JOINT SOLUTION BRIEF

zscaler™ + Silverfort

Adaptive Access Engine Integration

INTEGRATION HIGHLIGHTS

- Reduce the attack surface with dynamic, risk-based Zero Trust access
- Detect and restrict insider threats and risky activity
- Enable consistent Zero Trust enforcement across hybrid environments

The Market Challenge

Today's enterprise environments are increasingly complex; spanning cloud, on-prem, and hybrid infrastructures, with users accessing applications from anywhere using a growing mix of identities, devices, and access methods. As identity becomes the primary control plane for Zero Trust, traditional access decisions based on static credentials and roles are no longer sufficient to protect critical applications and data.

At the same time, security teams rely on siloed tools that generate fragmented signals about user behavior and risk. Identity threats such as credential compromise, abnormal authentication behavior, and lateral movement are often detected in isolation, slowing response times and allowing threats to persist.

To effectively reduce risk, organizations need a unified, real-time approach, one that continuously shares identity risk intelligence and dynamically adapts access decisions across the environment, without adding friction or operational complexity.

The Solution

Through the integration between Zscaler and Silverfort, organizations can now enforce smarter real-time access decisions based on dynamic user risk. By delivering live identity risk signals from Silverfort to Zscaler's Adaptive Access Engine (AAE), organizations can ensure that access policies reflect a user's current risk level and not just static attributes or pre-defined roles.

This continuous risk awareness allows Zscaler to automatically tighten or revoke access when suspicious activity is detected, including abnormal authentication patterns or signs of credential compromise. Additionally, AAE can require a user to re-authenticate with their identity provider (IdP).

Together, Zscaler and Silverfort provide a unified approach to identity and network access security by extending complete visibility and access control across hybrid environments.

Together, Zscaler and Silverfort enhance access decisions by exchanging risk signals in real-time.

Solution Components Deep Dive

The joint integration is built on top of the Shared Signals Framework (SSF), an open standard that enables security systems to exchange real-time security event information. As part of this integration, Silverfort acts as a Shared Signals Transmitter, supporting the Continuous Access Evaluation Protocol (CAEP) RiskChange event.

When Silverfort detects a change in a user's risk posture, such as unusual authentication behavior, credential compromise, or lateral movement attempts, it immediately sends a RiskChange event to Zscaler via the framework. These dynamic risk signals are ingested by Zscaler's AAE, which can then automatically adjust access policies in real time, enforcing step-up authentication, session restrictions, or blocking access entirely.

With continuous risk data flow to Zscaler, access decisions are always based on the most up-to date identity and risk intel, dramatically reducing response time to emerging threats and enhancing the organization's security posture.

KEY USE CASES

Adaptive Access for Hybrid Environments

Users accessing applications across cloud and on-prem environments often present inconsistent risk signals. Silverfort provides unified identity risk visibility across hybrid environments, while Zscaler enforces adaptive access policies based on real-time risk. The result is consistent Zero Trust enforcement—regardless of where the user, application, or identity resides.

Insider Risk and Privilege

Insider threats and compromised insiders often exhibit subtle behavior changes that static policies miss. Silverfort continuously monitors identity behavior across environments and flags risky activity such as unusual access patterns or lateral movement. Zscaler uses this identity risk context to dynamically restrict access, ensuring that trust is continuously validated and excessive access is curtailed in real time.

Zscaler + Silverfort Benefits

ACTION	DESCRIPTION
Reduce the attack surface	Ensure zero trust access with risk-based authentication that securely connects users directly to authorized apps without accessing the network to prevent the lateral movement of threats.
Operational efficiency	Streamline policy enforcement by integrating identity intelligence directly into Zscaler's access control decisions.
Get unified visibility across environments	A centralized view of identity and access risk across cloud, on-prem, and hybrid environments.

Conclusion

Deliver better business results with Zscaler and Silverfort

By integrating Silverfort's real-time identity risk signals into Zscaler's Adaptive Access Engine, Zscaler strengthens Zero Trust access with continuous, identity-driven context. Access decisions dynamically adapt to user risk in real time—enforcing step-up authentication, restricting sessions, or blocking access when threats emerge. With Silverfort enhancing identity visibility across hybrid environments, Zscaler delivers faster threat response, stronger Zero Trust enforcement, and smarter access without added complexity.

Learn more at **www.zscaler.com/partners/technology**

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 SASE-based Zero Trust Exchange is the world's largest in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

©2026 Zscaler, Inc. All rights reserved.