Zscaler Private Access (ZPA) for RISE with SAP

The industry's first and only zero trust access solution natively available within RISE with SAP

Solution Brief

The Market Challenge

SAP products help businesses manage their core processes, such as finance, accounting, sales, supply chain, procurement, manufacturing, and human resources. They are designed to centralize data and streamline business information and process management across departments, enabling organizations to function smoothly.

Due to their business critical functions, SAP solutions contain sensitive business data, including intellectual property, financial records, personal data, and supply chain information. As a result, these systems are high-value targets for cybercriminals, espionage groups, and hacktivists seeking to encrypt data, extort ransoms, and disrupt business operations.

A compromised SAP system can completely halt business operations and hinder production, financial reporting, and service delivery, causing significant financial loss, reputational damage, or regulatory fines.

Traditionally, SAP systems have been accessed from within the office via standard multiprotocol label switching (MPLS) networks. But with the rise of cloud adoption and hybrid work, most organizations now enable remote user access to these systems via virtual private networks (VPNs).

Unfortunately, legacy network-centric access approaches are insecure by design. Known to massively increase the attack surface and make applications and data susceptible to break-ins and breaches, they are unreliable and unfit for ensuring failsafe connectivity between SAP users and business-critical SAP systems.

Today, organizations that run on on-premises SAP systems are up against a foreboding deadline. SAP ECC is due for end-of-life by 2027. Needless to say, a carefully planned migration from legacy SAP systems to cloud-based S/4HANA, including RISE with SAP, is fast becoming a priority for IT and business leaders.

To actualize a secure SAP migration and business transformation journey, organizations must also consider modernizing access by adopting alternate secure access technologies built on a direct user-to-app zero trust architecture, and therefore more effective in reducing security risks, removing operational complexity, and eliminating the performance bottlenecks associated with network-centric VPNs.

Zscaler Private Access (ZPA) for RISE with SAP

Zscaler Private Access™ (ZPA) can streamline access to all SAP applications, no matter where they are in their migration journey. As part of a groundbreaking new integration, we've been certified by SAP as the only cybersecurity vendor to natively integrate our zero trust access service within RISE with SAP.

We've achieved this by provisioning ZPA natively inside a SAP customer's RISE cloud environment to deliver fully compliant zero trust connectivity. Hosted by SAP, the natively integrated ZPA service creates outbound connections to the Zscaler Zero Trust Exchange™ delivering direct user-to-app access to both employees and partners.

ZPA follows a unique inside-out connectivity model, dynamically brokering an exclusive policy-based connection between the user and the SAP application. Additionally, the integrated data protection capabilities of the Zero Trust Exchange help RISE with SAP customers protect critical SAP data ensuring compliance with various regulatory standards like GDPR, HIPAA, and others.

Key Highlights

- **Streamlined access during cloud migration to RISE with SAP:** ZPA provides consistent user access to SAP apps during migration to RISE with SAP.
- **Secure remote access without VPNs:** The integration delivers secure SAP connectivity to employees and partners from any location, without requiring a VPN.
- **User-to-app segmentation:** auto-generates app segmentation recommendations based on user access patterns and enforces granular user-to-app access policies based on zero trust.
- **Full inline traffic inspection and data loss prevention:** performs inline security inspection of the entire SAP application payload to identify and block known and unknown threats while protecting business-critical data.

To better understand the nuances of this integration, it's important to dive deep into the unique aspects, including learning about RISE with SAP.

RISE with SAP: A Brief Introduction

RISE with SAP is SAP's subscription-based business-transformation-as-a-service (BTaaS) package that simplifies migration from legacy on-premises ERP solutions to cloud-based ERP solutions. Besides fully managed migration support, RISE with SAP offers comprehensive infrastructure, technical support, and transformation tools to its enterprise customers.

Under RISE, organizations migrate SAP ECC to SAP S/4HANA Private Cloud Edition (PCE), a cloud ERP solution hosted on hyperscalers such as AWS, GCP, or Azure, with technical management services from SAP baked into the subscription. RISE customers benefit from SAP-managed infrastructure and services while maintaining control over ERP configurations and upgrades.

Zscaler's Unique Differentiation with RISE with SAP

Zscaler offers value unlike any other secure remote access solution, specifically for RISE with SAP migrations by natively provisioning ZPA Application Connectors directly inside the RISE cloud.

The innovative approach to directly provisioning zero trust access inside RISE with SAP enables secure policy-based user-to-app connections without underlying OS-level dependencies or the need for hardware virtualization.

The ZPA for RISE with SAP service can dynamically scale to meet fluctuating demand from a growing or shrinking hybrid workforce. Benefiting from orchestration tools like Kubernetes, the cloud native provisioning of ZPA benefits organizations with more efficient resource utilization, self-healing, and lower overhead.

ZPA offers zero trust access to any SAP application, without relying on legacy network access approaches. It works seamlessly across migrations to S/4HANA, and uniquely for RISE with SAP.

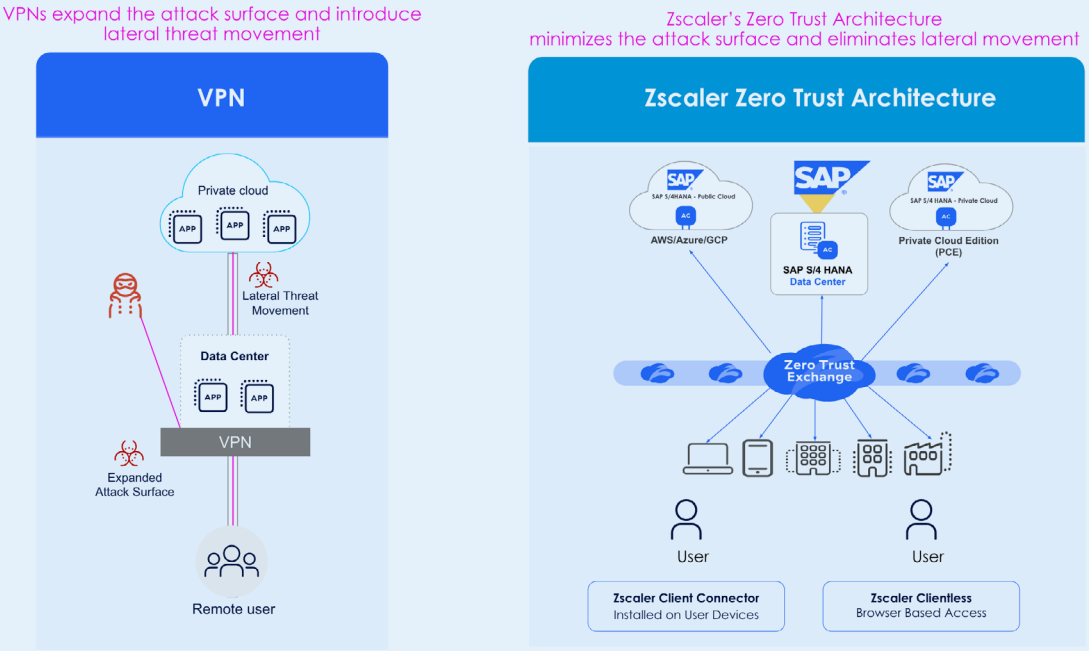

Figure 1: VPN versus Zscaler's Zero Trust Architecture

Streamlined and Secure Remote Access for Employees and Partners

With the rise of hybrid work, employees and users need access to SAP applications from anywhere. Therefore, ensuring secure and consistent user connections to your business-critical SAP systems is more critical than ever especially when you are planning a migration of your legacy SAP investment to the RISE with SAP cloud or are actively in the middle of your migration journey.

Organizations often rely on legacy network access approaches to ensure connectivity. However, legacy approaches are inherently insecure by design and grant excessive trust to users, allowing them unrestricted network-wide access to sensitive information within SAP applications. At the same time, by hairpinning traffic back to the data center, they tend to create latency in connections, negatively impacting the user experience.

ZPA is a more granular and secure alternative to legacy network access approaches like VPNs because it only provides access to specific SAP applications based on user identity and device security, adhering to the zero trust principle of "never trust, always verify."

Following a unique inside-out connectivity model, ZPA brokers secure policy-driven connections directly between authorized SAP users and specific SAP applications. Additionally, the data protection capabilities of the Zero Trust Exchange offer comprehensive visibility and control over sensitive information, playing a pivotal role in securing critical data within SAP applications and ensuring compliance with regulatory standards like GDPR, HIPAA, and others.

ZPA for SAP works seamlessly across S/4HANA, and uniquely also for RISE with SAP, with SAP's natively deployed ZPA service.

Client-Based Zero Trust Access for Employees

Zscaler offers the unique ability to provision ZPA Application Connectors directly inside RISE with SAP environments.

ZPA App Connectors are lightweight virtual appliances that provide a secure outbound connection from the RISE with SAP customer's network to the Zscaler cloud. Serving as a secure gateway, they enable access to a SAP application by establishing an encrypted outbound TLS connection to the Zero Trust Exchange platform.

This ensures that no inbound access or public IPs are required to connect a user to the SAP application. The outbound nature of the connection is a critical security feature that minimizes exposure to potential threats. Once the TLS connection is established, it microtunnels all traffic between the SAP application and the user, ensuring the transaction is secure and private.

Conversely, when a user requests access to a SAP application, Zscaler Client Connector (ZCC), a lightweight agent installed on the user's device, intercepts and microtunnels the request to the Zero Trust Exchange. The Zero Trust Exchange assesses the user's request, verifying the user's identity and device posture according to RISE with SAP customer's security policies. After validation, it directs the App Connectors to establish a secure connection to the SAP application.

By routing traffic only between the specific user and the application, ZPA prevents direct, unsecured access. Applying user-to-app microsegmentation, it isolates each user's access from others, adhering to a zero trust security model. If multiple users access the same SAP application, their traffic is segmented into individual encrypted microtunnels. This prevents unauthorized access and lateral movement across the network—even if one connection is compromised, it cannot affect other users or SAP applications.

Browser-Based Zero Trust Access for External Partners

ZPA also offers browser-based access to SAP applications for third-party users, contractors, or SAP users who may be using unmanaged devices to gain access. In such scenarios, ZPA's browser-based access capability securely connects a user to the specific requested SAP application, without requiring the ZCC agent to be installed on the user's device.

Accessing a SAP application using the browser-based option operates as follows:

1. **User authentication:** The user navigates to a specific URL associated with the SAP application. ZPA redirects the user to their organization's identity provider (IdP) for authentication.
2. **Policy enforcement:** Upon successful authentication, ZPA enforces access policies based on user identity and context, ensuring that only authorized users can access the SAP application.
3. **Application access:** ZPA establishes a secure, inside-out connection between the user's browser and the requested SAP application through the natively deployed App Connector in S/4HANA. This method ensures that applications remain hidden from the internet, reducing the attack surface.

By connecting users directly to a specific SAP application rather than via the network, ZPA's browser-based access enhances security and minimizes the risk of lateral movement within the network. This approach provides users with seamless and secure access to business critical applications from any location.

Prevent Internal and Third-Party Users from Exfiltrating Sensitive SAP Data

The integrated data protection capabilities of the Zero Trust Exchange help RISE with SAP customers protect critical SAP data from exfiltration ensuring compliance with various regulatory standards like GDPR, HIPAA, and others.

In addition to that, Zscaler's Cloud Browser Isolation (CBI) allows third parties to securely access SAP applications through a cloud-hosted virtual browser, streaming only safe visual content to their devices. It enforces Zero Trust policies with read-only access, prevents downloads/uploads, masks sensitive data, and ensures no code executes on unmanaged devices. This enables secure, controlled access without exposing the network or risking data leaks.

Key Value Drivers

Using legacy network access solutions to enable remote access to SAP applications presents challenges in terms of massively increasing the attack surface, making business-critical apps highly susceptible to breaches, and degrading the user experience with poor performance and latency issues. In contrast, the ZPA offers multiple benefits to organizations using SAP systems.

- **SAP users, whether employees or partners,** enjoy fast, secure, reliable to any SAP application, no matter where it is on its migration journey.
- **SAP applications** are securely accessed via inside-out connections, eliminating exposure to the public internet.
- **SAP applications** are hidden and unreachable, minimizing the blast radius of attacks or lateral movement.
- **RISE with SAP customers** no longer need to deal with the cost and complexity of investing in legacy network access technologies.

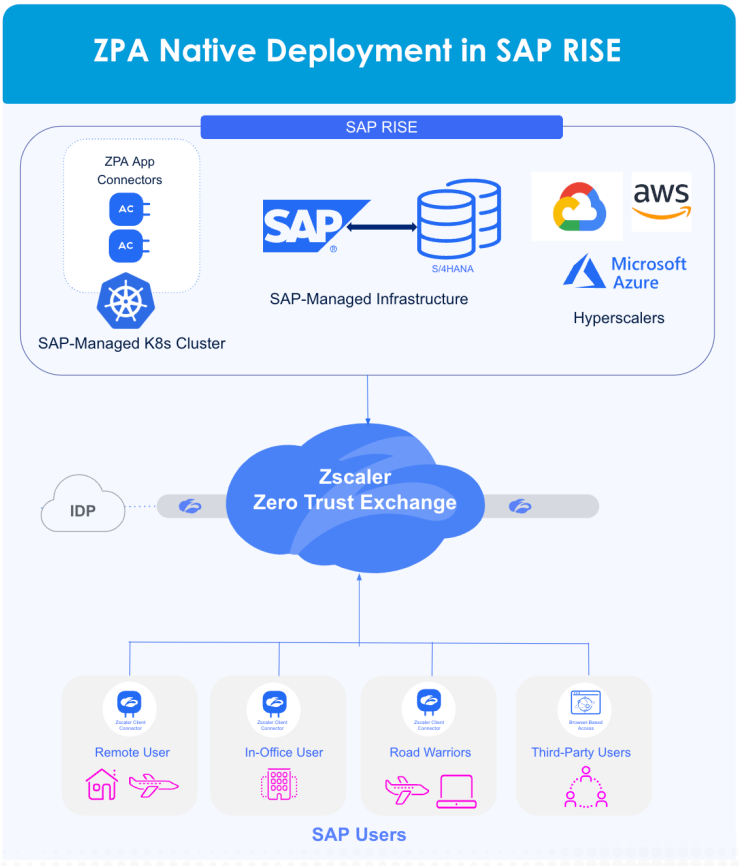

Figure 2. ZPA is natively deployed in RISE with SAP environments.

Native Integration of ZPA Within RISE with SAP

Server and networking management are moving from virtualization (which typically uses virtual machines [VMs]) to containerization (which uses lightweight containers). Containers are preferred for their portability, better security, simple management, and faster application delivery compared to VMs.

Kubernetes is one of the most popular platforms for container orchestration. It allows running applications inside of an isolated environment without parallel dependencies. SAP's cloud ERP is cloud native and orchestrated by Kubernetes.

As a way of enabling seamless integration with SAP's cloud native ERP, ZPA service is designed to run natively inside the SAP-managed Kubernetes cluster of the RISE customer's private cloud environment. By reaching this deployment milestone, Zscaler now delivers fully compliant zero trust access to SAP customers from within their bespoke cloud native RISE environments.

SAP-Hosted ZPA App Connectors in RISE with SAP

RISE customer-specific SAP-managed Kubernetes (K8s) clusters: RISE customers are provided a dedicated SAP-managed K8s cluster tailored to their unique SAP application workloads and security requirements. These customers now have the option to provision ZPA App Connectors within their SAP-managed K8s cluster, allowing for fully compliant zero trust connectivity to SAP applications running in the RISE with SAP cloud.

SAP-managed cloud infrastructure: SAP fully manages the underlying infrastructure stack in the cloud on behalf of RISE customers, including the Kubernetes clusters, host OS, and other components, and performs technical maintenance services that ensure high availability, uptime, resiliency, and automated disaster recovery.

RISE with SAP customer-controlled ZPA tenant: While RISE customers offload infrastructure management responsibility to SAP, they still have full control of their ZPA tenant via the Zscaler Cloud Admin Portal, from which they can configure user management and secure access policies and set security thresholds based on their organization's unique security requirements.

Zscaler ZPA-CS service shared responsibility model: To use the Zscaler ZPA-CS service, current RISE with SAP customers must first order the service from SAP, and then the licenses and provisioning key of the ZPA App Connectors directly from Zscaler.

- The RISE customer's ZPA admin provides the provisioning key to SAP, which is then responsible for installing the App Connector provisioning key in the RISE customer's S/4HANA PCE cloud ERP environments.
- After installation, SAP handles the underlying management and maintenance of the ZPA App Connectors, while the RISE customer's ZPA admin is in charge of maintaining full control over the ZPA tenant.

Key Value Drivers

Using VMs to deploy services like zero trust access for secure SAP application connectivity presents challenges such as higher operational overhead, slower scalability, and complex provisioning. As opposed to VMs, ZPA's SAP-hosted cloud native deployment offers:

Portability and performance: SAP-hosted ZPA App Connectors are OS- and hypervisor-agnostic. They can run consistently across different cloud environments without underlying OS-level dependencies or the need for hardware virtualization, providing faster response times for ZTNA service.

Scalability and optimization: SAP-hosted ZPA App Connectors can be spun up in seconds and quickly and dynamically scaled to meet fluctuating demand. They are easy to provision and simplify ZTNA connectivity.

Resource utilization and cost: SAP-hosted ZPA App Connectors are lightweight and benefit from orchestration tools like Kubernetes, offering more efficient resource utilization, self-healing, and lower overhead.

Rise with SAP and Zscaler: Better Together Benefits

- **Streamlined access during cloud migration to RISE with SAP:** ZPA provides consistent user access to SAP apps during migration to RISE with SAP.
- **Secure remote access without VPNs:** The integration delivers secure SAP connectivity to employees and partners from any location, without requiring a VPN.
- **Native ZPA App Connector provisioning:** ZPA App Connectors are provisioned inside RISE with SAP (S/4HANA – PCE) customer environments. The cloud native deployment simplifies the initiation of secure outbound connections to the Zero Trust Exchange, offering more efficient resource utilization, self-healing, and lower overhead.
- **Consistent service level agreements (SLAs):** ZPA App Connector workloads run alongside S/4HANA (PCE) workloads, and conform to the same SLAs in terms of availability, performance, and response times.
- **Attack surface minimization:** ZPA applies zero trust to restrict user access to only specific SAP applications rather than providing network-wide connectivity, significantly reducing the attack surface.
- **Lateral risk reduction:** User-to-app segmentation and connectivity based on least-privileged access ensures application access is granted on a one-to-one basis from the authorized user to the named application, preventing lateral movement.
- **Data protection and regulatory compliance:** Zscaler's unified data protection capabilities offer comprehensive visibility and control over sensitive information in SAP applications, enabling organizations to monitor and protect data effectively and ensuring compliance with regulations like GDPR, HIPAA, and others.
- **Enhanced user experience:** Native deployment of ZPA App Connectors ensure that users remain unaware of any underlying migration. The user-to-app connectivity experience remains consistent across different devices and geolocations, without disruptions during the transition of legacy SAP apps to cloud environments.
- **Improved performance:** SAP users get fast and direct access to business-critical SAP applications—delivered from 160+ points of presence worldwide—ensuring the shortest path of security enforcement and reliable access.
- **Business continuity and high availability:** Geolocations with poor internet connectivity benefit from ZPA Private Service Edge, which caches access policies for weeks, allowing for secure connectivity and business continuity even in the event of internet connectivity being lost.

Streamline and De-Risk Access with Zero Trust as You Migrate to RISE with SAP

As more and more organizations plan their migration journey from legacy SAP ECC deployments to RISE with SAP (S/4HANA PCE), Zscaler joins forces with SAP as a leading partner in streamlining access and securing business transformation.

Zscaler Private Access is a powerful alternative to legacy network access solutions, offering fast, reliable, and secure zero trust access to SAP applications, wherever users and apps are located.

Its unique capabilities drastically reduce the attack surface, ensuring exceptional user experiences anywhere and eliminating the need to invest in user-centric VPNs for access to SAP applications. Additionally, the unified data protection capabilities of the Zero Trust Exchange platform provide visibility and control over sensitive information in SAP applications, enabling organizations to effectively protect data and ensure regulatory compliance.

Learn more about ZPA for RISE with SAP >

About SAP
As a global leader in enterprise applications and business AI, SAP (NYSE:SAP) stands at the nexus of business and technology. For over 50 years, organizations have trusted SAP to bring out their best by uniting business-critical operations spanning finance, procurement, HR, supply chain, and customer experience. For more information, visit sap.com.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com