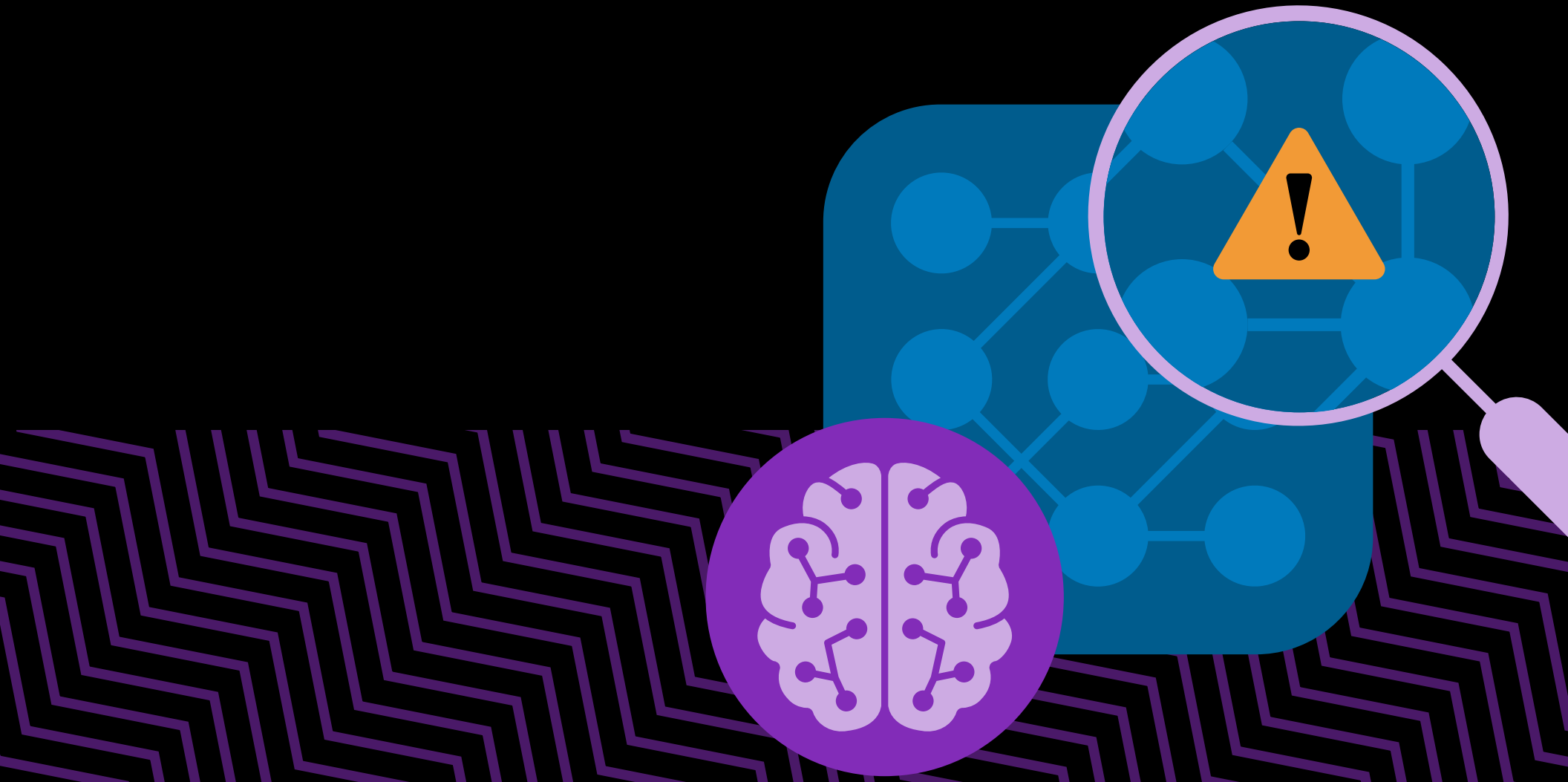
State of Application Strategy Report

2025

Contents

Introduction:

AI Has Arrived–
to Clash with Manual IT Ops



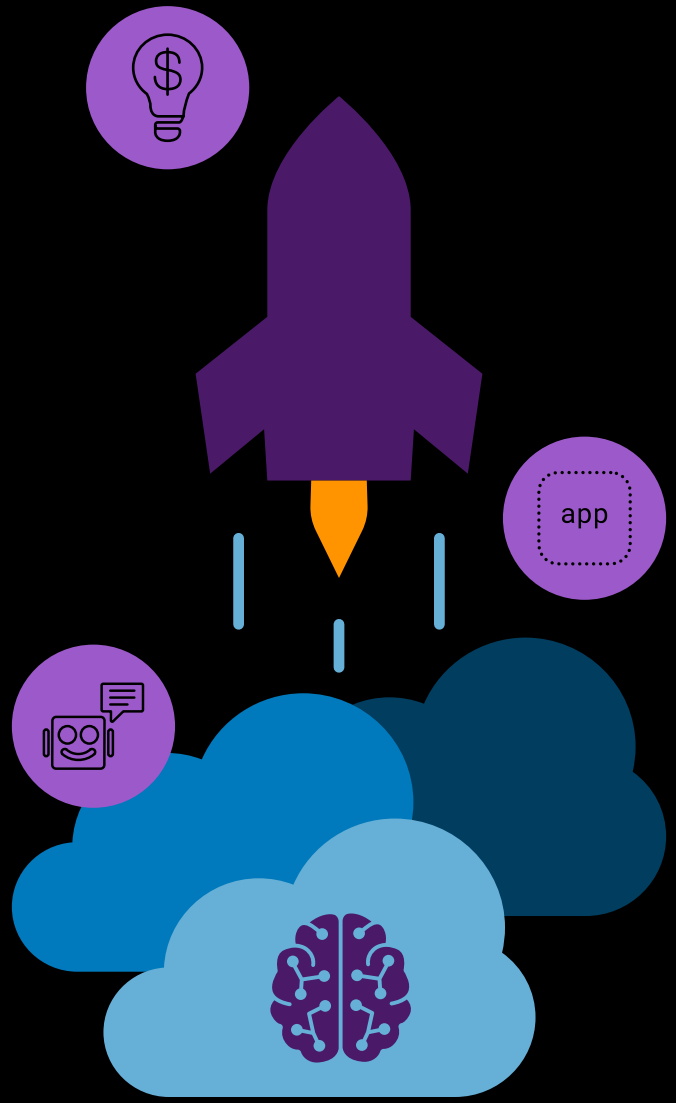
Society is more dependent on information technologies than ever before, and for many organizations, technology has rapidly driven transformation of the entire business model. One finding of the 2025 F5 State of Application Strategy survey indicates that 93% of organizations today, across industries, generate at least part of their revenue through digital applications. This fact reflects remarkably fast change. Only two years ago, in 2023, more than one-fifth of respondents (21%) still weren't providing digital services to anyone but their own employees. While those internal services enabled or improved productivity, they were not directly monetized. Now even traditional industries known for person-to-person interactions, such as healthcare and education, are building digital revenue streams. They're doing so by serving customers through innovative, customer-facing digital services—from self-service biometrics to subscription-model test preparation.

Another indication of light-speed rates of change is the exponential deployment of AI and machine learning (ML) now underway. In 2023, about one-quarter of organizations had implemented AI assistance. Most of this AI assistance came in the form of customer service chatbots. Two years later, 96% of organizations say they're currently deploying AI models, and today's models are more likely to support line-of-business decisions and employee productivity. The AI disruption we predicted in 2022 has arrived.

96% of organizations are deploying AI models

Amid the rush to intelligent apps, the eleventh annual F5 survey captures a snapshot of remarkable progress and persistent barriers. The results of the survey also suggest the path successful organizations are likely to take over the next two to five years.

Change is moving so fast that the next 12 months alone will no doubt bring upheaval and a few unforeseen impacts. This F5 State of Application Strategy Report can help you navigate rapid digital evolution and ensure your organization acts to keep up.



Summary of Key Findings

Hybrid complexity is entrenched

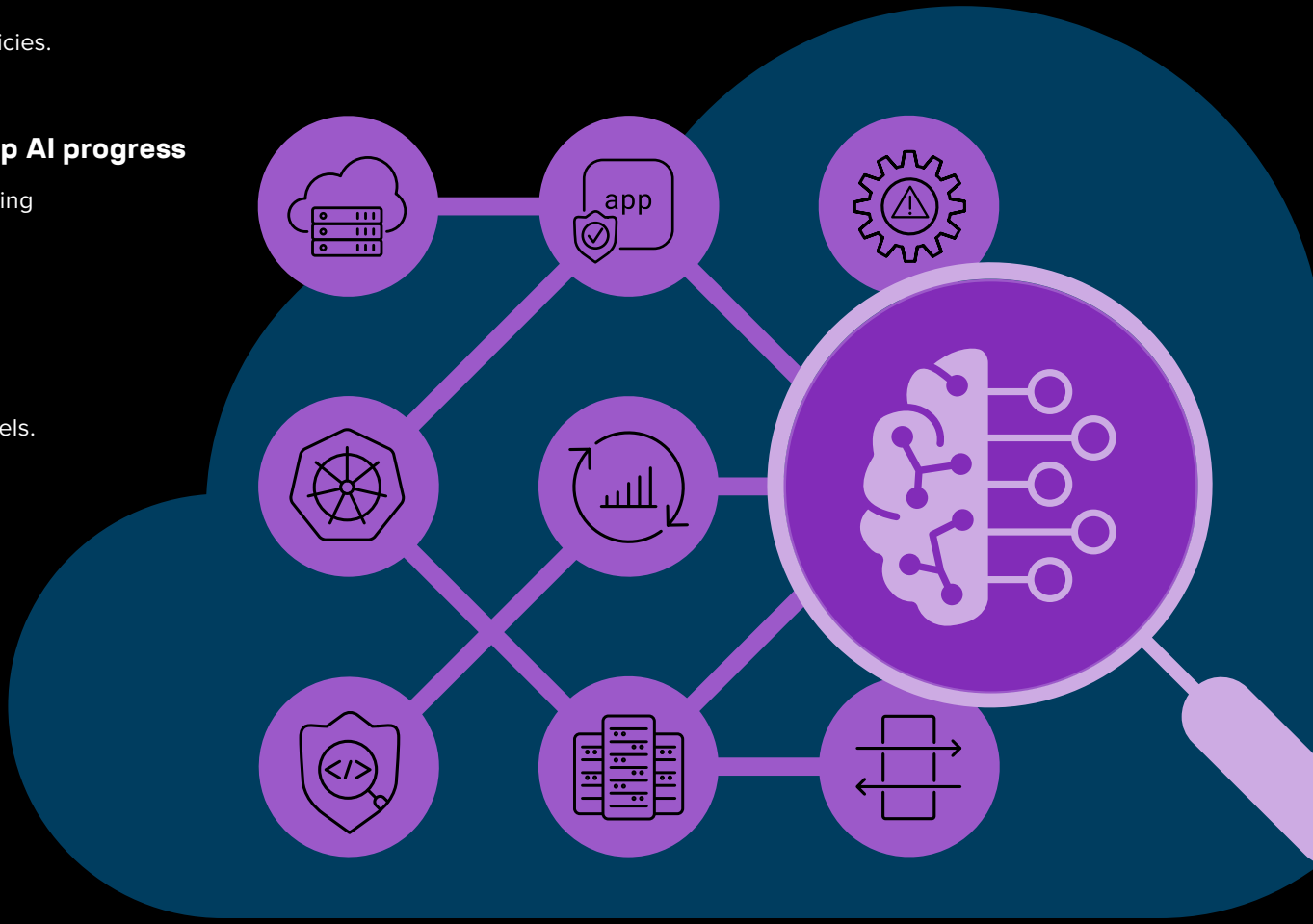
- 94% of organizations deploy apps across multiple environments.
- They deal with a median of four public cloud vendors.
- 79% report moving apps from public clouds back to on-premises or colocation environments.
- 53% struggle with inconsistent app security policies.
- 58% call API sprawl a significant pain point.

App delivery and security strategies help AI progress

- 93% of organizations have strategies for managing observability data.
- 96% of organizations are deploying AI models, and the majority worry about AI model security.
- 50% have deployed AI gateways.
- 50% expect API security to help protect AI models.

Traditional operations block AI aspirations

- 73% would like AI to optimize app performance.
- Unfortunately, 60% are mired in manual operational tasks.
- 54% lack sufficient AI skillsets.



This year's results indicate that many organizations have improved observability, gained data maturity, and adopted standardized frameworks such as OpenTelemetry. As a result, more are obtaining the insights needed for effective AI assistance. In 2024, data maturity and lack of scale were cited by nearly three-quarters of organizations (72%) as the top barrier to adopting AI. Today, more than nine in 10 organizations have strategies for managing observability data, which is a measure of data maturity. There's still work to be done, but many have made progress.

As noted above, AI deployments are exploding as a result. In addition to supporting business needs, IT organizations are embracing the efficiencies AI can bring to app security and deployment operations (AIOps). AIOps has long been a prioritized use case because it promises to help tame the complexities of today's hybrid, multicloud deployment models. Those complexities have become entrenched. In fact, 94% of organizations manage apps across multiple locations or deployment models, and organizations today deal with a median of four different public cloud vendors. AIOps can help reduce the resulting operational burdens.

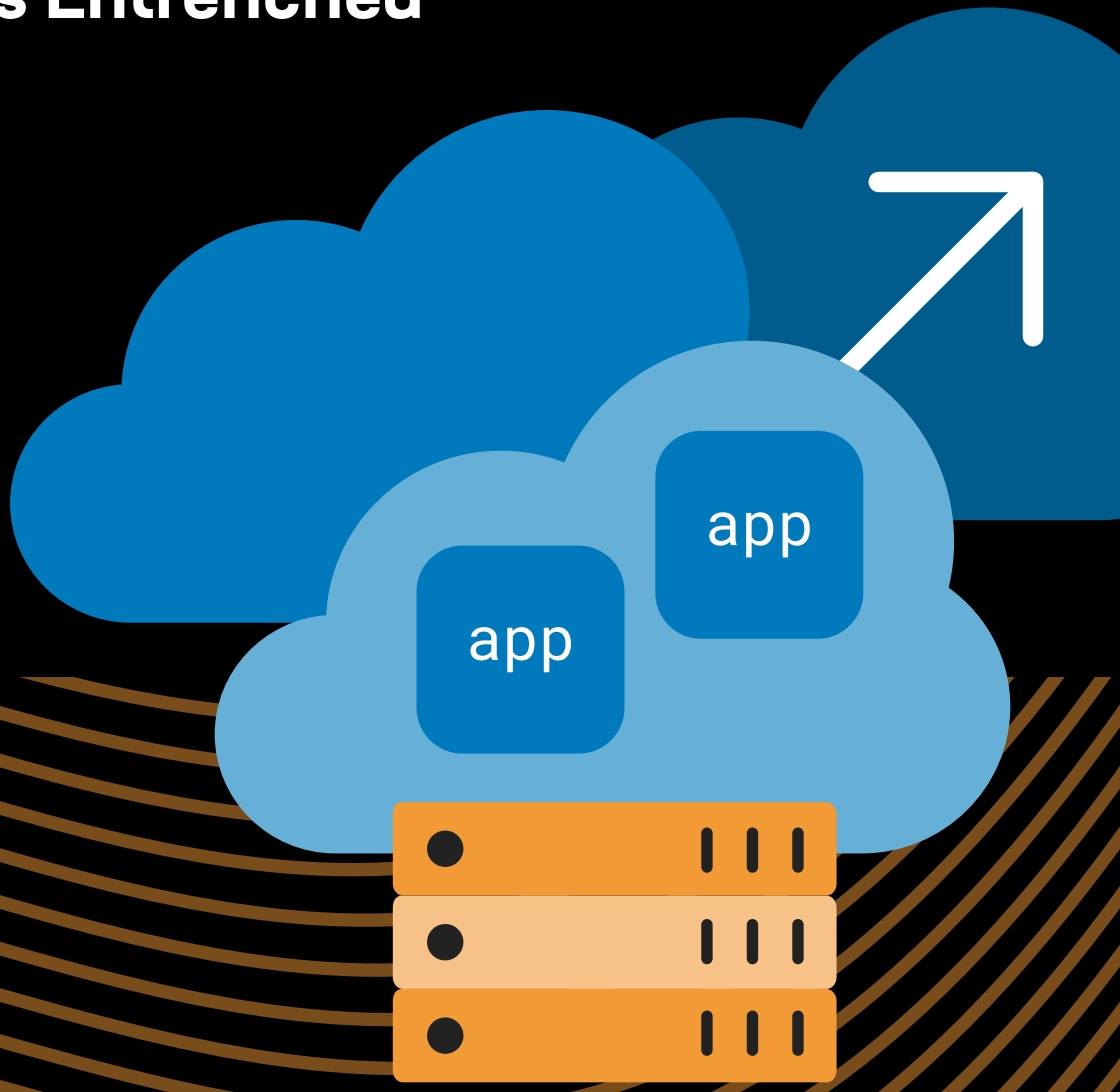
94% of organizations manage apps in hybrid deployment models

Unfortunately, there's a mismatch between AI aspirations and IT operational processes. The adoption of AIOps in particular is hindered by cumbersome workflows and traditional ticketing or management systems. Anyone who's tried to vacuum the floor of a busy family home will appreciate the tumult of toys, shoes, book bags, pets, and dirty socks that often must be dealt with manually first, before even a partly automated appliance can do a good job. IT teams are in a similar position when it comes to deploying AI and ML. Staff time is consumed juggling a multitude of APIs, languages, and vendor tools. Missing skillsets slow the work, and even tools that can make a tedious job faster can't operate as well as they might with so many varied bits and pieces in the way.

Fortunately, solutions to AI barriers have progressed this year, too. For instance, 96% of organizations are using or plan to use their operational telemetry to drive automation. Analysis, alerting, or reporting use cases, while still popular, rank lower than automation, which can better pave the way for AI. Greater focus on standardization—in operational processes and vendors, as well as in app security, delivery, and management solutions—will also speed AI deployments. Further progress in both areas will help IT teams and their organizations rise above mediocrity. Keep reading for insights about how to position your company or institution for an AI-driven (near) future where instant, relevant, and personalized digital services will deliver larger and larger shares of revenue for successful organizations.

Section 1:

Hybrid Complexity Is Entrenched



Anyone still hoping for hybrid complexity to fade might also be investing in meme coins. Most organizations deal with hybrid app portfolios as well as hybrid deployment models, multiple clouds, and numerous vendors. In 2025, modern apps represent 53% of app portfolios, and that percentage will continue to grow. We expect modern apps to represent 85% of the average portfolio by the end of the decade. Eventually, traditional apps may dwindle further—but only if new technologies don't create additional change, and that's unlikely.

But even if app portfolios grow more uniform, the data suggests deployment models will not. Today, 94% of organizations distribute apps across multiple deployment locations or models. Hosting decisions are based primarily on the best location for each app. For nine in 10 respondents, that per-app ability to choose is the key benefit of hosting in multiple clouds. And for most respondents, app performance is the top determinant of delivering a great digital experience and therefore a key factor in deployment decisions.

Organizations deal with a median of **four** public clouds

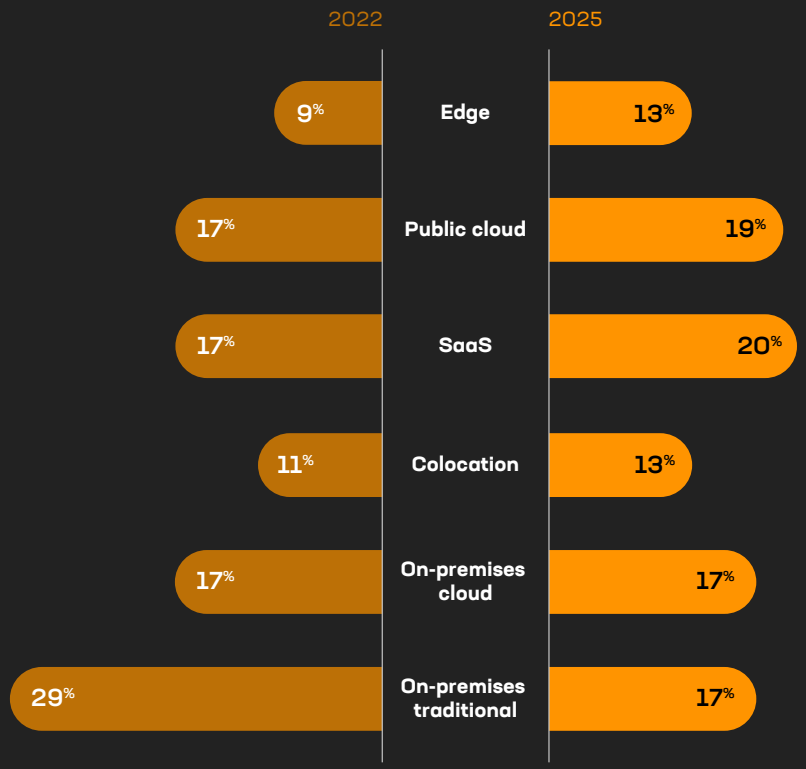
To achieve performance for customers everywhere, organizations turn to a variety of deployment models and hosting providers. Survey respondents report that their apps are deployed across a median of four public cloud vendors. (The average, considerably higher, is skewed by a few outliers.) Traditional on-premises deployments, although shrinking, won't disappear. Instead, app portfolios are settling rather evenly across all deployment models. These include edge locations, in part because the edge delivers performance by moving apps as close to customers as possible.

Apps Are Deployed Everywhere Almost Equally

Average percentage of app portfolios deployed in each model

We asked:
Of [your] applications deployed today, roughly what percentage are utilizing the following locations/ deployment models?

We learned:
App deployments are settling relatively equally across all models as hybrid strategies become entrenched.



All values are rounded to the nearest percentage

In addition, apps are on the move. Nearly eight in 10 organizations (79%) have recently repatriated at least one app from a public cloud to an on-premises or colocation environment, or they expect to do so within 12 months. That rate is up from only 13% in 2021. Cost control and predictability is the largest driver for these decisions, followed by security, privacy, and compliance issues. As circumstances change, organizations appreciate the flexibility to flow apps where they're best hosted now.

Flexibility to meet business needs is the **#1** benefit of hybrid deployments

As AI deployments rise, they'll only reinforce the hybridization (and perhaps fluidity) of app deployment. Survey respondents expect to deploy about one quarter of their AI models in public clouds (25%) and another quarter on-premises (24%). Nearly half (51%) plan to use both deployment environments. That figure has jumped from 35% just one year ago. Deployment of apps using AI follows a very similar pattern, although with slightly more AI apps deployed in public clouds (29%) and 46% in both places.

Organizations are making "both" decisions like this because the benefits are too great to ignore. Cost flexibility and app resiliency were cited as top benefits, but flexibility to meet business needs ranks highest.

Nonetheless, this flexibility comes at a cost. IT teams are left to deal with inconsistent security and delivery policies (cited by 53% and 47% of respondents, respectively). That inconsistency burdens the same IT teams responsible for deploying the AI-driven apps most organizations expect to rely on in the future. As a result, their ability to achieve those AI aspirations will depend on how well organizations can efficiently transcend the inherent complexity of hybrid operations.

Flexibility Keeps Hybrid Cloud Strategies Worthwhile

Percent of respondents naming each benefit

We asked:
What are the benefits of deploying in multiple clouds? Select all that apply. Why is your organization deploying apps in multiple public clouds? Select the top two.

We learned:
The flexibility to meet business needs, including cost control, drives organizations to deploy apps across multiple clouds.

91%
Flexibility to meet needs of business

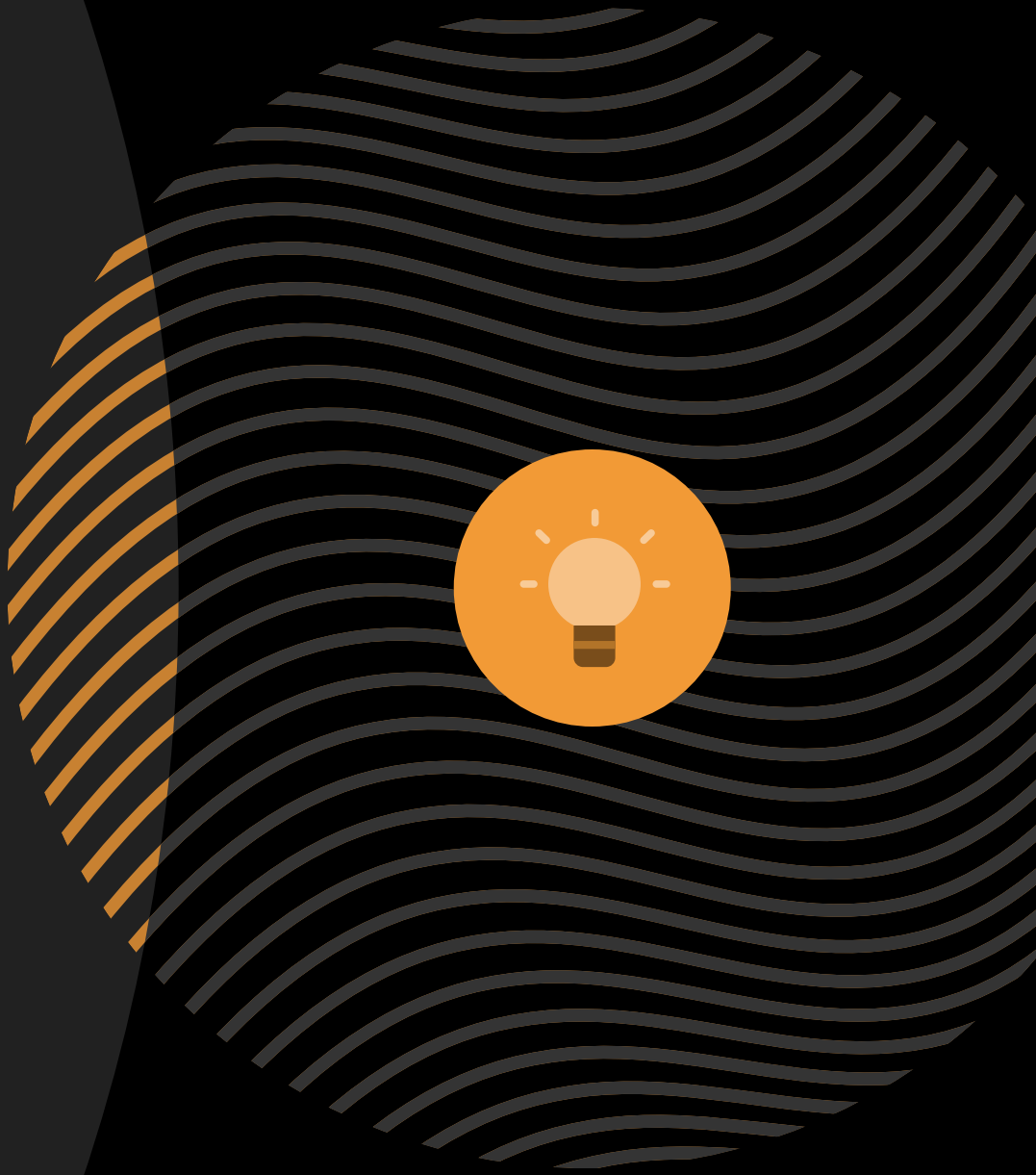
68%
Resiliency

59%
Flexibility to choose lowest costs

F5 Insight

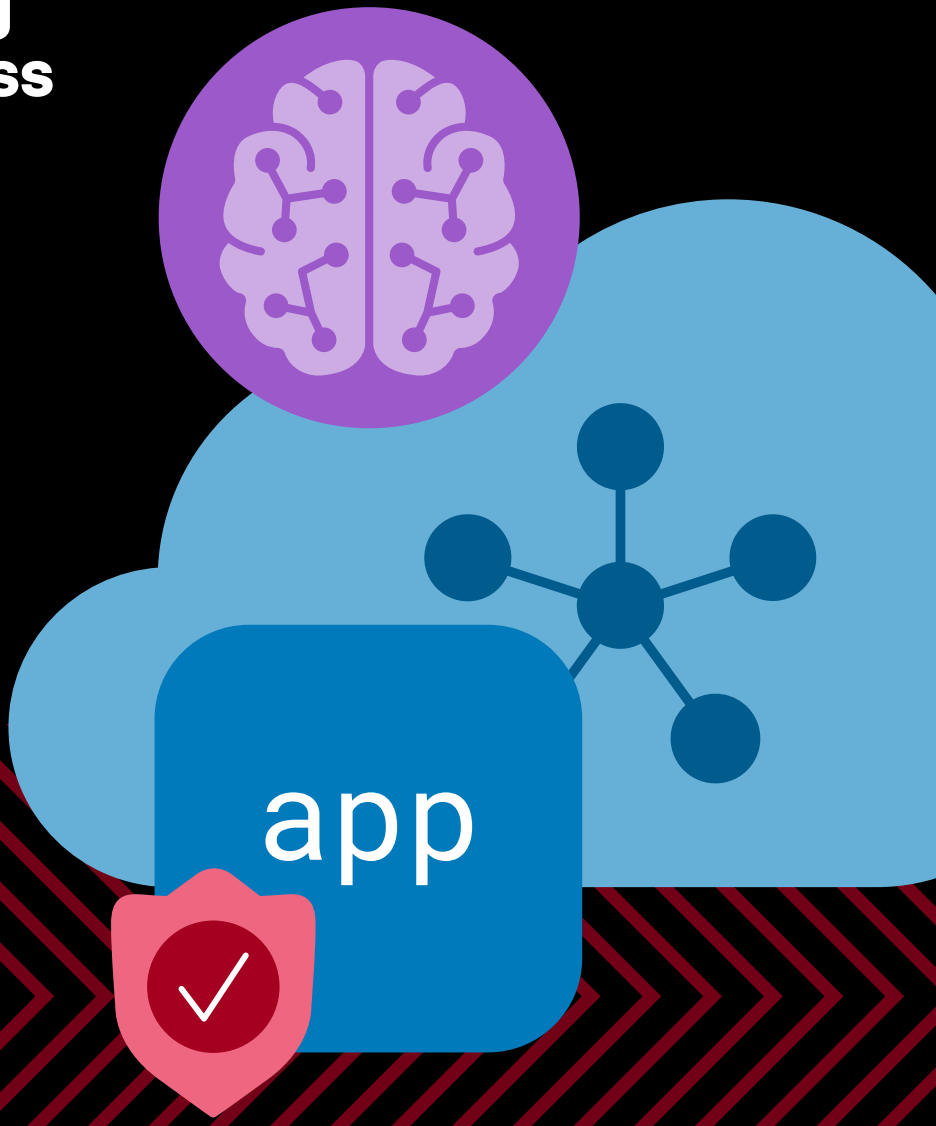
Hybrid deployment models will continue to dominate indefinitely as organizations optimize their AI and app deployments to react to constant change. Complexity is the tradeoff for agility—a price nearly everyone seems willing to accept. The frustrations that result may be alleviated with cross-environment, cloud-agnostic app delivery and security solutions that enforce consistent policies regardless of deployment model or hosting location.

Organizations that follow cloud-agnostic approaches cite benefits topped by application resiliency. Unforeseen downtime in one hosting environment, for instance, can be more easily mitigated when app delivery tools such as load balancing or performance optimizations apply equally anywhere the app is deployed. The ability to scale applications globally is the number 2 benefit, with comprehensive visibility ranking third.



Section 2:

App Delivery and Security Strategies Help AI Progress



Although hybrid complexity isn't going away, the results of our 2025 survey suggest that one way organizations are coping is by harnessing the telemetry and other capabilities of app delivery and security solutions.

For instance, data silos are falling. As telemetry and analytics become more advanced, they're providing richer, more comprehensive, and integrated data. This not only lowers the risk of bad decisions but will help enable AI.

Data issues are no longer the top barrier to AI

In 2024, 72% of organizations cited data issues as a barrier to AI adoption. Data quality, in particular, troubled 56%. Although data quality is still a challenge for 48% of respondents in 2025, it's no longer the highest hurdle. Most organizations (95%) say they're standardizing with observability tools such as OpenTelemetry, and more than one-third (38%) are consolidating data into a single data lake. The majority still maintain multiple data stores, but the percentage of organizations without any strategy for managing observability data has fallen to less than one in 10.

As a result of these advances, the most-cited AI barrier is now a lack of human skillsets. Nonetheless, as organizations harness and gain confidence in their data, they're empowered to shift decision making and execution into more automated processes (which can include those driven by AI).

In fact, rather than using operational telemetry primarily for analysis, alerting, or reporting, respondents in 2025 are using data first to drive automation—the top use case today. That's a marked shift from 2024, when nearly half of respondents (47%) were focused on telemetry primarily to drive operational alerts. Alerts and other use cases are still popular, with roughly half of respondents reporting current use of data for those purposes, too. But more have realized that effective automation can prevent the need for alerts by helping apps dynamically adapt in real time.

Automation Has Become the Top Telemetry Use Case
Percent of respondents using operational telemetry

We asked:
In what ways do you use, or plan to use, your operational data?

We learned:
Telemetry drives automation for two-thirds of organizations, and most of the remainder expect to soon join them.

As organizations harness operational data to gain actionable insights, monitor performance, and automate routine tasks, their confidence in automation is growing. Virtually every respondent (99%) reported feeling comfortable using AI not merely to support decision making but to automate at least one operational function.

Further, most organizations want AI to handle both strategic and operational tasks. For instance, nearly three-quarters (72%) are comfortable asking AI to optimize app performance—such as through traffic management—and more than half (59%) would support AI-driven cost optimization, such as decisions about where a given app can be most efficiently hosted. A similar 59% would rely on AI to mitigate zero-day vulnerabilities by automatically injecting security rules. Majorities also want to use generative AI to speed decision making, generate policies and configurations, accelerate other automation such as scripting, and even execute those scripts autonomously. AIOps is clearly the future.

For most organizations, that AIOps future has not yet arrived, but it's on the horizon. App delivery and security have long been among the least automated IT functions. Nonetheless, progress is occurring in stages, starting with human-driven automation such as with scripts. The most efficient organizations proceed to AI-driven execution—which, as we've reported in previous State of Application Strategy Reports, yields more benefits to those who can achieve it. Today, 45% of survey respondents automatically execute various functions across app delivery and security operations.

54% want generative AI to analyze app and API traffic

GenAI Expected to Act to Speed IT Operations

Percent of respondents selecting each task

We asked:
Which IT operational tasks would you like generative AI to assist with? Select all that apply.

We learned:
Majorities want generative AI to not only speed decisions but accelerate automation and act.

57%

Generation of scripts to deploy new or adjust existing configurations and policies

56%

Generation of policies, configurations, and custom functions

55%

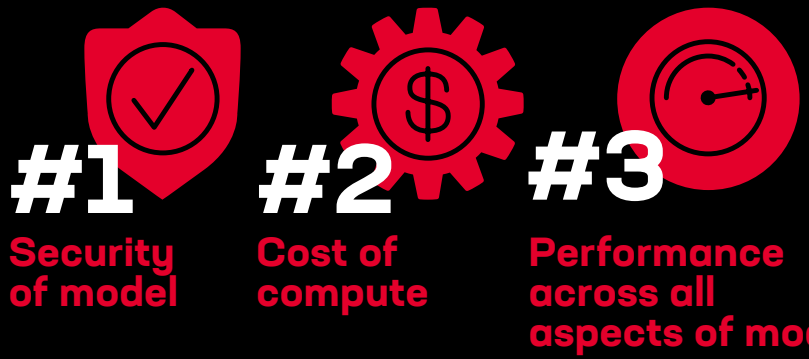
Executing scripts to deploy new or adjust existing configurations and policies

AI is expected to help more organizations make that transition, reducing the frequently manual nature of tasks related to app delivery and protection. When it comes to app delivery specifically, 54% of respondents say the most valuable use of generative AI will be exploring and analyzing app and API traffic. Automating policy adjustments to meet service level objectives (SLOs) is still important to many, but not as pressing.

In the realm of app security, on the other hand, attitudes are reversed. More than half of respondents (51%) prioritize using generative AI to automatically adjust security policies, workflows, and configurations to respond to threats or new vulnerabilities. Only one-third (34%) consider it more valuable to explore and analyze security data using natural language.

Speaking of security, the solutions that protect apps and AI models can both contribute to complexity and help solve it. With 96% of survey respondents deploying AI models, the security of those models tops the list of concerns. Security is equally an issue for the 95% of respondents who are also engaging in model training.

Security and Cost Remain Top AI Model Concerns

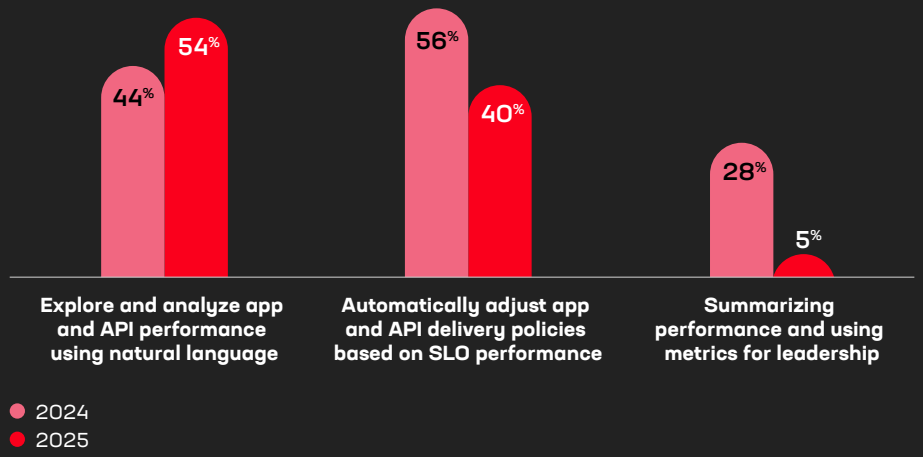


For App Delivery, GenAI Is Most Valued for Performance Analysis

Percent of respondents selecting each use case

We asked:
What use of generative AI is the most valuable for you with respect to application delivery? Select one.

We learned:
App and API performance analysis now outranks automated policy adjustments for more than half of respondents.



As organizations determine where to focus their security investments, they're prioritizing the security of AI models and apps, often because they directly interact with sensitive data. For instance, half of survey respondents are already using AI gateways. Another 40% expect to be using one within 12 months. A few organizations expect to take longer to deploy an AI gateway, but no one expects to go without one.

50% have deployed AI gateways

The top use case for these AI gateways is protecting and managing AI models. But more than half of respondents also expect their AI gateway to reduce complexity by providing a central point of visibility and control for protecting and managing both traffic and data.

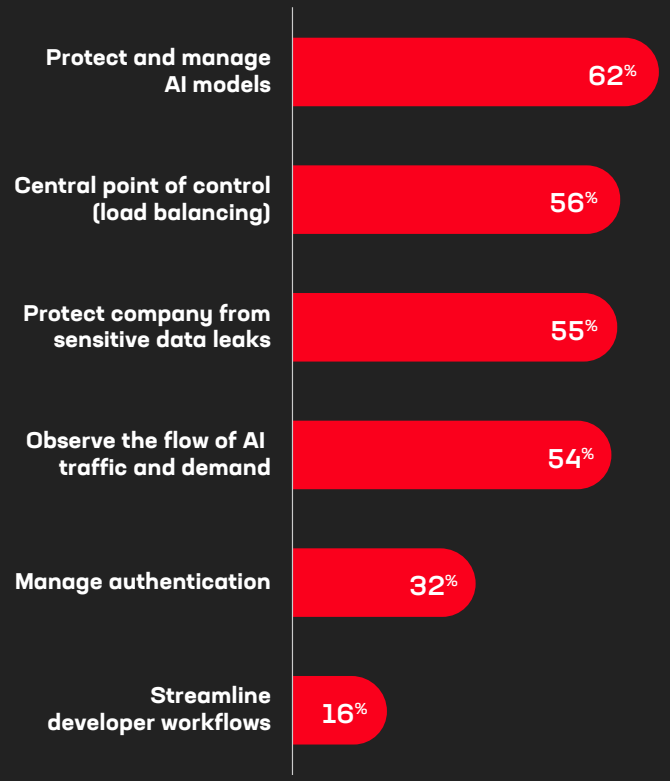
As useful as AI gateways may be, however, app and AI security need to be more comprehensive. For instance, microservices are perceived as less critical to protect than AI models and therefore receive less security investment. But as crucial components of modern apps, they act as gateways or functional intermediaries, and they're equally at risk.

AI Gateways Appeal for Multiple Uses

Percent of respondents selecting each use case

We asked:
How do you use or plan to use an AI gateway? Select all that apply.

We learned:
More than half of organizations hope to use AI gateways to manage both traffic and data.



58% call API sprawl a significant pain point

Similarly, API security needs more attention. More than two-thirds of organizations (68%) say they use APIs to manage app delivery and security. That makes APIs the dominant method, ahead of alternatives ranging from graphic user interfaces (GUIs) to third-party orchestration tools. Broader approaches to security that can provide more comprehensive protection to APIs, microservices, and AI models and apps at once can help correct a mismatch between security risks and priorities. The right solutions could also help reduce operational complexity.

Organizations appear to be recognizing this possibility. Services collectively known as web application and API protection (WAAP), such as bot and DDoS mitigation, are evolving into a key strategy for protecting AI models. Indeed, 91% of organizations plan to use at least one WAAP service to protect their AI models. That's up from 77% in 2024. API security, including API gateway deployment, is the top strategy today for protecting data as it traverses AI training models and applications. Other WAAP capabilities follow close behind.

WAAP Services Lead AI Model Protection

Percent of respondents selecting each service

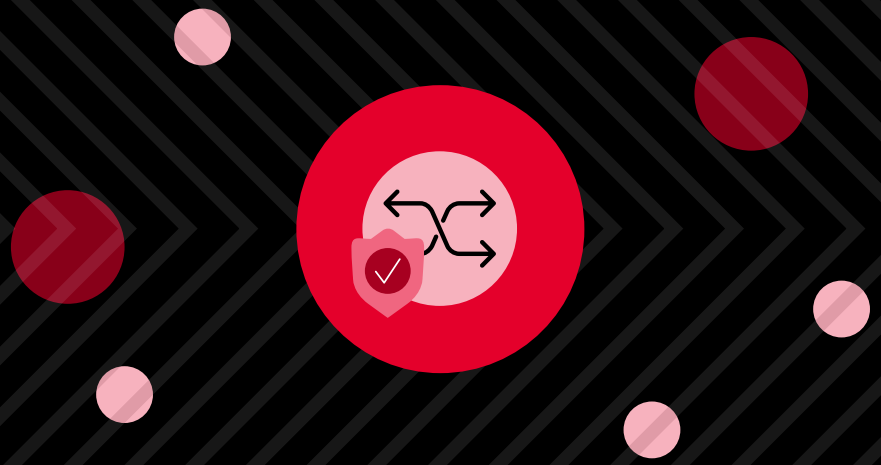
We asked:
Which of the following app security services are you using or planning to use specific to protecting the integrity of your AI/ML model? Select all that apply.

We learned:
API security solutions lead plans for AI model protection.

Regardless of the type of security solution implemented or what it's meant to protect, programmability of the solution is vital. More than two-thirds of survey respondents called programmability very or extremely important for more than 20 purposes related to both inbound and outbound traffic. Other F5 research suggests that for API security solutions in particular, programmability is viewed as the most important capability.

This valuation is driven, in part, by the uniqueness of each environment built from a diverse set of applications, infrastructures, networks, and platforms. No two environments are exactly alike, necessitating the need for bespoke solutions to solve problems, such as mitigating zero-day vulnerabilities and providing the breathing room operations need to patch systems and applications.

Programmability provides organizations with the ability to implement their scaling strategies, optimize resource consumption, and block attackers—all on demand. The ability of a digital business to take control of its own digital destiny through programmability is an advantage that most respondents appear unwilling to part with.

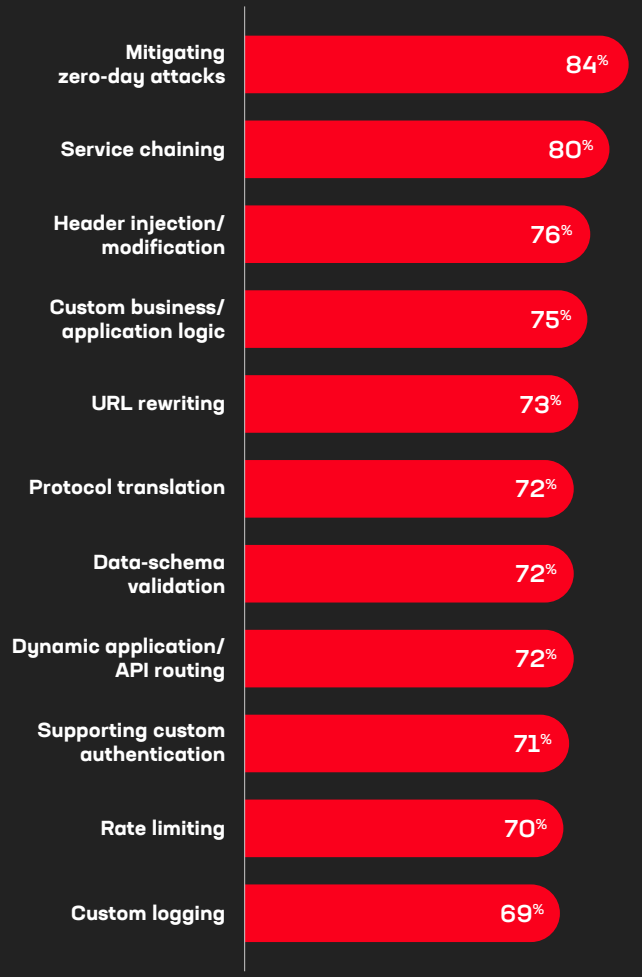


Data Path Programmability Is Vital Across Traffic Management Purposes

Percent of respondents identifying each aspect as very or extremely important

We asked:
Please rate the level of importance of the following aspects of being able to use a programming language to inspect, modify, and direct traffic–first for *outbound* traffic, then for *inbound* traffic.

We learned:
More than two-thirds of respondents consider programmability highly important for a wide variety of traffic inspection and management needs, with identical results for both inbound and outbound traffic.



F5 Insight

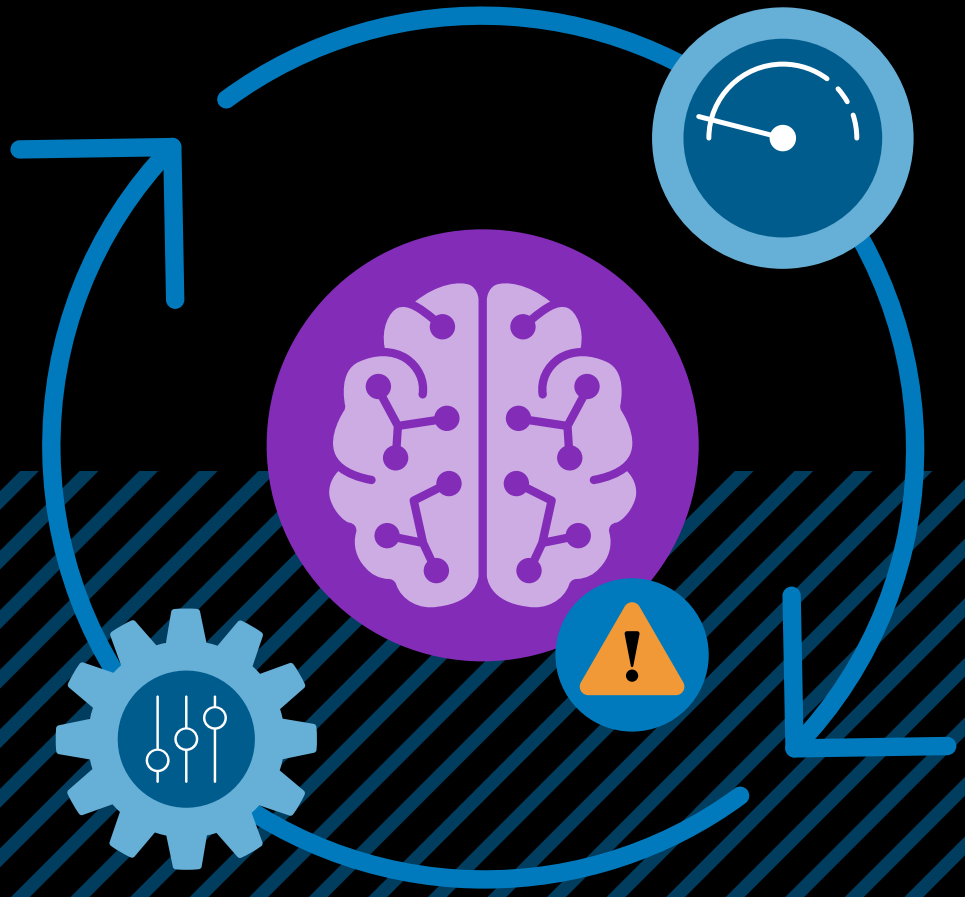
Growing data standardization helps solve some of today's complexity problems. Standardization also makes it easier to capture the insights required for AI-assisted app delivery and security policies. As confidence in organizational data and the ability of AI to effectively use it for automation both grow, organizations will begin to obtain measurable benefits. At that point, AI automation will naturally expand from isolated tasks to entire processes currently handled by IT staff through management consoles. We expect a steep adoption curve to reach a tipping point as early as 2026, with nine out of 10 organizations using AI-driven automation in their IT operations by 2035. Human intervention could become minimal, making traditional management consoles obsolete, as the most efficient and successful organizations use AIOps with natural language interfaces.

In the meantime, as organizations move to secure their AI models and apps, they can't leave microservices or APIs vulnerable. Attacks at those pressure points can disrupt AI apps just as effectively as threats to the model itself. What's known today as WAAP will likely evolve to embrace a greater remit, namely web app, API, and AI protection. Whether that's abbreviated WAAP or WAAAP, cloud-agnostic and programmable approaches protecting everything from microservices to machine learning models can deliver this more comprehensive protection while helping to solve complexity challenges.

Transcending point solutions and per-app (or per-API) security management is key, regardless of how automation progresses. Effectively turning AI back on itself to better manage security and performance will require broad visibility and control. More comprehensive protection and streamlined management are prerequisites for the advanced AI that will drive business success.

Section 3:

Traditional Operations Block AI Aspirations



While many organizations are solving challenges with data maturity and security on the way to AI assistance, the barriers that remain are significant. In 2025, acquiring the necessary skillsets rises highest among them. Worry about skillsets hasn't changed much over the past year. Meanwhile, concerns about costs, trust, and the ability to scale are growing.

60% are mired in manual tasks

However, our survey results indirectly reveal another staff-related barrier to AIOps or even more traditional automation: one-off, manual tasks that consume too much time. Today's modern architectures offer automation capabilities such as auto-scaling or dynamic policy updates. Unfortunately, few organizations can take advantage of those efficiencies. Instead, reliance on legacy processes and operational workflows buries 60% of respondents in time-sucking manual tasks.

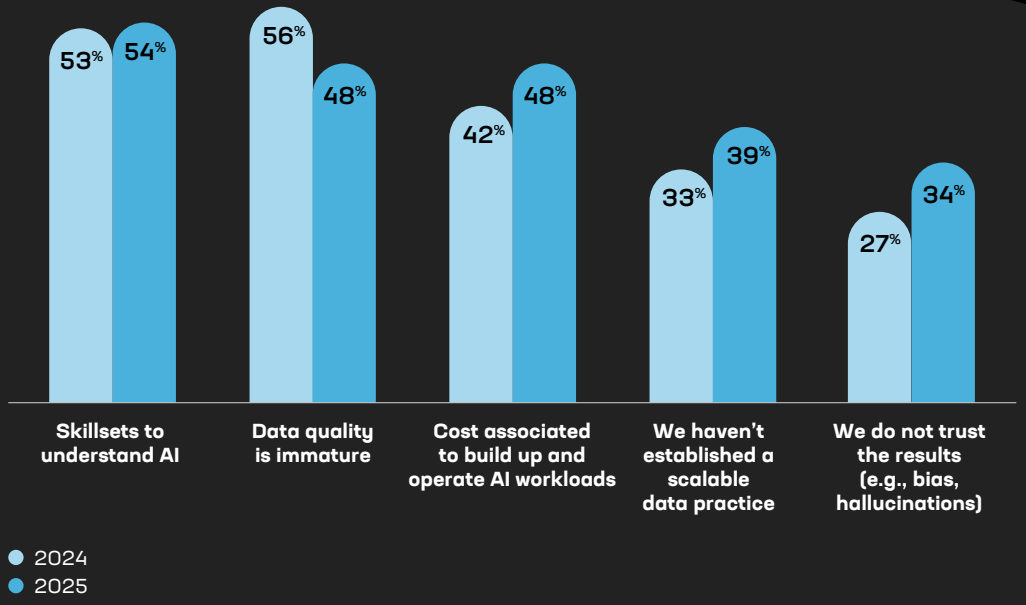
In addition, nearly one-quarter (23%) cited integration with ticketing or management systems as getting in the way of automating app delivery and security. Fragmentation of processes and integration points is increasing the need for manual intervention and slowing operations, making even agile methodologies too inefficient for IT operations today.

Human Skills Are the Biggest AI Blocker

Percent of respondents identifying each challenge

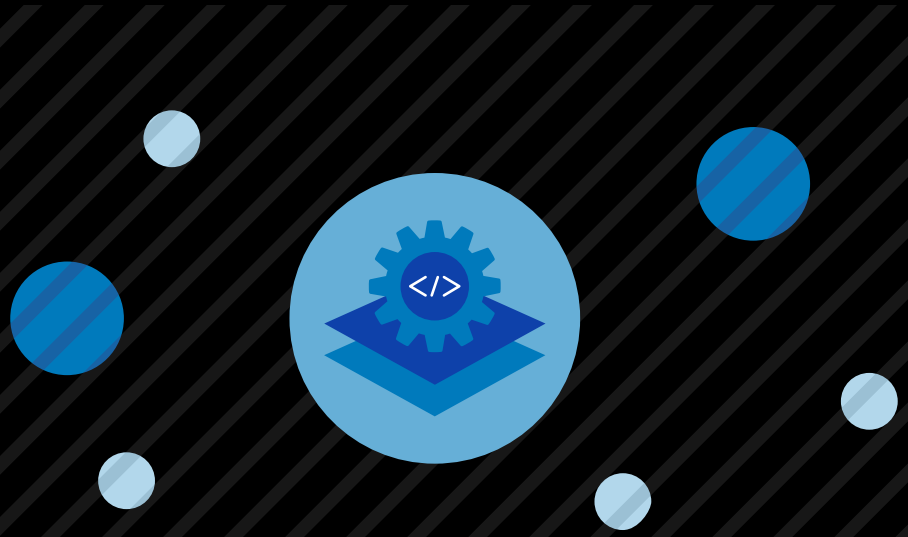
We asked:
Please select the top challenges standing in the way of using AI in your organization. Select all that apply.

We learned:
Data quality is no longer the top barrier to AI.



Even technologies that solve one problem contribute to another via fragmentation. For instance, more than half (58%) of organizations call APIs a significant pain point, whether in managing app delivery and security generally or multicloud environments more specifically. Respondents report spending up to half their time managing complex configurations involving myriad APIs and languages. In fact, working with vendor API complexity was named the single most time-consuming automation-related task by 31% of respondents. Another 29% complained about the time demanded by custom scripting.

These fragmentation challenges do more than slow operations and increase the risk of misconfiguration; they prevent the entire organization from moving as quickly as it might. Although modern deployment pipelines are designed for agility and speed, old approaches to app delivery and security—namely manual IT operations and approval processes—are slowing release cycles and minimizing some of the benefits of modern architectures. Organizations that can't modernize their operational processes along with their architectures can't expect to efficiently deliver and secure AI.

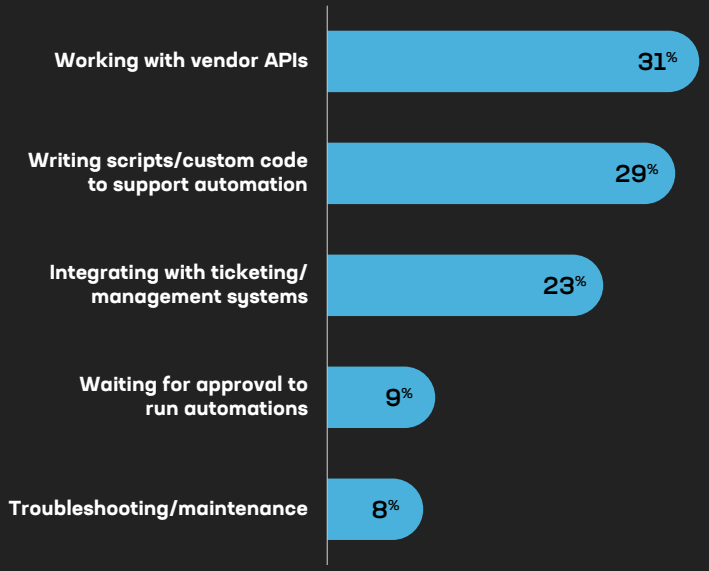


API Sprawl Hinders Automation

Percent of respondents identifying each task

We asked:
What is the most time-consuming task related to automation today? Select one.

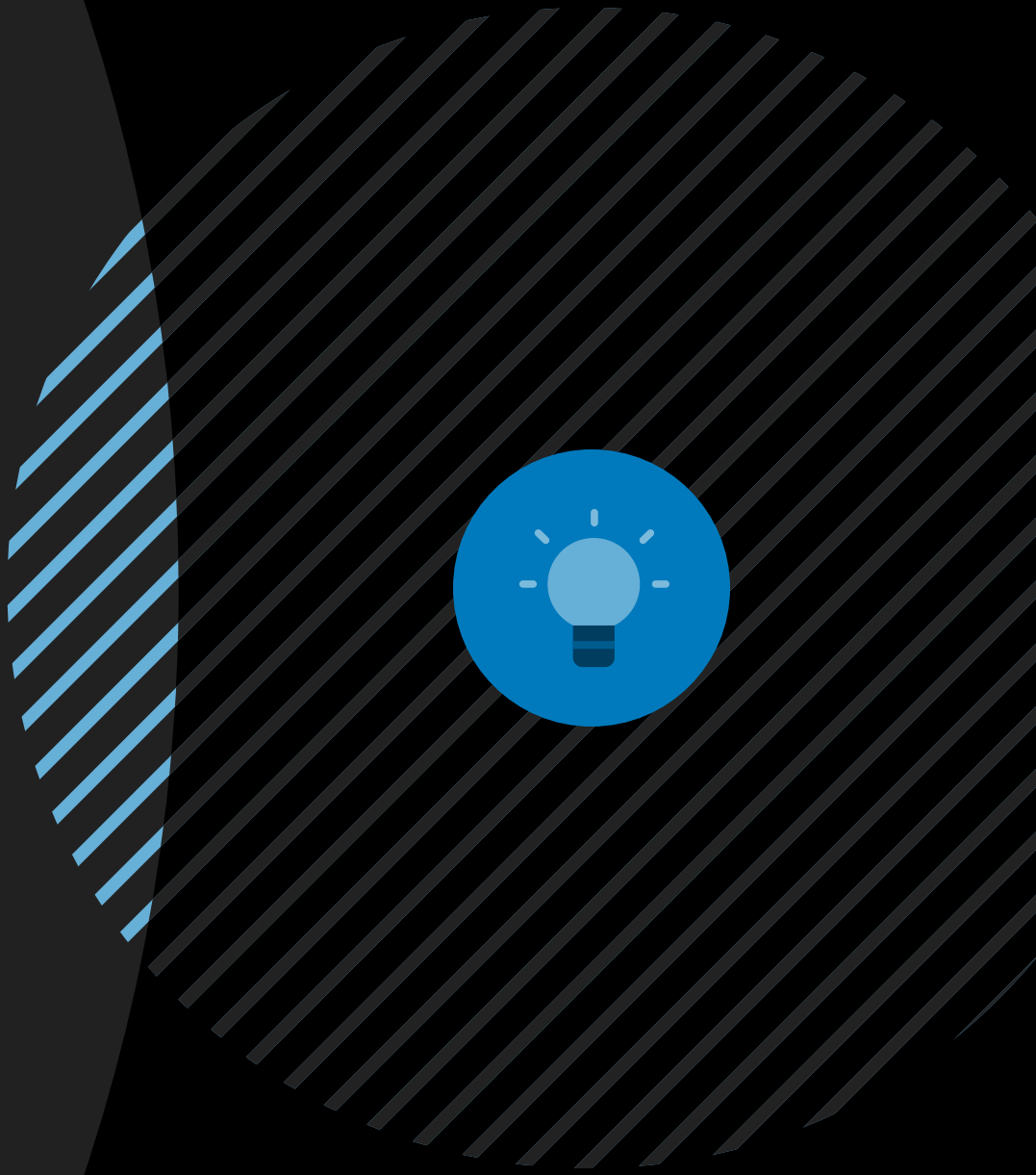
We learned:
Respondents struggle most with myriad APIs. Scriptwriting and manual systems aren't far behind.



F5 Insight

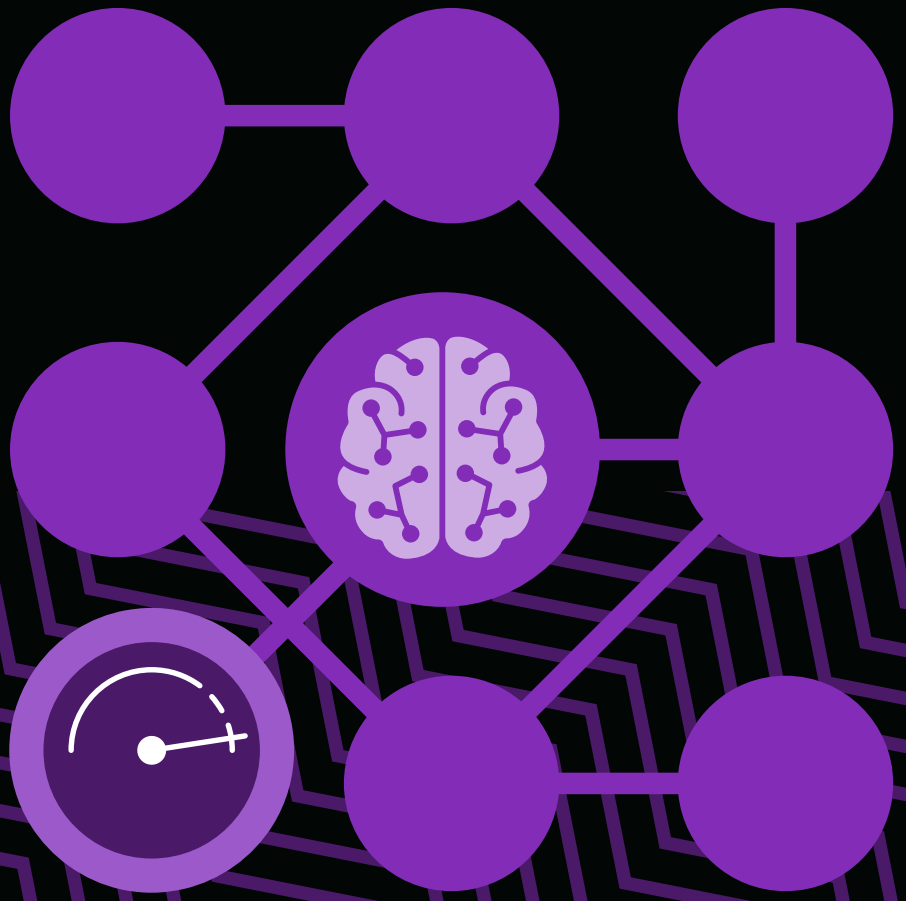
Manual and fragmented IT operations limit the benefits of advanced architectures and AI-powered apps. To rise above mediocrity, organizations need to focus on those operations as an additional source of complexity that needs simplification and standardization. Streamlining APIs, technologies, and tasks across tiers will be critical to take full advantage of AI, including AIOps.

Fortunately, AI systems are well-suited to handle the complexity of APIs without manual intervention. When based on sound data practices, AI can generate and deploy effective app security and delivery policies, helping to solve workflow complexity issues. Programmable app security and delivery solutions—especially those that can serve any app, regardless of deployment model or architecture tier—can help by reducing fragmentation and simplifying processes to enhance deployment efficiency. Better and more comprehensive orchestration tools can streamline process complexity and accelerate the organizations that use them into leadership positions.



Conclusion:

Tame Process and API Complexity to Unleash AI

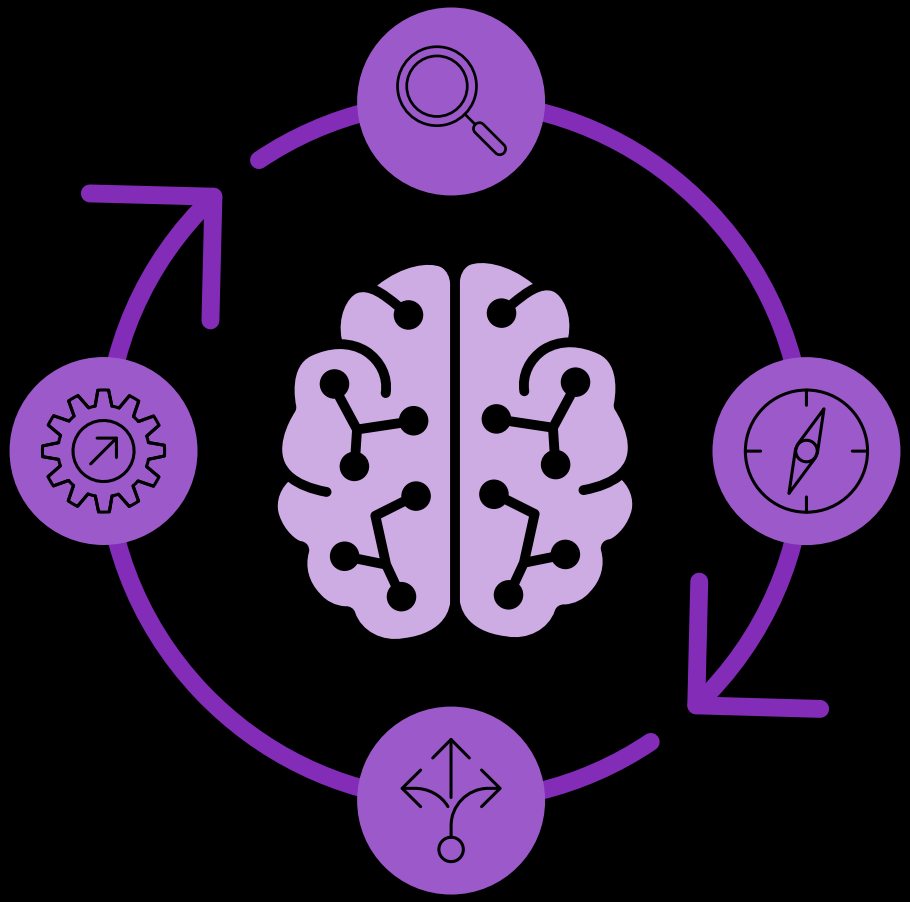


AI/ML implementations continue to gather momentum as organizations take advantage of maturing data strategies and more integrated telemetry to enhance everything from personalized purchase recommendations to the behavior analysis that can distinguish a legitimate user from a sophisticated but malicious bot. The complexity of the current app deployment landscape will continue to grow, since AI apps and integrated, high-performance digital experiences rely heavily on APIs, modern apps, and hybrid deployment models.

In this miasma of complexity, traditional approaches to IT management will slow progress and limit the agility needed to effectively respond to rapidly shifting customer demands and competitive threats. Survey respondents want to automatically generate, deploy, and update app delivery and security policies, with AI not only assisting but orchestrating that work. But many organizations still struggle with operational and process inefficiencies that hinder the use of AI and even human-driven automation in their operational workflows. In effect, they're unable to use AI as much as they'd like in the business because they're unable to use AI in their IT operations.

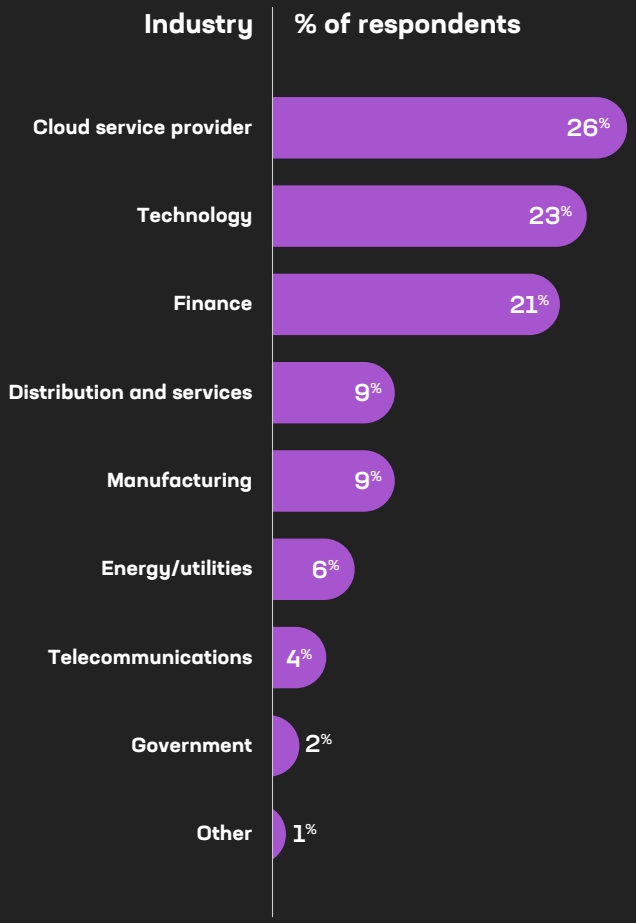
Their challenges can be solved by moving toward AI-powered decision processes that rely on observability, APIs, and automation to power ongoing innovation in Observe, Orient, Decide, Act (OODA) loops. That process transition can be accelerated by streamlining APIs, languages, tools, and the vendors who supply them. In particular, management and security platforms that tame API complexity can remove one of the biggest barriers to increased efficiency. We expect management consoles to eventually become obsolete, but in the meantime, the right orchestration platforms can transcend complexity to deliver cloud-agnostic and AI-ready services and security for both AI models and all the apps that will rely on them.

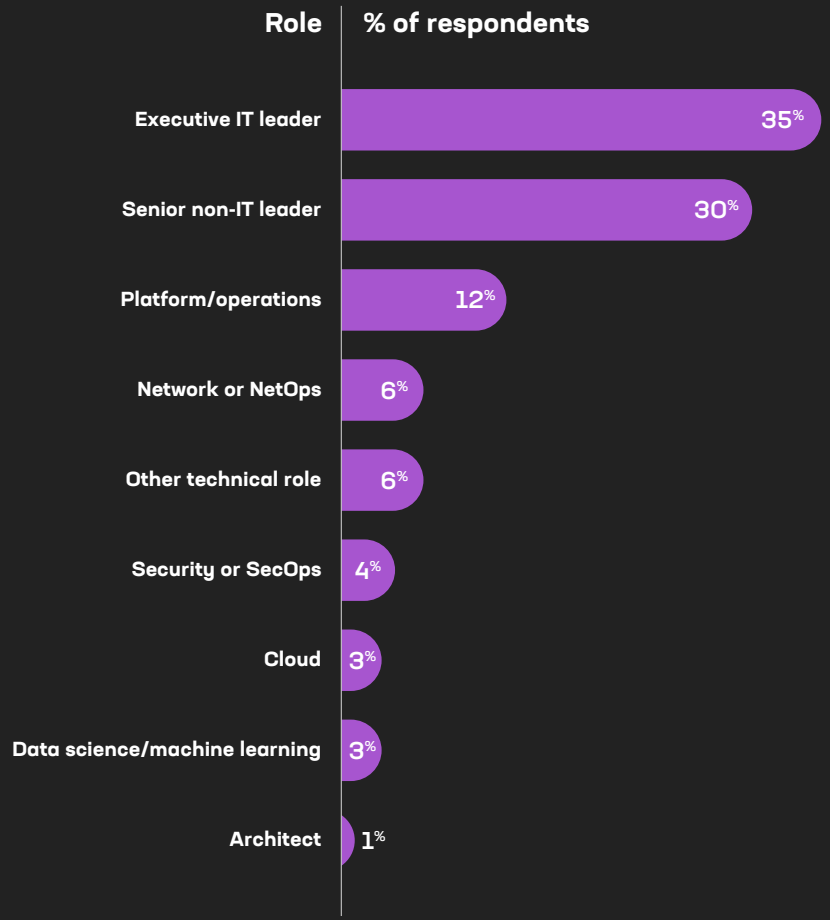
Companies that deploy such comprehensive—and programmable—tools for real-time traffic and performance management, app behavior modification, and ecosystem support will be best positioned to meet customer and business efficiency demands and deliver the dynamic digital experiences that build customer loyalty and drive financial success.



About the Report

Approximately 650 IT decision makers from around the globe completed the 2025 State of Application Strategy survey, our eleventh annual. They represent organizations of all sizes, from those generating less than $200 million USD in annual revenue to a significant number of companies generating more than $1 billion annually. Nearly two-thirds of respondents (65%) hold executive or senior leadership roles. The technology, cloud, and financial services industries were particularly well represented, but a wide variety of other sectors also contributed.





ABOUT F5

F5 is a multicloud application delivery and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure every app—on premises, in the cloud, or at the edge. F5 enables businesses to continuously stay ahead of threats while delivering exceptional, secure digital experiences for their customers. For more information, go to f5.com. (NASDAQ: FFIV)