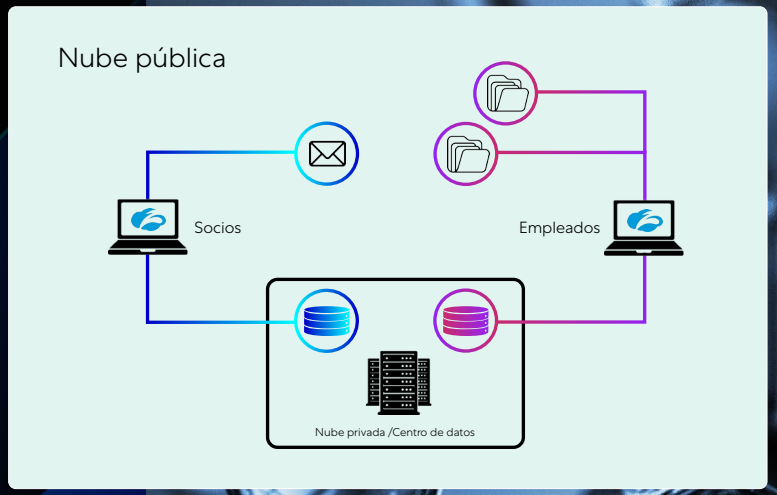
Los usuarios esperan una experiencia digital rápida y fluida. Zero Trust Exchange de Zscaler ofrece esto y más. La medición y mejora de las experiencias digitales en un entorno de trabajo híbrido y en la nube requiere una vista unificada de las aplicaciones, Cloudpath y las métricas de rendimiento de los puntos finales. Zscaler Digital Experience es un servicio nativo de la nube que analiza, repara y resuelve problemas de experiencia del usuario como parte de la mayor nube de seguridad del mundo.

Más información sobre
Zscaler Cloud Protection

Seguridad

Pasar de una arquitectura de seguridad rígida y centrada en el perímetro a una arquitectura que se adapte a una infinidad de arquitecturas y puntos de control diferentes en la nube requiere tanto cambios teóricos como prácticos. Para ello es necesario tanto una nueva forma de pensar sobre una solución como la tecnología adecuada para implementarla. La seguridad en sí misma debe trasladarse a la nube. La nube y la confianza cero crean las condiciones para una solución integral. Este es el núcleo del **enfoque de confianza cero para la transformación segura de la nube**.

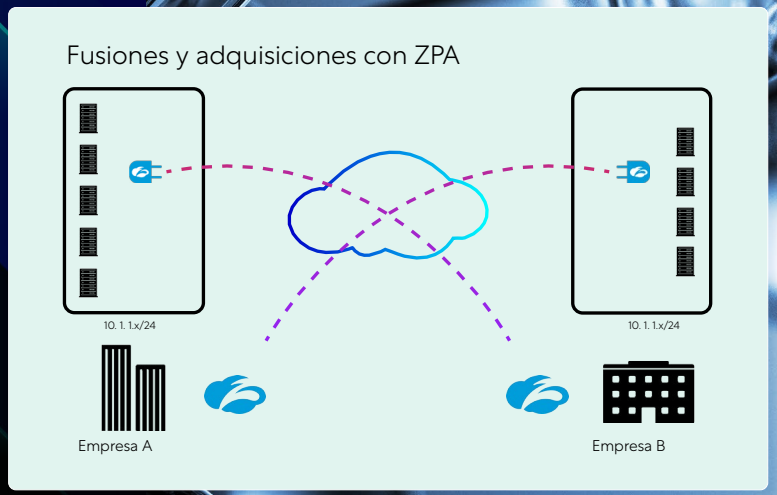
Más información sobre
Asegurar la transformación
en la nube



Fusiones y adquisiciones

Cada año se completan más de 50 000 fusiones, adquisiciones y desinversiones. La fusión de redes suele llevar mucho tiempo. Un enfoque de seguridad basado en la nube no solo simplifica la integración de TI durante fusiones y adquisiciones o desinversiones (y acorta el proceso a unas pocas semanas), sino que también reduce la superficie de ataque de la empresa.

Zscaler Private Access (ZPA) es una solución basada en la nube que proporciona acceso seguro a las aplicaciones internas alojadas en la nube o en un centro de datos a través de Zero Trust Exchange de Zscaler. Al conceder permisos de acceso granulares, ZPA puede garantizar que los empleados autorizados tengan acceso a las aplicaciones que necesitan en la red adquirida, incluso durante las adquisiciones corporativas, sin dar acceso a toda la red



Más información sobre
Zscaler Private Access (ZPA)

Mike Towers

CISO de Takeda

> En general, el valor empresarial y el impacto de nuestra asociación con Zscaler y nuestra marcha hacia la confianza cero nos ha permitido obtener valor en menos tiempo

4 IMPULSAR LA TRANSFORMACIÓN DE TI, CON **CONFIANZA CERO**

Los responsables de TI de las empresas farmacéuticas evalúan el uso de las nuevas tecnologías basadas en la nube desde una perspectiva técnico-estratégica. Se preocupan especialmente por impulsar la transformación digital de su empresa.

Implementar la transformación digital de forma estratégica

Una estrategia para implementar la transformación digital es particularmente importante en mercados de rápida evolución y altamente competitivos, como el sector farmacéutico, con el fin de mantener y ampliar las ventajas competitivas anteriores. Aquí se abordan los tres pilares de ciberseguridad, transformación de TI y experiencia de usuario.

Ciberseguridad significa garantizar el funcionamiento seguro de las aplicaciones y las redes, tanto in situ como a distancia. Hay que tomar medidas preventivas para encontrar los puntos vulnerables de seguridad y cerrarlos lo antes posible. Esto es especialmente importante en la integración de las infraestructuras informáticas en el curso de las actividades de fusiones y adquisiciones. La segmentación de aplicaciones/redes y la restricción de acceso (por ejemplo, en el desarrollo de vacunas) son las herramientas adecuadas para ello. Minimizan los movimientos laterales dentro de la red y garantizan la colaboración con partes externas concediéndoles el menor acceso privilegiado posible.

La transformación de TI consiste en reducir la complejidad de la infraestructura (que generalmente aumenta en el curso de las actividades de adquisiciones y fusiones). Las fusiones empresariales deben implementarse técnicamente. Se deben sustituir los sistemas heredados y las operaciones empresariales se acelerarán posteriormente mediante el cambio a herramientas modernas basadas en la nube.

Permitir que los empleados trabajen de forma fiable desde cualquier lugar, independientemente del dispositivo que utilicen, manteniendo un buen rendimiento constante es el objetivo de la optimización de la Experiencia del usuario. Un alto nivel de seguridad no puede estar reñido con la productividad en el trabajo.

5 FORTALECER EL CRECIMIENTO EMPRESARIAL SEGURO, CON **CONFIANZA CERO**

Mediante la implementación de una estrategia de confianza cero a través de una plataforma de seguridad basada en la nube, los líderes empresariales desean fortalecer el poder innovador de su empresa, garantizar su crecimiento y rentabilidad y lograr una monetización rápida de las actividades de fusiones y adquisiciones e I+D.

Aprovechar el poder de la innovación

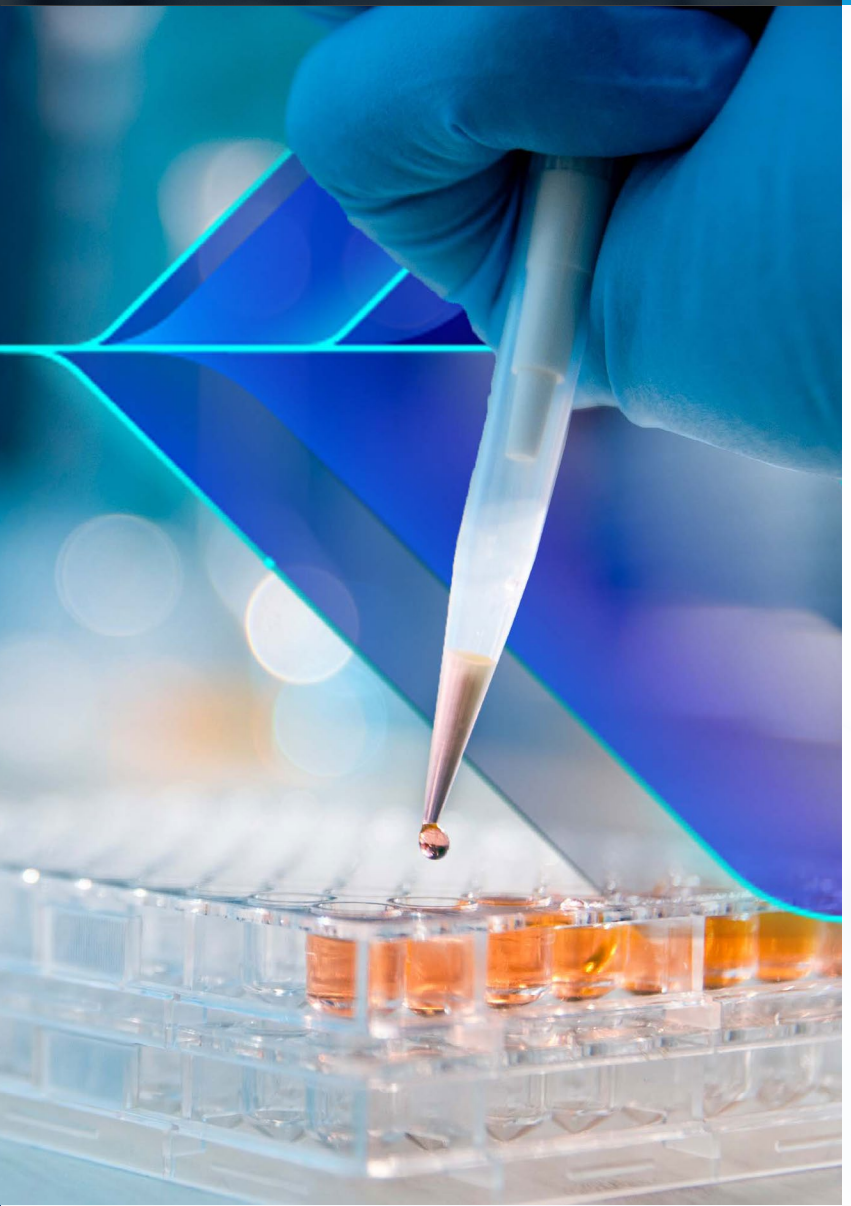
Para seguir siendo competitivos en este entorno de mercado altamente competitivo del sector farmacéutico, son esenciales la capacidad innovadora, la eficiencia y confiabilidad de los procesos y un corto tiempo de comercialización. La elección correcta y el uso de las tecnologías adecuadas ayudan a los responsables de las empresas a alcanzar estos objetivos estratégicos. Se centra la atención en tres áreas secundarias: crecimiento y desarrollo, reducción del riesgo empresarial y excelencia operativa.

Crecimiento y desarrollo significa que las actividades de fusiones y adquisiciones se aceleran y, por lo tanto, se monetizan rápidamente, y se reduce el tiempo de comercialización (por ejemplo, el desarrollo de vacunas). Una infraestructura de TI moderna ayuda a explotar el potencial de innovación de la mejor manera posible y a mejorar la cooperación con los socios en todas las áreas. También respalda la implementación de nuevos modelos de ingresos y cadenas de suministro adaptadas.

Reducción del riesgo empresarial significa minimizar los riesgos de seguridad con una tendencia simultánea al trabajo a distancia, garantizando así la protección de los activos más valiosos. Esto se debe a que el aumento de los modelos de oficina en casa, la colaboración con partes externas y la integración en el curso de las fusiones y adquisiciones han aumentado visiblemente el riesgo de posibles ciberamenazas.

Excelencia operativa significa optimizar la productividad y la eficiencia para acelerar la innovación. La monetización rápida y el menor tiempo posible hasta llegar a la comercialización para los nuevos productos farmacéuticos también son factores críticos.

6 LOS PRINCIPALES BENEFICIOS CON ZSCALER



Con Zscaler encabezando la transformación digital segura en el sector farmacéutico, las empresas de este sector cuentan con un experto con abundante experiencia a su lado. Al utilizar la mayor plataforma de intercambio de confianza cero del mundo con su arquitectura de proxy de confianza cero, las empresas farmacéuticas pueden reforzar su poder de innovación. Esto las sitúa en posición de abordar el proyecto de "transformación digital" con el mayor valor añadido y minimizando los riesgos.

- **Las arquitecturas**: Existentes se superponen para acelerar la transformación digital y brindar servicios eficientes, seguros, centrados en el cliente y escalables.
- **Eficiencia**: Una informática sencilla reduce la complejidad y los costes.
- **Seguridad**: La mejora de la capacidad de recuperación y una mejor posición general de seguridad gracias a la supervisión centralizada e interdepartamental evita la pérdida de datos y minimiza los riesgos de seguridad.
- **Enfoque al cliente**: Un enfoque de seguridad de confianza cero admite entornos de trabajo desde cualquier lugar, aumenta la capacidad, reduce la latencia y crea una experiencia de usuario consistente.
- **Escalable**: Es una plataforma moderna y ágil que sustenta la innovación digital, acelera la transformación digital y genera capacidad para el crecimiento.
- **Actividades de fusiones y adquisiciones**: Esta suponen un reto para los equipos de red y seguridad responsables de garantizar la conectividad de los usuarios a las aplicaciones internas y la seguridad de los datos sensibles. Una plataforma de confianza cero proporciona seguridad y una monetización más rápida de las fusiones y adquisiciones.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.es