IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

KEYSIGHT

Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise

June 2022 EMA Research Report Summary

By Shamus McGillicuddy, Vice President of Research

Table of Contents

1 Introduction
2 Key Findings
3 Research Methodology
5 Overall Visibility Architecture Strategies
6 Visibility Architecture Spending is Increasing
6 Drivers of Visibility Investment
6 Technology Initiatives as Drivers
7 Visibility Architecture Benefits and Challenges
8 Success and Failure with Solutions
9 Key Benefits of Using Network Visibility Solutions
10 NetSecOps Collaboration
11 Visibility Architecture Challenges
12 The Access Layer of Visibility Architecture
13 Mirroring Network Traffic From Physical Infrastructure
13 TAPs Versus SPANs
14 Benefits of TAPs Over SPANs
15 The Architectural Core: Network Packet Brokers
16 Platform Characteristics That Drive ROI
17 Critical Packet Manipulation and Data Generation Features
18 Supporting Hybrid, Multi-Cloud Visibility
19 The Importance of Packet Data to Cloud Operations
19 Packet Data is Essential to Security Monitoring and Analysis in the Cloud
20 Packet Data is Essential to Performance Management in the Cloud
20 Packet Data is Essential to Capacity Management in the Cloud
21 Cloud-Related Network Blind Spots
21 Multi-Cloud Networks Struggle More
22 Visibility Solutions for the Cloud
22 Acquiring Cloud Traffic Data
23 The Benefits of Using Third-Party Visibility Software in the Cloud
24 End-to-End Hybrid-Cloud Visibility Architecture
26 Trends in Traffic Data
27 The Problem of Encrypted Traffic
28 Preferred Methods for Decryption
29 Packets and Observability Data
30 Conclusion
32 Appendix. Demographics

Introduction

This summary of Enterprise Management Associates (EMA) research explores how IT and security organizations use network visibility architectures to deliver network packets to critical performance and security analysis tools. It especially examines how organizations need to evolve their network visibility architectures as they adopt hybrid, multi-cloud architectures.

Network traffic data is essential to IT and security operations. Simply put, the data packets that traverse networks are the best source of truth about what is happening with digital infrastructure and services. With full access to packets crossing the wire, analysis tools can diagnose and warn users about security incidents, network and application performance issues, compliance violations, capacity trends, and more.

IT and security organizations use network visibility architectures to deliver this packet data to analysis tools. These architectures can span data centers, campus networks, and the public cloud, using a mix of hardware and software to mirror traffic from various points on the network, then aggregate, modify, and filter relevant data for delivery to analysis tools. Traffic is usually mirrored from the network via a hardware test access point (TAP), a port on a network device configured as a switch port analyzer (SPAN), a software TAP, or a traffic mirroring feature offered by virtual infrastructure and cloud service providers. The data is aggregated and delivered to tools by network packet brokers, available as both hardware and software, with varying levels of advanced features for packet manipulation and metadata generation.

A network visibility architecture is essential to any organization that relies on packet data for IT performance management and security analysis. As companies migrate applications and data to the cloud, a comprehensive visibility architecture will be essential to network and security operations.

Key Findings

- Only 34% of organizations are fully successful with their network visibility architecture
- Top challenges to using this technology are scalability issues and architectural complexity
- Improved technical team productivity and reduced security risks are the top benefits of using a visibility architecture
- 88% of organizations believe visibility architectures can improve collaboration between network teams and security teams
- 46% of organizations say the migration of applications to the cloud has created blind spots on their networks
- 60% of companies are adopting virtual network packet brokers and taps for cloud visibility, primarily to improve overall reliability of data collection
- 89% of organizations believe it is at least somewhat important to have an end-to-end visibility architecture that spans on-premises and cloud-based networks
- 96% of organizations are interested in combining packet analysis with analysis of traditional observability data (metrics, events, logs, and traces), particularly to support cybersecurity operations

Research Methodology

This research is based on an online market research survey of 302 North American and European technology professionals that was conducted in May 2022. Respondents confirmed that they either used network visibility technology and/or had responsibility for evaluating, selecting, implementing, and/or maintaining such technology. They worked for organizations ranging in size from 500 global employees to 20,000 or more.

Job titles ranged from IT administrator to chief information officer (CIO). Functional groups represented included cloud operations, data center operations, IT program management, network engineering and operations, and IT or cyber-security. Full details on demographics are detailed in the Appendix.

In addition, EMA analysts interviewed several technology professionals with deep experience as administrators and users of network visibility solutions. EMA used their insights to enrich the analysis of the data in this report. These professionals are quoted anonymously throughout this report.

Overall Visibility Architecture Strategies

Visibility Architecture Spending is Increasing

Figure 1 reveals that 78% of companies expect their budgets for visibility architecture solutions to increase over the next two years, with nearly 23% of respondents describing that budget growth as significant. Successful users of visibility architectures were the most likely to expect a large budget increase.

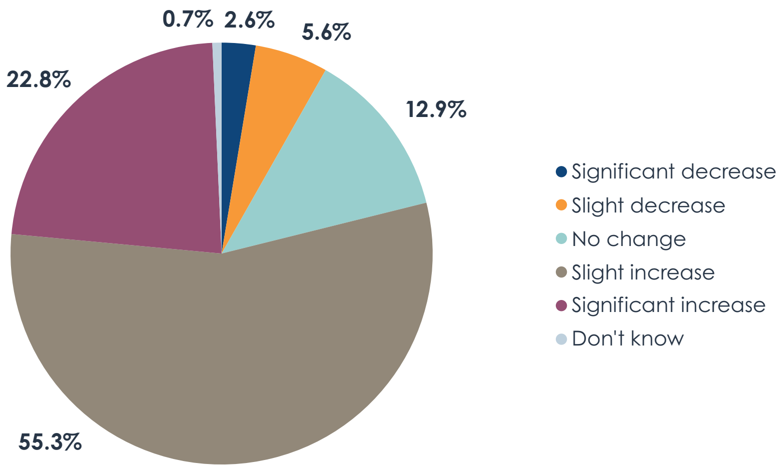


Figure 1. Anticipated changes to visibility architecture budgets over the next two years

78% of companies expect their budgets for visibility architecture solutions to increase over the next two years.

Technology executives are more likely than staff and middle management to expect significant budget growth. Multi-cloud architectures appear to drive budget. Organizations that use three or more cloud providers were three times as likely as those that use only one provider to expect a significant increase in visibility architecture budget. On the other hand, smaller companies were more likely to expect a budget increase than larger ones.

Sample Size = 302

Drivers of Visibility Investment

Technology Initiatives as Drivers

Figure 2 reveals that a majority of companies are investing in visibility solutions to support their hybrid and/or multi-cloud networks. The move toward these cloud architectures creates the need for better access to traffic data for performance and security analysis. Members of the IT executive suite and security teams were most likely to cite the cloud as an investment driver. Companies that use three or more cloud providers were the most likely to cite cloud as a driver.

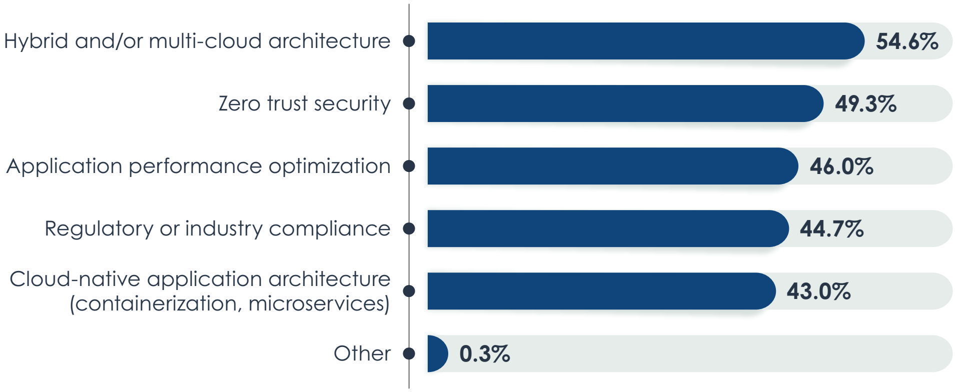


Figure 2. Initiatives or technical requirements that are significant drivers of investments in visibility architectures and related technology

The chief secondary driver is zero trust security. Zero trust security requires continual monitoring of network activity. Security team members were much more likely than others to cite this as an investment driver.

Application performance optimization, compliance, and cloud-native application architectures are significant secondary drivers. The most successful users of visibility architectures were most likely to identify cloud-native applications and application performance optimization as investment drivers. Application performance optimization is also a major driver of companies with three or more cloud providers.

Sample Size = 302, Valid Cases = 302, Total Mentions = 719

Visibility Architecture Benefits and Challenges

Success and Failure with Solutions

According to **Figure 3**, only 34% of organizations believe they are fully successful with their network visibility architectures. More than half are somewhat successful, meaning they see room for improvement. Only 3% claimed to be somewhat unsuccessful and no respondents believed they were completely unsuccessful. Companies that operate the largest networks reported more success. North Americans reported more success than Europeans.

In EMA's 2020 research on this topic, 40% of respondents claimed complete success with network visibility solutions. It's unclear exactly why there was a decline in success, but EMA research generally found over the last couple of years that network infrastructure and operations teams are struggling generally with the impacts of cloud migration, increased network complexity, tool complexity, and a shortage of skilled personnel.

Throughout this report, EMA highlights differences between the most successful organizations and all others, pointing to potential best and worst practices for using visibility solutions.

Only 34% of organizations believe they are fully successful with their network visibility architectures.

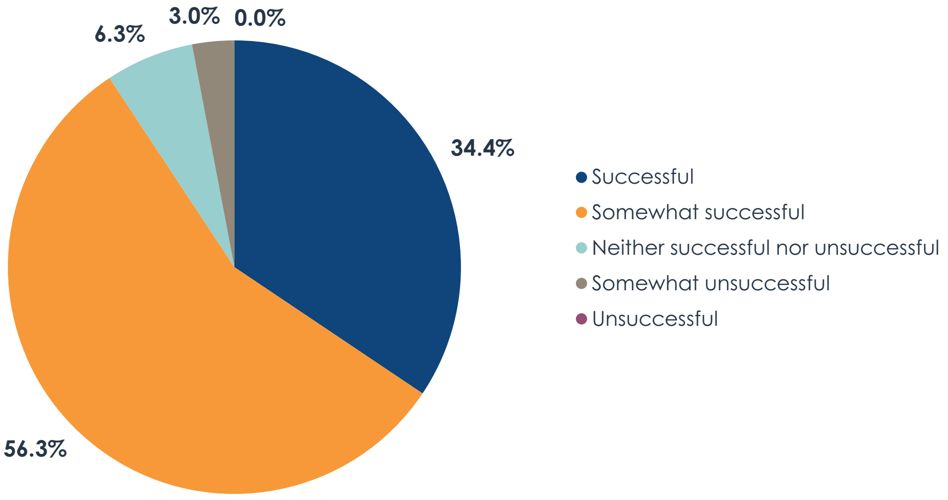


Figure 3. Self-reported levels of success with using network visibility architecture

Sample Size = 302

Key Benefits of Using Network Visibility Solutions

Organizations that use a network visibility architecture will improve IT and security productivity and reduce overall security risk, according to **Figure 4**. The chart highlights the most common benefits of using these visibility solutions. Members of security teams and IT executive suites were the most likely to perceive an opportunity for reduced security risk. North Americans had a stronger affinity for productivity benefits than Europeans. Very large companies are more likely to perceive the opportunity to reduce security risk.

The secondary opportunities are improved capacity management, optimized cloud migration, and network and application performance and resiliency. Performance, resiliency, and capacity management are more important to organizations that use multiple cloud providers.

Better cross-team collaboration, reduced compliance risk, and extended life of analysis tools are the least common opportunities. Data center operations teams were more likely to see an opportunity for reduced compliance risk.

An enterprise monitoring systems engineer with a Fortune 500 healthcare company believes that extending the life of analysis tools is essential. "We can't afford the tool upgrades," he said. "Tools are pretty expensive. Our maintenance costs from [our network performance management vendor] last year were $1.3 million."

Organizations that use a network visibility architecture will improve IT and security productivity and reduce overall security risk.

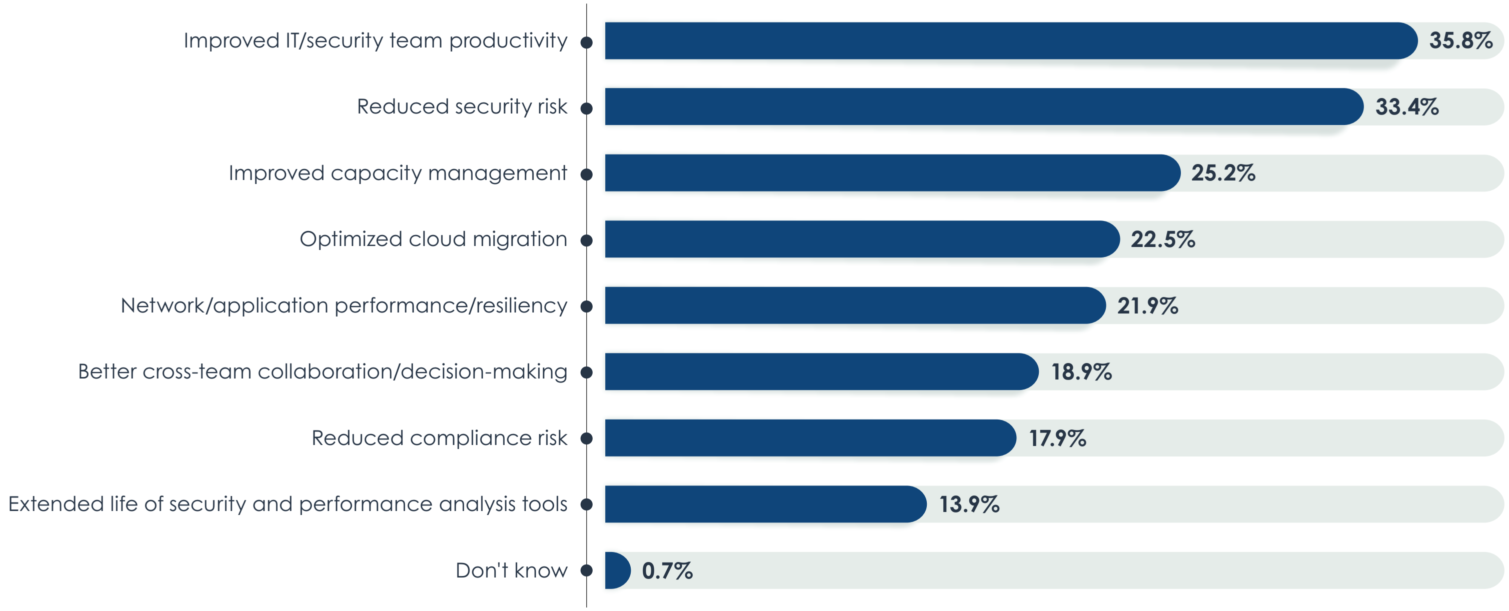


Figure 4. Most important benefits of using a network visibility architecture

Sample Size = 302,
Valid Cases = 302,
Total Mentions = 574

NetSecOps Collaboration

Collaboration between network teams and security teams has become a critical focus for many enterprises over the last few years. EMA research recently found that 75.4% of organizations have observed an increase in this collaboration. Eighty-three percent of companies have told EMA that the security team's need to analyze network traffic is a major driver of NetSecOps collaboration in general.

Figure 5 reveals that a network visibility architecture can support successful collaboration between these groups, with 88% of research respondents saying that this technology is at least somewhat important to network teams and security teams working together successfully. Successful users of visibility architecture in general were the most likely to say visibility solutions are very important to this collaboration. Members of security teams and the IT executive suite were the most likely to agree, but network team members were less convinced. Agreement was strongest in midmarket and large enterprises, but very large enterprises (10,000 or more employees) were less enthusiastic. North Americans were more enthusiastic than Europeans.

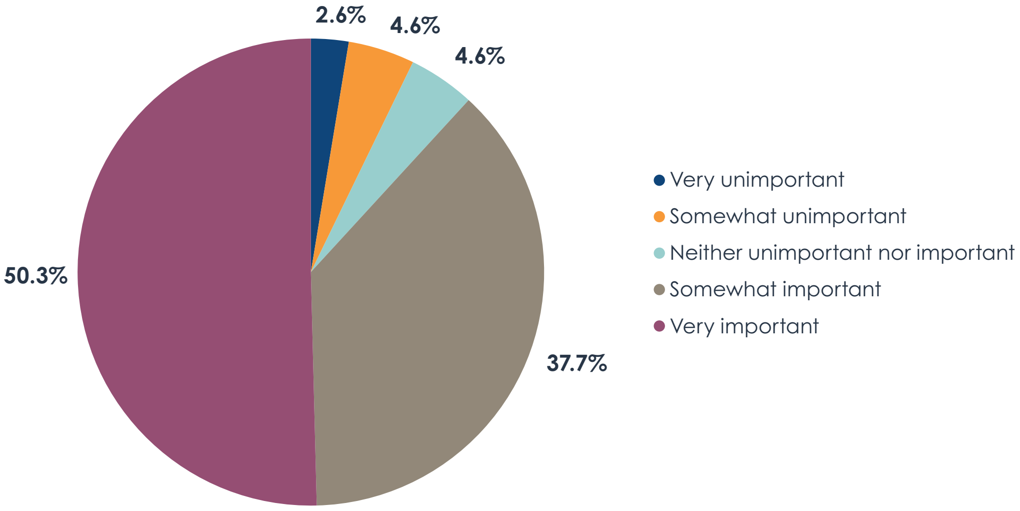


Figure 5. Importance of a visibility architecture to successful collaboration between network teams and security teams

Sample Size = 302

Visibility Architecture Challenges

As with any technology, IT and security organizations encounter issues that challenge their ability to achieve their goals with network visibility architectures. **Figure 6** reveals that the top issues are scalability and complexity. Organizations are struggling to match the scale of their visibility solutions to the sheer volume of traffic they need to analyze off their networks. Also, complexity increases as companies embrace the cloud and add new on-premises solutions, such as network virtualization and cloud-native application architectures. Less successful users of visibility architecture identified three other challenges that are particularly troubling to them: insufficient budget, architectural complexity, and limited cloud visibility. Europeans were more likely than North Americans to select budgets as an issue.

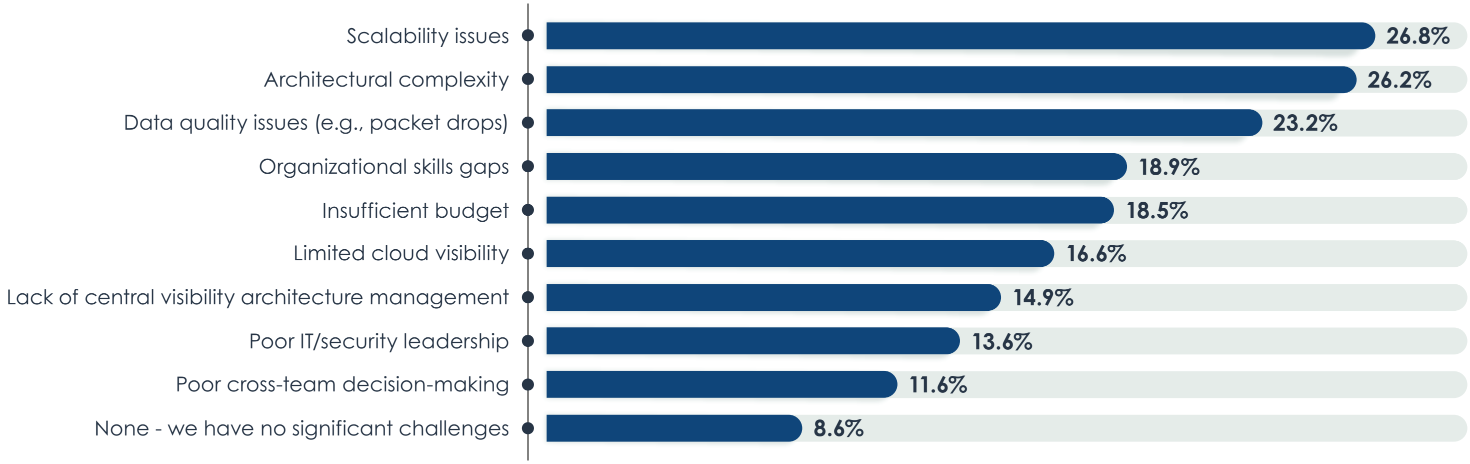
An enterprise monitoring systems engineer with a Fortune 500 healthcare company saw budgeting as a major issue. "People are questioning the expense of this technology—and not just the packet brokers, but all the TAPs that feed into them. I think it's partly due to how we incentivize our network engineers. They are focused on getting networks up and running, but they don't care about day 2 operations."

Poor cross-team decision-making is an infrequent challenge overall, but members of network teams and data center operations teams see it as one of their biggest issues. Security teams and the IT executive suite do not, suggesting which teams are failing to come together.

"We have to talk to other groups, and communication is not always an IT person's strong suit," said an enterprise monitoring systems engineer with a Fortune 500 healthcare company. "You've got to talk to them and get their requirements. We do not give administrative access to other groups."

Technical staff were more likely to perceive skills gaps, poor IT leadership, and budget shortfalls, while middle management was more likely to perceive problems with data quality and central architecture management. In general, larger companies also struggled more often with a lack of central management for visibility architecture.

A senior information security engineer with a Fortune 500 healthcare company noted that visibility vendors need to be more open with their technologies in general. "I would say network packet brokers are too much of a black box. It takes too long for customer service to resolve a problem."



Sample Size = 302,
Valid Cases = 302
Total Mentions = 540

Figure 6. Top challenges that companies encounter when using network visibility architecture technology

The Access Layer of Visibility Architecture

To qualify for this research, survey participants had to verify that they use network packet broker appliances. With their high-capacity hardware and full-featured software, packet brokers are the heart of a visibility architecture, but they are not the only critical component. These devices receive multiple flows of mirrored traffic from various parts of the network. The technology used to mirror this traffic is essential to a successful visibility architecture. These components form the access layer of the architecture.

Mirroring Network Traffic From Physical Infrastructure

TAPs Versus SPANs

On a physical network, there are two primary options for mirroring traffic onto a visibility architecture. Engineers can configure an interface on a network device as a switched port analyzer (SPAN). SPAN ports are a cheap option since no additional hardware or software is required, but they are less reliable. Typically, the SPAN port function is a low priority for a switch. During times of high utilization, the switch will devote its resources production traffic. SPAN ports often drop packets when this happens. They also require manual configuration, which adds to management complexity.

The other option is a test access port (TAP): a dedicated, purpose-built device that passively copies traffic as it crosses the wire. TAPs are more reliable and potentially easier to manage, but also more expensive.

Most companies use a mix of TAPs and SPANs to mirror traffic onto a visibility architecture. The more TAPs they use, the more reliable and manageable their visibility architecture. This research found that only 30% of companies use TAPs for the majority of their traffic mirroring today. Another 37% have roughly a 50/50 split of TAPs and SPANs. Nearly 31% have a majority of SPANs.

EMA research has been tracking these numbers for years. **Figure 7** reveals that companies have slid toward using mostly SPANs for traffic mirroring over the last four years. In 2018, 49% of companies had mirrored most of their traffic with TAPs and in 2020, 45% of companies relied mostly on TAPs. Now, only 30% use mostly TAPs. Larger companies and operators of larger networks were more likely to use SPAN ports for most of their traffic mirroring.

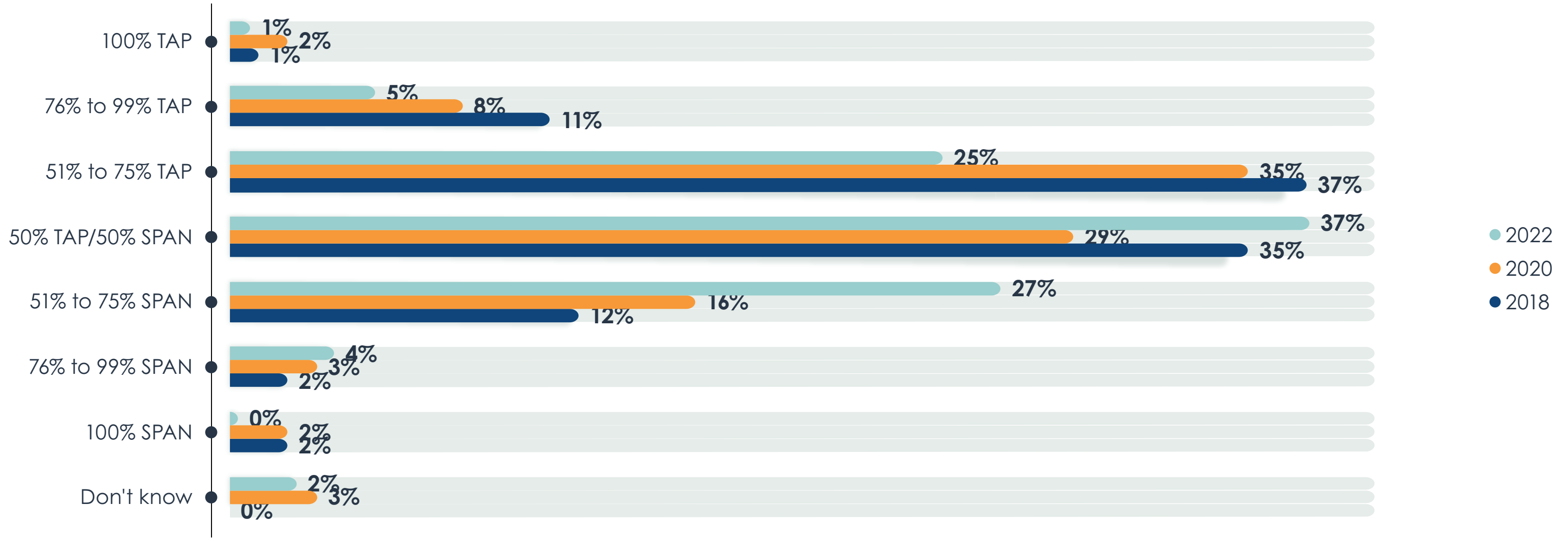


Figure 7. In your organization's visibility architecture, what percentage of port mirroring is accomplished via SPAN ports versus TAPs?

Benefits of TAPs Over SPANs

Figure 8 reveals the top reasons why organizations choose to mirror traffic with a TAP rather than a SPAN port. The biggest opportunity is improved administrative overhead. TAPs are easier to manage, usually via a central console offered by the TAP vendor. Management of those TAPs can also integrate with management of the rest of a visibility architecture, including network packet brokers and software probes. Companies that are the most successful with visibility architecture were much more likely focus on management.

The second driver is data quality. With dedicated resources to traffic mirroring, TAPs—especially premium-quality TAPs—do not drop packets. Security analysis solutions are especially sensitive to missed packets, so this benefit is essential. IT executives were the most likely to select this benefit.

The lowest-priority benefit is reduced resource consumption on network devices, which makes sense since most switches will simply stop mirroring traffic via a SPAN port if the process is contending with resources required for receiving and forwarding production traffic. Less successful users of visibility architectures were the most likely to think this is an important benefit.

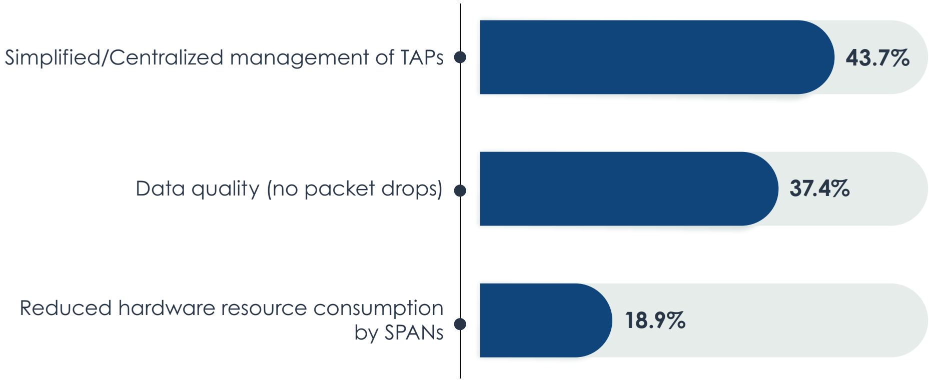
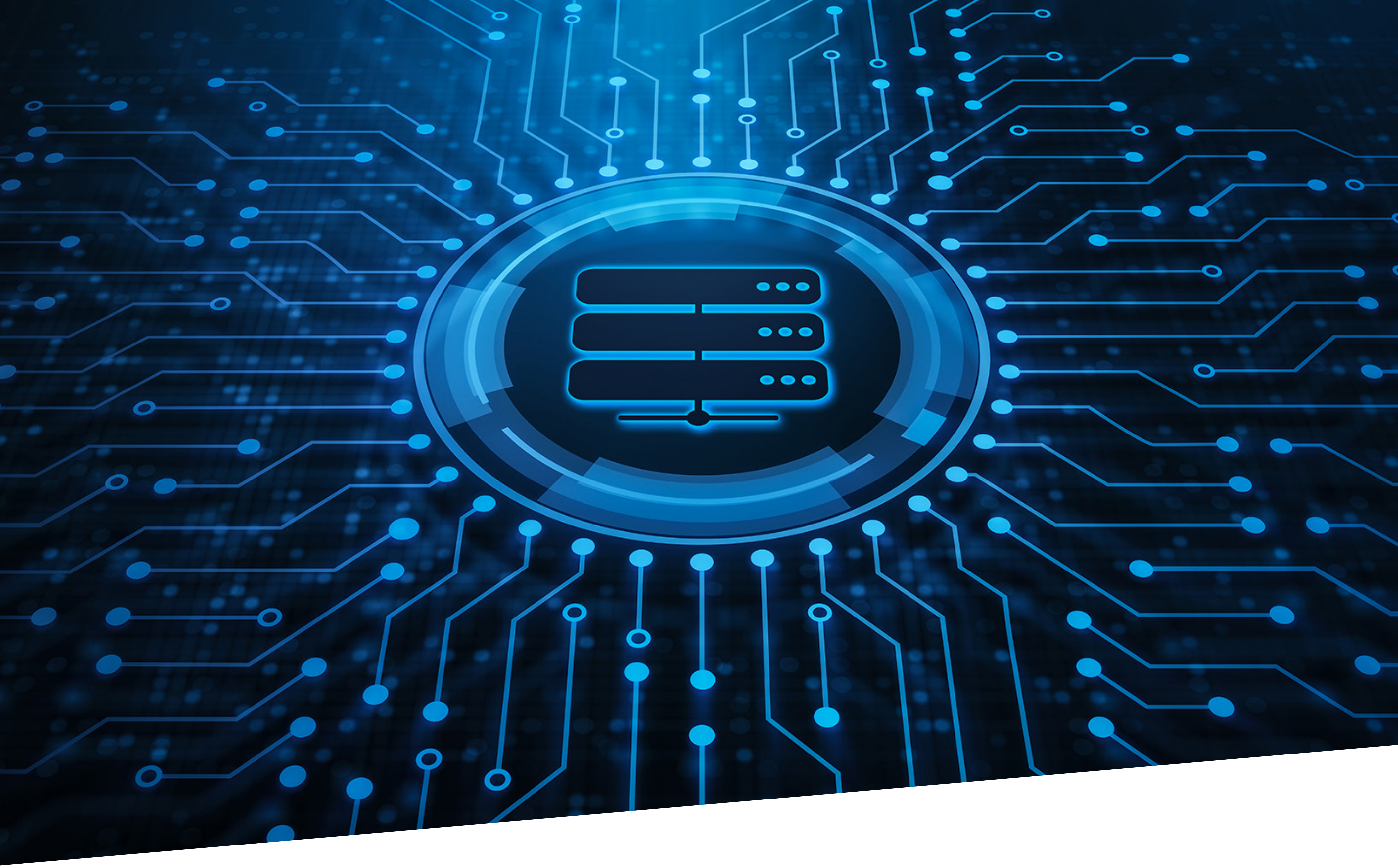


Figure 8. Most compelling reasons for using TAPs over SPAN ports when mirroring traffic onto a visibility architecture

Sample Size = 302



The Architectural Core: Network Packet Brokers

Network packet brokers, whether an appliance or a software solution for the public cloud, remains at the heart of any visibility architecture. This section explores the requirements that companies have for these solutions moving forward.

Platform Characteristics That Drive ROI

EMA asked research respondents to identify the one general platform characteristic of a network packet broker that is most important to earning a return on investment in the technology. The top response, as **Figure 9** reveals, was advanced features, such as packet filtering, manipulation, and metadata generation. EMA believes this is especially important as software-based packet brokers become more relevant in virtual infrastructure and cloud-based infrastructure removes hardware as a platform differentiator. The IT executive suite and security teams were more likely to select advanced features, while network infrastructure and operations teams and data center operations teams, who may still maintain a hardware mindset, were less likely to select advanced features.

Instead, network teams and data center operations teams were more likely to select the second priorities: resilience and reliability, which security teams were less concerned about. Manageability and automation were the third leading platform priorities. Technical staff (engineers, architects, analysts) were much more likely to select manageability, while middle management and executives were not particularly concerned with it.

An enterprise systems monitoring engineer with a Fortune 500 healthcare company offered a long list of platform requirements that he thinks about when evaluating solutions. “Performance is number one for me. Then it’s ease of upgrades. We think about the longevity and stability of the company, too. I also want to know if their customer support is any good. Packet broker management tools are also very important if you have an enterprise-scale deployment.”

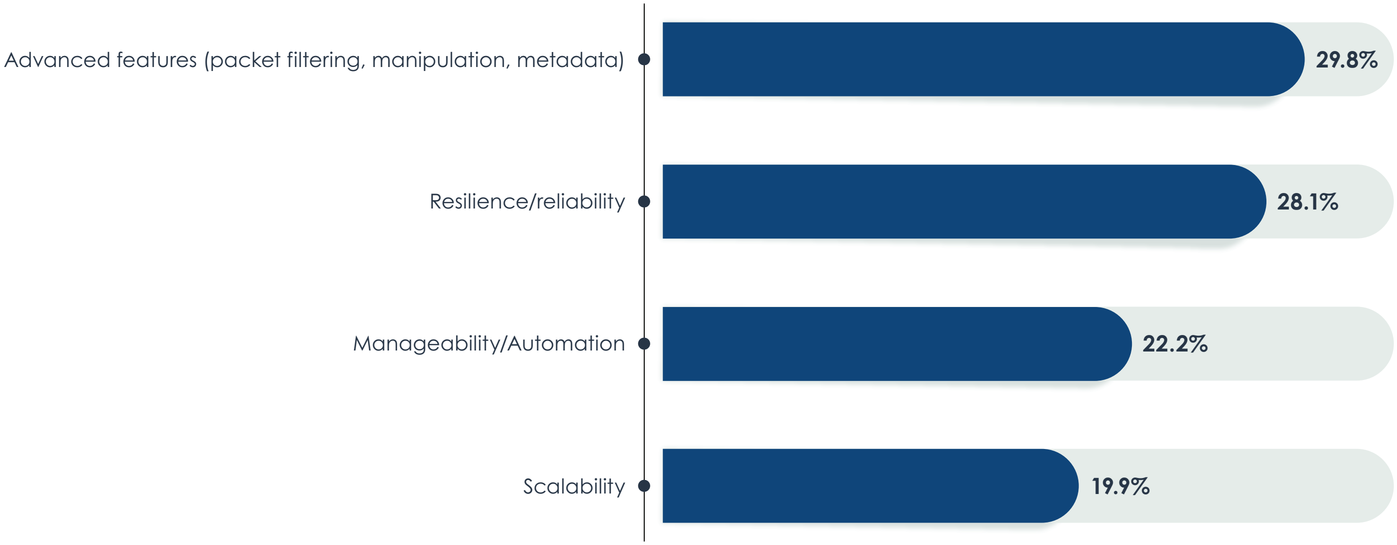


Figure 9. Platform characteristics most important return on investment in network packet brokers and related technology

Sample Size = 302

Critical Packet Manipulation and Data Generation Features

Figure 10 reveals how critical network packet brokers have become to cybersecurity. The most valued packet manipulation or data generation feature in a packet broker is threat intelligence. This is a relatively new capability for packet brokers and only a select few vendors offer it today. Organizations that are the most successful with visibility architecture were the most likely to value threat intelligence, suggesting that it's a best practice to seek this capability from packet broker vendors.

"Threat insights, if they are actionable, look like a value-add to me," said an enterprise monitoring systems engineer with a Fortune 500 healthcare company. "As long as they do the analysis in the cloud so I don't have to host it on-premises, and they keep it up to date."

Decryption leads the list of secondarily important features. This finding reflects the rising global ubiquity of encrypted traffic. Many security and performance analysis tools need access to packet payloads, and packet brokers remain an ideal option for providing that access to tools.

NetFlow, packet metadata generation, packet slicing, and masking are the other secondary priorities. Cloud engineering and operations teams were especially likely to prioritize masking.

Companies that use three or more cloud providers showed more interested in header stripping and geolocation tagging, which are tertiary priorities for most companies. Another low-priority feature, flow slicing, drew more interest from operators of larger networks (1,000 or more network devices under management).

The most valued packet manipulation or data generation feature in a packet broker is threat intelligence.

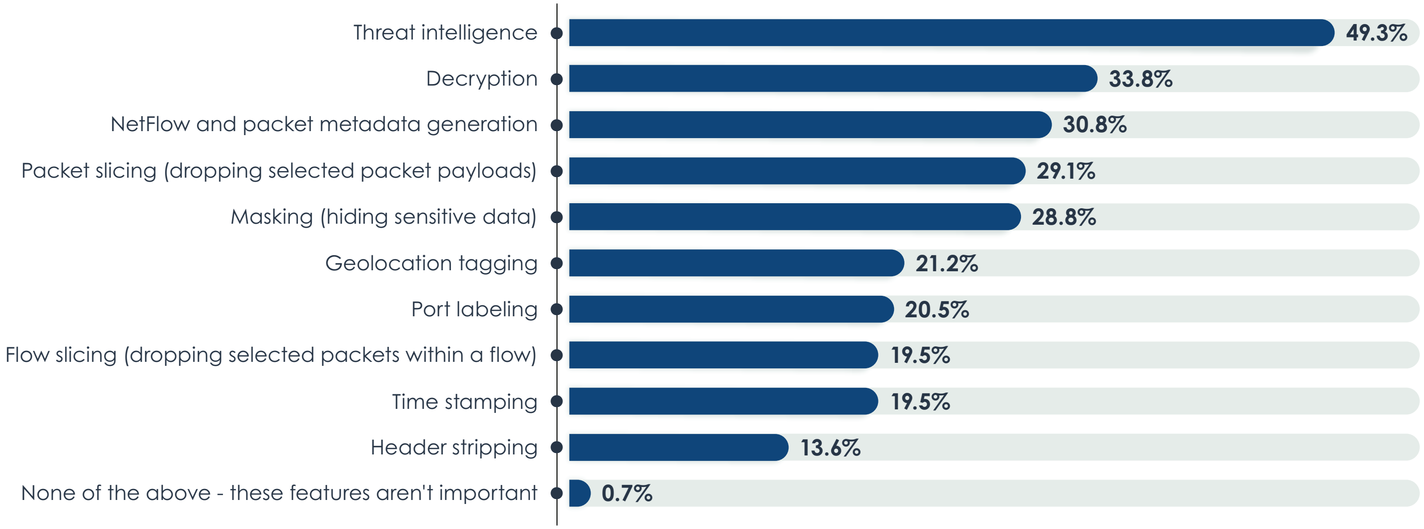


Figure 10. Packet manipulation and data generation features that are most valuable in a network packet broker

Sample Size = 302, Valid Cases = 302, Total Mentions = 806

Supporting Hybrid, Multi-Cloud Visibility

The Importance of Packet Data to Cloud Operations

This research found that packet data is essential to cloud operations, especially for security monitoring and analysis.

Packet Data is Essential to Security Monitoring and Analysis in the Cloud

Figure 11 reveals how survey respondents ranked the value of packet data to security monitoring and analysis in the cloud. Nearly 65% say this data is very important to this practice. Only 10% consider it unimportant. Organizations that are the most successful with their use of visibility architecture were the most likely to believe packet data is very important for cloud security.

Members of security teams and people who work within an IT executive suite are the most convinced of packet data's value to cloud security monitoring and analysis. Network infrastructure and operations and cloud operations professionals are the least convinced. Respondents who work for midmarket and large enterprises were very likely to value this data for cloud security, but people from very large enterprises (10,000 or more employees) were less likely to feel this way. North Americans are more likely than Europeans to recognize the importance of packets to cloud security.

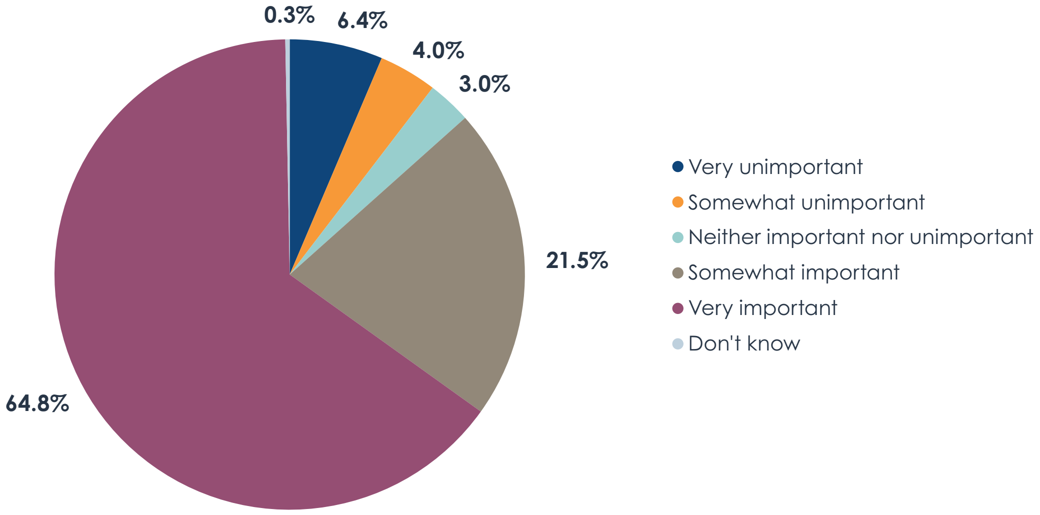


Figure 11. The importance of packet data to security monitoring and analysis in the cloud

Sample Size = 298

Packet Data is Essential to Performance Management in the Cloud

Figure 12 reveals that more than half of companies believe that packet data is very important to performance management in the cloud. This enthusiasm is a little less ubiquitous than it is for security monitoring and analysis. Respondents who reported the highest levels of success with visibility architecture were more likely to see the importance of packets to performance management in the cloud.

"We work with almost every cloud provider out there, and we have a project right now aimed at gaining specific visibility there," said a senior information security engineer with a Fortune 500 healthcare company. "It's not driven by security, but it's for troubleshooting."

Members of security teams and IT project management teams are most likely to see the importance of packets for cloud performance analysis, but network infrastructure and operations teams are less likely. IT executives were more likely than middle managers and technical staff to identify packets as important to cloud performance management, and North Americans were more likely than Europeans.

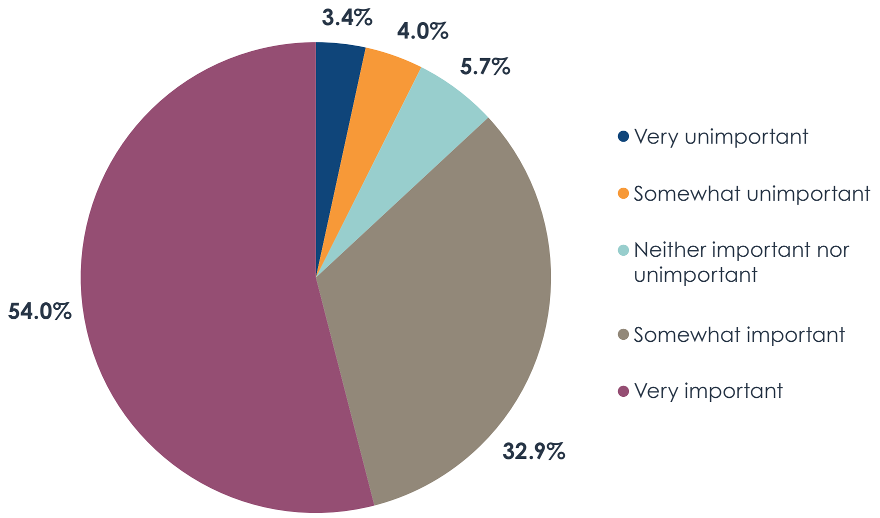


Figure 12. The importance of packet data to performance management in the cloud

Packet Data is Essential to Capacity Management in the Cloud

Figure 13 reveals that exactly half of respondents believe that packet data is very important to cloud capacity management. Enthusiasm for using packets for this use case is lower than it is for performance management and security monitoring and analysis. Still, the vast majority of companies perceive at least some value to using packets for this purpose.

Successful users of visibility architecture were the most likely to perceive the importance of packet data for capacity management in the cloud. Middle management in IT was more likely to perceive the value than technology executives and technical staff. North Americans perceived its value more than Europeans did.

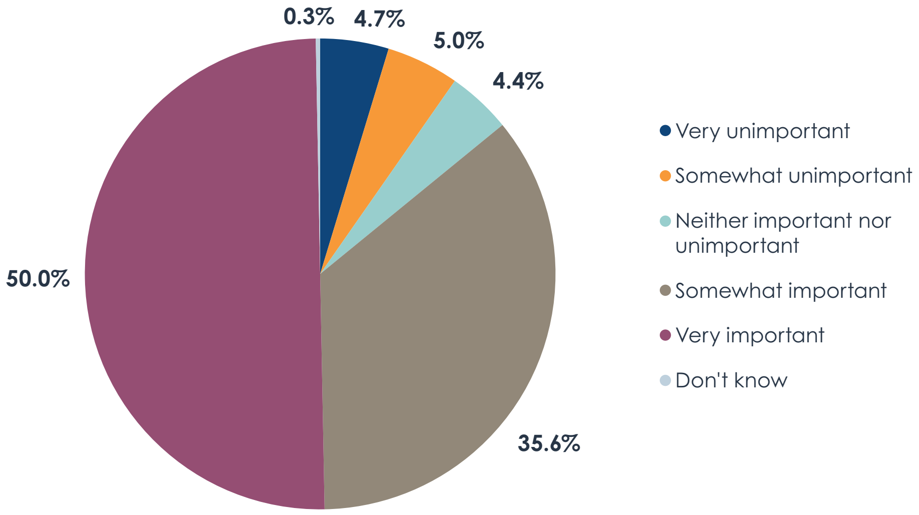


Figure 13. The importance of packet data to capacity management in the cloud

Sample Size = 298

Cloud-Related Network Blind Spots

More than 46% of the IT professionals surveyed for this research reported that the migration of applications to the public cloud created blind spots in their network, places where they are unable to collect data for performance and security analysis, as **Figure 14** indicates. Another 4% said they were unsure if they had cloud-related network blind spots. Companies that report the most success with their visibility architectures were the least likely to experience these blind spots, suggesting that an effective approach to hybrid, multi-cloud visibility can mitigate these blind spots.

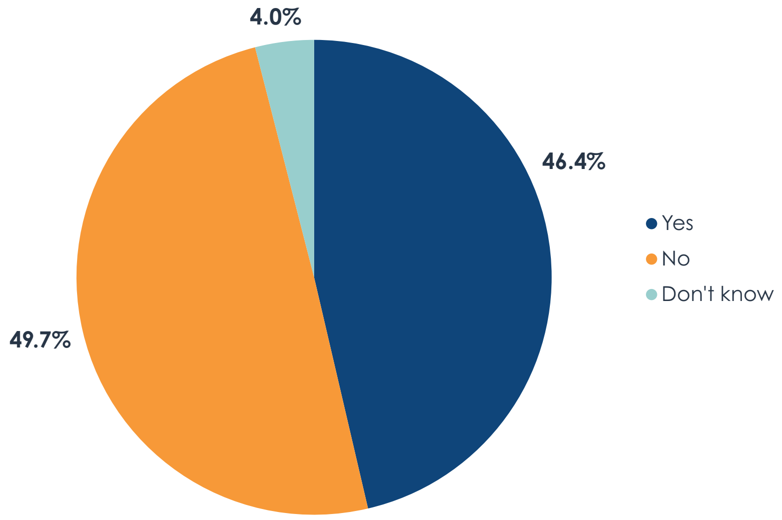


Figure 14. Has the migration of applications to the public cloud created any blind spots in your organization's network?

Members of cloud operations teams, data center operations teams, and people working in IT executive suites were all more likely to perceive these blind spots. Members of network engineering and security groups were less aware of such problems. Overall, technical staff are more likely to report blind spots, while IT middle management and executives are less likely.

Multi-Cloud Networks Struggle More

Figure 15 reveals that multi-cloud companies are more likely to experience blind spots. Using multiple cloud providers adds operational complexity, and the tools and services that individual providers offer for visibility are highly proprietary, making it extremely difficult for some companies to create an end-to-end solution for monitoring multi-cloud performance and security.

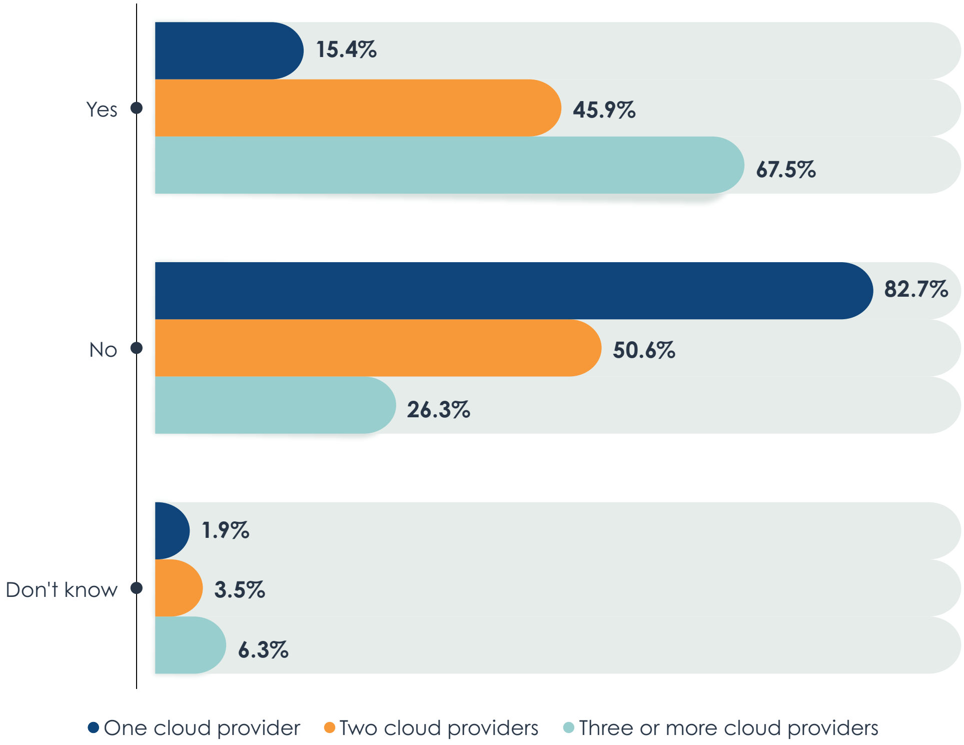


Figure 15. Has the migration of applications to the public cloud created any blind spots in your organization's network? By number of cloud providers in use

Sample Size = 302

Visibility Solutions for the Cloud

Acquiring Cloud Traffic Data

99% of companies are making at least some attempt to collect packet data in the cloud.

Figure 16 reveals that 99% of companies are making at least some attempt to collect packet data in the cloud and supply it to performance and security analysis tools. Less than 40% rely primarily on the native traffic mirror services of cloud providers. More than 60% are using third-party software from visibility vendors to acquire this data.

"If you want to deploy analysis tools in the public cloud, you will need the services of a cloud-deployed network packet broker," said an information security engineer with a managed security services provider.

Network visibility architecture solutions "can definitely offer value in the cloud, because you need that network traffic when you're doing end-to-end transactions. Without a packet broker in the cloud, I could deploy a fleet of Linux servers in the cloud running TCPDUMP, but that would be too costly," said an infrastructure analyst with a Fortune 500 energy company.

Companies in the financial services, construction and civil engineering, energy and utilizes, and retail industries were all more likely to use third-party visibility software. Healthcare companies were more likely to use native cloud provider services. Members of network infrastructure and operations, security, and data center operations teams all indicated a preference for third-party software. Cloud operations teams and IT executives preferred native cloud services.

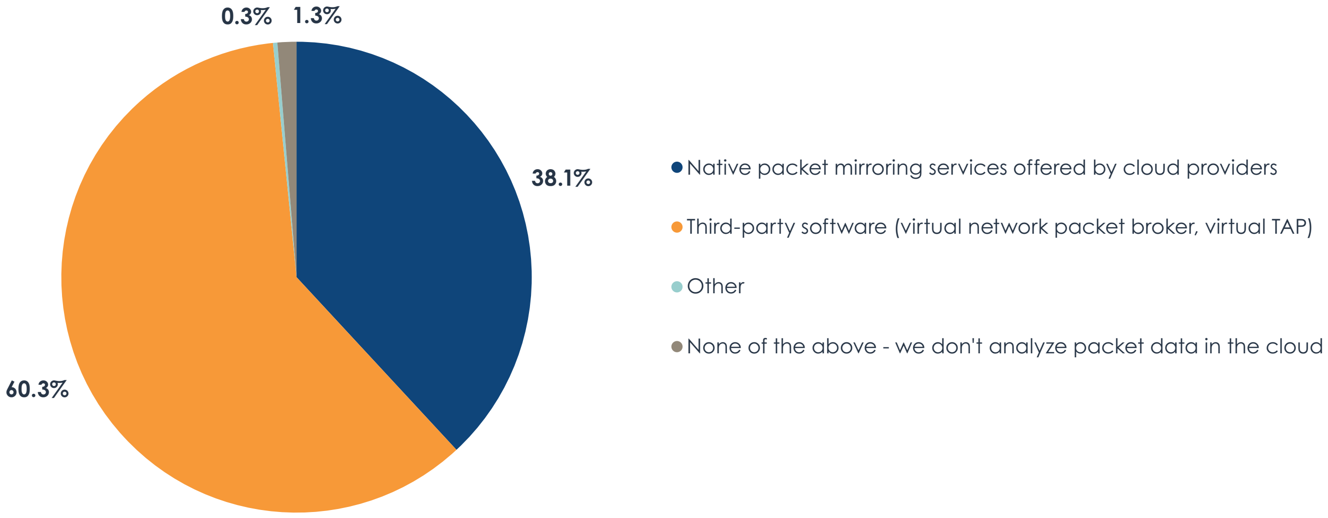


Figure 16. Primary method for supplying cloud-related network packet data to security and performance analysis tools

Sample Size = 302

The Benefits of Using Third-Party Visibility Software in the Cloud

With the majority of companies preferring to use third-party visibility software in the cloud, such as virtual network packet broker software, EMA asked all respondents to identify the most compelling benefits of this approach to acquiring packet data in the cloud.

Figure 17 reveals that only 1% find no compelling benefits to using this software in the cloud. The biggest payoff is the reliability of data collection. Specialized software is better at acquiring data without packet drops and errors across multiple cloud providers.

All other potential benefits, with improved administrative security and overall manageability and automation of visibility solutions, offer the most compelling opportunities. Organizations that are the most successful with visibility architecture were twice as likely as others to selected advanced packet filtering and modification features as an important benefit. Very large companies (10,000 or more employees) identified integration with on-premises visibility architecture as a very important benefit.

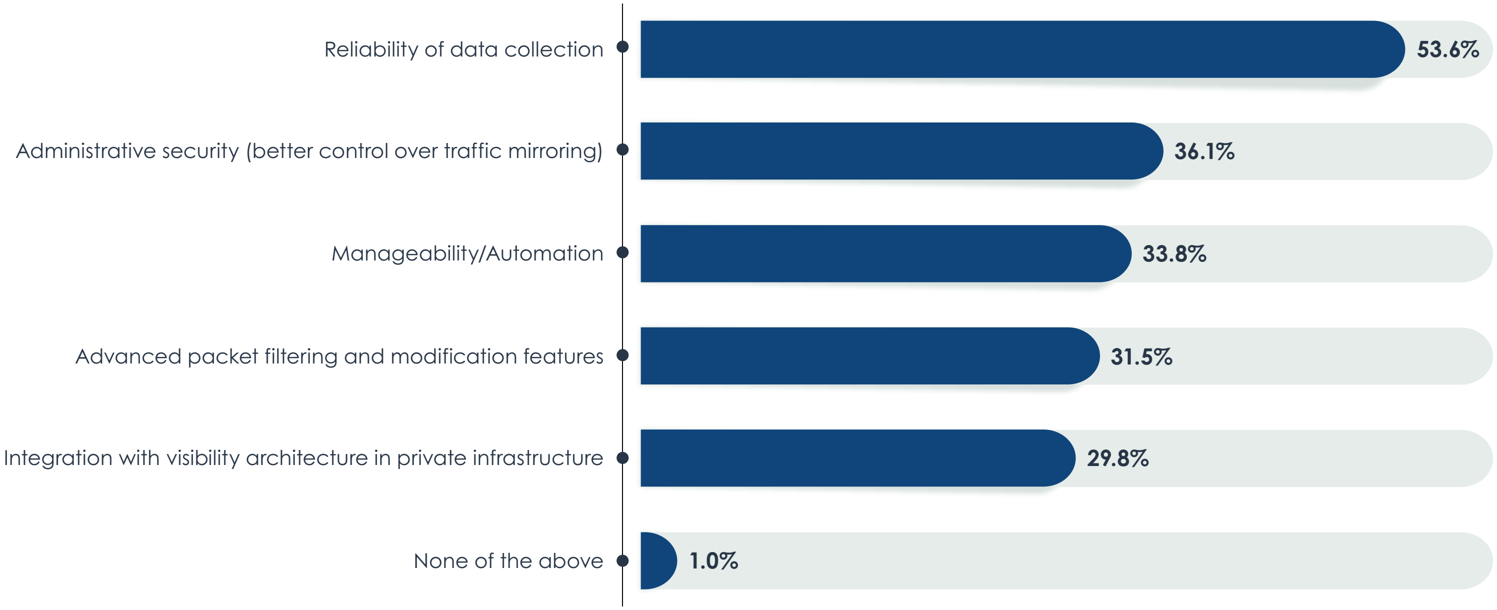


Figure 17. The most compelling benefits of using third-party visibility software (e.g., network packet broker software) in the cloud rather than a cloud provider's native packet mirroring service

Sample Size = 302, Valid Cases = 302, Total Mentions = 561

End-to-End Hybrid-Cloud Visibility Architecture

The visibility solutions that a company uses in its cloud environments should not be siloed from the rest of an organization's visibility architecture. **Figure 18** reveals that nearly 87% of organizations believe it is at least somewhat important to establish a single visibility architecture that spans physical, virtual, and cloud-based networks.

The IT executive suite was especially convinced of the importance of this end-to-end visibility architecture. Data center operations and network teams were less convinced. North Americans were more likely than Europeans to recognize its importance.

87% of organizations believe it is at least somewhat important to establish a single visibility architecture that spans physical, virtual, and cloud-based networks.

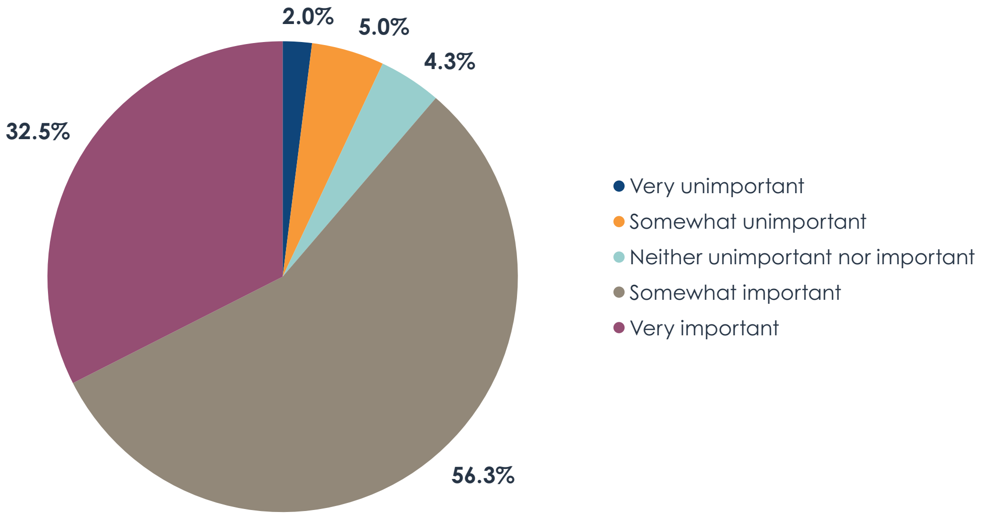


Figure 18. The importance of building a single visibility architecture that spans physical, virtual, and cloud-based networks

Sample Size = 302

Figure 19 suggests that an end-to-end approach to visibility architectures across on-premises and cloud infrastructure is a best practice. The most successful organizations are the most likely to recognize its importance. The least successful organization were the most likely to believe this end-to-end approach is unimportant.

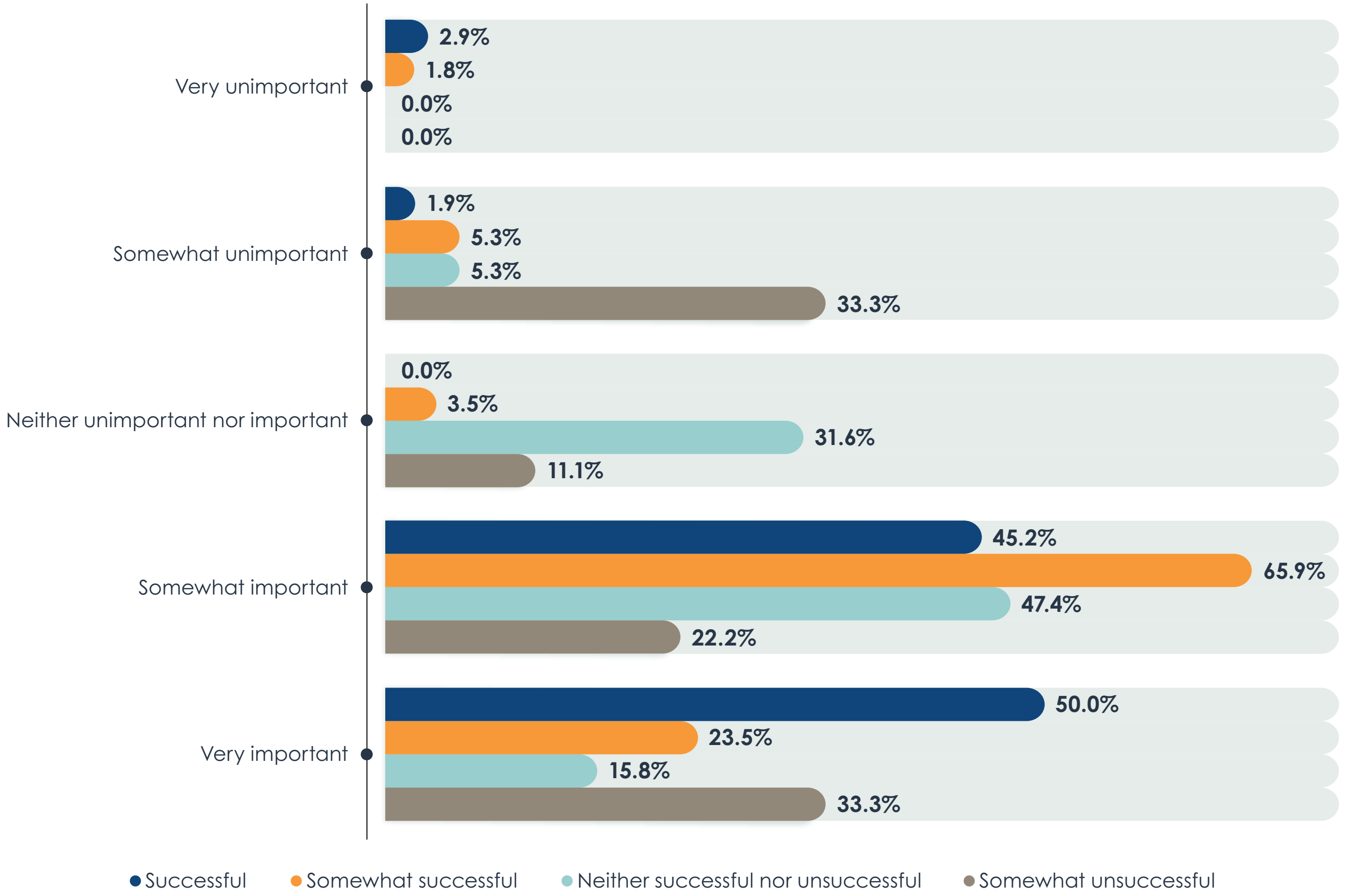


Figure 19. The importance of building a single visibility architecture that spans physical, virtual, and cloud-based networks, by success with visibility architectures

Sample Size = 302

Trends in Traffic Data

The Problem of Encrypted Traffic

Encryption is becoming ubiquitous across networks. Internet companies like Google encrypt traffic associated with most of their services to protect the privacy of users. Enterprises encrypt traffic to protect sensitive data. Malicious actors encrypt traffic to hide their attacks. Encryption obscures payloads and undermines the effectiveness of security and performance analysis tools.

EMA asked research participants to estimate how much of the malicious activity detected on their networks was hidden within encrypted traffic. In the average company, 27% of detected malicious network activity is found in encrypted traffic. EMA suspects that the true number is higher than 27%, but companies are failing to detect the full extent of encrypted attacks.

EMA also believes that an effective network visibility architecture can help companies uncover more encrypted malicious activity on networks. **Figure 20** confirms this. Successful companies are detecting more encrypted malicious traffic than somewhat successful companies and companies that are uncertain of their success (EMA did not find a statistically significant difference in responses form unsuccessful companies).

Companies that use three or more cloud providers also reported a higher frequency of encrypted malicious traffic. It's impossible to know for certain why this correlation emerged, but EMA suspects it reflects the larger attack surface associated with using multiple providers. Technical staff reported a higher percentage of malicious traffic than middle management and IT executives, suggesting that people further up the chain of command are unaware of how serious the problem is.

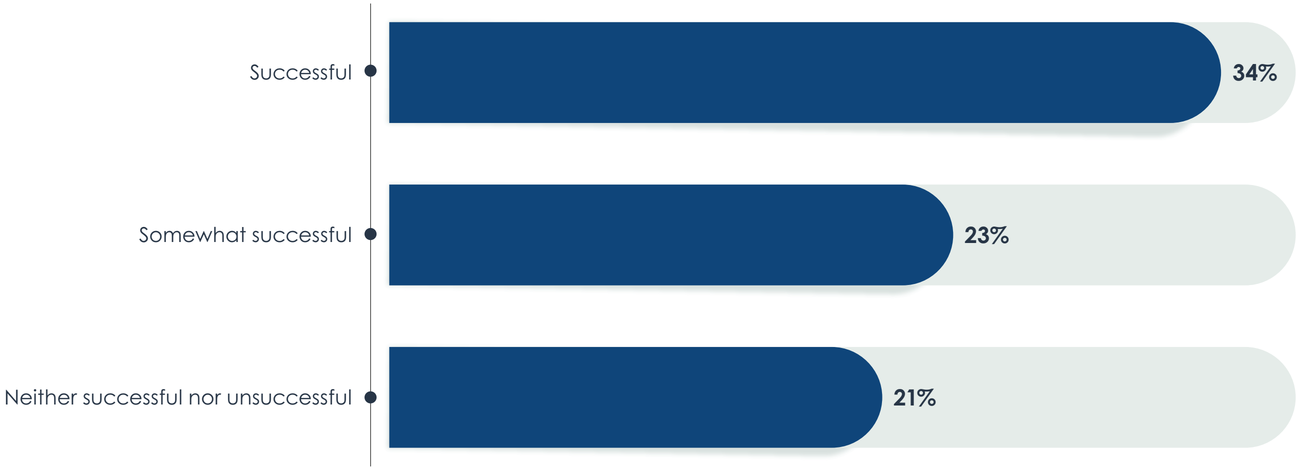


Figure 20. Percentage of the malicious activity detected on networks over the last year that was hidden within encrypted traffic, by overall success with network visibility architectures

Sample Size = 302

The most popular method for decrypting traffic is by using individual security and performance analysis tools. This is the most inefficient strategy for traffic decryption.

Preferred Methods for Decryption

Figure 21 reveals that 98% of companies attempt to decrypt at least some traffic for analysis. It also reveals that the most popular method for decrypting traffic is by using individual security and performance analysis tools. This is the most inefficient strategy for traffic decryption. First, this leads to redundancy, since multiple tools will decrypt the same flows of traffic. Second, the decryption process leaches resources from the tools' primary analysis function. IT executives and project and program management professionals were the most likely to prefer this method. Members of cloud operations and security teams were most averse to decrypting traffic on their analysis tools.

"If you're looking for suspicious traffic, you've got to be able to read into that payload," said an infrastructure analyst with a Fortune 500 energy company. "Otherwise, all you're left with is determining the risk based on source and destination information."

More than one-quarter of companies prefer to decrypt traffic on the network packet broker. Many vendors, but not all, offer this feature. Companies that use multiple cloud providers were more likely to prefer this method. Dedicated encryption appliances and packet capture appliances are less popular, as are application delivery controllers. Data center operation teams and security teams were the most likely to prefer decrypting on a packet capture appliance.

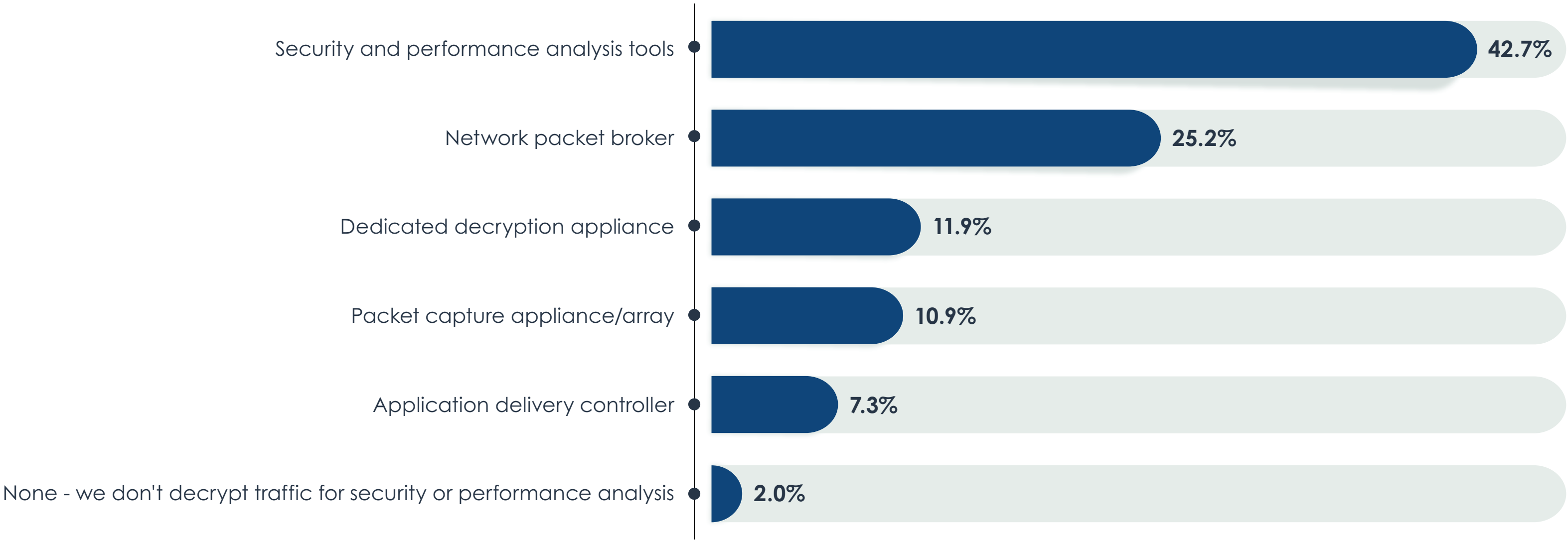


Figure 21. Preferred resource for decrypting TLS/SSL traffic for inspection by security and performance analysis tools

Sample Size = 302

Packets and Observability Data

Observability is a concept most associated with DevOps and cloud operations, but network operations and security operations teams are increasingly interested in the concept. In the context of DevOps, observability is about understanding the state of an application by extracting data from the application environment. The pillars of observability data are metrics, events, logs, and traces (MELT).

Network and security teams often try to manage their environments from an application perspective to better understand how their domain of responsibility is interacting with critical business applications. Thus, there is increased interest in combining analysis of traffic data (e.g., packets) with MELT data for more contextualized network performance and security insights.

Figure 22 reveals that nearly 60% of companies are combining their analysis of MELT data and packet data today. Nearly 37% are planning to do this in the future. Companies that are the most successful with their network visibility architectures are the most likely to be performing this combined analysis today. Interest in this practice is also the highest combined across multi-cloud companies.

60% of companies are combining their analysis of MELT data and packet data today. Nearly 37% are planning to do this in the future.

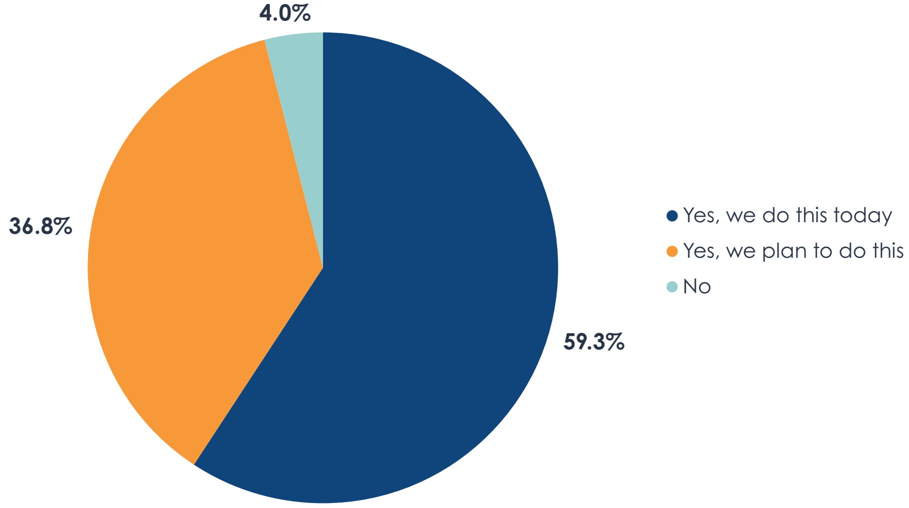


Figure 22. Is your organization interested in combining packet analysis with analysis of observability data?

Sample Size = 302

Conclusion

This research made it clear that hybrid and multi-cloud architectures are the primary drivers of network visibility strategies today. As companies migrate more applications and data to multiple cloud providers, network visibility architectures will be essential for success. IT organizations should work with their existing visibility vendors to extend these architectures into the hybrid multi-cloud.

Some companies may be tempted to adopt an ad hoc approach to cloud visibility, using the native traffic mirroring services of each service provider to deliver packet data to analysis tools. However, in a true multi-cloud enterprise, only an end-to-end network visibility architecture can ensure that performance and security analysis tools can get a full picture of the global, multi-cloud network. Organizations should extend their on-premises visibility architectures into the cloud by using a mix of software, hardware, and services from their trusted vendors.

Cross-team decision-making and collaboration will be essential to successful multi-cloud visibility architectures. Network, security, cloud, and DevOps teams need to work together to ensure that every team has access to the data they require for successful operations.

If enterprises follow the example of the most successful users of visibility architectures in this research, they can expect to improve overall IT and security team productivity, reduce security risk, and strengthen overall IT operations.

Hybrid and multi-cloud architectures are the primary drivers of network visibility strategies today.

Appendix. Demographics

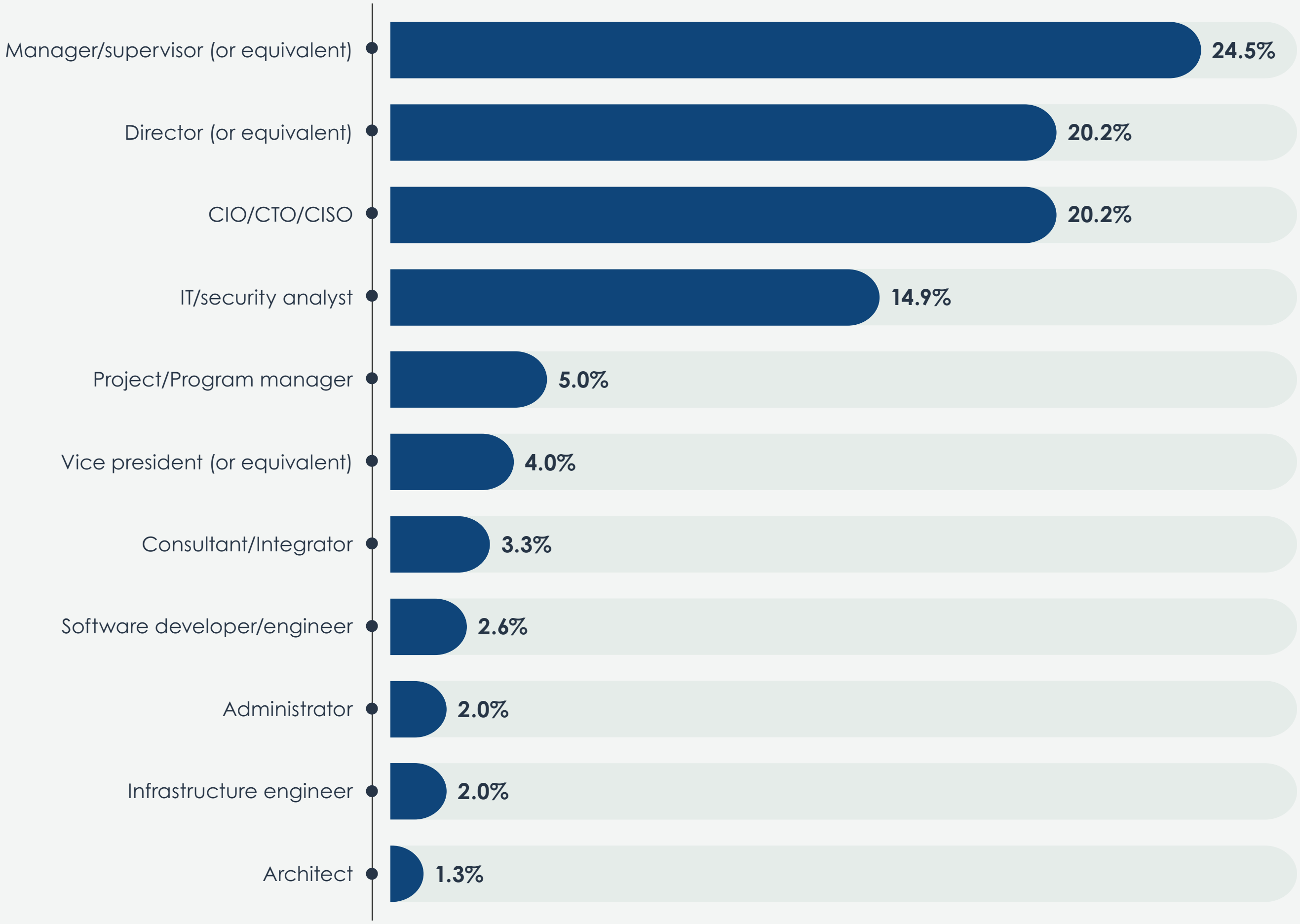


Figure 23. Job titles

Sample Size = 302

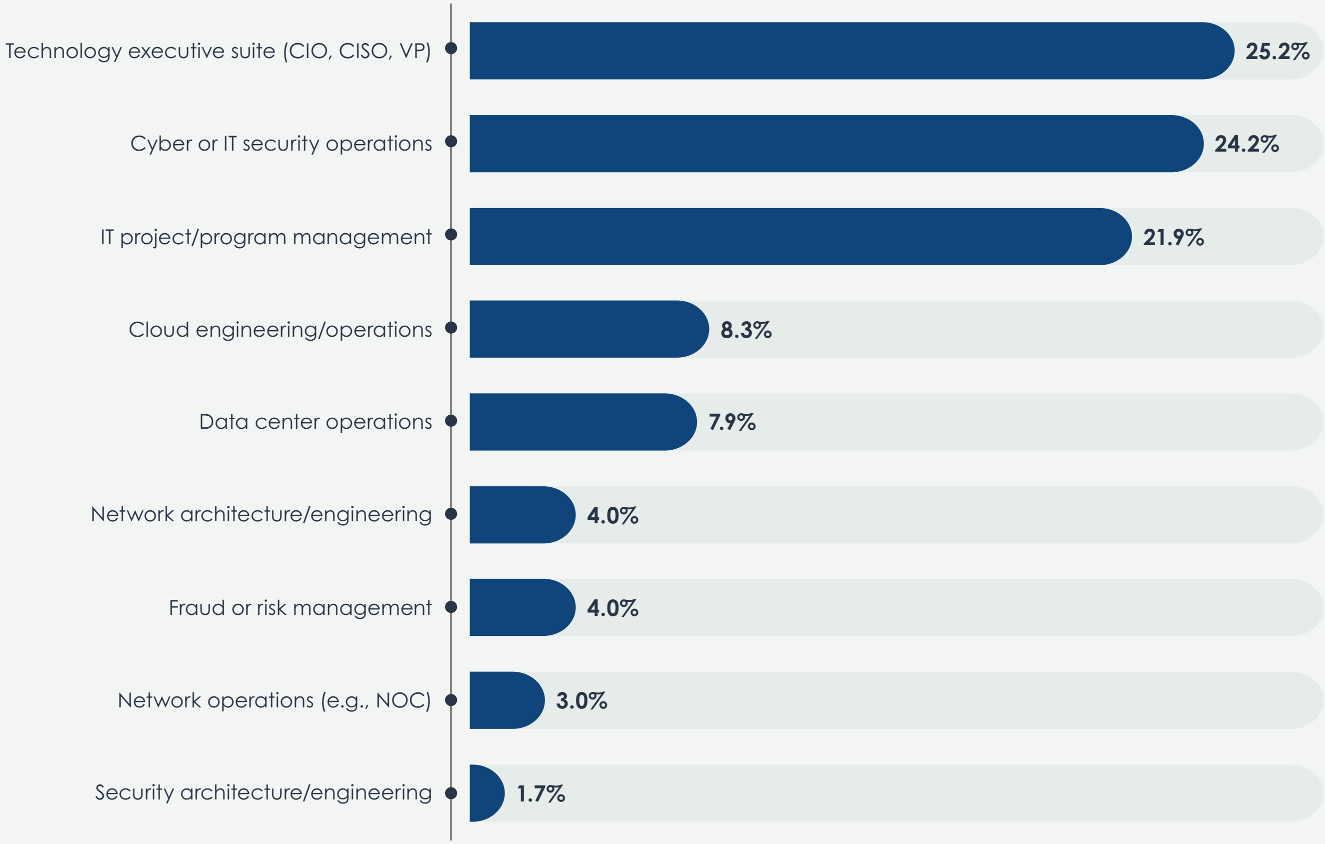


Figure 24. Functional groups in IT or security organization

Sample Size = 302

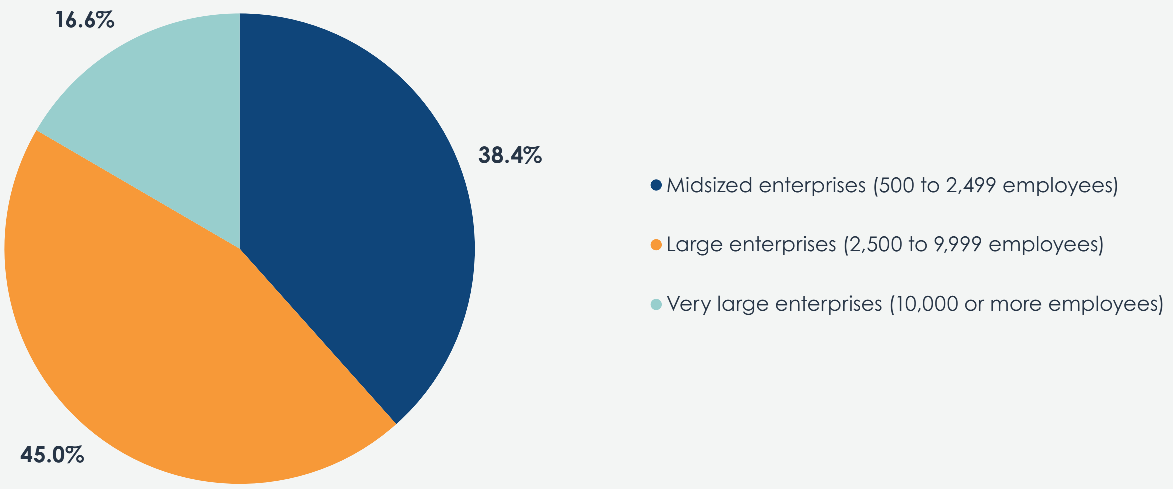


Figure 25. Company size

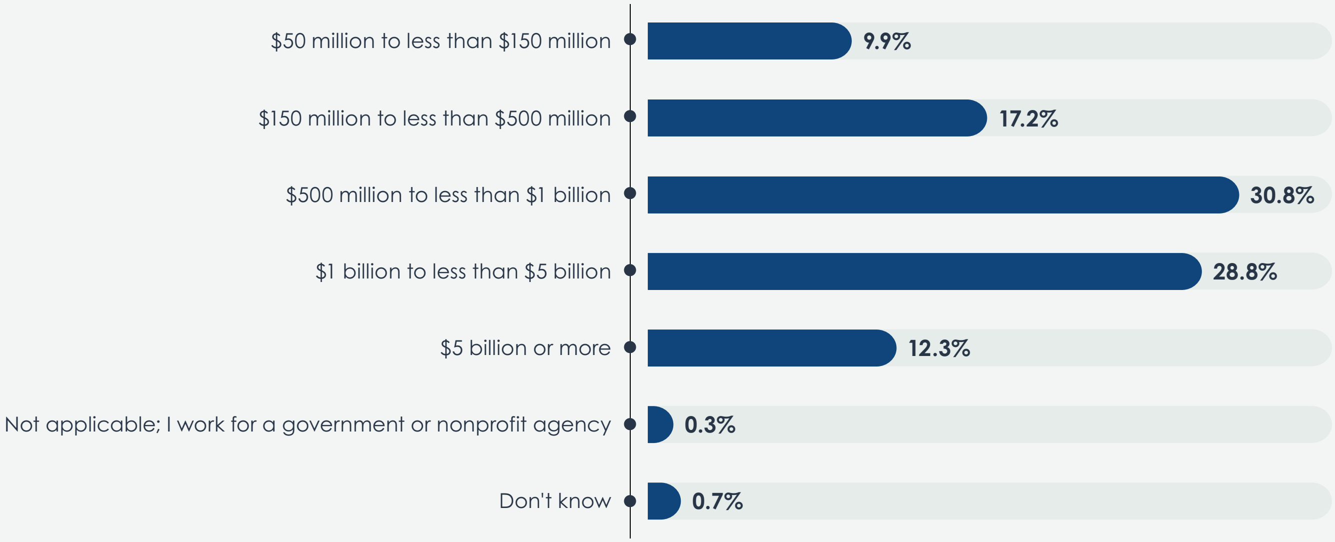


Figure 26. Annual sales revenue

Sample Size = 302

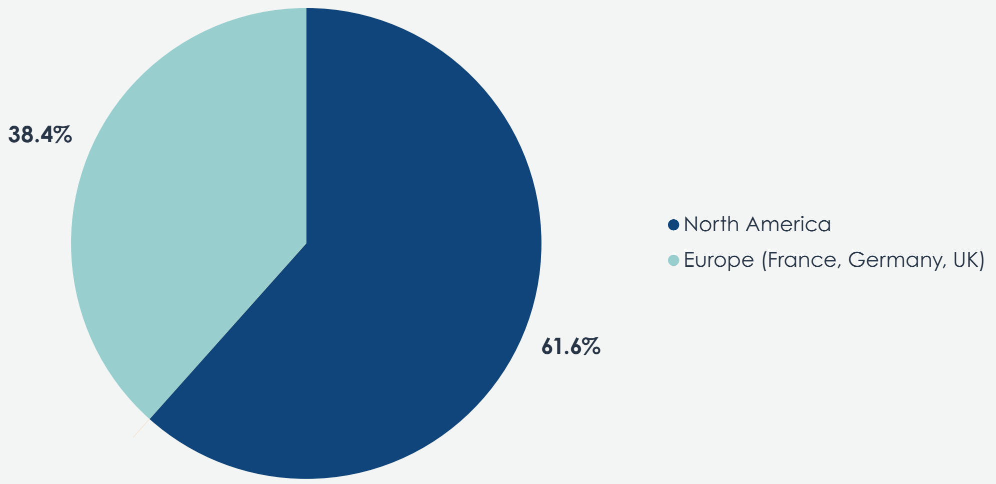


Figure 27. Location

Sample Size = 302

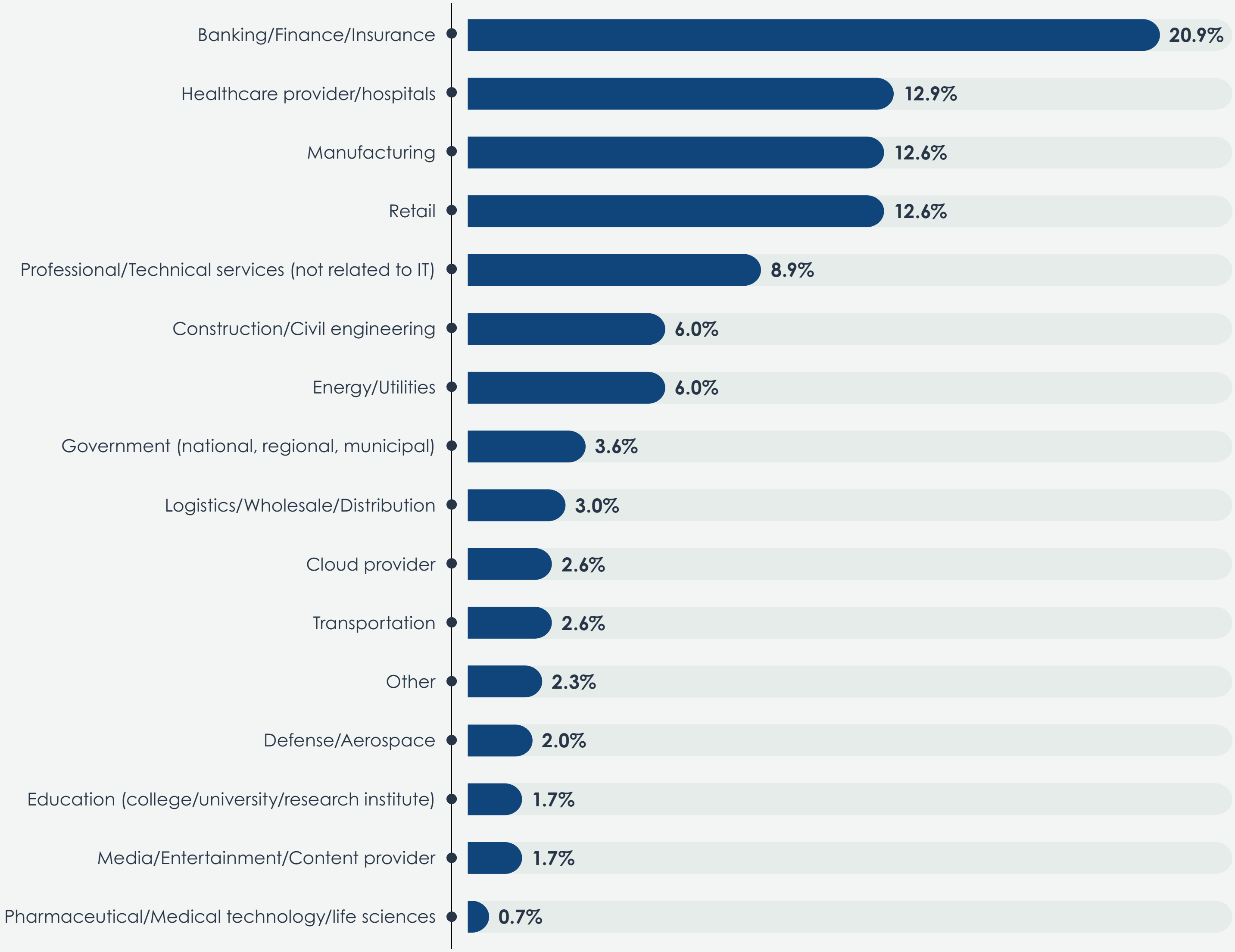


Figure 28. Industry

Sample Size = 302

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**

1995 North 57th Court, Suite 120, Boulder, CO 80301   +1 303.543.9500   **www.enterprisemanagement.com**   4192.070622