Optimize Your Zscaler Internet Access Controls

Reach

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

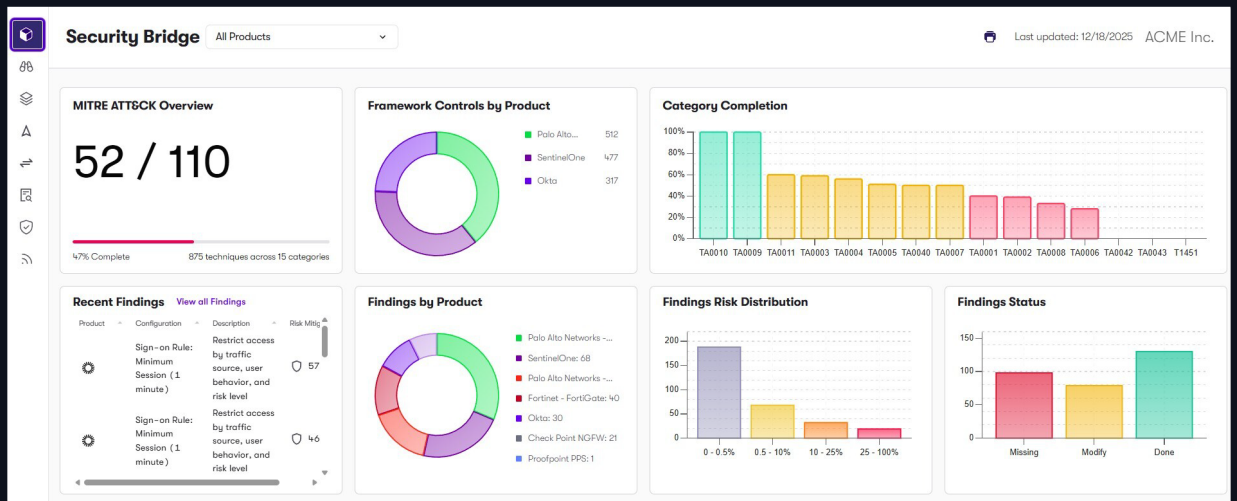
Zscaler ZIA provides deep policy configuration and inspection capabilities, but misconfigured security controls or incomplete deployments can reduce its effectiveness. As policies evolve, rule sprawl and conflicting policy logic can weaken security enforcement. These issues often arise as security teams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

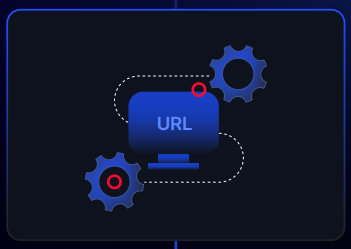
Common Misconfigurations

- **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

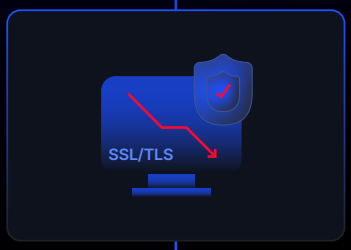
Reach connects to Zscaler Internet Access to analyze web security policies, inspection settings, and access control configurations. Reach develops a genius-level understanding of how your Zscaler ZIA controls are being used (and misused), and then automatically identifies and remediates misconfigurations,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





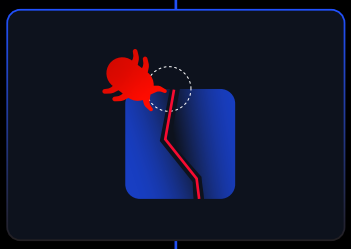
URL filtering policies and web access controls

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.

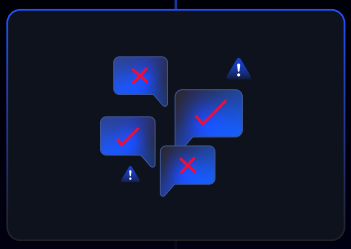


Advanced threat protection and malware inspection settings

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 | **Webpage**