

DATASHEET:

Prosimo Application eXperience Infrastructure

A modern cloud networking platform that ensures the best application experience without compromising security

IT infrastructure is rapidly changing to meet the needs of digital transformation. Enterprises need an architecture that will scale to support the rapid evolution of their application requirements and a myriad of user access patterns—whether in a hybrid setup with a single cloud provider or in an environment that spans multiple cloud service providers (CSPs).

However, existing cloud networking infrastructure is complex, requiring cloud architects and operations teams to stitch together services across cloud connectivity, security, performance, and app delivery services—along with operational tools from each of these layers. Unfortunately, enterprises today tend to take a one-size-fits-all approach to this problem, leading to a lack of visibility and control while providing no means to accurately measure application experience. The end result is poor application experiences for users, time-to-market delays because of complexity, rising cloud costs, and widened security gaps.

A Modern and Secure Cloud Transit Layer for Multi-Cloud Environments

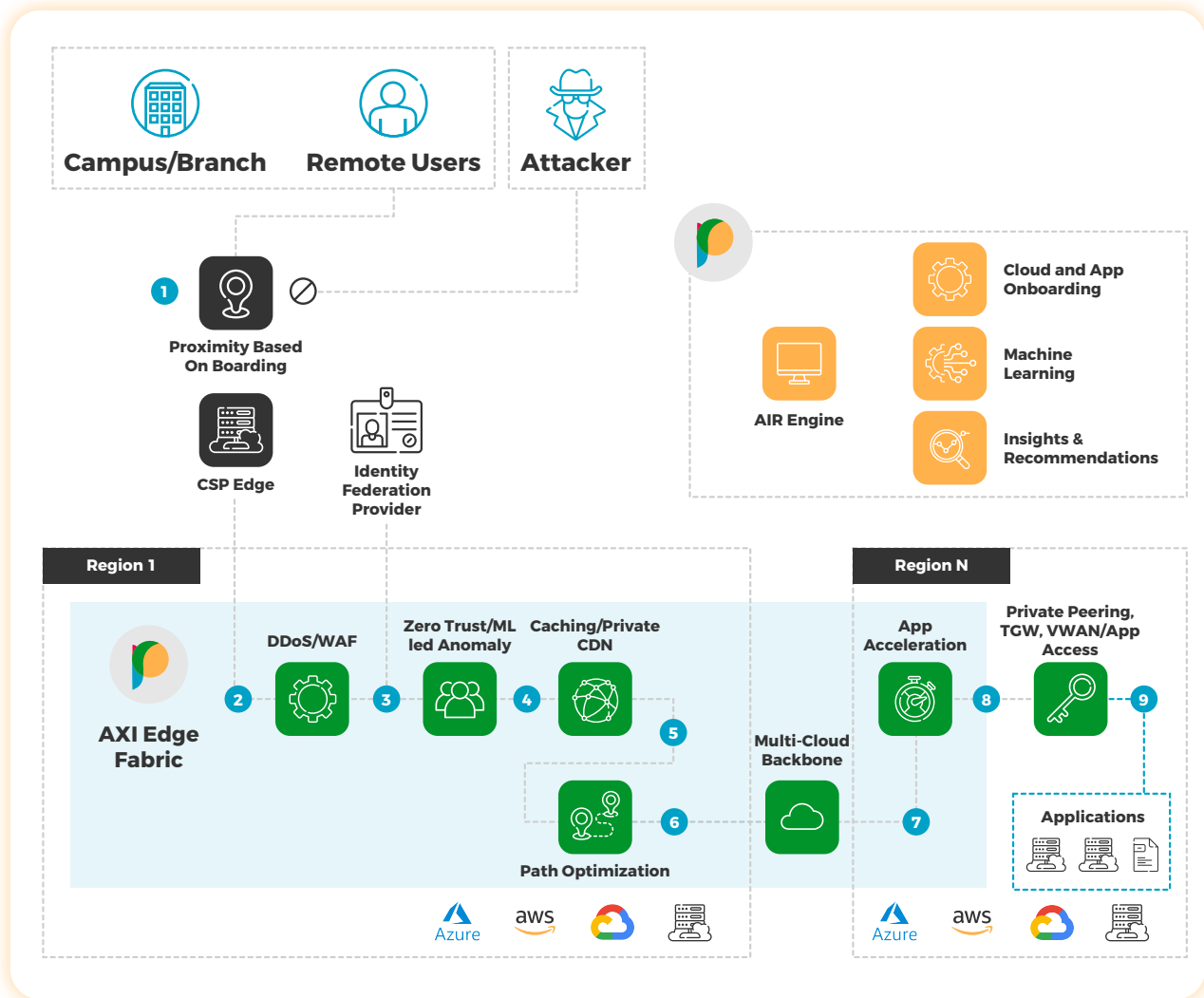
Prosimo eliminates the need for this complexity by serving as a unified cloud networking platform to connect distributed users and DC apps to multiple regions within the same CSP or across multiple CSPs.

It does this by utilizing an application layer mesh network to interconnect user identity and application endpoint for any type of applications in the cloud—including web apps, VDI, PaaS, SaaS, and developer tools. This simplicity allows cloud architects and operations teams to seamlessly onboard applications and easily set policies for security posture and performance lanes to applications.

The Prosimo AXI fabric is automatically built between AXI edges hosted in an enterprise's own cloud subscription, using cloud-native constructs with end-to-end encryption between regions or across clouds. While the service runs in the enterprise's cloud in order for them to maintain full administrative control of the service, it is delivered as a managed PaaS offering. This removes the overhead of managing the life cycles of individual infrastructure services for administrators, such as HA, scaling, and version upgrades. In addition, ML-based recommendations are provided to aid architectural decisions regarding footprint, performance, and cost—all driven by data pertinent to the enterprise's applications and users.

Powered by machine learning (ML) and delivered as a service, Prosimo's AXI platform continuously optimizes application end-user experience and enforces detailed posturing capabilities and app security through inbuilt WAF/Client IP rep. By unifying connectivity, security, and performance in a single stack, AXI simplifies cloud networking operations for the different types of apps that permeate the cloud networking environment.

Prosimo AXI Platform



Inside View of Prosimo AXI Building Blocks

- 1 Proximity based onboarding to CSP Edge (e.g. AWS GA)
- 2 Network-layer DDoS attacks and inspect web requests to detect & block malicious threats like SQL injections, XSS
- 3 Continuous Zero-Trust with Identity federation provider. Including dynamic behavioral checks.
- 4 Serve content if cacheable
- 5 Optimal cloud path - choose based on ML/sensors. Avoiding high latency path, lossy mid-mile and use optimization techniques like connection pooling, Fast TLS, QUIC/HTTP2 to improve application experiences
- 6 Multi-cloud backbone
- 7 Health checkers, accelerations
- 8 Different Peering types - AWS TGW, Private Link, Azure VWAN Hub
- 9 App-to-app and user-to-app last leg connectivity

Zero Trust and Secure Access to Cloud and Data Center Workloads

Identity-aware, secure, and private access to apps	Enables 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 step-up authentication for any anomalous behavior.

Cloud Networking and App Security

Multi-cloud networking	Prosimo AXI builds a multi-cloud networking transit utilizing cloud-native constructs (example: AWS TGW, private link, VPC peering or Azure VWAN hub, Vnet peering, etc.) to provide end-to-end connectivity to application endpoints across regions and VPCs/VNETs without using IPsec or GRE tunnels. This enables the cloud infra team to move from hub-spoke architectures to a modern cloud-native approach that works at application layer.
Cloud-native application load balancing	Provides elastic layer 7 load-balancing capabilities at both global and regional levels with health checks, URL rewriting, and path-based routing.
WAF, DDOS, SSL offload, and IP reputation	Includes an inbuilt web application firewall with the Prosimo core ruleset, modsec ruleset, and rich visibility. SSL offload removes the processing burden on application web servers from decryption and improves response time. DDOS protection at cloud scale and IP reputation provides the extra layer of protection by verifying the source against the known blacklist.
App-to-app policies	Prosimo's AXI fabric enables application endpoints hosted across multiple regions or multiple clouds to connect to each other in a secure and optimized fashion utilizing Zero Trust principles and performance lanes.
On-demand auto-scaling	AXI edges are delivered as cloud-native clusters with inbuilt auto-scaling functions managed by Prosimo, eliminating the need for manual operations.

Performance Optimization for Cloud Apps

Proximity intelligence with L4 optimization

Ensures that users enter the Prosimo AXI fabric to the most optimal edge based on their location, with TCP and HTTP layer optimizations to improve performance.

HTTP(s) optimizations, caching, private CDN

Enables private CDN with HTTP layer optimizations such as content caching, pre-fetching, FastTLS, QUIC/HTTP2, connection pooling, and compression for better user experience.

Multiple performance lanes to cloud

To balance cost vs. performance needs, applications can be set to any of the three available performance lanes, without having to tinker with individual features at DNS, layer 3 routing, or L7 settings individually.

Insights and Integration

Insights: App, users, network, and security

Prosimo's insights framework can provide visibility at the fabric level about all users/all apps or at a granular level for a single user/single application session. This eliminates the need to gather data from different stacks that sit between the user and the application to root out the cause of access problems.

Log streaming

Provides real-time log streaming of logs and insights such as end-user experience score for each session or hourly risk score for users that pass through the fabric.

Integration with SIEM/SOAR

Integrates with platforms like Splunk and Azure Sentinel for security automation and orchestration workflows.

Infra as code (IaC) integration

Supports infra-as-code (IaC) tools such as Terraform to automate fabric deployment steps and ongoing day N changes to fabric policies.

ML-Driven Infrastructure and Security Posture Recommendations

Data-driven cost and performance optimization

Helps enterprises adhere to the cloud cost governance framework by tying infrastructure decisions to balance performance needs vs. cost optimization requirements at a granular level for every application.

Dynamic risk score-based fabric policies

Enables security teams to define access policies based on risk posture of the user based on their recent activities and how they correlate to their baseline to prevent insider threats.

Fabric expansion based on user access

Fabric can be expanded or shrunk dynamically based on the recent user access pattern and the ROI seen for each of the edges in the fabric.

Deliver Application Experience Across Multi-Cloud.

The Right Way.



[www.twitter.com/Prosimo_io](https://twitter.com/Prosimo_io)



www.linkedin.com/company/prosimo-io