Partner Brief

Zscaler & Beyond Identity Integration Solution Brief

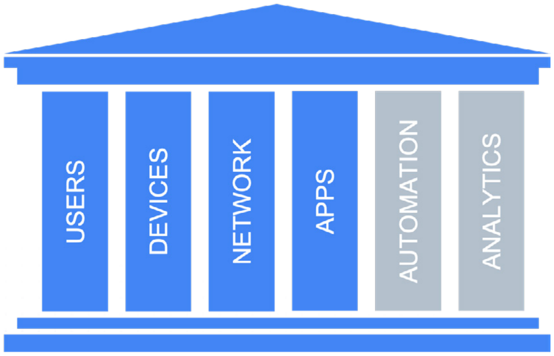
Organizations today are challenged by increased network architecture complexity, phishing, ransomware and sophisticated credential theft that includes the ability to bypass traditional forms of MFA.

Companies support complex network architectures with on-premises, cloud and hybrid segments and applications. Securing these with a high degree of certainty and low risk is a persistent challenge for network, operations and security teams. In addition, credential phishing and legacy MFA attacks continue to increase in volume and impact.

How can users securely and easily access applications and dispersed network services?

How to Solve

Extend the reach of your zero trust program with a focus on securely and continuously authenticating users and devices while protecting networks and delivering workload access.



NIST Pillars of Zero Trust[1]

Figure 1: NIST SP 800-207: Zero Trust Architecture

The solution requires three key components: zero trust network access (ZTNA) to secure networks and applications, unphishable secure authentication, and the evaluation of the device security control settings upon initial access and on a continuous basis.

Required capabilities for unphishable MFA and ZNTA

- Protect applications and networks with always-on threat protection based on identity and context.
- Authenticate securely who and what are requesting access to your applications.
- Evaluate regularly if the connecting device meets your organization's security posture requirements.

Solution

The combination of the Zscaler Zero Trust Exchange that provides secure access to applications plus Beyond Identity's Secure Workforce to validate users and devices delivers these needed capabilities.

Zscaler, the industry leader in ZTNA, allows direct and secure connections to applications based on the principle of least-privileged access, which means that no user or application is inherently trusted. Connections are authorized based on validation of the user's identity, risk-based context, and business policy.

Beyond Identity provides the user and device validation required for phishing-resistant, zero trust authentication and identity-centric zero trust.

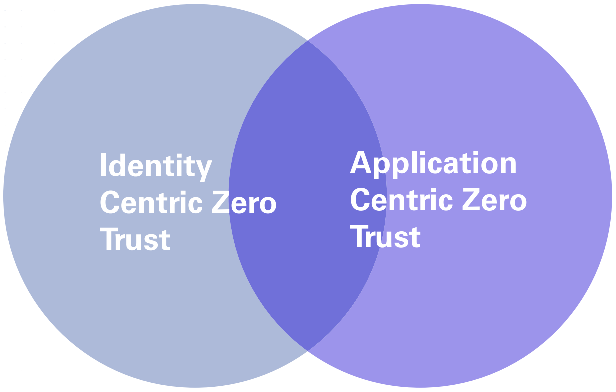


Figure 2: Intersection of Application and Identity centric zero trust initiatives

This synergy achieves a high degree of certainty on who and what are accessing your network and applications and if they are authorized to do so.

Features

Increase security with passwordless authentication for Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA). Minimize risk by eliminating passwords, the most exploited threat vector.

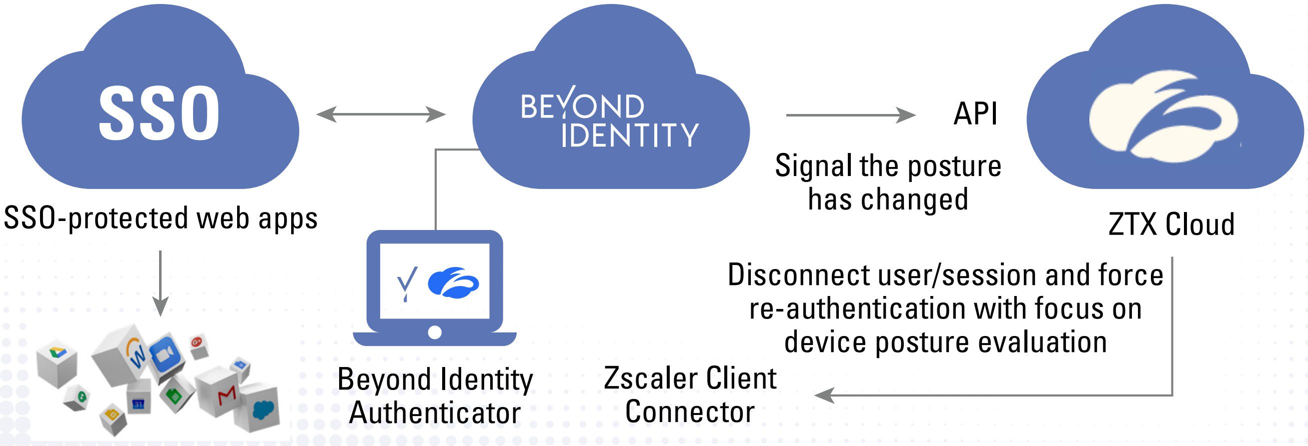
Validate device security controls for all connected devices. Prior to authentication, confirm the device meets your organization's security requirements. If not, deny access via policy directives.

Assess on a continuous basis that connected devices remain aligned with security prerequisites. For example, confirm disk encryption or Endpoint Detection & Response (EDR) has not been disabled and remains active during the connected session.

Minimize risk by disabling access when the risk of the identity or endpoint falls out of compliance with policy. Beyond Identity continuously checks device security settings. If a setting is found to fail policy, it signals Zscaler to log the user out and the user must re-authenticate. Access will not be granted until the device posture comes in line with policy.

Reference Architecture

Figure 3: Zscaler + Beyond Identity Integration architecture


SSO
SSO-protected web apps
BEYOND IDENTITY
API
Signal the posture has changed
ZTX Cloud
Beyond Identity Authenticator
Disconnect user/session and force re-authentication with focus on device posture evaluation
Zscaler Client Connector

Key Benefits

- Combining the Zscaler Zero Trust Exchange with Beyond Identity's identity-centric zero trust solution reduces the risk of two of the most targeted attack vectors - the individual and their device.
- The joint solution strengthens a zero trust architecture and minimizes the attack surface by validating the user and device and enabling secure access to applications.
- Device security checks and continuous reassessment moves security to a proactive stance, actively disconnecting non-compliant devices.

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

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.