

Cloud Visibility & Governance

Industry's only solution with single-click provisioning of the entire global multi-cloud network and network services. Connect users and sites to public clouds and connect public clouds together, while cutting provisioning time from months to minutes.



Cloud adoption continues to accelerate. Organizations are increasingly transitioning business critical applications from on-premise data centers to the public cloud and SaaS environments.

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 now focus 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.

Key Challenges

In contrast, the network (and network services) has not made a similar transition, nor does it operate in true concert with the cloud. Building a network for the cloud comes with the following key challenges:

- Limited visibility due to the use of cloud-native services on individual public clouds, lacking a uniform multi-cloud view. Visibility and Governance blind spots resulting from disparate cloud architectures and the lack of single point of control.
- Overlapping IP addresses and inconsistent security group controls resulting from lack of uniform enforcement of organizational usage policy.
- Increased IT spend resulting from inability to perform departmental chargeback for consumed cloud resources.

The network and network services are under increasing pressure to provide an agile, highly performing and cost-effective solution to cloud business needs, while eliminating visibility and governance blind spots.



End-to-end visibility
and governance for
deep network and
network services
insights eliminating
operational blind
spots.

Cloud Visibility & Governance with Alkira Cloud Services Exchange

Alkira Cloud Services Exchange™ (Alkira CSX) is the industry's first as-a-service unified multi-cloud network with integrated network services marketplace, visibility and governance. It removes obstacles to successful cloud and multi-cloud adoption.

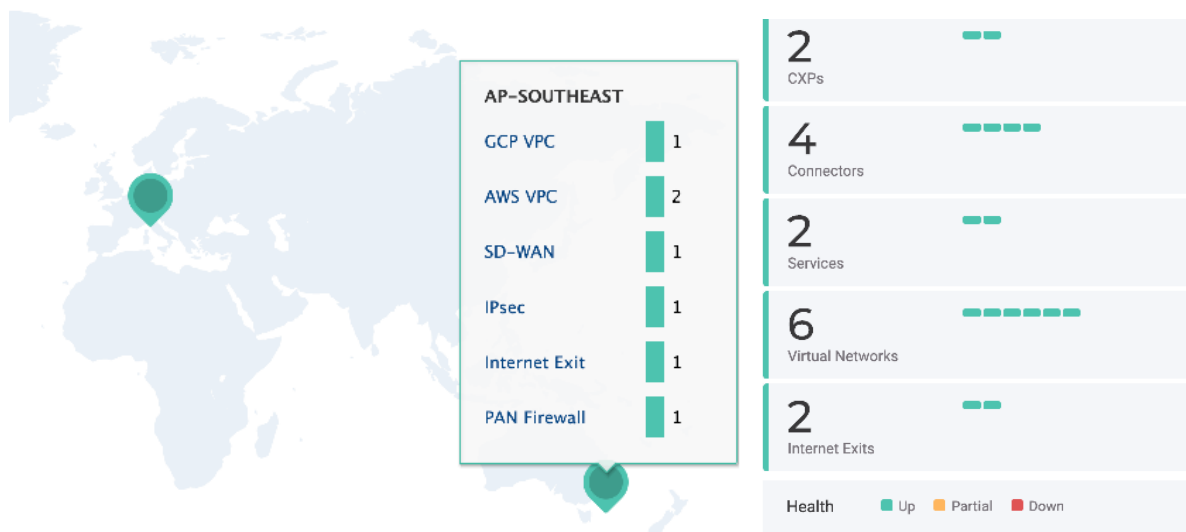
Alkira Cloud Services Exchange Portal is a single web interface for designing, provisioning and operating your entire multi-cloud network. Leveraging industry-leading graphical visualization, Alkira solution offers insights into numerous critical visibility elements for applications, networks and network services, allowing organizations to not only deploy global multi-cloud network and network services in minutes, but also achieve operational excellence.

It is time for the network to evolve. It is time for the network to be reinvented for cloud. Read a white paper by Atif Khan, Alkira CTO. [↗](#)

Multi-Cloud Visibility & Inventory

Alkira Cloud Services Exchange Portal provides a single web interface for full multi-cloud view, health and inventory of all elements connected to the global Alkira Cloud Exchange Points. The elements include public cloud instances (AWS VPCs, Microsoft Azure VNets and GCP VPCs), IPsec connected sites, connected Cisco SD-WAN fabric, Internet exit points and network services (Palo Alto VM-series Firewalls). The health is expressed as either up, down or degraded (partial).

Multi-Cloud View & Inventory

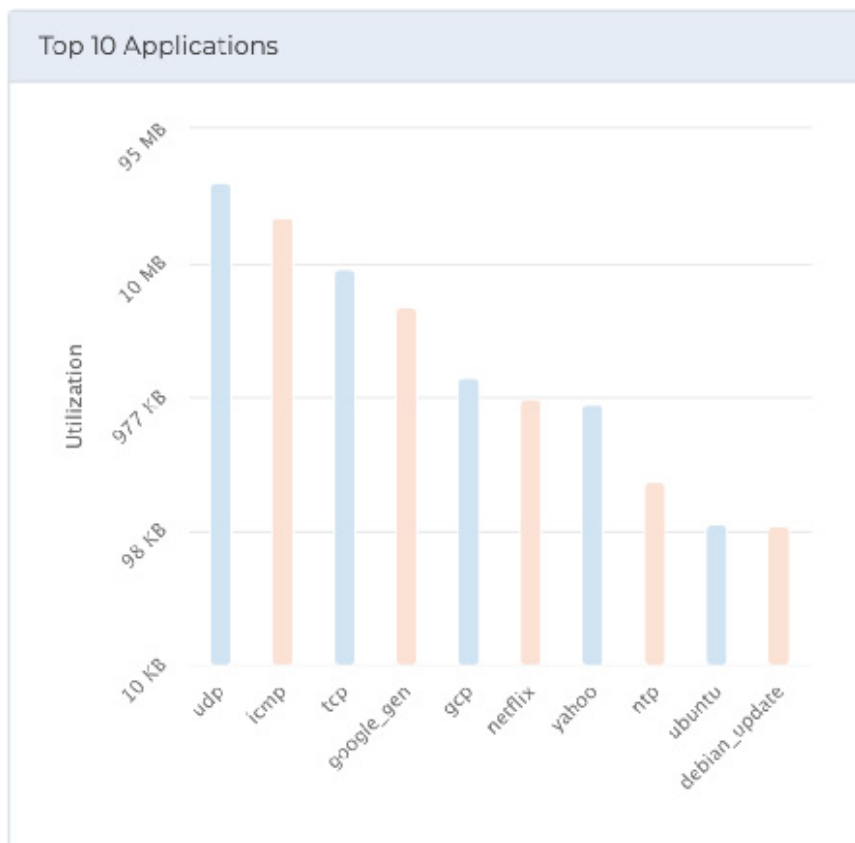


From the multi-cloud view, customers can drill deeper by accessing dashboards for each Alkira Cloud Exchange Point to get further details.

Application Identification

Alkira Cloud Services Exchange identifies application traffic flowing through the globally distributed Alkira Cloud Exchange Points. Top applications, as well as their consumed capacity, are displayed in the dashboard section of the Alkira Cloud Services Exchange Portal.

Application Identification



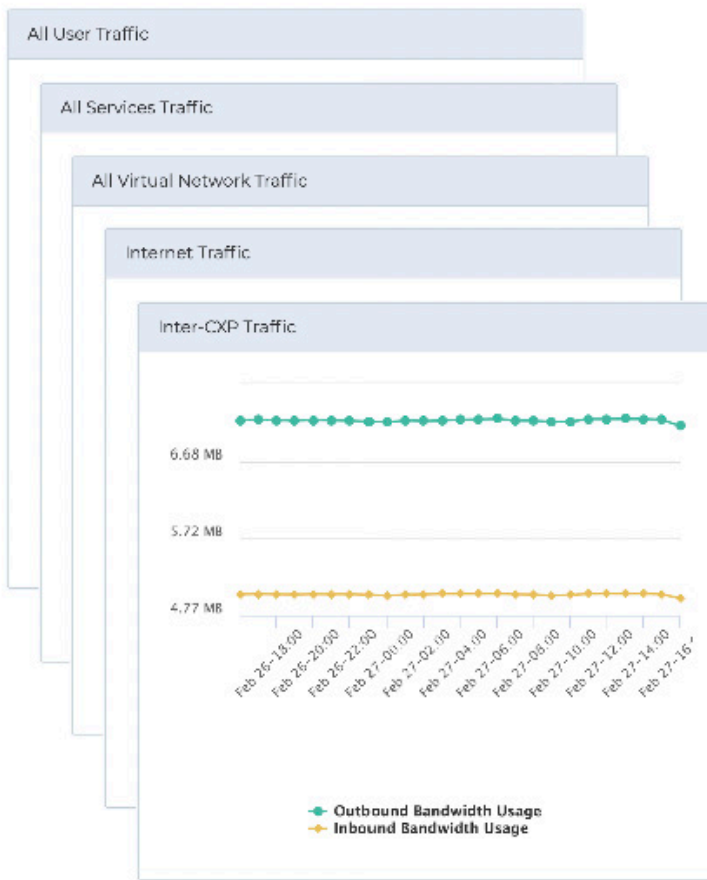
Application identification is important for tightening security controls and ensuring appropriate use of organizational network resources by blocking unwanted application traffic. Application identification can also help with better capacity planning and cost optimization.

Experience the power of Alkira solution today and watch your multi-cloud network come to life in minutes. [↗](#)

Network Usage Visibility

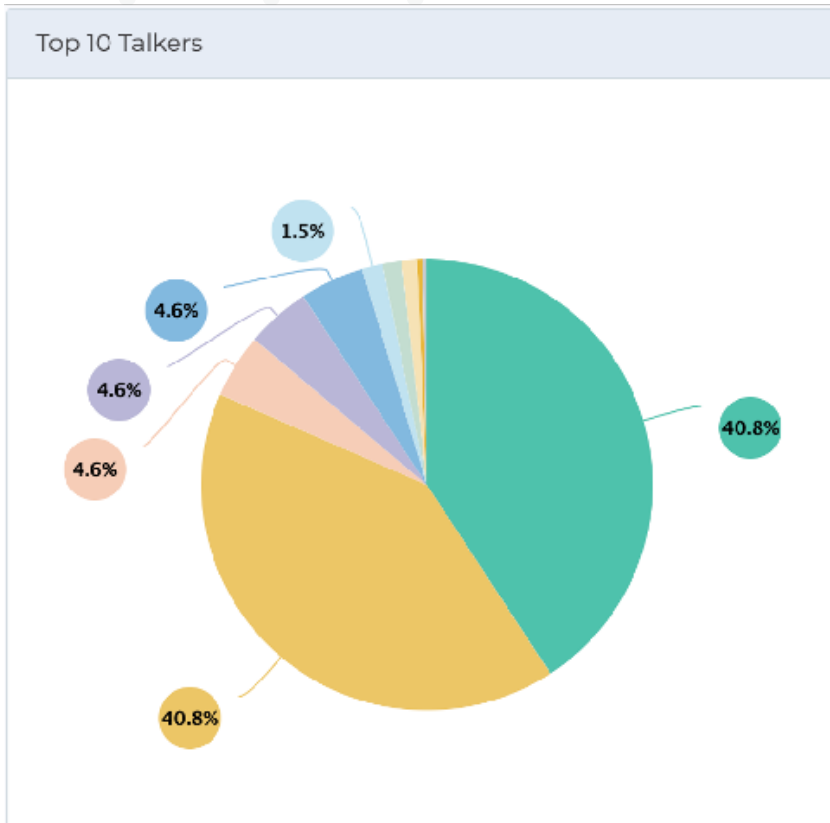
Alkira Cloud Services Exchange Portal exposes numerous network usage statistics for all elements connected to the Alkira Cloud Exchange Points. The elements include public cloud instances (AWS VPCs, Microsoft Azure VNets and GCP VPCs), IPsec connected sites, connected Cisco SD-WAN fabric, Internet exists and network services (Palo Alto VM-series Firewalls).

Network Usage



In addition to the network usage on a per-element level, Alkira Cloud Services Exchange Portal also exposes fine-grained information about top (10) talkers communicating to and across clouds, as well as accessing SaaS/Internet applications. The top talkers chart identifies the source and destination of the communication, the amount of network traffic transmitted and its representative percentage.

Top Talkers



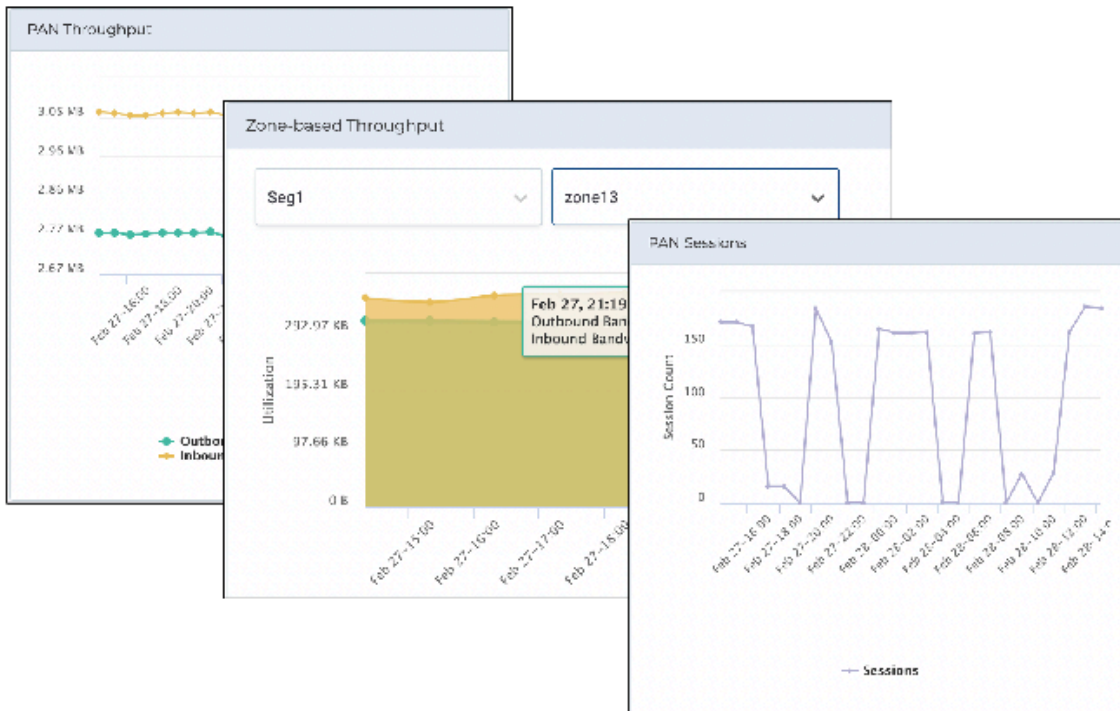
Information about top talkers is important for tightening security controls and ensuring appropriate use of network resources by blocking unwanted application traffic. Information about top talkers can also help discover new network communication trends for better capacity planning and cost optimization.

Network Services Usage Visibility

Alkira Cloud Services Exchange network services marketplace allows customers to select and deploy network services into their global On demand multi-cloud network. The most popular network service is the Palo Alto Firewall, which allows enforcing security policy for traffic between remote sites and public clouds, between multiple public cloud instances and multiple public clouds, and the Internet-bound traffic through the Alkira Cloud Exchange Points.

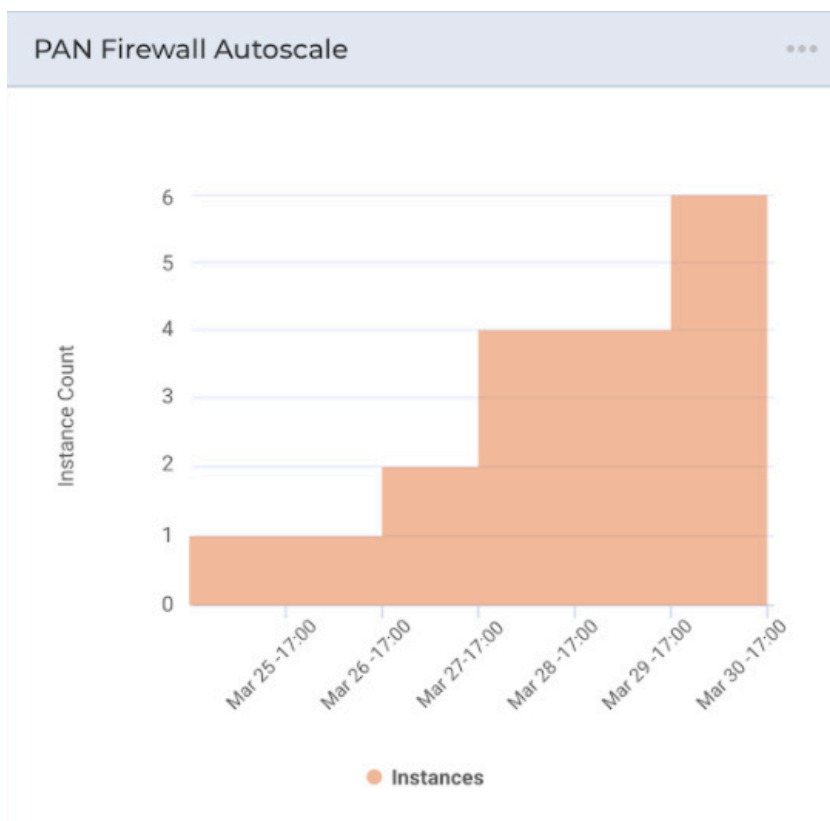
Alkira Cloud Services Exchange Portal exposes network throughput toward the Palo Alto VM-series Firewalls deployed in the Alkira Cloud Exchange Points. The throughput can be shown as aggregate or per-Firewall zone. Alkira Cloud Services Exchange Portal also exposes the number of sessions forwarded to the Firewall.

Network Services Usage



In cases of increased real-time demand for Firewall capacity, the Alkira solution will automatically bring-up additional instances of the Palo Alto VM-series Firewall in the appropriate Alkira Cloud Exchange Points up to the maximum number specified in the Firewall configuration in Alkira Cloud Services Exchange Portal. When the demand for real-time Firewall capacity subsides, the Alkira solution will automatically remove unneeded instances of the Palo Alto VM-series Firewall down to the minimum number specified in the Firewall configuration in Alkira Cloud Services Exchange Portal.

Palo Alto VM-series Firewall Autoscaling



Alerts

Alkira Cloud Services Exchange captures the details of events occurring in the global customer network. These events are logged in the Alerts section of the Alkira Cloud Services Exchange Portal. Summary and tags associated with each alert allow administrators to quickly understand the elements affected by the alert. Alert priority allows properly prioritizing events, where high priority events can be dealt with ahead of medium or lower priority ones.

Alerts

Type	Priority	Summary	Status	Tags	Timestamp
Network Provisioning	Medium	Successfully provisioned network	ACTIVE	tenantprod@prodswan2 CRP: EU-CENTRAL-AP-SOUTH-1 segment=Seg23	02/07/2020 16:31
Network Provisioning	Medium	Successfully provisioned network	ACTIVE	tenantprod@prodswan1 CRP: EU-CENTRAL-AP-SOUTH-1 segment=Seg23	02/06/2020 21:02
Network Provisioning	Medium	Network configuration available for connector instance 'tenantprod@prodswan2-tenantprod@prodswan2'	ACTIVE	CRP: AP-SOUTH-EAST segment=Seg23 connector@prodswan2 group=prodswan2	02/06/2020 20:34
Network Provisioning	Medium	Network configuration available for connector instance 'tenantprod@prodswan1-tenantprod@prodswan1'	ACTIVE	CRP: EU-CENTRAL segment=Seg23 connector@prodswan1 group=prodswan1	02/06/2020 20:18
Network Provisioning	Medium	Network configuration available for connector instance 'tenantprod@prodswan1-tenantprod@prodswan1'	ACTIVE	CRP: EU-CENTRAL segment=Seg23 connector@prodswan1 group=prodswan1	02/06/2020 20:18

Audit Logs

In the environment where multiple customer administrators have access to the Alkira Cloud Services Exchange Portal, it is important to keep track of administrative actions to ensure personal accountability. It is equally important to keep track of actions in order to simplify the process of rolling back configuration changes, if needed.

Audit Logs

Type	Status	Description	Initiator	IP Address	Tags	Timestamp
Network Configuration	SUCCEEDED	PAN Service 'tenantprod9FW1' updated on CXP EU-CENTRAL	veera@alkira.net	10.3.11.199	CXP: EU-CENTRAL Segment: Sg1Sop2 Service: tenantprod9FW1	02/23/2020 22:58
Network Configuration	SUCCEEDED	AZURE VN2T Connector 'tenantprod9-vnet1' updated on CXP EU-CENTRAL	veera@alkira.net	10.3.11.199	CXP: EU-CENTRAL Segment: Sg1 Connector: tenantprod9vnet1	02/23/2020 22:54
Network Configuration	SUCCEEDED	AWS VPC Connector 'tenantprod9-vpc1' updated on CXP AP-SOUTHEAST	veera@alkira.net	10.3.11.199	CXP: AWS-2017-HEAD-1 Segment: Sg1 Connector: tenantprod9vpc1	02/23/2020 22:53
Network Configuration	SUCCEEDED	Policy Sg2-PL-AllowAllPAN' added	veera@alkira.net	10.3.11.199	PolicyName: Sg2-PL-AllowAllP...	02/23/2020 22:52
Network Configuration	SUCCEEDED	Policy AllowAllPAN enabled	veera@alkira.net	10.3.11.199	PolicyName: AllowAllPAN	02/23/2020 22:51
Network Configuration	SUCCEEDED	Policy AllowAllPAN added	veera@alkira.net	10.3.11.199	PolicyName: AllowAllPAN	02/23/2020 22:50

User Management

Alkira Cloud Services Exchange Portal integrates user management for administrative access. Each user can be assigned a role that determines the level of access allowed in the portal. Access is defined as Read Only, Read Write and No Access to specific portal elements. The system comes with three predefined roles of Admin, Netadmin and Operator. Predefined roles cannot be changed; however custom roles can be created where each specific portal element can be assigned Read Only, Read Write or No Access, as needed.

Custom Roles

Settings / Roles

DEFAULT ROLES CUSTOM ROLES

AlertsAdmin

	Read Only	Read Write	No Access
Alerts	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Audit Logs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Billing	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Jobs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Alkira Cloud Services Exchange Portal access can also be integrated with supported Single Sign-on (SSO) systems. This allows customers to institute uniform strong mechanisms for access authentication and authorization.

Billing & Chargeback

Cost is one of the most significant factors of cloud adoption. Alkira Cloud Services Exchange comes with full visibility and transparency in regard to costs incurred when consuming the Alkira service. The cost is broken down to geographic locations, provisioned connectors (sites, clouds and Internet exits), provisioned network services and the consumed network traffic. Customers can view past, present and forecasted spend in the Alkira Cloud Services Exchange Portal, as well as produce invoices.

The Alkira solution allows the assignment of administrative billing tags to the configured resources. This helps IT departments institute a chargeback policy. For example, all resources provisioned for the HR department, such as connectivity to public cloud resources (VPCs and VNets), Internet exit points and the associated network traffic can be aggregated into a single bill that can be passed on to the HR department for charge.

APIs

Alkira Cloud Services Exchange Portal supports a rich set of REST APIs. This allows customers to access, control and monitor all elements of the solution exercising the DevOps approach. Leveraging HTTP POST calls, customers can create new configurations. Meanwhile HTTP PUT calls allow editing configuration and HTTP GET calls allow pulling data out. Pulling data out can be especially beneficial when integrating with third-party tools, such as various monitoring tools or higher-level orchestrators.

The Alkira CSX supports the Swagger interface that allows customers to easily discover the supported API calls without a need for separate documentation.

API Call Example (HTTP PUT)



The screenshot shows a REST client interface with the following details:

- Method:** PUT
- URL:** `https://(alkira-portal-url)/api/user/tenant/b4f-1b82-44cf-9aa4-55b677c68f0e`
- Body:**

```
{ "lastLoggedIn": 1571383901788, "id": "8cca5b4f-1b82-44cf-9aa4-55b677c68f0e", "tenantId": "2", "userName": "test", "firstName": "test", "lastName": "user", "email": "test@alkira.net", "roles": [ "netadmin" ], "roleIds": [ "269b5e3b-3bbd-4919-9a6b-e4e49/c2516f" ] }
```

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 reduces deployment time from months to minutes in full alignment with business SLAs.
- High bandwidth, low latency network from 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.
- Global security policy enforcement by leveraging firewalls of choice and global symmetric traffic steering.
- End-to-end segmentation between sites, public cloud instances, cloud network services and SaaS/Internet exit points for compliance, sensitive and secure applications.
- Elasticity to accommodate On demand capacity, e.g. periodic high-volume data transfers, seasonal retail customer uptake, etc.
- High availability and resiliency backed up by a high uptime service guarantee.
- Full visibility to eliminate operational blind spots and improve day-2 operations.
- On demand/subscription consumption cost model to ensure customers are only charged for the network and network services resources they actually consume.



Summary

In summary, Alkira Cloud Services Exchange™ offers the industry's first leapfrog solution focusing on removing obstacles to successful cloud and multi-cloud adoption. Leveraging globally distributed network of Alkira Cloud Exchange Points™ (multi-cloud virtual points of presence), organizations can establish global On demand connectivity between remote locations and the public clouds. Organizations can easily insert On demand stateful global network and security services from the Alkira services marketplace, leveraging intent-based policies. End-to-end visibility and governance offer deep network and network services insights eliminating operational blindspots. The Alkira™ industry-leading graphical user interface enables dramatic operational simplification by offering a point-and-click modeling canvas with single-click provisioning of the entire end-to-end multi-cloud service in minutes.

The Network. Reinvented for Cloud.™



www.alkira.com

©2020 Alkira, Inc. All rights reserved