

# Reinventing Enterprise Networks For The Cloud Era



Atif Khan  
CTO and Founder, Alkira



## Table of Contents:

Network Connectivity Is Challenging	04
Do-It-Yourself (DIY) Cloud Networking	05
What About Cloud Orchestration Tools?	07
WAN Evolution In The Cloud Era	08
Cloud Backbone	09
The Alkira Platform	10
Governance In The Cloud	12
Customer Benefits	13
Summary	14

## Glossary of Terms

**CXP** Cloud Exchange Point: is a fully virtualized point of presence delivering an entire network stack with rich network services

**Connector:** is a termination point connecting on-prem and cloud networks

**CSP** Cloud Service Provider: provides a wide range of cloud computing services

**MCN** Multi-cloud Networking: utilizing multiple CSPs to build, deploy, and manage applications and workloads

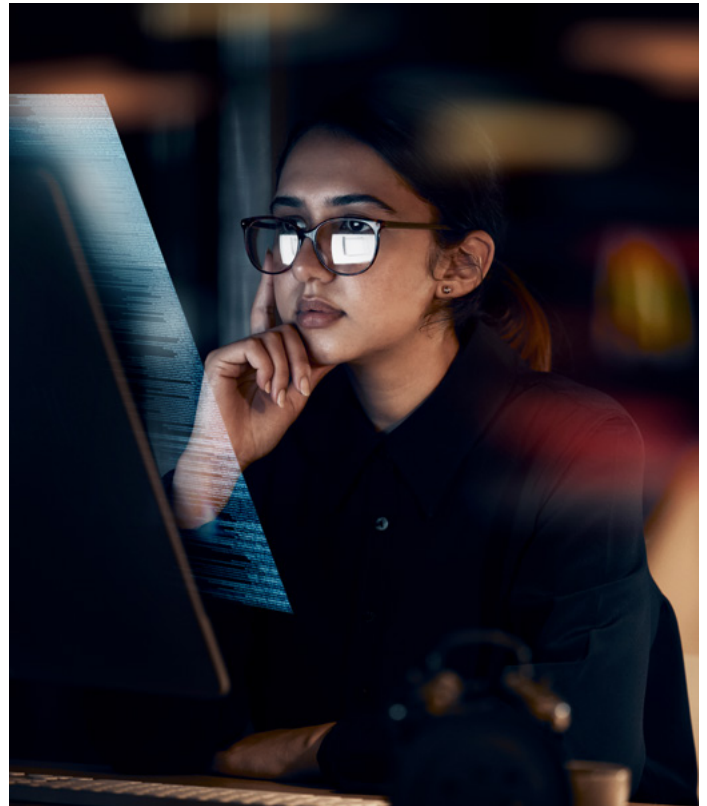


As organizations increasingly transition their workloads and business applications from on-premise data centers to one or multiple public clouds and take advantage of SaaS offerings, networking becomes a challenge. While compute and storage have long inherited cloud attributes and have evolved to become available for as-a-service consumption, networking has not.

It is time for the network to evolve. It is time for the network to be reinvented for cloud with the following key attributes:

- **Delivered as-a-service** with easy point and click consumption and no need for cloud specific network expertise
- **On demand** with ubiquitous ability to be deployed when, where and for as long as needed
- **Global and multi-cloud** connecting on-premise locations to public clouds and SaaS applications, as well as interconnecting multiple public cloud regions or multiple public clouds together
- **Secure with integrated security and network services** and ability to seamlessly insert these services into the desired application flows and provide full operational life-cycle management
- **Elastically scalable** with ability to accommodate real-time growing or shrinking demands for network and network services capacity
- **Highly available** with SLAs to accelerate transition of business-critical applications to the cloud

- **Transparent** with full visibility, monitoring and comprehensive day-2 operations
- **Cost effective** with zero upfront investments, pay only for what you use, and only for as long as you use it



## Network Connectivity Is Challenging

Today's organizations are rapidly transitioning their workloads and business applications to public cloud and SaaS environments, oftentimes working with multiple cloud providers. Even corporate networks with just a handful of locations and cloud instances (VPCs/VNets) have many considerations and use-cases when building a cloud network.

Organizations need to extend their private network infrastructure to one or multiple public clouds, allow and manage distributed Internet exit points, define and manage consistent network and security policies, and achieve deep visibility across both on-premises and public cloud network environments. At the same time, it is critical for organizations to have full day-2 controls with comprehensive troubleshooting and monitoring capabilities for operational excellence.

We can identify several leading use cases and capabilities that are often times required in the typical enterprise cloud deployment.

- Building a global private multi-cloud network that connects on-premise environment to single or multiple public clouds with Internet and SaaS connectivity
- Strict security policy enforcement for intra and inter-cloud traffic via next-generation firewalls, SWG, etc., while autoscaling the network services capacity based on real-time demand
- Application high availability leveraging external (ELB) and internal (ILB) cloud native load-balancers or third-party Application Delivery Controllers (ADCs)
- Remote access and teleworking solutions for mobile users to be able to ubiquitously access cloud and on-premises resources

- Optimized distributed access to SaaS and Internet applications.
- Global cloud network governance with IP address management (IPAM) and ability to leverage network address translation (NAT) to resolve IP address conflicts
- End to end segmentation extended from on-premise environment, including SD-WAN, to the public cloud and across multiple public clouds, irrespective of individual public cloud capabilities
- Mergers and Acquisitions (M&As) or divestitures
- Deep end to end visibility and troubleshooting capabilities for day-2 operations

Current cloud networking methods are slow, difficult and costly with both high upfront investments and high ongoing operational expenses. Each cloud may provide similar capabilities as far as cloud networking is concerned but each cloud is different when it comes to orchestration, provisioning and operation. This in turn forces organizations to acquire deep cloud networking expertise, pursue technology certifications and make human capital investments.



**Current cloud networking methods are slow, difficult and costly with both high upfront investments and high ongoing operational expenses.**



Complex or even moderately complex multi-region and multi-cloud routing requires significant amount of planning and oftentimes tedious time-consuming manual provisioning. Insertion of network services with auto-scale functionality, especially stateful network services like firewalls, further complicates cloud networking environment due to the necessity to engineer symmetric traffic flow. This task becomes almost impossible when the cloud network stretches across multiple public clouds with a need to enforce multi-cloud security policy.

Reliance on cloud native monitoring and visibility capabilities creates operational blind spots that force organizations to procure and operate third-party network management systems.

With the accelerating adoption of cloud and multi-cloud, the network is struggling to keep up with the agility demanded by cloud business needs.

Before discussing how Alkira's Cloud Area Networking, the global cloud network infrastructure as-a-service, dramatically changes the landscape, it is important to review in a little more detail the currently available options, so the contrast becomes even clearer.

## Do-It-Yourself (DIY) Cloud Networking

It might be tempting for organizations to try building their own cloud network using an in-house IT team with cloud and networking experience. With a complex or even moderately complex network and cloud environments, this can prove quite challenging.

### Colocations

Some organizations leverage colocation facilities and interconnection-oriented architectures to achieve the task of connecting on-premise locations to one or more public clouds. Provisioning of direct cloud connectivity through colocations requires first and foremost establishing a colocation footprint in all locations where such cloud connectivity is desired. For organizations not yet leveraging colocations, it means procuring rack space with power from the colocation provider, procuring, installing and configuring network and security gear in these facilities, extending corporate Wide Area Network (often times MPLS) into the colocations and of course procuring and configuring the direct cloud connectivity itself. Due to their complexity, it is not uncommon for these projects to consume many months or over a year in some cases. Needless to mention, there is not only high upfront cost, but also high operations cost to keep the network running.



## SD-WAN

Some organizations are looking into the cloud on-ramp capabilities of SD-WAN solutions. These solutions allow organizations to extend their deployed SD-WAN network into the public cloud. SDWAN solutions oftentimes leverage AWS transit VPC or Azure HUB or similar capabilities in the case of other clouds. Some SD-WAN providers leverage the notion of cloud gateways for managed cloud on-ramp. All SD-WAN solutions are limited to establishing basic cloud connectivity. When it comes to inserting network services, defining and controlling security policies and security groups, requiring multi-gigabits per second throughput, these solutions fall short.

There also happen to be many mid-mile network providers claiming to offer multi-cloud networking solutions. The piecemeal approach offered by these providers at best compares with SD-WAN capabilities.

With any of the above approaches, organizations are required to gain a deep understanding of each individual cloud and understand the specifics and limits of each cloud provider's capabilities. On top of that, learning how to provision third-party or cloud native security services and third-party or cloud native loadbalancers, as well as engineer and implement connectivity through those services in order to meet the desired use cases, becomes a monumental task.



**Network engineers leveraging cloud orchestration tools still have to have a deep understanding of the cloud providers' networking capabilities.**



## What About Cloud Orchestration Tools?

Cloud orchestration tools are designed to assist organizations in orchestrating cloud network connectivity leveraging cloud native constructs. Some such tools employ two elements - cloud controller and cloud gateway. Instead of using the cloud providers' console, network engineers can use these controllers to orchestrate connectivity that they would otherwise do from the cloud provider's console.

Network engineers leveraging cloud orchestration tools still have to have a deep understanding of the cloud providers' networking capabilities, constructs, and limitations in certain cases. They still have to know and learn each cloud and understand the capabilities and functionality of a given cloud in order to meet each use case. Now engineers not only need to be well versed in each cloud but also need to build expertise in using such orchestration tools.

For example, consider the organization that has a need to provide multi-gigabit network connectivity into AWS.

For such a relatively high network throughput the options are to leverage either AWS Direct Connect and/or AWS Transit Gateway (TGW) based on the specific design scenario. Now, instead of provisioning AWS Direct Connect and/or AWS TGW from AWS management console, organizations can leverage an orchestration tool. The use of the tool still requires obtaining an intimate knowledge of both AWS Direct Connect and AWS TGW operation in addition to learning how to operate the tool itself. Misconfiguration of the knobs in the tool will result in misconfiguration of AWS Direct Connect and AWS TGW, in the same way it would have happened had an organization leveraged AWS management console directly.

One can argue that in case of multiple public clouds, a cloud orchestration tool helps simplify cloud orchestration and operation. While it is true to a certain extent, the use of cloud orchestration tool does not remove the necessity of obtaining intimate knowledge of each individual public cloud, its capabilities and functionality to meet each use case.

What's more, these vendors who sell multi-cloud orchestration tools and solutions offer their own certifications. How much simpler are they really making your life if you need certifications and coursework in order to be able to use their tools effectively?



## WAN Evolution In The Cloud Era

Networking technologies are shaped by the IT environments of the day. MPLS was born before the cloud and served its purpose well in the late 1990s and early part of this century for virtual private network connectivity between data centers, branches, remote offices and campuses.

MPLS suited the centralized topology of networks with applications running in the data center and the network mainly responsible for moving data between sites. Internet-bound traffic was typically back-hauled to the data center which housed the firewall. Bandwidth requirements were not generally high.

All this changed with the advent of the cloud. Enterprises adopted Software-as-a-Service applications and connected to public clouds. Enterprise applications, infrastructure and networks also migrated to the cloud. Bandwidth requirements increased and it became impractical to backhaul data to the data center over relatively low-speed MPLS connections.

MPLS was inflexible and slow to deploy. It took months to get new services provisioned. It was also expensive.

SD-WAN emerged in response to these issues and enabled enterprises to take steps in the right direction. It enabled the virtualization of the WAN over existing MPLS connections and broadband. Organizations no longer had to wait for MPLS providers to switch on new capacity, they could leverage broadband services or 4G/LTE where broadband wasn't available.

SD-WAN allowed enterprises to match the available transport underlay to application needs – MPLS for voice and video, for example, and broadband for less demanding applications. It also improved resilience through its ability to manage multiple transports and made the network easier to manage by centralizing software upgrades and other administrative tasks.

SD-WAN also simplified the job of connecting to the cloud via on-ramps, but connectivity was basic. Inserting network services, such as firewalls, was a tedious manual process. Routing between clouds was a complex process, and applying a single policy or taking an integrated management view of the whole network was difficult. These difficulties multiplied with the number of cloud environments the organization wished to use.

So while SD-WAN simplified and introduced new dimensions of flexibility and performance to the WAN, it had limitations. For customers who simply needed to connect a few sites over a single network segment it represented a breakthrough. For larger enterprises with complex networks and their eyes on the cloud, it was not enough. For example, not only does SD-WAN fail to provide a simple and comprehensive way to integrate network services with cloud, it often does not allow for a complete replacement of legacy infrastructure. Internet transports are still not reliable enough for applications sensitive to jitter or latency, so enterprises continue to deploy MPLS transports for those applications.



## Cloud Backbone

Before we consider the requirements of multi-cloud networking, it is worth asking how enterprises might reinvent their existing networks to reduce costs and complexity and accelerate the development of new applications and services.

Ideally, they would be able to:

- Build a global, low-latency cloud network
- Provision the network in minutes, not the weeks or months required with MPLS
- Achieve the flexibility, immediacy and ease of integration that can't be achieved with SD-WAN
- Integrate on-premises and cloud-native applications and data
- Ensure a fully secure anywhere to anywhere environment

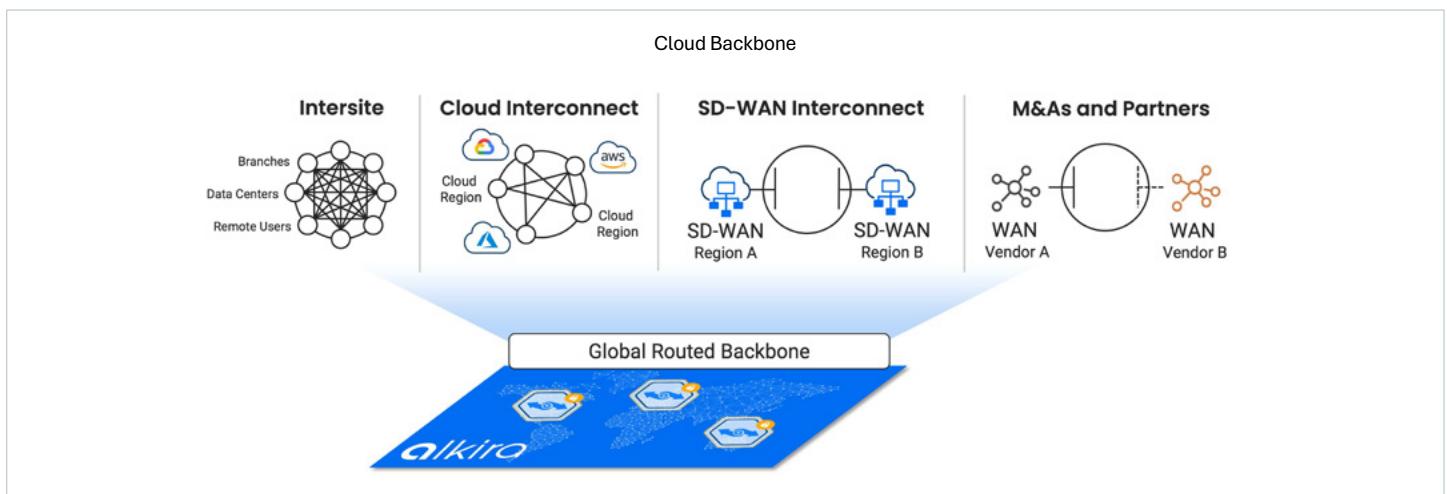
Alkira makes this possible with our integrated Cloud Backbone, which enables cloud connectivity to be extended to any network.

- Overcome issues of legacy infrastructure or, better still, obviate the need to build any of their own infrastructure

This service enables organizations to move to a consumption-based model for network infrastructure enabling reduced capex and real-time autoscaling of network capacity to allow for fluctuations in demand. Cloud Backbone leverages Alkira's platform, a global network infrastructure of virtual points of presence spanning all cloud types. Cloud Backbone delivers a high bandwidth, low latency network with advanced routing controls, integrated security and segmentation and end-to-end visibility, control and governance.

Cloud Backbone use cases include:

- Tying together data centers, branches, campus locations and remote users
- Cloud interconnect
- Interconnect for SD-WAN islands from the same vendor or different vendors
- Network integration to support mergers and acquisitions or to onboard partners.



In response to this rapid adoption of the cloud, compute and storage have evolved beyond virtualization and automation to as-a-service offerings. Cloud architects and engineers are now focused on choosing the service attributes they want to consume, such as compute instances and storage volumes, rather than worry about implementation details. Complexity has been eliminated and cloud computing has become a business enabler for compute and storage.

By adhering to secure access service edge (SASE) and zero-trust network access principles, the Alkira model also ensures that remote employees, partners and developers can be connected to the network at the speed of business without compromising security. Advanced routing and network segmentation ensure that users only ever have access to the resources defined by the enterprise's security policy without erecting unnecessary barriers to productivity and collaboration.



## The Alkira Platform

In response to the rapid adoption of the cloud, software platforms, compute and storage have evolved to as-a-service offering.

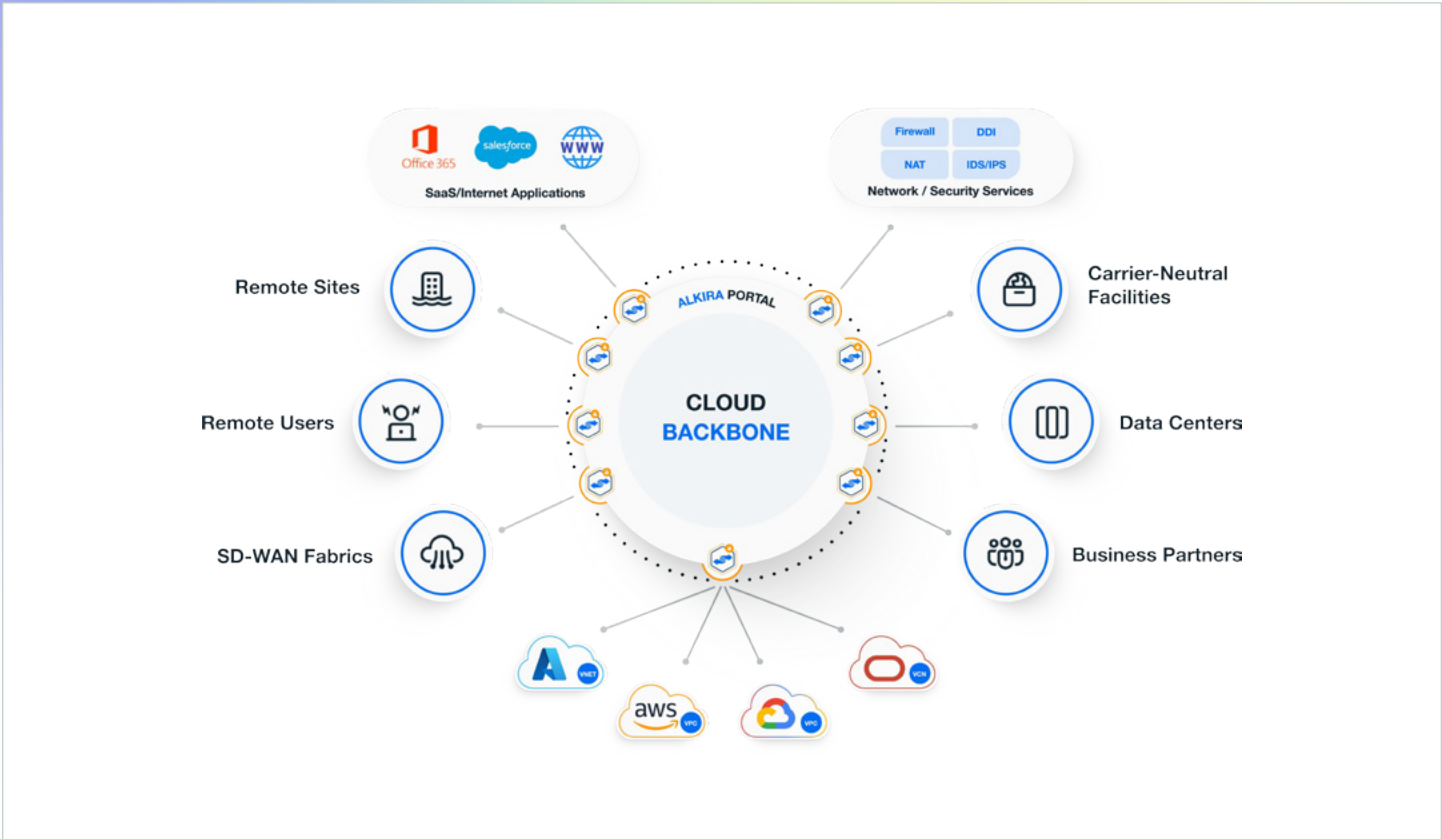
The ideal situation would be for network and network services to be consumed in the similar way. What if you could simply draw your entire global on demand multi-cloud network on an intuitive design canvas, then provision everything in a single click?

There would no longer be any concern about how and which functions of a given public cloud provider must be leveraged to meet the requirements and execute on the desired use cases. Organizations would simply pay for the network and network services as needed, and for as long as they use them.

This ideal solution would couple an as-a-service multi-cloud network with an integrated network services marketplace, deep network insights and governance. It would immediately remove obstacles to successful cloud and multi-cloud adoption eliminating upfront costs.

Introducing the Alkira Platform, global cloud network infrastructure as-a-service. Organizations do not need to procure any additional hardware or download any software, provision costly colocation cloud interconnects or perform tedious configuration tasks.

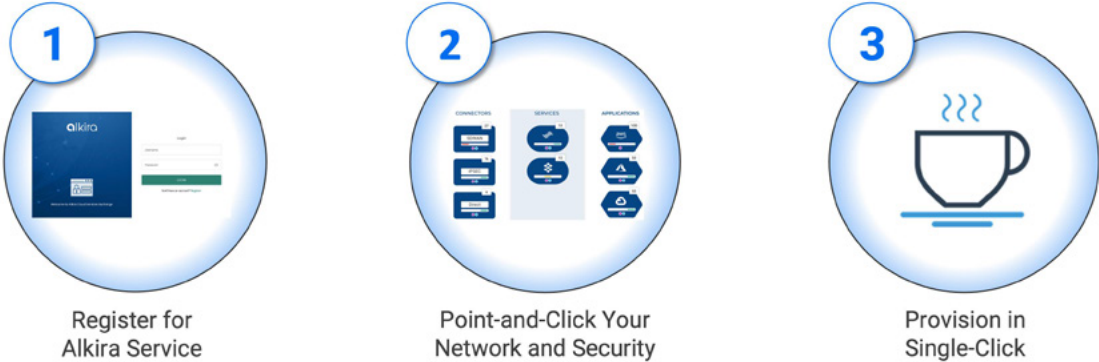




The entire global multi-cloud network is modeled through the intuitive patent pending Alkira portal in a point-and-click fashion.

Organizations consume Alkira in a similar manner to any SaaS service in the market today. First, select the geographic regions where connectivity for workloads, applications, and users is required. Second, add Alkira and third-party network services, from Alkira’s network services marketplace. Finally, simply click the “Provision” button. The entire on demand global unified multi-cloud network with integrated network services is brought to life within minutes.

Cloud network as easy as 1, 2, 3



## Governance In The Cloud

As cloud networking becomes more critical to how fast enterprises are able to respond to the demands of innovation and growth, enterprises want to know that their networks are secure, resilient and manageable. As cloud networks become more fundamental to business success, but also more complex and highly distributed, governance becomes more challenging.

Boards need to be assured that expansion of technical capability and scale is matched by sound governance of the network.

Alkira's view is that cloud networks should exactly mirror corporate governance, which means that the technical and architectural characteristics of the network must provide for:

- Application of consistent policies – e.g. a single security posture – just as they would in any other area of the business
- End-to-end visibility of traffic, users and operating conditions throughout the network
- Management and control tools that allow governance rules to be applied, e.g. what can be instantiated within a cloud or a domain, in what circumstances and by whom.

From a management perspective, the network is a single entity regardless of the number of clouds, cloud regions, WANs, on-premise networks, core or edge data centers and remote users it spans. From a technical perspective achieving coherence, simplifying management and control and maintaining adherence to governance principles requires:

- Consolidation of services such as firewalls
- End to end segmentation and micro-segmentation
- End to end routing between cloud regions, on-prem and Internet/SaaS
- Intelligent intent-based networking to steer traffic through services
- End to end monitoring, visibility and troubleshooting capabilities.

All of these capabilities are difficult to deliver today in a single cloud and almost impossibly challenging in multi-cloud environments. Alkira's solution simplifies the network by abstracting its complexity, clarifying Day 2 operations and reducing the barriers to effective governance.



## Customer Benefits

The Alkira solution allows organizations to turn networking for the cloud from a business inhibitor to a business enabler, while providing the following main benefits:

- Faster time to cloud, with deployment times reduced to minutes in full alignment with business SLAs
- High bandwidth, low latency networking from remote sites to public clouds (AWS, Microsoft Azure and GCP) and SaaS/Internet applications, and between multiple public clouds or multiple regions of the same public cloud
- Eliminate cloud-specific limitations by building a multi-region, multi-cloud overlay network, leveraging cloud-native and advanced routing and security constructs
- Integration of legacy systems and networks using Cloud Backbone to improve return on existing infrastructure investments and enable migration strategies
- Global security policy enforcement by leveraging firewalls of choice and global symmetric traffic steering
- Elasticity to accommodate on demand capacity, e.g. periodic high-volume data transfers, seasonal retail customer uptake, etc.
- End-to-end segmentation between remote sites, public cloud instances, cloud network services and SaaS/Internet exit points for compliance and sensitive or secure applications
- On demand/subscription consumption cost model to ensure customers are charged for only the network and network services resources they actually consume
- High availability and resiliency backed up by high uptime service guarantee
- Deep end to end visibility and troubleshooting capabilities for day-2 operations.



**Alkira focuses on removing any obstacle to successful cloud and multi-cloud adoption.**





## Summary

Alkira® is the industry's first solution offering global unified network infrastructure as-a-service. With Alkira, enterprises can have a consistent and significantly simplified experience deploying a global cloud network for end-to-end and any-to-any network connectivity across users, sites, and clouds with integrated network and security services, full day-2 operational visibility, advanced controls, and governance. The entire network is drawn on an intuitive design canvas, deployed in a single click and is ready in minutes!

### **The Fastest Way to the Cloud.**

To learn more about Alkira and get your personalized demo, please visit our website at: <https://www.alkira.com/demo>

