



The State of Network Security in Transportation & Logistics

Key Findings on Operational
Visibility, Cloud Readiness,
and GenAI Impact

CONTENTS

Executive Summary	03
Introduction	04
Who We Surveyed	05
Survey Findings	06
Comparison with Manufacturing Sector	18
Strategic Recommendations & Concluding Thoughts	19



Executive Summary

The Network Security Trends in Transportation and Logistics Survey, conducted from February to May 2025, offers an in-depth view of how IT and security leaders across the sector are preparing for digital transformation. With a focus on performance, visibility, and security, these organizations are facing mounting challenges tied to legacy infrastructure, limited resources, and growing cyber threats.

The report identifies a consistent demand for simplification, stronger observability, better protection against ransomware, and support for hybrid application environments. Most are still in early stages of GenAI preparedness and security convergence, with many seeking solutions that can meet both operational and strategic objectives.

Cheers,

Team Aryaka





Introduction

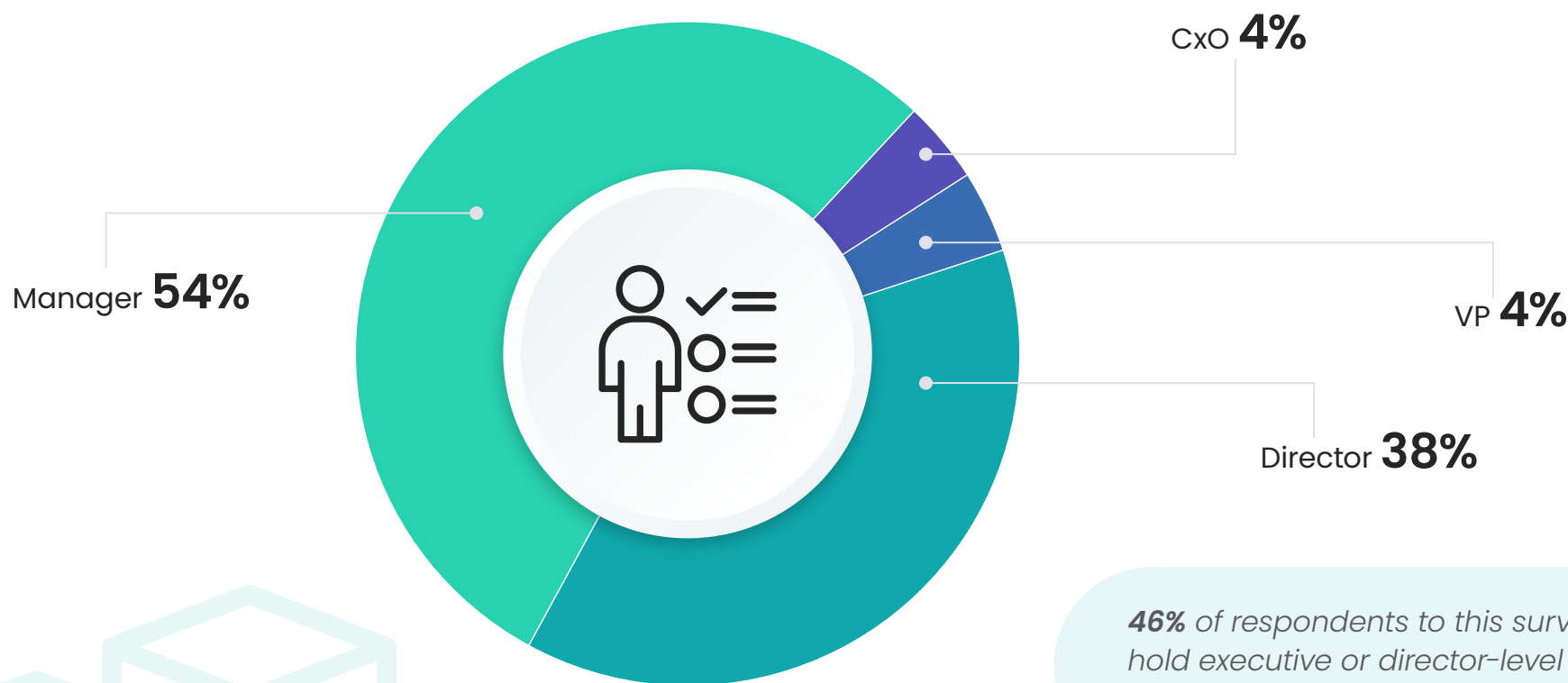
The transportation and logistics sector sits at the intersection of physical and digital infrastructure. As supply chains become more connected and cloud-enabled, network complexity and cybersecurity risk have increased. Organizations now operate global, hybrid environments supporting warehouses, fleets, air and sea transport, and real-time systems. This survey captures the challenges and goals of IT leaders in the industry, offering a snapshot of evolving trends and readiness.



Who We Surveyed

? Who participated in the survey?

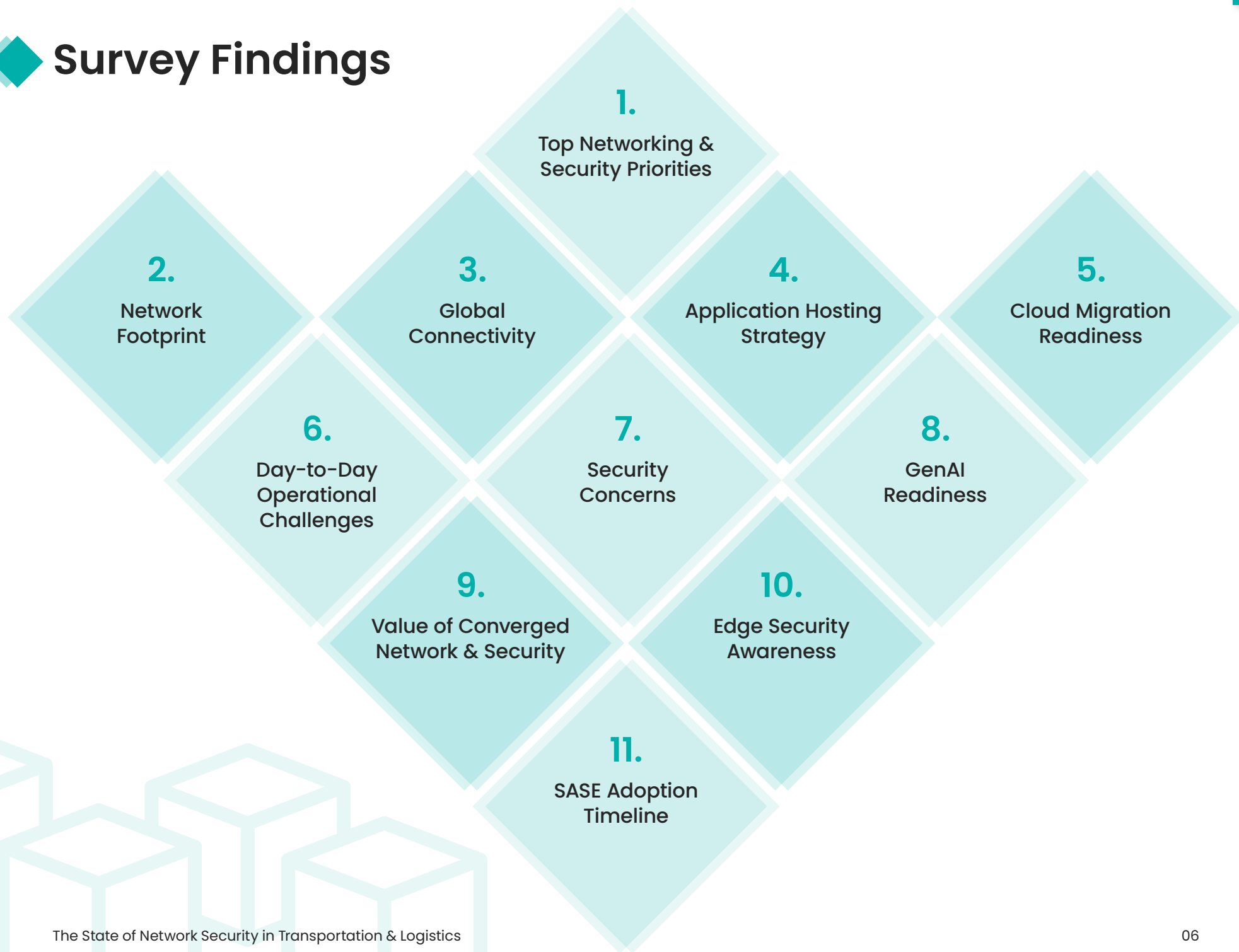
Executives from the transportation and logistics industry responded. The group included C-level executives, IT directors, and operations managers—representing a range of perspectives across digital transformation, infrastructure, and security.



46% of respondents to this survey hold executive or director-level positions in their organization.



Survey Findings

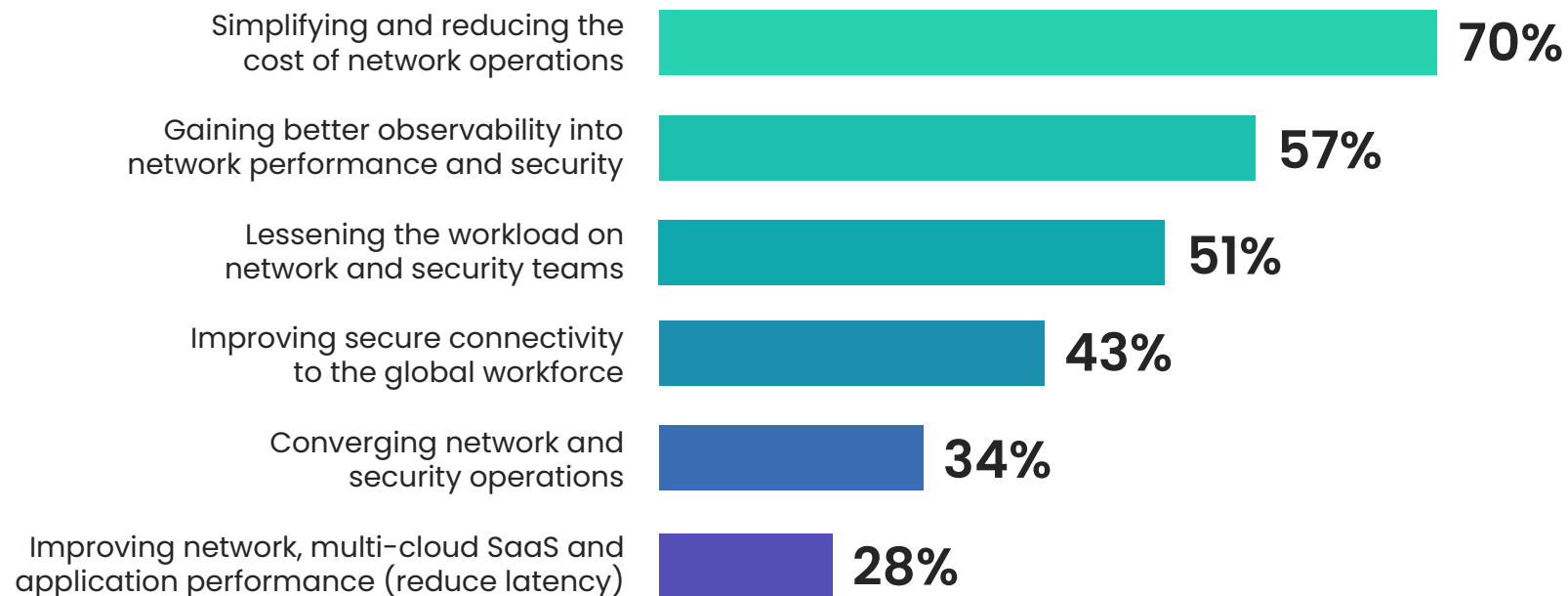




1. Top Networking & Security Priorities

? What are your top three networking and network security priorities in the next 12 months?

Simplifying and lowering network costs (70%) leads the list, followed by the need to improve network performance and security visibility (57%) and reduce workload on IT teams (51%).



Implications: Organizations are focused on operational efficiency and visibility. Reducing manual oversight and gaining more transparent insights into performance and risk are immediate goals.

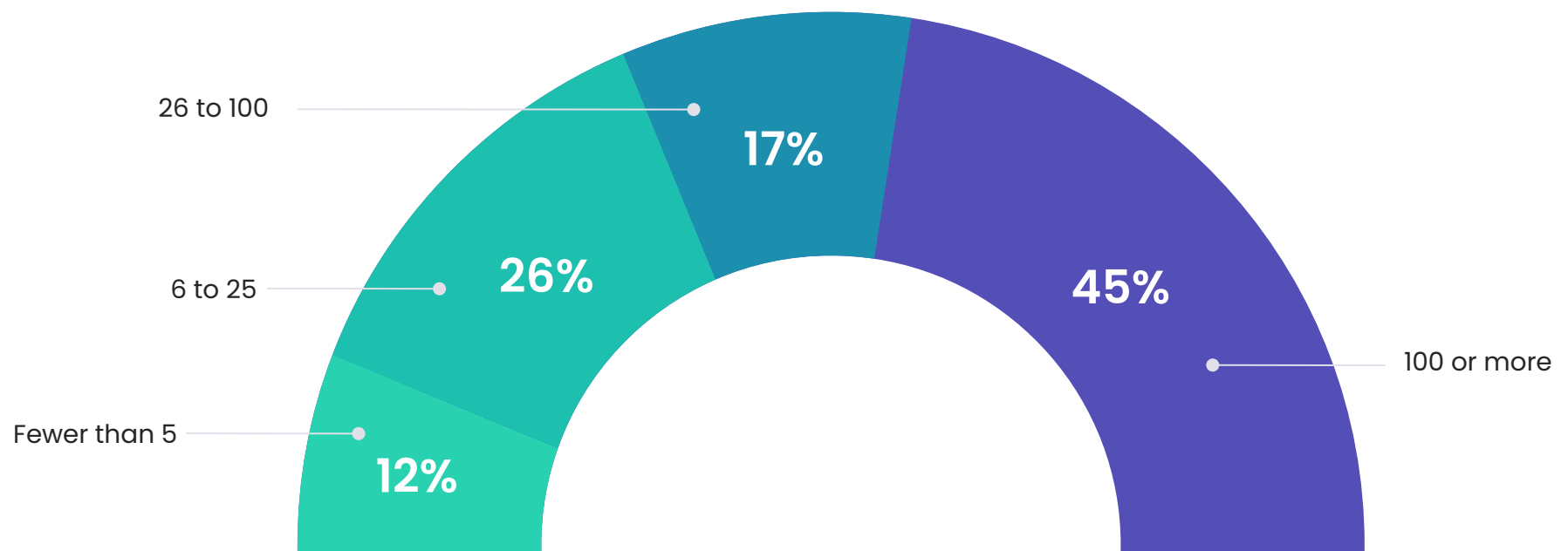




2. Network Footprint

? How many networked facilities do you have?

Nearly half of respondents (45%) have more than 100 connected sites, while another 26% manage between 6 and



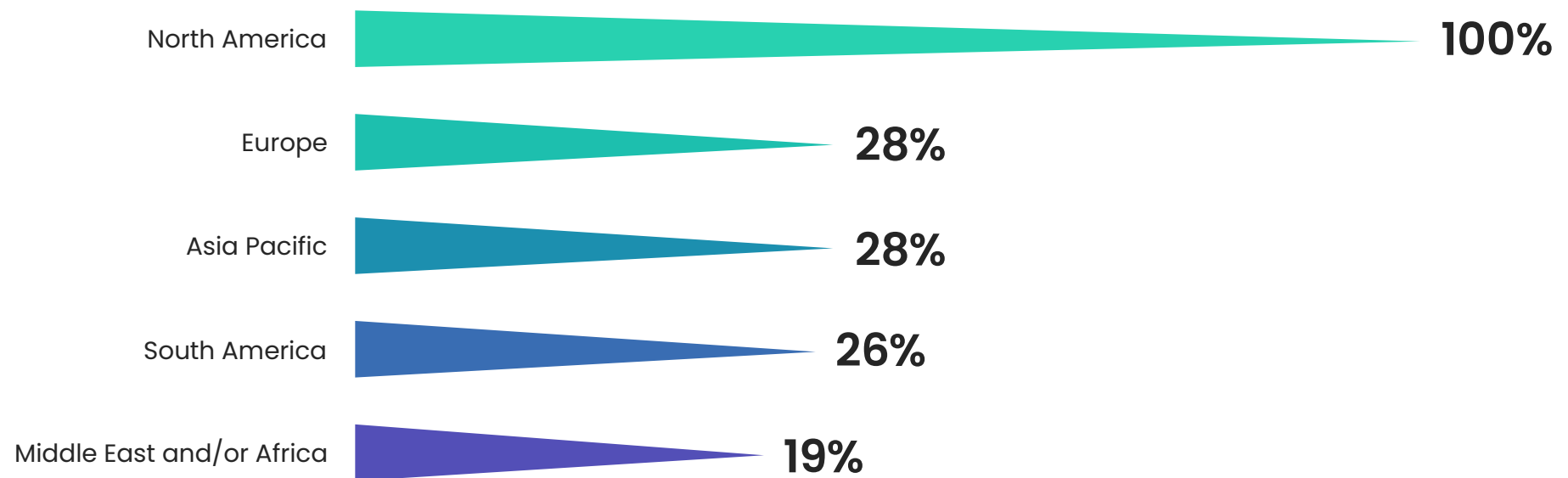
Implications: The large and varied geographic spread increases the complexity of consistent policy enforcement, access control, and incident response across sites



3. Global Connectivity

? Where are your connected facilities located?

100% operate in North America, while nearly a third have facilities in Europe (28%) and Asia-Pacific (28%), with South America (26%) and MEA (19%) following.



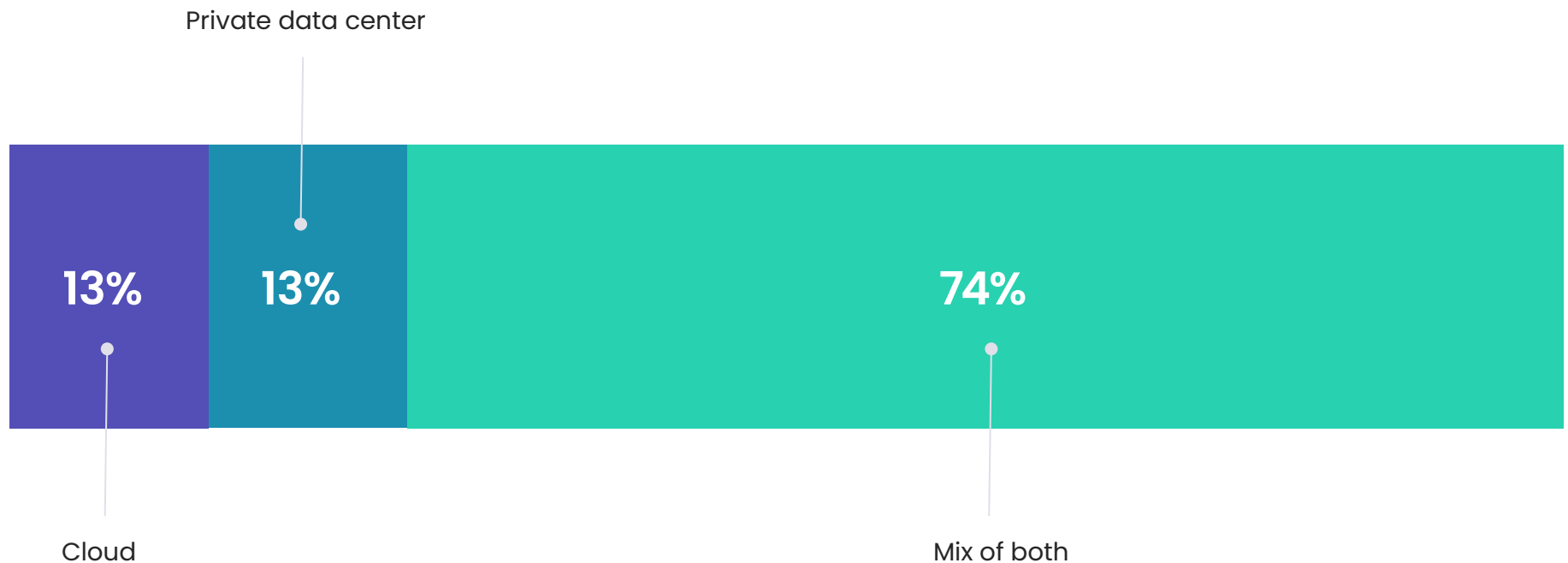
Implications: Distributed operations increase the need for reliable, global connectivity and consistent network security across regions and time zones.



4. Application Hosting Strategy

? Where do your critical applications sit?

Most respondents (74%) rely on a hybrid mix of private data centers and cloud environments.



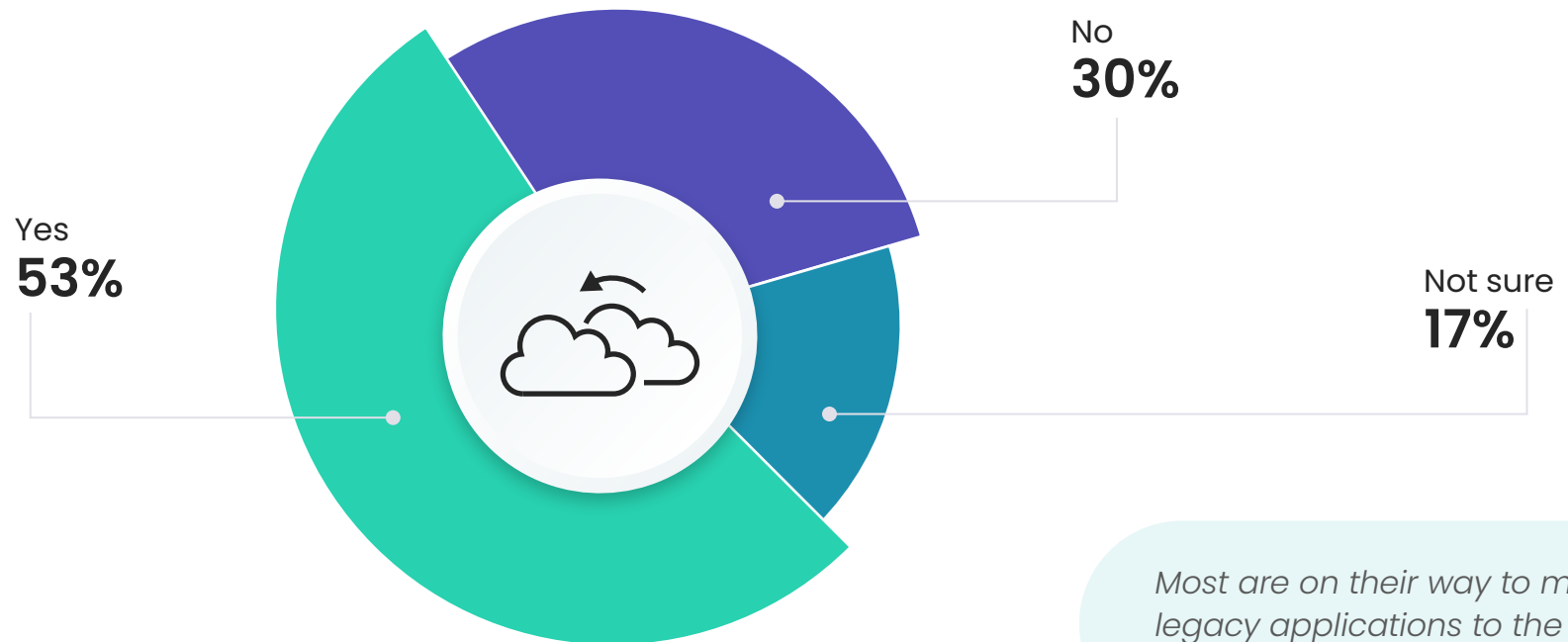
Implications: Hybrid IT strategies reflect a need for integration flexibility, data protection, and consistent performance across diverse hosting environments.



5. Cloud Migration Readiness

? Is your organization on a path to move legacy applications to the cloud?

Most organizations are actively migrating or planning for cloud transitions, while a smaller percentage remain on-premises.



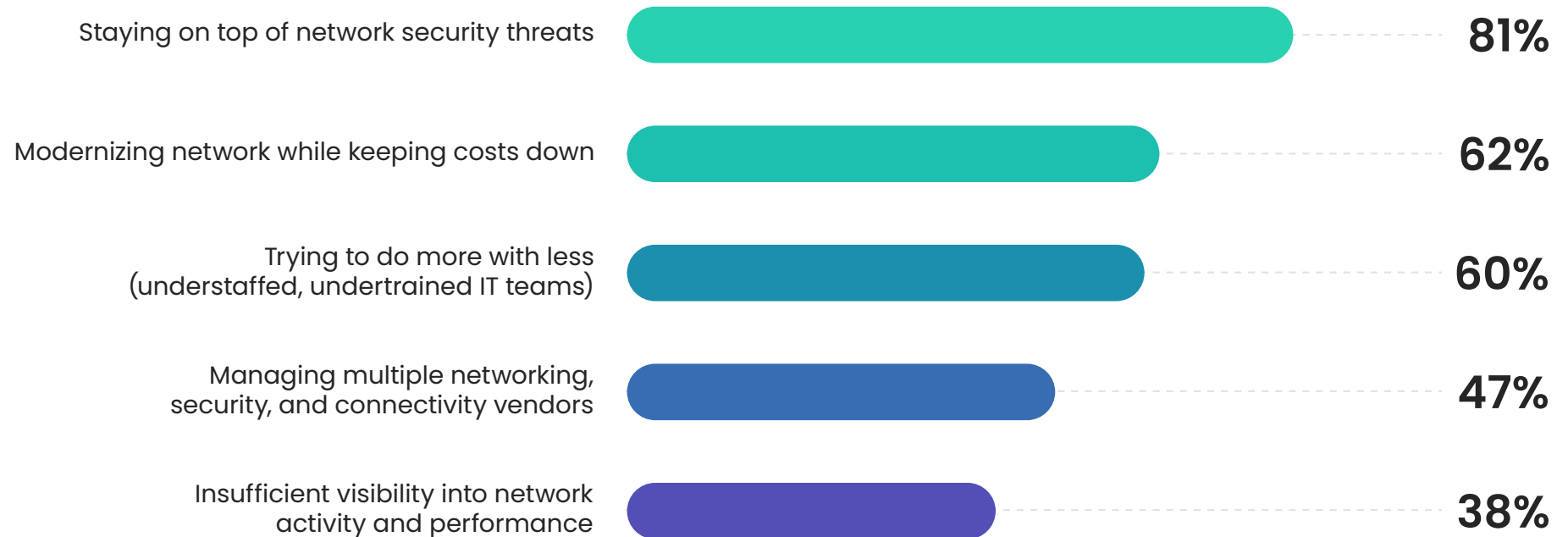
Implications: Enterprises must manage transitional complexity while ensuring legacy and cloud systems can securely interoperate.



6. Day-to-Day Operational Challenges

? What are your top three networking challenges?

Staying ahead of cybersecurity threats (81%) is the most cited issue, followed by cost-effective modernization (62%) and understaffed IT teams (60%).



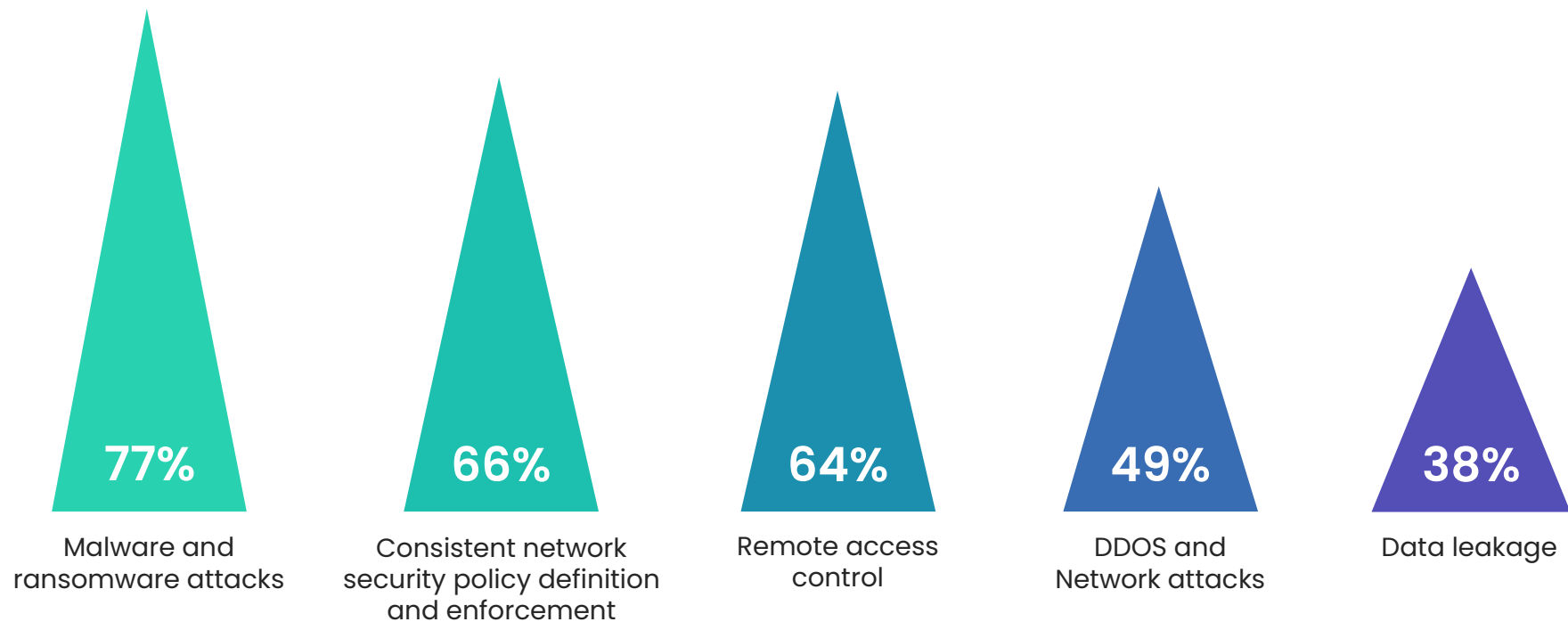
Implications: There is strong demand for solutions that relieve pressure on lean teams while strengthening cyber resilience and supporting infrastructure upgrades.



7. Security Concerns

? What are your top three network security concerns?

Ransomware and malware threats (77%) are the top concern, with policy enforcement (66%) and remote access control (64%) also significant.



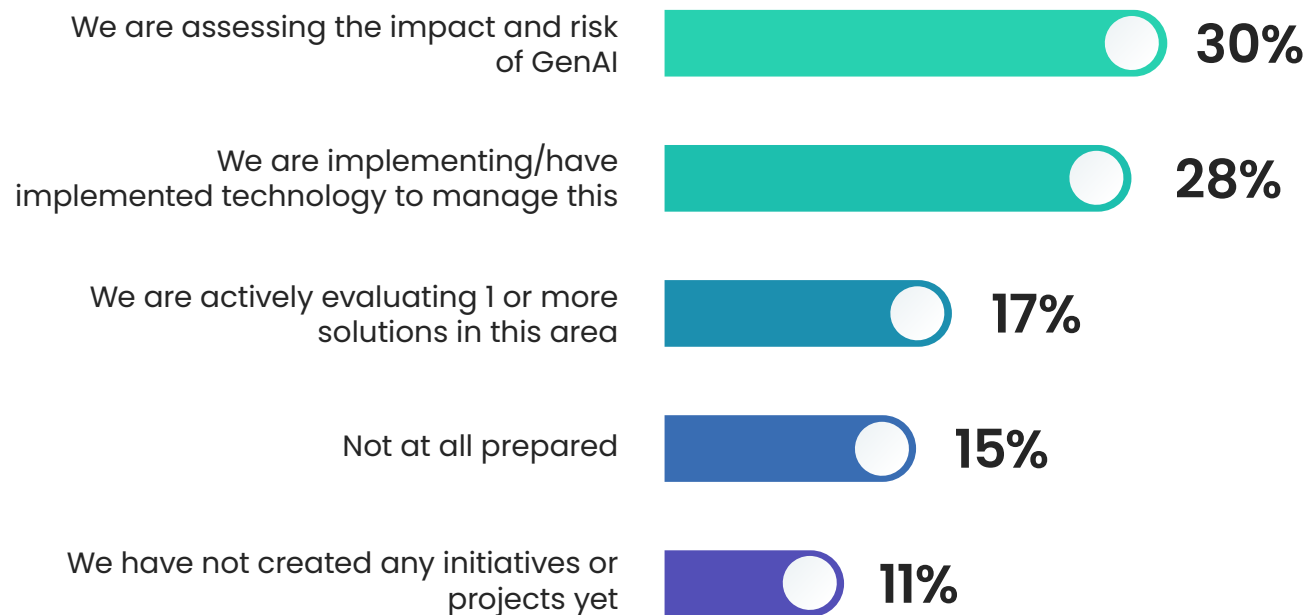
Implications: IT teams are balancing access flexibility with security enforcement. Tools that provide policy consistency without hampering performance are essential.



8. GenAI Readiness

? How prepared is your team to deal with GenAI-related network and security issues?

Only 28% have started implementing solutions, while 56% are either still evaluating risks or unprepared.



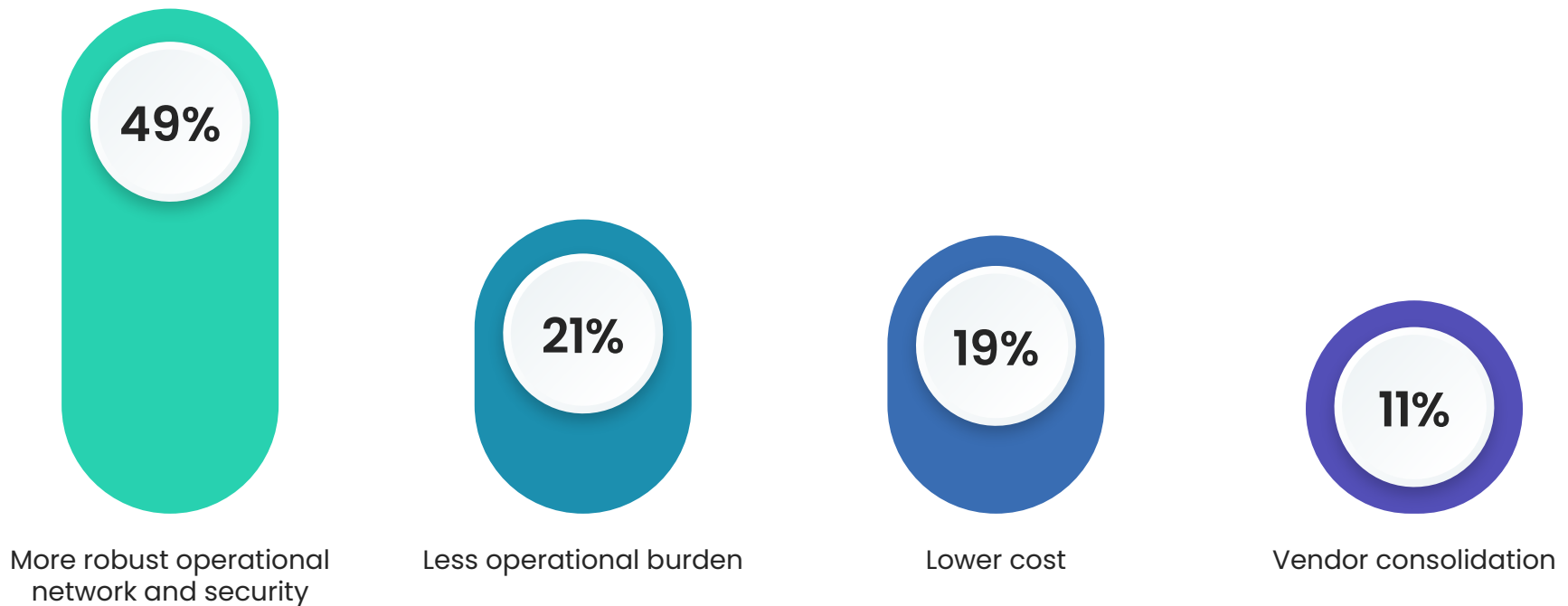
Implications: GenAI introduces bandwidth, latency, and security demands that few teams are fully equipped to handle. Strategic planning and scalability will be key.



9. Value of Converged Network & Security

? What do you consider the main benefit of converging networking and security?

Nearly half (49%) see convergence as a way to create stronger, more efficient operations.



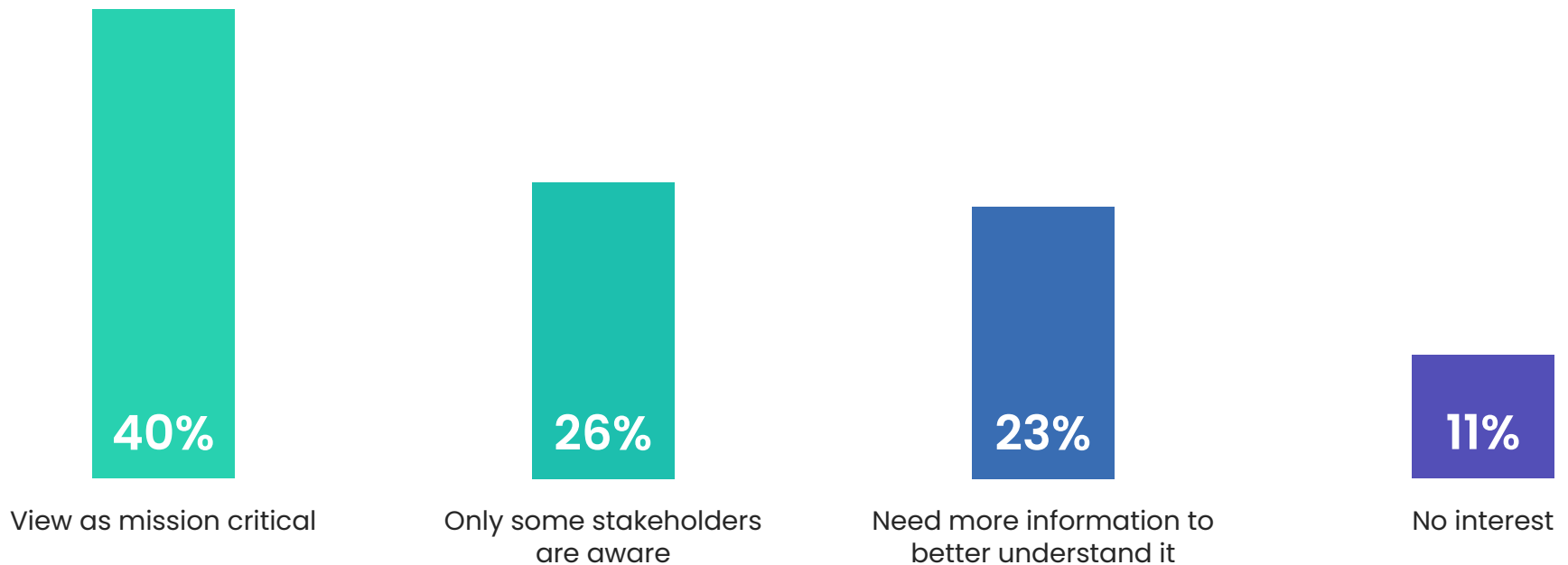
Implications: Integrated approaches are gaining support, though broader education and proof-of-value are likely needed to drive adoption.



10. Edge Security Awareness

? What is your IT organization's perceived value of implementing application security at the network edge?

Only 40% consider edge security a mission-critical capability, while 49% are unsure or unaware.



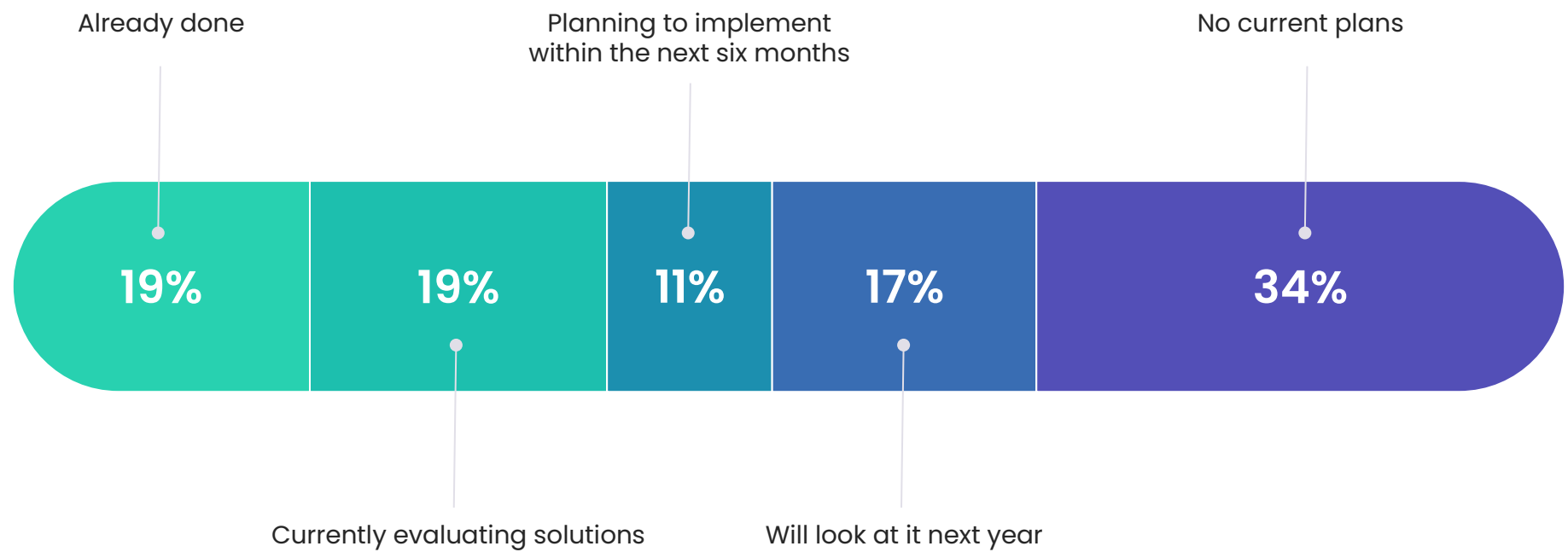
Implications: There's a significant gap in awareness around the role of edge protection, suggesting a need for internal alignment and knowledge building.



11. SASE Adoption Timeline

? When do you plan to implement a converged networking and security solution such as SASE?

19% have implemented a solution. Another 30% are evaluating or planning near-term rollouts. One-third have no current plans.



Implications: Interest in convergence is growing, but budget constraints and legacy environments may be slowing adoption.



Comparison with Manufacturing Sector

This survey echoes many of the findings reported in Aryaka's State of Network Security in Manufacturing (2024), which examined similar challenges in a related operationally intensive industry.

Shared Trends:



High prioritization of cost control, visibility, and network modernization



Hybrid and cloud migration strategies dominate

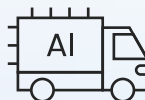


Limited IT resources pose barriers to modernization

Transportation vs. Manufacturing:



Transportation respondents place more emphasis on mobility and remote access control



GenAI preparedness appears slightly lower in transportation



Manufacturing respondents showed stronger early movement toward multi-cloud acceleration and edge security

Strategic Recommendations

1

Improve Observability

Gain holistic insights across network and application layers.

2

Relieve IT Burden

Evaluate opportunities for co-management or service-based delivery.

3

Secure the Edge

Align access and enforcement with remote and distributed user needs.

4

Pursue Integration

Reduce fragmentation between network and security tools to boost agility and reduce complexity.

Concluding Thoughts

Transportation and logistics enterprises are entering a period of digital acceleration. With globally distributed facilities and increasing reliance on cloud and AI, the need for resilient, high-performance, and secure network infrastructure is urgent. This report confirms the direction of change and underscores the importance of cohesive strategies that support operational scale, visibility, and cyber readiness.

About Aryaka

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions.

For more on Aryaka, please visit www.aryaka.com.



Schedule a Free Network
Consultation with an Aryaka Expert

See How It Works



Experience Aryaka's
Unified SASE as a

View Interactive Tour



info@aryaka.com | +1.888.692.7925

