2023

State of Application Strategy Report

Contents

Introduction
Embrace the Power of “And”

SUCCESS IN TODAY'S global culture is about transcending geographic and other boundaries to overcome conflicts, bridge diversity, and bring together people, ideas, opportunities, and resources. This is true on a personal level, where most of us juggle a variety of roles. We're professionals *and* family members, neighbors *and* hobbyists, citizens of nations *and* a multicultural global community. The same is true for organizations connecting far-flung resources and people to accomplish complementary objectives. To thrive while embracing all of their roles, individuals and organizations require agility—a fluency of action increasingly supported by quick, efficient digital experiences delivered by applications and APIs.

Hybrid IT is challenging but sustainable.

Today, 40% of those apps are modern or use modern components, and it's no longer news that nine in 10 organizations are involved in digital transformation to further modernize, better integrate their IT stacks, and take advantage of the performance and engagement possible at the edge. Other results of the ninth annual F5 State of Application Strategy survey are more surprising and may spark insights and debates that can guide business strategy.

If one finding particularly emerges this year, it's that the average IT stack will remain hybrid, with capabilities such as compute, network, storage, and applications distributed widely across core, cloud, and edge environments. It's not only clouds that can be considered "hybrid." Organizations will continue to manage multiple, disparate technology stacks and support different generations of infrastructure and apps. (A familiar example is the continued, multi-billion-dollar market for fax machines, even in the era of email, texts, and apps.)

Many CIOs who have responsibility for the enterprise architecture will recognize this balancing act. They must simultaneously enable a digital business and satisfy customer expectations—which can mean adopting emerging technologies—while juggling resource constraints, the challenges of technical debt, and organizational needs for stability, resiliency, and effective change management. As a result, IT professionals must become ever more fluent across disparate and dynamic systems and technologies.

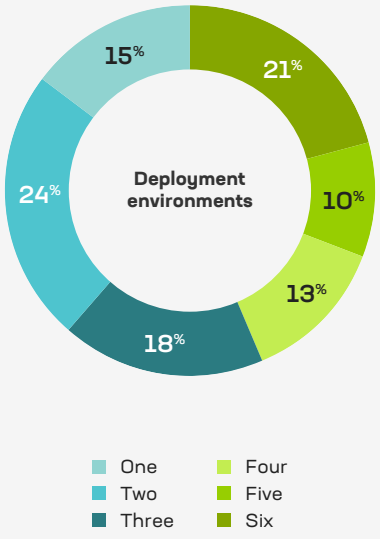
The good news is that hybrid IT is proving sustainable—as hybrid roles and interests are in many other aspects of our lives, where the operative word is "and," not "or." Business velocity and long-term growth will rely on finding ways to connect and protect apps and APIs across locations while easing the management of complex hybrid environments. This reality is reshaping application security and delivery. The latest F5 annual survey of IT decisionmakers reveals which approaches are growing in popularity, why—and what your organization may need to do to stay abreast of those setting the pace toward our shared hybrid future.

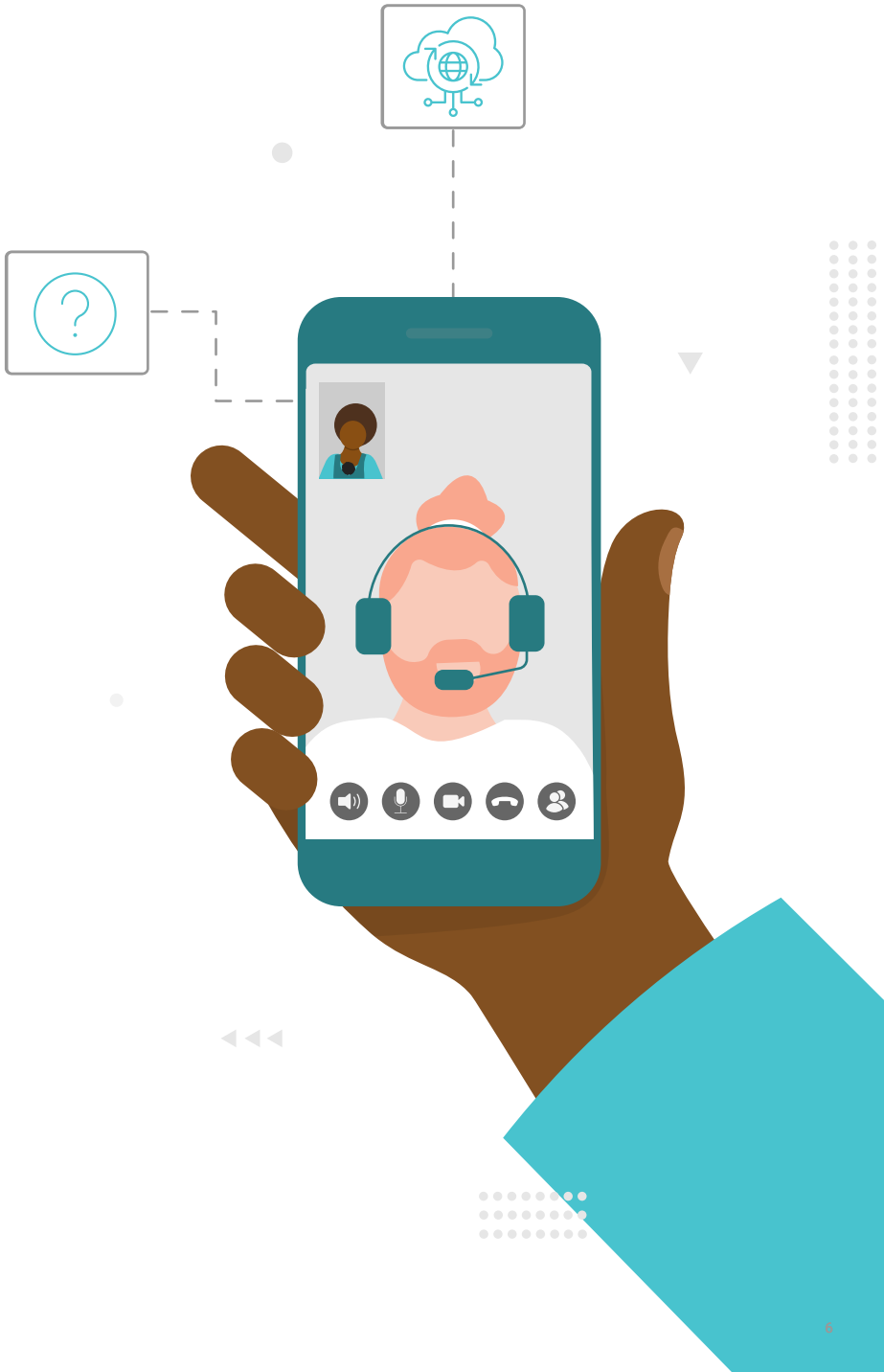
01

IT Will Remain Hybrid Indefinitely

THIS YEAR'S DATA is convincing: Hybrid IT is here to stay. Just 15% of survey respondents report deploying applications in a single environment, while more than one-fifth of respondents say they deploy apps in six different environments. With hosting decisions typically made one app at a time to achieve app-specific goals, organizations have realized that there's simply no one environment that's best for them all. Some require an on-premises data center, and others need the speed, scalability, and efficiency of one or more clouds.

Apps Are Widely Distributed





Public cloud deployments are far from ubiquitous.
We also found that public cloud aspirations (and hype) are returning to Earth. Five years ago, in 2018, 74% of survey respondents told us they planned to deploy "up to half" their apps in "a cloud." Two years later, in 2020, only about a quarter were implementing those plans, but cloud computing still ranked as the single most exciting technology trend, by far.

Jump ahead three more years. Today, just under half of all respondents (48%) say they currently have *any* apps deployed in the cloud, and on average organizations deploy only 15% of their app portfolio in the cloud. The considerations limiting public cloud deployments probably include concerns about data control, security, or cost at scale.

Business continuity is the top public cloud use case.

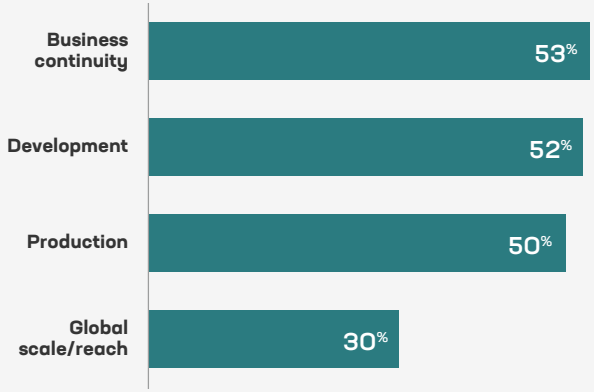
Public clouds remain an option for many organizations, particularly for backup and business resilience purposes, but public clouds are not always the first choice for hosting applications. That primacy belongs to on-premises deployments—and after a period of consolidation, the pendulum has swung, and on-premises deployments are again on the rise.

On-premises deployments remain the foundation of today's application architectures.
After years of decline, the percentage of applications hosted in traditional, on-premises data centers grew by two percentage points over 2022 levels to 37%. The share of on-premises deployments exceeds half in total, because while many people think of on-premises data centers as a monolithic environment, the reality is that both traditional and cloud environments exist on premises. Although most other deployment models—such as public cloud and SaaS—have been on the rise in recent years, each leveled out or slightly decreased in 2023.

Public Cloud Delivers Resilience First

We asked:
How are you using the public cloud (IaaS)? Select all that apply.

We learned:
Backup and disaster recovery is the top use case for the roughly half of respondents who use a public cloud.



Repatriation is one driver of this trend. App repatriation continues at high rates for the second year in a row, with more than a third (43%) of respondents saying they've recently repatriated apps or plan to do so soon. The need to control app sprawl in a multi-cloud world is the top motive, cited by 54% of those repatriating apps.

Enthusiasm for repatriation is especially concentrated in the financial services, telecommunications, and technology industries—those likely to be juggling multiple clouds and presumably also the most likely to have the needed skills to efficiently manage their apps on premises themselves.

After on-premises deployments, there's a steep drop to the next most common model. Private clouds host only 17% of the average enterprise portfolio—barely half as much as on-premises data centers.

SaaS offerings are close behind at 16% (though technically this is a consumption model, not a deployment model). The overall picture is one of hybrid diversity anchored by on-premises data centers.

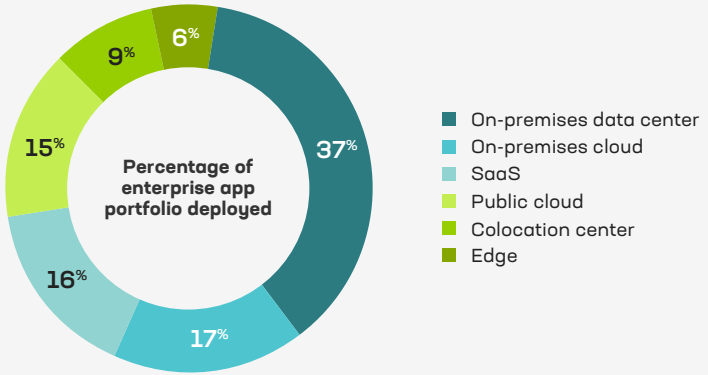
Modern app architectures are everywhere.

App architectures are blended, too. Everyone responding to the survey operates modern apps, consumes SaaS, or both. Respondents report that, regardless of where they're deployed, on average more than a third (40%) of their app portfolios (excluding SaaS) can be described as modern, which includes mobile apps and the use of microservices. This percentage has been growing steadily as anticipated, and we expect it to exceed 50% (and probably 60%) by 2025. But today nearly everyone—95% of organizations—also still operates traditional apps. As a result, a large majority (85%) of organizations face the challenge of managing and securing both modern and traditional apps, often across a variety of hosting environments.

Multi-Cloud Environments Will Endure

We asked:
Of [your] applications deployed today, roughly what percentage are utilizing the following deployment models? Please enter numbers for a sum of 100%.

We learned:
A diversity of app locations is the norm.



As app portfolios trend increasingly modern over time, we expect the percentage of organizations managing both modern and traditional apps to dwindle. This percentage may have peaked at 88% in 2022. But it's unlikely to reach zero any time soon, because CIOs taking a measured approach to modernization are leaving intact traditional applications that continue to add value and align to business priorities.

When it comes to retiring traditional apps, 59% of respondents are replacing them by building modern versions. Organizations in manufacturing and government are most likely to build their own. Meanwhile, about 46% of organizations—healthcare prominent among them—are replacing traditional apps with SaaS offerings provided by vendors. In effect, they're outsourcing their modernization, building less and deploying more, often to gain the value more quickly. One in five expect to simply decommission apps that are no longer needed.

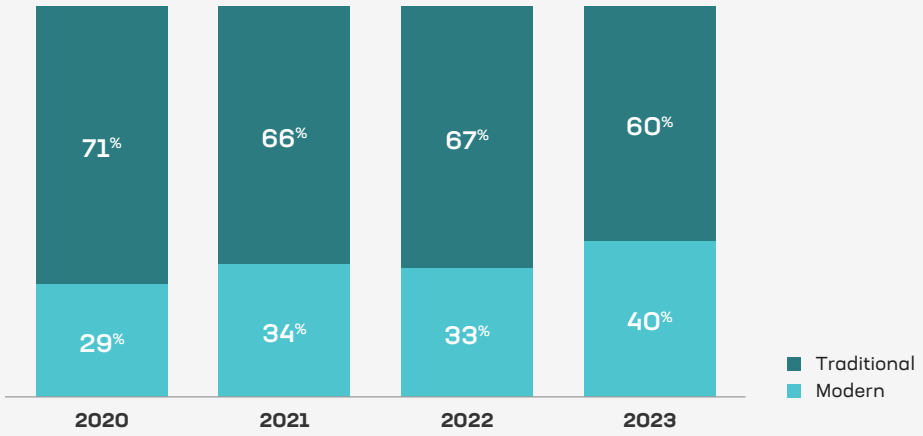
But a solid 16% of respondents have no plans to retire traditional apps. These apps may preserve core business functionality, as in banking or insurance. In industries such as energy, healthcare, or telecommunications, where slow-moving regulatory requirements tend to lock in technologies, up to 33% of respondents expect to retain traditional apps. As a result, the percentage of modern apps in the average portfolio across industries is likely to top out this decade near 85%. And a significant portion of those may be microservices chained together solely to interface with a traditional app.

In short, the majority of CIOs will oversee hybrid app architectures and multi-generation apps distributed across hybrid environments for the foreseeable future.

Modern App Architectures Continue Their Growth

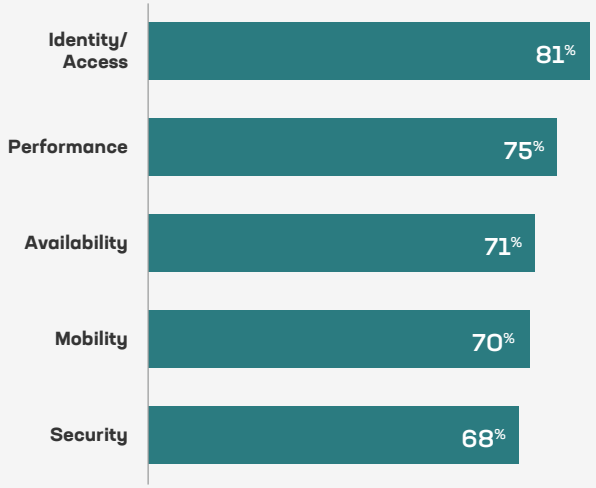
We asked:
Of all your applications deployed today, roughly what percentage fit into the following categories? Please enter numbers for a sum of 100%.

We learned:
Modern app architectures are approaching half of the average portfolio.



App security and delivery technologies are distributed, too.
The technologies that support application security and delivery, like the apps themselves, are distributed across environments. The decision about where to deploy specific technologies (sometimes known as app services) often depends on what purpose they serve. In addition, the environment itself can influence the ideal technology or form factor. For instance, web application firewall (WAF) hardware might best suit an on-premises data center, while apps deployed in a cloud might be protected more efficiently by a Security as a Service (SECaaS) offering. In other situations, security services are best deployed as close to the user as possible, because stopping attacks sooner prevents oversubscription of resources, while layer 7 routing services may be best positioned nearest the app itself. That's why, in hybrid environments, multiple deployments of important app security and delivery technologies often make sense.

Respondents Rely on Identity and Access Technologies Most



Application security technologies are especially likely to be deployed in the cloud.

As a result, a majority of respondents (59%) deploy such services on premises, and an equal majority deploy at least one in a cloud. Cloud deployments are especially common for security technologies. But the delivery of app security and delivery technologies via third-party SaaS is growing in popularity and accounts for the next most common means of provisioning them. Nearly one-third (30%) of respondents report using this method, which can help them grow and scale apps across clouds or other environments without increasing complexity or reducing control.

Regardless of where they're hosted, the use of app security and delivery technologies is on the rise as organizations proceed through digital transformation and work to balance digital velocity with safety and operational stability. Identity and access management (IAM) technologies such as SSL VPN, single sign-on (SSO), and identity federation are the most commonly deployed app services today, but the number of different app services deployed overall has more than doubled since 2017. This is a measure of their importance when the digital services provided by applications aren't merely the face of the business but its heart (or, more accurately, its pocketbook).

Multi-cloud challenges continue, but solutions exist.
In this hybrid and distributed application landscape, it's not surprising that nearly nine of every 10 respondents who operate in multiple clouds continue to cite challenges with multi-cloud security, performance, and cost. The top challenge in 2023 is the complexity of tools and APIs that results from the lack of standardization or interoperability of the tools used for different deployment models. Applying consistent security policies is the next largest challenge for the second year in a row, with performance optimization not far behind.

The increasing API attack surface is compounding multi-cloud challenges.

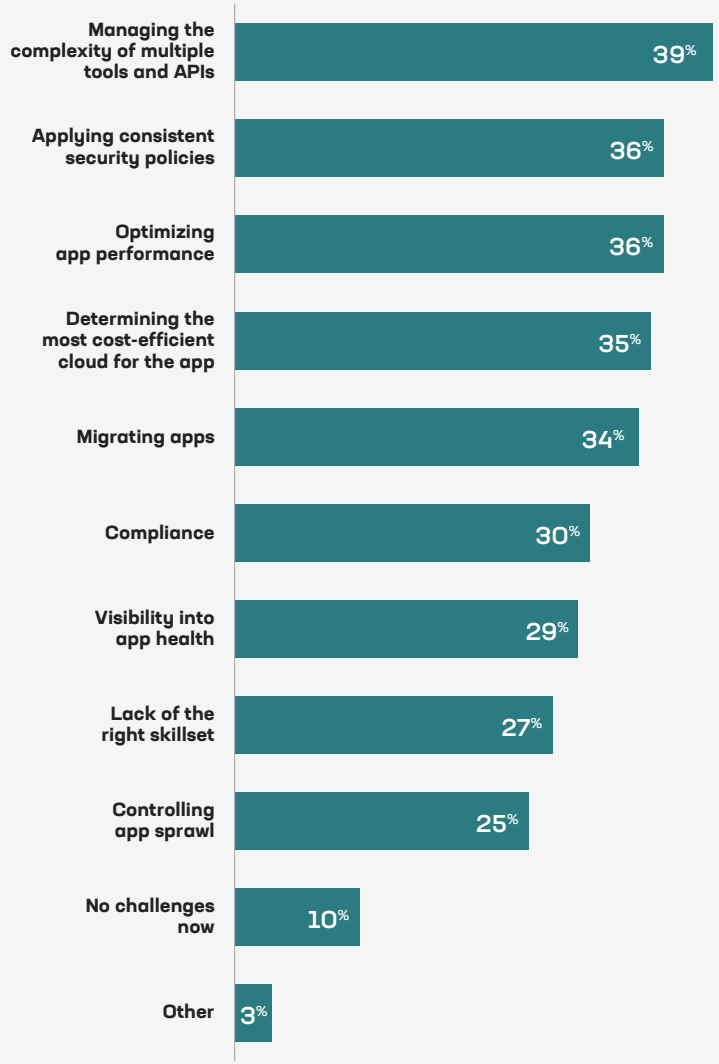
These challenges are no doubt why organizations in the Americas and in Europe, the Middle East, and Africa (EMEA) called multi-cloud networking the most exciting trend over the next few years, though other trends ranked slightly higher in other regions and globally. Notably, respondents in Asia Pacific, China, and Japan (APCJ) were more enthused by the convergence of IT and operational technologies (IT/OT). While this is likely a function of the region's status as a global manufacturing center, it also speaks to the need to better integrate machinery controls with other business systems to improve efficiency.

Other solutions that are available now for connecting, protecting, and managing a multi-cloud reality include more automation, ecosystem approaches, and partners who can help simplify by consolidating tools and policy enforcement for applications distributed across environments. Declarative deployment policies that deliver consistent security can extend protection globally while helping to remove friction between functional silos. And since hybrid IT is not going away, the same solutions that ease multi-cloud management will increasingly prove helpful to most organizations.

Complexity Tops Many Multi-Cloud Challenges

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

We learned:
Complexity and security issues continue, while visibility–number 1 in 2022–fell to seventh.



F5 Insight

Most organizations today would like to ease infrastructure complexity, extend the lifecycles of chosen infrastructure, consolidate deployment environments, and reduce the need for multiple point solutions. But as they modernize, repatriate apps, and often expand their app portfolios, they're typically not eliminating architectures or app distribution, just changing the proportions, the purposes for each environment, and the nature of the resulting challenges. Furthermore, we expect the proportion of modern app architectures in the average portfolio to top out near 85% by 2030, when the growth of those architectures will either slow or stop as newer architectures emerge—and the meaning of "hybrid" evolves. Because cost, control, latency, business continuity, and the ability to scale are perennial concerns, there will always be good reasons to retain more than one deployment option. No single environment will suit every purpose or equally satisfy multiple goals.

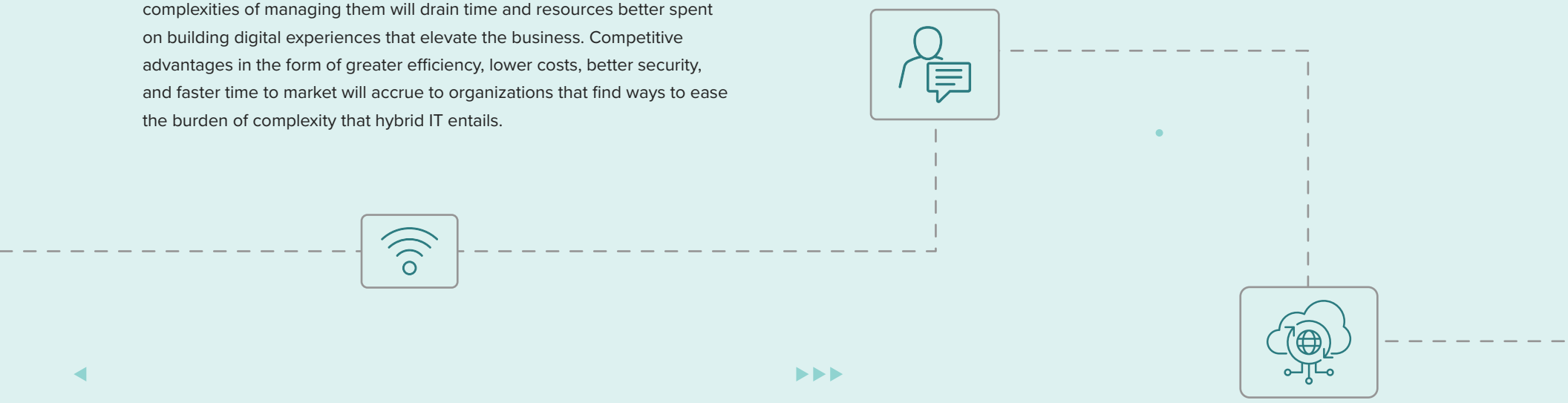
What this means for you

Digital business requires an adaptive IT infrastructure. To achieve their goals, organizations need solutions that mitigate the challenges of operating in hybrid and often multi-cloud landscapes. Otherwise, the complexities of managing them will drain time and resources better spent on building digital experiences that elevate the business. Competitive advantages in the form of greater efficiency, lower costs, better security, and faster time to market will accrue to organizations that find ways to ease the burden of complexity that hybrid IT entails.

The winners will combine complementary approaches, including:

- IT practitioners who aren't limited to siloed expertise but gain fluency across systems and technologies.
- Process methodologies such as site reliability engineering (SRE).
- Tools such as declarative deployment policies.
- App security and delivery technologies that cross deployment models, may be delivered as a service, perform consistently across all the organization's distributed apps and architectures—including those it obtains as SaaS—and both work for the architecture now and adapt as that architecture changes.

For many organizations, the key to easily hitting most of these targets will be engaging with partners whose solutions extend the connectivity of multi-cloud networking to secure and deliver all kinds of apps and APIs that are distributed across various clouds, data centers, and edge locations.



02

Digital Transformation Transcends IT as a Business Strategy

IN 2023, ROUGHLY NINE in 10 survey respondents across industries report digital transformation projects underway—just as in each of the three prior years. And while digital transformation in our hybrid world is no longer new, it remains news for two reasons.

On the individual level, it's impacting nearly everyone—from grocery customers to political protesters to children served by global charities. On the business level, it's delivering value in improved efficiency, new opportunities, improved customer experiences and relationships, and the ability to scale faster. These benefits are making digital transformation a top-level business strategy, not merely an IT concern.

Modernization powers digital transformation today.

When it comes to how those benefits are achieved, modernization currently takes center stage.

As we've noted before, digital transformation takes place in three phases: task automation, digital expansion (which includes scaling and integrating automations), and decision making assisted by telemetry, artificial intelligence (AI), and machine learning (ML). Phase two includes the modernization of existing systems and applications. In 2023, such activities dominate.

In fact, more than eight in 10 organizations are presently working on modernization and digital expansion. Such efforts are more than twice as common as before the COVID-19 pandemic, when only slightly more than a third of organizations (37%) undertook them. The pandemic jolted digital transformation forward by years.

Current modernization activities include the development of modern applications and the addition of modern components to traditional apps that provide core business functions to change how those apps are accessed and experienced. Examples include mobile apps that interface with the fundamental logic powering industries such as banking and insurance, or order entry and tracking integrations for the controls of manufacturing equipment.

Nearly Everyone Is Engaged in Modernization

27%

Phase 1
Task automation: Applications

81%

Phase 2
Digital expansion: Modernization

54%

Phase 3
AI-assisted business: Data & analytics

Although more than half of organizations are also working in digital transformation's phase three, AI-assisted business, that proportion has ebbed below 2021 rates, probably for two reasons. The challenges of implementing AI or ML at production scales can cool enthusiasm for them. More generally, digital transformation is an iterative process. It's common for organizations to work in all three phases at once or make progress in one before returning to a previous phase for more automation. Particularly when it comes to AI assistance, what may look like a step backward can provide the basis for another surge forward. This is also why work in phase one, task automation, has dropped from 46% in 2020 but is likely to continue for some time as organizations automate more back-office functions.

IT ops remain a top priority for digital transformation.
Nearly two-thirds of respondents (64%) are currently modernizing IT operations, even more than in previous years. Modernization is necessary not only to enable AI assistance but to keep the burden on IT teams manageable, because transformation that spreads across the organization increases the demand on limited IT resources. The related IT processes also must be modernized to prevent bottlenecks.

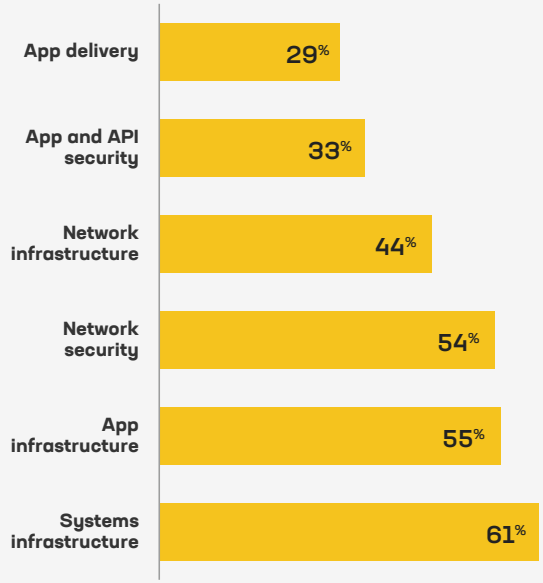
More automation generally correlates with greater IT efficiency.

Awareness of this need is also reflected in the plans of more than half of respondents (59%) to adopt site reliability engineering (SRE) practices, which imply the use of digital tools and automation to scale and augment operations.

Automation Varies Across IT Functions

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

We learned:
Automation of application security and delivery remains an opportunity.



But automation, not modernization, is the primary route to increasing IT efficiency. Automation can be achieved in any of six core IT functions: systems infrastructure, network infrastructure, app infrastructure, network security, app delivery, and app security. Much of the automation to date has targeted systems infrastructure, network security, and app infrastructure.

- Automation of systems infrastructure—such as virtual machines and the use of Kubernetes—benefits from the maturity of virtualization and robust industry support for container ecosystems.
- Automation of network security, which is increasingly offloaded to service models, is supported by AI and the existence of well-defined scenarios to follow.
- Automation of app infrastructure, which can help protect apps as well as speed deployments, is being driven by security threats and the need to reduce time to market for new features and apps.

Two-thirds of organizations say they've already increased IT efficiency, which in 2018 ranked as the top potential benefit of digital transformation. Five years later, that value is being realized.

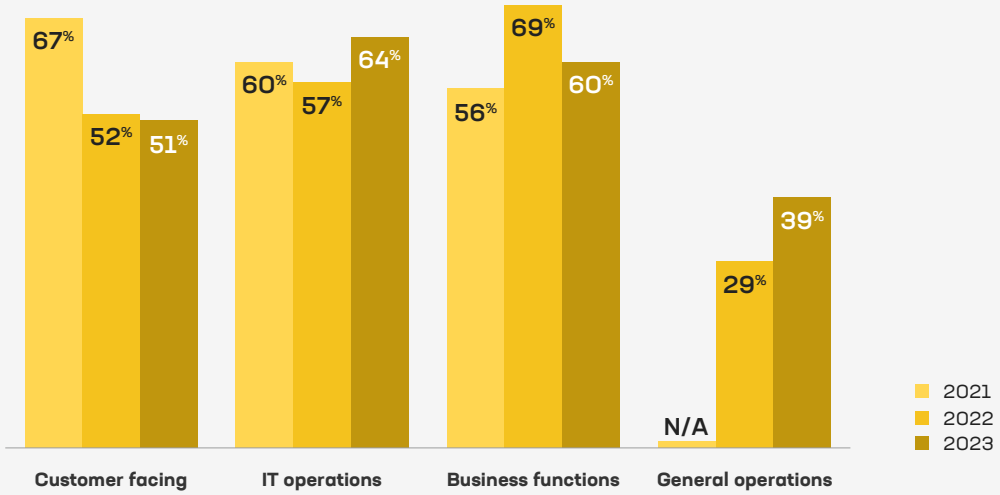
Those survey respondents who report increased IT efficiency have automated, on average, in at least three of the six areas. They naturally report the strongest efficiency benefits in the three areas of greatest activity and automation maturity, which are systems and app infrastructures and network security. But since more automation generally correlates with more efficiency, organizations looking for a competitive advantage would do well to automate in all six.

The rewards are particularly potent for businesses whose operations are primarily digital. A traditional manufacturing operation entails fixed costs ranging from capital investments in equipment to warehouse space. A brick-and-mortar retail business faces similar fixed costs.

Digital Transformation Priorities Are Shifting

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

We learned:
Digital transformation of business functions and general operations has increased since 2021.



By contrast, for a digital business—even retailers predominantly selling online—variable labor and IT expenses typically represent a significant or even the primary cost of the "product," which is frequently a service. In such cases, increased IT efficiency directly impacts the bottom line.

Digital transformation benefits all aspects of the business.
Of course, IT efficiency is not the only benefit of automation, and the advantages of modernization also apply to other business processes. While customer service remains an important priority for modernization, customer-facing apps and processes overall (which include sales and marketing) shrank considerably over the last two years as a priority. This may be in part because significant work has already been done in those areas, but it's also clear that leaders are increasingly turning attention to inefficient internal processes and siloed legacy apps so they don't drag down performance in today's uncertain economic conditions.

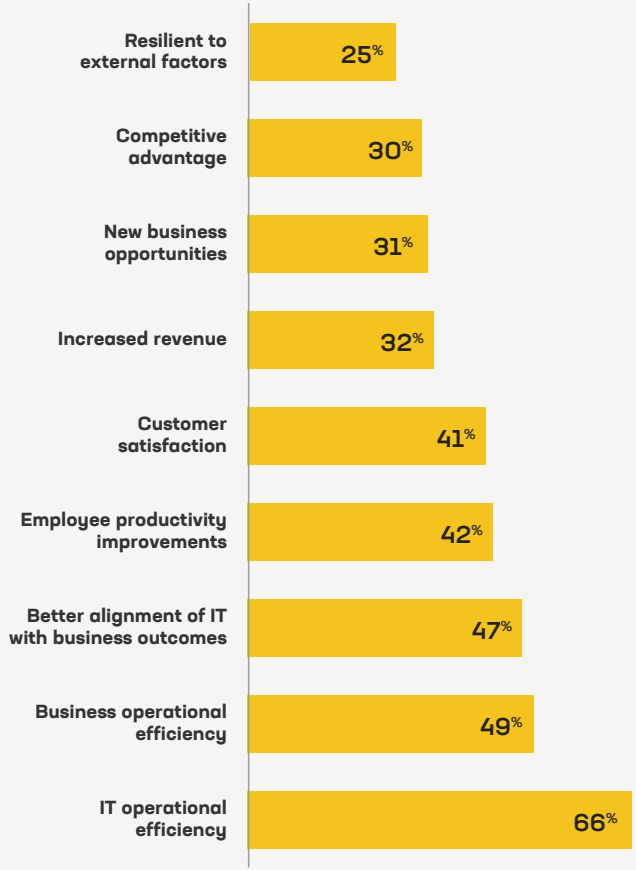
As a result, digital transformation is increasingly touching—and enhancing—all aspects of the business, from customer interactions and relationship management through product design and development to manufacturing and other business activities, including the HR and legal functions that manage risk and the productivity of all employees. This comprehensive impact is why remaining competitive in a rapidly digitizing world requires modernization across the business.

Fortunately, nearly half of respondents engaged in digital transformation report increased operational efficiency across the business, not just in IT. Improved overall employee productivity and customer satisfaction aren't far behind. Similarly, nearly one-third report increased above-the-line revenue and new business opportunities.

Operational Efficiency Follows Digital Transformation

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

We learned:
While two-thirds are improving IT operational efficiency, other benefits are also significant.



No one transformation journey fits all.

Whether your organization is capturing any of the benefits of digital transformation may be a function of just how digital its business model is. Today, more than three-quarters of respondents (79%) say they deliver digital services to consumers, other organizations, or both. Only one in five (21%) provide those services only for their own employees.

We define digital services as a collection of apps, APIs, app delivery and security technologies, and data and other resources seamlessly stitched together to create a digital experience that delivers an outcome for the organization providing those services. Examples range from gig worker apps and employee time reporting to digital media subscriptions, mobile airport check-in, and mobile payments. They may be provided to users at no (separate) charge or rely on various revenue models, including on-demand, pay-as-you-go, or subscriptions.

But while nearly all respondents deliver digital services, slightly more than half (58%) are using them to substantially drive the business, with those services accounting for half or more of the firm's annual revenue.

Furthermore, there's a split between the organizations prioritizing those lucrative digital services and organizations that primarily earn money through analog interactions. Specifically, the digital revenue generators are more likely than others to:

- Operate modern app portfolios.
- Deploy a variety of app security and delivery technologies.
- Use public clouds for any purpose, but especially in production to quickly scale infrastructure and apps globally, as well as to ensure business continuity.
- Purchase SaaS and SECaaS.
- Use the edge for any purpose—and they're three times as likely to use it to better reach customers.

In other words, more than half of organizations are digital dynamos keeping pace, more or less, with the latest IT technologies. The other half may be prioritizing other needs and directing limited resources elsewhere, from geographical expansion or product development to security concerns. It's a balancing act. Plus, no two organizations, even in the same industry, will focus on the same priorities at the same time—or make the same progress when they do.

That said, the digitization of contemporary life is unlikely to revert. Depending on their objectives, CIOs and other company leaders should remain mindful that dropping substantially behind the state of the art or lingering for too long in a mainly analog revenue model could make it hard to catch up later. Modernization can be a long journey that looks different for every organization, but wise CIOs will want to keep moving forward, in one way or another, to avoid falling too far behind.

F5 Insight

Regardless of how much revenue they derive from digital services, organizations that want to compete well in the app- and API-driven economy of the future will need to stay abreast of the activities, technologies, and strategies of those who most effectively monetize digital services.

It's not only that no one can afford to be outpaced by competitors. Even the most traditional industries are likely to add digital services in the future. That might mean anything from new virtual offerings in education to robotics in elder care to drone-assisted resource extraction.

And regardless of whether the organization relies primarily on digital experiences, it still risks high-profile security or operational failures that damage reputations or invoke regulatory repercussions. Leaders who invest in automation and modernization—and thus efficiency—when others are satisfied with the status quo will be better positioned for innovation and perhaps leapfrog the competition in the face of change.

What this means for you

Any organization whose IT operations team hasn't already automated systems infrastructure, app infrastructure, and network security can still gain substantial benefits—benefits that many competitors may be enjoying already. Those ahead of the game also should explore automation of the other three core IT functions: network infrastructure, app delivery, and app security. The less-common efficiencies available in these areas could ultimately provide an advantage.

In particular, the automation of app delivery and app and API security represent huge opportunities for most organizations. Of course, it may be more challenging to automate in these areas because individual apps often involve unique circumstances that rule out easy leverage of existing resources or tools. But automation in these realms is more closely associated with increased customer satisfaction, greater revenue, and the capture of new business opportunities than automation in other core IT areas. These alternate benefits, which transcend IT efficiency to impact the whole business, can make the effort worthwhile.

Finally, it's increasingly clear that as part of this automation and modernization, organizations pursuing long-term success need integrated app security and delivery technologies, including advanced and adaptive protections that help connect applications distributed from the core to the edge. The response speed and ease of management available with SaaS-based solutions can help businesses balance digital velocity with control and performance, securing web applications and APIs, as well as the infrastructure hosting those apps.

03

Time Pressures Inform Security Strategies

SECURING THIS HYBRID and rapidly modernizing digital world only continues to grow more difficult. In an increasingly app- and API-driven economy, balancing risk and reward to successfully detect and mitigate emerging threats—without adding friction that dissuades customers—is a strategic marathon. Yet cybersecurity operations also must move at a sprint to stay ahead of quickly evolving attacks.

That need for speedy adaptation is influencing security strategies. For instance, organizations moving to SECaaS, a proven means to quickly remediate new attacks and vulnerabilities, cited speed as the most significant driver. Those in security roles or with SRE and DevOps responsibilities were especially likely to name speed as the motivation.

Of course, SECaaS also offers other benefits, delivering expert security while potentially simplifying operations and easing management. That makes the shortage of sufficiently skilled people a related driver for adoption. As a result, more organizations are trusting their SaaS providers to deliver security at speed, keeping up with and blocking emerging threats more quickly and expertly than can be managed in-house.

Organizations still handling their own security aren't standing still, though. Their focus can be seen in deployments of app security technologies between the start of the COVID-19 pandemic and today:

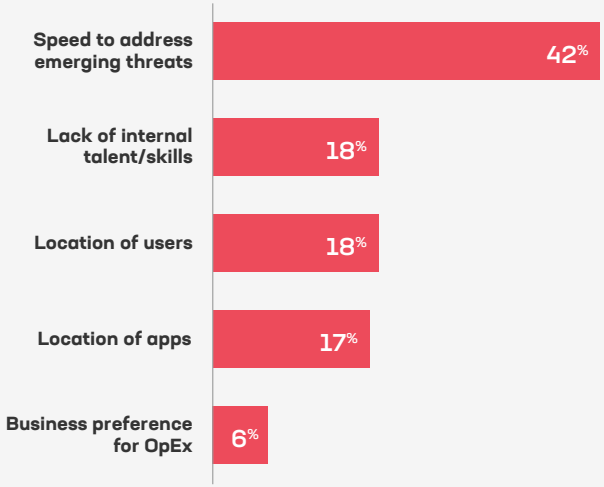
- Use of API gateways more than doubled, from 35% to 78% of respondents.
- ID federation deployments increased from 52% to 75%.
- Endpoint security grew from 65% to 86%.
- Secure web gateway (SWG) services jumped from 61% to 85%.
- WAF use grew from 66% to 82%.

This growth in deployment of app security technologies reflects increasing awareness of their vital role in quickly remediating the risks in a changing threat landscape.

The Speed of SECaaS Is Attractive

We asked:
What is the primary reason that you are using Security as a Service (WAAP, WAF, DDoS, API protection, etc.). Select one.

We learned:
The main motivator is threat mitigation speed.



Businesses are racing toward zero trust.

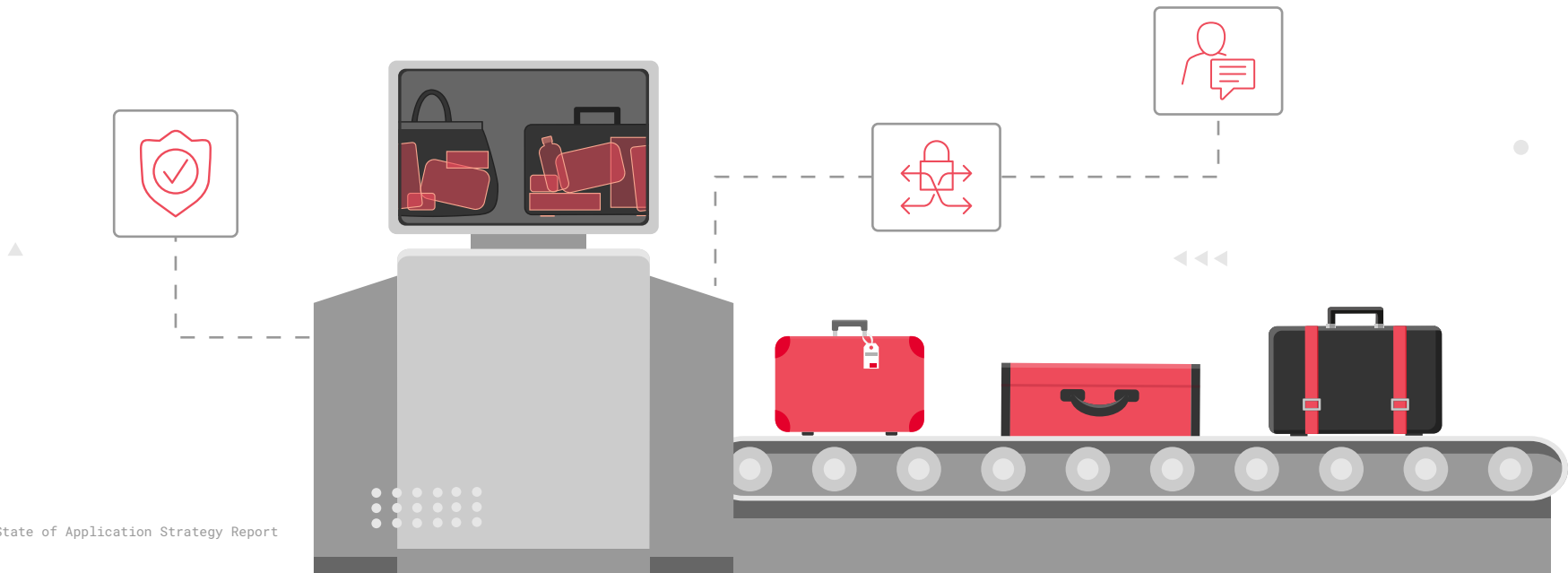
Velocity is also a factor in the rise of zero trust security models, which can transcend various architectures and hybrid deployments and simplify the security aspect of development and deployment processes. More than 80% of respondents say they're adopting zero trust or planning to do so. In fact, zero trust tied with the convergence of IT and operational technologies (IT/OT) as the most exciting global trend for the next few years. That's up from third place in 2022.

More than 80% of organizations are adopting zero trust.

Among other things, the continuous verification of zero trust models prevents mid-session compromises and coercive use of any authorized access to reach unauthorized resources. Relying on this identity-centric approach to security can reduce time to market for new features and apps as well as help prevent breaches that must be manually mitigated or patched. That's partly why deployments of IAM technologies have increased.

The promise of faster reaction speeds is also driving the use of AI/ML for security. Nearly two-thirds of organizations have plans (41%) or have already implemented (23%) AI assistance. Those already using AI or ML call security their top use case, and security is cited as a primary driver for those still in planning. (AI operations ranks second.)

Similarly, speed motivates ongoing efforts toward automation. The need is apparent: App development, transformed through automation, moves ever faster, while security and risk management still typically require high manual effort, oversight, and intervention. But organizations are making progress. In 2023, network security ranked not far below systems infrastructure as the third-most automated of the six core IT functions. Network security, which is increasingly offloaded to service models, also benefits from the application of AI.



Platforms and zero trust frequently go hand in hand.

Nearly nine in 10 respondents (88%) say their organizations are adopting a security platform, virtually the same proportion as those working toward a zero trust model. The trends overlap. Both reflect the complexity of securing a hybrid, multi-cloud world. But platform security also meets the desire to limit the proliferation of different solutions and vendors—while still providing consistent security for hybrid infrastructures, legacy and modern apps, and distributed APIs.

Organizations providing digital services to external users are especially likely to adopt a platform approach, as are businesses in the Americas and the tech industry, possibly because these survey respondents are also more likely to require global reach and scale.

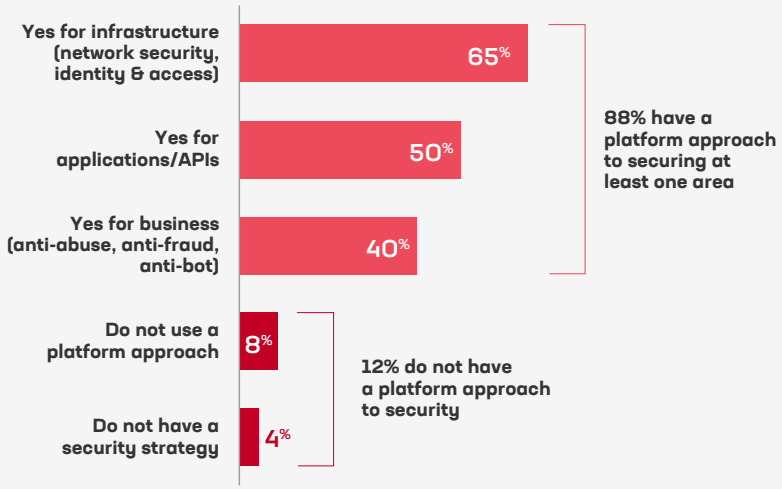
In terms of how it's applied, the platform approach is most common for securing infrastructure: Almost two-thirds (65%) expect to use a platform for network security or identity and access management. It helps that platforms designed to protect infrastructure have been available for a while. But half (50%) of respondents also are moving to a platform to secure web apps and APIs from the data center to the edge. Another 40% want a platform for business security needs such as anti-bot and anti-fraud solutions.

Regardless of exactly what they hope to protect, speed to address emerging threats is particularly important to the 40% of respondents who are using an ecosystem approach to select their security platform. The ecosystem approach (such as reliance on the partner marketplaces of a public cloud provider) offers two benefits. First, choosing from among multiple vendors enables organizations to choose the highest efficiency solution compatible with that ecosystem. Second, knowing that public cloud providers insist on basic integrations for third parties in the ecosystem shortens the time to value for security solutions.

Security Platforms Target Infrastructure Most

We asked:
When you consider your security strategy, are you adopting a platform approach? Select all that apply.

We learned:
Nearly 90% are adopting a platform approach, and many plan to use a platform to secure more than one area.



Interestingly, senior IT managers particularly lean toward an ecosystem approach. SecOps teams, however, prefer a single-vendor security platform. The difference of opinion probably rests on the likelihood that those higher in the organization are more keenly aware of the costs of fragmentation across IT functions.

Security services are the most common edge workload, but monitoring is growing most quickly.

Security is a top edge workload.

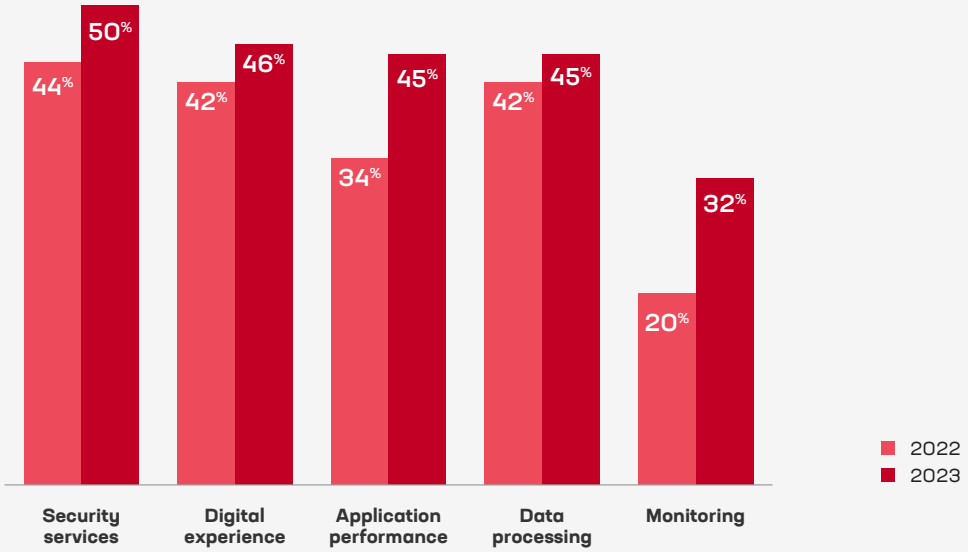
Of all organizations planning workloads for the edge, half expect to place security workloads there. But almost two-thirds of respondents currently adopting zero trust strategies plan to deploy security workloads at the edge, in recognition that fully executing zero trust—and gaining its full benefits—require use of the edge to secure every endpoint.

But while security services are the top edge use case, the edge workload growing fastest since 2022 is monitoring. This is likely a reflection of multiple factors: the explosion of remote work, IoT applications, the tendency toward wide distribution of applications, the global reach of markets today, and enthusiasm about the IT/OT convergence, which will depend on real-time data to guide process adjustments.

Security Is the Top Edge Workload

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

We learned:
Security accounts for the top edge workload, but monitoring is growing the fastest.



More organizations need to adopt a secure software development lifecycle.

Strong security starts well before deployment, however, regardless of where those workloads may be hosted. Accordingly, three-quarters (75%) of respondents are adopting or plan to adopt a secure software development lifecycle (SDLC). This result is a recognition that security and risk management are not a “one and done” activity that can take place only at the infrastructure or app deployment levels, for instance. Rather, comprehensive and consistent protection requires multiple, coordinated efforts over time and across IT and business roles. Addressing security as apps are developed saves time lost in trying to retrofit later, not to mention mitigation once an attack has succeeded.

Still, the minority of organizations not yet thinking about SDLC are better off than the 4% of survey respondents who say they have no security strategy at all—not for software and not for the business. Ouch.

Fortunately, most organizations are more proactive and looking upstream to mitigate all possible risks. Concerns about software supply chain security, for instance, are being addressed in various ways.

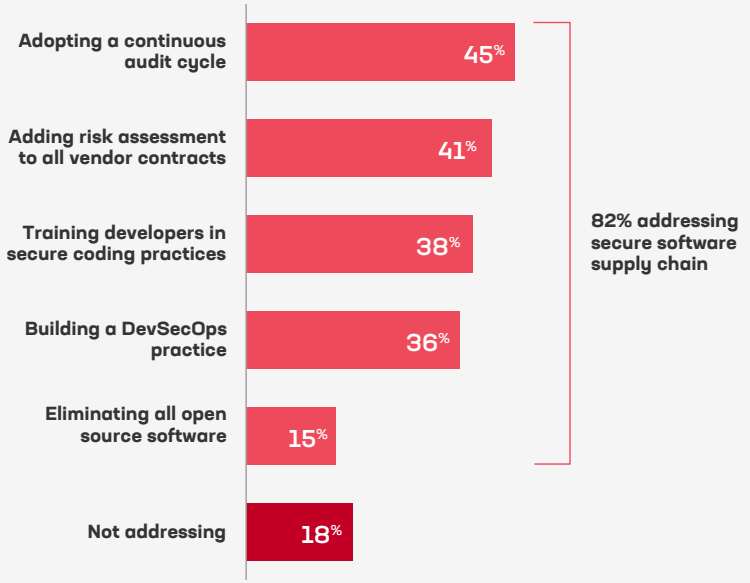
The most popular approach is adoption of a continuous audit cycle. More than one-third of businesses (36%) are building a DevSecOps practice. Roughly another third (38%) are training developers in secure coding practices.

Perhaps unsurprisingly, organizations in the financial services and healthcare industries are most likely to address software supply chain security in some manner. Meanwhile, nearly one in five organizations (18%) apparently have no concern about software supply chain security and are making no plans to address it.

Software Remains a Security Risk

We asked:
How is your organization addressing its secure software supply chain? Select all that apply.

We learned:
While most are taking at least one approach, the software supply chain remains an unaddressed risk for nearly one-fifth of respondents.



F5 Insight

In today's hybrid world, securing the business is harder than ever, and implementing consistent security policies is particularly difficult—but also key to greater velocity, agility, and resilience. While zero trust strategies are increasingly associated with network or infrastructure security, identity management technologies—including the use of authentication and authorization for API security—are still seen as the most valuable approaches to securing applications.

To support those apps, security and identity technologies are already the app services most likely to be deployed both on premises and in the cloud. They're also increasingly positioned at the edge as organizations take advantage of its performance and engagement potential. We expect the difference between deployment rates across environments to continue to shrink, even as the edge takes a growing share of security workloads, because app technologies, and especially security technologies, are necessary everywhere apps and APIs are deployed.

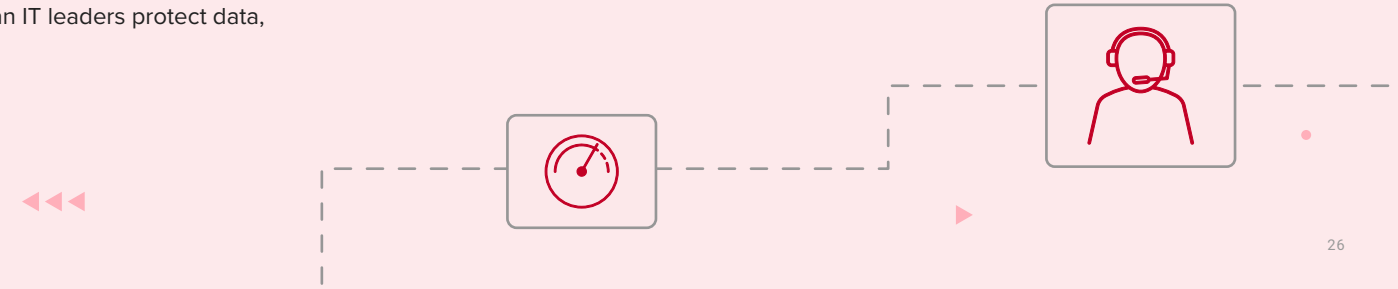
What this means for you

Security can become a digital differentiator, enabling app development teams to increase the speed of innovation without elevating risk or building friction between IT functions. Zero trust models, identity management, secure software development, and other security strategies and methods can—and should—coexist. Organizations should consider extending the notion of zero trust to the tools in their software development pipeline, including code repositories. To defeat highly motivated attackers, businesses need to protect not only the doors and windows but the mail slot, the chimney, and the stove vent. That's why software security processes such as SDLC need to be developed and followed. Only by addressing every possible point of vulnerability can IT leaders protect data, customers, and the business.

One example of this thinking is the expansion of API security beyond its traditional use in the data path. The more interesting API security solutions emerging today address east/west communications, such as via a POST agent. Such creative thinking can keep organizations ahead of attackers and free IT resources from manual mitigation so they can accelerate the business instead.

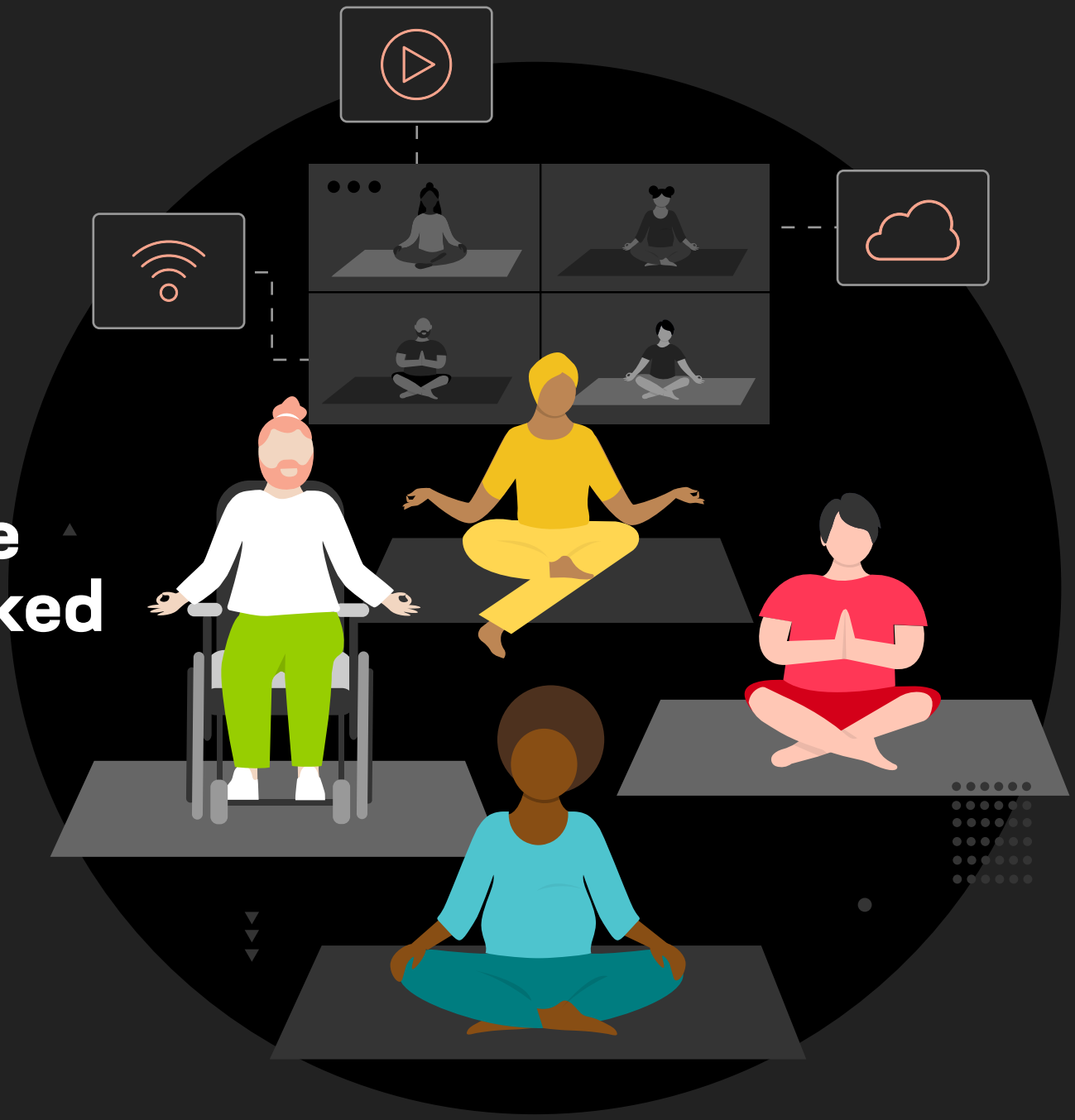
Moreover, applications and their underlying API fabrics are only as secure as the infrastructure they are built, deployed, and operated on. The simplest way to obtain the comprehensive protection that provides resilience and agility will be to use environment-agnostic solutions, consumption models, and vendors that protect both apps and infrastructure everywhere. SECaaS is one option that may be particularly useful for organizations with pressing mitigation needs, limited in-house security expertise, or a preference for operating expenditures over capital costs, for instance.

The ability to implement uniform security policies for any app and any API, anywhere, is important. Security platforms, including SaaS-based services, can help secure hybrid apps and APIs across all host environments, from the core to the edge, with policy consistency, broad visibility, and simplified management. This type of approach can defend both modern and traditional architectures and hybrid apps with WAF, DDoS protection, and bot defenses integrated with behavioral-based intrusion protection and attack mitigation for the entire security stack. Such effective security, running at the speed of business, protects what matters most while unleashing the organization's potential for growth.



Conclusion

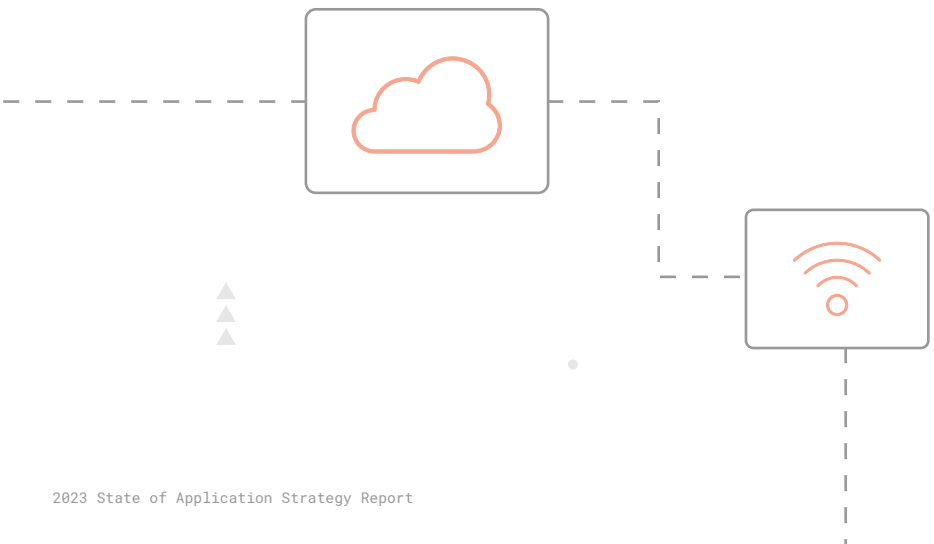
There's Hope for Overworked IT Teams



AS APP PORTFOLIOS grow increasingly modern, organizations will continue to adjust their deployment architectures to balance operational and market demands and to find the right distribution between on-premises, cloud (whether private, public, or both), and edge environments—as well as which apps to consume as SaaS. They'll surely consolidate where they can. Nonetheless, we expect the vast majority to use hybrid and multi-cloud models indefinitely.

This view is supported by the pace of technological change, the tradeoffs of technical debt, and the fact that as a result, most organizations must juggle two or three generations of technology. Those technologies may leapfrog each other, just as mobile phones have conquered markets that had few or no landlines, but multiple paradigms will coexist.

Perhaps more important, hybrid models provide the greatest flexibility for deployment decisions, which are generally made per application based on app-specific needs, benefits, and objectives. In the face of competitive time-to-market pressures and the importance of customer satisfaction, most organizations will keep choosing agility, speed, and the ability to optimize the digital experience. Modern apps and microservices enable the necessary connections, such as between traditional, monolithic apps at the core of the business and mobile interfaces.



As a result, the challenges of multiple clouds, distributed deployments, and hybrid IT stacks will continue in one form or another. There's hope, however, for overworked IT teams. More automation, a layer of consistent security enforced by declarative deployment policies, AI/ML in IT operations, and standardized methodologies such as SRE—plus the right technologies, solutions, and partners—can help organizations rise above the complexity to increase business velocity. Continued growth in real-time monitoring at the edge, as well as solutions that make that telemetry actionable, can feed the AIOps that reduce manual management. Zero trust security approaches and cross-environment platforms can connect and protect apps and APIs everywhere they're deployed, as well as the infrastructure that supports them. Abstraction layers, such as those utilized by app security and delivery technologies, can transcend boundaries and provide a nexus for more centralized, and thus simplified, connection and control.

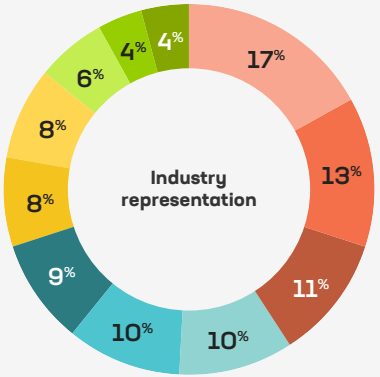
The vast majority of organizations will use hybrid models indefinitely.

Since no organization has the expertise to do all that alone, business partners who understand and thrive in the hybrid world can offer significant value. In particular, technology providers like F5 can be a force for simplifying the complexity to provide comprehensive protection and consistent performance. The right partner can help you deliver and protect modern and traditional apps distributed across hybrid IT stacks using a variety of consumption models, including SaaS. Together we can make the hybrid life we're all living easier, safer, and more rewarding.

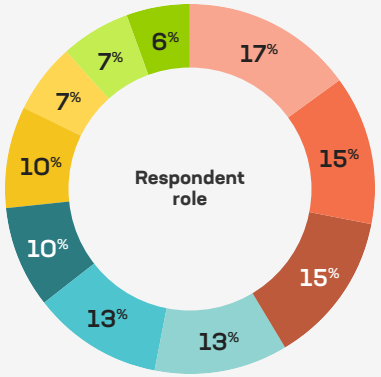
About the report

More than 1,000 IT decisionmakers from around the globe shared their priorities and concerns with F5 in this year's survey. The APCJ region was particularly well represented this year. As always, the respondents represented a broad mix of industries, with government sectors more well represented than in the past and technology companies slightly less prominent.

Data was provided by people in a wide range of IT and managerial roles, from the C-suite to the trenches of app development, with more business app owners than in previous years. F5 greatly appreciates the contributions of everyone who took the time to share their activities, interests, and insights about digital transformation.



- Technology
- Financial services
- Manufacturing and resources
- Distribution and services, including retail, wholesale, transportation, and media
- Government/public sector
- Cloud service provider
- Telecommunications
- Education
- Other
- Healthcare
- Energy/utilities



- IT leader
- Network
- Data science
- Operations
- Other
- Security
- Business leader
- Business or tech app owner
- Cloud or enterprise architect
- Site reliability engineer (SRE), developer, DevOps, or DevOps manager

About F5

F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure and optimize apps and APIs anywhere–on premises, in the cloud, or at the edge. F5 enables organizations to provide exceptional, secure digital experiences for their customers and continuously stay ahead of threats. For more information, go to f5.com. (NASDAQ: FFIV).