WHITE PAPER

RISE with SAP and Zscaler Private Access (ZPA)

A Zero Trust Approach to Business Transformation

Contents

Executive Summary

Introduction

In today's fast-paced cloud-first world, cyberattacks and data breaches are increasing both in frequency and complexity, posing significant challenges for organizations, their employees, and end customers. To strengthen defenses, many organizations are increasingly turning their focus to zero trust security strategies. A zero trust security approach ensures that digital ecosystems function securely by reducing exposure risks and mitigating the chances of disruptive attacks on critical business systems, enhancing business agility and accelerating cloud adoption.

Why SAP and Zero Trust?

SAP ERP solutions are vital for enterprises as they support core business operations. Given their importance, organizations must prioritize secure access to SAP solutions. Two main reasons drive the adoption of a zero trust security strategy among enterprises that use SAP:

- The evolution of enterprise networks into hybrid environments—consisting of on-premises resources, hosted data centers, and multicloud services—has led to blurred network perimeter boundaries.
- The increasing sophistication of threats, both internal and external, necessitates the removal of implicit trust within enterprise environments.

Hybrid deployment landscapes require consistent policy enforcement and software-defined networking for seamless security. Adopting a zero trust architecture ensures that every user-to-application transaction, flow of data, and the endpoint in use is secured regardless of location. This approach relies on robust security processes such as adaptive access control, continuous verification and monitoring, and inline encryption to eliminate trust assumptions and proactively mitigate risks.

Why Now?

Regulations, such as those issued by the National Institute of Standards and Technology (NIST) and the U.S. government, mandate that federal customers adopt zero trust access methods for applications. In response to these directives, organizations in highly regulated industries are aligning their operations to federal standards, driving the demand for zero trust solutions as a replacement for traditional VPN-based access to critical applications like SAP.

Additionally, SAP has set a deadline for customers to migrate from SAP ERP to SAP S/4HANA by 2027, placing added pressure on IT leaders such as CISOs and CIOs to allocate budgets for solutions that ensure smooth and secure transitions. With SAP applications now increasingly hosted in multi-cloud environments and operated across regions, many organizations are actively seeking cloud security solutions that improve user experiences and ensure operational continuity.

Why Is Zscaler the Right Partner?

Zscaler emerges as a leading partner for secure, zero trust access across all enterprise applications, including SAP systems. Zscaler Private Access (ZPA) is validated as a secure access service that supports RISE with SAP cloud deployments. With its proven success among enterprise customers, Zscaler's reputation as a trusted partner solidifies its role in facilitating zero trust connectivity. The ZPA-CS service presence in the SAP Store underscores its official partnership and expertise in securing SAP in the cloud.

Introduction

SAP products are software solutions that help businesses manage their core processes, such as finance, accounting, sales, supply chain, procurement, manufacturing, and human resources. These systems centralize business data and streamline critical operations, enabling organizations to function smoothly across departments.

Due to their business-critical functions, SAP systems often store regulated data such as personally identifiable information (PII), health records, and financial information, requiring compliance with laws like GDPR, HIPAA, and others. These systems are high-value targets for cybercriminals, espionage groups, and hacktivists seeking to encrypt data, extort ransom, and disrupt business operations.

Breaches in SAP systems can erode trust with customers and partners if sensitive information is compromised. A compromised system can disrupt operations, resulting in financial loss, regulatory fines, and reputational damage. Therefore, modernizing access to these systems with Zscaler's zero trust security framework is critical to ensuring secure access and data protection.

Embracing the Cloud ERP Future

Cloud ERP is increasingly recognized as the future of enterprise resource planning due to its scalability, flexibility, and cost efficiency. Unlike traditional on-prem systems, cloud ERP eliminates the need for extensive infrastructure and enables businesses to scale resources based on demand, making it ideal for dynamic, global operations. It also facilitates access to cutting-edge technologies like artificial intelligence, real-time analytics, and IoT, empowering organizations to innovate and make data-driven decisions more effectively. Additionally, cloud platforms offer advanced security, regular updates, and compliance features, providing a robust foundation for modern business needs without the burden of managing on-premises security and maintenance.

Why S/4HANA Migration is a Necessity

The migration to SAP's S/4HANA cloud ERP has become a necessity for organizations relying on SAP ECC, which will no longer be supported after 2027. S/4HANA offers significant advantages, such as faster performance through its in-memory database, enabling real-time analytics and agile operations. It also supports streamlined workflows, automation, and improved visibility across business processes, helping companies maintain a competitive edge. Moreover, S/4HANA is designed for seamless integration with cloud environments, aligning with the broader shift to digital transformation and ensuring compatibility with future technologies. Migration is not just about avoiding legacy system risks—it's about future-proofing business operations for sustained growth and innovation.

RISE with SAP is Key to Smooth Migration

RISE with SAP is a comprehensive business transformation package designed to simplify and accelerate the migration to SAP S/4HANA. It provides a unified, subscription-based offering that includes all the tools, services, and infrastructure needed to modernize core business processes. By bundling cloud hosting, SAP S/4HANA licenses, technical migration support, and process intelligence tools, RISE eliminates the complexity of managing multiple vendors and integrations, streamlining the migration journey. RISE with SAP also offers organizations access to industry best practices and business process intelligence tools that help identify inefficiencies and reimagine workflows during the migration process. Furthermore, its scalability and flexibility allow businesses to choose their preferred cloud environment—whether private, public, or hybrid—ensuring alignment with organizational needs. By minimizing disruptions, reducing risk, and enabling a tailored, end-to-end transformation approach, RISE with SAP is essential for organizations looking to future-proof their operations while transitioning seamlessly to SAP S/4HANA.

Migrating SAP Investments to the Cloud Requires Derisking Access

Before hybrid work became the norm, in-office employees were provided access to SAP systems via standard multiprotocol label switching (MPLS) networks. With the rise of hybrid work, today's SAP users—whether they are employees, contractors, or partners—need access to SAP systems from anywhere in the world.

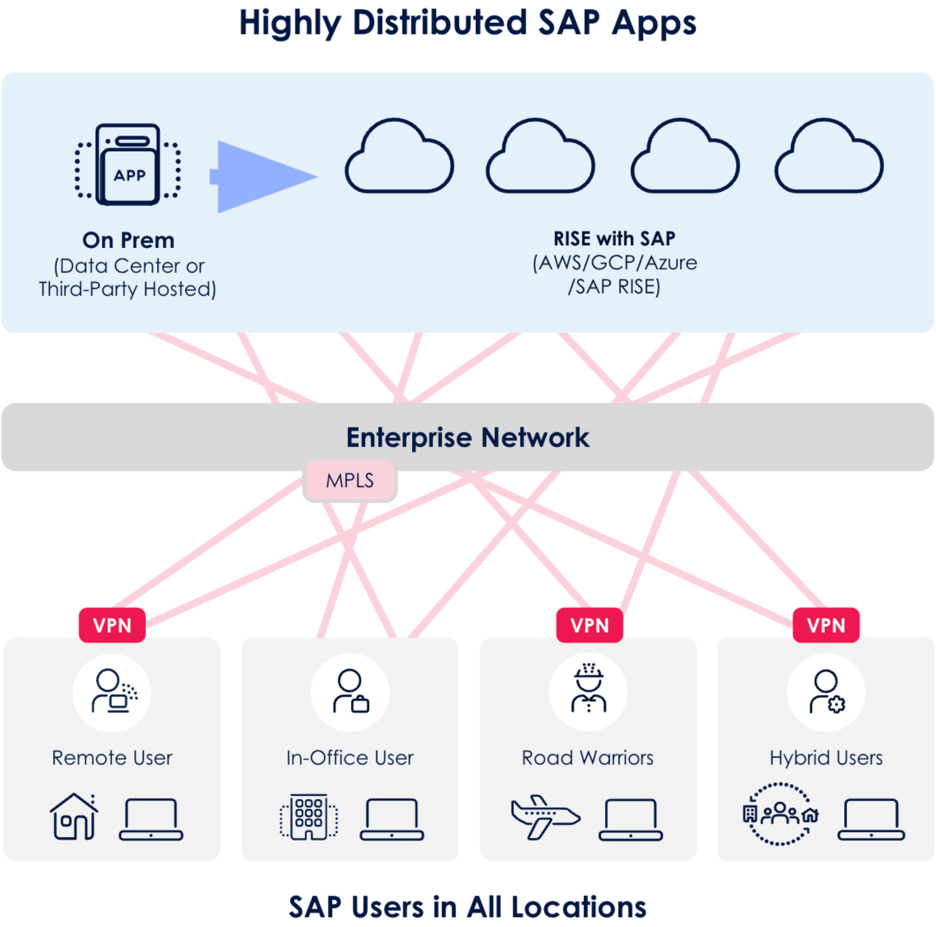

Figure 1: Highly distributed SAP users need access to SAP systems during migration to the cloud from anywhere. Legacy network access controls add complexity to the migration journey.

The Challenges of Legacy Network Access Solutions

Organizations have increasingly relied on legacy network access solutions such as Virtual Private Networks or VPNs to enable remote access. While these approaches suffice, organizations fail to realize that by opting them, they are inviting grave security and performance risks.

- **Complex VPN Dependencies:** Traditional VPNs require users to connect to the entire corporate network, increasing latency and introducing vulnerabilities.
- **Performance Bottlenecks:** Routing traffic through centralized data centers creates friction, impacting RISE with SAP S/4HANA performance and user productivity.
- **Security Risks:** VPNs increase the attack surface, exposing critical systems to unauthorized access and lateral movement.

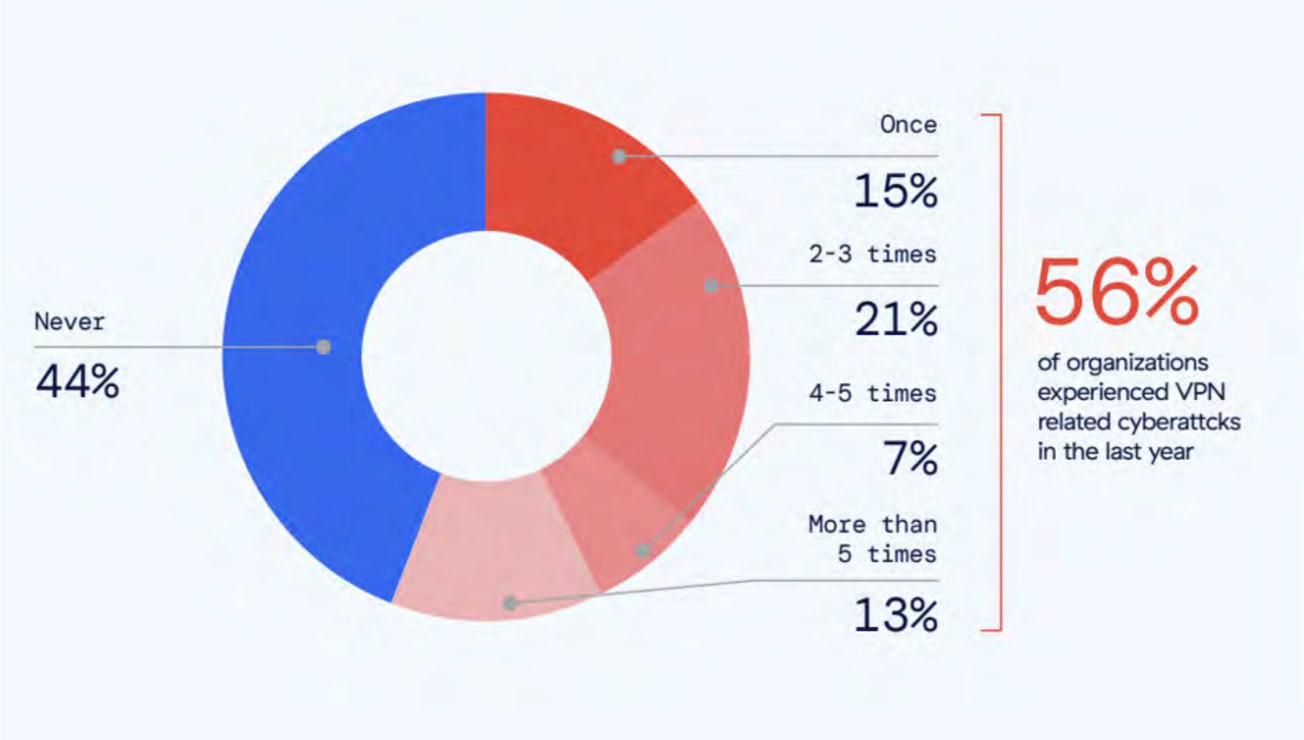

Figure 2: Organizations commonly use VPNs to enable remote users, but end up with security risks and performance issues.

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 S/4HANA and RISE with SAP, is fast becoming a priority for IT and business leaders.

When modernizing SAP investments, organizations must also consider modernizing security by adopting access and security frameworks built on zero trust. Zero trust access frameworks are more effective in reducing security risks, protecting data, removing operational complexity, and eliminating the performance bottlenecks associated with traditional perimeter-based defenses such as firewalls and VPNs.

Zscaler Private Access: A Modern Secure Access Solution for RISE with SAP

Zscaler Private Access (ZPA) reimagines access to RISE with SAP by implementing industry leading zero trust architecture. ZPA is a modern and secure alternative to legacy access mechanisms such as VPNs. And unlike VPNs, it only provides access to specific SAP applications based on continuously verifying the user's identity and their device security posture, adhering to the zero trust principle of "never trust, always verify."

ZPA's inside-out connectivity model dynamically brokers policy-based connections directly between users and specific SAP applications by employing user-to-app segmentation—a security feature within the Zscaler platform. This feature allows for granular control of access between individual users and specific applications, essentially creating isolated "microsegments" by only allowing access to the specific application a user is authorized to use, significantly reducing the attack surface within a network and limiting potential lateral movement of threats.

In addition to that, Zscaler's integrated data protection capability offers comprehensive visibility and control over sensitive information residing in RISE with SAP applications. It plays a pivotal role in protecting data within SAP applications, ensuring compliance with industry regulations such as GDPR, HIPAA, and others.

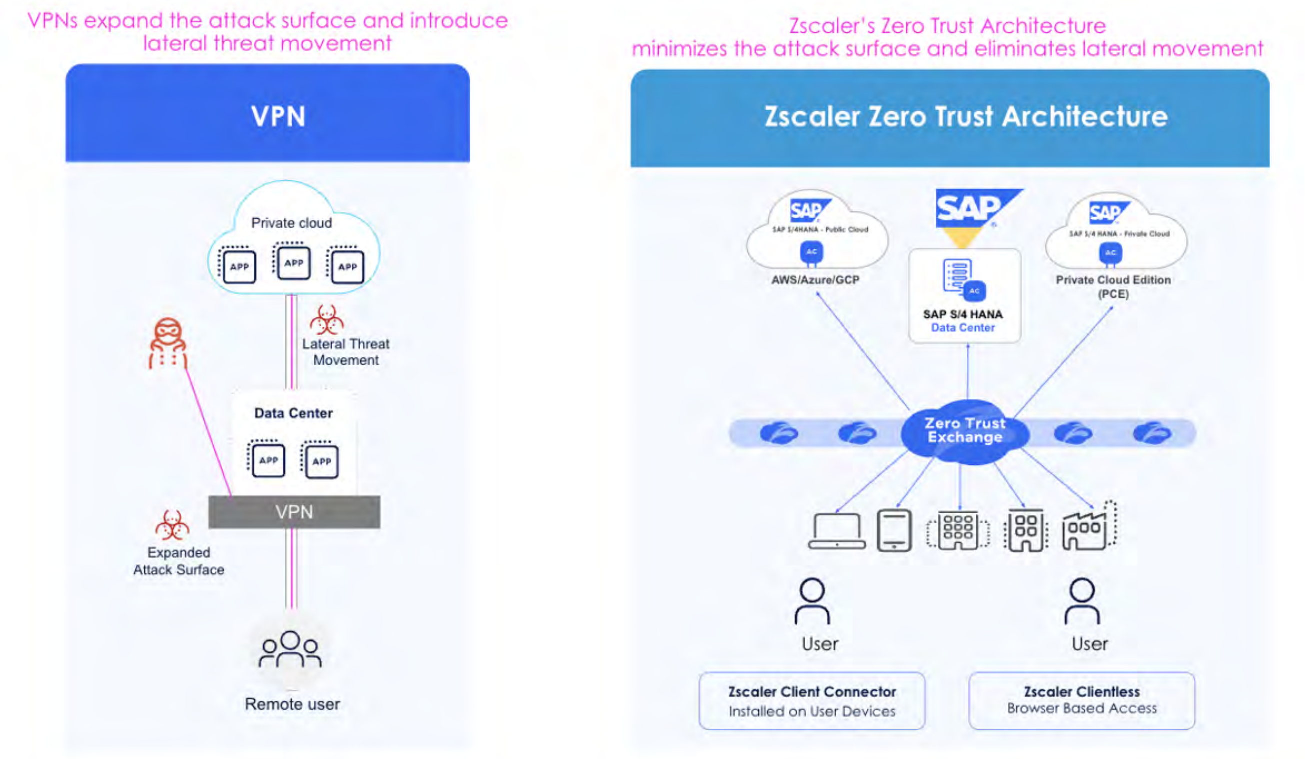
VPNs expand the attack surface and introduce lateral threat movement
VPN
Private cloud
APP
APP
APP
Lateral Threat Movement
Data Center
APP
APP
VPN
Expanded Attack Surface
Remote user
Zscaler's Zero Trust Architecture minimizes the attack surface and eliminates lateral movement
Zscaler Zero Trust Architecture
SAP
SAP S/4HANA - Public Cloud
AC
AWS/Azure/GCP
SAP
AC
SAP S/4 HANA
Data Center
SAP
SAP S/4 HANA - Private Cloud
AC
Private Cloud Edition (PCE)
Zero Trust Exchange
User
User
Zscaler Client Connector
Installed on User Devices
Zscaler Clientless
Browser Based Access

Figure 3: VPN versus Zscaler's Zero Trust Architecture

Key Uses Cases Addressed by Zscaler Private Access for RISE with SAP

Accelerated cloud migration to RISE with SAP (S/4HANA Private Cloud): RISE with SAP combines all the components that businesses need to pursue their business digital transformation strategies securely. But businesses moving to RISE with SAP require secure access during migration and post-deployment.

ZPA integrates natively within RISE with SAP deployments, ensuring zero trust connectivity without relying on hardware or OS-level dependencies. This enables seamless transitions to multicloud environments while maintaining access security and optimal user performance.

SAP-managed Zero Trust Protection

By provisioning of Zscaler App Connectors, zero trust access is natively enabled within the SAP-managed RISE environment, without the need for VPNs. This ensures that customers can run their technology operations in a managed, secure cloud infrastructure with built-in security and data protection. ZPA's app Connectors serve as a secure gateway establishing an encrypted outbound TLS (Transport Layer Security) connection to the Zscaler Zero Trust Exchange (ZTE), ensuring 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.

Secure Access for the Hybrid Workforce and Third-parties

ZPA delivers seamless client-based and browser-based zero trust connectivity, ensuring secure, direct access for employees and third-parties from anywhere to RISE with SAP applications and resources.

- **Client-based access for the workforce:** ZPA's client-based access capability, powered by Zscaler Client Connector, delivers a seamless and persistent connection to RISE with SAP applications for enterprise users. This model ensures optimized performance for hybrid employees using managed devices.
- **Browser-based third-party access:** Third-party users such as contractors and partners often operate unmanaged or BYOD devices while needing access to business crucial SAP systems. ZPA's browser-based access capability enables secure, agentless access to RISE with SAP applications via a web browser. It allows third-party contractors and partners to securely connect to RISE with SAP applications using a web browser, eliminating the need for client installation.

Both access models leverage ZPA's zero trust principles to provide secure, least-privileged connectivity while maintaining a consistent user experience.

SAP Data Protection and Compliance

The Zscaler Zero Trust Exchange (ZTE) integrates advanced data protection capabilities to safeguard sensitive data within RISE with SAP applications, ensuring secure handling of critical business information such as financial records, customer data, and intellectual property. By identifying, classifying, and monitoring sensitive data, ZTE data protection engine ensures compliance with industry regulations and corporate policies. Advanced content inspection and contextual analysis helps prevent unauthorized access or accidental data leaks, while tailored policies enable secure data sharing and usage within RISE with SAP applications, mitigating risks to data integrity and confidentiality in SAP systems.

To further protect data from third parties, ZTE leverages browser isolation technology. This approach creates a secure, virtual environment for third-party users accessing SAP applications, isolating the browser-based session from the endpoint and the broader applications. By rendering business resources remotely and delivering them as an image or interactive stream to the user's device, browser isolation prevents unauthorized data extraction by third parties. This ensures sensitive SAP data remains secure, during browser-based access from unmanaged endpoints.

Key Value Drivers of Zero Trust for RISE with SAP

1. **Minimized attack surface:** RISE with SAP applications remain invisible to unauthorized users and attackers. ZPA creates microtunnels between users and applications, reducing exposure risks.
2. **Client-based and browser-based access:** ZPA supports both client-based access for employees and browser-based access for third-party users, ensuring secure connectivity from any managed or unmanaged device.
3. **Improved user experience:** ZPA bypasses network bottlenecks, enabling direct and faster access to RISE with SAP applications, regardless of user location.
4. **Enforced least-privileged access:** ZPA ensures that users access only the applications and resources required, reducing lateral movement risks.
5. **Cloud native scalability:** ZPA integrates seamlessly into SAP-managed Kubernetes clusters and cloud environments, supporting large-scale deployments with minimal operational overhead.
6. **SAP data protection and compliance:** The Zero Trust Exchange protects sensitive data within RISE with SAP applications, including leveraging browser isolation to remove the threat of data exfiltration by third party users.

The Zscaler Difference for RISE with SAP

RISE with SAP is SAP's subscription-based Business-Transformation-as-a-Service (BTaaS) offering, simplifying migration from legacy on-prem ERP systems (SAP ECC) to cloud-based ERP solutions (SAP S/4HANA). With comprehensive infrastructure, technical support, and managed services, RISE with SAP accelerates business transformation while providing customers full control of their ERP configurations and upgrades. Organizations leveraging RISE with SAP benefit from SAP-managed cloud native environments hosted on hyperscalers like AWS, Azure, and GCP for scalability and flexibility.

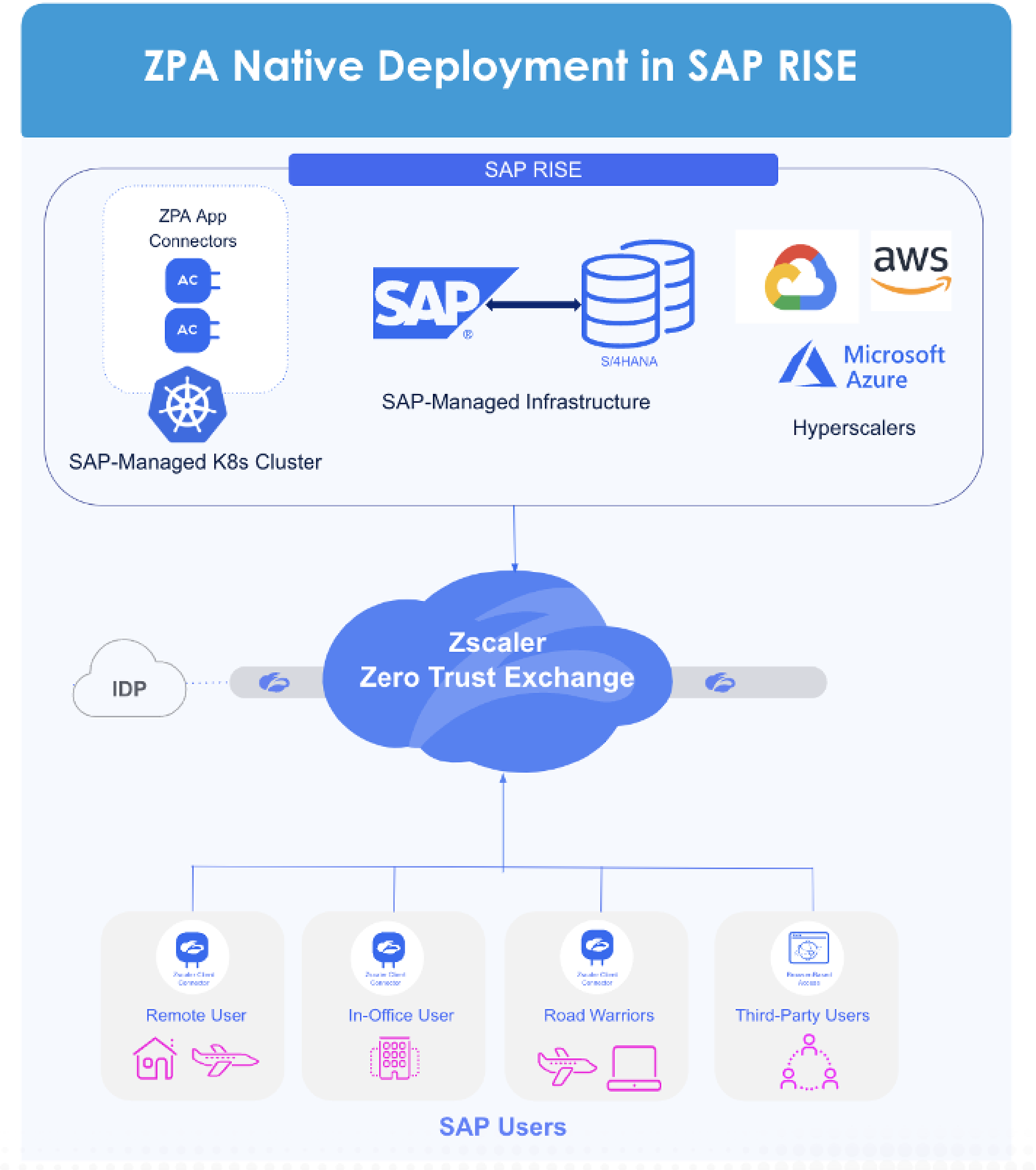

Figure 4: ZPA is natively deployed in RISE with SAP environments.

Zscaler's cloud native ZPA solution is uniquely integrated with RISE with SAP to deliver unparalleled zero trust access through:

- **Cloud native integration:** ZPA supports deployment within SAP-managed Kubernetes clusters, offering hypervisor-agnostic and containerized access that improves scalability and performance.
- **Compliant zero trust:** ZPA App Connectors are provisioned directly inside RISE environments, providing secure, compliant connectivity without requiring VPNs.
- **Operational simplicity:** ZPA eliminates hardware dependencies, reduces complexity, and enables faster provisioning of secure access to critical RISE with SAP workloads.

Cloud Native Deployment Based on a Shared Responsibility Model

SAP-hosted ZPA connectors enable organizations to seamlessly integrate Zscaler Private Access into SAP environments. SAP and Zscaler share responsibility for managing and maintaining secure access through SAP-managed infrastructure and ZPA services:

- **RISE customer-specific Kubernetes clusters:** SAP provides dedicated Kubernetes clusters tailored to ERP workloads and security requirements. ZPA App Connectors are provisioned within these clusters, delivering fully compliant zero trust connectivity.
- **SAP-managed cloud infrastructure:** SAP fully manages the underlying infrastructure stack, including Kubernetes clusters, Host OS, and disaster recovery services, ensuring high availability, resilience, and uptime.
- A customer-controlled ZPA tenant: While SAP manages the infrastructure, customers retain full control of their ZPA tenant through the Zscaler Cloud Admin Portal. Customers can configure access policies, user management, and security thresholds to meet their specific requirements.

Key Value Drivers of SAP-Hosted ZPA Connectors:

- **Portability and performance:** ZPA App Connectors are operating system (OS) and hypervisor agnostic, ensuring consistent performance across different cloud environments without underlying OS dependencies or hardware virtualization.
- **Scalability and optimization:** App Connectors can be provisioned dynamically to meet fluctuating demand, simplifying zero trust access for business-critical applications.
- **Resource utilization and cost:** SAP-hosted ZPA connectors benefit from Kubernetes orchestration, ensuring efficient resource utilization, self-healing, and simplified operations while reducing costs.

This shared responsibility model ensures that ZPA integrates seamlessly with SAP environments, simplifying operations while maintaining full visibility and control over secure access.

Business Value of ZPA for RISE with SAP

- **Seamless cloud migration and app modernization:** Enable secure access to SAP apps during migration from legacy SAP ECC to RISE with SAP.
- **Secure remote access without VPNs:** Deliver reliable and secure remote access to employees and third-parties ensuring consistent connectivity, without requiring a VPN.
- **Improved security:** Minimize attack surfaces and lateral movement with direct, zero trust access to SAP applications using user to app segmentation and connectivity based on least-privileged access.
- **Cloud native scalability:** Enable scalable deployments with SAP-managed Kubernetes clusters and cloud environments with simplified initiation of secure outbound connections to the Zscaler Zero Trust Exchange™, offering more efficient consistent SLAs, resource utilization, self healing, and lower overhead.
- **Data protection and compliance:** Get 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:** Deliver fast, reliable access to business-critical applications from any location, ensuring that users remain unaware of any underlying migration of legacy SAP apps to cloud environments.
- **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.
- **End-to-end visibility during SAP cloud migration:** ZDX tightly integrates with ZPA to eliminate digital experience monitoring silos with end-to-end visibility—from the endpoint to the application—during migration.

Conclusion

The combination of RISE with SAP and Zscaler Private Access (ZPA) empowers enterprises to modernize access to critical applications, improve security, and enable business transformation. By adopting a zero trust approach, organizations can ensure seamless, secure, and scalable connectivity to RISE with SAP for employees, contractors and partners. ZPA's cloud native integration, operational simplicity, and advanced security make it the ideal solution for businesses preparing for the next phase of business transformation.