EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Prepared for:

aviatrix

Multi-Cloud Networking: Connecting and Securing the Future

January 2023 EMA Research Report Summary

By **Shamus McGillicuddy**, Vice President of Research and **Robert Gates**, Senior Analyst
Network Infrastructure and Operations

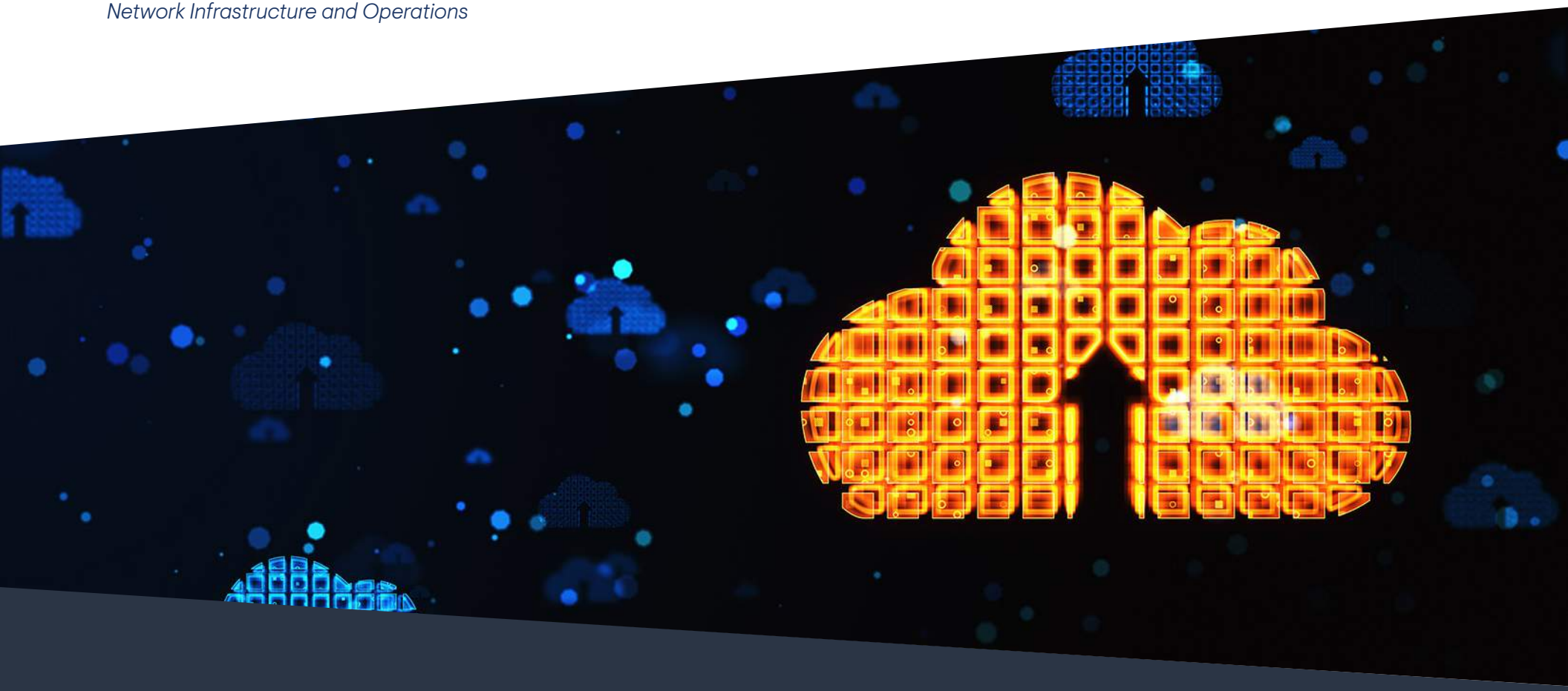


Table of Contents

Executive Summary

Today's enterprises are increasingly using multiple cloud providers for a variety of reasons. This market research from Enterprise Management Associates explores how enterprises are addressing the networking requirements of their multi-cloud architectures. It explores pain points, technology requirements, and operational strategies for multi-cloud networks.

Introduction: Multi-Cloud is a Networking Problem

This document is a summary of new research that explores how enterprises address the networking requirements of their multi-cloud architectures. More and more, enterprises are using multiple cloud providers to host applications and data. Previously in its "Network Management Megatrends" research, published in April 2022, Enterprise Management Associates (EMA) found that 72% of enterprises were using multiple cloud providers. By 2024, nearly 88% will be multi-cloud.

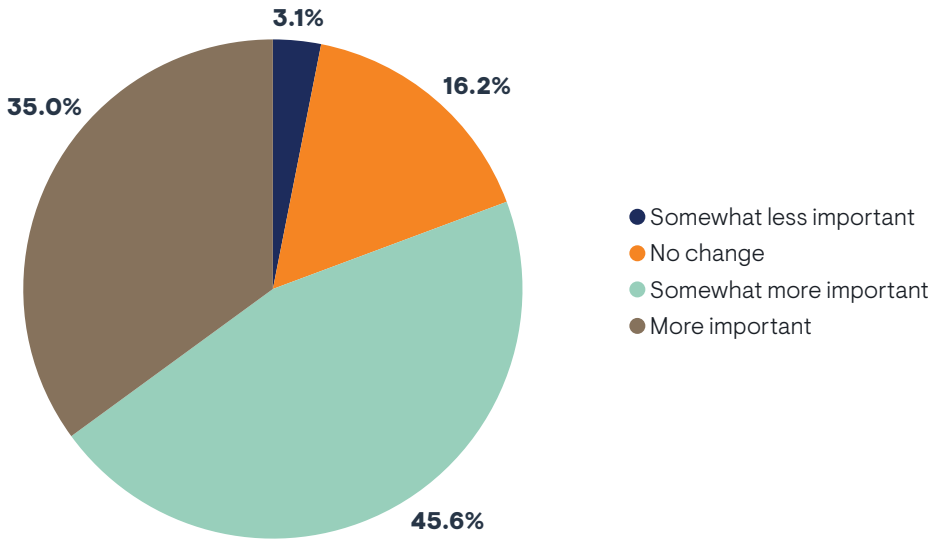
That same research also found that public cloud and multi-cloud adoption was the number-one driver of enterprise network operations strategies. As enterprises increase their use of multiple cloud providers, network teams need better visibility and control. EMA predicts that multi-cloud network architecture will be a major focus of enterprise network organizations over the next few years.

81% of respondents told EMA that networking has become more important to their cloud strategies over the last couple years.

In this new multi-cloud networking research, based on a survey of 351 IT stakeholders who work in multi-cloud enterprises, 81% of respondents told EMA that networking has become more important to their cloud strategies over the last couple years. **Figure 1** reveals that only 3% believe that networking has decreased in importance to cloud strategies. IT executives and middle management are especially likely to believe networking has become critical to the cloud. This perception is also strongest within cybersecurity and IT program management groups. Network engineering and network operations teams are less convinced.

If networking has become more important to cloud strategies in the multi-cloud era, what role should the network play, and how can network infrastructure and operations teams contribute to success? This research seeks to answer those questions.

FIGURE 1. HAS NETWORKING BECOME MORE IMPORTANT OR LESS IMPORTANT TO YOUR CLOUD STRATEGY OVER THE LAST TWO YEARS?



Sample Size = 351

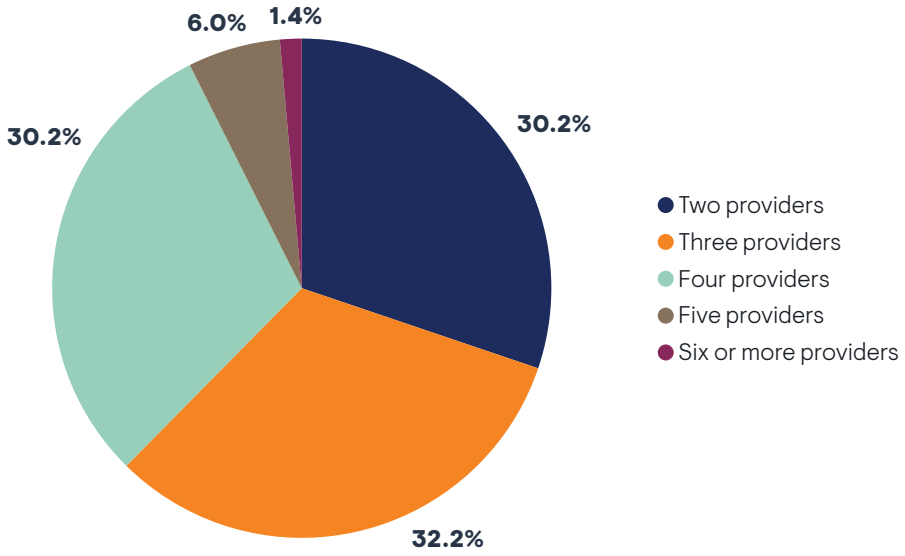
Research Methodology

Methodology

This research summary is based on a survey of 351 enterprise IT stakeholders and one-on-one interviews with a handful of IT professionals. Both the surveys and the interviews investigated how IT organizations are addressing multi-cloud networking. To ensure participants had relevant experience, EMA asked two screening questions.

First, EMA asked survey participants to identify how many cloud providers their companies use. Only respondents who selected two or more providers were allowed to complete the survey. **Figure 2** reveals that most of the enterprises represented in this research are using two, three, or four providers. Larger companies (both by total employees and by revenue) tended to use a larger number of cloud providers.

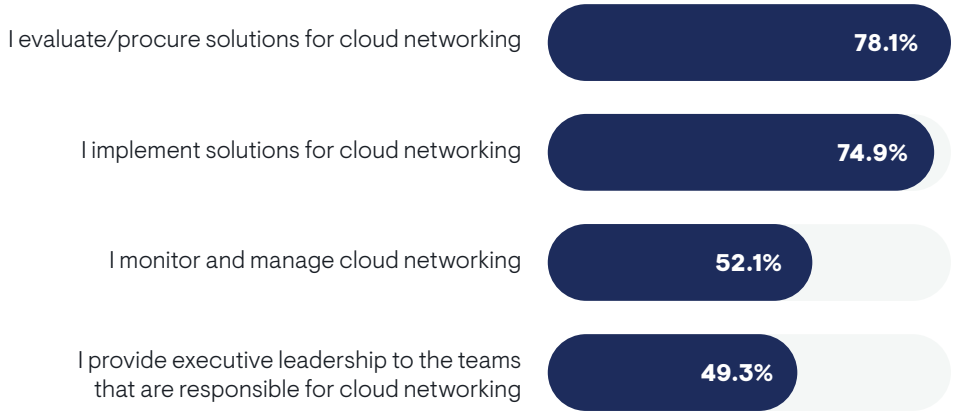
FIGURE 2. NUMBER OF IAAS CLOUD PROVIDERS USED



Sample Size = 351

Second, EMA asked respondents to describe what responsibility they had for their organizations' cloud networking strategies. **Figure 3** reveals that a majority of them evaluated, selected, purchased, and implemented cloud networking. A little more than half monitored and managed cloud networks. Less than half provided executive leadership to teams responsible for cloud networks.

FIGURE 3. RESPONDENTS' RESPONSIBILITIES FOR THEIR ORGANIZATIONS' PUBLIC CLOUD NETWORKING SOLUTIONS



Sample Size = 351, Valid Cases = 351, Total Mentions = 893

Demographics

Figure 4 provides a demographic overview of the 351 survey participants. They work in a range of midsized to very large enterprises across North America and Europe.

The chart reveals a variety of job titles, ranging from technical personnel to middle management to IT executives, with strong representation from network engineering and architecture groups, cloud architecture and operations groups, and cybersecurity.

FIGURE 4. DEMOGRAPHIC OVERVIEW

Top job titles

- **31%** Network engineer
- **14%** CIO/CTO
- **14%** IT director
- **9%** Network architect
- **9%** IT manager/supervisor

Top IT groups/teams

- **39%** Network engineering/architecture
- **21%** CIO's office
- **15%** Cloud architecture/operations
- **11%** IT security/cybersecurity

Company size (employees)

- **27%** 500 to 2,499
- **40%** 2,500 to 9,999
- **33%** 10,000 or more

Top industries

- **21%** Manufacturing
- **14%** Banking/Finance/Insurance
- **13%** Government
- **13%** Healthcare
- **11%** Retail
- **7%** Energy/Utilities
- **5%** Education

Annual sales revenue

- **27%** $5 billion+
- **47%** $1 billion to <$5 billion
- **12%** $500 million to <$1 billion
- **12%** $50 million to <$500 million
- **2%** Unknown or no revenue

Region

- **64%** North America
- **36%** Europe

Key Findings

- Only 35% of enterprises believe they have been fully successful with their multi-cloud networking strategies
- The biggest sources of multi-cloud networking pain are:
  - Security risk
  - Collaboration challenges
  - Complexity across cloud providers
  - Performance issues
  - Cloud networking product maturity
- Native networking features and services that cloud providers offer are the most popular technologies that enterprises use today for multi-cloud networking, but only 24% of enterprises are fully satisfied with these solutions.
  - In particular, they say these cloud provider solutions have bandwidth issues, present cost management problems, lack advanced network security capabilities, and present provider lock-in risk.
- 93% of organizations want to implement an end-to-end multi-cloud networking solution, and 15% report that they already have one in production.
  - Network security, VPN controls, and transit routing are the most important functionalities in such a solution
  - Network complexity and budget issues are the biggest barriers to adoption of end-to-end solutions
- Only 24% of organizations are fully satisfied with their multi-cloud network monitoring and observability capabilities.
- 68% of organizations have acquired new tools to address multi-cloud network monitoring.
  - Organizations are particularly interested in tools that can report on cloud-to-data center connections and cloud-to-cloud connections
- Only 24% of organizations believe that their network teams have enough influence over a multi-cloud networking strategy.

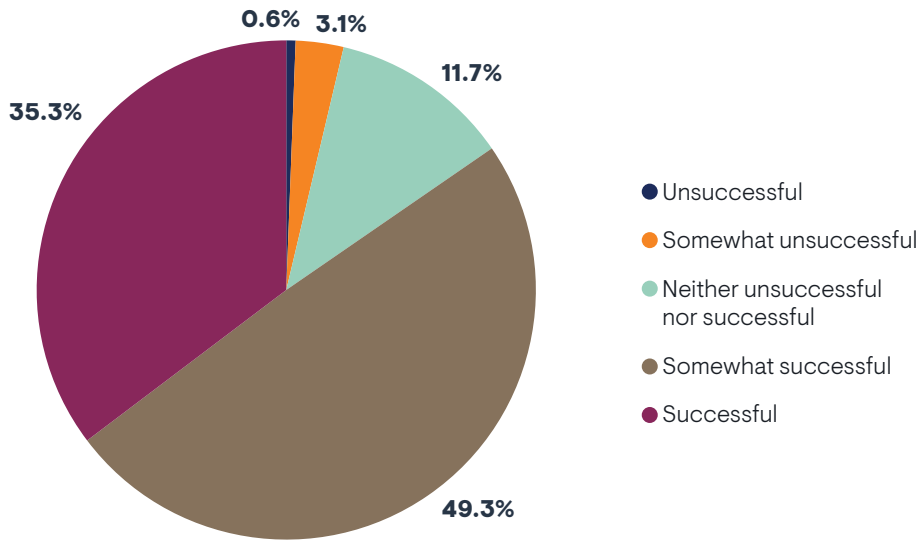
Multi-Cloud Networking Success and Pain Points

Overall Success with Multi-Cloud Networking

Figure 5 reveals how successful research participants have been with their multi-cloud networking strategies so far. While very few admit to being unsuccessful, only 35% believe they have been completely successful. Instead, 49% believe they have been somewhat successful, meaning they see room for improvement. Members of the network engineering team and the CIO suite were more enthusiastic than people who work in cloud operations, cybersecurity, and IT financial/asset management.

The people responsible for selecting and implementing multi-cloud networking solutions were more optimistic about success than people who were responsible for monitoring and managing such solutions, which suggests that change management and observability are undermining success.

FIGURE 5. PERCEPTIONS OF OVERALL SUCCESS WITH MULTI-CLOUD NETWORKS



Sample Size = 351

Issues with Cloud Providers' Native Networking Solutions

Most enterprises begin their cloud networking journey by relying on the native networking solutions offered by their chosen cloud providers, whether those are native VPC subnetting tools, load balancing functions, or routing services. These solutions are typically proprietary to a specific cloud provider, which can add complexity as organizations add additional providers to a network.

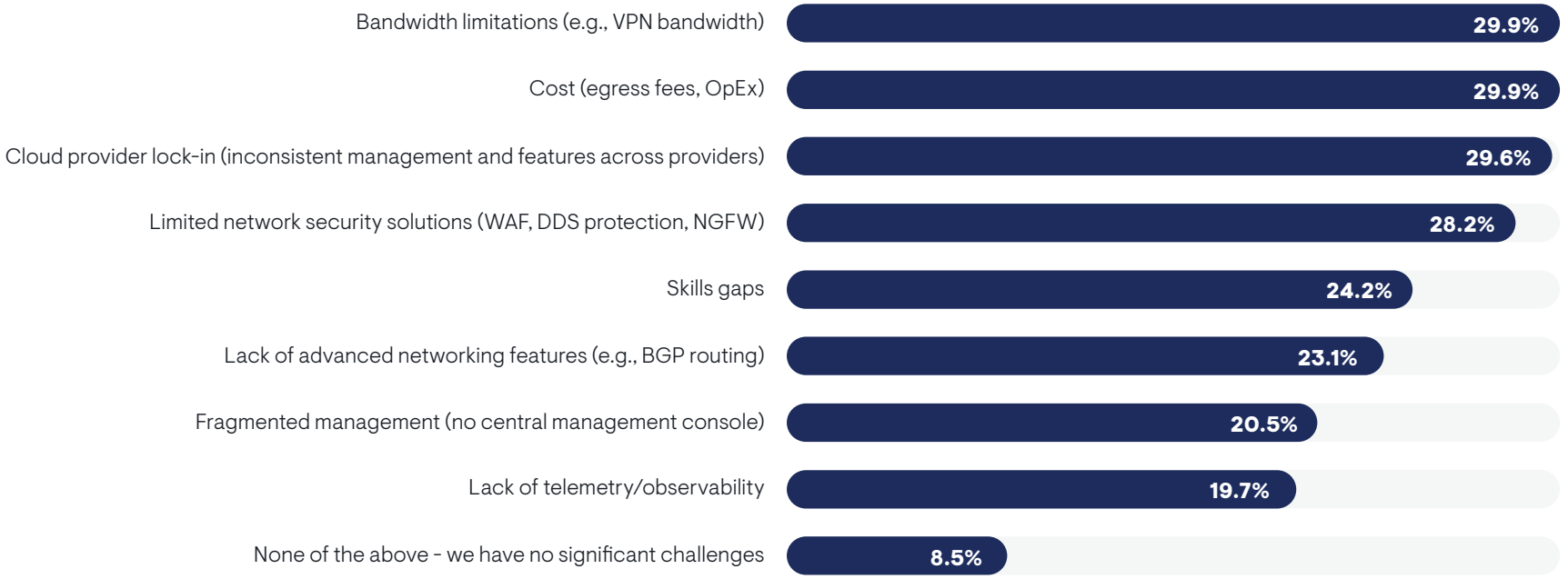
For example, at a $15 billion retailer, a network architect said they rely almost entirely on the native networking capabilities of Azure.

"We do have some firewalls that are Fortinet that are network virtual appliances. But all of the VNet builds, the networking LANs, and IP address is all native Azure stuff," he said. "We don't have any overlay. We've looked at them. We're going to continue looking at them."

Figure 6 explores the issues that organizations have encountered while using the native networking solutions of cloud providers. First, the chart shows that nearly 92% of organizations are dealing with at least one significant pain point.

Bandwidth limitations, cost, cloud provider lock-in, and limited security features are the four main problems with network functions and services native to cloud providers.

FIGURE 6. ISSUES THAT ORGANIZATIONS HAVE ENCOUNTERED WHEN USING THE NATIVE NETWORK FUNCTIONS AND NETWORK SERVICES THAT YOUR CLOUD PROVIDERS OFFER



Sample Size = 351, Valid Cases = 351, Total Mentions = 750

Bandwidth limitations, cost, cloud provider lock-in, and limited security features are the four main problems with network functions and services native to cloud providers. Cybersecurity professionals were less likely to worry about limitations of security solutions than people in the CIO's suite, network engineering, or cloud operations. Cost is less of an issue for organizations as they go from using two cloud providers to three or four, suggesting that they leverage multi-cloud to minimize network-related billing, such as data egress fees.

While a lack of advanced networking features was a minor issue, technical personnel, such as network engineers and architects, found it to be a top problem. It's also a more frequent problem for companies that are using a larger number of cloud providers, which points to inconsistency of advanced features across different providers.

The strengths and weakness vary across clouds and just getting to know the differences can be a challenge, a security operations manager at a $4 billion media company told EMA. "We struggled with understanding all these different offerings and how they could solve problems," he said. "Each cloud vendor is expert on their own domain, but not other cloud domains."

Skills gaps were a minor problem overall, but less successful organizations were more likely to struggle with them, suggesting a potential barrier to success that organizations must plan for by focusing on training and hiring.

Keeping up to speed with technology is the most challenging part of multi-cloud networking, according to a network architecture executive at a bank with about $1 billion in annual revenue.

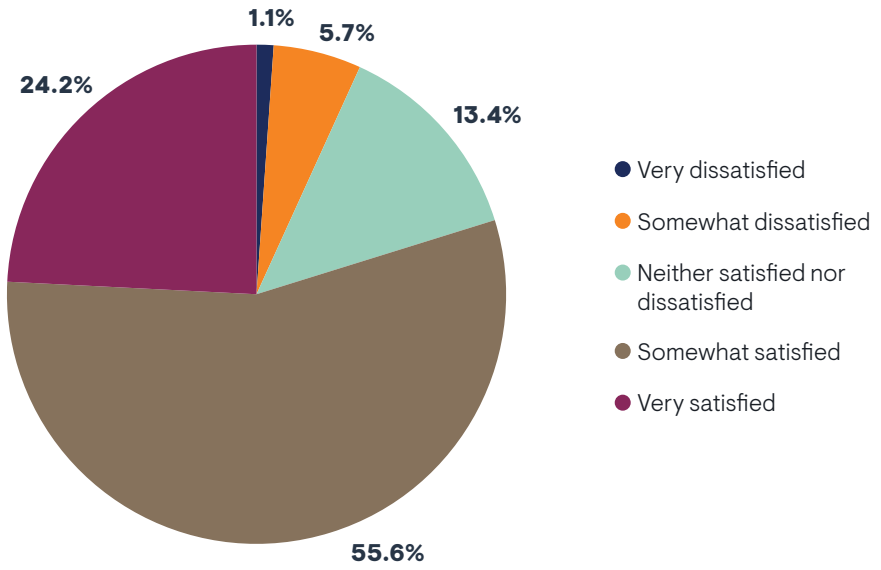
"The way that the cloud has sped up and with software-defined everything, just staying on top of things is a nightmare. Even when you wrap your head around one of the cloud providers, new things come out or they change," he said. "It's a full-time job just to be aware of the various services. I studied Azure for four hours a day for a year and that was just for one cloud provider—most people can't do that, so you have fewer people understanding multi-cloud enough."

Figure 7 reveals that only 24% are fully satisfied with the native networking functions that cloud providers offer. Most are somewhat satisfied, making it clear that they would like their cloud providers to improve their network offerings. Satisfaction with these functions and services was highest among enterprises that are the most successful with multi-cloud networking overall. Members of the CIO's suite and cybersecurity were more satisfied than members of network engineering and cloud operations.

Only 24% are fully satisfied with the native networking functions that cloud providers offer.

Larger companies were more satisfied than smaller companies, and North Americans were more satisfied than Europeans.

FIGURE 7. SATISFACTION WITH THE NATIVE NETWORK FUNCTIONS AND SERVICES THAT CLOUD PROVIDERS OFFER



Sample Size = 351

Multi-Cloud Networking Pain Points

Business Issues

Figure 8 reveals the business issues that are causing organizations the most pain with multi-cloud networking. Security risk is the top source of trouble, although the CIO suite is more likely to worry about it than the network engineering team. It's also a bigger issue in Europe than it is in North America.

A security operations manager at a $4 billion media company said he spends much of his time trying to manage security risk in his multi-cloud network. "We want to know if there are any [forgotten] site-to-site tunnels or remote tunnels in place that are doing nothing. We want to discover that," he said.

All other business issues are secondary to security risk. The CIO's suite is relatively unconcerned about a lack of processes or best practices to follow with multi-cloud networking, but network engineering and cloud operations teams are twice as likely to believe it's a problem.

IT leadership is a minor issue overall, but it rises as organizations increase the number of cloud providers they work with. North Americans selected it as a problem more often than Europeans. Companies that are more successful with multi-cloud networking were also more likely to struggle with IT leadership. IT executives should remain engaged with multi-cloud networking strategy, even if early successes suggest they can take their eyes off the ball.

FIGURE 8. BUSINESS ISSUES THAT ARE CAUSING ORGANIZATIONS THE MOST PAIN IN THEIR MULTI-CLOUD NETWORKS

Sample Size = 351, Valid Cases = 351, Total Mentions = 641

Technical Issues

Technical pain points are highlighted in **Figure 9**. Multi-vendor is a source of trouble. Complexity from using multiple cloud networking vendors is the biggest technical issue for enterprises. However, IT executives perceived this as a more common issue than technical personnel and middle management, suggesting that it's overblown.

Performance issues, cloud networking product maturity, and inconsistent multi-cloud provider support are the secondary technical pain points. The CIO's suite was less likely to worry about multi-cloud support, but the cloud operations team listed it as a top problem. Organizations that use a larger number of cloud providers cited product maturity more frequently, suggesting that as a multi-cloud network expands beyond the big three of AWS, Azure, and Google, cloud networking products struggle to keep up.

A network architecture executive for a $1 billion bank said multi-cloud makes it difficult to adopt a standard network architecture. "That's a big deficiency in the cloud—strongly lacking higher-level reference architecture. I think it's improving a bit over last year."

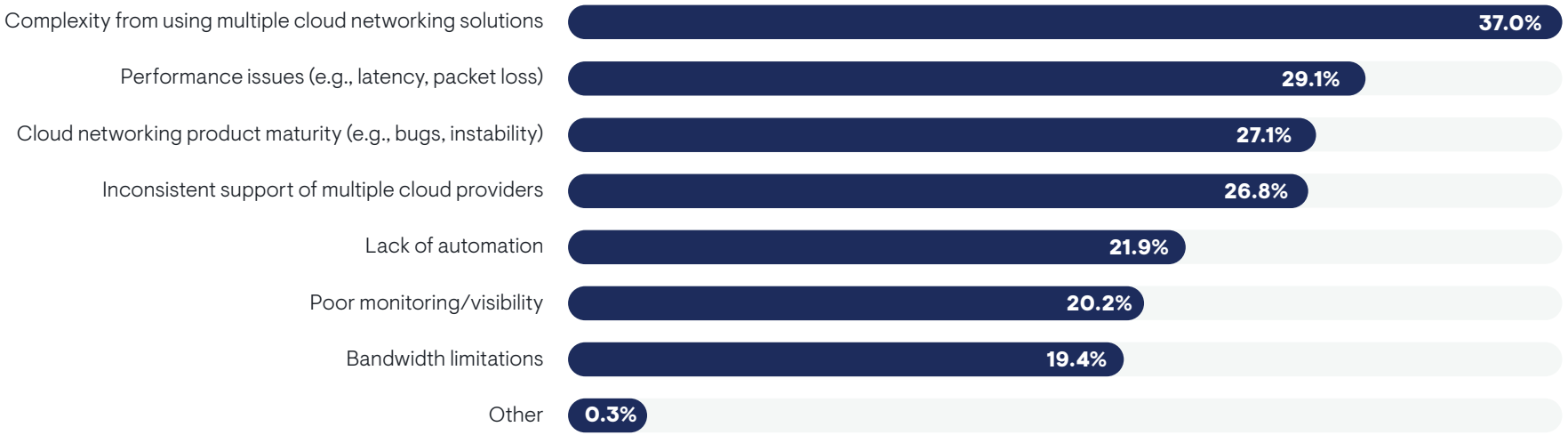
A lack of uniform architecture could make it difficult to move into new clouds, he said.

Poor monitoring was a minor issue, but less successful organizations were more likely to struggle with it, suggesting an early pitfall that can undermine multi-cloud networking strategy.

Complexity from using multiple cloud networking vendors is the biggest technical issue for enterprises.

Lack of automation, another minor issue, was a more common complaint for the network engineering team and the network operations team, but the CIO's suite was relatively unaware of the problem.

FIGURE 9. TECHNICAL ISSUES CAUSING ORGANIZATIONS THE MOST PAIN WITH MULTI-CLOUD NETWORKS



Sample Size = 351, Valid Cases = 351, Total Mentions = 638

Multi-Cloud Networking Technologies

This section is the heart of our research. It explores the technology that enterprises are using and considering for use in their multi-cloud networks. Today, many enterprises are still leaning on the native networking solutions their cloud providers offer. However, EMA believes a change is coming.

General Multi-Cloud Networking Requirements

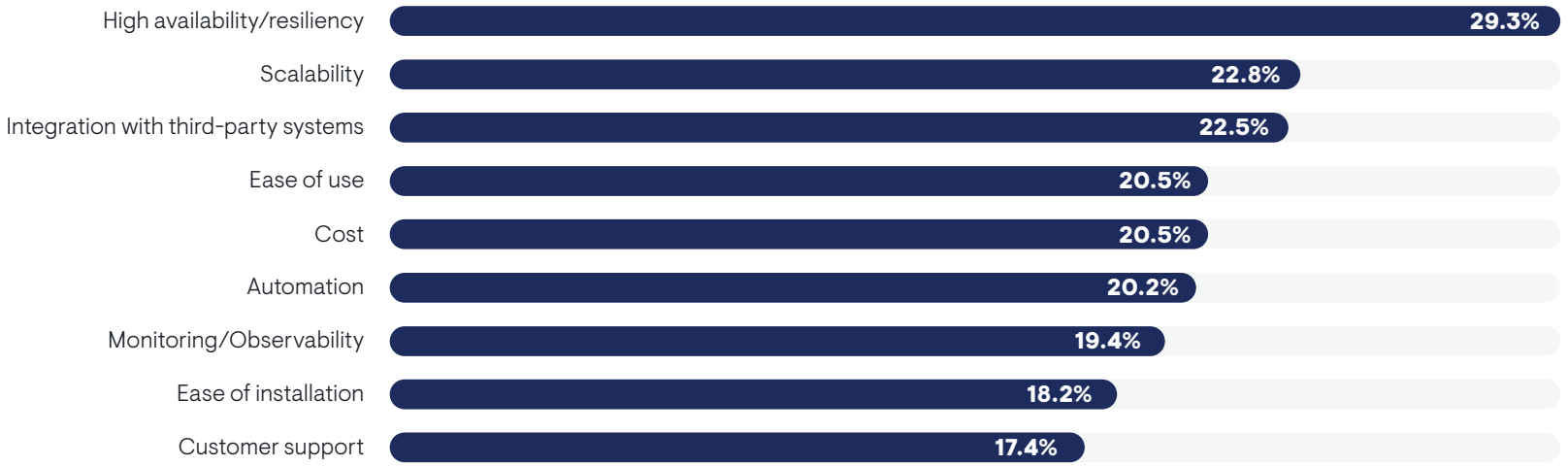
Figure 10 reveals the top requirements that enterprises have when selecting a cloud networking solution. Resiliency is the top priority, and top-performing organizations favored this.

Scalability and integration with third-party systems are secondary in importance. Integrations were a more prominent requirement for successful organizations, suggesting a potential best practice strategy. Scalability was a focus for less successful organizations, suggesting a misplaced priority. Scalability was also a higher priority for the CIO's suite, but less important to the network engineering team. Integrations were important to the cloud operations team, but not to cybersecurity. Finally, integrations were more important to organizations that use five or more cloud providers, suggesting that they can mitigate some of the complexity of using a large number of providers.

Ease of use, cost, and automation were tertiary priorities. Cost was a higher priority to smaller companies and to companies that operate in only two cloud providers, rather than three or more. Again, ease of use and cost were more popular among less successful organizations, suggesting that other requirements would be more valuable. For instance, monitoring and observability were one of the lowest-priority requirements, but they were very popular among more successful organizations. They were also a high priority for the network engineering team, but not for the CIO's suite.

Ease of installation and customer support are the lowest priorities. Ease of installation appears to grow in importance as organizations expand from using two or three providers to four. EMA observed a similar pattern for monitoring and observability requirements.

FIGURE 10. SOLUTION CHARACTERISTICS MOST IMPORTANT TO ORGANIZATIONS WHEN SELECTING A CLOUD NETWORKING SOLUTION



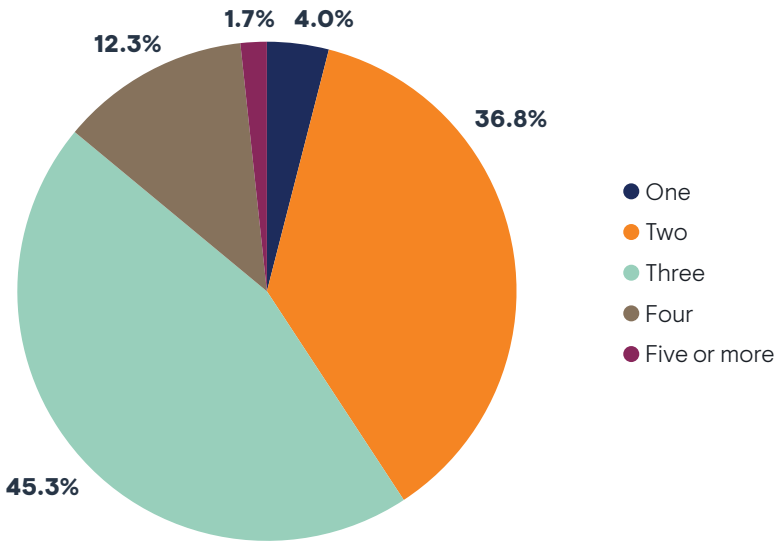
Sample Size = 351, Valid Cases = 351, Total Mentions = 670

Multi-Cloud Networks are Multi-Vendor

Only 4% of companies claim to have one vendor serving all their cloud networking needs.

Multi-cloud networking is a multi-vendor world. **Figure 11** reveals that only 4% of companies claim to have one vendor serving all their cloud networking needs. Most have two or three. More successful organizations tended to have a higher number of vendors. EMA also found that the number of cloud networking vendors increased as organizations added new cloud providers.

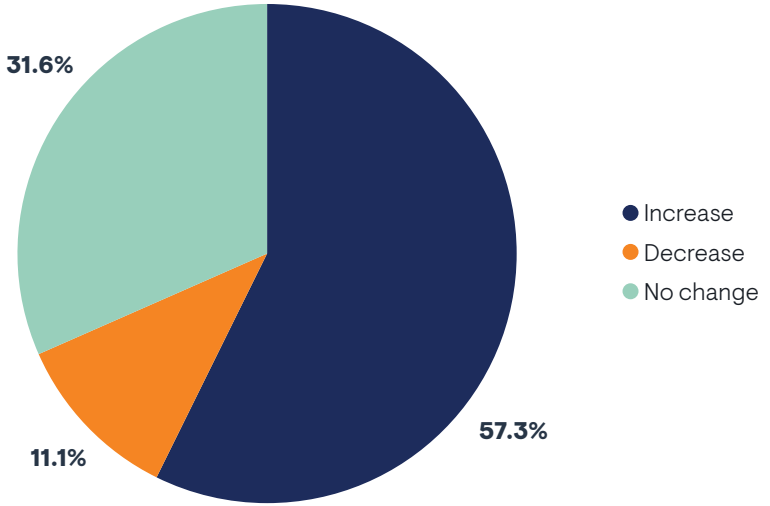
FIGURE 11. NUMBER OF CLOUD NETWORKING VENDORS ENTERPRISES CURRENTLY USE, INCLUDING NETWORKING SOLUTIONS CLOUD PROVIDERS OFFER



Most enterprises expect the number of vendors they use to increase even more, as **Figure 12** reveals.

Although teams using a multi-vendor approach to multi-cloud networking have the most success, EMA found that successful organizations are more likely to anticipate a consolidation of cloud networking vendors in the future. As the cloud networking market matures these successful teams will consolidate, perhaps by replacing native offerings from cloud providers with end-to-end multi-cloud networking solutions. Network engineering teams are more likely than the CIO's suite, cloud operations, and cybersecurity to anticipate vendor consolidation and the least likely to expect an increase in vendors.

FIGURE 12. EXPECTED CHANGE IN NUMBER OF CLOUD NETWORKING VENDORS ENTERPRISES EXPECT TO USE OVER THE NEXT TWO YEARS



Sample Size = 351

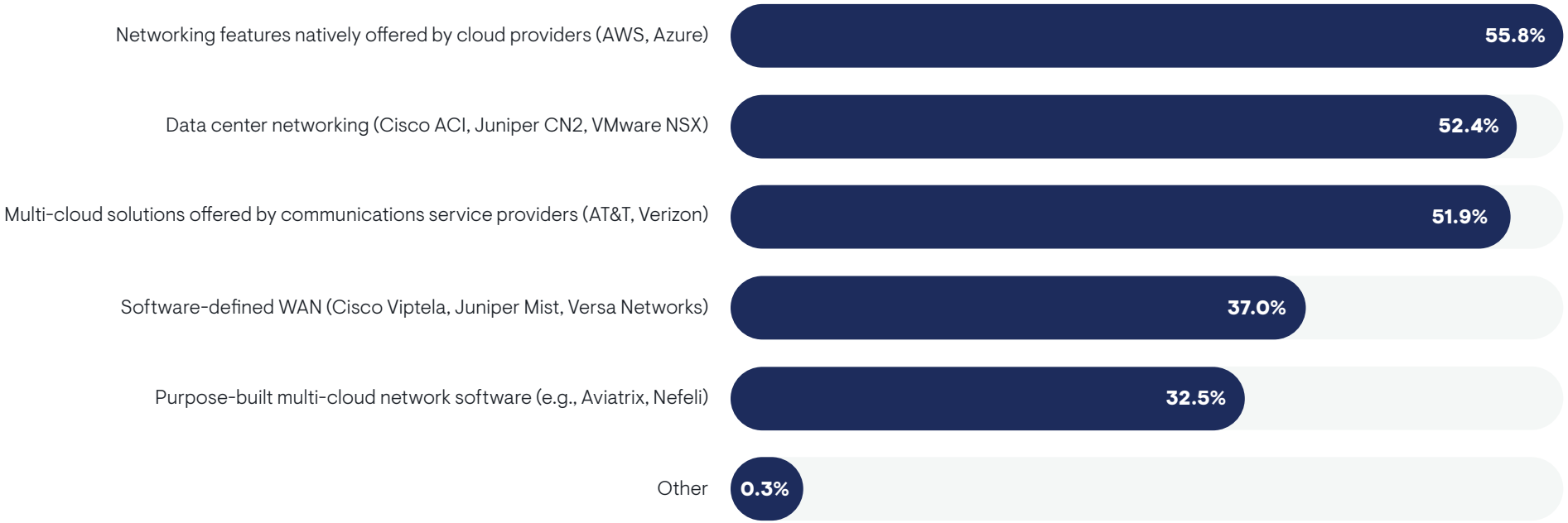
Essential Networking Technologies

Figure 13 reveals the types of cloud networking solutions that vendors are using. Networking solutions native to cloud provides are the most popular. Smaller companies were more likely to use them. AWS and Azure customers were more likely than Google Cloud Platform customers to rely on cloud providers' network solutions.

Data center networking solutions (which can be extended into the cloud) and multi-cloud solutions from service providers are the other two popular multi-cloud networking technologies. All three of the top solutions highlighted in Figure 13 were more popular with IT executives than with technical personnel, suggesting that actual implementers and operators of cloud networking solutions are looking elsewhere.

SD-WAN and purpose-built multi-cloud networking products were the lowest priorities with networking strategies. The network operations team was more likely to prioritize SD-WAN.

FIGURE 13. TECHNOLOGIES THAT ARE IMPORTANT PARTS OF RESPONDENTS' OVERALL MULTI-CLOUD NETWORKING STRATEGIES

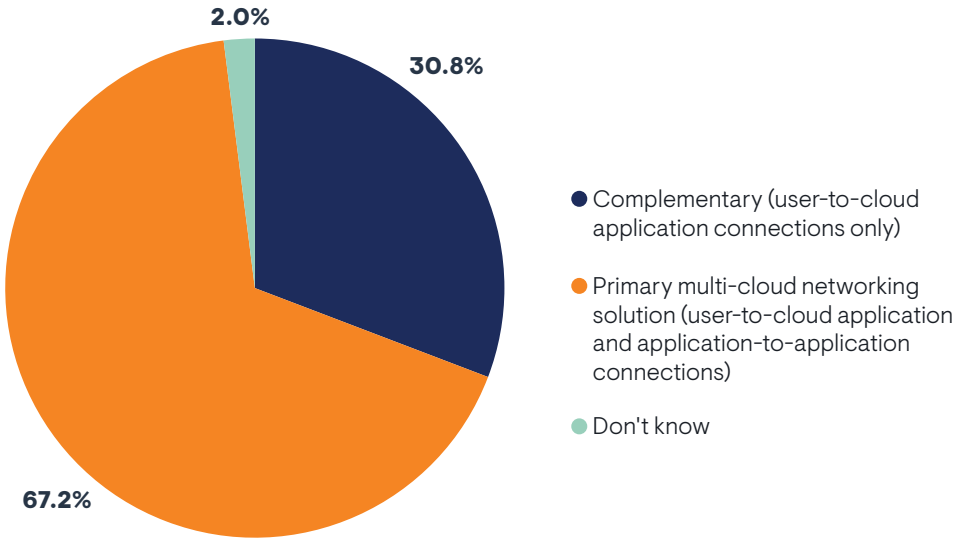


Sample Size = 351, Valid Cases = 351, Total Mentions = 807

SD-WAN has a Future in Multi-Cloud

SD-WAN is not widely deployed as a multi-cloud networking solution. Today, other technologies are much more popular. However, **Figure 14** reveals that two-thirds of respondents believe that SD-WAN should and could play a bigger role as a primary solution.

FIGURE 14. ROLE THAT SOFTWARE-DEFINED WAN (SD-WAN) SHOULD PLAY IN A MULTI-CLOUD NETWORK



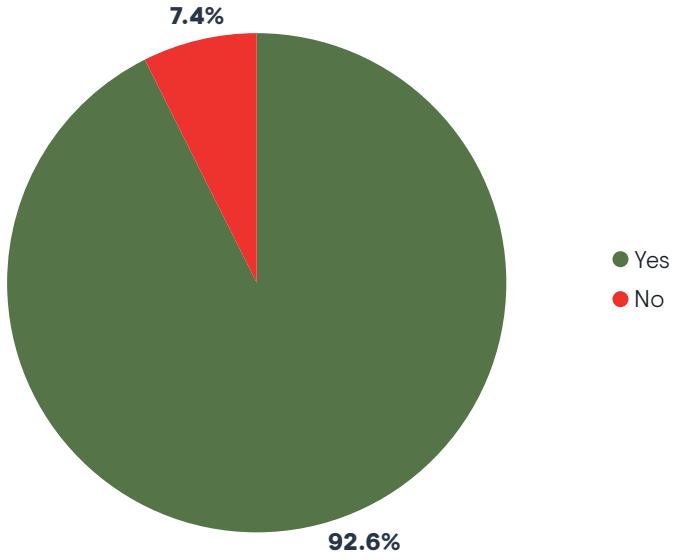
Successful multi-cloud networking strategies correlated strongly with the belief that SD-WAN should be a primary part of their multi-cloud networking solution. Most silos in the IT organization tended to believe in SD-WAN's importance with the exception of the IT architecture group, which views SD-WAN as more of a complementary solution.

Sample Size = 351

End-to-End Multi-Cloud Networking Solutions are the Future

End-to-end multi-cloud networking solutions make up an emerging class of technologies that can provide multiple networking capabilities across the cloud, from routing and security to VPC subnetting. EMA suspects that vendors from multiple parts of the networking industry will converge on this space, including dedicated specialists, SD-WAN vendors, and data center networking vendors. According to **Figure 15**, 93% of organizations are interested in an end-to-end multi-cloud networking solution. Interest is highest among successful organizations. It's also strong in the CIO's suite and the network engineering team, but the security team has less interest.

FIGURE 15. IS YOUR ORGANIZATION INTERESTED IN USING AN END-TO-END MULTI-CLOUD NETWORKING SOLUTION THAT ADDRESSES MANY OR ALL NETWORKING REQUIREMENTS ACROSS MULTIPLE CLOUD PROVIDERS?

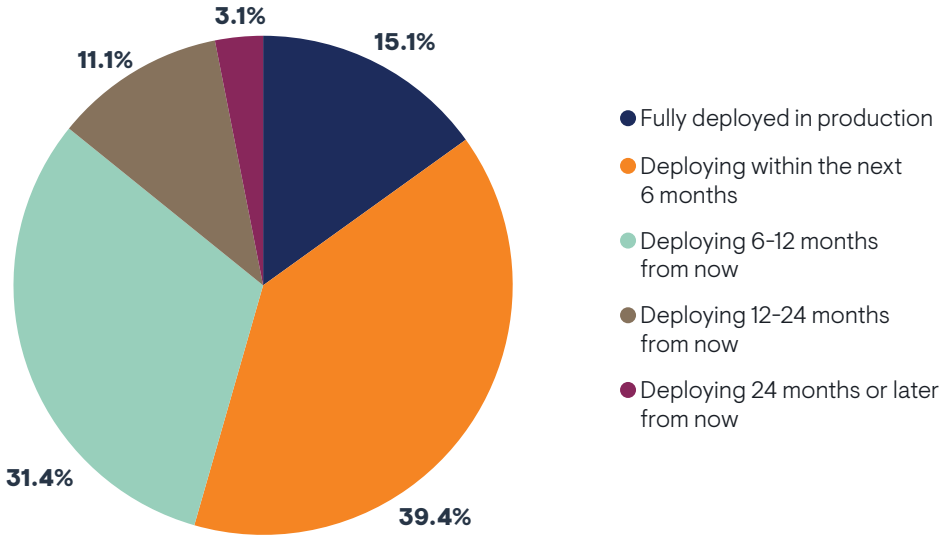


Sample Size = 351

Current Engagement

Figure 16 reveals that 15% of organizations that have interest in end-to-end multi-cloud networking solutions are already in production with such a technology. Another 39% will deploy within six months. Adoption timelines are more advanced among organizations that use a greater number of cloud providers. For instance, organizations that have five or more providers are three times as likely as those with just two providers to be in production with such a technology today.

FIGURE 16. CURRENT ENGAGEMENT WITH END-TO-END MULTI-CLOUD NETWORKING SOLUTIONS



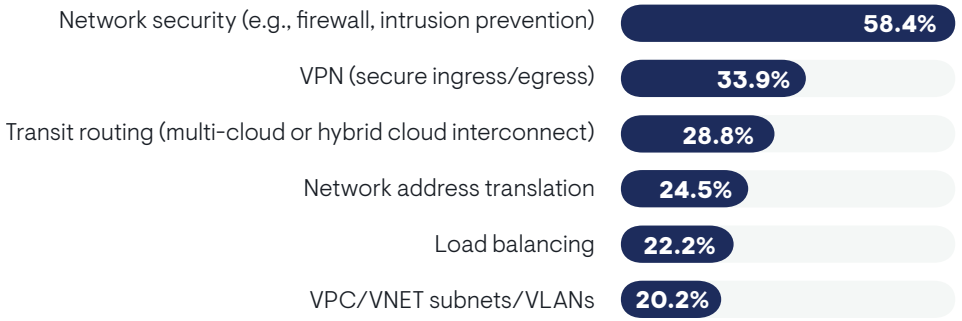
The CIO's suite was the most likely to report that such a solution is already implemented, while network engineering, cloud operations, and security all expect future adoption. This suggests that IT executives misunderstand this concept to some extent. Possibly, they are buying into the marketing hype fed to them by networking vendors that address only a subset of requirements of an end-to-end solution. Technical personnel working closely with network technology are savvier, recognizing that they're not quite there with these end-to-end products.

Sample Size = 325

Priority Functionality

Figure 17 reveals the functionality enterprises want from an end-to-end multi-cloud networking solution. Security stands out as the dominant priority. Enterprises want a networking solution that can implement network security controls across multiple providers. Security was more important to organizations that use two or three cloud providers, but less important once organizations reach five or more providers.

FIGURE 17. MOST IMPORTANT NETWORK FUNCTIONS TO HAVE IN AN END-TO-END MULTI-CLOUD NETWORKING SOLUTION



Once enterprises have five cloud providers, they start looking for a solution that can manage VPC and VNET subnets and VLANs, which is otherwise the lowest priority for these solutions. This suggests as enterprises reach five or more cloud providers, they need to impose some consistent configurations for local networking inside the cloud. We also found that the most successful multi-cloud networking strategies prioritized subnet and VLAN functionality in their multi-cloud networking solutions.

Enterprises identified VPNs and transit routing as their secondary functionality priorities. Less successful organizations tended to favor VPN functionality.

Network address translation (NAT) was a lower priority, but successful organizations put it at the top of their lists. Technical personnel tended to favor it more than IT middle management. NAT also increases in importance as organizations expand the number of cloud providers they work with.

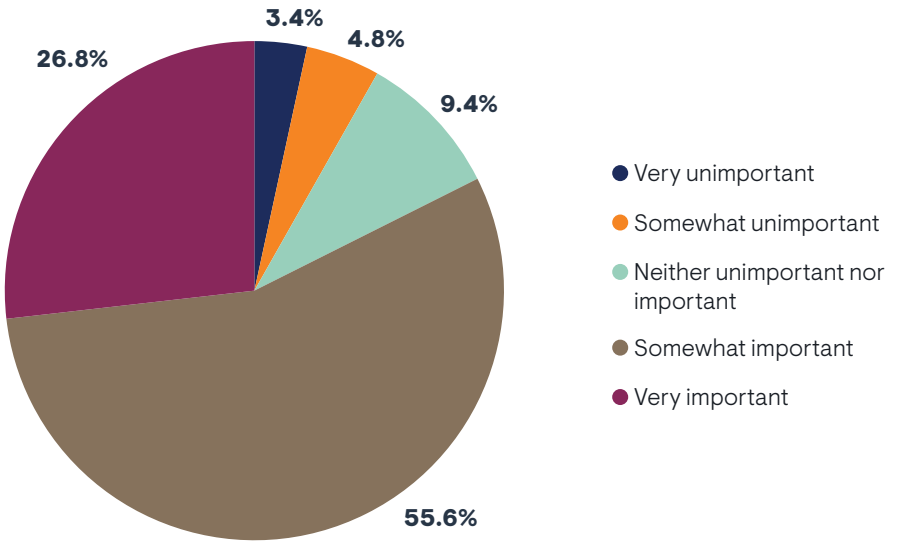
Sample Size = 351, Valid Cases = 351, Total Mentions = 660

APIs and Integrations

More than 82% of organizations believe that it is at least somewhat important for their cloud networking solutions to have open APIs.

As this report revealed, today's multi-cloud networks are multi-vendor. Integrations between these vendors will be essential. Moreover, these cloud networking solutions need to integrate with other parts of the cloud management stack. **Figure 18** reflects this reality. More than 82% of organizations believe that that it is at least somewhat important for their cloud networking solutions to have open APIs. Successful organizations were much more likely to recognize the importance of these APIs. The IT architecture group, the security team, and the CIO's suite were the most likely to believe them to be very important.

FIGURE 18. IMPORTANCE OF OPEN APIS TO YOUR CLOUD NETWORKING SOLUTIONS



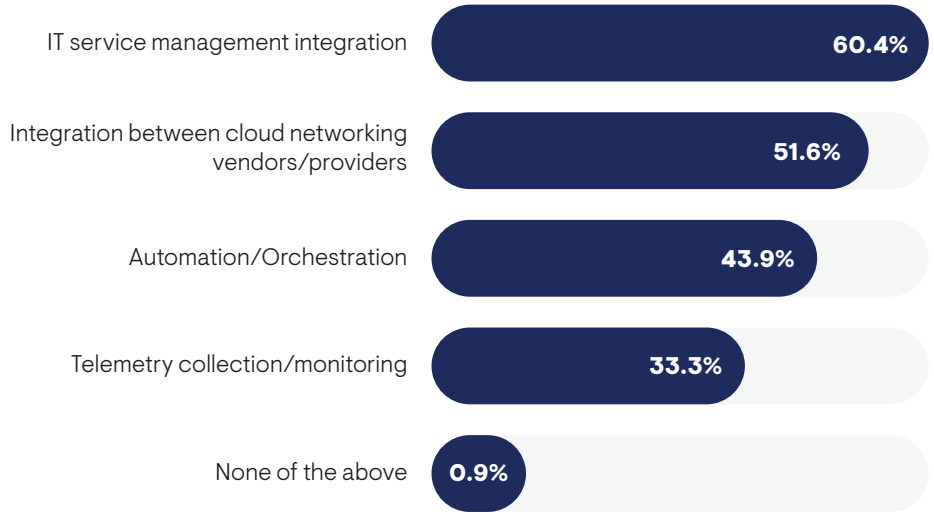
Sample Size = 351

Figure 19 reveals how organizations want to use these APIs. IT service management integration and integration between cloud networking vendors are the priority use cases. The CIO's suite appears to push harder for ITSM integration than cloud operations, network engineering, or security.

Automation and orchestration and telemetry collection for monitoring were the secondary priorities for APIs. However, successful organizations were much more likely to prioritize telemetry, suggesting a possible best practice.

Integration between cloud networking vendors is a lower priority for organizations that use five or more cloud providers. Note that organizations are also more likely to see the value of an end-to-end multi-cloud networking solution, which suggests they are less likely to have multiple vendors that need to be integrated.

FIGURE 19. HOW ORGANIZATIONS WANT TO USE OPEN APIS THAT CLOUD NETWORKING SOLUTIONS OFFER



Sample Size = 351, Valid Cases = 351, Total Mentions = 667

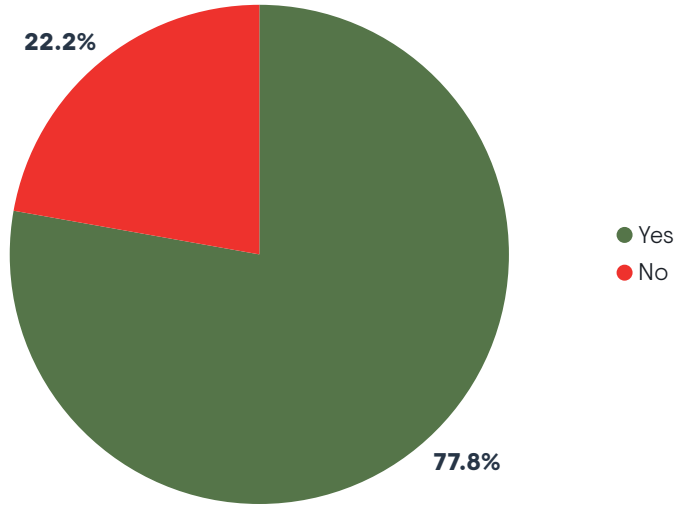
Multi-Cloud Network Operations

Centralized Management

End-to-end management of a multi-cloud network will be essential for mitigating complexity and streamlining operations. **Figure 20** reveals that more than three-quarters of enterprises can manage all aspects of cloud networking via a single console. Successful cloud networking strategies accounted for many of the affirmative answers to this question. For instance, 93% of successful organizations said yes, versus 75% of somewhat successful, 64% of somewhat unsuccessful, and 0% of unsuccessful organizations.

The network engineering team was the most likely to believe it has single-pane-of-glass management, while the security team and the IT architecture group were the least likely. Oddly, organizations were more likely to have a single-console management capability as they increased the number of cloud providers they have. This suggests that IT organizations become more rigorous with network management as the cloud environment gets more complex.

FIGURE 20. ARE YOU ABLE TO MANAGE ALL ASPECTS OF YOUR CLOUD NETWORK FROM A SINGLE MANAGEMENT CONSOLE?



Sample Size = 351

A network architecture executive at a $1 billion bank told EMA he uses a tool that gives him good visibility on a single pane of glass. "The challenge is that too much money and work goes into using it—we're running thin these days," he said.

Despite so many organizations claiming to have centralized management, organizations struggle to manage networking consistently across cloud providers. **Figure 21** reveals how easy or difficult organizations find it to consistently manage load balancing, ingress/egress controls, network security policy, and network traffic routing across multiple cloud providers. Very few organizations find it easy to perform any of these operations. Successful organizations were more likely to consider all of these operations to be easier to manage consistently, suggesting that organizations should address management complexity in each of these areas in order to succeed with multi-cloud networking.

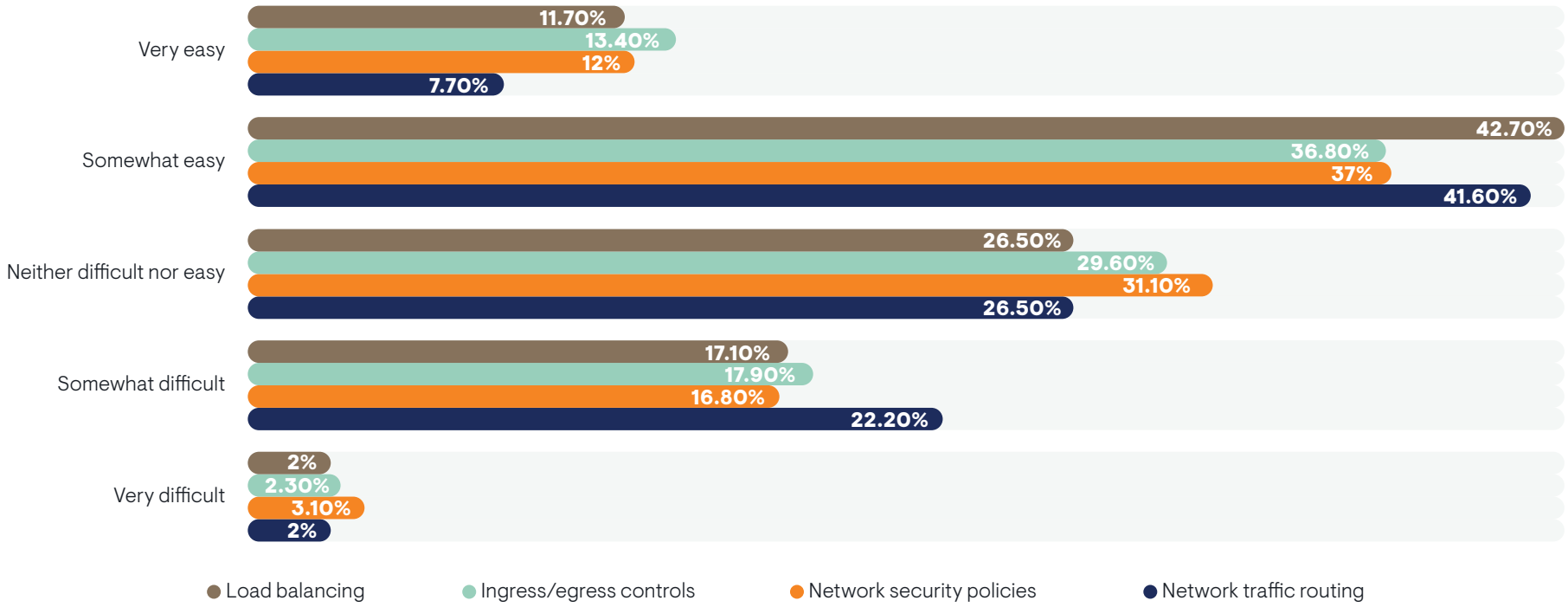
Network traffic routing is most challenging. Technical personnel were much more likely than IT executives to report difficulty with it. In fact, the network engineering team and the cloud operations team were both more pessimistic about consistent network traffic routing than the CIO's suite.

The cloud operations team and the CIO's suite were more optimistic about consistent network security policy management, but again, the network engineering team perceives challenges.

The security team and the CIO's suite were more optimistic about consistent management of ingress and egress controls than network engineering.

The security group and the CIO's suite were more optimistic about consistent load balancing management, but the network engineering and cloud operations teams were pessimistic.

FIGURE 21. HOW EASY OR DIFFICULT IS IT TO APPLY THE FOLLOWING CONSISTENTLY ACROSS MULTIPLE CLOUD PROVIDERS?



Multi-Cloud Network Observability

Over the last several years, EMA research consistently found that network operations teams are trying to improve their ability to monitor and troubleshoot the public cloud. In the past, the use of a single cloud provider challenged the network team's monitoring toolsets. With multi-cloud becoming ubiquitous, the visibility gap will only widen. Network teams will need new tools.

Nearly 44% are also using incumbent tools, and 36.5% are leaning on the native monitoring capabilities of their cloud networking solutions. The data suggests that organizations are using a multi-tool strategy for multi-cloud network monitoring.

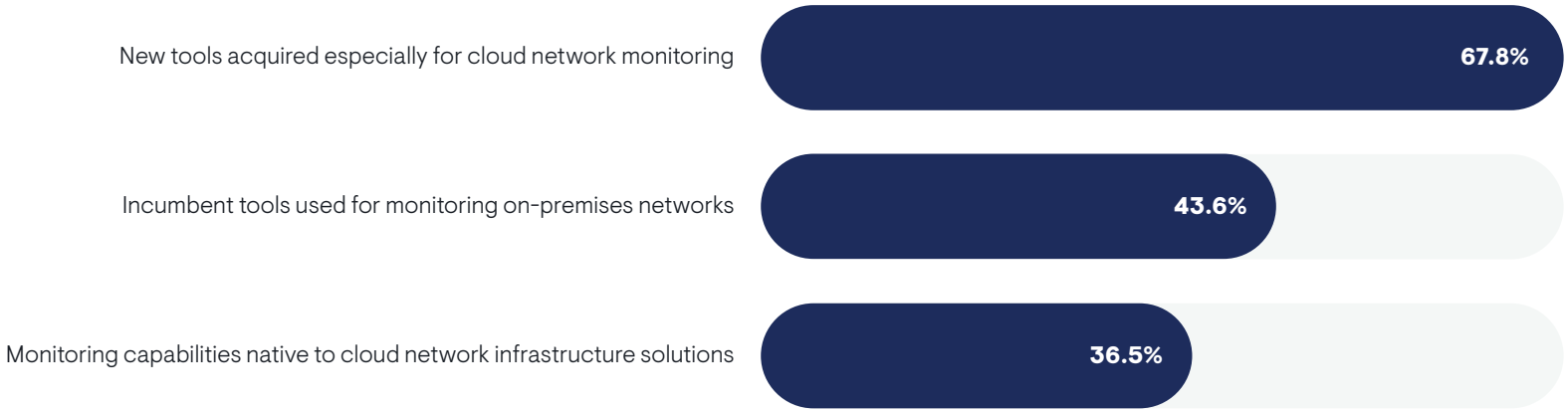
Incumbent tools have more to offer than many organizations give them credit for. For instance, the most successful multi-cloud networking strategies are more likely to use incumbent monitoring tools. Organizations that use four or more cloud providers were more likely than others to use incumbent tools, too.

IT executives and middle management were more likely than technical personnel to rely on the native monitoring their cloud networking vendors offer.

68% of organizations are acquiring new tools for cloud network monitoring.

Figure 22 reveals that 68% of organizations are acquiring new tools for cloud network monitoring. Smaller companies were more likely to seek new tools.

FIGURE 22. TOOLS ORGANIZATIONS USE OR PLAN TO USE TO MONITOR AND TROUBLESHOOT CLOUD NETWORKS

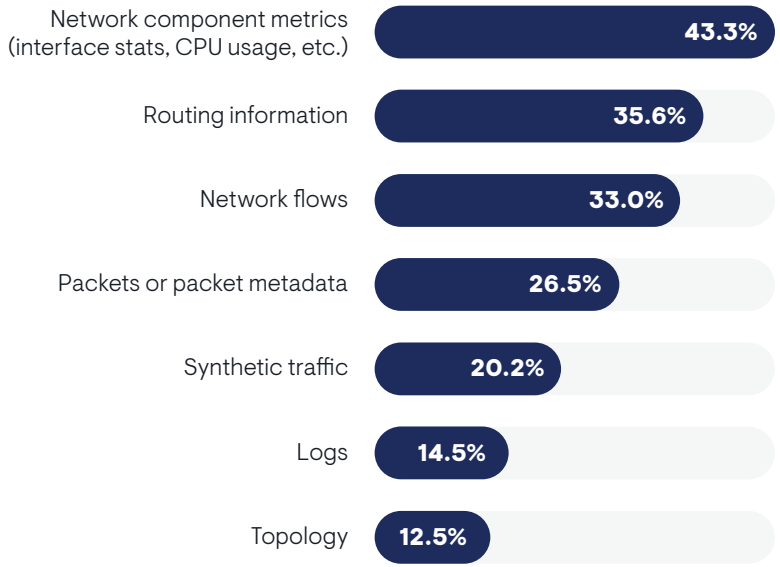


Sample Size = 351, Valid Cases = 351, Total Mentions = 519

Observability Data

Figure 23 reveals the data that organizations need for monitoring their cloud networks. Network metrics, like interface stats and CPU utilization, are the highest priority. The most successful cloud networking teams are more likely to cite their importance.

FIGURE 23. SOURCES OF INFORMATION MOST CRITICAL TO MONITORING CLOUD NETWORKS



Secondarily, organizations want routing information and network flow records. Larger companies are more likely to want routing information.

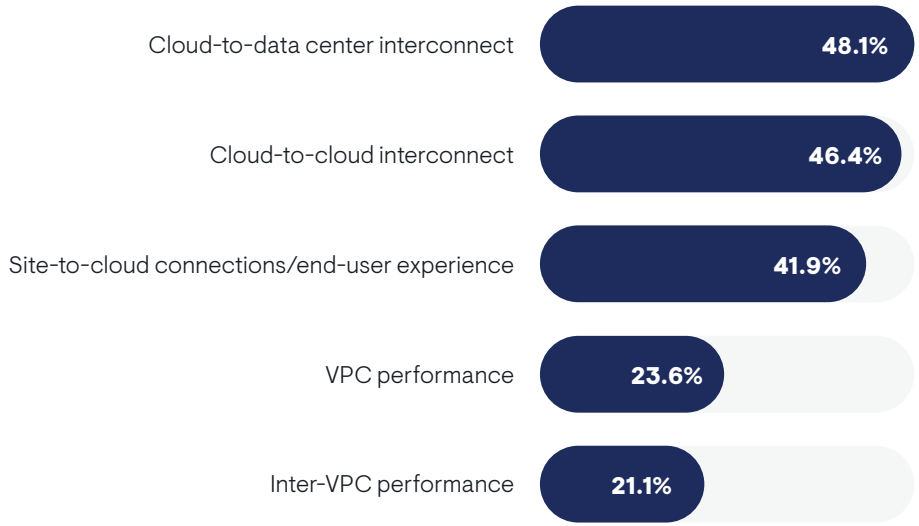
Packet data and synthetic traffic round out the top five. Logs and topology are the lowest priorities for network monitoring in the cloud. Logs are more popular among less successful organizations. Topology information is more valuable to the cloud operations team than it is to network engineering.

Sample Size = 351, Valid Cases = 351, Total Mentions = 652

Reporting Priorities

Figure 24 reveals what kind of reports network teams need in their cloud monitoring solutions. Cloud-to-data center and cloud-to-cloud reporting are the top priorities. Cloud-to-data center reporting was a lower priority for larger companies, but cloud-to-cloud reporting was a higher priority for them.

FIGURE 24. REPORTS THAT ARE MOST IMPORTANT WHEN MONITORING A MULTI-CLOUD NETWORK



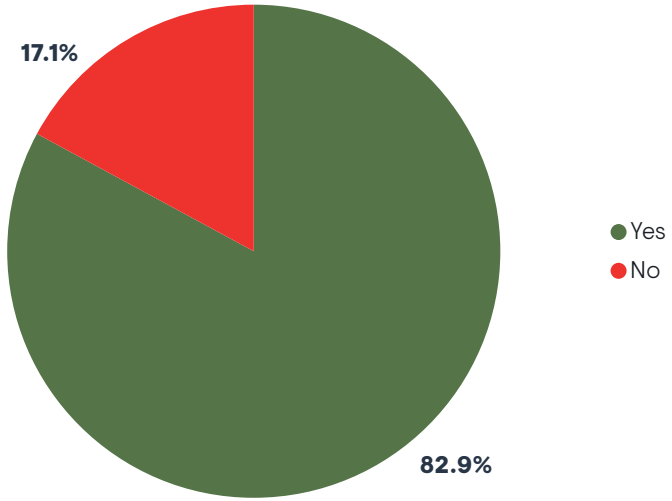
Site-to-cloud reporting was another big monitoring priority, but VPC performance and inter-VPC performance were low priorities. IT executives were the least likely to want VPC performance insights, while technical personnel and middle management were more interested.

Sample Size = 351, Valid Cases = 351, Total Mentions = 636

Quality of Observability

Figure 25 reveals that nearly 83% of organizations claim they can get an end-to-end view of the health and performance of their multi-cloud network. Affirmative responses were most common in organizations that are successful with cloud networking. While 96% of successful teams claim to have this visibility, only 55% of somewhat unsuccessful and 50% of unsuccessful organizations agree.

FIGURE 25. CAN YOUR NETWORK MONITORING TOOLS PROVIDE AN END-TO-END VIEW OF THE HEALTH AND PERFORMANCE OF YOUR MULTI-CLOUD NETWORK?

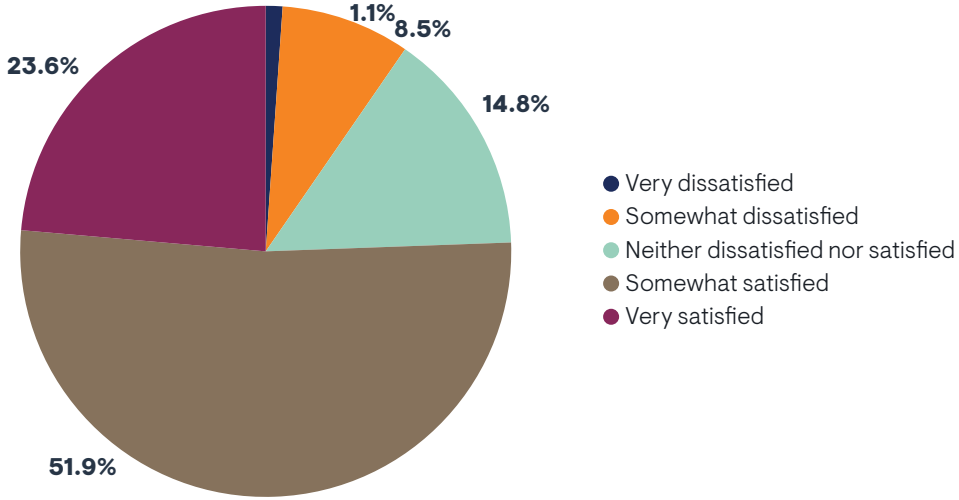


Members of cybersecurity and IT architectures groups were the most pessimistic about their ability to get end-to-end visibility. Larger companies were also pessimistic.

"There is no tool that can help us identify our needs in cloud management," said a security operations manager at a $4 billion media company. "There is no tool that can identify all of our VPN clusters and draw a picture to show us our weaker management controls and where our weaker policies need to be adjusted."

Despite the large number of people who claim to have end-to-end multi-cloud visibility, only 23.6% are fully satisfied with their multi-cloud network monitoring and troubleshooting capabilities, as revealed in **Figure 26**. Unsurprisingly, overall multi-cloud networking success correlates strongly with visibility satisfaction.

FIGURE 26. OVERALL SATISFACTION WITH CURRENT TOOLSET'S ABILITY TO MONITOR AND TROUBLESHOOT MULTI-CLOUD NETWORKS



The visibility gap in the cloud is evident to a senior network engineer at a large university hospital system and medical school.

"Compared with on-prem—where we have visibility into everything—in the cloud, it's all opaque," he said. "We don't know if something is wrong, and we don't get alerts if a region is having a problem."

He can see that a cloud link is up, but that is about all. "This is a problem of integration between on-prem and the cloud. I would love to have visibility into traffic and interfaces in the cloud. It's possible, but it needs to be done from the beginning," he said.

Members of network engineering teams were the least satisfied with monitoring and troubleshooting capabilities, while members of the CIO's suite and cybersecurity were the happiest.

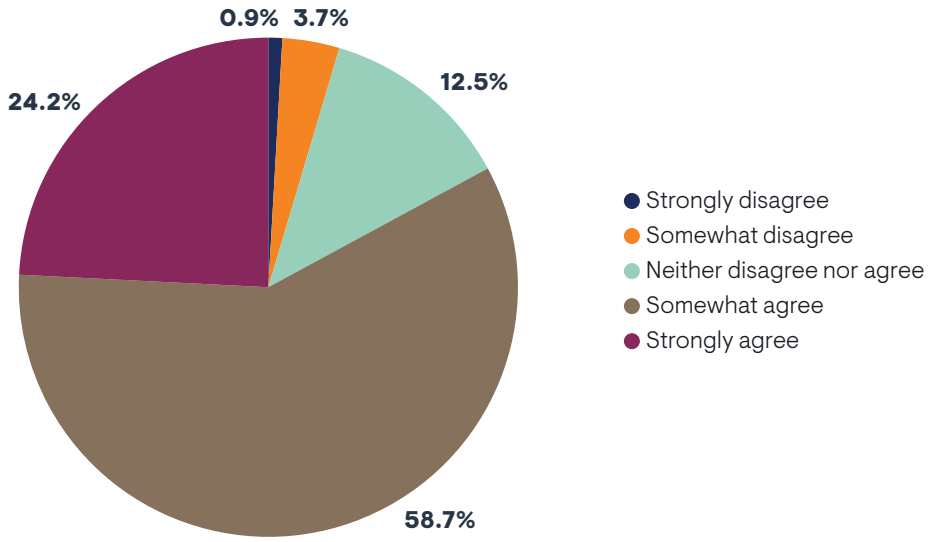
Sample Size = 351

The Multi-Cloud Networking Team

Network Team Influence

EMA believes that the network team must have a seat at the table if an organization is going to succeed with multi-cloud networking. Unfortunately, **Figure 27** reveals that only 24% believe the network team has enough influence over cloud networking. Nearly 59% think the network team has a decent amount of clout but could be doing better.

FIGURE 27. DO YOU AGREE OR DISAGREE WITH THE FOLLOWING STATEMENT? OUR NETWORK INFRASTRUCTURE AND OPERATIONS TEAM HAS ENOUGH INFLUENCE OVER THE COMPANY'S CLOUD STRATEGY.



A senior network engineer at a large university hospital system and medical school told EMA that better collaboration and communication with major players in the cloud would help his team's ability to provide timely and secure connectivity. "We cannot react to changes quickly because we don't know too much about what's going on in the cloud, and we can't proactively say 'next month we will need more bandwidth.' We're just reacting to thresholds."

Successful multi-cloud strategies are more likely to give the network team enough influence. Members of the network engineering team and the network operations team were the most pessimistic about the networking group's influence over the cloud. The CIO's suite, the cloud operations team, IT architecture, and cybersecurity were all more optimistic. This gap is stark. Networking professionals want more influence, but everyone around them believes that they already have enough.

Networking professionals want more influence, but everyone around them believes they already have enough.

Sample Size = 351

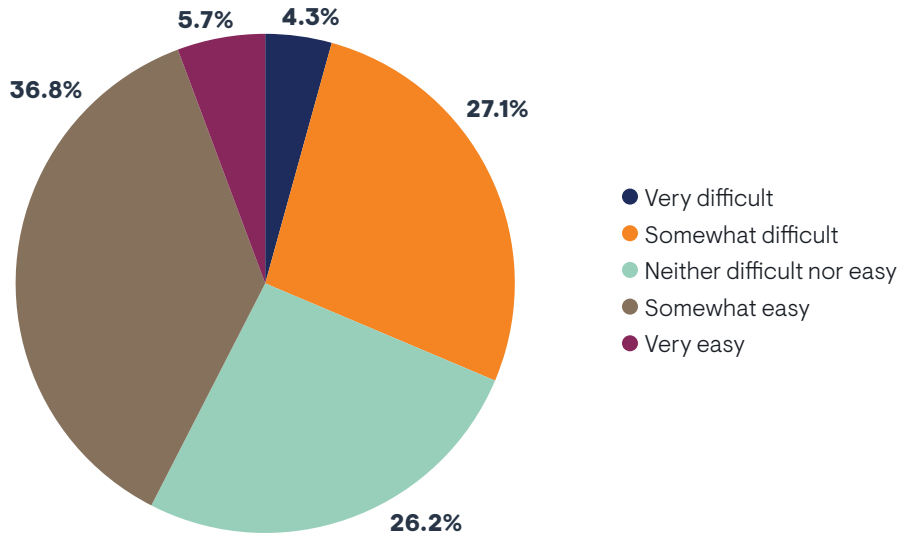
Finding Cloud Network Expertise

Speaking of hiring, it isn't easy to find experts on cloud networking. **Figure 28** reveals that only 37% consider it very easy to hire such people. More than 31% believe it's genuinely difficult, and this is a major challenge to multi-cloud networking success. Organizations that struggle the most with their multi-cloud networking strategy are the most likely to report roadblocks to hiring cloud networking experts.

Europeans were more likely than North Americans to report a challenge with hiring, and smaller companies struggle more than larger ones. EMA observed that as organizations increase the number of cloud providers they work with, they report less difficulty hiring. These organizations are more likely to already have an end-to-end multi-cloud networking solution in production, which reduces the need to hire people with skills specific to individual cloud providers' networking solutions.

A network architecture executive at a $1 billion bank said his multi-cloud networking tool has a "boiled down approach to all the clouds" that makes it easier to use versus learning multiple clouds. "When you're training on one provider, it's very different to be oriented to the one cloud provider," he said.

FIGURE 28. IS IT EASY OR DIFFICULT FOR YOUR ORGANIZATION TO HIRE PEOPLE WITH CLOUD NETWORKING EXPERTISE?



Sample Size = 351

90% of companies are allocating resources to train their people on cloud networking.

With many organizations struggling to hire cloud networking experts and others adopting new technologies and working with new cloud providers, training will be essential. **Figure 29** reveals that 90% of companies are allocating resources to train their people on cloud networking.

Training is more likely in organizations in which the cloud is driving an increased workload for the network team and in organizations that are struggling with hiring. It's also happening more often in the most successful multi-cloud networking organizations.

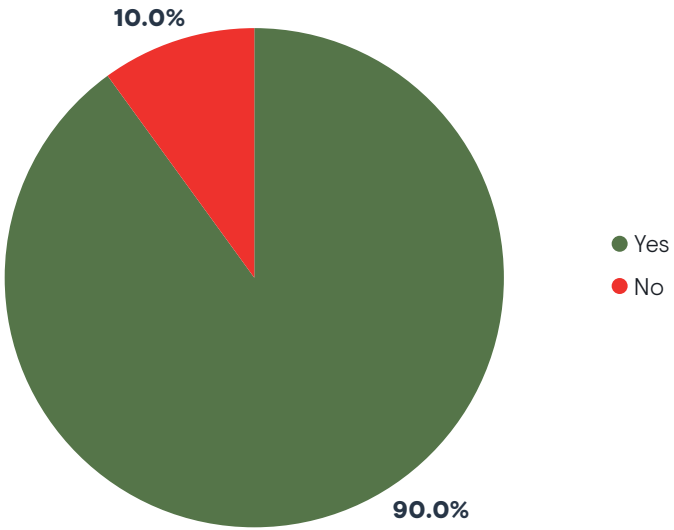
"There is a learning curve for a network engineer to go to cloud. There are different concepts and everything is virtual," said the senior network engineer at a large university hospital system and medical school. "Every cloud provider is using different names for the same service or device, and some colleagues don't feel like putting in the time to learn those concepts. That's a big problem."

Organizations that are using purpose-built, multi-cloud networking software and the native networking features of cloud providers are more likely to allocate resources to training. Training is also more common in organizations that have a strong focus on using open APIs offered by their cloud networking solutions, particularly those trying to integrate these solutions with IT service management platforms.

Training also has the following impacts on multi-cloud networking strategies:

- Multi-cloud network design is easier
- Cloud networking chargebacks are enabled
- It's easier to consistently manage ingress/regress controls and load balancing across multiple cloud providers

FIGURE 29. IS YOUR ORGANIZATION ALLOCATING RESOURCES TO TRAIN EXISTING PERSONNEL ON CLOUD NETWORKING CONCEPTS AND TECHNOLOGY?



Sample Size = 351

Conclusion

EMA believes that multi-cloud enterprises are at an inflection point with networks. Most organizations know they could be doing better with these networks. Too many of them are leaning heavily on the native networking solutions their individual cloud providers offer. With many of them using three or four providers, it's extremely difficult to build a consistent network across their multi-cloud estate.

Given this reality, it's no surprise that nearly all the organizations in this survey are interested in deploying an end-to-end, multi-cloud networking solution that can enable a consistent architecture across their cloud providers and their on-premises networks.

These multi-cloud networking solutions must offer a rich set of functionality, including integrated network security solutions, VPN for ingress and egress controls, and a robust routing stack for optimal traffic engineering across the multi-cloud architecture.

At the same time, multi-cloud network teams need better visibility. Satisfaction with cloud networking monitoring has been low for years. Companies are acquiring new third-party monitoring tools to improve observability across the multi-cloud network. Many are also trying to adapt their existing tools, and others are hoping their multi-cloud networking providers can offer native monitoring capabilities that can close their visibility gaps.

As organizations optimize their networks for multi-cloud, the network team will face an uphill battle. Most of them lack enough clout to influence overall multi-cloud strategy. They're also struggling to hire people with cloud networking expertise. Training will be essential. EMA advises these network teams to find partners that can empower them. The security group is a priority partner, and end-user support appears to be an underrated ally in the multi-cloud world.

As organizations optimize their networks for multi-cloud, the network team will face an uphill battle.

This research should offer IT professionals an early roadmap to multi-cloud networking success. Given that most enterprises are planning to migrate more applications to the cloud over the next two years and increase the number of cloud providers that they use, EMA will continue to explore the topic in its ongoing research.

Case Study: HAPEV Successfully Launches its Multicloud Network with Aviatrix

When Hamburger Pensionsverwaltung eG (HAPEV), a German service provider for company pension schemes, decided to adopt a multicloud architecture, its IT infrastructure team implemented a multicloud networking solution from Aviatrix to apply consistent network security and compliance.

Two years ago, HAPEV used no public cloud services. It hosted all its applications in its on-premises data centers. Then, the business decided to transition directly to a multicloud strategy, with applications hosted in both Amazon Web Services (AWS) and Microsoft Azure. The IT infrastructure team immediately realized that networking was going to be a challenge.

Security and Compliance Requirements Dictated a Multicloud Networking Solution

"When we looked at multicloud, we tried to anticipate the problems we would have," said Keven Hamann, IT Solution Architect for HAPEV. "The main problem we saw was with networking. Each cloud provider has a specific way of doing networking, from a global level to a regional level down to subnets. You have to learn specific naming schemes. To secure a workload in AWS, you have to use a completely different technical solution than what you have in Azure. It's not easy to handle both at the same time."

Getting the network right was critical for HAPEV because they must adhere to highly regulated industry requirements. Hamann noted that the network needed consistent compliance controls across AWS and Azure. Regulatory compliance also required that the IT infrastructure team be able to inspect traffic across the multicloud network to detect potential malicious activity.

Aviatrix Makes Multicloud Networking "Too Easy"

After defining these requirements, Hamann and his team selected multicloud networking software and services from Aviatrix to build HAPEV's new network. The IT infrastructure team used Aviatrix to deploy gateways in each AWS and Azure region with centralized, secure ingress and egress and firewalling. They also interconnected all cloud regions with Aviatrix's cloud transit capability.

"At first, it seemed a little too easy," Hamann said. "When you have two separate hyperscale cloud providers, building interconnects between them is not simple. But deploying Aviatrix gateways and using them to connect the providers was not difficult. All our traffic is now centralized over the transit gateways. We have a full mesh network with firewall inspection."

Automation and Orchestration with Terraform

Hamann integrated his Aviatrix solution with Terraform, the tool that HAPEV uses for multicloud infrastructure orchestration. This allows his team and the DevOps team to make automated changes to the network as needed.

"It's very easy to scale up and down the mesh. We can expand the mesh into other regions in two clicks," he said.

Deep Visibility with CoPilot

On top of the resilient and secure network that HAPEV was able to establish, Hamann's team has the network visibility it needs, too. Aviatrix offers CoPilot, which provides full visibility into network traffic. CoPilot leverages Aviatrix network software that is directly in the data plane across the multicloud network. It collects and analyzes traffic data and metrics from these data plane elements to provide global visibility.

CoPilot not only helps address HAPEV's security and compliance requirements, but it also provides excellent support for operational monitoring and troubleshooting. "It's cool how you can get traffic visibility over the whole multicloud network mesh," Hamann said. "You can get a quick view of where packets are coming from and where they are going."

Up-Skilling IT with ACE Certifications

Finally, to ensure that the IT infrastructure team is fully capable of meeting the networking needs of HAPEV's multicloud environment, Hamann and his team are working with Aviatrix on multicloud networking training. Hamann and three other members of his team completed the company's training and certification programs to become Aviatrix Certified Engineers (ACE).

"ACE certifications are the best knowledge you can get on public clouds," Hamann said.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

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

4235.032223