2022

State of Application Strategy Report

At a Glance

THE EIGHTH ANNUAL F5 survey on the state of application strategy found that digital transformation continues to accelerate around the world. Modernization of applications and architectures is permeating more deeply into organizations to transform back-office functions as well as those that directly impact the customer experience. However, the survey results also indicate pitfalls ahead that, if ignored, may inhibit further progress. In particular, the risks may prevent effective use of artificial intelligence (AI) to make business more responsive and agile.

Highlights of the findings include:

- **Business today is digitally enabled,** and the need to increase automation is driving a convergence of IT and operational technologies (OT)—a trend survey respondents ranked as the most exciting over the next several years.
- **Hybrid cloud architectures and their complexity—and challenges—are here to stay,** as evidenced by an unexpected jump in app repatriation and the fact that 70% of organizations manage five different application architectures.
- **Application security and delivery technologies are no longer necessarily tethered to the applications they serve** but are deployed in different environments and may support multiple applications.
- **Security increasingly focuses on identity.** As organizations embrace the principles of zero trust, identity and access management technologies—used by 96% of respondents—are now the most commonly deployed category of app security and delivery technologies.
- **Threat mitigation is maturing**. With greater leadership alignment on the importance of security, the desire to unilaterally block all threats is evolving toward a more balanced risk-management approach.
- **Nearly everyone lacks critical insights** into the root causes of performance degradations, outages, and threats. These missing insights represent a significant risk to the nine in 10 organizations planning to adopt AI to support business operations.
- **New approaches are needed**. Site reliability engineering (SRE) practices help organizations better manage complexity, but the real solution will require more strategic change.

Read more of the sometimes surprising results in the F5 2022 State of Application Strategy Report.

Contents

03 Executive Summary

07 Modernization Is Expanding Throughout Organizations

11 The Application Landscape Keeps Changing

15 App Security and Delivery Technologies Are on the Move

20 Security Is Evolving Toward Risk Management

24 Challenges Require More Strategic Attention

29 Conclusion

30 About the Survey

Executive Summary
Digital Expansion Speeds Toward Disruption Ahead

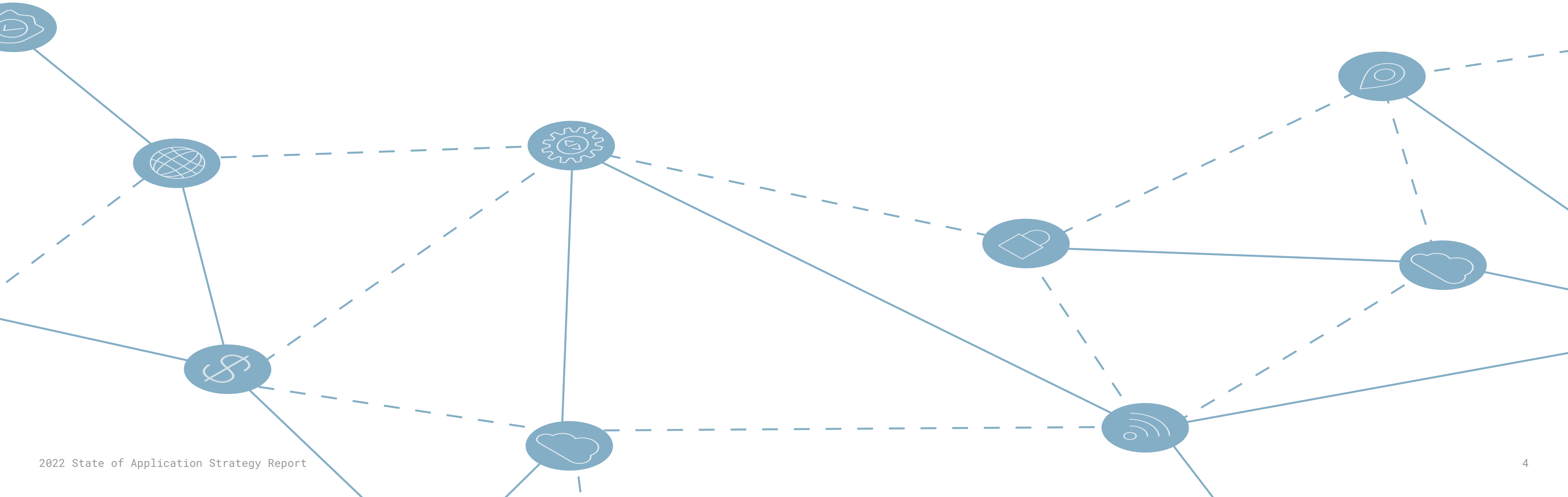
AMID WIDESPREAD DIGITAL transformation, IT objectives and business objectives are converging to increasingly elevate technology from a supporting role to driving the business. It's no exaggeration today to say that every business is a digital business. Technologies ranging from remote work solutions to virtual medicine are transforming society. The need to adapt the business to add value for customers, seize new opportunities, and respond to attacks in real time is fueling widespread interest in artificial intelligence (AI), which can streamline how work gets done.

But there's a breakdown blocking the fast lane to that future—because as digital transformation expands, the exploding numbers of applications, integrations, and environments are creating complexity that is increasingly unmanageable. The average organization today manages more than 200 applications—in addition to using several third-party as-a-Service offerings. These apps are deployed across data centers, multiple clouds, and the edge. Plus, most organizations rely on nearly two dozen different application security and delivery technologies, which are increasingly deployed where they can be most effective rather than being tethered to the deployment model or location of the applications they serve.

This complexity will continue to grow, because more than two-thirds of organizations have realized that creating superior digital interactions for customers requires also modernizing less visible business processes and back-office functions. Those operational tasks need to be automated to prevent them from becoming bottlenecks. Failure to use data quickly enough to source raw materials, hire employees, plan production, or complete a plethora of other support tasks can degrade customer relationships, delay time-to-market for new offerings, and hurt the bottom line.

Most organizations manage **200-1,000 apps**.

Until recently, modernization projects have focused primarily on optimizing the digital experience for customers, from shopping carts and delivery tracking to customer support chatbots. Now, to capture the full value of those modernizations and position themselves to realize the benefits of AI, a majority of survey respondents are expanding their digital transformation efforts to include internal functions deeper in the organization. For instance, in 2022, IT operations became a priority focus for 78% of survey respondents. That's up from 62% in 2021.



Most exciting development: **the convergence of IT and OT**.

This operational emphasis is also reflected in the plurality of respondents who called the convergence of IT and operational technology (OT) systems the most exciting development over the next few years. OT systems monitor events, processes, and devices to help businesses manage industrial and enterprise operations. Examples range from supervisory control and data acquisition (SCADA) systems managing the speed of production machines to automated control systems for building lighting, temperature, and access. Integrating OT systems like these with data-centric IT systems will help close the automation loop and make digital businesses more adaptive so they can better anticipate and respond to shifting customer interests and market conditions.

Disruption lies ahead

But look out for disruption ahead, because for most organizations, maintaining momentum and capturing the full value of digital transformation efforts will require systems and resources not currently in place.

For instance, nine in 10 organizations across industries plan to better serve customers by implementing AI or machine learning (ML):

- Of those, more than three-quarters (76%) anticipate using the results to support their lines of business, whether that means targeted customer purchase recommendations or AI-assisted medical treatments.
- Security purposes such as real-time fraud identification rank a close second, at 71%.

Just over half (52%) plan to use AI in IT operations, which leaves the remaining 48% of IT teams struggling to secure and manage hundreds

AI Implementation Plans

We asked:
In what areas are you using or do you plan to use AI and ML? Select all that apply.

We learned:
More than three-quarters of respondents are using AI to support their lines of business.

76%
Use or plan to use AI for lines of business

71%
Use or plan to use AI for security

52%
Use or plan to use AI in operations (AIOps)

of applications using largely manual processes—the equivalent of building and supporting a rocket with hand tools and an ox. It may be technically possible, but it's not easy, safe, or scalable.

In addition, regardless of the AI use case, it's likely to be difficult to extract and process the telemetry from their applications and application security and delivery technologies. To successfully mine data currently trapped in bespoke clouds or on-premises silos and use it to enable greater automation, security, and efficiency, it won't be sufficient for organizations to modernize and scale applications alone. They also need to modernize the operational systems behind them. That means automating, integrating, and scaling typically manual processes for app deployment and management, including the means for leveraging telemetry to drive change.

But many IT organizations simply don't have the resources. The skills gap continues to widen, and a whopping 98% say they don't have the insights they need now to address business objectives and improve the customer experience.

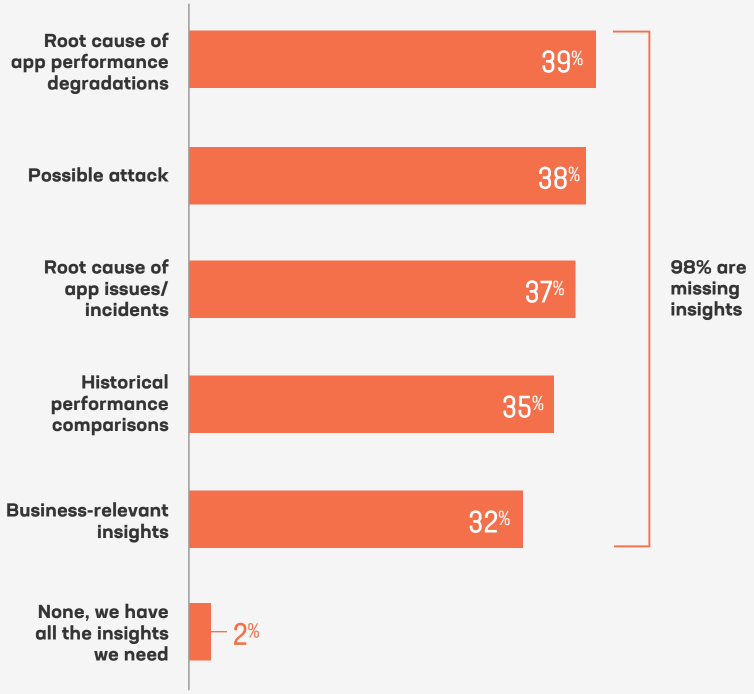
Meanwhile, security threats proliferate, and fragmentation across multiple environments with insufficient automation is fostering fragility. The difficulty of stitching applications together into a secure, consistent portfolio continues to grow. In an increasingly digital economy, leaders can't ignore these behind-the-scenes challenges and still expect to succeed.

Fortunately, other trends that surfaced in our survey results—including the rise of site reliability engineering (SRE) practices and the benefits enjoyed by organizations that use them—suggest a successful path forward. Significant additional progress in the digital transformation journey will require entirely new approaches for managing telemetry, data, and application security and delivery technologies across today's distributed architectures.

Missing Insights

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

We learned:
Only 2% have all the insights they need, and most respondents are missing more than one type.



01
Modernization Is Expanding Throughout Organizations

AS NOTED IN previous State of Application Strategy reports, digital transformation efforts typically proceed through three phases:

1. Task or process automation
2. Digital expansion
3. AI-assisted business

For our 2021 report last year, we saw the percentage of organizations working in the later phases leap forward as they rapidly adjusted to a suddenly remote workforce, distanced customer interactions, and other effects of the global COVID-19 pandemic. Today an even larger majority are scaling their businesses with technology, and nearly two-thirds are currently working on AI-related projects.

But the percentage of organizations working in phase one—business task automation—has grown too. First, more and more businesses are embarking on the journey of digital transformation. In addition, however, adapting to the digital economy is both a long-term and iterative effort, and most organizations tackle projects in multiple phases of transformation. For instance, this year nearly one-third (32%) of financial services organizations are automating business tasks in phase one even as more than half (58%) simultaneously have AI-related projects in phase three.

While improving the customer experience has been a priority focus for a majority of these digital transformation initiatives—and remains a priority for nine in 10—modernization activities increasingly address internal processes, too. In the many global labor markets where skilled workers are scarce, the employee experience is also important. Plus, organizations can't afford to let manual, paper-based processes—from employee onboarding to compliance management—constrain the organization's agility in an accelerated digital economy. That's particularly true for IT operations, which won't be able to implement production-scale AI without the data mining and process automation required. As a result, modernization efforts are accelerating.

Activity in the Three Phases of Digital Transformation

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

We learned:
Nine in 10 organizations are executing on digital transformation, with most organizations active in multiple phases at once.

Phase 1:
Task automation

33%

↑ From 25% in 2021

Phase 2:
Digital expansion

70%

↑ From 57% in 2021

Phase 3:
AI-assisted business

61%

↑ From 56% in 2021

Automating employee and vendor processes

Among the one third of total survey respondents automating formerly manual business processes, certain industries—including education and healthcare—are busier in this phase than others. The overall percentage, up 8 points from last year, likely reflects some organizations just getting started. But the survey results also show digital transformation projects bringing automation to internally focused business functions ranging from human resources processes to customer credit control and vendor contract management. Back-office processes like these previously held lower priority for modernization, especially as organizations scrambled to respond to the pandemic.

> While the customer experience remains a priority for nine in 10 respondents, **modernization efforts are expanding**.

Specifically, over the past few years many companies focused on two broad areas: the IT service desk and the customer experience. Projects to modernize IT support helped to ensure employees could continue to do their jobs efficiently (or, given COVID-19 restrictions, at all). Even more projects tackled an improved digital customer experience, from marketing and sales processes through fulfillment and customer support.

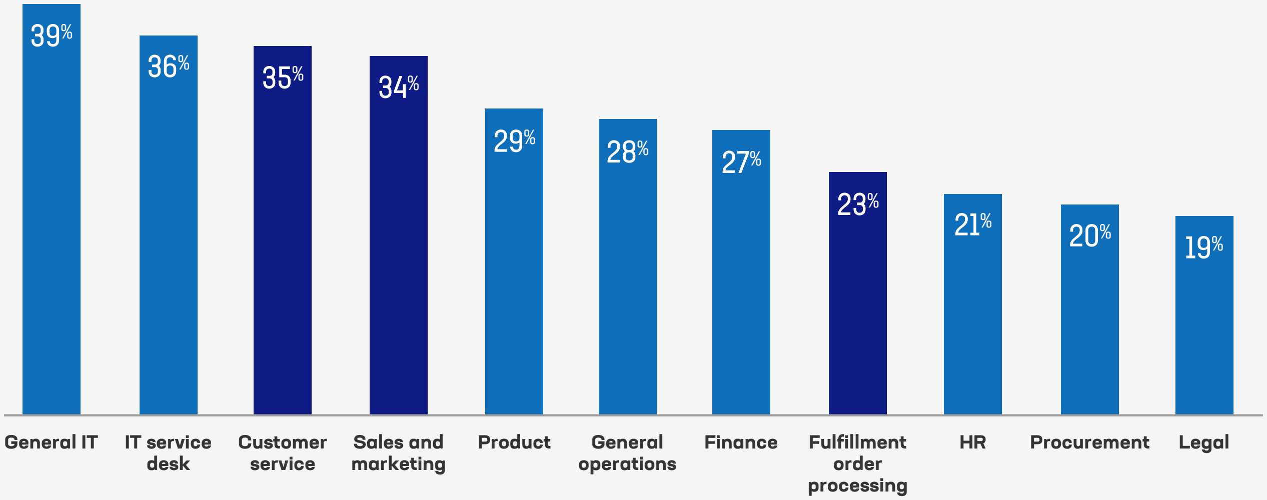
This year, the number of organizations who said they're modernizing various internal business functions and the employee experience jumped. Efforts in human resources, finance, procurement, and other departments have increased, automating and accelerating activities that were once predominantly paper-based and manual. Modernization activities related to products, from design and development to pricing and packaging, occupy 29% of respondents. Another 19% reported that legal functions—a category that didn't appear in previous surveys—have become a priority for digitization, which can prevent these processes from becoming bottlenecks for organizations moving faster than ever to satisfy customer needs.

Digital Transformation Priorities

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

We learned:
While customer-facing functions are still high priorities, modernization is also spreading to many back-office functions.

■ Customer experience
■ Operational/back-office



Just like customer-facing processes, these internal processes need to scale through technology, integrate seamlessly with others, and respond to changes in real time. When they're digitized, they also need the improved security, availability, and performance that application security and delivery technologies provide. Similarly, organizations that modernize internal processes with SaaS often need to integrate those offerings with others while protecting the customer or employee data they consume.

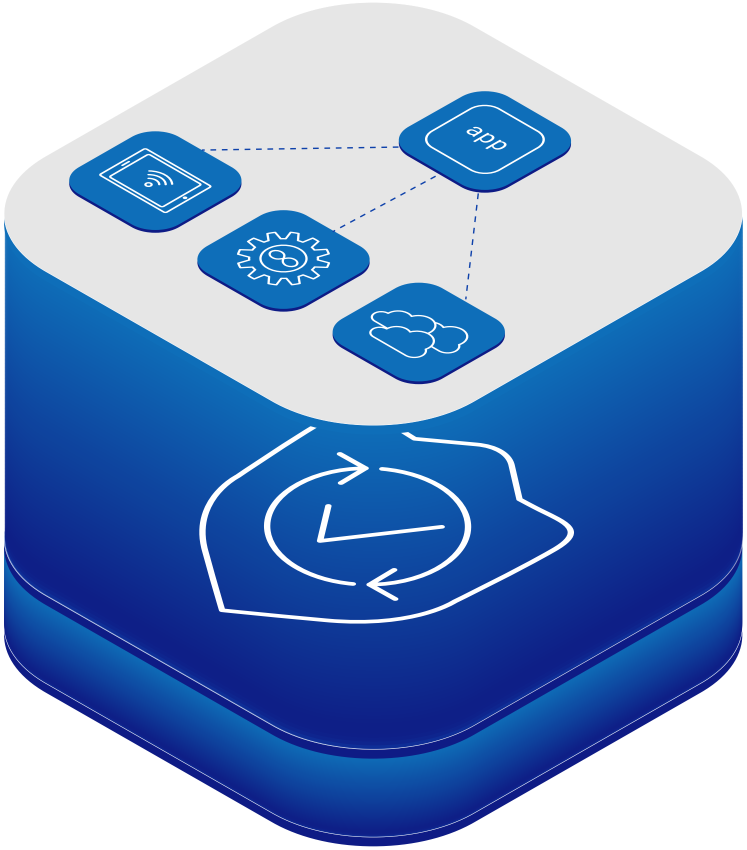
That's why modernization of internal processes is exacerbating complexity even as it automates formerly manual tasks. Organizations are juggling a growing number of applications and the security and delivery technologies that enable them. This portfolio growth isn't uniform, though, and managing those applications is more complex than ever because—as the next section details—the application landscape continues to dramatically change.

F5 Insight

With modernization expanding more broadly across business functions, a consistent approach to securing, delivering, and integrating those applications will be critical to ensuring that back-office applications protect sensitive data and perform as effectively as customer-facing apps.

What this means for you

Smart organizations will resist the temptation to manage their application portfolios by functionality or chase false efficiencies by categorizing which functions need specific security, app delivery, or telemetry services and which can get along without them. Rather, platform-level solutions that provide consistent protection, performance, and data access across the entire app portfolio will be simpler to manage and will better position the organization to implement AI assistance by releasing more data from silos. Only then will the entire business be able to react holistically, in real time, to satisfy customers, innovate, and more quickly bring differentiated services to market.



02

The Application Landscape Keeps Changing

DIGITAL SERVICES PLAY an increasing role in our day-to-day lives, and the average number of applications organizations manage is creeping upward. A growing percentage (41%) juggle between 200 and 1,000 apps. That's up from 31% only five years ago. But at the same time, the largest portfolios are being consolidated, and the percentage of organizations managing more than 1,000 apps is shrinking. This consolidation is natural as older, legacy applications are retired and sometimes replaced by more modern applications, such as team collaboration software, that integrate capabilities previously performed by more than one app.

Such consolidation makes sense because reducing the number of applications to be managed—a form of standardization—can significantly increase the organization's ability to quickly deliver digital services at scale despite deployment decisions and processes that are more complex than ever.

Deployment decisions continue to challenge

Whatever their size, the complexity of app portfolios is an issue, since most IT organizations manage everything from a growing collection of new, container-native and mobile applications to legacy monoliths that are fundamental to the operation of the business. Modernization of older applications—whether through the addition of modern components or APIs, lift and shift to public clouds, or other means—has become nearly universal, with 95% of respondents undertaking such projects—up from 77% last year. But many organizations will likely continue to manage a few legacy applications indefinitely.

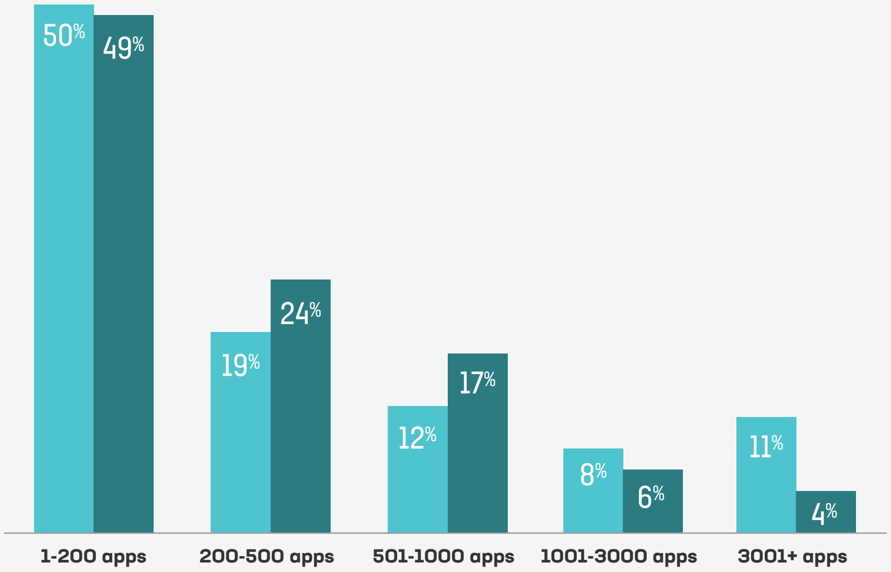
With nearly everyone (88% of respondents) operating both traditional and modern application architectures across a variety of environments including the edge, decisions about where and how to deploy applications and the technologies that support them are harder than ever. The challenges range

Application Portfolio Sizes

We asked:
How many applications does your organization have today?

We learned:
Portfolios are trending to encompass from 200 to 1,000 applications, on average.

■ 2017
■ 2022



from inconsistent security policies and fragmented data to the deployment of point solutions that make sense at the time or for some purposes but ultimately add complexity or degrade performance and therefore increase the overall fragility of the system.

The growth of as-a-Service offerings is another complicating factor that solves some of these problems and yet may create others. More than three-quarters of respondents (77%) say they run applications in multiple clouds. However, 93% use some type of cloud-based as-a-Service offering—often grouped as XaaS. Salesforce, Microsoft Office 365, SAP, and Atlassian are familiar and nearly ubiquitous examples. That means nearly every organization must manage security and performance across multiple environments. Plus, these XaaS offerings are increasingly integrated via APIs into other business processes and proprietary applications, further complicating secure administration.

Organizations use an average of **three XaaS offerings**.

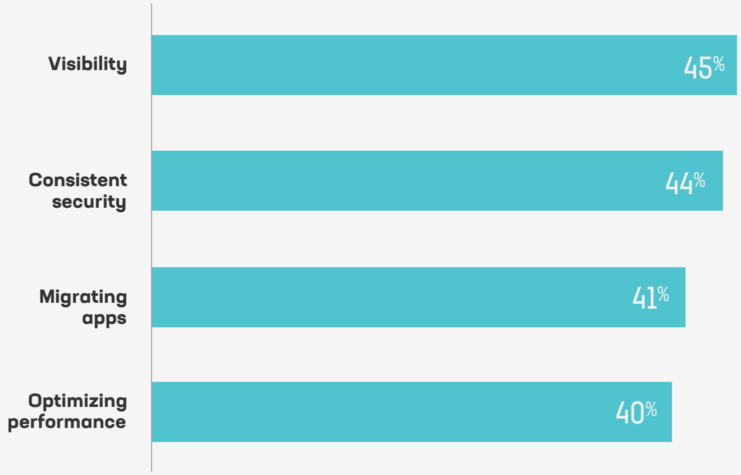
Amid this complexity, it's no wonder visibility across different environments is ranked as the top challenge for those deploying applications in multiple clouds, followed closely by consistent security. These security concerns are rapidly driving organizations to cloud-based security platforms and edge deployments.

The difficulty of migrating applications between complex and disparate environments also remains a top concern for multi-cloud deployments. Nonetheless, this year's survey results reveal a new fluidity of workloads and growing sophistication in deployment decisions. With many apps deployed in multiple locations, on-premises deployment is still the most common, but other hosting locations continue to gain ground. Strong public cloud adoption persists, with three-quarters of organizations reporting that they deploy apps there. At the same time, 92% of organizations host apps

Top Multi-Cloud Challenges

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

We learned:
Visibility tops the list, but many other challenges remain significant, too.



in on-premises data centers, and repatriations—migrating applications from the public cloud back to an on-premises data center—have jumped, with 37% of respondents reporting they'd repatriated apps. Another 30% plan to do so. These repatriations are taking place at a rate more than double the expectations reported by respondents just one year ago.

What's changed? The difficulty of managing multiple clouds is probably a factor, along with public cloud drawbacks that mitigate their acknowledged efficiency benefits. Repatriation rates vary significantly both by region and by industry, but in general, hybrid architectures—and the implications for how to best manage applications across them—are probably here to stay.

But there's also an interesting correlation between repatriation and the adoption of SRE practices, which ease application migration challenges. Read more about this and other benefits of SRE, as reflected in the survey results, in Section 5.

F5 Insight

Hybrid architectures, including on-premises data centers and XaaS offerings, are not going away, while applications and workloads will be increasingly containerized and mobile. That means complexity's here to stay, too.

What this means for you

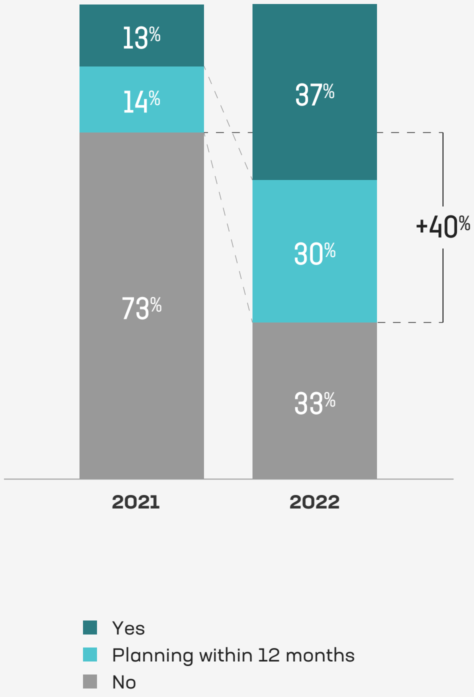
Managing applications and the technologies that support them across disparate environments will remain a challenge. Meeting that challenge is likely to require not only a distributed cloud architecture but also:

- Platform-agnostic security and delivery technologies that provide consistent protection, visibility, and performance for all applications—legacy, modern, and mobile—across environments.
- Real-time telemetry that transcends data silos and intelligent technologies that use the resulting data to drive automation instead of manual integration and administration.

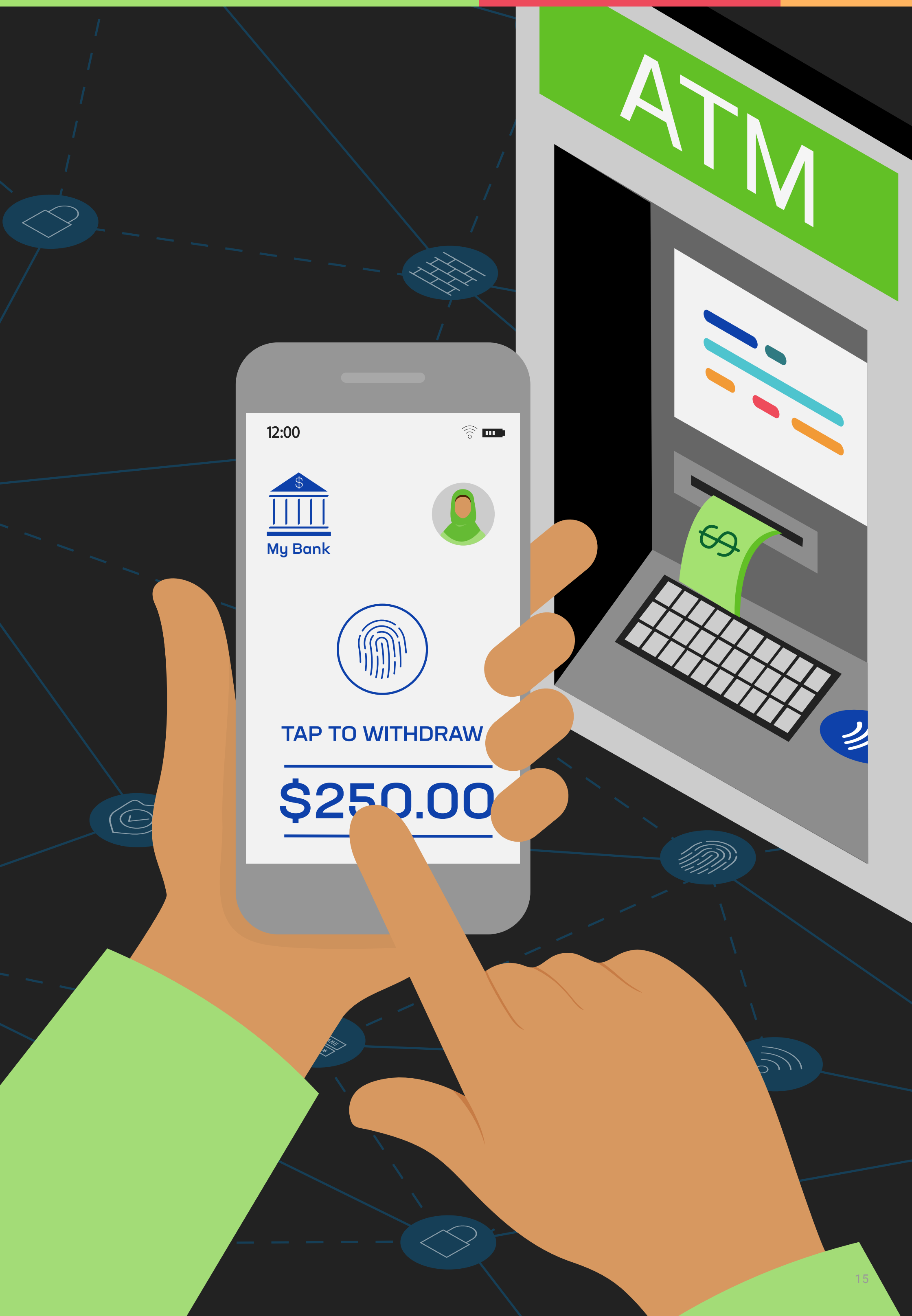
Repatriation of Applications from the Cloud

We asked:
Have you repatriated applications from the public cloud back to your on-premises or colocation data center?

We learned:
Repatriation rates vary by region and by industry, but in general, hybrid architectures are probably here to stay. They're made more practical by environment-agnostic app security and delivery technologies that can consistently enforce declarative policies across multiple clouds.



03
App Security and Delivery Technologies Are on the Move



WHETHER APPLICATIONS ARE repatriated or remain deployed in public clouds, this year's survey makes another major change clear: Application security and delivery technologies are increasingly deployed in different locations from the applications they're serving. These application support services, which range from DDoS protection to access management to anti-fraud technologies, are increasingly found in whatever location—or locations—make the most sense for the specific situation and the function they serve.

For instance, 92% of organizations deploy applications on premises as noted, but only 53% host app security and delivery technologies there. Meanwhile, nearly an equal 52% percent of organizations deploy supporting technologies in the public cloud or at the edge.

This decoupling of applications and their support services is a direct result of widespread cloud adoption, the emergence of the edge, the resulting distributed nature of applications, and the benefits and drawbacks of various placement for their security and delivery technologies. More now than ever, the best deployment location for a given support technology depends not only on where the application is hosted but also on:

- The nature and locations of users.
- The nature of the support service itself.
- Whether the technology is available and cost-efficient through a cloud provider or other third party.
- Related business objectives.

Security services such as DDoS and API gateways may perform best on or near the edge, where they can stop attacks before the entire network is affected. Similarly, identity-based access control might perform best when deployed as near users as possible—whether those users are people with mobile devices or microservices. A service mesh, on the other hand, should be deployed with the application it's supporting as part of the same cluster as container-based microservices.

Not everyone is scattering application technologies so widely; nearly one quarter of survey respondents (22%) deploy application security and delivery technologies only in their data centers. Truly, for certain technologies, such as endpoint security or SSL VPN, on-premises deployments make sense most of the time. However, as SaaS adoption and edge deployments generally increase, the balance may continue to shift toward greater dispersal.

96% deploy identity and access management technologies.

Of the many app security and delivery technologies available, identity and access management are now the most common, deployed by 96% of organizations. This represents a startling shift, since availability technologies such as load balancing or more traditional security technologies such as SSL VPN and firewalls always previously topped the list.

The popularity of identity and access management technologies today partly reflects the adoption of zero trust security and the explosion of remote work in the past two years, but it's due even more to the proliferation of microservices, scripts, sensors, workloads—even refrigerators and light bulbs—that now access applications. In the context of applications and the technologies that support them, the definition of "user" has exploded far beyond the notion of a person with a device, even a mobile one. As a result, most (if not all) security solutions are moving to an identity basis to enable secure authorization of users that are far less likely to be an employee than an API, a service, or a machine.

After identity services, traditional security services, as a group, run a close second as the most frequently deployed, with availability technologies third. Nine in 10 organizations deploy all three, and another 85% deploy application delivery technologies intended to improve performance.

In fact, the average organization (across all respondents to this year's survey) uses 21 different application security and delivery technologies to support rich and robust customer experiences. On average, a majority of these technologies are deployed on premises, but a significant percentage are deployed in the cloud, and a single application may rely on various services deployed in multiple locations. And vice versa.

The average organization uses **21 application security and delivery technologies**.

This deployment flexibility has advantages but also generates complexity and operational fragmentation. It increases the challenge of maintaining consistent policies across multi-cloud architectures—a problem that has existed for years—even as those architectures and workload mobility make policy-based uniformity more important than ever. It also can trap data and stymie broad visibility at a time when using telemetry to make rapid business decisions has never been more crucial to business success.

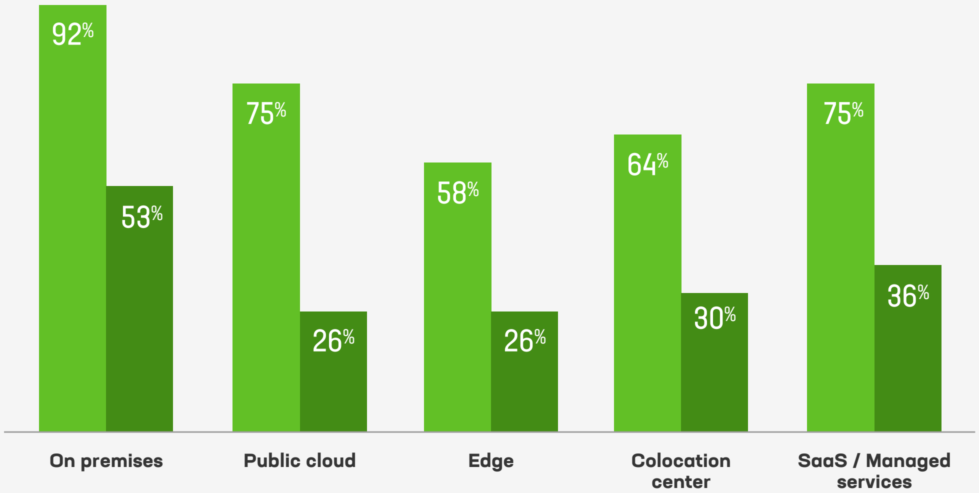
26% of app security and delivery technologies **are deployed at the edge**.

These data challenges and the need for more real-time data processing are among the reasons edge deployments are gaining popularity. Edge deployments can improve application performance and the customer experience, but they can also increase the efficiency of the security and delivery technologies that support applications.

Deployment Location Divergence

Applications today are deployed in a variety of different environments, with a high percentage of organizations using each and most using more than one. Meanwhile, application security and delivery technologies are increasingly deployed in locations that differ from the deployment model of the applications they serve.

🟩 Apps
🟩 App security and delivery technologies



The evolving purpose of edge deployments

More than four of every five respondents (84%) plan to deploy workloads at the edge to improve the employee experience as well as that of customers. In fact, respondents' near-term plans for edge deployments suggest a maturation in how organizations are using the edge.

Initially, edge deployments were aimed primarily at performance improvements achieved by moving content and applications closer to users. Content delivery networks (CDNs) played a key role. Security quickly became an important focus as well, since it makes sense to identify and resolve threats before they reach the data center or the cloud.

The rise of the Internet of Things (IoT) and containerization, plus fundamental changes in the nature of endpoints from fixed and passive to virtual and dynamic, have altered the paradigm of the edge. Along with that shift, objectives for deploying at the edge have changed, too. Organizations increasingly expect the edge to play a more significant role in their architectures. While performance improvements and security are still important, particularly for their impacts on the digital experience, 32% of respondents cited greater operational efficiency—due to better workload distribution and more accurate data from remote endpoints—as a desired outcome for edge deployments.

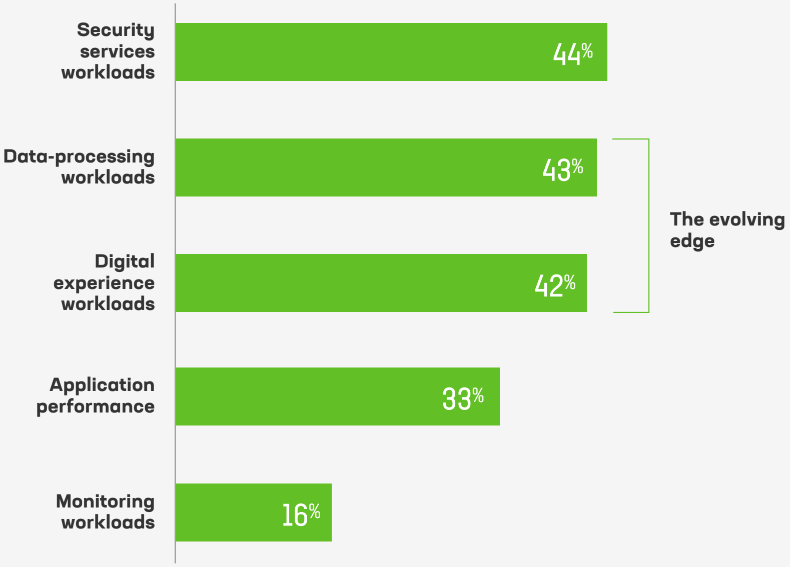
32% are moving to the edge for **efficiency outcomes**.

Furthermore, the workloads organizations plan to deploy at the edge are nearly equally balanced between security services, real-time data processing, and digital experience workloads such as mobile applications and customer-facing websites. More traditional application performance workloads aren't far behind.

Edge Workloads

We asked:
What types of workloads do you plan to deploy at the edge? Select all that apply.

We learned:
The rise in data processing and digital experience workloads herald an evolution in use of the edge.



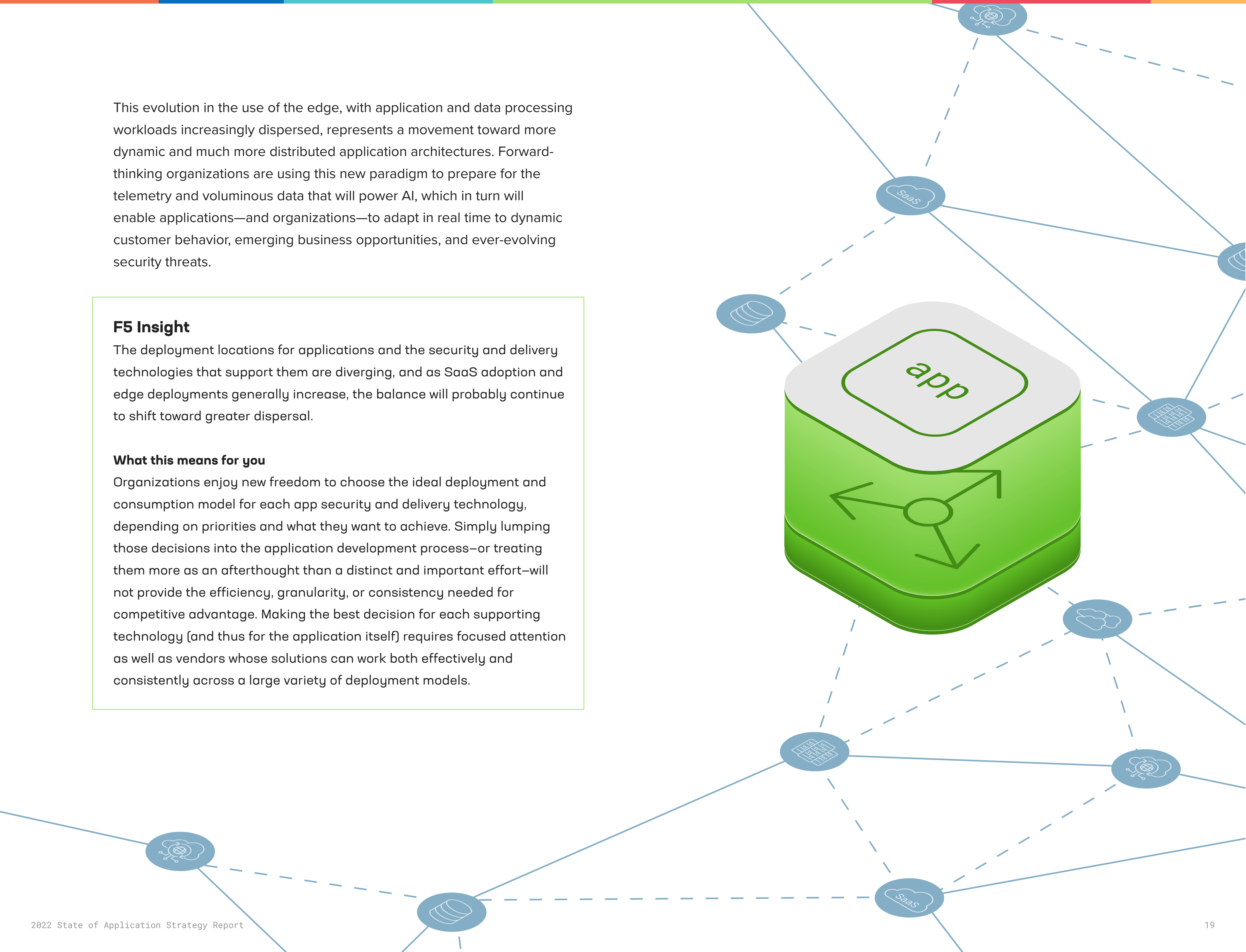
This evolution in the use of the edge, with application and data processing workloads increasingly dispersed, represents a movement toward more dynamic and much more distributed application architectures. Forward-thinking organizations are using this new paradigm to prepare for the telemetry and voluminous data that will power AI, which in turn will enable applications—and organizations—to adapt in real time to dynamic customer behavior, emerging business opportunities, and ever-evolving security threats.

F5 Insight

The deployment locations for applications and the security and delivery technologies that support them are diverging, and as SaaS adoption and edge deployments generally increase, the balance will probably continue to shift toward greater dispersal.

What this means for you

Organizations enjoy new freedom to choose the ideal deployment and consumption model for each app security and delivery technology, depending on priorities and what they want to achieve. Simply lumping those decisions into the application development process—or treating them more as an afterthought than a distinct and important effort—will not provide the efficiency, granularity, or consistency needed for competitive advantage. Making the best decision for each supporting technology (and thus for the application itself) requires focused attention as well as vendors whose solutions can work both effectively and consistently across a large variety of deployment models.



04

Security Is Evolving Toward Risk Management

IN THE REALM of security, this year's survey results reveal good news, starting with the closest alignment we've seen between IT and business leaders on the importance of protecting not only the overall business but infrastructure and applications, too.

This hard-won alignment, unfortunately nudged along by high-profile breaches and significant fraud losses, reflects the convergence of business and IT objectives as digital businesses mature. As complexity has increased the number of points of potential failure, slightly more senior IT leaders rank security—particularly application security—as very important than do senior business leaders, but only a few percentage points separate the large majorities in both roles who prioritize such protection.

Still, performance matters, and more than three-quarters of survey respondents admitted that—given a choice—they'd turn off security measures to improve performance. Half would do so even for performance improvements under 50%. This rather shocking preference for performance has always been true and may be driven partially by security compliance requirements that seem more like empty mandates than effective protection.

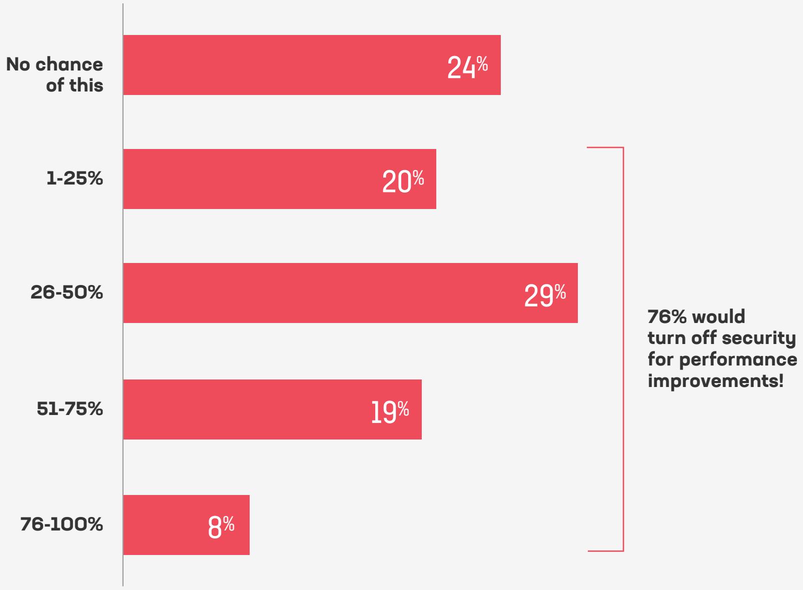
An alarming **76% would turn off security measures** to improve performance.

But this yearning for performance over security also reflects a growing awareness that unassailable threat mitigation doesn't exist—or if it did, it would cost more in operational expense, user frustration, or lost opportunities than the business could tolerate. Rather, running a secure digital business requires managing a spectrum of risks in light of other real-world objectives. That means balancing acceptable performance, customer experience, and cost with acceptable protection and security compliance.

Performance Improvements Worth Removing Security Controls

We asked:
What performance improvement would entice you to turn off security controls?

We learned:
Most respondents would sacrifice security for performance gains, and many would even for relatively small improvements. Neither their roles nor their industry made much difference.



Proactivity and contextual intelligence are the keys to this balance. It will always be important to quickly detect and neutralize significant security threats before they cause harm. But mature risk management should be able to ignore reactive (and sometimes arbitrary) security rules such as maximum session length when the user is much more likely to be a customer having difficulty than a bot. Behavioral analysis can deliver such intelligence, and a mature organization can assess risk in context to deliver adaptive security and performance. In effect, mature digital security becomes another domain of overall business risk management, especially for digitally advanced enterprises.

This emerging risk-management perspective is one reason identity-based security has become a significant trend. The trend is also partly a response to the explosion of microservices joining the ranks of “users” whose identity needs verification, even if those workloads only interact within a single data center. In addition, organizations with significant investments in APIs—including those making liberal use of XaaS—need to modernize their approach to API security, and 78% have already implemented API security measures or plan to within the next 12 months. That ratio is even higher—91%—among those organizations deploying at the edge.

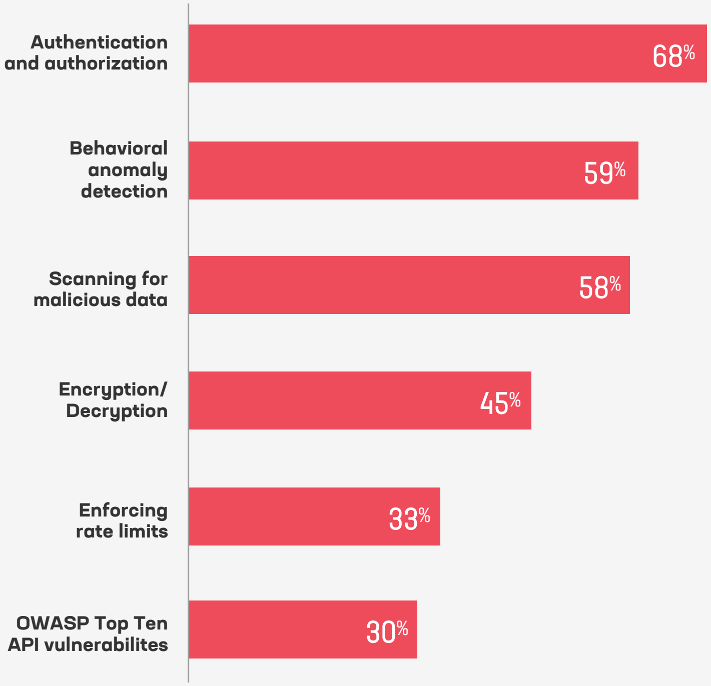
API security is also maturing, with organizations using a variety of approaches that can be grouped into traditional, modern, and adaptive:

- Fewer than half of survey respondents said they valued traditional methods, including encryption and decryption, rate limit enforcement, and OWASP Top Ten mitigation, which were called out by 45%, 33%, and 30% of respondents, respectively.
- The modern approach of user authentication and authorization (AuthN/AuthZ) was deemed valuable by 68% of respondents, while 58% valued another modern approach, traffic inspection.
- Finally, 59% of survey respondents said they valued the use of behavioral analysis to determine user legitimacy.

API Security Measures

We asked:
Which of the following are valuable protections for APIs? Select all that apply.

We learned:
Identity-based security is a key risk-management response to API vulnerabilities.



API security concerns are also a factor in the technologies that survey respondents report they're most excited about over the next few years. As addressed earlier, the convergence of IT and OT—and the agility and business efficiencies it promises—took the top spot. In keeping with the longing for greater performance, 5G comes in at number two, in part because it enables greater use of the edge and IoT connectivity. But API-centric security—the zero-trust security model and web application and API protection (WAAP)—follows close behind.

In the wake of COVID and as part of attempts to reduce complexity, nine in 10 organizations have been actively adjusting their security postures, raising awareness through training, and exploring additional solutions and approaches. For instance, in the last year, 48% of businesses increased their focus on vulnerability management and automation. Other key tactics include the adoption of cloud security, additional employee training, and consolidation of security vendors. In the days to come, most organizations will need to apply several of these tactics in combination to sufficiently manage the risk of security breaches.

F5 Insight

As applications and APIs continue to proliferate–along with the threats to each–identity-based security is quickly becoming as important as more traditional approaches to threat defenses. Fortunately, increasing organizational alignment on the importance of security and the emerging risk-management approach support greater investments in application security.

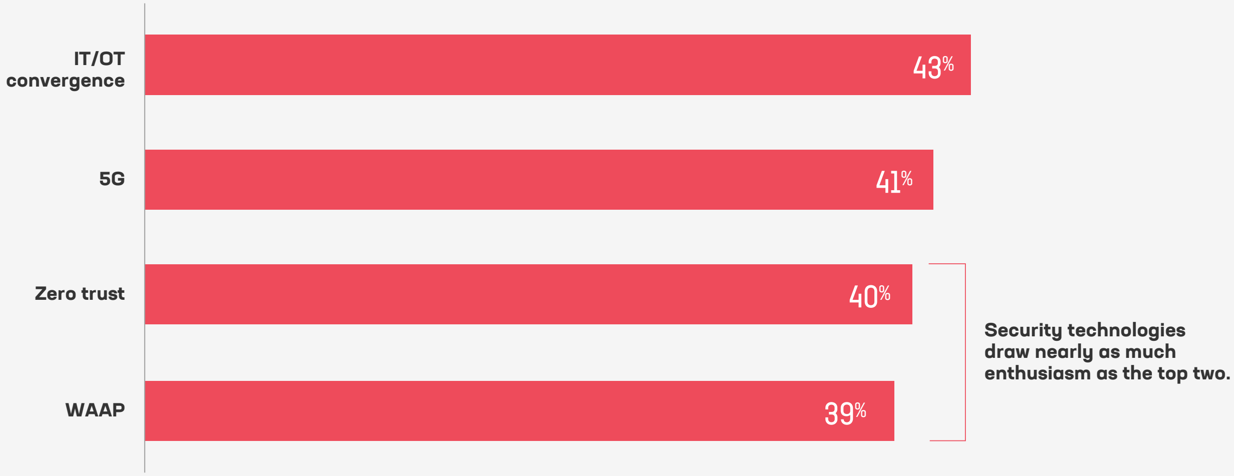
What this means for you

Now is the time to take meaningful steps toward elevating the organization's security posture and helping secure the entire business by focusing on protecting apps, which are increasingly fundamental to most businesses and where the greatest risks converge. As new vulnerabilities are discovered daily, organizations that adopt identity-based security will be able to manage threats contextually and continue modernizing while efficiently balancing risk with performance. In addition, more effective deployment and management of WAFs, API security, and bot defenses across the portfolio will lower risk profiles and enable better overall risk management.

Technologies to Watch

We asked:
Which technologies are you most excited about over the next few years? Select all that apply.

We learned:
In addition to IT/OT convergence and the opportunities 5G may enable, security solutions are a key area of enthusiasm.



Security technologies draw nearly as much enthusiasm as the top two.

05
Challenges Require More Strategic Attention

EVEN AS TACTICS such as behavioral analysis and AI assistance take hold, there are hitches that may block their full implementation. These include missing insights, missing skills, and the need for evolution in both processes and how IT decision-makers think about and make strategic plans for applications, data, and application security and delivery technologies.

Missing insights

Not only are the insights necessary to capitalize on AI missing, the deficit has grown worse in the last year. Some 95% of organizations plan to mine operational data for insights they hope to use to improve the customer experience and drive business growth. Their plans sound overly optimistic, however, when you consider that nearly every business (98% of respondents) is missing insights they need right now.

Across respondents and roles, the top three missing insights are:

- The root causes of application **performance degradation**, cited by 39% of respondents.
- Information about **possible attack**, which eludes 38% of respondents and moved up from third place to second place this year.
- The root causes of **application issues** or incidents, missed by 37% of respondents.

A variety of challenges prevent organizations from obtaining the insights they'd like, but the most common is a lack of data caused by insufficient visibility. The desire for full stack observability—driven by that need for more actionable data to adapt to constantly changing conditions—has never been greater but remains elusive.

98% are missing insights they need.

Still, organizations are working to improve their use of data, and it's no surprise that missing root causes are a top focus for analytics projects.

More than half (52%) of survey respondents currently have projects designed to provide root cause analytics. Improving the customer experience ranks a close second.

The number one focus for data and analytics projects: **mining for the root cause of incidents**.

Predictably, organizations reported a strong preference for managing their own operational analytics, regardless of where the data is hosted. In addition, the value of that data, concerns about data security and compliance, and the need to turn it into insights and responses in real time motivated nearly 48% of respondents who plan to use analytics for operational data to expect to host it themselves in their own data centers or private clouds.

Missing skills

Whether they'll have the skills to do so is another question. Skills deficits in all areas continue to challenge IT departments, whether it's a lack of expertise in the organization's data platform—the number two cause of missing insights—or a lack of the necessary skills to increase automation. In fact, the percent of respondents reporting skills deficits in key areas jumped from already high rates in 2021:

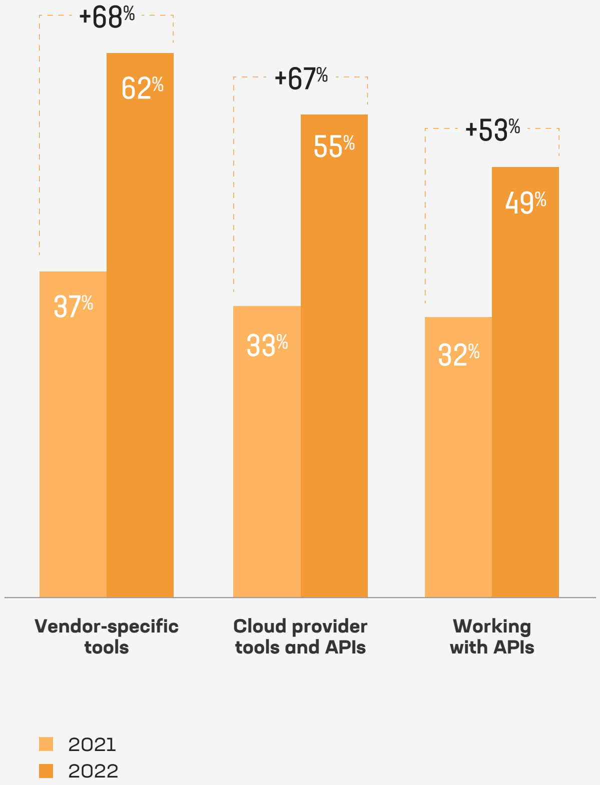
- Nearly two-thirds (62%) say they lack needed skills related to vendor-specific tools.
- More than half (55%) are missing the skills to use cloud provider tools and APIs.
- Finally, despite the importance of APIs to the digital economy, 49% of organizations lack API skills.

These skills deficits must be overcome if organizations truly expect not only to better manage their current operations but to take on the more in-depth data analytics and machine learning (ML) that will be required to fulfill their AI aspirations.

Growing Skills Gaps

We asked:
In which areas do you believe your organization has a skills deficit in automation and orchestration?

We learned:
Skills deficits of all types continue to grow.



Adopting SRE practices: a piece of the puzzle

However, a striking finding of the survey this year points to solutions for some of these challenges: site reliability engineering (SRE) practices. More than three-quarters (77%) of organizations say they're now adopting or plan to adopt software SRE approaches, at least for a portion of their applications and systems. These SRE practices include working under the premise that systems will fail, accommodating that expectation, and moving toward expected failure to manage incidents more fluently using service-level objective (SLO) budgets instead of service-level agreement (SLA) contracts. This shift toward SLOs reflects a closer alignment of IT and business objectives, a marker of a mature digital business. And when the activities and plans of those adopting SRE are considered apart from other survey respondents, the benefits become clear.

For instance, organizations adopting SRE practices are less likely to report that they're missing skills in most areas, other than vendor-specific tools and codifying their own business processes. They also cite fewer automation challenges even as they gain workload mobility. They're much more likely to repatriate applications because they can manage them with the efficiency and ready scaling offered by public clouds, but in their own data centers, gaining the benefits of both at the lowest possible cost. Specifically, more than 95% of SRE practice adopters expect to repatriate apps, and 74% already have. By comparison, only 6% of those with no plans to adopt SRE practices have repatriated applications, probably because most simply can't operate them on premises with equal efficiency.

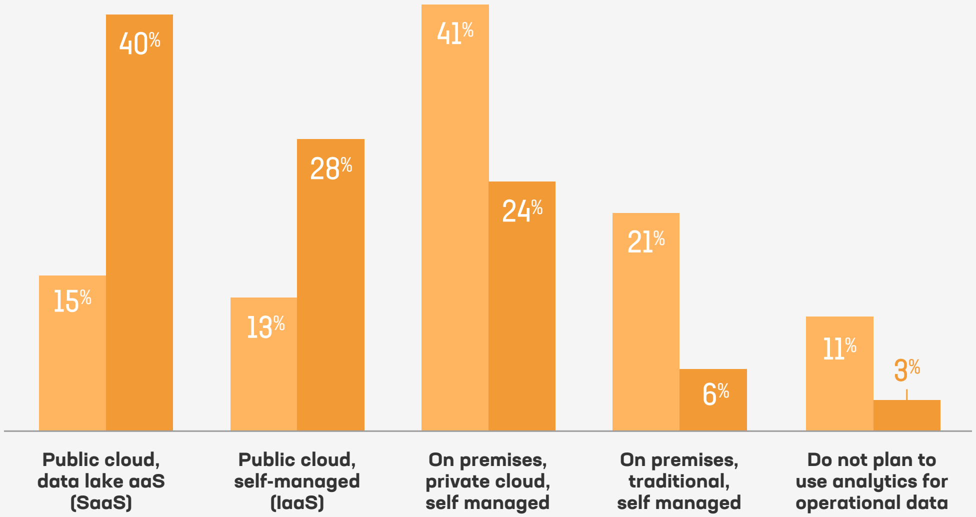
77% plan to adopt SRE practices or already have.

On the other hand, organizations adopting SRE practices are far more likely to prefer hosting operational data in the public cloud, whether in Data Lake as a Service or self-managed form. More than two-thirds (68%) would do so, compared with 28% of those not adopting SRE practices. The SRE adopters

Hosting Preferences Shift with SRE Adoption

We asked:
What is your organization's preference for hosting analytics for your operational data?

We learned:
Those who've adopted SRE are far less likely to use on-premises hosting for operational data analytics.



■ No SRE
■ Use SRE

clearly are confident they have the processes and skills to obtain the efficiency benefits of multiple environments while still controlling, securing, accessing, and using that data in real time.

In other words, the efficiency, security, or performance benefits of various environments may have more to do with how the IT team operates than where various workloads are hosted. It appears those who invest in SRE practices are using them as a method of modernizing their IT operations and managing applications in a more robust, cloud-like manner regardless of architecture. And in fact, those who apply SRE practices are three times more likely than others to manage applications in multiple clouds, considerably more likely to deploy at the edge with data-processing objectives, and nearly twice as likely to be planning AI use for business and security purposes. Simply put, SRE approaches are a marker of digital IT sophistication.

Few organizations currently apply SRE practices to more than a minority of their applications or IT operations; they're just getting started. Nonetheless, this approach is likely to expand and is emerging as an attractive means of aligning the skills and capabilities needed to fully transition to digital businesses.

Missing strategic focus

SRE practices can help organizations increase efficiency, performance, and automation with data. But to respond even more quickly to changing circumstances—and to truly eliminate the pain of inconsistent policies and missing insights—most organizations will need to not only modernize their IT operations but change how they think about applications and the technologies that secure and deliver them. The current approach is simply too complex, too inconsistent, and too labor-intensive to support an agile and innovative digital business.

In a world that only grows more application-centric—with complex, distributed deployments that include cloud and edge environments—security, application delivery technologies, and telemetry require more attention as distinct IT concerns (and areas of expertise). These are make-or-break aspects of application—and thus business—success. Until organizations address them as such, AI pilots will remain difficult to scale to production, the desired deployment flexibility will continue to be constrained, and organizations will struggle to realize the full promise of a digital business.

F5 Insight

The challenges faced by IT teams today reflect the pace of change and organizational systems that can't really keep up. Yet the technological innovation that has caused this complexity will no doubt continue, and AI assistance can't help without more uniform data access and the tools and skills to put it to work.

What this means for you

Organizations can adopt SRE practices and cloud-like operations, but to nimbly adapt to accelerating change, it's more important than ever to deploy platform- and environment-agnostic application security and delivery technologies that work with existing architectures to deliver consistent security, performance, and visibility across the entire application portfolio.

Taking a more strategic approach to such solutions includes assessing vendors based on their ability to provide solutions that bridge disparate architectures and environments. Only such an approach and more cross-platform application technologies will deliver the consolidated telemetry to drive effective AI and enable organizations to better adapt to the unexpected shifts of a constantly evolving marketplace.

Conclusion

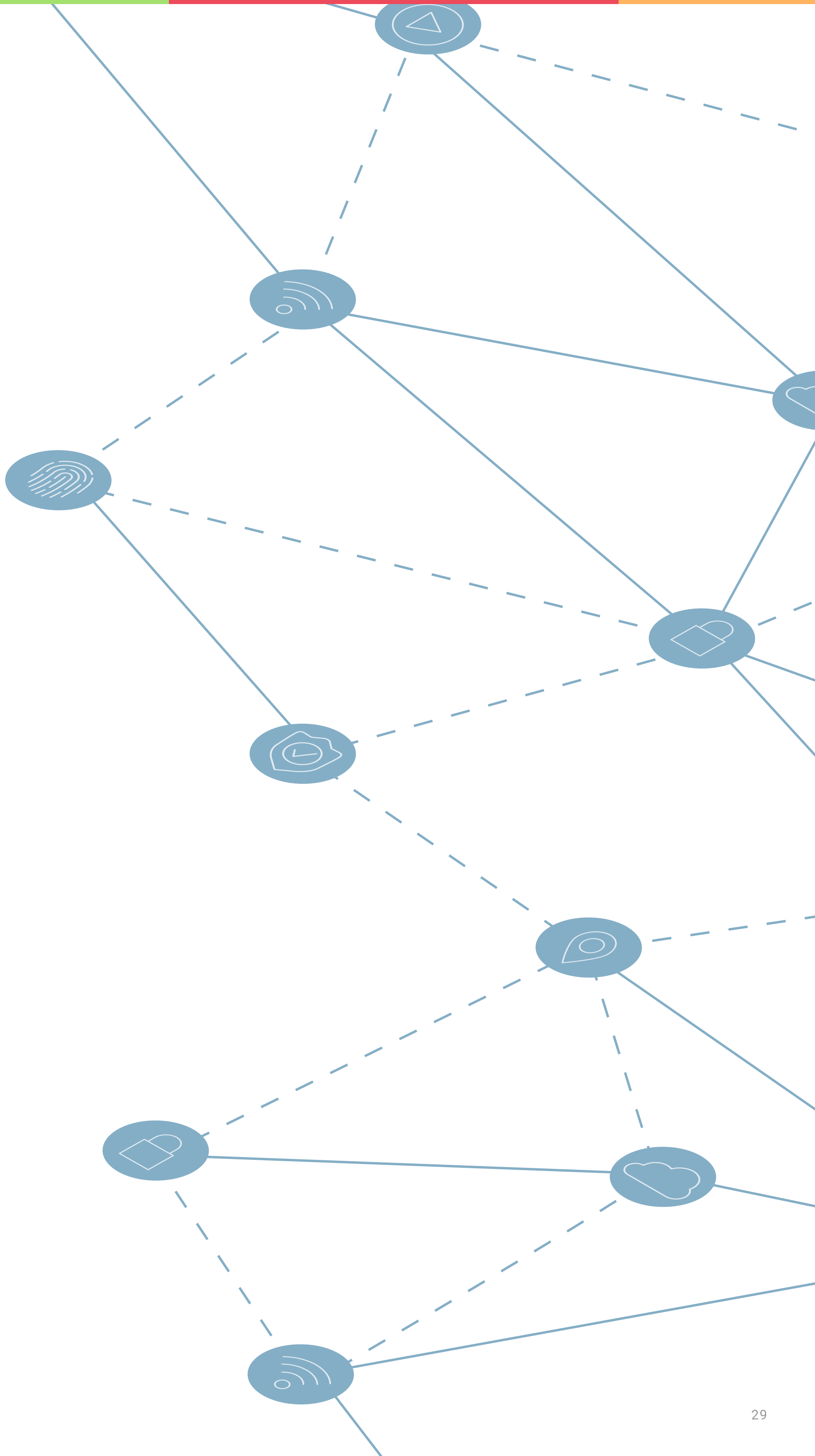
RAPID MODERNIZATION CONTINUES across industries and around the globe to achieve customer-based definitions of success, including fast, seamless digital experiences; robust protection of customer data and the business reputation; and the innovations that build customer loyalty and expand revenues. Organizations are anticipating greater automation as IT and OT converge while embracing the promise of AI assistance to adapt to conditions that change faster than ever.

Continued progress, including AI implementation at production scales and a more intelligence-based, risk-management approach to security, generally will require investments in data mining and analytics, automation, and machine learning not yet in place. That's because AI can't effectively work without better data transparency, integration, and governance than is currently available.

In addition, maintaining the current momentum of digital transformation will require changes across the areas of people, processes, and tools:

- Addressing skills gaps and building expertise in AI, machine learning, and data management and compliance to create more capable teams and more digital value.
- Improving processes, which likely include wider adoption of SRE practices, to increase IT operational efficiency.
- Consolidating telemetry and management toolsets for more comprehensive visibility and control, plus app security and delivery technologies deployed to perform consistently across environments.

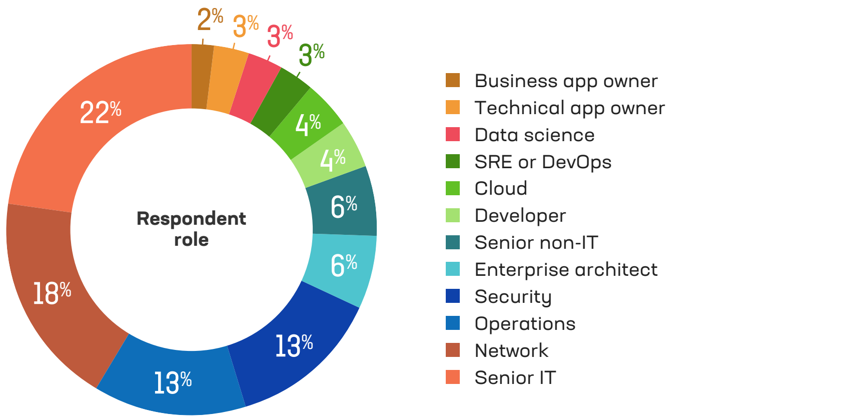
Only when all three concerns can be addressed will IT departments conquer the complexity of multiple architectures and distributed applications to gain the end-to-end visibility needed for AI assistance to fulfill its promise of helping organizations adapt to change in real time to better satisfy customers and meet business objectives.

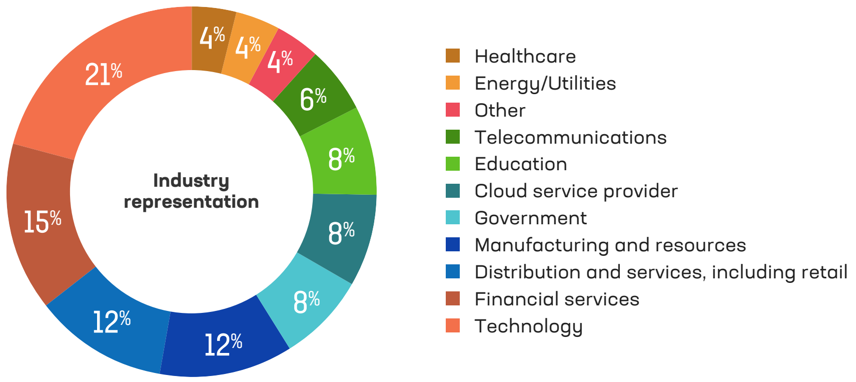


About the survey

NEARLY 1,500 IT decision-makers from organizations around the globe responded to our eighth annual survey on the state of application strategy today. The data was collected over a three-week period in September and October of 2021.

This year's results incorporate the priorities and concerns from an unusually broad range of industries, with cloud service providers, manufacturing, and education represented at higher rates than in the past. Technology, financial services, and retail, distribution, or professional services firms were also well-represented. Individuals from organizations of all sizes participated, providing insight into their current IT activities and challenges as well as their expectations for the coming few years. While the results reflect a few interesting variations between regions or industries, for instance, overall they provide a reliable snapshot of the perspectives, needs, and direction of typical IT organizations today. The results also illuminate broader trends and potential pitfalls as businesses and institutions everywhere become increasingly digital and application-centric.


Respondent role
Business app owner
Technical app owner
Data science
SRE or DevOps
Cloud
Developer
Senior non-IT
Enterprise architect
Security
Operations
Network
Senior IT


Industry representation
Healthcare
Energy/Utilities
Other
Telecommunications
Education
Cloud service provider
Government
Manufacturing and resources
Distribution and services, including retail
Financial services
Technology