

2022 Cloud-Native Alignment Report

Key Success Factors in the
Transition to Cloud-Native



Report Overview



IT DECISION-MAKER

Responsible for oversight of a business' technology infrastructure



DEVELOPER

Responsible for building software, often report into engineering

Introduction **3**

Key Findings **4**

Open Source Drives Digital Transformation **5**

Unified Focus on Security **10**

Who Owns Security? **15**

Conclusion **16**

INTRODUCTION

Assessing Cloud-Native Alignment

Historically, IT leaders **controlled all infrastructure decisions** across network, storage, compute and more. But as applications continue moving to the cloud, modern developers — who often report into engineering rather than IT teams — **have far more nuanced needs.**

Developers require control of cloud-based tools and infrastructure, as well as the code that runs on them — making the choice of tools and technology **crucial.** And without a unified approach between IT decision-makers and developers on cloud expansion strategy, **the process can be stifled.**

To gauge where organizations stand during this period of rapid digital transformation and cloud migration, we surveyed **350 IT decision-makers** and **350 developers** at organizations that use cloud-native environments as part of their operations.

In this survey, we sought to determine how aligned these groups are in terms of managing digital transformation at their organization. IT decision-maker and developer respondents have **big plans for cloud-native expansion.** However, there were also a few gaps between the two groups in strategy and responsibilities that need to be addressed for effective progress to be achieved.

“Our results show that IT decision-makers and developers have big plans for cloud-native expansion.”



Key Findings



Cloud-native and open source are booming

97% of IT decision-makers and 96% of developers said their organizations plan on expanding use of cloud-native and open-source tools over the next 12 months.

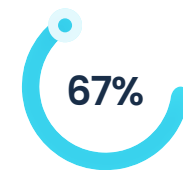


IT decision-makers plan to boost data privacy efforts

77% of IT decision-makers said their organizations are focused on enhancing data privacy security measures over the next 12 months.

Developers think more should be done for legacy application migration

67% of developers think their organizations should prioritize migrating legacy applications to the cloud in the next 12 months.



Confidence in cloud-based security is extremely high

97% of IT decision-makers and 97% of developers rated their organizations' ability to manage security for cloud-based applications as strong.



INSIGHT 1

Open Source Drives Digital Transformation

Developers and IT decision-makers plan to increase adoption of open-source solutions in the transition to cloud-native architecture



The Journey Toward Digital Transformation

Based on responses from IT decision-makers and developers, it's clear that cloud-native and open-source technologies are no longer experimental — they're the new standard.

The overwhelming majority of IT decision-makers (97%) and developers (96%) said their organization plans on expanding its use of cloud-native and open-source tools over the next 12 months. Additionally, IT decision-makers appear to be focused on the employee responsibilities for this expansion, while developers are more focused on changes involving the rollout of new technologies.

Cloud-native and open-source technologies are no longer experimental — they're the new standard.

IT DECISION-MAKER



97% of IT decision-makers said their organization plans on expanding its use of cloud-native and open-source tools over the next 12 months.



DEVELOPER



96% of developers said their organization plans on expanding its use of cloud-native and open-source tools over the next 12 months.

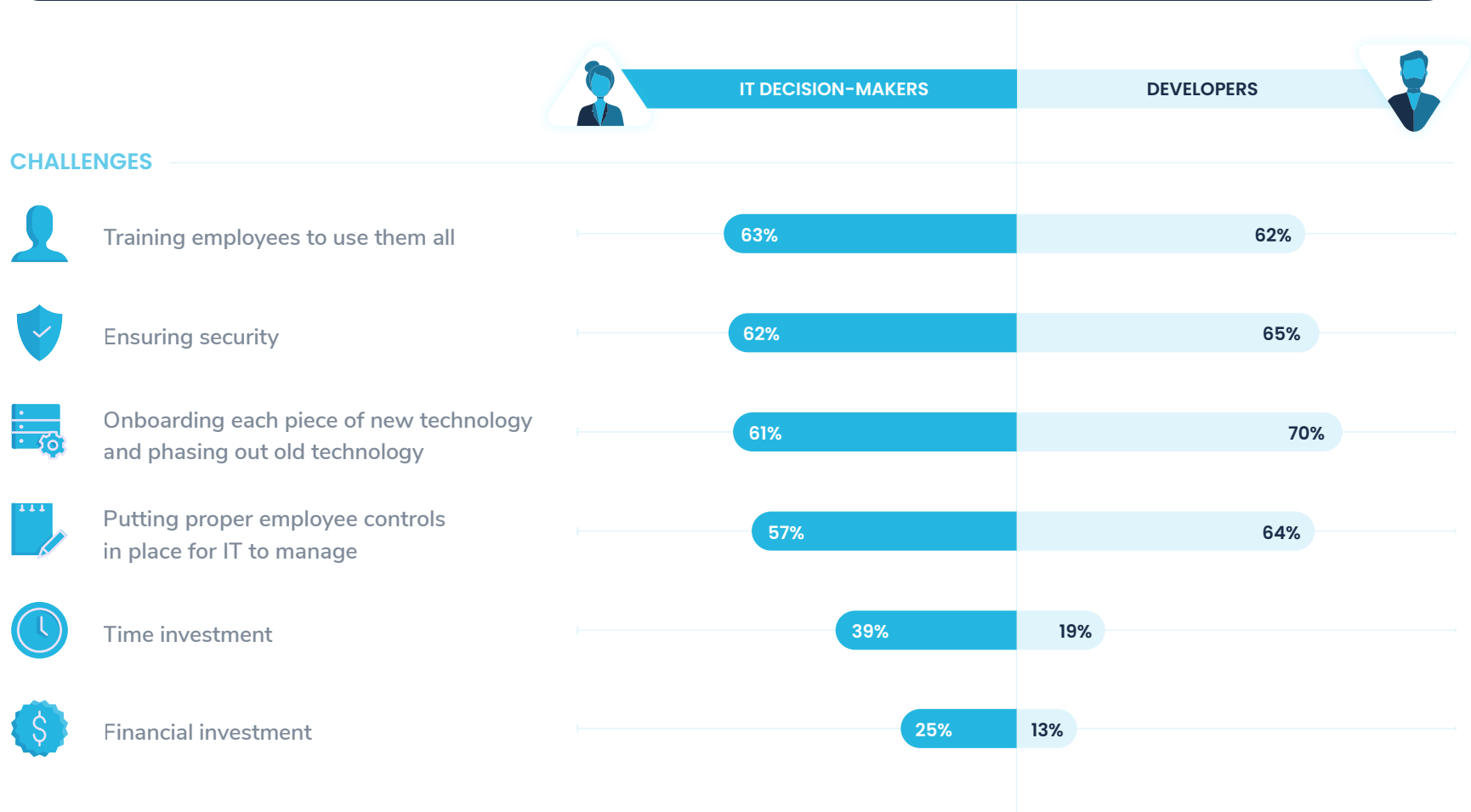


= 2%

FIGURE 1

The Expansion Challenges That Lie Ahead

What are the biggest challenges your organization faces in expanding its use of cloud-native and open-source tools over the next 12 months?



Each group differed in the challenges they anticipate for cloud-native and open-source expansion. IT decision-makers said training employees to use cloud-native and open-source tools was their biggest anticipated challenge, while developers noted onboarding each piece of new technology and phasing out old technology as their biggest challenge (Figure 1).

Tension can mount between IT decision-makers and developers over the implementation of new tools. According to respondents, developers typically want to launch offerings as quickly as possible, while IT decision-makers are cautious because they are responsible for a successful organizational rollout.

Although developers are in the thick of micro-level tech changes in the cloud with onboarding and installing employee controls, they should also be mindful of the macro-level personnel and training initiatives IT decision-makers are navigating. Each group's role is vital for cloud-native and open-source technology expansion and ultimately doesn't work effectively without unified efforts.

For example, alignment in cloud-native and open-source expansion is especially important for organizations that historically take longer to adopt new technology. In 2022, many of these enterprises will be implementing lift-and-shift styles of cloud migration to move on-prem technologies to the cloud.



“Each group’s role is vital for cloud-native and open-source technology expansion and ultimately doesn’t work effectively without unified efforts.”

TAKEAWAY

Getting On the Same Page

Developers and IT decision-makers need to keep communication open as each group navigates their respective responsibilities in these endeavors. For instance, identity and access management (IAM) and developers need to ensure proper entitlements are in place for formerly on-prem systems now migrating to cloud. Additionally, application developers need to understand and define control traffic flow to, from and between microservices with fine-grained authorization policy and enterprise-grade service mesh. And IT decision-makers need to ensure employees know how to properly access former on-prem tools in the cloud.

Developers should be mindful of what they can do to help with employee adoption and IT decision-makers should understand the steps developers must take for successful lift and shift. The more developers and IT decision-makers can stay in lockstep during this process, the smoother the transition will ultimately be.



“The more developers and IT decision-makers can stay in lockstep during this process, the smoother the transition will ultimately be.”

INSIGHT 2

Unified Focus on Security

Security is expanding beyond IT
decision-makers to developers



A New Shared Philosophy

Cyberattacks have risen since the start of the COVID-19 pandemic, with responsibility for mitigation often falling on the shoulders of chief information security officers (CISOs) and chief information officers (CIOs). **This could indicate why IT decision-makers surveyed were focused on data privacy security measures.**

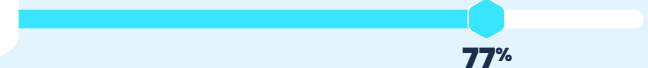
More than three-quarters of IT decision-makers (77%) said their organizations are focused on enhancing data privacy security measures over the next 12 months. And while developers thought their organizations should place the greatest priority on cloud application initiatives, 51% also believed their companies should enhance data privacy security measures [\(Figure 2\)](#).

Security is no longer solely a focus for IT decision-makers, it has become a higher priority for developers.

IT DECISION-MAKER



DEVELOPER



77%

77% of IT decision-makers said their organizations are focused on enhancing data privacy security measures over the next 12 months.



51%

51% of developers said their organizations should focus on enhancing data privacy security measures over the next 12 months.

FIGURE 2

Priority Perspectives

IT DECISION-MAKERS

Which of the following initiatives is your organization prioritizing in the next 12 months?

DEVELOPERS

Which of the following initiatives do you think your organization should prioritize in the next 12 months?

CHALLENGES



Enhancing data privacy security measures

77%

51%



Migrating legacy applications to the cloud

59%

67%



Building a proof-of-concept application in the cloud

57%

65%



Building production, customer-facing cloud applications

56%

66%



Strengthening DevOps (i.e., adopting DevOps best practices)

56%

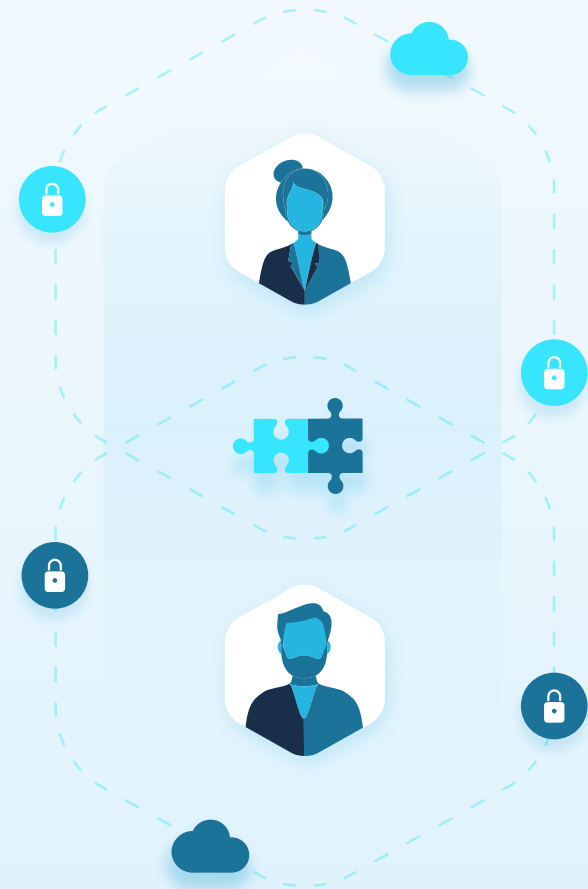
33%

TAKEAWAY

Increased Collaboration Through a Unified Focus

Developers' strong feelings about security mark a major shift in mindset. The rise of [new compliance regulations](#) and more complex internal authorization policies could be responsible for the rise in security concerns among developers as they develop applications for the cloud. With a greater focus on security from both IT decision-makers and developers, there's an opportunity for greater collaboration between the two groups through shared purpose.

In taking advantage of this shared purpose for security, IT decision-makers and developers must approach it the right way for a cloud-native environment. Cloud-native enables greater speed and flexibility across an organization's network. But to optimize the use of its tools, security can't be managed with manual processes. Instead, IT leaders need to equip their developers with solutions that automate manual security checks so time and resources don't go to waste for cloud production.



“With a greater focus on security from both IT decision-makers and developers, there’s an opportunity for greater collaboration between the two groups through shared purpose.”

INSIGHT 3

Who Owns Security?

IT decision-makers and developers believe cloud security is strong at their organizations, but aren't clear about which team owns it



The Potential Consequences of Not Knowing Who Does What

The overwhelming majority of both IT decision-makers and developers indicated a high level of confidence in their security capabilities: Ninety-seven percent of IT decision-makers and 96% of developers rated their organizations' ability to manage security for cloud-based applications as strong. Additionally, 99% of IT decision-makers and 97% of developers indicated they were confident that their organizations' existing security tools and technology will extend to protect their cloud environments.

Although both groups of respondents were virtually unified in their positive outlook on their organizations' cloud security capabilities, IT decision-makers and developers were not aligned on which teams within their organizations manage various policy, compliance and cloud security responsibilities.

IT decision-makers and developers may be overly confident in their cloud security processes.

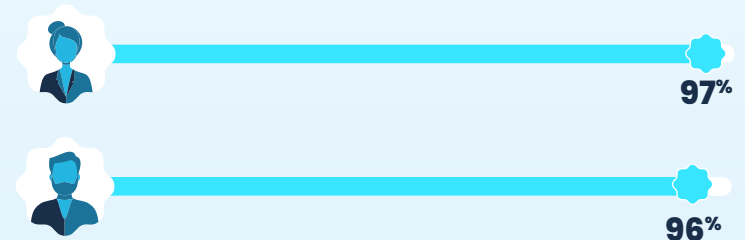
IT DECISION-MAKER



DEVELOPER



Percent that rated their organizations' ability to manage security for cloud-based applications as strong.



Percent that are confident that their organizations' existing security tools and technology will extend to protect their cloud environments.

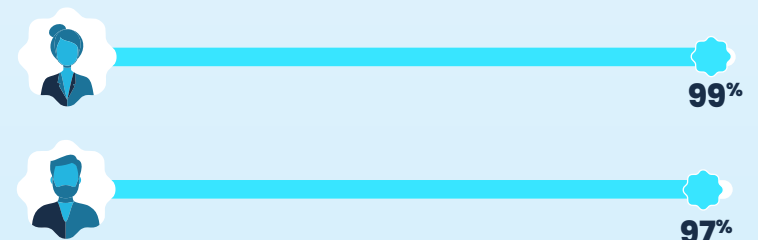


FIGURE 3

*Answers of "Not Sure" are not shown due to low respondent volume

Misaligned Perspectives

Which group within your organization takes on the majority of the role for the following tasks?

IT DECISION-MAKERS

DEVELOPERS

	DevOps Team	Software Engineering Team	Security Team	IT Infrastructure/Operations Team
Defining the policies that control how cloud applications are secured and managed	17%	14%	24%	45%
	31%	24%	23%	23%
Proving that applications are compliant with internal policies (legal, IT governance, etc.)	15%	17%	27%	41%
	13%	38%	27%	22%
Meeting with, and proving compliance to, external compliance auditors (PCI, HIPAA, GDPR, etc.)	19%	20%	25%	35%
	14%	22%	42%	21%
Provisioning new users into cloud infrastructure	16%	25%	21%	37%
	13%	28%	23%	34%
Deploying workloads into the cloud (e.g., which group owns the CI/CD pipeline)	23%	24%	14%	39%
	16%	27%	30%	24%
Managing your Git and provisions Github accounts	17%	22%	24%	34%
	16%	32%	30%	21%

Most IT decision-makers indicated their IT infrastructure/operations teams managed all six policy, compliance and cloud security responsibilities outlined in the survey (Figure 3). Conversely, most developers indicated a scattered sharing of the listed responsibilities across various teams and were only in alignment with IT decision-makers on IT infrastructure/operations teams provisioning new users into cloud infrastructure (Figure 3).

This misalignment between IT decision-makers and developers on policy, compliance and cloud security responsibilities can lead to wasted time and resources on redundant work being done by multiple departments. In addition, not fully understanding which departments handle certain roles can cause tasks and responsibilities to be missed entirely, which ultimately creates insecure, vulnerable cloud environments.

Misalignment between IT decision-makers and developers can equate to wasted spend, missed assignments and an insecure cloud.



“This misalignment between IT decision-makers and developers can lead to wasted time and resources on redundant work being done by multiple departments.”

Even when working with cloud providers, there is a division of responsibility for security between the likes of Amazon Web Services, Microsoft Azure or Google Cloud and an organization. As organizations move forward with complex cloud-native implementations, a critical way they can clear up ambiguity among team groups is by implementing policy-as-code for security. Policy-as-code tools like [Open Policy Agent](#) (OPA) and a unified control plane such as [Styra Declarative Authorization Service](#) (DAS) enable developers to codify security and operational policies directly into tech infrastructure, helping reduce errors and close security gaps in cloud-native application development.

As a result, these tools encourage collaboration between IT decision-makers and developers. IT decision-makers can communicate which security and compliance policy guardrails (both internal and external) need to be accounted for within an organization's tech stack. In turn, developers can code in the policies early and measure their impact before deploying across the entire tech stack, ensuring all policies and security responsibilities are covered before a new app is introduced.



“As organizations move forward with complex cloud-native implementations, a critical way they can clear up ambiguity among team groups is by implementing policy-as-code for security.”

TAKEAWAY

Control of Cloud Security Equals Effective Cloud-Native Expansion

Before organizations can truly believe in the security of their cloud environments, IT decision-makers and developers need to understand the exact division of responsibilities. Because without control of cloud security, proper cloud-native expansion can't be achieved. And with the help of the right policy tools, these two groups can ensure everyone is on the same page about departmental responsibilities — and feel truly confident the cloud is protected.



“...with the help of the right policy tools, these two groups can ensure everyone is on the same page about departmental responsibilities.”

CONCLUSION

Learn From Your Fellow IT Decision-Makers and Developers

As organizations continue investing in more cloud-native and open-source technology, it's critical that IT decision-makers and developers are unified in their endeavors. CIOs and CISOs can help ensure they're aligned in cloud-native expansion while keeping up with compliance and internal policies by investing and leveraging open source and commercial policy-based solutions.

A tool like [Open Policy Agent](#) (OPA) and an OPA control plane solution like [Styra DAS](#) can help streamline cloud expansion efforts, make cloud security easier to understand and enable collaboration between your IT decision-makers and developers. And by having a unified team of leadership and development teams, you can ensure digital transformation reaches its full potential now and is set up for even greater capabilities in the future.

Styra invented authorization for cloud-native applications. If you're ready to uplevel security in your cloud-native environment, [request a custom demo](#) to see how we can help accelerate development at your organization.

"... by having a unified team of leadership and development teams, you can ensure digital transformation reaches its full potential..."

Methodology

Styra surveyed 350 IT decision-makers and 350 developers from the United States in late September and early October 2021. IT decision-maker respondents worked in the IT department at the manager level up to the C-suite and were directly involved in helping their organizations with cloud planning and implementing new technology, including buying/selecting new tools. Developer respondents were part of the IT or engineering department at their organizations, worked in engineer, programmer or developer roles and developed software as part of their jobs. In addition, all respondents worked at companies that leverage a cloud-native environment for part of their operations.

About Styra

Styra enables enterprises to define, enforce and monitor policy across their cloud-native environments. With a combination of open source (Open Policy Agent) and commercial products (Declarative Authorization Service), Styra provides security, operations and compliance guardrails to protect applications, as well as the infrastructure they run on. Styra policy-as-code approach lets developers, DevOps, and security teams mitigate risks, reduce human error and accelerate application development. Learn more at [Styra](#).