



State of Application Strategy Report

2021

XOps Edition



Contents

3	Introduction
5	Section 1: Life in the Trenches of Digital Transformation
8	Section 2: Automation and Orchestration Challenges
11	Section 3: Missing Tools, Missing Insights
13	Section 4: Strong Confidence in Security
15	Conclusion

Introduction

A Digital Leap Toward Our Data-Driven Future

As recounted in the global F5 2021 State of Application Strategy report, digital transformation has leaped ahead in the crucible created by the COVID-19 pandemic. When the lives of people around the globe rapidly became more dependent on digital devices and applications, organizations responded by expanding their digital capabilities, elevating the experiences provided by their applications, and accelerating their movement toward AI-assisted business.



This year, F5's annual survey of IT decision-makers included a look at the opinions and attitudes of IT operational staff—not only DevOps and site reliability engineering (SRE) team members but also those with responsibilities for cloud, network, and security operations. These respondents represent the core (if not exclusive) roles commonly grouped under the term XOps.

As a whole, XOps responses largely tracked with the overall survey results, but the unique XOps perspectives also led to a few interesting variations compared to responses from senior managers and application owners—particularly when it came to organizations' most important challenges, missing tools, and missing insights.

About the survey

In this seventh annual survey, participants were screened for the first time to include only those with decision-making authority or influence on IT purchasing decisions. Final survey results captured information from more than 1,500 decision-makers from around the globe and across a wide range of industries. Roughly a third of respondents identified themselves as holding XOps responsibilities, with this figure relatively balanced across the operational areas of expertise. Respondents in NetOps roles were the most well represented, with DevOps respondents in the smallest group.



01

Life in the Trenches of Digital Transformation

Digital transformation occurs in three distinct phases, starting with task automation and moving into business process automation to serve digital expansion and then AI-assisted business. In the last year, most organizations moved beyond phase 1 and well into phase 2. A majority progressed even further to phase 3 with projects that engage AI in operations and business decisions.



Of course, this progression is probably not news to many XOps team members at work in the trenches. Rapid digital expansion, which is all about using technology to meet challenges and grow the business, likely affected—or comprised—much of their day-to-day work in the past year. They're on the front lines of digital transformation, which is why it's important to understand operational teams' views about their greatest challenges and how they expect their organizations to solve them.

Respondents with operational responsibilities were significantly represented in the total survey population, which ensured general alignment between their answers and the overall survey results. This was especially true for questions that addressed organizational metrics or concerns likely to reflect organizational philosophies or policies.

For instance, when asked whether their organization treated infrastructure as code, XOps respondents validated the answers provided by their colleagues in other roles,

with the same 52% reporting they treated infrastructure as code and 48% saying they didn't. In many cases like this, significant disparities between the answers from senior managers or application owners and operations teams might raise warnings about organizational alignment. Fortunately, such flags generally did not appear.

A few survey questions might be expected to reveal predictable variances between senior management and operations respondents—or between types of operations staff—due to their different roles and daily concerns. For instance, global survey results ranked Secure Access Service Edge (SASE) as the technology trend most likely to be strategically important over the next two to five years, and SecOps and NetOps respondents agreed. However, CloudOps and DevOps/SRE respondents chose SaaS as number one, a reflection of their focus on the most dominant trends influencing application development, deployment, and delivery.

Progress in Digital Transformation

We asked:

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

We learned:

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



Phase 1:
Task Automation

25%

↓ From 45% in 2020



Phase 2:
Digital Expansion

57%

↑ From 37% in 2020



Phase 3:
AI-Assisted Business

56%

↑ From 17% in 2020

Other survey responses, such as those about missing tools, skills, and insights, are more fruitful to explore from the operational viewpoint. In short? While nearly everyone—95% of global respondents and XOps alike—noted they are missing insights they need, some of the biggest gaps between the survey’s global results and those of operations respondents related to operational challenges and missing tools and skills.

40% of XOps respondents ranked multi-cloud availability as a **top-three purchase criteria**.

One variable addressed by the survey that appeared to influence views about what’s missing was the importance of multi-cloud availability when selecting application security and delivery technologies. In the global results, multi-cloud availability jumped five spots from last year as a purchase criteria, now ranking third behind ease of use and total cost. XOps teams placed even more importance on application technologies being available for all environments, with 40% calling it a top-three criteria compared to 38% of all respondents. This should not be surprising, since operations teams may be most impacted by the complexities of modern architectures.

Interestingly, however, XOps respondents who valued multi-cloud availability also expressed somewhat different views about the tools and insights they most lack. Keep reading for these and other details.

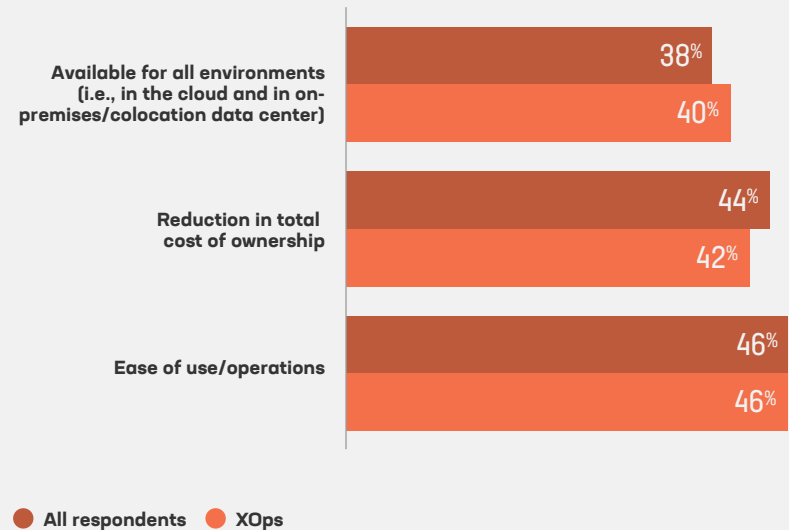
Desired Characteristics of Application Services

We asked:

When evaluating application services, what are the top three characteristics you are looking for?

We learned:

XOps teams are slightly more concerned about multi-cloud availability, and slightly less concerned about cost, than global respondents.



02

Automation and Orchestration Challenges

Two-thirds of XOps respondents noted they were using automation for network and security management. When asked to consider related challenges, XOps respondents agreed with others that their greatest challenge was a lack of skilled professionals to manage automation projects, though they were slightly less concerned about this number-one problem (46% to 47% globally), just as they were slightly less concerned about budgets for automation tools. On the other hand, XOps reported somewhat more concern about toolset integration (43% to 41% globally).



However, XOps respondents who prioritized multi-cloud availability were slightly more likely to report challenges than those who didn't, and they were also more concerned than global respondents about the top three challenges of availability of skilled professionals, toolset integration, and budgets.

Moreover, respondents' precise operational responsibilities affected their answers, not only in terms of how challenged they felt but which specific challenges were the most formidable. As a group, NetOps teams felt these top three automation challenges most keenly, while DevOps teams pointed to political or cultural resistance to change as more of a difficulty for them. Such resistance was also a top problem for CloudOps and other operations respondents. Still, CloudOps respondents were more likely than others to say they had no challenges now (23%). Meanwhile, SecOps respondents called not using automation their single biggest challenge.

NetOps and other operations staff identified the **most skills deficits**.

When considering skills deficits specifically, XOps respondents agreed with global respondents—and were slightly more emphatic—that their single greatest skills deficit for automation and orchestration related to toolsets such as Terraform, Ansible, and GitHub. That is, 42% of XOps respondents reported toolset deficits, compared to 40% globally. Similarly, slightly more XOps respondents than global respondents reported a skills deficit related to working with APIs.

Automation Challenges

We asked:

As you think about the use of automation in the network, what do you find challenging, frustrating, or difficult?

We learned:

Top automation challenges vary significantly by role.



CloudOps
No challenges now



NetOps
Integration of toolsets across vendor/devices



Operations
Budget for new tools



SecOps
Not using automation



SRE/DevOps
Political or cultural resistance to change

Respondents in different operational roles were fairly evenly split when reporting their top skills deficits, with unsurprising variations related to their roles. For instance, CloudOps respondents ranked cloud-provider tools and APIs as their number one skills deficit, while NetOps respondents pointed to languages used for templates and scripts as their biggest skills need. Meanwhile, NetOps and other operations staff were the most likely of the various operations teams to identify skills deficits at all.

Nonetheless, 6% of XOps respondents reported they had no automation and orchestration skills deficit, compared to 8% of total respondents. Finally, as with automation challenges generally, DevOps and SRE respondents were considerably less likely than other operations staff to say they faced a skills deficit.

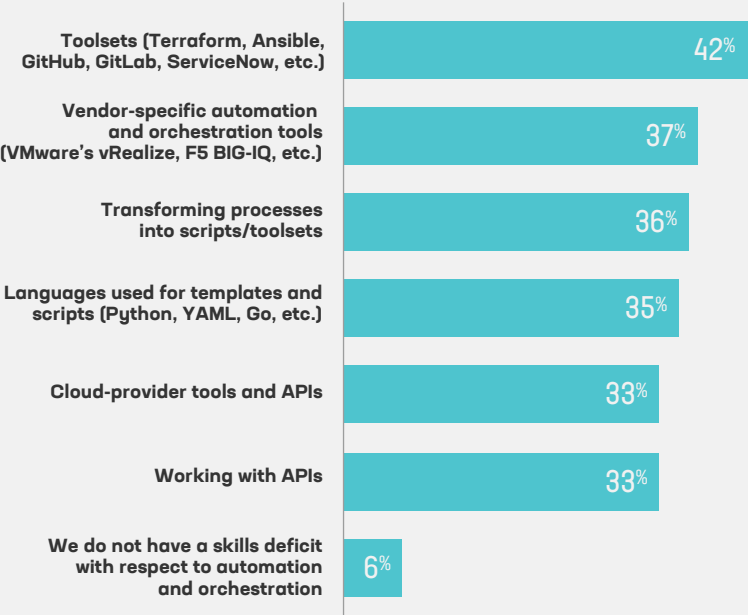
Skills Deficits in Automation

We asked:

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

We learned:

Toolsets represented the biggest skills deficit, but answers varied significantly by operational role, and NetOps and other operations staff identified the most skills deficits.



03

Missing Tools, Missing Insights

As with missing automation and orchestration skills, XOps respondents were slightly more likely than global respondents (44% to 42%) to report they were missing the tools they needed to report on the health of high-priority business applications.



When asked to consider what insights they were missing from their monitoring, reporting, and analytics solutions, XOps respondents mostly agreed with their colleagues in other roles, with 95% reporting missing insights and identifying the root causes of application issues and of application performance degradation as their top two gaps. Perhaps intuitively, given their jobs, XOps respondents were equally concerned about utilization and performance comparisons, while global respondents gave slight priority to performance comparisons.

97% of XOps respondents who valued multi-cloud availability said they were missing insights they needed.

Again, XOps respondents who valued multi-cloud availability felt these gaps more keenly, with 97% saying they were missing insights, compared to 95% overall. The proportion of those indicating they needed insights into the root causes of application incidents, the root causes of performance degradation, and possible attack jumped to 50% or more among those who valued multi-cloud availability, while the proportion of those missing utilization comparisons jumped from 39% to 41%. These results suggest that while multi-cloud availability facilitates the deployment of application security and delivery solutions, the scarcity of truly multi-cloud solutions keeps visibility fractured between different data formats and subject to report data selection biases. That means it's still difficult to obtain needed insights. Meanwhile, most organizations do not yet have a comprehensive strategy to deal with telemetry, which is one of the reasons F5 believes that OpenTelemetry and open access to all metrics may help unlock the value of insights.

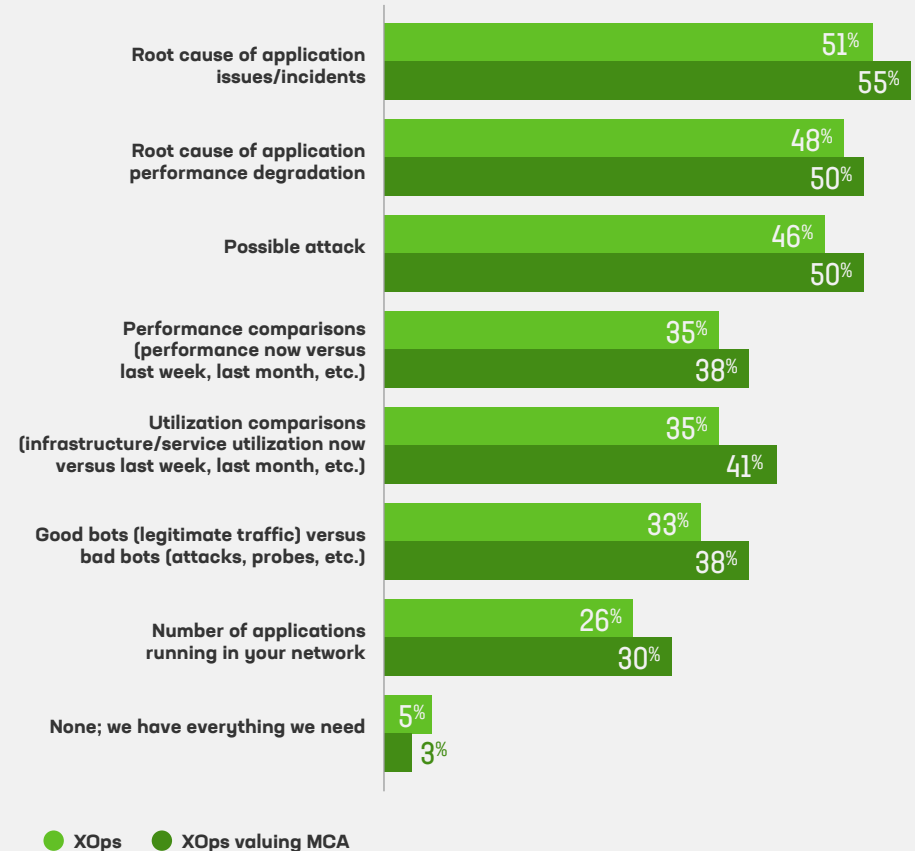
Missing Insights

We asked:

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

We learned:

XOps respondents who value multi-cloud availability are slightly more concerned about missing insights across the board.



04

Strong Confidence in Security

Despite dealing with perceived gaps in skills, tools, and insights, XOps respondents were generally confident in their ability to protect their organizations' applications and APIs. Just as with global respondents, 72% felt confident or very confident about protecting their applications and 65% felt confident or very confident about the security of their APIs. Of course, this means that roughly a third of XOps respondents don't have much confidence in their organization's security posture—an area of concern as organizations move forward amid increasingly sophisticated threats.



Notably, considerably more XOps respondents (and global respondents) think security protection is important than expressed confidence about their current security posture. Specifically, nearly 9 of 10 XOps respondents ranked protecting the infrastructure as important or very important, slightly more than did global respondents. Similarly, three-quarters of those in XOps roles rated protecting the business from fraud and protecting applications as important or very important, again slightly more than did global respondents.

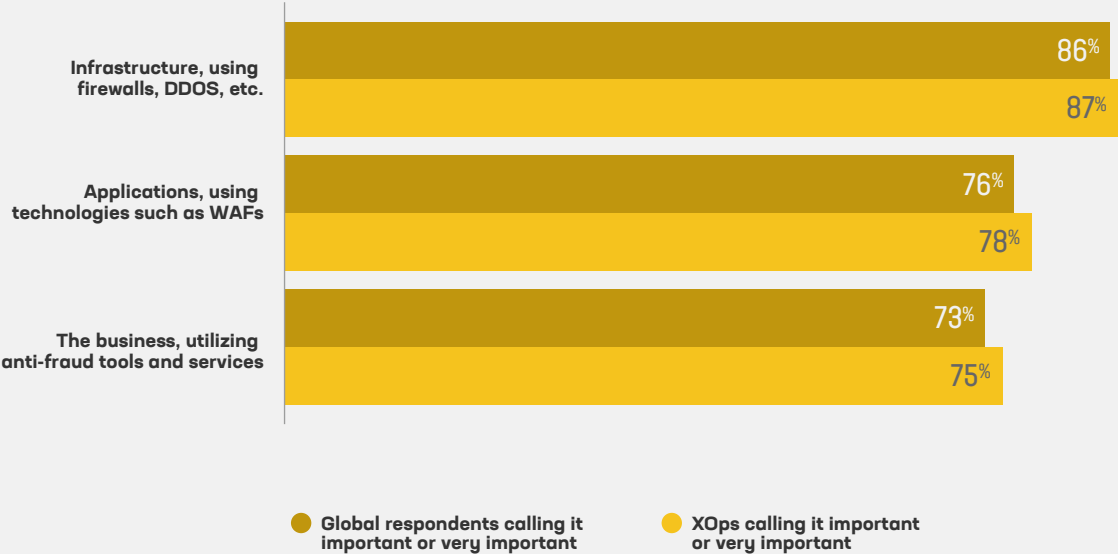
Nearly a third of XOps respondents lack confidence in their firm’s security postures.

This greater valuation of security makes sense, given the specific responsibilities of NetOps, SecOps, and other operational roles. But the gap between security’s acknowledged importance and XOps respondents’ confidence in actual protection is concerning. XOps teams are probably the most familiar with and aware of both the rapid evolution of attack strategies and any gaps in their organizations’ current security practices and tooling. The gap in their confidence suggests organizations could do more now to protect themselves in ways that would build confidence among those most responsible for ensuring that protection.

Importance of Security

We asked:
Please rate the importance of deploying protection technologies for the following categories.

We learned:
XOps place slightly higher priority on security across the board.



Conclusion

Digital transformation has accelerated in the past year and is unlikely to slow back down.

XOps teams in the trenches are the people directly responsible for increased digitization of customer experiences, making those experiences fast and satisfying while managing the infrastructure, development, integration, automation, and AI that will support business growth and success. Most of these teams probably didn't need a global survey to tell them about the increased modernization, increased architectural complexity, or significant challenges prompted by the global pandemic. When considering the state of application strategy today, however, it's useful to reflect on the opinions of those personally developing applications and executing related strategies.

As organizations proceed from automating tasks toward automating entire processes and then deploying AI, it becomes critical to operationalize the functions and processes that enable rapid scaling. That's true whether the needed operationalization makes it faster and easier for DevOps teams to roll out new applications with predictable results, or for SecOps to improve the consistency, reliability, and automation of security management. Scaling applications isn't enough if security, network, and infrastructure don't scale, too, and maintaining compliance with regulatory mandates while driving revenues and growth depends on solving the challenges faced by all operations teams as they arise. An organization

unable to agree on a skills deficit, for example—let alone solve it—will struggle to operationalize all the necessary building blocks for success. Such challenges could become bottlenecks preventing the organization's digital transformation from moving ahead at the pace necessary to remain competitive.

On the other hand, the significant alignment between XOps respondents and other decision-makers revealed by the survey suggests that many organizations are on the right track and need mostly to maintain momentum as they implement AI assistance.

Even organizations doing well, however, need to look ahead. For many, the third phase of transformation will eventually demand additional operational teams, whether they're called AIOps, machine learning or MLOps, or DataOps. The extensive telemetry of AI will require a scientific discipline of its own to convert the resulting volumes of data into insights and actions. That is, after all, where AI can fail—when small projects, however successful, are scaled into production. Without a discipline to harness the upscaled data volumes, digital transformation can screech to a halt. That's why F5 expects both the definition and importance of XOps to expand as organizations plot their digital transformation paths forward into AI assistance and beyond.



©2021 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5. DC0419 | JOB-CODE-615244685