Five Steps to Simplify a Multi-Cloud Adoption Strategy

Radically rethink application experience for users anywhere in the multi-cloud era with true visibility and control.

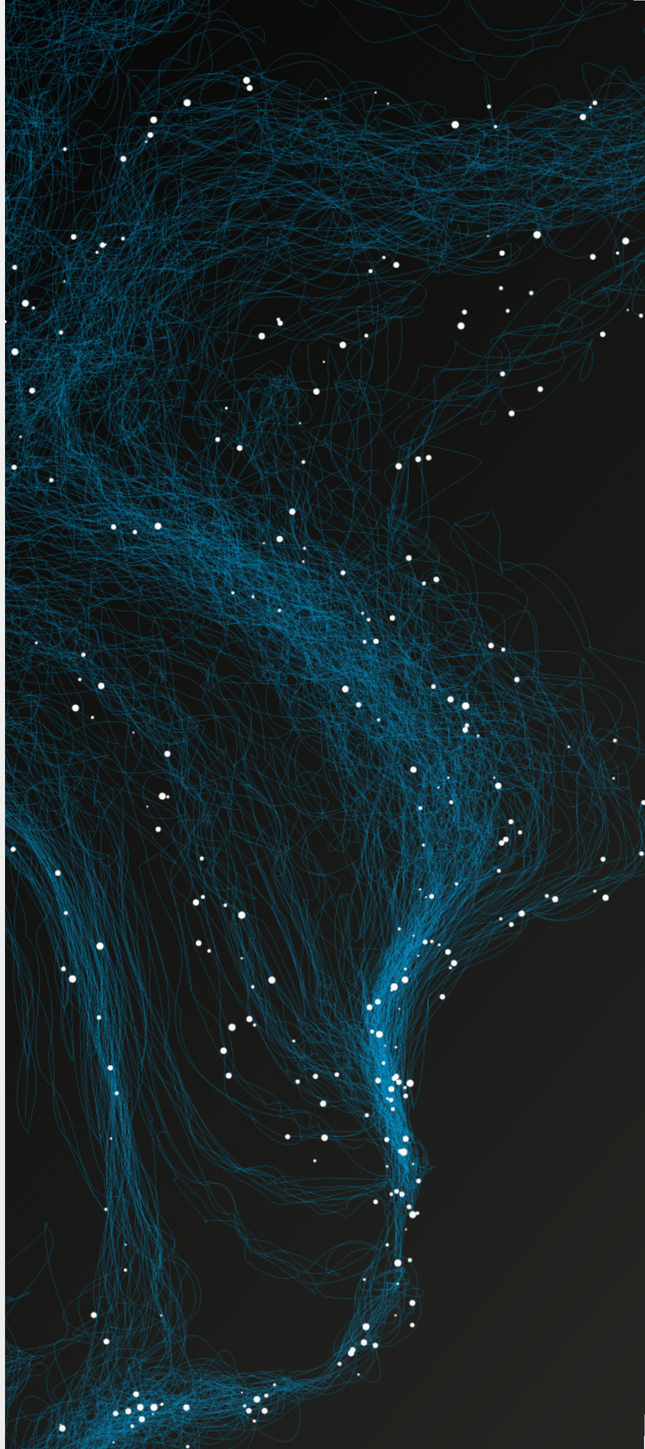
prosimo

The world is being digitized, and even the most technically savy organizations are at risk of being left behind. Modern applications are fragmented, highly distributed, and cloud native. They're often spread across various cloud providers and on-premises infrastructures in a truly multi-cloud environment. Users no longer log in from the corporate headquarters—instead, they access the tools and information they need from remote offices, customer sites, on the road, living rooms, and kitchen tables. Despite these changes, users expect the same application experience they enjoyed in the office.

Cloud architects and operations teams are under pressure to just "make it all work." Unfortunately, they lack the tools to even accurately measure application experience, much less deliver consistent experiences in the multi-cloud world. Instead, they spend the majority of their time stitching together disparate services and point solutions across multiple layers of the application delivery stack—each one with different performance, reliability, and security requirements. The end result is poor application experience for users, increasing infrastructure complexity, more problems for the help desk that are difficult to diagnose and fix, rising cloud costs, and wide security gaps.

But a new world requires a new approach—one that acknowledges the changing realities of modern applications, the future of work, and rising user expectations. It's time to radically rethink how applications can be delivered and accessed in the multi-cloud era with true application experience, visibility, and control.

Cloud architects and operations teams are expected to provide users with fast and secure experiences across all enterprise applications—no matter the underlying infrastructure. Five trends stand in their way.



This eBook will explore how:

Five trends are standing in the way of successful cloud migration

Application eXperience Infrastructure (AXI) can deliver consistent, powerful application experiences quickly and cost effectively

AXI unlocks the power of the cloud

Five simple steps work for starting your cloud migration strategy:

STEP 1
Draw up a migration road map.

STEP 2
Establish a Zero Trust policy framework for users and applications.

STEP 3
Standardize performance.

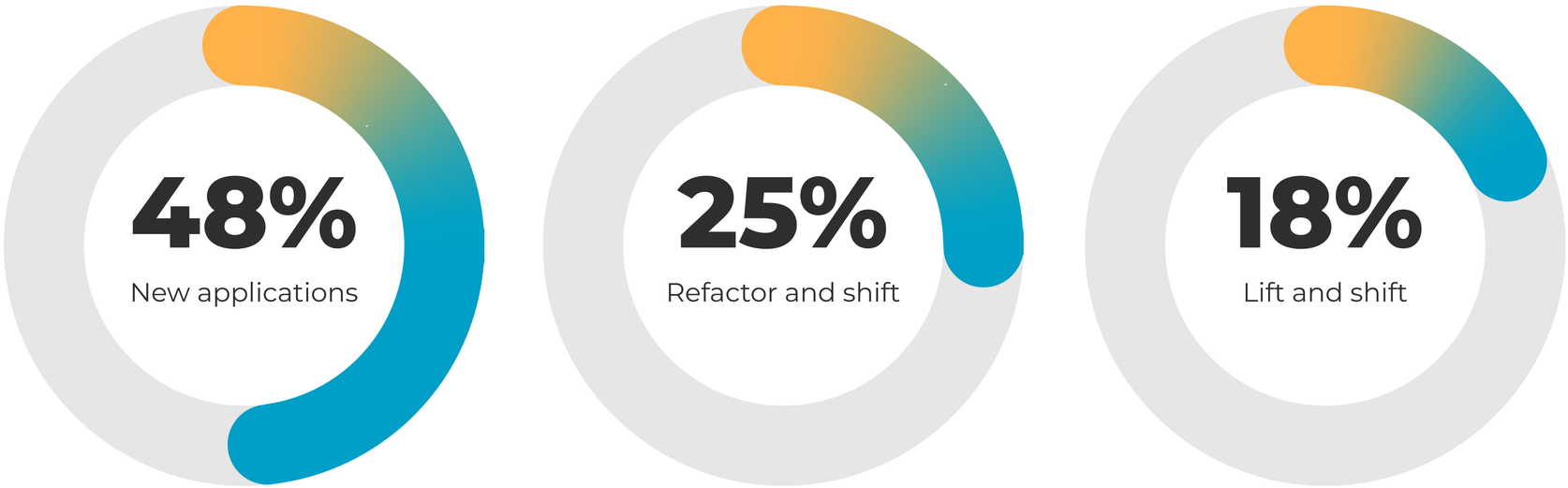
STEP 4
Ensure that you're ready for AI/ML and the power of big data.

STEP 5
Simplify cloud infrastructure operations.

Five Trends Are Standing in the Way of Successful Cloud Migration

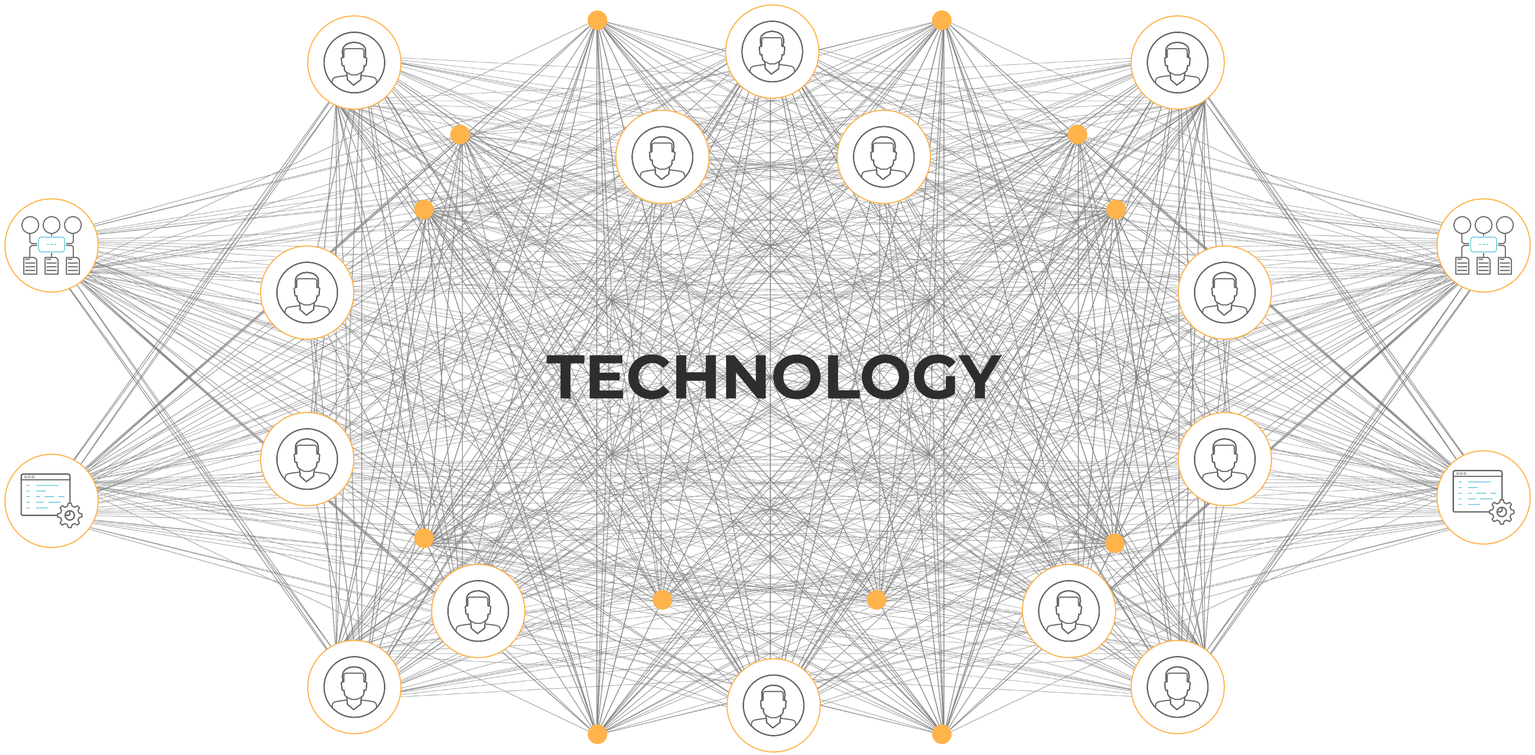
1 **Organizations are typically at different stages in their cloud migration strategies**—often within the same organization. A one-size-fits-all strategy for moving modern and legacy applications to the cloud is one reason that many cloud migrations slow down or fail.

Applications moving to the cloud



2

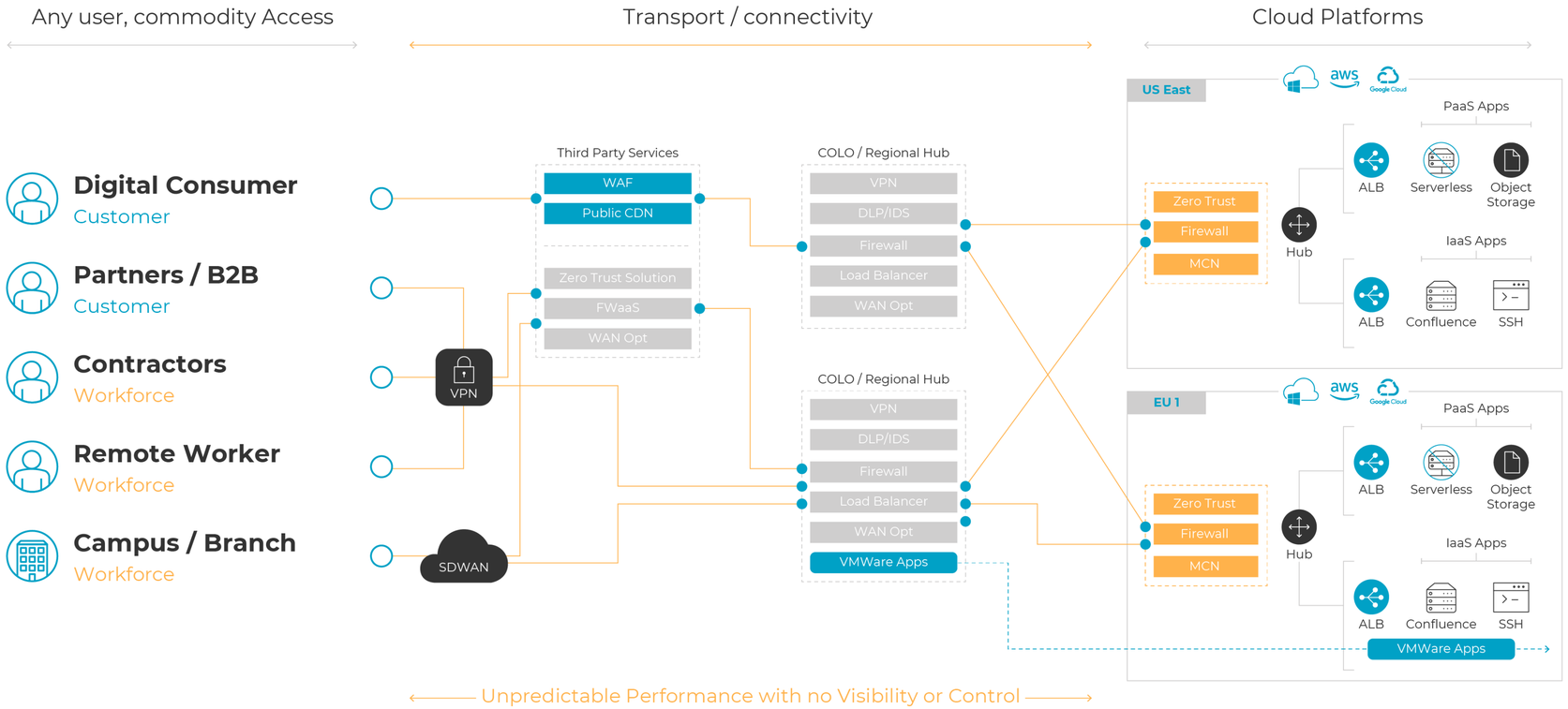
Applications are subject to a complex array of different enterprise policies that are enforced in different clouds and spanning availability, performance security, and compliance. Cloud operations teams are required to stitch together these services from on-premises to cloud service providers and security SaaS vendors in a seamless, frictionless manner—but it's a manual, tedious process that prevents true operational agility.



3

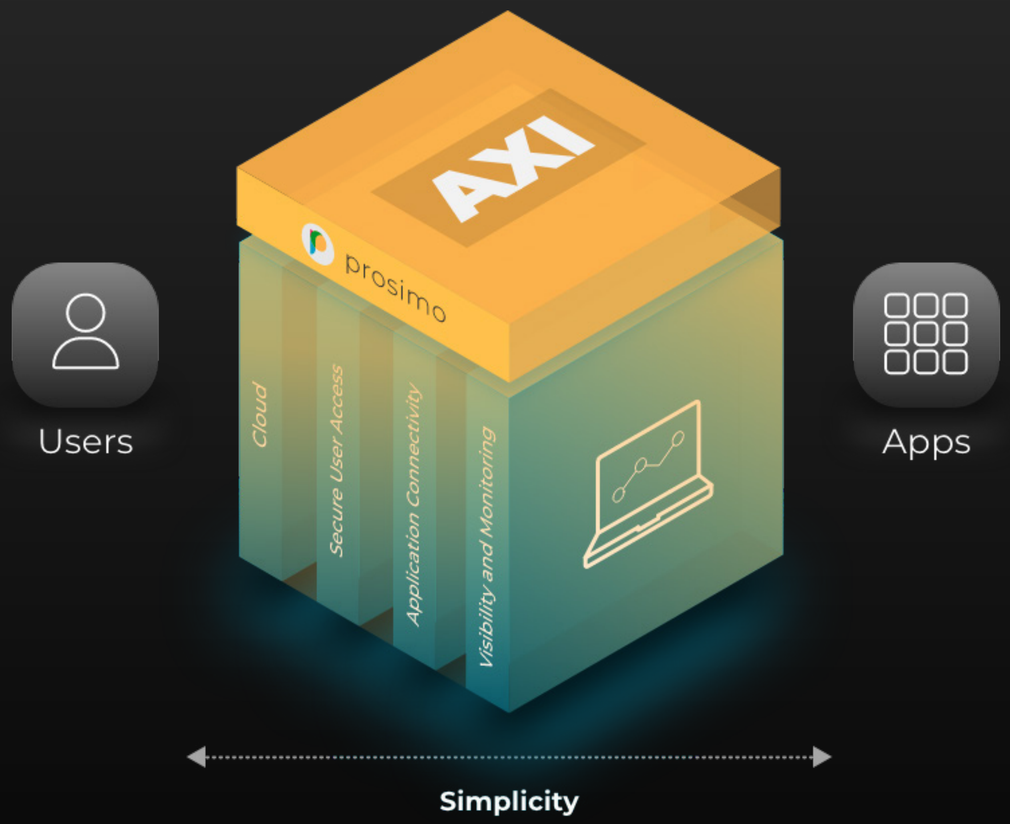
Application experience is directly influenced by the network solutions that users have on the path between the user and the application. Network devices and services that do advanced protocol-level processing and network optimization may interfere with client connectivity and impact application availability, performance, interoperability, and supportability.

Improve Application Experience, Quickly: Before



4 **Infrastructure today is no longer a static pipeline of appliances in the cloud.** Instead, it's extremely elastic, with each user-to-app and app-to-app combination unique. Merely turning some knobs fails to take into account this fast-changing, dynamic nature of infrastructure today.

5 **The complexity and loss of visibility and control into multi-cloud environments** prevents cloud architects and operations teams from measuring application experience. The service level agreements (SLAs) should be able to measure application performance in terms of page load time, reduced the attack surface, cut cloud costs, and meet any experience requirement across an array of personas.



Gain Visibility and Control Over Application Experience in the Cloud

Application eXperience Infrastructure (AXI) gives cloud architects and operations teams a singles vertically integrated infrastructure stack in which to measure and deliver consistent, powerful application experiences quickly and cost effectively within their administrative control. Powered by data insights and machine learning models, AXI is a decision-focused and results-oriented platform that is easy to use and enables a multi-cloud infrastructure strategy that can deliver apps that are fast, secure, and cost-optimized.

Essentially, AXI makes multi-cloud infrastructure transparent, delivers the desired level of application experience, and ensures context-aware secure access to users. This is done using data-driven insights powered by AI and ML on top of a multi-cloud infrastructure utilizing cloud-native constructs. This gives cloud architects and operations teams complete control into application experiences without stitching together multiple services for secure and optimized application delivery. It also allows enterprises to take advantage of the cost, flexibility, and scalability of the cloud without unnecessary complexities.

AXI Unlocks the Power of the Cloud

Unlocking the power of the cloud with AXI allows organizations to accelerate cloud migration, enable work from anywhere, and drive business agility through app modernization.

Meet Application SLAs

Up to 90 percent improvement in page load time

Shrink Threat Surface

99 percent reduction in app attack surface

Reduce Operating Costs

Up to 60 percent operational savings

Enable Business Agility

90 percent reduction in deployment time

STEP 1 Draw Up a Migration Road Map

Before you embark on any journey—literal or figurative—it's important to take stock of where you are and where you are going. Think about the types of applications you currently have, how they are being used, and what you need to do to optimize performance for your key user demographics. Are some apps already in the cloud? Which ones are on premises and why? How do users access these applications and why are their expectations?

You can then create a phased migration plan for legacy versus modern applications and business-critical apps with low-latency requirements versus less critical apps. This will help you determine the best infrastructure to run and deliver these applications and enable a true multi-cloud environment.

Questions to Consider:

- Why are you migrating your data and application to the cloud in the first place?
- Are you considering a lift-and-shift strategy or a full transformation?
- Where is your IT organization from a skills perspective?
- What's your expected timeline to complete the migration and which apps do you want to move first?
- Does your enterprise employ a barbell approach to infrastructure—one end is a traditional on-premises data center, the other end in cloud native?

STEP 2 Establish a Zero Trust Policy Framework for Users and Applications

The cloud will never fulfill its potential unless organizations are able to extend enterprise security controls to multi-cloud environments. The cloud enforces a shared responsibility model that requires a Zero Trust approach to security, in which users are automatically authenticated and authorized whenever they log in. This ensures identity-based, contextual-aware access to enterprise applications.

Exposing internal applications and access infrastructure to the Internet makes them vulnerable to different vectors of attack, such as DDoS, SQL injection, and other application-layer attacks. Bad actors use ever-evolving techniques to scan enterprise network configurations to discover vulnerable assets and valuable data. We recommend that you isolate applications and access architecture from the public Internet, so they cannot be targeted by malicious actors using open listening ports or known vulnerabilities.

You will need to start by establishing an identity federation and user trust framework for your personas (remote employees, B2B partners, third-party applications, IoT devices, customers, etc.), so you can slowly rollout the framework out to select groups of users. Then prioritize users in three groups:

- **Test lab users who will be responsible for verifying the functional integrity of the application when it is first made accessible in your multi-cloud environment.**
- **External users, such as B2B partners, contractors, and third-party users with a high-risk profile.**
- **Finally, internal users.**

It is critical that high-risk users are onboard first and that you continuously validate and assess them based on a risk profile powered by access patterns.

Questions to Consider:

- Do you use VPN currently to provide access to your applications in the data center or in cloud for your users?
- Is providing Zero Trust access important to your business-critical applications in multi-cloud?
- Is securing data and maintaining administrative control inside your own cloud important to you?
- What percentage of your users are internal versus external, and do you plan to set up a separate identity store for your external users?
- Do you have a centralized Identity framework for all your internal users, or are they distributed across multiple identity islands for every application?
- What threat protection capabilities do you have in place to defend your users, devices, and internal assets?

STEP 3 Standardize Performance

Users and applications today are spread across the world—working in branch offices, at customer sites, or from the dining room table. Cloud architects and operations teams need to ensure the best application performance wherever business takes users by layering advanced networking technologies on top of existing infrastructures. This includes the deployment and orchestration of cloud on-ramp, WAN gateways, multi-cloud networking, content delivery networks (CDN), and global load balancing.

Questions to Consider:

- Which applications are critical to the business and need guaranteed low-latency access from users across the world?
- Which cloud regions are optimal and cover a large set of users? Where do you need to spend on your infrastructure footprint to extend AXI and deliver an optimized application experience?
- Do you have the right tools to measure performance—from users, to cloud, through infrastructure?
- Do you have a well-thought-out road map for how users access apps and how apps talk to each other?

STEP 4 Ensure That You're Ready for AI/ML and the Power of Big Data

Artificial intelligence and machine learning continue to be one of the greatest trends of the decade. Broadly speaking, AI can support three important business needs: automating business processes, gaining insight through data analysis, and engaging with customers and employees. These needs will continue to be more dominant in the next decade. It's important to remember that AI/ML is only as good as the data you feed into the algorithms. Make sure you are able to carefully manage the sets of data, as well as access to the data, and that the data stays within your control. Think about how data lakes can be created, how they are connected, how they need to be secured and made compliance ready, and how you can ensure fast connectivity.

Questions to Consider:

- What is the impact on application experience cause by app and data placement, especially in a multi-cloud world?
- How can you ensure Zero Trust access for data buckets?
- Are you able to restrict private access to data lakes?
- Do you have external controls in place to prevent data exfiltration?
- How can you extend enterprise-level control over cloud-native PaaS (S3/Azure storage/Google BigQuery, etc.)?

STEP 5 Simplify Cloud Infrastructure Operations

Finally, it's time to make your life easier and automate many of the manual tasks that cloud architects and operations teams were previously forced to do. Validate your application-specific SLA scoring to ensure application availability, security, and performance. Then you can confirm your security posture faster by establishing a security automation framework that uses alerting and response automation to block threats.

Questions to Consider:

- What are your SLA expectations for your applications in the cloud?
- Is application performance (in terms of page load time) important for your business-critical apps?
- Have you factored infrastructure cost into your application SLA requirements?
- Would you prefer a modern data-driven model to provide cost and performance improvement recommendations or a static upfront infrastructure configuration?
- Do you have a geographically distributed workforce that requires access to your applications in multi-cloud?
- Would you prefer to develop a skill set for one common platform or for multiple cloud service providers and third-party vendor services to deploy and publish your applications?
- Do you usually have tight timelines to bring an application to market?

Learn more at Prosimo.io

Cloud migration isn't simply a matter of spinning up an instance in AWS and pushing code to a new environment. It requires careful planning, a solid road map, and the ability to automate cloud operations in a seamless, frictionless way. Above all, you need complete visibility and control into public cloud infrastructure and a way to measure and guarantee application experience.

Take our assessment and see how we can improve your enterprise application experience today.

TAKE ASSESSMENT

prosimo