The Infrastructure Automation Report, 2025

Overconfidence and the Speed-Control Paradox

This survey was conducted and produced by Panterra Group, a strategic consulting and research firm, and commissioned by Spacelift.

Contents

Executive Summary

A flood of new automation tools has hit the market, and automation adoption is at an all-time high. But here's the reality — many teams think they're performing better than they actually are. They've built slick new workflows and automated processes, but when you look under the hood, the results aren't as impressive as they claim. High failure rates, inefficient resource utilization, and gaps in security and compliance show that automation maturity isn't just about adopting new tools — it's about implementing them effectively.

The truth is, it's not just the technology that drives better performance — it's the processes and team structures that make automation successful. **Platform engineering, self-service enablement, and a culture of automation-first thinking are what separate high-performing teams** from those who are simply layering new tools onto legacy workflows. Our data show that leading companies are more than twice as likely to have implemented infrastructure-as-code best practices, are over three times as likely to have implemented automated testing for infrastructure changes, and are five times as likely to have implemented a platform engineering team as their less advanced peers. Without these foundational elements, automation efforts stall, leading to operational inefficiencies, security blind spots, and a false belief in progress.

Thankfully, automation can solve many of these challenges. Faster resource provisioning with automated workflows, on-demand scaling with auto-provisioning, version-controlled toolchains to simplify provisioning and config management — the list goes on. We have come a long way. So much so that many organizations believe they've nailed infrastructure automation.

But the data tell a different story — one riddled with inefficiencies, bottlenecks, and misconfigurations.

> Our research[1] has uncovered a stark gap across many organizations between their self-perceived infrastructure automation and their actual execution.

[1] This report is based on a survey of n=413 IT infrastructure tool purchase decision-makers and influencers, representative by gender, age, company size, revenue, industry, and years of experience. Our goal with this research was to understand where teams stand in their automation journey and identify what sets high-performing organizations apart from the rest. [See appendix for full methodology.]

While 45% of organizations believe they have achieved a high level of infrastructure automation, according to our recent research, only 14% exhibit the behavior and technology patterns of true infrastructure automation leadership.

If so many organizations believe they've achieved automation maturity, why does the reality tell a different story? The answer lies in a fundamental trade-off: Speed has come at the expense of control. This is what we call the **Speed-Control Paradox** — where the pursuit of faster deployments inadvertently introduces a loss of control in the areas of security, compliance, and cost management.

Top-performing organizations have found a way to navigate this Speed-Control Paradox, striking a balance between rapid deployments, developer self-service and governance. **Using our survey, we developed the Infrastructure Automation Leadership Index** based on robust analysis of behaviors, tooling, performance, and results across organizations to identify these top performers and isolate success patterns. The good news is, their situations are not unique. There is nothing special about what leaders are doing which cannot be emulated by others. Key patterns include:

- **Implement developer self-service.** Reduce bottlenecks to developer productivity while ensuring app performance and maintaining the right guardrails to mitigate risk.
- **Integrate security and compliance early.** Ensure security and compliance are part of your automation strategy from the beginning, not just an afterthought.
- **Adopt a platform team approach.** Automating speed, control, and security is a balancing act that requires deliberate focus to maintain. A unified platform team approach enables this.
- **Prioritize cost optimization.** Actively manage infrastructure resource utilization to eliminate overprovisioning and avoid waste.
- **Avoid siloed automation.** Centralize management of automation that both provisions infrastructure (Day 1) and manages resources long term (Day 2).

In this report, we'll break down how infrastructure automation leaders achieve this balance and what other organizations can do to follow suit. Our goal is for this to serve as a roadmap for teams looking to advance their infrastructure automation maturity. By leveraging insights from our **Infrastructure Automation Leadership Index**, your team can move from overconfidence to actual excellence.

Our self-assessment tool, built on insights and data from this report, provides a clear and objective view of where your organization ranks on the **Infrastructure Automation Leadership Index.** At the end of the self-assessment, we offer resources specific to your stage of automation maturity to help you craft a strategic roadmap toward automation excellence.

Have you done your self-assessment yet?

Click here to begin

Introduction

Infrastructure Automation & The Speed-Control Paradox

At the core of the infrastructure automation challenge is the Speed-Control Paradox. How can teams move fast without sacrificing security, compliance, or stability?

Infrastructure teams today are navigating increasingly distributed architectures, multicloud environments, on-premises infrastructure, and an ever-growing stack of tools and processes — in fact, **81%** report operating in a hybrid cloud environment.

At the same time, development teams face mounting pressure to ship faster, deliver blazing fast user experiences, and minimize downtime. These teams must also ensure compliance with stringent security and regulatory requirements.

Many organizations assume they've struck the right balance in the Speed-Control Paradox, but in reality, they've only accelerated deployment frequency without putting the right guardrails in place.

Our survey found that over **50%** of companies take a week or more to deploy infrastructure changes in production, and **43%** need to rerun their infrastructure deployments more than four times to get it right. Not quite the balance companies are looking for.

For those who do master infrastructure automation, the benefits are real. Our research indicates leaders are:

more likely to get infrastructure deployments right on the first try

more likely to provision new resources in 4 hours or less

more likely to deploy changes in production daily or multiple times a day

Interestingly, the focus of automation shifts as a company becomes more mature. Leaders prioritize control; those earlier in their automation journey prioritize speed. When asked about their automation priorities, only **29%** of early stage companies focus on control (getting infrastructure changes done correctly), whereas only **39%** of leaders focus on speed. The difference is stark.

So what is it Leaders do to find this balance? This is what we explore next. Hint, they don't just use infrastructure-as-code (laC) tools, they build and orchestrate workflows that tie infrastructure pipelines together.

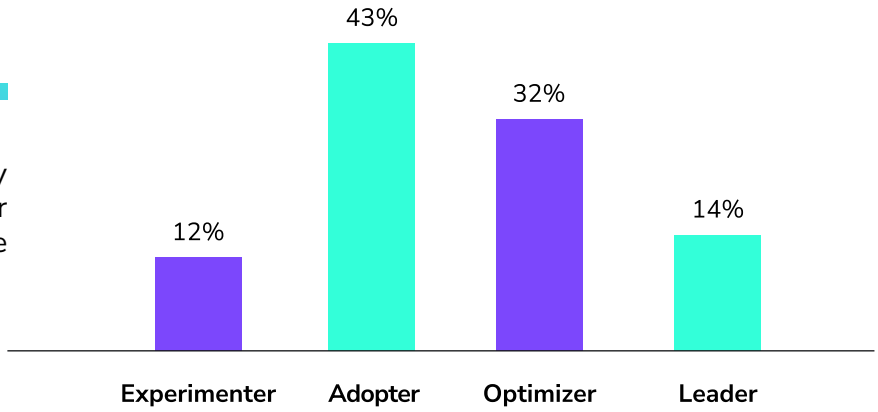
Orchestration is the automated coordination and management of infrastructure provisioning, configuration, and governance. By integrating with laC tools, unifying workflows, enforcing policies, and automating workflow execution, it ensures efficient, secure, and resilient laC pipelines. Whether you build it yourself or use a vendor-provided solution, orchestration reduces time to market, eliminates manual effort, ensures resiliency and enhances security.

Solving the Speed-Control Paradox

Identifying the Leaders

Automation excellence is a journey, not a switch you flip. We developed the **Infrastructure Automation Leadership Index** to provide a structured approach to evaluating automation maturity and to define a clear progression from basic automation practices to advanced, scalable, and secure automated infrastructure management.

Distribution of survey participants across the four levels of the Infrastructure Automation Leadership Index



- **Experimenter:** Organizations at this stage are in the early phases of automation, testing tools and processes in isolated areas. While some manual workflows remain, they are actively exploring ways to improve efficiency and reduce operational burden. 59% of Experimenters are still working with partially automated or mostly manual infrastructure processes. The primary challenge is consistency — without standardization across teams, automation efforts produce variable results.

- **Adopter:** Automation has moved beyond experimentation and is becoming a part of infrastructure strategy, with 52% reporting having mostly automated, with some manual processes. However, standardization and governance remain challenges. Different teams may use varied tools and methodologies, creating opportunities for greater alignment and efficiency as automation scales.

- **Optimizer:** Significant progress has been made, with streamlined deployments and improved governance, but gaps persist in security, compliance, and scalability. 55% have automated security scanning, and 46% have implemented self-service provisioning for developers. A dedicated platform team is often in place, working to standardize automation and reduce operational friction. The key challenge is fully aligning infrastructure management with the development team and business objectives.

- **Leader:** Automation is deeply integrated, with security, compliance, and scalability built into every process. 83% report having most of the infrastructure processes automated, with 24% fully managing their infrastructure pipeline by automated workflows, and 73% report having established automated security and compliance scanning. Infrastructure provisioning is self-service, enabling developers while maintaining strong guardrails. Deployments are fast, predictable, and secure, shifting focus from troubleshooting to delivering business value. Infrastructure automation is centrally orchestrated and covers not only provisioning but configuration management for ongoing resource management and related Day 2 operations. At this stage, platform teams act as force multipliers, enabling true automation at scale.

Dimensions of Infrastructure Automation Excellence

The Infrastructure Automation Leadership Index was developed based on real-world automation practices and their impact on organizational success.

The model includes five questions that capture critical aspects of infrastructure automation within an organization across three principal categories:

Speed

Faster deployments, shorter provisioning times, and lower failure rates, leading to fewer retries

Control

Proper implementation of infrastructure as code (IaC), drift management, cybersecurity, and compliance automation

Collaboration

Strong platform engineering practices and seamless cross-team workflows

We ran several models to determine the most important infrastructure automation factors correlated with positive business outcomes and arrived at these five questions.

1. What percentage of your infrastructure is managed by infrastructure as code (IaC)?
2. Which infrastructure processes are currently automated at your organization?
3. What strategies does your organization use to handle configuration drift?
4. To what extent does your infrastructure automation foster collaboration between your software engineering, platform engineering, and security teams?
5. Is your organization considering a shift to platform engineering to centralize automation efforts?

Challenges Identified

As organizations scale their infrastructure, the Speed-Control Paradox becomes more evident. Moving fast requires automating governance, security, and compliance to minimize the operational burden of change management processes. But doing this at scale introduces its own set of challenges.

- **Increased risks:** Unchecked automation can expose organizations to security vulnerabilities, misconfigurations, downtime, compliance failures, and even business disruptions. To mitigate these risks, automated workflows must include built-in validation steps, security checks, and policy enforcement. Three times as many Leaders automate security scanning compared with Experimenters, and over twice as many automate compliance checking.

Without proper governance, organizations may experience:

- **Escalating costs** — Without well-defined guardrails that enforce resource limits, teams can inadvertently spin up excessive or over-provisioned resources. Whether through scaling out (creating more resources of the same kind) or scaling up (using overpowered resources), costs can quickly spiral out of control without delivering proportional benefits. Leaders keep an eye on this and are three times more likely than Experimenters to use infrastructure costs to track and measure infrastructure automation performance.

- **Infrastructure drift** — A lack of visibility and governance over infrastructure changes leads to drift — where the actual state of deployed infrastructure deviates from its intended configuration. This results in unpredictable failures, degraded performance, and unnecessary costs, as organizations struggle to track and manage their infrastructure effectively. Our data show that four times as many Leaders automate drift detection and remediation than Experimenters. In fact, 92% of Leaders handle configuration drift via regular automated checks.

- **Downtime and compliance violations** — Security gaps and misconfigurations don't just create operational inefficiencies — they come with real business risks. Unaddressed vulnerabilities can lead to service outages, compliance breaches, and even reputational damage, ultimately impacting revenue and customer trust.

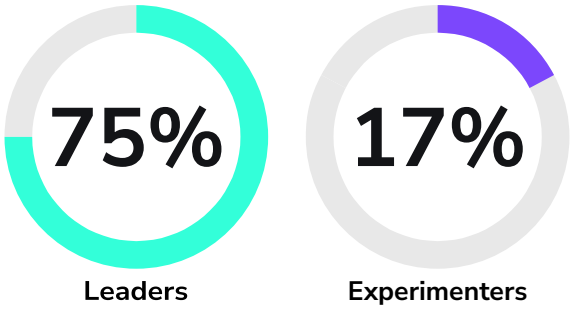
Organizations may also experience complexity creep as they scale automation across teams and tools without a structured approach. This leads to fragmentation and inefficiency. Three times as many Experimenters as Leaders are still struggling to reduce complexity. Teams inside your organization may adopt different tools and processes leading to a hard-to-maintain ecosystem. In this way, they will encounter:

- **Siloed teams** — Without a centralized automation strategy, teams operate in isolation, making it hard to maintain consistency, enforce best practices, and prevent misconfigurations or deployment failures.

- **Operational overhead** — Debugging failures across multiple loosely connected systems increases troubleshooting efforts, leading to higher downtime and slower resolution times. This reduces developer velocity and drains valuable engineering resources.

- **Reduced cross-team collaboration** — When teams use different automation approaches, aligning workflows becomes a challenge. Disjointed processes hinder knowledge-sharing and make it harder to integrate systems effectively, slowing down your overall time to market.

75% of Leaders say their infrastructure automation fosters collaboration between software engineering, platform engineering, and security teams compared with **17%** of Experimenters.



The Roadmap to Infrastructure Automation Excellence

Leaders don't start off that way. They overcame the same challenges most companies face today or will face tomorrow. But you can learn from their hard-won efforts and jump straight to their position, no matter where you stand today.

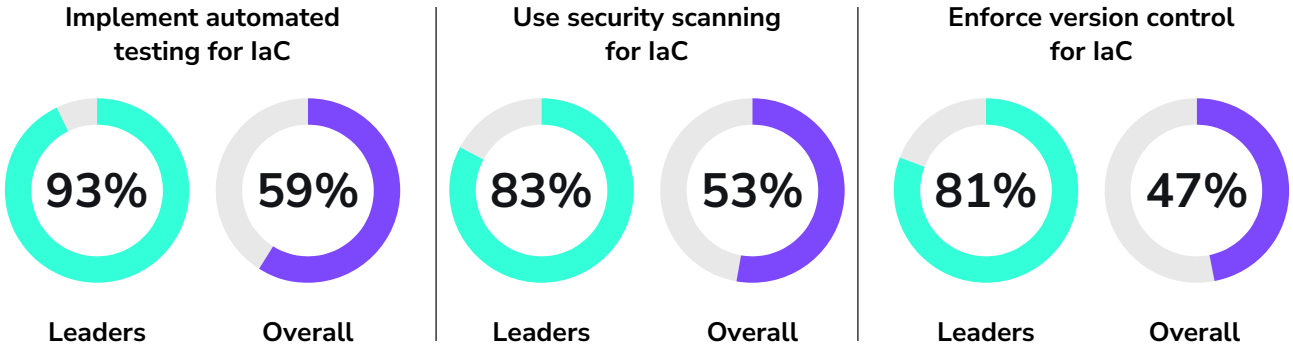
Here are some key patterns Leaders exhibit and ideas for how to emulate them.

1. **Assess your current state:** The first step toward automation maturity is understanding where you stand. Find out where you score on the **Infrastructure Automation Leadership Index** using the self-assessment below to benchmark your automation capabilities. Identify your current strengths, weaknesses, and gaps in speed, control, and collaboration. Conducting a self-assessment can help organizations gain clarity on their automation journey and avoid blind spots that could hinder progress.

2. **Reduce risk through automation:** Security and compliance must be integral to the automation process, not an afterthought. Putting security into your infrastructure is the ultimate shift left approach. Organizations can introduce tools and processes that help them easily identify and remediate security issues and vulnerabilities faster, without waiting for these issues to reach production and become critical. By using policy as code, security vulnerability scanning tools, observability platforms, and testing mechanisms, you ensure that infrastructure security is automated and issues are caught early before they become a risk.

Click here to begin your self-assessment

Leaders embrace security, integrating it into their automation approach:



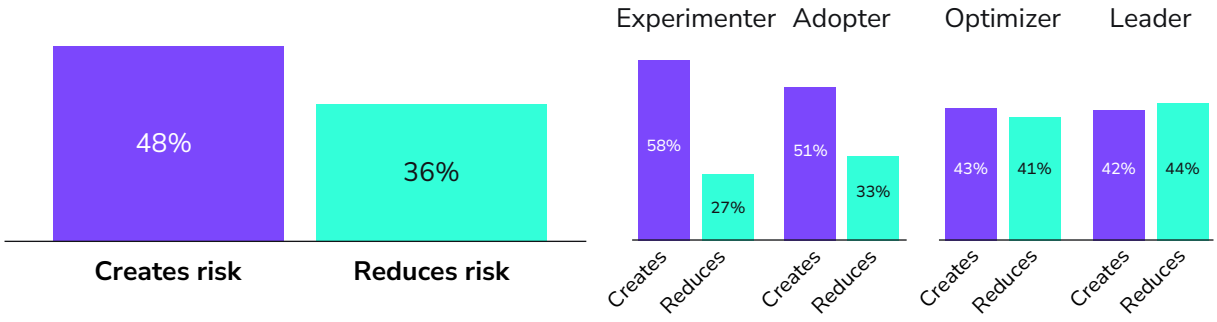
3. **Prioritize speed, but set standards for control:** Ramping up automation without the right safeguards leads to instability and risk. Before focusing on deployment velocity, ensure compliance, security, and drift management are solid. Organizations looking to ensure compliance often introduce policies, which are fundamental for ensuring standardization, as your team won't be able to provision resources that they shouldn't. They also ensure that resources respect the guardrails imposed by your organization. Security checks, especially those that detect vulnerabilities, ensure that your organization is safe and reduce the risk of downtime. With drift management, you can ensure that the desired state of your infrastructure is the state deployed, reducing the potential for misconfiguration, performance degradation, and downtime.

   Highly mature teams integrate automated security checks, policy enforcement, and version control into their workflows — **61%** of Leaders track security incidents as a way to measure infrastructure automation performance, compared with **32%** overall. This foundation prevents automation from becoming a liability.

4. **Accelerate developer velocity with self-service:** Automation should make work easier, not introduce new bottlenecks. Leaders empower developers with self-service automation while maintaining guardrails to mitigate risk. They prioritize infrastructure agility, ensuring they can scale resources in real time to meet demand without waiting for manual approvals or navigating a complicated ticketing service. By enabling self-service for developers, you reduce costs, increase scaling capabilities, and enhance collaboration. Ultimately, all these benefits translate to increased business value.

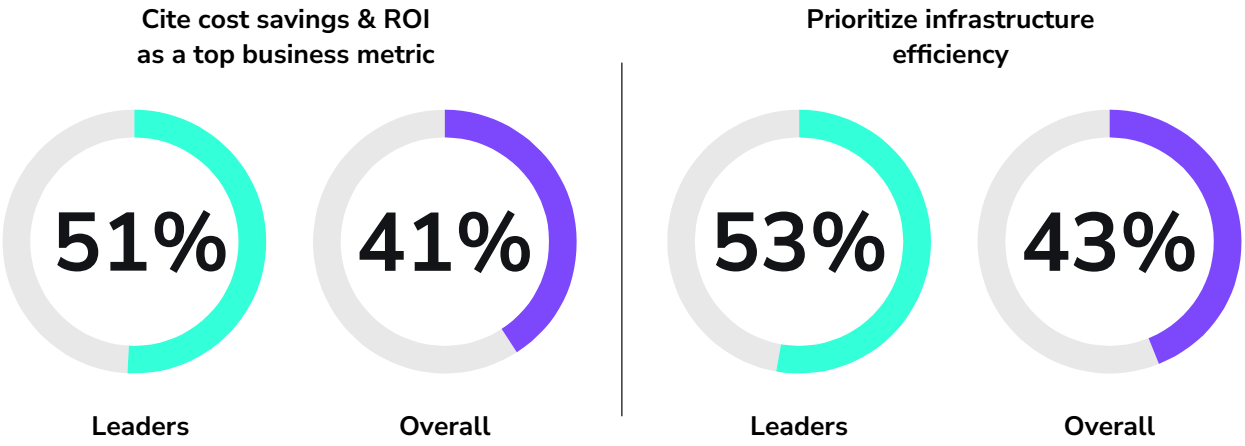
a. Leaders excel at developer self-service. Compared with Experimenters, Leaders are +33 points more likely to say that introducing developer self-service reduces risk rather than increases it.

Leaders more adept at reducing risk from developer self-service



5. **Prioritize cost optimization as a business driver:** Smarter automation eliminates overprovisioning and waste. By using policy as code in conjunction with automated cost estimation, you can create clear guardrails around your budget. You can automatically deny deployments that would result in overprovisioning, and ensure resources meet pre-approved parameters. Self-service templates also optimize costs by only allowing users to deploy pre-approved templates, ensuring resources have a predictable cost and reducing human error.

   Leaders view cost efficiency as essential to business success. They actively manage infrastructure resource utilization to avoid waste.



6. **Adopt platform engineering for consistency and scale:** Siloed automation efforts create fragmentation and inefficiency. To scale effectively, organizations should centralize automation through platform engineering teams. These teams standardize infrastructure, enforce best practices, and provide self-service capabilities that balance autonomy with governance. **29%** of Leaders have implemented platform teams compared with just **7%** of total respondents. Platform engineering ensures automation scales efficiently without introducing chaos.

> *"We were able to begin democratizing access to the infrastructure, which was really key in enabling everybody to move faster. We had work queued for weeks at a time that teams could now run themselves within the hour. It was smooth, and it was fast, and it maintained our high level of security standards."*
>
> **Maxx Daymon** – Staff Cloud Platform Engineer at 1Password

The Payoffs of Making the Automation Journey

Organizations that follow this roadmap don't just automate — they **orchestrate**, enabling:

- **Streamlined workflows & developer efficiency:** Leaders create high-velocity environments where developers can focus on building rather than troubleshooting. 61% of Leaders have streamlined workflows and reduced friction, compared with 45% of all respondents. By eliminating bottlenecks and enabling self-service automation, teams experience fewer disruptions and increased productivity.
- **Proactive, embedded security & compliance:** Instead of reacting to incidents, Leaders bake security and compliance into their workflows from the start. 58% of Leaders have cut security incidents compared with just 41% overall, and 56% report fewer compliance violations versus 36% of total respondents. With automated testing, policy enforcement, and security scanning at every stage, they ensure that infrastructure remains resilient and compliant without slowing down innovation.
- **Optimized infrastructure costs:** Efficiency isn't just about speed — it's also about smart resource allocation. 47% of Leaders have successfully reduced infrastructure costs, compared with 32% of all respondents. By avoiding overprovisioning, optimizing infrastructure utilization, and leveraging automation to scale only when necessary, they ensure that infrastructure spending is not inflated or inefficient and that it aligns with business goals.

Automation maturity isn't a one-time achievement — it's a continuous evolution. By following these steps, organizations can build a scalable, secure, and high-performing automation strategy that fuels long-term success.

For those who do master infrastructure automation, the benefits are real. Our research indicates leaders are:

2x

more likely to get infrastructure deployments right on the first try

4x

more likely to provision new resources in 4 hours or less

5x

more likely to deploy changes in production daily or multiple times a day

Conclusion

The journey to infrastructure automation is not simply about adopting new tools, finding the right blend of tools and processes, or strategically integrating automation into your provisioning, configuration, and governance processes. It's about orchestrating workflows that securely streamline infrastructure pipelines, enabling the organization to go fast without sacrificing control.

> Our research reveals a critical gap: While many organizations believe they have achieved high levels of automation, few have progressed to true orchestration. As teams evolve from Experimenters to Optimizers, they encounter the Speed-Control Paradox — the trade off between accelerating deployments and maintaining governance.

Early in their journey, Experimenters and Adopters prioritize speed, leveraging tools like Terraform, OpenTofu, Ansible, and CloudFormation to streamline provisioning and configuration management. While these tools each accelerate a different part of infrastructure management, that speed comes at the cost of security, governance, and cost control. As organizations mature into Optimizers, their focus shifts to control. They provide developer self-service to accelerate further but begin to implement guardrails like policies, role-based access control (RBAC), security scanning, drift detection, and observability tools to enhance the security, stability, and compliance of their infrastructure.

Yet, even with these tools and a platform team in place, balancing speed and control remains a challenge — especially at scale. Fragmented tools and processes make it difficult to maintain efficiency and consistency as teams and infrastructure grow. This is where the Leaders stand out. They've moved beyond automation, tying provisioning, configuration, and governance into a single, integrated workflow. This orchestration is how they master the Speed-Control Paradox.

The good news is that any organization can overcome the Speed-Control Paradox. It starts with getting a clear picture of where you stand with our self-assessment tool. Once you know where you are on your journey, use the Roadmap to Infrastructure Automation Excellence to plan your next steps. Whether you're just getting started or on the doorstep of full orchestration, the key is to keep evolving.

If you want to accelerate your journey, Spacelift offers an orchestration platform that manages your entire infrastructure lifecycle — provisioning, configuration, and governance. It integrates with all of your infrastructure automation tooling to provide a single integrated workflow so you can move at the speed developers demand, with the control your platform team requires.

Sign up for a **demo** or a **free trial** at **Spacelift.io**.

Appendix

Research methodology

This survey was conducted and produced by Panterra Group (formerly ClearPath Strategies) (www.panterra.global), a strategic consulting and research firm, and commissioned by Spacelift. Following are the firm's research notes for this survey.

Respondent selection

The survey included 413 respondents sourced from a leading global online panel provider. They were selected from the panel based on geographic and role-based quotas, as well as screening questions based on role in IT, decision making role, company size, and how long they have been in IT. Selected respondents were further screened based on self-reported IT knowledge and attentiveness to survey questions.

Role quotas

The survey divided respondents into four broad roles: CIO / CTO 23%, IT Leadership **46%**, IT Director / Manager **14%**, and Line of Business leadership **17%**. Respondents were asked to select which role — from a list of 16 options — most closely described their primary responsibility, even if no one was quite right or even if they performed more than one of these roles. Answers were consolidated into those four broad roles.

Geographic quotas

The survey included respondents from the US and North America.

Industry

Although no industry-level quotas were deployed, we monitored the data to ensure that no single industry was over-represented in the data. The final breakdown of respondents by industry is as follows: IT (software products & services, SaaS) **47%**, Financial Services **12%**, Retail / eCommerce **11%**, Industrials and Manufacturing **8%**, Transportation and Logistics (including supply chain) **6%**, Healthcare (excluding pharmaceuticals) **4%,** Business / Professional Services **4%**, Energy & Resources **3%**, Insurance **2%**, Government / Public Sector **1%**, Telecommunications **1%**, Life Sciences (excluding healthcare) **1%**.

Respondent screens

Potential respondents were screened out on several criteria:

- **Role:** All respondents were required to indicate that they were responsible for or had influence in evaluating and/or selecting IT infrastructure solutions or software for their organization.
- **Company size:** All respondents must self-report that their companies have a minimum of 250 employees. All potential respondents from smaller companies were excluded. In total, the survey includes **24%** from companies with 250-499 employees, **31%** from companies with 500-999 employees, **31%** from companies with 1,000 to 4,999 employees, and **14%** from companies with 5,000 or more employees.
- **Time in IT:** Respondents must have spent a minimum of 3 years managing, planning, or purchasing software services or infrastructure in order to qualify for the survey. In total, **7%** of respondents have spent 3-5 years in this role, **56%** have spent 6-10 years in this role, **28%** have spent 11-15 years in this role, and **9%** have spent 16 years or more in this role.
- **Information level:** In our experience, it is possible to have "qualifying respondents" who nevertheless prove to have too little information or knowledge about the space to provide useful data from which to draw insights. We therefore apply an "information" screen to respondents as well. Specifically, we ask whether or not respondents could explain certain terms to their colleagues if asked to do so. In order to qualify for this survey, a respondent must say "yes" to this question for the terms "cloud computing" and "Infrastructure as Code."
- **"Attention" level:** It is easy for respondents to speed through surveys or not pay enough attention to provide useful data. We make an effort to exclude these respondents as well, as they provide generally less useful data. In this survey, respondents were screened out for "attention" reasons if they said they could explain the made-up term "Greenfield as a Service (GaaS)" to a colleague in the same question used for the Information Screen noted above.

A note on margin of error

It is technically impossible and improper to list a margin of error for a survey of this type. The respondents for this sample were drawn from an online panel with an unknown relationship to the total universe, about which we also do not know the true demographics. As such, the exact representativeness of this, or any similarly produced sample, is unknown.


spacelift