Partner Brief

Zscaler & Okta:

Deliver seamless authentication and security to cloud-based applications

Introduction

The adoption of cloud-first strategies continues to expand to support today's work-from-anywhere environments. But as applications move beyond traditional on-premises data centers and into the cloud, protecting employees wherever they work poses challenges:

- **Increased risks:** Remote employees, more devices, and perimeter-based architectures expand the attack surface, increasing risks.
- **Poor user experiences:** Separate credentials for cloud vs. on-prem applications and latency caused by VPNs and firewalls frustrate users.
- **Costly and complex processes:** Manual integration processes, VPN deployment and management, MPLS, and firewalls are expensive and complex to manage.

A new approach based on zero trust is required to securely connect users, devices, and applications over any network, regardless of location.

What is Zero Trust?

Zero trust is a framework to secure modern organizations based on least-privileged access and the principle that no user or application should be inherently trusted. Connections are authorized based on validation of the user's identity, risk-based context, and business policy.

End-To-End Zero Trust With Okta + Zscaler

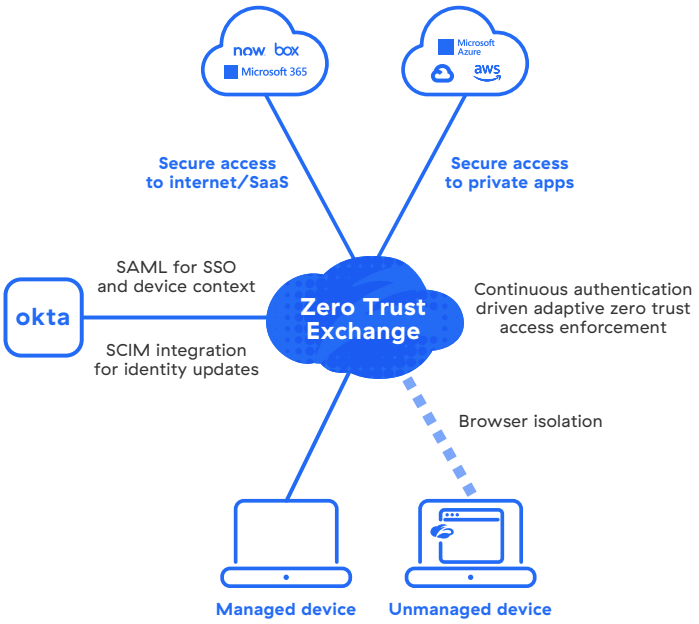
As the leading identity provider, Okta protects and enables an organization's employees, contractors, and partners to use the technology they need to be productive. It's a flexible platform with an identity-centric approach to zero trust, securely connecting the right people to the right technologies at the right time to empower remote workforces with full confidence.

Zscaler is a pioneer in zero trust, enabling customers to accelerate their secure digital transformation journey. The cloud-delivered Zero Trust Exchange platform acts like an intelligent switchboard that securely connects users and applications. All communication goes through the Zero Trust Exchange, and nothing reaches applications without the platform allowing it. Applications become invisible to unauthorized users, so your resources can't be discovered and exploited on the internet.

Zero Trust Starts With Identity

The first step to implement zero trust is to confirm the user is who they say they are. Once authenticated, Zscaler inspects all traffic and validates access rights based on identity and context using the principles of least-privileged access. This ensures users can only access applications for which they've been authorized.

Together, Okta and Zscaler deliver a cloud-based, end-to-end zero trust solution that provides users fast and secure access to the internet, SaaS, and private applications— over any network, at any location, and on any device. Risk-based access provides a seamless user experience and increased security when needed.



Key Integrations

Okta and Zscaler integrate with each other using industry standard authentication protocols, including Security Assertion Markup Language (SAML) and System for Cross-domain Identity Management (SCIM). Together, Zscaler and Okta:

- **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.
- **Improve the user experience:** Simplify deployment and enable fast, direct, and secure access to apps anywhere with seamless SAML integration for single sign-on (SSO) and sharing of user and device context.
- **Increase agility and reduced TCO:** Enable work from anywhere, dynamically manage role changes for full user lifecycle management, and simplify management with cloud delivery and SCIM integration—without costly VPNs and firewalls.

Key Use Cases

The Okta and Zscaler integrations support the following use cases:

Verify user identity

Okta maintains credentials about the user ID to verify they are who they say they are. SAML integration enables strong authentication to verify user credentials and provide zero trust access to only the required resources.

SAML authentication also allows organizations to auto provision new users. For example, once a user logs into Okta, Okta sends the user and group information for that user to Zscaler via a SAML assertion. Zscaler takes that information and populates its database so that policies can be applied to the user/group/device. The next time the user logs in, since he or she is already in the Zscaler database, the user is redirected to Okta to refresh the SAML assertion, and any changes are updated in the Zscaler database.

Securely enable work-from-anywhere

Okta can provide the trusted/untrusted device status to Zscaler for SaaS applications via the user's authentication response when using Okta device trust integration. This reduces the risks associated with BYOD and unmanaged devices, enabling users to securely work from anywhere, on any device, at any time.

For example, when a user tries to access a SaaS application that requires enhanced authentication, if the device is 'trusted' (managed), then the user would be granted full access. However, if the device is 'untrusted,' then Zscaler could either block the user altogether or redirect the user to browser isolation depending on the policy. Browser isolation provides a pixelated version of the application so an authorized user can still access it, but they can't perform functions such as copy and paste or file transfers.

Dynamically manage access rights

SCIM integration allows organizations to synchronize users and security groups between Okta and Zscaler in near-real time to automatically update, manage, and remove access to company resources based on role changes (adds, transfers, exits).

For example, if an employee leaves the company and the Okta database is updated to reflect the person leaving, that person is automatically removed from the Zscaler database and they can no longer login (vs. with SAML auto provisioning, that employee may be able to access applications based on their previous access privileges until their access token expires or they log out).

Deliver better business results with Zscaler and Okta

Okta and Zscaler deliver an end-to-end zero trust solution that replaces traditional security architectures that leverage VPNs and firewalls. Instead of implicitly trusting users and devices, connections are authorized based on the user's identity, business policies, and context; including user location, device security posture, application being accessed, and content being exchanged. The net results are reduced risk, an improved user experience, and simplified management and deployment.

Learn more:

zscaler.com/partners/okta
Zscaler and Okta Deployment Guide

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 14,000 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.com.**

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 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