IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Alkira

Enterprises often overlook the network when adopting multicloud, only to discover it is more important than ever. Organizations that fail to appreciate the importance of modernizing networks for multicloud are destined to fall short of their larger digital transformation objectives, including greater business agility and enhanced continuity.

Meeting the Challenge of Unifying and Simplifying Multicloud Networking

April 2020

Written by: Brad Casemore, Research Vice President, Datacenter Networks

Introduction

Digital transformation is an overriding strategic imperative for enterprises worldwide. It's also a never-ending but absolutely necessary and beneficial journey involving continuous improvements to iterative processes that increase business efficiencies, enhance the digital experiences of customers and other stakeholders, and produce tangible business outcomes such as faster time to market, increased revenue, and greater competitive advantage.

AT A GLANCE

KEY STATS

In IDC's 2019 *Multicloud Management Survey,* 89% of enterprise respondents indicated that they use public IaaS clouds, with 81% saying that they use multiple public IaaS clouds and dedicated/private clouds.

For enterprises, cloud has become an essential means of pursuing and realizing digital transformation. It's important to realize that cloud, properly understood, is not just a destination for workloads but also an operating model and set of key technologies. What's more, the inherent agility and flexibility of cloud processes and technologies must extend throughout IT infrastructure and operations if digital transformation strategies are to achieve their full promise.

The Need for Modernized Multicloud Networks

The embrace of cloud entails extensive modernization and transformation of IT infrastructure, including the network. IDC has found that enterprises that fail to properly appreciate the need for network infrastructure modernization invariably discover that the network becomes an inhibitor, rather than an enabler, of digital transformation.

That is particularly true in the context of multicloud, which is now the preferred cloud posture of enterprises. In IDC's 2019 *Multicloud Management Survey,* 89% of enterprise respondents indicated that they use public infrastructure-as-a-service (IaaS) clouds, with 81% saying that they use multiple public IaaS clouds and dedicated/private clouds. Even so, while enterprises are adopting multicloud postures and strategies across industries and geographies, most remain in the early stages of executing those strategies, with considerable work still to be done to refine processes and bring strategies to fruition.

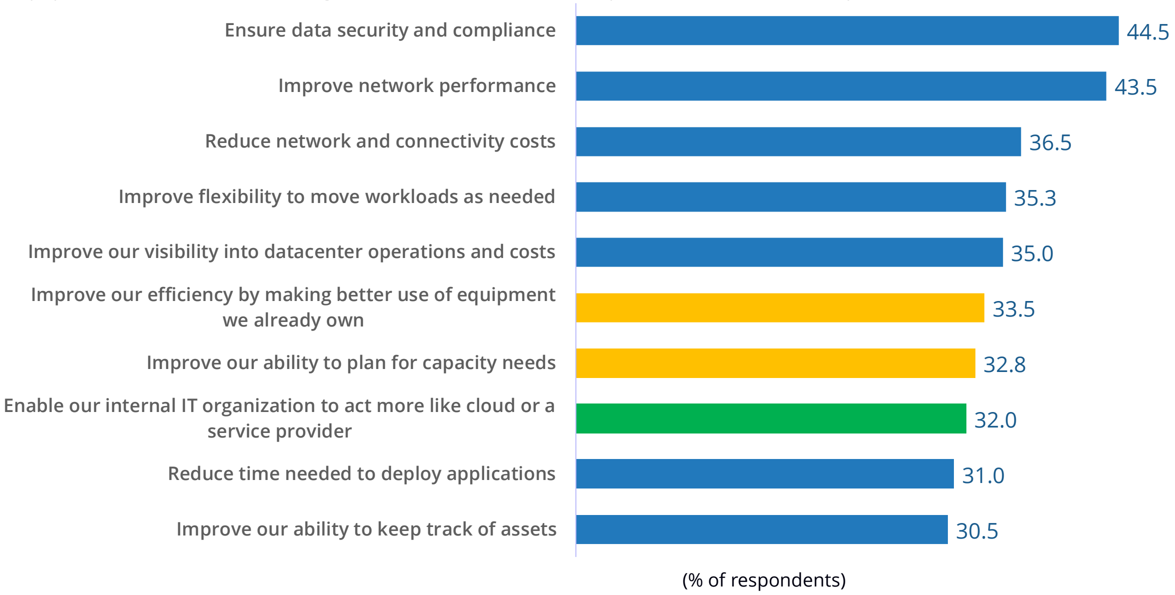
Infrastructure modernization is both acutely required and particularly challenging for multicloud. While compute and storage infrastructure and operations have largely aligned with cloud principles and the needs of multicloud, networking has struggled to keep pace. Enterprises often aren't initially aware of the network's multicloud deficiencies and limitations until they experience them firsthand.

In fact, IDC has found that enterprises frequently overlook the network in their adoption of multicloud only to discover that the network is more important than ever in a multicloud context. Enterprises that fail to appreciate the importance of modernizing their networks for multicloud are destined to fall short of meeting their larger digital transformation objectives.

However, enterprises that have experienced these problems or given the matter a greater degree of consideration realize what they're up against. Indeed, in IDC's 2019 *Datacenter Operational Survey,* enterprise respondents identified "ensure data security and compliance" and "improve network performance" as their top 2 priorities and challenges in hybrid IT and multicloud (see Figure 1). Similarly, in IDC's latest *Cloud Pulse Survey,* 59% of enterprise respondents indicated that "integrated network processes across cloud providers" will be an important area for their cloud investments during the next two years.

FIGURE 1: ***Living in a Multicloud World***

Top priorities and challenges across traditional, private cloud, and public cloud datacenters



n = 400

Source: IDC's Datacenter Operational Survey, January 2019

Limitations of Current Approaches

Today, enterprises are attempting to address multicloud networking in a variety of ways. Some leverage colocation facilities and interconnection-oriented architectures, or they attempt to address the need themselves in a piecemeal fashion or in conjunction with service providers and managed service providers. Others adopt network virtualization, SD-Core middle miles, virtual private networks (VPNs), or a variety of cloud tools to address multicloud networking.

Despite their utility and benefits, those approaches also have drawbacks. Most notably, they tend not to align well with the agility and speed that are characteristic of and inherent to cloud. That's because a piecemeal approach to building a comprehensive multicloud network is apt to involve a high degree of architectural and operational complexity. That complexity includes months of tedious manual provisioning, the need for specialized expertise across various APIs and cloud-specific network processes and technologies, daunting routing challenges across regions and clouds, and overcoming the constraints and limitations of specific clouds in areas such as number of routes and segmentation and available throughput.

In networking, complexity always manifests in costlier and lengthier processes. In addition to the previously mentioned issues, enterprises pursuing multicloud often find that they must overprovision their firewall services and implement convoluted symmetric routing to accommodate firewalls across clouds. They also struggle to achieve the cloud's promise of elastic autoscaling, especially in relation to seamless insertion of network and security services. These issues are compounded by the lack of cross-cloud networking expertise in most enterprise IT departments. To be fair, it isn't easy to quickly come up to speed on the disparate cloud providers' architectures, network APIs, and network and security services offered by various IaaS clouds much less devise an in-house (DIY) approach that helps bring consistency and unity to the management of this increasingly critical infrastructure.

Similarly, the need for as-a-service consumption models, another defining attribute of cloud, goes unmet. This results in the following deficiencies:

- High initial costs (overprovisioning rather than "as a service")
- Slow responses to change requests (lack of agility, inefficiency)
- Sprawl of automation/orchestration tools, which results in the management complexity of using a disparate array of legacy on-premises tools, orchestration tools, and cloud-specific tools, each of which entail capex and opex costs
- Inability to meet line-of-business (LOB) time-to-service needs or establish the requisite chargeback mechanisms

In a multicloud context, the issue of visibility comes to the forefront and poses a difficult challenge. Network visibility is crucial across this new landscape both because applications are more valuable than ever — serving as systems of engagement and experience as well as systems of record — and because they are increasingly distributed across a multicloud landscape.

The network provides the all-important digital nervous system for these business-critical applications and must possess the telemetry, visibility, and intelligence to ensure that applications are kept available and responsive at all times. Visibility informs faster troubleshooting and remediation, and it ultimately helps IT operators move toward a more proactive and preventive approach to obviating network and security issues before they result in application and service disruptions and outages. Today, however, enterprises pursuing multicloud are encountering a range of visibility challenges, including intermittent or partial visibility across clouds and too many blind spots.

Additional challenges in multicloud networking can result from poorly configured access control lists (ACLs) or inconsistent security group policies. These challenges often are exacerbated by the use of overlapping IP addresses in clouds and by the "shadow IT" phenomenon of developer or LOB applications that are neither known nor detected by IT operations. Moreover, many enterprises struggle with a range of day 2 operational challenges, ranging from installing consistent and timely patches and updates to providing fast troubleshooting and remediation of network issues.

Collectively, these challenges represent a morass of complexity, resulting in costly efforts to control, manage, and maintain multicloud networks.

Requirements and Benefits

Requirements

The comprehensive multicloud network should deliver a range of attributes and capabilities:

- **As-a-service consumption.** The cloud has spawned service-based consumption models that align cost effectively with evolving needs and don't force enterprises to make significant up-front expenditures for overprovisioning. A multicloud network must accord with the same cloud principles.
- **On-demand.** Like the cloud, a multicloud network should be on demand — provisioned, deployed, and available as needed.
- **Autoscaling.** Just as cloud resources scale up and down automatically based on demand, a multicloud network must similarly autoscale in alignment with cloud resources.
- **Agility and speed.** Traditional network infrastructures and the operational practices that accompany them have long been cited for lack of agility. A multicloud network, which necessarily supports distributed cloud workloads, must be agile, capable of operating at the speed of digital business.
- **Pervasive, real-time visibility.** To speed the process of troubleshooting and remediation, and to help IT operations achieve a more proactive posture toward network management, multicloud networks must possess pervasive, real-time visibility.

Benefits

Presuming those requirements are satisfied, the multicloud network can accommodate several use cases and provide a range of tangible business and operational benefits:

- A global on-demand multicloud network (with deployment time reduced from weeks to minutes)
- Integrated, on-demand network and security services (allowing for the use of less capacity as well as lower costs for functions such as firewalls, load balancers, DDI/IPAM, SSL VPNs, and NAT)
- Visibility and governance (to expedite troubleshooting, meet service-level agreements [SLAs], and move toward more proactive operations)
- As-a-service consumption (resulting in significantly lower total cost of ownership [TCO])
- Faster time to service, especially in quickly meeting the needs of LOBs and expediting business outcomes

Considering Alkira

The Alkira Cloud Services Exchange (CSX) is a global, unified multicloud network delivered "as a service." It has been designed to provide enterprises with global multicloud connectivity, on-demand network and security services, end-to-end network visibility, and strong governance.

Alkira CSX is designed to deliver on the following cloud principles:

- Agility and speed
- On-demand functionality
- As-a-service consumption
- Elastic scalability (up and down, as required)

Alkira CSX addresses speed and agility by making the complex simple, specifically by eliminating the need to learn and understand cloud-specific capabilities and APIs and mitigating their various limitations as well as by minimizing the multicloud network provisioning process to a single mouse click.

On-demand capabilities ensure that organizations can establish global multicloud networks where they're needed, when they're needed, and for as long as they're needed — just like other cloud infrastructure and resources. These on-demand capabilities can be scaled up and down contingent on administratively requested capacity or on dynamic real-time demands, such as ebbs and flows in transactions and traffic.

Alkira CSX is offered on a subscription basis and a pay-as-you-go (PAYG) basis, again aligned with cloud consumption models. The PAYG option offers a higher degree of deployment flexibility, with customers paying only for network traffic consumed and for provisioned elements, such as sites, cloud instances, and network services. Alternatively, the subscription model offers greater cost-effectiveness, in that it is based on committed target spend for the service, irrespective of the provisioned elements.

Alkira CSX provides organizations with the ability to define their multicloud network and network services through a digital design canvas that allows them to leverage existing hardware investments to limit or reduce costs. This approach contrasts with others that can involve new investments in colocation facilities, private cloud interconnects, and hardware investments or the need to procure and manage orchestration tools to automate configuration workflows.

Architecture Overview

The CSX architecture includes the following elements:

- **Alkira Cloud Exchange Point (CXPs).** CXPs are virtual multicloud points of presence (POPs) with full routing stacks and a range of network services capabilities. They are available in service locations worldwide, and they collectively form a fully meshed, secure, high-bandwidth, low-latency multicloud network.

  CXPs are elastically scalable to accommodate the need for dynamic multicloud network capacity. They also are designed to provide high availability to meet the needs of multicloud SLAs. These elasticity and high-availability capabilities are supported in both the control-plane element and the data-plane element of the Alkira Cloud Exchange Point.

- **Connectors.** These elements are leveraged to connect organizations' on-premises, public cloud, and other internet-connected resources (e.g., colocation facilities and edge environments such as branch offices) to the CSX through the geographically closest CXP. For on-premises locations, connectors can include standards-based IPSec VPNs, Cisco (Viptela) SD-WANs, or AWS Direct Connect (if deployed in colocation facilities). For internet locations, such as branches, connectors link to the nearest Alkira CXP to provide optimal regional breakout to software-as-a-service (SaaS) and other internet applications.

- **Network Services.** Alkira CSX supports the integration of various network services available from the company's network services marketplace. Alkira provisions each network service and ensures that it automatically and elastically scales based on real-time capacity demand, symmetrically steering the specified network traffic to the network service pursuant to defined policies. It is, however, a customer's responsibility to provide configuration of the network service itself, such as defining the security policy of a firewall.

- **Alkira Cloud Services Exchange Portal.** The portal provides a simple web-based interface that allows customers to design and provision their multicloud networks and to manage day 2 network operations. All functions of the Alkira CSX are also available through a set of REST APIs.

Customers register for and deploy the service in a simple three-step process.

First, customers register for the Alkira multicloud network service through the registration portal, which is like registering for any other SaaS service. Next, customers log in to the Alkira Cloud Services Exchange Portal, where they can design and model their entire global multicloud network consisting of remote users, remote sites, datacenters, colocation facilities, public clouds, SaaS applications, and internet applications, with network and security services, including firewalls. Modeling involves pointing and clicking on a design canvas. Once the multicloud network has been modeled, it can be provisioned — the third and final step of the process. With a single mouse click (or API call), customers can deploy an entire multicloud network globally. Depending on the size of the deployment, the multicloud network can be live in less than an hour.

Challenges

Various options are available to enterprises as they consider how to build and maintain a full-featured multicloud network to support their digital transformation initiatives. Similarly, enterprises have existing investments in infrastructure and technology that should be evaluated carefully in the context of multicloud networking. Further, enterprises must consider the acumen and expertise of their in-house IT departments and network operations teams, especially in relation to the potential adoption of new processes, products, and technologies.

In seeking to help enterprises build multicloud networks, Alkira will have to show how it can address these challenges. It will also face the competitive challenge from established enterprise infrastructure vendors, including datacenter SDN and SD-WAN vendors, as well as other vendors that provide alternative approaches to multicloud networking.

Nonetheless, there is a clear need for an approach to multicloud networking that unifies functionality across clouds, is well aligned with cloud principles and practices, and offers the benefits associated with cloud, namely on-demand functionality and elastic autoscaling.

Conclusion

As enterprises continue to migrate applications to public IaaS clouds and SaaS environments, the need for an on-demand, elastically scalable, and highly available multicloud network becomes clear. The multicloud network must adhere to the same cloud principles and possess the same cloud attributes as the public clouds with which it connects.

The Alkira Cloud Services Exchange is well positioned to help enterprise customers mitigate the complexity of deploying and managing multicloud networking, including the network and security services that need to run consistently across those environments. Presuming Alkira can work with prospective enterprise customers to overcome the challenges previously outlined, it could play a meaningful and valuable role in enabling those organizations to both harness the promise of multicloud and bring their digital transformation strategies to fruition.

Infrastructure modernization is both acutely required and particularly challenging for multicloud.

About the Analyst

Brad Casemore, *Research Vice President, Datacenter Networks*

Brad Casemore is IDC's Research Vice President, Datacenter Networks. He covers networking products and related technologies and platforms typically deployed in the datacenter. Mr. Casemore also works closely with IDC's Enterprise Networking, Server, Storage, Cloud and Security programs to assess the impact of emerging IT and converged and hyperconverged infrastructure.

MESSAGE FROM THE SPONSOR

Alkira delivers the first unified, multicloud network as-a-service that allows customers to build and deploy global cloud networks in minutes. Alkira Cloud Services Exchange is delivered on demand and so simple to use that no training or certification is required. Alkira was founded by Amir Khan, CEO and founder of Viptela, and Atif Khan, founding team member of Viptela (acquired by Cisco Systems in 2017), and is funded by Kleiner Perkins, Sequoia Capital, and GV, formerly Google Ventures.

Learn more at ***www.Alkira.com*** or follow us @AlkiraNet

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.