Futurum

NOKIA

The Data Center Networking Imperative:

Key Trends Driving the Next Era of Data Centers

SEPTEMBER 2025

The Data Center Networking Imperative: Key Trends Driving the Next Era of Data Centers

The decisions that shape a data center network's architecture, design, technology, security, and day-to-day operations carry more weight than ever. They influence not only how reliably the network performs under normal conditions, but also how it responds in moments of stress. The network is central to the availability, integrity, and performance of nearly every business service. Choices about topology, protocols, technology solutions, security models, and operational workflows set the parameters for how well an organization can adapt to new demands, recover from disruptions, protect critical data, and deliver service expected by the business and its customers.

The environment for making these decisions has shifted. Networking technologies have matured in ways that make high availability, dynamic scaling, and integrated security both more achievable and more cost-effective. At the same time, operational expectations have changed. Business leaders now assume that the data center can support constant change, deliver predictable performance, and recover from failures without noticeable impact to customers or partners. These expectations place reliability at the forefront, not as a feature to be weighed against other factors, but as the foundation for all other objectives.

This is also a moment to revisit long-standing assumptions. Designs optimized for static workloads and human-paced change may no longer be fit for purpose. Security approaches that once seemed adequate may now leave gaps in an environment where attack surfaces are broader and more dynamic. Operational practices built for manual intervention can quickly become bottlenecks when uptime and responsiveness are measured in seconds, not minutes or hours.

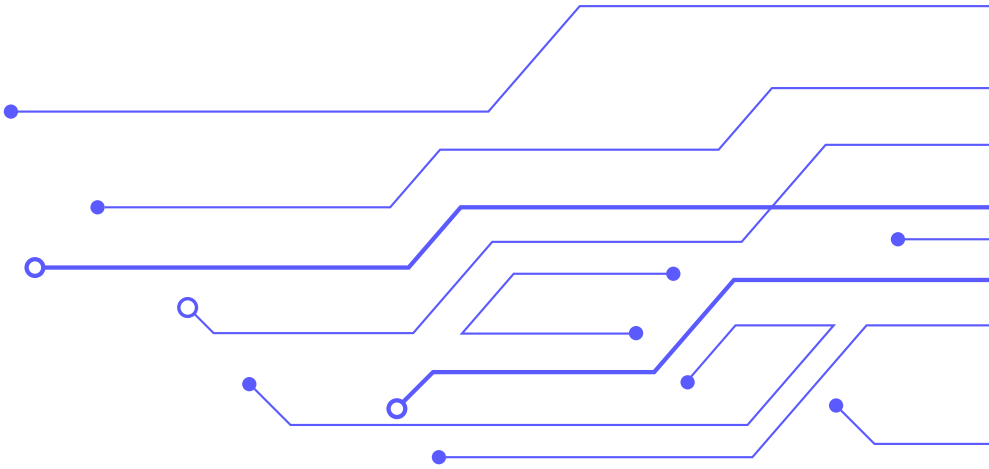
The findings that follow reflect how senior IT and infrastructure leaders are confronting these realities. They point to where organizations are investing, which operational models are proving most effective, and how emerging practices are reshaping what "reliable" means in a modern data center. Understanding these priorities and patterns will help guide the next set of decisions that define your own network's resilience and relevance.

This Futurum Research report is based on a survey of 100 IT infrastructure leaders. The research findings identified five key trends that are shaping data center strategies:

1. Reliability is the #1 decision criterion
2. Operational challenges, especially human error & skills gaps
3. Broad adoption of automation & AIOps, both planned and underway
4. Planned investments focus on network resilience
5. Hybrid & modernized infrastructure dominate

The purpose of this report is to help business and technology leaders understand the critical role of reliability in modern data center operations, providing insights into what their peers are prioritizing. The information here can guide you in making intelligent decisions about your own infrastructure modernization, automation investments, and operational strategies in a rapidly changing business and technology environment.

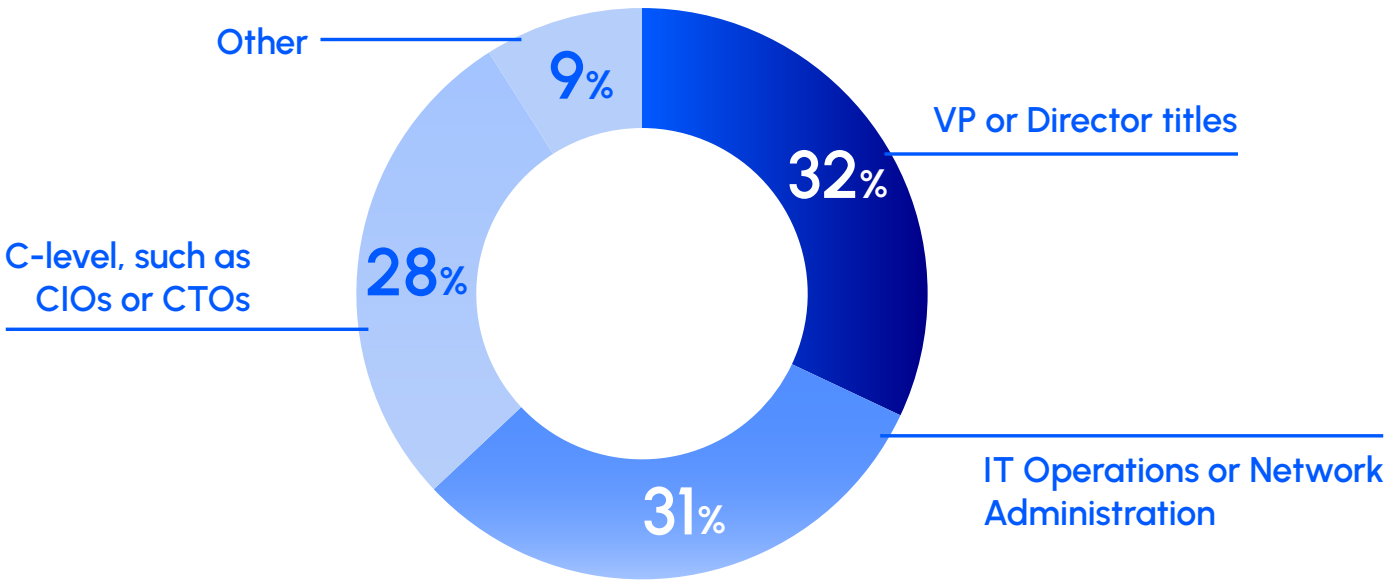
Nokia sponsored this research. All research, content, data, and conclusions are the independent work of Futurum Research.



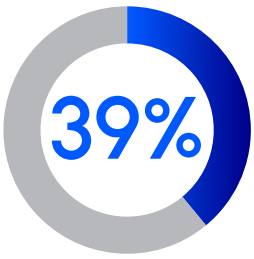
Survey Methodology and Respondent Profile

The Futurum Modern Data Center Survey gathered insights from IT infrastructure professionals, with all respondents having primary responsibility in either Information Technology or Infrastructure (97%) or Network Engineering and Operations (3%).

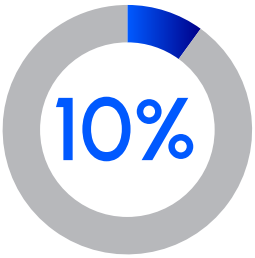
The participants roles are as shown in the figure below:



The organizations they represent are mostly large enterprises:

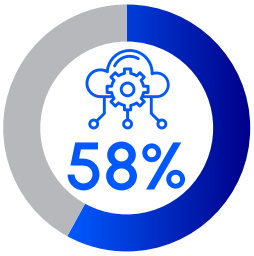


5,000 and 9,999 employees

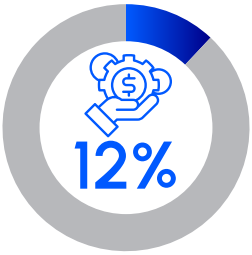


10,000 and 49,999 employees

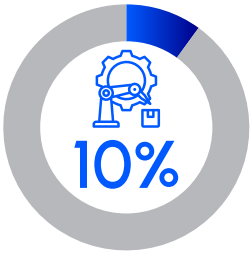
The primary industries represented are:



Technology and Cloud Services

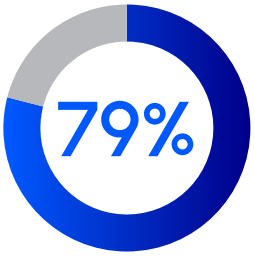


Financial Services

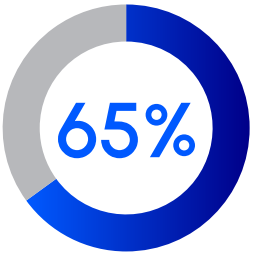


Manufacturing and Industrial

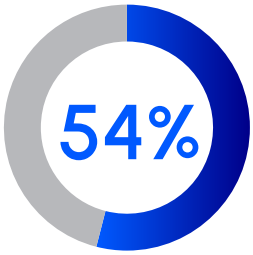
In terms of data center footprint, a significant majority of respondents operate on-premises data centers while also using third-party public cloud services. Over half of the participants are themselves service providers, with data centers generating revenue.



on-premise

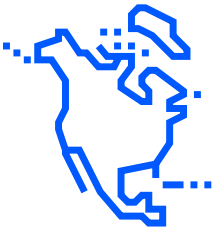


also using third-party public cloud

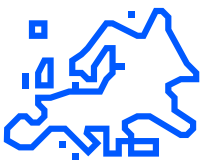


are service providers

Geographically, their primary data center infrastructure is located overwhelmingly in North America with some presence in Europe and APAC. This global spread highlights the complexity of managing these distributed environments.

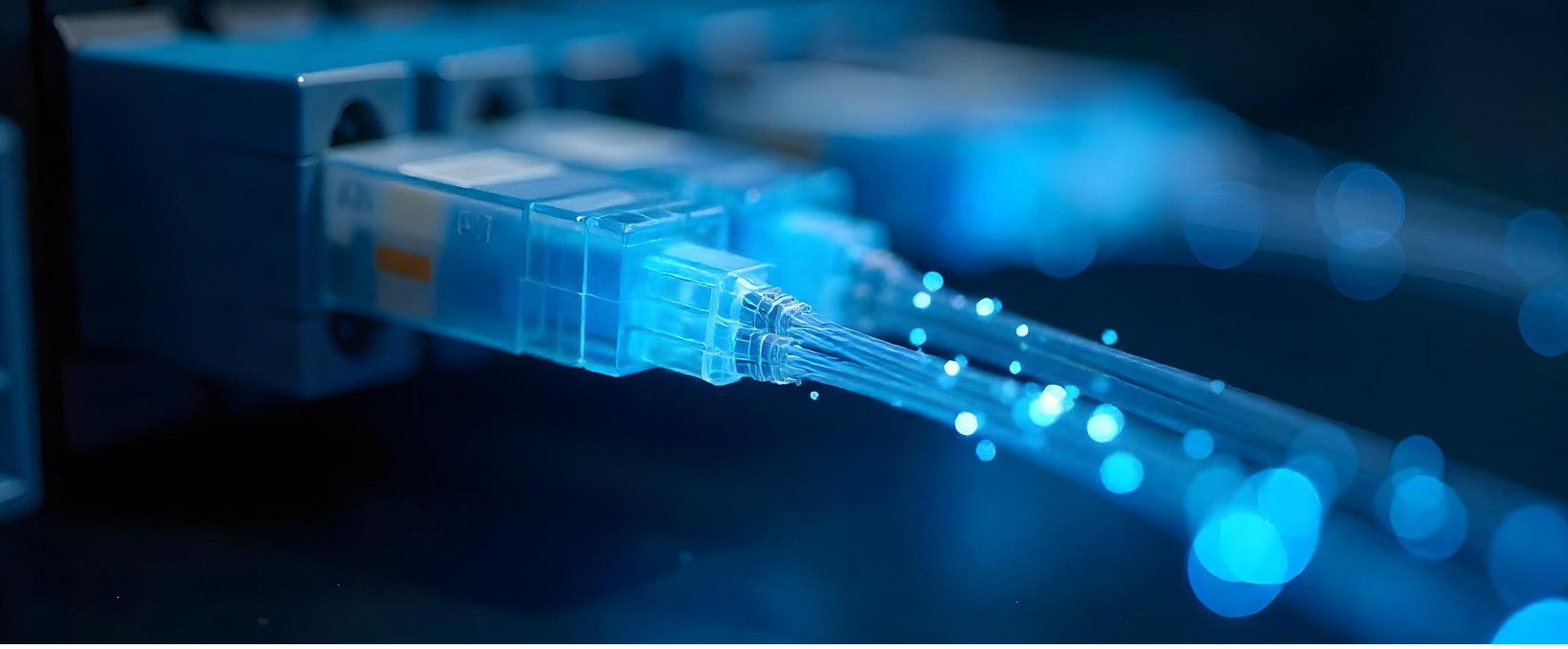


98% North America



25% Europe

10% APAC



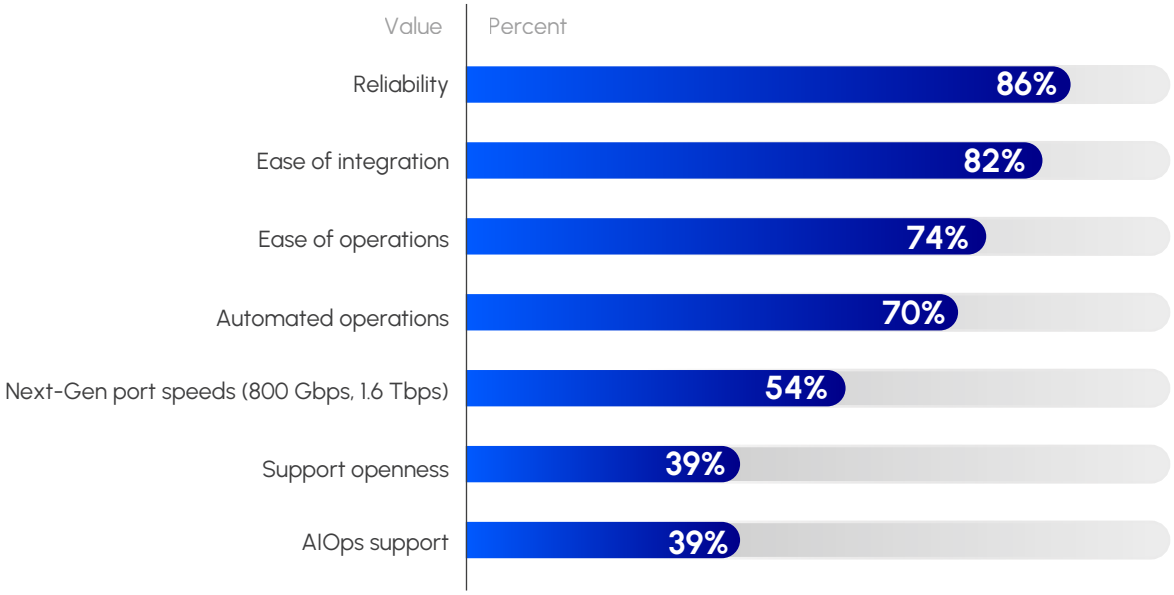
1. Network Reliability Is the Top Priority

Network reliability is the single most important factor for leaders building their next data center network. When asked to rate decision criteria (see Figure 1), 86% of respondents selected reliability, which outranked ease of integration (82%) and ease of operations (74%). This priority is driven by the severe consequences of downtime. A single hour of unplanned data center network downtime would cause critical internal disruptions for 80% of organizations.

Furthermore, 74% anticipate major service disruptions that could risk customer churn or a breach of SLAs. Over two-thirds (68%) expect significant direct revenue loss from such an event.

.

Figure 1. What are your decision criteria for building your next data center network?

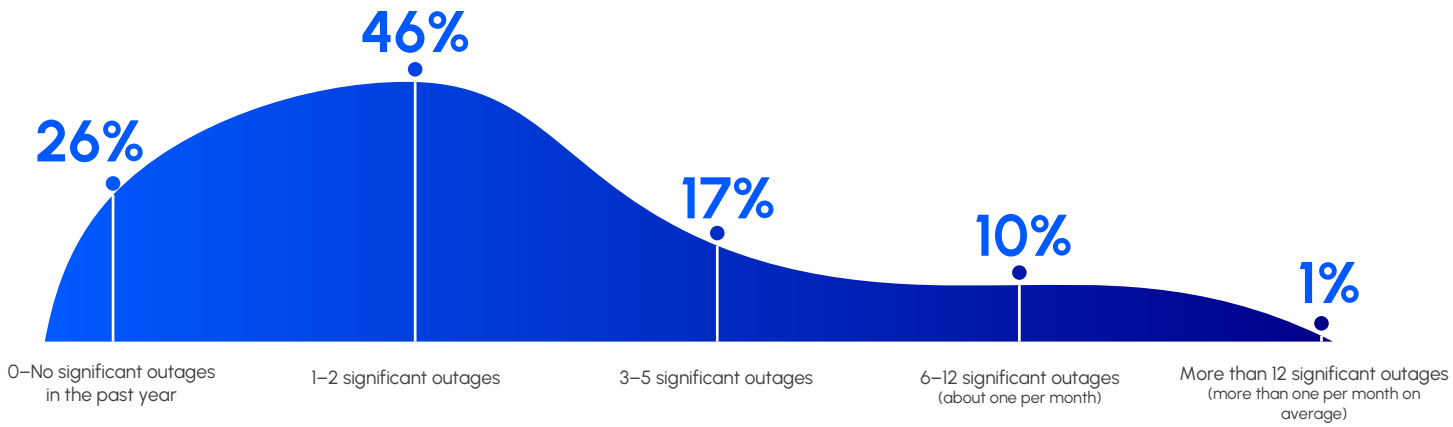


Outages Are a Common Experience

Unfortunately, downtime is a common experience for most organizations. The survey found that 74% of companies have experienced at least one significant data center outage in the past 12 months. Of these, 46% had one or two outages, 17% had between three and five, and 11% had six or more. Only 26% of respondents reported no significant outages in the past year (see Figure 2).

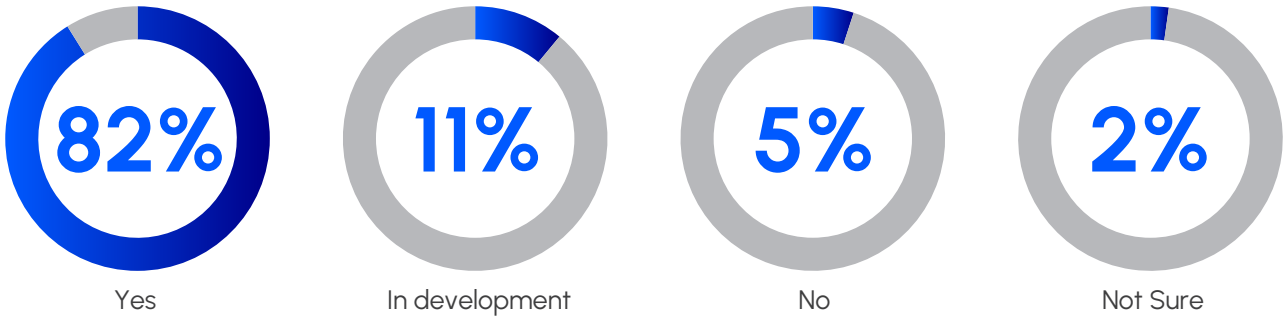
The causes of these disruptions are varied. Network device hardware failures and human error were each cited by 18% as a frequent top cause. Network device software bugs were an occasional culprit for 35% of respondents.

Figure 2. How many data center outages has your organization experienced in the past 12 months?



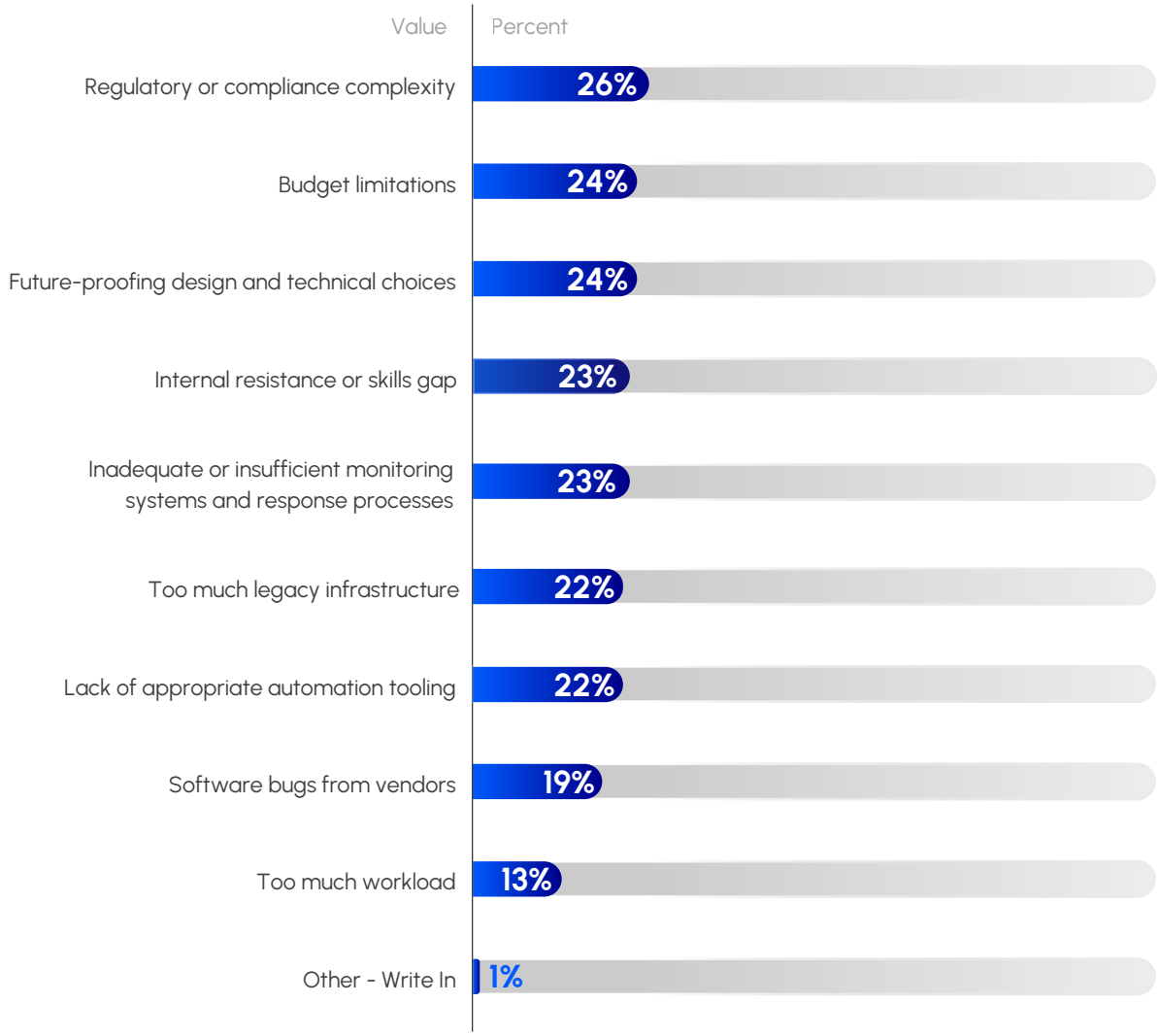
To address these challenges, 82% of organizations maintain formal KPIs or SLAs for network reliability (see Figure 3). The metrics used often reflect a balance between technical and business impacts. Roughly 29% focus on low-level networking metrics such as packet loss and latency, while 27% focus on business service availability and SLA compliance. Another 27% track overall network availability and incident recurrence rates.

Figure 3. Do you maintain formal KPIs / SLAs for network reliability?



Improving network reliability remains a pressing challenge for data center leaders, with obstacles spanning technical, organizational, and regulatory dimensions. When asked to identify the two biggest barriers, respondents pointed to a wide range of issues—highlighting not just infrastructure limitations but also strategic and operational hurdles. The results show a near-even distribution across several top concerns, from regulatory complexity and budget constraints to future-proofing design decisions and addressing internal skill gaps (see Figure 4). This dispersion underscores that reliability challenges are multifaceted, requiring coordinated solutions that balance compliance, investment, technology choices, and workforce readiness.

Figure 4. What do you see as the two biggest barriers to improving data center network reliability?



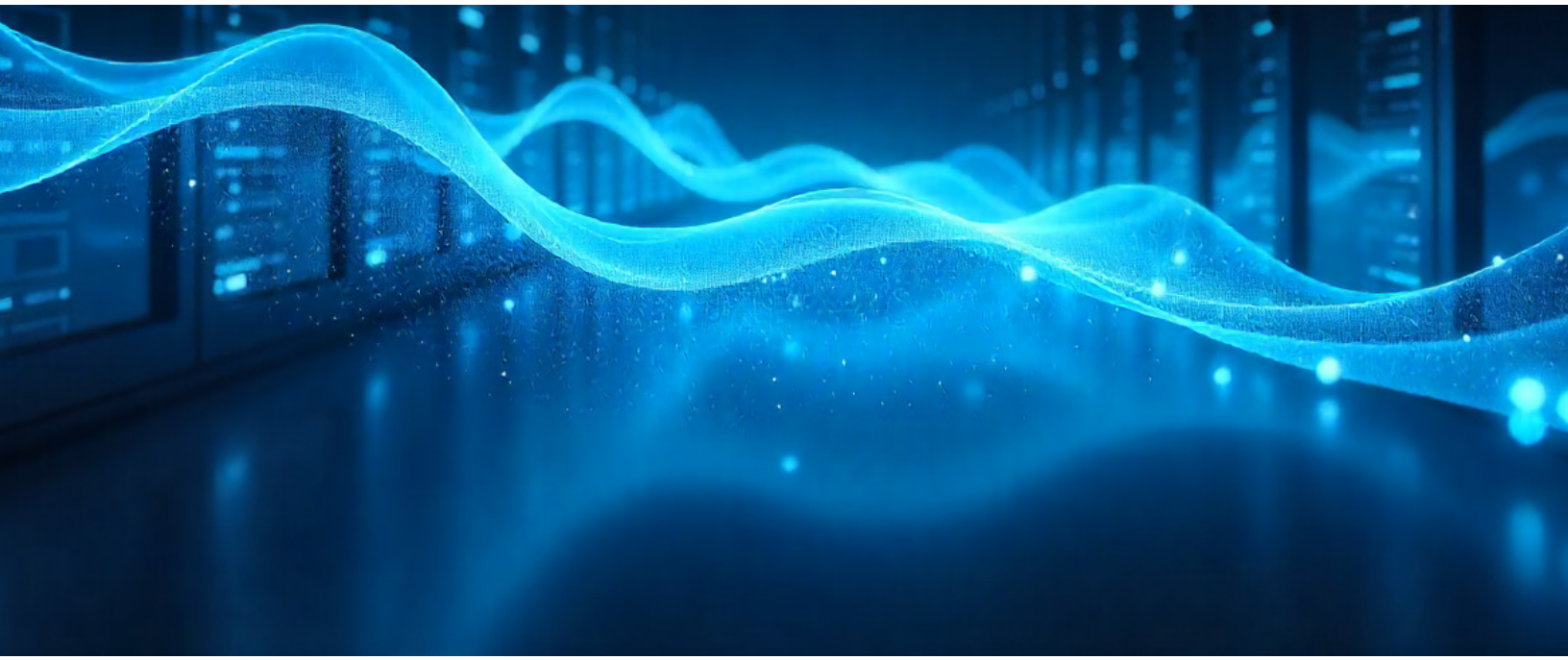
When grouped into broader themes, the survey findings reveal that product capabilities and deficiencies are the most pressing obstacles to improving data center network reliability, cited by a combined 41% of respondents through mentions of software bugs and inadequate automation tooling. Close behind are staffing-related challenges (36%), including skills gaps and excessive workloads that strain teams' ability to maintain reliable operations. Structural and process complexities—such as regulatory requirements, legacy infrastructure, and monitoring gaps—each affect roughly one in four IT leaders, while budget limitations (24%) remain a notable but comparatively secondary concern. This reframing highlights that reliability barriers are most often rooted in technology shortcomings and human resource pressures, with financial and systemic issues playing important but smaller roles.

Beyond outages caused by hardware failures or human error, software quality itself is a significant reliability risk. Nearly three-quarters (73%) of organizations report bugs requiring vendor patches, while more than half (54%) say they must take on additional QA practices themselves or rely on vendor test labs (See Figure 5). Silent failures—reported by 45%—are especially concerning, as they can evade detection until they trigger severe disruptions. These findings underscore why reliability is seen as the top decision criterion and why product quality remains a core concern.

Figure 5. How does poor software quality (poor design and test practices) impact your teams?

Given these high stakes, it's clear that network reliability is no longer just a technology or service level objective. It is a fundamental business necessity that directly impacts customer satisfaction, revenue, and brand reputation. To address the persistent problem of downtime, which plagues most organizations, leaders must look beyond traditional solutions.

The next section of this report will explore how the human factor, particularly operational challenges and skill gaps, continues to be a major hurdle to achieving true reliability, even in the most modern data centers.



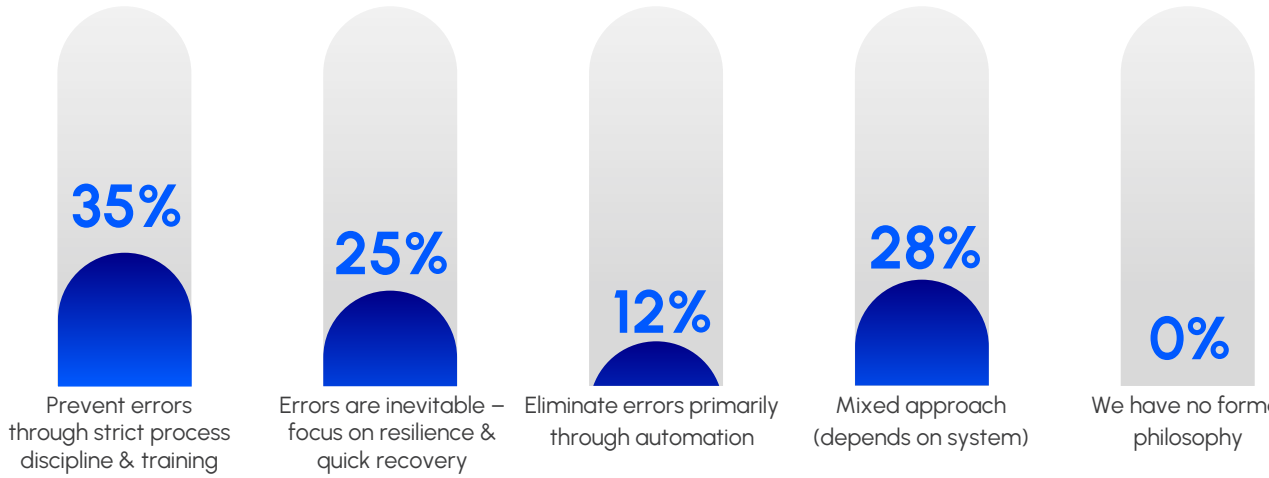
2. Operational Challenges: The Human Factor

Human error remains a persistent risk to uptime and a notable cause of incidents. Nearly every organization has experienced an outage or issue due to human error. While 41% said such errors rarely have a service impact due to mitigations, 17.5% admitted that human errors are a frequent top cause of disruption.

In total, more than 80% of respondents said human error at least occasionally impacts service continuity. When asked to estimate the percentage of reliability issues caused by human mistakes, 57% believe it accounts for no more than 25% of incidents. This suggests that while human error is a factor, it is often seen alongside other causes such as hardware or software failures.

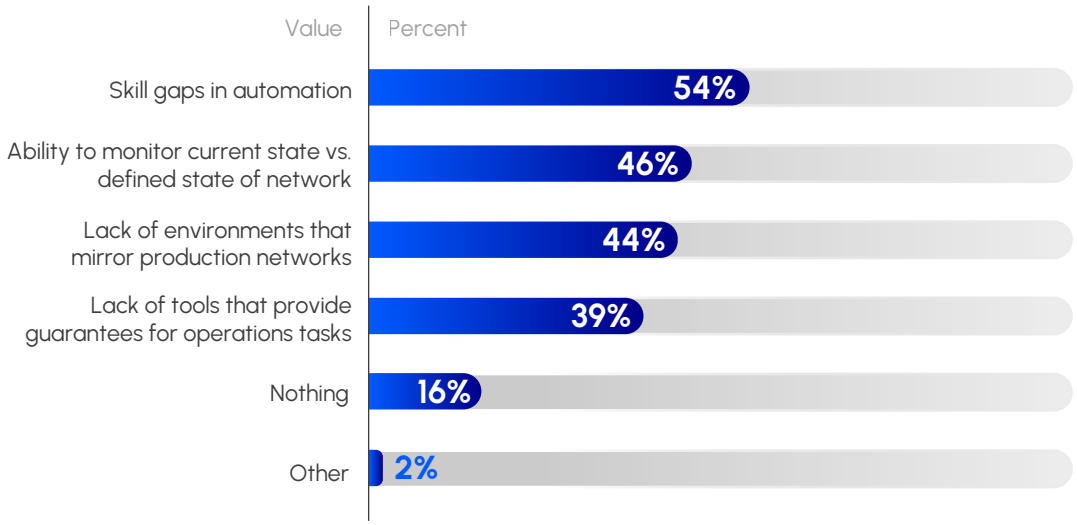
Organizations approach this human factor in different ways. The most common philosophy, held by 35% of respondents (see Figure 6), is to "prevent errors through strict process discipline and training." Another 28% take a mixed approach, and 25% accept that "errors are inevitable" and instead focus on resilience and quick recovery. Only 12% believe in eliminating errors primarily through automation. This suggests that many leaders still rely on people and processes to manage reliability, even as they invest in automation.

Figure 6. Which statement best matches your operational mindset toward the impact of human error on network reliability?



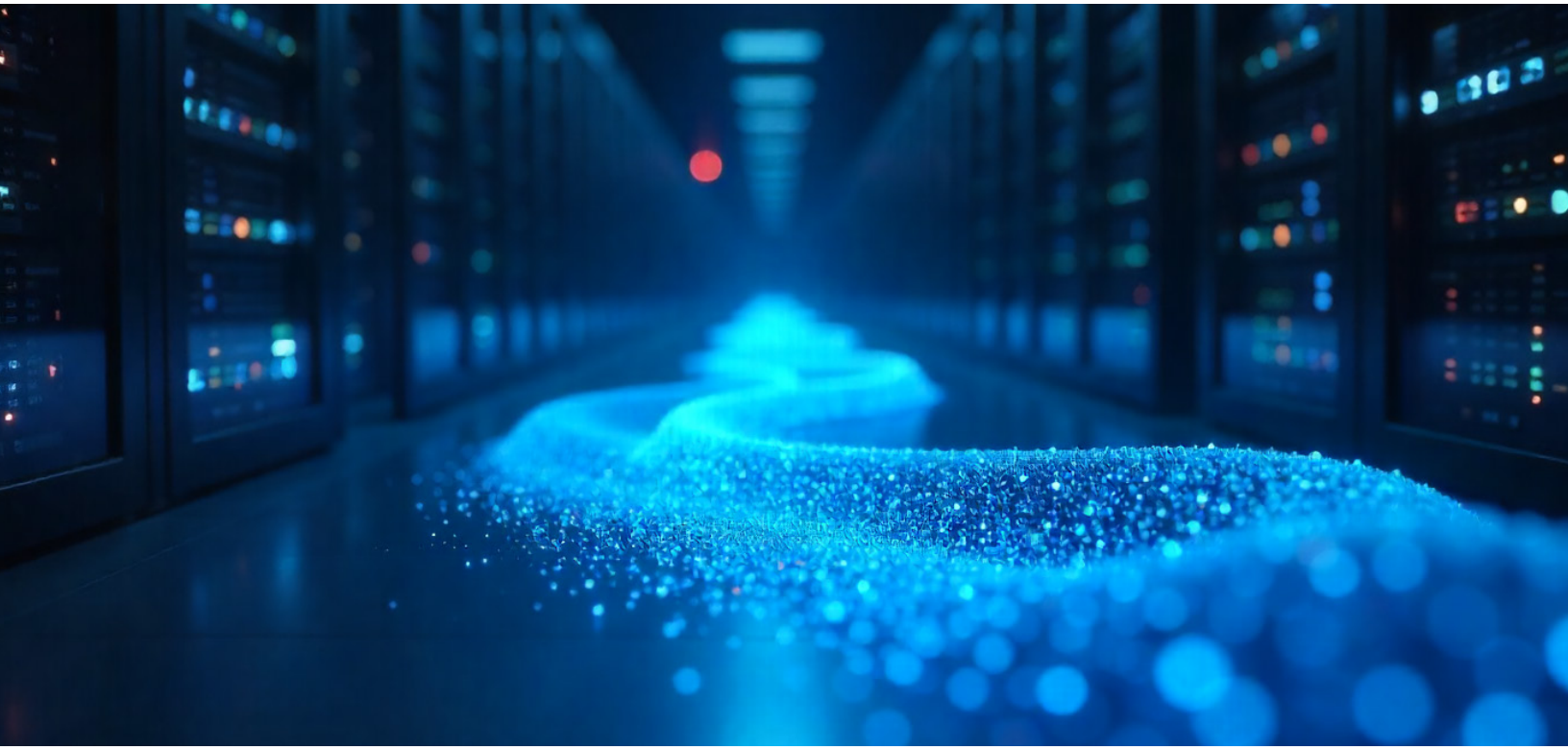
A lack of skills is a major barrier to adopting automation. The top impediment to achieving network automation goals, cited by 54% of respondents, is a skills gap in automation (see Figure 7). Furthermore, 46% reported an inability to monitor the network's current state versus its desired state as a barrier. Other significant challenges include a lack of test environments that mirror production (44%) and a lack of tools that provide guarantees for operations tasks (39%). The survey also identified broader barriers to reliability, such as budget limitations (24%), regulatory complexity (26%), and the presence of too much legacy infrastructure (22%).

Figure 7. What's holding back or impeding achieving your network automation goals, if at all?



Human error, skill gaps, and a reliance on manual processes are significant hurdles to data center reliability, so while a mix of process, training, and automation is the current approach for many organizations, it's not enough to keep pace with the increasing complexity of modern infrastructure.

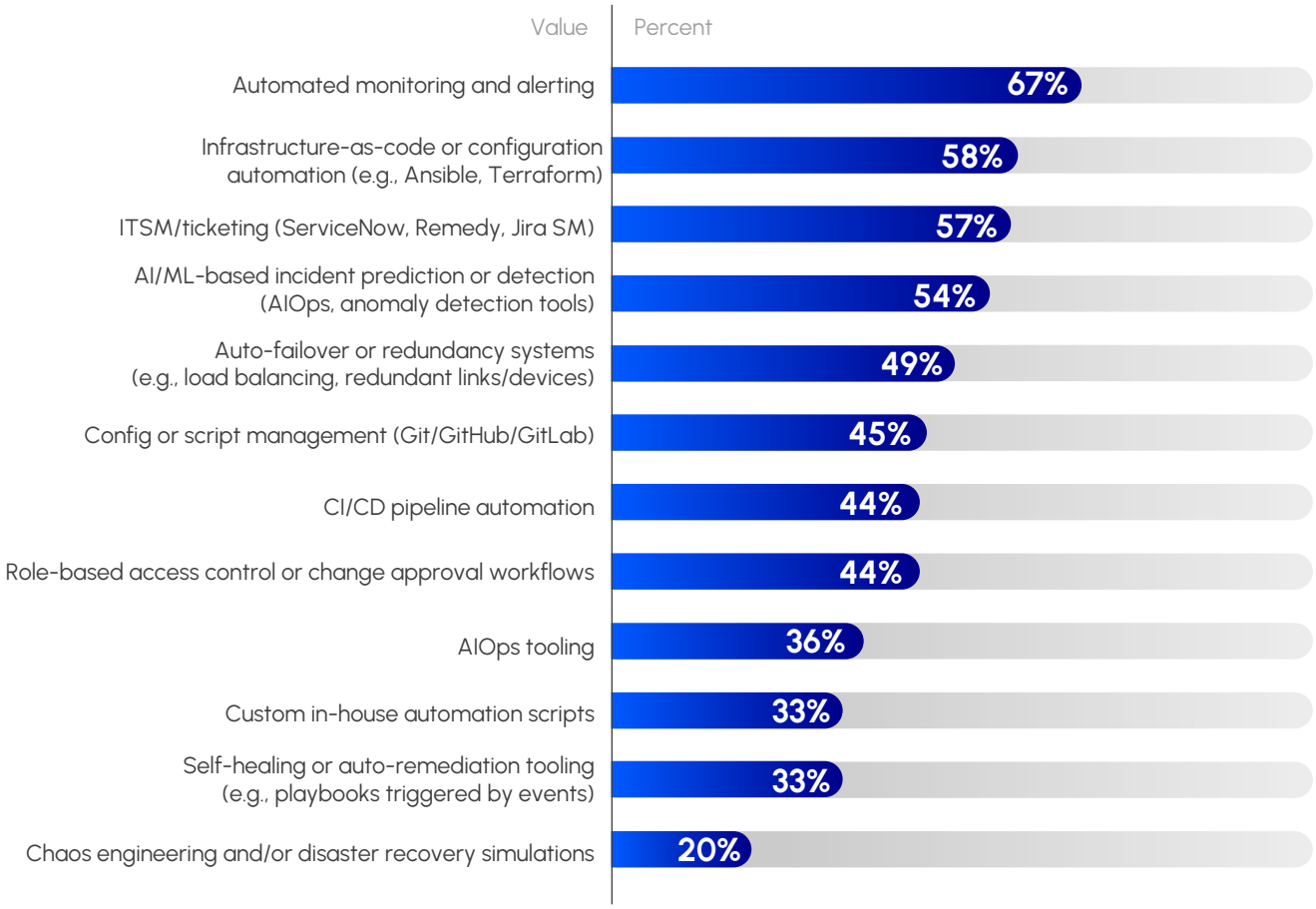
The next section of this report will delve into how organizations are beginning to use automation and AI to move beyond these limitations. By adopting technologies such as AI-driven automation, network digital twins, and pre-check validation, organizations can reduce human error, close skill gaps, and achieve the predictable, self-healing data center operations that are crucial for future success.



3. Rise of Automation and AIOps

Organizations are leaning heavily into automation, AI, and advanced tooling to achieve reliability. The survey shows broad adoption of modern NetOps practices. Two-thirds of organizations use automated monitoring and alerting. A majority also use infrastructure-as-code or configuration automation (58%) and ITSM or ticketing systems (57%). A significant number of organizations (54%) are already using AI or ML-based tools for incident prediction and anomaly detection, a core component of AIOps. In addition, 49% have auto-failover or redundancy systems in place (see Figure 8). use infrastructure-as-code or configuration automation (58%) and ITSM or ticketing systems (57%). A significant number of organizations (54%) are already using AI or ML-based tools for incident prediction and anomaly detection, a core component of AIOps. In addition, 49% have auto-failover or redundancy systems in place.

Figure 8. Which of the following technologies or practices does your organization use today?



More advanced practices are also gaining traction. Around 45% of respondents use Git for managing network configurations and scripts, and 44% have implemented CI/CD pipeline automation for infrastructure changes. The survey also found that 36% of organizations use dedicated AIOps tooling, and 33% use self-healing or auto-remediation tools. Even chaos engineering, which deliberately introduces failures, is practiced by 20% of respondents.

The perceived importance of advanced capabilities is high. The ability to pre-check and post-check configuration changes was rated as highly critical by 80% of respondents. Similarly, 78% rated an integrated network digital twin as very important for validating changes before they go to production. Capabilities such as closed-loop monitoring and AIOps mechanisms were also rated highly, with average scores of 4.0 out of 5.

Automation and AIOps are clearly moving past the early adoption phase and into the mainstream for data center operations. Organizations are no longer just thinking about these technologies; they're actively implementing a wide range of tools, from automated monitoring to CI/CD pipelines, to improve reliability. The focus now must shift from the novelty of AI to its practical application.

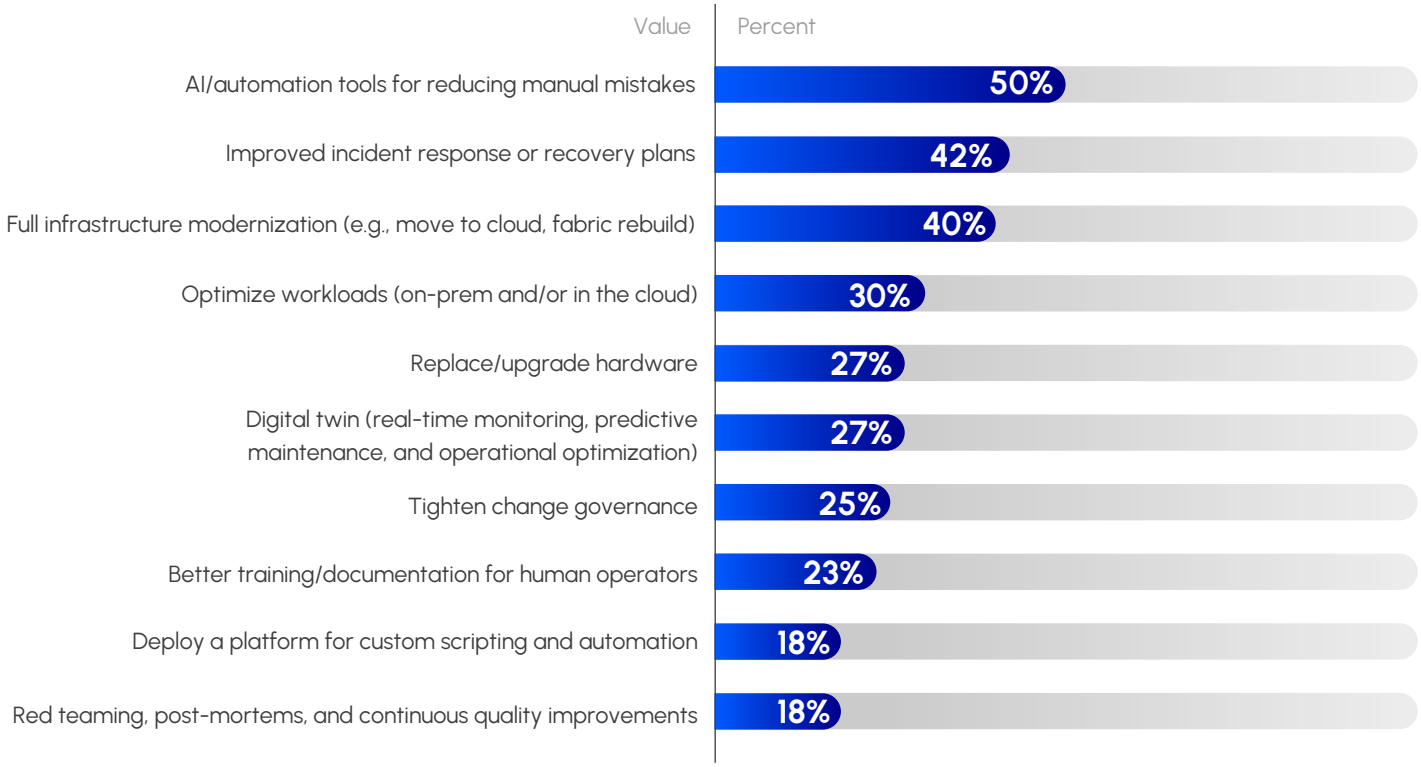
Leaders need to set a clear strategy for how these technologies will integrate into their existing infrastructure and a long-term plan for how AI can continuously improve operations.

This forward-looking approach will be vital for staying ahead, so the next section will explore the specific investment priorities organizations are setting for the coming year to continue this push for resilience and modernization.

4. Future Investment Priorities

Organizations are clearly prioritizing investments to improve reliability, with a heavy focus on automation and resilience. The top planned initiative, selected by half of all respondents, is investing in AI and automation tools to reduce manual mistakes (see Figure 9). The second-highest priority (42%) is improving incident response or recovery plans. This is followed by full infrastructure modernization (40%), which may include moving to the cloud or rebuilding network fabrics.

Figure 9. If you were to invest in three initiatives to improve your reliability posture next year, what would they be?



Other significant priorities include optimizing workload placement (30%) and upgrading or replacing hardware (27%). About a quarter of respondents plan to invest in deploying a digital twin for real-time monitoring and predictive maintenance (27%). Additionally, 23% plan to invest in better training and documentation for human operators, reinforcing the importance of human skills alongside technology.

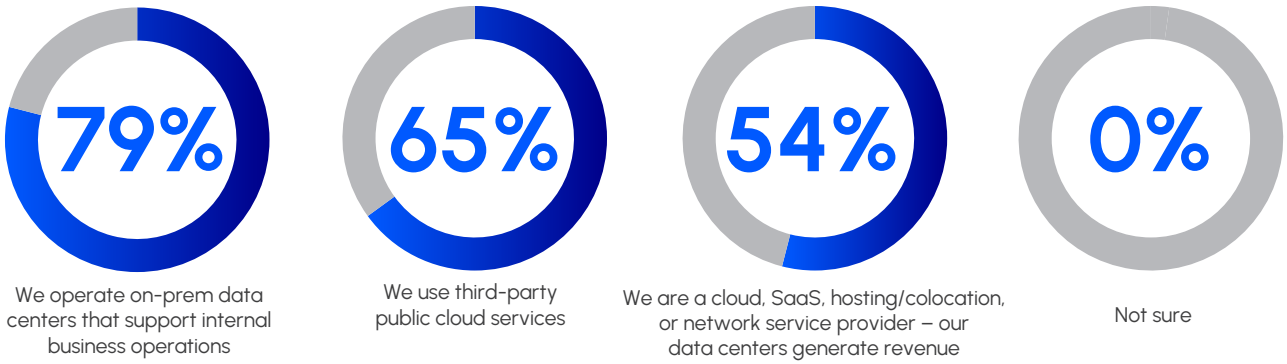
Based on the data, it's clear that investments in AI and automation are paramount for organizations seeking to improve their data center reliability. These initiatives, along with modernizing infrastructure and enhancing incident response, form a cohesive strategy for building resilient operations. However, these investments don't happen in a vacuum. The effectiveness of these new tools and practices depends on the underlying infrastructure.

The next section of the report will examine the shift toward hybrid and modernized footprints, exploring how the physical and virtual environments themselves are evolving to support these new reliability-focused initiatives.

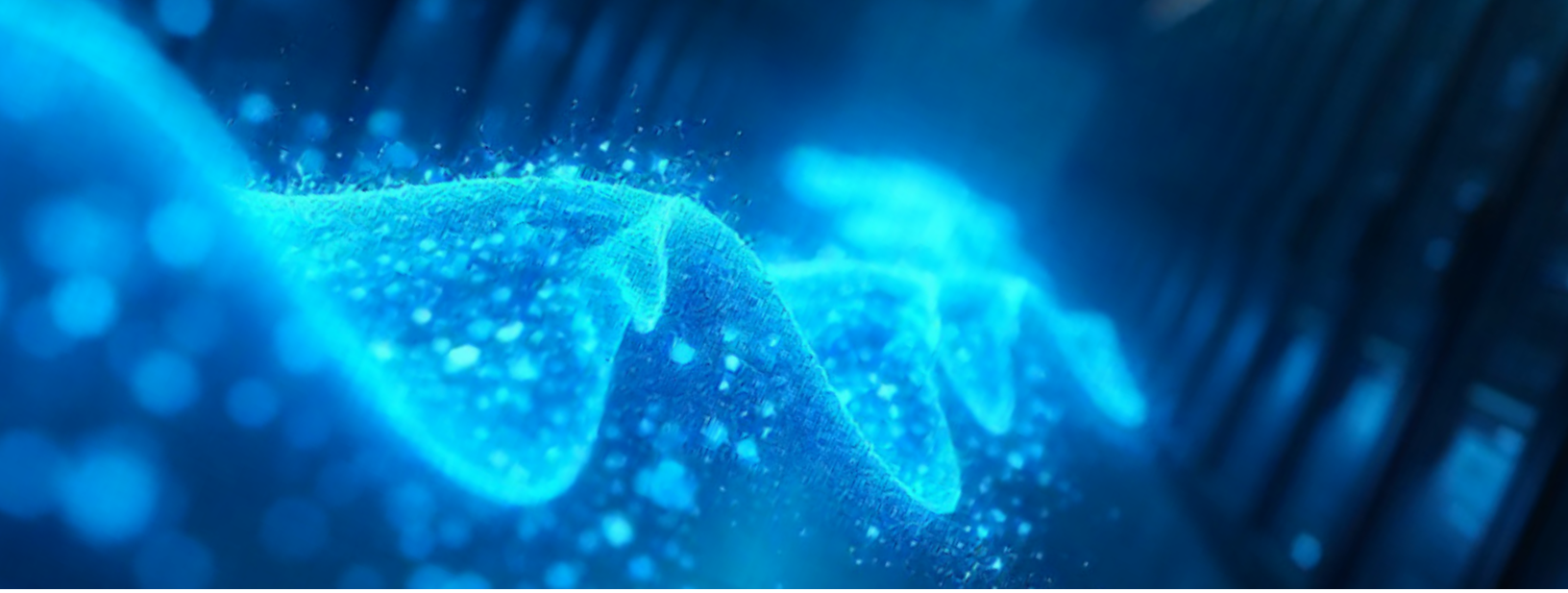
5. Hybrid and Modernized Footprint

The survey confirms that a hybrid and modernized infrastructure is the new norm for today's enterprises. Nearly 8 out of 10 organizations (79%) operate on-premises data centers, while 65% use public cloud services (see Figure 10). The organizations are actively modernizing these environments. When asked about their technology stack's maturity, 43% described it as "very modern" and an additional 21% as "cutting-edge," with high levels of automation and resiliency. Only a small minority (9%) admit to having a somewhat or very outdated infrastructure. This indicates a widespread industry trend toward cloud-integrated, up-to-date data centers.

Figure 10. Which statements describe your organization's data center networking infrastructure?



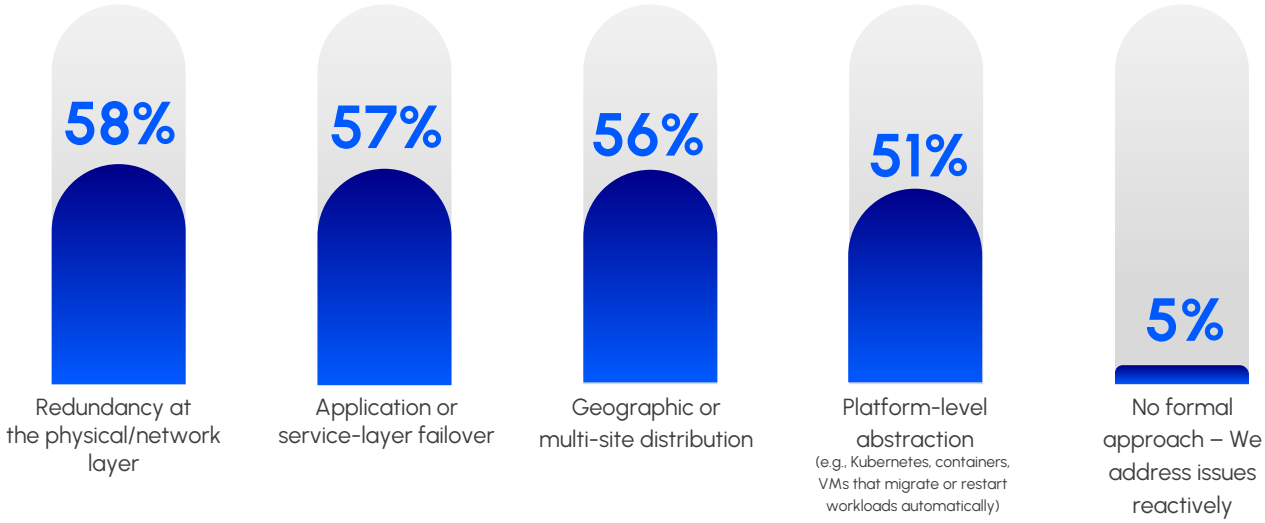
This distribution of infrastructure types and maturity levels has implications for IT leaders and vendors. Solutions must be able to operate seamlessly across on-premises and cloud environments. Given that most IT teams already see their stacks as modern, vendors should highlight how their solutions integrate with modern architectures and are ready for advanced technologies such as AI.



Notable Secondary Patterns

Beyond the core trends, the survey revealed other important patterns. For instance, organizations design for fault tolerance in multiple ways. The most common strategies are redundancy at the physical or network layer (58%) and application- or service-layer failover (57%) (see Figure 11). Geographic or multi-site distribution is used by 56%, and platform-level abstraction with technologies such as Kubernetes is used by 51%.

Figure 11. How does your organization design for fault tolerance?



When it comes to improving reliability, the skills organizations most want to develop are in automation frameworks (ranked #1), troubleshooting and diagnostics (ranked #2), and cloud and data center network architectures (ranked #3). This reinforces the idea that a combination of new skills and foundational knowledge is necessary for success.

Finally, while most organizations track reliability metrics, the emphasis varies between technical and business-focused measures. While a third focus on low-level network metrics, another third focuses on business service availability and SLA violations. The remaining third looks at network availability, customer impact, and operational metrics such as MTTR. This diversity shows that organizations are trying to link network performance directly to business outcomes.

Strategic Implications for IT Executives

The survey findings show a clear path forward for IT executives: champion investments that directly address reliability as a business imperative. Your company's ability to compete, innovate, and maintain customer trust is directly tied to the resilience of your data center network. This means not only funding technology upgrades but also focusing on the human and process-related aspects. You should prioritize investments in automation tools (top of the list for our respondents), upskilling your teams, and improving incident response plans. You must also continue to track reliability with metrics that resonate with the C-suite, such as revenue impact and SLA adherence, to show the value of your efforts.

Conclusion

The findings from the Futurum Modern Data Center Survey point to an industry-wide shift toward an autonomous, resilient data center. The dominant theme of "resilience through modernization and automation" reflects a strategic response to the growing complexity and demands for continuous availability. The modern data center is becoming an intelligent ecosystem that can largely manage itself, allowing teams to move beyond manual firefighting and focus on higher-level strategic work.

Organizations that successfully navigate this shift will gain a significant competitive advantage. They will be able to prevent outages, accelerate service delivery, and operate with greater agility and confidence. This requires a balanced approach: investing in cutting-edge automation tools while simultaneously strengthening human skills and processes. The imperative is clear: embrace the tools, practices, and mindsets that make your data center a rock-solid foundation for innovation and growth.

Appendix

Appendix

This appendix contains additional survey data that was considered when writing this report. The information here provides a more comprehensive view of the responses, covering a range of topics from team responsibilities and operational confidence to specific pain points.

Appendix Table 1. Team Responsibilities and Involvement

Summary: This table provides a more detailed view of the roles and responsibilities within IT. It shows a high degree of involvement in key areas such as architecture, design, and operations, with a significant percentage of respondents holding primary responsibility for these functions.

Survey Question: How would you describe your personal involvement in your organization's data center networking and infrastructure strategy?

	Architecture	Design	Implementation	Operations
I have primary responsibility for making decisions and setting strategy	60%	52%	61%	61%
I am highly involved in implementing or managing strategy	27%	34%	31%	27%
I provide input, but others lead the effort	8%	8%	7%	10%
I am not involved in data center decisions or operations	5%	5%	1%	2%

Appendix Table 2. Specializations in Data Center and Infrastructure

Summary: This table outlines the major areas of specialization among the survey respondents. It reveals that Cybersecurity, Cloud Architecture, and AI for Network Operations are the most common specializations, highlighting the growing importance of these fields in modern data center management.

Survey Question: What are your major areas of specialization in data center and infrastructure?

Specialization	Percentage of Respondents
Cybersecurity	56%
Cloud Architecture	48%
AI for Network Operations	41%
Operations (NOC, SOC)	37%
Network Architecture	35%
Network Operations	32%
Performance Measurement and Management	32%
Network Engineering	28%
Project or Program Management	23%
Disaster Recovery/Business Continuity/Backups	21%
Capacity Planning	20%
Network Automation and Orchestration	19%
Regulatory Compliance	16%
Maintenance	15%
Vendor Management	15%
Other IT Service Automation and Orchestration	10%

Appendix Table 3. Impact of Poor Operational Practices

Summary: This data shows the consequences of an inability to perform network operations reliably and predictably. A majority of teams find it challenging to meet evolving business needs, and many delay important tasks due to a lack of confidence in their tools and processes.

Survey Question: How does the inability to perform network operations reliably and predictably affect your operational practices? (Select all that apply)

Impact	Percentage of Respondents
Our operations teams are often challenged to meet the evolving business needs	64%
We limit the scope of our network operations and have to perform multiple planning cycles to complete the task	44%
We put off important operations tasks due to a lack of confidence that things will work as expected	40%
Deficiencies in our tool technologies require we put too many temporary fixes and manual work arounds in place	38%

Appendix Table 4. Overall Maturity of Data Center Technology Stack

Summary: This table provides a breakdown of how organizations self-assess the maturity of their data center technology stack. A significant majority consider their infrastructure to be Very modern or Cutting-edge, with only a small portion reporting their systems are outdated.

Survey Question: How would you describe the overall maturity of your current data center technology stack and infrastructure?

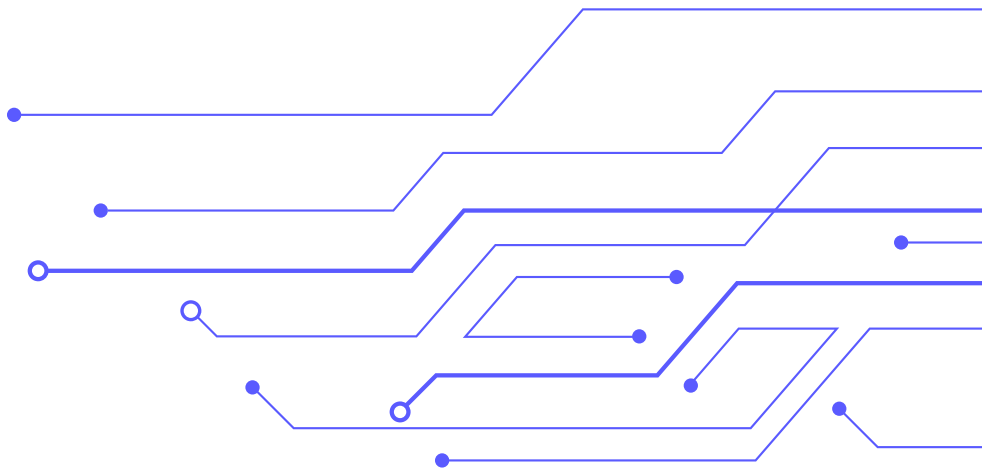
Maturity Level	Percentage of Respondents
Very modern	43%
Moderately modern	27%
Cutting-edge	21%
Somewhat outdated	6%
Very outdated	3%

Appendix Table 5. Technologies and Practices in Use Today

Summary: This comprehensive table shows the adoption rates for a variety of modern network operations technologies and practices. It highlights the widespread use of automated monitoring, infrastructure-as-code, and AI/ML for incident detection.

Survey Question: Which of the following technologies or practices does your organization use today?

Technology or Practice	Percentage of Respondents
Automated monitoring and alerting	67%
Infrastructure-as-code or configuration automation	58%
ITSM/ticketing	57%
AI/ML-based incident prediction or detection (AIOps)	54%
Auto-failover or redundancy systems	49%
Config or script management (Git/GitHub/GitLab)	45%
CI/CD pipeline automation	44%
Role-based access control or change approval workflows	44%
AIOps tooling	36%
Custom in-house automation scripts	33%
Self-healing or auto-remediation tooling	20%
Chaos engineering and/or disaster recovery simulations	20%



Appendix Table 6. Criticality and Implementation of Advanced Technologies

Summary: This table details both the perceived criticality and the current implementation status of advanced network technologies. It shows that technologies such as pre-check and post-check configuration changes and intent-based networking are highly valued, and many organizations are already in the process of implementing them

Survey Question: Which of the following technologies or practices does your organization use today?

Technology	Average Criticality (1–5)	Already Implemented (%)
Pre-check and post-check configuration changes	4.2	59%
Intent-based networking	4.2	50%
Support for an integrated network digital twin	4.1	49%
Closed loop monitoring and automation	4.0	50%
AI-Ops mechanisms	4.0	43%
Rollbacks	4.0	60%
Revision control	4.0	58%
CI/CD pipeline	3.8	50%

Appendix Table 7. Primary Focus of Reliability Efforts

Summary: This ranked data shows where teams primarily focus their reliability efforts. Network Infrastructure is the top priority, followed by Software and systems and Security architecture.

When your team discusses "reliability," which layer is the primary focus of your efforts? (Rank order from most important to least important)

Layer	Overall Rank
Network infrastructure	1
Software and systems	2
Security architecture	3
Server & compute infrastructure	4
Operational processes & automation	5
Storage infrastructure	6
Physical infrastructure	7

Appendix Table 8. Impact of Poor Software Quality

Summary: This table reveals how poor software quality from vendors affects operational teams. The most common impact is the need for vendor patches, followed by performing internal QA practices and experiencing silent failures.

How does poor software quality (poor design and test practices) impact your teams?

Impact	Percentage of Respondents
Bugs needing vendor patches	73%
Perform QA practices myself or use a special vendor test lab	54%
Silent failures	45%

Appendix Table 9. Size of Teams

Summary: This table provides a breakdown of the number of employees who work on or support data center network infrastructure. The responses are split, with a large portion of companies having either very small or very large teams dedicated to this function.

Survey Question: Approximately how many employees work in or support your data center network infrastructure?

Team Size	Percentage of Respondents
50 or more	43%
Fewer than 10	42%
26–50	12%
10–25	3%

Important Information About This Report

AUTHORS

Mitch Ashley
Vice President & Practice Lead Software Lifecycle Engineering | The Futurum Group

Scott Robohn
CEO of Solutional

PUBLISHER

Futurum Research

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

NOKIA

ABOUT NOKIA

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Futurum

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

Futurum

CONTACT INFORMATION: The Futurum Group LLC | futurumgroup.com | (833) 722-5337