Optimize Your Zscaler Private Access Controls

Reach

Find and Fix Misconfigurations and Activated Unused Security Capabilities

Zscaler Private Access (ZPA)

Zscaler Private Access (ZPA) is a cloud-delivered Zero Trust Network Access (ZTNA) platform that provides secure access to private applications without exposing them to the internet or requiring traditional VPNs. ZPA connects users directly to authorized applications based on identity, device posture, and access policies, eliminating the need to place users on the corporate network.

Key Capabilities

- **Zero Trust access** to internal applications
- **Application-level segmentation** and access control
- **Identity-aware** policy enforcement
- **Secure access** for remote users and hybrid work environments

The Configuration Challenge

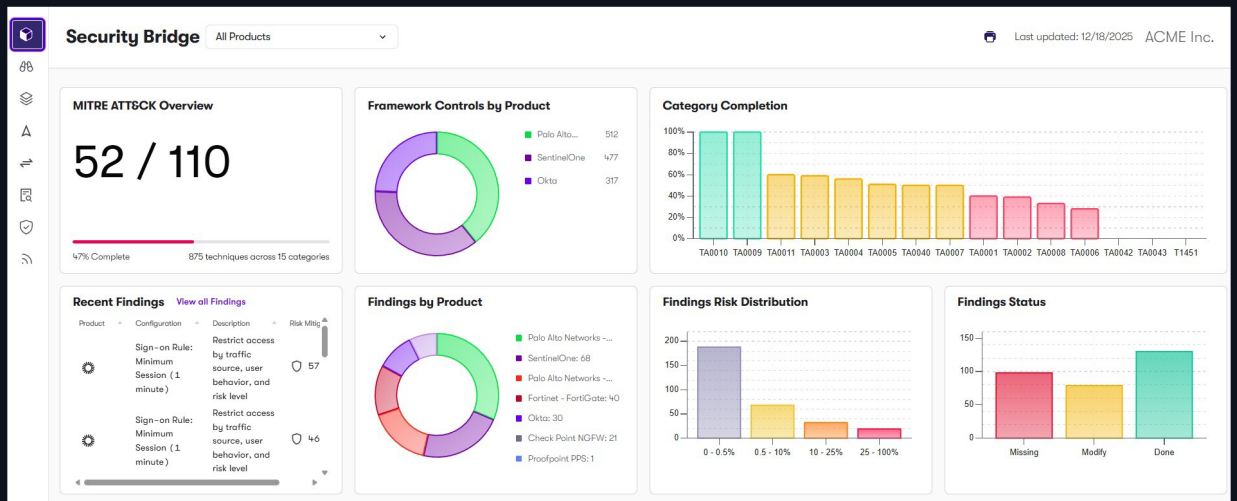
ZTNA platforms like ZPA depend heavily on correct access policies and application segmentation. Misconfigurations can unintentionally expose applications or allow excessive access. Overly broad application segments and permissive access policies can allow unmanaged devices to connect, weakening Zero Trust protections and increasing lateral movement risk.

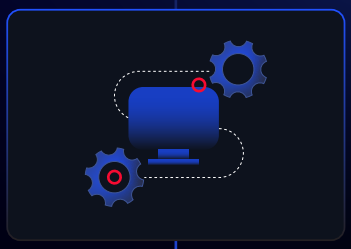
Common Misconfigurations

- **Insufficient application segmentation,** such as grouping applications too broadly, weaken the benefits of Zero Trust segmentation.
- **Misconfigured identity-based access policies** may not properly enforce identity or device posture requirements.
- **Overly broad application access policies** may allow users or groups to gain access to more applications than necessary.
- **Incorrect connector configuration or incomplete application definitions** may create unintended access paths.

Reach Supercharges Your Zscaler ZPA Security Controls

Reach connects to Zscaler Private Access to analyze application access policies, segmentation configurations, and identity-based access controls. By continuously evaluating how ZPA policies are implemented, Reach identifies access misconfigurations and policy gaps that weaken Zero Trust protections.



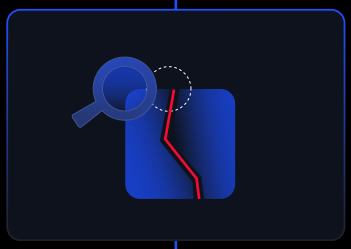


Application access policies and user entitlements

Reach analyzes access policies and entitlement configurations and identifies overly broad access permissions or excessive user privileges so that organizations can enforce least-privilege access to private applications.

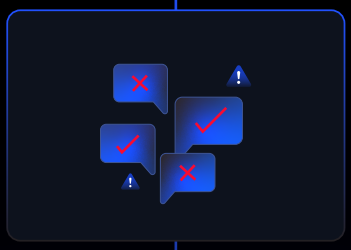
Application segmentation and access grouping

Reach analyzes how applications are grouped and segmented within ZPA and identifies overly broad application segments or insufficient segmentation so that organizations can limit lateral movement and better isolate sensitive applications.



Identity and device posture enforcement settings

Reach analyzes identity-based access policies and posture enforcement controls and identifies missing or underutilized device posture requirements so that organizations can ensure only trusted users and healthy devices can access private applications.



Application connector configuration and deployment coverage

Reach analyzes connector configurations and application access paths and identifies misconfigured connectors or incomplete application definitions so that organizations can maintain secure and reliable connectivity to private applications.

Access policy consistency and configuration drift

Reach analyzes policy logic and rule precedence and identifies conflicting rules or configuration drift so that organizations can maintain consistent Zero Trust access enforcement across all applications.

Reach + zscaler

Together, Zscaler ZPA and Reach help organizations maintain secure, identity-driven access to private applications without exposing internal resources to unnecessary risk. Reach optimizes ZPA controls in order to strengthen least-privilege access controls, reduce lateral movement risk, and provide continuous validation of access policies. By optimizing ZPA configurations, organizations strengthen Zero Trust access to internal applications.

Learn More reach.security/connect | Webpage