SCALABLE, IDENTITY-CENTRIC ACCESS WITH APPGATE ZTNA AND PING IDENTITY

Overview

Appgate ZTNA (Zero Trust Network Access) delivers identity-centric, policy-based access control that enables secure and efficient access for users, devices, and workloads—regardless of location. Built to operate across hybrid and multi-cloud environments, Appgate ZTNA supports integration with a wide range of Identity Providers (IdPs) using standard protocols like LDAP (Active Directory), LDAP certificate, OIDC, RADIUS and SAML. Ping Identity is a trusted leader in enterprise identity and access management, offering scalable solutions for Single Sign-On (SSO), adaptive authentication, identity federation, and robust Multi-Factor Authentication (MFA). Organizations choose Ping for its flexibility, standards-based architecture, and ability to enforce secure, seamless access across complex IT ecosystems.

Together, Appgate ZTNA and Ping Identity strengthens Zero Trust strategies by serving as the authoritative source of identity, enabling dynamic access decisions based on real-time identity context and risk signals.

How it Works

Appgate ZTNA and Ping Identity work together to deliver secure, streamlined access by separating authentication from access enforcement. Ping Identity acts as the identity authority, validating users through SSO and MFA while assessing contextual risk signals. Appgate ZTNA consumes this identity data and enforces access policies in real time, dynamically creating encrypted network segments based on identity and context. This combination enables continuous, adaptive Zero Trust access that adjusts to evolving risk and user behavior.

- **Authentication via Ping Identity**
  Users initiate login through Ping Identity using SSO and MFA; Ping verifies credentials and evaluates risk signals (e.g., device, location, behavior).
- **Token Exchange and Identity Federation**
  Upon successful authentication, Ping issues a token (SAML assertion or OIDC ID token) to Appgate ZTNA—this token contains user attributes and group memberships.
- **Policy Evaluation and Access Granting**
  Appgate ZTNA consumes the identity token, evaluates contextual policies (user identity, device posture, time, location), and establishes an encrypted network segment tailored to the user's permissions—"a segment of one."
- **Continuous Validation**
  Access is continuously monitored and re-evaluated, changes in identity posture (e.g., session risk, expired token, device health) can trigger session termination or reauthentication.

Benefits

- **Stronger Security Posture:** Combines Ping's advanced identity verification, MFA, and risk signals with Appgate's identity-centric ZTNA controls to enforce least privilege access and minimize attack surfaces.
- **Consistent, Frictionless User Experience:** Enables seamless SSO and authentication workflows across all environments—cloud, on-premises, and hybrid—without requiring users to reauthenticate or navigate inconsistent login experiences.
- **Reduced Operational Overhead:** Centralizes identity and access policies, reducing complexity for security teams and streamlining user onboarding, offboarding, and policy updates.
- **Adaptive and Context-Aware Access:** Leverages Ping's risk-based authentication and Appgate's dynamic policy enforcement to adjust access based on real-time user, device, and network context.
- **Vendor Flexibility and Future-Proofing:** Appgate ZTNA is IdP-agnostic, allowing organizations to use any standards-compliant identity provider without rearchitecting access controls.

Conclusion

Integrating Appgate ZTNA with Ping Identity empowers organizations to implement a modern, Zero Trust approach to access control that is both secure and scalable. By combining Ping's robust identity services—including adaptive authentication, MFA, and federated SSO—with Appgate's dynamic, identity-centric enforcement engine, organizations can protect critical assets without compromising user experience or operational efficiency.

This integration ensures that access decisions are informed by real-time identity intelligence and enforced through encrypted, least-privilege network paths. Whether supporting a global remote workforce, enabling secure contractor access, or extending modern identity workflows to legacy systems, Appgate ZTNA and Ping Identity provide the foundation for resilient, future-ready access strategies. Together, they help organizations strengthen security posture, improve operational agility, and embrace Zero Trust without adding unnecessary complexity.

BUSINESS-CRITICAL USE CASES

Secure Remote Workforce Access: Enforce adaptive, identity-based access for remote users accessing critical systems or data.

Third-Party and Contractor Access: Provide secure, time-bound access to vendors or partners with full identity verification and dynamic policy enforcement.

Hybrid Cloud Access Control: Manage access to on-premises and multi-cloud workloads with unified policies tied to Ping-authenticated identities.

Secure Access to Legacy Applications: Extend Zero Trust access controls and modern identity workflows (SSO, MFA) to legacy systems that were not built with native support for modern authentication standards.

MFA-Driven Access for Sensitive Applications: Require Ping MFA for users accessing high-risk or compliance-sensitive systems.

SSO Across Heterogeneous Environments: Deliver consistent login experiences across legacy, on-premises, and cloud-native applications.

ABOUT APPGATE

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.