State of Application Strategy Report

2021

Telecom Edition

Contents

Introduction

Telecom Leads as Digital Transformation Leaps Ahead

As telecommunications providers continue their digital transformation initiatives and the transition to 5G, leaders are augmenting operations with AI and looking toward the edge, which the industry has generally been approaching from the perspective of multi-access edge computing (MEC). This move toward the edge, with 5G serving as a catalyst for new business opportunities, will likely help telecom organizations deliver on the promise of their 5G networks and better provide the rich quality of experience (QoE) their subscribers and customers have come to expect.

In the past year, the COVID-19 pandemic vastly accelerated global digital transformation toward a more data-driven future, with progress leaping forward across industries. Telecom providers, already among the leaders, have progressed further than their peers in other industries, with 62% of organizations in an advanced stage of digital transformation marked by the use AI and machine learning. That compares with 57% of other global respondents.

Digital transformation generally occurs in three phases: task automation, digital expansion, and AI-assisted business. Telecom survey respondents indicated that nearly two-thirds of companies are undertaking projects in the third stage of transformation. The majority are also working on digital expansion in the second phase.

The phases of digital transformation are not mutually exclusive, of course. Automation and orchestration, last year's top trend for telecom organizations, continue at a rapid pace, with 77% of telecom providers using automation for their networks and security. That's 9 points higher than reported by other survey respondents. Automation is helping providers integrate their applications and reduce the operational cost of managing them across the complex multi-cloud environments of their increasingly virtual networks. Meanwhile, 55% of telecom providers are treating infrastructure as code—that is, they provision and manage infrastructure, including platforms, container systems, and services, through declarative or scripted definitions or code. This percentage, which is slightly higher than for other industries, is an indicator of advanced progress in digital transformation.

Among the past year's unprecedented changes to how organizations and individuals use digital tools, one truth stands out: It is no longer sufficient for business leaders to think of applications and application security and delivery technology as merely part of an effective IT strategy. Applications are particularly critical for the mobility network, and they have become so central to how we live, work, and interact daily that a strategic approach to applications is required to support a distributed business driven by real-time application data.

Digital Transformation Toward a More Agile Network

We asked:

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

We learned:

Nearly two-thirds of organizations have projects related to AI-assisted business, such as AI-based security, business process optimization, or AI operations (AIOps).

Phase 1: Task Automation

31%

Compared to 25% across industries

Phase 2: Digital Expansion

56%

Compared to 57% across industries

Phase 3: AI-Assisted Business

62%

Compared to 56% across industries

01

API Management Increases Security

As digital transformation proceeds globally, application modernization is a focus for organizations across industries, and telecommunications companies are no exception. Three-quarters of telecom respondents report application modernization efforts underway, with APIs as the method of choice. APIs help to provide the connective tissue in the industry's complex and multi-vendor ecosystems as organizations move away from hardware with network function virtualization. They've become increasingly popular as a means of modernizing applications and enabling seamless digital experiences for customers.

But security is a bigger issue for telecom providers than ever. As enterprises modernize and applications become increasingly dispersed in multi-cloud and edge deployments, the attack surface for those applications expands significantly, thanks to the composite services within these applications and the various environments in which they operate. APIs are an area of particular concern, in part because they often self-document information about their structure and implementation. Weak authentication, a lack of encryption, and insecure endpoints can also make APIs vulnerable. In addition, telecom respondents report a shortage of the needed skills to work with APIs. (See Section 4.)

Telecom companies lead in deploying API gateways and security solutions.

Accordingly, telecom companies are slightly more likely than average to rely on the APIs and other tools of public cloud providers while also managing their private clouds and related toolsets. Amid this complexity, telecom firms are more likely than those in other industries to have implemented an API security solution. Almost three-quarters have done so, compared to 59% of the total survey population.

Telecom respondents are also more likely than firms in other industries to have an API gateway, with 56% already using one and another 19% with imminent plans to do so. Telecom respondents are slightly lagging in API call volumes compared to other respondents, with 37% reporting over 1 million API call volumes compared to 40% of

API Security

We asked:

Have you implemented an API security solution or plan to implement one in the next 12 months?

We learned:

71% of respondents will have done so before the end of 2021, compared with 59% of respondents across all industries.

other respondents. This is likely due to the industry's more traditional architectures and security concerns about opening up the infrastructure to third parties. However, the substantial use of API gateways and security solutions is probably why telecom respondents report slightly greater confidence than most other respondents regarding their ability to mitigate API vulnerabilities and protect their applications.

F5 insight

The 5G network core is based on a service-based architecture (SBA), which makes heavy use of API protocols. That fact, combined with the integral role of APIs in the explosion of app modernization, creates the need for an API-first application security and delivery strategy to help manage the expanded attack surface as more applications become distributed across clouds and the edge.

02

Respondents Embrace AI-Assisted Business

The need to protect applications, the network, and customer data is among the factors driving telecom providers increasingly to AI, which is being leveraged to better detect, predict, and prevent attacks. Nearly a quarter of telecom respondents are already using AI for application security, and two-thirds are expecting to do so by the end of 2021.

Telecom organizations are also further along than other industries in using AI for operations to manage their global systems and ensure the resiliency of the signaling network. Just over half (51%) of global respondents reported plans to use AI by the close of 2021, compared to 60% of respondents in the telecom industry.

Telecom organizations blaze the way in **AIOps**.

Even more significantly, telecom organizations are increasingly employing AI and machine learning to automate and optimize business processes for greater efficiency. This is the industry's top focus for digital transformation projects, and well over a third of the telecom respondents are using AI for this purpose—a rate 7 points higher than for other organizations globally. In this way, AI and automation are being used to enhance adaptability as well as security.

F5 insight

Telecom organizations that deploy machine learning and AI will be better positioned to protect security and service reliability while taking advantage of innovations and AI-assisted business as the technology evolves.

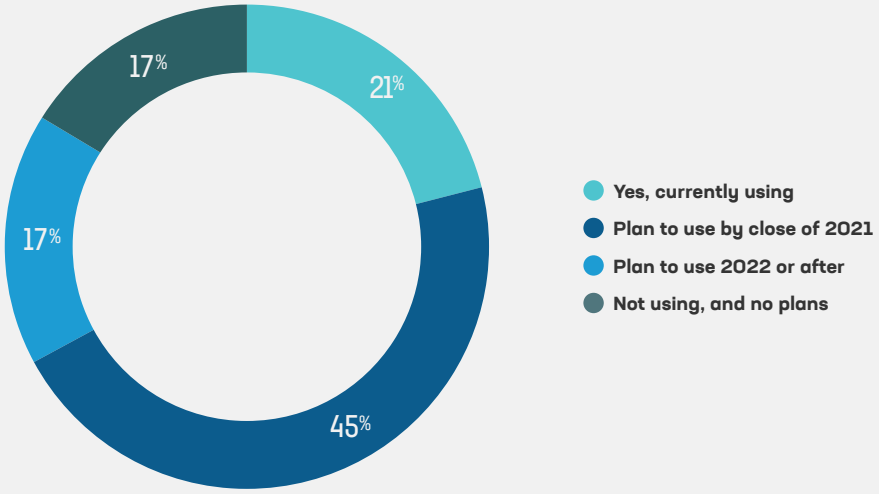
Application Security Through AI

We asked:

Are you using currently using and/or planning to use AI and/or machine learning to protect your applications?

We learned:

Two-thirds of telecom organizations will be using AI or machine learning for security by the end of 2021.



03

Edge Computing Ranks as the Top Trend

While global survey respondents across industries identified Secure Access Service Edge (SASE) and AIOps as the two technology trends they expected to be most strategically important in the next several years, the telecom industry—already well into AI—is looking ahead to edge computing just as much as to SASE. Most acknowledge that having a distributed edge, with network functions such as the core and compute resources close to end users, is becoming critical to achieving the required traffic volumes, speed, and latency reduction.

Accordingly, 88% of telecom respondents are already planning edge deployments, considerably more than the global average. Application performance and the demands of proliferating IoT applications likely drive this interest as the 5G migration proceeds.

Edge computing and SASE ranked equally as telecom's top trend.

What telecom organizations have yet to resolve is how best to secure applications from the core to the edge and from legacy applications into containers and Kubernetes clusters.

F5 insight

In a sense, the edge is just the next step outward in an expanding universe of distributed applications, with benefits—and drawbacks, notably issues of security and compliance—aligned with those of multi-cloud strategies in general. Having the right application security and delivery solutions will be one key to addressing those drawbacks.

Edge Use Cases

We asked:

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

We learned:

Application performance and IoT support are driving telecom interest in the edge.

04

Organizations Have Data but Lack Insights

Cloud deployments are nothing new for telecom providers, who've long led in this aspect of digital transformation, including preparing for 5G with service-based architectures and cloud-native functions (CNFs) across all elements of the network. The global COVID-19 pandemic, and the resulting leap in remote work and digital interactions with customers, only magnified this trend. In fact, telecom providers indicated that the pandemic affected their application deployments even more than for the average global organization, accelerating deployments in on-premises data centers as well as across SaaS and public clouds. As a result, just under 80% of telecom respondents reported use of public cloud deployments, compared to 68% of organizations across all industries.

It's therefore no wonder that, with hundreds and sometimes thousands of apps to support, telecom providers call multi-cloud availability their top purchase criteria for application security and delivery solutions—even more important than cost or speed of implementation. Those solutions and the telemetry from them are considered highly important to meeting service-level agreements (SLAs) related to service reliability, including security, performance, availability, and aligning with business outcomes.

Multi-cloud availability is telecom's top purchase criteria for application security and delivery solutions.

Telemetry by itself is not sufficient, however. Telecom organizations are struggling to turn their data into actionable insights, let alone automate responses to protect application performance. In fact, 96% say they don't have the insights they need, particularly when it comes to predicting, identifying, and responding to attacks. In addition, barely half report having the health monitoring tools they need.

A skills deficit is also a concern for nearly all—98%—of telecom respondents. Sufficient skills to manage a proliferation of toolsets is the top concern expressed by more than a third of telecom organizations, but the know-how to work with APIs is almost equally in demand. In fact, the percentage of telecom organizations reporting

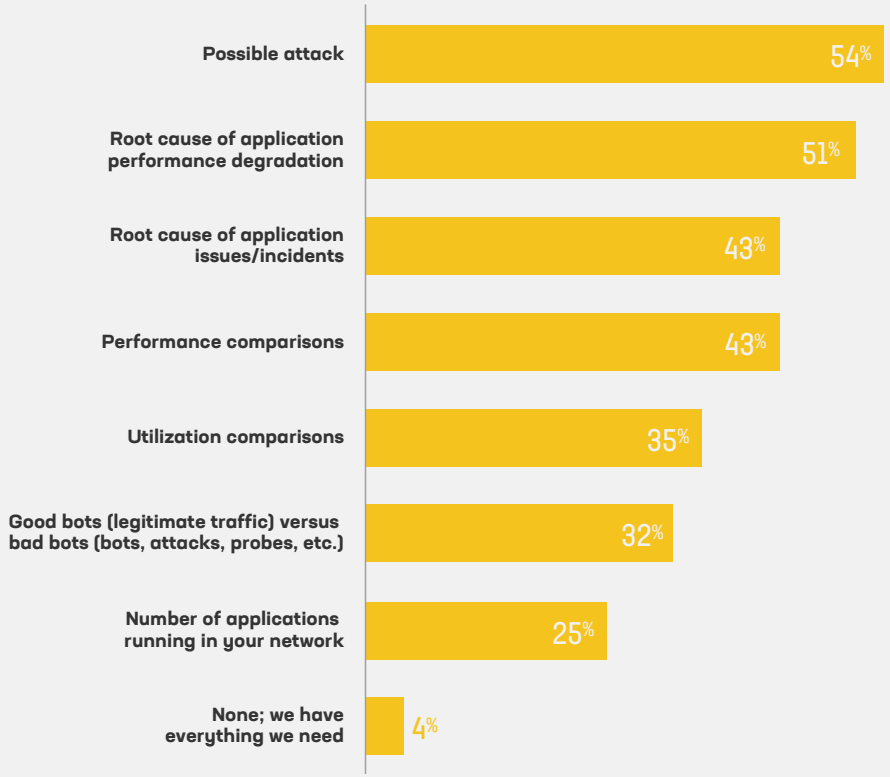
Missing Insights

We asked:

What insights are you missing from your monitoring/reporting/analytics solutions?

We learned:

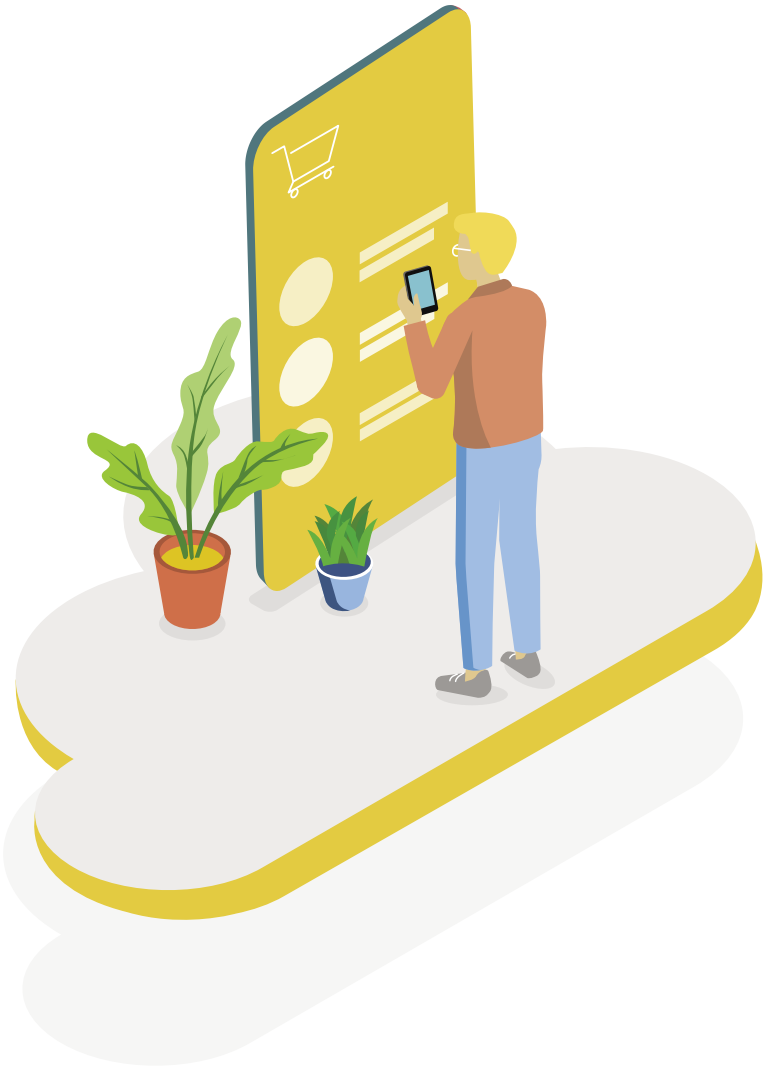
96% of telecom organizations are missing insights they need.



a lack of API skills was almost 10 points higher than for respondents across industries. The complexity of telecom ecosystems, with their proliferation of both applications and vendors, is likely reflected in this result, as is increasing containerization and virtualization intended to enhance portability across the network.

F5 insight

Architectural complexity and application proliferation will only increase, exacerbating existing issues with the availability of tools, skills, and needed insights. That makes multi-cloud application security and delivery technologies more crucial than ever, because without them, other efforts to improve service and QoE can't yield maximum returns to the bottom line.



Conclusion

Protecting the Network Hinges on a Distributed, Multi-Cloud Application Strategy

The telecom industry remains ahead of the curve in digital transformation, modernizing architectures with software-defined networking, increasing portability through containerization, and automating manual tasks to reduce total cost of ownership (TCO). As organizations plan to support a host of new use cases at the edge, the right application security and delivery strategy will help simplify toolsets and required skills. It can also provide the telemetry and actionable insights that can drive AI and enable applications that scale and defend themselves as needed to deliver the QoE that builds revenue. As those applications become increasingly distributed and their data drives more business decisions, an application strategy has become a keystone of any successful telecom business strategy.

About the survey

For this seventh annual survey, F5 heard from 68 individuals with responsibility for making decisions about technology for their telecom organizations. More than a third of these respondents work for large companies with more than 10,000 employees, although a fifth represent companies with fewer than 100 employees, providing balance across organizational size. People from both fixed-line and mobility companies around the globe participated, with the Americas region accounting for the single largest proportion of telecom respondents (48%), followed by responses from Asia Pacific and EMEA. Where this document compares telecom industry results with the overall results of the global survey, the overall results are based on the total responses from more than 1,500 individuals working in decision-making roles for a broad range of organizations of all sizes in the technology, financial services, retail/ distribution, manufacturing, government, education, healthcare, and energy sectors.