

A close-up, profile view of a man with short dark hair and a beard, wearing glasses and a dark green sweater. He is looking intently at a computer screen, which is partially visible on the left. The background is blurred, showing an office environment.

Secure Your SAP S/4HANA Migration with Zero Trust



By 2027, SAP will end support for legacy ECC ERP, accelerating the shift to SAP S/4HANA via RISE with SAP. As a cloud-based next-generation ERP, S/4HANA improves agility and operational excellence with real-time data access, advanced analytics, and AI-driven insights.

The Complex Hybrid Environment of S/4HANA

Modernizing to S/4HANA is a multi-year journey. Most organizations don't move SAP data and applications to the cloud overnight—they run a hybrid environment where some systems stay on-premises while others move to the cloud. Legacy SAP ECC and SAP BW often remain on-prem as S/4HANA is implemented in parallel. These systems must interoperate, sharing data and processes across SAP and non-SAP workloads—creating a complex hybrid landscape that must be secured end-to-end.

Migrating to SAP S/4HANA Creates Security Multipliers

The complex distributed hybrid architecture creates security multipliers that traditional security models were never designed to address.

- **Expanded attack surface and lateral threat movement:** S/4HANA integrations with internet, SaaS, partners, and internal systems increase exposed endpoints (web apps, APIs, gateways). If one path is compromised, attackers can pivot laterally into critical SAP systems and data.
- **Operational complexity & inconsistent protection:** Firewalls/VPNs create policy sprawl across on-prem and cloud. Private links with firewalls at both ends add overhead. Disparate tools fragment enforcement, increasing blind spots, misconfigurations, and inconsistent controls.
- **Data exfiltration from sophisticated attacks:** SAP holds financial data, PII, and operational records. Without consistent inspection of outbound and east—west traffic, attackers can abuse trusted channels to siphon data, triggering compliance failures, regulatory reporting, fines, and lawsuits.

Secure the Journey to SAP S/4HANA with Zscaler Zero Trust Cloud

Zscaler Zero Trust Cloud delivers a Zero Trust architecture for securing S/4HANA's hybrid reality. Powered by the Zscaler Zero Trust Exchange with ZIA and ZPA, it replaces network-centric controls with granular, workload identity-based protection. It hides workloads to reduce exposure and enables only one-to-one connectivity to stop lateral movement across SAP systems. Cloud-scale TLS inspection and in-line data protection eliminate blind spots and help prevent data exfiltration. Below are the key benefits customers realized.

Secure connectivity for S/4HANA workloads in a multicloud environment

Zscaler provides Zero Trust based connectivity between S/4HANA and other applications using a reverse proxy architecture. It hides the SAP modules eliminating the need for public IP addresses.

Grant secure access to business partners without exposing S/4HANA

Partners often need near-real-time access to S/4HANA. Zscaler secures this connectivity with a Zero Trust model without directly exposing SAP modules.

Secure communication between S/4HANA and print servers

When a user submits a print job from S/4HANA, it's routed through the Zero Trust Exchange and delivered securely to the printer—bridging the hybrid cloud without complex legacy networking or firewall rules.

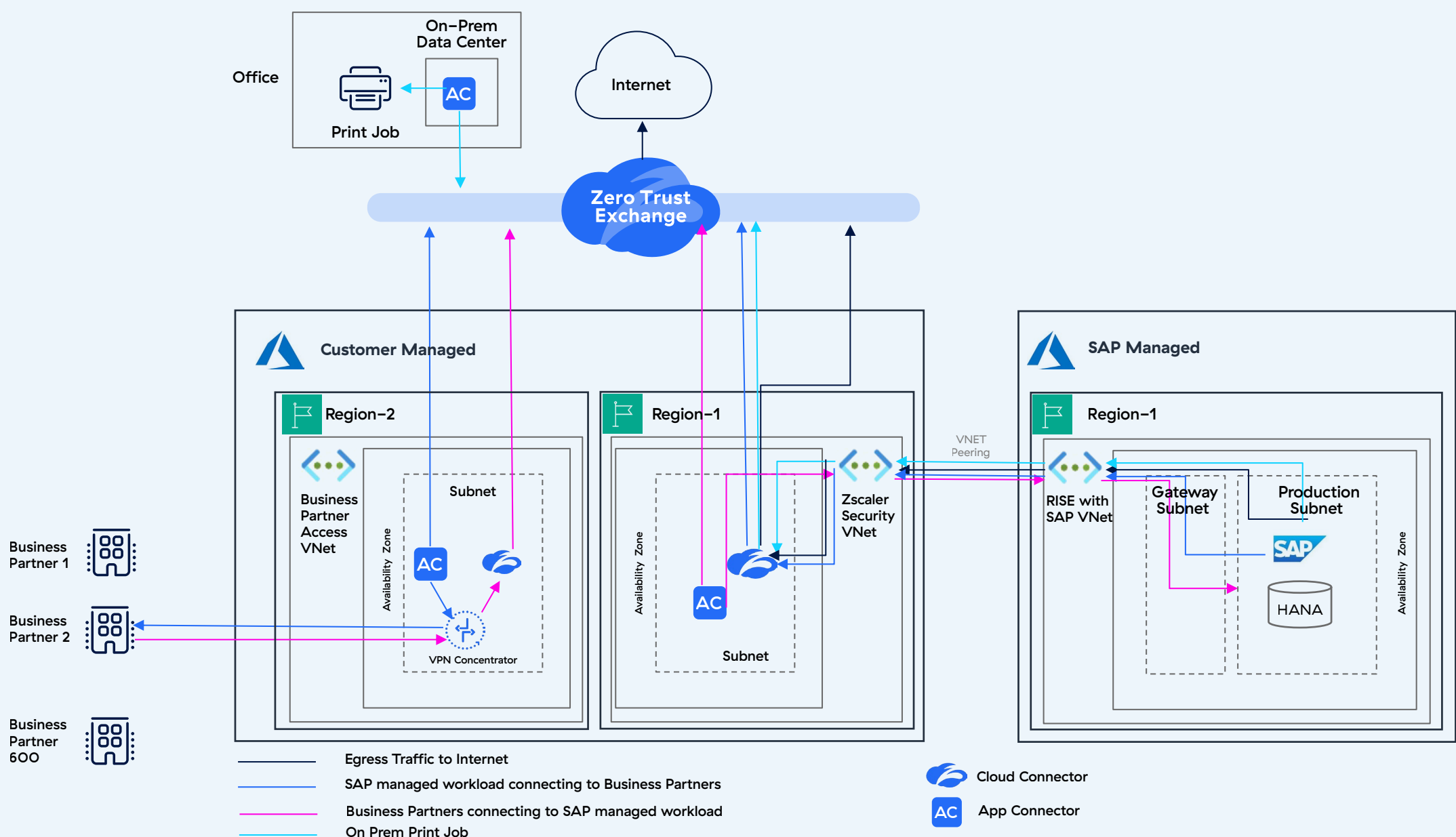
Protect sensitive data during migration from SAP ECC to S/4HANA

ZTC provides secure connectivity for data migration between on-prem SAP workload and the S/4HANA target, limiting access to only the required endpoints and preventing data loss.

Secure traffic from S/4HANA to SaaS apps

Enable safe outbound access with cloud-scale TLS inspection and inline data protection for SaaS from S/4HANA.

A Medical Technology Giant Used Zscaler Zero Trust Cloud to Secure S/4HANA Migration



A medical technology giant migrated to SAP S/4HANA using a RISE with SAP subscription on Microsoft Azure. The “black-box” nature of the environment limited visibility and control. Traditional security models couldn’t deliver granular policy enforcement required by company policy for users, offices, and partners.

THE CHALLENGE

- 1. Securing internet bound traffic:** S/4HANA outbound traffic was routed directly to the internet, while the company required policy-based inspection and control.
- 2. Secure access to offices:** Remote offices needed secure connectivity from S/4HANA to on-prem printers worldwide.
- 3. Providing secure access to business partners:** Thousands of partners needed secure, least-privileged access to S/4HANA without the complexity and risk of legacy security networks.

THE SOLUTION

The company built an innovative solution using the Zscaler Zero Trust Cloud. A dedicated Azure tenant was set up as a secure landing zone and a VNet peering connection was established with SAP managed subscription. All inbound and outbound S/4HANA traffic was redirected through the secure landing zone for inspection, enabling centralized control and a true Zero Trust security control plane.

THE OUTCOME

With this approach, Zero Trust Cloud enabled the company to secure SAP S/4HANA across a hybrid environment. All internet-bound traffic was protected and compliant. It delivered seamless, least-privilege access for business partners without disrupting operations, while also enabling secure execution of on-premises print jobs from S/4HANA. In doing so, the company modernized its security controls alongside its broader SAP transformation.

Next Steps

To learn more about securing your SAP S/4HANA migration with Zscaler Zero Trust Cloud, contact us today.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 in-line cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.



**Act Fast.
Stay Secure.**