Zscaler & Okta

Improve the user experience by simplifying authentication, automating provisioning, and enabling adaptive zero trust access to applications.

Partner Brief

The Market Challenge

In hybrid work environments, protecting employees wherever they work poses challenges for organizations. More remote employees across different locations using multiple devices creates more points of vulnerability. Users get frustrated with the need for separate credentials for cloud vs. on-premises applications, and by the latency caused by VPNs and firewalls.

For IT and security teams, managing multiple point products to ensure appropriate access to corporate resources is complex and expensive. Remote work and cloud adoption have expanded the attack surface, complicating security. To make things worse, the cost and impact of breaches have risen significantly. Burdened with a variety of disconnected tools, IT security teams face fragmented visibility and struggle to balance risk mitigation with the user experience.

Integration highlights:

- Enable seamless single sign-on (SSO) and multifactor authentication (MFA) for fast, secure access to applications and an improved user experience with SAML and OIDC integrations.
- Dynamically manage application access policies and automate provisioning via SCIM to simplify life cycle management.
- Contain threats and enable adaptive zero trust access, up to and including Universal Logout, by exchanging risk signals in real time through the Shared Signals Framework (SSF), delivered by the Zscaler Deception and Okta ITP integration.

The Solution

Let's Start with, "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.

Zero Trust and Continuous Authentication with Okta + Zscaler
Okta and Zscaler deliver a cloud-based, zero trust security solution that combines Okta's robust identity management capabilities with the Zscaler Zero Trust Exchange™ platform.

The first step to implement zero trust is to confirm the user is who they say they are. As the leading identity provider, Okta enables an organization's employees, contractors, and partners to safely use any technology they need, powered by their identity. This covers every part of the identity life cycle, from governance to access to privileged controls. Okta's identity-centric approach to zero trust ensures the right people have access 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 serves as an intelligent switchboard that securely connects users and applications.

Once a user is authenticated via Okta, the Zero Trust Exchange inspects all traffic and validates access rights based on the user's identity and context using the principles of least-privileged access. This ensures users can only access applications they're authorized for, and makes applications invisible to unauthorized users preventing them from being discovered and exploited.

Together, Okta and Zscaler deliver a cloud-based 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

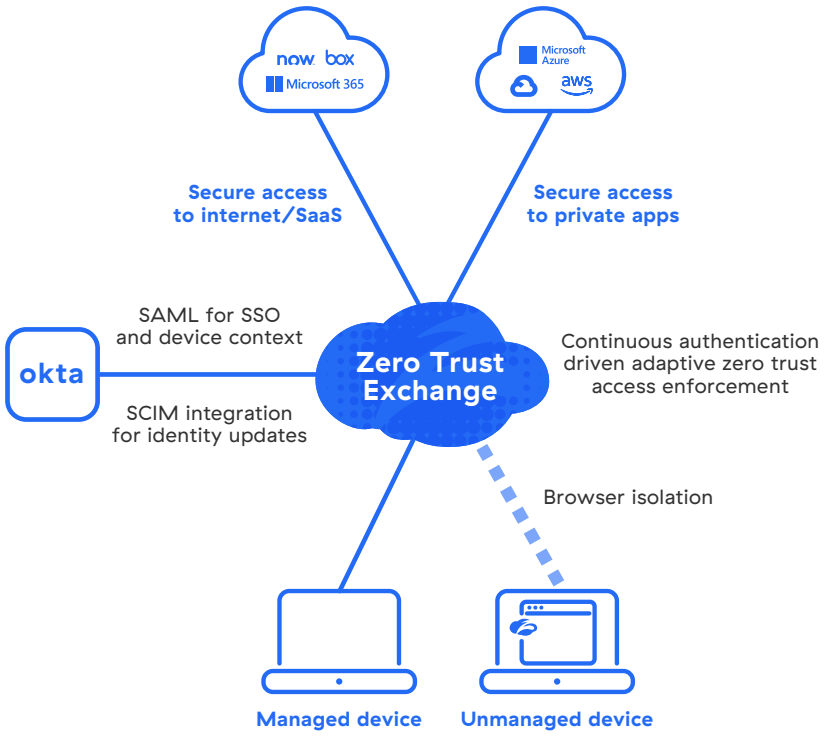
Okta and Zscaler integrate using industry-standard authentication protocols, including Security Assertion Markup Language (SAML) and OpenID Connect (OIDC). SAML and OIDC enable seamless authentication for capabilities like SSO and MFA, which improve the user experience and enhance security.

Zscaler and Okta also support the System for Cross-domain Identity Management (SCIM) for automated provisioning and life cycle management, ensuring the real-time, API-based synchronization of user information for role changes (i.e., adders/movers/leavers). SCIM provisioning reduces the time and effort spent on manually ensuring that only authorized users have access to the appropriate resources.

Additionally, Zscaler and Okta support Open Authorization (OAuth), an open standard for authorization that enables applications to obtain limited access to a user's data without giving away a user's password. A critical timesaver in modern work environments where the average employee switches job-critical applications multiple times a day, the OAuth protocol seamlessly passes authorization from one application to another, all while protecting the user's username and password.

Finally, Zscaler Deception integrates with Okta Identity Threat Protection (ITP) to contain threats from compromised insiders or targeted external attacks. The integration supports adaptive security measures and continuous authentication to ensure zero trust security policies are enforced in real time. Zscaler Deception uses decoy systems and data to send high-fidelity risk signals to Okta using SSF, which Okta can use to make authentication-based decisions, up to and including enforcing universal logout.

> "Our seamless integrations with Okta help customers provide continuous authentication and zero trust access to applications without compromising on security or user experience."
>
> **—Punit Minocha, EVP, Business and Corporate Development, Zscaler**



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 and OIDC integrations enable strong authentication to verify user credentials and provide zero trust access to only the required resources, regardless of where those users are located.

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).

Mitigate and contain identity risk
The integration between Okta Identity Threat Protection (ITP) and Zscaler Deception enables comprehensive defense against identity-based threats. Risk signals from Zscaler are sent to Okta, allowing real-time automated responses to mitigate risk up to and including Universal Logout.

Zscaler Deception delivers high-fidelity, early detection of targeted attacks and insider threats through the use of decoy systems and data. By sharing these validated threat signals with Okta ITP, organizations can trigger real-time access policy changes and targeted mitigation actions based on confirmed indicators of compromise.

This powerful integration enables policy-based actions and workflow-driven responses in Okta for identity-related risk events in real time, empowering organizations to configure countermeasures that can mitigate further risk.

Customer Benefits

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 integrations for single sign-on (SSO), multifactor authentication (MFA), and life cycle management (LCM).

Continuous Authentication and Universal Logout: Maintain user identity verification throughout the user's session to detect anomalies or potential risks in real time. If suspicious activity is detected, take proactive actions like session termination using Universal Logout, triggering adaptive policy-based actions on the Zscaler platform.

Conclusion

Deliver better business results with Zscaler and Okta

Okta and Zscaler deliver a cloud-based zero trust solution that replaces traditional security architectures that leverage VPNs and firewalls. Connections to applications 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. Additionally, by integrating Okta ITP with Zscaler Deception technology, organizations can confidently prevent cyberattacks arising from identity-based risks.

Learn more at zscaler.com/okta

Download our Zscaler and Okta Deployment Guide

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at **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