Zscaler for SAP Security

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

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 across RISE/PCE and hyperscalers, but access and security often remain network-based. Legacy tools built for static networks add complexity across tenants, fragment connectivity, and create inconsistent controls—raising risk and slowing transformation.

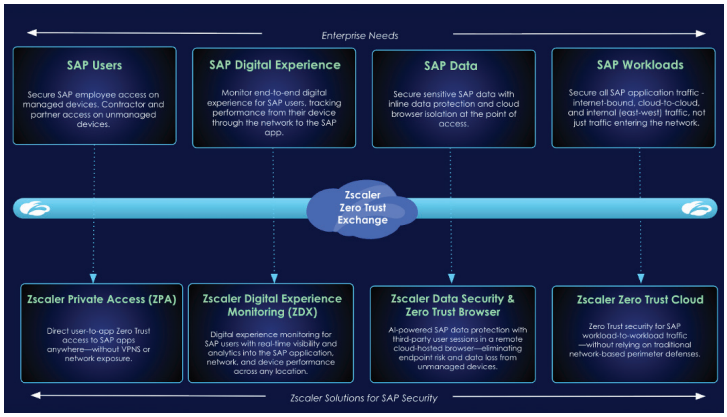
Four intertwined challenges:

- VPN/firewall-based SAP access expands exposure.
- SAP experience is hard to monitor across device, network, and application layers.
- High-value SAP data faces leakage and malware risk, especially with third parties and unmanaged devices.
- Distributed SAP workloads often rely on overly permissive connectivity, increasing lateral movement risk.

The Solution

Zscaler Zero Trust Exchange (ZTE) for SAP Security

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



- **Zscaler Private Access (ZPA):** Direct, app-level access to SAP without VPNs or network exposure—for employees on managed devices and partners/contractors on unmanaged devices.
- **Zscaler Digital Experience (ZDX):** End-to-end visibility into SAP user experience across device, network path, and SAP application responsiveness to isolate issues and reduce MTTR.
- **Zscaler Data Security + Zero Trust Browser:** Inline protection that reduces SAP data leakage risk by controlling exfiltration actions during SAP sessions, including third-party access.
- **Zero Trust Cloud:** Consistent Zero Trust controls for SAP workload connectivity across distributed clouds and data centers to reduce lateral movement risk.

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

How 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.

Use Cases

Use Case 1:
Secure User Access to SAP

Zscaler Private Access (ZPA) modernizes SAP access with secure, direct user–to–application connectivity. Replaces VPN–based "on–the–network" access with least–privilege, policy–based access. Supports client–based access and clientless browser–based access for third parties.

Use Case 2:
Monitor the SAP Digital Experience

Zscaler Digital Experience (ZDX) provides end–to–end visibility into SAP experience across device health, network path, and application responsiveness—helping teams pinpoint root cause and reduce MTTR.

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

Zscaler Data Security and Zero Trust Browser protect sensitive SAP data at the point of access, including for third–party sessions and unmanaged devices. Reduces leakage risk by restricting exfiltration actions (copy/paste, download, print) and using isolation to limit endpoint risk.

Use Case 4:
Secure SAP Workloads in Distributed Clouds

Zscaler Zero Trust Cloud secures SAP workload–to–workload communication across clouds and data centers with consistent least–privilege controls—reducing lateral movement risk in distributed SAP architectures.

Benefits of De–Risking SAP with Zscaler

- Reduced attack surface + granular Zero Trust access
- Simplified operations + better user experience
- Flexible deployment and resilience
- Scales with SAP cloud choices
- Faster SAP troubleshooting and higher availability
- Lower SAP data leakage risk (including third parties)
- Safer SAP workload–to–workload connectivity

Transform Your SAP Estate with Zero Trust

Replace legacy network access that introduces risk, expand Zero Trust to SAP apps, and reduce risk during migration and steady–state operations—especially with RISE with SAP.

zscaler™ | Experience your world, secured.™

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