Top Global Consulting Firm

PROSIMO AXI CASE STUDY

Consolidating Cloud Infrastructure to Lower Costs and Improve User Experience

prosimo

AT A GLANCE

INFRASTRUCTURE

The firm's fragmented infrastructure started with one cloud but ended with three

INITIATIVES

The three-layer cloud infrastructure blueprint required stitching various services together and spans across 8+ IT initiatives

CHALLENGES

- Complex to manage multi-layered services for application delivery in multi-cloud
- Costly, with overprovisioned resources
- Security gaps
- Lack of visibility for cloud infrastructure and application insights
- Bad user experience

PROSIMO BUSINESS ENABLER

- Uses an elastic and scalable cloud-native infrastructure to help launch business products a lot faster to clients and customers
- Reduces cloud spend by 50 percent or more with a vertically integrated stack consistent across hybrid and multi-cloud
- Makes it easier to adopt multi-cloud and helps in migrating apps to preferred cloud service provider at scale
- Increases employee engagement and productivity with better application experience

PROSIMO AXI TECHNICAL VALUE

- Cost savings with cloud-native blueprint for multi-cloud
- Performance lanes
- Content caching
- Avoid lossy mid-mile by using data patterns
- Context-aware secure access
- Layer 7 optimization
- Peering using cloud-native constructs and direct connect with Citrix Workspace

"I started to rethink whether the traditional four-layer model with network underlays, tunneling using overlays, network-focused security, and hub-and-spoke architectures was how I wanted to build for the cloud. **I wanted to modernize my infrastructure to focus on user identity and workload endpoints—not IP addresses, VPCs, and subnets."**

- Enterprise Cloud Architect

COMPANY PROFILE

As the firm started adopting multi-cloud (Azure and AWS) at scale for business-critical applications for customers and partners, productivity tools for their employees, and CI/CD tools for DevOps using both monolithic and modern cloud-native containerized apps/functions distributed across multiple regions, the existing stack started unmasking the operational challenges. In order to make it all work, the cloud infrastructure team started with the existing cloud blueprint and stitched together a range of disjointed services. Virtual appliances and mid-mile services sprawl quickly resulted in lack of visibility and control, complexity in managing multi-layer stacks, fragmented security control, increased cloud infrastructure costs, and poor user experience.

CHALLENGE

With a global presence, hundreds of offices, and thousands of users accessing business-critical applications, this accounting firm helps organizations create value by delivering quality in their consulting services.

In recent years, the company's network infrastructure team has been tasked with cloud adoption initiatives, particularly focusing on multi-cloud (AWS and Azure) to take full advantage of differentiated features from cloud service providers with varying cloud costs and to address the requirements of specific applications and tools. The infrastructure team developed a cloud blueprint based on their previous Azure deployment and wanted to replicate it for AWS, which divides their infra stack in three different layers—access, transit, and application layers.

PAINPOINTS OF EXISTING CLOUD BLUEPRINT

- At the cloud access layer, remote users from different global locations used VPN to connect to enterprise applications and tools in the cloud, while SD-WAN provided branch connectivity to cloud apps through the transit layer. Clients and customers were provided with access to Internet-facing applications and sites using ALB for SSL termination and load balancing.

- A network-based firewall layer was employed for port and protocol-level access control.

- At the cloud transit layer, SD-WAN controllers were configured in HA pairs in different availability zones (AZs) for branch-to-cloud connectivity, network firewall virtual appliances for network segmentation, and ALB for load balancing.

- The applications were distributed across multiple VPCs, AZs, and other AWS regions that required peering between VPCs within the region and across regions. To address this requirement, the cloud infrastructure team deployed the multi-cloud networking solution stitched together with the rest of the security, ALB, and SD-WAN stacks. In a traditional hub-and-spoke architecture, multi-cloud gateways and controller appliances were deployed in multiple AZs in HA pairs to provide a meshed network peering and other regions through the transit layer across VPCs, regions, and AZs, and with other cloud service providers through routed IPsec tunnels at the network layer.

- In order to provide the best possible experience and application security for public-facing apps, the team took a service chaining approach and integrated the public app endpoints with WAF + CDN stitched with MCN to route the traffic to the application back-end layer.

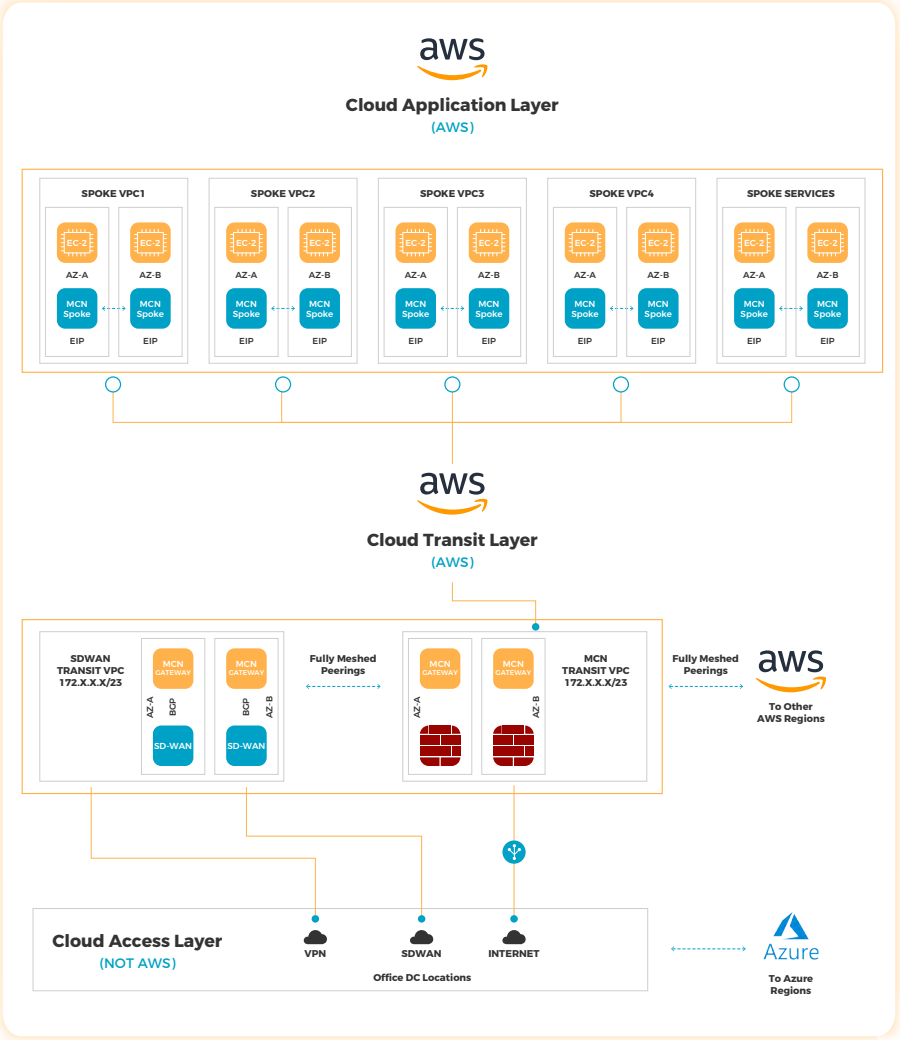
- To make all of this work based on identity, an SSO proxy was then tied to the application load balancer.

- And to debug problems, a layer of NPM and network monitoring was tied in, in addition to sending logs over to SIEM.

Existing cloud blueprint for single AWS region

As depicted in the high-level architecture, the three-layer cloud infrastructure blueprint requires stitching various services together and spans across eight different IT initiatives.

- VPN for remote
- SDWAN for branches
- Multi-cloud Networking
- FW for segmentation
- WAF + CDN for external apps
- AppGW for ALB
- SSO proxy
- NPM



Where it all started to fail

As per the recommended vendor best practices, most of these appliances required for connectivity and security were deployed in HA pairs, including MCN gateways and hubs in different availability zones, firewalls, and load balancers to provide active/standby functionality.

Soon enough, the team realized that they couldn't scale by simply applying the same hub-and-spoke architectures and HA principles used traditionally in data centers 20 years ago.

As the global workforce started experiencing performance issues and the time needed to identify and mitigate issues increased, the ops team found it difficult to cobble together insights gathered from multiple monitoring and vendor dashboards in an effort to gauge the health of the infrastructure. Network and TCP port-level insights made it even more difficult to quickly fix application layer experience issues.

All these operational challenges made it highly difficult and time consuming to bring new business apps to the marketplace for clients, resulting in delayed project timelines, lost revenue, and user experience issues that were hard to diagnose and fix. The team also lost visibility into infrastructure cost and accidental overspending with overprovisioned resources.

THE SOLUTION

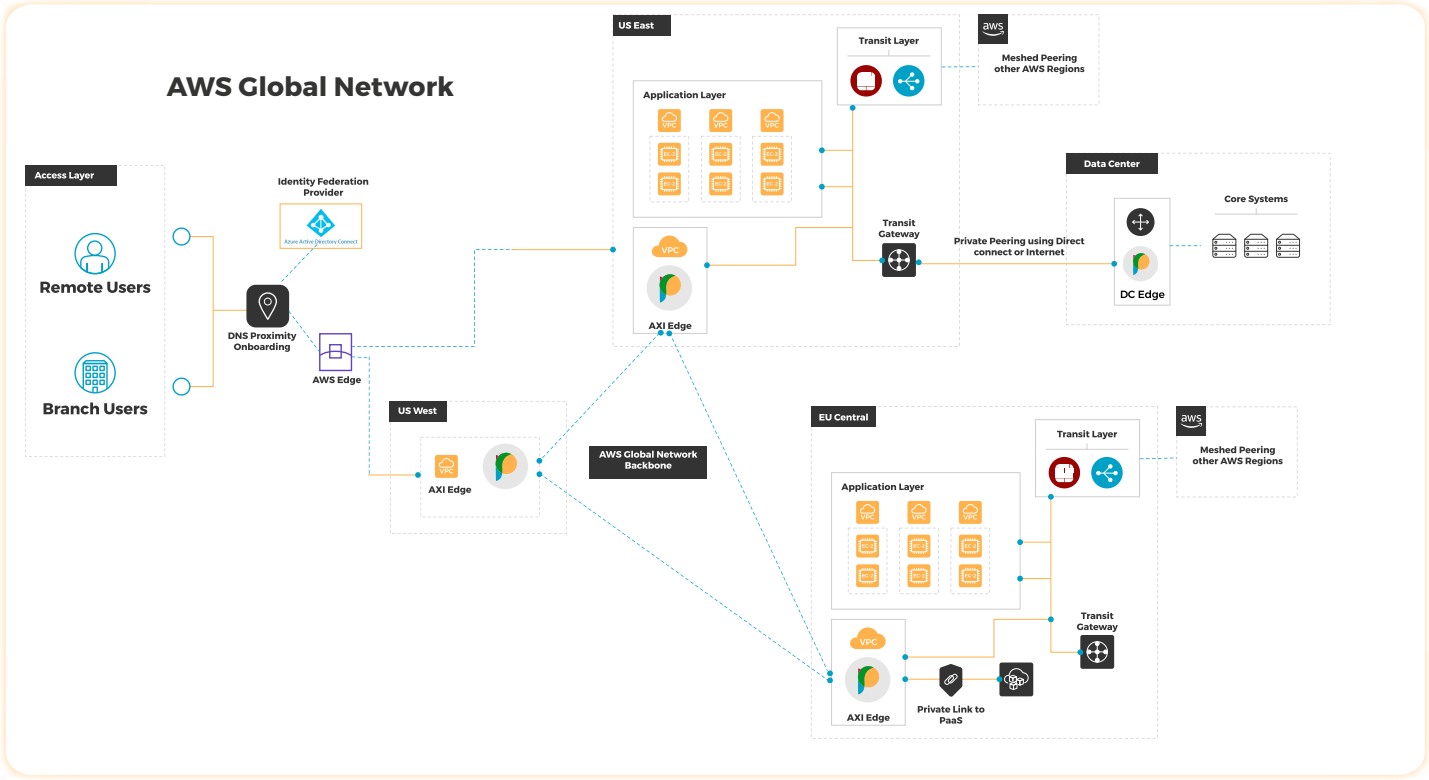
Prosimo's cloud-first approach is different

To take full advantage of the scale, elasticity, and economy of the cloud for distributed workloads in AWS, the accounting firm engaged with Prosimo to jointly develop a new cloud-native blueprint that is equally applicable and consistent across multi-cloud and their data center environments. This new cloud-native blueprint needed to provide the required application experience using cloud-native constructs, without reinventing the wheel, and it needed a modern architecture to better deliver application performance to the firm's globally distributed workforce and customers.

> "With Prosimo AXI, we were able to transform and consolidate the infrastructure stacks all the way from application to cloud network and transport layers. This change gave us a lot of flexibility to **add applications to our preferred cloud service provider without spending cycles in building** hub-spoke architectures with traditional SD-WAN and multi-cloud networking vendors. Our users got optimal application experience along with Zero Trust Access through Prosimo AXI."
>
> - Enterprise Cloud Architect, Consulting Firm

Prosimo cloud-native blueprint for AWS regions

(Equally applicable to any cloud)



During the controlled pilot for a set of users across three different locations, the cloud infrastructure team deployed Prosimo AXI (Application eXperience Infrastructure) edges in AWS US East and EU Central regions, as well as in the data center to front-end a diverse set of applications. AXI edges, which are packaged as modern cloud-native Kubernetes clusters, run various microservices to deliver Zero Trust Access for users, Layer 4-7 optimization with private CDN, cloud networking orchestration, application security, and deep visibility powered by machine learning to make data-driven decisions in improving user experience. Configuring and publishing applications to users is a straightforward task driven by a wizard-based model to configure these settings and policies—all from the same management pane:

- Required application settings
- Connectivity/peering orchestration in multi-cloud suited for different applications
- Traffic lanes for optimal experience optimized for cost and performance
- Zero Trust and WAF policies

After initial deployment for a few apps, the team used Terraform scripts to automate the infrastructure and application provisioning at scale.

THE RESULT

Faster performance, lower costs, greater visibility, and improved security

Prosimo AXI was able to simplify the firm's cloud infrastructure stack significantly—taking it from seven to eight disparate IT initiatives solved with traditional hub-and-spoke and virtual appliances to a more vertically integrated modern stack delivered as a service, with full administrative control and compliance over the datapath to the cloud team. The team was able to slim up the stack without stitching multiple services, and they used a single consistent platform to get complete visibility and insights all the way up to actual packet and byte bucket level. This level of visibility helped the team quickly identify and fix application experience issues for any given set of users at specific time stamps.

Prosimo AXI using the cloud backbone and CSP edge infrastructure was able to deliver a high-performance application experience to all the firm's users accessing applications from different locations—without any VPN agent software on users' devices—through a highly scalable and elastic fabric. The cloud-native stack, Zero Trust Access, application security (WAF), traffic optimization, multi-cloud networking, and deep visibility made it possible to use machine learning and data usage patterns to reduce cloud consumption and costs, which was a huge advantage to the firm's cloud infra and ops teams. Prosimo AXI enabled them to repurpose the same cloud blueprint for any cloud service provider and data center for user-to-app and application-to-application access with a cloud-first approach.

With Prosimo AXI, the firm was able to:

1. Deliver improved performance for users accessing apps by more than 80 percent.

2. Reduce deployment time to five to seven minutes, compared with their previous deployments that required hours to set up disparate sets of services and virtual appliances in HA pairs.

3. Significantly cut infrastructure costs for stitching together services (firewalls, load balancers, SSO proxies, multi-cloud networking, CDN, WAF, etc.) by 50 percent.

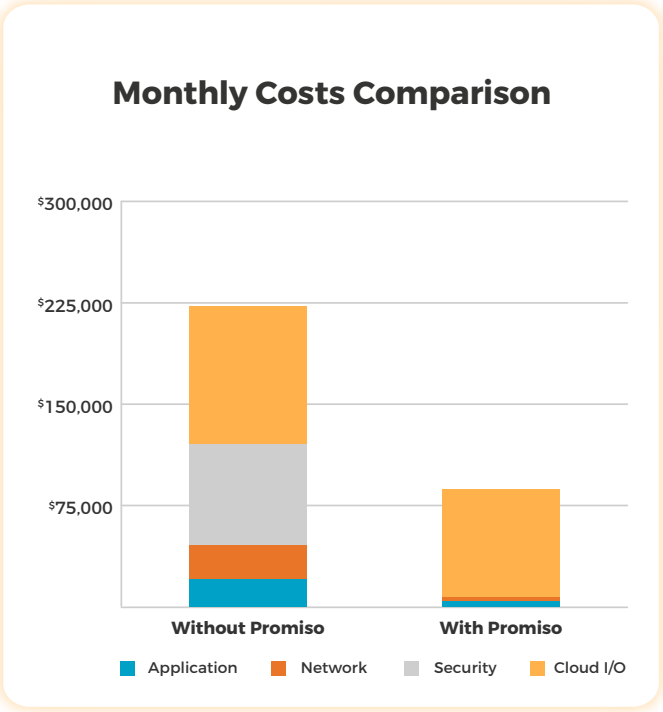
4. Provide continuous authorization and posture assessment based on dynamic risk scoring to reduce the attack surface by 99 percent.

5. Bring up additional infrastructure based on ML-led recommendations provided by Prosimo AIR engines in minutes for additional user locations, application hosting regions, and other cloud service providers.

Delivered value in terms of cost and infrastructure consolidation

- Consolidated VPN/ZTNA, MCN, CDN, SD-WAN & NPM stacks into one common infra
- Common platform for AWS, Azure, GCP
- App diversity - HTTP/HTTPs, PaaS, modern & VM based apps

- 70% reduction in page-load times
- ~60% cloud savings for infrastructure
- Deployed in a day - remotely



Learn how you can reimagine application experience in a multi-cloud world.

Contact optimize@prosimo.io today to learn more.

prosimo

https://twitter.com/Prosimo_io

www.linkedin.com/company/prosimo-io