Solution Brief March 2023

Deliver seamless authentication and security to cloud-based applications

Securely connect users, devices, and applications over any network, regardless of location.

Key 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 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 & reduce 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

The adoption of cloud-first strategies continues to expand to support today's work-from-anywhere environments. But as applications move beyond traditional on-premise 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.

This leads to the need for a new zero trust approach that replaces traditional security architectures.

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.

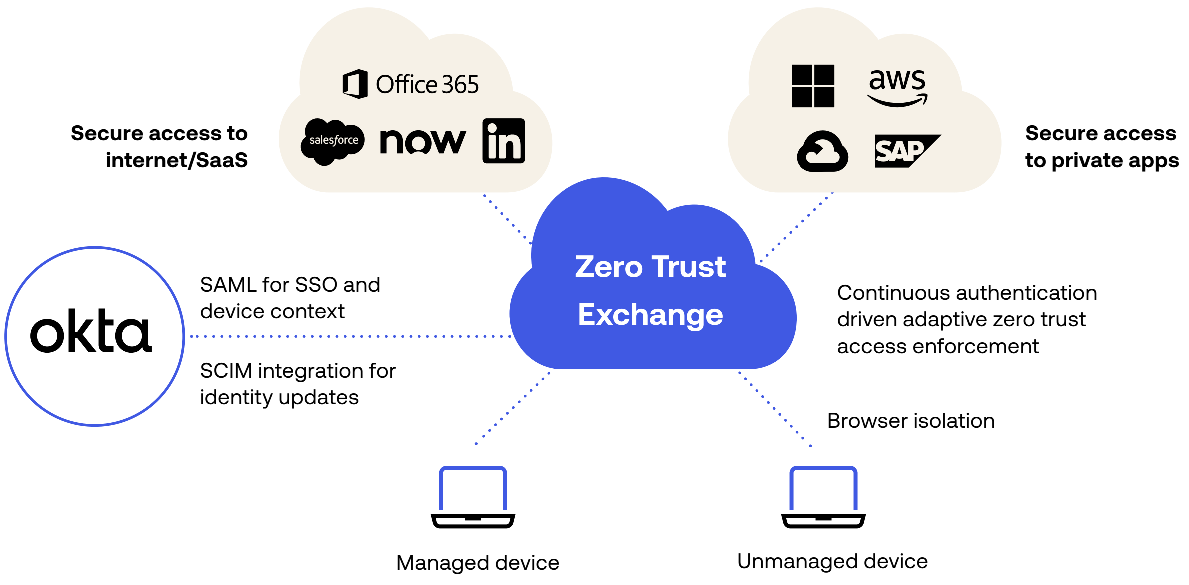
Supporting Zero Trust Architecture with Okta + Zscaler

Okta has an identity-centric approach to Zero Trust, securely connecting the right people to the right technologies at the right time to empower remote workforces. Zscaler's Zero Trust Exchange platform securely connects users and applications so nothing reaches applications without the platform allowing it, ensuring your resources can't be 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. 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. Risk-based access provides a seamless user experience and increased security when needed.

Zero Trust starts with identity

Our integration uses industry standard authentication protocols, including SAML and SCIM. The first step to implementing a zero trust strategy 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 access to applications is authorized based on the user.


Secure access to internet/SaaS
Office 365
salesforce
now
in
aws
SAP
Secure access to private apps
Zero Trust Exchange
okta
SAML for SSO and device context
SCIM integration for identity updates
Continuous authentication driven adaptive zero trust access enforcement
Browser isolation
Managed device
Unmanaged device

Key Use Cases

Verify user identity

Okta maintains credentials about the user ID for verification. The SAML integration enables strong authentication to verify user credentials and provide zero trust access to only the required resources. SAML authentication also allows organization to auto provision new users.

For example, once a user logs into Okta, Okta sends the user and group information 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, they are already in the Zscaler database and 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. 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 or redirect the user to browser isolation depending on the policy.

Dynamically manage access rights

The 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.

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

For more information on this integration, visit okta.com/partners/zscaler
If you have more questions, please contact our sales team at okta.com/contact-sales