Prosimo Zero Trust Network Access for Private Apps

Reduce attack surfaces and provide secure access to applications across any cloud environment without compromising performance.

Zero Trust Network Access (ZTNA) solutions improve security but not without impacting performance while adding operational overhead from complex routing and incomplete visibility. To unleash the true power of the multi-cloud world, organizations should not have to choose between security and performance. Only Prosimo can deliver an unparalleled application experience to any user anywhere without compromising security.

The distributed nature of multi-cloud architectures has made cloud-centric organizations less secure. Today's highly-sophisticated malicious actors can breach the network perimeter through unprotected devices, Software as a Service (SaaS) platforms, or insecure web applications.

They lay in wait and then spread through the network unchallenged. Zero Trust Network Access (ZTNA) solutions prevent this lateral spread by continuously authenticating entities within the network and at every new connection—providing a more efficient and controllable way to grant secure, remote access to applications, data, and services.

Implementing ZTNA requires backhauling traffic to the security services of the corporate network or re-routing to a mid-mile security layer for enforcement. Either option results in a significant impact on latency and bandwidth. This impact on the network leads to a poor application experience for users accessing apps from different geo-locations.

The other option - manually stitching together external security layers between cloud applications and users - is time-consuming, resource-intensive, and hampers network agility.

Organizations are forced to choose: gain peace of mind from a zero-trust security strategy, but lose application performance.

Prosimo Zero Trust Network Access: ZTNA with built-in performance and scale

Built on the Prosimo Application eXperience Infrastructure (AXI) platform, Prosimo Zero Trust Network Access (ZTNA) for Private Applications reduces the attack surface that provides secure access to applications across any cloud environment without compromising performance. This allows organizations to extend Zero Trust access across their multi-cloud environments while ensuring fast, reliable connectivity to the cloud and between regions and cloud providers.

Prosimo makes applications accessible over the Internet behind a context-aware, reverse web proxy that works as a Policy Enforcement Point. It requires authorization and enforces policies based on user identity, context, and risk score calculated from Machine Learning (ML) insights. Due to this deflect before connect mechanism, an air gap exists between application infrastructure and users. While this end-to-end encrypted session runs across public infrastructure, a malicious actor or entity has no idea that the application exists - you can't attack what you can't see.

Limit your exposure

Eliminate the need to expose applications directly to the Internet by building a secure fabric that spans both private and public cloud infrastructure.

Reduce your attack surface

Connect users to applications without exposing your traffic to malicious actors.

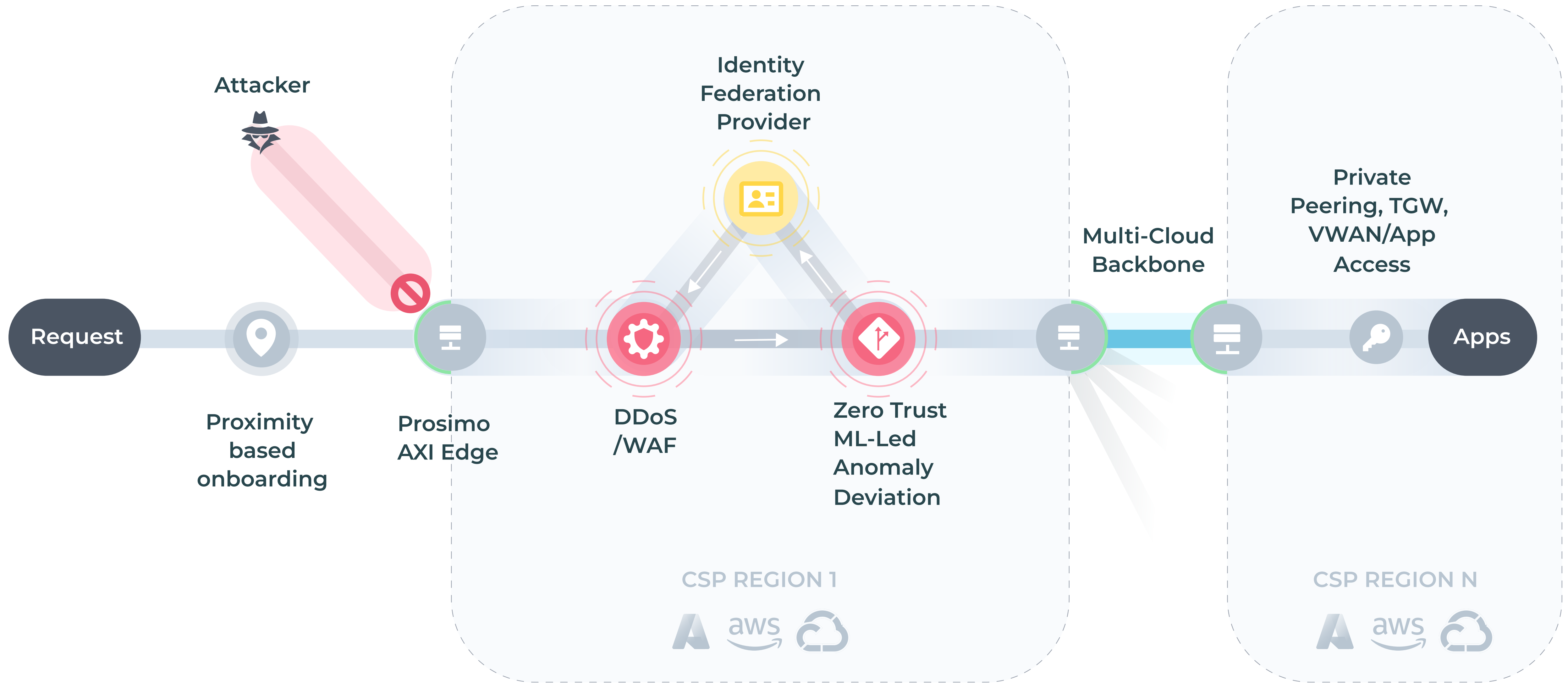
Integrate security within your cloud network

Secure your environments with a built-in identity-aware proxy with MFA, ML-based triggers, WAF, optimization, and agent-less access.

Enable rich policy control

Provide consistency across users, apps, regions and cloud providers for data and cloud compliance.

Prosimo ZTNA Architecture



Prosimo ZTNA Key Features

FEATURE	WHY IT MATTERS
Identity-aware, secure, and private access to apps	Enable users to access enterprise applications from anywhere without exposing applications directly to the Internet by using identity-aware proxies without any agents or VPN clients.
Identity provider (IDP) integration	Prosimo's AXI fabric seamlessly integrates with federated identity providers like Okta, Azure AD, OneLogin, or any IDP with SAML or OAuth 2.0 support for authentication and authorization.
Multiple identity provider support for B2B partners	B2B partners of enterprises can bring their own IDPs with multiple IDP support for the fabric, eliminating the need for enterprise security admins to manage user life-cycle management for third-party users.
Context-aware access policies	Enables granular access control to applications based on user identity and context such as geo-location, SAML attributes, OIDC claims, device certificate, device OS, time of the day, and URL path-based authorization.
Client for all non-HTTPs apps	Provides an ability to access non-HTTPs applications using TCP and UDP ports either through hostnames or RFC 1918 IP CIDR block (e.g., 10.10.10.0/24) using lightweight clients on user machines.
Dynamic risk posture assessment	Checks security health of the end user's device before providing access to sensitive applications based on native device signals, third-party integrations, user behavior analysis, etc., and enforces re-authentication for any irregular behavior.