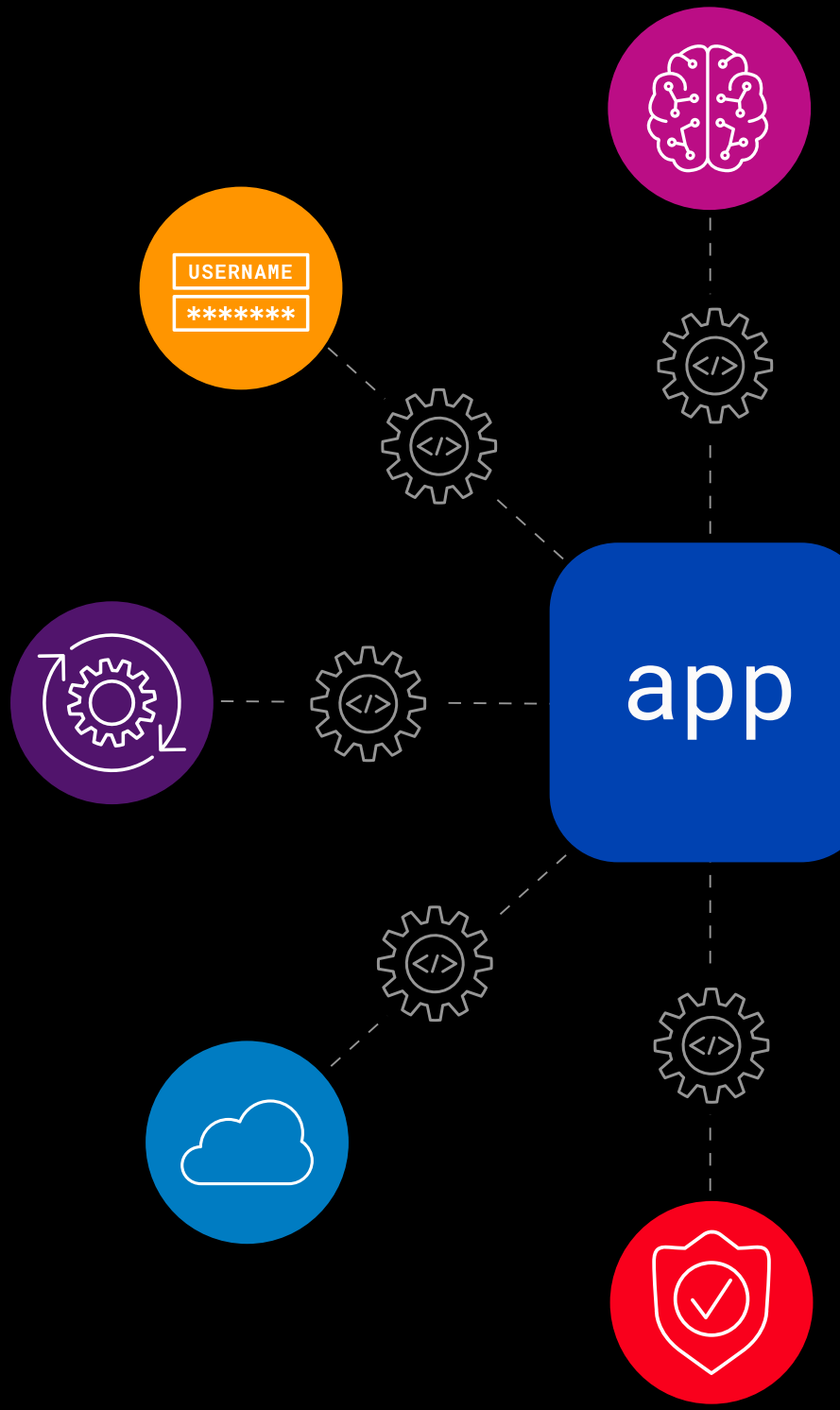
2024 State of Application Strategy Report

10 years of insights



Contents

Introduction

Digital Evolution Enters a New Stage

IT decision makers today face an abundance of choices for how to deliver and manage their apps to create great digital experiences, capture fresh revenue streams, and unlock new opportunities or business models. The options range from various app architectures to a profusion of deployment alternatives, APIs, security technologies, tools, and uses for telemetry, including artificial intelligence (AI).

In fact, exploding use of AI—as revealed by the results of our tenth annual State of Application Strategy survey—is powering this evolution. Increasingly mature AI and machine learning (ML) deployments will require even more new approaches and technologies for application and API security, delivery, connectivity, and management.

The pace of change may feel daunting, and many IT leaders long for greater simplicity. But while the diversity of choices creates complexity and management headaches, it also brings significant benefits, agility high among them. This tension between complexity and flexibility is driving today's hottest trends, from microservices and multicloud networking to interest in generative AI.

Fortunately, solutions for the toughest challenges are emerging. A decade of survey results provides a solid foundation for drawing conclusions and plotting wise paths forward. This 2024 State of Application Strategy Report captures the top areas of focus, biggest concerns, and best hopes of organizations around the world that are successfully leveraging digital services to thrive in our app-centric economy today—and lead innovation tomorrow. IT decision makers at all levels can use these insights to better position their teams for a bright future that involves less stress and more satisfaction for customers and the business.

How this report can help your organization:

The information to follow can help IT leaders:

- Assess how well your organization is positioned for challenges to come.
- Prioritize projects and practices most likely to yield strategic benefits.
- Equip decision makers with context and data for competitive decisions.
- Plan for the emerging technologies and trends likely to play significant roles in driving future innovation.

Summary of Key Findings

APIs Rise over Apps

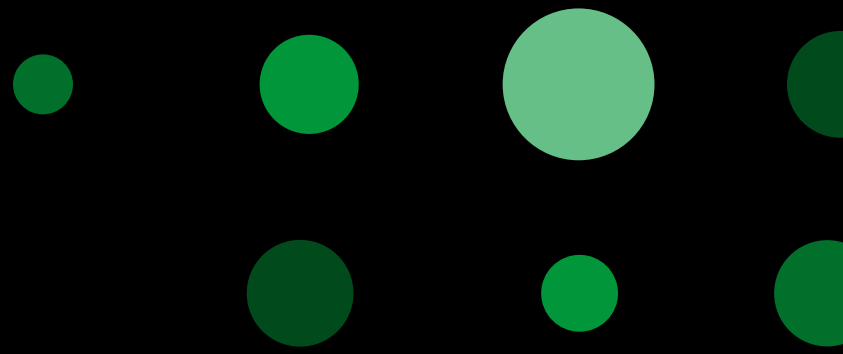
- Digital transformation is driving an explosion of APIs even as the average number of applications decreases.
- 41% of organizations manage at least as many APIs as apps, and API numbers will continue to increase as AI implementations move forward.
- The proliferation of APIs is driving changes in security practices.
  - 95% of organizations have deployed an API gateway, a dramatic rise from 2019 when only 35% had done so.
  - Organizations are almost twice as likely to have automated their app and API security (43%) as their app delivery (25%).
  - API security is the top security service expected to protect the integrity of AI/ML models and services.

Hybrid, Multicloud Operations Are the New Normal

- Case-by-case app considerations continue to drive multicloud deployments.
- Organizations plan to deploy AI engines (development, training, inference) and AI apps both in public cloud and on-premises environments, solidifying hybrid, multicloud operations as the norm.
- The resulting complexity continues to challenge nearly everyone.
  - The benefits of flexibility and business resilience make overcoming the challenges worthwhile.
  - Secure multicloud networking—named the number 3 most exciting trend for the second year in a row—is a key solution for the daunting complexity of multicloud operations.

Use of App Delivery and Security Technologies Has Exploded

- The average overall deployment rate has jumped from 57% in 2020 to 93% in 2024.
- Security technologies continue as the most indispensable.
  - Security as a Service (SECaaS) use is on the rise because it delivers speed.
  - Visibility is converging with speed as interdependent factors in app protection.



Digital Transformation Has Progressed Rapidly to AI-Assisted Business

- Three-quarters of organizations are working in the latter stages of digital transformation, namely digital expansion (which focuses on modernization) and AI-assisted business (which focuses on data analysis).
- The percentage of modern apps in the average portfolio has overtaken that of traditional apps a year sooner than we predicted.
    - The accompanying growth in microservices prompted respondents to call microservices networking the most exciting technology in 2024.
- Two-thirds of organizations say they're benefitting from digital transformation, with greater IT operational efficiency the top achievement.
    - Employee productivity has leapt forward in the ranking of benefits achieved.
    - The full potential of transformation—including better alignment between the business and IT—remains to be captured.

AI Will Help Solve Complexity Through Increased Automation

- Generative AI is the year's most exciting trend.
    - For both app delivery and app security, automation is the top use for generative AI as a means to faster responses and greater efficacy.
    - Automation is also the top use case for telemetry.
    - Nearly half of organizations plan to locate AI workloads in the public cloud, but significant percentages have other plans.

2015-2024

A Decade at a Glance

App security

In 2015, availability services were the most valued app security technologies. In 2024, security technologies reign supreme.

Use of app delivery and security technologies

Deployment rose from 11 separate technologies per organization in 2016 to 30, on average, in 2024.

Identity federation

Deployment of this app services technology rose from 35% of organizations using it in 2016 to 91% in 2024.

Private clouds

2015's top trend became 2024's second biggest regret. Although this may stem from early management challenges, other survey data suggest it's not that respondents are sorry they adopted private clouds—rather, they wish they'd done so even sooner.

APIs

In 2015, 69% of respondents considered them important or very important. Today, they're so important that 41% of organizations manage more APIs than apps.

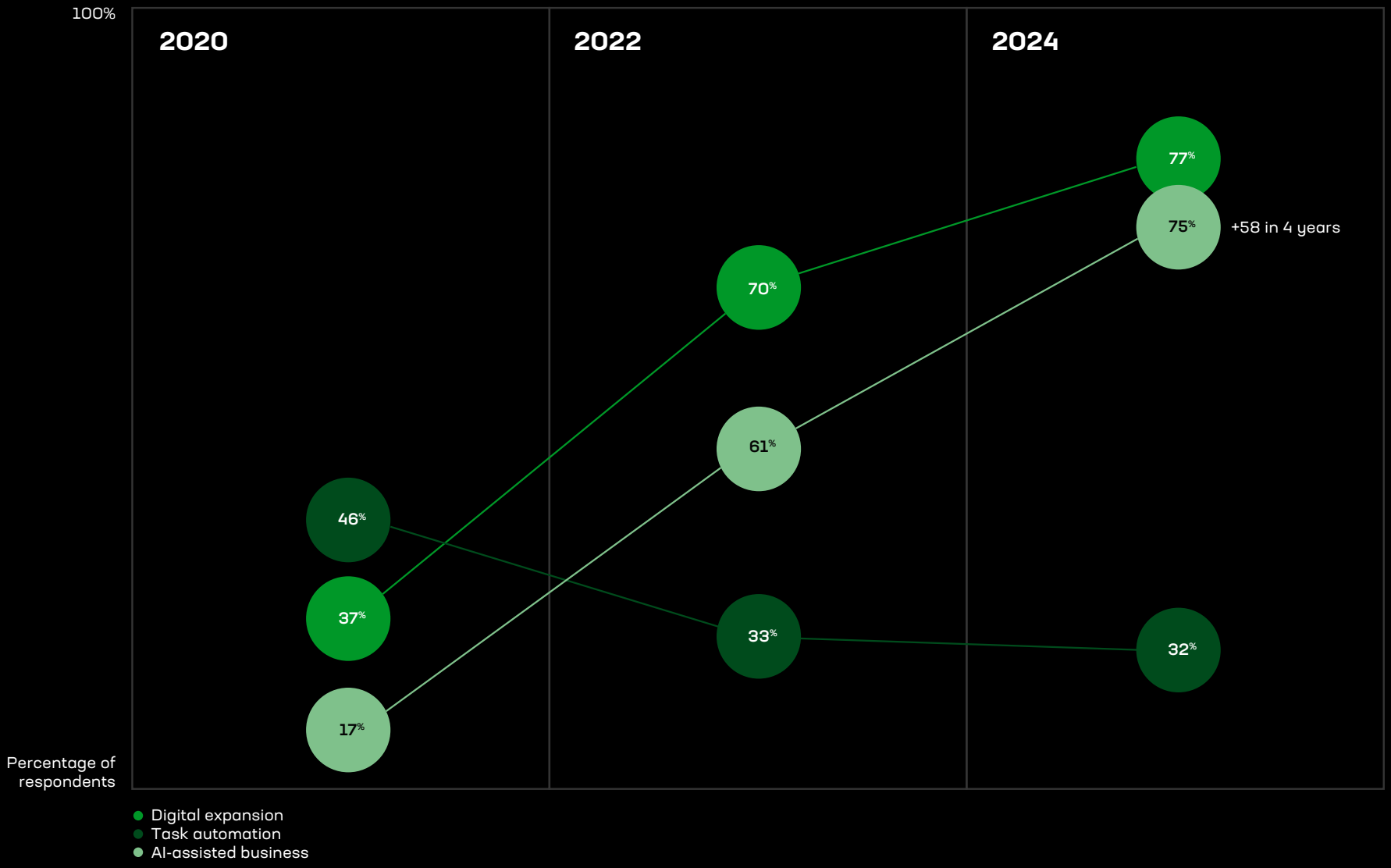
Hybrid everything

Hybrid app deployment models were relatively new in 2015. Today app architectures, app environments, IT stacks, and deployment models are typically hybrid, too.

Digital transformation

Our reports first mentioned digital transformation in 2017 in the context of economic pressure to shift to digital business models. With the COVID-19 pandemic as an accelerant, the subsequent years saw dramatic changes in IT project focus, priorities, and ways of working.

Organizations Have Rapidly Advanced on Their Digital Transformation Journeys



A Few Regrets

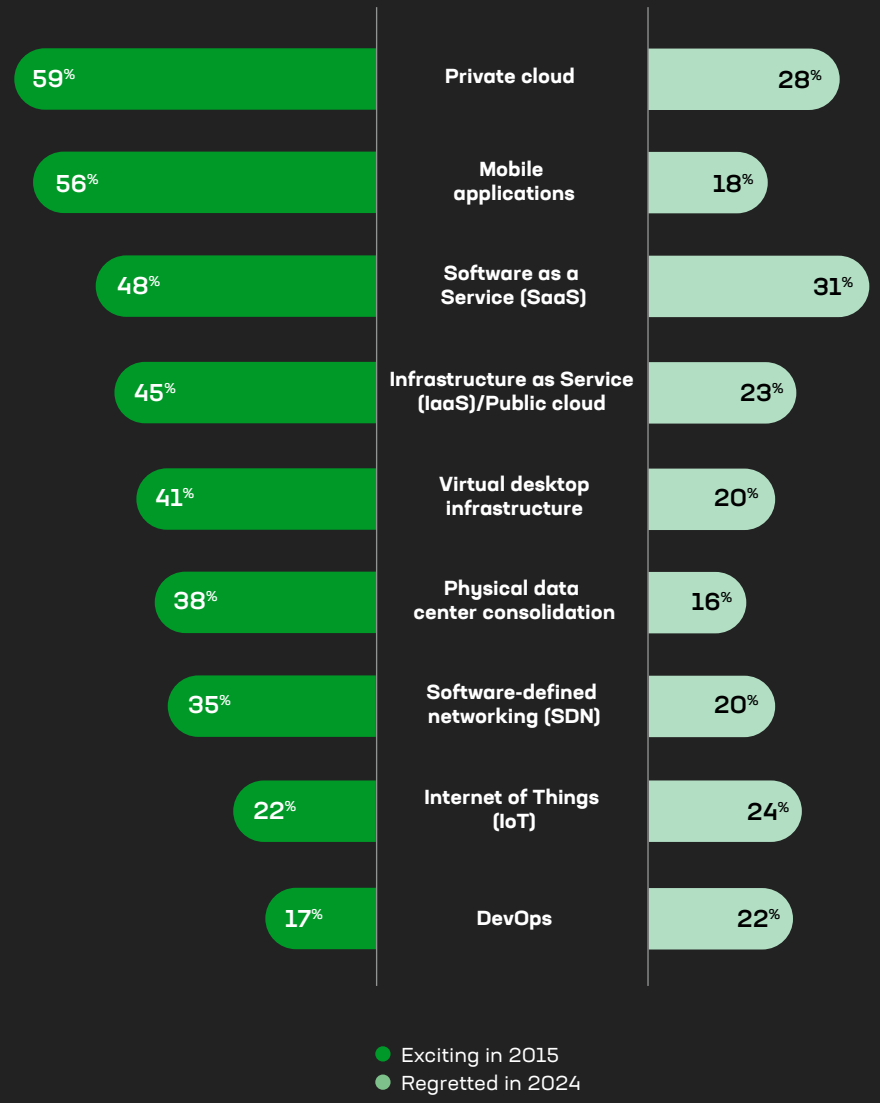
When change is this rapid, it's natural to regret a few of the top trends from a decade ago:

- The Software as a Service (SaaS) trend is regretted by nearly one-third of respondents, who perhaps lost control amid "shadow IT" created by SaaS use beyond the IT team's knowledge. Of course, a majority of organizations still find that the right SaaS delivers affordable innovation without the hassle of planned upgrade cycles.
- More than one-quarter regret the private cloud trend—the most strategically important in 2015. Although private cloud technologies were initially immature, research into other survey results suggests respondents are primarily sorry they didn't deploy private clouds *sooner*.
- For all the previous noise about the Internet of Things (IoT), nearly a quarter of respondents—and nearly half of those in telecommunications—regretted it. We suspect their sorrow is a result of projects with poorly defined value propositions—such as "smart" hairbrushes or dishwashers that can be started from a mobile phone.
- Ten years ago, nearly half of respondents looked to Infrastructure as a Service (IaaS) as a cost-reduction measure. Today, public cloud cost savings, if they materialize, don't always make up for increased management complexity or the challenges of adopting native toolsets. That's why regrets continue to drive repatriation.

Looking Ahead

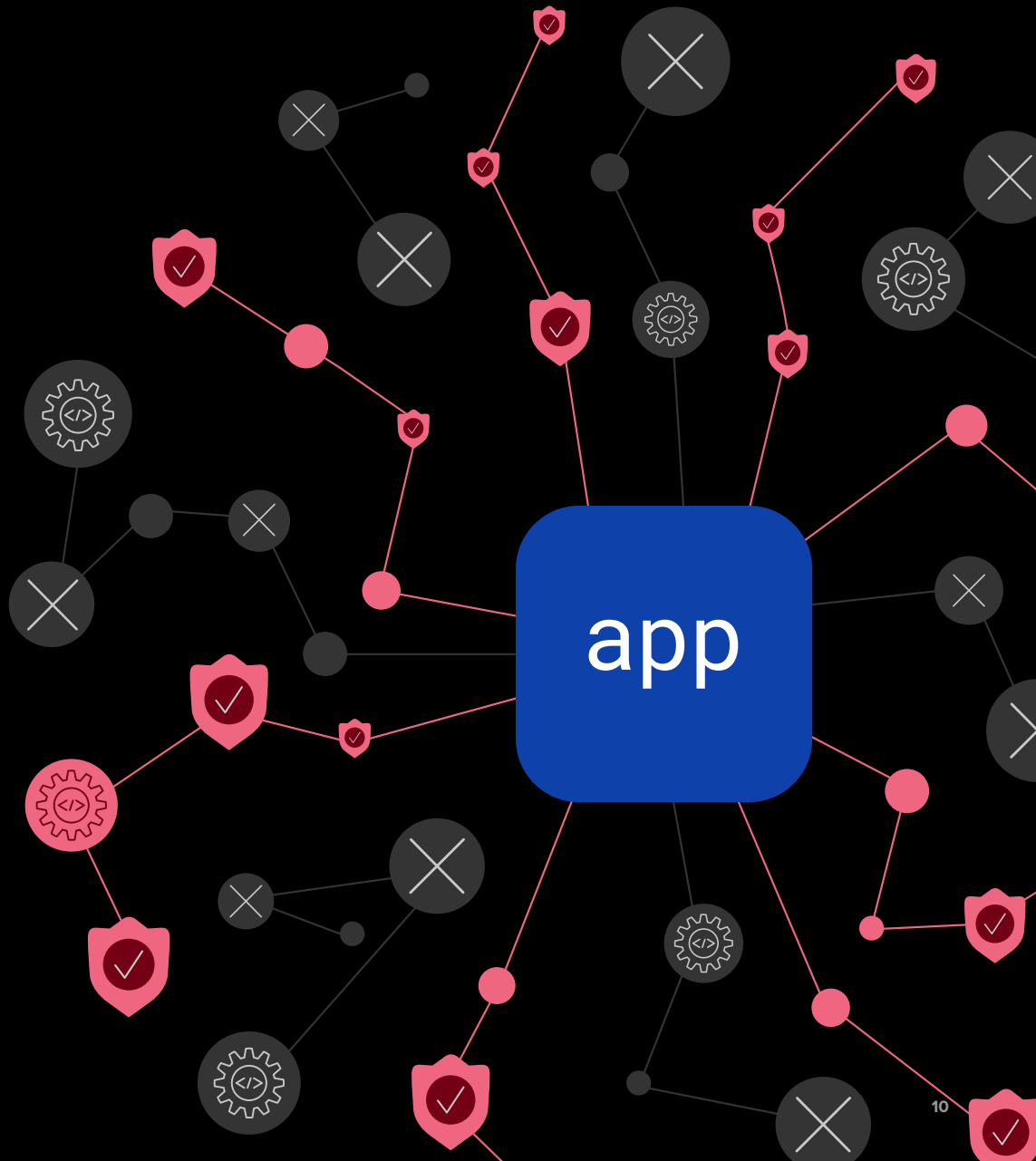
The good news is that one of every five respondents has no regrets. Those in energy and healthcare were most likely to regret nothing. And frankly, the pace of change today doesn't afford much time to reminisce. So let's look ahead! Keep reading for a detailed view of the State of Application Strategy in 2024 and what to expect in the years to come.

Top 2015 Trends Have Become Top 2024 Regrets



Key Finding 1

APIs Rise over Apps



The digital economy runs on applications, which is why apps have been a key target of IT modernization—whether that means replacing them with cloud-native alternatives, lift-and-shift cloud migrations, or the addition of modern components such as APIs. Thanks to those efforts over the past several years, we've reached a milestone: The average enterprise app portfolio today includes more modern than traditional (monolithic) apps.

This watershed happened a year sooner than F5 predicted in 2023, and we still expect the percentage of modern apps to reach 60% by 2025. The largest organizations (by revenue), which are generally farther along in their digital journeys, are already there. Modern apps represent an average of 65% of the portfolio for those organizations.

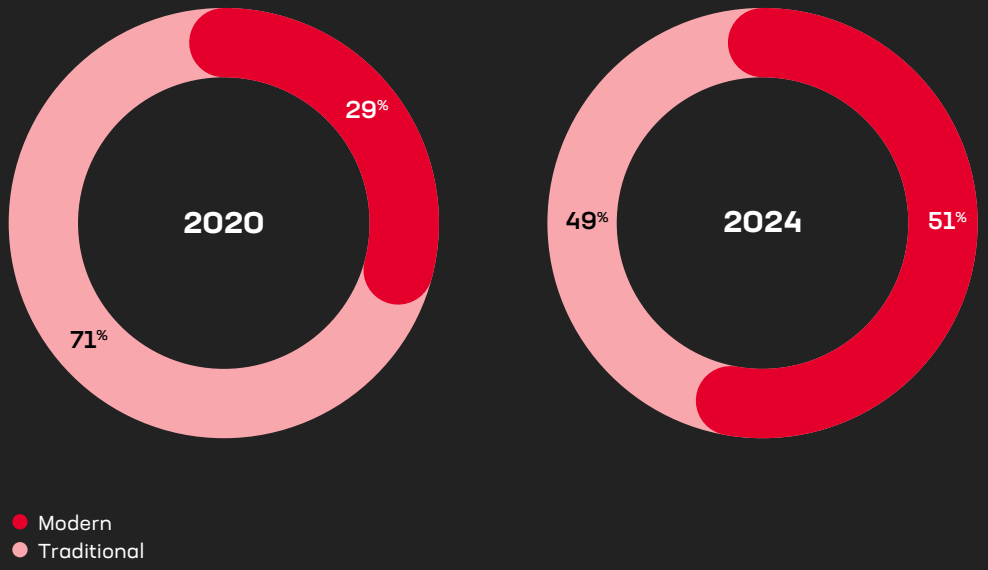
As they modernize, organizations typically retire (or combine the functions of) legacy apps, which has helped consolidate app portfolios in recent years. The average number of apps in the enterprise portfolio has declined. But that drop hasn't necessarily reduced the number of app instances, and it also doesn't mean the remaining apps are easier to manage. Modern, mobile, and cloud-native apps that deliver digital services are often composed of microservices and rely on APIs for orchestration and exchange of data. In addition, modern interfaces used to modernize traditional apps are often deployed in cloud and edge environments, adding to the complexity challenges.

The Balance Has Tipped to Modern Apps

We asked:
Of all your applications deployed today, roughly what percentage fit into the following categories?
(Results are averaged across all respondents.)

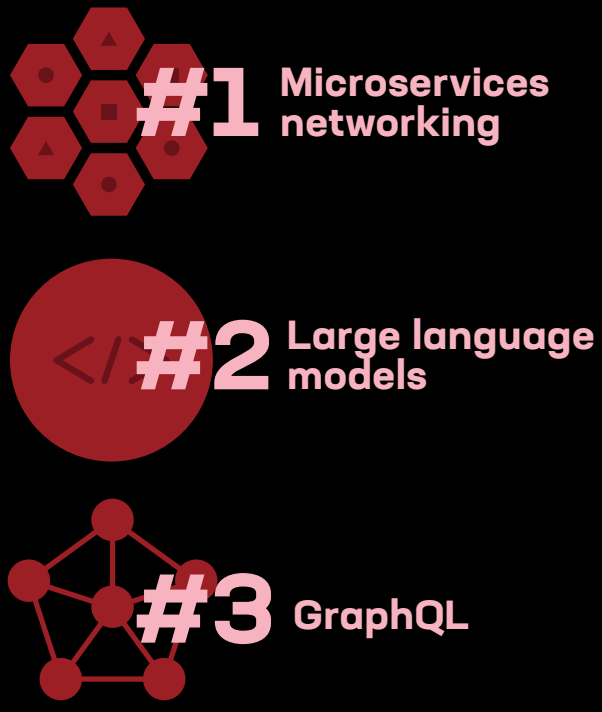
We learned:
The rate of modern app growth is accelerating.

F5 Insight:
The proportion of modern apps is likely to top out near 85%, probably before the end of the decade. The remaining minority will be traditional apps deemed too fundamental to replace. Instead, organizations will surround those old-timers with modern interfaces.



With more modern apps and microservices on the way, it's no wonder that microservices networking was named today's most exciting technology trend. Microservices networking, including ingress controllers and service meshes, connects container-based microservices in both north-south and east-west directions. This helps to ensure reliable communication between them while keeping them secure and observable. Although several other exciting technologies are likely to help with AI deployments, AI implementations at scale are still to come for many organizations. On the other hand, containerized apps are already in heavy use, which may be why microservices networking topped the list as a more immediate hope.

Most Exciting Technology



APIs Have Grown Exponentially

The explosive growth in modern apps and their microservices has created an exponential rise in the number of APIs, too. First, the addition of a layer of APIs has been a preferred method of modernizing apps for several years running. In addition, digital transformation tends to consolidate applications but increase the use of APIs as processes are automated, individual apps are integrated, and siloed business data converge into one source of truth. Increased use of AI also means more APIs. Because AI apps are frequently based on multiple APIs, further deployment will create an even greater flood of public APIs. The result has ushered in a new era in which APIs can be as critical to the business as apps themselves—and even harder to protect, monitor, and manage.

In fact, our survey results reveal that the average number of APIs an organization manages increases by five percent with each successive phase of digital transformation. (See Key Finding 4 for more about these phases.) Just as the largest organizations typically have the biggest share of modern apps, their API numbers are expansive, too. On average, companies with over $10 billion USD in annual revenue say they manage more than 1,000 apps and nearly 1,400 APIs—although a handful of behemoths report managing more than 10,000 APIs!

41% manage at least as many APIs as they do apps

But even the smallest organizations are dealing with an API flood. Today, 90% of survey respondents manage fewer than 200 apps, and that number tends to decrease as digital transformation proceeds. Meanwhile, API counts only go up. More than one-third of respondents (41%) manage at least as many APIs as apps.

API security is a particular concern. An individual API can have dozens or hundreds of endpoints, which serve as critical gateways to apps and their valuable data. All endpoints must be secured to protect app integrity, customers, and the business.

To help manage the resulting security nightmare, more than one-third of organizations (43%) have automated their app and API security infrastructures. Nearly everyone (95%) has deployed API gateways to help simplify API management and better guard their security.

API gateways offer a valuable layer of protection by authenticating API calls, ensuring valid requests, and rate limiting to guard against being flooded with attacks. In general, the more APIs an organization deals with, the more its decision makers value API gateways. Overall, 91% consider them very important or critical.

95% use API gateways

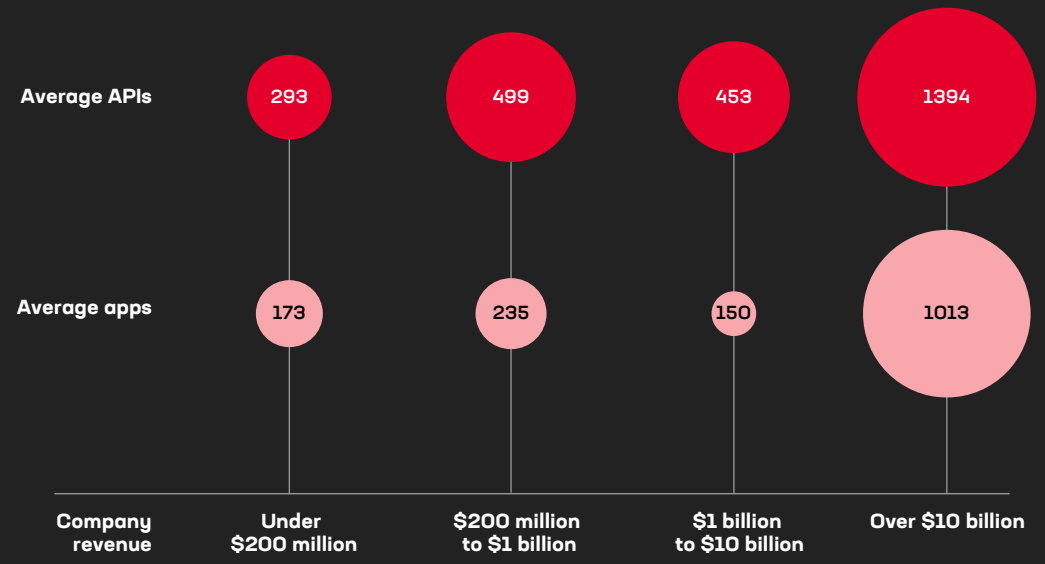
Protecting APIs is particularly important for the majority of organizations eagerly pursuing AI assistance. Survey respondents are looking to API security as their number one protective technology for AI/ML models and services. Any organization hoping to make strategic use of AI would be wise to follow suit.

APIs Proliferate

We asked:
Estimate the number of applications that are currently deployed in your company; Estimate the number of APIs that are currently deployed in your company; What is your company's approximate annual revenue?

We learned:
On average, deployed APIs significantly outnumber apps, and the ratio of APIs to apps tends to increase with company size.

F5 Insight:
Large organizations—and those wanting to get larger—can expect API proliferation to continue and can't afford to lose track of them.



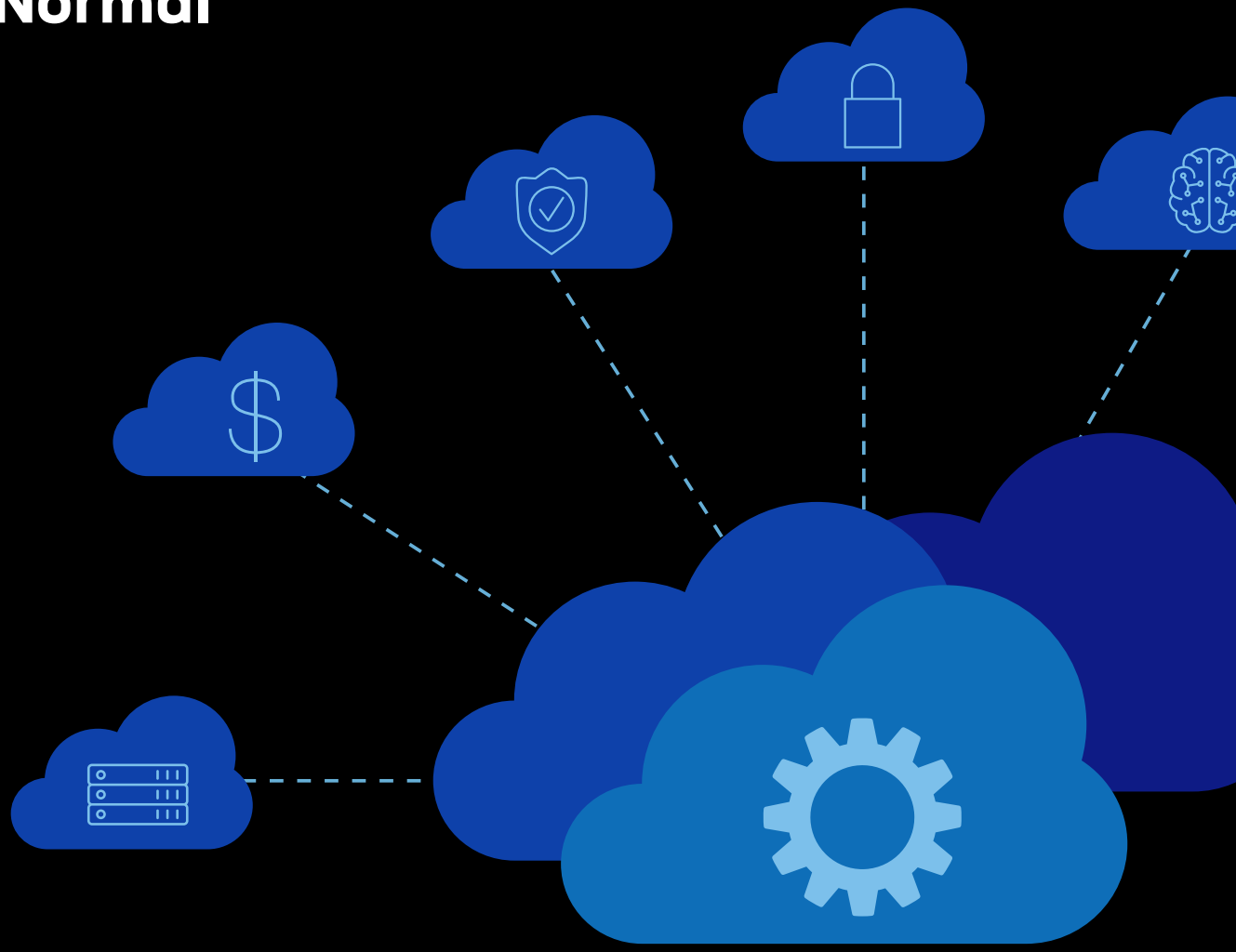
F5 Insight

The percentage of modern apps—and therefore the number of APIs—in the average enterprise portfolio will continue to grow. This growth will accelerate as organizations adopt AI, which relies heavily on modern apps and infrastructure to operate and scale. The growth in modern apps and their tendency to be distributed (thus increasing complexity) make the excitement over microservices networking completely understandable.

At the same time, the ongoing increase in APIs will make API-related security and management solutions imperative as APIs, apps, and the data they exchange become ever more strategic to the business. Individual technologies such as API gateways won't be enough. Automating the app and API security infrastructure can help, but automation rates in this IT domain are still below 50%. The best-protected and most efficient organizations will deploy comprehensive strategies for discovering, testing, managing, and protecting their APIs.

Key Finding 2

Hybrid, Multicloud Operations Are the New Normal



Whether modern or traditional, today's apps and the APIs that accompany them are overwhelmingly being deployed into a hybrid, multicloud landscape. Nearly 90% of organizations are operating in hybrid deployment models, and that percentage has held virtually steady in the high 80s since 2019 (even before the changes prompted by COVID-19). Predictions made in 2016 for a hybrid, multicloud world have come true.

88% of organizations operate in multiple models

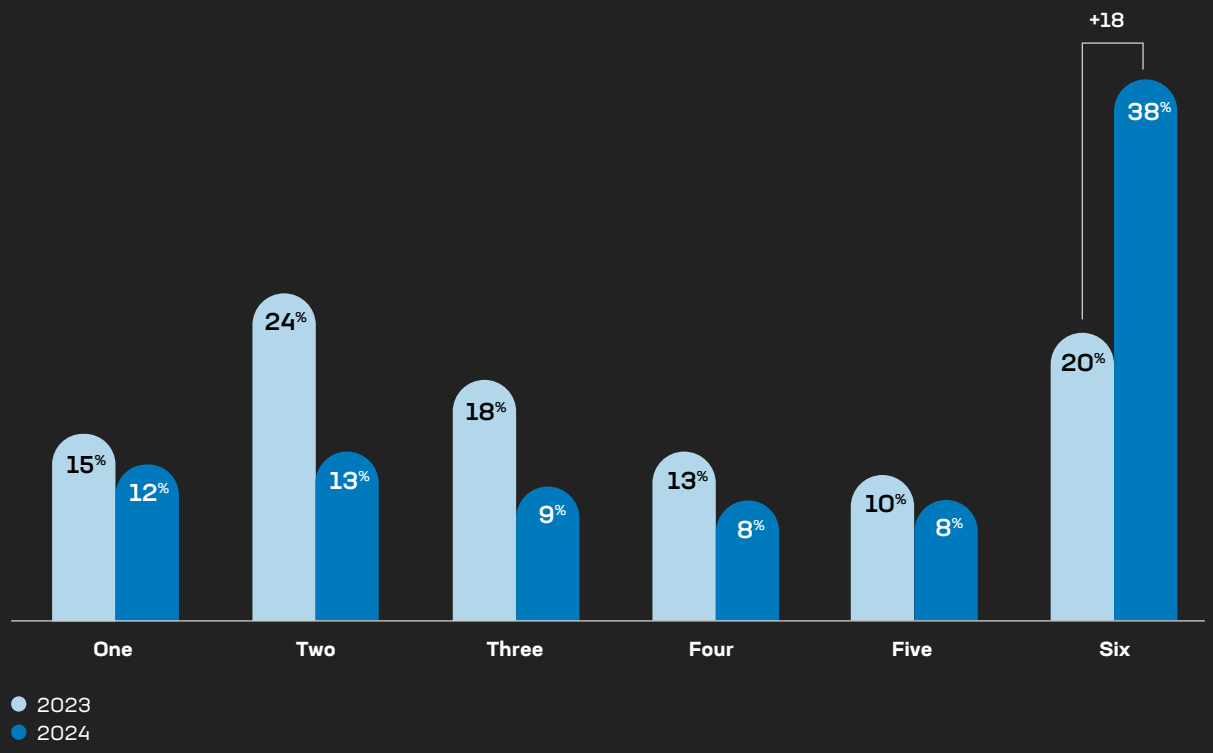
In fact, more than one-third of respondents (38%, nearly double the 2023 figure) operate apps deployed in *six* different models. In 2020, only 18% used even five, so the share of organizations using many models more than doubled in just a few years. This expanding number of deployment models reflects not only increasing use of the edge but also the growing share of containerized modern apps, which are more easily deployed in multiple locations and models. In short, organizations are using more models because they can (and find benefits in doing so). Apps are more widely distributed than ever, with the resulting operational complexity and security challenges as well as the flexibility benefits.

The Number of App Deployment Models Is Trending Upward

We asked:
Of [your] applications deployed today, roughly what percentage are utilizing the following deployment models? SaaS, public cloud/IaaS, on-premises (traditional), on-premises (cloud), colocation, edge.

We learned:
More organizations than ever use many deployment models, and this is as true for smaller companies as for large enterprises.

F5 Insight:
The benefits of choice clearly outweigh the challenges of managing apps across so many different deployment models.



In addition, the broad distribution of apps goes beyond multiple clouds to multiple types of app deployment models—in other words, organizations may be cloud-first, but few are cloud-only. The notion popular a decade ago that clouds might eliminate on-premises data centers has proven wrong. Nearly half of respondents (49%) use all five of on-premises, public cloud, co-location, edge, and SaaS deployment types.

This multi-layered variety exists because each data center facility, deployment location, and operational model offers benefits, and decision makers appreciate being able to select for those benefits. As a result, in addition to juggling both modern and traditional apps and multiple clouds, most organizations of all sizes operate hybrid IT stacks using both cloud and traditional operational models.

There are exceptions, of course. For instance, small minorities of respondents (under one-quarter each) have either no traditional on-premises or no public cloud deployments at all. But most organizations have an embarrassment of riches—and possibly headaches—when it comes to deciding where and how to deploy applications.

56% of organizations make app-by-app deployment decisions

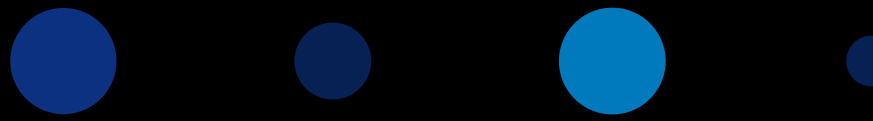
The majority of organizations (56%) make those decisions on an app-by-app basis, particularly when they're selecting a cloud. What's best for the individual app has remained the top factor in cloud deployment decisions since 2018, although the type of app—collaborative, business, data management, etc.—briefly took precedence in 2019. The user type (for example, employee, customer, or partner) has risen in importance to become the third most common factor.

Multicloud Madness Continues

The desire to do right by each app in a landscape populated by multiple clouds and deployment models leads to complexity across IT domains, erecting barriers to everything from consistent app security to automation and vendor consolidation. Moreover, the past five years have seen almost no improvement in the pervasiveness of the associated challenges. Multicloud challenges trouble 94% of respondents—and organizations usually confront more than one. Three-quarters of respondents report between two and five challenges. About one in six (16%) struggles with even more. And fewer than 10% of respondents say they can focus on overcoming just one.

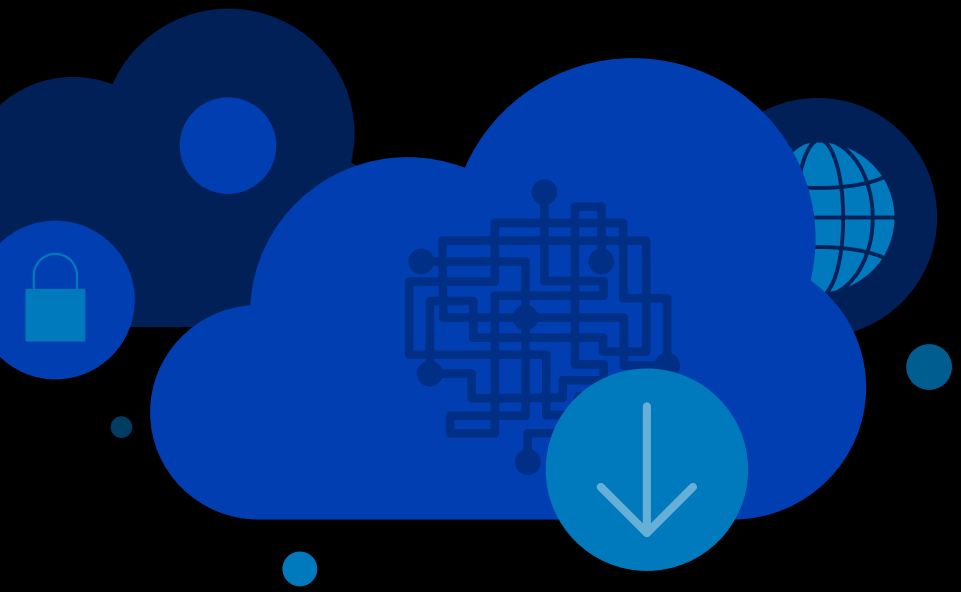
94% report at least one multicloud challenge

Although no single challenge rules them all, the top difficulty, as in 2023, is managing operational complexity. Day to day, this manifests as multiple tools and dashboards, bespoke security solutions and policies, lack of visibility into app health, too many vendors, and telemetry that's trapped in silos.



Migrating apps between environments has risen from fifth place last year to become the second most cited challenge. About one-third of respondents still struggle with multicloud security, a perennial concern since at least 2017. However, nearly twice as many respondents cited security in 2020, making it the top challenge that year. App visibility, also a previous leader, hovers this year in the middle of the pack. These shifts suggest some organizations are meeting those two challenges with solutions such as with Security as a Service (SECaaS).

Nonetheless, the urgency to further alleviate the difficulties is driving intense interest in technologies that promise to reduce multicloud complexity. These include multicloud networking and the distributed cloud perspective it can enable.

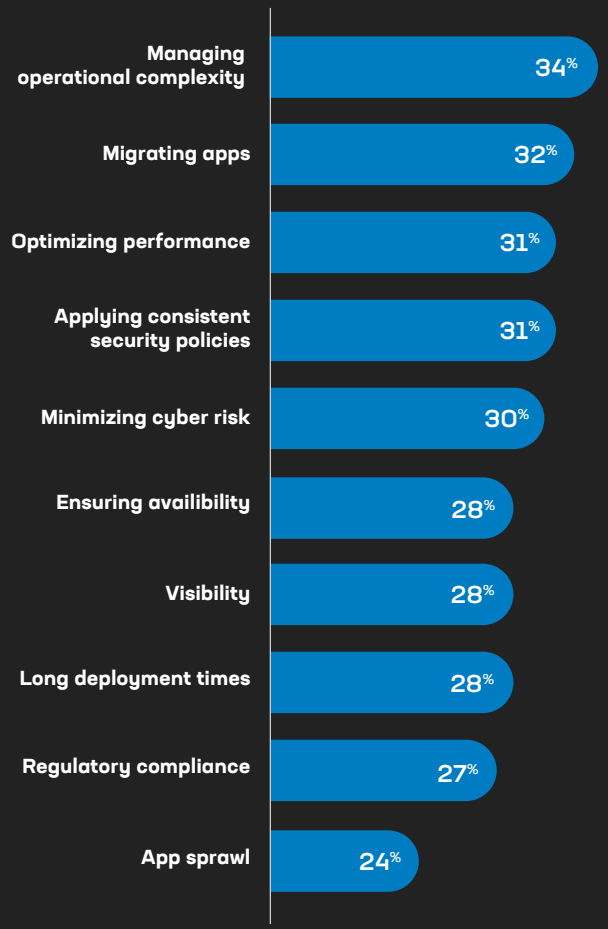


Multiple Clouds Means Multiple Challenges

We asked:
What challenges do you currently have with deploying applications in multiple clouds? Select all that apply.

We learned:
Operational complexity is the most common burden, but there are so many that no one challenge stands out.

F5 Insight:
Consistent app security and visibility–both top challenges in recent years–have dropped in the rankings, which suggests organizations may be partly solving both challenges with SECaaS.



Multicloud Benefits Ease the Pain

Why do organizations accept these challenges? Because multicloud architectures offer benefits that outweigh the difficulties.

Specifically, more than half of organizations using multiple clouds choose complexity over higher costs that might prevent them from remaining competitive. Furthermore, almost two-thirds of those who struggle with migrating apps (62%) cite cost flexibility as the benefit that makes those tough migrations worthwhile. Although cost-optimizing cloud usage on a per-workload basis can be a challenge, the desire to do so is clear.

Multicloud Cost Savings and Continuity Matter

We asked:
What are the benefits of deploying applications in multiple clouds? Select all that apply.

We learned:
The top benefits–flexibility and business continuity–appeal to more than half of respondents.

F5 Insight:
Business continuity, the top use case for public clouds in 2023, remains a key selling point for multicloud deployments.

Business continuity and disaster recovery are also key motivations for putting up with multicloud management. For many digital businesses, outages could be catastrophic, and when disaster does strike, recovery needs to be fast.

Other organizations want the flexibility to determine the best deployment fit for each app given factors such as performance, reliability, and the locations of users, whether remote workers or global customers. Benefits like these override the simplicity and convenience of a single cloud, and today's containerized apps and workloads make it easier to take advantage of that per-app flexibility.

Of course, the enterprise portfolio is not wholly composed of modern apps. Traditional and legacy apps still exist, many of which were "lifted and shifted" into the cloud to capture cloud benefits. As those benefits are coupled to the ability to operate apps using modern practices like SRE, many organizations never realized the hoped-for benefits. So it's no surprise to see repatriation remain a trend this year. Half of this year's respondents say they've repatriated apps or plan to within the year.

In fact, over the past several years, repatriation rates have remained substantial even as the average number of deployment models in use grows. This near contradiction is not a reflection of public cloud flight but simply shifts in which apps are deployed using which models when many are deployed into multiple clouds or using multiple models. Since modern apps generally are a better fit for cloud environments, whether on-premises or provider hosted, we expect both private and public cloud use to continue growing as modern apps swell as a percentage of the average portfolio.

Multicloud Complexity Can Be Tamed

One predictor—or enabler—of cloud repatriation is the use of site reliability engineering (SRE) practices, which include moving toward expected failure to manage incidents more fluently using Service Level Objectives (SLOs). SRE practices can improve reliability and time-to-market for organizations making frequent software or feature upgrades. In essence, the practices help ease app and feature deployments. It's logical, then, that organizations using SRE are nearly four times as likely to repatriate apps. They have the skills to manage complex deployments themselves.

Even among those who don't repatriate, SRE and multicloud management go hand in hand. Most organizations without multicloud apps have not adopted SRE practices. They probably don't feel it's necessary. But of the two-thirds of organizations that deploy application components (such as microservices) into multiple public clouds, nearly half (48%) have adopted SRE practices. Only 7% of those with scattered microservices for a single app get by without SRE practices.

SRE adopters are **4 times** more likely to repatriate apps

Whether SRE is in your organization's future or not, there's hope for those struggling with complexity. Multicloud networking can connect apps across deployment environments and enable a distributed cloud architecture. In essence, multicloud networking simplifies and standardizes the way networks operate across environments—whether public or private cloud, data center, or the edge. A network mesh imposed across them all reduces complexity by employing the same constructs, configurations, and consoles to operate and monitor every app location.

Among other things, multicloud networking can increase visibility, reveal outdated or overlooked APIs, ensure more consistent and more dynamic policy deployment, and enable app migration as a service across environments and cloud providers. As a result, hybrid, multicloud deployments become more sustainable. These benefits prompted survey respondents—and especially those struggling to migrate apps between clouds—to name multicloud networking the year's third most exciting trend for the second year in a row.

It may be that successful multicloud networking will help organizations transcend complexity to enjoy the many benefits of distributed deployments with fewer challenges. In addition, some form of multicloud networking will be required for supercloud architectures. This buzz-worthy idea—which is a cloud architecture that enables hybrid IT to seamlessly operate every layer of the IT stack across cloud environments and providers, on-premises traditional environments, and the edge—has the potential to solve today's complexity hardships. Those hopes make the current excitement around multicloud networking unsurprising.

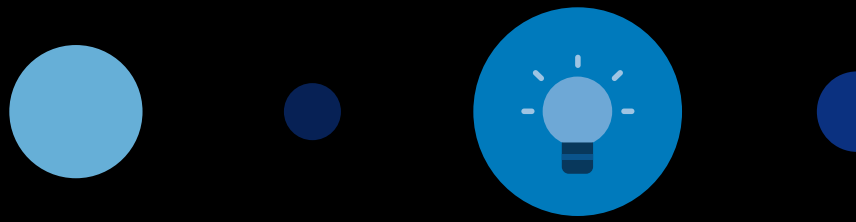
Multicloud networking is the #3 trend

F5 Insight

The need to simplify hybrid, multicloud operations is urgent for organizations aiming to maximize the benefits of distributed deployments without paying a price in IT operating costs, security risks, or management headaches. The adoption of SRE practices is one path many digital leaders are taking to enhance their management of complex and dynamic situations. Multicloud networking is a complementary route generating enthusiasm because it delivers more comprehensive visibility, security, and control.

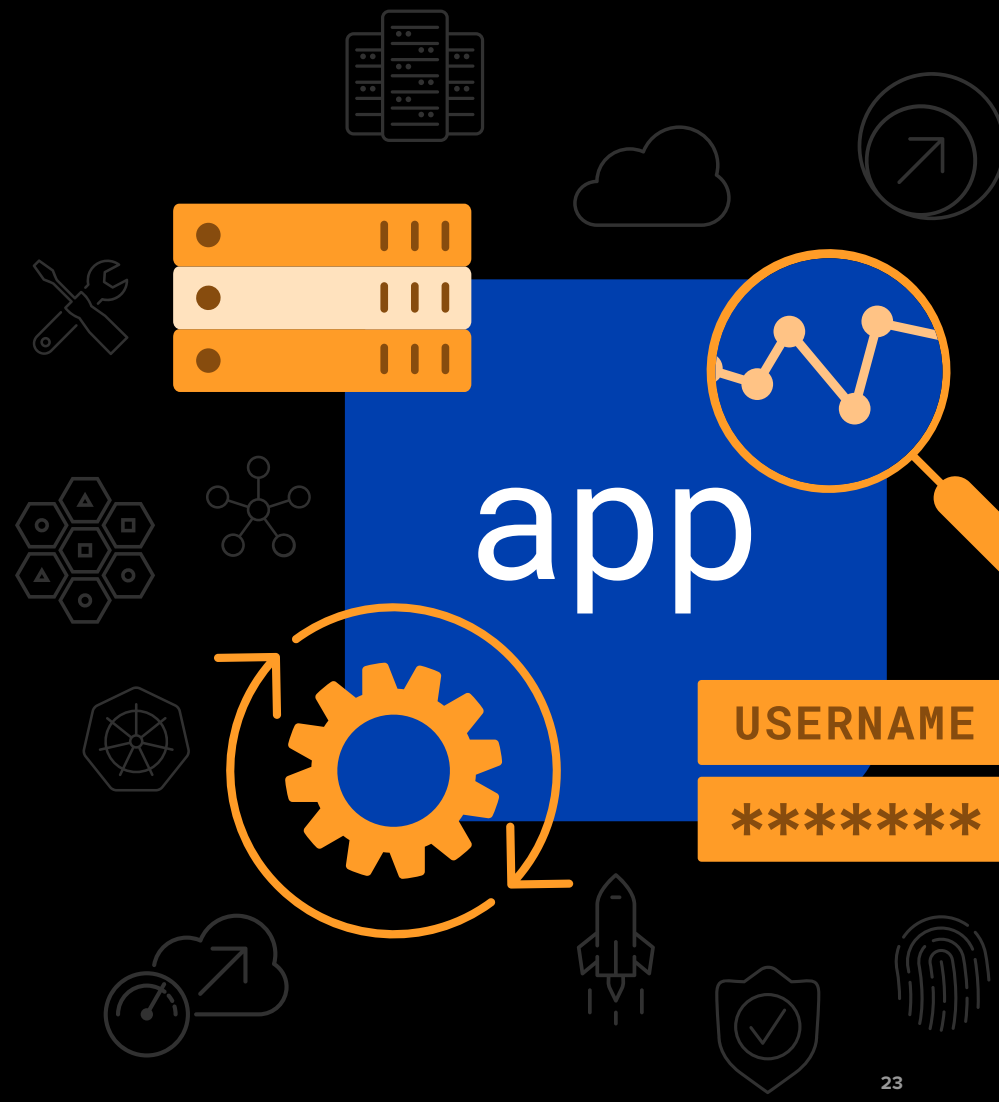
However, connecting environments with multicloud networking will not be enough by itself. The multi-dimensional complexity caused by mixed app portfolios, hybrid IT stacks, different security paradigms, and diverse technologies, solutions, and vendors—as well as different deployment models—requires multi-dimensional solutions. To significantly reduce complexity, an effective distributed cloud approach must go beyond multicloud networking to also secure the apps deployed and optimize the delivery of digital services. After all, it's the performance of those digital services—their speed, global reach, and ability to scale—that drives organizations to multiple clouds and the edge in the first place.

Consequently, comprehensive and integrated app security and delivery technologies are a crucial component of the ideal multicloud networking solution. By incorporating app services such as WAF services, API security, DDoS, bot defense, and performance optimization, a multicloud networking solution is more likely to substantially reduce complexity by streamlining the necessary tools, dashboards, and vendors. Only then will the organization be able to easily manage and protect all its apps and APIs, wherever they reside, to efficiently deliver digital services that create loyal customers.



Key Finding 3

Use of App Delivery and Security Technologies Has Exploded



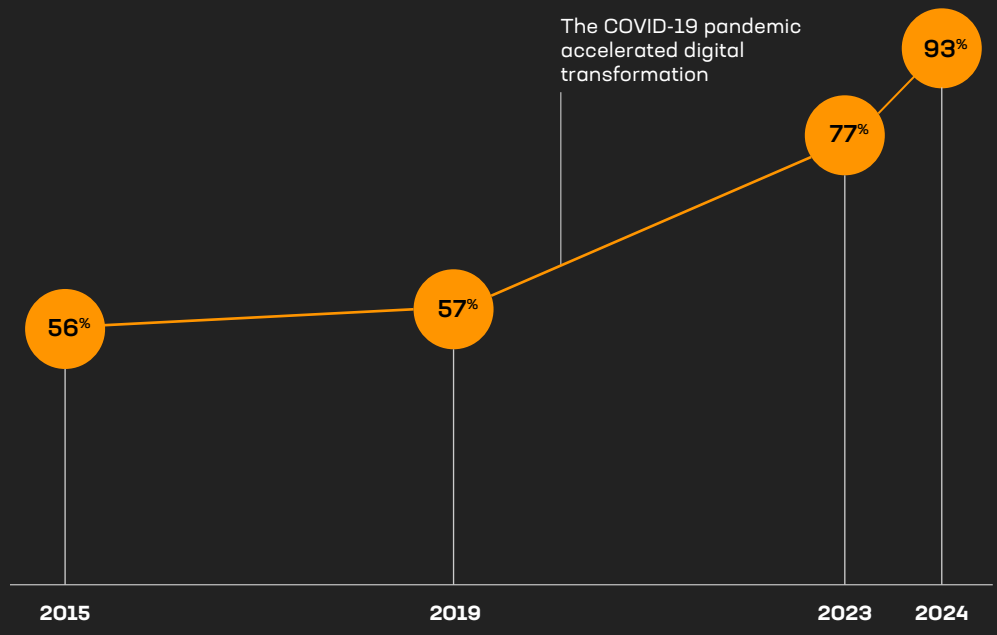
In addition to diversifying app deployment environments, rapid digital transformation has also driven massive growth in the use of app delivery and security technologies, from ingress controllers and API gateways to WAFs and content delivery networks (CDNs). Each of the 30 most common technologies enjoys an average deployment rate of 93%—a huge increase from 57% four years ago and a significant leap in just the past year. When you consider that in 2016, the number of app support services deployed by the average organization was only 11—a figure that has more than doubled—it's easy to see that attitudes about the necessity of even the less-common technologies have shifted enormously.

App Delivery and Security Technologies Are Booming

We asked:
If you have any of the following app services deployed today, how important are they to the applications they are supporting?

We learned:
Even less-common technologies such as QUIC/HTTP3 and mTLS are in use by more than 4 in 5 organizations.

F5 Insight:
For years now, the roles of these technologies and their unique positioning in the app delivery process have warranted an IT domain and strategy of its own. Clearly, app delivery and security technologies are increasing in strategic importance to businesses in the digital economy.



App security and delivery technologies are commonly grouped into the categories of security, identity, performance, availability and mobility. In that context, app performance services (such as CDNs and performance monitoring) are deployed least. But no category averages lower than 90% deployment, and no single technology in our survey was deployed by fewer than 85% of respondents.

Security Technologies Remain Most Vital

While identity and access technologies remain the most frequently deployed as a category, security-related services are the ones respondents say they can least dispense with. This has been true since 2016, when the security category overtook availability services (such as service discovery) as the top priority. It's not hard to understand why. The threat of breaches that could involve data from millions of users or customers, and the resulting financial and reputational losses, make security services fundamental.

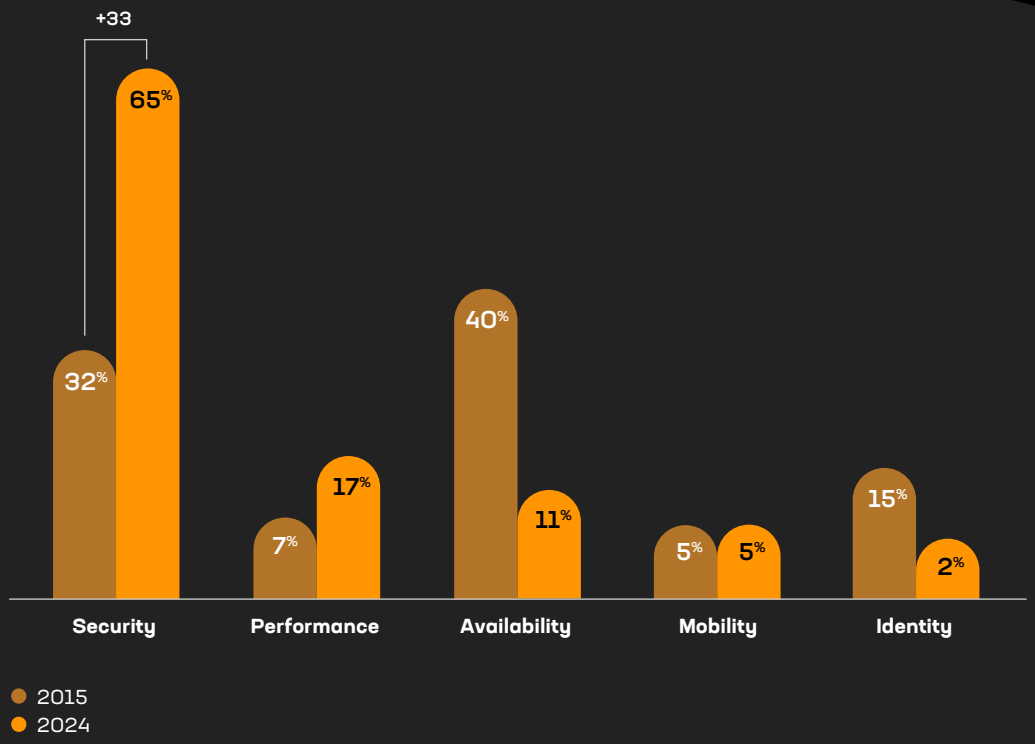
Nonetheless, about one-third of respondents say they'd deploy an app without a supportive security technology before they'd give up something else.

Security Technologies Are Indispensable

We asked:
Please complete this sentence: "The worst thing I could do is deploy an application without…?" Select one.

We learned:
The imperative of security technologies as a group has more than doubled in the last decade.

F5 Insight:
The majority of organizations have learned the hard way that if you don't protect an app from attackers, its availability and performance become moot.



When app delivery and security technologies are considered individually, those most frequently deployed are nearly all in the security category. It's no misalignment, however, that authentication/identity technology—typically grouped in the identity category—has the single highest rate of deployment. Authentication is a key to zero trust security as well as other widely adopted protections. The overlap in categories is merely a reminder of how interdependent app delivery and security services can be—one reason their average overall use is increasing.

Regardless of their category, the majority (66%) of app delivery and security technologies are deployed in the cloud. Organizations in the public sector, healthcare, and the largest organizations by revenue are somewhat more likely to deploy them on-premises, probably because they're considering on-premises legacy apps. SaaS delivery and edge hosting are also relatively common.

Two-thirds of app services are deployed in the cloud

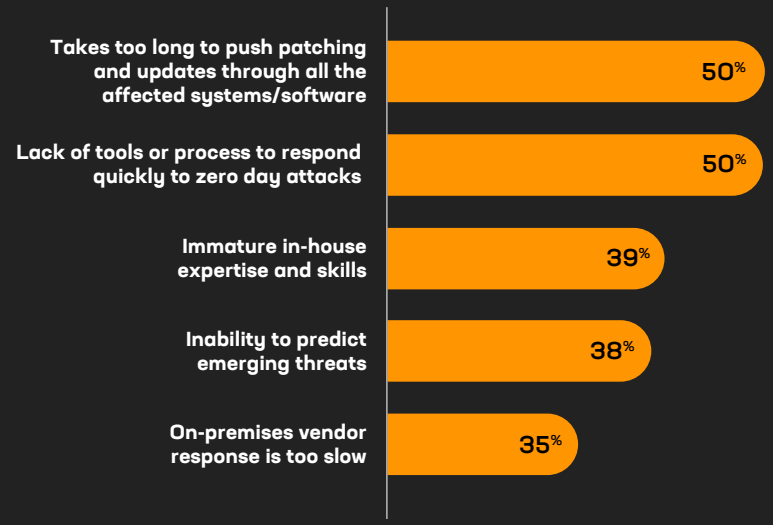
Speaking of SaaS, Security as a Service (SECaaS) use is on the rise. Why? Speed. Organizations choose this deployment model because it both accelerates needed defensive maneuvers and helps them respond faster to actual threats. Without it, the daunting complexity can slow or prevent critical updates and patches. SECaaS helps resolve that dilemma while keeping teams out of reactive, all-hands-on-deck "war rooms" and focused on proactively improving apps and the customer experience.

Speed Is the Number One SECaaS Benefit

We asked:
What operational challenges does Security as a Service solve for your organization? Select all that apply.

We learned:
An inability to move quickly enough amid daunting complexity continues to be the top operational challenge that SECaaS helps solve.

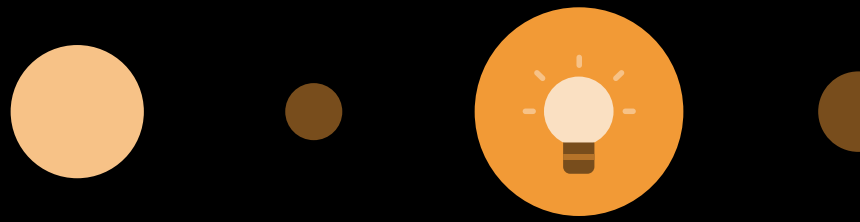
F5 Insight:
The answers to a related question about what motivates organizations to use SECaaS indicate that visibility is becoming as important as speed in ways that make the two considerations converge. If you can't see an emerging threat, the speed of your response hardly matters–you won't have one until the damage has begun. This hard truth makes threat intelligence mandatory as a prerequisite for speedy mitigation.



F5 Insight

The use of app delivery and security technologies is skyrocketing. The emphasis on security services in particular reveals that organizational focus on protecting apps is likely to influence other investments. As a result, many initial automation, AI, and other modernizations will probably start with security solutions.

App security is already relatively mature, although its evolution will continue to address attacker innovations. By contrast, the challenges of protecting APIs and API endpoints will likely fuel the rise of more revolutionary options for API security. Creative protections will be particularly crucial to protect new AI models and services and AI-driven apps. Given the daunting complexity inherent in the delivery of digital services today, we expect interest in such solutions to explode.



Key Finding 4

Digital Transformation Has Progressed Rapidly to AI-Assisted Business

Given the complexity created by the explosion of APIs, the rise of hybrid, multicloud deployments, and the need for entire suites of app delivery and security technologies, it's no wonder that organizations are increasingly focused on AI-assisted business. Their interest is a hallmark of the third stage of digital transformation, an iterative journey typically tackled in three phases:

1. Task automation, including deployment of apps that streamline manual processes.
2. Digital expansion, which includes modernizing, connecting, and scaling those apps.
3. Making decisions based on telemetry from those apps plus AI and machine learning (ML).

Most organizations work in more than one phase at a time as automation and modernization reach more deeply into the business. Today, although task automation is still underway, collective digital transformation has progressed rapidly into its later phases.

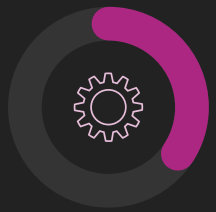
Organizations working in these latter phases of transformation tend to view digital business as a strategy more than those in early stages, who may see technology as an enabler rather than the core of the business. Either way, the benefits of transformation are clear to 98% of respondents, with efficiency and productivity—doing more with less—way out front.

AI Assistance Activity Has Exploded

We asked:
Please select the project(s) below that are the current focus of your organization's digital transformation. Select all that apply.

We learned:
The percentage of those working on AI-assisted business is up nearly 40 percent in 2023 (from 54%).

F5 Insight:
The telemetry necessary for AI assistance—and systems to integrate and manage it—are now crucial for most organizations.



32%
Task automation: Applications

77%
Digital expansion: Modernization

75%
AI-assisted business: Data and analytics

#2 benefit of digital transformation: more productive employees

The most frequently named benefit, increasing the efficiency of IT operations, has held its top spot since 2018. Efficient IT operations are a tactical steppingstone to more strategic digital transformation projects that can reach further into the organization and bring other benefits.

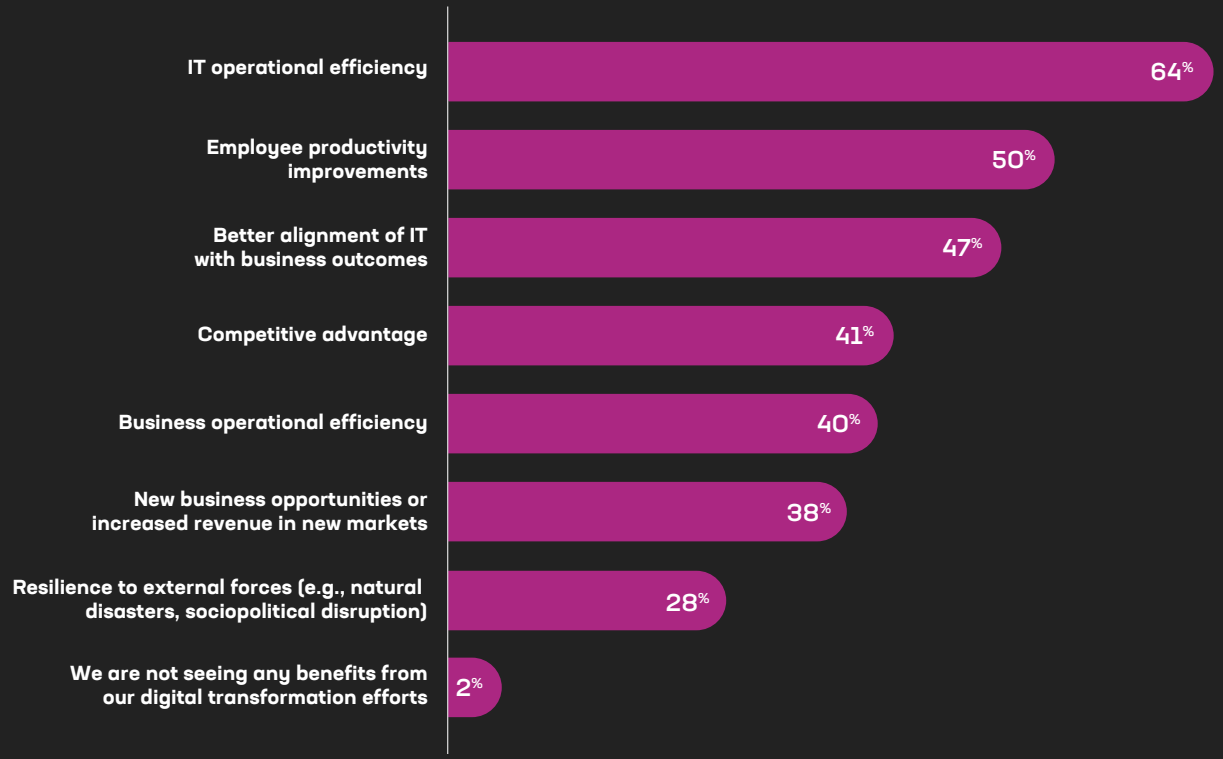
Similarly, improving the productivity of all employees may sound less enticing than, for instance, a competitive advantage—but in a world of almost universal cost pressure, more productive employees can lower costs and create a meaningful pricing advantage. That may be why this benefit, which ranked fourth just last year (as well as in 2018 when we first asked this question), has risen to second place.

Transformation Elevates IT Efficiency

We asked:
What benefits are your organization seeing from your digital transformation efforts? Select all that apply.

We learned:
Nearly two-thirds of organizations have increased IT operational efficiency.

F5 Insight:
Higher IT operational efficiency can enable other projects that promise broader and more strategic benefits.



More Strategic Benefits Can Still Be Achieved

Better alignment between IT and the business is a more strategic benefit that nearly half of respondents say they're obtaining. However, compared to their efficiency improvements, even the most advanced organizations miss out on ideal alignment.

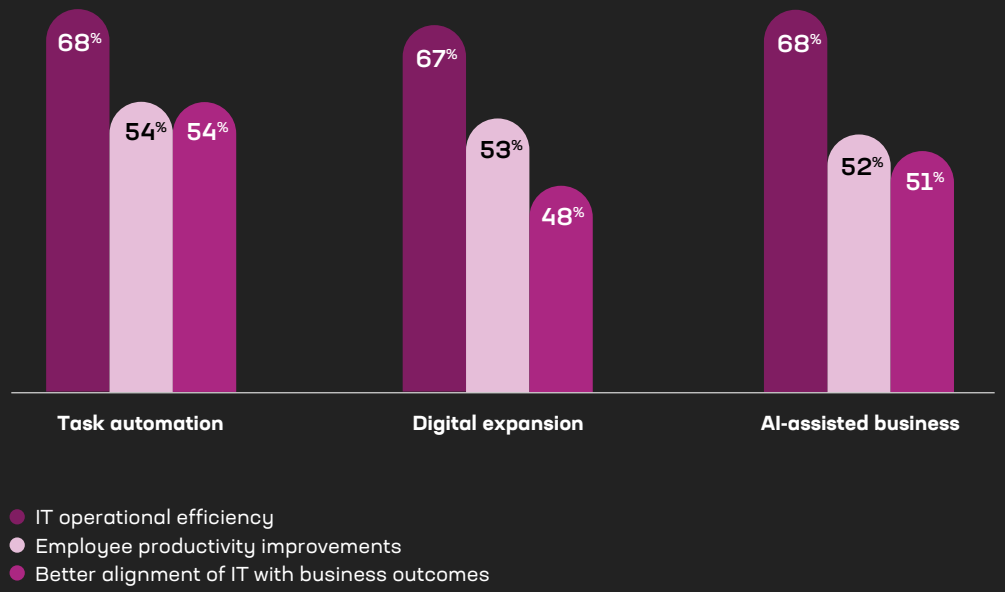
Regardless of where organizations are in the journey, they face similar challenges throughout, including budget constraints, skills gaps, and the complexity generated by modernization itself. In addition to the promise of multicloud networking and superclouds, organizations are increasingly looking toward automation, in particular automation supported by AI, to help tame the challenges moving forward.

Business Alignment Is Improving for Roughly Half of Us

We asked:
Please select the project(s) below that are the current focus of your organization's digital transformation. Select all that apply. ***The results were cross-tabulated with the answers to a second question:*** What benefits is your organization seeing from your digital transformation efforts? Select all that apply.

We learned:
Organizations are achieving the same top benefits regardless of their phase of digital transformation, and half cite better alignment between IT and the business. Unfortunately, that alignment doesn't seem to advance with the phase of transformation.

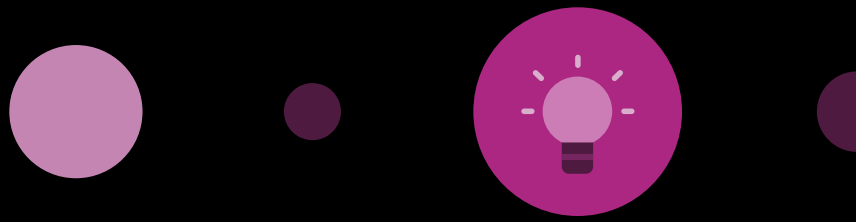
F5 Insight:
This may be because AI use to date tends to be more tactical—for instance, securing apps—rather than representing strategic, line-of-business deployments such as customized purchase suggestions for customers.



F5 Insight

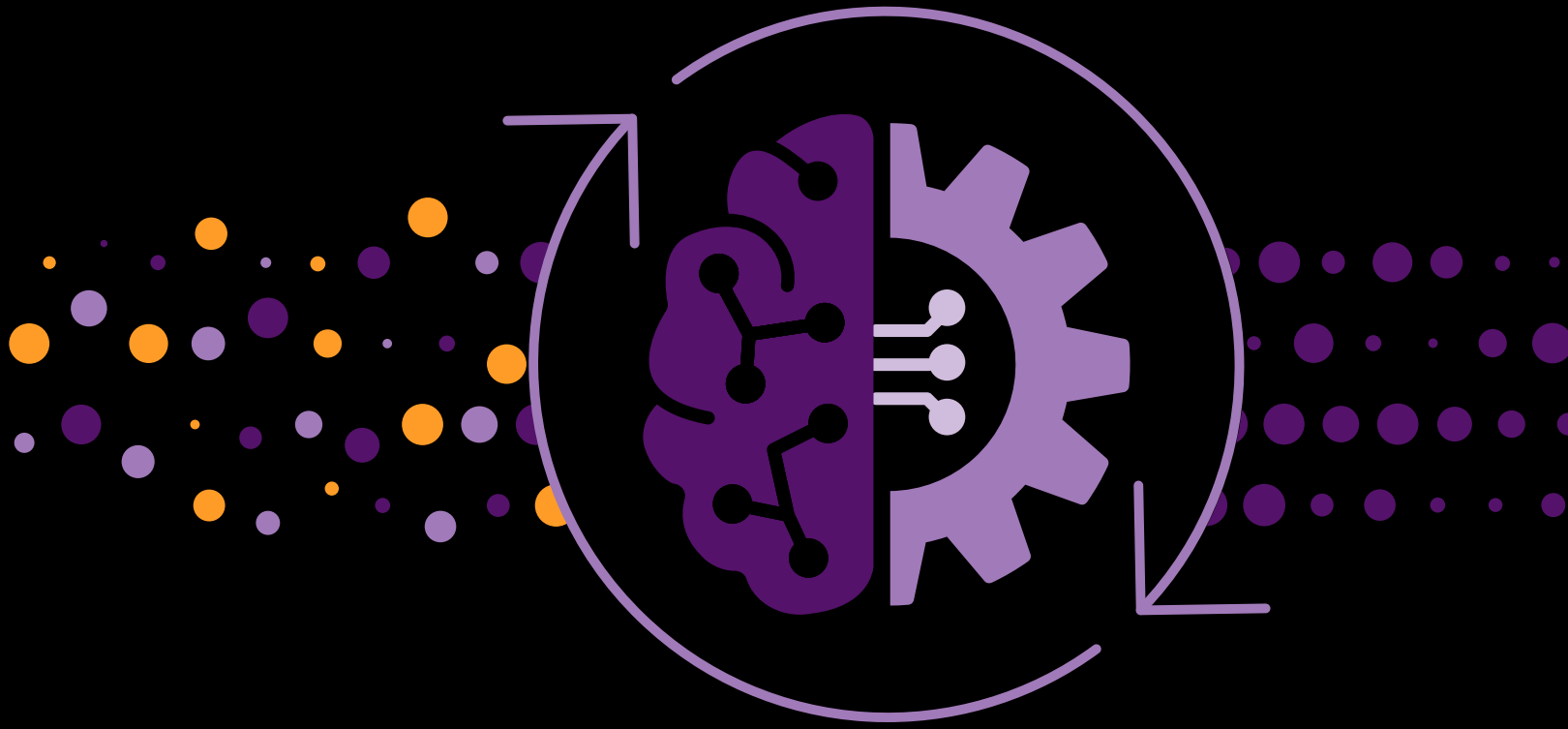
In a world of technological innovation, digital transformation has no fixed destination. No one's ever done. As AI use matures and unforeseen technologies enter the scene, complexity and hybrid IT will continue as the status quo. The advantage will go to organizations that build a flexible IT stack capable of rapidly supporting new technologies and delivering the capabilities the business needs to reap the benefits of the resulting competitive advantage. With the right foundation in place, those organizations can capitalize on whatever innovations emerge.

Unfortunately, attackers are proceeding through digital transformation too, and—lured by huge financial incentives—at least as quickly as their targets. Malicious use of AI is already increasing the sophistication of cyberthreats, which organizations face now at global attack rates counted in seconds, not minutes or days. In such a hostile environment, it's essential for organizations to transcend operational complexity to effectively protect their digital estates. Only then can they continue their evolutions toward whatever else the digital future may bring.



Key Finding 5

AI Will Help Solve Complexity by Increasing Automation



Automation of IT functions is central to the second phase of digital transformation, and automation and orchestration efforts have kept organizations busy in recent years. The domains of highest automation tend to be those viewed as most dynamic or most critical to the business and thus are addressed early in modernization efforts. The ease of standardization in that functional area also plays a role.

As a result, the automation of IT functions tends to lag, even though they are a significant enabler for the rest of the business. Additionally, despite remarkable progress through digital transformation in recent years, some IT functions remain more automated than others. For instance, app infrastructure has been the most automated. Automation there has been relatively accessible in part because organizations can readily standardize to one vendor, such as by using a single brand of servers in the app infrastructure. In that way they eliminate complexity that can block automation. More than half of respondents report automating their app infrastructures, up from 37% in 2019.

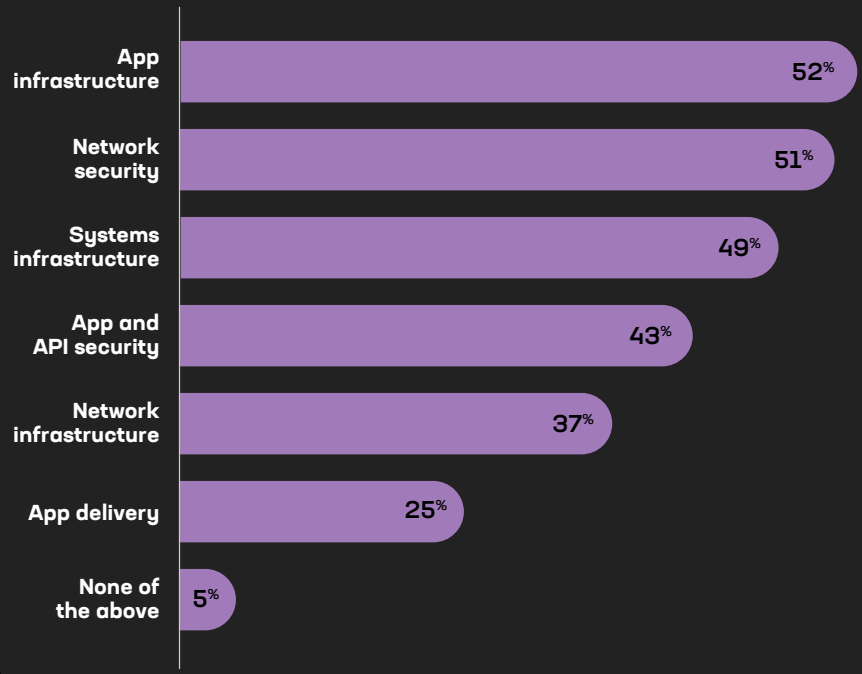
More than a third of organizations have also made progress automating app and API security. But more have a long way to go.

App Delivery Automation Lags

We asked:
What IT functions have you automated? Select all that apply.

We learned:
Thanks to their growing complexity, app delivery–and to a lesser degree, app security–remain among the least automated IT functions.

F5 Insight:
App and API security automation increased from 33% to 43% over the past year. Many decision makers probably feel they have no choice but to prioritize it, given the high costs of successful attacks.



Complexity Can Stymie Automation

Automation of app delivery continues to represent a big opportunity. According to survey respondents, budget limitations are the top barrier. A close second is the complexity fostered by use of different app delivery products and vendors, all using various APIs and tools. This complexity is exacerbated by bespoke configurations and a variety of policies that deliver and optimize the apps, making automation a difficult and time-consuming chore. Other challenges include a lack of skills. No wonder three-quarters of organizations aren't automating their app delivery.

46% say budgets prevent automation while **39%** blame complexity

Of that majority, however, some have probably pursued SaaS solutions to deliver the speed and efficacy unavailable with manual configurations and deployments. SaaS is also a valid way to work around missing skillsets, which is the third most common barrier to automation. Of course, operating expenses dedicated to SaaS further limit the organization's ability to invest in automation elsewhere.

The Benefits Make Automation Worthwhile

Regardless of their original motivations, those who do find the resources to automate enjoy significant benefits. Three-quarters (74%) say they've grown more efficient, and two-thirds save money, probably in part due to more efficient operations.

Automation Benefits

The method of automation used matters. More than half (54%) of those leveraging full automation cited consistency as a benefit, compared to only 44% of those who rely on human-driven scripts or toolsets. Similarly, 80% of organizations with full automation report efficiency gains, while only 72% using scripts or toolsets initiated by humans did. Organizations adopting a fully automated approach were more likely to cite benefits of all kinds.

These benefits are no doubt why automation was named a top telemetry use case, along with root cause analysis, by those using or planning to use operational telemetry.

Organizations that want to deploy more automation typically have difficulty obtaining and integrating the data to generate needed insights. Nothing stands in their way more than multiple solutions, tools, and operational silos that do not share telemetry. Standardization in the data protocols and solutions could help by providing better visibility while mitigating solution sprawl.

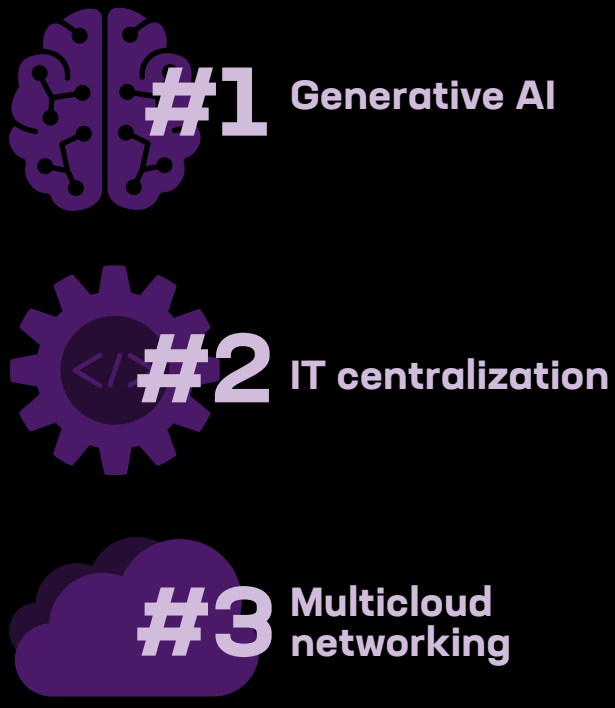
Top telemetry use cases: automation and root cause analysis (54% each)

Amid all these challenges rising from complexity, it's probably not a coincidence that the second most exciting trend for respondents this year is IT centralization. Interest in restructuring the IT organization is likely a response both to cost pressure and to issues such as tool proliferation and the need for end-to-end visibility. Many teams hope to move away from siloed operations based on traditional server, storage, and networking domains. Better aligning skillsets to focus on the business's digital workflows and cross-discipline system management could help streamline tools and integrate data, yielding greater insights and, ultimately, a better customer experience.

Generative AI May Put More Benefits in Reach

When operational complexity keeps automation elusive, generative AI holds out hope. Respondents showed more consensus than usual in naming generative AI as the top trend causing excitement in 2024.

Top 2024 Trends



Although operations and business use cases for AI are gaining traction, app security is still seen as the priority. The top value decision makers expect to gain from using generative AI for security is the automation of policy deployment and configurations—potentially reducing one of the vectors driving operational complexity. And of course, speeding the proper and more consistent application of those policies would contribute to more effective protection, the next most valued use. Insight into vulnerabilities and threats is worthwhile, too, but less important.

Attitudes about how generative AI can benefit app delivery are similar, with 44% calling automatic policy adjustment based on service level objectives the most valuable use.

Unfortunately, most of the AI assistance available today is not delivering adaptive policy management or greater efficacy. Chatbot "assistants" in app delivery and security solutions can be relatively easy to implement, but survey respondents called those use cases—which explore and analyze data using natural language—the least valuable. The market clearly wants generative AI systems that can *act*.

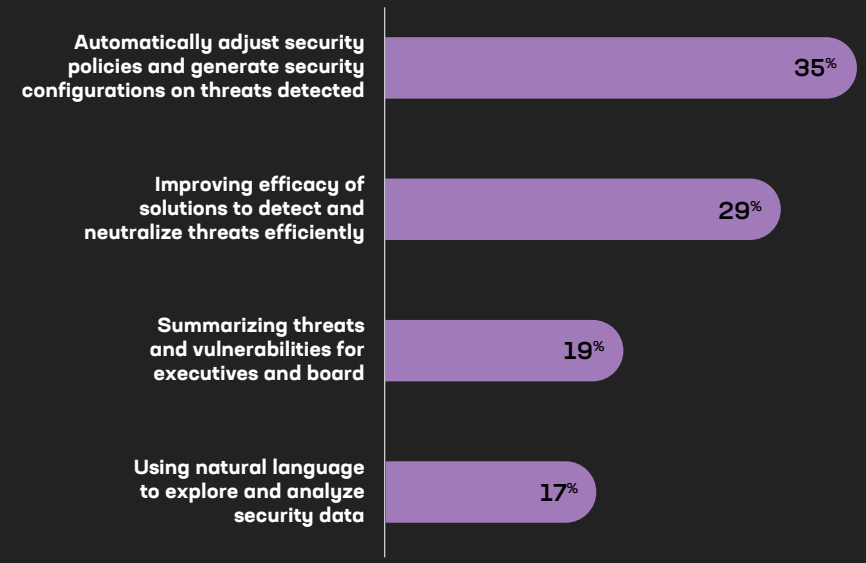
That's why AI operations (AIOps) will continue to grow as a discipline, despite dropping in the ranking of trends from second place in 2021 to number 7 today. Perhaps AIOps are no longer thrilling, but rising use of telemetry for automation will drive their growth. This prediction is supported by survey respondents. Those struggling with automation complexity were more likely than average to value generative AI most for AIOps purposes.

Generative AI Is Valued for Adaptive Security

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

We learned:
Policies and configurations that adjust to threats appeal most.

F5 Insight:
Security's "next frontier" has evolved. The zero trust model, which first started to generate buzz in 2016 and was one of two most exciting trends in 2023, has taken hold in a majority of organizations–who are now looking toward AI as the next silver bullet for app and data protection.

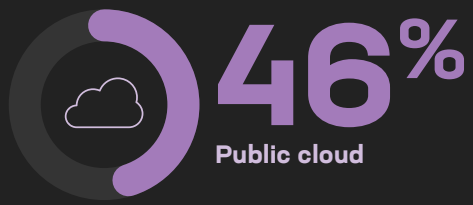


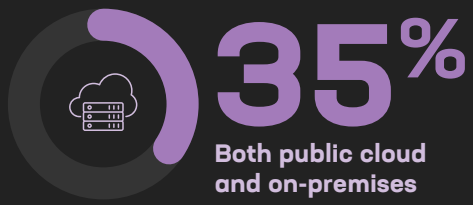
Meanwhile, AI workloads all but ensure the continuation of hybrid, multicloud operations (and the complexity that follows). Nearly half of organizations plan to locate AI engines in the public cloud, but significant percentages plan on-premises hosting as well or instead. And apps tend to follow the engines, so the challenges of performance and consistent security across environments will live on. AI assistance will mitigate but not eliminate the difficulties.

Besides, as with automation, AI will most benefit organizations that can deploy it strategically. AI deployments that prevent security breaches or reduce operational costs are useful but primarily tactical. As business success increasingly relies on digital apps and data, the most strategic uses of AI will be tailored to support specific business functions and execute on core business strategies. The benefits can go beyond tactical targets such as cost savings. More strategic use will yield even greater value, such as creating new and better customer experiences or delivering a competitive advantage.

In 2024, more than a third of respondents said they were already realizing strategic benefits like these. We expect others to join them. As organizations mature in their digital transformations, the focus on AI for lines of business will increase.

AI Engine Locations

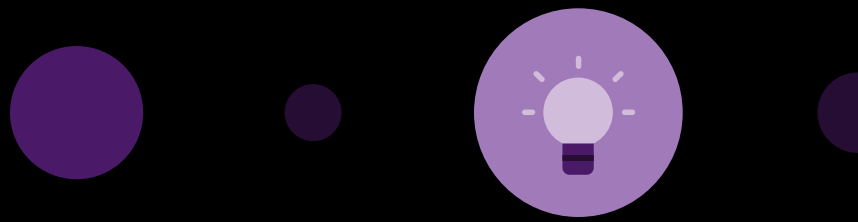




F5 Insight

AI is no longer in the future. It's here—although not everyone has the telemetry they need, and those who do may not be using it to greatest effect. For instance, 47% of respondents said they planned to use telemetry not for automation but for operational alerts. Those organizations may be making a mistake. Go ask security teams: Alert fatigue is real. On the other hand, effective automation can prevent the alerts in the first place, overcoming IT complexity and helping apps adapt to threats and changing circumstances in real time. Only real-time responses enabled by automation will ultimately deliver the speed and efficacy organizations say they want. Then decision makers can turn their attention to AI assistance that more fundamentally supports strategic business objectives.

Since the barriers of budget and complexity will continue, any standardization that can be achieved is useful. To that end, we expect organizations to increasingly turn to integrated product suites or a consolidated team of vendors that can offer more automated, connected, and scalable app delivery and security support across hybrid, multicloud environments. As part of that movement, use of multicloud networking will increase. The benefits will include not only the speed and efficacy of automation but greater visibility, too, to further amplify the virtuous cycle of insights driving automated and intelligent actions.



Conclusion

Approaches for Future Success Are Emerging

As organizations adopt AI, which relies heavily on modern apps and infrastructure, both modern apps and APIs will continue to proliferate. Even where AI is not adopted, digital transformation and expectations about digital experiences will reach more deeply into organizations, increasing use of modern apps and APIs. Many of those modern apps and any AI engines they rely on are likely to be hosted in one or more public clouds, on-premises, or at the edge. Virtually all of them will need the support of a variety of app delivery and security technologies, management interfaces, and telemetry tools. In other words, delivery of the digital services we all count on today will only grow more complex in the decade to come.

Several established and emerging approaches can help organizations meet the resulting challenges. First, standardization (whether of protocols, processes, tools, solutions, or vendors) can reduce the complexity, increase visibility, and streamline management.

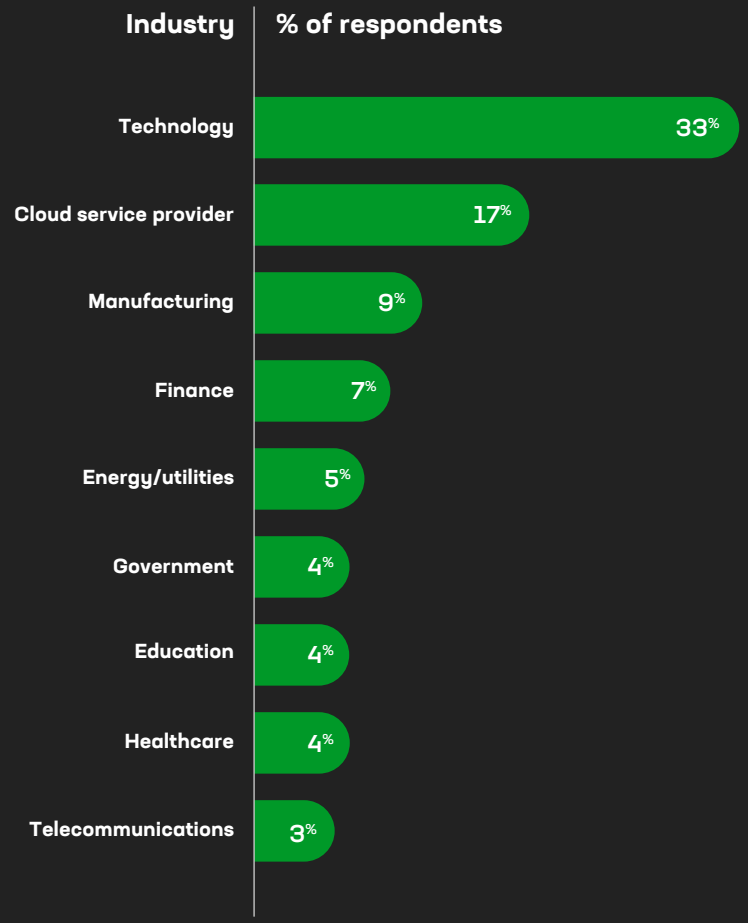
Second, better connectivity—from data sharing to microservice(s) and multicloud networking to app-to-app connectivity—is obligatory. Integrated app security and delivery technologies have a critical role to play, securing and ensuring performance across distributed apps and APIs. These technologies can also help standardize and automate policy deployment for greater consistency, security, and control with shorter response and management times. Distributed architectures that include consistent app services for L4 through L7 can also centralize and ease management by providing a reassuring layer of control and advanced services such as API discovery and runtime protection. By delivering a single (or at least fewer) dashboards, this approach brings focus to an otherwise blurry view across hybrid IT stacks supporting distributed apps and multiple deployment models. The ubiquitous “supercloud” of 2030 cannot happen without some form of multicloud networking that connects both the distributed infrastructures that apps run on and the apps themselves.

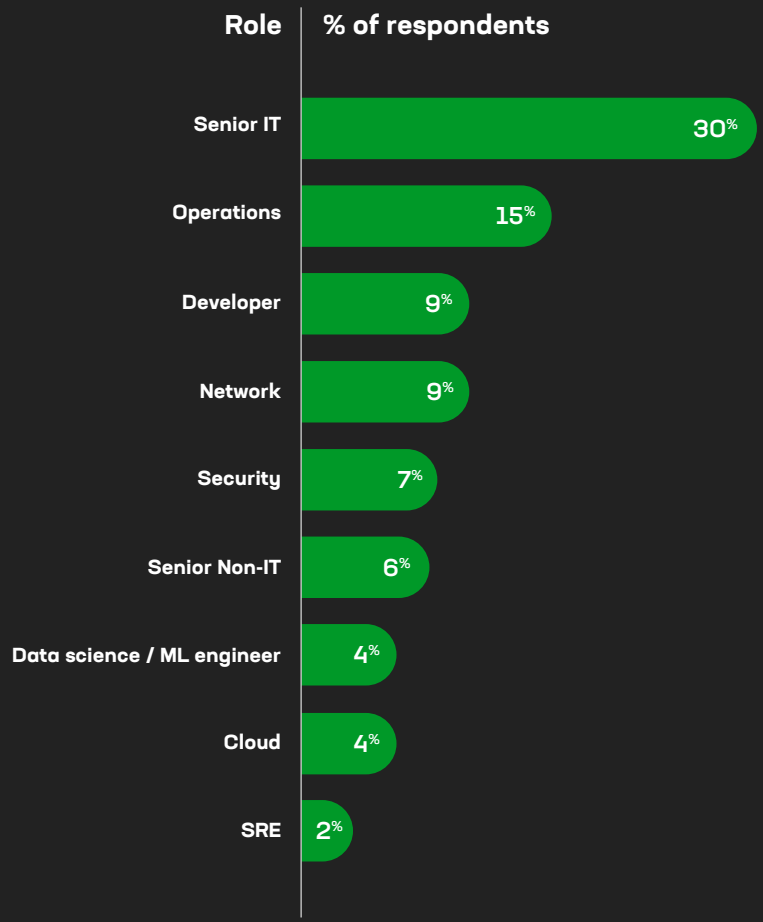
Third, AI can help automate policy deployment and configuration tasks too complicated to manually manage—but not without better visibility and integrated telemetry first. Improved telemetry and analytics will be central to converting the massive momentum of digital transformation into ongoing digital evolution.

Ultimately, the most mature and successful digital businesses will be those that can rapidly implement measures to solve their complexity challenges. Then they can shift the power of AI assistance to more strategic line-of-business purposes that more directly enhance the customer experience, allow the business to innovate and scale, and provide access to rewarding new markets and innovative revenue streams.

About the Report

More than 700 global respondents representing organizations of all sizes completed the 2024 State of Application Strategy survey, our tenth annual. Approximately one-third of those organizations operate on less than $200 million USD in annual revenue, while about one-quarter operate on over $1 billion. As usual in the last decade, the technology industry was best represented, but many others participated. Meanwhile, the percentage of respondents from senior IT roles has increased significantly in recent years to nearly one-third (30%). Other respondents represented a wide variety of operational roles and their respective interests and decision making perspectives.





ABOUT F5

F5 is a multicloud application services 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 and API—on premises, in the cloud, or at the edge. F5 enables organizations to continuously stay ahead of threats while providing exceptional, secure digital experiences for their customers.

For more information, go to f5.com. (NASDAQ: FFIV).