zscaler™ | Reach

Optimize Zscaler Security Controls

Find and Fix Misconfigurations across your Zscaler Private Access (ZPA) and Zscaler Internet Access (ZIA) Deployments

Joint Solution Brief

Optimize Your Zscaler Internet Access Controls

Find and Fix Misconfigurations and Activated Unused Security Capabilities

Zscaler Internet Access (ZIA)

Zscaler Internet Access (ZIA) is a cloud-native security platform that provides secure internet and SaaS access for users, devices, and workloads through a zero trust architecture. It replaces traditional on-premises network security appliances with a cloud-delivered secure web gateway and firewall – enabling inline inspection of traffic and SSL/TLS decryption to stop advanced threats and prevent data loss.

Key Capabilities

- **Secure Web Gateway (SWG)** for inspecting and filtering internet traffic
- **SSL/TLS inspection** to detect threats hidden in encrypted traffic
- **Cloud firewall and access control policies** to regulate outbound traffic
- **Data Loss Prevention (DLP** to prevent sensitive data exfiltration

The Configuration Challenge

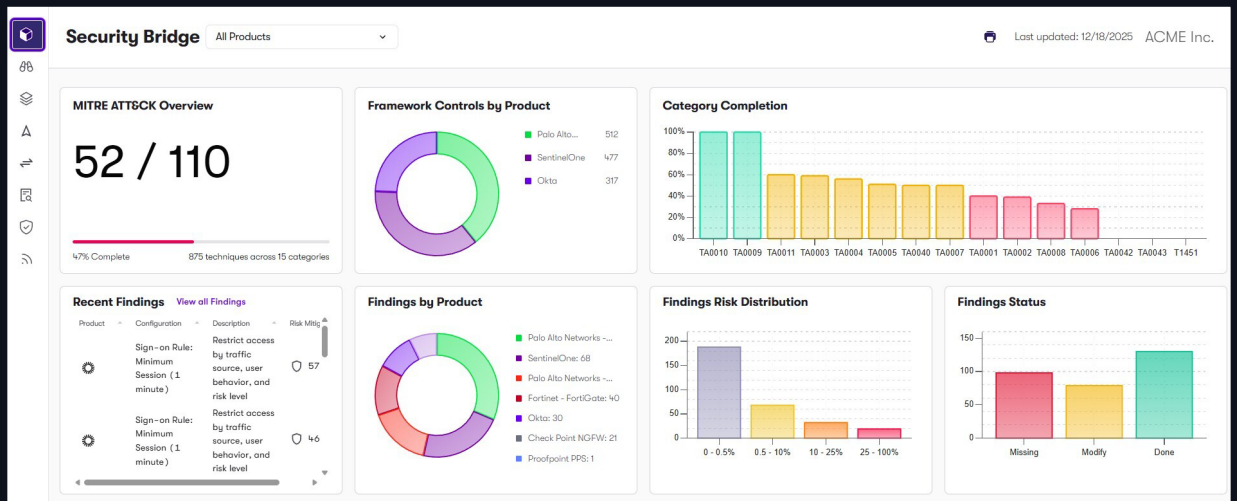
Zscaler ZIA provides deep policy configuration and inspection capabilities, but misconfigured security controls or incomplete deployments can reduce its effectiveness. As policies evolve, rule sprawl and conflicting policy logic can weaken security enforcement. These issues often arise as security teams balance usability with security enforcement across complex environments.

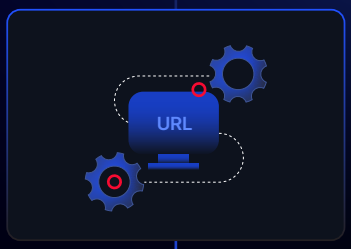
Common Misconfigurations

- **Incomplete SSL inspection coverage,** such as partially enabled encrypted traffic inspection, can allow threats to evade detection.
- **Overly permissive URL filtering policies** may include broad exceptions that permit access to malicious sites.
- **Misconfigured firewall and access control policies** may fail to properly restrict risky traffic.
- **Underutilized threat protection capabilities** such as sandboxing or advanced malware detection may not be fully enabled.

Reach Supercharges Your Zscaler ZIA Security Controls

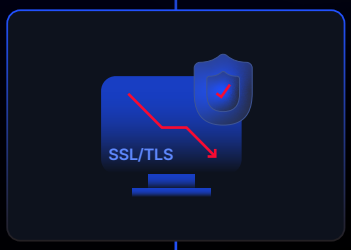
Reach connects to Zscaler Internet Access to analyze web security policies, inspection settings, and access control configurations. Reach develops a genius-level understanding of how your Zscaler ZIA controls are being used (and misused), and then automatically identifies and remediates misconfigurations, activates unused capabilities, stops configuration drift, and validates over time that security posture remains strong.





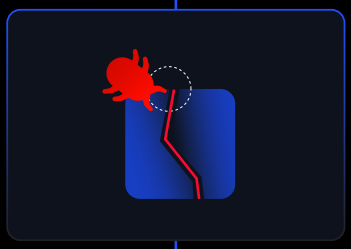
URL filtering policies and web access controls

Reach analyzes web category policies and URL filtering configurations and identifies overly permissive rules, risky category allowances, or policy exceptions that bypass filtering so that organizations can reduce exposure to malicious websites and risky internet destinations.



SSL/TLS inspection coverage and policies

Reach analyzes encrypted traffic inspection settings and identifies disabled SSL inspection, incomplete coverage, or policy bypasses so that organizations can detect threats hidden within encrypted web traffic and strengthen web threat visibility.

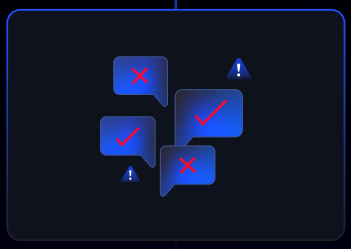


Advanced threat protection and malware inspection settings

Reach analyzes malware detection and sandboxing controls to identify underutilized threat protection capabilities or misconfigured inspection policies. Armed with this visibility, organizations can improve detection and blocking of web-delivered malware and advanced threats.

Cloud firewall and outbound access control policies

Reach analyzes outbound firewall rules and traffic control policies and identifies overly permissive outbound access rules or unnecessary destination allowances. This allows organizations to limit outbound connectivity and reduce attacker command-and-control communication paths.



Data Loss Prevention policy enforcement

Reach analyzes DLP policy configurations and identifies unenforced policies, incomplete inspection rules, or gaps in data protection enforcement. Security teams can better prevent sensitive data from leaving the organization through web channels.

Reach + zscaler

Together, Zscaler ZIA and Reach help organizations maintain consistent, effective protection for internet-bound traffic across their entire workforce. Reach optimizes ZIA controls in order to reduce the web-based attack surface, identify risky access policies, improve detection of web-delivered threats, and increase protection of sensitive data through properly enforced DLP policies. Reach continuously monitors policy configurations to prevent policy rot over time and and maintain strong internet security protections.

Learn More reach.security/connect | zscaler.com

Optimize Your Zscaler Private Access Controls

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

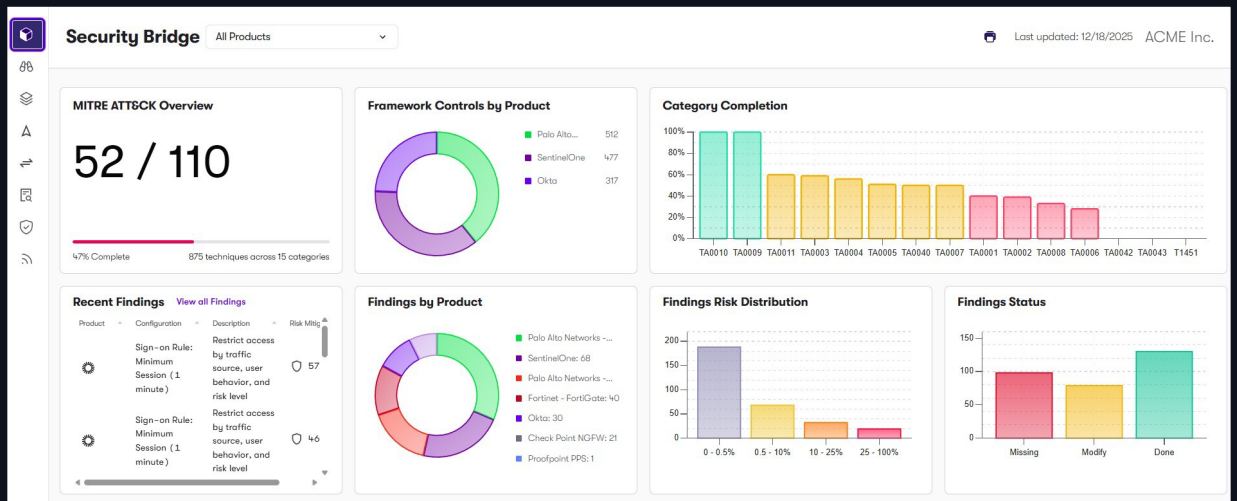
ZTNA platforms like ZPA depend heavily on correct access policies and application segmentation. Misconfigurations can unintentionally expose applications or allow excessive access. Overly broad application segments and permissive access policies can allow unmanaged devices to connect, weakening Zero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

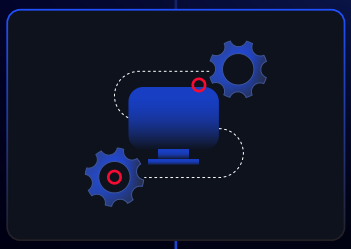
Common Misconfigurations

- **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.



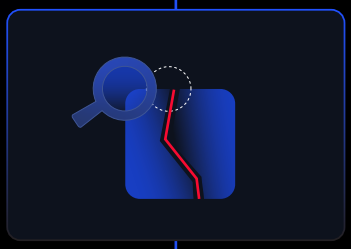


Application access policies and user entitlements

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.

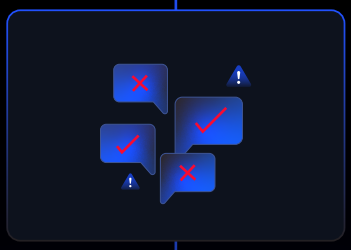
Application segmentation and access grouping

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 | zscaler.com