FUTURIOM
THE FUTURE OF TECH

Cloud Market Trend Report - September 2020

The Future of Multi-Cloud Networking

September 2020

Sponsored by aviatrix

www.futuriom.com

Key Findings

- **The Great Cloud Wave – the shift of IT applications to multiple and hybrid clouds – is creating demand for a new multi-cloud networking (MCN) solutions than can unify networking infrastructure among cloud constructs.**

- **Enterprise IT, Network, and Security managers want a unified networking infrastructure that can connect with multiple cloud and integrate with their existing networking and IT investment.** Futuriom collected this feedback from a survey of 150 enterprise end users with technology roles, qualified as Director-level and above.

- **The key drivers of MCN include providing more options for multi-cloud and hybrid cloud (69%), consolidating data-center with public cloud infrastructure (69%), improving the performance of distributed applications (65%), and managing security policy and visibility (61%), according to Futuriom survey work.**

- **MCN solutions will be used to create software-defined virtual networks that can integrate private data center, public cloud, and enterprise networks.** This will drive the uptake of Network as a Service (NaaS), software-defined networking (SDN), and Application Programming Interfaces (APIs) to connect and integrate existing networks and cloud platforms.

- **Top use cases of MCN, according to end-user survey feedback, include security integration and virtual firewall management, multi-cloud application integration and performance assurance, network visibility, security analytics, and unified multi-cloud network monitoring and management.**

- **Companies highlighted in this report:** Alkira, Arrcus, AT&T (T), Aviatrix, Amazon (AMZN), Aryaka Networks, Cato Networks, Ciena (CIEN), Cisco (CSCO), Citrix (CTXS), Digital Realty (DLR), DriveNets, Equinix (EQIX), Fortinet (FTNT), Google (Alphabet) (GOOGL), IBM, Itential, Juniper Networks (JNPR), Masergy, Megaport, Microsoft (MSFT), NetFoundry, Nokia (NOK), PacketFabric, Pureport, Tata Communications, Teridion, Verizon (VZ), Versa Networks, Volterra, VMware (VWW)

(Note: This is not an exhaustive list of companies in the MCN space, but an overview of top companies that Futuriom has analyzed in its research.)

AVIATRIX CLOUD NETWORK PLATFORM

One Architecture. One Network. Any Cloud.

Simplify Enterprise Cloud Networking

The Aviatrix cloud network platform delivers the advanced networking, security and operational visibility services required by enterprises, while maintaining the simplicity and automation of cloud.

Advanced Multi-Cloud Network Transit

Aviatrix software enables enterprise IT to easily deploy a high-availability, multi-cloud network data plane with end-to-end and high-performance encryption, multi-cloud security domains and operational data IT teams need. Aviatrix transit provides the intelligence to ensure network correctness and the traffic engineering control network architects are missing from the basic transit constructs CSPs deliver.

Enterprise Class Operational Visibility

The Aviatrix platform brings day-two operational visibility not available from any cloud provider to help you pinpoint traffic anomalies and suspicious behavior, resolve connectivity problems faster, and share network health metrics and dynamic network topology maps with staff and management.

Multi-Cloud Network Training

Aviatrix offers hands on Aviatrix Certified Engineer (ACE) training and certifications to quickly bring your whole team up to speed on native AWS, Azure and GCP networking, multi-cloud reference architectures and the Aviatrix cloud network platform.

> *"Aviatrix's cloud network platform intelligently programs the native cloud network constructs and goes well beyond that by adding network segmentation policies, rich visibility, and automation that we require to support our customers. Aviatrix makes cloud networking much easier for us and our customers."*
>
> JOHN GOODSON
> SVP AND GENERAL MANAGER OF PRODUCTS
> VERINT

CLOUD NETWORK SIMPLICITY AND AUTOMATION WITH ENTERPRISE VISIBILITY AND CONTROL

As an enterprise IT leader, your organization is driven by business transformation and tasked to accelerate your migration to public cloud. However, large scale enterprise application or service transformations are not as simple as cloud providers would make it seem. The promise of cloud is simplicity and automation, but the reality for enterprise IT is much more challenging – shadow IT, cloud and networking skills gaps, limited visibility and lack of a well architected network design – all contribute to your team's everyday challenges.

Aviatrix cloud network platform is a foundation upon which you can regain visibility and control and shift your focus from managing disparate cloud network to controlling a consistent global cloud network that provides enterprise class networking, security and operational features that are simply not available from any cloud provider.

Aviatrix is helping put you and your operations team back in control. Cloud 1.0, driven by automation and infrastructure as code, often went around traditional IT, viewing IT processes, security, compliance as roadblocks to agility and speed. And, according to Gartner, cloud networking has been "ad-hoc" at best – driven by on-premises solutions lifted and shifted to cloud or limited by native cloud services that simply couldn't meet enterprise networking requirements. For Cloud 2.0 and beyond however, you need the network visibility and control you enjoyed on premise, now for your cloud networks. You want day-two operations, visibility, control, regulatory compliance and other enterprise IT architectural structures that make large scale IT environments operational for the long term. But it's different, you don't want to do it the same way, you want it modernized for the cloud and maintain the simplicity and automation cloud offers.

It's time to take an architectural approach.

As a forward-thinking enterprise cloud network architect, you realize that establishing a cloud architecture correctly is critical and the cloud network is the foundation. Business decisions will drive network design, so architect for flexibility. Each cloud provider has unique networking constructs, limitations and architecture. You must decide if you are going to attempt to bridge the skills gap, hire, train and grow your staff to manage the complexity of multiple cloud architectures or establish a single, multi-cloud architecture.

Aviatrix cloud networking experts engage directly with enterprise cloud network architects to guide cloud network designs based on a multi-cloud network architecture and your unique business requirements – resulting in a repeatable network design with consistent operational visibility and security across any cloud. Aviatrix experts have guided hundreds of customers through this architectural process and bring proven reference designs for single-cloud, multi-region and multi-cloud network environments.

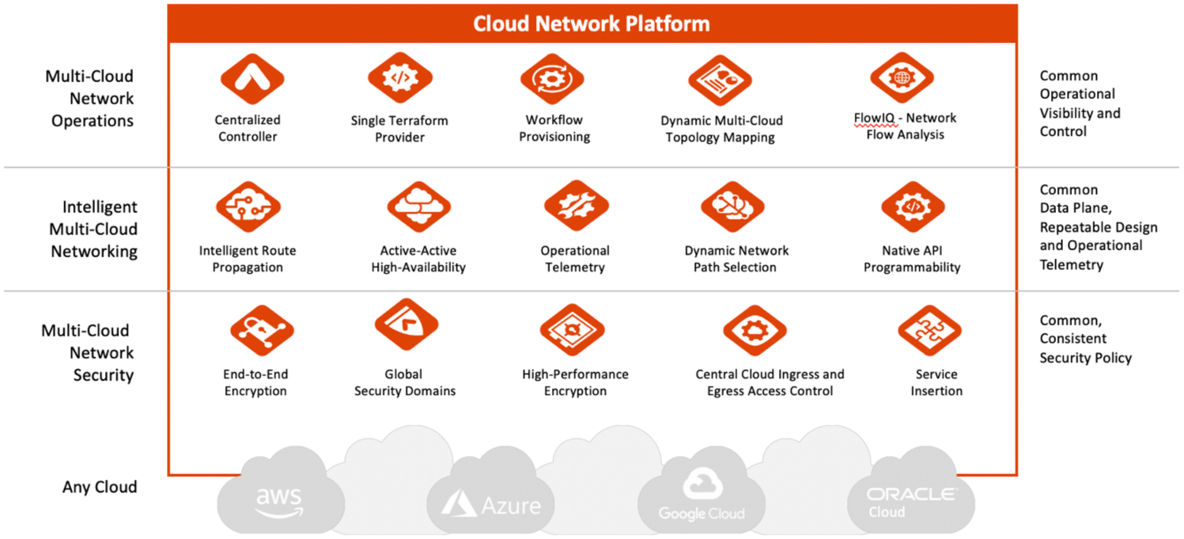

Cloud Network Platform
Multi-Cloud Network Operations
Centralized Controller
Single Terraform Provider
Workflow Provisioning
Dynamic Multi-Cloud Topology Mapping
FlowIQ - Network Flow Analysis
Common Operational Visibility and Control
Intelligent Multi-Cloud Networking
Intelligent Route Propagation
Active-Active High-Availability
Operational Telemetry
Dynamic Network Path Selection
Native API Programmability
Common Data Plane, Repeatable Design and Operational Telemetry
Multi-Cloud Network Security
End-to-End Encryption
Global Security Domains
High-Performance Encryption
Central Cloud Ingress and Egress Access Control
Service Insertion
Common, Consistent Security Policy
Any Cloud
aws
Azure
Google Cloud
ORACLE Cloud

Figure 1: The Aviatrix cloud network platform brings multi-cloud networking, security, and operational visibility capabilities that go beyond what any cloud service provider offers.

One Architecture. One Network. Any Cloud.

The Aviatrix cloud network platform brings multi-cloud networking, security, and operational visibility capabilities that go beyond what any cloud service provider offers. Aviatrix software leverages public cloud provider APIs to interact with and directly program native cloud networking constructs, abstracting the unique complexities of each cloud to form one network data plane, and adds advanced networking and security features including:

- Intelligent Cloud Network Correctness
- Active-Active High-Availability Transit
- End-to-End and High-Performance IPSec Encryption (wire speed up to 75 Gbps)
- Single Terraform Provider for Day-One Multi-Cloud Infrastructure as Code Automation
- Enterprise Class Day-Two Operational Visibility and Troubleshooting

Aviatrix customers leverage the capabilities of the Aviatrix cloud network platform in many ways. While each deployment is similar, each is also unique to each customer's requirements and network design. Similarities start with the Aviatrix Controller's ability to deploy Aviatrix networking and security services in a common, repeatable manner across clouds. Aviatrix Transit offers the same networking and operational capabilities across all cloud providers. Security policies for SAML User VPN, site-to-cloud connections and Internet egress, for example, are consistent and centrally managed across your multi-cloud network environment.

Beyond Orchestration.

Cloud providers will position automation scripts as orchestration, but orchestration only provides the initial deployment of network resources – it doesn't help you with day-two operations, visibility, network correctness verification or troubleshooting that your operations team needs to do their jobs effectively.

Aviatrix multi-cloud operational visibility includes features such as cloud network flow analysis, geographical source-destination heat maps, time series traffic analysis to visually identify flow anomalies, communication path evaluation to verify both routing correctness and security configurations for application communications and more.

> *"I really like the added visibility Aviatrix brings to my cloud network operations team. It's a great reminder of the visibility and troubleshooting ability we took for granted when infrastructure was 'on prem,' now we have even more for our multi-cloud network."*
>
> TOBY FOSS
> DIRECTOR OF CLOUD NETWORK OPERATIONS
> INFORMATICA

FEATURES AND CAPABILITIES

Multi-Cloud Network Architecture

Aviatrix helps enterprise cloud network architects create a multi-cloud network architecture and offers a cloud network platform that provides the software and services required to plan, deploy and operate a secure enterprise multi-cloud network.

Centralized Controller

The Aviatrix controller is the brain of the cloud network platform. The platform leverages the centralized intelligence and knowledge of the controller to dynamically program both native cloud network constructs and Aviatrix's own advanced services. Our single Terraform provider enables network and security Infrastructure-as-Code automation across your multi-cloud environment.

Network Service Gateways

Aviatrix gateways deliver advanced cloud networking and security services. Gateways are primarily deployed to deliver transit network and security services such as intelligent dynamic routing, active-active network high-availability, end-to-end and high-performance encryption and collect operational visibility data, but also for secure network ingress and egress filtering and external service insertion.

High-Availability Networking

Aviatrix secure network transit is designed with active-active high-availability and redundant pathing. Pairs of Aviatrix Gateways, deployed in separate availability zones, establish a full mesh, multi-path connection that maximizes both throughput performance and network availability.

High-Performance Encryption

Standard IPSec encryption is limited to 1.25 Gbps. Aviatrix's high-performance encryption distributes processing across multiple cores and aggregates IPSec tunnels to achieve wire speed encryption, up to 75 Gbps.

Multi-Cloud Network Segmentation

Some clouds enable the creation of security domains. Aviatrix extends secure network segmentation beyond cloud boundaries, enabling multi-cloud security domains, with consistent, centrally managed, global network segmentation and connection policies.

Secure Cloud Ingress and Egress Controls

Aviatrix gateways offer both ingress and egress L4 and Fully Qualified Domain Name (FQDN) filtering. Centrally managed filter groups ensure consistent multi-cloud security for any cloud application communicating with Internet-based resources and service.

Multi-Cloud Network Service Insertion

Aviatrix Transit provides a secure point of access for network and security services such as next-generation firewalls, IDS/IPS and SD-WAN cloud edge connections. Aviatrix gateways provides load balancing to scale out connected services and ensure redundant and failover high availability.

Operational Visibility

Enterprise network operations teams must have deep visibility into network activity. Native public cloud networks are opaque, even basic analytics must be obtained from multiple sources and require skilled human correlation to become actionable. Multi-cloud visibility is simply not available from any cloud provider.

Dynamic Network Mapping

Aviatrix leverages the central intelligence and knowledge of the controller to dynamically generate and maintain an accurate multi-cloud network topology map that includes all network resources and network configurations the controller is managing. The map includes both native network resources and Aviatrix secure transit and cloud ingress and egress control gateways.

FlowIQ – Intelligence Network Traffic Flow Analytics

Aviatrix extracts detailed network traffic flow data from Aviatrix Transit infrastructure including source, destination, port and protocol filtering and combined with additional meta data such as latency and tagging to deliver never before possible multi-cloud flow inspection and global traffic heat maps.

More

Additional advanced networking features which are not included in this overview include BGP propagation, traffic engineering, optimal path routing and more.

Try Aviatrix Today or Schedule an Architectural Review Session

Aviatrix is simple to deploy; our intelligent central controller is launched from cloud provider marketplaces and automates the deployment of additional network and security services, as required. Most customers launch and begin using Aviatrix services in an afternoon, easy to try and evaluate. We have experts available to help you.

Contact your Aviatrix account executive or email info@aviatrix.com to schedule an architectural overview or design session with one of our solution architects. Learn about Aviatrix Certified Engineer (ACE) training or for more information go to aviatrix.com.

1. Intro: Networking the Great Cloud Wave

The great Cloud Wave is here. As public cloud infrastructure has expanded to provide billions of dollars of infrastructure and services to enterprise end users, businesses and organizations have become more confident in moving large portions of their IT infrastructure to the cloud, which has become a more complex environment for distributed applications that can run in private clouds, public clouds, and hybrid clouds.

This rolling Great Cloud Wave has accelerated in 2020. The COVID-19 pandemic and the ensuing business crisis has demonstrated the utility of using cloud technology to scale and support virtual work and applications, whether it's remote learning, software-as-a-service (SaaS), or real-time collaboration and conferencing. The use of multiple cloud resources and the building of distributed cloud applications using technology such as microservices has now become a board-level priority across the globe.

Futuriom believes that this new phase of accelerated cloud growth will drive demand for solutions providing high-performance, secure multi-cloud networking (MCN), which can provide on-demand connectivity network connectivity to applications regardless of which clouds they reside in. Before we talk about how networking must evolve to support distributed applications and multiple clouds, let's clarify some of the terminology involved in connecting these clouds.

Private Cloud: A private cloud generally describes a datacenter built with current cloud technologies that runs "on-premises," or hosted and managed by an organization or an enterprise itself, rather than in a public cloud.

Hybrid Cloud: When enterprises build distributed applications that share resources on both private and public clouds, it is generally referred to as hybrid cloud.

Multi-cloud: Enterprises might need services or resources from multiple public clouds, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP). In this case they need to connect their networking infrastructure to multiple clouds.

Multi-cloud Networking (MCN): MCN technology provides the capability to build a logical, software-defined, secure network to cloud applications across multiple private clouds, datacenters, and public clouds.

As public cloud resources and hybrid-cloud applications proliferate, enterprises are finding a rising need to connect these services using a more efficient, software-defined approach to networking. Cloud resources and applications may move around or change quickly, and the legacy model of building static networks tied to specific hardware devices such as enterprise firewalls and routers is not agile enough for a multi-cloud and hybrid cloud world. All of this will put new demands and requirements on networking technologies, which must scale and provide agile and secure bandwidth to the many different types of cloud connections.

This report, the first of what we expect to be many on the topic of MCN, details the drivers for these new multi-cloud networking technologies, the required feature sets, use cases, and the emerging ecosystem of vendors looking to create MCN technologies.

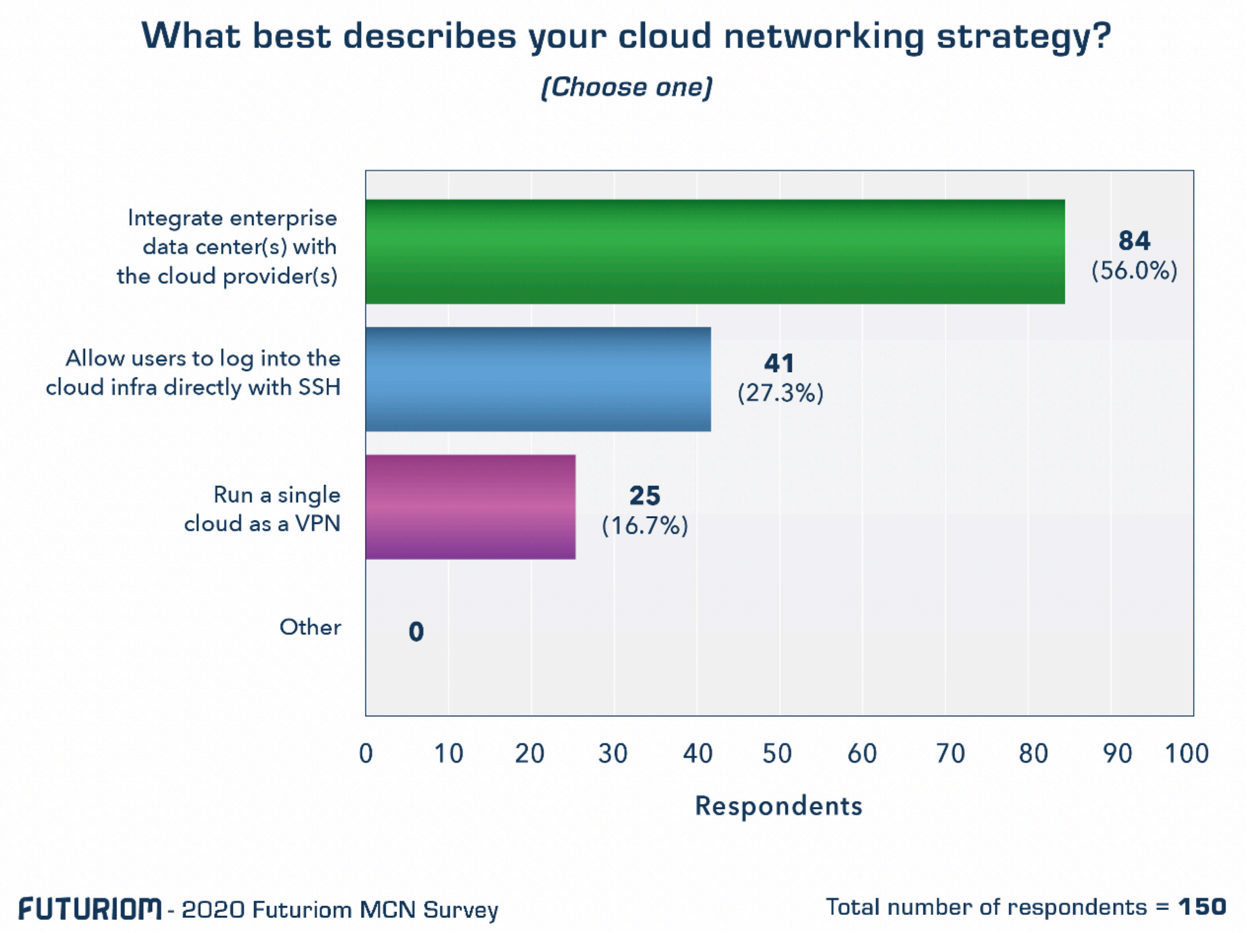
Our research has included dozens of interviews with end users as well as several end-user surveys, including the 2020 Futuriom MCN and a Network Automation surveys. In the Futuriom MCN Survey, we received responses from 150 enterprise end users qualified with Director-level and above roles in networking, IT, and security. We've also spoken to dozens of technology vendors in the space about emerging trends. In this report we have compiled all of this information into our vision of where MCN is likely to go over the next decade.

2. Technology Drivers for Multi-Cloud Networking

The evolution of cloud has created both challenges and opportunities for networking. It's time for the network to be re-invented. Think about the basic cloud approaches as creating "islands" of compute and applications workloads that need to be connected by networks. As the public cloud players have quickly expanded their infrastructure and subsumed large amounts of private and public traffic, they have become the de facto public infrastructure, rivaling both enterprise datacenters and public communications networks.

At the same time, the emergence of both private and public clouds has created a huge expansion in co-location facilities and Internet exchanges, where enterprises and cloud providers can easily connect to each other under one roof. One can think of this co-location infrastructure as the "edge" of the network and the place where the bulk of multi-cloud networks will meet. All of this infrastructure can now be more easily connected through the presence of software-based Application Programming Interfaces (APIs), which are the building blocks of cloud infrastructure.

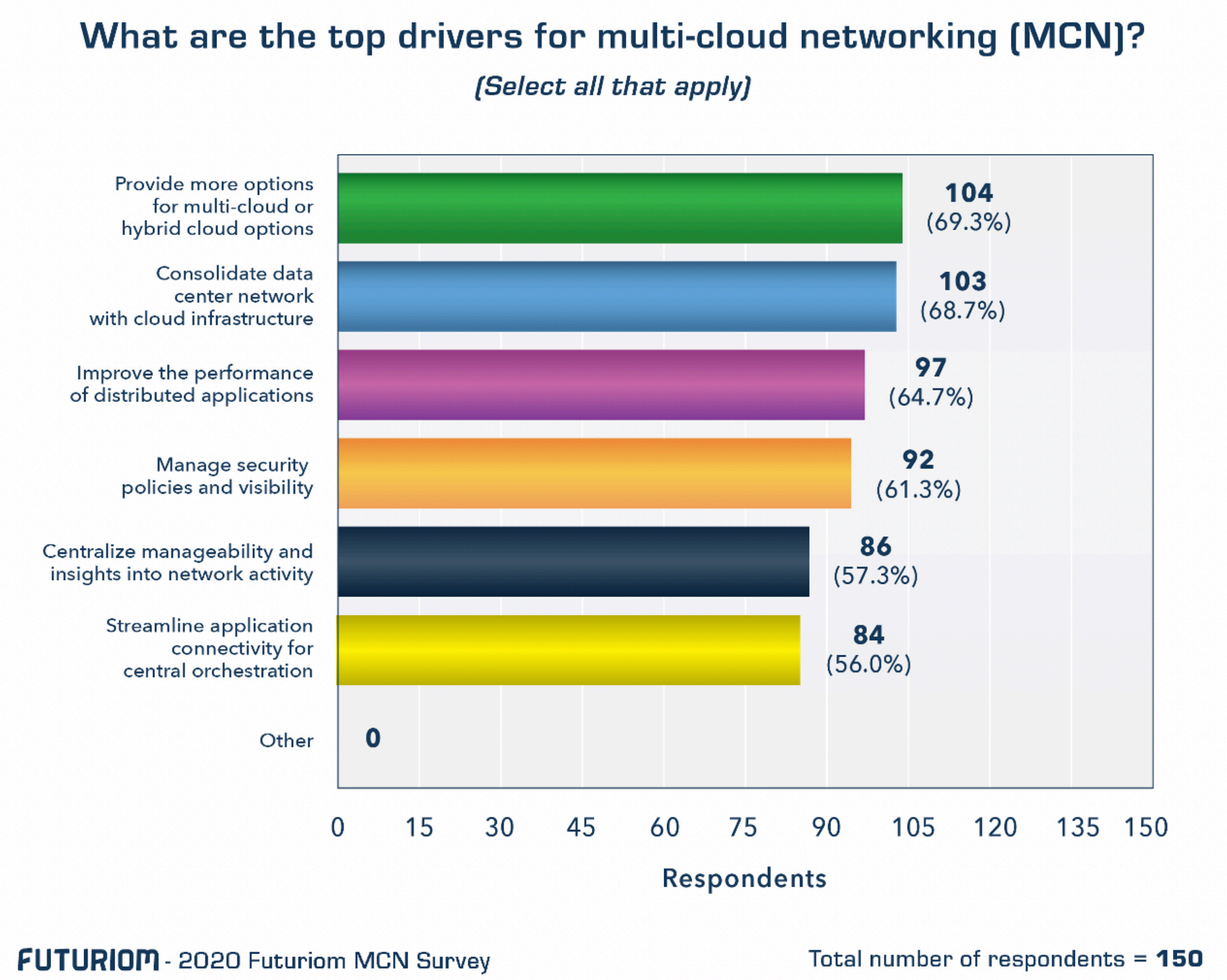
On a broad level, end users simply want one logical network to connect all of their applications and clouds. When we asked 150 enterprise network operators about their cloud networking strategy, the top focus was on integrating their enterprise networks with the cloud providers (56%).



If you are a public cloud or private cloud customer looking to build distributed applications that run in multiple clouds, this presents a bunch of challenges for your network. These challenges include:

- **The public cloud vendors have their own networks and their way of building them – known as "constructs" – and their goal is not necessarily to enable you to easily connect to other clouds, but to keep you inside their cloud.**
- **Running applications across multiple clouds poses security and compliance risks, because you may not always have insight and visibility into what's happening to your applications on networks in other clouds.**
- **In the cloud world, network capacity, connection topology, and bandwidth demand can be highly variable, requiring a more agile way to manage logical networks on demand, including providing auto-scaling, virtualization, and resiliency.**
- **Better network connectivity is needed to connect distributed apps, both geographically across multiple clouds and multiple microservices (multi-cluster).**

These are a few of the higher-level challenges. In the MCN survey of enterprise end users, we drilled down into the primary drivers of MCN technology. These top drivers included providing more options for multi-cloud and hybrid cloud (69%), consolidating data-center with public cloud infrastructure (69%), improving the performance of distributed applications (65%), and managing security policy and visibility (61%).



How will these goals be reached? The MCN approach to connecting across clouds requires a wide variety of network virtualization, integration, and application-layer technologies to address specific use cases, as we will detail in the following section. These users cases will be addressed by specific technology building blocks of enabling MCN technologies. These enabling technologies will need to operate across the entire networking stack, from the physical infrastructure (referred to in the networking as Layer 0-1), to networking layers 2 and 3, and up to higher applications layers (Layer 4-7 or above).

The MCN enabling technologies fit into the following categories:

Global Internet infrastructure: As they say in the networking world, respect the physical layer. In the cloud world, there is a lot focus on software and applications, which reside at the higher levels of the technology “stack,” but you cannot forget the physical infrastructure in the ground that supplies the raw bandwidth for the cloud. This includes optical fiber infrastructure operated by global service providers, cloud providers, and Internet Service Providers (ISPs), as well as other physical-layer networks such as mobile infrastructure and satellite providers. The leading cloud providers are making it easier for customers to connect their datacenters to the cloud faster using AWS Direct Connect, Azure Express Route, and Google Interconnect. One thing that’s interesting about the MCN networking movement is that this infrastructure is becoming more diverse, with cloud providers becoming more important players in building out and acquiring physical infrastructure and assets. These assets can now be leveraged by organizations that want to extend their enterprise network or build an entirely new network-as-a-service (NaaS).

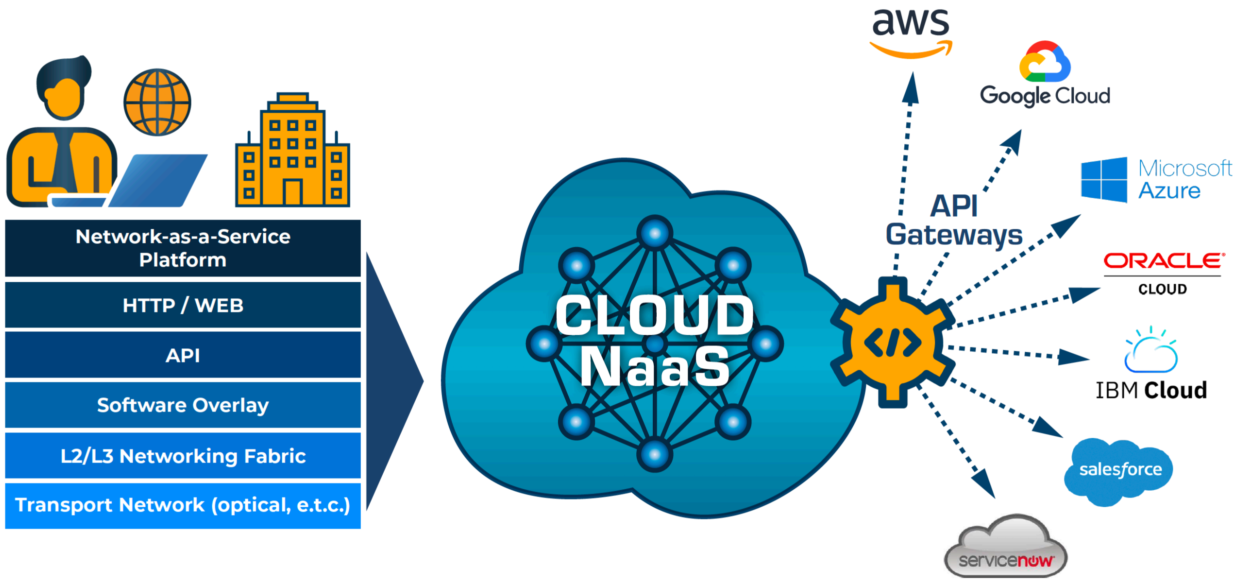
Colocation Facilities and Points of Presence (PoPs): The proliferation of colocation facilities and PoPs such as Internet peering points is one of the more important elements in the evolution of the cloud and MCN. PoPs and colocation facilities offer shared datacenters that allow operators in the cloud ecosystem to connect and “peer” their traffic. Global service providers, cloud providers, and enterprises alike use co-location facilities to build a global network of networks using a variety of Internet and cloud networking technologies.

Layer 2 and Layer 3 Virtualization: In order to manage and connect networking resources such as Ethernet services (Layer 2) or Internet Transit using technologies such as Internet Protocol (IP) routing and Border Gateway Protocol (BGP) (Layer 3), MCN will require a variety of network virtualization technologies that can connect to multiple clouds at gateways or PoPs. What’s most important about applying Layer 2 and Layer 3 virtualization is that it should be based on open, cloud-native technologies and APIs and automation, rather than being attached to specific proprietary hardware. This is one of the largest shifts from legacy enterprise networking to MCN.

Application Programming Interfaces (APIs) and Gateways: Futuriom sees a substantial shift in cloud and traditional operator networks from legacy models involving proprietary, vertically oriented systems to the open and scalable systems in the cloud ecosystem, which are driven by APIs and programmability – which is fundamental to the approach of the largest cloud or “webscale” services. A commonality among emerging technologies such as SDN, SD-WAN, and MCN is that they use cloud-native architectures and APIs to abstract, automate, secure, and improve networking within and between multiple public clouds. This enables the integration of traditional enterprise and datacenter networks with both private clouds and public clouds.

Application-layer Networking and Service Meshes: The fabric of the cloud is based on distributed applications communicating and exchanging data with each other, and service meshes and applications-layer connectivity can be used to connect these applications across clouds. The service mesh is an abstraction layer that manages communications, observability, and resiliency in distributed cloud-native applications. Innovations in MCN will include new ways to monitor and manage service meshes – as well as integrate them with physical infrastructure and network underlay -- to ensure the performance and security of multi-cloud connectivity and hybrid cloud applications.

Cloud-Native Approach to Multi-Cloud Networking



3. Key MCN Requirements and Use Cases

Emerging technology markets always start by solving very specific problems. The MCN challenges are numerous and complex, meaning it will require a variety of technologies to solve specific use cases. The enabling technologies of MCN will be used across the networking stack to deliver on specific use cases. This means there is plenty of room for technology providers to build and integrate solutions from a variety of providers, many of which are profiled in this report.

Overall, Futuriom sees MCN and cloud-native networking solutions solving the following general areas:

Compliance and security: When connecting applications across clouds, enterprises need to build a common multi-cloud network that can employ both cloud-native networking constructs and advanced network and security services that can operate across multiple clouds. Having a single, abstracted MCN could solve many operational challenges including network visibility, security, compliance, redundancy, and applications reliability.

Building MCN across clouds can present some complex security challenges – such as managing firewalls in the enterprise network as well as the public cloud at the same time. Many of the new wave of MCN tools can manage security such as encryption as well as firewall connectivity across clouds. This, for example, can help IT managers ensure consistent security by configuring consistent multi-cloud ingress and egress security and remote access control policies across a multi-cloud network.

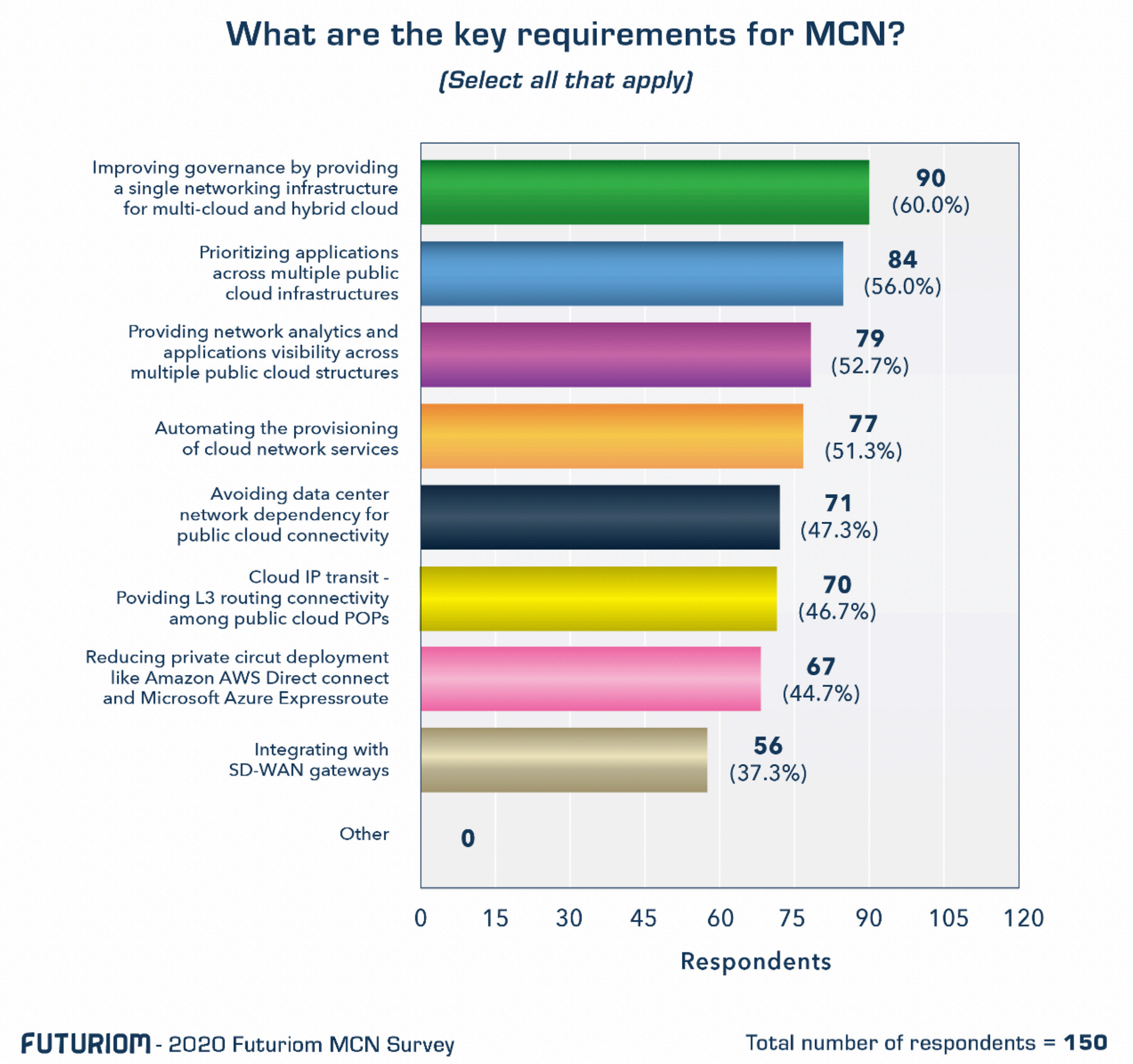
Integrated networking approach: One of the challenges with existing public cloud constructs is that using these tools risks cloud "lock-in" with a specific provider. These constructs may present challenges of integration with the existing legacy enterprise network. MCNs can help improve the flexibility of the enterprises by using cloud gateways, APIs, and software provisioning and orchestration to build a single infrastructure that can connect applications across multiple clouds. MCN tools can also be used to integrate routing, for example by resolving routing tables, Domain Name Services (DNS), Network Address Translation (NAT), and configuring cloud-based firewalls. These are important elements of integrating private networks with cloud networks.

Operational visibility, compliance, and security: One of the biggest areas to watch in MCN is how to provide management teams with peace of mind when they extend their networks across clouds. In our interviews and surveys, end users frequently cite the need to **build a logical, virtualized network that can integrate multiple cloud services while at the same time ensure compliance, security, and visibility into their networking infrastructure and applications.**

Connecting distributing applications. MCN technology can help solve some of the challenges of multi-cloud and hybrid cloud applications, many of which are built on microservices or use popular cloud-native orchestration tools such as Kubernetes. MCN can be used to optimize multi-cloud application performance, policy, and security. Service meshes and APIs can be used to connect and secure these applications at the higher layers of the networking stack.

Drilling Down Into Key Requirements

When we drilled down deeper into specific used cases and requirements through our survey and interview work, we discovered common patterns in the key requirements and use cases for MCN, as seen in the chart below.

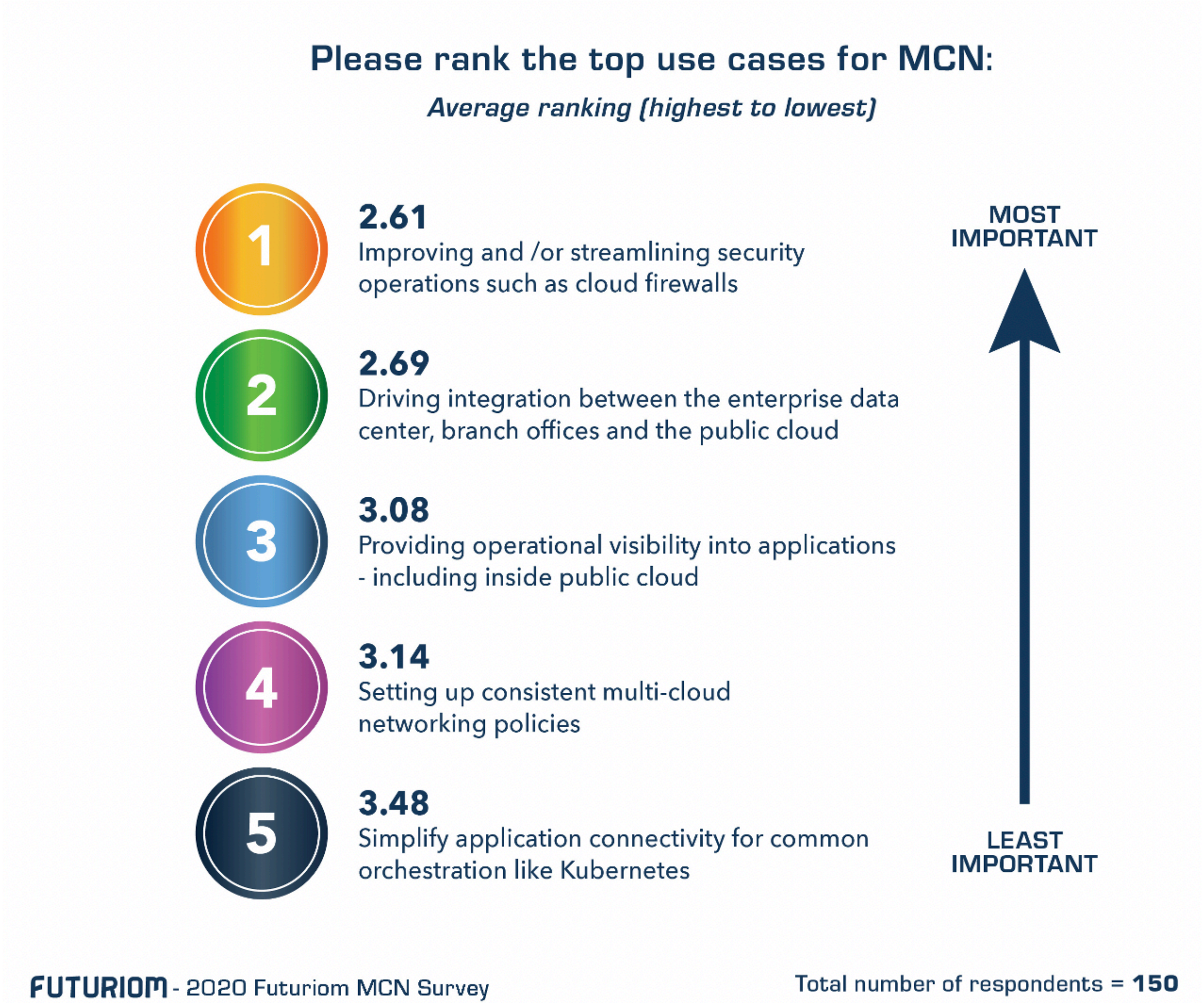


Note that the features and requirements are quite broad-based. Survey respondents were asked to select all that apply, and responses were widely distributed, reflecting a diversity of needs. But the top choice, "Improving governance by providing a single infrastructure for multi-cloud and hybrid cloud," selected by 90 respondents or 60%, is a common theme in our interview work as well. Managers need visibility into what's going on with their network and applications – they're not willing to connect into multiple public clouds unless they can monitor and integrate what's happening as a single logical infrastructure. Prioritizing applications across multiple cloud infrastructures (84 respondents, 54%), and providing applications visibility and analytics (79 respondents, 53%) are natural complements to theme of observability and control.

The common theme of nearly all the responses reflects the need to ensure that networks connecting multiple clouds can support the security, visibility, and performance of applications. This shows how MCN technology can be used to help organizations transition from "shadow IT" world of the cloud, in which many of their operations are operating in the dark, to the "official IT" world of the cloud, where MCN technologies are used to solve compliance and operational challenges.

Additional MCN Use Cases

In Futuriom's recent MCN survey, users were asked to rank top MCN use cases from highest to lowest. Below, you can see the ranking of the top uses cases for MCN, with the lowest score representing the highest ranking (survey respondents were asked to rank the uses cases from a scale of 1 to 5, with 1 = best).



Please rank the top use cases for MCN:

Average ranking (highest to lowest)

1 **2.61** Improving and /or streamlining security operations such as cloud firewalls

2 **2.69** Driving integration between the enterprise data center, branch offices and the public cloud

3 **3.08** Providing operational visibility into applications - including inside public cloud

4 **3.14** Setting up consistent multi-cloud networking policies

5 **3.48** Simplify application connectivity for common orchestration like Kubernetes

FUTURIOM - 2020 Futuriom MCN Survey

Total number of respondents = **150**

While these survey results have highlighted some of the most common goals of MCN technology, the use cases are plentiful and are likely to expand. In our discussion with end users as well as MCN vendors, it is clear that MCN will develop as a complex ecosystem that may require several tools to solve the expanding use cases. Let's take a look at what's in these top use cases.

Improving security operations including firewalls: In our survey, improving security operations got the highest ranking as a use case. The reason this is emerging as a key MCN use case is that network traffic policy needs to be consistent from the enterprise datacenter into the public cloud. Native cloud networking constructs often provide obstacles to managing virtual firewalls, requiring IPSec VPNs or other overlays that can't integrate with the enterprise networking security architecture. Multi-cloud solutions can be used to automate the deployment of virtual firewall instances in the cloud, on demand; remove the need for IPSec tunneling; and maximize throughput performance.

Driving network integration: The second-ranked use case was driving network integration, which is a more broad category. One of the major trends developing in the industry is the use of cloud IP transit networking to support applications. Organizations see a lot of value in connecting their networks to the large cloud networking infrastructures to extend the network. But enterprises don't want their data and applications to be limited to a specific cloud network, and they want the approach to be consistent. For example, they might want to use services such as Microsoft Azure Virtual WAN or an Amazon VPC, but they need consistent operational visibility and integration. They may want to extend the cloud out to the enterprise premises using Google Anthos, Amazon Outposts, or Azure Arc. But as enterprises and other organizations extend the resource of the public cloud, they don't want to be locked into a single cloud network. MCN networking tools will use a variety of techniques including APIs and cloud gateways to build a heterogenous, multi-cloud network that can be operated by an organization as one virtual entity.

Workflow and operational visibility: As detailed, implementing a unified operational model for networking, whether it's in private cloud, datacenter, or multi-cloud, is a top priority. For example, a multi-cloud approach can unify telemetry, monitoring, and network policy visibility across clouds. Desired features include traffic flow analysis, network segmentation control, and troubleshooting in a single console. A multi-cloud network approach can also be used to automate provisioning with a single Terraform provider or leverage simple workflow-based deployment processes.

Consistent policy implementation. Managing network segmentation and application policies across multiple clouds can be challenging. MCN solutions can help facilitate applications and security segmentation by unifying policy management across multiple clouds. This can include integration with the enterprise firewall platform by providing connectivity to the virtual firewall instances located in public clouds.

Additional Use Cases to Watch

Integration with the enterprise edge, including SD-WAN. Futuriom has tracked the explosive growth in the software-defined wide-area networking (SD-WAN) market, which, according to our annual SD-WAN Infrastructure Growth Report, is growing at a rate in excess of 30% compound annual growth rate (CAGR). SD-WAN merged as a tool for integrating, optimizing, and automating the connection to the enterprise edge. MCN can be seen as a way to integrate, optimize, and automate the connection of multiple clouds, including those connected via SD-WAN at gateways or edge PoPs. The integration between SD-WAN and MCN is likely to grow over time as a way for enterprises to extend their WAN resources.

5G Edge and private wireless connectivity. In several end-user surveys conducted by Futuriom this year, 5G has come to the fore as priority for both enterprises and service providers. Operators see 5G as the key to deploying value-added services and supporting potentially gigantic markets such as autonomous driving and virtual reality/augmented reality (AR/VR). At the same time, enterprises are looking at building new wireless networks of their own, which may or may not be connected to the public communications infrastructure, in order to support industrial automation or business analytics, processing data in real-time at the “edge” or as close to their facilities and devices as possible. MCN is likely to play a large role in connecting 5G networks to the cloud.

4. Key Tech Trends in the MCN Ecosystem

There is an exciting amount of innovation in the multi-cloud and cloud-native networking space, which Futuriom has been following for the last year. In the last six months, we have tracked an explosion of innovation in the startup community that will be quickly adopted by organizations to solve their MCN headaches.

As you can see from the described multiple use cases, the application of MCN is both complex and substantial. Just as it would be silly to think that one solution could solve all the problems of the cloud, it’s simplistic to think that all the networking needs of the cloud can be solved with one tool. Futuriom expects a wide variety of incumbent networking providers as well as MCN startups to work together to solve the challenges.

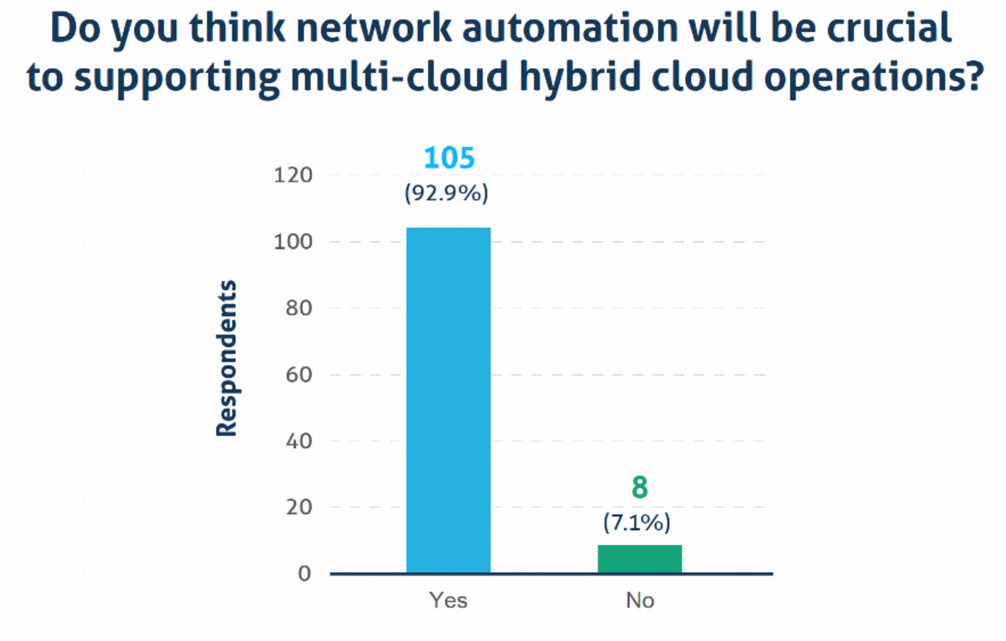
In looking at emerging technologies from the startup and cloud community, Futuriom has discovered a wide range of innovative companies pursuing many uses cases for MCN. While there is much overlap between many of these tools, they can be seen as addressing the following key areas of the MCN ecosystem. Let's examine some key trends and groups of technology vendors.

Cloud NaaS: Automating the Network Infrastructure

While virtualization is the key to introducing automation and agility into networks, you still need an underlying infrastructure to meet these needs. Optical networks, wireless networks, co-location facilities, and even good-old-fashioned copper networks are still needed to provide the last mile and connectivity into the cloud at PoPs.

The difference between legacy infrastructure and next-generation MCN will come in the form of automation, orchestration, and full network visibility. Legacy infrastructure is manually configured and tied to proprietary hardware interfaces or hard-wired circuits such as MPLS and private lines. The new MCNs will be driven by adaptable interfaces based on cloud principles such as web interfaces, APIs, and SDN. They will include a more heterogeneous approach that can adapt both open-source networking hardware and software as well as more flexibly proprietary technology using APIs.

As demonstrated in our recent CSP Networking Automation Survey and report, results from 100 network operators indicate that automation will be key to multi-cloud efforts.



N=100

Several groups of companies are pursuing this model as they adapt and look to develop more flexible tools. They include the following groups of companies.

Cloud providers such as **AWS, Microsoft Azure, Google, IBM**, and others are building substantial cloud infrastructure that help enterprise connect directly to their global networks using API gateways at local PoPs. This trend enables enterprises as well as SD-WAN providers to boost application performance by plugging directly into cloud networks using services such as Azure ExpressRoute or Virtual WAN, Google Virtual Private Cloud (VPC), and Amazon VPC or Transit Gateway. The three major cloud providers have also made a major push into helping extend public cloud to on-premises with Google Anthos, Amazon Outposts, and Azure Arc.

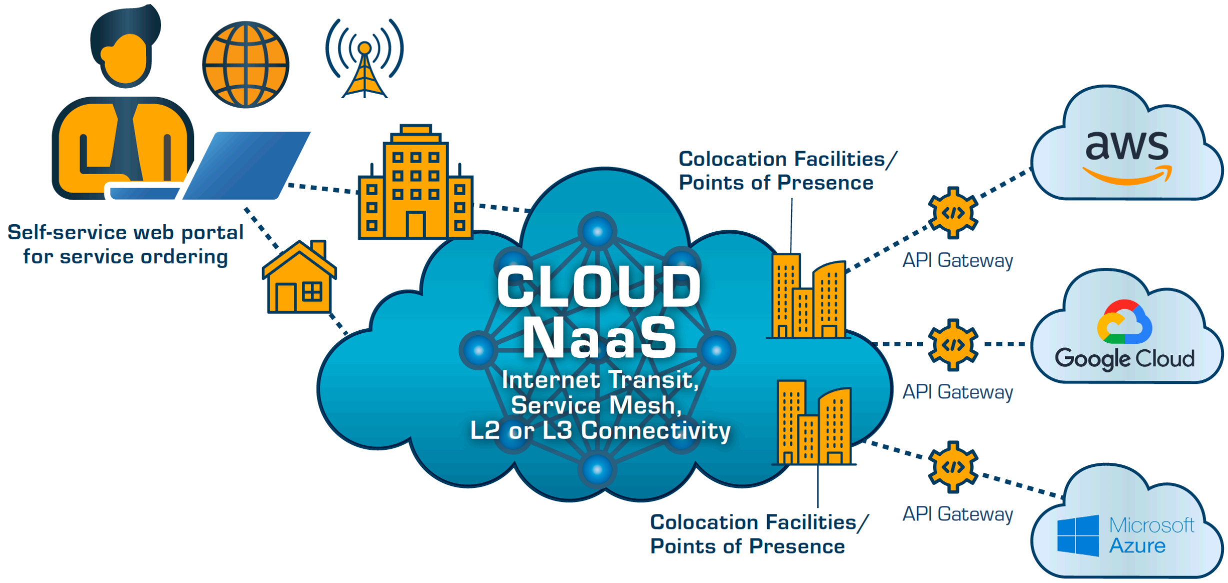
Colocation providers such as **Equinix and Digital Realty** have built large footprints of hosting facilities but are now expanding into the software management domain with virtual network connectivity tools such as Equinix's ECX, which is designed to help networking managers create cloud fabrics among colocation facilities.

A number of virtualized network-as-a-service (NaaS) providers are using cloud-native approaches to help organizations connect to infrastructure on the fly. For example, **Megaport** uses a virtual networking overlay and software-based provisioning to provide private point-to-point Ethernet links between cloud networks. **PacketFabric** provides a web-based NaaS provisioning platform to instantly build multi-cloud connectivity, including adding bandwidth, without waiting for manual provisioning of circuits. **Alkira,** founded by the founders of SD-WAN pioneer Viptela (Cisco), provides a NaaS targeting MCNs with its own cloud infrastructures using a slick self-service portal that abstracts out all network configuration. Alkira is also white-labeling its platform to service providers to reduce the friction in provisioning MCNs. **Teridion**'s public-cloud based Internet overlay targets improving route optimization. **Cato Networks** started in the SD-WAN camp but is rapidly expanding the number of PoPs it offers on a global IP Transit network bundled with a cloud security suite.

Traditional service providers such as **AT&T, Telefonica, Tata Communications, and Verizon** are racing to virtualize the software control of their substantial networking assets. The question is will they be able to overcome their legacy business models and slow provisioning times to move directly to a virtualized model. Many of them have made strides in building more modern OSS and BSS software that can provision and bill for value-added MCNs, as well as building customer portals that enable customers to order their own networks. Further MCN functionality will be extended by their partnerships with SD-WAN vendors, who are starting to provide MCN features. Some are making further investment.

For example, Tata has invested in NetFoundry Inc, which provides a cloud-native network platform, including a dynamic Internet overlay Fabric comprised of a mix of edge and cloud PoPs.

Building the Virtual NaaS



All of this is headed in the same direction: Picture a giant virtual cloud that can be accessed using software-based NaaS tools that can build any-to-any network connectivity among private networks, datacenters, and public clouds.

How IP Routing Innovation Will Drive MCN

A new generation of cloud-based routing underlay solutions are emerging to target cloud-scale networks. MCN requires different characteristics for routing. Instead of being tied to a specific hardware box, cloud-based routing needs to be built in software, typically using a microservices approach, so it can be hosted and scaled across clouds. It should also be disaggregated from a specific flavor of hardware and implemented as a discrete Networking Operating System (NOS) that can run in any type of cloud – private cloud or public cloud. This way, IP routing with encryption and security can be used to create resilient, secure networks that connect multiple clouds. Routing market leader Cisco's recent unbundling of its IOS routing software as part of its effort to deliver its new Silicon One chip strategy reflects the mainstream pressure to adopt a disaggregated, cloud-based approach to IP routing.

Some of the new NOSes with advanced IP features are being provided by cloud-native network startups **Arrcus** and **DriveNets**. Cloud-based IP routing will be an area to watch as next-generation technologies such as Segment Routing (SR-MPLS and SRv6) add features to make IP routing part of MCN solutions, setting the stage for a new era of routing innovation. Incumbent NOS routing leaders such as **Cisco, Nokia, and Juniper Networks** are also retooling and "disaggregating" (unbundling software) for routing in MCN applications. As an example, Nokia has announced revamped NOS strategy including Nokia Service Router Linux (SR Linux) and Nokia Fabric Service Platform (FSP), targeting cloudscale routing and boasting an impressive customer with Apple. Nokia is also integrating virtual networking and underlay capabilities with its SD-WAN and data-center networking platform, **Nuage Networks**. Even optical networking leader **Ciena** has entered the routing market, with solutions targeting the edge market. **Pureport's** Multicloud Fabric platform provides a distributed, layer-3 fabric that is based on FRR for enabling MCN over their infrastructure. Additionally, Pureport partners with other service providers, including PacketFabric, to extend hybrid cloud capabilities to a partner's customer base.

Expect to hear more about this as the landscape shifts quickly. Who will win? There are a lot of NOSes and approaches to cloud-native routing on the market. One battle will come in the form of open-source versus proprietary. In some applications, end users believe that open-source solutions such as FRR can be effective in scaling multi-cloud connectivity, while others say that proprietary solutions are needed to address high performance and the scalability issues of some open-source solutions. The religious wars will heat up as various factions tout their cloud routing solutions as the best. But Futuriom believes the trend is exciting and offers ways in which routing can be reinvented for the cloud.

Up the Stack: MCN Management and App-layer Services

As you move up the cloud networking "stack" away from physical infrastructure and into MCN software applications, there are a wide variety of approaches that can be used with overlays at the L4-7 level to improve connectivity to clouds, as well as provide app-layer services.

For example, **Aviatrix** provides a cloud network platform, which through an intelligent controller and integration with Terraform directly programs the native cloud networking constructs of AWS, Azure, GCP and OCI, while adding advanced networking and security services to help network managers and IT professionals maintain a single point of operational visibility, control, security and compliance across the MCN.

But that's not all! Innovators can put app-layer networking and security in the cloud and tie it into many different cloud-based services, in the same way that Hyperconverged Infrastructure (HCI) combined virtualization of storage, networking, and compute as one scalable service.

There are emerging multi-layer integrated stacks for MCN in the cloud. For example, **Volterra** provides an entire SaaS-based suite of app networking and security services, including a distributed load balancer and ingress-egress controller, a distributed API gateway, WAF/DDoS, and API auto-discovery and control.

Volterra has also built its own application delivery network in what resembles a content delivery network (CDN) for MCN, but for stateful workloads, hosted and secured on a private network with 10+ terabits of capacity. **NetFoundry** has an intriguing cloud-native networking fabric to provide Quality of Experience (QoE), zero-trust / virtual private networking (VPN), and application network control through a software development kit (SDK) and APIs.

Virtualization pioneers **Citrix** and **VMware** don't want to be left out of the MCN party either. Cloud overlay pioneer **VMware** has been busy integrating its virtual networking platform NSX with VeloCloud SD-WAN and Avi's load balancer to build a multi-cloud solution that extends from the enterprise SD-WAN edge to inside of the cloud. At the same time, VMware is folding in software-based security and firewalls into this cloud networking portfolio. **Citrix** provides a variety of tools designed for building MCN, including its virtual Citrix ADC, Citrix SD-WAN, Applications Delivery Management, and the Citrix Web App Firewall.

SD-WAN: Set for Integration with MCN

SD-WAN is a growing technology that emerged from the need to consolidate a number of branch-office networking technologies such as routing, WAN optimization, and route optimization with software control. SD-WAN typically terminates at the cloud instance or PoP of the SD-WAN provider, but it's now being extended into cloud services such as AWS and Azure using technologies such as Direct Connect or Azure Virtual WAN.

It seems obvious that SD-WAN functionality will be extended into the cloud to provide MCN features. The way to think about it is that SD-WAN optimized and virtualized the enterprise edge, providing a platform for a variety of WAN apps ranging from route optimization and applications delivery to security. These same functions will be enabled when connecting networks across multiple clouds.

It's going to be interesting to see how the such as leaders such as **Aryaka Networks**, **Cisco**, VMware's **VeloCloud,** and **Silver Peak (HPE),** among many others (please see our 2020 SD-WAN Growth Infrastructure report for the full ecosystem), take SD-WANs from regional PoPs into MCN. The focus will be on further integration through direct connections to other cloud providers as well as service provider networks. This will break down differently depending on whether the SD-WAN providers focus on PoP infrastructure on their own vs. partnering with service providers and cloud providers. For example, Cato Networks is building out a network of

PoPs, last numbering 55+, focused on security services or Secure Access Services Edge (SASE). Aryaka already operates their own middle mile cloud network and offers SmartServices from its PoPs, including direct connectivity to AWS, Azure, Google, Oracle, and Alibaba Cloud -- in addition to 400+ SaaS services. Aryaka also has an agreement with Equinix to use ECX Fabric to extend coverage to regions beyond its PoPs.

Some of the other SD-WAN providers are also partnering with cloud providers using direct connections and PoP colocation, but they are more focused on SD-WAN platform functionality and partnerships rather than building their own infrastructure. For example, **VMware's** VeloCloud has been deepening partnerships with service providers to expand their PoPs as gateways and integrating with the physical infrastructure. **Versa Networks** is focused on providing the SD-WAN platform in partnership with infrastructure providers including service providers such as Comcast and Verizon as well as Managed Service Providers (MSPs). Another interesting example is the integration being demonstrated by **Fortinet**, an SD-WAN and security software and hardware provider, with **Masergy**, an enterprise-focused service provider, to provide an integrated SD-WAN, security, and infrastructure bundle. Integration between SD-WAN enterprise edge and MCN is likely to increase over time, resulting in many partnerships and potential combinations.

Company Leadership Profile: Aviatrix
Aviatrix cloud network platform delivers advanced networking, security and operational visibility required by enterprises with the simplicity and automation of cloud. More than 400 customers worldwide leverage Aviatrix and it's proven multi-cloud network reference architecture to design, deploy and operate a repeatable network and security architecture that is consistent across any public cloud. Aviatrix CoPilot visibility platform provides a global operational view of an entire multi-cloud network, which is not available from AWS, Azure or any other cloud provider. Finally, enterprise IT teams use Aviatrix's Multi-Cloud Terraform provider to bring networking in as an integrated part of their Infrastructure as Code CI/CD pipeline. These capabilities combined with the industry's first and only multi-cloud networking certification (ACE), Aviatrix is empowering IT to lead and accelerate the transformation to the cloud. Learn more at Aviatrix.com.

Cloud Market Trend Report - September 2020

FUTURIOM

THE FUTURE OF TECH