Zscaler AI–Powered App Segmentation

Eliminate lateral threat movement with precise user–to–app segmentation

Remote access solutions like VPNs grant full network access, and they expose IPs and applications to the internet. VPNs extend the internal network to remote devices and, by design, require inbound traffic, exposing a public attack surface.

Without proper network segmentation, a breach in one segment could compromise the organization's entire network. Having said that, implementing segmentation requires complex firewall rules that are difficult to maintain, often disrupt applications, and can complicate access for VPN users. Within large organizations, this often requires high–availability, complex routing, and costly private links.

Solution Overview

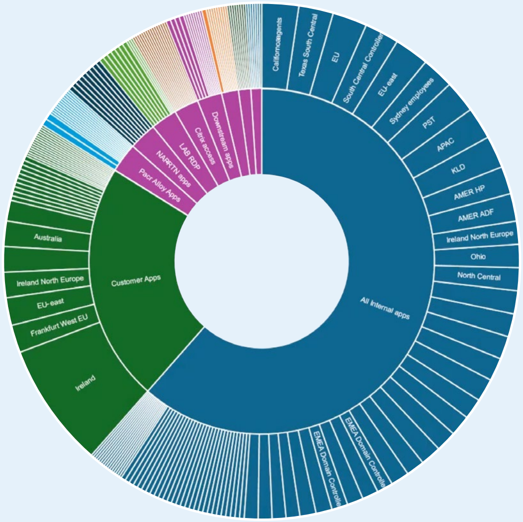
Zscaler Private Access (ZPA) enables application segmentation without needing to segment the network, and restricts users only to the applications they are allowed to access. Application segmentation lets security and IT teams organize applications into discrete groups and provide least–privileged access without having to segment the network. In the event of a network breach, app segmentation helps contain the threat at a more granular level, preventing attackers from accessing other parts of the network.

Zscaler AI–powered App Segmentation, at the core of ZPA, delivers precise user–to–app segmentation and a robust solution for easily deploying consistent policies at scale, eliminating lateral threat movement. It helps you discover all applications within your organization and provides visual insights into which users or user groups have access to which applications.

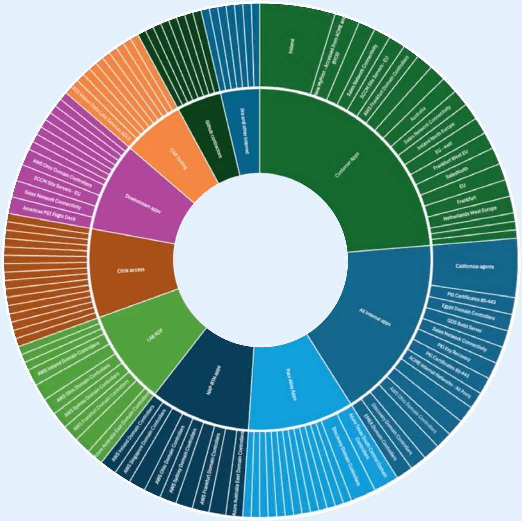
Zscaler AI–powered App Segmentation automatically generates recommendations for app segments and policies based on machine learning models, simplifying implementation.

Accelerate your journey to zero trust segmentation

- Bootstrap apps by importing from customers CSV or 3rd party sources (Qualys, Tenable, ServiceNow) or through app discovery
- Generate AI/ML recommendations for user–to–app assignments, and apply granular policies
- Segmentation Insights provides visibility into users access patterns and policy usage; assess access policy utilization



Discover apps based on wildcards like *.acme.com



Enable secure, least–privileged access to user group

Discover all applications based on wildcards like *.acme.com, fine–tune policies to ensure the right access levels for the right user groups through multiple ML runs. Ensure secure, least–privileged access to all users or user groups.

Solution Benefits

Enhanced security and efficiency with simplicity at scale
Provide least–privileged access to users, including employees and third–parties, through precise user–to–app segmentation. Simplify management by making it easier to configure app segments and policies at scale.

Eliminate lateral threat movement
Dynamically discover apps and drastically reduce the internal attack surface with AI–generated recommendations for app segments and policies.

Faster onboarding of private applications
Easily onboard application information into ZPA from third–party sources like Qualys, Tenable, and ServiceNow, enabling faster implementation of app segments and the creation of granular policies, minimizing errors.

Visual insights into existing app segments, user groups, and policy usage
Gain visibility into users' access patterns and policy usage, allowing you to assess and identify overly permissive rules and determine unused access policy rules.

zscaler™ | Experience your world, secured.™

Zscaler, Inc. (HQ)
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
zscaler.com