State of Application Strategy Report

2021

At a glance

Digital transformation has raced forward in the last year.

The astonishing progress is apparent through several key markers revealed in our seventh annual survey:

- AI-assisted business has tripled.
- Applications continue to be modernized rapidly, with APIs a method of choice.
- The importance of SaaS-delivered security is rising as organizations work to unify security across distributed applications while managing more architectures than ever.
- Architectural complexity makes multi-cloud availability an imperative, and edge deployments are increasing, too.
- Telemetry will take us to the future—but now, nearly everyone is missing the insights they need.

This remarkable past year, filled with newly remote work, education, and consumer activities, has driven significant changes in organizations' outlooks for the future—including which trends decision-makers consider most strategic over the next 2–5 years.

Welcome to the F5 2021 State of Application Strategy Report.

Contents

Introduction

A Digital Leap Toward Our Data-Driven Future

We all know how much the world has changed in the last year. As the results of the most recent F5 State of Application Strategy survey make clear, however, the COVID-19 pandemic also vastly accelerated a global digital transformation that was already underway. Progress that might normally have taken a decade has leapt forward in a single year—with respondents maturing in their journeys toward digital expansion.

A dramatic increase in remote work and socially distanced ways of interacting with customers—both driven by the global pandemic—have exploded demand for digital services across industries, geographies, and communities.

Providing digital access to products and services previously purchased through in-person transactions is not enough. Improving connectivity, reducing latency, enhancing performance, and ensuring security have become critical to business survival. As everything from restaurant orders and telehealth to governmental assemblies has gone digital, a streamlined and supportive user experience has become indispensable. Yet IT infrastructures and skillsets typically don't change so quickly. As a result, organizations are embracing the public cloud and SaaS, rapidly adopting edge strategies, and seeking application security and delivery technologies that are easy to deploy and provide data for decisions.

Key survey findings that support these conclusions reflect changes in four strategic areas intended to improve the customer experience and defend the digital business.

1. Continued modernization of applications and architectures
2. Accelerating cloud and SaaS deployments driving a multi-cloud approach and growth in SaaS security.
3. The rise of the edge as containerization expands.
4. The importance of telemetry to applications that can adapt to change.

Each area captures a different aspect of progress toward digital transformation.

1. Continued modernization of applications and architectures to enable better digital experiences

It's no surprise that organizations continue to modernize their applications to better deliver the digital experiences their customers expect. APIs are the method of choice, with a majority of organizations using them to create modern workloads that are a mixture of traditional and modern application components.

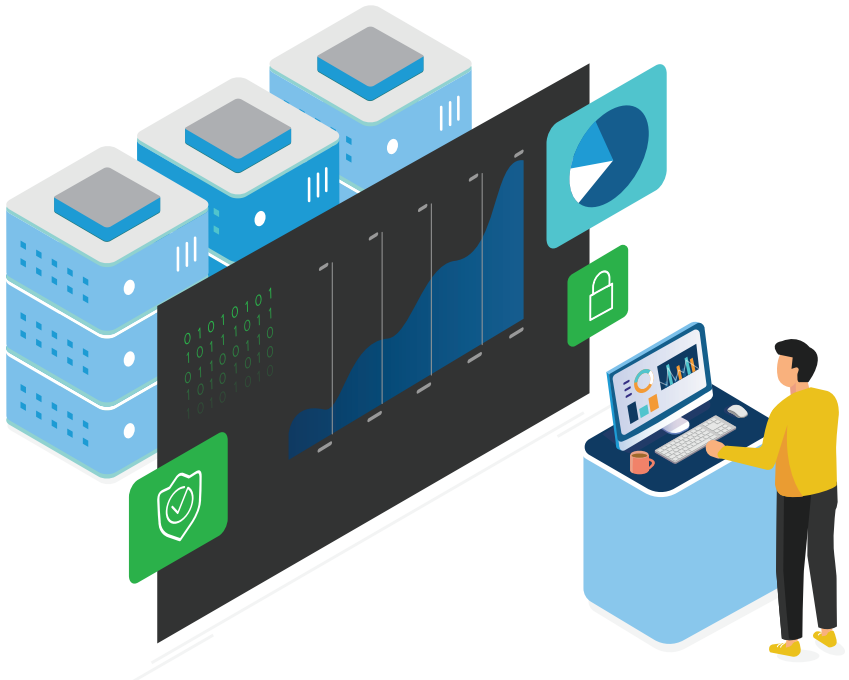
Nearly **nine of ten** operate both modern and traditional architectures.

As modernization continues, more organizations than ever—87%—operate both modern and traditional application architectures. Although mobile and modern architectures will continue to exist side-by-side with traditional architectures for the foreseeable future, client-server and three-tier web architectures are decreasing relatively dramatically, their share of the portfolio dropping 12 points in a single year.

2. Accelerating cloud and SaaS deployments driving a multi-cloud approach and growth in SaaS security

The percentage of applications deployed in the cloud is expanding. Both Infrastructure as a Service (IaaS) and Software as a Service (SaaS) account for this growth. Efforts to stay ahead of cyberattacks frequently require AI and machine learning beyond what organizations have the resources to manage on premises, and they turn to the cloud for help. As a result, leveraging SaaS for security has become the number one strategic trend for a majority of respondents. Meanwhile, colocation deployments are slowing, and applications hosted on premises continue to represent a shrinking share of app portfolios.

Number one strategic trend: **SaaS security**



3. The rise of the edge as containerization expands

Edge computing can be defined as operations performed outside of a centralized data center, in the intermediary spaces between the connected endpoints and the core IT environment. The edge—which is different for each industry and business function—enables new services and better performance by placing applications as close as possible to the sources and users of data. In financial services, for example, keeping data closer to users—and only periodically using secure channels to sync with the bank—can improve security by reducing use of vulnerable web interfaces. In manufacturing, the edge can ensure an efficient global supply chain with faster responses to real-time alerts.

The edge is evolving to meet the need of enterprises to support modular application components that reside in containers across multiple cloud and edge locations. Containers enable faster, more efficient, more consistent deployment, and placing them at the edge can improve scalability and the customer experience, among other benefits. More than three-quarters (76%) of respondents are already using, or have plans to use, the edge to capture benefits related to application deployment, performance, and data availability.

This overwhelming interest in the edge is driven by the need to improve application performance, and it can be seen in the criteria organizations consider when they make decisions about application security and delivery technologies. As in previous years, ease of use and reduction in total cost of ownership are the first and second most-desired characteristics, respectively, for decision-makers evaluating a purchase. Multi-cloud availability rose dramatically up the list from eighth to third place in only one year, a reflection of increasingly distributed applications.

4. The importance of telemetry to applications that can adapt to meet evolving customer and business expectations

Nearly three quarters of respondents (75%) consider telemetry about application security and delivery important for meeting business outcomes. This finding is most likely related to the whopping 95% of respondents who said they are missing insights from their existing monitoring and analytics solutions.

75% call telemetry important—as **95%** are missing insights.

Given these perspectives, the heightened pace of the digital transformation is unlikely to slow. Businesses and their employees are increasingly dispersed and data-driven, and applications, which frequently rely on modular components and multiple platforms, are increasingly distributed—not only to support remote work but also to provide faster, more interconnected, more entertaining, and more supportive user experiences. Delivering those experiences efficiently and securely requires more telemetry. Only an organization with sophisticated, real-time application data can achieve the insights and automation needed to adapt to conditions and threats across platforms, protect customers and assets, and deliver the extraordinary digital experiences that customers demand.

Among the unprecedented changes to how organizations and individuals use their digital tools, one truth stands out: It is no longer sufficient to think of applications and application security and delivery technology as merely part of an effective IT strategy. Applications have become so central to how we live, work, and interact that it's more relevant to speak of an application strategy as a keystone of any successful business strategy. We've changed the name of this report to the 2021 State of Application Strategy Report to reflect the importance of a strategic approach to applications that supports a distributed business driven by real-time application data.

F5 insight

With applications as the beating heart of our increasingly dispersed but hyper-connected world, no business strategy will be complete without an application strategy—and for many organizations, the two may be nearly synonymous.

Some background on the survey

This, our seventh annual survey, drew more than 1,500 responses from individuals around the world who represented a wide range of industries, organization sizes, and roles. While there were some regional variations—respondents in Asia Pacific identified AIOps as their top strategic trend over the next 2–5 years, for example, while organizations in EMEA favored SaaS—the findings were fundamentally similar across geographies. The survey focused for the first time on IT decision-makers. Its results reliably capture the priorities, concerns, and near-term expectations of the people most responsible for meeting the digital economy's toughest challenges, today and tomorrow—which is coming faster than ever.

01

Digital Expansion Requires Application Modernization

Over the past year, organizations were forced to enable remote work at unprecedented levels and invent new ways of serving customers using technology. These changes have driven demand for digital services in every industry, for every role, and across our professional and personal lives.

For businesses, COVID-19 has accelerated digital transformation. Last year we noted that digital transformation occurs in three distinct phases: task automation, digital expansion, and AI-assisted business. While organizational efforts may focus in multiple phases at once, the emphasis over time indicates change within an organization. The incredible progression of survyed organizations through these three phases in a single year can be seen in the adoption rate of AI and machine learning, a marker of late-phase transformation, which has more than tripled.

More than **three times growth** in AI-assisted business

Last year, organizations were mainly executing in the first two phases of digital transformation, with most focusing on task automation—improving efficiency by digitizing IT and business functions, from the provisioning of virtual machines to accounts payable systems.

This year, the majority have progressed to the second phase, digital expansion. With task automation well in hand, nearly half of digital transformation projects today focus on business process automation, orchestration, and digital workflows, stitching together disparate applications to create more seamless digital experiences. The same objective is being achieved through the use of APIs. With these approaches combined, more than half of all organizations (57%) are deep in the second phase of their digital transformations.

Meanwhile, only a slightly smaller majority of respondents—56%—is already moving into the last phase, turning to AI for a broad range of advanced processes. These include performance analysis, anomaly detection, and other AI-based security methods that can help protect growing portfolios of digital assets against increasingly sophisticated attacks. The pandemic, one driver of the acceleration, will eventually be resolved, but related integration, automation, and reliance on data will persist.

Progress in Digital Transformation

We asked:
Please select the projects that are the current focus of your digital transformation mission. Select all that apply.

We learned:
The largest majority of organizations are undertaking digital expansion projects focused on scaling their businesses with technology.

Phase 1: Task Automation

25%

↓ From 45% in 2020

Phase 2: Digital Expansion

57%

↑ From 37% in 2020

Phase 3: AI-Assisted Business

56%

↑ From 17% in 2020

Modernization efforts have more than doubled

With a relatively small fraction of organizations still preoccupied with automating tasks, application modernization has become the focus for CIOs in the second phase. Modernization is necessary when legacy systems are too rigid to adapt to rapidly changing business conditions—from new competition to pandemic restrictions—which is why digital applications are becoming the default. More than three-quarters of respondents (77%) told us they were modernizing internal or customer-facing applications. That's an increase of 133% over last year.

133% increase in organizations modernizing apps

Some types of applications are more likely to receive this attention than others. IT service desk applications take priority, probably because of their potential to improve the efficiency of workers across the organization. Applications that impact the customer experience, particularly those for customer service, ranked close behind, since business success, and even survival, depend on them.

Of course, there are many ways to modernize applications. The methods can be grouped into four broad categories:

1. Enabling modern interfaces via APIs.
2. Enabling modern interfaces via modern components.
3. Refactoring to adopt modern architectures and design approaches.
4. Performing lift and shift to the public cloud, effectively modernizing operations.

About two thirds of respondents are using at least two methods to create modern workloads—the combination of traditional and modern app components that result

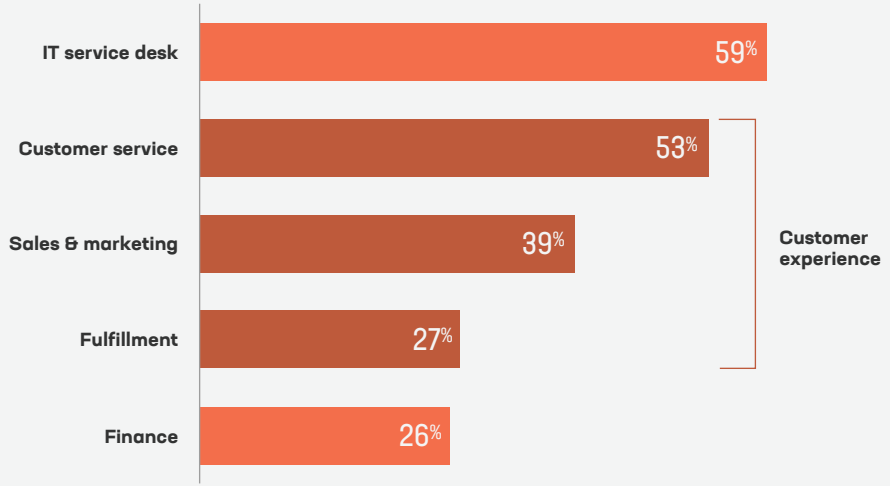
Modernization Priorities

We asked:

Which business functions are priorities for your digital transformation initiatives? Select all that apply.

We learned:

Once employee productivity is well supported, functions that improve the customer experience take priority for modernization.



from modernization. Of those using only one method, 44% are enabling modern interfaces, either via APIs or components such as containers. A mere 11%—largely technology organizations—are exclusively refactoring applications. All methods are valuable, and every organization must balance the costs and complexities of maintaining older systems with the data and knowledge it will lose if it starts from a clean slate. This is one reason adding a layer of APIs to enable modern interfaces can often be the most practical and cost-effective way to meet the needs of digital-native consumers while maintaining the necessary data security of legacy systems.

The reliance on APIs increases the importance of application security and delivery technology

The popularity of APIs has significant implications for application security and delivery technology. APIs are vulnerable attack targets because, by definition, they expose application logic and sensitive data to other applications or third parties. As they proliferate, organizations need to mitigate the growing risk by deploying API gateways (which provide a layer of security) and API security services (which can protect the business logic). As you'd expect, the more API calls an organization handles, the more likely it is to have adopted both security options to ensure the benefits of digitalization are not outweighed by the security risks.

Organizations handling more than 10 million API calls per month, such as those in financial services and healthcare, are nearly twice as likely (68%) to have deployed an API security solution as those handling fewer than 1 million API calls per month (37%). As modernization proceeds, we expect deployments of API services to increase.

F5 insight

The explosion of app modernization and the integral role of APIs in digital ecosystems create the need for an API-first application security and delivery strategy. API-related vulnerabilities and mitigating technologies that once received little attention must become essential concerns to manage the expanded attack surface.

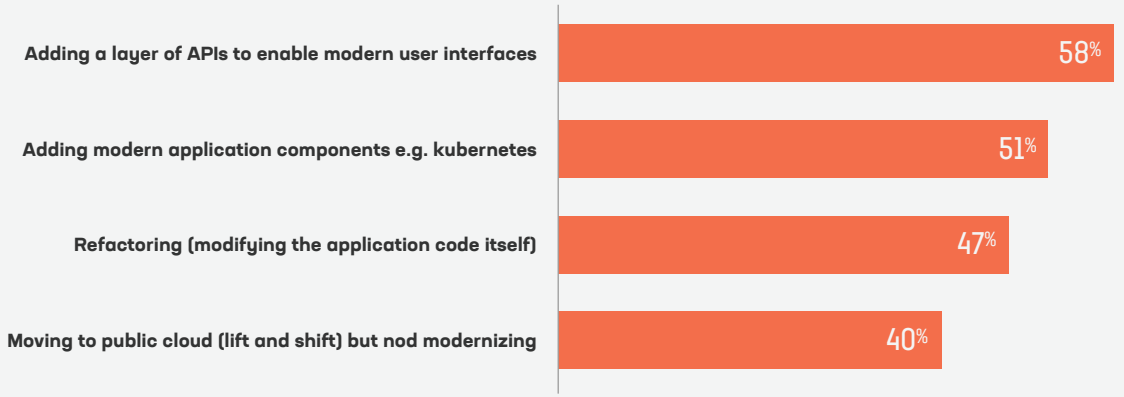
Modernization Methods

We asked:

What methods are you using to modernize applications?

We learned:

While most organizations use two or more methods, APIs are the most common.



02

Complexity Rises as Modernization Proceeds

As applications are modernized to drive digital transformation, the composition of the enterprise app portfolio shifts. When 2021 survey results are compared with those from 2020, we see that traditional applications, especially those built for client/server and three-tier architectures, are slowly being replaced by modern and mobile applications.

Application portfolios are evolving as a natural consequence of older, legacy applications being consolidated, superseded, or replaced, with three types of change responsible:

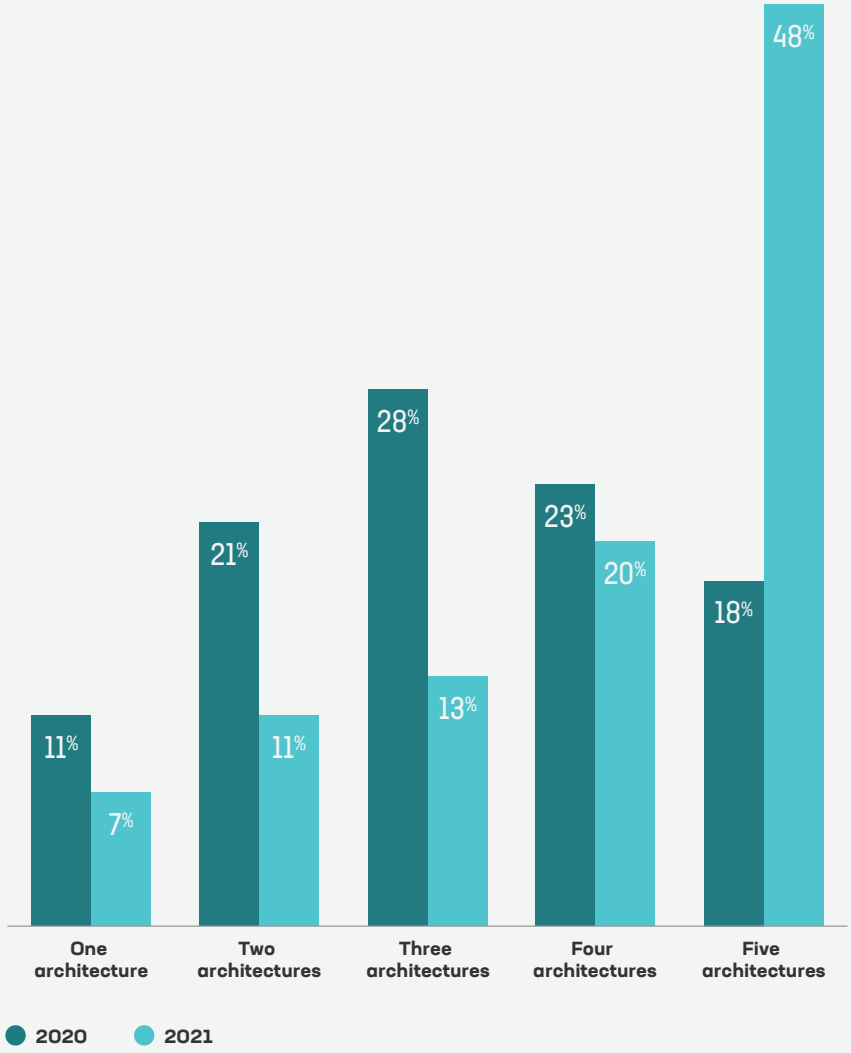
- Traditional but aging applications that once served as a user interface are retired and replaced by modern and mobile applications.
- Creating new applications and extending others with APIs and modern components—part of efforts to provide customers with satisfying digital experiences—necessarily increase the application workloads in the portfolio and add new tools into the tech stack.
- Traditional applications are increasingly replaced by SaaS as vendors offer new, cloud-friendly alternatives.

Survey respondents noted a dramatic decrease in client/server and three-tier web architectures, which dropped twelve points and four points, respectively. Both were used from the 1980s through the early 2000s as “modern” interfaces, compared to monolithic, core business applications. Today, those applications are increasingly being provided by SaaS, as indicated in the deployment plans of survey respondents. (Keep reading for more about that.)

As digital transformation efforts continue, we expect ongoing reductions in the share of traditional applications and architectures and similar, but smaller, increases in modern architectures as they replace older systems. And while traditional architectures are on the decline, most organizations will continue to manage multiple architectures in complex portfolios that are likely to keep expanding as new technologies emerge.

Architectural Proliferation

Complexity rises as an increasing number of organizations operate multiple application architectures.



On-premises deployments aren't going away

Alongside the modernization occurring today and the urgency to transform created by COVID-19, the survey data suggests that some applications will remain on premises and others may be repatriated to accommodate significant interdependencies. In particular, traditional applications that are tightly coupled to core business functions likely will remain in on-premises data centers because the risk of disruption is too high.

As a result, the vast majority of organizations will continue to manage both traditional and modern applications and architectures. This expectation is supported by the 87% of survey respondents who say they juggle both now—an 11-point jump compared to last year.

In fact, most organizations are operating more architectures than ever, with nearly half managing five different architectures, a full 30 points higher than in 2020.

Nearly half of organizations manage **five architectures** or more.

This level of complexity has major implications, not only for IT tools and skillsets but also for how organizations ensure security and performance for applications hosted in a variety of environments.

Applications must be managed across on-premises and cloud data centers and the edge

COVID-19 is a key reason for this year's growth in the number of architectures. According to nearly half of survey respondents, the pandemic accelerated their organizations' movement to the cloud and to SaaS. This trend was already underway, but it jumped forward when workloads were redistributed away from on-premises

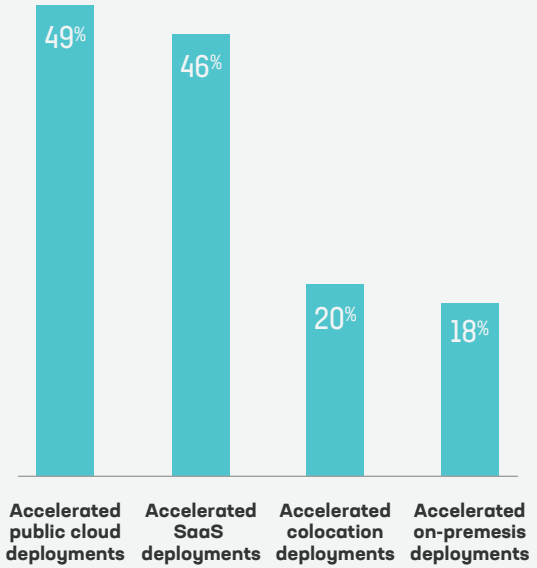
Accelerating Movement to the Cloud

We asked:

How has COVID-19 changed the pace of your deployment of applications within each of these models?

We learned:

Nearly half of respondents accelerated their public cloud and SaaS deployments, while the majority maintained consistent deployment levels for colocation and on-premises.



data centers to address a suddenly remote workforce and digital-first economy. Application deployments in the cloud (both IaaS and SaaS) are accelerating, while the pace of on-premises deployments slowed.

This pandemic-fueled interest in the cloud is unlikely to be reversed. Looking forward, more than three-quarters of organizations plan to maintain current deployment levels across public clouds, colocation, and SaaS. On-premises deployments will continue, with slightly more than half of organizations expecting to maintain their current levels. But even as 27% of respondents have repatriated or plan to repatriate applications from the public cloud, the platform has proven viable. Workloads will flow between cloud and on-premises data centers as it makes sense for the organization.

`

Application security and delivery technology solutions are on the move, too

As applications are deployed in the cloud, the application security and delivery technology that protects and optimizes those apps must be deployed with them. The critical roles these enabling technologies play for customer experience and service level agreements (SLAs) are recognized by nearly four of five respondents.

Four of five call application security and delivery technology critical.

More than 70% of organizations host application security and delivery technology in on-premises data centers. With cloud deployments increasing, more than two-thirds of respondents also host application security and delivery technology in the cloud—nearly at parity with on-premises deployments. The two are not mutually exclusive, since the average organization uses two hosting locations. Meanwhile, 15% of organizations are already hosting application security and delivery technology at the edge.

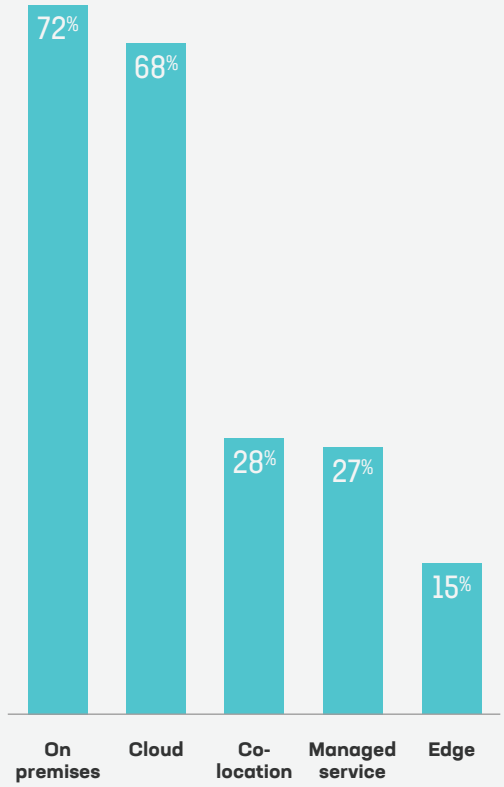
Hosting Locations for Application Services

We asked:

How are your application services hosted? Select all that apply.

We learned:

Cloud deployments are nearly as common as on-premises deployments.



The multi-cloud family expands with the edge

Our increasingly distributed reality has made the edge a new imperative. Cloud data centers, while supporting ubiquitous access, are only slightly more distributed than on-premises data centers. By contrast, the edge enables organizations to deliver applications closer to users. In a sense, the edge is just the next step outward in an expanding universe of distributed applications, with benefits—and drawbacks—aligned with those of multi-cloud strategies. Data analytics represents a key edge use case, enabling the insights required for digital transformation initiatives. It's no wonder that 39% of respondents reported that edge computing would be strategic in the coming years.

Another use case for the edge is the distribution of modern workers. A plurality of organizations plans to continue supporting at least a partly remote workforce. More than a third (42%) will support a fully remote workforce for the foreseeable future. Only 15% plan to require all employees to return to the office. With remote work becoming the norm, businesses face increased pressure to provide secure, fast remote access to all applications—including any that may have been less accessible in the pandemic's first year.

Recognizing the advantage of decreasing latency, over three-quarters of respondents have already deployed or plan to deploy application security and delivery technologies at the edge. While organizations are using the edge for a variety of reasons, the most common are improving application performance and collecting data or enabling analytics.

While an edge deployment can indeed improve performance and processing speed, edge security is an open question. It follows that respondents identified the secure access service edge (SASE) as a key strategic trend, with 56% identifying it as the top trend.

Top Edge Use Cases

We asked:

What are the primary use cases underpinning your current or future edge deployments? Select all that apply.

We learned:

Application performance improvement is the top goal.

Application security and delivery technologies must apply everywhere

Security concerns motivate an increasing percentage of respondents who plan to deploy performance and security-related application technology in the next 12 months. More than a quarter of organizations, on average, are making such plans, particularly for solutions that enable remote work.

No matter where such application security and delivery solutions are hosted, they need to be ubiquitous—available in all environments for consistency and ease of use.

Because 100% want application security and delivery technology in all environments, **the importance of multi-cloud availability jumped five spots.**

While ease of use is still the top criteria for those making decisions, multi-cloud availability is now number three, up from number eight last year. This jump can be attributed, at least in part, to the growing percentage of organizations managing multiple architectures. In that context, multi-cloud availability may be partly synonymous with "easy to use."

In considering these trends, a question arises: How do organizations determine whether their efforts are improving application performance? Survey respondents had plenty to say about the state of monitoring and telemetry in their enterprises.

F5 insight

The fast-moving efforts to modernize applications, improve their performance, and enhance the digital experience will intensify IT management challenges. First, architectural complexity will only increase as organizations pursue SaaS and edge strategies while maintaining on-premises data centers. This growing complexity will exacerbate existing issues with tool or skill availability, IT processes, and cross-architecture analytics.

As a result, application security and delivery technology that's easy to use and works across architectures is more crucial than ever—not only to make the lives of IT teams easier but because without such support, other efforts to improve performance, including a move to the edge, can't yield optimal returns.

03

Organizations Have Data but Lack Insights

As digital transformation proceeds, the organizations best able to harness data from their applications, APIs, and app security and delivery technology will enjoy a competitive advantage based on the ability to make better, faster decisions and more quickly act to protect application performance and data. According to survey respondents, however, sufficient data does not necessarily deliver the insights they really need.

What causes the gap? It's apparently not the tools. More than half of respondents believe they already have the tools they need to report on the health of high-priority applications. What may be missing, based on survey responses, are related skillsets, as well as consensus on what the data should be used for, when, and by whom.

59% say they have the data tools they need.

Respondents from across roles agreed that the data collected by these tools is primarily used for troubleshooting, followed by early warnings about performance problems. A mere 12% report the data back to business units—suggesting that most organizations have not fully recognized that business and technology are increasingly intertwined.

Opinions about the purpose of telemetry differ

Note, however, that when asked about application monitoring relative to their modernization efforts, respondents reveal an apparent disconnect between the use of data from existing applications and from the components that modernize those apps (such as APIs). Specifically, fewer than one-quarter of organizations use data and insights to watch for potential performance degradations. As noted, the majority are more concerned with troubleshooting, using those insights only after a problem has become apparent. By contrast, when it comes to monitoring components that modernize apps, nearly two-thirds of respondents (62%) are measuring performance in terms of response time. While this data may be used primarily to track performance against SLAs, it can serve as an early warning system before problems affect the user experience.

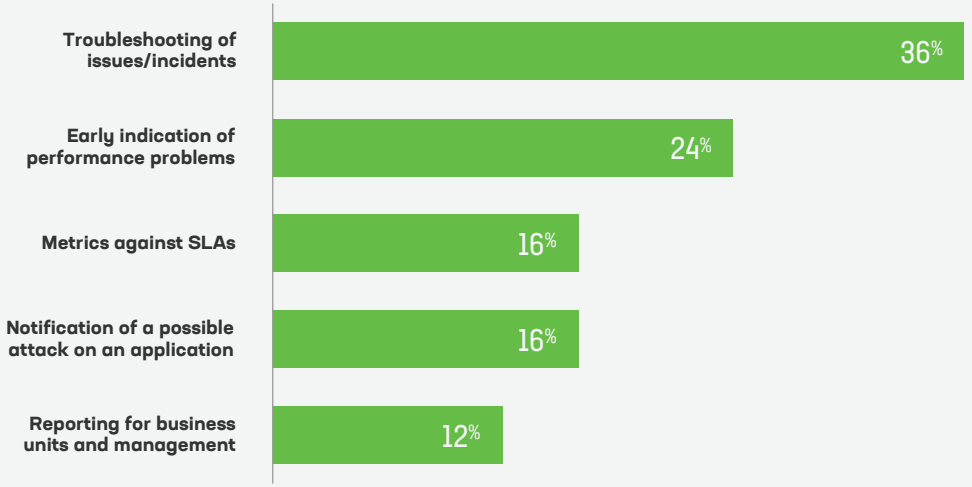
Top Uses for Application Insights

We asked:

As you think about the ways in which you use data and insights about application health, performance, and security, what is the most valuable to you? Select one.

We learned:

Troubleshooting leads the way while reporting to business decision-makers lags.



Differences of opinion about the purposes of telemetry become significant when considering the overwhelming 95% of respondents who told us they are missing insights from their existing monitoring and analytics solutions.

95% are missing insights about performance, security, and availability.

People across organizational roles say they need more insight than their current tools provide. It isn't enough for a monitoring tool to provide alerts when performance conditions degrade, for instance. Across respondents and roles, the top three missing insights are:

- The root cause of application issues.
- Performance degradations.
- Possible attack.

Depending on their roles, respondents take slightly different views of the most important insight gap, with non-IT senior leaders more focused on performance, while senior IT leaders and security teams focus more on security.

The missing insights align with the purpose telemetry serves in the average organization: meeting SLAs on the way to achieving business outcomes.

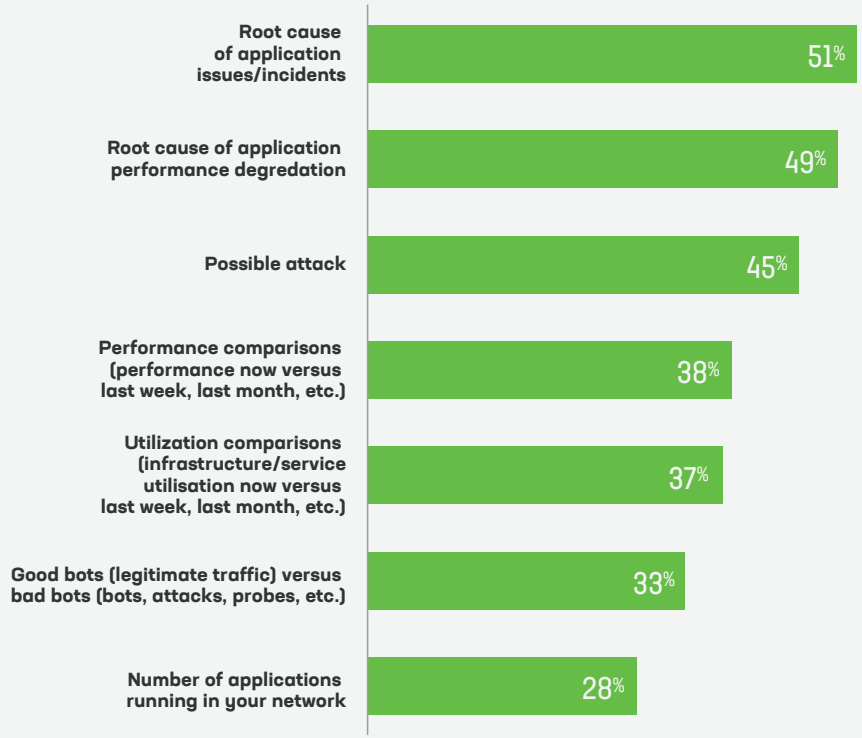
Top Missing Insights

We asked:

What insights are you missing from your monitoring/ reporting/analytics solutions? Select all that apply.

We learned:

Half of organizations need better insight into the root causes of security and performance issues.



Top Missing Insights by Role

Possible attack & root cause of app incidents

53%

Security

Root cause of app incidents

51%

Senior IT Leaders

Root cause of app performance degradation

53%

Senior Non-IT Leaders

Which SLAs are most important to meet—and which are best suited to the support telemetry can provide—can be viewed somewhat differently. Organizations turn to telemetry today for application security, availability, and performance, in that order.

More than 80 percent of respondents said data and telemetry were very important to security, and the frequent use of telemetry to meet security SLAs aligns with the high value leaders place on security-related solutions and their contribution to business outcomes. As always, security includes both keeping the business safe and protecting customers and their data from fraud. But just as leaders in different roles disagree somewhat on which insights they're most missing, there are two notable gaps in the importance they place on protecting various attack targets.

Senior IT leaders consider it more important to protect the infrastructure than non-IT senior leaders do—a result that probably reflects both deeper understanding of the infrastructure's importance and their personal responsibilities. What's more unexpected is the relatively low value senior IT leaders place on protecting the business from attack compared to their non-IT counterparts. We interpret this as an indicator that IT leaders see themselves as business enablers but not yet full partners in the achievement of business goals—that IT helps the business, but not that IT is the business. The latter mindset is characteristic of the third phase of digital transformation, and many organizations just aren't there yet.

Use of Service-Level Agreements

We asked:

Which of the following service-level agreements (SLAs) do you apply to the components that modernize traditional applications?

We learned:

Application services are important to meeting these SLAs, and telemetry from those services can help.

To drive digital transformation forward and further integrate IT into core business strategies, analytics need to better provide critical insights tailored to the concerns of leaders in different roles and with different priorities and concerns.

AI-assisted business improves adaptability

AI-assisted technologies can provide these missing analytics. That's one factor driving IT toward AI operations (AIOps). AIOps can be defined as platforms that combine big data and machine learning to enhance a broad range of processes and tasks for IT operations, including performance analysis, anomaly detection, and event correlation. With AIOps, organizations can better manage large volumes of data and use it to predict and mitigate availability and performance issues. Survey respondents picked AIOps as the second most strategic trend for the next 2–5 years.

Senior IT leaders rank protecting the business **below protecting applications and infrastructure.**

As AI increasingly takes hold, particularly for those organizations farther along in their digital transformations, businesses will be able to capitalize on a parallel evolution from visibility—with its focus on postmortem analysis—to real-time observation and control. They'll gain the ability to respond faster to changing conditions and threats, especially when aided by automation, so they can deliver the great customer experiences that result in higher conversion rates, greater retention, and increased profitability. This stage, marked by real-time observation and control, is where nearly three quarters of survey respondents find themselves now, at least in part, although a significant two thirds of all respondents are still missing basic insights of visibility they need.

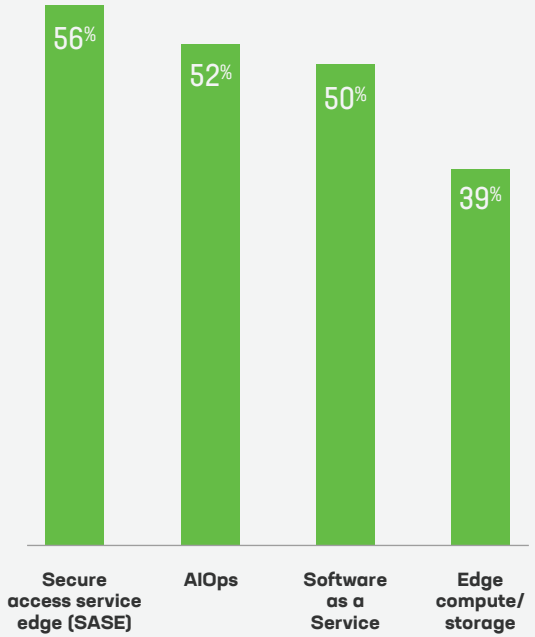
Top Trends

We asked:

Which technology trends do you think will be strategically important for your organization in the next 2-5 years?

We learned:

While SASE is the top trend, more than half of respondents are also looking to AIOps to help them deliver the insights and automation needed for higher performing, more secure applications.



More than half, however, are already looking forward to the impact of AI, which can help them transition toward applications that can adapt proactively and in real time to better defend themselves and respond to situational changes.

The strategic importance of AIOps is not only about adaptability, though. Growing challenges in automation also make AIOps an important trend for the near future.

Automation is not automatic

Automation is fundamental to digital transformation, but there is risk in assuming you can simply provide IT with the right tools and APIs and automation will magically ensue. Although the majority of organizations feel they have the toolsets they need, almost as many are experiencing significant frustration related to those tools—whether cross-IT or vendor-specific. That frustration is largely caused by integration across existing toolsets and insufficient budgets for others that are needed.

An even greater challenge, however, is a skills deficit. This is particularly true for those who called AIOps their top strategic trend. Half of those respondents cited a lack of skilled professionals as their top challenge.

47% struggle to find the talent they need.

Organizations focused on AIOps generally agree with others in their ranking of automation challenges. The lack of toolset integration across vendors and devices ranked second, with 44% calling it a problem. Lack of budget for new tools came in a close third at 42%.

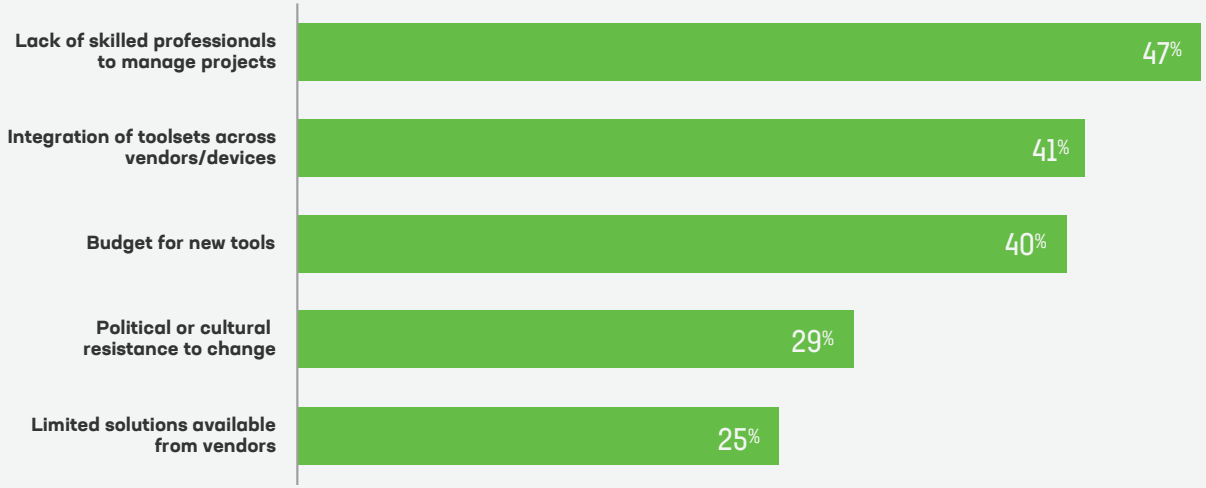
Automation Challenges

We asked:

As you think about the use of automation in the network, what do you find challenging, frustrating, or difficult? Please select up to three.

We learned:

Finding professionals with the right skills is a significant automation challenge.



These challenges are among the reasons ease of use is the consensus top criteria for application security and delivery technology solutions. But the struggle with tools and talent also likely increases the value of solutions that are available in all environments. A solid majority (52%) of organizations facing toolset challenges value such availability. Even more organizations without adequate skills (57%) value multi-cloud application security and delivery technologies. And no wonder, since part of the value of such solutions is their ability to extend domain expertise across environments. Rather than learning to operate a new offering—whether a service of the cloud provider or another vendor—practitioners can confidently provide the same solutions in every environment.

Treating infrastructure as code is beneficial

In this fraught environment for automation, just over half of respondents say they now treat infrastructure as code. In other words, they provision and manage infrastructure, including platforms, container systems, and services, through declarative or scripted definitions—code. Those definitions take the place of manual configuration or traditional configuration tools. As a result, configurations, policies, profiles, scripts, and templates are separated from the hardware or software on which they're deployed and can be stored, shared, revised, and applied like code can.

Organizations that use this approach reap tangible benefits. Specifically, they are:

- Twice as likely to deploy more frequently, even when using automation.
- Four times more likely to have fully automated application pipelines.
- Twice as likely to have more than half of their application portfolios deployed using fully automated pipelines.

These results suggest that treating infrastructure as code is a key to enabling AIOps, which increases efficiency and operational scale by automating security and optimization of the digital experience. Application rollouts that are faster, more consistent, and more secure also benefit customers by more effectively delivering delightful features and experiences, which translate into revenue. We expect more organizations to adopt this "secret sauce" as digital transformation proceeds.

Those treating infrastructure as code are **four times more likely** to have fully automated application pipelines.

F5 insight

With a scarcity of skills and architectures of increasing complexity, treating infrastructure as code can help enable the automation required to move toward a more AI-assisted business and the improved security and customer experiences AI can deliver. For most organizations, greater progress in the third phase of digital transformation will involve not only more automation and telemetry but also a cultural change in which business units use the resulting data for strategic decisions, with IT as an integrated partner as well as an enabler.

Conclusion

Rewarding Customer Experiences Hinge on Successful Digital Transformation

In many ways, organizations around the world have risen admirably to the challenges of COVID-19 and its accompanying upheaval. Faced with unexpected and urgent shifts in how work, customer interactions, and daily living were accomplished, they responded with effective technological solutions.

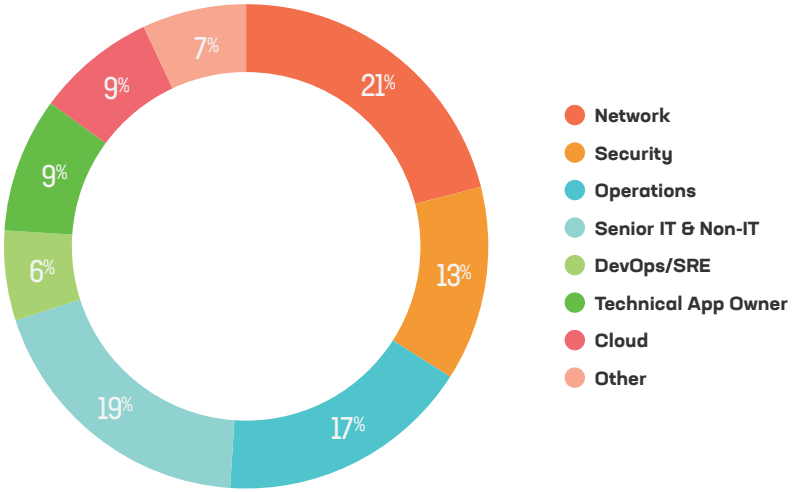
In a short time, they have modernized and distributed applications—and the application security and delivery technology solutions that support them—closer to users. Add in use of the edge, which is helping to improve performance and the user experience, and these organizations have greatly accelerated their digital transformations and now are generating incredible momentum toward realizing applications that are truly adaptive.

More progress will require advances in two areas. The first is real-time application data. The second is the insights that data can deliver. Telemetry from application security and delivery technology must be available in every deployment location to provide those insights, as well as the automation that will enable more responsive, higher performance and more secure applications. Only organizations with the right combination of insights and automation will be able to sort through overwhelming data, recognize looming availability and performance issues before they occur, and act quickly enough to prevent them to ensure customer experiences remain delightful.

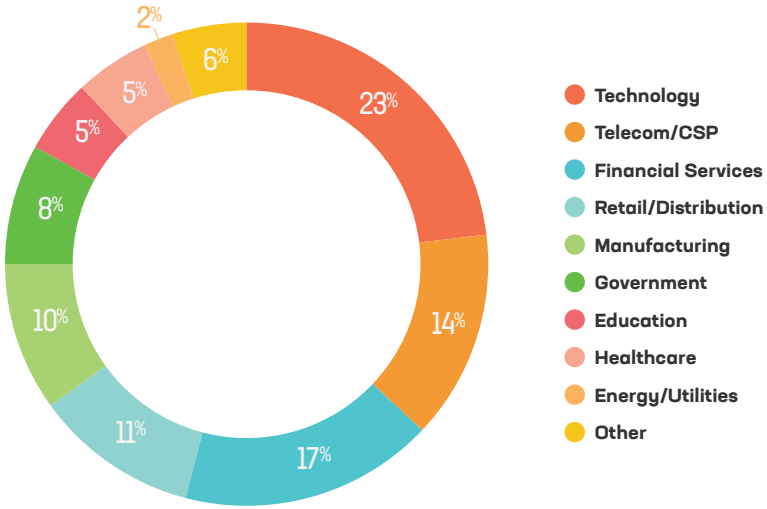
Until then, many organizations won't be able to take full advantage of their progress in digital transformation or generate additional speed toward AI-enabled business. To achieve those goals, organizations need an application strategy that includes application security and delivery technology solutions that follow the apps, even as deployments continue to be spread among multiple environments positioned nearer to users and at the edge. Management of multiple architectures, and deployments that cross them, will continue as the norm, even as modernization proceeds. For such complex portfolios, multi-cloud availability will be critical. Only easy-to-use, multi-cloud solutions can deliver the telemetry needed to uncover insights and enable the AIOps that will improve the customer experience—the objective of digital transformation and the source of its value.

Appendix: survey methodology

For this seventh annual survey, F5 surveyed people across a range of company sizes and industries. In all, we heard from 1,544 respondents validated as having job responsibilities related to IT solutions. These ranged from corporate senior management to IT roles. For the first time, respondents were screened based on their degree of responsibility for making or influencing purchase decisions.



Respondents also work for a broad swath of industries. Technology and financial services were especially well represented, but the results incorporate a range of interests, from manufacturing and retail to education and government.



Many industry surveys attract only a few hundred respondents or focus on particular business segments. The strong and broad response to this survey—in a year with pandemic disruption and related screen fatigue—gives us a high level of confidence in the results and their general applicability.