LF NETWORKING

THE LINUX FOUNDATION | Research

The 2025 Open Source Networking Study

The Role and Value of Open Source in the Networking Industry's Software Stack

April 2025

Stephen D. Hendrick, *The Linux Foundation*
Ranny Haiby, *The Linux Foundation*

Foreword by Arpit Joshipura, *The Linux Foundation*

The 2025 Open Source Networking Study

63% of respondents **use and contribute to OSS**, 35% only use, and just 2% have no OSS involvement.

92% of organizations believe that OSS projects are important to **the future of their organization.**

94% of orgs see an **open source foundation's support** of projects as important, very important, or extremely important.

83% of organizations see **the business value derived from OSS** as high or very high.

73% of organization workloads leverage **cloud native networking**, listing automation, orchestration, scalability, and resilience as top benefits.

Organizations are evenly distributed between those whose workloads are **just beginning to use cloud native** networks (41%) and those where **much or nearly all of their workload is cloud native** (41%).

The main barriers to adopting OSS in networking include the **skills gap** (38%), **security and compliance concerns** (37%), and **licensing and legal risk** (35%).

85% of respondents believe that OSS organizations should focus on **Super Blueprints**, as they provide adaptable solutions that cater to the evolving demands of modern networks.

OpenRAN functions are currently modest at single-digit deployment, but this is predicted to **double** in 2025 and **double again** in 2026 & 2027.

The top reasons for accelerating networking AI adoption are the **availability of high quality datasets** (56%) and **frameworks for AI application development** (29%).

Network automation & orchestration (57%), security & threat detection (50%), and predictive maintenance (41%) are the **leading AI applications** being evaluated or deployed.

74% of organizations prefer **open source** as the foundation for **AI network development.**

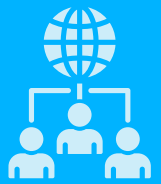


Table of Contents

Foreword

The landscape of networking technology has undergone a dramatic transformation in the past decade. The evolution has been so profound that a time traveler from the 2000s would find today's network architectures and operations virtually unrecognizable. The era of specialized hardware running proprietary software is firmly in the past. The decoupling of software from hardware, coupled with the rise of Network Function Virtualization (NFV) and its subsequent evolution to Cloud native Network Functions (CNF), paved the way for the current age of truly Software-Defined Networking (SDN). Today, network functions that enable connectivity between endpoints are essentially software applications akin to enterprise or consumer apps. Concepts such as continuous deployment are now standard practice in networking, ensuring that software is consistently up-to-date and performs optimally. Furthermore, companies can readily apply familiar IT observability and control tools to networks, enhancing their resilience and improving the end-user experience.

Several key forces have propelled this rapid network innovation. First, the industry has embraced open networking, with interfaces increasingly defined by open source projects and open standards, as the Open Radio Access Networks (OpenRANs) exemplify. Second, network functions are being fundamentally re-architected based on cloud native principles, breaking them down into smaller, independent, and portable modules capable of adapting to infrastructure changes and fluctuating capacity demands. Third, the advent of artificial intelligence (AI) presents significant opportunities to reimagine network operation, design, and maintenance. Open source software (OSS) has been instrumental in translating these trends into tangible networking advancements. Communities of experts have collaborated to drive innovation through OSS projects, which serve as the fundamental building blocks of modern networks. Time and again, these OSS initiatives have demonstrated that the most effective path to innovation lies in creating shared technologies that industry players can leverage to build competitive and groundbreaking products.

This transformation is far from complete. Creative minds within the industry, particularly those in the open source community, are continuously adapting emerging technologies to deliver functionality and performance that were unimaginable just a few years ago. The pace of innovation and creativity appears to be accelerating, with open source communities constantly exploring the next transformative technology.

Against this backdrop, it seemed opportune to engage with industry leaders to gain insights into critical questions, such as: "Where is the industry heading?", "What role should OSS play in this future?", and "Which technologies are already demonstrating their value in real-world deployments?". This research paper synthesizes the responses to these survey questions, aiming to provide guidance for those deeply involved in OSS for networking, as well as those who are still considering its potential.

Arpit Joshipura
Senior Vice President & General Manager
Linux Foundation Networking, IoT, & Edge

Executive Summary

The 2025 LF Networking Report offers critical insights into the evolving role of open source software (OSS) in the networking industry, highlighting a widespread shift toward open, scalable, and cloud native infrastructure. Based on a global survey of experienced IT and networking professionals, the findings reveal how organizations adopt these technologies and the opportunities and challenges that accompany transformation.

Open Source: A Strategic Imperative

The report clearly establishes open source as a foundational component of modern networking. An overwhelming 92% of respondents consider open source projects important to their organization's future, with 94% emphasizing the value of open source foundations for governance and long-term support. These findings point to OSS as more than just a cost-saving mechanism—it is now a strategic enabler of agility, innovation, and vendor independence.

Organizations are also realizing substantial business value from OSS: 84% report high or very high returns, particularly in terms of faster development, reduced time-to-market, and lower infrastructure costs. The deep level of OSS participation in the networking community—where 63% both use and contribute—underscores a growing commitment to community-driven development.

Cloud Native Networking Gains Momentum

Cloud native networking adoption is well underway, with 90% of organizations reporting progress. Larger enterprises lead the charge: 73% have completed some or much of their development. Medium-sized organizations show steady progress, while smaller firms display a bifurcated pattern—some fully embracing cloud native tools from the outset and others still hesitant due to resource and expertise gaps.

The primary driver behind this shift is the need for scalability, automation, and agility in network management. Tools such as Kubernetes, service meshes, and container-based architectures are becoming essential as companies modernize infrastructure to meet dynamic workloads and security demands.

Collaboration and Community: The Why Behind Open Source Adoption

Organizations engage with the open source community for multiple reasons, but the top motivators are cost savings and reduced vendor lock-in, according to 61% of respondents. This pragmatic focus reflects both economic pressures and the strategic desire for flexibility.

Other benefits include accelerated innovation (46%), strong ecosystem support (44%), and improved software quality (40%). Interestingly, the reasons for OSS collaboration shift based on an organization's maturity in cloud native adoption. Newer adopters prioritize future-proofing and security transparency, while mature users focus more on innovation and roadmap influence.

Critical Capabilities and Top Challenges

The most-valued open networking capabilities are scalable and high-performance operations (73%), edge performance (49%), and multi-architecture support (47%). These reflect the need to manage distributed environments, integrate legacy and modern systems, and enable real-time services.

However, significant challenges persist. Architectural complexity (50%), legacy system integration (47%), and a persistent skills gap (44%) top the list of obstacles in adopting cloud native networking. Mid-journey adopters—those that have completed some of the implementation—face the most friction, as they must manage both modern and traditional environments while scaling internal knowledge and capabilities.

Barriers to Broader OSS Adoption

The leading barriers to wider OSS usage are skills gaps (41%), security and compliance concerns (37%), and legal/licensing risks (36%). These barriers vary depending on an organization's progress. Those just beginning cloud native networking cite cultural resistance and integration challenges, while mature cloud native networking organizations grapple with community participation and contribution complexities.

Strong Demand for Super Blueprints

A striking 86% of respondents support the development of end-to-end Super Blueprints—modular, open source-based reference architectures that streamline deployment and integration. These frameworks offer a path to reduce risk, improve interoperability, and promote vendor-neutral solutions. Respondents see them as essential to accelerating adoption and simplifying complex open networking environments.

OpenRAN: Early but Accelerating

While OpenRAN is still in the early stages of adoption, growth is likely to surge through 2027. Respondents cite standardization and interoperability (56%) as the primary drivers, followed by Kubernetes integration and innovation potential. Organizations further along in cloud native networking are significantly more likely to adopt OpenRAN, viewing it as a natural extension of their modern infrastructure strategies.

Predicted growth rates for OpenRAN network functions, including CU/DUs and RICs, average 200% in 2025 and 100% from the beginning of 2026 through 2027, indicating a transition from early adopters to the early majority within the next three years.

The Expanding Role of AI in Networking

AI is rapidly becoming integral to network operations. Top use cases in development include network automation and orchestration (57%), threat detection (50%), and predictive maintenance (43%). Organizations with advanced cloud native deployments are leading in AI application experimentation and development because of their robust infrastructure and real-time data capabilities.

A majority of organizations (75%) prefer building AI tools on open source foundations, leveraging flexibility and ecosystem benefits. The top two actions to accelerate AI development in open source networking are ensuring the availability of high-quality datasets (ranked #1 by 56% of respondents) and frameworks for AI application development (ranked #1 by 34% or respondents). These foundational elements are critical for building effective, scalable, and domain-specific AI solutions.

Introduction

Networking plays a foundational role in modern IT, enabling communication between systems, applications, and users across diverse environments—on-premises, in the cloud, and at the edge. As IT infrastructure becomes more dynamic and distributed, networking has evolved from static configurations to highly programmable, automated systems deeply integrated into the software stack. In cloud native architectures, networking is essential for service discovery, load balancing, and secure communication between microservices. Tools such as Kubernetes, service meshes, and ingress controllers now embed networking directly into application platforms, blurring the lines between infrastructure and software.

A significant force shaping the future of networking is open networking—the move toward disaggregated, software-defined solutions based on open standards and community-driven innovation. Open networking allows organizations to decouple hardware from software, reducing vendor lock-in and enabling rapid innovation. Projects such as SONiC, FRR, OpenDaylight, ONAP, and FD.io are shaping how companies are building modern networks to be open, automated, and software driven. This shift supports interoperability, agility, and transparency, making networks more adaptable to changing workloads and security requirements. As IT continues to embrace DevOps and automation, open networking aligns with the broader trend of treating infrastructure as code, where networking becomes programmable, version controlled, and integrated with CI/CD pipelines. In essence, networking is now as much about software engineering as it is about connectivity.

Linux Foundation (LF) Networking has been hugely influential in driving the open source networking movement. It is one of the key collaborative organizations shaping the future of network infrastructure, particularly around disaggregation, openness, and cloud native alignment. LF Research partnered with LF Networking to craft a survey that would explore the most significant trends in open source networking and inform decision-makers. Key topics in this survey included involvement in open source, involvement in cloud native networking, open source networking uses and challenges, OpenRAN plans, and how AI apps will influence the direction of networking. This report discusses the most important findings from this survey.

This LF Networking survey was designed, fielded, and analyzed in Q1 2025. The findings were reported and published in April 2025. Respondents were sampled from the networking community, with 83% having more than 10 years of professional experience and 61% having 20 or more years of experience.

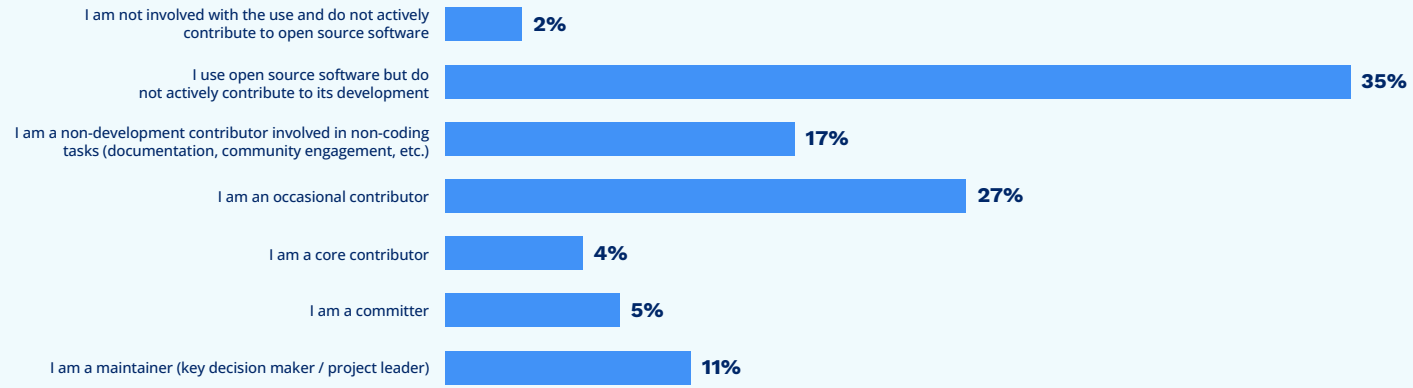
About the respondents and organizations who answered this survey

While LF Research reports generally talk about respondents in the *Methodology* section, which appears near the end of this report, the sample for this survey was a little different than what we usually encounter. An appreciation for the makeup of this sample will help with the reader's interpretation of the findings. Figure 1 shows how engaged respondents are with OSS. Perhaps the most compelling statistic is that 63% of respondents use and contribute to open source and 35% are users of open source (although not contributors). Comparing these results to an identical question we asked to a more heterogeneous collection of developers where 51% of respondents used and contributed to OSS and 47% were just users,[1] we see a significantly higher level of involvement in OSS in the networking survey. This demonstrates that the respondents in this networking survey are both highly experienced and more deeply involved in contributing to OSS. Therefore, questions in this survey on open networking progress, adoption, barriers, reasons, challenges, and benefits will reflect the perspectives of highly informed and knowledgeable sources.

FIGURE 1

INVOLVEMENT IN OSS PROJECTS

Which option best describes your level of engagement with open source software projects? (select one)



2025 LF NETWORKING SURVEY, Q6, SAMPLE SIZE = 169, "OTHER" RESPONSES EXCLUDED FROM THE ANALYSIS

1 Open Source Software Developers Report, October 2024, Stephen Hendrick & Bianca Trinkenreich OSS_Developer_Report_2024.pdf

The importance and value of open source to organizations

Figure 2 highlights the growing significance of OSS in modern organizations. The results clearly underscore the strategic importance and business value that open source initiatives provide across various sectors.

First, the data reveals that a substantial 92% of respondents consider open source projects either *important*, *very important*, or *extremely important* to their organization's future. This high percentage reflects a deep reliance on OSS for innovation, scalability, and cost efficiency. Open source projects allow companies to leverage community-driven development, accelerate deployment, and reduce vendor lock-in, offering a more agile approach to technology adoption.

Furthermore, respondents see open source foundations—which provide structure, governance, and support to these projects—as crucial. According to the survey, 94% of participants rate these foundations as *important*, *very important*, or *extremely important* in supporting the projects their organizations depend on. This indicates that they highly value the structured collaboration and long-term sustainability of open source initiatives, which help ensure the quality and continuity of mission-critical software.

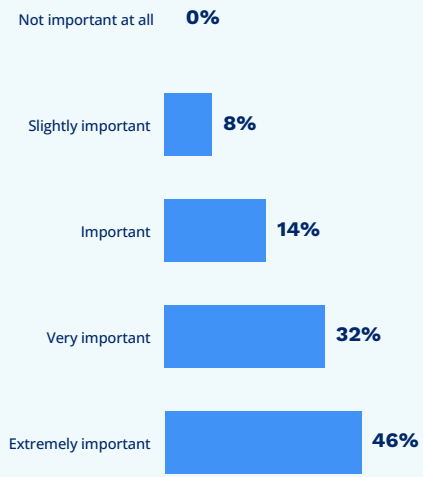
The business impact of open source is equally striking. A combined 84% of organizations report deriving either *high* or *very high* business value from open source. This suggests that OSS not only drives technical innovation but also translates directly into measurable business benefits such as reduced development costs, faster time-to-market, and improved interoperability.

Collectively, these questions clearly demonstrate that OSS is not just a technical preference—it is a strategic asset. Organizations increasingly rely on open source to drive growth, enhance collaboration, and maintain a competitive edge in a fast-evolving digital landscape.

FIGURE 2

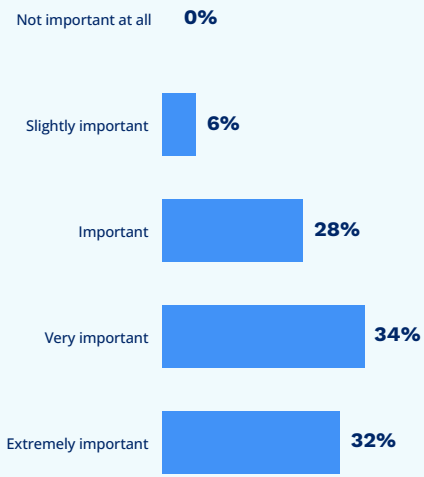
EVALUATING THE IMPORTANCE OF OSS PROJECTS AND FOUNDATIONS AND THEIR ORGANIZATIONAL VALUE

How important are open source projects to the future of your organization? (select one)



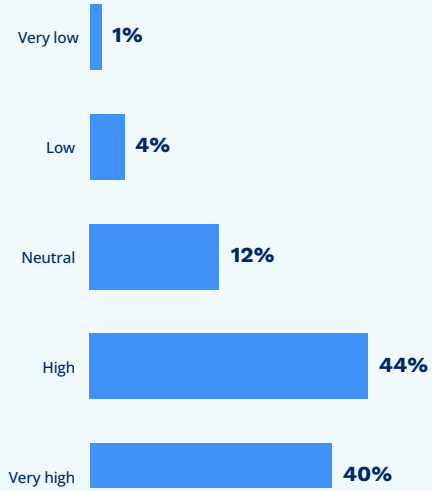
2025 LF NETWORKING SURVEY, Q11, SAMPLE SIZE = 153

How important are open source foundations in supporting the projects that your organization relies on? (select one)



2025 LF NETWORKING SURVEY, Q12, SURVEY, SAMPLE SIZE = 145, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

How much business value your organization derives from open source? (select one)



2025 LF NETWORKING SURVEY, Q13, SAMPLE SIZE = 149, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Organizational adoption of cloud native networking

Cloud native networking is essential for organizations of all sizes because it enables greater scalability, flexibility, and automation in managing modern infrastructure. By integrating networking into cloud native architectures, businesses can respond more quickly to changing demands, improve application performance, and reduce operational overhead. For large enterprises, it supports complex, distributed environments, while for smaller companies, it offers cost-effective, agile solutions that promote innovation. Cloud native networking also enhances security, observability, and resilience, making it a vital component of digital transformation. Regardless of size, organizations benefit from improved efficiency, faster deployment cycles, and the ability to stay competitive in a cloud-driven world.

Figure 3 illustrates how organizations (segmented by company size) are progressing on their journey to cloud native networking. The data provides key insights into the adoption curve and maturity levels across small, medium, and large enterprises.

Overall, most organizations have initiated cloud native networking development, with only 10% of respondents indicating no progress. Larger companies (10,000+ employees) are clearly leading the charge—38% report that some of their cloud native networking is complete, while 35% say much is complete. This suggests that larger enterprises are further along in both planning and implementation, likely due to greater resources, technical expertise, and the pressing need to modernize infrastructure at scale.

Medium-sized companies (500 to 9,999 employees) show steady progress but are more distributed across the stages. Around 31% have completed some development, 31% have completed much of it, and only 8% report that they have finished nearly all development. This indicates a healthy adoption rate, though not as accelerated as in larger firms.

The data on cloud native networking adoption among small organizations (1 to 499 employees) reveals a split landscape. While 17% have not started and 22% are just beginning, 25% have nearly completed their development. This reflects the diverse nature of small businesses, which vary widely in technical maturity, industry, and resource availability. Some small organizations, particularly tech startups and digital-native companies, are well positioned to adopt cloud native technologies early. They often build their infrastructure with scalability and automation in mind, leveraging Kubernetes, service meshes, and container networking from the outset.

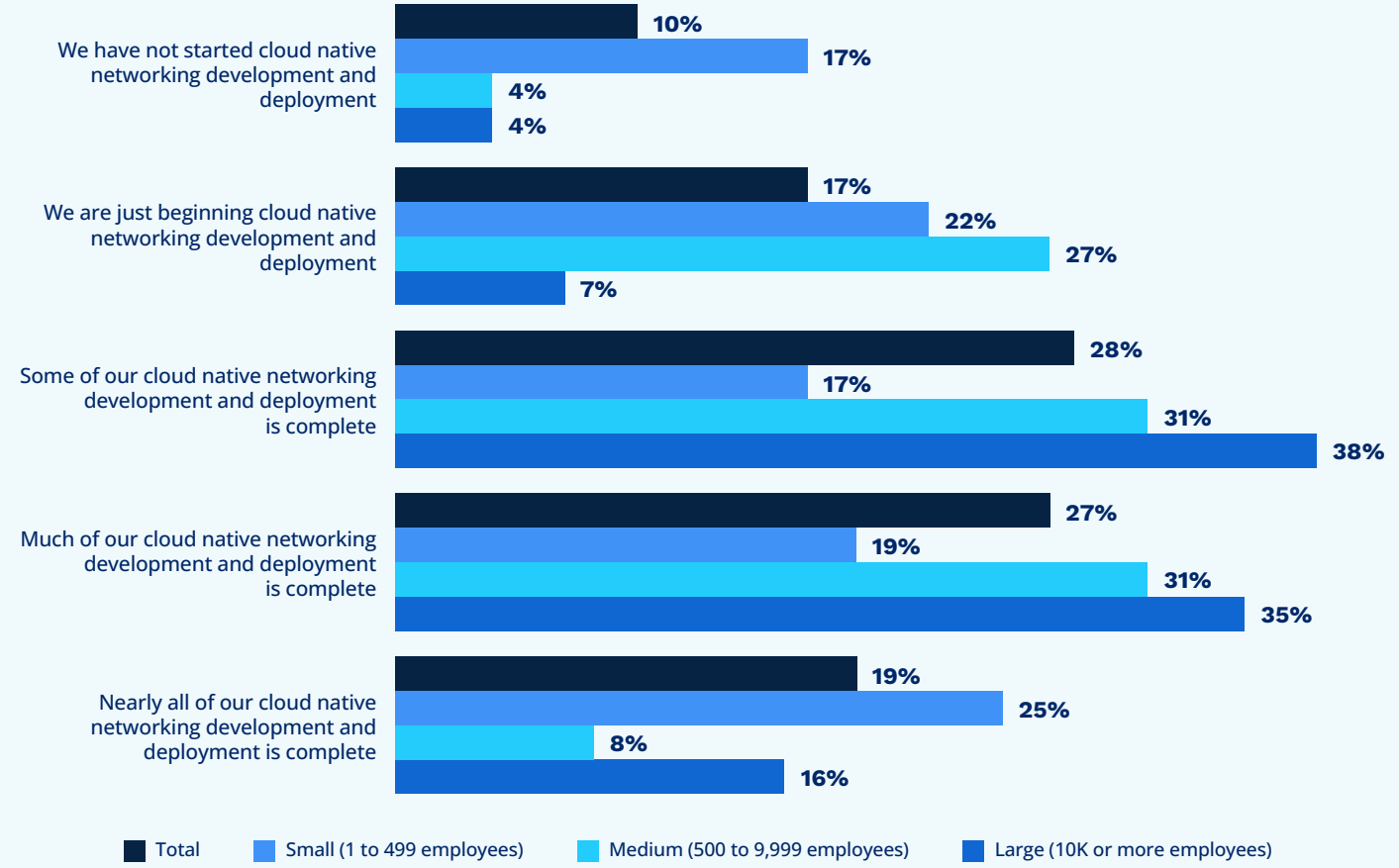
Conversely, many traditional small businesses—especially in industries such as retail, healthcare, or professional services—lack the internal expertise or urgency to adopt modern networking paradigms. These organizations may be slower to invest in cloud native solutions due to legacy systems, budget constraints, or unfamiliarity with the benefits. At the same time, the growing availability of managed platforms and simplified tools allows more agile teams to accelerate adoption without deep infrastructure investments. The result is a bimodal distribution: a significant group just beginning the journey and a similar-sized group that has already advanced far. This split underscores that company size alone does not determine progress and that strategic intent, technical capability, and industry challenges play key roles.

The data highlights a broader industry trend: cloud native networking is no longer experimental. It is becoming a foundational element of enterprise infrastructure, especially among organizations aiming for scalability, agility, and automation in their networks.

FIGURE 3

ORGANIZATIONAL ADOPTION OF CLOUD NATIVE NETWORKING

How much progress has your organization made on the journey to cloud native networking? (select one) **segmented by: company size** (employees)



2025 LF NETWORKING SURVEY, Q17 X Q7, SAMPLE SIZE = 145, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Reasons for collaborating with the open source community to achieve technology goals

Cost savings and reduced vendor lock-in stand out as the most important reasons organizations collaborate with the open source community, according to 61% of organizations (Figure 4). This dominance over other reasons reflects both economic and strategic priorities in today's technological landscape.

Financially, open source solutions significantly reduce licensing and operational costs compared to proprietary software. This is particularly critical as organizations scale their infrastructure, especially in cloud native environments, where containerization and microservices can otherwise incur high costs if organizations can only use specific vendors.

Strategically, reducing vendor lock-in enhances agility and future-proofing. Organizations gain the flexibility to switch providers, integrate best-of-breed tools, and avoid dependency on a single vendor's pricing, roadmap, or ecosystem limitations. This freedom is especially valuable for companies advancing in their cloud native journey, where rapid innovation and scalability are essential.

Unlike innovation or ecosystem support—which offer long-term advantages—cost and independence deliver immediate, measurable business value. For many decision-makers, especially in tight economic climates or high-growth scenarios, this makes cost savings and vendor independence not just preferable but essential. They are foundational benefits that enable and support all the others, making them the top motivators across all stages of cloud native maturity.

As Figure 4 shows, other reasons why organizations collaborate with the open source community include:

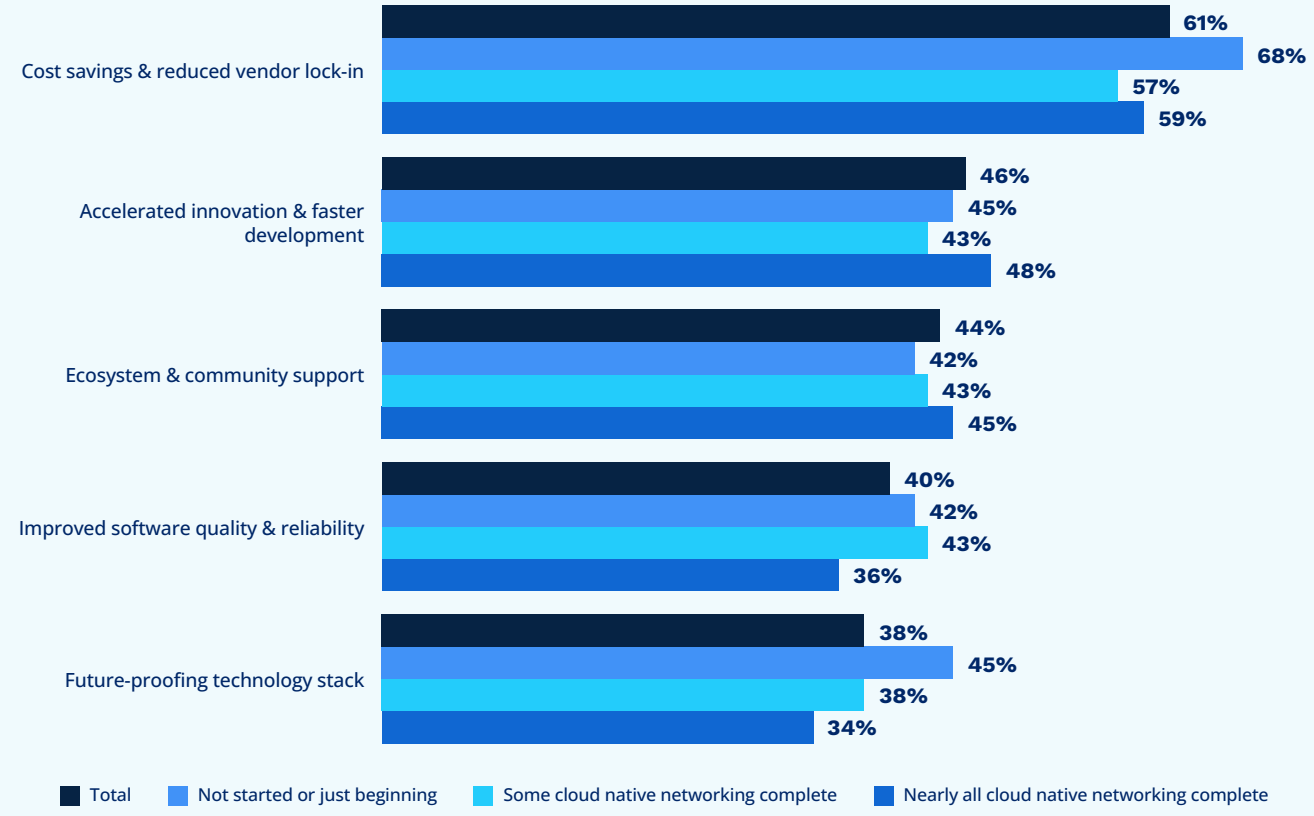
- Accelerated innovation and faster development (46%). This reflects how open source fosters faster iteration cycles and allows organizations to stay ahead in rapidly evolving tech landscapes.
- Ecosystem and community support (44%). This factor indicates that, regardless of cloud native maturity, organizations value community collaboration and the shared knowledge it brings.
- Improved software quality and reliability (40%). Commonly used OSS software components benefit from undergoing community vetting, which improves software quality and reliability. Interestingly, only 36% of organizations close to completing their cloud native networking journey cite this, suggesting that organizations might place relatively less emphasis on these benefits once other benefits, such as security or innovation, become more apparent in later adoption stages.
- Future-proofing the technology stack (38%). This reason for collaborating with the open source community jumps to 45% among those who have not started or are just beginning their cloud native networking implementation. This reinforces the notion that open source collaboration helps ensure long-term adaptability and relevance in fast-changing technology environments.

Segmentation by cloud native networking adoption is especially relevant in areas such as enhanced security and code transparency, compliance and industry collaboration, and strategic influence over open source roadmaps. These reasons also show that once organizations have established themselves on their journey to cloud native networking, these factors become significantly more important.

FIGURE 4

REASONS FOR COLLABORATING WITH THE OPEN SOURCE COMMUNITY TO ACHIEVE TECHNOLOGY GOALS

What are your reasons for collaborating with the open source community to achieve your organization's technology goals? segmented by: cloud native networking progress



2025 LF NETWORKING SURVEY, Q22 X Q17, SAMPLE SIZE = 139, VALID CASES = 139, TOTAL MENTIONS = 517, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

The top three open networking capabilities

The survey asked participants to select their top three networking capabilities from a list of 10 areas, and Figure 5 shows that the leading choice was clear and that the two follow-up choices were competitive across the sample.

For large enterprises, scalable and high-performing network operations are fundamental, as 73% of organizations indicated. These organizations manage extensive infrastructure spread across multiple locations, regions, and time zones. Scalability ensures the network can grow in step with business needs, user bases, and data volumes. Performance is equally critical to maintaining efficiency, minimizing latency, and delivering seamless user experiences across applications and services. Without these capabilities, large organizations risk bottlenecks and operational inefficiencies, leading to potential revenue loss and degraded customer trust.

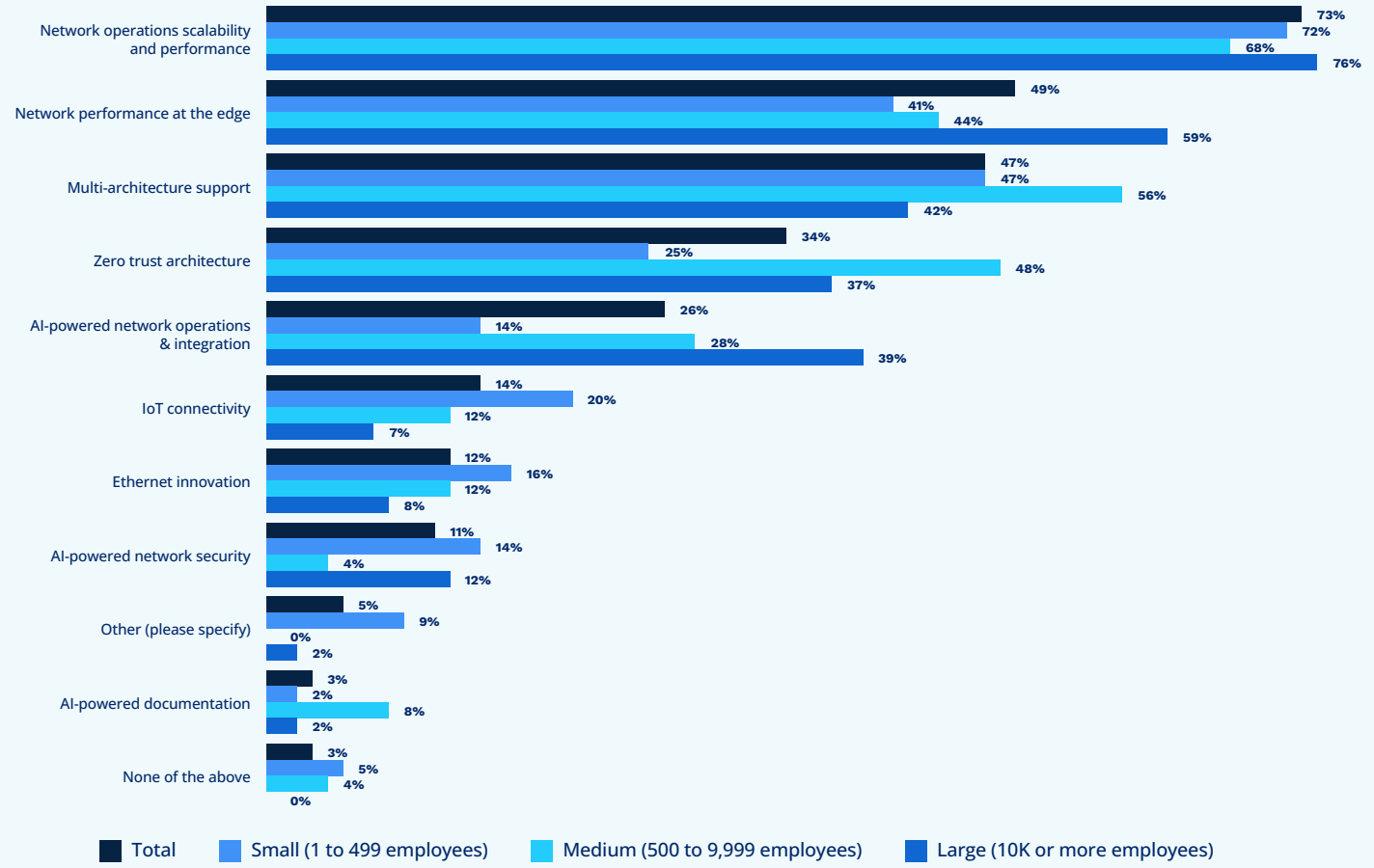
Network performance at the edge (49% overall) and multi-architecture support (47% overall) are effectively tied for the second and third top capabilities, but the ranking can vary considerably based on the size of the organization. Large enterprises typically operate at a global scale, with offices, data centers, and users spread across multiple geographic locations. To meet the demands of distributed operations and support low-latency, real-time services, these organizations increasingly rely on edge computing. High network performance at the edge enables them to process data locally, reducing reliance on centralized infrastructure, improving responsiveness, and ensuring business continuity. This is especially important for use cases such as smart manufacturing, remote diagnostics, or content delivery networks—common in large, complex enterprises. On the other hand, medium-sized organizations often operate in a hybrid environment as they scale up and modernize their IT infrastructure. They need the flexibility to run workloads across different platforms, such as the cloud, on-premises, and the edge. Multi-architecture support allows them to adopt the best tools and technologies for their specific needs without restricting themselves to a single vendor or platform. It is also a way to optimize costs, extend the life of existing investments, and prepare for future growth.

Zero-trust architecture and AI-powered network operations and integration are both critical innovations in networking, but they do not appear among the top three capabilities in Figure 5 because organizations may still view them as emerging or enabling technologies rather than immediate operational priorities. Zero-trust architecture, while gaining momentum due to rising cybersecurity threats, often requires complex redesigns, policy shifts, and cross-functional collaboration to implement. Many organizations are still in the planning or early adoption phases, which may explain their lower prioritization of zero-trust architecture. AI-powered networking and integration promises long-term value through automation and intelligent decision-making, but its perceived complexity, cost, and lack of mature solutions may lead some organizations to see it as a next-phase investment rather than a top priority today.

FIGURE 5

THE TOP THREE NETWORKING CAPABILITIES SEGMENTED BY COMPANY SIZE

Please select the top three capabilities that are most important to your organization. (select up to three responses)
segmented by: company size (employees)



2025 LF NETWORKING SURVEY, Q15 X Q7, SAMPLE SIZE = 148, VALID CASES = 148, TOTAL MENTIONS = 408, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Organizations' challenges in adopting cloud native networking

The leading challenges that organizations have in adopting cloud native computing include architectural complexity (50%), integration with legacy systems (47%), the skills gap and organizational readiness (44%), and tool fragmentation and vendor lock-in (42%). Figure 6 lists these challenges (and more) in descending order of importance and segments this data by level of cloud native networking maturity.

Architectural complexity represents the most significant barrier to cloud native networking. Cloud native networking often requires a deep re-architecture of systems to embrace microservices, containers, and dynamic workloads. This complexity makes it difficult for teams to design and implement scalable, secure, and resilient networking models, especially in large or heavily regulated environments.

Integration with legacy systems follows closely. Many organizations operate on hybrid infrastructures, where cloud native applications must interact with traditional systems. Bridging the gap between old and new technologies without compromising performance, security, or data consistency is a non-trivial challenge that demands considerable time, expertise, and customization.

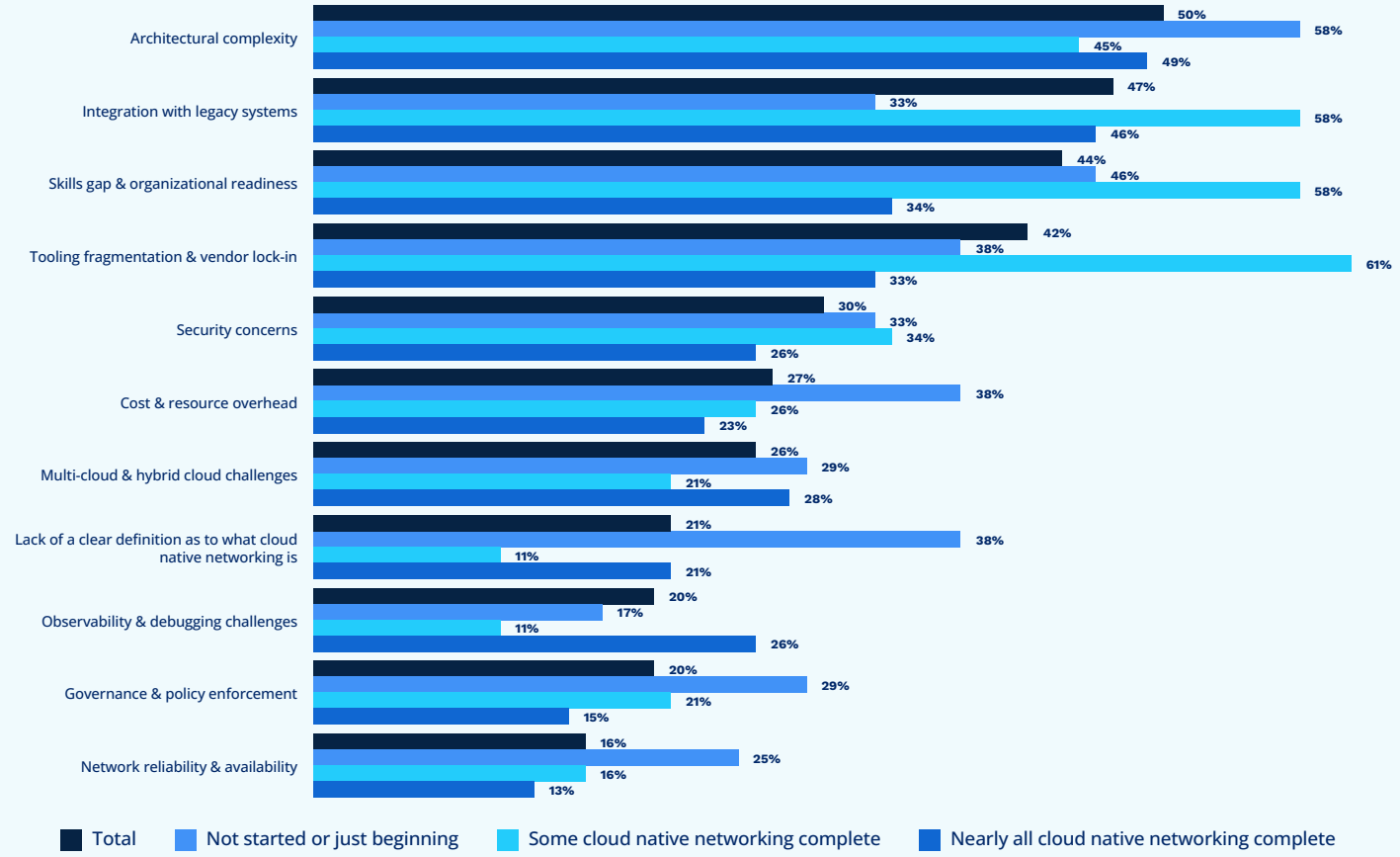
Skills gap and organizational readiness is the third-highest concern. Cloud native networking involves new paradigms, such as service meshes, container orchestration, and CI/CD pipelines. A lack of skilled personnel or sufficient training hampers the ability to adopt and operate these tools effectively, slowing down the overall transformation process.

Finally, tooling fragmentation and vendor lock-in is a key obstacle. The cloud native ecosystem offers a wide array of tools, many of which are not interoperable. Organizations often struggle with choosing and integrating tools that suit their needs while avoiding dependency on specific vendors, which can limit flexibility and increase long-term costs.

FIGURE 6

ORGANIZATIONAL CHALLENGES IN ADOPTING CLOUD NATIVE NETWORKING

What are your organization's biggest challenges in adopting cloud native networking? (select all that apply)
segmented by: cloud native networking progress



2025 LF NETWORKING SURVEY, Q19 X Q17, SAMPLE SIZE = 123, VALID CASES = 123, TOTAL MENTIONS = 421, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Organizations with some cloud native networking complete report significantly greater concern over integration with legacy systems (58%), skills gap and organizational readiness (58%), and tooling fragmentation and vendor lock-in (61%) compared to their peers further behind or ahead in adoption. This stage often represents a critical transitional phase where organizations are shifting from experimentation to broader deployment but have not yet reached full maturity.

At this point, teams face real-world friction integrating modern cloud native architectures with existing legacy systems, which are often deeply embedded in business operations. Unlike those just beginning (who may not yet feel the impact) or those fully migrated (who may have phased out older systems), these mid-stage adopters must bridge both worlds simultaneously.

Similarly, the skills gap becomes painfully apparent at this stage. While early champions or consultants might have driven initial progress, scaling efforts highlight broader internal knowledge and readiness deficiencies.

Tooling fragmentation and vendor lock-in become more visible, too. As teams incorporate more cloud native tools, they often realize the challenges of integrating disparate solutions and the risks of relying too much on a single vendor. These organizations are actively confronting the complexities of operationalizing cloud native networking—not just planning or optimizing—which is why these challenges rank so high.

Barriers to adopting more OSS

Barriers to adopting more OSS are extremely dependent upon the progress that an organization has made toward cloud native networking. Figure 7 shows these barriers in overall descending order and segments them by cloud native networking progress. Skills gap and knowledge requirements (41%), security and compliance concerns (37%), and licensing and legal risk (36%) are the leading barriers across all organizations.

The prominence of the skills gap highlights that many organizations lack personnel with the necessary expertise to deploy, manage, and contribute to open source projects effectively. This shortage can slow adoption, increase operational risk, and raise costs due to additional training or reliance on external consultants.

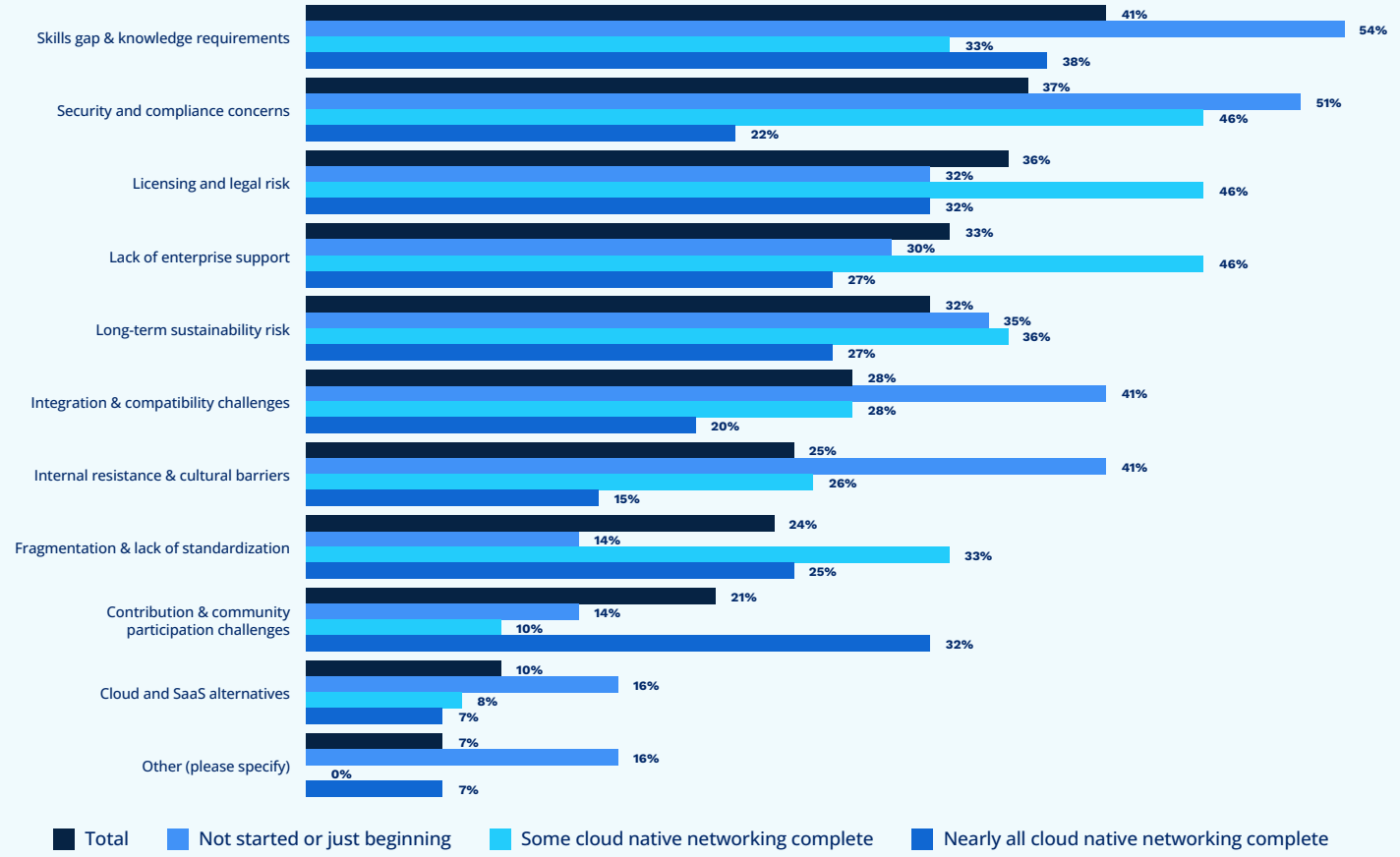
Security and compliance concerns come next, reflecting the complexities of validating the integrity of open source code and ensuring it meets internal or regulatory compliance standards. Without clear ownership or standard security practices, organizations may struggle with vulnerability management, patching, and audit readiness.

Licensing and legal risks are also significant because of the diverse and often ambiguous nature of open source licenses. Misunderstanding licensing obligations—such as copyleft provisions—can inadvertently expose companies to legal liabilities or force unwanted disclosure of proprietary code. In combination, these barriers reflect the growing need for organizations to balance the agility and innovation of open source adoption with structured governance, legal due diligence, and workforce development to mitigate risks and unlock its full potential.

FIGURE 7

BARRIERS TO ADOPTING MORE OSS

What are the barriers, if any, in adopting more open source software across your stack? (select all that apply) **segmented by: cloud native networking progress**



2025 LF NETWORKING SURVEY, Q20 X Q17, SAMPLE SIZE = 136, VALID CASES = 136, TOTAL MENTIONS = 399, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Barriers to organizations that have not started or are just beginning cloud native networking

For organizations that have not started or are just beginning their cloud native networking journey, barriers such as skills gap and knowledge requirements (54%), security and compliance concerns (51%), integration and compatibility challenges (41%), and internal resistance and cultural barriers (41%) are particularly high due to a lack of foundational readiness.

The most significant hurdle is the skills gap, as these organizations often lack the in-house expertise to manage and operate open source, cloud native technologies. This makes adoption risky and resource-intensive, deterring initial investments. Without experienced personnel, even basic implementation tasks can become overwhelming.

Security and compliance concerns increase at this early stage because newer adopters typically do not have established frameworks for evaluating and managing the risks inherent in open source components. The lack of mature policies and automation makes them more vulnerable to misconfigurations, vulnerabilities, and compliance failures.

Integration and compatibility challenges arise from trying to mesh open source tools with existing legacy systems. Organizations just starting out may not yet have modular, flexible infrastructures, making it harder to implement open source solutions without significant rework.

Finally, internal resistance and cultural barriers play a major role. Teams used to proprietary software or traditional methods may resist change, especially when they do not yet understand or see the benefits of open source adoption.

Barriers to organizations where some cloud native networking is complete

For organizations with some cloud native networking development complete, key barriers such as security and compliance concerns (46%), licensing and legal risk (46%), lack of enterprise support (46%), and fragmentation and lack of standardization (33%) reflect the growing complexity and scale they encounter mid-journey.

At this stage, these organizations have likely moved beyond experimentation and are deploying open source technologies into production or hybrid environments. As a result, security and compliance become more pressing due to the need to manage vulnerabilities across more extensive deployments, meet regulatory requirements, and ensure consistent policy enforcement across platforms. These concerns are no longer theoretical—they are operational realities.

Similarly, licensing and legal risk rise in importance as usage expands. The more open source components that organizations integrate into a production stack, the greater the chance of encountering diverse, sometimes incompatible licenses. Mismanagement can lead to IP exposure, compliance issues, or even legal consequences, especially if teams lack a centralized governance model.

Lack of enterprise support is another key barrier. As adoption scales, organizations increasingly require professional-grade support, training, and documentation—areas where some open source projects may fall short. Without this support, troubleshooting and ongoing maintenance become time-consuming and risky.

Lastly, fragmentation and lack of standardization pose integration and operational challenges. Organizations often struggle to align tools, APIs, and configurations across different environments, leading to inefficiencies and increased overhead.

These barriers illustrate the challenges of moving from partial to full maturity in a cloud native strategy while maintaining control, compliance, and consistency.

Barriers to organizations where nearly all cloud native networking is complete

For organizations that have nearly completed all of their cloud native networking development, skills gap and knowledge requirements (38%) and contribution and community participation challenges (38%) emerge as the top barriers to further OSS adoption. At this advanced stage, the focus often shifts from basic implementation to optimization, customization, and long-term sustainability—areas that demand highly specialized expertise.

Even though these organizations have matured in their cloud native journey, the skills gap persists because deeper engagement with open source projects requires knowledge beyond deployment—such as contributing code, understanding complex project roadmaps, and integrating bleeding-edge tools. Maintaining and evolving open source-based systems often depends on niche expertise that is not widely available.

Contribution and community participation challenges become prominent because mature adopters increasingly need to influence the direction of the projects they rely on. However, contributing effectively requires time, resources, and alignment with internal priorities—something many organizations struggle to balance. Navigating community dynamics, governance structures, and open development processes can also be difficult for teams used to vendor-led support models.

Ultimately, these barriers highlight that, at the high end of the adoption curve, technical depth and active engagement with the open source ecosystem are critical—but not always easy to achieve or sustain within enterprise environments.

Should open source organizations focus on end-to-end Super Blueprints?

An end-to-end Super Blueprint in open networking is a comprehensive, modular framework that provides detailed guidance for designing, deploying, and managing open, disaggregated network architectures. It encompasses hardware, software, and operational best practices across all layers of the network stack—from physical infrastructure to orchestration and automation. Industry groups including the Linux Foundation and Open Compute Project collaborated to develop these blueprints, which support interoperability by integrating open source and vendor-neutral components. They aim to simplify complex network deployments, improve scalability, and reduce vendor lock-in. A Super Blueprint typically includes reference designs, validated configurations, and implementation guides for use cases such as data centers, edge computing, and telco networks. By covering the full lifecycle of network operations—planning, implementation, and optimization—it enables operators to build flexible, cost-effective, and future-ready networks. Ultimately, an end-to-end Super Blueprint serves as a roadmap for accelerating innovation and adoption of open networking at scale.

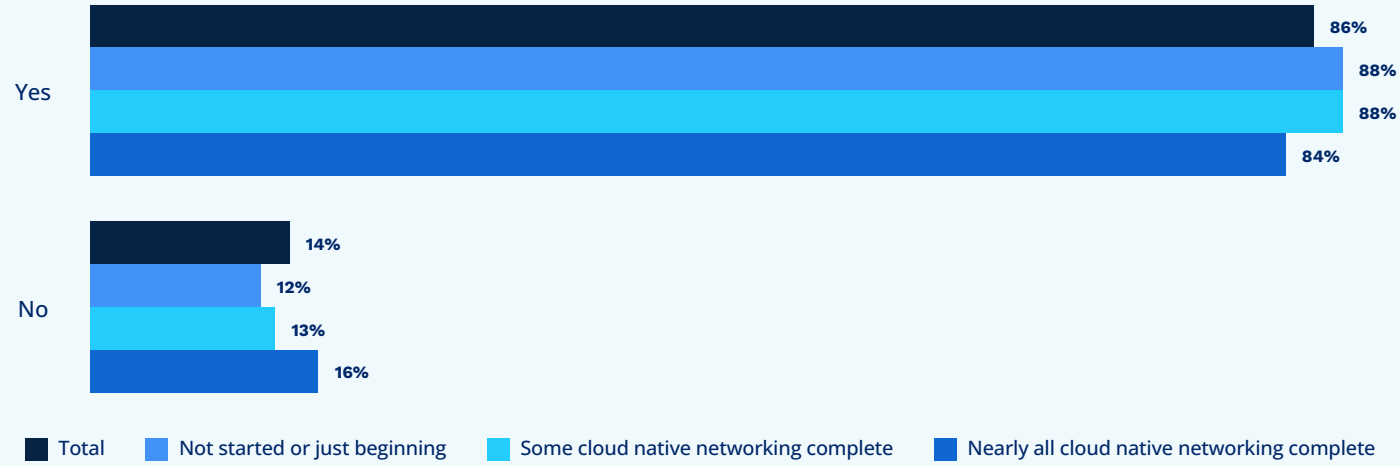
When the survey asked respondents if open source organizations should focus on the development of end-to-end Super Blueprints and solutions across multiple software projects and technologies, the result, as Figure 8 shows, was a resounding yes. The figure shows that 86% of networking professionals support the development of end-to-end Super Blueprints across multiple open source projects because they see them as essential for simplifying complex network deployments. In an environment where networks span diverse technologies—such as cloud, edge, and telco infrastructure—professionals value clear, unified guidance that connects disaggregated components into cohesive solutions. Super Blueprints reduce the time and risk associated with integrating multiple software stacks by providing validated, interoperable designs. They also encourage best practices, enable scalability, and support vendor neutrality—key drivers in modern, open networking. Professionals recognize that without such blueprints, organizations often face integration challenges and duplicated efforts.

By aligning efforts across different projects, Super Blueprints promote collaboration, accelerate innovation, and improve confidence in deploying open solutions. Ultimately, they help organizations deliver reliable, production-ready networks faster and with lower costs, making them a strategic focus for the open source community.

FIGURE 8

FEEDBACK ON WHETHER OPEN SOURCE ORGANIZATIONS SHOULD DEVELOP SUPER BLUEPRINTS

Should open source organizations also focus on end-to-end Super Blueprints and solutions across multiple software projects and technologies? (select one) **segmented by: cloud native networking progress**



2025 LF NETWORKING SURVEY, Q27 X Q17, SAMPLE SIZE = 99, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

The importance of open source in OpenRAN integration

When we asked networking professionals about the importance of OSS in OpenRAN integration, 34% gave a *don't know or not sur*e (DKNS) response. This uncertainty likely reflects the indecisiveness of many organizations toward this technology and the desire to wait for the technology to mature more before determining how it would evolve and how the role of OSS would unfold. Additionally, the technical complexity of integrating multiple components—often from different vendors—can make it difficult to clearly understand where open source fits into the equation. In some cases, professionals may associate open source with general IT infrastructure, not realizing its increasing relevance in telecom networks. This points to a broader need for education and clearer communication around how open source contributes to OpenRAN's success, especially as this technology gains momentum globally.

Figure 9, which excludes DKNS responses from the analysis, provides key insights into industry views on the role of OSS in OpenRAN integration and segments the insights by the progress organizations have made in adopting cloud native networking.

Figure 9 shows that the majority of respondents—across all levels of cloud native maturity—view open source in OpenRAN integration as *important, very important, or extremely important*. This widespread recognition likely stems from open source's central role in enabling interoperability, vendor flexibility, and innovation in OpenRAN ecosystems. As OpenRAN seeks to disaggregate traditional network architectures, open source offers a foundation for shared development, faster standardization, and cost reduction—benefits that appeal to both emerging and established network operators.

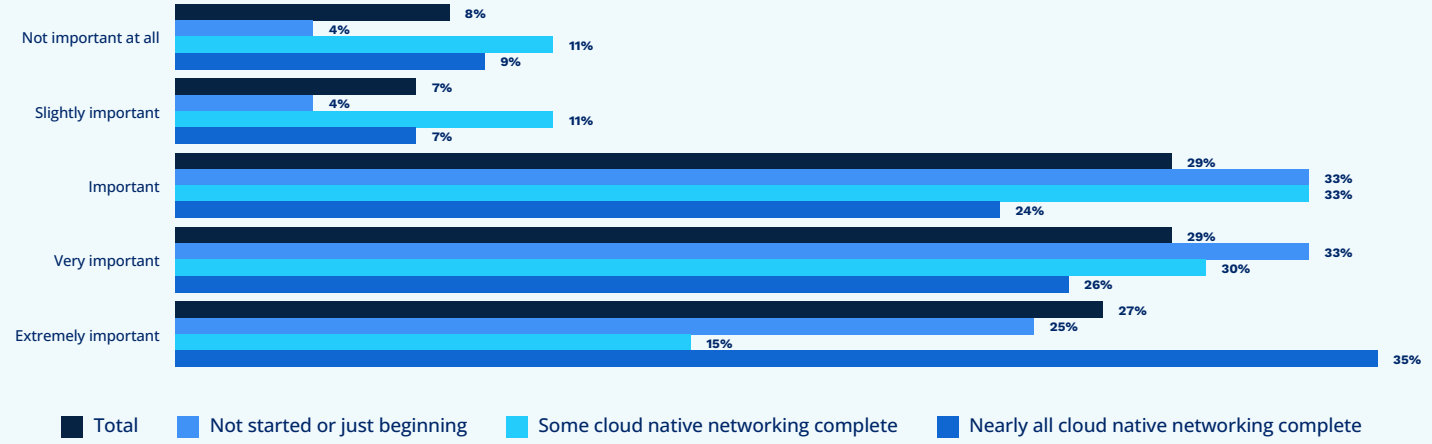
Interestingly, both ends of the spectrum—those just beginning and those nearly done with cloud native transitions—rate open source as highly important. For the former, open source may represent a cost-effective, lower-barrier entry point into OpenRAN. These organizations may rely on open communities and tools to accelerate early development. On the other hand, highly mature organizations are more likely to be strategically invested in open ecosystems. They have likely experienced firsthand the benefits of open source—such as automation, agility, and reduced vendor lock-in—and see it as essential to successful integration at scale.

Organizations that report having some cloud native networking complete are notably less likely to view open source as critical. This may reflect a transitional phase where open source has not yet demonstrated its full value or where integration challenges have overshadowed its benefits. These organizations might still be dealing with hybrid environments and struggling with the complexity of aligning proprietary and open solutions, leading to uncertainty or underestimation of open source's role.

FIGURE 9

THE IMPORTANCE OF OPEN SOURCE IN OPENRAN INTEGRATION

How important is the role of open source software in OpenRAN integration? (select one)
segmented by: cloud native networking progress



2025 LF NETWORKING SURVEY, Q28 X Q17, SAMPLE SIZE = 97, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Primary reasons for adopting OpenRAN technologies

OpenRAN is a transformative telecommunications technology that aims to open up and standardize the hardware and software in mobile networks. Traditionally, a single vendor with proprietary equipment builds radio access network (RAN) systems, limiting flexibility and innovation. OpenRAN changes this by promoting interoperability among components from different vendors through standardized interfaces. This approach enables network operators to mix and match hardware and software from multiple suppliers, reducing costs, fostering innovation, and avoiding vendor lock-in. OpenRAN leverages cloud computing, virtualization, and AI to make network management more agile and efficient. It is particularly important for the deployment of 5G networks, where flexibility and scalability are critical. OpenRAN is reshaping how companies are designing and deploying mobile networks, especially in developing markets and rural areas where cost-effective solutions are essential for expanding connectivity.

Figure 10 shows organizational reasons for adopting OpenRAN technologies. However, it is important to recognize that OpenRAN is in its infancy. Only 85% of our sample answered the question from Figure 10, and of those that answered the questions, 52% responded by selecting DKNS. Therefore, Figure 10 reflects the views of the sample (40%) that selected one or more responses.

The one reason for adopting OpenRAN technologies that resonated strongly across organizations, regardless of their progress on cloud native networking, was standardization and interoperability (56% overall). Standardization and interoperability are key drivers behind the adoption of OpenRAN technologies. By enabling components from different vendors to work together seamlessly, OpenRAN breaks the traditional reliance on single-vendor solutions. This flexibility allows operators to reduce costs, accelerate innovation, and tailor network solutions to specific needs. Standardized interfaces foster a more competitive ecosystem, encouraging collaboration and rapid technological advancement. Interoperability also simplifies network upgrades and maintenance, making it easier to deploy scalable and future-ready networks such as 5G. Ultimately, this open approach empowers operators with greater control, adaptability, and efficiency in building and managing modern telecom infrastructure.

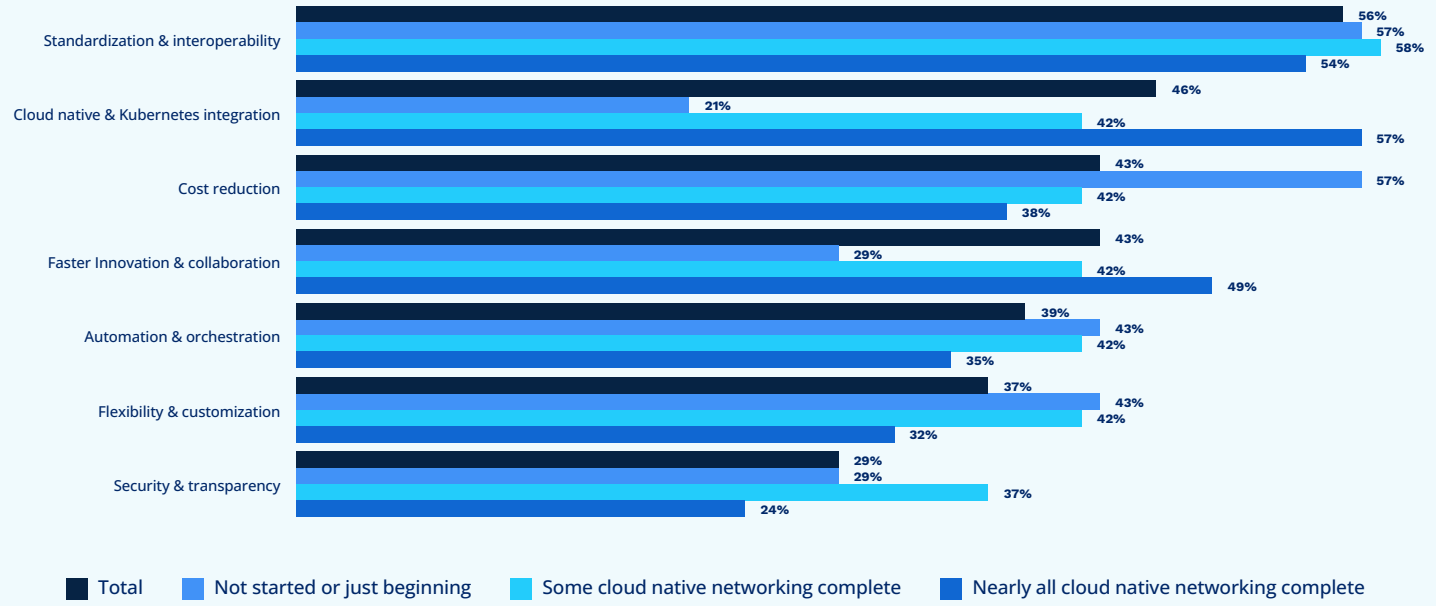
The strong correlation between cloud native networking progress and the adoption of OpenRAN for cloud native and Kubernetes integration and faster innovation and collaboration reflects how organizations with mature cloud strategies are leveraging OpenRAN to unlock its full potential. As Figure 10 shows, 57% of organizations that have nearly completed cloud native networking cite Kubernetes integration as a primary reason for adopting OpenRAN—far above the 21% for those just beginning. These organizations are already invested in containerization, microservices, and orchestration, so aligning OpenRAN with Kubernetes offers seamless integration, scalability, and automation.

Similarly, 49% of cloud native leaders prioritize faster innovation and collaboration, while only 29% of those starting out prioritize them. This reflects how cloud native maturity enables more agile development cycles, cross-vendor collaboration, and rapid deployment of new network functions—all of which OpenRAN supports through open interfaces and modular design. Ultimately, cloud native organizations view OpenRAN not just as an upgrade but as an enabler of modern network transformation.

FIGURE 10

PRIMARY REASONS FOR ADOPTING OPENRAN TECHNOLOGIES

What are your organization's primary reasons for adopting OpenRAN technologies? (select all that apply)
segmented by: cloud native networking progress



2025 LF NETWORKING SURVEY, Q29 X Q17, SAMPLE SIZE = 70, VALID CASES = 70, TOTAL MENTIONS = 204, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Organizations' plans for deploying OpenRAN show strong growth through 2027

Response rates regarding OpenRAN plans shared a pattern of limited visibility, as Figures 9 and 10 show. Figure 11 reflects responses from 91% of our sample. Of the 91%, approximately 52% answered with a DKNS response when asked what their organization's plans were for deploying OpenRAN network functions. Therefore, Figure 11 reflects the perspectives of 43% of the sample who were able to share organizational information about OpenRAN implementation plans. However, when respondents say DKNS, that does not mean that the organization they work for is not involved with OpenRAN or planning to implement OpenRAN soon. It just means that they are not able to answer the question. Therefore, OpenRAN penetration and growth rates are likely somewhat higher than Figure 11 shows.

In Figure 11, the definitions of the acronyms representing the responses are as follows:

- **RICs (nRT and nonRT) – SMO.** RICs (RAN intelligent controllers) are platforms for hosting intelligent applications (xApps and rApps) that manage and optimize RAN behavior. There are near-real-time (nRT, <1 second latency) and non-real-time (NonRT, >1 second latency) RICs. SMO (Service management and orchestration) is a component that oversees the lifecycle management of RAN functions.
- **CU/DU.** These are parts of the base station that OpenRAN splits up for flexibility and efficiency. The DU (distributed unit) is closer to the radio unit and handles real-time processing such as MAC and RLC. The CU (central unit) manages higher-layer protocols such as PDCP and RRC.
- **RU.** The RU (radio unit) is the physical unit that transmits and receives RF signals to/from the user equipment.
- **O-cloud.** O-Cloud (open cloud infrastructure) is a cloud computing platform that hosts OpenRAN, functions, and apps and provides the compute, storage, and networking resources necessary to run RICs, CU/DU functions, SMOs, and other virtual network functions.

Figure 11 shows a low *already deployed* penetration rate (6.3% on average) for OpenRAN network functions, reflecting its early stage of industry adoption. Challenges such as integration complexity with legacy systems, limited ecosystem maturity, and lack of standardized interoperability hinder rapid deployment. Additionally, operators are cautious due to concerns over performance, security, and return on investment. The dominance of established vendors and internal resistance to change further slows adoption. Many organizations are still evaluating OpenRAN's long-term viability, resulting in a high percentage of delayed or uncertain deployment plans. However, this is all going to change rapidly over the next several years.

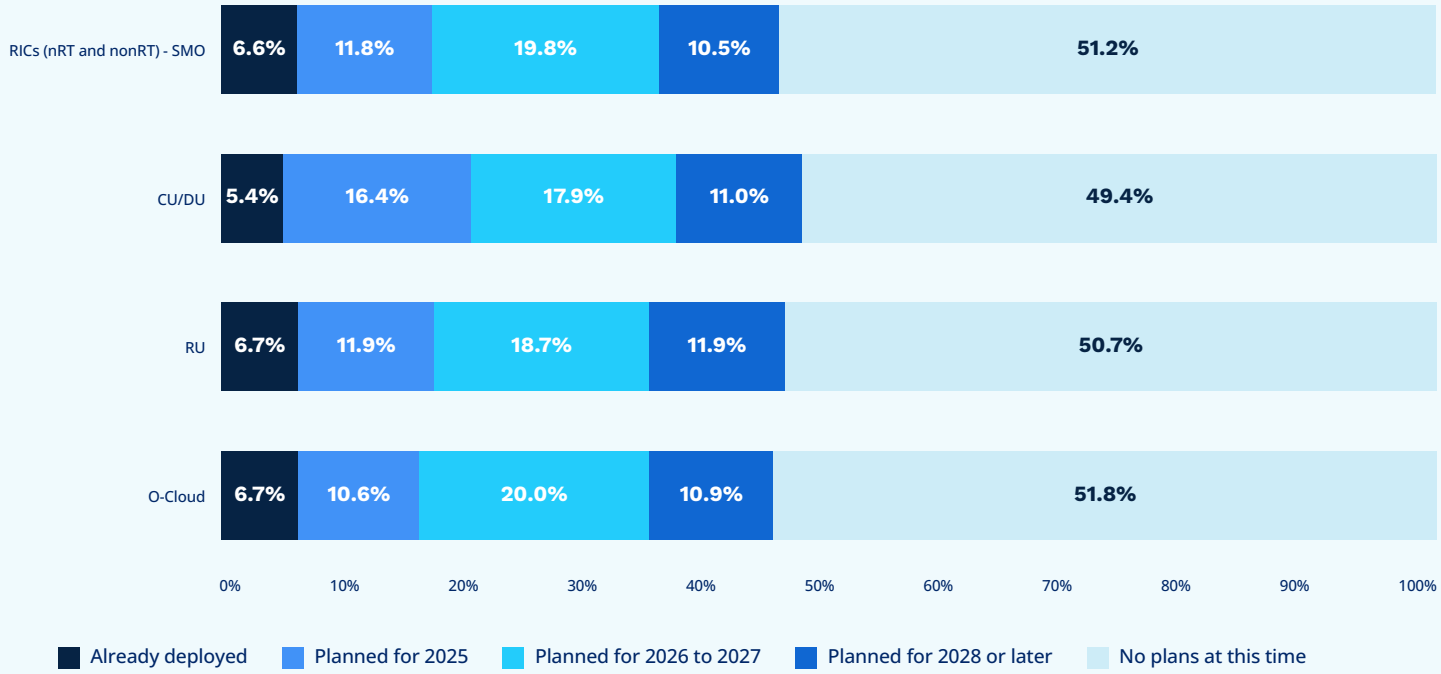
If we assume that the segment of our sample that was able to answer this OpenRAN deployment question (other than DKNS) is representative of the overall sample, then we can estimate what OpenRAN growth will look like over the next several years. The planned implementations in this chart for 2025 and then 2026 through 2027 will have a profound impact on penetration rates. For example, for CU/DU, the penetration rate at the beginning of 2025 was 5.4%. Based on the *planned* for 2025 additions of 16.4%, the estimated penetration rate at the end of 2025 would be 21.8%. Likewise, based on the *planned* for 2026 to 2027 additions, by the end of 2027, penetration for CU/DU would be 39.7%. This yields a growth rate of 304% for 2025 and 82% from the beginning of 2026 to the end of 2027.

Looking across these OpenRAN network functions, the average growth rate for 2025 was 200%, and the average growth rate from the beginning of 2026 to the end of 2027 was 100%. This suggests a strong acceleration of OpenRAN deployments and implies that OpenRAN technologies are transitioning from innovators/enthusiasts at the beginning of 2025 to early adopters/visionaries by the end of 2025 and will include the early majority by the end of 2027. For more information from LF Networking on 2025 predictions, *see 2025 Predictions: Open Networking & Edge*[2].

FIGURE 11

ORGANIZATIONAL PLANS FOR DEPLOYING OPENRAN NETWORK FUNCTIONS

What are your organization's plans for deploying open source OpenRAN network functions in your network? (one response per row)



2025 LF NETWORKING SURVEY, Q30, SAMPLE SIZE = 73-76, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

2 2025 Predictions: Open Networking & Edge, December 2024, Arpit Joshipura and Ranny Haiby, 2025 Predictions: Open Networking & Edge - LF Networking

AI use cases for supporting open networking

AI plays a vital role in supporting open network operations by enabling automation, intelligence, and adaptability across complex, distributed systems. It enhances efficiency through automated orchestration, reduces human error, and accelerates fault detection and resolution. AI-driven analytics provide real-time insights, allowing proactive network management and improved decision-making. In open, cloud native environments, AI ensures seamless integration, scalability, and security by dynamically responding to changing network demands and threats. As networks become more software-defined and data-driven, AI becomes essential for maintaining performance, reliability, and innovation, making it a cornerstone of next-generation open network operations.

Figure 12 shows that there is a valuable role for AI in transforming network operations, particularly in the areas of network automation and orchestration (57%), AI for network security and threat detection (50%), and predictive maintenance and fault detection (43%). These three categories represent the most explored or deployed AI applications among organizations progressing toward cloud native networking.

AI significantly supports network automation and orchestration by enabling intelligent and autonomous management of network infrastructure. It automates routine processes such as configuration management, software deployment, and traffic routing, reducing the need for manual intervention. With the help of machine learning, AI can analyze real-time data to make decisions, ensuring optimal resource utilization and minimizing latency. Organizations with advanced cloud native capabilities are leveraging AI to implement closed-loop automation, where systems self-monitor and self-correct without human input.

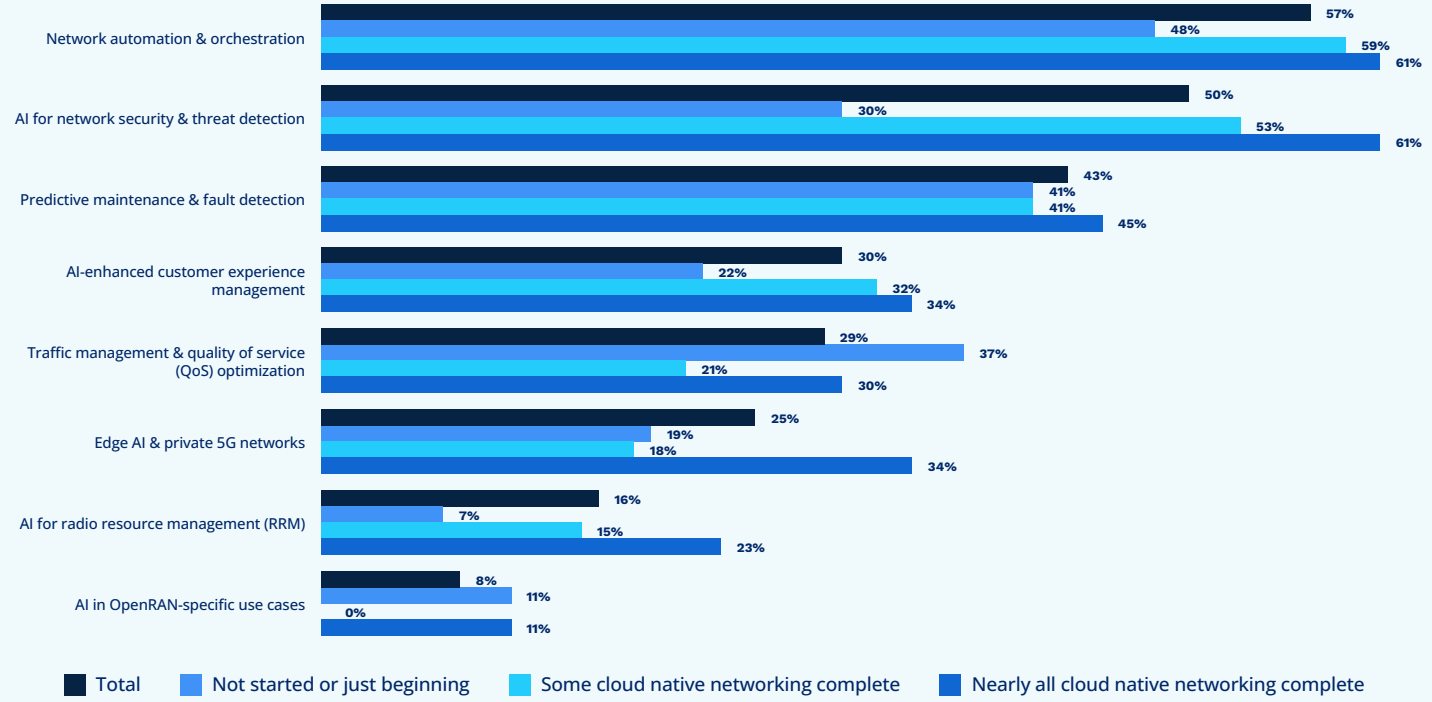
In network security and threat detection, AI plays a crucial role in proactively defending digital infrastructure. By leveraging machine learning algorithms, AI can learn normal traffic behavior and identify anomalies that may signal potential threats. This enables real-time detection and prevention of cyberattacks, malware, and intrusion attempts. AI also enhances threat intelligence by integrating with external data sources and updating security protocols dynamically. Organizations with more mature cloud native implementations are more likely to deploy AI for advanced, automated threat response.

For predictive maintenance and fault detection, AI helps organizations move from reactive to proactive network management. By analyzing historical and real-time performance data, AI predicts failures before they occur and identifies underlying patterns associated with network faults. This minimizes downtime, reduces operational costs, and improves service reliability. AI-driven analytics also support rapid root cause analysis and efficient fault resolution, making it a key enabler in maintaining network health in complex environments.

FIGURE 12

AI APPLICATION USE CASES FOR OPEN NETWORK OPERATIONS

Which AI applications are your organization currently exploring or deploying within your open network operations? (select all that apply) **segmented by: cloud native networking progress**



2025 LF NETWORKING SURVEY, Q33 X Q17, SAMPLE SIZE = 105, VALID CASES = 105, TOTAL MENTIONS = 271, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Figure 12 also shows that organizations with nearly all cloud native networking complete lead across most AI application categories because they have already optimized their infrastructure for automation, scalability, and real-time data processing—key enablers for AI. These organizations have the architecture and tools needed to integrate AI into operations such as orchestration, security, and predictive maintenance.

Their advanced maturity allows them to move beyond foundational capabilities and focus on intelligent optimization. The only exception is AI in OpenRAN-specific use cases, which remains low across all segments due to its niche complexity and emerging nature, requiring specialized expertise and ecosystem support that even mature organizations may not yet possess.

Approaches for developing networking-focused AI applications

Figure 13 highlights the key approaches organizations are taking to develop AI applications. A significant majority (75%) prefer using open source as a foundation to build organization-specific applications. This strategy offers flexibility, cost efficiency, and often faster time-to-market. Open source tools allow organizations to leverage a broad ecosystem of community-tested components, accelerating innovation while retaining the ability to customize solutions to their unique networking needs.

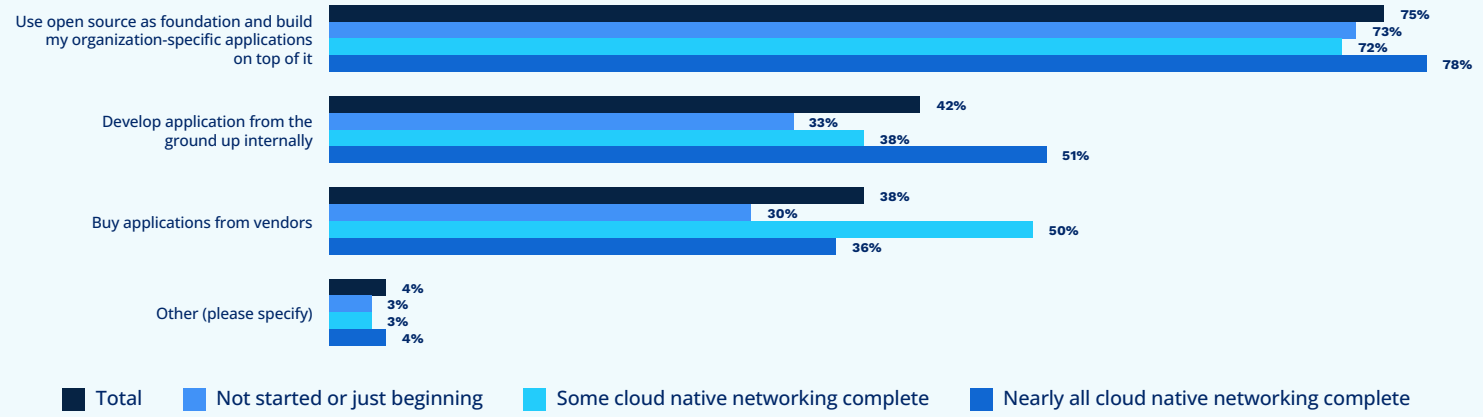
In contrast, 42% of respondents develop AI applications from the ground up internally. This method provides full control over the architecture and functionality, which is essential for highly specialized use cases or industries with strict regulatory requirements. Although more resource-intensive, it ensures tailor-made solutions that closely align with internal infrastructure and long-term goals.

Alternatively, 36% of organizations are likely to buy applications from vendors. This approach reduces development time and ensures support and maintenance from the vendor, making it ideal for organizations that may lack in-house AI expertise or need rapid deployment. However, it can lead to vendor lock-in and limited customization. Each approach reflects a balance between control, speed, cost, and capability—often depending on how advanced an organization is in adopting cloud native networking.

FIGURE 13

APPROACHES ORGANIZATIONS ARE USING TO DEVELOP AI-BASED NETWORKING APPLICATIONS

What approaches will your organization use to develop these AI applications? (select all that apply) **segmented by: cloud native networking progress**



2025 LF NETWORKING SURVEY, Q35 X Q17, SAMPLE SIZE = 107, VALID CASES = 107, TOTAL MENTIONS = 170, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Figure 13 also shows that organizations with some cloud native networking applications complete (50%) are more likely to buy AI applications from vendors because they are in a transitional phase—needing quick, reliable solutions to bridge capability gaps. Purchasing from vendors allows them to deploy functional tools without internal development delays, enabling faster progress while internal infrastructure matures. This approach balances operational needs with ongoing modernization, helping them stay competitive without overextending limited in-house development resources.

AI foundational capabilities necessary to accelerate the development of open networking frameworks and applications

Developing AI frameworks and applications in support of open networking operations is critical for driving innovation, scalability, and interoperability in modern network environments. Open networking encourages collaboration across vendors and organizations, allowing AI solutions to be more adaptable and future-proof. By leveraging open standards and open source tools, organizations can avoid vendor lock-in, reduce costs, and accelerate development cycles. AI enhances network automation, fault prediction, and performance optimization—key aspects in managing complex, cloud native infrastructures. Together, AI and open networking foster agile, intelligent systems that can evolve with emerging technologies and meet dynamic business demands more effectively.

Figure 14 clearly highlights that organizations perceive the availability of high-quality data sets and frameworks for AI application development as the most critical foundational elements for accelerating the development of open source, network domain-specific AI applications.

A significant 56% of respondents ranked high-quality data sets as the number one factor, indicating that data is the cornerstone of effective AI. In the context of networking applications, high-quality, domain-specific data is essential for training models that are accurate, reliable, and generalizable. Without such data, even the most sophisticated algorithms cannot perform well. Data is what enables models to learn patterns, identify anomalies, and make decisions in complex, real-world networking environments. The emphasis on data reflects a broad industry recognition that real progress in AI is heavily dependent on having the right kind of data available in sufficient volume and quality.

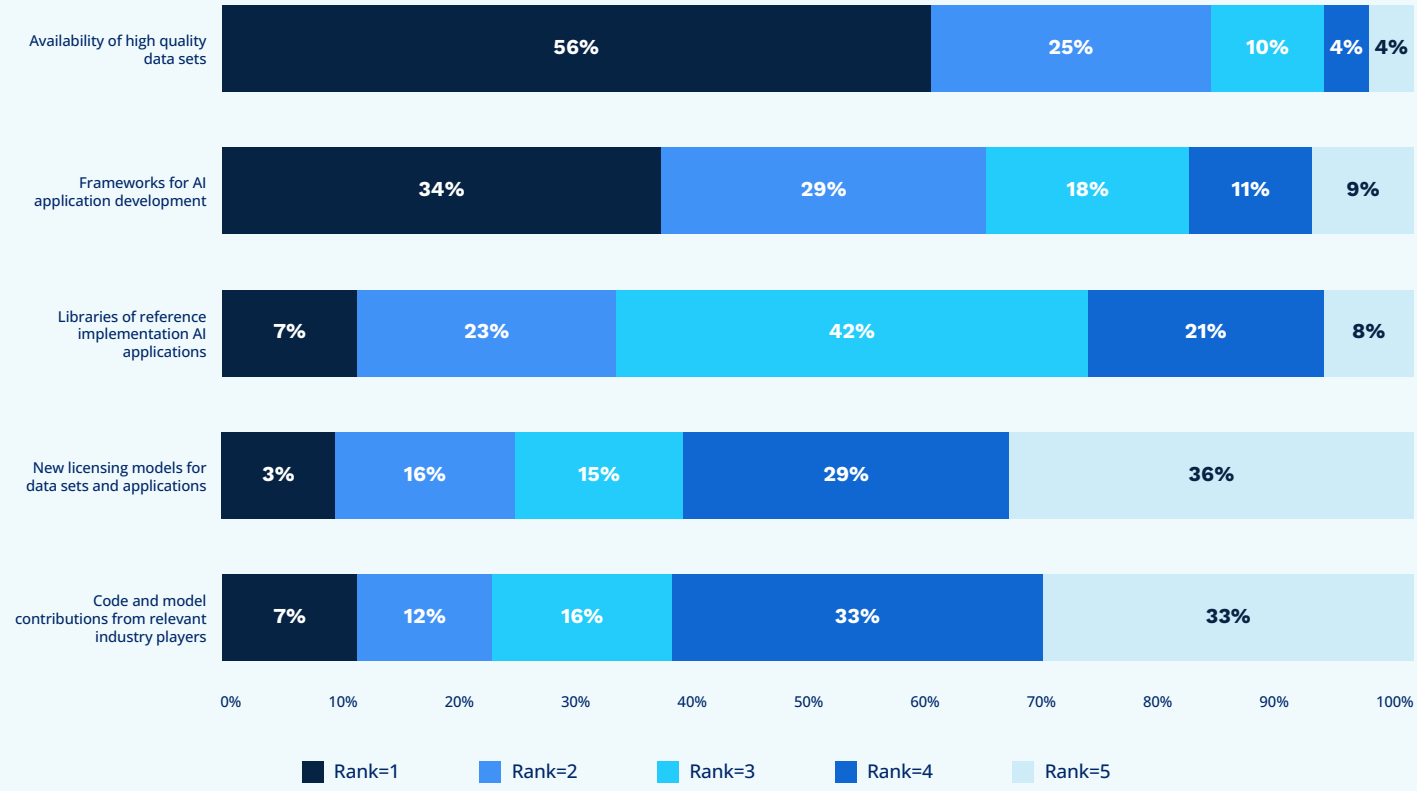
Following this, 34% of respondents ranked frameworks for AI application development as the top priority. Frameworks such as TensorFlow, PyTorch, and domain-specific tools provide the necessary infrastructure for developers to build, test, and deploy AI models efficiently. These frameworks abstract away much of the complexity involved in model development, enabling faster innovation and easier collaboration. In network-focused AI, where time-to-market and performance are critical, having robust development frameworks accelerates experimentation and deployment.

Together, these two elements—quality data and powerful development frameworks—form the foundation for building scalable, effective AI solutions in the networking space, driving forward innovation and adoption.

FIGURE 14

LEADING AI FOUNDATIONAL CAPABILITIES NECESSARY TO ACCELERATE AI OPEN NETWORKING APPLICATIONS

Please rank order the following AI actions based on their ability to best accelerate development of open source, network domain-specific AI frameworks and applications? (rank order each response)



2025 LF NETWORKING SURVEY, Q36, SAMPLE SIZE = 96-104, DKNS RESPONSES EXCLUDED FROM THE ANALYSIS

Conclusions

The 2025 LF Networking Report offers a comprehensive view into the current landscape and future trajectory of open source networking, cloud native adoption, OpenRAN, and AI integration. A central takeaway is the critical and strategic role that OSS now plays across organizations, irrespective of size or industry. An overwhelming majority of respondents (92%) deem OSS crucial to their future, while 94% emphasize the importance of open source foundations, signaling strong trust in community-led innovation and governance.

Adoption of cloud native networking is accelerating across the board. Large enterprises are leading with higher completion rates, but smaller and medium-sized organizations are also actively engaging, albeit with greater variance due to resource disparities. A notable insight is the bimodal adoption pattern among small organizations, in part because agile startups are embracing modern technologies early.

The top motivations for engaging with the open source community align around cost savings, vendor independence, accelerated innovation, and community support. Importantly, organizations across all stages of cloud native maturity cite reduced vendor lock-in and cost efficiency as the leading drivers—reflecting a universal desire for flexibility and long-term value.

In terms of technical capabilities, scalable and high-performing operations rank as the top open networking priorities, with edge performance and multi-architecture support following closely behind. These capabilities address the diverse demands of modern infrastructures, especially as organizations scale globally and embrace hybrid environments.

Yet, challenges remain. Architectural complexity, legacy integration, and skills gaps consistently rank as the leading obstacles. These challenges are especially acute for organizations midway through their cloud native journey, where the realities of large-scale transformation come into sharp focus. Similarly, barriers to OSS adoption—such as licensing risks and security concerns—remain prominent, particularly among organizations still building foundational readiness.

Support for end-to-end Super Blueprints is nearly unanimous (86%), reflecting a widespread desire for standardized, modular frameworks that ease deployment, reduce risk, and improve interoperability across open networking solutions. Respondents see Super Blueprints as a path toward more scalable and production-ready systems that minimize integration complexity and accelerate innovation.

OpenRAN adoption, while still in its early stages, shows strong momentum through 2027. Although a significant portion of respondents were unsure about their organization's specific OpenRAN plans, those who could respond highlighted a clear high growth trend across those OpenRAN network functions that we asked about. Standardization, interoperability, and Kubernetes integration are the main drivers for OpenRAN, particularly among organizations with mature cloud native infrastructures.

The role of AI in open networking is rapidly expanding. Organizations are widely deploying AI applications for automation, security, and predictive maintenance, with mature organizations leading the charge due to their optimized infrastructure and readiness for intelligent operations. Development strategies favor building on open source foundations (75%), demonstrating alignment between OSS and AI adoption goals.

Crucially, the report emphasizes that data quality and accessible AI frameworks are essential to accelerate AI use in networking. Organizations recognize that without robust, domain-specific datasets and scalable development tools, AI innovation in networking will remain constrained.

Ultimately, the report underscores that open source networking is evolving from an experimental initiative into a core architectural principle. Organizations that embrace community-driven, cloud native, and AI-integrated strategies are in a better position to innovate, reduce costs, and future-proof their infrastructure. However, to fully capitalize on these opportunities, greater investment in skills development, standardized practices, and community engagement is essential.

As the ecosystem matures, collaboration—both within the open source community and across industries—will be the defining force in shaping the future of network infrastructure.

Methodology

The survey's goal was to explore the most significant trends in open source networking. Key topics include:

- Organizational involvement in open source
- Engagement in cloud native networking
- Challenges and benefits of using open source in support of networking
- Interest in and adoption of OpenRAN
- Focus on network-specific AI applications

We collected survey data from industry-specific companies, IT vendors and service providers, and nonprofit, academic, and government organizations. Respondents spanned many vertical industries and companies of all sizes, and we collected data from several geographies, including the Americas, Europe, Asia-Pacific, the Middle East, and Africa.

From a research perspective, it was important to eliminate any perception of sample bias and ensure high data quality. We eliminated sample bias by sourcing our usable sample from Linux Foundation subscribers, members, partner communities, and social media. We addressed data quality through extensive prescreening, survey screening questions, and secondary data quality checks to ensure that respondents had sufficient professional experience to answer questions accurately on behalf of the organization they worked for.

This study is based on a web survey that LF Research and its partners conducted in Q1 2025. Data collection was heavily focused on IT networking professionals. There were 304 respondents who started the survey, with 204 passing our screening questions and 173 completing the survey, yielding a high *qualified completion rate* of 85%. None of these 173 respondents failed our secondary data quality tests—a finding that is unusual and indicates high-quality respondents. The margin of error for the sample was +/- 7.4% with 95% confidence and +/- 6.2% with 90% confidence.

The survey sampled respondents from the networking community, with 83% having more than 10 years of professional experience and 61% having 20 or more years of experience.

Although respondents had to answer nearly all questions in the survey, a provision was made when a respondent was unable

to answer a question. This is accomplished by adding a DKNS response to the list of responses for every question. However, this creates a variety of analytical challenges.

One approach was to treat a DKNS just like any other response to determine the percentage of respondents who answered DKNS. The advantage of this approach is that it shows the exact distribution of collected data. The challenge with this approach is that it can distort the distribution of valid responses (i.e., responses where respondents could answer the question).

Many of the figures in this report exclude DKNS responses when segmenting data because the sample size and percentage of DKNS responses always vary across segments. Excluding DKNS responses enables us to normalize the data to present segmentation results accurately.

The percentage values in this report may not total to exactly 100% due to rounding.

Data.World access

LF Research makes each of its empirical project datasets and this 2025 LF Networking survey available on data.world. Included in this dataset are the survey instrument, raw survey data, screening and filtering criteria, and frequency charts for each question in the survey. LF Research datasets, including this project, are available at *data.world/thelinuxfoundation*. Access to Linux Foundation datasets is free but does require you to create a data.world account.

Survey design

This 2025 LF Networking survey comprised 36 questions. The high-level design of the survey appears in Table 1.

TABLE 1

LF NETWORKING SURVEY DESIGN

LF Networking Survey Design

Section	Questions	Question categories	Who answers the questions
Introductory question	Q1 – Q3	Screening questions	All respondents (N=173)
Demographics	Q4 – Q6	Respondent attributes	All respondents (N=173)
Demographics	Q7 – Q8	Company attributes	Respondents who are employed (N=157)
OSS Involvement	Q9 – Q16	Respondent involvement in OSS	Respondents who use or contribute to OSS (N=153 to 169)
Cloud native networking	Q17 – Q19	Cloud native networks	Respondents who are employed & whose organization is involved in cloud native networking (N=132 to 157)
OSS impact on networking	Q20 – Q27	OSS networking use and challenges	Respondents who use or contribute to OSS (N=153 to 169)
OpenRAN	Q28 – Q31	Open Radio Access Networking	All respondents (N=157 to 173)
Networking & AI	Q32 – Q36	LF networking & AI	All respondents (N=157 to 165)

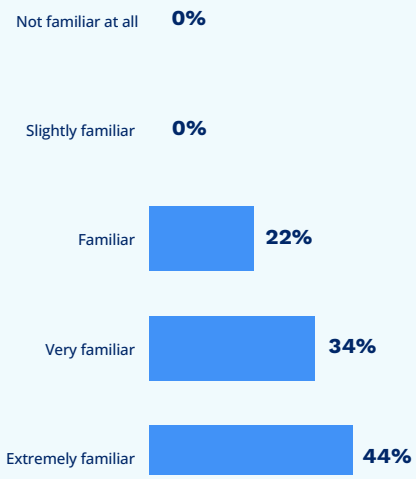
Survey demographics

These demographics provide you with a profile of the LF Networking survey respondents and the organizations they work for. We regrouped all of the demographics in Figures 15 and 16 to facilitate a more insightful analysis. To access the original source data and study frequencies, please see the data. world access section above.

FIGURE 15

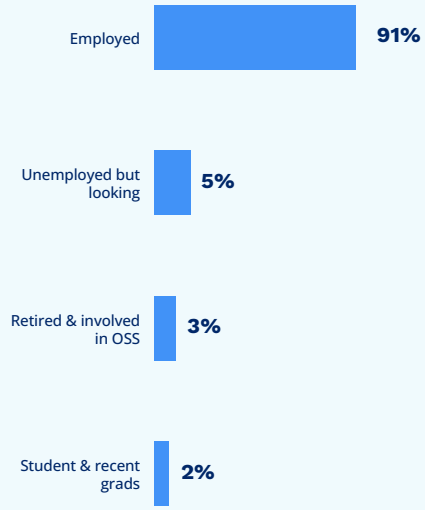
DEMOGRAPHICS I

How familiar are you with telecommunications, cloud, and enterprise networks? (select one)



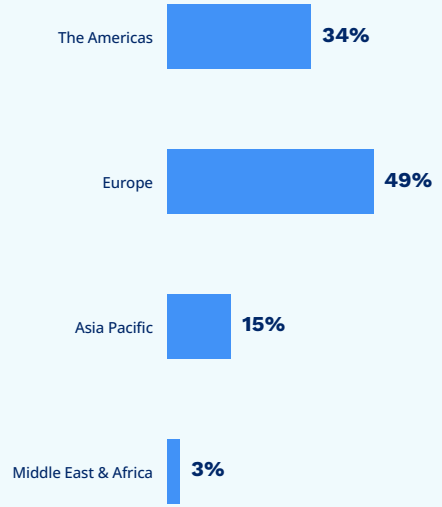
2025 LF NETWORKING SURVEY, Q1, SAMPLE SIZE = 173

Employment status



2025 LF NETWORKING SURVEY, Q3, SAMPLE SIZE = 173

Geographic region

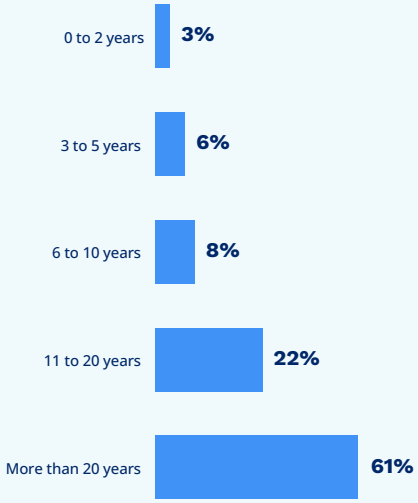


2025 LF NETWORKING SURVEY, Q4, SAMPLE SIZE = 173

FIGURE 16

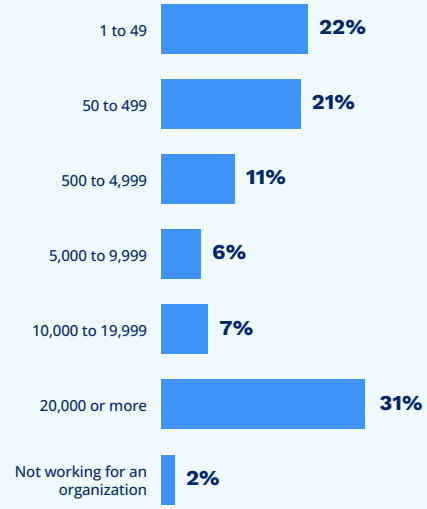
DEMOGRAPHICS II

How many years of professional experience do you have? (select one)



2025 LF NETWORKING SURVEY, Q5, SAMPLE SIZE = 173

Please estimate how many total employees are in the organization you work for. (select one)



2025 LF NETWORKING SURVEY, Q7, SAMPLE SIZE = 157

What is your primary job function? (select one)

2025 LF NETWORKING SURVEY, Q8, SAMPLE SIZE = 157

About the Authors

STEPHEN HENDRICK is the vice president of research at the Linux Foundation, where he is the principal investigator on a variety of research projects core to the Linux Foundation's understanding of how OSS is an engine of innovation for producers and consumers of IT. Steve specializes in primary research techniques he has developed over 30 years as a software industry analyst. He is a subject matter expert in application development and deployment topics, including DevOps, application management, and decision analytics. Steve brings experience in a variety of quantitative and qualitative research techniques that enable deep insight into market dynamics and has pioneered research across many application development and deployment domains. He has authored over 1,000 publications and provided market guidance through syndicated research and custom consulting to the world's leading software vendors and high-profile startups.

RANNY HAIBY is in charge of driving technical innovation further, creating opportunities for synergies among open source projects, and identifying emerging trends and projects. Ranny is a software veteran who has been focusing on pushing the envelope in open source innovation in recent years. Prior to joining the Linux Foundation Ranny was a director at Samsung Research America, leading the open source group. He provided leadership and guidance for engineering teams across Samsung who were actively contributing to open source projects such as ONAP, CNCF, ROS, and Matter (CHIP).

Acknowledgments

We thank all the participants of the survey for kindly sharing their insights and experience. Special thanks to the peer reviewers and Linux Foundation colleagues for their involvement in the various stages of the research process, including Elizabeth Bushard, Hilary Carter, Mia Chaszeyka, Ranny Haiby, Anna Hermansen, Arpit Joshipura, Adrienn Lawson, Jill Lovato, and Christina Oliviero.

LF NETWORKING

The Linux Foundation Networking (LF Networking, LFN) is the largest set of open source networking projects in the world. A broad industry coalition form LF Networking with the goal of fostering a commercial-ready networking ecosystem that embraces open, emerging, and evolving technologies. Now in its eighth year as an umbrella organization, LF Networking software and projects provide the foundations for network infrastructure and services across service providers, cloud providers, enterprises, vendors, and system integrators that enable rapid interoperability, deployment and adoption.

THE LINUX FOUNDATION | Research

Founded in 2021, Linux Foundation Research explores the growing scale of open source collaboration, providing insight into emerging technology trends, best practices, and the global impact of open source projects. Through leveraging project databases and networks and a commitment to best practices in quantitative and qualitative methodologies, LF Research is creating the go-to library for open source insights for the benefit of organizations the world over.

x.com/linuxfoundation

facebook.com/TheLinuxFoundation

linkedin.com/company/the-linux-foundation

youtube.com/user/TheLinuxFoundation

github.com/LF-Engineering

To reference this work, please cite as follows: Stephen Hendrick and Ranny Haiby, "The 2025 Open Source Networking Study: The Role and Value of Open Source in the Networking Industry's Software Stack," foreword by Arpit Joshipura, The Linux Foundation, April 2025.