Zscaler for SAP Security

Reimagine SAP security with a Zero Trust approach that simplifies access, reduces risk, and improves performance.

Solution Brief

Key Highlights

- Harden SAP security posture and simplify SAP access modernization with Zero Trust as the foundation.
- Reduce attack surface and enforce least-privilege, app-level access—often with a better experience than VPN.
- Accelerate troubleshooting by isolating SAP issues across device, network, and application layers to cut MTTR.
- Reduce SAP data leakage risk by controlling exfiltration actions during SAP sessions, including third-party access.
- Secure SAP workload-to-workload connectivity with consistent Zero Trust controls that limit lateral movement.

The Challenge

SAP landscapes are evolving fast—RISE with SAP, SAP Private Cloud Edition (PCE), and hyperscalers are now common parts of the journey. But security and access models often remain rooted in network-era constructs that weren't built for a hybrid workforce or workloads in the distributed cloud.

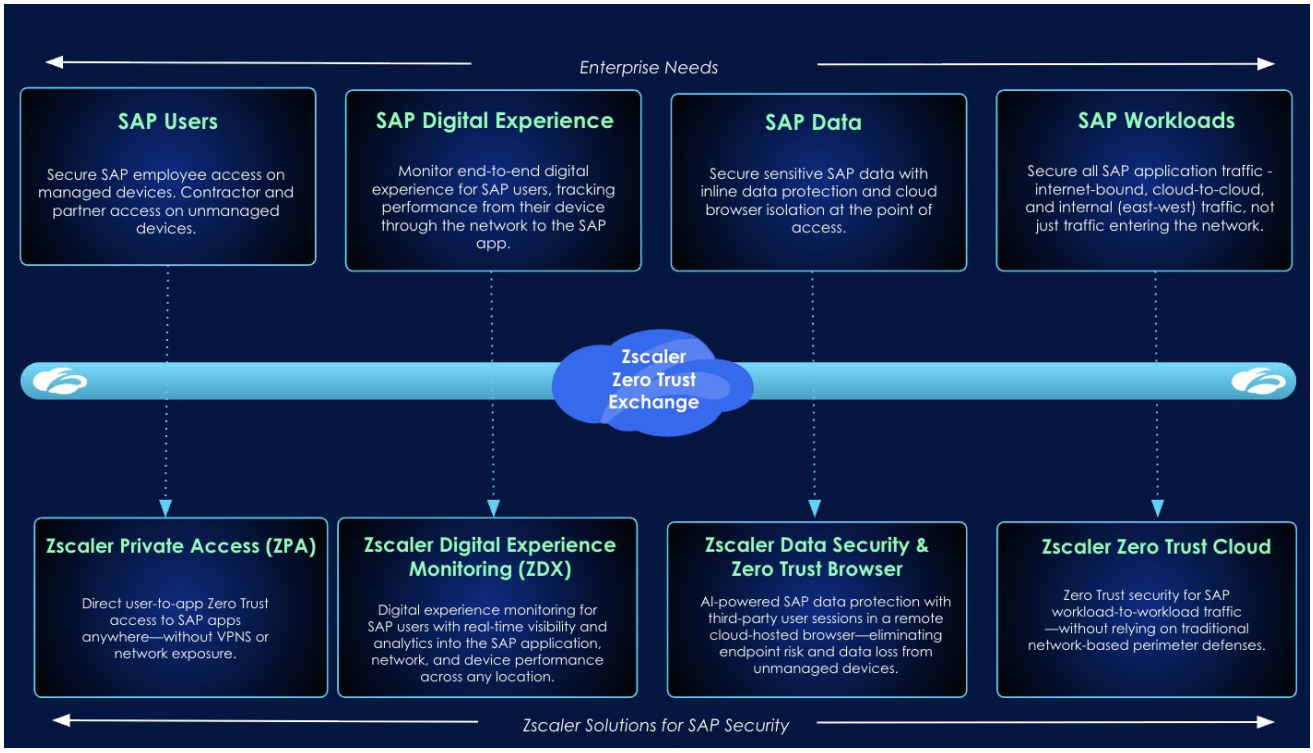
As SAP moves from on-prem to SAP-managed cloud (RISE/PCE) and customer-managed hyperscaler environments, new security gaps emerge. Legacy security tools designed for static networks struggle in modern hybrid architectures—creating complexity across multiple RISE tenants, fragmented connectivity paths, and inconsistent controls.

These issues can lead to a larger operational burden and make it harder to pinpoint SAP performance problems end-to-end. Modernization without modern security increases risk and slows transformation.

SAP environments concentrate some of the enterprise's most valuable data and processes—so security must address four intertwined challenges:

- Users still access SAP through legacy VPN/firewall networks that expand exposure.
- SAP digital experience is difficult to monitor and diagnose across device, network, and application layers.
- High-value SAP data faces leakage and malware pathways, especially with third parties and unmanaged devices.
- SAP workloads are increasingly distributed and often connected via overly permissive network paths, raising lateral movement risk.

Zscaler for SAP Security: Our Cloud-Native, Zero Trust Approach to SAP Access, Security, and Visibility

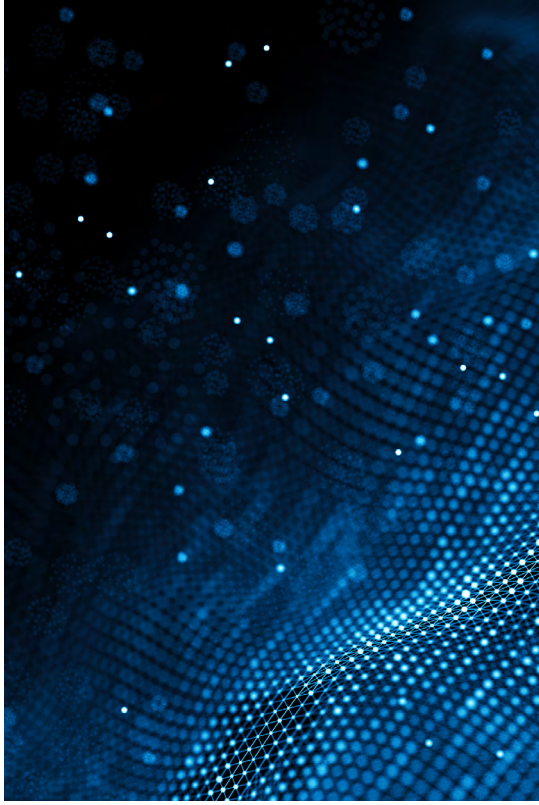


Zscaler brings a unified Zero Trust architecture to SAP by combining secure access, data protection, workload connectivity, and experience monitoring through the Zscaler Zero Trust Exchange.

With Zscaler Private Access (ZPA), users get direct, app-level access to SAP without VPNs or network exposure—supporting employees on managed devices and partners/contractors on unmanaged devices. Zscaler Digital Experience Monitoring (ZDX) provides end-to-end visibility into SAP user experience from device through network to the SAP app. Zscaler Data Security and Zero Trust Browser protect sensitive SAP data inline at the point of access, including for third-party sessions. And with Zero Trust Cloud, organizations can secure SAP workload connectivity across distributed clouds and data centers with consistent, zero trust controls.

Together, these capabilities harden the SAP security posture across users, workloads, data, and digital experience—with Zero Trust as the foundation.

How the Zscaler Zero Trust Exchange (ZTE) Works



Zscaler applies Zero Trust by enforcing access per session based on identity and context—rather than assuming anything inside the network is trusted. Each connection is evaluated in real time and only the specific application a user is authorized to reach is made available, which reduces exposure and helps limit lateral movement. Applications remain private, and traffic can be inspected inline to apply threat and data protection controls. This is purpose-built Zero Trust—not a bolt-on to VPNs and firewalls.

The same approach extends to workloads: workload-to-workload communications are connected and governed with least-privilege policies, so only approved services can talk to each other across clouds and data centers—helping reduce overly permissive connectivity and lateral movement risk in distributed environments.

The Zscaler for SAP Security solution supports the following use cases:

Use Case 1: Secure User Access to SAP

ZPA modernizes SAP access for employees, contractors, and partners by providing secure, direct user-to-application connectivity from any device and any location. Instead of placing SAP users "on the network" via VPN, ZPA brokers connections to specific SAP applications based on identity and policy, enforcing least privilege and minimizing exposure.

This approach simplifies remote access operations, improves security by eliminating inbound access paths and reducing lateral movement, and supports both client-based access (via the Zscaler Client Connector) and clientless browser-based access for third parties.

Zscaler's Zero Trust Architecture Secures Access to SAP Better than VPNs

VPNs were designed to extend a private network to remote users, but that model expands the attack surface and enables lateral movement once a user is connected. In SAP environments—where applications are highly sensitive—this network-level access creates unnecessary risk.

Zscaler's Zero Trust with ZPA flips the model: users connect only to the SAP application they're authorized to use, not the broader network. SAP applications remain hidden, and access is enforced with granular, context-aware policies.

The outcome is stronger containment, reduced blast radius, and simpler operations. Users also benefit from faster, more reliable access from anywhere, often outperforming VPN experiences—especially in hybrid cloud scenarios spanning data centers, PCE, and public cloud deployments.

We've Achieved an Integration Milestone with SAP

Zscaler has reached a major partnership milestone with SAP by delivering ZPA integration options that enable secure, Zero Trust access to the SAP Private Cloud Edition (PCE) in RISE with SAP.

Two deployment approaches are available: deploy the native App Connectors within SAP PCE using SAP-native methods, or establish VPC peering between your own private cloud (for example, in AWS) and your SAP PCE instance (also in AWS) for private, peer-to-peer connectivity. Both approaches support SAP Fiori and SAP GUI, helping organizations modernize access without compromising user experience.

Shared Responsibility Model

In SAP-managed PCE deployments, responsibilities are split across SAP (security of the cloud), the customer (security in the cloud), and ZPA's role (security of user-to-app connections). SAP covers the SAP application stack operations and lifecycle, and manages the underlying PCE infrastructure—compute, storage, and networking—plus OS and platform hardening, patching, and SLAs. ZPA app connectors are hosted and operated by SAP inside PCE (available in the SAP store) and enable outbound-only connectivity.

Customers own and manage their ZPA tenant, identity and access policies, and who can access which SAP applications. Zscaler Zero Trust Exchange connects to the tenant and inspects traffic (including SSL/TLS) to detect and block advanced threats, while keeping SAP apps invisible and non-routable.

A Third Flexible Deployment Option

Not every SAP modernization path runs through SAP-managed PCE. For SAP workloads running in customer-managed SAP-certified hyperscalers (AWS, Azure, GCP), ZPA App Connectors can be deployed alongside the SAP workloads, creating a turnkey, co-located Zero Trust access layer.

Use Case 2: Monitor the SAP Digital Experience

Security outcomes are only part of SAP success—user experience drives productivity and business processes. ZDX delivers end-to-end visibility into SAP digital experience across device health, network path, and application responsiveness, so IT teams can quickly pinpoint whether issues stem from endpoint constraints, Wi-Fi/connectivity, network latency/packet loss, or SAP availability and response time. With proactive insights and health scoring, teams can detect degradations early, reduce mean time to resolution, and deliver a consistent experience for employees and third parties across locations and access methods.

Use Case 3: Secure the SAP Data Estate and Protect It From Threats

SAP environments contain highly sensitive data, and exposure risk increases when third parties access SAP from unmanaged devices. Zscaler addresses this with data security controls and Zero Trust Browser isolation at the point of access. With inline protection, organizations can enforce DLP–aligned policies and reduce the chance of data leaks while still enabling necessary access.

Browser isolation further lowers risk by moving the browsing session to a remote, cloud–hosted environment and streaming only pixels to the user. This approach helps keep sensitive SAP data inside controlled environments, limits exfiltration pathways, and supports secure collaboration with vendors and partners—while maintaining usability for legitimate business needs.

Use Case 4: Secure SAP Workloads in Distributed Clouds

SAP security isn't only about user access—workload–to–workload communication across clouds and data centers is increasingly common and often overly permissive. Zscaler's Zero Trust Cloud secures cross–environment connectivity across the SAP cloudscape. By enforcing least–privilege policies for workload communication, organizations can better protect critical SAP systems while enabling modernization across multiple clouds, regions, and network constructs. The goal is secure connectivity that matches how SAP architectures actually run today—distributed, dynamic, and business–critical.

Benefits of De-Risking SAP with Zscaler

- **Reduced attack surface + granular Zero Trust access:** Private SAP apps stay hidden from the public internet, and direct connections to specific SAP apps prevent broad network reach.
- **Simplified operations + better user experience:** Streamlined, context-aware policy management ensures users only access what they need, while delivering fast, secure access from anywhere—often outperforming VPN.
- **Native deployment + Resilience:** Native deployment in SAP PCE means no bolt-on infrastructure or OS/hardware dependencies, while delivering SAP-aligned SLAs with business continuity and built-in disaster recovery for stronger reliability and resilience.
- **Marketplace availability + scalable control:** For hyperscaler deployments, you get marketplace availability across the major hyperscalers plus full control, flexibility, and scalability to adapt as needs change—without complex re-architecting.
- **Faster SAP troubleshooting and higher availability:** Speeds troubleshooting by pinpointing whether SAP issues originate on the device, network path, or SAP application layer—reducing mean time to resolution.
- **Lower SAP data leakage risk (including third parties):** Reduces data leakage risk by restricting exfiltration actions (copy/paste, download, print) during SAP sessions, including third-party access.
- **Safer SAP workload-to-workload connectivity:** Secures SAP workload connectivity across distributed clouds and data centers with consistent Zero Trust controls that reduce lateral movement risk.

Transform your SAP Estate with Zero Trust Security from Zscaler

If you're taking the first step toward Zero Trust, replace legacy network access solutions that introduce risk. If you already use Zscaler Internet Access (ZIA), expand your Zero Trust footprint by adding ZPA to deliver seamless, secure access to SAP applications.

And if you're undergoing a major transformation—especially using RISE with SAP—use Zscaler's "iron-clad" Zero Trust security to eliminate risks both during and after migration.

With one unified Zero Trust approach, you can secure SAP end-to-end—modernizing user and third-party access, protecting sensitive data, improving experience and troubleshooting, and enforcing least-privilege connectivity across distributed SAP workloads—so transformation moves faster with less risk.

Learn more about Zscaler and SAP >

zscaler™ | Experience your world, secured.™

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