IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Prepared for:

Enterprise Strategies for Hybrid, Multi-Cloud Networks

April 2025 EMA Research Summary Report

By **Shamus McGillicuddy**, VP of Research
Network Infrastructure and Operations

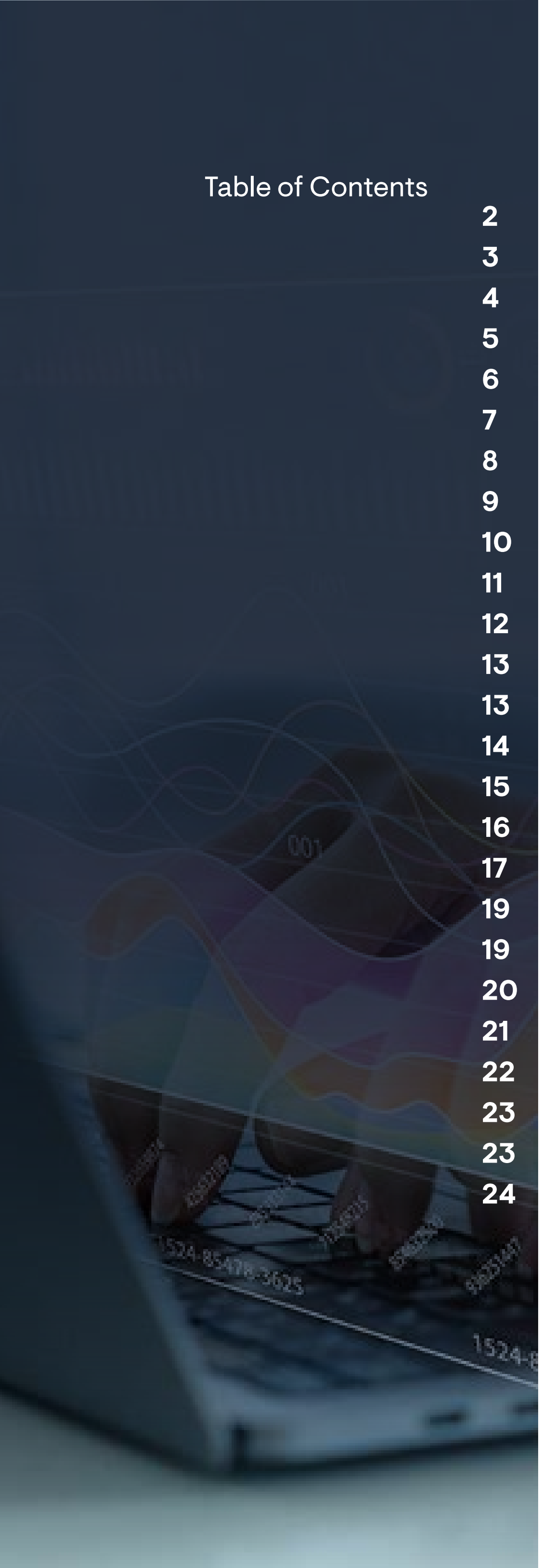


Table of Contents

Executive Summary

This summary of market research explores how enterprises design, build, and operate hybrid, multi-cloud networks. It is based on a survey of 354 IT professionals and decision-makers who work for enterprises that currently maintain private data center infrastructure and use two or more public cloud providers.

Introduction

Enterprise Management Associates (EMA) research consistently finds that many enterprises are maintaining hybrid cloud infrastructure that includes a mix of data centers (both on-premises and colocation data centers) and public cloud infrastructure. Furthermore, EMA recently found that 56% of enterprises are multi-cloud, using two or more public cloud providers of infrastructure as a service (IaaS) or platform as a service (PaaS). While enterprises are certainly migrating many digital services into the public cloud, EMA expects mainstream companies to continue to maintain hybrid cloud environments, including a mix of on-premises data centers, colocation providers, and multiple public cloud providers.

This research explores how enterprises are building and managing the networks that connect and enable these hybrid, multi-cloud architectures. It is based on a survey of 354 IT professionals who work for enterprises that operate hybrid, multi-cloud architectures.

Research Methodology

EMA's research goal was to understand hybrid, multi-cloud networks. Thus, survey respondents were only qualified to participate if they met three prerequisites:

1. Their organizations used one or more data centers (on-premises and/or colocation)
2. Their organizations used two or more providers of IaaS or PaaS cloud services
3. They were directly involved in how their organizations design, build, and/or manage their hybrid, multi-cloud networks

Figure 1 summarizes the demographic details of EMA's survey participants. This was a transatlantic survey (North America and Europe) of midsized to very large enterprises. EMA sought a broad cross-section of perspectives. Thus, respondents ranged from subject matter experts (admins, engineers, and architects) up to IT executives across multiple functional groups, including IT/network operations, cloud, project management, security, IT architecture, and network engineering. Seventy-five percent of respondents were concentrated in four vertical industries: finance services, manufacturing, health care, and retail/wholesale/distribution.

Figure 1. Demographics

Job titles

38%	Infrastructure subject matter experts (admins/engineers/architects)
5%	Software developers/engineers
25%	IT/cloud-related managers
21%	IT/cloud-related directors/VPs
11%	CIOs/CTOs

Company size (employees)

18%	Midsized – 1,000 to 2,499
56%	Large – 2,500 to 9,999
25 %	Very large – 10,000 more more

Region

68%	North America – United States and Canada
33%	Europe – France/ Germany/United Kingdom

Groups

21%	IT or network operations
18%	Cloud/DevOps/ Site reliability engineering
18%	IT project/ program management
14%	IT security/cybersecurity
11%	IT executive suite
11%	IT architecture
8%	Network engineering

Top industries

29%	Banking/Finance/Insurance
19%	Manufacturing
13%	Health care/pharmaceutical/hospitals
12%	Retail/Wholesale/Distribution
6%	Professional services unrelated to IT
6%	Transportation
4%	Education/Research

Sample Size = 354

Key Findings

- Only 25% of respondents believe their organizations are completely successful at building and managing their hybrid, multi-cloud networks
- Multi-cloud is driven by a desire for improved flexibility and scalability, cost optimization, and improved digital experience
- Only 37% believe their network and cloud teams are completely effective at collaborating
- Cloud service providers remain the most popular source of networking solutions in hybrid, multi-cloud networks
- Most organizations make it a high priority to unify and centralize management of nearly all aspects of networking across their clouds and data centers
- Only 27% have a comprehensive source of truth for their cloud networks
- Only 29% are completely satisfied with their cloud network observability capabilities. Most organizations use cloud provider tools and traditional network monitoring and observability tools for cloud network observability
- Most organizations think DNS data is valuable for threat detection and performance monitoring in their cloud networks
- Most organizations think packet data is important for security detection and response and performance monitoring in their cloud networks

Strategic Drivers of Cloud Strategy

Technical Factors that Motivate Multi-Cloud Adoption

Figure 2 identifies the technologies and technical initiatives that motivate companies to use more than one cloud provider. Four factors are most prominent:

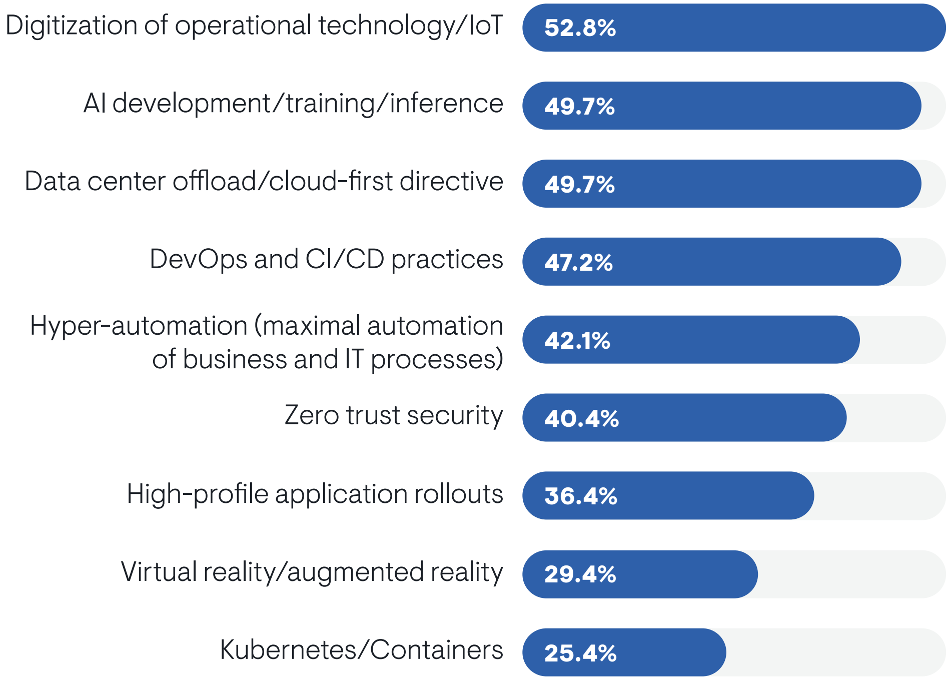
1. Digitalization of operational technology, such as industrial control systems and Internet of Things (IoT sensors. These systems are often highly distributed in remote areas, forcing enterprises to deploy applications in clouds that are closer to them to ensure network performance and meet compliance requirements, like data sovereignty.
2. AI development/training/inference. EMA interprets this as a recognition that enterprises may add one or more cloud providers to support their requirements for GPU as a service. They may also need to deploy AI applications with cloud providers who have footprints that are closer to the data at the edge of their networks.
3. Data center offload/cloud-first directives. A longstanding focus for many enterprises is to move as much of their infrastructure requirements into the cloud as possible. This creates more demands for cloud services, and that increased demand is forcing provider diversification.
4. DevOps and CI/CD practices. DevOps teams often push hard against vendor lock-in to allow them to build more flexibility and resiliency into the services they create. Multi-cloud can address these principles.

IT executives were more likely to select AI and digitization of OT. They were also more likely to select zero trust security as a multi-cloud driver.

Responses varied based on which parts of a company generally drive cloud strategy. For instance, AI was perceived as a multi-cloud driver if the cloud, IT, and security organizations were leading cloud strategy, but it was less of a factor if line of business of finance groups were cloud leaders. Data center offload was also a factor for IT-led cloud strategies, but not for those led by lines of business.

Finally, organizations that reported a larger number of cloud providers currently in use were more likely to select DevOps, hyper-automation, and high-profile application rollouts as drivers of multi-cloud.

Figure 2. Which of the following technical initiatives and trends are driving your organization's interest in using multiple public cloud providers?



Sample Size = 354

Business Factors that Motivate Multi-Cloud Adoption

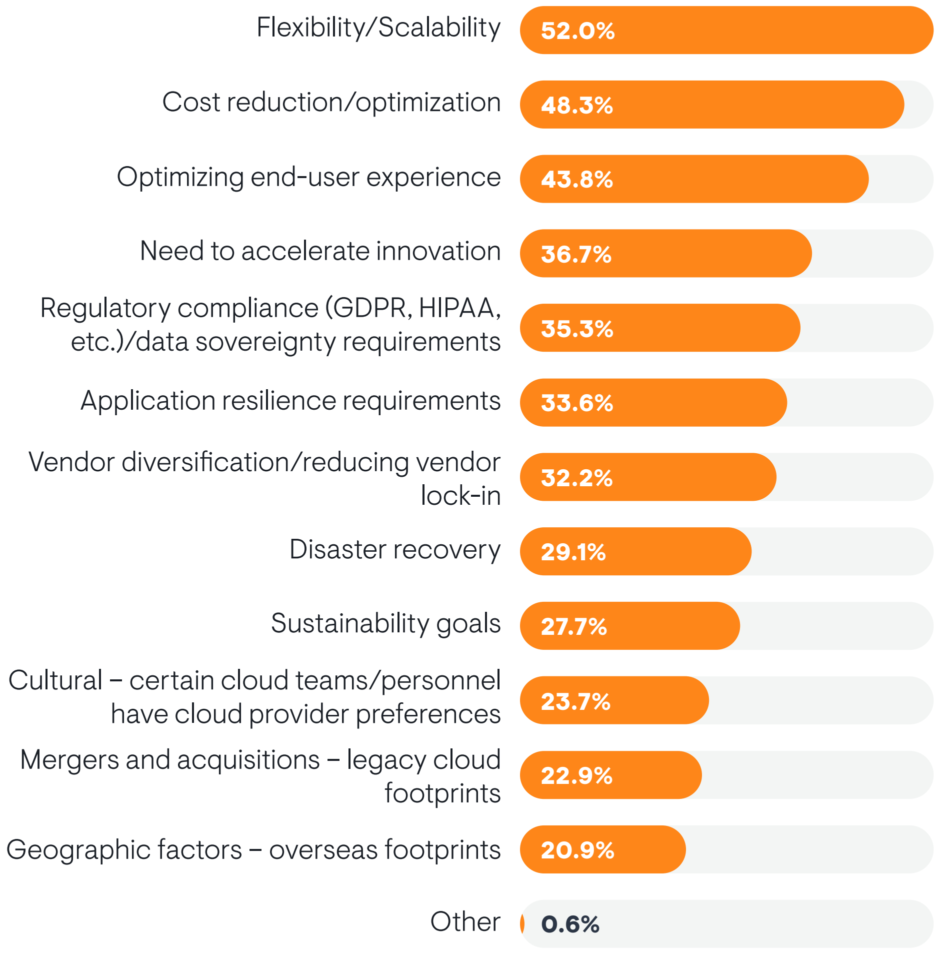
Figure 3 identifies the business factors that motivate a company to adopt multiple cloud providers. There are three top drivers:

1. Flexibility/Scalability. Companies want to be able to deploy and scale up applications wherever and however needed, without living within the confines of what a single provider can offer. Notably, respondents who selected this driver tended to report less overall success with their cloud networks.
2. Cost reduction/optimization. In theory, companies believe they can make cloud providers compete on price. They can also select which provider to use for a given application based on how that application's requirements will impact overall cost.
3. Optimizing end-user experience. By distributing applications across multiple providers, companies can bring those applications closer to customers and employees, reducing latency and improving user experience.

IT executives were more likely to perceive cost reduction, flexibility/scalability, compliance, disaster recovery, application resiliency, and vendor diversification as drivers. Subject matter experts, like IT engineers and architects, were more likely to select cost reduction and optimization.

Cultural preferences, mergers and acquisitions, and geographic factors were the least influential over multi-cloud adoption. However, very large enterprises (10,000 or more employees) were more likely to cite geographic factors. Smaller companies tended to cite disaster recovery, application resilience, and accelerated innovation more often. Cloud strategies led by the financial organization of a company correlated more strongly with mergers and acquisitions.

Figure 3. Which of the following business factors are driving your organization's use of multiple cloud providers?



Sample Size = 354

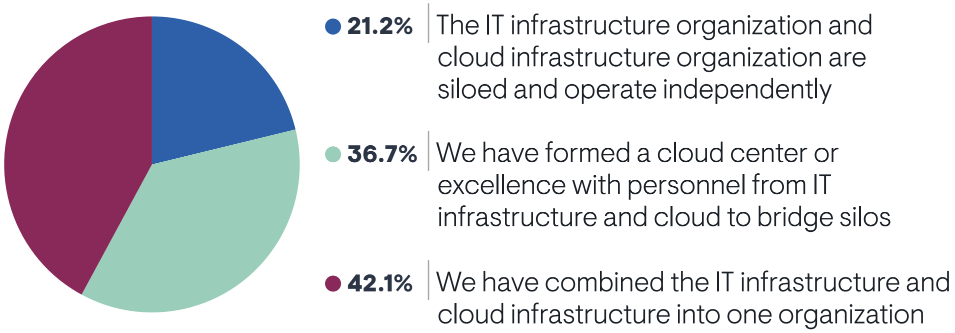
Cloud Stakeholders

Silos Between IT Infrastructure and Cloud Teams

Not only has the IT organization taken a leadership role in the cloud, IT infrastructure and cloud teams have become more integrated. **Figure 4** reveals that only 21% of companies have siloed cloud and IT teams operating independently. Instead, 42% have combined these groups into one organization and 37% have created cloud centers of excellence that straddle these groups.

Respondents who work within a cloud or DevOps team were more likely to report that cloud and IT groups are still completely siloed. Companies that let the security group drive overall cloud strategy are more likely to have dissolved silos entirely. Smaller companies (1,000 to 2,499 employees) also reported silos more often.

Figure 4. Which of the following best describes how your company organizes operations, budget, and personnel around IT infrastructure and cloud infrastructure?

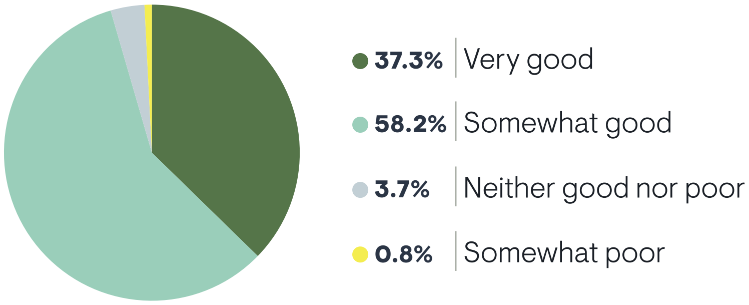


Sample Size = 354

Collaboration Between Cloud and Network Teams

EMA believes that good collaboration between network and cloud teams will ensure consistent and effective design, implementation, and management of hybrid, multi-cloud networks. **Figure 5** reveals that only 37% of research participants believe this collaboration is fully effective. Notably, 69% of organizations that consider their hybrid, multi-cloud networks to be completely successful reported very good collaboration between these groups, versus only 27% of partially successful and 14% of failing organizations. This collaboration tended to be stronger in smaller companies and in North America. Enthusiasm about this collaboration was higher among directors, vice presidents, and CIOs/CTOs. Technical personnel (developers, admins, engineers, and architects) saw more room for improvement.

Figure 5. How effective is the collaboration between the cloud team and the network infrastructure team inside your organization?



Sample Size = 354

EMA found that companies with good cloud and network team collaboration did the following:

- Had a cloud strategy driven by corporate leadership (CEO/COO)
- Established effective network observability across hybrid, multi-cloud networks
- Prioritized centralized management of IP address space, traffic routing, ingress/egress controls, and load balancing across public and private infrastructure
- Leveraged IP address management solutions to enable overlay management of multi-cloud DNS services
- Implemented an effective multi-cloud network source of truth, especially if that source of truth improved network data quality
- Leveraged automation to ensure network resources are decommissioned when no longer needed
- Leveraged multi-cloud to optimize user experience
- Leveraged network observability to optimize cloud costs
- Leveraged DNS to optimize cloud traffic engineering
- Leveraged network packet analysis for cloud infrastructure dependency mapping and compliance assessment and audits

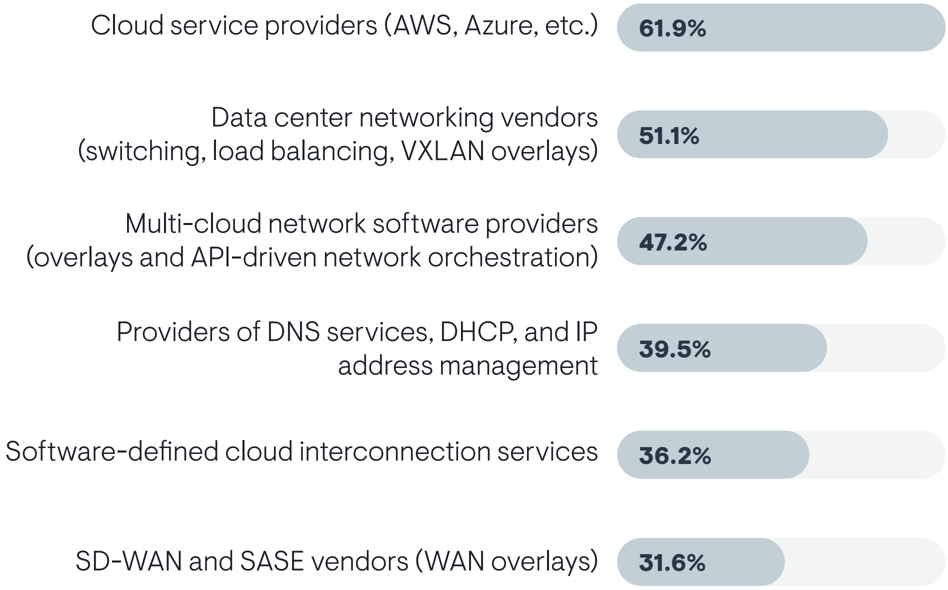
Examining Today’s Cloud Network Infrastructure Choices

Preferred Cloud Network Solution Providers

Figure 6 reveals the kinds of vendors and providers organizations most rely on to provide network technology in their hybrid, multi-cloud networks. Cloud service providers were the most popular source of products, which aligns with long-term trends. Cloud providers offer a broad ecosystem of networking solutions, from routing and load balancing to firewalls and DNS services.

The chief secondary sources of cloud networking solutions are data center networking vendors and multi-cloud network software providers. The former consists of solutions that extend data center networking overlay schemes based on technology, such as VXLAN, into the cloud. This enables hybrid cloud architectures by providing a consistent approach to Layer 2 and 3 networking within data center networks and public cloud VPCs. The latter consists of network software overlay solutions that enable consistent approaches to networking across multiple cloud providers.

Figure 6. Which of the following are essential suppliers of networking solutions in your hybrid and multi-cloud network?

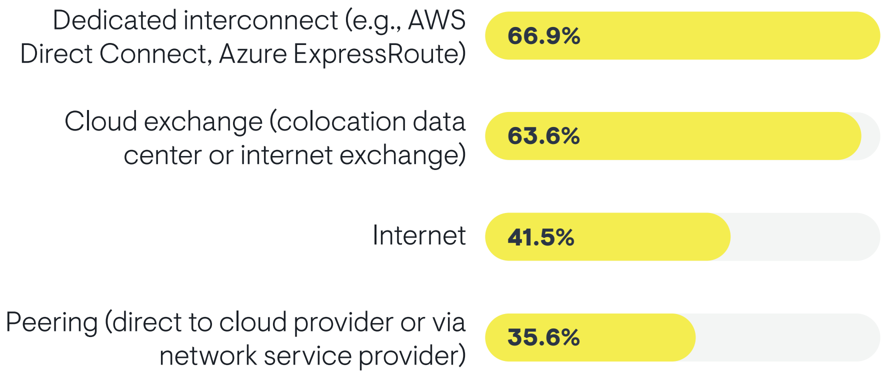


Sample Size = 354

Services Used for Cloud Connectivity

Figure 7 reveals how organizations are connecting their on-premises networks to their public cloud resources. Dedicated interconnects that cloud providers offer are the top choice, but cloud exchanges, like colo providers, are nearly as popular.

Figure 7. Which of the following methods does your organization use to connect its network to cloud providers?



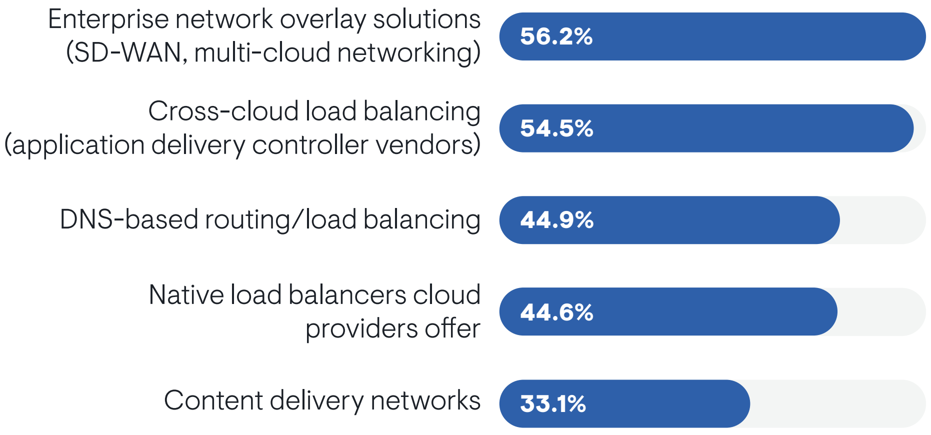
Internet connections, which present performance and security risks, were less popular. Indeed, this connectivity was more popular among organizations that experienced less success with their cloud networks. The least popular approach (peering via network service providers) was more common in the most successful cloud networks.

Sample Size = 354

Steering User Traffic to Optimal Cloud

Figure 8 identifies the tools that organizations use to steer incoming traffic to the optimal cloud providers and cloud regions in their networks. Enterprise network overlay solutions, like SD-WAN and multi-cloud networking, were the most popular. SD-WAN is likely to apply to traffic coming from corporate sites. Cross-cloud load balancing using application delivery controller vendors is also very common. Members of the IT executive suite were more likely than others to report using network overlays and cross-cloud load balancing.

Figure 8. What does your organization use to route traffic to optimal cloud regions and cloud providers across your hybrid, multi-cloud network?



Nearly 49% are using DNS-based routing and load balancing and slightly fewer are using native load balancing services that their cloud providers use. Members of the cloud team were more likely to report DNS-based routing. Content delivery networks (CDNs) were the least popular option, although it was more common among organizations that are the most successful with their cloud networks. Organizations that have three or more cloud providers were also more likely to use CDNs.

Sample Size = 354

Breaking Down Network Operations Silos Across Clouds

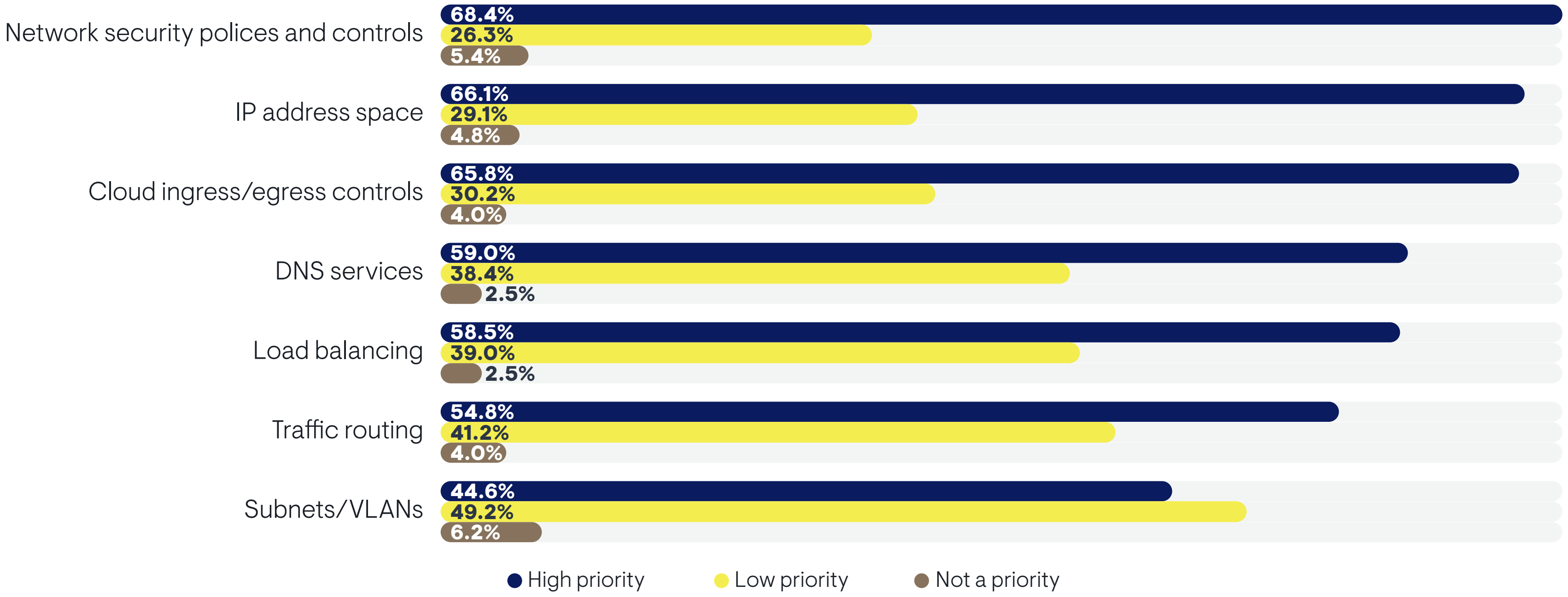
Priorities for Centralizing Network Management

Given the heavy reliance on networking solutions native to individual cloud providers, many organizations will struggle to manage different aspects of networking consistently across a hybrid, multi-cloud architecture. This adds complexity that can lead to inconsistent network performance and increased security risk. EMA asked research respondents whether it is a priority to centralize and unify their management of various aspects of their cloud networks. **Figure 9** shows that there are three tiers of priorities. Organizations are the most motivated to unify management of security policies and controls, IP address space, and cloud ingress/egress controls. Organizations that are the most successful with cloud networking make centralized management of IP address space a priority, as do members of network engineering, cloud, and IT operations teams. Network engineering and cloud teams are also more likely to prioritize centralized management of ingress/egress controls.

DNS services, load balancing, and traffic routing are secondary priorities for centralized network management. Centralized management of traffic routing is also a priority for successful organizations.

Finally, unified management of subnets and VLANs is the lowest priority. Network engineering teams are more likely to prioritize this than other groups.

Figure 9. To what extent is it a priority to manage each of the following in a centralized and unified manner across all your cloud providers, cloud regions, and data centers?



Sample Size = 354

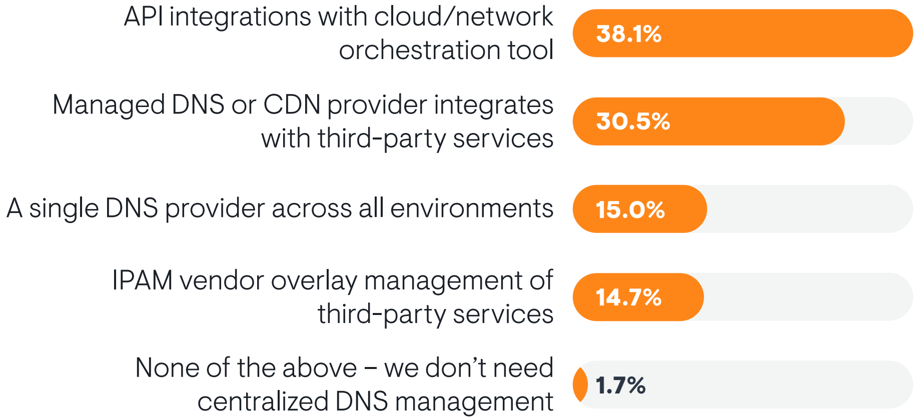
Approaches to Unifying DNS

Centralizing and unifying management of DNS services is particularly tricky. Many enterprises had fractured DNS management even before public cloud use became mainstream due to the availability of a variety of open source and free options. While network engineering teams often try to standardize on a single DNS platform, teams responsible for servers, Active Directory, and application development often adopt their own DNS solutions without the network team's involvement. Native DNS offerings from cloud providers have only made this issue worse.

Figure 10 reveals what organizations prefer to centralize and unify DNS management across their hybrid, multi-cloud networks. API integration with a cloud or network orchestration tool is the most popular choice. This integration was especially prevalent with members of cloud and DevOps teams. Integration with a managed DNS or CDN provider is also popular, especially among the smallest companies represented in EMA's survey.

Overlay management via an enterprise IP address management solution was less popular overall, but members of network engineering and security groups were more likely to prefer this option. IPAM overlays are also more popular when IT leadership and security drive an organization's cloud strategy.

Figure 10. How does your organization want to achieve centralized management of DNS across all cloud providers, cloud regions, and data centers?



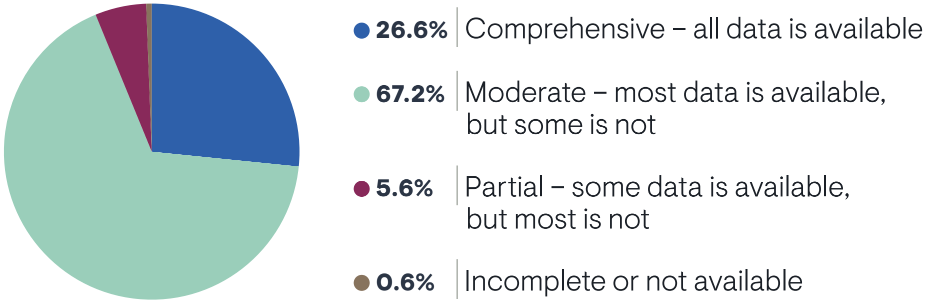
Sample Size = 354

Cloud Network Sources of Truth

The concept of a network source of truth is a frequently debated topic in the world of network engineering. People disagree on what kinds of data such a tool should contain. What is generally agreed upon is that a source of truth is a repository of network data that network teams can use for daily operations, such as network design, change management, and network troubleshooting. EMA asked respondents to describe the extent to which their organizations have a source of truth for their hybrid, multi-cloud networks. **Figure 11** shows that only 27% believe they have a comprehensive cloud network source of truth. Instead, most respondents describe their sources of truth as moderate, containing most but not all data needed for network operations.

Having a comprehensive source of truth is essential to cloud network operations. Organizations that reported a completely successful approach to cloud networking were three times as likely as others to have a comprehensive approach to a network source of truth. Respondents who work in an IT executive suite perceived a more complete source of truth than members of cloud, IT operations, and IT architecture groups.

Figure 11. To what extent do you have a network source of truth across your hybrid and multi-cloud networks in which all network-related data is captured and available to operations teams?

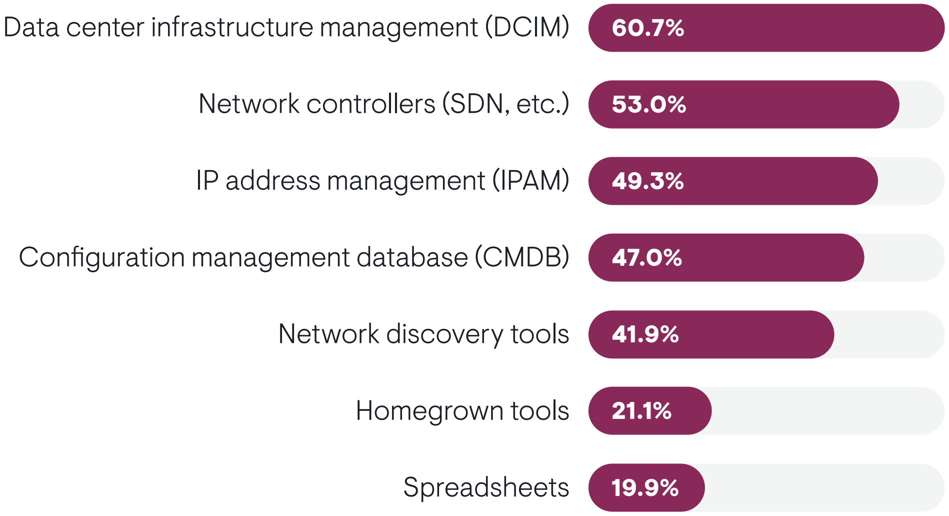


Sample Size = 354

Tools Involved in Sources of Truth

Figure 12 reveals the tools that organizations incorporate into their cloud network sources of truth. Data center infrastructure management (DCIM) tools, network controllers, IP address management (IPAM) tools, and configuration management databases (CMDB) were most common. Network discovery tools were also popular. It's important to note that there is often overlap with these tools. For instance, DCIM, network controllers, and IPAM often have network discovery engines. Also, an emerging set of network source of truth specialists combine DCIM and IPAM into a single platform.

Figure 12. Which of the following tools are involved in establishing your hybrid, multi-cloud network source of truth?



Homegrown tools were less popular, but successful organizations were more likely to use them. They were also more popular with organizations that use four or more cloud providers.

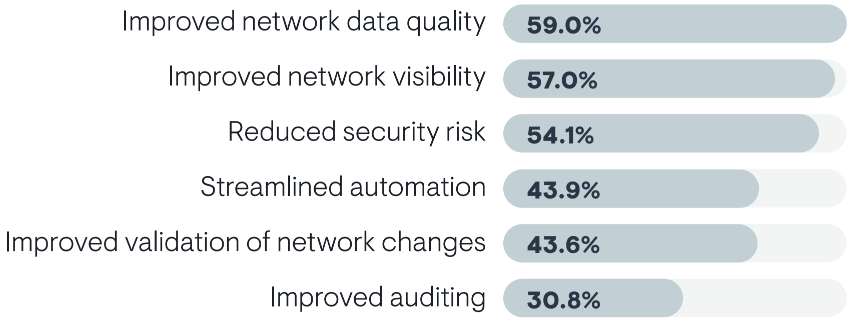
Sample Size = 354

Benefits of a Source of Truth

Figure 13 reveals how organizations benefit from a cloud network source of truth. There are three primary opportunities. EMA's observations of the industry have traditionally found that network engineers think of a source of truth as an enabler of network automation. The data in this research shows that a source of truth is about much more than that. It's about:

1. Improved network data quality
2. Improved network visibility
3. Reduced security risk

Figure 13. What benefits is your organization expecting or experiencing with its hybrid, multi-cloud network source of truth?



Truly, the first two benefits will lead to the third. With better data quality and improved visibility, IT organizations have the tools needed to identify vulnerabilities in their cloud networks.

Among the secondary benefits, IT executives especially perceived an opportunity with streamlined automation, a subject most often associated with the concept of a network source of truth. While improved auditing was the least frequent opportunity, members of cloud and DevOps teams made it one of their top selections.

Sample Size = 354

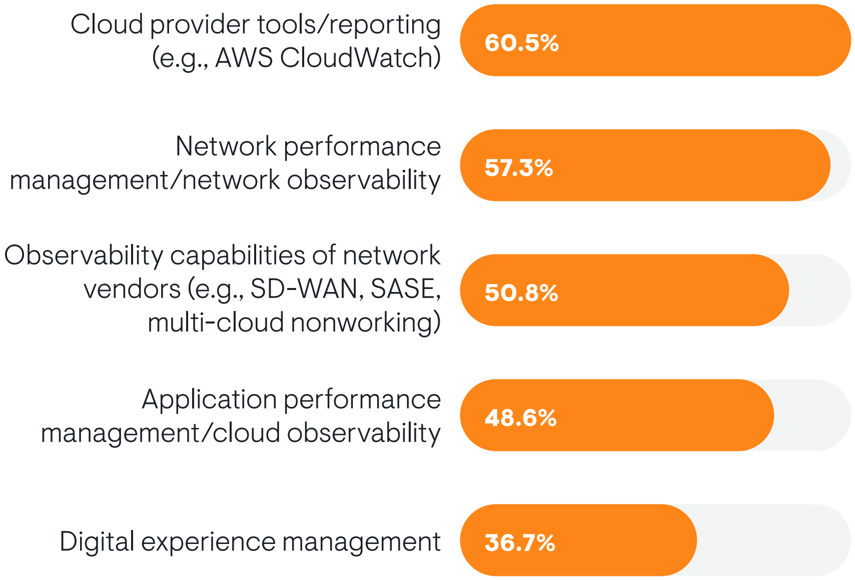
Cloud Network Observability

Solutions Used

Figure 14 reveals the tools that organizations use to understand and manage cloud network performance. Respondents primarily use tools and reports their cloud provider supplies and the network performance management or network observability tools their IT organization uses. Executives and upper management (CIOs, VPs, directors) were more likely to perceive the use of cloud provider tools than team managers and technical staff.

Secondarily, they rely on the observability capabilities of their networking vendors and application performance management solutions. Digital experience management solutions increase in importance with more cloud providers in use. For instance, only 29% of companies with two providers use it, versus 44% of those that use three and 52% of those that use four or more.

Figure 14. What kinds of tools does your organization use to monitor, troubleshoot, and optimize your cloud networks?



Sample Size = 354

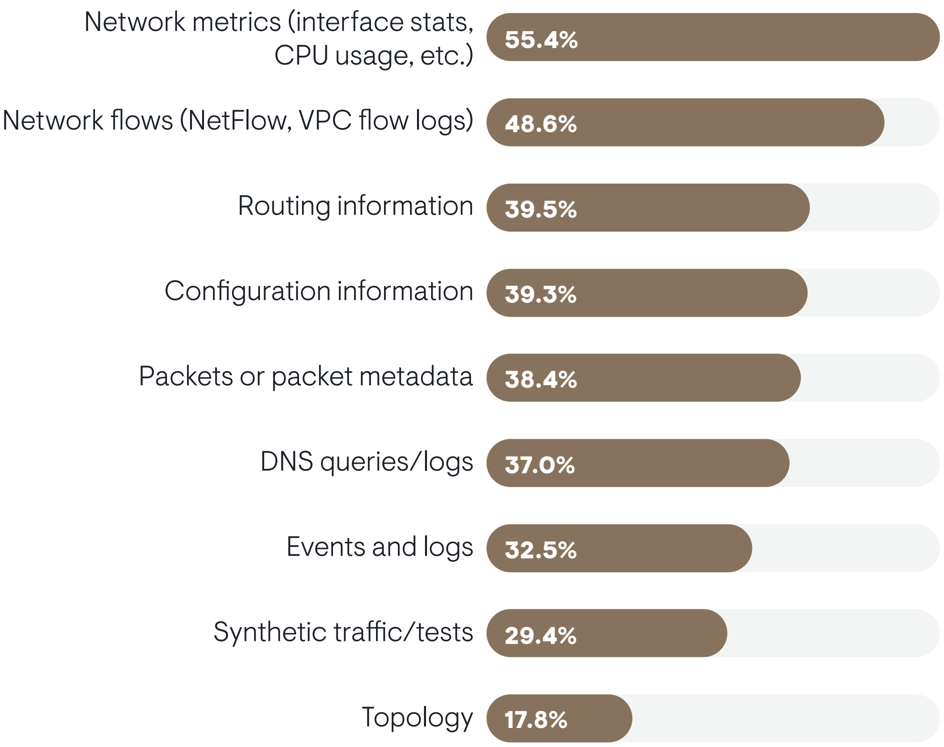
Critical Data

Figure 15 identifies the data that is most critical to cloud network observability. The top responses are classic examples of network monitoring data, network metrics, and network flows. On-premises, these would be SNMP MIBs and traps and network flow formats, like NetFlow and IP-FIX. In the cloud, observability solutions must be able to collect VPC logs and cloud provider metrics via APIS. Many organizations want their tools to analyze and present this data in an end-to-end context, in which they can compare what they're seeing with traditional network telemetry in their on-premises networks with the telemetry collected from the cloud.

There are many secondarily critical sources of cloud network observability data, from routing and configuration information to traffic data (packets and packet metadata) and DNS queries and logs.

The network engineering team was especially likely to select packet data (59%) and configuration information (52%). Respondents who work in the IT executive suite had a more expansive view of what data is critical. They were more likely to select routing information, metrics, flow data, and DNS data.

Figure 15. Which of the following types of network data are critical to monitoring, troubleshooting, and optimizing your cloud networks?

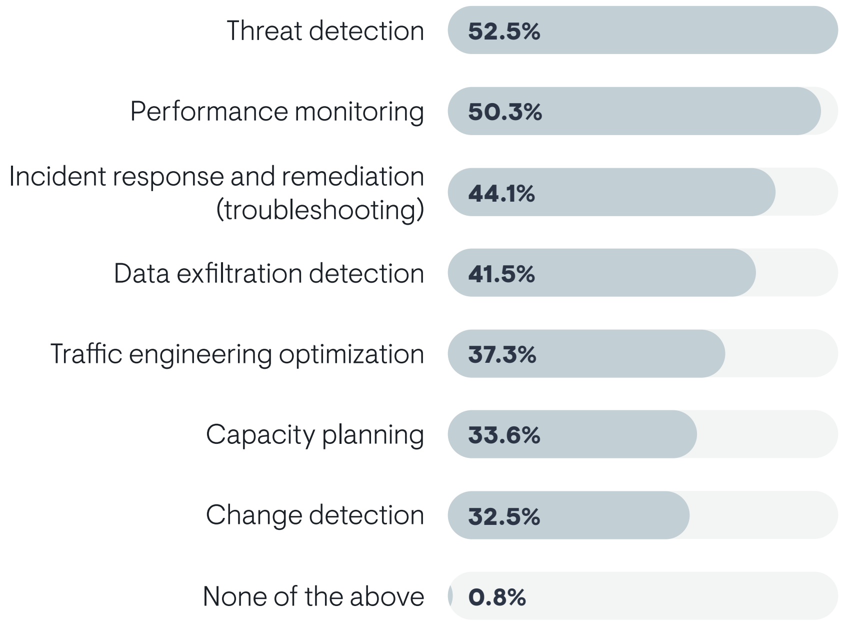


Sample Size = 354

Spotlight on DNS Observability

Figure 16 examines how organizations use DNS data for cloud network observability. Threat detection and performance monitoring are the major priorities. Many also leverage analysis of this data for troubleshooting and data exfiltration detection. Technical personnel were much more likely than upper management to select data exfiltration detection, as were respondents who work for organizations that use a larger number of cloud providers.

Figure 16. Which of the following use cases for DNS traffic analysis are useful for management of your hybrid, multi-cloud network?

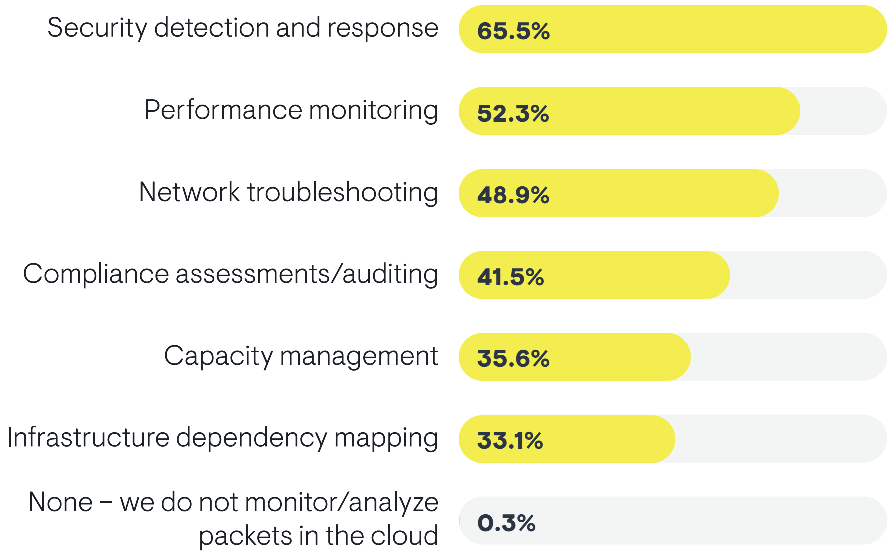


Sample Size = 354

Spotlight on Traffic (Packet Data) Observability

Figure 17 reveals how organizations want to use packet data for hybrid, multi-cloud network observability. Security detection and response is the major use case, and it was especially important to larger companies. A majority also apply it to performance monitoring, and nearly half use it for network troubleshooting.

Figure 17. What are your organization's most important use cases for monitoring and analyzing cloud network traffic (packet data)?

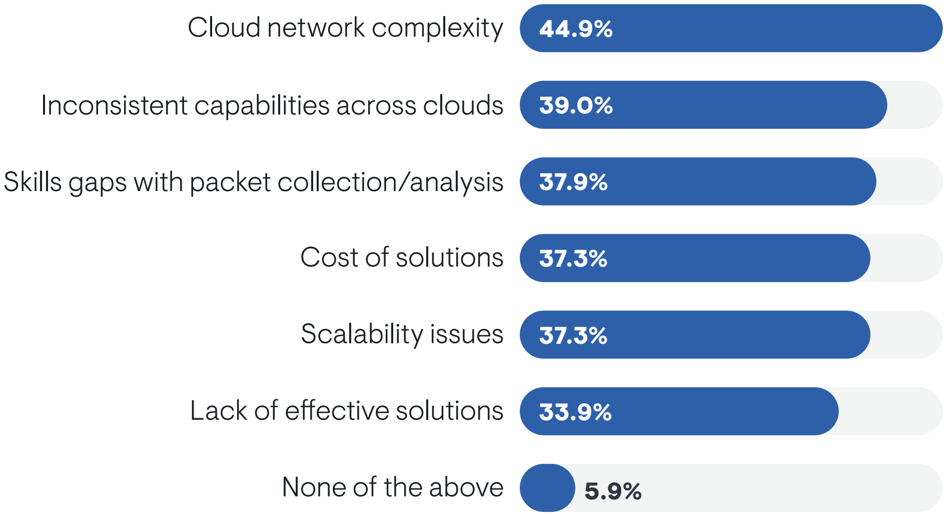


Compliance, capacity management, and dependency mapping are tertiary use cases. However, organizations that are the most successful with their cloud networks were more likely to select compliance and dependency mapping, suggesting best practices.

Sample Size = 354

Figure 18 reveals the challenges that organizations encounter with monitoring packet data across their hybrid, multi-cloud networks. Network complexity is the biggest issue. Among other things, this can manifest as difficulty with tapping networks properly to ensure that all relevant data is collected.

Figure 18. What are your organization's biggest challenges to monitoring network traffic (packets) across your hybrid and multi-cloud environments?



Sample Size = 354

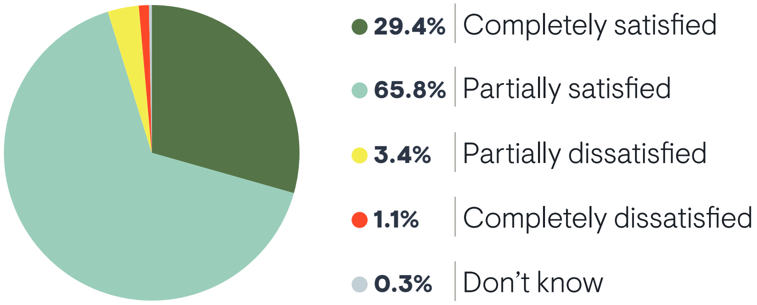
Secondarily, many organizations also struggle with inconsistent packet monitoring capabilities across clouds, skills gaps, cost, and scalability. Cost and complexity were selected less often by very large companies (10,000 or more employees).

Although selected least often, a lack of effective solutions for packet monitoring was cited most often by organizations that consider their cloud networks to be failing. This issue was also cited more often by cloud and IT operations teams.

Cloud Network Observability Satisfaction

Only 29% of research participants were completely satisfied with their cloud network observability capabilities, suggesting that IT and cloud teams and their vendors have work to do (see **Figure 19**). Satisfaction with cloud network observability correlated directly with overall success with cloud networking. Respondents from the IT executive suite and the security team were most satisfied. Executives have less granular requirements for observability, while security teams usually have more budget available for such tools. Meanwhile, members of the cloud, network engineering, and IT/network operations teams were all less satisfied.

Figure 19. How satisfied are you with the tools you currently use to observe/monitor networks across your hybrid, multi-cloud environment?



Notably, dissatisfied respondents were more likely to select performance issues as a top technical challenge to their overall cloud networking strategy. Also, dissatisfied respondents were less likely to say that their cloud networks are contributing to revenue or customer growth.

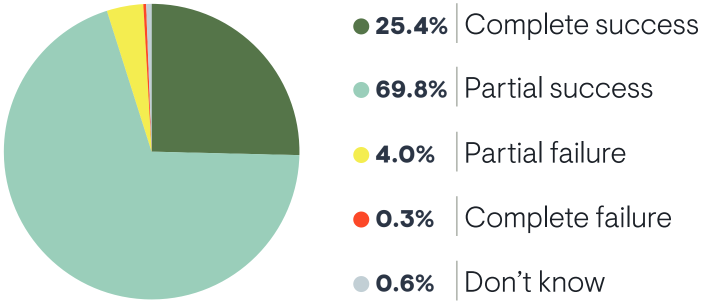
Sample Size = 354

Hybrid, Multi-Cloud Networking Outcomes

Overall Success with Hybrid, Multi-Cloud Networks

Figure 20 reveals that only 25% of respondents believe their organizations are completely successful with their efforts to build and manage their hybrid, multi-cloud networks. On the bright side, only 4% consider themselves failures. Infrastructure subject matter experts (admins, engineers, architects) were more pessimistic than middle and upper management, which should serve as a warning sign to business leaders. More specifically, members of cloud and DevOps teams were the most pessimistic. Large enterprises (10,000 or more employees) are experiencing the most success.

Figure 20. How would you rate your organization's success with building and operating networks across hybrid and multi-cloud architecture?



Sample Size = 354

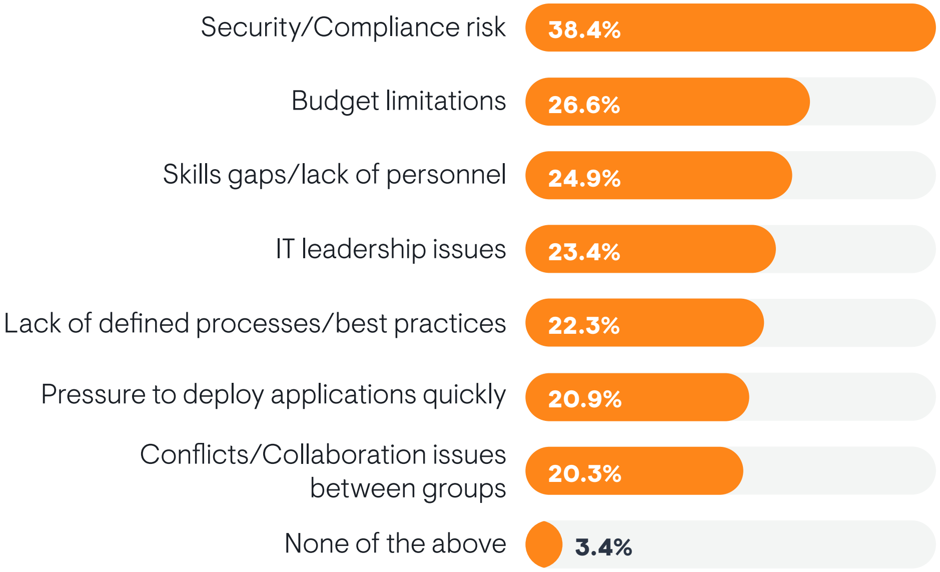
Challenges

General Business Issues

Figure 21 identifies the business issues that cause the most pain with today's hybrid, multi-cloud networks. Security and compliance risk is clearly haunting research participants more than anything else. Security personnel were especially likely to select this issue. Security and compliance risk is also a bigger issue for organizations that have less effective collaboration between network and cloud teams.

Budget, skills gaps, and IT leaderships issues are chief secondary challenges. Skills gaps and a lack of defined processes tend to be bigger issues for companies with fewer than 10,000 employees.

Figure 21. Which of the following business issues are causing your organization the most pain with its multi-cloud network?



Sample Size = 354

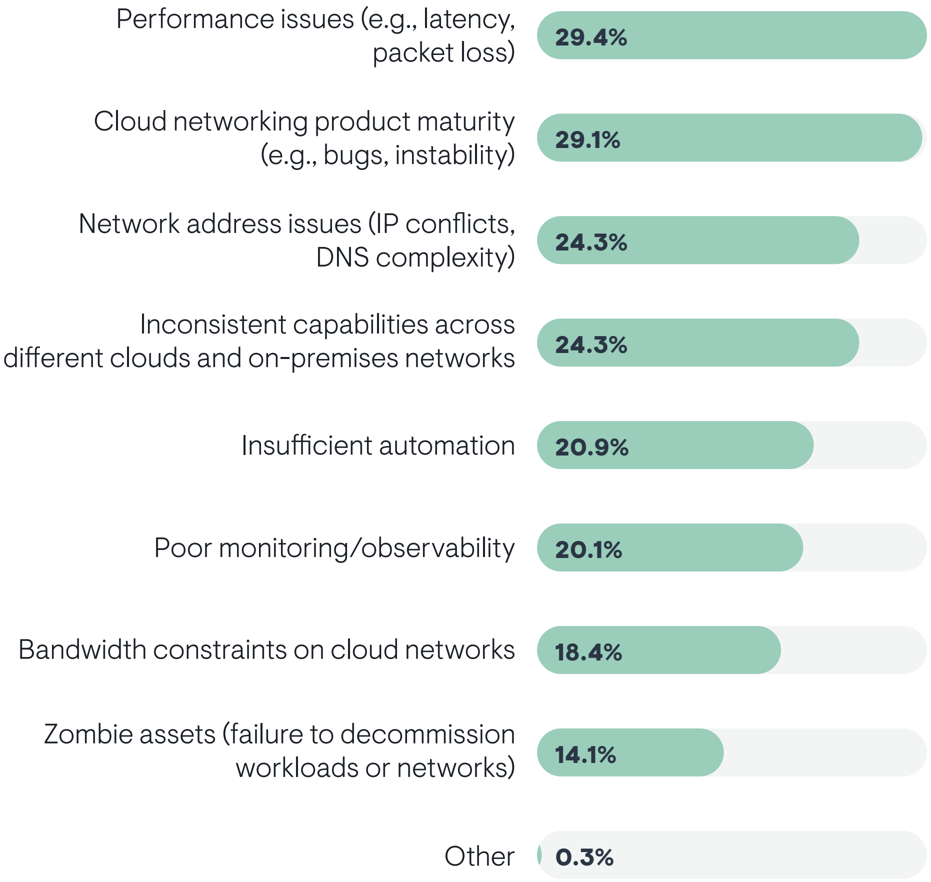
General Technical Issues

Figure 22 explores the general technical issues that are causing the most pain with hybrid, multi-cloud networks. There are four major problems:

1. Performance issues. This is a tradeoff when a company moves applications off-premises and into the cloud. Those resources are now further away from the business, which adds latency. The quality of cloud connectivity can also vary, which adds more performance uncertainty. Performance issues are more common in organizations that suffer from less effective collaboration between network and cloud teams.
2. Networking product maturity. Network vendors (both startups and incumbents) often introduce new product updates for existing products to address cloud use cases. Also, cloud providers are constantly adding new networking products. Naturally, early releases of products often have quality issues, leading to bugs and platform instability.
3. Network address issues. IP address space and DNS infrastructure are often fractured by multi-cloud, with organizations using multiple solutions. This adds to conflicts as operations teams struggle to manage things holistically. This issue is especially prominent among organizations that use four or more cloud providers.
4. Inconsistent capabilities across different clouds and on-premises networks. Certain networking capabilities are simply not available in every cloud, and those capabilities will vary in quality and depth from cloud to cloud. For instance, networking vendors who are adapting their products for public cloud use will usually start by supporting their technology in one or two cloud providers based on customer demand. A multi-cloud organization may find their preferred load balancing vendor has a mature offering in AWS, but not in Google or Digital Ocean.

Poor monitoring is a minor issue overall, but members of the security team complained more often about it. Zombie assets are the least common technical challenge. However, it was cited more frequently by respondents whose cloud strategy is driven by a line of business group.

Figure 22. Which of the following technical issues are causing your organization the most pain with its multi-cloud network?



Sample Size = 354

Shortcomings of Networking Solutions Native to Cloud Providers

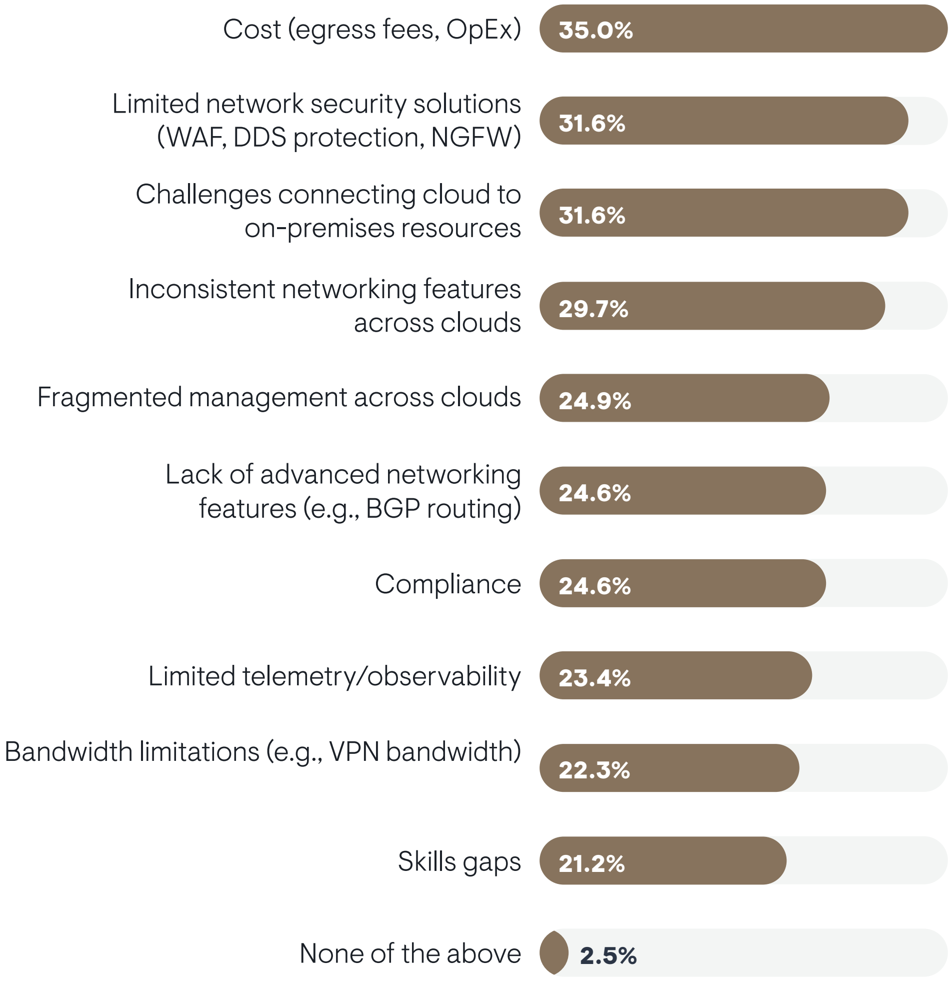
Given the prominence of cloud providers' networking solutions in today's hybrid, multi-cloud networks, EMA asked respondents to identify any challenges they encounter with these tools. **Figure 23** reveals that nearly 97% have at least one complaint. The average respondent selected about three issues. The top four problems are:

1. Cost. Egress fees come up often in EMA's conversations with network engineering leaders. Billing for various networking features can also get costly, given that many providers offer pay-as-you-go rather than subscription fees. Without careful planning and monitoring, these daily or hourly fees can pile up quickly. Less successful cloud networks correlated with cost challenges, suggesting it separates best-in-class companies from laggards.
2. Limited network security solutions. This is often an issue of maturity. Most cloud providers offer a broad suite of network security products, but they frequently lack the advanced features of traditional network security vendors.
3. Issues with direct connections to on-premises networks. Provisioning and managing direct connections to the cloud can get complex, especially in a multi-cloud environment where network teams have to learn how to work with multiple proprietary connectivity technologies.
4. Inconsistent networking features across clouds. This issue can refer to so many hidden problems in a multi-cloud network. For instance, each cloud provider has a different scheme for how to name features (VPC versus vNet), how to interact with features, and whether features are even available. For instance, traffic mirroring services for packet-based network observability is not available from every provider.

Fragmented management across clouds is a secondary issue, but it's more common when the network and cloud teams struggle to collaborate. Cost also plagues poor collaboration.

Another secondary issue is the lack of advanced networking features. Members of network engineering teams were especially concerned with this issue and the cost issue.

Figure 23. Which of the following do you find challenging when using the native network functions and network services that your cloud providers offer?



Sample Size = 354

IP Address Management Challenges

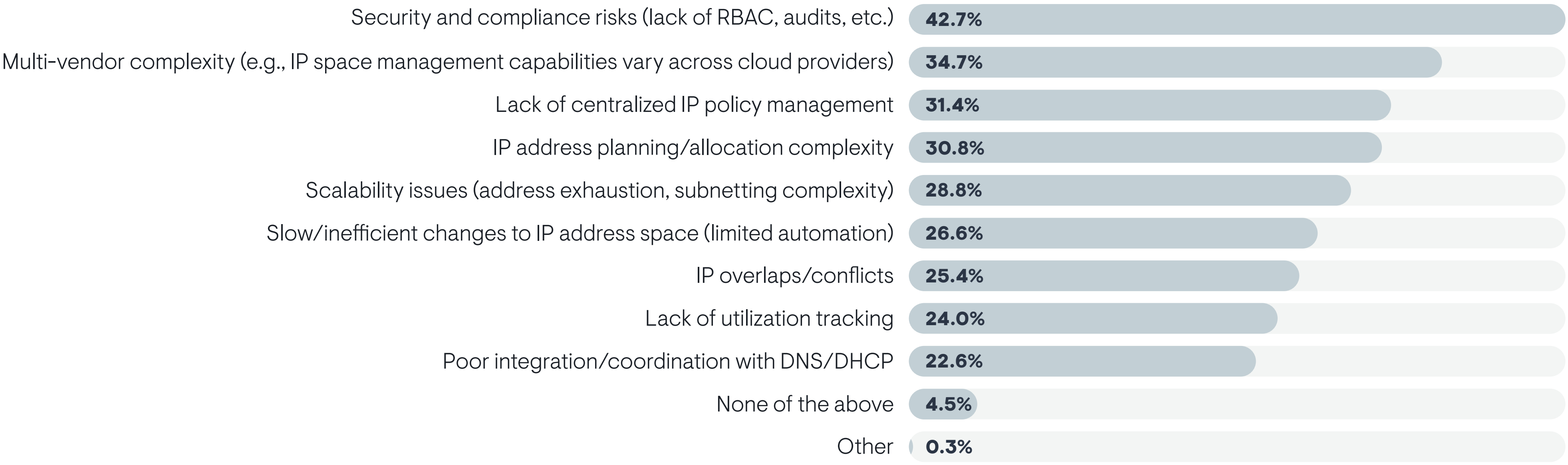
In a hybrid, multi-cloud network, it is critical to have a consistent approach to IP address management across data centers and multiple cloud providers. This isn't easy, given that IPAM is often siloed across clouds. **Figure 24** identifies the top challenges that organizations are encountering with hybrid, multi-cloud IPAM. The top two issues are:

1. Security and compliance risks. They lack enterprise-grade capabilities, like role-based access control and single sign-on. They also lack the ability to log and audit changes to IP address space. Organizations that are less successful with their cloud networks experience this issue more often.
2. Multi-vendor complexity. This is a common refrain in multi-cloud networks. Each cloud provider offers native IPAM capabilities, but they vary from cloud to cloud. It's difficult to have consistency across all environments.

The other top secondary challenges are the lack of centralized IP policy management and IP address planning/allocation complexity. Planning and allocation complexity are bigger issues when the finance department leads cloud strategy. Financial leadership also leads to multi-vendor complexity.

Slow and inefficient changes to IP address space is a minor issue, but software developers considered it one of their biggest headaches.

Figure 24. What do you find most painful about managing IP address space across your hybrid, multi-cloud network?



Sample Size = 354

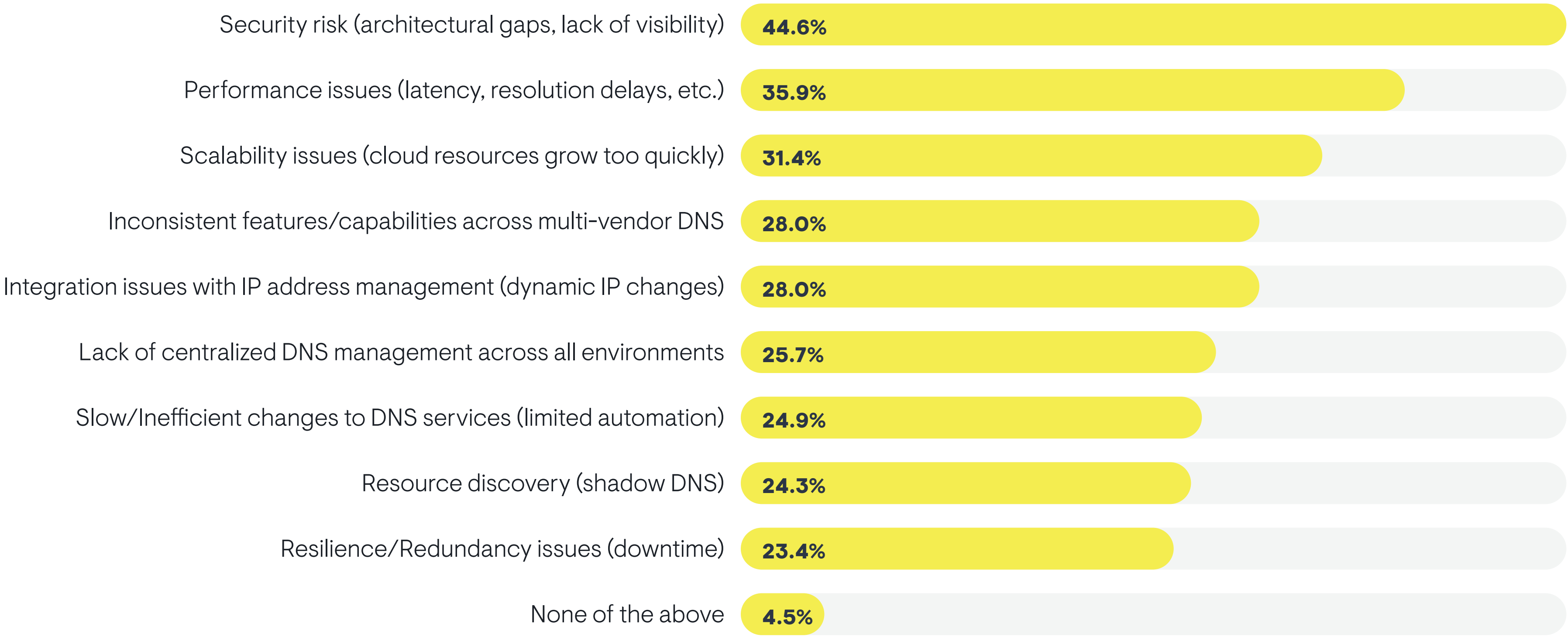
DNS Management Challenges

Figure 25 reveals how DNS is challenging these organizations. Security risk is the biggest source of pain, as companies struggle to detect gaps in DNS security architecture and also struggle to monitor DNS for malicious activity.

The top secondary challenges are issues with DNS performance and DNS scalability. Performance issues are more frequent among organizations that let lines of business drive cloud strategy. Scalability issues come up more often in companies with 1,000 to fewer than 10,000 employees.

A lack of centralized DNS management is a minor issue overall, but organizations that are less successful with cloud networking are more likely to experience this issue. This problem is also prominent in organizations in which network and cloud teams are struggling to collaborate.

Figure 25. What do you find most painful about managing DNS services across your hybrid, multi-cloud network?



Sample Size = 354

Conclusion

This research should serve as a network infrastructure and operations roadmap for enterprises that have not yet embraced hybrid or multi-cloud architecture. These are insights from your peers on what went right and what went wrong when they built networks for these hybrid and multi-cloud environments.

It's clear that many organizations still rely on the networking solutions that their cloud providers natively offer, such as routing, load balancing, DNS, network security, automation, and observability. This is not tenable. Most companies have identified unification and centralization of network management as high priorities. Cloud native networking offerings are siloed and add management complexity. As organizations mature their approach to hybrid, multi-cloud networking, they will need to adopt solutions that work across clouds and private networks. To accomplish this, IT leadership must set the agenda and ensure that technical teams are working together to create a consistent, resilient, and secure network across all clouds and data centers.

EMA has a few recommendations for hybrid, multi-cloud networking strategy based on our analysis of the research data.

- Take power away from line of business leaders and finance leaders. Cloud strategies driven by these groups correlated with failure. Cloud strategy must be led by the IT organization.
- Push your network and cloud teams to collaborate effectively.
- Unify and centralize management of networking across clouds and data centers, especially for IP address space, DNS, and traffic routing across clouds.
- Establish a comprehensive cloud network source of truth that can pull and push data to multiple systems of record.
- Update your network observability toolset to address hybrid, multi-cloud networking use cases
- Establish packet-level observability in your cloud networks, particularly for:
  - Security detection and response
  - Compliance assessments and audits
  - Infrastructure dependency mapping

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2025 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com** 4523.040825