2022
State of Application Strategy Report

Contents

Introduction
Financial Services Remain in the Digital Vanguard

THE EIGHTH ANNUAL F5 survey on the state of application strategy today found that across industries and around the globe, digital transformation continues to accelerate. As consumer expectations increasingly focus on secure digital interactions, financial services—from banks and payment processers to insurers and investment services—have had to adapt. Examples of such adaptations range from the innovation of mobile deposits not so long ago to today's selfie banking and robo-advisors. As a result, the industry has recently moved into a leading position when it comes to digital transformation and modernization efforts. That leadership has continued in 2022.

The results of our latest survey reveal what's on the minds of these leading financial services organizations now and for the near future. In general, the industry's focus on improving the customer experience is currently playing out through:
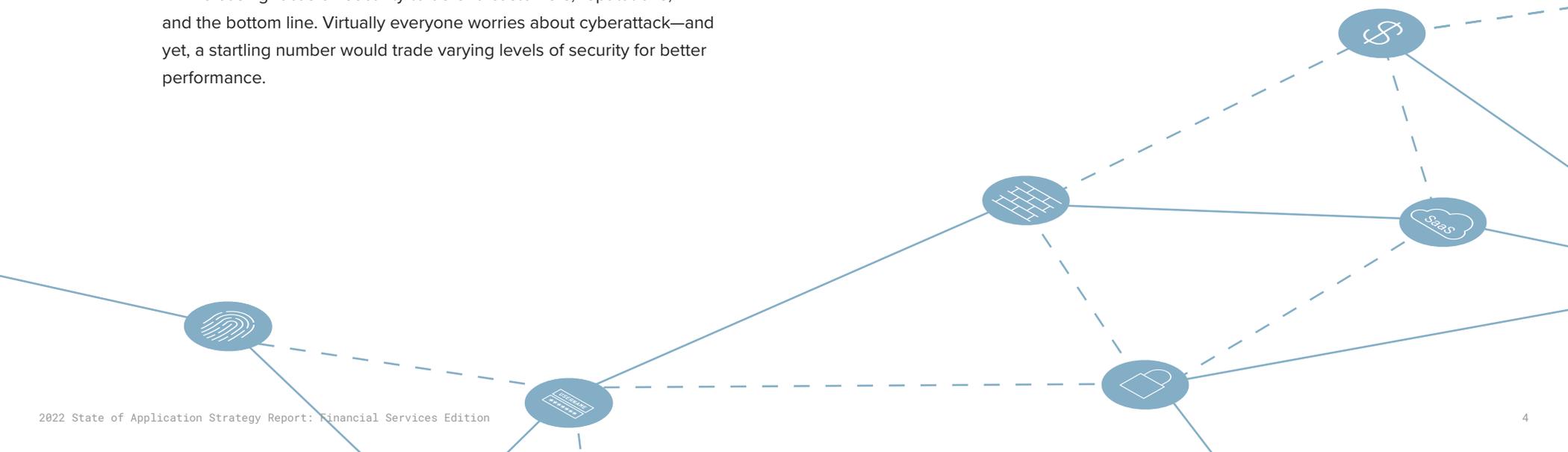
- Continued digital transformation and rapid modernization, including aggressive plans for artificial intelligence (AI) and machine learning (ML). A full 94% of financial services organizations have current projects related to digital transformation.
- Maturing multi-cloud strategies, with more than nine in 10 organizations planning significant use of the edge.
- An increasing focus on security to defend customers, reputations, and the bottom line. Virtually everyone worries about cyberattack—and yet, a startling number would trade varying levels of security for better performance.

Other shadows in this digital progress include a lack of insights—including some that will be needed to truly unleash AI and ML for the more than three-quarters of financial services organizations who expect these technologies to help deliver more personalized customer experiences.

More than **nine in 10** financial services organizations are actively pursuing digital transformation.

How do your organization's priorities stack up against the trends? The data and insights that follow reflect the responses of more than 200 financial services IT decision makers working for organizations of all sizes around the globe. The North American and the Asian Pacific regions were particularly well represented.

To put these results in context, get the full picture across industries from the global F5 2022 State of Application Strategy Report.

01

Rapid Digital Transformation and Modernization Continue

DIGITAL TRANSFORMATION EFFORTS are nearly ubiquitous in the financial services industry, with 94% of organizations actively automating business processes, employing APIs to participate in third-party ecosystems, or enhancing operations or processes with AI or ML. That's nine percentage points higher than 2020's results.

In addition, digital applications are more essential than ever for most financial services businesses. Two years ago, slightly fewer than three-quarters (74%) called apps "essential for business." In other words, more than a quarter of respondents considered them optional.

But the ramifications of the COVID-19 pandemic whittled away much of that ambivalence, and it's harder today to imagine a financial services business without digital applications. They're important to maximize the efficiency of employees and previously manual internal processes, of course. They also speed and streamline interactions with suppliers, analysts, regulators, and other organizations. But most importantly, they provide customers with

24-hour, self-service, on-the-go functionality—a competitive advantage in today's fast-paced digital society. In fact, banking representatives tell us their customers expect the experiences to be on par with those of consumer properties such as Google and Facebook.

90% provide digital services outside their own organizations.

The number of financial services organizations that provide digital apps beyond their organizational walls may be one indicator of their growing centrality, as well as of rising business interconnectivity. Today only 10% of financial services respondents provide applications for employee use only. Conversely, nine in 10 provide digital services to others, with a larger share of those apps for consumers than in any other industry. Nearly half of financial services respondents also provide digital services to other businesses (B2B)—a rate second only to the technology industry.
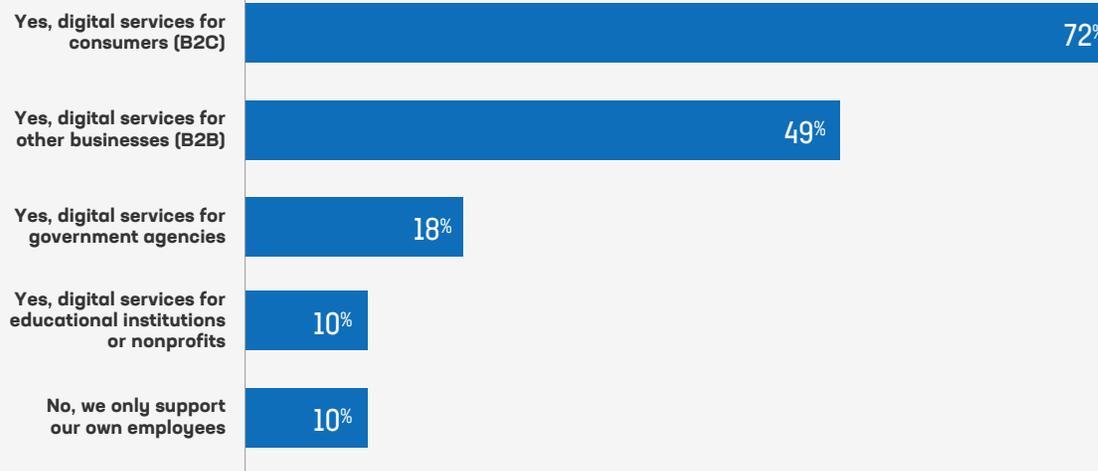
The Recipients of Digital Services

We asked:
Does your organization provide digital services in support of other organizations or consumers? Select all that apply.

We learned:
Financial services are more likely to provide digital services to consumers than any other industry.

Category	Percentage
Yes, digital services for consumers (B2C)	72%
Yes, digital services for other businesses (B2B)	49%
Yes, digital services for government agencies	18%
Yes, digital services for educational institutions or nonprofits	10%
No, we only support our own employees	10%

Everyone is modernizing

Regardless of who uses those applications, 99% of financial services organizations are modernizing them—a considerable jump from 83% in 2021. Their motives range from enhancing security and the customer experience to streamlining management and speeding the release of new features.

Most financial services organizations use multiple methods for modernization. Last year, APIs were the method of choice, but APIs can't do the job by themselves. To take advantage of them, organizations across industries are adding modern components such as microservices or new user interfaces, and financial services are particularly busy with this activity in 2022. In addition, more than a third of financial services respondents say they're modernizing by applying site reliability engineering (SRE) practices, which typically enable greater speed, automation, and agility in the development and deployment of modern apps and components.

F5 Insight

Digital transformation will never be done, and application modernization is a moving target. That's particularly true in competitive financial services markets. While they're not yet a majority method of choice, we expect SRE practices to give those who adopt them a competitive edge as the number of new applications continues to explode and the balance of traditional and modern (or modernized) apps continues to shift toward the latter.

What this means for you

Successful organizations will evaluate all their options for modernization—including the adoption of SRE practices—and choose those best suited for the organization's goals and skills.
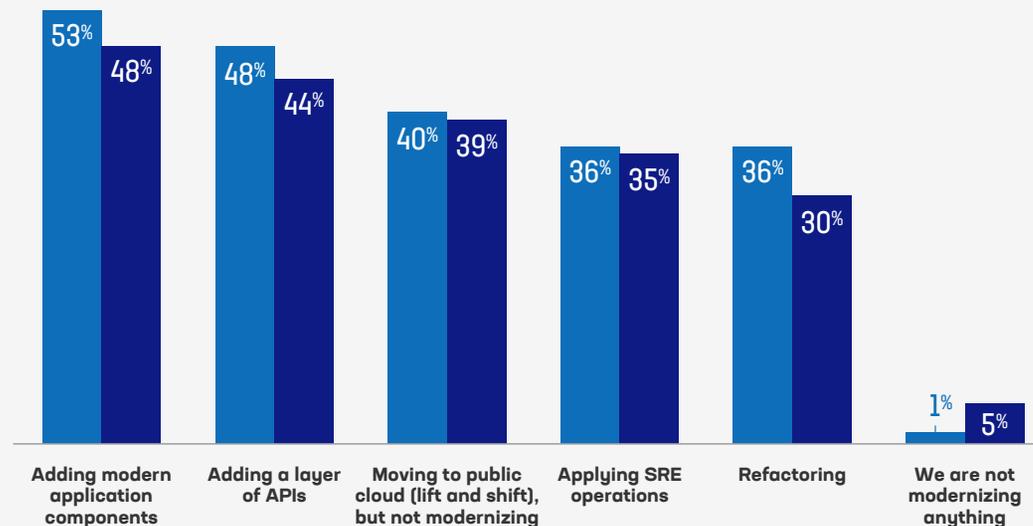
App Modernization Methods

We asked:
What methods are you using to modernize applications? Select all that apply.

We learned:
The addition of modern application components is increasingly complementing the layering of APIs.

- ■ Financial Services
- ■ All Other Industries

	Financial Services	All Other Industries
Adding modern application components	53%	48%
Adding a layer of APIs	48%	44%
Moving to public cloud (lift and shift), but not modernizing	40%	39%
Applying SRE operations	36%	35%
Refactoring	36%	30%
We are not modernizing anything	1%	5%

02
Multi-Cloud Strategies Are Maturing

ALONGSIDE THE EFFORTS to modernize applications, financial services have largely adopted cloud, hybrid cloud, and multi-cloud strategies. Our survey results indicate that 71% of financial services organizations have multi-cloud strategies, a rate equal to that across industries globally. But the story contains some interesting wrinkles.
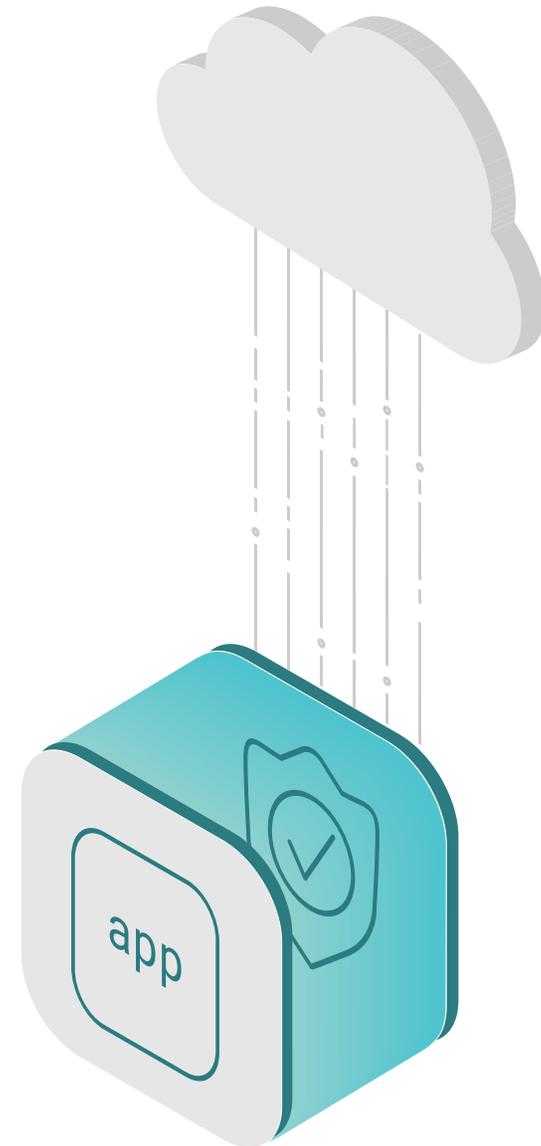
In 2020, the top strategic trend for financial services was adoption of public cloud platforms. This represented a big shift from the prior year and predictions that security concerns would limit the industry's cloud use. We noted in our report for that year that although mission-critical or core apps would likely be the slowest to be moved to the cloud, the sudden jump in cloud interest suggested that financial services organizations were "'all in' with respect to the cloud."

That shift reflected the growing realization that most attacks don't happen at the network and infrastructure levels anyway. Rather, the biggest threats target applications and APIs, which need protection no matter where those apps are hosted. Accordingly, although public cloud providers are increasing the sophistication of their security offerings, organizations still need to proactively protect their applications and APIs everywhere. That often means moving toward the same zero trust security models regardless of the deployment location.

Two years later, growing industry confidence in public and hybrid clouds is evidenced by cloud deployment not only of commoditized functions such as data lakes but also increasing use of:

- Infrastructure as a Service (IaaS), used by 32% of financial services respondents.
- Platform as a Service (PaaS), used by 34% of respondents.
- Security as a Service (SECaaS), used by 42% of respondents.

These usage rates for PaaS and SECaaS are higher than the average across all other industries. Similarly, only 58% of organizations outside

of the financial services industry rely on the environment's native services when deploying a container or cloud-native application environment. But nearly three-quarters (72%) of financial services organizations do so. Focused on reducing the friction and time-to-deployment for security and delivery services, financial services organizations seem to have confidence that the security postures of their public clouds have improved enough to dispel earlier doubts.

Repatriation has jumped

Nonetheless, application repatriation figures also jumped enormously over expectations just one year ago, not only across industries but in financial services particularly. In 2021, fewer than a third of financial services respondents had recently repatriated apps or were planning to do so. In 2022, more than double that amount—75%—said they had or soon would.

App repatriation exploded
168% over previous expectations.

This move to bring apps back home is probably being driven as much by cost, control, or flexibility needs as security concerns. First, the promised cost efficiencies of the public cloud may have been harder to capture than expected. Second, financial services organizations are figuring out, sometimes through trial and error, which data, applications, and app security and delivery technologies they truly must control themselves and which can be hosted and managed more efficiently in a public cloud.

Finally, the industry's significant use of SRE practices is likely a factor in these repatriations. That's because organizations adopting SRE practices can bring cloud-like agility to their on-premises environments without facing rising costs from third-party cloud providers. While 76% of respondents across industries have already implemented or expect to implement SRE practices, 84% of financial services have done so or plan to soon.
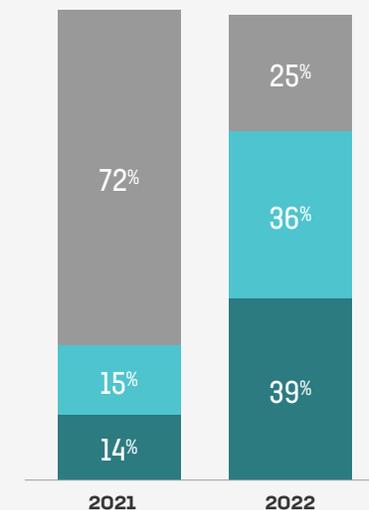
Application Repatriation

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

We learned:
Nearly three-quarters of financial services organizations have done so or soon will.

- No
- Planning
- Yes

	2021	2022
No	72%	25%
Planning	15%	36%
Yes	14%	39%

Whatever the motives for repatriation, its growth represents a rationalization and maturation of cloud strategies by the financial services organizations involved.

There's nothing fringe about the edge

Deployments at the edge can be considered an extension of a multi-cloud strategy, and 87% of financial services decision makers plan to use the edge. Workloads that support the digital experience, such as mobile apps and web front ends, were identified as the priority, with 49% of financial services respondents expecting to deploy such workloads at the edge—higher than for any other industry.

Security service workloads ranked a close second to digital experience workloads for this industry—in just one example of how security concerns are driving decisions for financial services organizations.

F5 Insight

On-premises data centers aren't going away, but at the same time, app modernization is helping to drive increased use of multiple clouds. Similarly, whether they're deployed in a public or private cloud or at the edge, applications—and the app security and delivery technologies that support them—will be increasingly distributed.

What this means for you

Most organizations will continue to contend with complexity and its challenges. In this context, a mature multi-cloud strategy will include systematic and well-planned deployment decisions, most likely supported by SRE practices. Policy consistency and ease of management can provide a competitive advantage, as can technology partners whose solutions work efficiently and consistently across a variety of deployment models and environments.
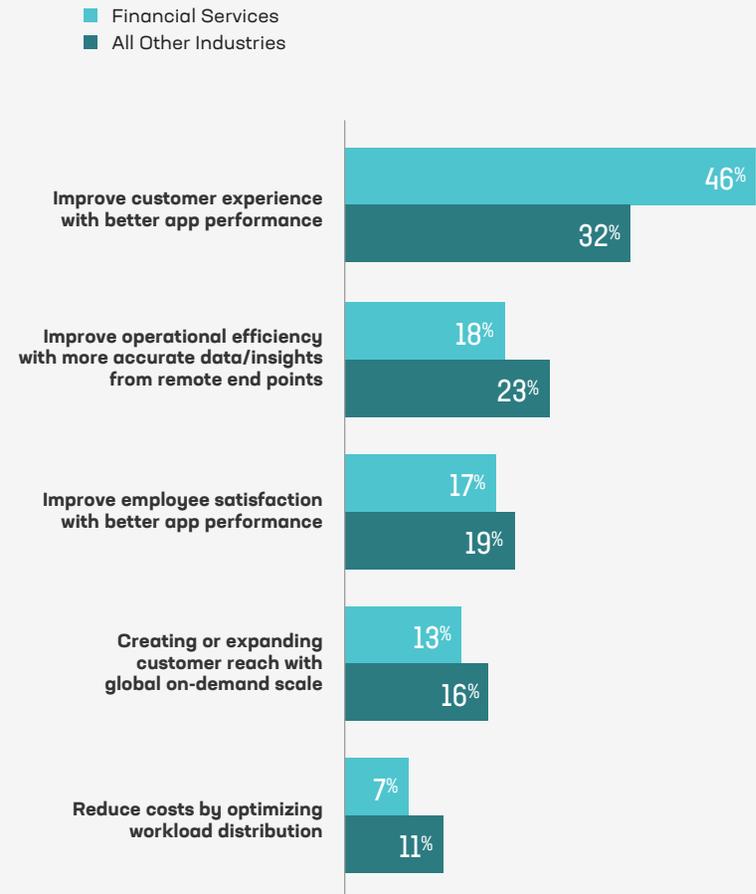
Edge Outcomes

We asked:
What is the primary business outcome you want to achieve using edge computing? Select one.

We learned:
Financial services organizations are considerably more motivated than others to use the edge as a means of improving the customer experience.

■ Financial Services
■ All Other Industries

Improve customer experience with better app performance	46% / 32%
Improve operational efficiency with more accurate data/insights from remote end points	18% / 23%
Improve employee satisfaction with better app performance	17% / 19%
Creating or expanding customer reach with global on-demand scale	13% / 16%
Reduce costs by optimizing workload distribution	7% / 11%

03

The Focus on Security Is Increasing– With Limits

FINANCIAL SERVICES ORGANIZATIONS are aware they're in the crosshairs of attackers. But today's attacks are often indirect, frequently targeting APIs through third parties such as FinTech data aggregators. As a result, the same innovations that can add features and improve customer service make it harder than ever to manage risk.

96% have made changes in the last year in response to security threats.

It's no surprise, then, that only one respondent, representing significantly less than 1% of survey responses, said they don't worry about cyberattacks. (And we wonder about the source of their confidence.) In addition, nearly every organization has made changes in the last year in response to threats. The most common change, reported by two-thirds of respondents, was to add ransomware training for employees. More than half also increased their focus on vulnerability management and automation.

Multi-cloud migraines
Multi-cloud strategies only complicate the picture. Financial services decision makers operating multiple clouds ranked consistent security as one of their top two concerns, with 45% calling it an issue. This may be another reason for the unexpected jump in application repatriation.

Consistent security remains a top multi-cloud challenge.

The good news, however, is that a larger 59% of financial services organizations called consistent security a multi-cloud challenge two years ago in 2020. The 15-point reduction suggests that a significant number of organizations are finding solutions while still pursuing their multi-cloud goals. Perhaps as a result, visibility into application health—not a major concern in 2020—ranks as an equal challenge today.
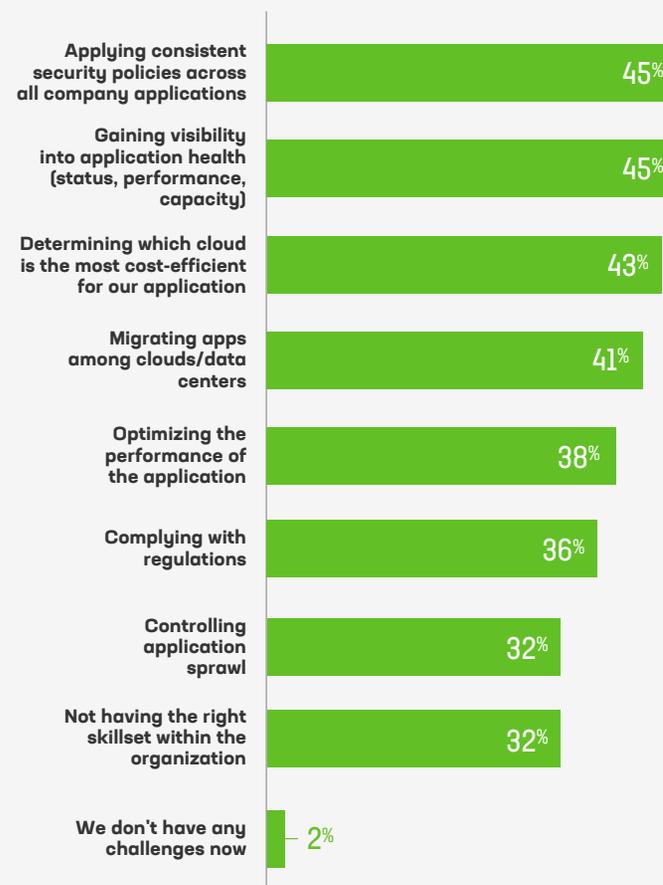
Multi-Cloud Challenges

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

We learned:
Nearly every multi-cloud organization faces related challenges, with security and visibility topping the list.

Challenge	Percentage
Applying consistent security policies across all company applications	45%
Gaining visibility into application health (status, performance, capacity)	45%
Determining which cloud is the most cost-efficient for our application	43%
Migrating apps among clouds/data centers	41%
Optimizing the performance of the application	38%
Complying with regulations	36%
Controlling application sprawl	32%
Not having the right skillset within the organization	32%
We don't have any challenges now	2%

Meanwhile, even for organizations without a multi-cloud strategy, open banking initiatives continue to make API use almost ubiquitous in the industry. It follows that API security solutions are nearly as common, with 86% of financial services organizations reporting that they've already implemented one or plan to within the next 12 months. That compares with 77% of respondents across all other industries and marks a big increase from the 69% of financial services deploying API security solutions in 2021. Not surprisingly, those who deploy at the edge are more likely to have implemented an API security solution than those without plans to do so.

Balancing security with performance
Still, security is just one aspect of the overall customer experience, and not everyone in the financial services industry agrees on how to achieve the right balance.

For instance, a reputation for security and trustworthiness remains a core tenet of the financial services industry. Accordingly, when asked if they'd turn off security for better performance, financial services decision makers were slightly more likely than others to say there was "no chance" of that.

Nearly three-quarters would trade security for better performance.

But not all of their colleagues are so security-minded. In fact a full third of the industry's decision makers said they'd trade security for even a small improvement in performance—less than 25%. Only 18% of respondents in other industries agreed; most would need larger performance gains to be lured. Likely the new competitive dynamics in the industry, including FinTech only apps, is contributing to this performance demand.
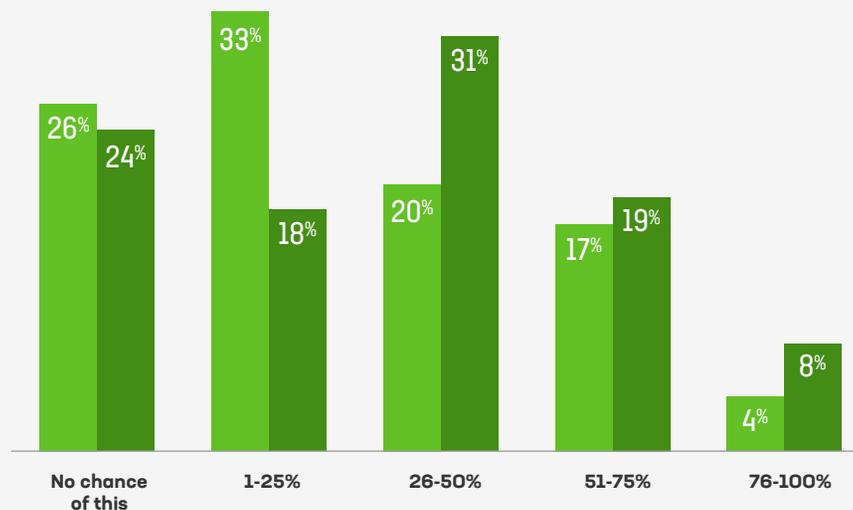
The Security/Performance Balance

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

We learned:
A rather shocking share of financial services organizations wouldn't need much temptation.

■ Financial Services
■ All Other Industries

	No chance of this	1-25%	26-50%	51-75%	76-100%
Financial Services	26%	33%	20%	17%	4%
All Other Industries	24%	18%	31%	19%	8%

This tension between security and performance influenced which technology trends most excite financial services decision makers. AI operations (AIOps) won the contest in 2021 but dropped to fifth place this year, and all three top trends in 2022 relate to security—from web application and API protection (WAAP) at the top through zero trust to secure access service edge (SASE). Respondents in other industries were more intrigued by the convergence of IT and operational technologies (OT), which ranked as the most exciting trend globally, and the opportunities presented by 5G.

The top three most exciting trends: **WAAP, zero trust, and SASE**.

Security is also a key driver in financial service organizations' plans to use AI and ML. But ambitious plans may collide with reality, because the survey results suggest that missing insights and processes may make it difficult to fulfill the industry's hopes for an AI-assisted future.

F5 Insight
The new vulnerabilities discovered daily fully warrant the industry's continued high interest in security—particularly for apps and APIs, where the greatest risks converge.

What this means for you
Rather than considering WAAP and zero trust security as solutions for sometime in the near future, now is the time to take meaningful steps toward implementing them. Financial services organizations should also ensure their web application firewalls (WAFs) and bot defenses are sophisticated enough to handle the latest threats with minimal friction and low false positives. Investments in these areas will increase the ability to contextually manage threats while also protecting performance and efficiently managing risk.

Conclusion
Big Plans for AI/ML Require a Stronger Foundation

FINANCIAL SERVICES ORGANIZATIONS have become accustomed to leading digital innovation, whether that means point-of-sale (POS) financing or interactive loan disclosures. Increasingly heated competition forces both leaders and startups to seek technologies that offer a competitive edge, and organizations that lag are likely to vanish. So it's not surprising that financial services organizations in 2022 report such high levels of application modernization and integration, multi-cloud adoption, movement toward the edge, and security pursuits ranging from API protection to WAAP, SASE, and zero trust models.

Similarly, it's impressive but not shocking that 94% of financial services plan to use AI assistance or are already doing so. That compares with 88% for other industries, and expected deployment rates are higher for financial services regardless of the business area affected.

There's a hitch in this collective planning, however, because only one in five financial services respondents expects to implement AIOps. But it won't be possible for resource-constrained IT teams to manually deploy and manage the microservices and analytics required to capitalize on AI or ML at scale.

94% plan to or will implement AI/ML, but 98% are missing needed insights.

A second limitation is having access to sufficient insights and analytics. Across industries, 98% of respondents say they're missing insights they need. The same percentage applies for financial services organizations. But meeting consumer demands for greater personalization will require better insights and more sophisticated analytics than currently are in place.
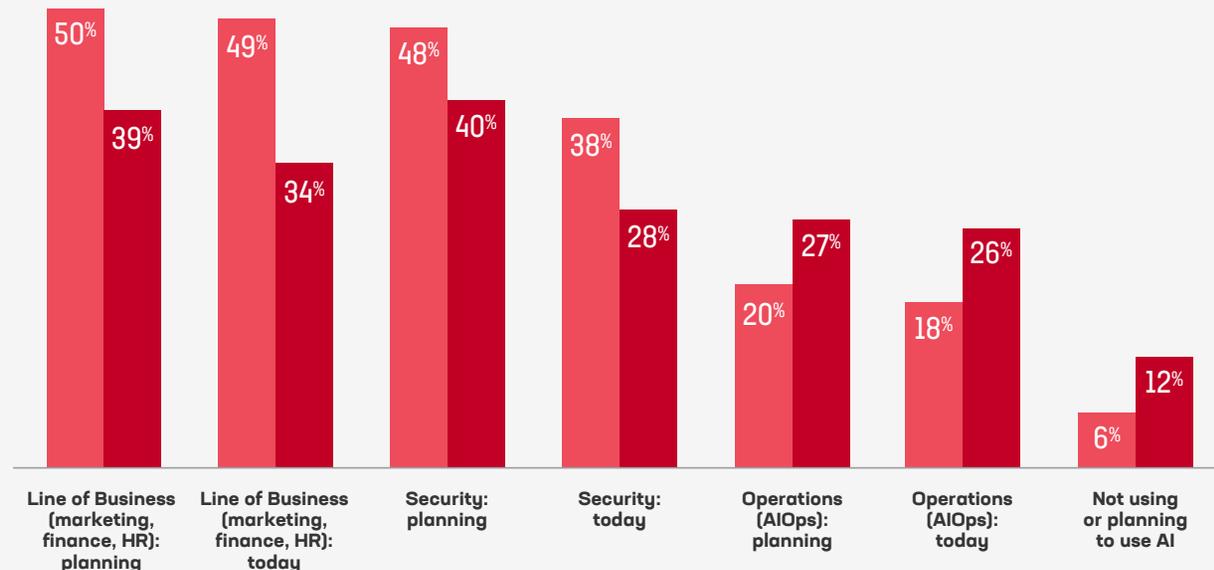
Use of AI/ML

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

We learned:
More than nine in 10 financial services expect to use AI-assistance.

■ Financial Services
■ All Other Industries

Line of Business (marketing, finance, HR): planning	50% / 39%	
Line of Business (marketing, finance, HR): today	49% / 34%	
Security: planning	48% / 40%	
Security: today	38% / 28%	
Operations (AIOps): planning	20% / 27%	
Operations (AIOps): today	18% / 26%	
Not using or planning to use AI	6% / 12%	

The IT decision makers in financial services organizations are undoubtedly aware of this dilemma. But awareness won't be enough. Organizations will likely need to match their AI ambitions with increased investments not only in security and ML technologies, but also in IT operations, telemetry, and analytics. It will take improved skills and processes as well as new technologies and platform-agnostic tools to overcome the complexity of multi-cloud architectures while delivering the insights, automation, and integration required for AI assistance to achieve business goals.
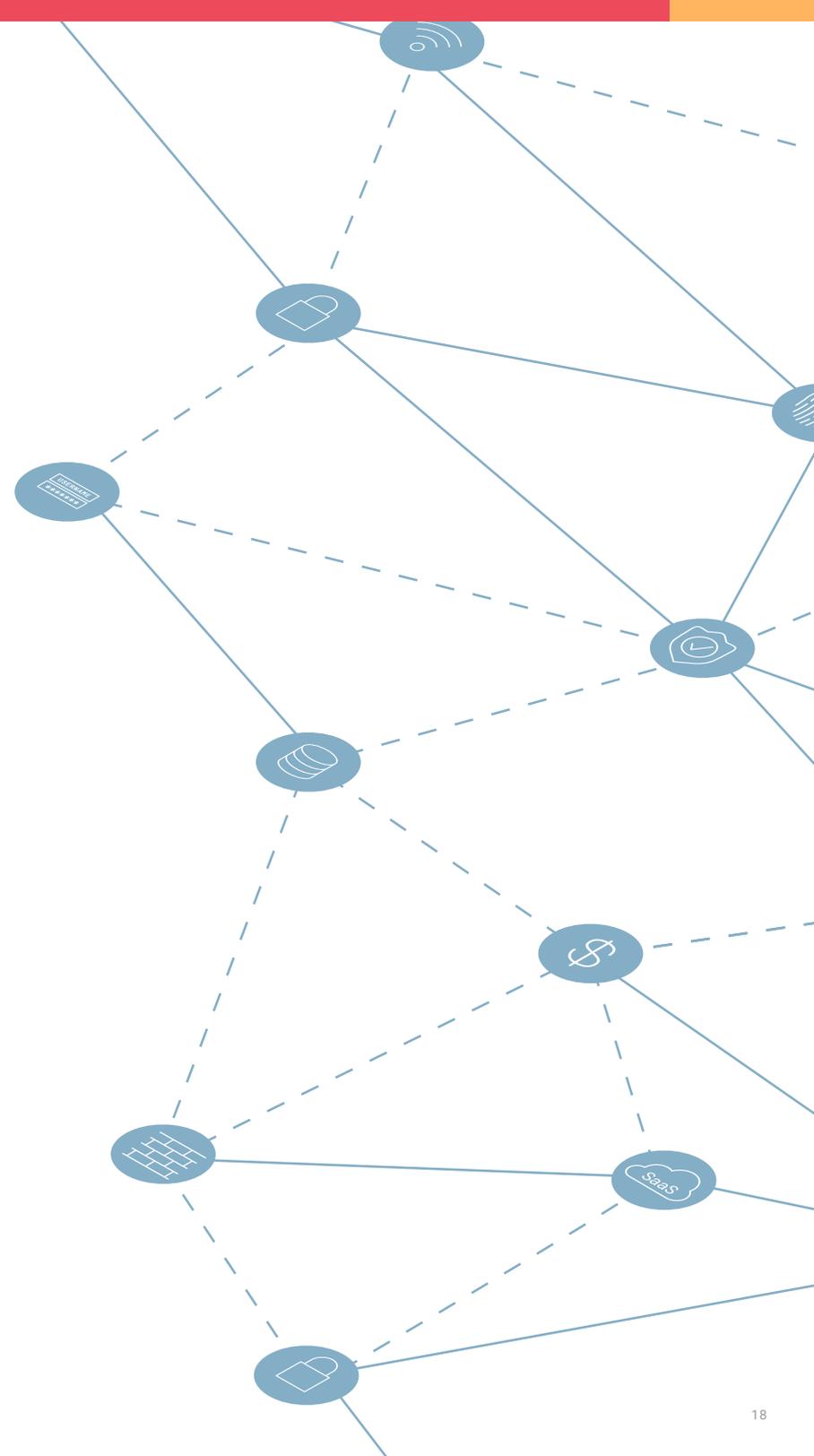
F5 Insight

Before AI or ML can be implemented at production scales, financial services organizations will need to solve the challenge of extracting and processing the telemetry from distributed applications, and the app security and delivery technologies that support them, with speed and scale. And the need for modernization and integration applies not only to apps but the operations and processes that support them.

What this means for you

SRE practices and intelligent, platform-level solutions that provide consistent protection, performance, and real-time telemetry across the entire portfolio can minimize administrative burdens and ensure the resulting data can be efficiently put to use without manual integration. Meanwhile, vendors whose solutions transcend data silos and support automation can help solve the security challenges of today's multi-cloud architectures.

Only when IT processes and telemetry—and the methods for collecting and analyzing it—are as up-to-date and integrated as modern apps will financial services organizations be able to react holistically, in real time, to changing conditions. Such dynamic adaptation will soon be essential to satisfy customers, innovate, more quickly bring differentiated services to market, and grow while competitors fall by the wayside.

About F5

F5 solutions for automation, security, performance, and insight empower industry leaders to create, secure, and manage adaptive applications that reduce costs, increase business success, and better protect people and organizations.

f5