EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Prepared for:

infoblox

DDI Directions:

DNS, DHCP, and IP Address Management Strategies for the Multi-Cloud Era

September 2023 EMA Research Report

By **Shamus McGillicuddy**, Vice President of Research
Network Infrastructure and Operations

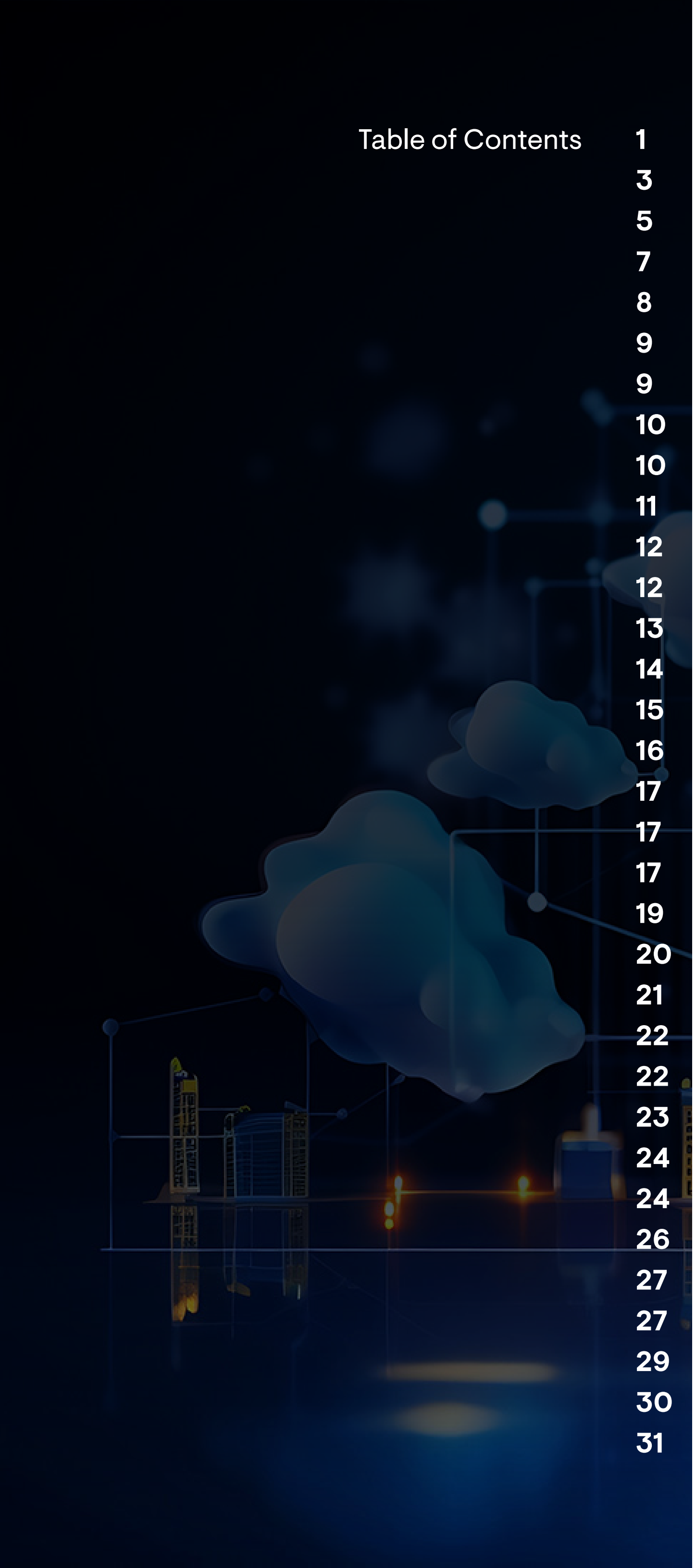
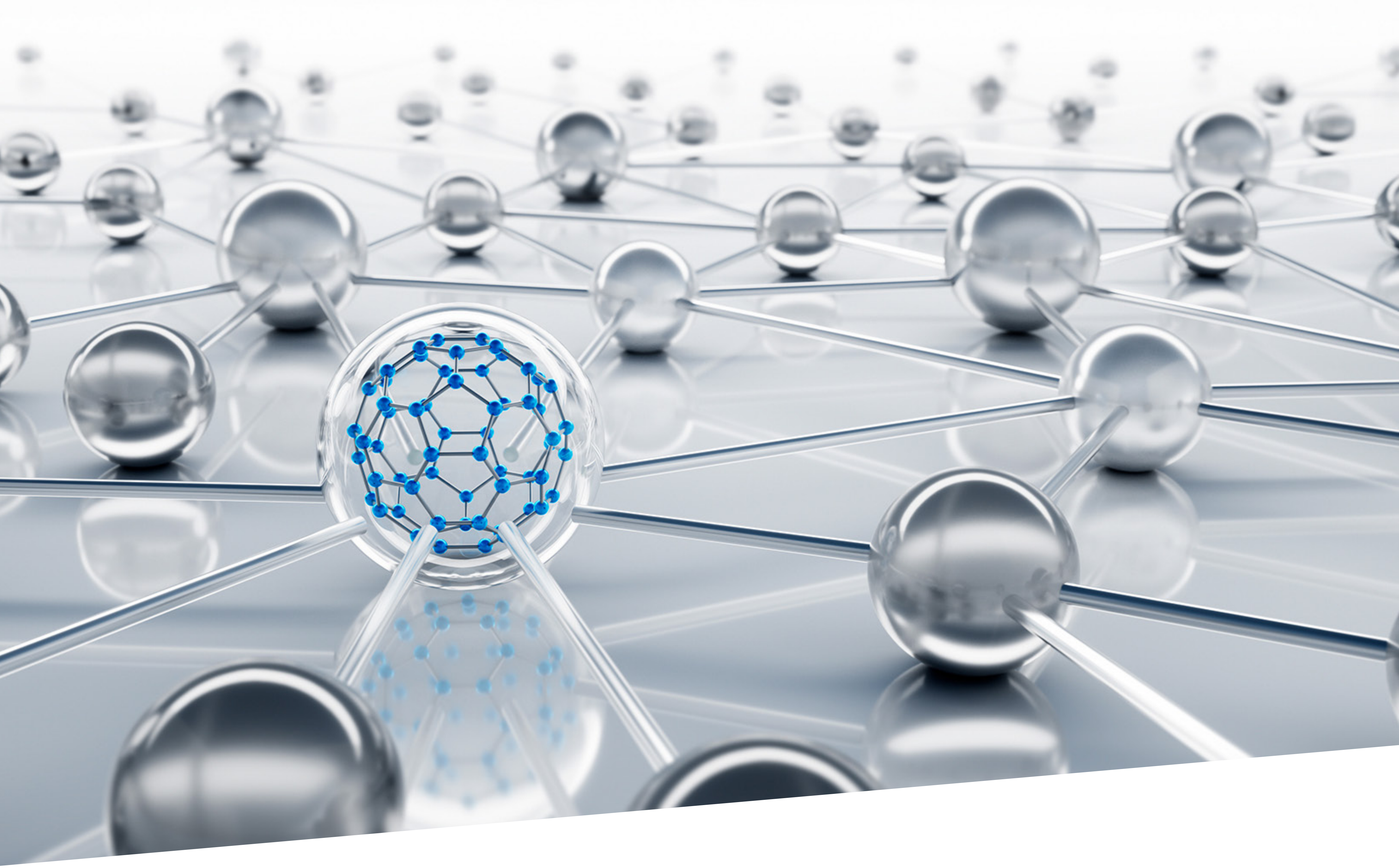


Table of Contents



Introduction

DNS, DHCP, and IP address management (DDI) are a suite of core services essential to network connectivity and communications. DDI suites manage the assignment of IP addresses and the mapping of those addresses to DNS domains for both internal and external communications. People who lack networking expertise may think DDI is trivial, but an ineffective approach to these core services can lead to sluggish network operations, chronic downtime, security breaches, and worse.

DDI technology has become more challenging in recent years with the rise of hybrid and multi-cloud architectures. As with switching, routing, and security, network teams often struggle to extend their DDI architecture into the cloud because they lack control and influence over cloud strategy. Cloud teams often adopt cloud-native tools without the network team's involvement, leading to a bifurcated approach to DDI services that creates complexity and inefficient operations. This research explores this issue in depth, along with several other major themes, including network automation, DDI security, APIs, integration, and IPv6.

This report represents the most comprehensive market research on DDI technology in more than a decade. Enterprise Management Associates surveyed 333 DDI experts on the state of their DDI strategies across multiple dimensions, including security, cloud, automation, and APIs and integrations. In addition, we conducted one-on-one interviews with DDI experts from several large enterprises to enrich our analysis of the survey data. These experts are quoted anonymously throughout the report.

This report reveals dozens of best practices for how IT organizations can improve their design and management of DDI services.

Methodology

EMA surveyed 333 IT professionals who had direct engagement with their organizations' DDI solutions. **Figure 1** reveals demographic highlights of these respondents. Full demographic details can be reviewed in Appendix 1.

FIGURE 1. DEMOGRAPHIC OVERVIEW

Job Titles

47.4%	Technical personnel (admin/engineer/architect)
36.3%	IT middle management (manager/supervisor/director)
16.2%	IT executives (CIO/CTO/CISO)

Top IT Groups

28.2%	Network engineering
15.6%	CIO suite
11.7%	Cybersecurity
10.8%	Cloud operations
9.0%	IT project management
8.1%	Network operations
7.8%	IT architecture

Top Industries

21.0%	Financial services
19.2%	Manufacturing
15.0%	Media/Entertainment/Content provider
10.8%	Retail
9.3%	Professional services
7.8%	Health care
4.5%	Energy

Company Size (Employees)

18.0%	Small enterprise (500 to 999)
49.8%	Midmarket enterprise (1,000 to 4,999)
32.1%	Large enterprise (5,000+)

Annual Revenue

28.2%	$100 million to <$250 million
32.7%	$500 million to <$1 billion
25.2%	$1 billion to <$5 billion
12.0%	$5 billion+
1.8%	Unknown/Not applicable

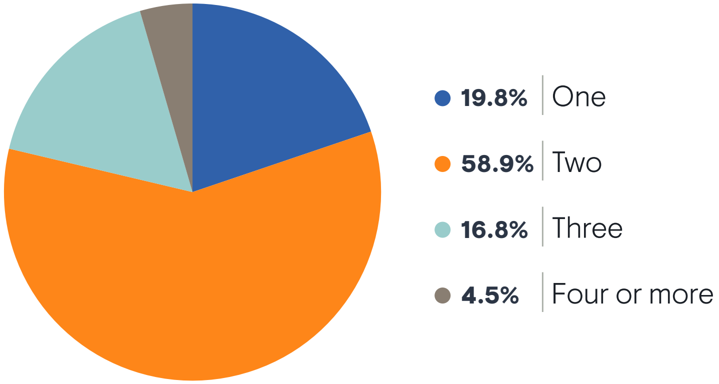
Region

63.1%	North America
36.9%	Europe

To qualify for this market research survey, respondents had to have direct engagement with their organization's DDI technology, either as someone who evaluates and selects solutions, implements and maintains them, or manages a network with them.

To ensure that this research could explore how cloud adoption impacts DDI strategy, all respondents had to be using the public cloud. **Figure 2** reveals qualified responses to a question about how many cloud providers were in use. Anyone who selected "none of the above" was removed from the survey. The chart reveals that most of the companies represented in this research are multi-cloud, using two or more providers.

FIGURE 2. NUMBER OF PUBLIC CLOUD PROVIDERS (IAAS, PAAS) ORGANIZATIONS USE



Sample Size = 333

Key Findings

The following are EMA's key findings in this research. The report will explore all this and more in detail in the following pages.

- Less than 40% of enterprises are completely successful with their DDI strategies
- Successful implementations of DDI technology typically lead to:
    - Increased network resilience
    - Enhanced IT productivity
    - Reduced security risk
- The top challenges to successful DDI strategy are:
    - Network complexity
    - IT cultural problems
    - Data quality and governance
    - Lack of skilled personnel
    - Lack of budget
- The most critical requirements of DDI solutions are:
    - Security features
    - Scalability and performance
    - Fully integrated functionality across DNS, DHCP, and IPAM
- Less than 31% of organizations are fully confident in the security of their DNS infrastructure
- 49% of DDI experts fully trust the automated workflows in their DDI tools
- 39% of organizations think their DDI solution is an effective source of truth for network automation
- 47% of DDI experts are completely satisfied with their DDI solution's APIs
- Top DDI API complaints are:
    - Quality
    - Complexity
    - Documentation issues
    - Extra licenses
- 59% of DDI teams have sufficient influence over cloud strategy
- 67% of organizations have consistent and effective integration between on-premises and cloud IPAM across all their cloud providers
- 38% of organization have implemented IPv6 extensively across their networks
- Top roadblocks of IPv6 adoption are:
    - Cost of upgrades
    - Skills gaps
    - Security concerns

DDI Strategy

We begin this report with an exploration of overall DDI strategies, from drivers and benefits to challenges and overall success with technology.

Drivers of DDI Technology Investment

Figure 3 identifies the technologies and initiatives that push IT organizations to invest in DDI solutions. Hybrid cloud tops the list, pointing to efforts to implement consistent and integrated network services across on-premises and cloud-based infrastructure. Technical personnel were more likely than middle managers and executives to cite this driver. It was also a major driver for smaller enterprises.

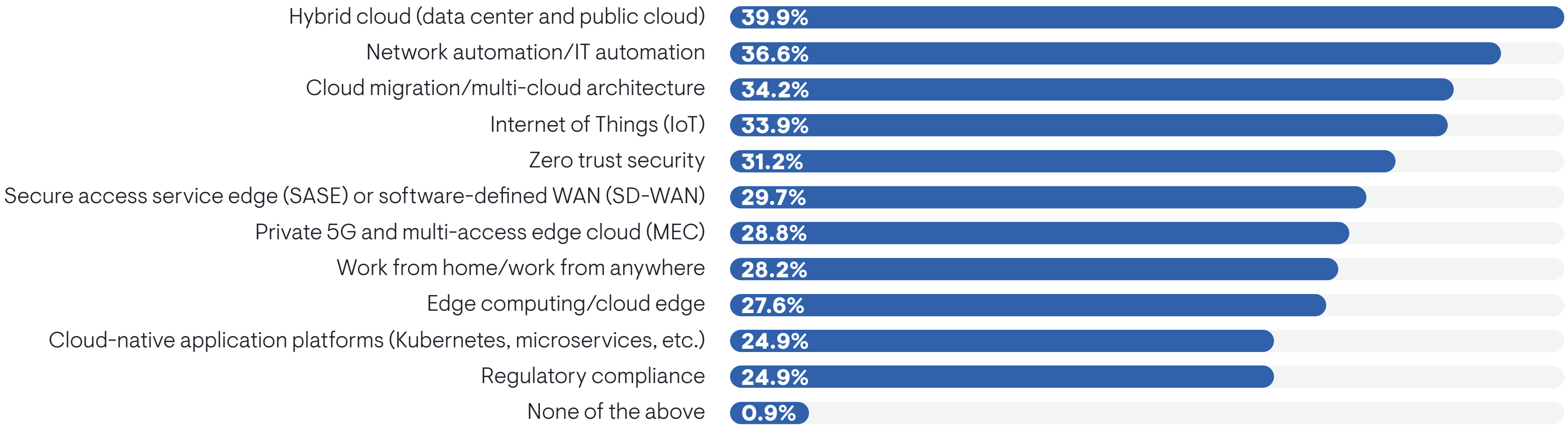
Network and IT automation is the second most prominent driver of DDI investment. Enterprise-grade DDI solutions offer many automated workflows around DNS, DHCP, and IP address management. DDI solutions are also important to broad automation solutions. Many network automation solutions require data from a DDI tool before an admin can push a change through the automation solution. Thus, DDI becomes an important source of network data for other automation tools. The CIO's suite, DevOps, and cybersecurity were all more likely to recognize the importance of automation.

Cloud migration and multi-cloud architecture combined to be the third most prominent drivers of DDI investment. DevOps and cloud operations were more likely to see the relevance of DDI to these cloud projects. Technical personnel were generally more engaged on this issue than middle managers and executives. Unsurprisingly, enterprises that are using multiple cloud providers also cited this driver more often.

IoT, zero trust security, and WAN technology (SASE, SD-WAN) were the other top drivers. Technical personnel were more engaged with zero trust than middle managers and executives, particularly members of the cloud operations team. Cybersecurity professionals were more likely than network engineering personnel to cite IoT as a driver.

Cloud-native platforms like Kubernetes were a minor driver overall, but North Americans were more engaged with it. Private 5G was another minor driver, but it was quite prominent in the largest enterprises in our survey. It was also more popular with organizations that struggle with DDI overall.

FIGURE 3. TECHNOLOGIES AND INITIATIVES DRIVING NEW OR EXPANDED INVESTMENTS IN DDI TECHNOLOGY

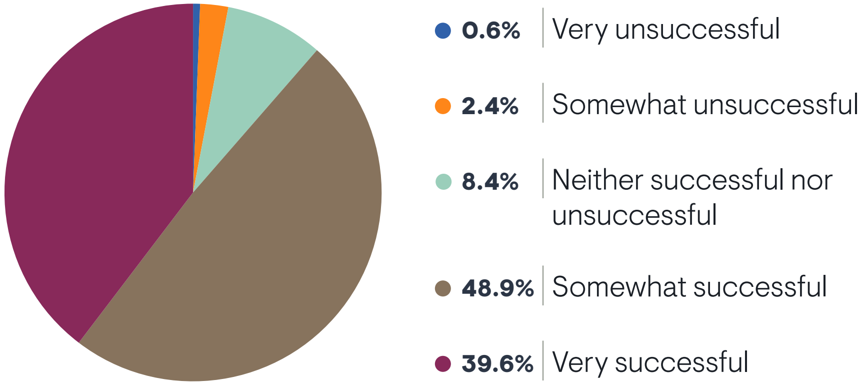


Sample Size = 333, Valid Cases = 333, Total Mentions = 1,136

Success with DDI

Figure 4 reveals how enterprises are faring with their DDI strategies today. Only 40% believe they are fully successful with DDI. Nearly 49% believe they have some room for improvement (somewhat successful), but only 3% admit that they're actually failing.

FIGURE 4. HOW SUCCESSFUL IS YOUR IT ORGANIZATION WITH ITS CURRENT APPROACH TO DDI TECHNOLOGY?



One of the issues at play here is complexity. DDI is a suite of three technologies and enterprises vary in their approaches to each of the three underlying technologies. For instance, the project manager for a Fortune 500 energy and chemical company said his DDI investment initially focused on centralizing IPAM, but DHCP and DNS remain fractured with multiple, unintegrated third-party services in use. "I would say we are great at IP address management. It's further along than DHCP and DNS. DHCP is a constant battle with multiple groups."

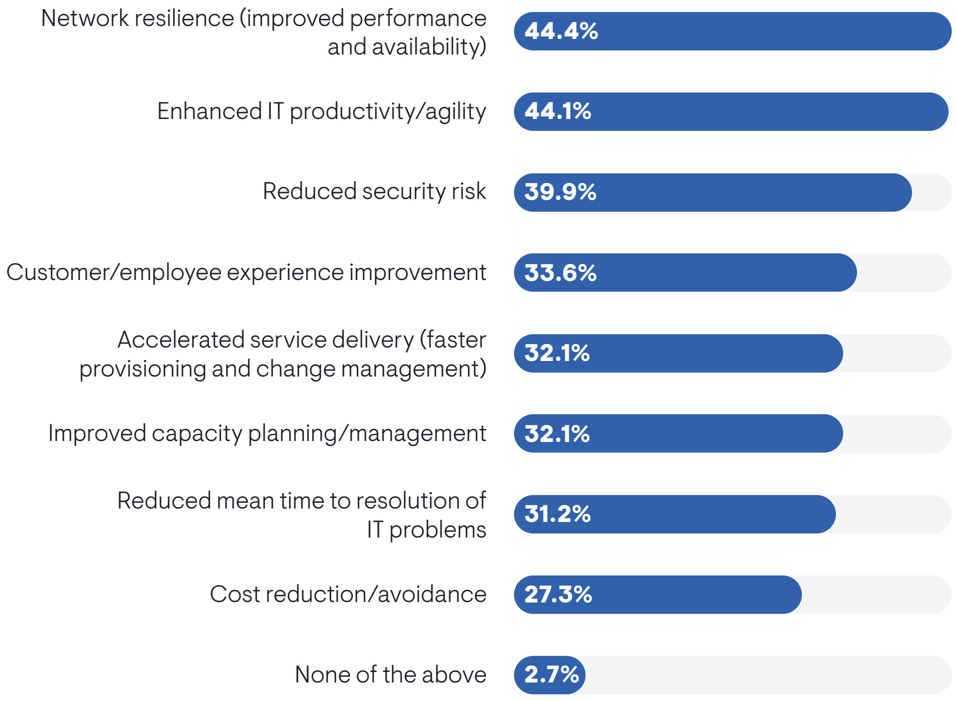
Only 40% believe they are fully successful with DDI.

Sample Size = 333

Returns on Investment

Figure 5 reveals the business benefits that organizations experience with their investments in DDI technology. The three leading outcomes are network resiliency, enhanced IT productivity, and reduced security risk. Multi-cloud enterprises were more likely to perceive the security benefits. Network engineering teams were less likely than other IT silos to recognize the security benefit.

FIGURE 5. BUSINESS BENEFITS EXPERIENCED BECAUSE OF INVESTMENTS IN DDI TECHNOLOGY



Sample Size = 333, Valid Cases = 333, Total Mentions = 958

A project manager at a Fortune 500 energy and chemical company said productivity and agility were major drivers of investing in an enterprise solution to replace spreadsheet-based IPAM. “It would take at least an hour just to provision a piece of networking gear...sometimes even half a day, because figuring out who had address space available wasn’t centralized enough. The spreadsheet had at least 10,000 lines, maybe even 100,000. As soon as we deployed [our commercial DDI solution], the first person to use it was able to deploy a device in 10 minutes when it would have taken him a couple hours before.”

Improved capacity planning and management was a minor benefit, but respondents who reported the most overall success with DDI selected it more often. The cloud operations team also saw a big opportunity with capacity.

Accelerated service delivery was cited most by cloud operations, DevOps, and network engineering teams. Given that DevOps and cloud teams often complain about the network engineering team getting in the way of service velocity, these three groups appear to have found common ground on how to solve the issue with DDI.

Troubleshooting (reduced mean time to repair) was another minor benefit, but a network engineer at a Fortune 500 consulting company said it was a huge priority for his organization. “It unifies everything,” he said. “It provides a single point of contact for troubleshooting.”

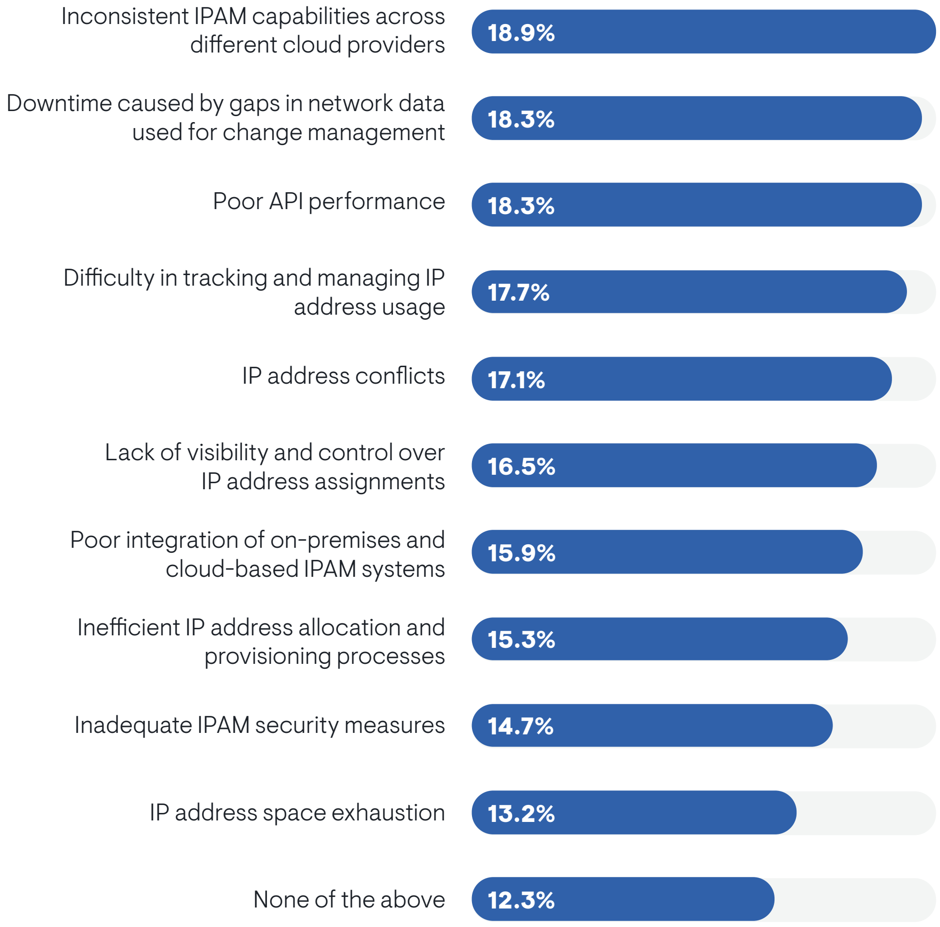
The most prominent source of IPAM pain is a lack of consistent capabilities across different cloud providers.

Sources of DDI Pain

IPAM Trouble

Figure 6 reveals the issues that cause organizations the most trouble with IP address management. Notably, more than 12% said they had no serious problems. In EMA’s experience with questions of this nature, less than 5% of respondents will usually select this option. This suggests that IPAM pain points are not as disruptive as other issues that IT organizations experience. Large enterprises were especially likely to have no complaints. However, the most prominent source of IPAM pain is a lack of consistent capabilities across different cloud providers. Network engineering and IT architecture groups are especially displeased with this issue.

FIGURE 6. IP ADDRESS MANAGEMENT CHALLENGES CAUSING THE MOST PAIN



Sample Size = 333, Valid Cases = 333, Total Mentions = 594

Next, gaps in network data used for change management lead to downtime for many organizations. Network operations and IT architecture teams were the most affected by this problem. The third problem is poor API performance. Cybersecurity teams especially selected this problem, suggesting that APIs' performance is impacting their ability to pull telemetry from DDI solutions into their analysis tools.

A lack of visibility and control over address assignments was a middling issue, but network operations teams were particularly feeling the pain from this. Midmarket companies also tended to struggle with this problem.

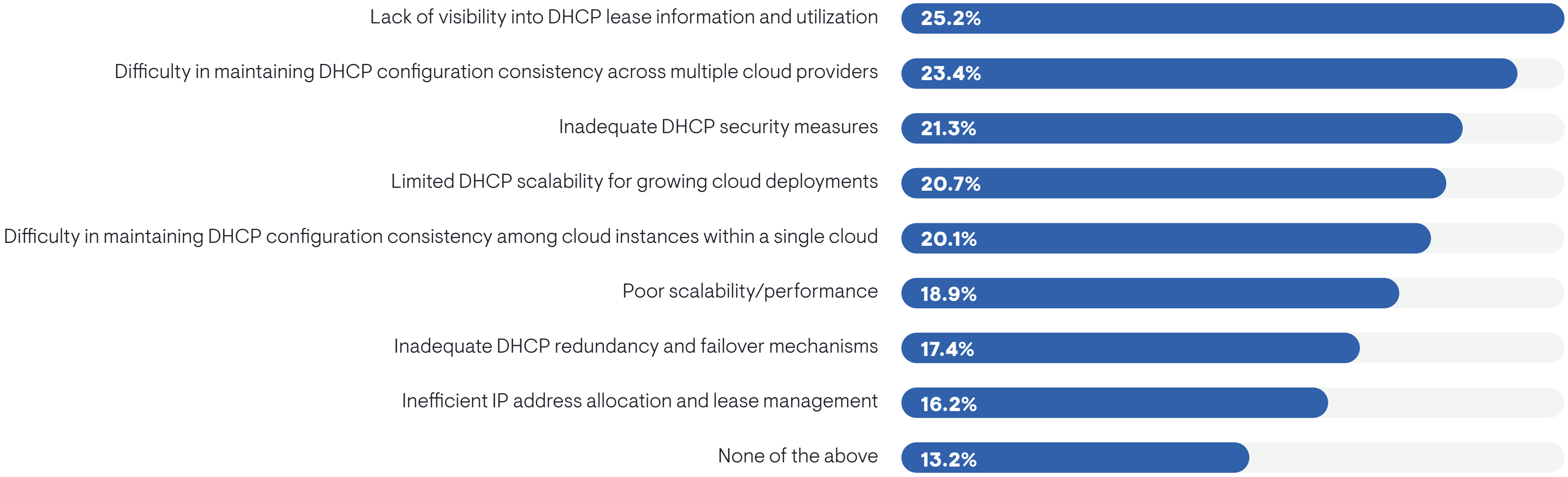
DHCP Trouble

Figure 7 identifies the DHCP challenges that cause organizations trouble. Lack of visibility into lease info/utilization, configuration consistency across cloud providers, and poor security are causing the most DHCP pain. The config consistency issue across cloud providers was a bigger headache for technical personnel and for members of DevOps teams. A related issue, config consistency across cloud instances within a single cloud, was a secondary issue overall, but DevOps also struggled with that one more often.

Poor visibility into lease and utilization information was a bigger problem for multi-cloud enterprises, as was the more minor complaint of poor mechanisms for redundancy and failover. Another less prominent issue, cloud-related scalability problems, was felt more by cloud operations and network operations teams.

As with IPAM, a significant percentage claimed to have no real pain points with DHCP. Much of this rosy view came from the CIO's suite (25%) and cybersecurity (23%). Only 5% of network engineering teams felt this way.

FIGURE 7. DHCP CHALLENGES CAUSING THE MOST PAIN



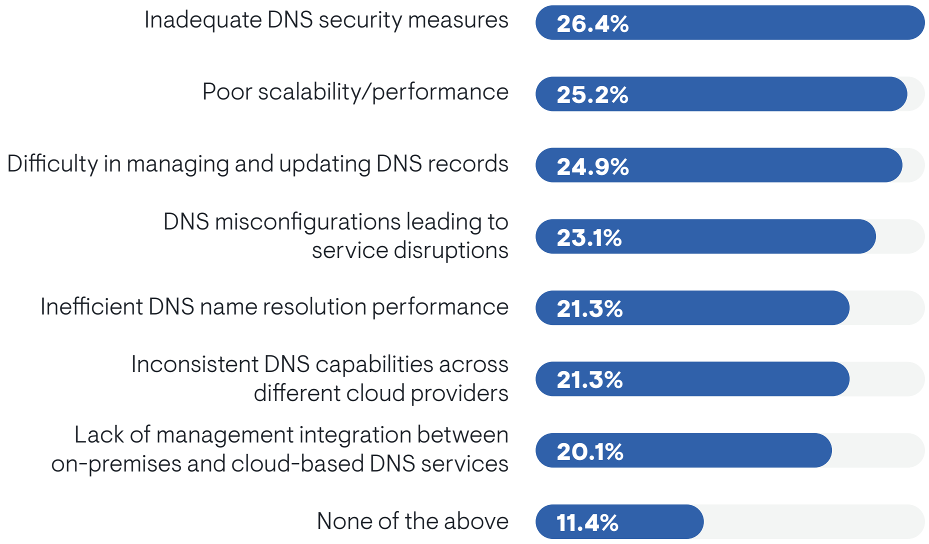
Sample Size = 333, Valid Cases = 333, Total Mentions = 588

DNS Trouble

Figure 8 reveals that inadequate security measures, scalability and performance issues, and difficulty with DNS records management are the biggest sources of pain associated with DNS. Multi-cloud enterprises are especially concerned with inadequate DNS security measures. Cloud operations and network engineering teams both cited difficult DNS records management as a pain point, while the CIO's suite tended to dismiss the issue. Scalability and performance were major issues for DevOps and the CIO's suite, but not much of a concern for cybersecurity. Small enterprises were particularly worried about scalability and performance.

Service disruptions caused by DNS misconfigurations were a secondary challenge, but cybersecurity was more likely to see this problem. Lack of management integration between on-premises and cloud-based DNS was the least prominent source of trouble, but the network engineering team singled it out as a major problem.

FIGURE 8. DNS CHALLENGES CAUSING THE MOST PAIN

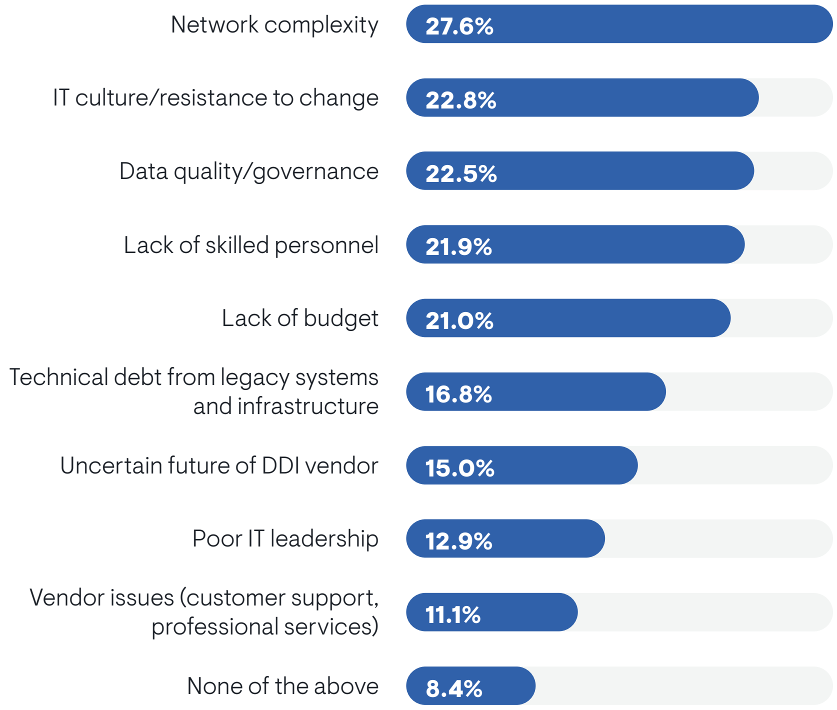


Sample Size = 333, Valid Cases = 333, Total Mentions = 579

General Challenges to DDI Strategy

Figure 9 explores the business and technical issues that typically undermine an organization's overall DDI strategy. The top issue is network complexity. Large enterprises were more likely to struggle with network complexity.

FIGURE 9. GENERAL BUSINESS AND TECHNICAL ISSUES MOST CHALLENGING TO DDI TECHNOLOGY STRATEGY



Problems with IT culture, data quality, and skill gaps are the main secondary challenges. Budget problems are also significant. Data quality was especially a headache for multi-cloud companies. The CIO's suite was very unlikely to recognize problems with IT culture, but DevOps and network operations both pointed to it as a top issue.

Sample Size = 333, Valid Cases = 333, Total Mentions = 600

“The main issue we had was training people to get off spreadsheets and start using a tool dedicated to IPAM,” said a project manager with a Fortune 500 energy and chemical company. “They’re always going around it. Old habits are hard to break.”

“Our company has had a lot of mergers and acquisitions, and we didn’t have a culture of owning IP addresses across them,” said a network engineer with a Fortune 500 consulting company. “So, I have a feeling that our IPAM is not as up to date as we would like it to be. It’s hard to find a person who owns an IP address sometimes. Vendors could help by providing good discovery tools that can go out, find devices, identify their addresses, and correlate that with our IPAM. IPAM should not be a passive tool. It should collect information from a live network and discover what’s happening.”

“The thing that bothers me the most is trying to keep IPAM data up to date,” said a network engineer with a Fortune 500 financial services company.

“The thing that bothers me the most is trying to keep IPAM data up to date,” said a network engineer with a Fortune 500 financial services company. “Everywhere I’ve been, you get data gaps and dirty data. People make changes without updating IPAM.”

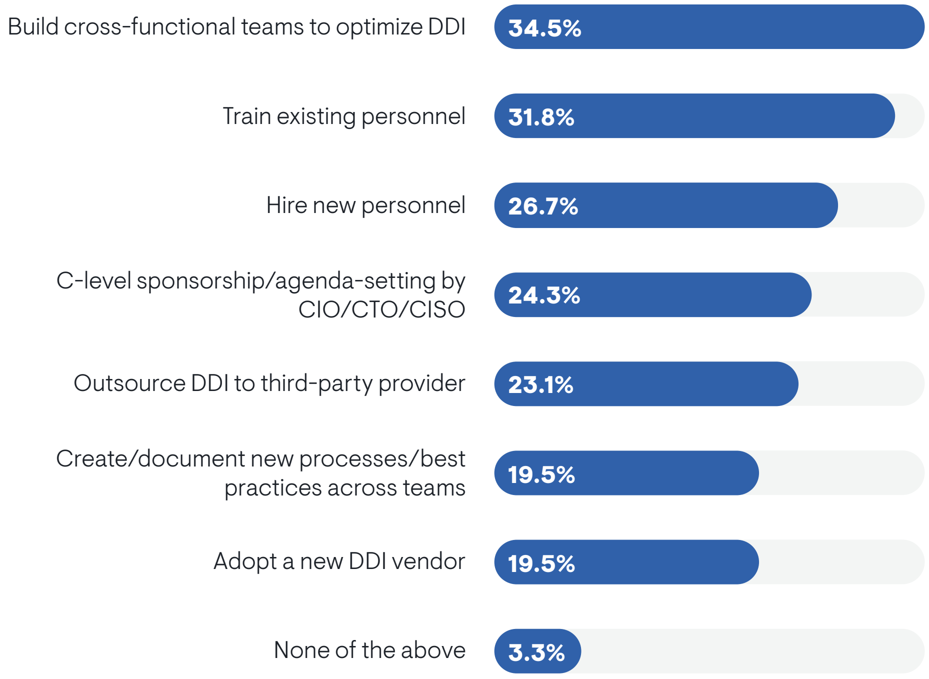
Respondents who were uncertain over their overall success with DDI technology struggled more often with skills gaps and poor IT leadership.

Vendor issues, such as poor customer support, was a minor challenge, but a network engineer with a midmarket software company said it was his biggest problem. “Support takes forever. And if you want premium support, it costs way too much money.”

Overcoming DDI Challenges

Figure 10 reveals how IT organizations try to overcome the challenges they encounter with DDI solutions. The most common response is to build a cross-functional team for DDI. Network engineering teams traditionally own DDI, but given its increased impact on security and the cloud, EMA recommends that these teams pull people from cloud operations, DevOps, and cybersecurity. The DevOps team was especially interested in this approach, but the CIO’s suite was less likely to see the value.

FIGURE 10. HOW IT ORGANIZATIONS TRY TO OVERCOME CHALLENGES TO DDI STRATEGY



Sample Size = 333, Valid Cases = 333, Total Mentions = 609

A cross-functional team can address some of the fractured operations that occur around DNS, which is often decentralized, with multiple groups managing their own infrastructure. “DNS is an internal struggle,” said a project manager with a Fortune 500 energy and chemical company. “We don’t have a set owner. It’s kind of a hot potato. It’s in this gray area where it is touched by multiple groups owning services for their own needs, including networks, servers, and end-device teams.”

The second most common reaction to challenges is to train existing personnel. Network teams might need security and cloud training. Other teams may require DDI tool training. The CIO’s suite was especially likely to see the value of training.

Many organizations also see the need to hire more DDI experts. IT executives were especially likely to pursue this. Multi-cloud enterprises also saw a need to hire.

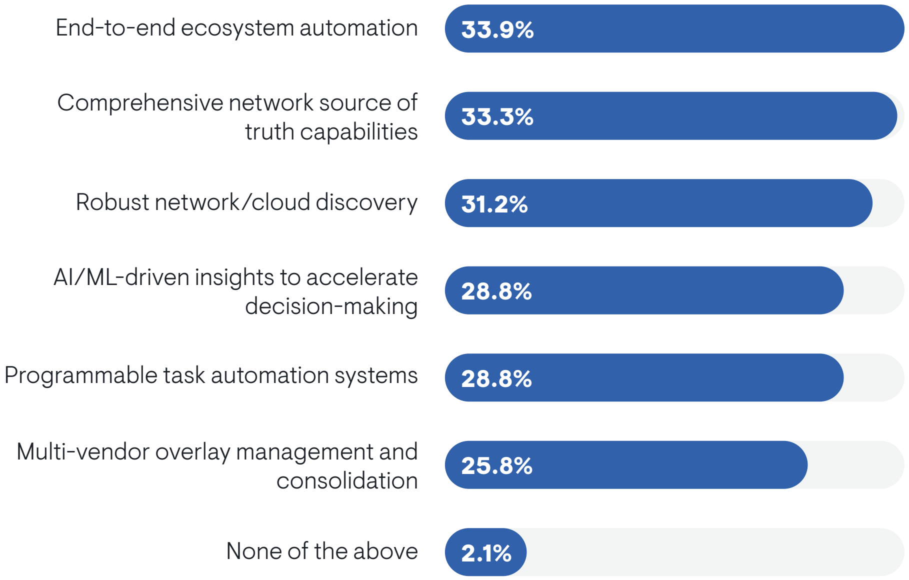
C-level sponsorship that sets a top-down agenda for improving DDI was favored by both technical personnel and IT executives, but middle managers were less convinced of its value. Members of the network engineering team were especially champions of this approach.

Adopting a new vendor appears to be the last resort for organizations. However, small enterprises were much more open to this idea than larger companies.

DDI Customer Wishlists

Figure 11 reveals what DDI professionals want their vendors to focus on delivering over the next two years. These innovations will be essential to addressing the challenges that IT teams are facing with this technology. First, over the next two years, they expect their vendors to deliver end-to-end ecosystem automation. In other words, they want a DDI vendor to enable automation across third-party DDI services. Less successful DDI teams are most interested in this capability, suggesting it’s less important than people think.

FIGURE 11. WHICH OF THE FOLLOWING DO YOU MOST WANT TO SEE YOUR DDI VENDOR DELIVER OVER THE NEXT TWO YEARS?



Sample Size = 333, Valid Cases = 333, Total Mentions = 613

Next, enterprises want a DDI solution that can serve as a comprehensive network source of truth for enabling automation. Most network engineers will tell you that DDI tools are not fit to this purpose for several reasons, such as poor integration, lack of network discovery, and a lack of certain types of data. For instance, some organizations want network config data, security policies, and inventory information included in their source of truth. Multi-cloud enterprises are especially interested in a source of truth, as are organizations that are more successful with overall DDI strategies.

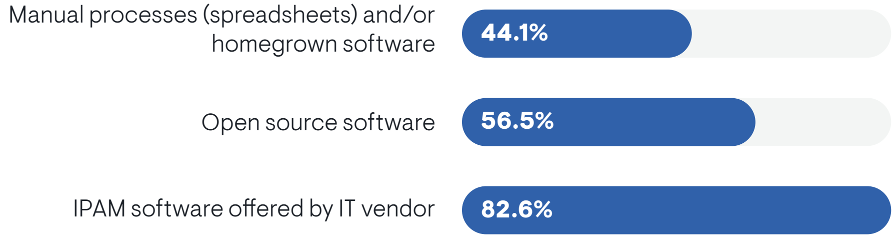
The third major wishlist item for 2025 is a robust network and cloud discovery mechanism. We will explore the issue of discovery later in this research.

DDI Technology Snapshot

IP Address Management Tools

IT organizations often have multiple IPAM tools and methods. For instance, one tool is used to manage IP address space in the on-premises network and a second is used in the cloud. Other organizations might use one tool in its data center and another for its enterprise network. In other cases, an organization might adopt enterprise IPAM software, but some individuals and teams will persist in using legacy spreadsheets or open source tools because they are unfamiliar with or distrusting of the new tool. **Figure 12** reveals that most organizations have multiple approaches to IPAM, with 83% of organizations using commercial IPAM software and 57% using open source software. Finally, more than 44% are using manual processes and homegrown tools, like Excel spreadsheets.

FIGURE 12. OVERALL APPROACH TO IP ADDRESS MANAGEMENT



Sample Size = 333, Valid Cases = 333, Total Mentions = 610

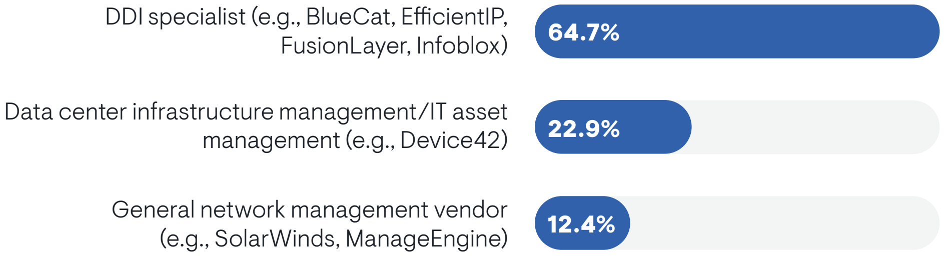
People who work the closest with network infrastructure were the most aware of manual IPAM processes.

"We had a senior manager who was managing all of it for a decade on Excel," said a project manager with a Fortune 500 energy and chemical company. "We deployed [an enterprise solution] two years ago. It was an intensive project that involved 150 hours of internal labor."

People who work the closest with network infrastructure were the most aware of manual IPAM processes. For instance, technical personnel (admins, engineers, architects) reported higher rates of manual processes than IT middle management and executives. Members of network engineering, network operations, and IT architecture teams perceived manual processes more often than people in the CIO's suite, cybersecurity, and cloud operations.

In EMA's experience, there are three types of suppliers of IPAM software. First, DDI specialists offer IPAM software designed to integrate with DHCP and DNS technology for full orchestration of network services. These tools tend to have more automation and scalability. Second, some data center infrastructure management vendors offer IPAM features, often combined with device inventory management features. Finally, general network management tool vendors offer IPAM modules or add-on tools that integrate with their suite of network management and monitoring tools. **Figure 13** reveals that nearly 65% of organizations that use a commercial IPAM tool work with a DDI specialist vendor. Organizations that experience the most success with their DDI technology used a DDI specialist for IPAM, while less successful organizations used a DCIM vendor.

FIGURE 13. SUPPLIERS OF COMMERCIAL IPAM SOFTWARE



Sample Size = 275

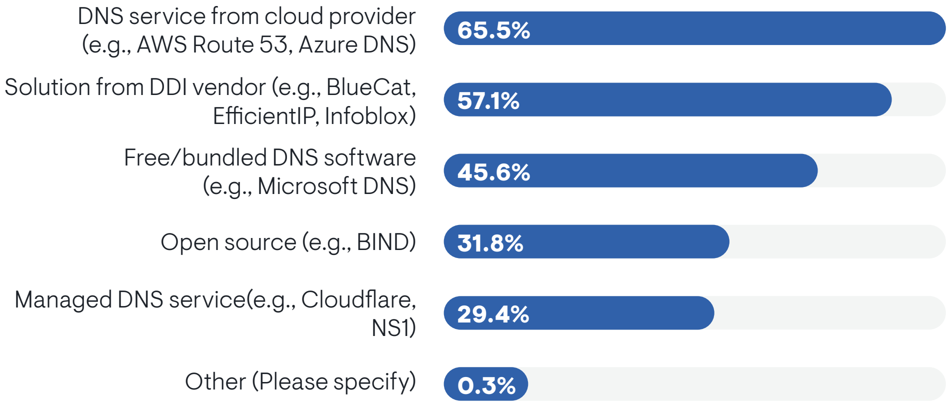
Technical personnel were more likely than middle managers to report use of a DDI specialist. The groups that reported higher adoption rates of DDI specialists included network engineering, network operations, IT architecture, cybersecurity, and DevOps.

DNS Technology

Suppliers of External DNS Services

Figure 14 reveals the general sources of DNS technology that organizations are using for their external, public-facing services. Enterprises often maintain external DNS services to ensure external users can reach their websites and other internet-accessible resources. Native DNS services from public cloud providers are the most popular choice for external services, pointing to criticality of cloud services to today's digital enterprises. Most organizations also have external DNS servers from a DDI specialist. Organizations that are the most successful with DDI technology were more likely to use a DDI specialist for external DNS. Members of network engineering teams reported higher adoption of DDI specialist software than members of the CIO's suite, suggesting a significant gap in visibility between network experts and executives.

FIGURE 14. TECHNOLOGIES USED FOR PUBLIC/EXTERNAL DNS SERVICES



Free or bundled DNS software is also quite popular. The leading example of such a DNS server is Microsoft DNS, which is typically bundled with Active Directory. Members of network engineering, network operations, cloud operations, and DevOps teams all perceived more usage of this bundled software than the CIO's suite.

Sample Size = 333, Valid Cases = 333, Total Mentions = 765

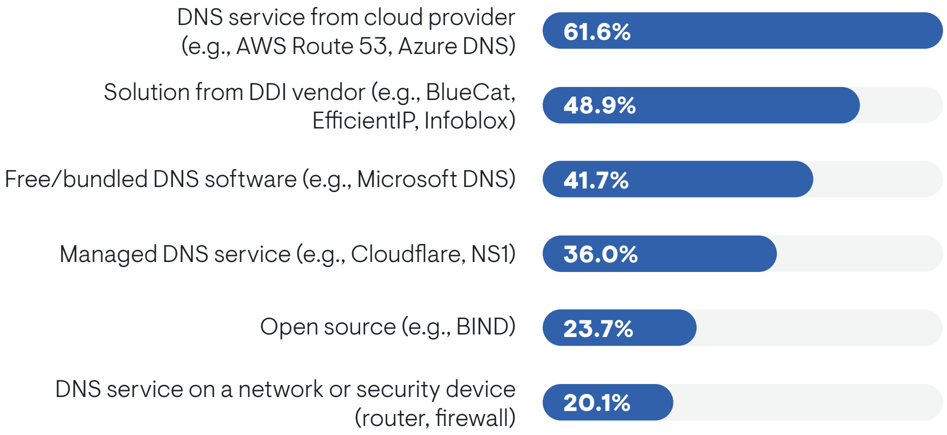
Open source DNS and managed DNS services are the least popular options. However, it's worth noting that managed DNS services are converging with cloud DNS. For example, some cloud providers have acquired managed DNS providers in recent years, while other DNS providers have openly discussed their plans to start offering public cloud services. DevOps and cybersecurity teams perceived more use of managed DNS services than the CIO's suite.

Multi-cloud architecture appears to drive public DNS diversity. The more cloud providers an organization was using, the more likely they were to use open source DNS, bundled DNS, cloud provider DNS services, and managed DNS services.

Suppliers of Internal DNS Services

Figure 15 reveals the source of internal DNS software that enterprises are using. Internal or private DNS typically enables the resolution of domain names to IP addresses for services, like application servers, file servers, and print services. If external DNS serves as the phone book for the internet, internal DNS is like the employee directory for a company's internal services.

FIGURE 15. TECHNOLOGIES USED FOR PRIVATE/INTERNAL DNS SERVICES



Sample Size = 333, Valid Cases = 333, Total Mentions = 773

Like with external DNS, DNS services from cloud providers and DDI specialists are the most popular options for internal services. The CIO's suite had a lower awareness of DDI specialists for internal DNS than highly technical groups, like network engineering, network operations, and IT architecture.

Free or bundled DNS software was a secondary source of internal DNS technology, Again, the CIO's suite tended to be ignorant of its use, while the network engineering, network operations, cybersecurity, and IT architecture teams saw more widespread adoption of it.

Open source software is relatively rare for internal DNS services, but DevOps and IT architecture groups saw heavy use of it, while cybersecurity, network engineering, and the CIO's suite were less aware of its presence on the network.

As with external DNS, EMA found that organizations had a more diversified approach to internal DNS when they operated a multi-cloud architecture. With more providers in use, organizations were more likely to use open source DNS, bundled DNS, DDI specialists, cloud provider DNS services, and managed DNS services.

Organizations had a more diversified approach to internal DNS when they operated a multi-cloud architecture.

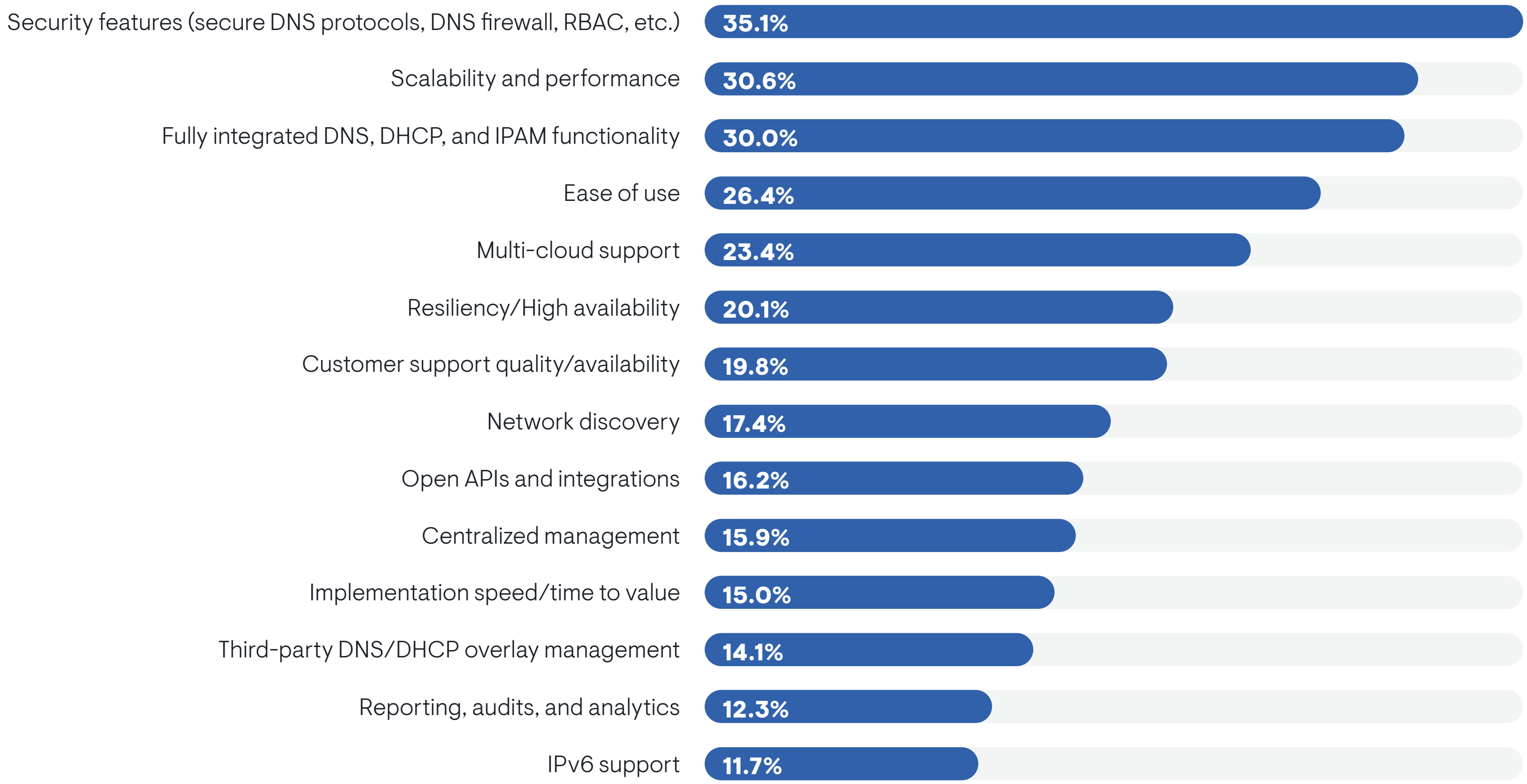
Core DDI Requirements

Overall Solution Requirements

Figure 16 reveals how organizations rank the overall requirements they have for their DDI technology. While DDI is traditionally about network infrastructure management, the chart clearly demonstrates that enterprises expect their solutions to address security. Security features are the top requirements.

Security is also a best practice focus, with successful organizations more likely to select it. DevOps and cloud operations teams both selected security more often, as did the CIO's suite. Network engineering teams were less likely to focus on it.

FIGURE 16. MOST IMPORTANT REQUIREMENTS FOR DDI SOLUTIONS



Sample Size = 333, Valid Cases = 333, Total Mentions = 960

Scalability and performance, fully integrated DDI functionality, and ease of use were secondary requirements. Large enterprises (5,000 or more employees) made scalability and performance a high priority.

Multi-cloud support, resiliency and high availability, and customer support were tertiary requirements. Small enterprises (fewer than 1,000 employees) made resiliency and high availability priorities. Resiliency was also important to DevOps and NetOps teams, but not as much to network engineering.

"The most important thing for me is a system that provides high availability," said a network engineer with a Fortune 500 consulting company. "DNS cannot go down."

Network discovery was overall a minor solution requirement, but organizations that experienced more success with DDI ranked it higher.

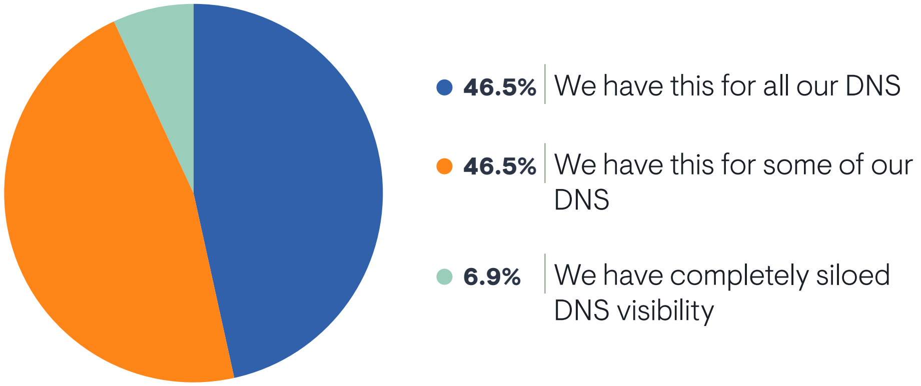
Network discovery was overall a minor solution requirement, but organizations that experienced more success with DDI ranked it higher, suggesting a best practice focus. The IT architecture group also tended to rank discovery higher, as did technical personnel in general. IT executives and middle management were less likely to think discovery is important.

"It would be great to have more robust discovery tools within whatever IPAM and full-stack DDI solution I am using," said a network engineer with a Fortune 500 financial services company. "I don't want to go in and homebrew a solution to get the data I need. I want to have it all in one place."

DNS Management from Single Pane of Glass

Figure 17 reveals that fewer than 48% of organizations can manage and monitor all their DNS infrastructure from a single pane of glass. Most companies must turn to a second or third tool to manage the rest of their DNS services. This lack of centralized management is more common in midsized and large enterprises. The ability to centralize DNS management correlates strongly with overall DDI success. As we will see in a later section, most enterprises make it a priority to integrate their IPAM tools with all of their DNS infrastructure. This integration is a key enabler for centralized management since it allows IPAM tools to coordinate management across disparate DNS services.

FIGURE 17. TO WHAT EXTENT CAN YOU MONITOR AND MANAGE ALL YOUR ORGANIZATION'S DNS INFRASTRUCTURE FROM A SINGLE CONSOLE (PANE OF GLASS)?

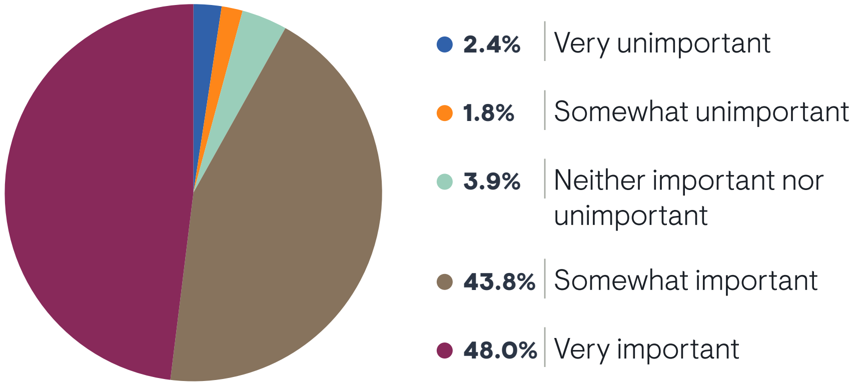


Sample Size = 333

IPAM/DNS Integration

One of the core value propositions of implementing a full-stack DDI solution is integration across the core components so that any changes implemented in the IP address space via an IPAM tool are coordinated across DNS and DHCP, too. This ensures consistent addressing across infrastructure. **Figure 18** reveals how important respondents believe IPAM/DNS integration is to their networks. Exactly 48% described this integration as very important, with 44% believing it to be only somewhat important. Very few said it was unimportant.

FIGURE 18. HOW IMPORTANT IS IT FOR YOUR IPAM TOOL TO INTEGRATE WITH YOUR DNS INFRASTRUCTURE SO THAT CHANGES MADE IN IP ADDRESS SPACE ARE COORDINATED WITH CHANGES IN DNS?



Sample Size = 333

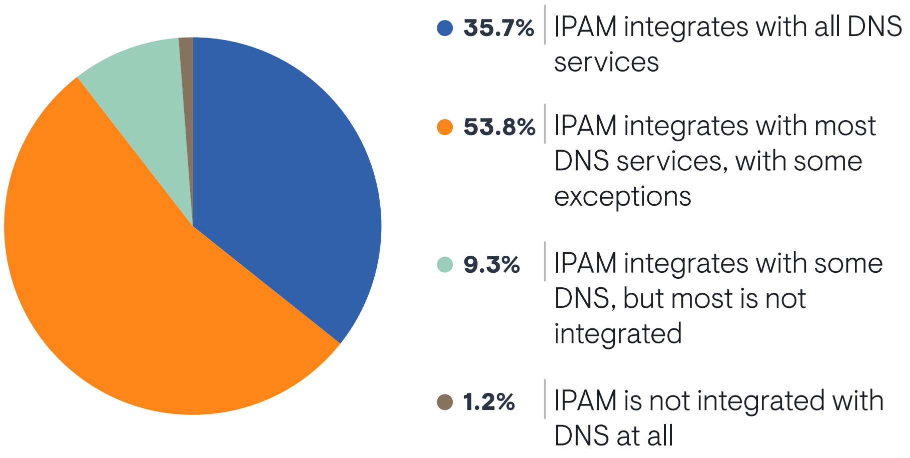
This integration is clearly a best practice. The most successful users of DDI technology were twice as likely as all other organizations to describe IPAM/DNS integration as very important. Multi-cloud architecture also makes this integration a priority. The more cloud providers an organization uses, the more likely it is to consider this integration important.

EMA observed some notable differences by IT silos. The CIO's suite, cybersecurity, and cloud operations all see IPAM/DNS integration as a high priority. DevOps, IT architecture, and network engineering were less likely to feel this way. EMA suspects that network engineering personnel are more comfortable with manual network operations.

Complete IPAM/DNS Integration is Rare

This research already established that enterprises typically have multiple DNS services in their networks and this diversity is challenging their ability to completely integrate their IPAM tools with these services. **Figure 19** reveals that only 36% of enterprises have managed to integrate their IPAM tool with all DNS infrastructure. Despite the wide recognition that this integration is important, nearly 54% acknowledged that they still have some DNS services that are siloed from their IPAM tool. Another 9% admitted that most of their DNS services are siloed.

FIGURE 19. CURRENT EXTENT OF IPAM INTEGRATION WITH DNS INFRASTRUCTURE



Sample Size = 333

"IPAM/DNS integration makes sense long-term, but we aim to get tools into production with basic functionality," said a project manager with a Fortune 500 energy chemical company. "We deployed IPAM just so we could get an understanding of our address space. Tying that into DNS…there's not a lot of time devoted to that yet."

Overall success with DDI technology correlates strongly with complete integration of all DNS services with IPAM. EMA's data indicated that only small enterprises (fewer than 1,000 employees) were able to achieve this complete integration often. Most midsized and large companies reported only partial integration.

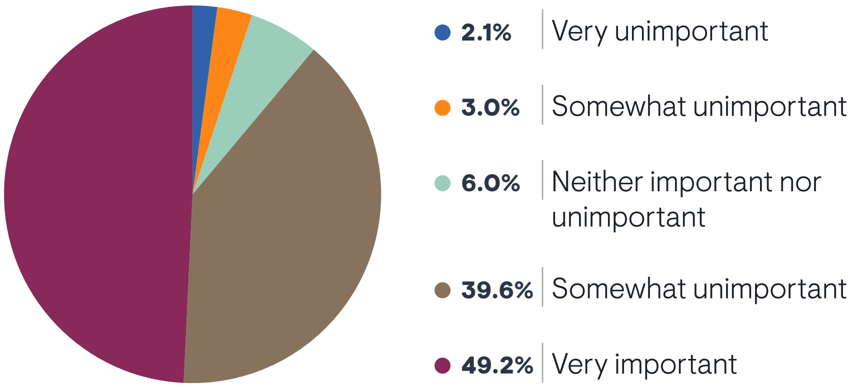
Cloud operations and cybersecurity teams perceived the most extensive levels of IPAM/DNS integration. Network engineering and IT architecture teams tended to report at least some pockets of siloed DNS services.

IPAM/DHCP Integration

Figure 20 reveals that integration of IPAM and DHCP services is also a high priority. The number of respondents who say this integration is very important is fractionally higher than those who say the same about IPAM/DNS integration. EMA also observed a strong preference for this integration among organizations that reported the most success with DDI technology.

The CIO's suite, network operations, cloud operations, and cybersecurity all tended to say this integration was very important. The network engineering team tended to report that it was only a secondary priority while the DevOps team believe it was a low priority. Finally, IPAM/DHCP integration was more important to organizations that use two or three cloud providers. Single cloud enterprises were less emphatic about its importance. However, organizations that use four or more cloud providers also reported less of a need for this integration.

FIGURE 20. HOW IMPORTANT IS IT FOR YOUR IPAM TOOL TO INTEGRATE WITH YOUR DHCP INFRASTRUCTURE SO THAT CHANGES MADE IN IP ADDRESS SPACE ARE COORDINATED WITH CHANGES IN DHCP?

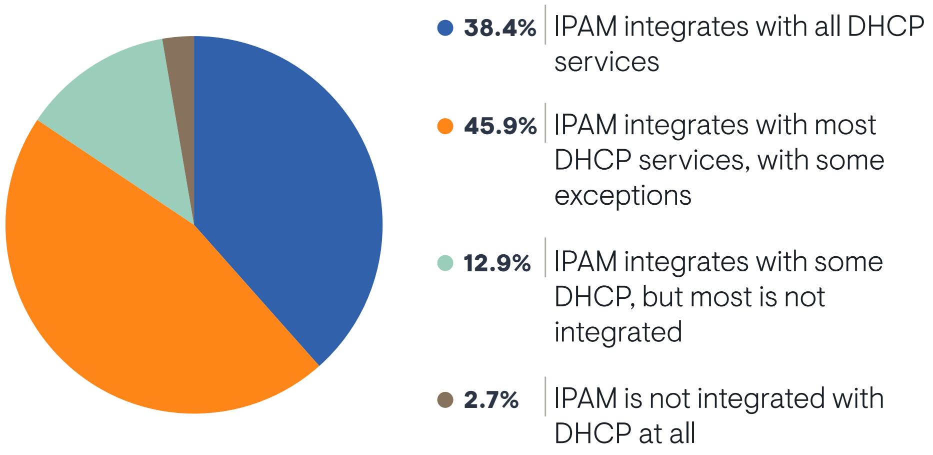


Sample Size = 333

Complete IPAM/DHCP Integration is Rare

Figure 21 reveals that enterprises are a little more likely to have complete integration of IPAM with all DHCP services than they are with DNS services. However, most organizations have at least some siloed DHCP services.

FIGURE 21. CURRENT EXTENT OF IPAM INTEGRATION WITH DHCP INFRASTRUCTURE



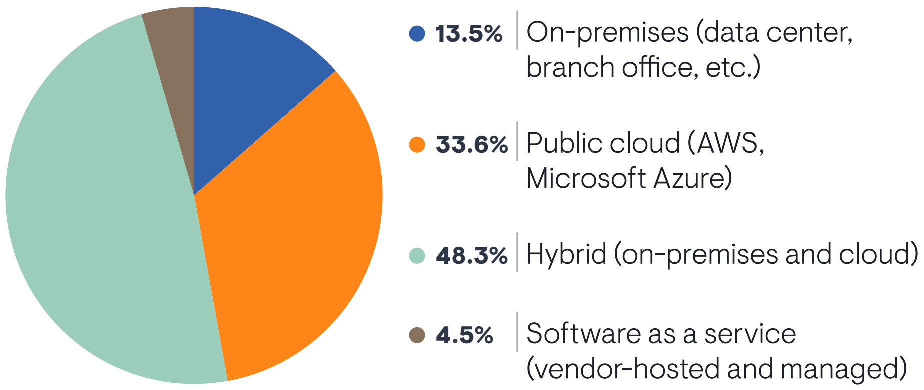
Success with DDI correlates strongly with complete integration of all DHCP services with IPAM. It's also more common in small enterprises. Most IT silos perceived comparable levels of overall integration, except for the IT architecture and IT project management groups, who saw more pockets of standalone DHCP services.

Sample Size = 333

Deployment and Administration Preferences

Figure 22 reveals that the days of network teams preferring their tools deployed on-premises are over. More than 48% of organizations prefer a hybrid deployment of their DDI tools in which they span both on-premises and cloud environments. This deployment model was a heavy favorite among organizations that were the most successful with their DDI solutions.

FIGURE 22. PREFERENCE FOR WHERE DDI TOOLS ARE DEPLOYED



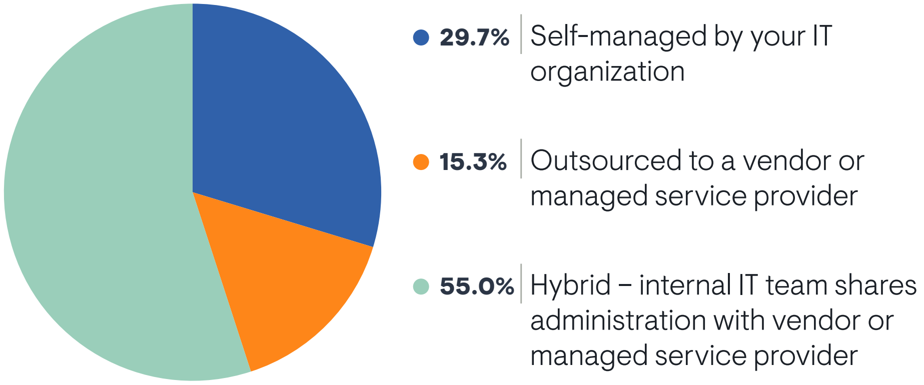
Less than 14% require an on-premises deployment. Members of the IT asset and vendor management group drove much of that preference. Members of the cloud operations team and the CIO's suite tended to prefer deployment of DDI tools in a public cloud.

Sample Size = 333

Figure 23 reveals that most organizations want to maintain at least some administrative control over their DDI tools. Only 30% want a fully self-managed solution and only 15% want to completely outsource it. The rest want a hybrid approach in which they and their vendors share administration of the technology. North Americans preferred the hybrid operating model while Europeans were split among fully outsourced or fully self-managed solutions.

Less successful organizations expressed a preference for outsourcing DDI administration, suggesting it's inadvisable. Small enterprises preferred a hybrid administrative model, as did members of DevOps teams.

FIGURE 23. PREFERENCE FOR HOW DDI SOLUTIONS ARE ADMINISTERED/MANAGED



Sample Size = 333

DDI Security

This section explores the security concerns organizations have with respect to their DDI technology and the steps they take to protect DNS, DHCP, and IPAM.

DNS Security

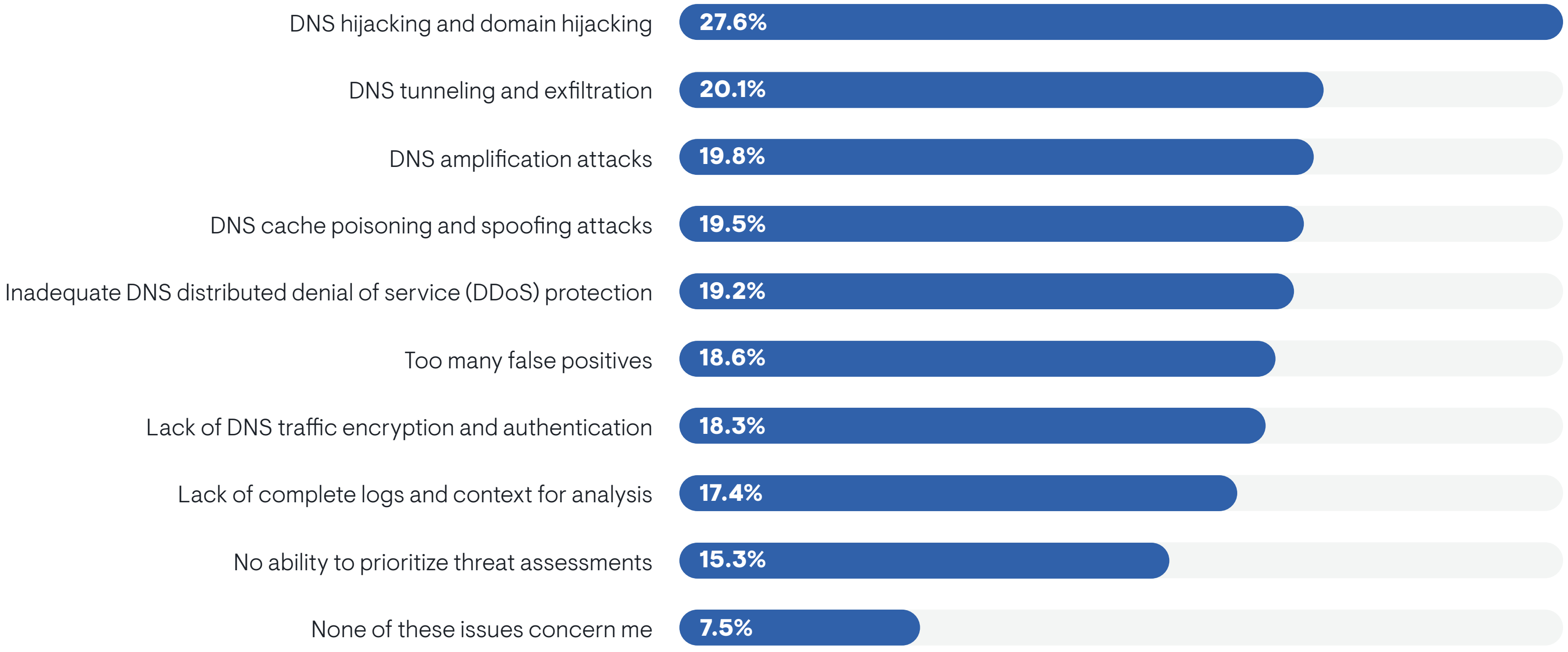
In recent years, enterprises discovered a broad and growing array of threats and exploitations malicious actors use against DNS. Consequently, DNS security has become a growing area of innovation and investment.

Threats and Risks

Figure 24 reveals the DNS security challenges that enterprises are most concerned about today. Only 7.5% of respondents claim to have no security concerns with DNS. The most pressing concern is DNS and domain hijacking. Also known as DNS redirection, this involves the use of incorrectly resolved domains to redirect users to malicious sites.

Only 7.5% of respondents claim to have no security concerns with DNS.

FIGURE 24. DNS SECURITY CHALLENGES THAT MOST CONCERN ORGANIZATIONS



Sample Size = 333, Valid Cases = 333, Total Mentions = 611

DNS tunneling and exfiltration and DNS amplification were the two chief secondary security concerns. With DNS tunneling and exfiltration, malicious actors evade detection of extracting stolen data by disguising it as a series of outgoing DNS queries from an infected device to an external, malicious domain. Amplification attacks are a type of indirect DNS-based DDoS attack that tricks third-party publicly accessible DNS servers into flooding a target with unwanted, spoofed query responses. Technical personnel were much more likely than IT middle management and executives to have concerns about these two threats. DNS amplification was also a major concern for companies that use four or more cloud providers.

Europeans were more likely than North Americans to believe that their overall DDoS protection was inadequate. Midmarket companies were more likely to have concerns about DNS cache poisoning and spoofing. This attack involves the insertion of false information into a DNS cache so that queries generate responses that direct users to the incorrect sites. This can form the foundation of a domain hijacking attack, sending users to a malicious site, but it can also be used to make a target website inaccessible, thus disrupting the target's business.

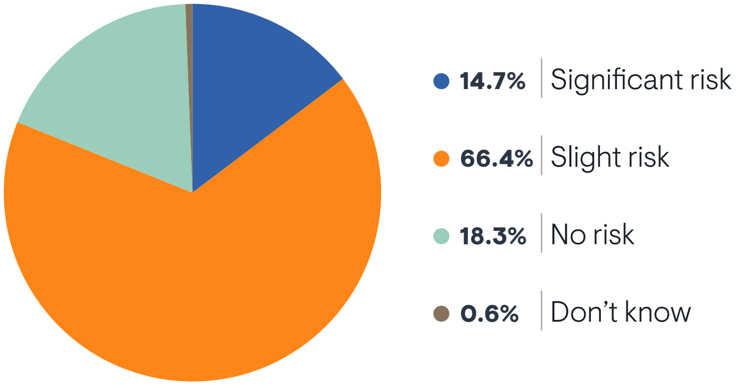
81% of respondents said that manual DNS configuration and administration errors present at least some risk to their organization's security.

Lack of complete logs and context for analysis was a minor issue overall, but a network engineer with a midmarket software company said this is a major source of pain for him. "Most DNS log data is crap. It makes it hard to analyze them. Too much of it isn't useful data."

Figure 25 reveals one other dimension of security concern for enterprises. Nearly 81% of respondents said that manual DNS configuration and administration errors present at least some risk to their organization's security.

Technical personnel were the most likely to perceive this danger while middle managers and executives tended to downplay it. Members of network engineering and IT architecture were the most concerned, but cybersecurity professionals perceived less risk. EMA suspects that many cybersecurity teams are unaware of the extent of manual administration that occurs with DNS infrastructure.

FIGURE 25. TO WHAT EXTENT ARE MANUAL DNS CONFIGURATION AND ADMINISTRATION ERRORS A SOURCE OF SECURITY RISK IN YOUR ORGANIZATION?

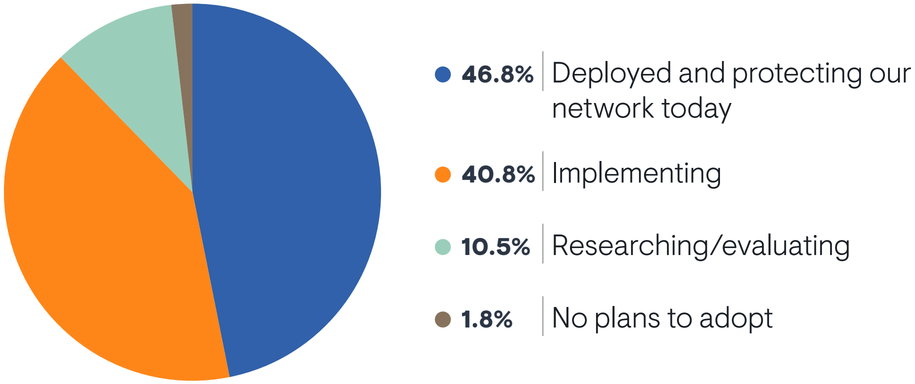


Sample Size = 333

DNS Firewall Adoption

A DNS firewall is a network security solution typically offered by a DDI vendor that inspects DNS queries between endpoints and blocks connections based on threat intelligence and policies. These products can prevent many DNS-based attacks and DNS-based policy violations. **Figure 26** reveals that nearly 47% of research respondents have deployed a DNS firewall. Another 41% are implementing a solution.

FIGURE 26. CURRENT ENGAGEMENT WITH DNS FIREWALL SOLUTIONS



Sample Size = 333

"We're not using a DNS firewall, but it would be useful," said a network engineer with a Fortune 500 consulting company. "It's important not just for security, but also for high availability."

This adoption rate is higher than expected. EMA suspects that much of this is driven by knowledge gaps in IT organizations. For example, 67% of IT executives said their network is currently protected by a DNS firewall, but only 38% of technical personnel said so. We believe that many of these executives have mistaken a traditional firewall with DNS-specific policies configured for a true DNS firewall. We observed similar patterns from a silo perspective. For instance, cloud operations teams and the CIO's suite were the most likely to report having a DNS firewall actively protecting their networks. Members of network engineering, network operations, cybersecurity, and even DevOps groups were much less likely to report the same thing.

On the other hand, DNS firewalls do appear to be helpful. For instance, successful users of DDI technology reported higher adoption rates than less successful organizations. Adoption was also highest in large enterprises, which makes sense because these are generally perceived as premium products that small enterprises often lack the money to pay with.

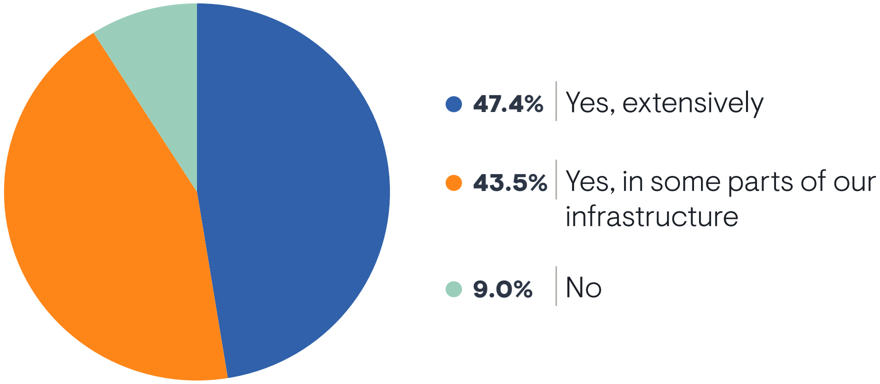
DNSSEC Engagement

DNS Security Extensions (DNSSEC) is a suite of specifications defined by the Internet Engineering Task Force (IETF) for hardening DNS infrastructure. It ensures authenticity of DNS records. DNS servers that have DNSSEC enabled will digitally sign records using public-key cryptography. DNS resolvers can verify the authenticity of DNS records through this mechanism. This protects DNS from forged and manipulated data.

91% of organizations are using DNSSEC today, although only 47% use it extensively.

Figure 27 reveals that 91% of organizations are using DNSSEC today, although only 47% use it extensively. Respondents who reported the most success with DDI technology were much more likely (65%) to use DNSSEC extensively. The technology was also more widely deployed in multi-cloud enterprises. North Americans were more aggressive with it than Europeans.

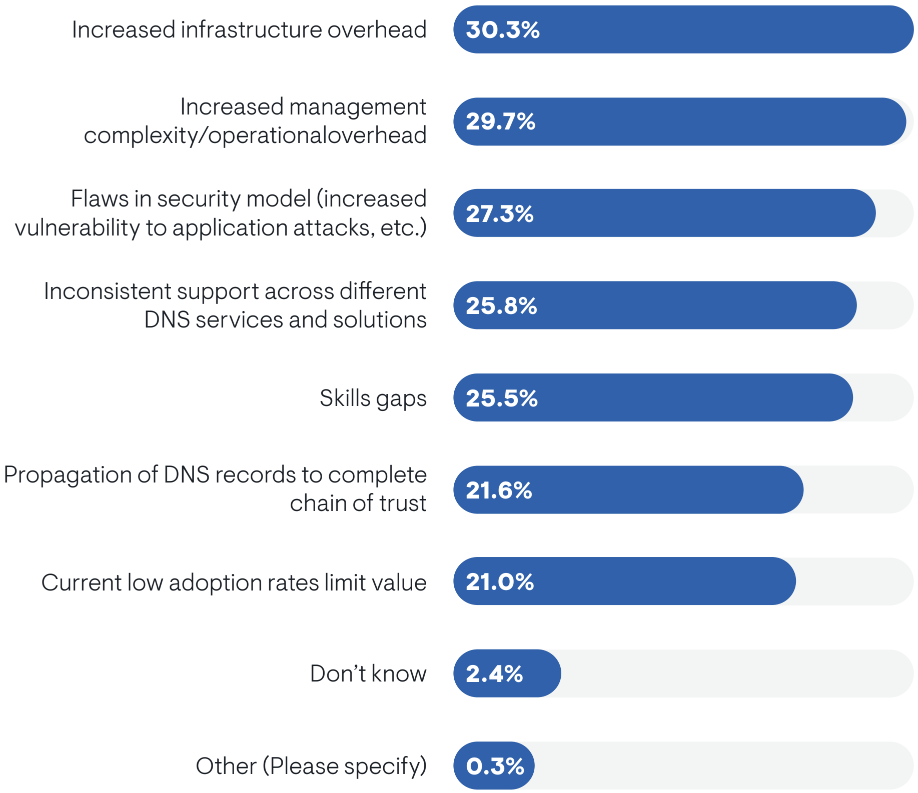
FIGURE 27. DOES YOUR ORGANIZATION USE DOMAIN NAME SYSTEM SECURITY EXTENSIONS (DNSSEC)?



Sample Size = 333

Figure 28 identifies the challenges that organizations encounter when they use DNSSEC. The top issues are infrastructure overhead (DNS servers expend resources on encryption and authentication) and management complexity. Infrastructure overhead was a bigger concern to cybersecurity, but not cloud operations. Management complexity is a concern for DevOps, but not network engineering or cloud operations.

FIGURE 28. CHALLENGES WITH USING DNSSEC



Sample Size = 333, Valid Cases = 333, Total Mentions = 613

Infrastructure overhead was an issue for a network engineer with a Fortune 500 consulting company. "DNSSEC increased the amount of TCP traffic on our external DNS. It increased the network load on our servers. But it wasn't as bad as I expected." This network engineer also pointed to skills and knowledge gaps as issues. "It was a pretty easy implementation, but adoption is low because people don't have a lot of knowledge about it. We needed to develop specific automation around it because we have 1,000 external domains. We needed to be able to update all of them, so it required working with a lot of external partners."

Flaws in the DNSSEC security model were a secondary concern. Network engineering personnel were most likely to cite this issue. The CIO's suite was less concerned. Skills gaps were also a secondary concern, mostly among network and cloud operations personnel. Network engineering and cloud operations were less likely to worry.

Given that DNSSEC relies on the adoption by multiple organizations, some respondents cited low adoption rates as a drag on overall value of the technology. This was more of an issue among North American respondents.

Other DNS Security Measures

Figure 29 reveals the other methods that organizations adopt to protect DNS. First, many implement automatic security policies that prioritize DNS threats. These can be implemented in a DNS server or in a network security device. Second, many are writing DNS policies in standard firewalls or IPS/IDS devices.

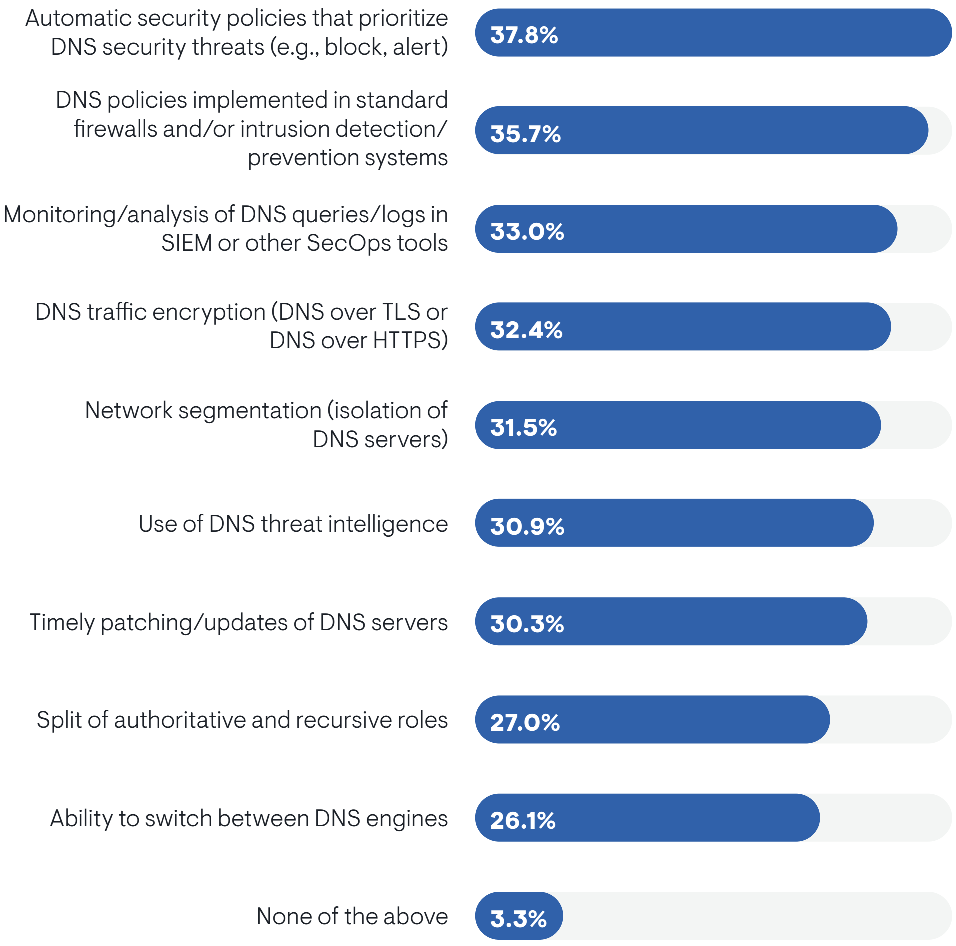
The top secondary method involves the analysis of DNS queries and logs in security monitoring and management tools. This approach was very popular among cybersecurity teams.

"We approach DNS security from a holistic cybersecurity perspective with dedicated tools that ingest data coming from DNS," said a network engineering with a Fortune 500 financial services company. "If we didn't have that ability to get that data out of there, we would be in trouble."

Encryption of DNS traffic was somewhat popular. Cybersecurity and DevOps teams especially favored this method, but network engineering and network operations teams were less likely to use it.

The two least popular methods were splitting authoritative and recursive roles across different servers and setting up the ability to switch to a different DNS engine if the primary is compromised. However, network engineering teams heavily favored both of these techniques.

FIGURE 29. OTHER MEASURES USED TO SECURE DNS INFRASTRUCTURE

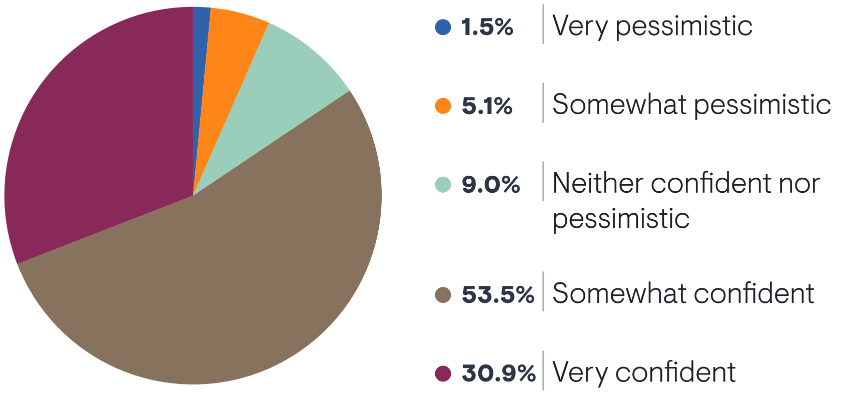


Sample Size = 333, Valid Cases = 333, Total Mentions = 960

How to Ensure DNS Security

Given all the steps that enterprises are taking to protect DNS infrastructure, how effective are these efforts? **Figure 30** reveals that less than 31% of respondents are fully confident in the security of their DNS resources. DNS security confidence correlates very strongly with overall feelings of success with DDI technology.

FIGURE 30. HOW CONFIDENT ARE YOU THAT ALL YOUR ORGANIZATION'S DNS INFRASTRUCTURE IS SUFFICIENTLY SECURE?



Sample Size = 333

EMA observed some concerning gaps between certain respondents on this question. First, IT executives were twice as confident in DNS security as middle management and technical personnel, suggesting that people working closest with DNS are seeing a lot of security risk that CIOs are missing. From a silo perspective, cloud operations and the CIO's suite are very optimistic about DNS security, but network engineering, network operations, and cybersecurity are more concerned. North Americans are more concerned than Europeans, and small enterprises are more concerned than large ones.

We identified several factors in our data analysis that led to better DNS security posture. EMA makes the following recommendations for assuring DNS security:

- Fight for budget – Underfunded DDI teams are least secure
- DDI team must have influence over cloud strategy
- Side note – Poor integration between on-premises and cloud-based DNS AND inconsistent DNS capabilities across multiple cloud providers BOTH erode DNS security confidence
- Remove free/bundled DNS solutions like Microsoft DNS
- Adopt a DDI vendor with strong APIs and make sure your team knows how to use them
- Establish extensive integration between IPAM and DNS
- Gain single-pane-of-glass visibility and management over all your DNS infrastructure
- Establish effective and trusted DDI automation, especially around DNS
- Establish DDI as an effective network source of truth
- Look for DDI vendors with strong network and cloud discovery features
- Deploy a DNS firewall
- Implement DNSSEC

Unsurprisingly, we also observed that organizations that make security features a factor in DDI vendor selection are more confident in DNS security. On the other hand, organizations that based vendor selection on third-party DHCP and DNS overlay management are less secure.

On the subject of DDI solution APIs, enterprises are less confident in DNS security when those APIs lack feature parity with the solution's GUI-based management.

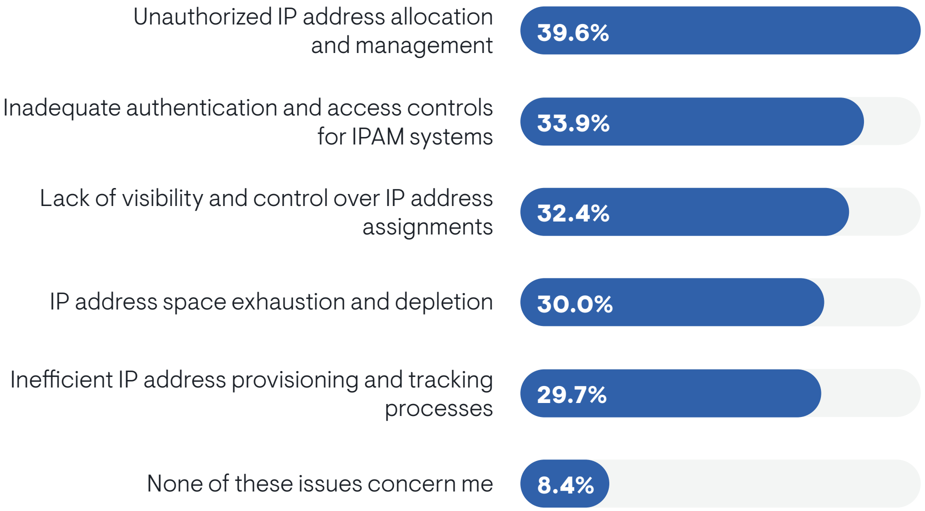
Finally, organizations that lack confidence in DNS security are more likely to feel vulnerable to DNS amplification attacks and don't think they have an adequate ability to access DNS logs for analysis.

IPAM Security

Threats and Risks

Figure 31 reveals the top IPAM security concerns that organizations are contending with. The top concern is unauthorized allocation and management of IP addresses. Cloud operations professionals expressed the most concern about this issue, suggesting it's something that becomes more problematic when enterprises deploy infrastructure into the public cloud.

FIGURE 31. WHICH IPAM SECURITY CHALLENGES CONCERN YOU THE MOST?



Secondarily, many organizations are concerned that their IPAM tools lack good authentication and access controls. For example, some organizations might want multifactor authentication and role-based access control. The network operations team was especially concerned about this issue, as were midmarket companies in general.

Sample Size = 333, Valid Cases = 333, Total Mentions = 580

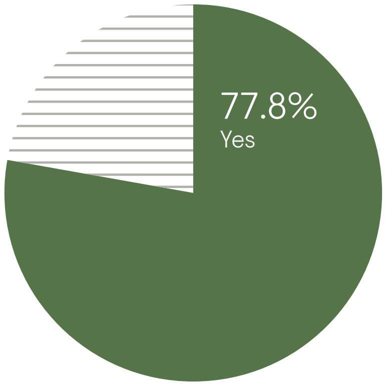
The other big issue is a lack of visibility and control over IP address assignments. Network teams lack the visibility they need to determine whether address assignments pose a security risk. IT executives were less concerned by this issue, but middle managers and technical personnel made it a top issue. Members of DevOps teams were also concerned.

IPAM Security Measures

Figure 32 shows that nearly 78% of organizations are taking specific actions to secure their IPAM tools. IT middle managers and executives were the most likely to report this activity. Technical personnel, who work the most closely with IPAM tools, are less aware of such steps to secure them. In fact, members of the network engineering team and the IT architecture group reported the least amount of activity on this front. Multi-cloud architecture appears to motivate a more secure approach to IPAM, especially organizations that use four or more cloud providers.

78% of organizations are taking specific actions to secure their IPAM tools.

FIGURE 32. DOES YOUR ORGANIZATION TAKE ANY SPECIFIC STEPS TO SECURE ITS IP ADDRESS MANAGEMENT SOLUTION?



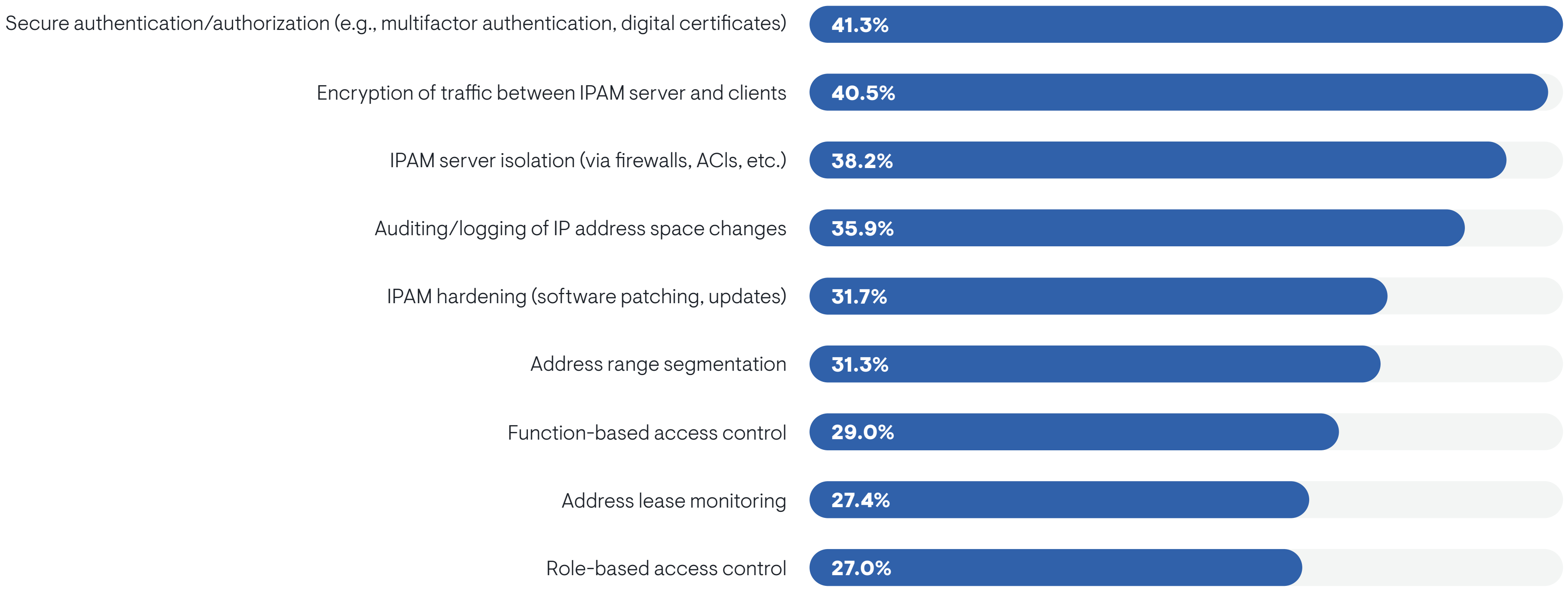
Sample Size = 333

Figure 33 reveals what measures organizations are adopting to secure IPAM. First, many organizations are leveraging advanced authentication and authorization controls, like multifactor authentication. Cybersecurity, cloud operations, and network operations teams all favored this technique, but the network engineering team and the CIO's suite were less likely to perceive its use.

The second most common security measure is encryption of traffic between IPAM servers and clients. However, this measure appears to add complexity to DDI services. Organizations that are less successful with their overall DDI efforts were the most likely to report this encryption.

The other most popular security measures were server isolation and auditing and logging of address space changes. Auditing and logging were particularly popular with multi-cloud enterprises, as was address range segmentation. Role-based access control was least popular but cloud operations and DevOps teams favored it, probably because it enables them to interact directly with IPAM solutions that network engineering and network operations teams own administratively.

FIGURE 33. IPAM SECURITY MEASURES THAT ARE IMPLEMENTED



Sample Size = 259, Valid Cases = 259, Total Mentions = 783

DHCP Security

DHCP security is a lower-profile issue than DNS security. In fact, EMA has observed very little discussion of the topic across the networking industry. Nevertheless, we explore it here in depth.

Threats and Risks

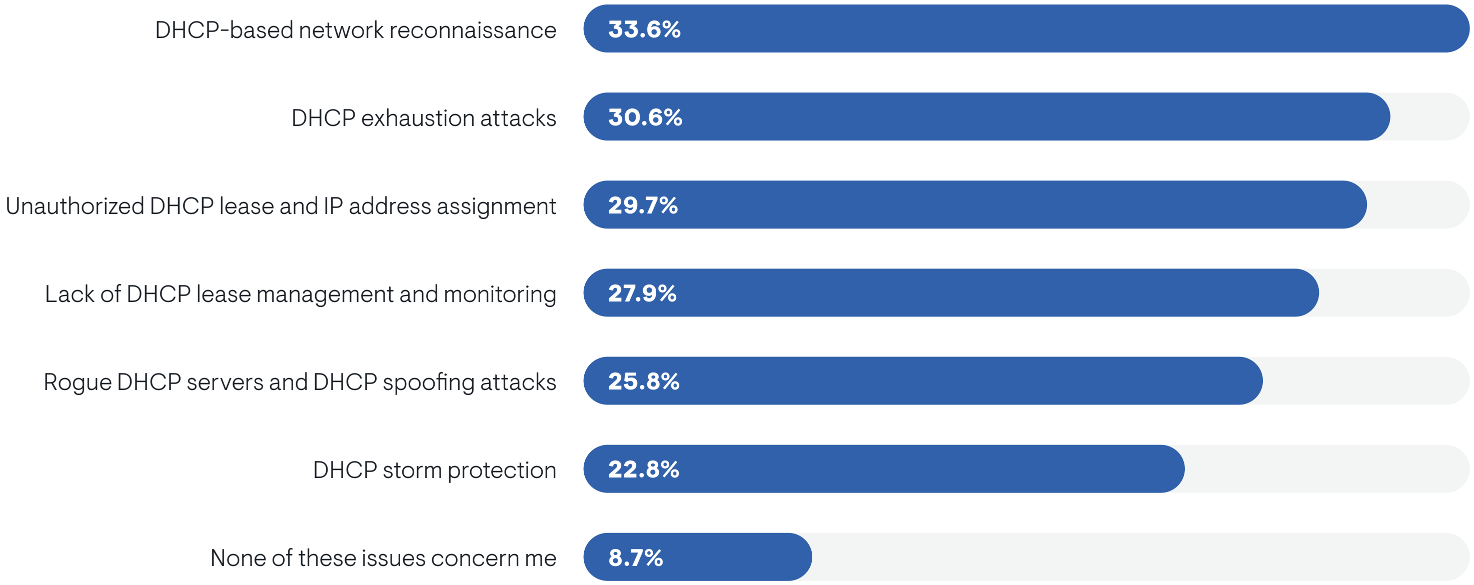
Figure 34 reveals the DHCP security issues with which organizations are most concerned. DHCP-based reconnaissance is the top issue. A malicious actor will send connection requests to a DHCP server, then use the information returned by the server to learn information about the rest of a network, such as domain names and server names.

DHCP exhaustion attacks are the next biggest concern. This involves a malicious actor flooding a DHCP server with connection requests until the server runs out of IP addresses. This disrupts operations because the DHCP server is unable to assign addresses to legitimate client devices, which are then unable to connect to the network. Multi-cloud enterprises were more likely to have concerns about this form of attack.

Unauthorized lease management is another major issue. This can involve an attacker sending fraudulent lease renewal requests to a DHCP server to hijack the address lease and intercept communications meant for the original lease holder. Multi-cloud enterprises were more concerned by this issue.

Rogue DHCP servers and spoofing are relatively minor concerns, but organizations that are less successful with DDI overall cited it as one of their biggest concerns. Cloud operations teams were also very concerned about it.

FIGURE 34. WHICH DHCP SECURITY CHALLENGES CONCERN YOU THE MOST?

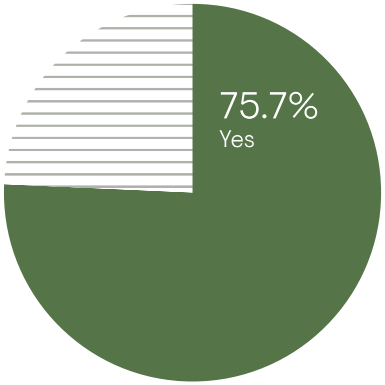


Sample Size = 333, Valid Cases = 333, Total Mentions = 597

DHCP Security Measures

Figure 35 reveals that nearly 76% of organizations take active measures to secure their DHCP infrastructure. Again, EMA believes this number is high. Only 66% of technical personnel were aware of such measures. Members of network engineering and IT architecture teams were the least aware of them, while members of CIO's suites, network operations, cloud operations, and cybersecurity were more likely to perceive them.

FIGURE 35. DOES YOUR ORGANIZATION TAKE ANY SPECIFIC STEPS TO SECURE ITS DHCP INFRASTRUCTURE?

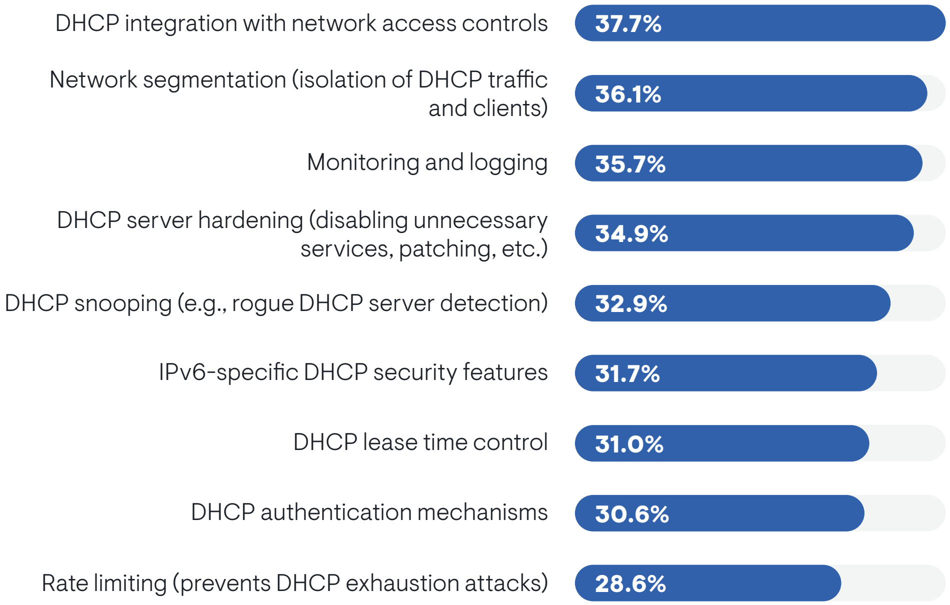


Sample Size = 333

Multi-cloud enterprises were more likely to lock down DHCP, suggesting that such architectures prompt more aggressive approaches to securing these services.

Figure 36 reveals the efforts that organizations take to secure DHCP. First, they integrate DHCP with network access controls, which enables DHCP to allocate addresses based on policies that are connected to things like user identity and device role. Next, they attempt to isolate DHCP servers via network segmentation to protect them and their communications from malicious activity. This approach is more popular in enterprises with multi-cloud architectures. Multi-cloud enterprises were also more likely to use DHCP snooping to look for issues like rogue DHCP servers.

FIGURE 36. DHCP SECURITY MEASURES THAT ARE IMPLEMENTED



DHCP monitoring and logging is the third most popular approach to securing DHCP. Cloud operations teams are more likely to favor this than network engineering and network operations teams.

Finally, rate limiting, which can prevent malicious activity like DHCP exhaustion attacks, was the least popular security tactic. However, organizations that have the most success with DDI overall are more likely to adopt this approach, suggesting that it's a best practice.

Sample Size = 252, Valid Cases = 252, Total Mentions = 754

Network Automation with DDI

DDI solutions play multiple roles in network automation. First, many enterprises rely on automated workflows within a DDI product to streamline operations. Second, the data contained within a DDI solution is essential to broader network automation toolsets. Network teams often reference this data to plan and implement the changes they make to their networks via their third-party network automation tools in this context. Many IT organizations refer to their DDI solution as a "source of truth" for network automation.

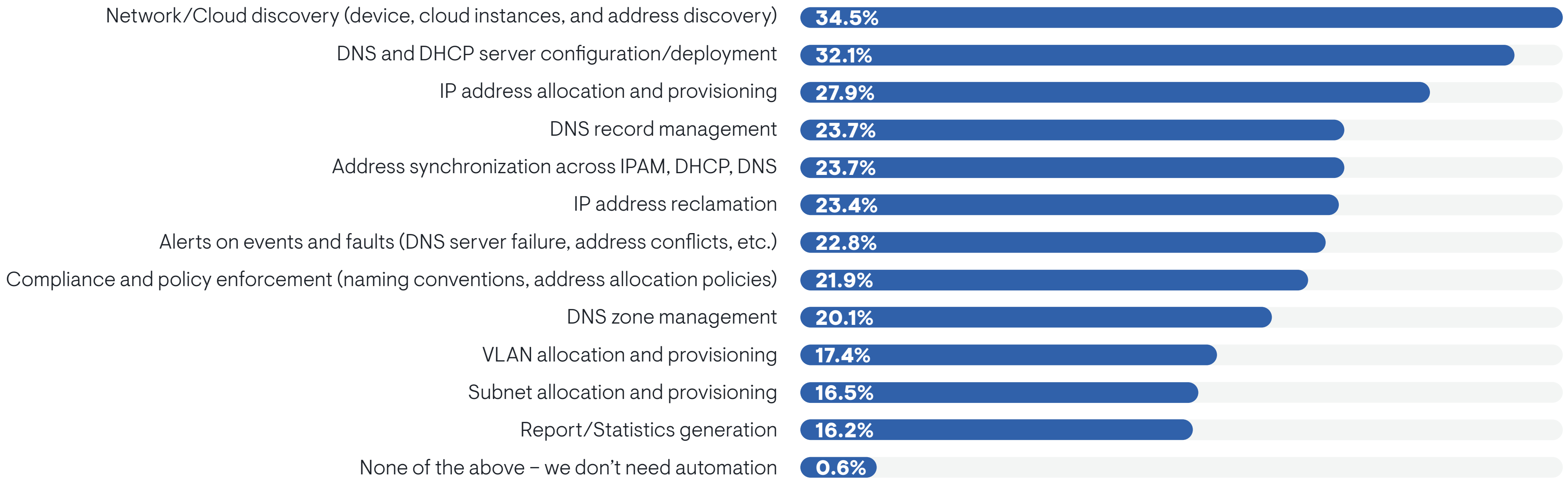
Automating DDI Workflows

Figure 37 reveals which workflows organizations most need to automate when managing network services with a DDI solution. Overall, 99% of respondents indicated that they need to automate at least one workflow. There are two clear priorities: they want to automate the process of discovering network and cloud infrastructure and they want to automate DHCP and DNS server deployment and configuration. Midmarket enterprises were especially likely to automate DHCP and DNS server management, and small enterprises had a stronger affinity for automating discovery.

Among the many secondary automation priorities, DNS record management was more important to the most successful users of DDI solutions, suggesting automation of this process is a best practice focus.

Cloud operations teams were more likely to automate address synchronization across the DDI stack, compliance and policy enforcement, and network/cloud discovery. Cybersecurity also prioritized discovery automation. The network engineering team singled out automated alerts on events and faults as a top priority.

FIGURE 37. MOST IMPORTANT AUTOMATED WORKFLOWS TO HAVE IN A DDI SOLUTION

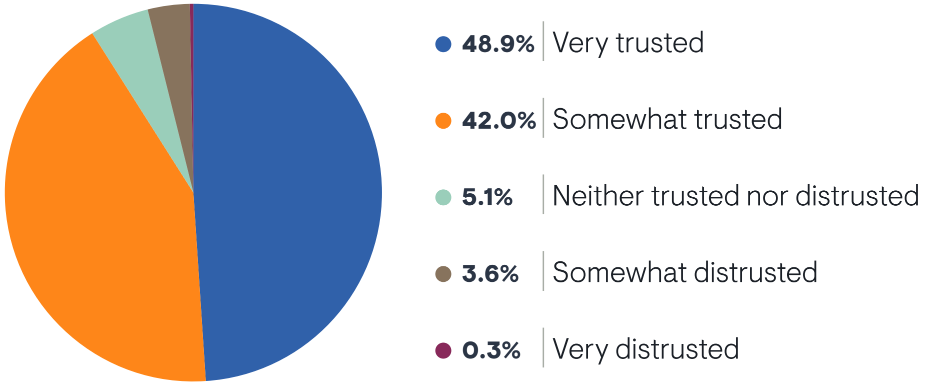


Sample Size = 333, Valid Cases = 333, Total Mentions = 936

Trust in Automated DDI Workflows

Figure 38 reveals that most organizations have at least some trust in the automated workflows in their DDI solutions. However, only 49% indicated that they had complete trust in this automation, while 42% had some misgivings (somewhat trusted) and nearly 4% outright distrusted this automation. Lukewarm trust in automation suggests that many enterprises have DDI solutions that are deficient in how they automate workflows. This can put organizations at risk of failure. EMA found that organizations that are more skeptical of their DDI automation are more likely to have unsuccessful or only partially successful implementations of DDI technology.

FIGURE 38. TO WHAT EXTENT DOES YOUR IT ORGANIZATION TRUST THE AUTOMATED WORKFLOWS IN YOUR DDI SOLUTION?



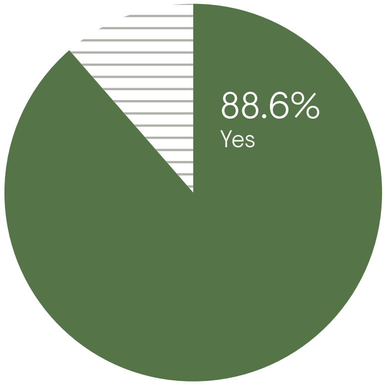
Midsized and large enterprises were also more skeptical than small enterprises. Technical personnel and IT middle management were more skeptical of this automation than IT executives. From a silo perspective, network engineering, DevOps, IT architecture, and IT project management groups were the biggest skeptics. The CIO's suite, cloud operations, network operations, cybersecurity, and IT asset/vendor management groups were more trusting of this automation.

Sample Size = 333

Network Source of Truth

A network source of truth is a repository of data that provides information about network intent and network state. As mentioned earlier, network managers rely on this data when using network automation tools to configure and manage a network. **Figure 39** reveals that nearly 89% of respondents consider their DDI solutions to be such a resource for automation.

FIGURE 39. DO YOU CONSIDER YOUR DDI SOLUTION TO BE A SOURCE OF TRUTH FOR NETWORK AUTOMATION?



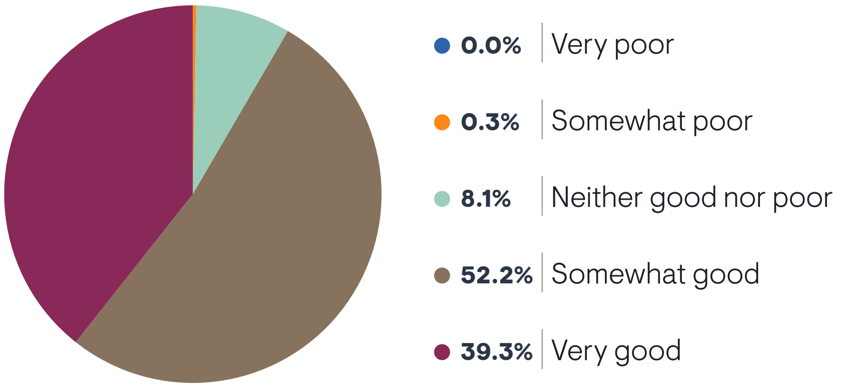
Multi-cloud enterprises were more likely to use DDI as a source of truth, suggesting that it plays an important role in enabling network automation across multiple cloud providers. Network engineering and IT architecture groups were less likely to use DDI as a source of truth. Instead, most of the interest came from the CIO's suite, network operations, cloud operations, and cybersecurity. Small enterprises were most likely to use DDI as a source of truth.

Sample Size = 333

Effectiveness as a Source of Truth

Figure 40 reveals that most respondents who use DDI as a source of truth believe it is at least somewhat effective. More than 39% believe their DDI solution is a very good source of truth and 52% believe it is somewhat good, but has room for improvement.

FIGURE 40. HOW WOULD YOU RATE YOUR DDI SOLUTION AS SOURCE OF TRUTH FOR NETWORK AUTOMATION?



Sample Size = 295

Anecdotally, technical debt and skills gaps appear to be an issue with sources of truth. “Our lead engineer, who deployed IPAM, also built the Ansible playbook to integrate IPAM as a source of truth,” said a project manager with a Fortune 500 energy and chemical company. “That engineer left and Ansible hasn’t been kept up to date. Now, that process is pretty broken.”

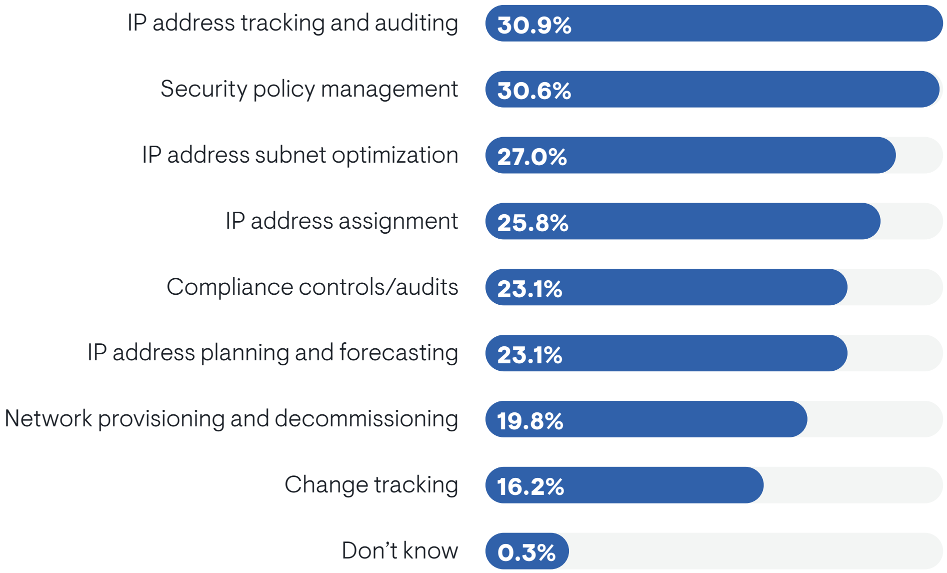
Overall success with DDI technology correlates strongly with whether a DDI solution is a very effective source of truth for network automation. Much of the optimism about this issue comes from IT executives, while technical personnel are more skeptical. Respondents from DevOps, cloud operations, and network operations were also optimistic, while members of network engineering and IT architecture groups wanted to see more improvement in this area.

Source of Truth Use Cases

Figure 41 reveals the use cases for a source of truth respondents were most enthusiastic about. IP address tracking and auditing and security policy management are the biggest opportunities. Cybersecurity professionals were especially interested in security policy, while network engineering personnel were less interested.

IP address subnet optimization and IP address assignment were secondary priorities. Compliance controls and audits were a lower priority, but Europeans were especially interested. IP address planning and forecasting was another low priority, but network engineering, network operations, and cybersecurity all made it a high priority. Change tracking was the lowest priority, but people who worked in a highly technical role selected it more often.

FIGURE 41. MOST VALUABLE USE CASES FOR A DDI-BASED NETWORK SOURCE OF TRUTH



Sample Size = 333, Valid Cases = 333, Total Mentions = 656

APIs and Integration

Application programming interfaces (APIs) are an essential part of any IT operations management tool, and DDI solutions are no exception to that rule. EMA spoke to DDI engineers at very large companies who have switched vendors due to poor APIs. DDI APIs enable IT organizations to customize DDI solutions, automate them, and integrate them with other systems. Nearly 83% of respondents in this research told EMA that their DDI solutions had APIs available.

The Criticality of Effective DDI APIs

Figure 42 reveals that less than 44% of respondents who have APIs available to them are fully satisfied with those APIs. Larger enterprises, which have more engineering resources capable of using APIs and more use cases to pursue, were the least satisfied with their APIs. Members of network engineering teams and the CIO's suite were more satisfied, but IT project management professionals were less satisfied.

API satisfaction is extremely important to overall success with DDI solutions.

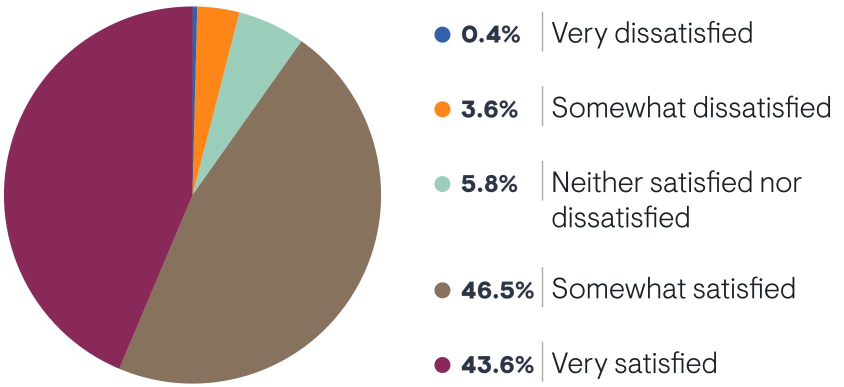
Respondents who use a DDI specialist vendor for IPAM, as opposed to a DCIM vendor or general network management vendor, tended to be happy with their APIs.

EMA's research data revealed that API satisfaction is extremely important to overall success with DDI solutions. For instance, 70% of successful DDI professionals were completely satisfied with their APIs, but only 17% of unsuccessful DDI professionals felt that way.

Satisfaction with DDI APIs also correlated very clearly with:

- Trust in automated DDI workflows
- Satisfaction with using DDI tools as a source of truth for network automation
- DDI teams having enough influence on overall cloud strategy
- Confidence in DNS security
- Effective integration of on-premises IPAM tools with IPAM tools used in the public cloud

FIGURE 42. HOW SATISFIED ARE YOU WITH THE APIS YOUR DDI SOLUTION OFFERS?



Sample Size = 275

API Problems

Figure 43 reveals the challenges that organizations are having with DDI APIs. API quality and complexity are the two top issues. The secondary problems with APIs are documentation, additional API licensing, performance, and poor SDK API documentation. Overall, API dissatisfaction correlated directly with complexity and documentation problems, suggesting these two issues have strong impacts on whether organizations can effectively use APIs.

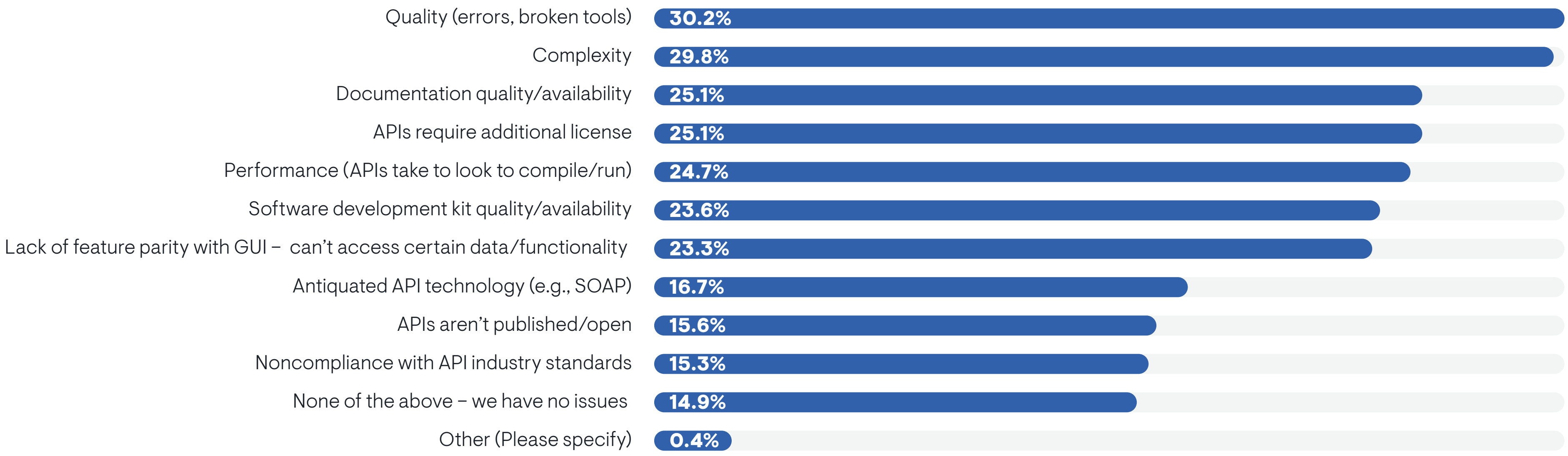
Although only a secondary challenge, organizations that cited additional API licensing as a problem were more likely to report less overall success with DDI technology. Certain API challenges become more painful with multi-cloud adoption. Organizations that use more than one cloud provider reported more problems with API quality and SDKs.

Documentation and SDKs would help a network engineer with a midmarket software company get more value from his vendor's APIs. "Those APIs are wonderful. I only wish they had more examples in their knowledgebase for how to use them. I need a library for how you can use them, with examples like quick tools for generating reports or making a VPN connection."

API feature parity with a tool's GUI is a relatively minor issue, but small enterprises struggled with it more often, as did the cybersecurity team. Cybersecurity also complained about API performance more than other groups, including network engineering.

"I would like to interact with the system through the API the same way I would through the GUI," said a network engineer with a Fortune 500 financial services company.

FIGURE 43. MOST SIGNIFICANT PROBLEMS ORGANIZATIONS ENCOUNTER WITH APIS ON THEIR DDI SOLUTIONS



Sample Size = 275, Valid Cases = 275, Total Mentions = 673

Essential API Use Cases

Figure 44 reveals how organizations want to use these APIs. The priority is the enablement of automation. For example, by integrating a DDI solution with third-party network automation tools, the DDI solution can serve as a source of truth for that automation tool. The second use case is security and compliance enforcement. For example, when integrated with a DDI solution, a network access control tool can confirm that IP addresses are assigned to the right users and devices before making a policy enforcement decision. Unfortunately, EMA uncovered evidence that organizations that pursue API-driven security and compliance enforcement often struggle. They are more likely to be dissatisfied with their APIs and more likely to be unsuccessful with their overall DDI efforts.

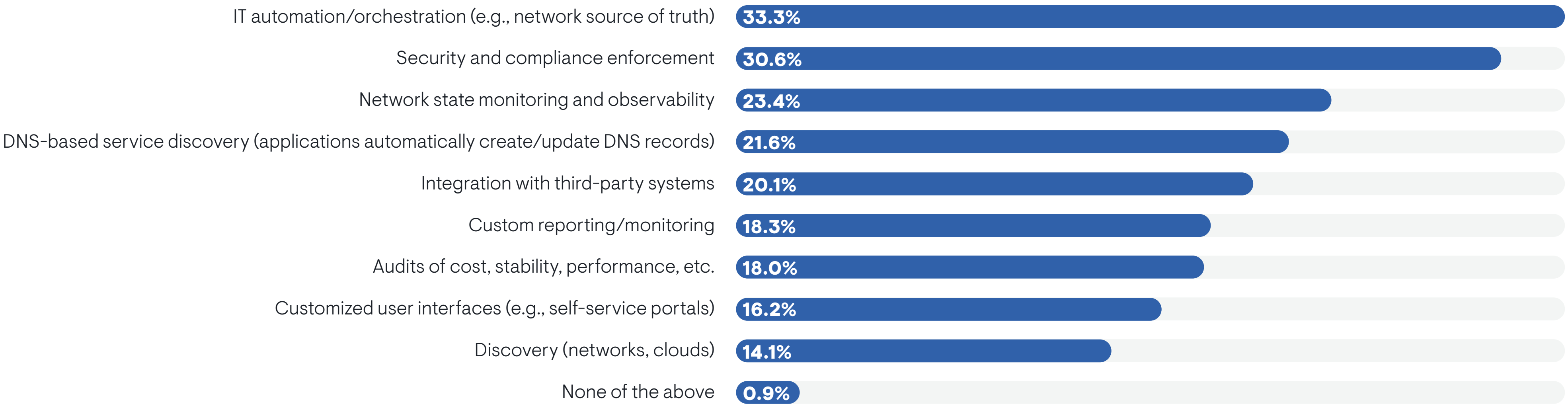
“We use the APIs for everything from collecting information and automating tools to generating reports,” said a network engineer with a Fortune 500 consulting company. “We also use it for configuration. We have a ticketing system that says, ‘I need to update this rack and reserve its network,’ and the ticket goes out to operations.”

Enablement of network monitoring and observability with APIs is a secondary use case, but it was much more popular with organizations that are highly satisfied with their APIs.

Network operations teams were the most likely to use APIs to integrate DDI with third-party systems. The DevOps group and the CIO’s suite were more likely to create customized user interfaces, such as self-service portals. DevOps and cybersecurity were more likely to enable audits with APIs.

> *“We use the APIs for everything from collecting information and automating tools to generating reports,” said a network engineer with a Fortune 500 consulting company.*

FIGURE 44. TOP USE CASES FOR APIS OFFERED BY DDI SOLUTION



Sample Size = 333, Valid Cases = 333, Total Mentions = 655

DDI Integrations

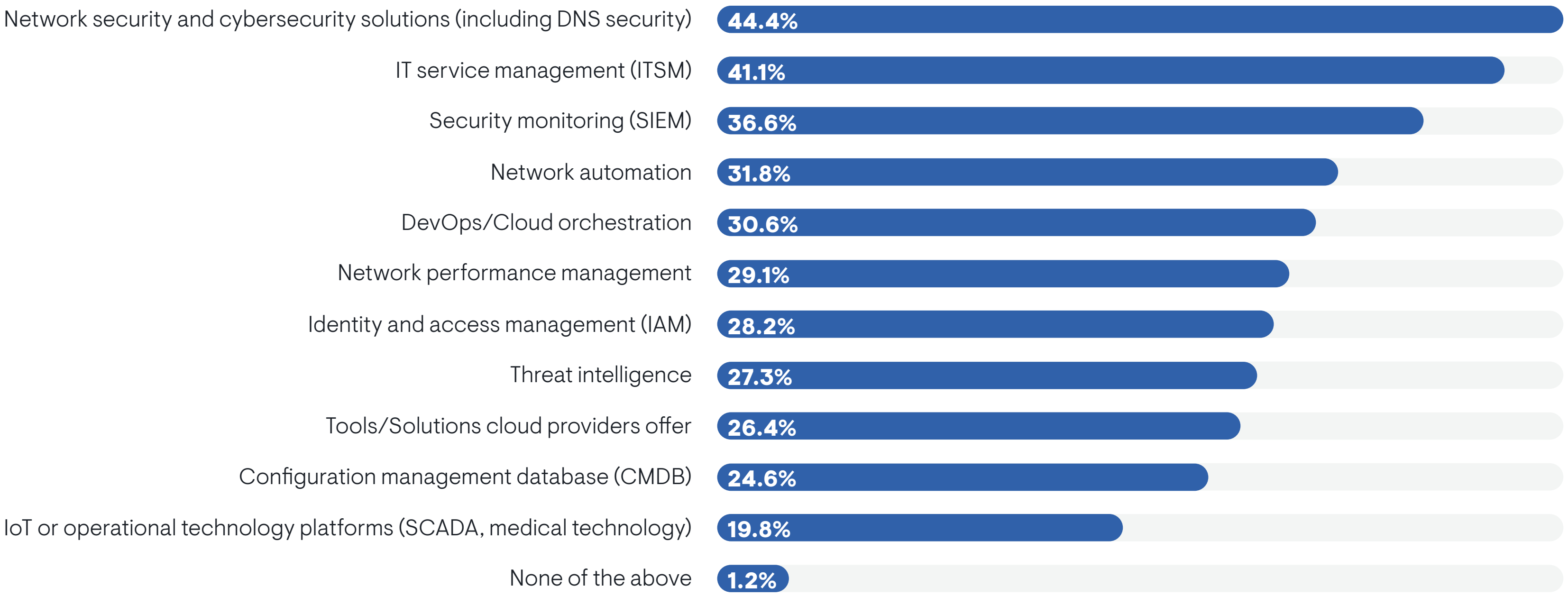
Figure 45 reveals the systems organizations need to integrate with their DDI solutions. The top priority is with network security and cybersecurity solutions, which echoes the popularity of the security and compliance enforcement API use case revealed in the previous chart. The second integration priority is with IT service management, which enables integration of change and trouble tickets.

"We're trying to get to the point where we can take advantage of APIs to get DDI integrated with ServiceNow. There would be an automation benefit. But we're not there yet," said a project manager with a Fortune 500 energy and chemical company.

Security monitoring, network automation, and DevOps/cloud orchestration round out the top integration priorities. Multi-cloud enterprises were more likely to integrate DDI with security monitoring solutions, as well as tools and solutions cloud providers offer. Cybersecurity teams had more interest in integrating with network automation and DevOps/cloud orchestration, as well as identity and access management tools.

Successful users of DDI technology were more interested in integrating with network performance management tools. The largest enterprises in this research were integrating with CMDBs.

FIGURE 45. SYSTEMS THAT ORGANIZATIONS INTEGRATE OR NEED TO INTEGRATE WITH THEIR DDI SOLUTIONS



Sample Size = 333, Valid Cases = 333, Total Mentions = 1,137

DDI and Public Cloud

Many DDI Teams Lack Cloud Influence

In other research, EMA observed that many cloud teams adopt DNS, DHCP, and IPAM technology in the public cloud without the involvement of the core DDI team. This leads to fragmentation of core network services across cloud and on-premises networks. We believe the enterprise DDI team needs to be involved from the beginning of any cloud migration so cloud networks are effectively integrated into the overall corporate network.

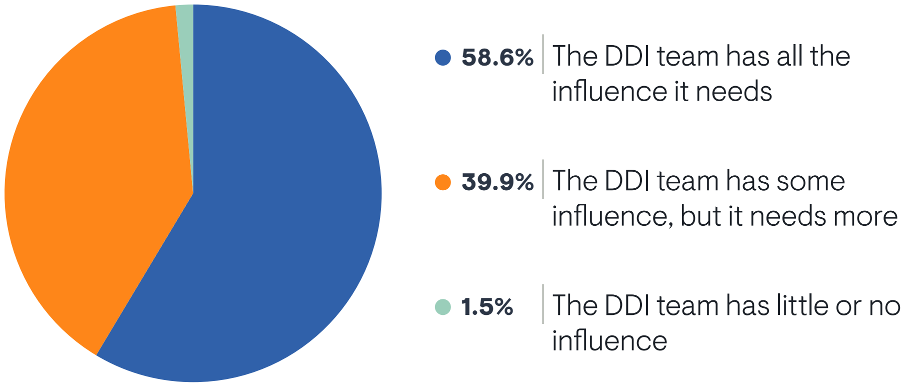
44% of DDI teams believe they don't have enough influence over how DNS, DHCP, and IPAM are implemented and managed in the public cloud.

Figure 46 explores this issue. It reveals that 44% of DDI teams believe they don't have enough influence over how DNS, DHCP, and IPAM are implemented and managed in the public cloud.

"We try to work together with the cloud team," said a network engineer with a Fortune 500 consulting company. "Five years ago, that wasn't happening. There was a lot of risk. It's easy to do things in the cloud without collaborating with network engineering and security. It can create problems."

DDI teams that lack enough influence in the cloud are more likely to report that their overall DDI technology strategy is less successful. EMA also found that IT teams that are peripheral to network management are the only ones who think the DDI team has enough influence. For instance, the CIO suite, the cybersecurity team, and the DevOps team were all very likely to say the DDI team had plenty of say over cloud DDI. On the other hand, the network engineering team, the network operations team, the cloud operations team, and the IT architecture group all tended to say the DDI team needed a bigger voice on cloud matters.

FIGURE 46. DO YOU BELIEVE THAT THE PERSON(S) RESPONSIBLE FOR YOUR DDI TECHNOLOGY HAS SUFFICIENT INFLUENCE OVER HOW DNS, DHCP, AND IPAM ARE IMPLEMENTED AND MANAGED IN YOUR ORGANIZATION'S PUBLIC CLOUD ENVIRONMENT?



Sample Size = 333

Boosting the DDI Team's Voice

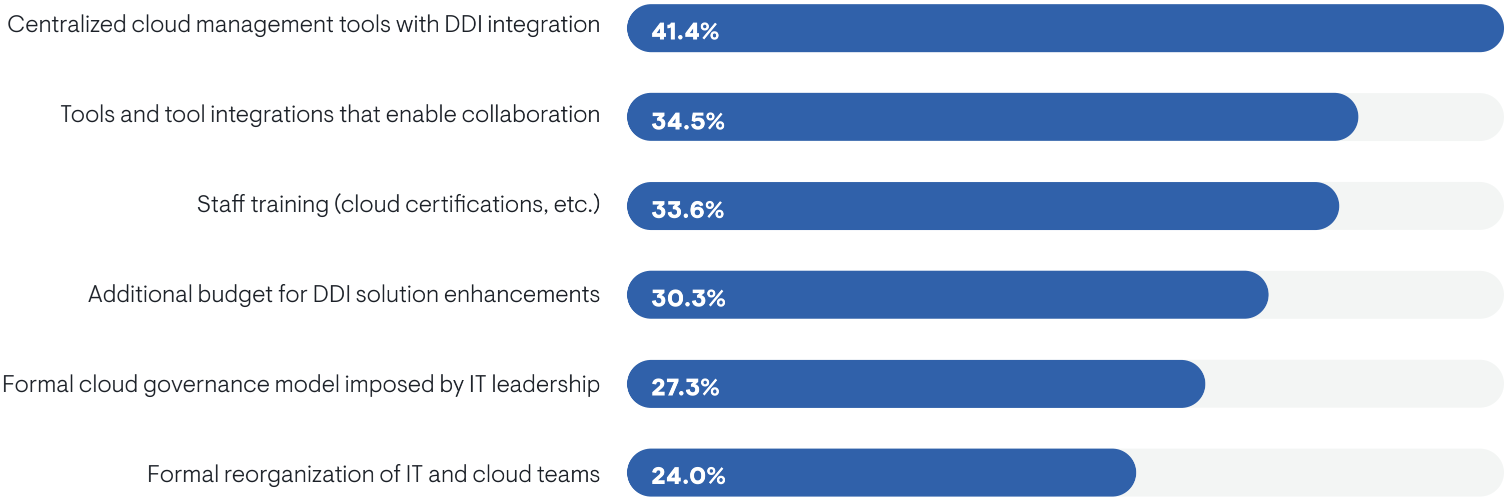
Figure 47 reveals how organizations successfully enhance the influence of DDI teams over cloud strategy. The most popular tactic is to integrate enterprise DDI solutions with a centralized cloud management tool. This allows cloud teams to implement or request changes to a network team's chosen DDI solution through their own management environment. IT executives were more likely than technical personnel to think this fix was effective.

Next, many organizations think that collaboration tools are helpful. These tools encourage DDI and cloud teams to interact directly and solve problems together. This was another solution that IT executives favored more often than technical personnel.

Thirdly, many organizations are training their DDI teams on cloud technology. By upskilling, the DDI team will have more credibility and will be able to assert itself more readily. Technical personnel made this their top priority while IT executives were less likely to favor it.

Some IT leaders try to solve this problem by establishing a formal cloud governance model. Overall, this was a tertiary solution, but it was much more popular in North America than Europe.

FIGURE 47. WHICH OF THE FOLLOWING BEST HELPS TO ENSURE THAT YOUR DDI TEAM HAS SUFFICIENT INFLUENCE IN THE CLOUD?

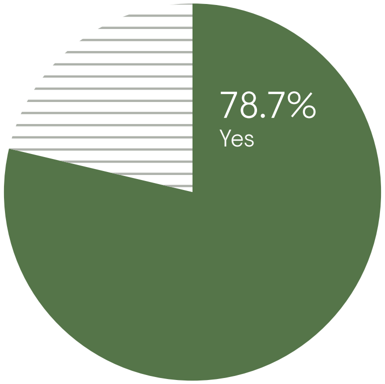


Sample Size = 333, Valid Cases = 333, Total Mentions = 637

Integrated On-Premises and Cloud IPAM

Figure 48 reveals that nearly 79% of enterprises integrate their on-premises IPAM solution into their cloud environment so that it can manage IP address space in the cloud. Organizations that use multiple cloud providers were more likely to do this integration, suggesting that multi-cloud complexity is an incentive for creating consistent approaches to IPAM across on-premises and cloud-based networks.

FIGURE 48. DOES YOUR ORGANIZATION INTEGRATE IP ADDRESS MANAGEMENT IN THE CLOUD WITH ITS ON-PREMISES IP ADDRESS MANAGEMENT SOLUTION?



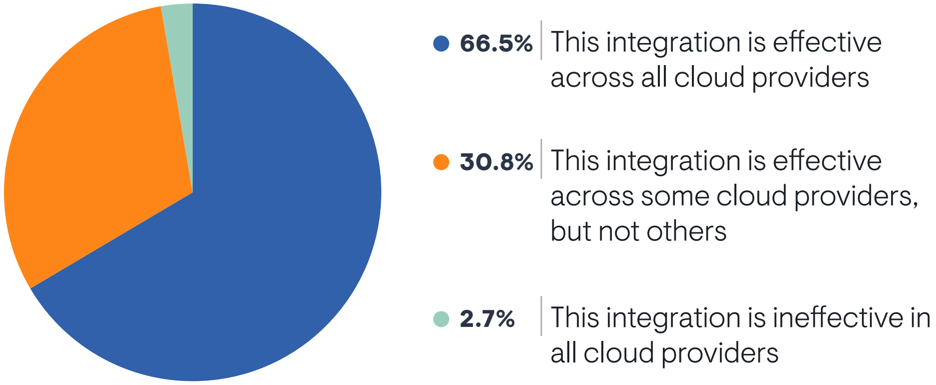
Sample Size = 333

EMA saw two critical knowledge gaps among respondents. First, IT executives and middle management reported a higher number of integrations than technical personnel. Given that technical personnel work the closest with DDI tools, their assessment is probably more accurate. We observed a similar pattern across IT silos. The network engineering and IT architecture groups perceived lower rates of integration while the CIO's suite, cloud operations, DevOps, and cybersecurity all saw more integration happening.

Multi-Cloud Impacts on IPAM Integration

Figure 49 reveals that nearly 34% of multi-cloud enterprises lack consistent and effective integration of IPAM across all their cloud providers. On one hand, it's good that two-thirds claim to have good integration, but the last third will need help.

FIGURE 49. HOW CONSISTENT AND EFFECTIVE IS THE INTEGRATION OF YOUR ON-PREMISES IPAM SOLUTION WITH IP ADDRESS MANAGEMENT IN THE CLOUD ACROSS ALL YOUR CLOUD PROVIDERS?



Members of network engineering and cybersecurity teams were more confident in IPAM integration across cloud providers, while the CIO's suite and cloud operations were pessimists.

Organizations with two or three cloud providers were quite confident in this integration, but that confidence drops once organizations reach four or more cloud providers. Only 36% of respondents with four or more providers were confident in IPAM integrations.

Sample Size = 221

IPAM Requirements in the Cloud

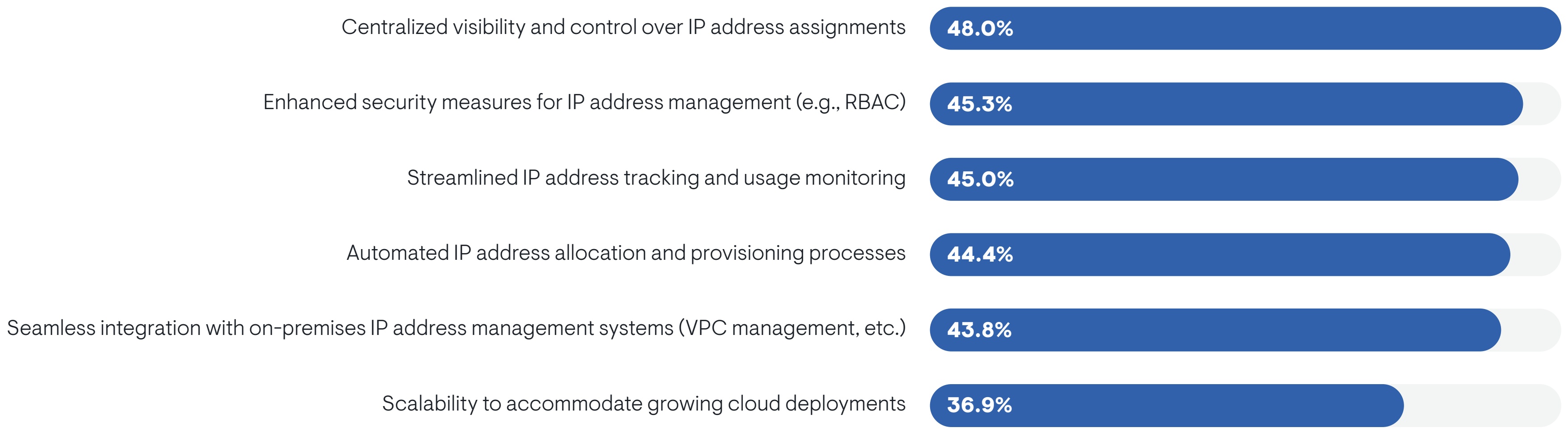
Figure 50 reveals the IP address management requirements that enterprises have identified as important in their public cloud environments. Centralized visibility and control over address assignment is the biggest need, which makes sense given the lack of control that network teams often have over what happens in the cloud. Respondents who were the most successful with DDI were the most likely to want this capability. This control was more important to respondents from network engineering and CIO's suites and less important to cybersecurity personnel.

Centralized control over address assignments in the cloud was especially important to a network engineer at a Fortune 500 financial services company. "Some of our processes have shifted to ensure we limit the number of overlapping subnets we have in Azure. Our vendor doesn't handle that, so it's been a bit of a headache working in the cloud. It slows things down a bit."

The second requirement is enhanced security measures around IPAM, such as role-based access control, alerting for suspicious behavior, and encrypted communications between an IPAM system and endpoints. Again, more successful DDI professionals were more likely to seek these capabilities.

Scalability to accommodate growing cloud deployments was the lowest priority overall, but respondents from multi-cloud enterprises were much more likely to select it. Members of cloud operations and cybersecurity teams also made it a top priority.

FIGURE 50. SPECIFIC REQUIREMENTS FOR IP ADDRESS MANAGEMENT IN THE PUBLIC CLOUD



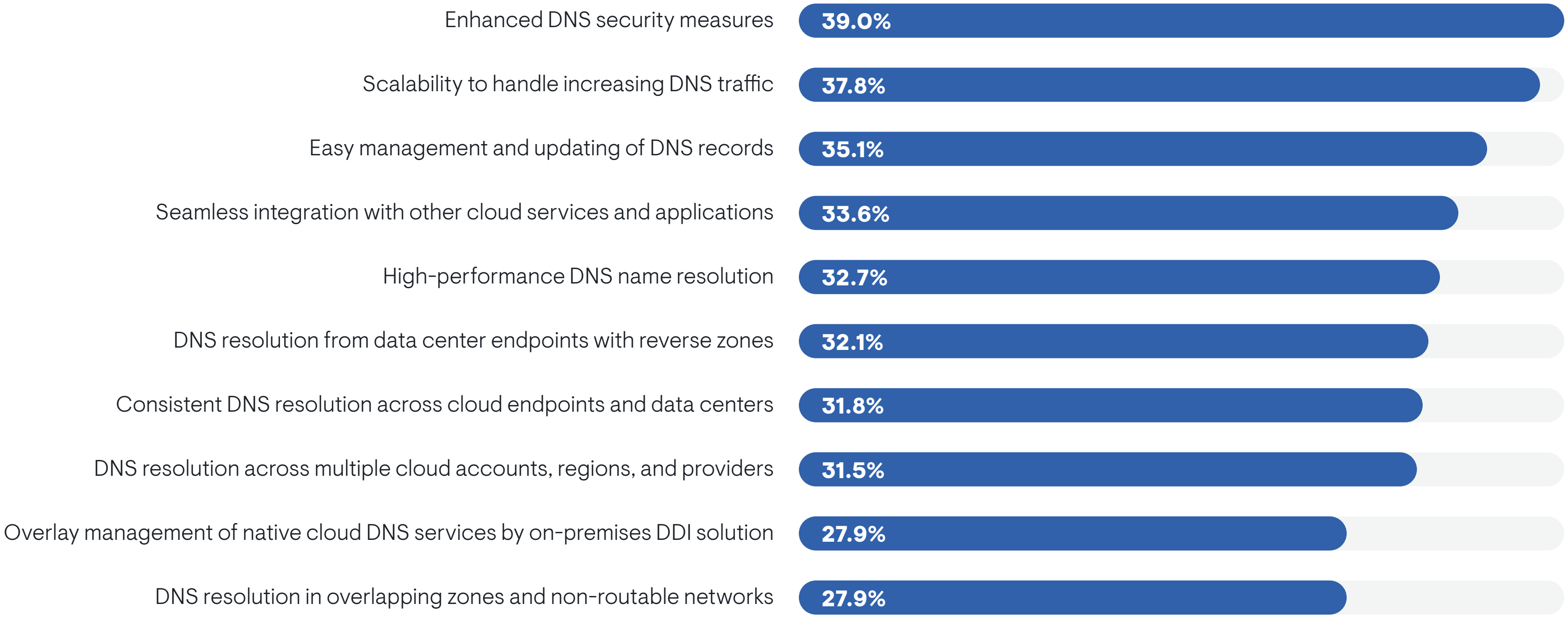
Sample Size = 333, Valid Cases = 333, Total Mentions = 878

DNS Management Requirements in the Cloud

Figure 51 identifies the top DNS management requirements that enterprises have for public cloud environments. Enhanced security is the top concern, and it's a best practice. Respondents who reported the most success with their DDI efforts were more likely to select this option. The second priority is scalability to handle increases in DNS traffic. This second requirement makes perfect sense given that many enterprises use the cloud to rapidly scale applications and services. Cybersecurity and IT asset/vendor management teams were more likely to identify this requirement.

Easy management and updating of DNS records was also a top priority. The network engineering team was especially likely to see a need for this enhancement. Small enterprises were more likely than large enterprises to need high-performance DNS resolution and resolution in overlapping zones and non-routable networks. This latter requirement was very important to DevOps teams. The cloud operations team prioritized seamless integration with other cloud services and applications, and the cybersecurity team selected DNS resolution from data center endpoints with reverse zones more often than other groups.

FIGURE 51. SPECIFIC REQUIREMENTS FOR DNS MANAGEMENT IN THE PUBLIC CLOUD



Sample Size = 333, Valid Cases = 333, Total Mentions = 1,099

DNS resolution across multiple cloud regions was a top priority for a network engineer with a Fortune 500 financial services company. “We’ve had to deploy servers in every major Azure region that we’re in to provide that extra step of resolution and to make sure we’re able to resolve things the way we need.”

Overlay management of cloud DNS by an on-premises DDI solution was a top priority for a network engineer with a Fortune 500 consulting company, but he had challenges with his current vendor. “We want to replicate what we have on-premises in the cloud, but we need some special features on our DDI product so that it can go out and discover cloud resources, which are a lot more dynamic. Right now, we don’t have the same control.”

Multi-cloud enterprises had three unique DNS management requirements:

- High-performance DNS resolution
- DNS resolution in overlapping zones and non-routable networks
- DNS resolution across multiple cloud accounts, regions, and providers

Multi-Cloud Networks and DDI

Throughout this research, we have highlighted instances where DDI experts who are supporting multi-cloud networks differ from their peers at single-cloud enterprises. Here are those findings consolidated and presented as recommendations for multi-cloud DDI:

- Treat DDI investments as an opportunity to reduce multi-cloud security risk, especially around DNS
- Integrate DDI solutions with your security monitoring tools (e.g., SIEM)
- Implement DNSSEC for improved security
- Be vigilant for unauthorized DHCP leases and DHCP exhaustion attacks
- Integrate your on-premises IPAM solution with your cloud IPAM processes
- Your IPAM tool must be scalable enough to handle growth in the cloud
- Look for DDI solutions that can help you manage multiple third-party DNS services
- Your multi-cloud DNS must provide high performance resolution across overlapping zones and non-routable networks
- Evaluate DDI vendor APIs for quality and ask for a software development kit
- DHCP services in multi-cloud should be architected for high availability with good visibility into lease information
- When evaluating DDI for multi-cloud, evaluate solutions for the quality of their data and data governance
- Look for a DDI solution that can provide a comprehensive network source of truth
- Futureproof your network with IPv6. You may still have surplus IPv4 addresses, but in the meantime, the protocol could improve network performance and enhance security

IPv6 Engagement

The IETF formally ratified IPv6 in 2017. Development of the protocol began decades ago in anticipation of IPv4 address exhaustion. That address exhaustion has largely occurred as of 2019, but service providers, enterprises, and regional internet registries continue to manage, exchange, and auction off reserves of unused and reclaimed IPv4 addresses. IPv6 champions envisioned a future in which IPv4 was retired, but that future appears unreachable. Dual-stack networks are an ongoing reality.

Obviously, IPv6 adoption impacts DDI strategies. If an enterprise elects to implement the protocol, the network team will need to ensure that its DDI solutions can enable that transition.

Very few IT organizations are ignoring IPv6.

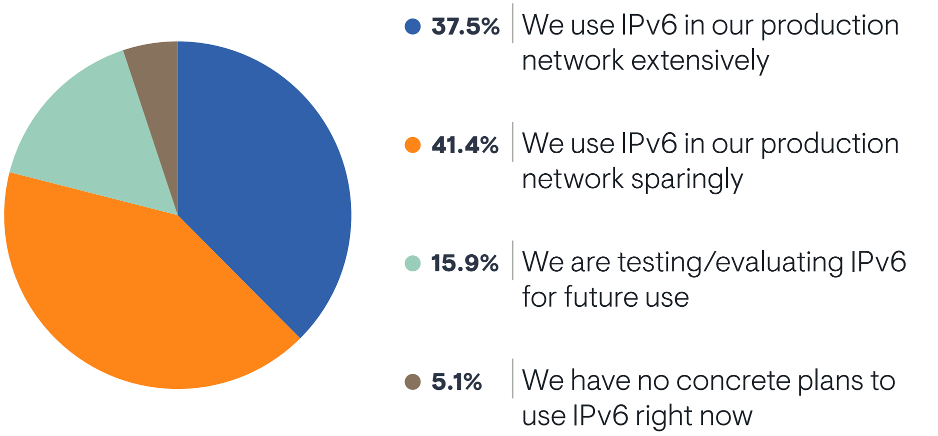
Figure 52 reveals that very few IT organizations are ignoring IPv6. In fact, 95% are using it or anticipate using it in the future. Nearly 38% claim they are using it extensively. IPv6 is a best practice; 61% of the most successful DDI teams reported extensive use of the protocol. Multi-cloud appears to be a driver, too. Only 24% of single-cloud enterprises use the protocol extensively. On the flip side, small enterprises were the most aggressive with their IPv6 usage, possibly because their networks are smaller, less complex, and easier to update.

“In 2019, we sold off a block of IPv4 space with the intention of migrating to IPv6, but we didn’t do it,” said a project manager with a Fortune 500 energy and chemical company.

“We are piloting it,” said a network engineer with a Fortune 500 consulting company. “We’re trying to implement it on-premises.”

DevOps teams were the most likely to perceive broad adoption of IPv6. Cloud operations and cybersecurity teams perceived moderate use. Network engineering and IT architecture teams were the least likely to see significant use. This suggests again that multi-cloud and modern application architectures in general are driving IPv6 engagement. Traditional infrastructure teams are less active.

FIGURE 52. CURRENT USE OF IPV6

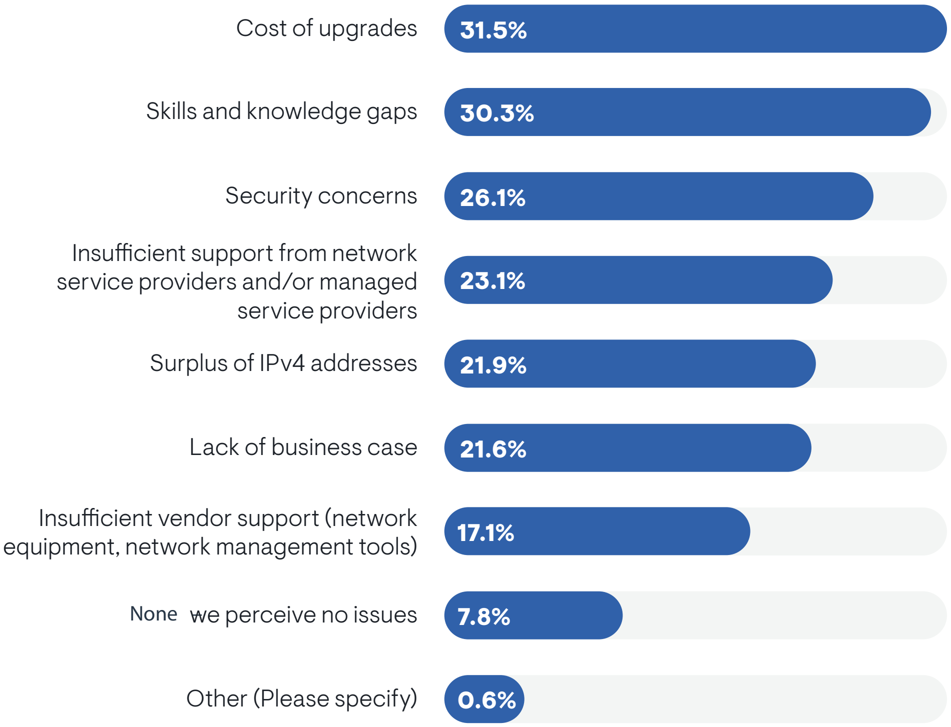


Sample Size = 333

IPv6 Adoption Roadblocks

Figure 53 indicates that IPv6 adoption is most typically delayed by network upgrade costs, skills gaps, and security concerns. Small enterprises were the most likely to cite skills gaps as an issue. It was also a more prominent issue for organizations that report less success with overall DDI strategies. Finally, DevOps and cloud operations teams were more likely to cite the skills gap issue, but network engineering was not.

FIGURE 53. ISSUES MOST RESPONSIBLE FOR INHIBITING OR DELAYING ADOPTION OF IPV6



Sample Size = 333, Valid Cases = 333, Total Mentions = 600

Poor support from service providers, surpluses of IPv4 addresses, and a lack of business case were secondary issues. Network operations and cloud operations teams both pointed to service provider issues more often. Multi-cloud enterprises were more likely to have a surplus of IPv4 addresses. Single cloud enterprises complained more often that they couldn't find an IPv6 business case.

"It's mostly a lack of knowledge. People are afraid of it," said a network engineer with a Fortune 500 consulting company. "Also, not all the ISPs are able to implement IPv6 on their side, so we had some issues with providers who don't implement it properly. The most difficult thing is selling it internally. The only reason we do it is to look like a modern consulting company. We should be cutting edge."

A project manager with a Fortune 500 energy and chemical company said leadership issues inhibited his IPv6 migration. "We've gone through multiple leadership changes and a lot of the leadership that made the decision to sell our IPv4 block and go to IPv6 is gone. So, our strategy has shifted. Now, we're doing a network redesign and IPv6 was just dropped."

"I haven't seen any use for it," said a network engineer with a midmarket software company. "I know we are running out of IPv4 blocks, but I just don't see a need yet. I understand that it's a superior technology, but if vendors put out a guidebook for how I can really benefit from it and outline how to get those benefits, I'd be interested in learning more."

Motivations for IPv6 Adoption

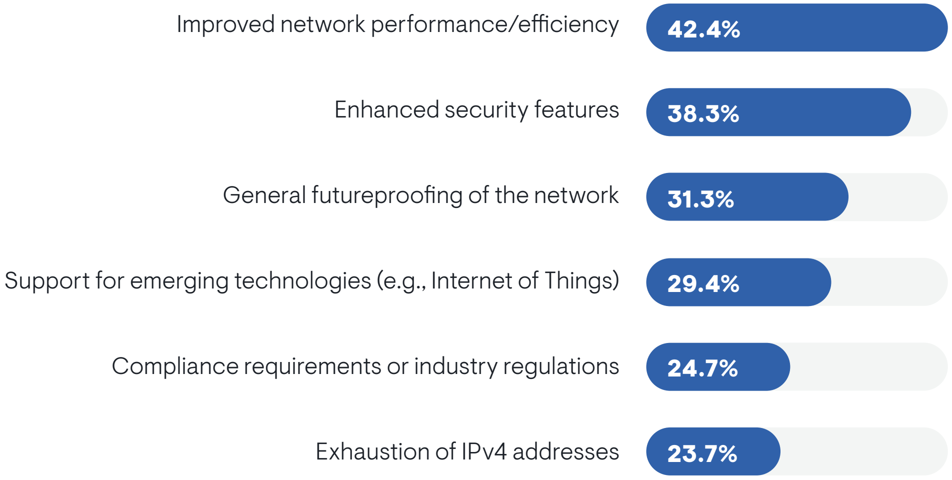
Figure 54 reveals why 95% of organizations are at least planning if not already using IPv6. Exhaustion of IPv4 is not the reason companies move to the new protocol. Instead, they typically look at IPv6 as a technology that can improve network performance and efficiency and enhance security. IT executives were more aware of the opportunity to boost network performance but less likely to see the security benefits. In fact, the one group that was especially focused on security enhancement was cybersecurity.

Secondarily, many companies are anticipating a future in which IPv4 does run out, so they are futureproofing their networks. Many also are driven by a need to support emerging technologies that require IPv6. Compliance was generally an insignificant driver, but the cloud operations team cited it more often.

Multi-cloud enterprises were more likely cite three drivers:

- Futureproofing networks
- Enhanced security
- Improved network performance/efficiency

FIGURE 54. PRIMARY DRIVERS OF USING IPV6



Sample Size = 316, Valid Cases = 316, Total Mentions = 600

Conclusion

This research established that DDI technology is essential to network engineering and operations in the cloud. IT organizations need to integrate their traditional DDI solutions with the tools and processes organizations use for DNS, DHCP, and IP address management in the cloud. With many organizations evolving toward multi-cloud, this need to cloud-enable DDI services is becoming even more critical.

Moreover, EMA found that DDI security is extremely challenging. Few organizations are entirely confident in their DNS security and many are not even taking specific steps to secure DHCP and IPAM. DDI services, especially DNS, are becoming a more frequent target of malicious actors, so organizations must become more vigilant.

Finally, DDI is an essential component of network automation. Workflow automation within DDI tools is essential, but DDI also powers automation in several other ways. Through integrations with other systems like ITSM and security, the technology can automate ticketing of network changes and the collection of telemetry for security analysis. Moreover, DDI tools can serve as a source of truth for broader network automation and IT orchestration platforms. However, data governance will be essential for this to succeed.

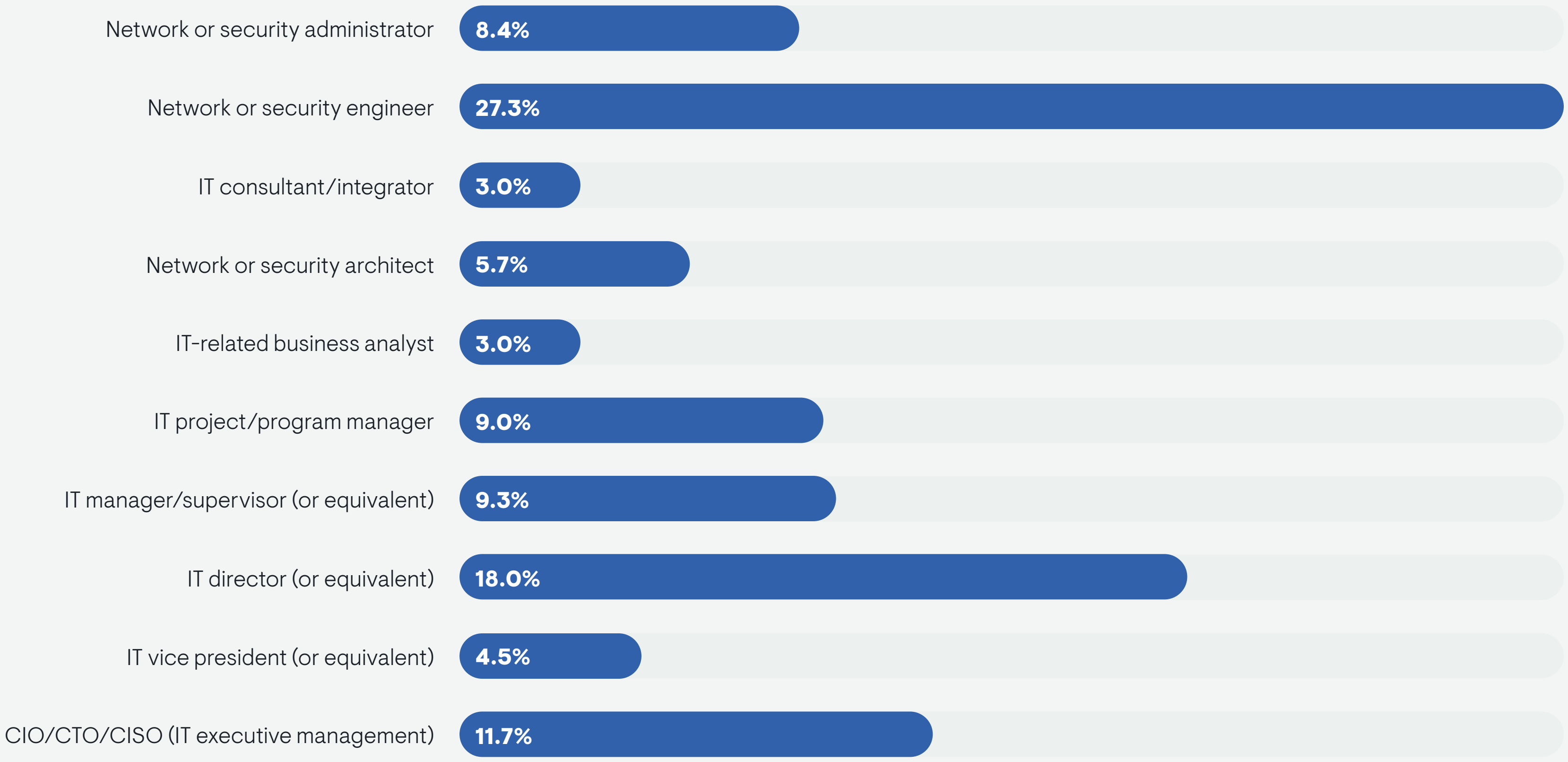
DDI Best Practices

In conclusion, based on our analysis of survey responses by the most successful organizations in this study, EMA offers the following recommendations for DDI best practices:

- Work with DDI specialist vendors for IPAM and DNS.
- Make sure your IPAM tool is extensively integrated with both DNS and DHCP services, either natively or via overlay integration.
- Security features and discovery should be at the top of your list of product requirements when evaluating DDI vendors. DDI services are increasingly targeted and must be protected. Discovery can help network engineering improve visibility into network state, optimize data governance, and track changes.
- Improve DNS security throughout your enterprise by adopting a DNS firewall and DNSSEC.
- Establish DDI as a network source of truth for network automation. If your vendor doesn’t support this, push them to develop this capability.
- Effective DDI APIs are essential to modern IT operations.
- DDI APIs should offer feature parity with the DDI solution’s GUI, they should be based on modern API technology like REST, and they should not require additional licensing.
- DDI teams must have influence over cloud strategy.
- In the cloud, the DDI team should focus on security, especially DNS security and IPAM tool security.

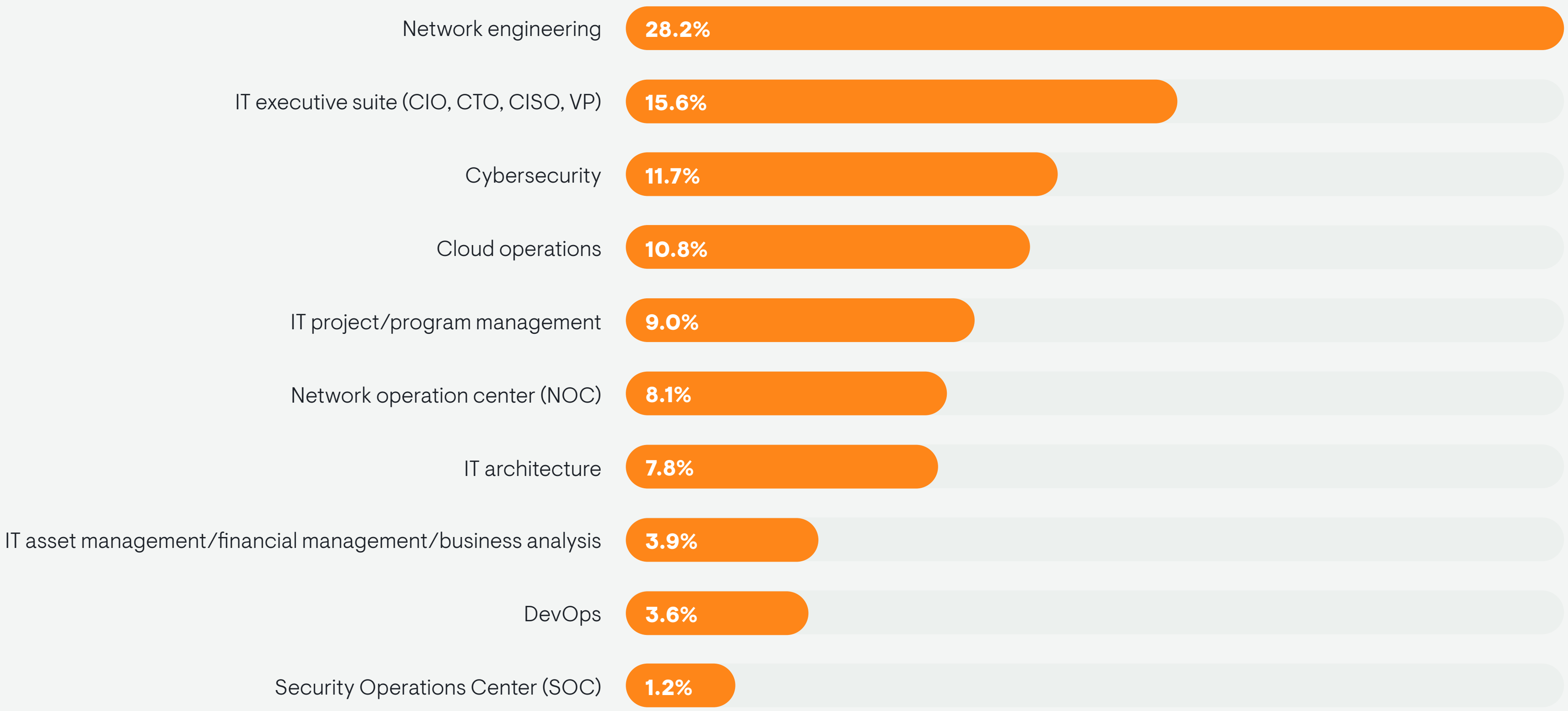
Appendix: Demographics

FIGURE 55. JOB TITLES



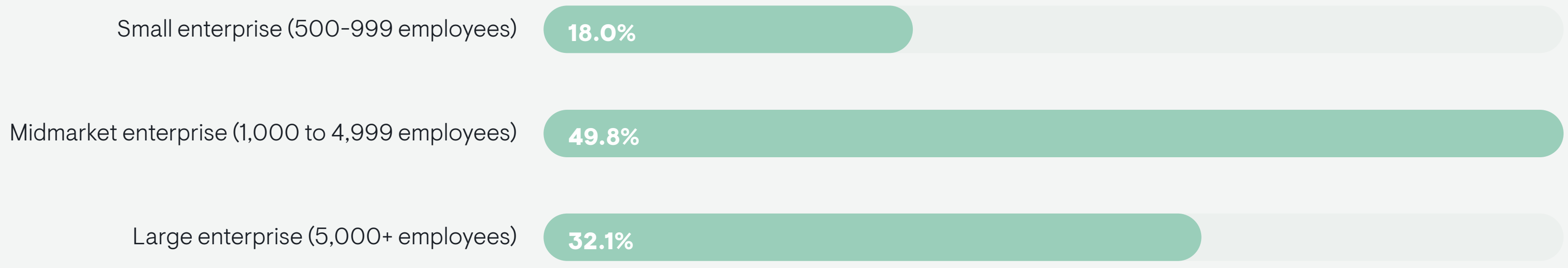
Sample Size = 333

FIGURE 56. IT GROUPS



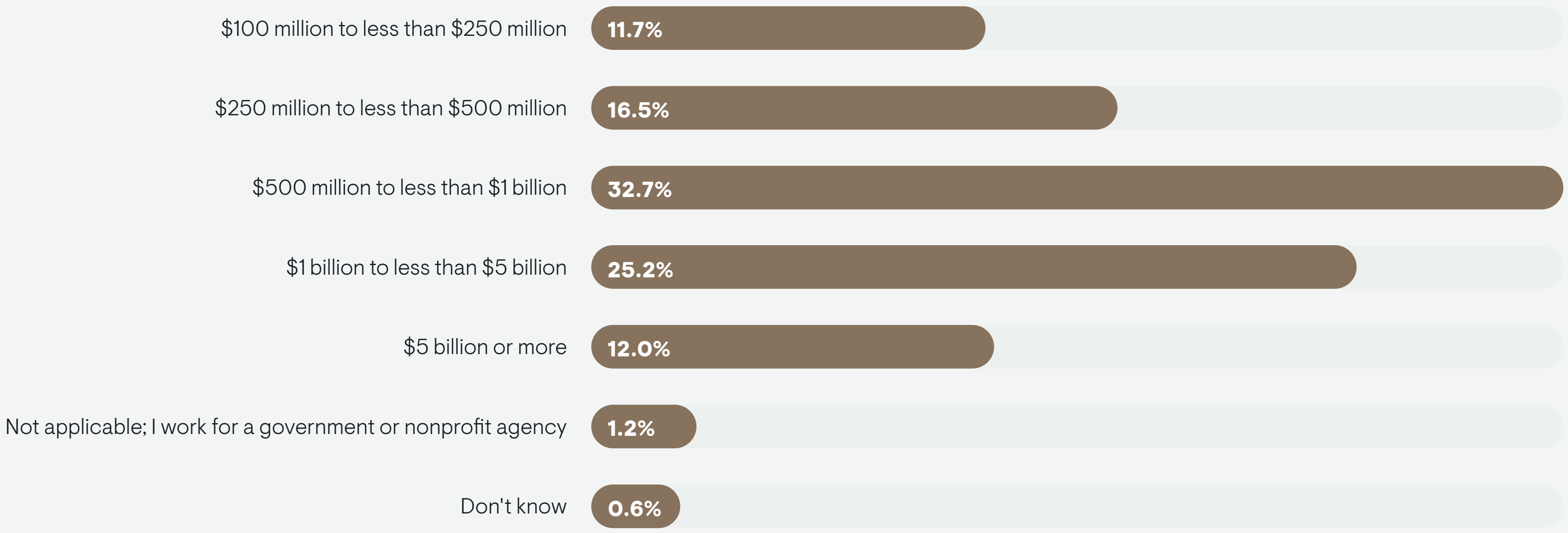
Sample Size = 333

FIGURE 57. COMPANY SIZE (EMPLOYEES)



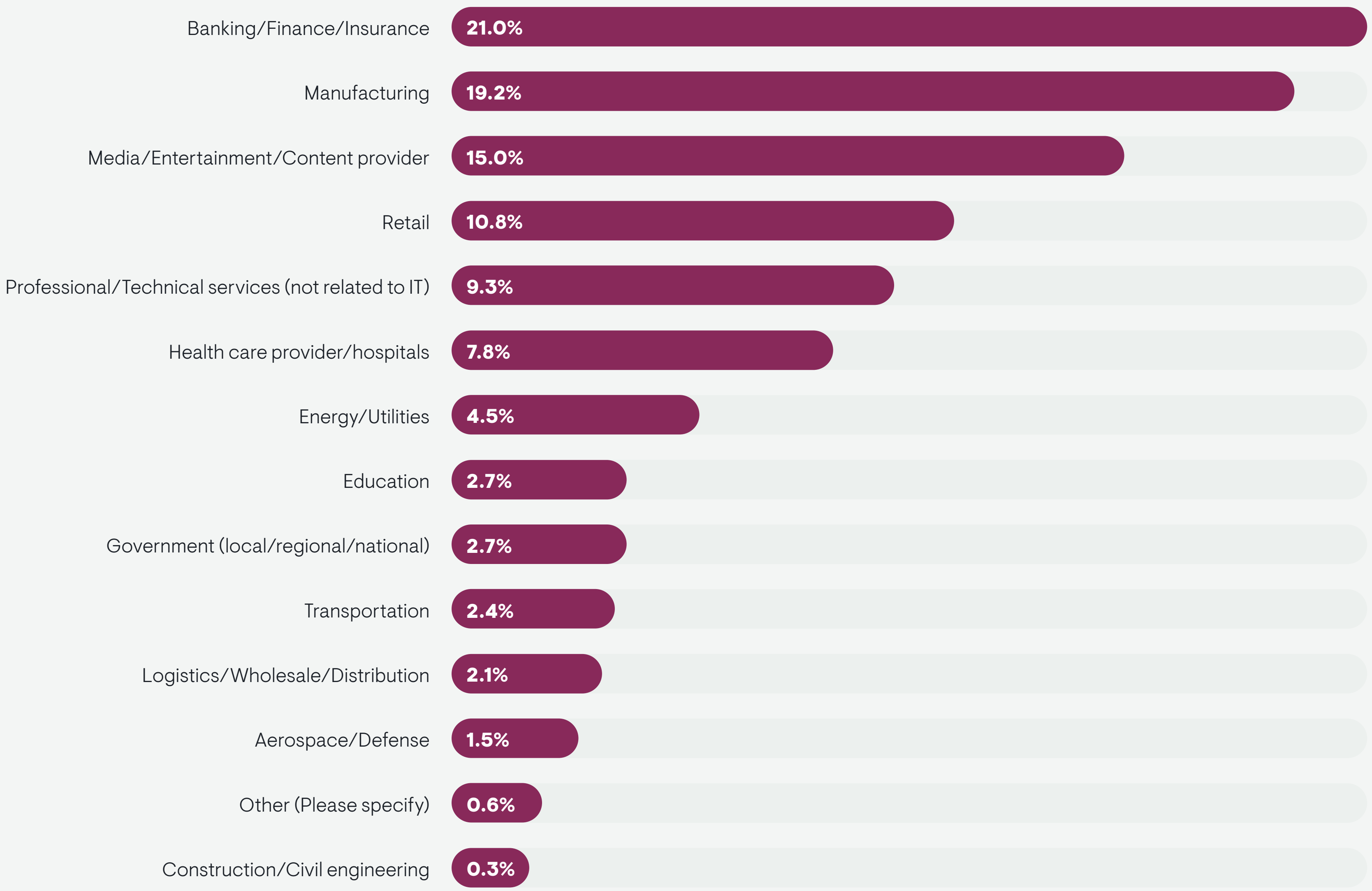
Sample Size = 333

FIGURE 58. REVENUE



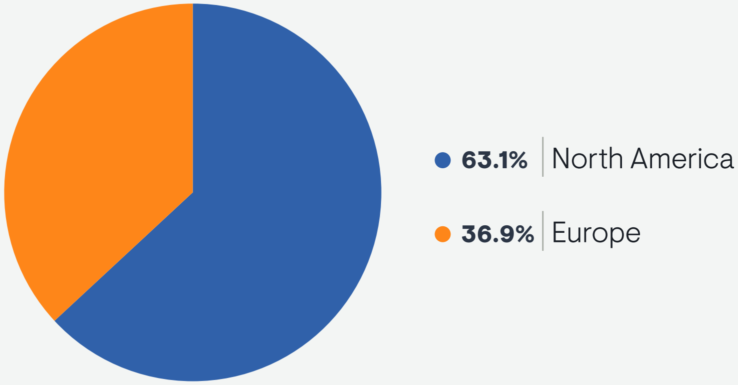
Sample Size = 333

FIGURE 59. INDUSTRIES



Sample Size = 333

FIGURE 60. REGION



Sample Size = 333

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 4341.031524