Enterprise Strategy Group™
by TechTarget

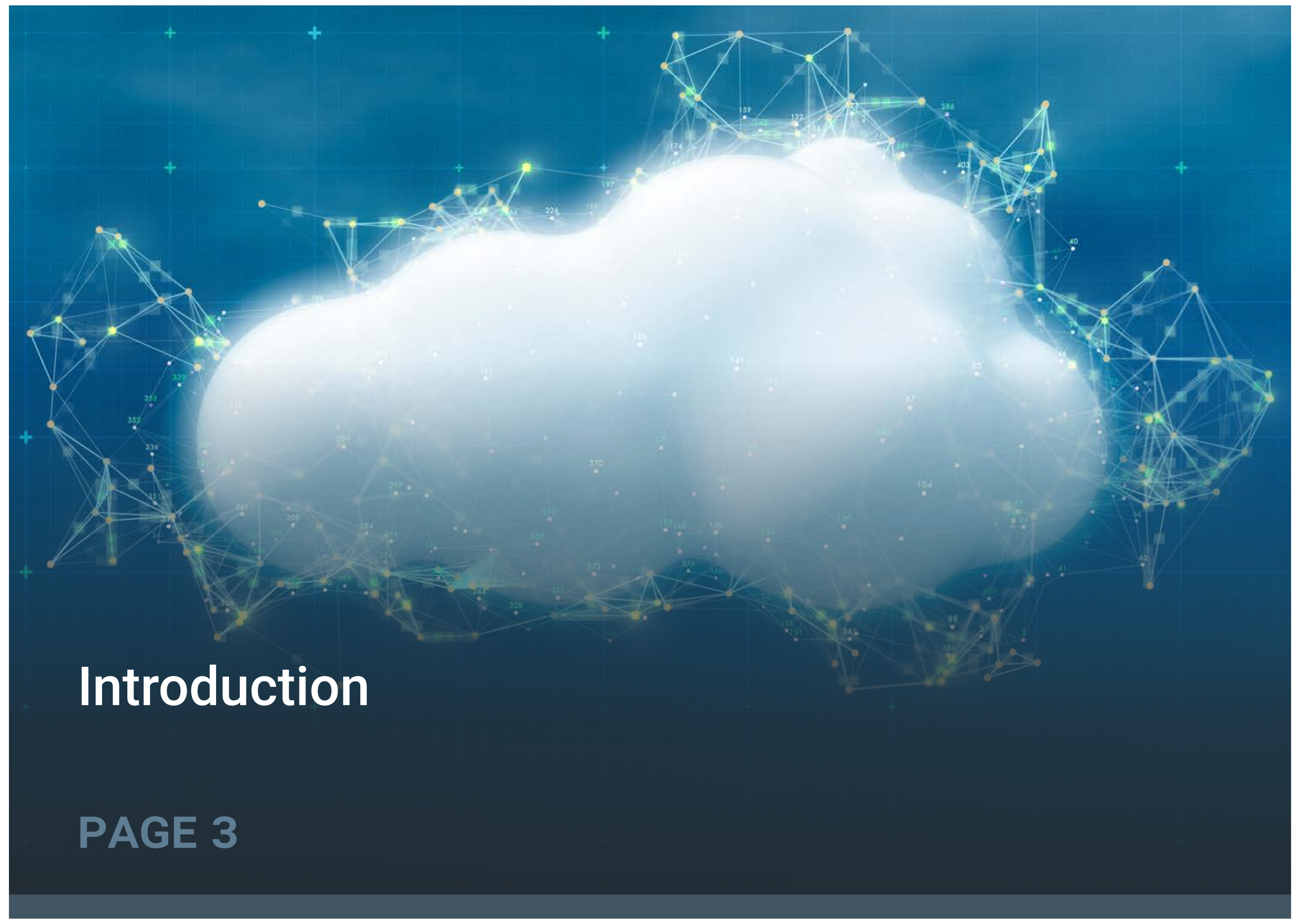
The State of Hybrid, Multi-cloud Management Maturity in Europe:

Where the Region Trails and Why It's So Important to Improve

infoblox.

This Enterprise Strategy Group eBook was commissioned by Infoblox and is distributed under license from TechTarget, Inc.

CONTENTS



> “There are **specific, actionable steps every organization can employ** to improve their hybrid, multi-cloud operations and associated business outcomes.”

Introduction

Objectives

Recently completed primary market research executed by TechTarget's Enterprise Strategy Group and Infoblox validated that there are specific, actionable steps every organization can employ to improve their hybrid, multi-cloud operations and associated business outcomes.

The goal of this eBook is to go a level deeper and inspect how responses from individuals and organizations based in Europe compared to their peers in the rest of the world. Additionally, we seek to understand if the benefits of becoming a hybrid, multi-cloud Leader are as pronounced in Europe when we compare those Leading organizations to their less-mature counterparts in the region.

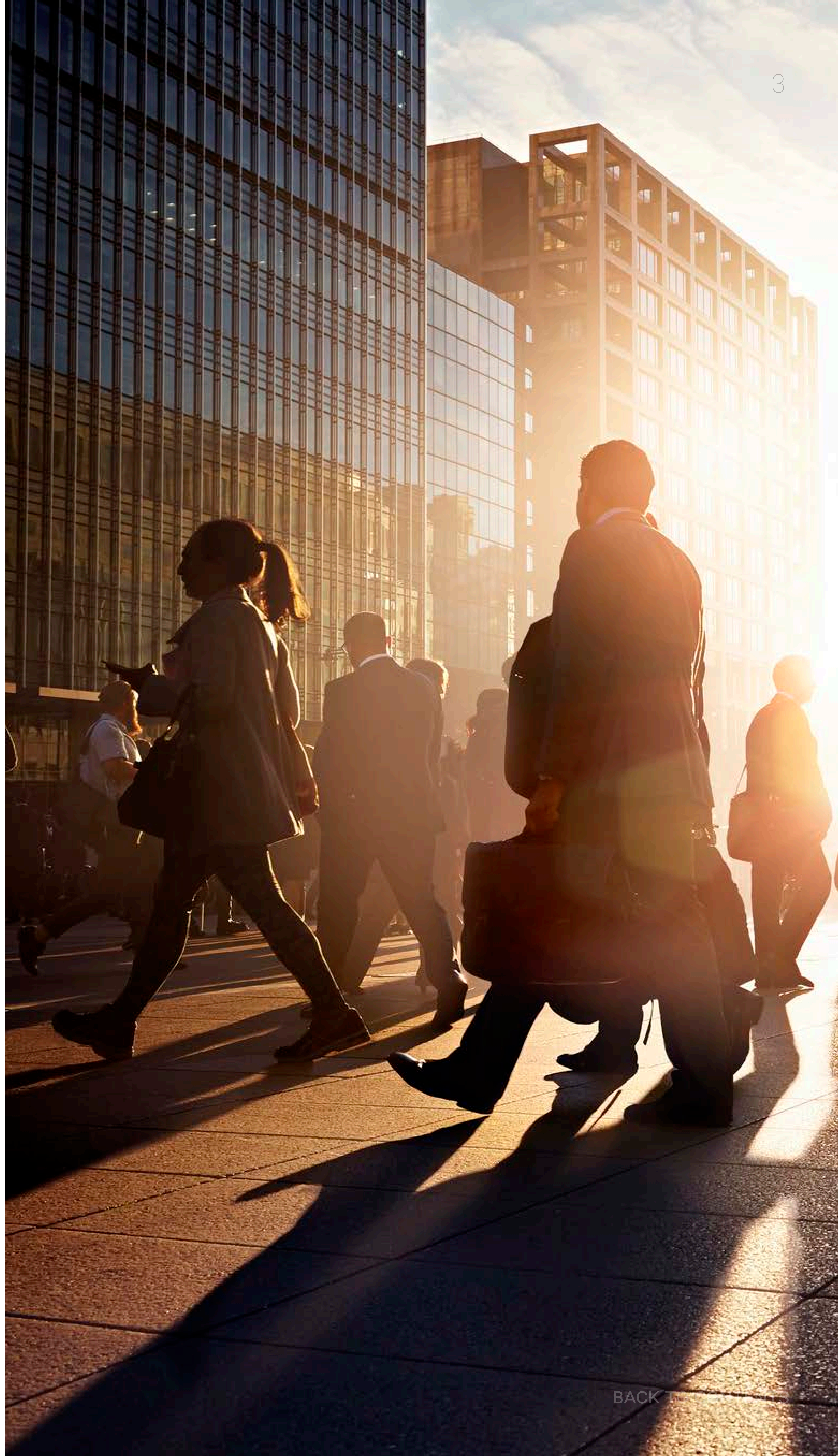
Highlighted Findings

Organizations with more mature hybrid, multi-cloud operations in Europe significantly outperform their peers:

Leaders are more efficient: They have reduced cloud costs by 50% more than Nascent organizations over the last year through better management.

Leaders get their products to market faster: 76% say they are typically first movers in their markets versus just 12% of Nascent organizations.

Leaders delight cloud users: They are 2.9x as likely to say they generally exceed their employee satisfaction goals related to cloud-hosted workloads (61% versus 21%) and were 2.3x as likely to say they generally exceed their customer satisfaction goals related to cloud-hosted workloads (58% versus 25%).



How European Organizations Differ From Their Peers on Hybrid, Multi-cloud Maturity

The Current State of Hybrid, Multi-cloud Management Maturity

To assess the state of the market, Enterprise Strategy Group created a survey focused on the people, processes, and technologies in place to enable organizations to manage their cloud environments. The answers to these questions enabled Enterprise Strategy Group to determine how well-aligned all participating organizations were to a range of best practices. The organizations that are most mature are designated as Leading, followed by *Converging, Emerging,* and *Nascent.*

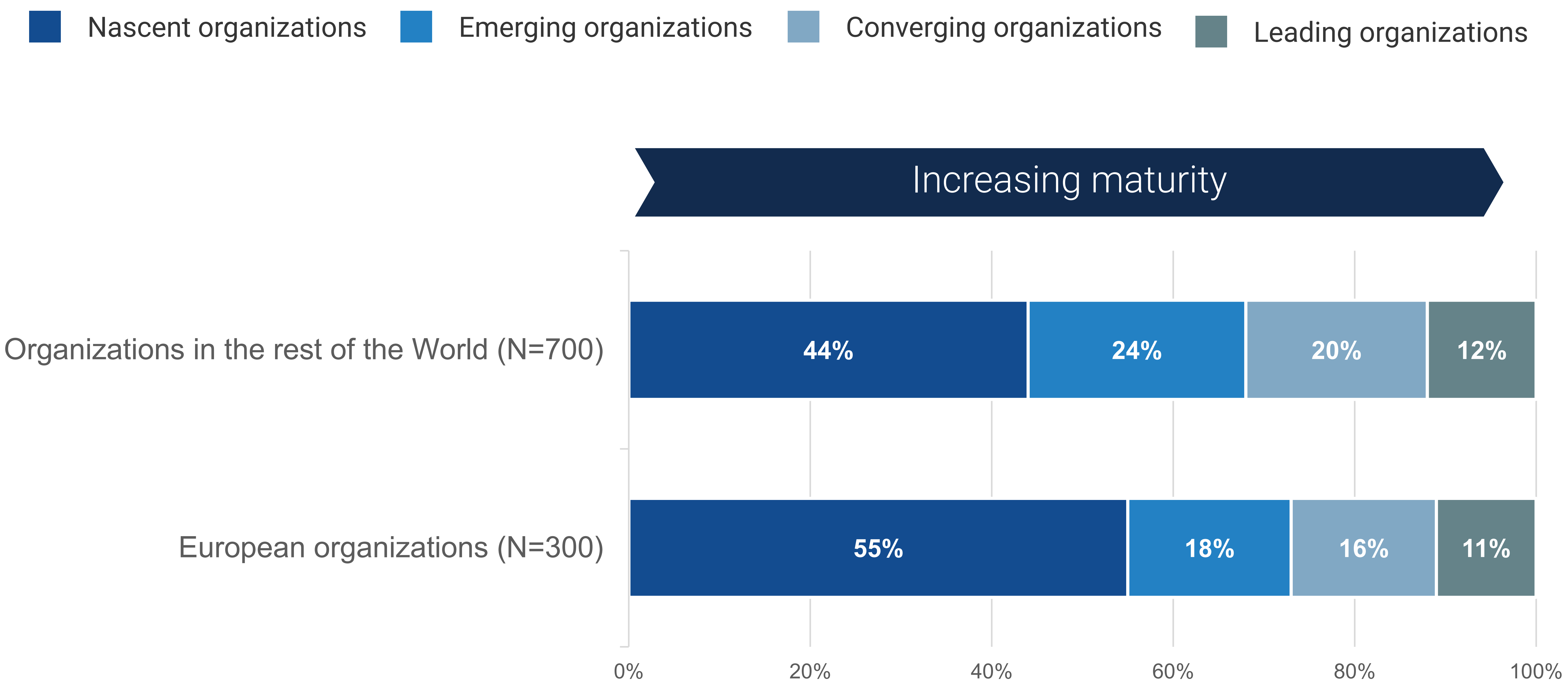
Enterprise Strategy Group's analysis employed a point-based scoring system in which organizations were evaluated as having (or not having) mature cloud management attributes and practices. They could then earn (or not earn) maturity points as a result. A maximum of 105 maturity points could be earned.

Attributes and practices assessed include:

- Has the organization established a cross-functional cloud platform team that combines network, security, and cloud operations practitioners?
- Is the organization leveraging enterprise-grade, cloud-neutral networking solutions?
- Does the organization take a defense-in-depth approach to security solutions, including using DNS for a broad range of security use cases?
- Is the organization intelligently automating a broad range of both NetOps and SecOps workflows in the cloud?

Comparing the maturity level of organizations in Europe to the rest of the world shows that, while there is a fair degree of consistency across the globe, organizations in Europe are significantly more likely to be in the least mature cohort (55% versus 44%), meaning organizations in Europe, on balance, have a lower degree of hybrid, multi-cloud maturity.

Organizations, by hybrid, multi-cloud management maturity.



What Distinguishes a Hybrid, Multi-cloud Leader From Its Peers?

Enterprise Strategy Group's hybrid, multi-cloud maturity model is multifaceted, spanning people, processes, and technologies. Below, key differences between Leading organizations and other maturity cohorts are summarized:

Establishment of a converged cloud platform team:
Converging network and security to be part of an organization's cloud operations center of excellence can yield significant benefits in terms of efficiency, agility, and security. By breaking down traditional silos between these two teams, the organization can foster better collaboration and alignment of goals, leading to streamlined processes and faster decision-making. In the context of the maturity model, questions to assess an organization's progress include specific steps taken to converge teams, like creating hybrid roles that span these disciplines or increasing the frequency of collaboration, the propensity of the organization to have deployed common tools used in both of these teams, and the establishment of a cross-functional cloud or platform engineering team focused on meeting the organization's requirements for scalability, reliability, security, and performance in cloud environments.

Use of enterprise-grade, cloud-neutral networking solutions:
These solutions, such as third-party-provided DNS, DHCP, and IPAM (DDI), provide robust management capabilities, enabling efficient provisioning, allocation, and tracking of network resources in dynamic cloud environments. By leveraging tools that are designed for multi-cloud operations, as opposed to cloud service provider (CSP)-provided tools that only work on a single provider's infrastructure, organizations can enhance cross-cloud consistency and attain greater agility, reliability, and performance. The centralized management and reporting capabilities provided by these solutions enable better visibility and control over network infrastructure, simplifying compliance efforts and reducing operational overhead.

Taking a defense-in-depth approach to cloud security solutions:
The maturity model advocates for an organization not to be solely reliant on the cloud security and monitoring tools provided by IaaS providers. This is because every organization has different specific security policies, regulatory obligations, and/or governance standards that may require additional security measures beyond what cloud providers offer. In particular, the use of DNS across a spectrum of security use cases—like enforcing acceptable use policies, detecting and blocking malware, and incident investigation or threat hunting—is an organizational attribute rewarded in the maturity model.

Automation of both NetOps and SecOps workflows in the cloud:
Automation increases operational efficiency by reducing manual effort and human error, enabling organizations to deploy, manage, and scale network infrastructure and security services more quickly and consistently. This agility enables faster response to changing business requirements and security threats and also improves productivity, both within technical teams and for stakeholders like developers.

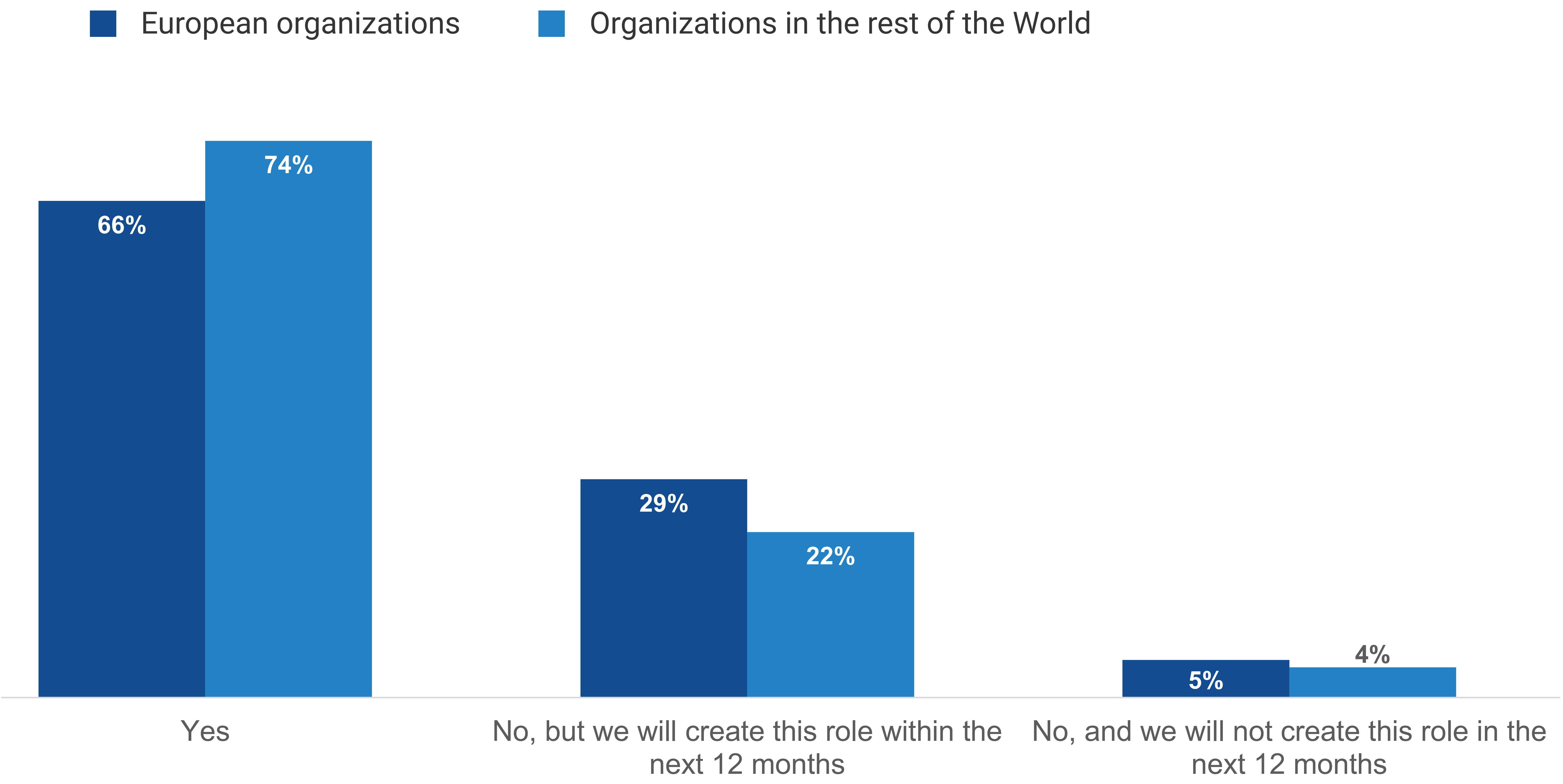
Taken together, these four organizational attributes determine where any given organization lands on the hybrid, multi-cloud maturity model. Organizations looking to increase their level of maturity should first and foremost seek to drive more alignment with these principles.

European Organizations Lag in a Pivoting to Platform Engineering

Organizations with platform engineering team topologies score higher in the maturity model as they tend to promote a more streamlined and scalable development environment. Platform engineering teams seek to ensure a higher degree of standardization and automation in cloud operations. They focus on implementing best practices for security, network configuration, compliance, and performance optimization uniformly across the organization, leading to more consistent and reliable cloud environments. This focus reduces the workload on product and development teams, enabling them to dedicate their efforts to delivering features and innovations.

European organizations were less likely than their peers across the rest of surveyed regions to report they currently employ platform engineers (66% versus 74%). On a positive note, these same organizations were more likely to report these roles will be created at their organization over the next 12 months (29% versus 22%), meaning the region as a whole is poised to catch up to the global benchmark.

Does your organization employ any full-time employees you would describe as being completely focused on platform engineering?



European Organizations Trail Their Peers in Terms of Security and Networking Tool Convergence

Convergence represents a critical area of focus in the maturity model. A centralized platform team is one aspect of this, but another is tool convergence.

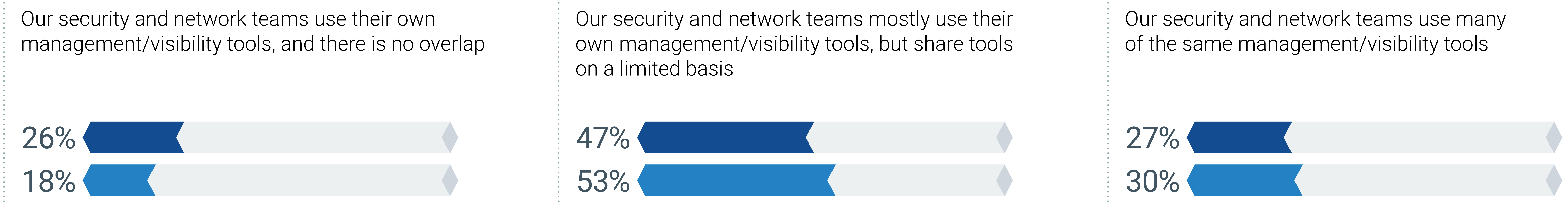
When network and security teams use a common set of tools, it simplifies communication and coordination, enabling these teams to work together more easily. This convergence also helps prevent security gaps that can arise from using disparate tools and processes. Additionally, the use of common tools also streamlines incident response and troubleshooting, as all teams have a consistent view of the organization's infrastructure.

Once again, European organizations tend to be taking a less-mature approach when it comes to networking and security tool convergence. Relative to their counterparts in other regions, they were 44% more likely to be taking a completely siloed approach (26% versus 18%).

Organizations in Europe would be well-served to consider if there are opportunities in their environment to drive more tool consistency across their cloud operations teams.

With which of the following statements do you most agree as it relates to the tools in use across your organization's network and security teams to manage cloud resources?

■ European organizations ■ Organizations in the rest of the World

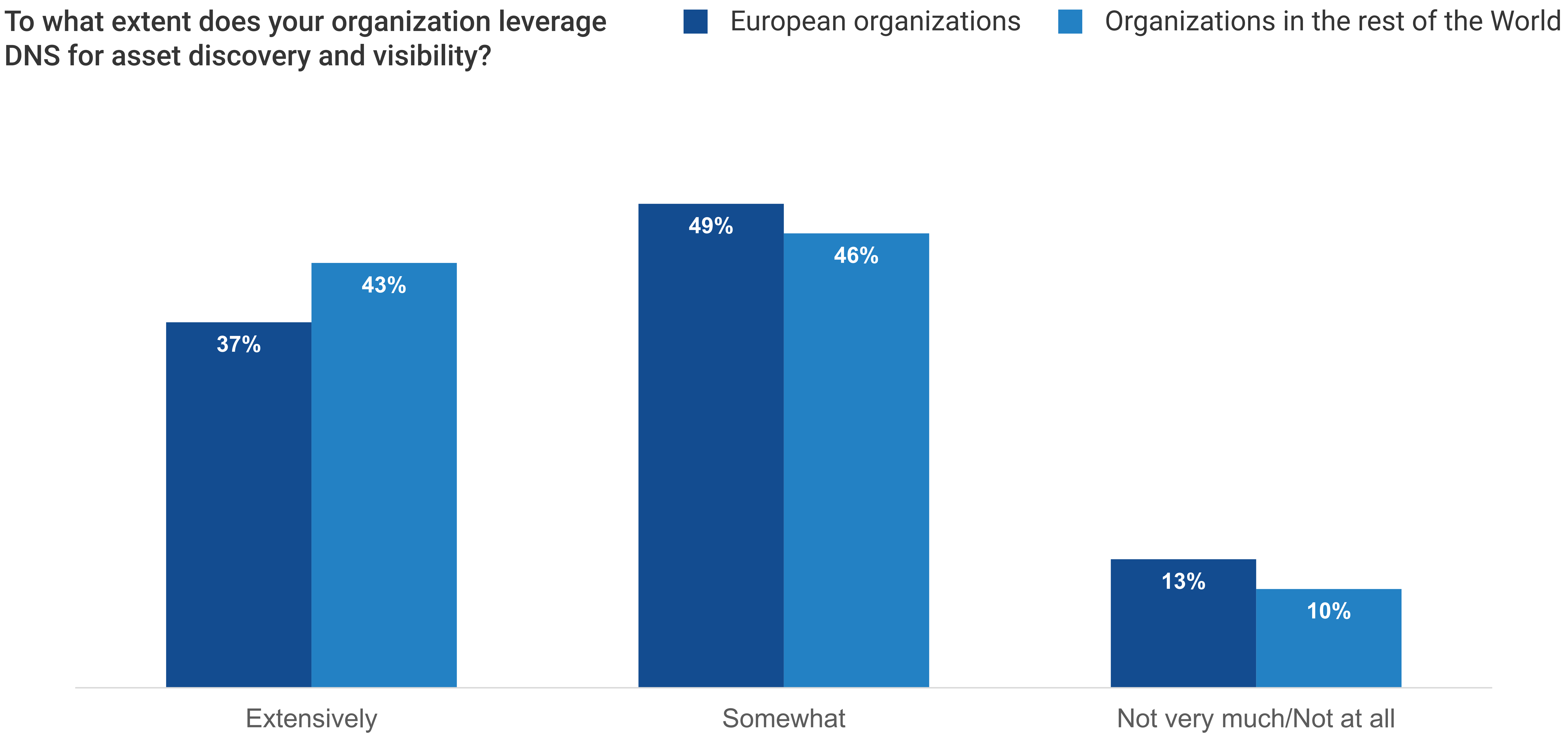


European Organizations Do Not Leverage DNS for Asset Discovery as Extensively as Their Peers

Integrating DNS as a primary security control is a logical cybersecurity strategy due to its potential to thwart a wide array of threats. By leveraging DNS for security use cases, organizations can effectively detect and block malicious activities at the network perimeter, including malware infections, data exfiltration attempts, and phishing attacks.

The data shows that European organizations less often use DNS extensively for cloud asset discovery and visibility. Leveraging DNS for infrastructure discovery enables security teams to automatically map out all active devices and services within the cloud environment. DNS-based discovery helps in identifying unauthorized or rogue devices that may pose security risks, enabling quicker isolation and mitigation. Similarly, it facilitates better monitoring of traffic patterns and user behavior, enabling the detection of suspicious activities such as lateral movement by attackers within the network. Organizations in Europe should consider if they are fully embracing DNS to optimize security operations.

> “DNS-based discovery helps in **identifying unauthorized or rogue devices that may pose security risks,** enabling quicker isolation and mitigation.”



To what extent does your organization leverage DNS for asset discovery and visibility?

BACK TO CONTENTS

Why European Organizations Should Focus on Increasing Their Hybrid, Multi-cloud Maturity

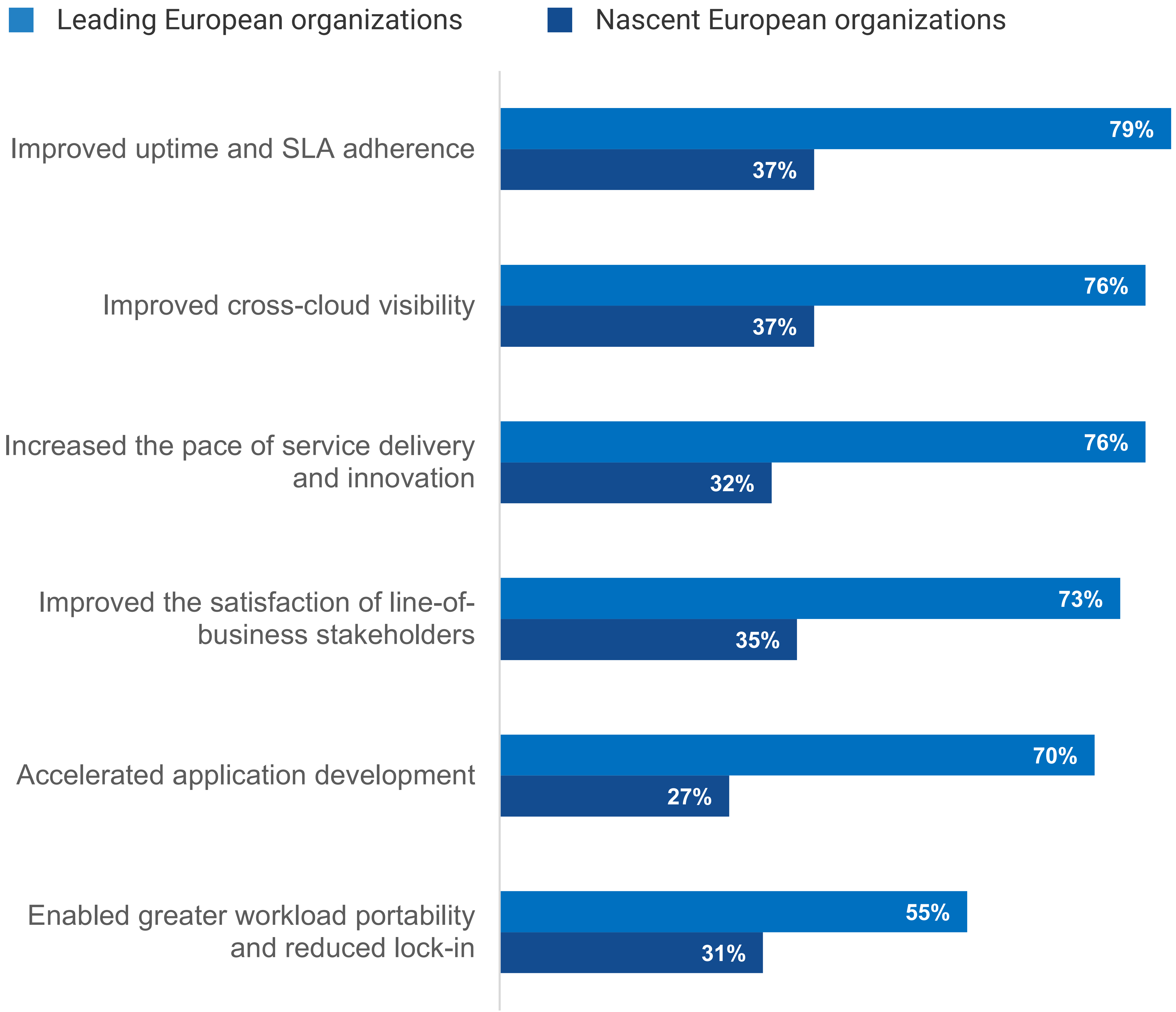
Leaders’ Technology Investments Have a Bigger Payoff

In the survey, respondents were asked if their organization’s approach to cloud networking and security technologies was materially improving ITOps and SecOps outcomes in the cloud.

Respondents could answer with a range of responses, from “yes, significantly” to “not at all.” When the maturity model is applied to the answers to this question, it quickly becomes clear that Leading organizations in Europe are getting much more benefit from their technology investments than their in-region peers. Specifically, they more often say their approach to cloud network and security technology is significantly:

- Improving uptime and SLA adherence (79% versus 37% of Nascent organizations).
- Improving cross-cloud visibility (76% versus 37%).
- Increasing the pace of service delivery and innovation (76% versus 32%).
- Improving the satisfaction of line-of-business stakeholders (73% versus 35%).
- Accelerating application development (70% versus 27%).
- Enabling greater workload portability and reducing lock-in (55% versus 31%).

The percentage of respondents reporting their Identity solutions are significantly driving each benefit.



A Deeper Inspection of Application Development Outcomes

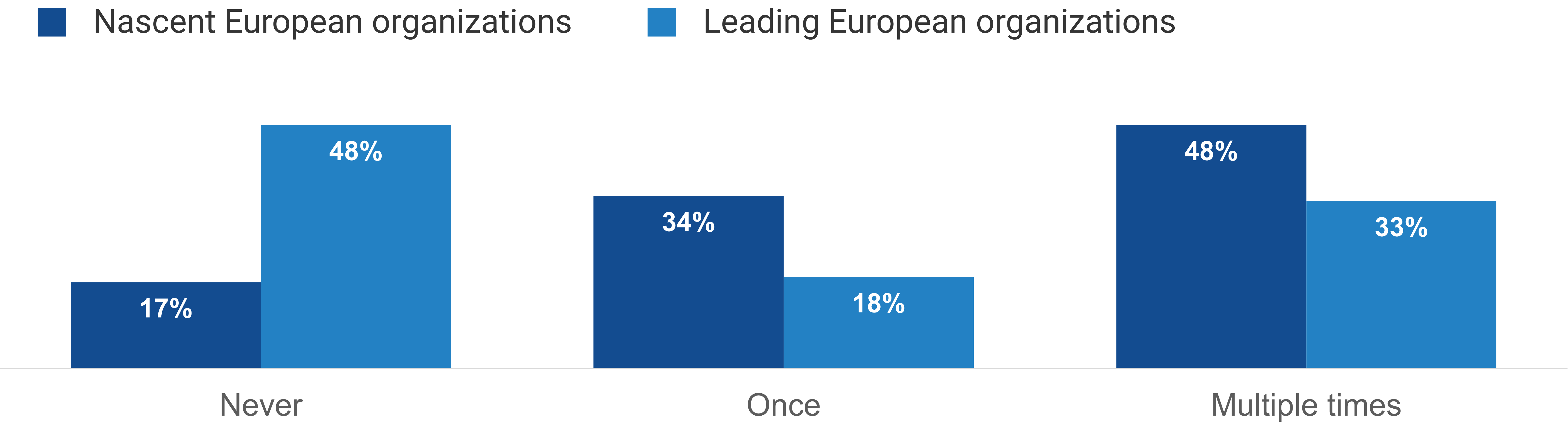
Not only did respondents at Leading organizations in Europe say their cloud networking and security solutions were helping improve application development outcomes, but their outcomes were also *objectively superior* to their less-mature counterparts in the region.

Respondents were asked how often in the past year an application development project had been delayed due to the IT or security team's need for more time to inspect cloud services that underpin the project. 48% of Leaders in Europe said they have never delayed or disrupted the development team's progress on new apps or features because the IT or security team needed more time to inspect cloud services in use. Only 17% of Nascent organizations could say the same.

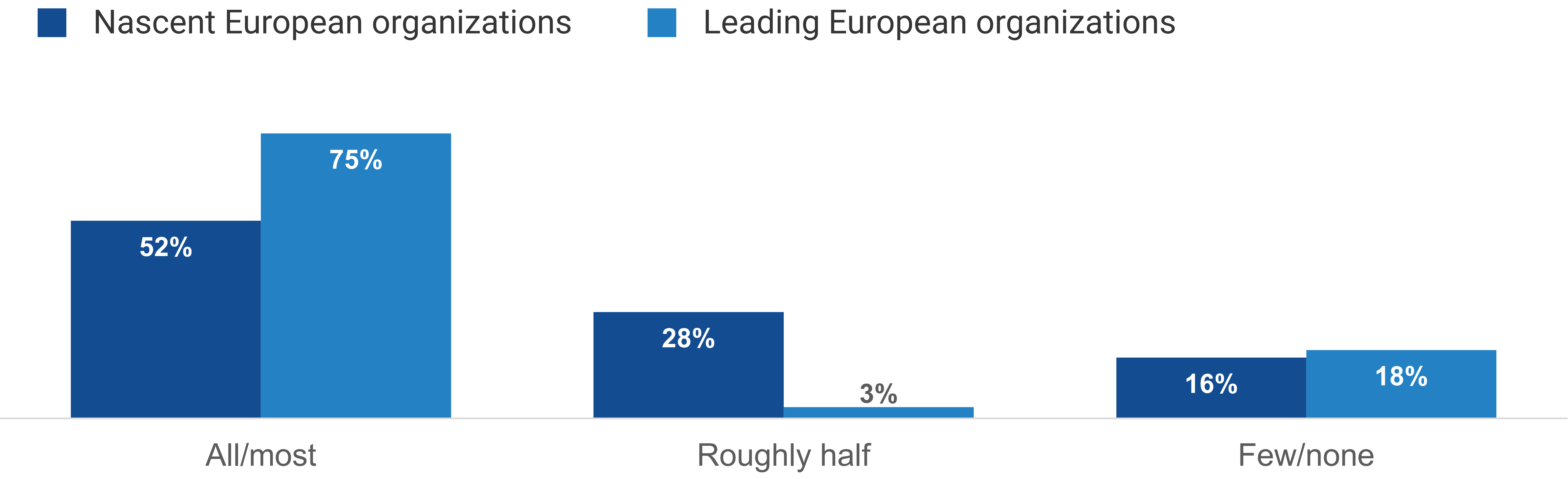
Respondents were also asked to consider all of their organization's internally developed applications and estimate the proportion for which code was able to be pushed to production "on demand." 75% of Leaders in Europe said that developers can push code to production for most or all of their applications (versus 52% of Nascent organizations).

Both proof points show just how much more prepared Leaders are to enable their development teams.

In the past 12 months, how often has an application development project been delayed due to the IT or security team's need for more time to inspect cloud services which underpin the project?



Considering all of your organization's internally developed applications, for what proportion is code able to be pushed to production "on demand"?



Leaders Have More Efficient and Resilient Cloud Environments.

Leaders also reported dramatically different results relating to the cost effectiveness, reliability, and security of their cloud environments:

Cost efficiencies

50%
larger reduction

All respondents were asked to estimate how much their cloud monitoring and visibility solutions were helping them reduce their cloud costs (relative to if those solutions were not in place), and Leaders reported a 50% larger reduction.

Improved resilience

3.3x as likely to say they can recover from outages in minutes versus hours or days

- All respondents were asked to estimate how many times in the past year cloud-hosted, business-critical workloads had gone down or seen severely degraded performance. 75% of Leaders said they had never (33%) or only once (42%) experienced a cloud-hosted, business-critical workload outage in the past 12 months (versus 44% of Nascent organizations).
- When workloads do go down, Leaders detect issues and recover from them faster: They were 4.1x as likely to detect outages in real time or near-real time (33% versus 8%) and were 3.3x as likely to say they can restore service in a matter of minutes versus hours or days (36% versus 11%).
- As it relates to security, looking back over the prior 12 months, 72% of Leaders said they had never (45%) or only once (27%) experienced a successful attack on cloud-hosted, business-critical workloads (versus 56% of Nascent organizations).

BACK TO CONTENTS

Leaders Get to Market Faster With Solutions That Delight Users

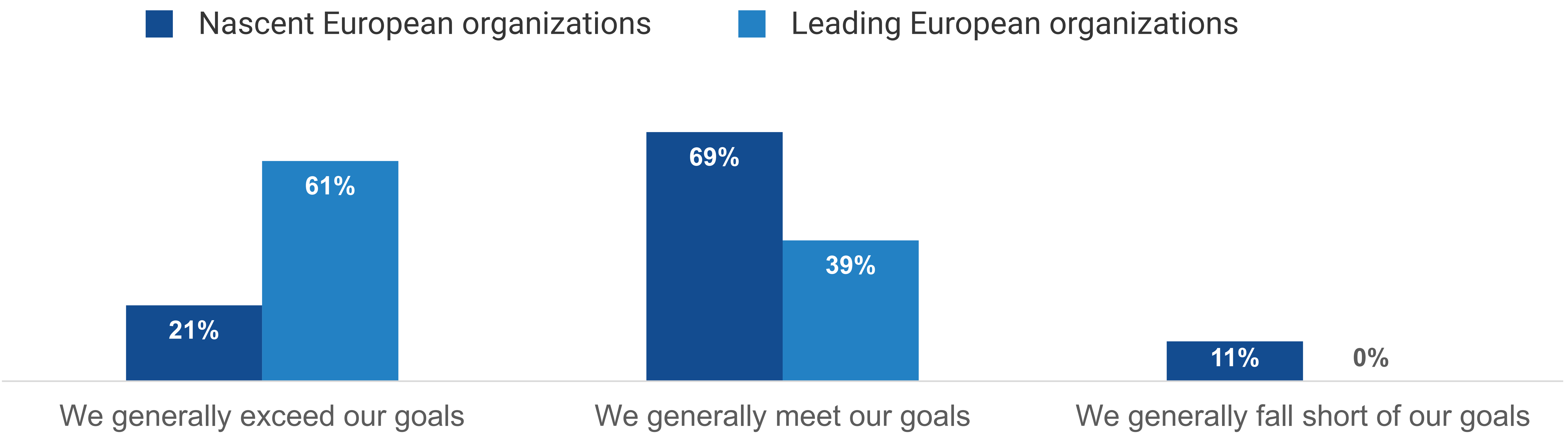
Finally, the research shows that Leaders' advantages in agility and resilience are helping them succeed as businesses in a quantifiable and material way.

All respondents were asked how their organization performs in terms of time to market. Leaders in Europe were much more likely than their less-mature peers to report success: 76% said they are typically first movers in their markets versus just 11% of Nascent organizations.

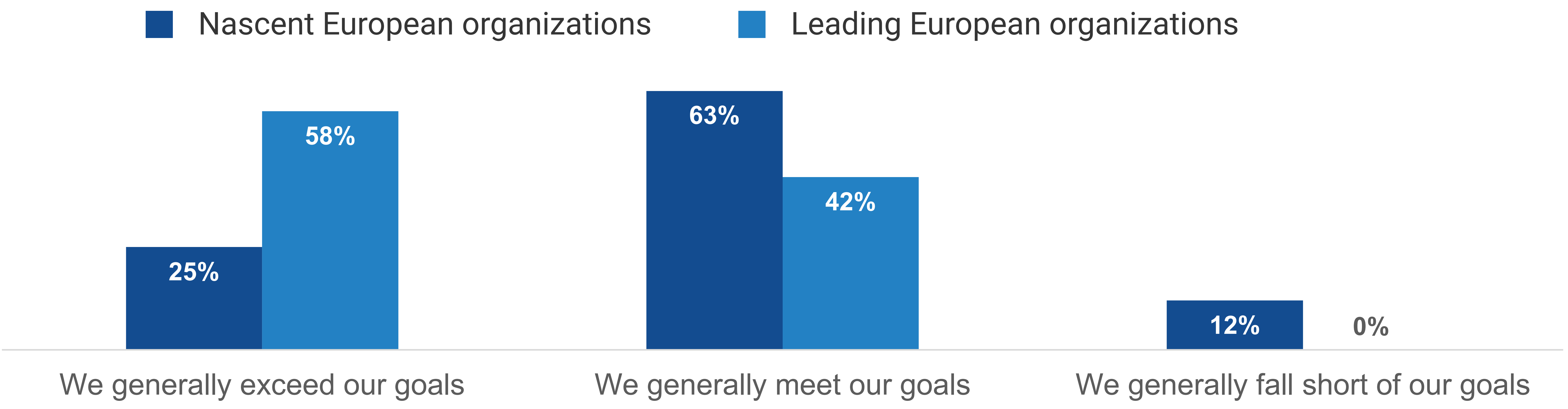
And the solutions brought to market are meeting users' expectations:

- Leaders were 2.9x as likely to say they generally exceed their employee satisfaction goals related to IT-managed, cloud-hosted workloads (61% versus 21%).
- Leaders were 2.3x as likely to say they generally exceed their customer satisfaction goals related to IT-managed, cloud-hosted workloads (58% versus 25%).

Generally speaking, how does your organization perform in terms of employee end-user satisfaction with IT-managed cloud workloads?



Generally speaking, how does your organization perform in terms of customer satisfaction with IT-managed cloud workloads?



Conclusion

Evaluating the data from European-based respondents provides two clear learnings. First, on balance, organizations in Europe have a moderate amount of catching up to do relative to their peers across the globe. While the gap is not insurmountable, it is consistent across areas like establishing platform teams, converging cloud networking and security tools, and using DNS to improve asset management and security. Second, the effort to close these gaps will pay off for organizations in the region. Leaders in the region consistently report dramatically better technical and business outcomes associated with their cloud environments. Cloud strategists in Europe would do well to prioritize investments and establish processes that are aligned to the hybrid, multi-cloud management maturity model discussed in this eBook.

How Infoblox Can Help

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, Infoblox provides real-time visibility and control over who and what connects to an organization’s network so that it runs faster and stops threats earlier.

LEARN MORE

infoblox®

RESEARCH METHODOLOGY AND RESPONDENT DEMOGRAPHICS

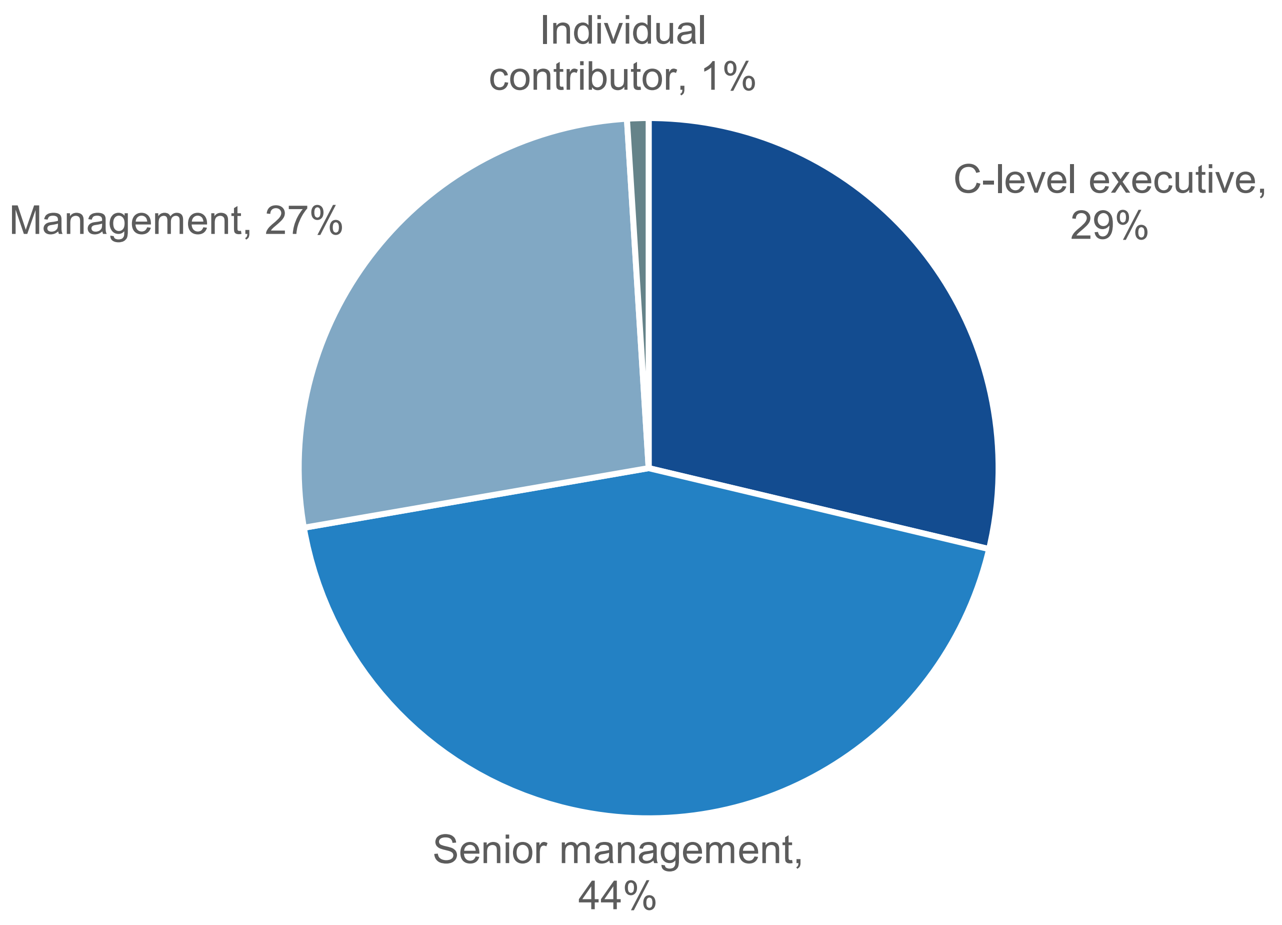
To gather data for this report, Infoblox commissioned Enterprise Strategy Group to conduct a comprehensive online survey of 1,000 networking and security decision-makers and influencers knowledgeable about their organization's public cloud environment.

Organizations represented span private- and public-sector organizations across the globe, including respondents based in North America (U.S. and Canada), Western Europe (France, Germany, Spain, and the U.K.), and the Asia-Pacific region (Australia, India, Japan, New Zealand, and Singapore). The survey was fielded between December 15, 2023 and January 17, 2024. The margin of error at the 95% confidence level for this sample size is + or - 3 percentage points.

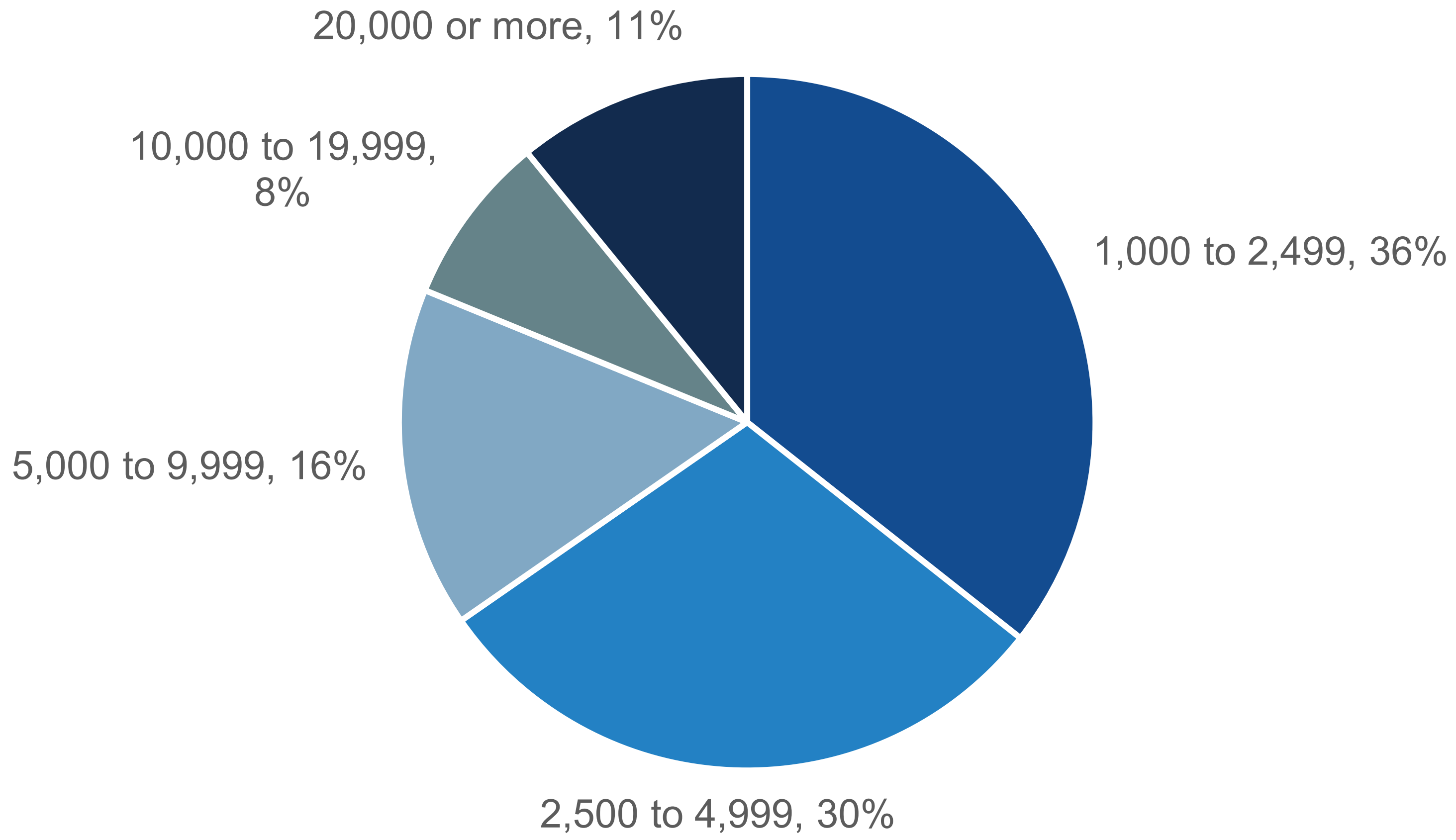
The demographics of the N=300 respondents based in Europe are displayed here.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

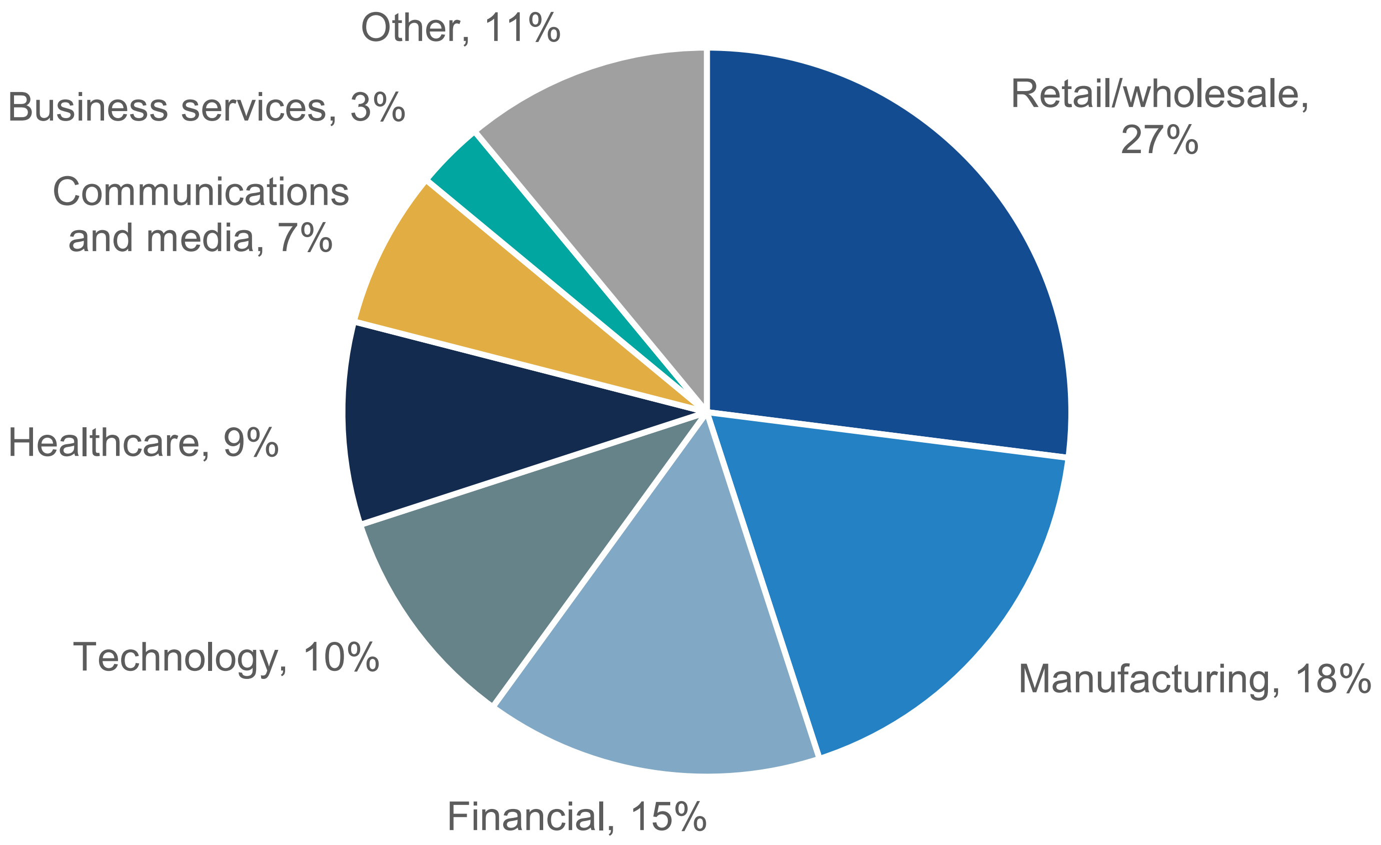
Which of the following best describes your current job title/level? (Percent of respondents, N=300)



How many total employees does your organization have worldwide? (Percent of respondents, N=300)



What is your organization's primary industry? (Percent of respondents, N=300)



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise
Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.