Zscaler Private Access (ZPA) para RISE con SAP

La primera y única solución de acceso Zero Trust del sector disponible de manera nativa en RISE con SAP

Resumen de la solución

El desafío del mercado

Los productos SAP ayudan a las empresas a gestionar sus procesos principales, como las finanzas, la contabilidad, las ventas, la cadena de suministro, las compras, la fabricación y los recursos humanos. Están diseñados para centralizar los datos y agilizar la información empresarial y la gestión de procesos en todos los departamentos, lo que permite a las organizaciones funcionar sin problemas.

Debido a sus funciones críticas para el negocio, las soluciones de SAP contienen datos comerciales confidenciales, incluida propiedad intelectual, registros financieros, datos personales e información de la cadena de suministro. Como resultado, estos sistemas son objetivos de gran valor para los ciberdelincuentes, los grupos de espionaje y los hacktivistas que buscan cifrar datos, extorsionar con pedidos de rescate e interrumpir las operaciones empresariales.

Un sistema SAP comprometido puede detener por completo las operaciones empresariales y obstaculizar la producción, la elaboración de informes financieros y la prestación de servicios, causando importantes pérdidas financieras, daños a la reputación o multas reglamentarias.

Tradicionalmente, se ha accedido a los sistemas SAP desde la oficina a través de redes estándar de conmutación de etiquetas multiprotocolo (MPLS). Pero con el auge de la adopción de la nube y el trabajo híbrido, la mayoría de las organizaciones permiten ahora el acceso remoto de los usuarios a estos sistemas a través de redes privadas virtuales (VPN).

Lamentablemente, los enfoques de acceso centrados en la red tradicionales son inseguros por diseño. Conocidos por aumentar masivamente la superficie de ataque y hacer que las aplicaciones y los datos sean susceptibles de sufrir intrusiones y violaciones, no son confiables ni aptos para garantizar una conectividad a prueba de fallas entre los usuarios de SAP y los sistemas SAP críticos para la empresa.

En la actualidad, las organizaciones que funcionan con sistemas SAP locales se enfrentan a una fecha límite inquietante. Está previsto que SAP ECC finalice su vida útil en 2027. Sobra decir que una migración cuidadosamente planificada de los sistemas SAP heredados a S/4HANA basado en la nube, incluyendo RISE con SAP, se está convirtiendo rápidamente en una prioridad para los líderes empresariales y de TI.

Para llevar a cabo una migración SAP segura y realizar un proceso de transformación empresarial, las organizaciones también deben considerar la modernización del acceso mediante la adopción de tecnologías de acceso seguro alternativas basadas en una arquitectura Zero Trust directa de usuario a aplicación y, por lo tanto, más eficaces para reducir los riesgos de seguridad, eliminar la complejidad operativa y suprimir los cuellos de botella en el rendimiento asociados a las VPN centradas en la red.

Zscaler Private Access (ZPA) para RISE con SAP

Zscaler Private Access™ (ZPA) puede optimizar el acceso a todas las aplicaciones de SAP, sin importar dónde se encuentren en su proceso de migración. Como parte de una nueva integración innovadora, SAP nos ha certificado como el único proveedor de ciberseguridad que integra de manera nativa nuestro servicio de acceso Zero Trust dentro de RISE con SAP.

Lo hemos conseguido aprovisionando ZPA de manera nativa dentro del entorno de nube RISE de un cliente de SAP para ofrecer una conectividad Zero Trust totalmente conforme. Alojado en SAP, el servicio ZPA integrado de manera nativa crea conexiones salientes al Zscaler Zero Trust Exchange™ ofreciendo acceso directo de usuario a aplicación tanto a empleados como a socios.

ZPA sigue un modelo único de conectividad de adentro hacia afuera, negociando dinámicamente una conexión exclusiva basada en políticas entre el usuario y la aplicación SAP. Además, las capacidades integradas de protección de datos de Zero Trust Exchange ayudan a los clientes de RISE con SAP a proteger los datos críticos de SAP garantizando el cumplimiento de diversas normas reguladoras como RGPD, HIPAA y otras.

Puntos clave

- **Acceso optimizado durante la migración a la nube a RISE con SAP:** ZPA proporciona acceso de usuario uniforme a las aplicaciones de SAP durante la migración a RISE con SAP.
- **Acceso remoto seguro sin VPN:** la integración ofrece conectividad SAP segura a empleados y socios desde cualquier ubicación, sin necesidad de una VPN.
- **Segmentación de usuario a aplicación:** genera automática-mente recomendaciones de segmentación de aplicaciones según los patrones de acceso de los usuarios y aplica políticas granulares de acceso de usuario a aplicación basadas en Zero Trust.
- **Inspección completa de tráfico en línea y prevención de pérdida de datos:** realiza una inspección de seguridad en línea de toda la carga útil de la aplicación SAP para identificar y bloquear amenazas conocidas y desconocidas, al tiempo que protege los datos críticos de la empresa.

Para comprender mejor los matices de esta integración, es importante profundizar en los aspectos únicos, incluido el aprendizaje sobre RISE con SAP.

RISE con SAP: una breve introducción

RISE con SAP es el paquete de transformación empresarial como servicio (BTaaS) basado en suscripción de SAP que simplifica la migración de soluciones ERP locales heredadas a soluciones ERP basadas en la nube. Además de un soporte de migración totalmente gestionado, RISE con SAP ofrece una infraestructura completa, soporte técnico y herramientas de transformación a sus clientes empresariales.

Con RISE, las organizaciones migran SAP ECC a SAP S/4HANA Private Cloud Edition (PCE), una solución ERP en la nube alojada en hiperescaladores como AWS, GCP o Azure, con servicios de gestión técnica de SAP incorporados en la suscripción. Los clientes de RISE se benefician de infraestructura y servicios gestionados por SAP al tiempo que mantienen el control sobre las configuraciones y actualizaciones de ERP.

Diferenciación única de Zscaler con RISE con SAP

Zscaler ofrece un valor como ninguna otra solución de acceso remoto seguro, específicamente para las migraciones RISE con SAP mediante el aprovisionamiento nativo de conectores de aplicaciones ZPA directamente dentro de la nube RISE.

El innovador enfoque de aprovisionamiento directo de acceso Zero Trust dentro de RISE con SAP permite conexiones seguras de usuario a aplicación basadas en políticas sin dependencias subyacentes a nivel de sistema operativo ni necesidad de virtualización de hardware.

El servicio ZPA para RISE con SAP puede escalarse dinámicamente para satisfacer la demanda fluctuante de una plantilla híbrida en crecimiento o en disminución. Al beneficiarse de herramientas de orquestación como Kubernetes, el aprovisionamiento nativo en la nube de ZPA beneficia a las organizaciones con una utilización más eficiente de los recursos, autorreparación y menos gastos generales.

ZPA ofrece un acceso Zero Trust a cualquier aplicación SAP, sin depender de los enfoques de acceso a la red heredados. Funciona a la perfección en todas las migraciones a S/4HANA, y de manera exclusiva para RISE con SAP.

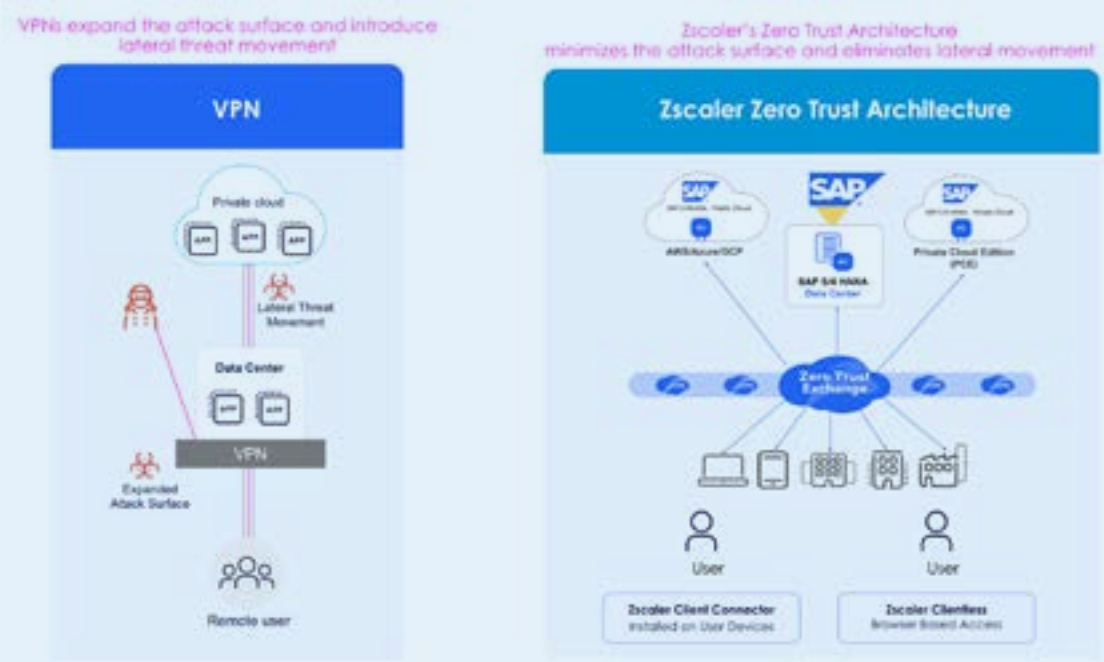

Figura 1: VPN frente a la arquitectura Zero Trust de Zscaler

Acceso remoto optimizado y seguro para empleados y socios

Con el auge del trabajo híbrido, los empleados y usuarios necesitan acceso a las aplicaciones de SAP desde cualquier lugar. Por lo tanto, garantizar conexiones de usuario seguras y uniformes a sus sistemas SAP críticos para el negocio es más importante que nunca, especialmente cuando está planificando una migración de su inversión SAP heredada a la nube RISE con SAP o se encuentra activamente en medio de su proceso de migración.

Las organizaciones a menudo dependen de enfoques de acceso a red heredados para garantizar la conectividad. Sin embargo, los enfoques heredados son intrínsecamente inseguros por diseño y conceden una confianza excesiva a los usuarios, permitiéndoles un acceso sin restricciones a la información confidencial de las aplicaciones SAP en toda la red. Al mismo tiempo, al dirigir el tráfico hacia el centro de datos, tienden a crear latencia en las conexiones, lo que repercute negativamente en la experiencia del usuario.

La ZPA es una alternativa más granular y segura a los enfoques de acceso a la red heredados, como las VPN, porque solo proporciona acceso a aplicaciones SAP específicas basándose en la identidad del usuario y la seguridad del dispositivo, adhiriéndose al principio Zero Trust de “nunca confiar, siempre verificar”.

Siguiendo un modelo único de conectividad de dentro hacia fuera, ZPA intermedia conexiones seguras basadas en políticas directamente entre los usuarios SAP autorizados y aplicaciones SAP específicas. Además, las capacidades de protección de datos Zero Trust Exchange ofrecen una visibilidad y un control exhaustivos de la información confidencial, desempeñando un papel fundamental en la seguridad de los datos críticos dentro de las aplicaciones SAP y garantizando el cumplimiento de normas reglamentarias como RGPD, HIPAA y otras.

ZPA para SAP funciona a la perfección en S/4HANA, y de manera única también para RISE con SAP, con el servicio ZPA de SAP implementado de manera nativa.

Acceso Zero Trust basado en el cliente para empleados

Zscaler ofrece la capacidad única de aprovisionar conectores de aplicaciones ZPA directamente dentro de RISE con entornos SAP.

Los ZPA App Connectors son dispositivos virtuales ligeros que proporcionan una conexión saliente segura desde la red del cliente de RISE con SAP a la nube de Zscaler. Al servir de puerta de enlace segura, permiten el acceso a una aplicación SAP estableciendo una conexión TLS saliente cifrada con la plataforma Zero Trust Exchange.

Esto garantiza que no se requieran accesos entrantes ni IP públicas para conectar a un usuario a la aplicación SAP. La naturaleza saliente de la conexión es una característica de seguridad crítica que minimiza la exposición a amenazas potenciales. Una vez establecida la conexión TLS, realiza un microtunelado de todo el tráfico entre la aplicación SAP y el usuario, garantizando que la transacción sea segura y privada.

Por el contrario, cuando un usuario solicita acceso a una aplicación SAP, Zscaler Client Connector (ZCC), un agente ligero instalado en el dispositivo del usuario, intercepta y envía la solicitud por un microtúnel al Zero Trust Exchange. El Zero Trust Exchange evalúa la solicitud del usuario, verificando su identidad y la postura del dispositivo según RISE con las políticas de seguridad del cliente SAP. Tras la validación, indica a los App Connectors que establezcan una conexión segura con la aplicación SAP.

Al enrutar el tráfico solo entre el usuario específico y la aplicación, la ZPA impide el acceso directo y no seguro. Al aplicar la microsegmentación de usuario a aplicación, aísla el acceso de cada usuario de los demás, adhiriéndose a un modelo de seguridad Zero Trust. Si varios usuarios acceden a la misma aplicación SAP, su tráfico se segmenta en microtúneles cifrados individuales. Esto impide el acceso no autorizado y el movimiento lateral a través de la red: incluso si una conexión se ve comprometida, no puede afectar a otros usuarios o aplicaciones SAP.

Acceso Zero Trust basado en navegador para socios externos

ZPA también ofrece acceso basado en navegador a aplicaciones SAP para usuarios externos, contratistas o usuarios de SAP que puedan estar usando dispositivos no administrados para obtener acceso. En tales escenarios, la capacidad de acceso basada en navegador de ZPA conecta de manera segura a un usuario con la aplicación SAP específica solicitada, sin necesidad de instalar el agente ZCC en el dispositivo del usuario.

El acceso a una aplicación SAP mediante la opción basada en navegador funciona de la siguiente manera:

1. **Autenticación del usuario:** El usuario navega hasta una URL específica asociada a la aplicación SAP. ZPA redirige al usuario al proveedor de identidades (IdP) de su organización para que se autentique.
2. **Aplicación de políticas:** tras una autenticación exitosa, ZPA aplica políticas de acceso basadas en la identidad y el contexto del usuario, garantizando que solo los usuarios autorizados puedan acceder a la aplicación SAP.
3. **Acceso a la aplicación:** ZPA establece una conexión segura desde adentro hacia afuera entre el navegador del usuario y la aplicación SAP solicitada a través del App Connector implementado de manera nativa en S/4HANA. Este método garantiza que las aplicaciones permanezcan ocultas a Internet, reduciendo la superficie de ataque.

Al conectar a los usuarios directamente a una aplicación SAP específica en lugar de hacerlo a través de la red, el acceso basado en navegador de ZPA mejora la seguridad y minimiza el riesgo de movimiento lateral dentro de la red. Este enfoque proporciona a los usuarios un acceso seguro y sin inconvenientes a aplicaciones críticas para el negocio desde cualquier ubicación.

Evite que usuarios internos y externos filtren datos confidenciales de SAP

Las funciones integradas de protección de datos Zero Trust Exchange ayudan a los clientes de RISE con SAP a proteger los datos críticos de SAP frente a la exfiltración, garantizando el cumplimiento de diversas normas reglamentarias como RGPD, HIPAA y otras.

Además, Cloud Browser Isolation (CBI) de Zscaler permite a terceros acceder de manera segura a las aplicaciones SAP a través de un navegador virtual alojado en la nube, transmitiendo solo contenido visual seguro a sus dispositivos. Aplica políticas Zero Trust con acceso de solo lectura, impide las descargas/cargas, oculta los datos confidenciales y garantiza que ningún código se ejecute en dispositivos no gestionados. Esto permite un acceso seguro y controlado sin exponer la red y evitando el riesgo de filtraciones de datos.

Factores clave generadores de valor

El uso de soluciones de acceso a la red heredadas para permitir el acceso remoto a las aplicaciones SAP presenta desafíos en términos de aumento masivo de la superficie de ataque, lo que hace que las aplicaciones críticas para el negocio sean muy susceptibles de sufrir violaciones y degrada la experiencia del usuario con un rendimiento deficiente y problemas de latencia. Por el contrario, el ZPA ofrece múltiples beneficios a las organizaciones que utilizan sistemas SAP.

- **Los usuarios de SAP, ya sean empleados o socios,** disfrutan de una conexión rápida, segura y confiable con cualquier aplicación SAP, sin importar en qué etapa se encuentre en su proceso de migración.
- **A las aplicaciones SAP** a través de conexiones de adentro hacia afuera, lo que elimina la exposición a Internet pública.
- **Las aplicaciones de SAP** están ocultas e inaccesibles, lo que minimiza el radio de alcance de los ataques o el movimiento lateral.
- **Los clientes de RISE con SAP** ya no necesitan lidiar con el costo y la complejidad de invertir en tecnologías de acceso a red heredadas.

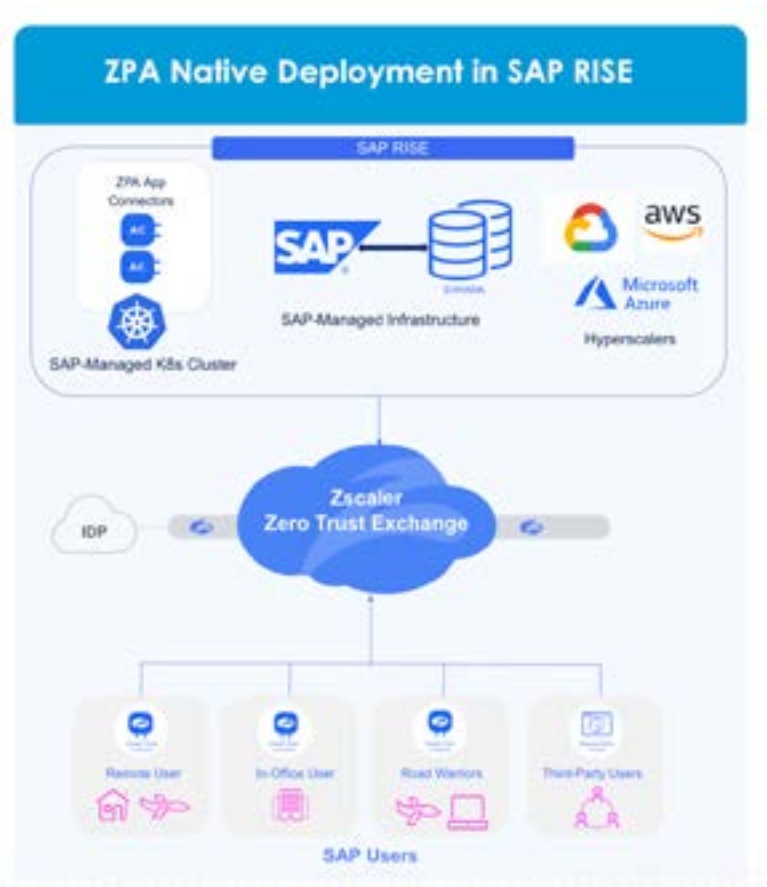

Figura 2. ZPA se implementa de manera nativa en RISE con entornos SAP.

Integración nativa de ZPA dentro de RISE con SAP

La gestión de servidores y redes está pasando de la virtualización (que suele utilizar máquinas virtuales [VM]) a la contenedorización (que utiliza contenedores ligeros). Se prefieren los contenedores por su portabilidad, mejor seguridad, gestión sencilla y mayor rapidez en la entrega de aplicaciones en comparación con las máquinas virtuales.

Kubernetes es una de las plataformas más populares para la orquestación de contenedores. Permite ejecutar aplicaciones dentro de un entorno aislado sin dependencias paralelas. La ERP en la nube de SAP es nativa de la nube y está orquestada por Kubernetes.

Para permitir una integración perfecta con la ERP nativa en la nube de SAP, el servicio ZPA está diseñado para ejecutarse de manera nativa dentro del clúster Kubernetes gestionado por SAP del entorno de nube privada del cliente de RISE. Al alcanzar este hito de implementación, Zscaler ofrece ahora a los clientes de SAP un acceso Zero Trust totalmente conforme desde dentro de sus entornos RISE nativos de nube a medida.

App Connectors de ZPA alojados en SAP en RISE con SAP

Clústeres Kubernetes (K8s) gestionados por SAP específicos para clientes de RISE: Los clientes de RISE disponen de un clúster K8s gestionado por SAP dedicado y adaptado a sus cargas de trabajo de aplicaciones SAP y requisitos de seguridad exclusivos. Estos clientes tienen ahora la opción de aprovisionar ZPA App Connectors dentro de su clúster K8s gestionado por SAP, lo que permite una conectividad Zero Trust totalmente compatible con las aplicaciones SAP que se ejecutan en la nube de RISE con SAP.

Infraestructura en la nube gestionada por SAP: SAP gestiona por completo la pila de infraestructura subyacente en la nube en nombre de los clientes de RISE, incluidos los clústeres Kubernetes, el sistema operativo anfitrión y otros componentes, y realiza servicios de mantenimiento técnico que garantizan una alta disponibilidad, tiempo de actividad, resiliencia y recuperación automatizada en caso de desastre.

RISE con usuario ZPA controlado por el cliente SAP: Aunque los clientes de RISE descargan la responsabilidad de la gestión de la infraestructura a SAP, siguen teniendo el control total de su inquilino ZPA a través del portal Zscaler Cloud Admin, desde el que pueden configurar la gestión de usuarios y las políticas de acceso seguro y establecer umbrales de seguridad basados en los requisitos de seguridad exclusivos de su organización.

Modelo de responsabilidad compartida del servicio Zscaler ZPA–CS: Para utilizar el servicio Zscaler ZPA–CS, los clientes actuales de RISE con SAP deben solicitar primero el servicio a SAP y, a continuación, las licencias y la clave de aprovisionamiento de los ZPA App Connectors directamente a Zscaler.

- El administrador de ZPA del cliente de RISE proporciona la clave de aprovisionamiento a SAP, que se encarga de instalar la clave de aprovisionamiento de App Connector en los entornos ERP en la nube S/4HANA PCE del cliente de RISE.
- Tras la instalación, SAP se encarga de la gestión y el mantenimiento subyacentes de los ZPA App Connectors, mientras que el administrador ZPA del cliente RISE se encarga de mantener el control total sobre el usuario de ZPA.

Factores clave generadores de valor

El uso de máquinas virtuales para implementar servicios como el acceso Zero Trust para la conectividad segura de aplicaciones SAP presenta desafíos como una mayor sobrecarga operativa, una escalabilidad más lenta y un aprovisionamiento complejo. A diferencia de las máquinas virtuales, la implementación nativa de la nube alojada en SAP de ZPA ofrece:

Portabilidad y rendimiento: Los ZPA App Connectors alojados en SAP son independientes del sistema operativo y del hipervisor. Pueden ejecutarse de manera uniforme en distintos entornos de nube sin dependencias subyacentes a nivel de sistema operativo ni necesidad de virtualización de hardware, lo que proporciona tiempos de respuesta más rápidos para el servicio de ZTNA.

Escalabilidad y optimización: Los ZPA App Connectors alojados en SAP pueden ponerse en marcha en cuestión de segundos y escalarse rápida y dinámicamente para satisfacer una demanda fluctuante. Son fáciles de aprovisionar y simplifican la conectividad con ZTNA.

Utilización de recursos y costos: Los ZPA App Connectors alojados en SAP son ligeros y se benefician de herramientas de orquestación como Kubernetes, ofreciendo una utilización más eficiente de los recursos, autorreparación y menores gastos generales.

Ascenso con SAP y Zscaler: Mejores beneficios juntos

- **Acceso optimizado durante la migración a la nube a RISE con SAP:** ZPA proporciona acceso de usuario uniforme a las aplicaciones de SAP durante la migración a RISE con SAP.
- **Acceso remoto seguro sin VPN:** la integración ofrece conectividad SAP segura a empleados y socios desde cualquier ubicación, sin necesidad de una VPN.
- **Aprovisionamiento nativo de ZPA App Connector:** Los ZPA App Connectors se aprovisionan dentro de los entornos de clientes RISE con SAP (S/4HANA – PCE). La implementación nativa en la nube simplifica el inicio de conexiones seguras salientes al Zero Trust Exchange, ofreciendo una utilización más eficiente de los recursos, autorreparación y menor sobrecarga.
- **Acuerdos de nivel de servicio (SLA) uniformes:** Las cargas de trabajo de ZPA App Connector se ejecutan junto con las cargas de trabajo de S/4HANA (PCE) y se ajustan a los mismos SLA en términos de disponibilidad, rendimiento y tiempos de respuesta.
- **Minimización de la superficie de ataque:** ZPA aplica Zero Trust para restringir el acceso de los usuarios solo a aplicaciones SAP específicas en lugar de proporcionar conectividad a toda la red, lo que reduce significativamente la superficie de ataque.
- **Reducción del riesgo lateral:** La segmentación de usuario a aplicación y la conectividad basada en el acceso con privilegios mínimos garantizan que el acceso a la aplicación se conceda de manera individual desde el usuario autorizado a la aplicación designada, lo que impide el movimiento lateral.
- **Protección de datos y cumplimiento normativo:** Las capacidades de protección de datos unificadas de Zscaler ofrecen visibilidad y control integrales sobre la información confidencial en las aplicaciones de SAP, lo que permite a las organizaciones supervisar y proteger los datos de manera efectiva y garantizar el cumplimiento de regulaciones como RGPD, HIPAA y otras.
- **Experiencia de usuario mejorada:** La implementación nativa de ZPA App Connectors garantiza que los usuarios permanezcan ajenos a cualquier migración subyacente. La experiencia de conectividad usuario–aplicación se mantiene uniforme a través de diferentes dispositivos y geolocalizaciones, sin interrupciones durante la transición de aplicaciones SAP heredadas a entornos en la nube.
- **Rendimiento mejorado:** Los usuarios de SAP obtienen acceso rápido y directo a aplicaciones SAP críticas para el negocio, desde más de 160 puntos de presencia en todo el mundo, lo que garantiza la ruta más corta de aplicación de la seguridad y un acceso confiable.
- **Continuidad comercial y alta disponibilidad:** Las geolocalizaciones con mala conectividad a Internet se benefician de ZPA Private Service Edge, que almacena en caché las políticas de acceso durante semanas, lo que permite una conectividad segura y continuidad comercial incluso en caso de que se pierda la conectividad a Internet.

Optimice y reduzca los riesgos del acceso con Zero Trust mientras migra a RISE con SAP

A medida que más y más organizaciones planifican su proceso de migración de las implementaciones SAP ECC heredadas a RISE con SAP (S/4HANA PCE), Zscaler une fuerzas con SAP como socio líder para agilizar el acceso y asegurar la transformación empresarial.

Zscaler Private Access es una potente alternativa a las soluciones de acceso a la red heredadas, que ofrece un acceso Zero Trust rápido, confiable y seguro a las aplicaciones SAP, independientemente de dónde se encuentren los usuarios y las aplicaciones.

Sus capacidades únicas reducen drásticamente la superficie de ataque, garantizando experiencias de usuario excepcionales en cualquier lugar y eliminando la necesidad de invertir en VPN centradas en el usuario para acceder a las aplicaciones de SAP. Además, las capacidades de protección de datos unificadas de la plataforma Zero Trust Exchange brindan visibilidad y control sobre la información confidencial en las aplicaciones de SAP, lo que permite a las organizaciones proteger eficazmente los datos y garantizar el cumplimiento normativo.

Obtenga más información sobre ZPA para RISE con SAP >

Acerca de SAP
Como líder mundial en aplicaciones empresariales e IA empresarial, SAP (NYSE:SAP) se sitúa en el nexo de unión entre el negocio y la tecnología. Durante más de 50 años, las organizaciones han confiado en SAP para sacar lo mejor de sí mismas uniendo las operaciones críticas para el negocio que abarcan las finanzas, las compras, los RR.HH., la cadena de suministro y la experiencia del cliente. Para obtener más información, visite sap.com

zscaler™ | Experience your world, secured.™

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134 zscaler.com/mx