



The bridge to possible



2022 Global Hybrid Cloud Trends Report

How cloud-based technologies are impacting enterprise infrastructure, operations, and strategies.



Table of contents

Executive summary	2
About this report	2
Key findings	3
Hybrid Cloud is the new normal	4
Top customer challenges	6
Building cloud-ready: DevOps and CloudOps perspectives	9
Cloud-smart operations require new technologies	12
Accelerating cloud-native	13
Conclusion	17
Methodology	18

About Secure Agility

Ever feel like technology is expected to solve almost every question in your organisation? Welcome to Secure Agility, where we provide the answers and then deliver the solutions. Secure Agility is a specialist IT, cloud and managed services provider to Enterprise and Government. Secure Agility delivers enterprise technology expertise in cloud, network and security, IoT and workplace modernisation solutions. We enable customers to drive business growth and efficiency by adopting cloud services that deliver secure, optimised, innovative and cost effective outcomes. The answers, for when IT gets asked all the questions.





The bridge to possible



Executive summary

Hybrid cloud models that incorporate both on-premises infrastructure and cloud-based resources have become the enterprise norm, according to our global survey. The vast majority (92%) of the organizations we polled are using multiple public clouds, not only to leverage the unique strengths of those offerings, but also to improve operational agility, security, application performance, and business resiliency.

The respondents of our survey are acutely aware of the challenges hybrid cloud models create, and they are adapting in a variety of ways. Many cited cooperation

among NetOps, CloudOps, and DevOps teams as a key to overcoming technological and operational challenges. Modernizing infrastructure, refactoring applications, and enhancing operations with AIOps and automation were also seen as essential enablers of hybrid cloud success.

Respondents see value in cooperation between networking, cloud operations, and DevOps teams. The transition to cloud-native and hybrid cloud is driving DevOps teams to adopt hybrid optimized infrastructures to strike a middle ground between existing and new applications.

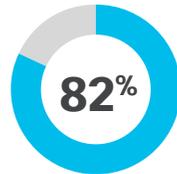
About this report

This report examines the latest trends surrounding hybrid cloud adoption, the impact on enterprise infrastructure and operations, and the strategies being utilized to achieve better technology and business outcomes. Unless otherwise noted, the insights and data in this report stem from a global survey conducted by 451 Research, part of S&P Global

Market Intelligence, on behalf of Cisco, which polled 2500 IT decision makers in 13 countries. Respondents included cloud computing, DevOps, and enterprise networking professionals from organizations that are advanced users of cloud technologies. (See the [Methodology section](#) for further details.)

Key findings

Hybrid cloud and multicloud are the norm.



82% of survey respondents have adopted hybrid cloud.



92% of organizations use more than two public cloud providers.



8% of organizations use a single public cloud provider.



Security and complexity are the biggest challenges.

- 37% of respondents say security is a significant challenge when deploying hybrid cloud.
- Increased operational complexity and cost management were also cited as prominent challenges (33%), followed by compliance and privacy (31%).



Collaboration is required for success.

- 55% of respondents have created a cross-functional team with technical and business representation.
- 50% of respondents have a centralized CloudOps and NetOps function to help ensure their organization's hybrid cloud strategy meets business objectives.
- Respondents said greater collaboration between networking and cloud operations teams helps improve cloud security (45%) and operational efficiency (41%).



Developers are embracing hybrid cloud and Infrastructure as Code (IaC).

- 53% of organizations are moving workloads between on-premises and cloud environments weekly.
- 58% are adopting Infrastructure as Code (IaC), and 44% are deploying cloud-native technologies to improve their security posture.



Hybrid cloud is driving the adoption of emerging technologies.

- A significant percentage of respondents are deploying AIOps (45%), infrastructure automation (41%), and edge computing (41%).
- 79% of respondents say more than half of their workloads will run on different hardware across all environments, reinforcing the need for a comprehensive toolset for managing workloads.



Cloud-native is accelerating.

- 91% of respondents in DevOps and CloudOps roles say their organization has or will refactor applications using cloud-native technology.
- 47% of CloudOps and DevOps respondents say a "cloud first" mandate is the tipping point for changing development processes and tools.



Hybrid Cloud is the new normal

Most organizations around the world now use multiple clouds to support myriad applications and deliver improvements in business agility and scalability. In our global survey, 82% of respondents said they currently use cloud-based Infrastructure as a Service (IaaS) to host their workloads. This hybrid approach enables their organization to achieve a more agile and scalable development

environment (42%) and accelerate business agility and innovation (40%). In addition, as organizations consider the best venue for their workloads today and in the future, the use of multiple clouds has become a popular approach that allows organizations to select the best environment for their workloads, considering factors such as regional compliance, security, and performance.

Figure 1. Hybrid cloud models are being used to support a myriad of workloads



Q. Which of the following workloads or processes do you currently run in a hybrid IT environment?

Base: All respondents (N = 2,577)

Source: Cisco 2022 Global Hybrid Cloud Trends Report

Only 8% of surveyed organizations use a single public IaaS cloud provider.

Most surveyed organizations (58%) use 2–3 public IaaS cloud providers for their workloads, with 31% of respondents using 4–10 public cloud providers. The organizations that use more than three cloud providers make use of alternative cloud providers outside of AWS, Azure, and Google Cloud, which may include pure-play public cloud providers or cloud services

offered as part of a broader portfolio (for example, telcos). The survey indicated organizations with 5000+ employees are slightly more likely (8% of respondents) than smaller organizations (5%) to have more than 10 public cloud providers in use, since large organizations have more line-of-business requirements that can drive usage across platforms and outside the view of IT.

Figure 2. Why organizations are using multiple clouds



Q. What are the most significant motivations for your organization to use multiple (public and private) clouds for all services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and SaaS?

Base: All respondents (N = 2,577)

Source: Cisco 2022 Global Hybrid Cloud Trends Report

Bottom line: Models that combine on-premises and cloud-based resources have become the norm. The vast majority of companies utilize multiple clouds to manage security, enhance application development, and improve business agility, and they choose the best venue for each workload.

Interestingly, there were only small variations across geographies in most areas of the study. That speaks to a common set of experiences of those who are operating hybrid cloud environments. They are a select group that is dealing with issues that are common around the globe.

When it comes to SaaS, organizations are stretched across even more providers, with 23% of respondents reportedly using 20–100 different SaaS providers for their

business, across categories such as email, collaboration and video calling, customer relationship management (CRM), and human capital management (HCM). Nearly half of respondents (45%) in the survey have 5–10 SaaS vendors in use. Many SaaS applications address a specific business or IT need and require organizations to spread usage across numerous vendors.



Top customer challenges

The road to hybrid cloud and multicloud use is not without its challenges, and security stands above the rest as the greatest challenge that survey respondents face in using multiple clouds. As noted earlier, security is also the top reason that survey respondents use multiple clouds (37%), as they look to balance security with the needs of performance and scale (42%), while one-third of respondents face challenges related to operational complexity (33%) and managing costs (33%) in these environments. Survey respondents employ various strategies to overcome these roadblocks and demonstrate a strong appetite for implementing new technologies to help them do so.



Challenge No. 1: Security

Regardless of where an organization is in its journey toward multicloud use, security remains a critical challenge as threats are constantly changing, and technology and processes need to adapt. It is important to keep in mind that security encompasses many aspects of hybrid operations. Operational security concerns are common to any expanding environment. Hybrid approaches allow organizations to implement one of security's most fundamental controls, segmentation, as well as isolation, which allows them to use different clouds for different use cases.

One factor in the maturing of cloud operations is managing risk by being selective about where workloads and data are placed. Hybrid environments can give security teams options that allow them to balance placement, putting some workloads

in public clouds while keeping others on-prem, or using different regions for data residency requirements. While that is an advantage, it is one that has risk elements of its own in terms of the additional complexity caused by operating in multiple, dissimilar realms. Each cloud environment can have its own operational model and management environment. Without a common framework to manage them, security teams need to develop fluency in each new cloud – a significant investment in time and resources.

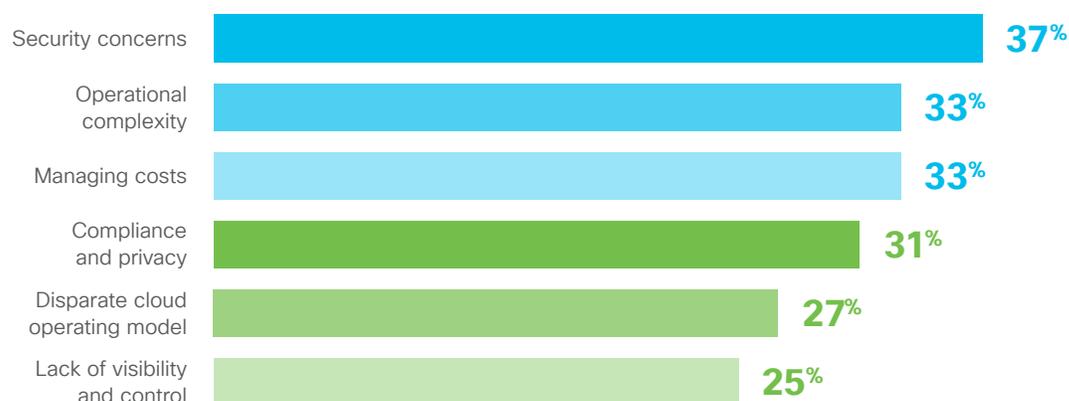
Security can be even more difficult to handle when you consider how often applications move from one environment to another – more than half of total survey respondents say they move applications between on-premises and off-premises environments weekly. In addition to segmenting workloads between on-premises and different public clouds, enterprises are looking at all options to improve their security posture. This includes using cloud-native technologies (44% of respondents) and using infrastructure as code (58%). In addition to managing the security of the overall environment, securing APIs across multiple clouds is a significant challenge for 32% of respondents.

Enterprises are looking at all options to improve their security posture, including using cloud-native technologies...

This is an area where automation and abstraction can deliver the best of hybrid cloud’s promise for security while overcoming complexity-related challenges. If security teams can implement tools that let them use a common framework for security management across multiple clouds, they can mitigate the largest risks

of misconfiguration and operational mistakes, while ensuring that guardrails are in place to get the right workloads deployed in the proper environments. The abstractions that capable management platforms offer can be force multipliers for security teams that are already overtaxed by hybrid complexity.

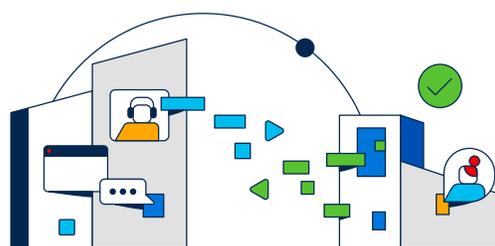
Figure 3. The top operational challenges when utilizing multiple clouds



Q. What are the most significant challenges your organization faces or would face using multiple clouds?

Base: All respondents (N = 2,577)

Source: Cisco 2022 Global Hybrid Cloud Trends Report



Challenge No. 2: Operational Complexity

Despite the proliferation of tools designed to simplify the management of cloud environments, 33% of responding organizations said operational complexity is a significant concern when adopting hybrid or multicloud models. Hybrid environments not only mean that organizations must

manage disparate cloud environments, but also different hardware. Many survey respondents (79%) tell us more than half of their workloads will run on different hardware across all environments, which reinforces the need for a comprehensive toolset for managing workloads regardless of where they reside. For instance, the majority of survey respondents use a cloud-based IT operations platform delivered as a service (94%), which can help an organization quantify operational complexity, provide full lifecycle management, and offer proactive support of on-premises infrastructure – all key capabilities identified by respondents as top criteria in selecting a cloud-based ITOps platform.

The majority of survey respondents (94%) use a cloud-based IT operations platform delivered as a service.

Concerns about visibility into more complex infrastructure have placed a focus on management support that can span multicloud environments. To ensure they

meet their business objectives, a SaaS-based operations platform is the leading choice (60%) for respondents.



Challenge No. 3: Managing Costs

Managing cloud costs can be challenging; however, most organizations' use of multicloud is not driven by the expectation that this approach will help reduce cloud-services costs (66% of respondents). Rather, more than half of respondents (56%) use a cost/benefit approach to justify and load balance cloud-service purchasing.

Cost optimization is one measurement of multicloud success, but saving money is not a guarantee in the cloud. Managing multiple disparate clouds increases complexity, which can inflate operating costs. As understanding of cloud's value matures, expectations are shifting from cost reduction to cost management to enable greater agility and scale, two of the top motivations for multicloud adoption.

To be effective, efforts to manage costs should be in the context of achieving desired business outcomes. Organizations have employed a variety of approaches to improve operational and cost efficiency. According to our survey, establishing a cloud Center of Excellence (57%), adopting a cost/benefit approach or AIOps model (53%), and centralizing CloudOps and NetOps functions (50%) are the most popular.

Bottom line: The use of multiple clouds in hybrid cloud environments increases the challenges related to security, operational complexity, and cost management. Most organizations are adopting SaaS operations platforms, infrastructure as code, and an AIOps operating model to address these challenges. They are also implementing a cloud Center of Excellence and centralizing CloudOps and NetOps functions.

Figure 4. The strategies being employed to ensure desired business outcomes



Q. Which of the following strategies have you adopted to ensure your cloud strategy successfully meets your business objectives?

Base: All respondents (N = 2,577)

Source: Cisco 2022 Global Hybrid Cloud Trends Report



Building cloud-ready: DevOps and CloudOps perspectives

Developers have become more influential in defining an organization’s cloud strategy, and they frequently play a key role in selection of cloud platforms and services that support application development and infrastructure modernization. Survey respondents in cloud operations and DevOps roles indicate that a cloud-first mandate for all new application development (34%) is the tipping point toward changing development processes and tools at their organization, while cost optimization (19%) and automation (18%) are contributing factors. This is another indication of the maturing expectations around cloud environments as organizations expect operational capabilities to be part of their multicloud journey.

A cloud-first mandate may be applied to net-new applications because most businesses are dealing with legacy applications that require a different approach to transformation. The vast majority (91%) of CloudOps and DevOps respondents say their organization has or will refactor applications using cloud-native technology. Their approach to mission-critical and legacy applications moving forward is to modernize in place (38%) or refactor and shift (25%), leveraging cloud-native technologies to support this transition. Our survey respondents are bullish on transformation, with only 8% planning to retain mission-critical workloads as they are.

The importance of cloud-ready networks

Regardless of where an organization decides to run a particular application, networking is a critical capability that ensures applications function and perform properly, and developers consider their involvement in determining networking priorities as non-negotiable. The majority of developers either agree or strongly agree (92%) that having a seat at the table in determining their organizations’ networking strategy and priorities is important. The importance of networking is reinforced by the frequency with which survey respondents move workloads between off-premises and on-premises environments – 53% move workloads and/or applications between these venues weekly, while 39% do so monthly.

Organizations we surveyed are generally optimistic and open-minded about working with collaborators outside of their core team to ensure that hybrid cloud environments are secure, while delivering efficiency and performance. Respondents see value in cooperation between NetOps, CloudOps, and DevOps teams.

91% of CloudOps and DevOps respondents say their organization has or will refactor applications using cloud-native technology.

Survey respondents agree that greater collaboration between NetOps and CloudOps teams has numerous benefits, with improved cloud security (45%) at the top of the list...

Developing a culture of collaboration

Survey respondents agree that greater collaboration between NetOps and CloudOps teams has numerous benefits, with improved cloud security (45%) at the top of the list, followed by greater operational efficiency overall (41%) and enhanced cloud application performance (39%).

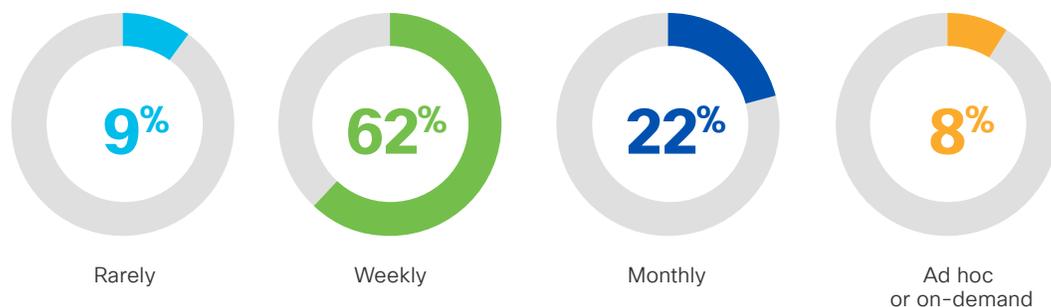
More than half of respondents (55%) have created a cross-functional team with technical and business representation, while 50% of respondents have a centralized CloudOps and NetOps function to help ensure their organization’s hybrid cloud strategy meets business objectives. Respondents in North America are slightly more likely to have this function in place (58%) than organizations in APAC (48%).

Meanwhile, networking professionals also view this relationship as critical: 57% of respondents in networking roles strongly agree that it is important for their DevOps team to be involved in developing their organization’s network strategy. In fact, most developers indicate they already have a process in place to collaborate with networking teams, with 84% of DevOps respondents having a regular cadence of meetings with this team – either weekly (62%) or monthly (22%).

Although most survey respondents feel their current level of collaboration between DevOps and networking teams is sufficient (83%), there are roadblocks that prevent even more cooperation. Competing priorities between teams (45%), resistance to change (43%), and different objectives and incentives (41%) are all factors that prevent more



Figure 5. Collaboration between NetOps and DevOps teams is frequent



Q. How often do you collaborate with your network operations team.

Base: Respondents in DevOps roles (N = 647)

Source: Cisco 2022 Global Hybrid Cloud Trends Report



48% of developers note that network reliability is one of the most pressing challenges they encounter.

effective collaboration between DevOps and networking teams. Speaking the same language around how networking can drive faster and more effective development and identifying common business goals could go a long way in bringing these teams together. It is evident that while collaboration is happening at some level, there is still room to improve outcomes that address developers' concerns around networking.

want more visibility into networking issues, and 41% of developers tell us that accessing root-cause analysis is a key challenge they face, along with lack of common tools, platforms, and interfaces. More productive collaboration would help developers better understand networking priorities while ensuring that application requirements and business needs are considered as part of the overall networking strategy.

In our survey, 48% of developers note that network reliability is one of the most pressing challenges they encounter. DevOps teams



Bottom Line: Coordination between NetOps, CloudOps, and DevOps functions is essential for hybrid cloud success. It reinforces the need for centralized platforms that provide visibility, orchestration, and automation across teams, tools, and environments.



Cloud-smart operations require new technologies

The respondents to our survey show keen interest in a range of leading-edge technologies that can benefit from hybrid architectures, including deployment of infrastructure automation (49%), edge computing (41%), and composable infrastructure (27%).

Some form of edge computing capability is already deployed by 41% of survey respondents, while an additional 53% expect to deploy edge in the next two years. It is a technology that has broad applications, and hybrid approaches to edge computing can ensure that the right level of capacity is in the right place to optimize application performance and customer experience. Organizations that use 10 or more IaaS cloud platforms were more likely to be further along (57% already in deployment) in edge computing.

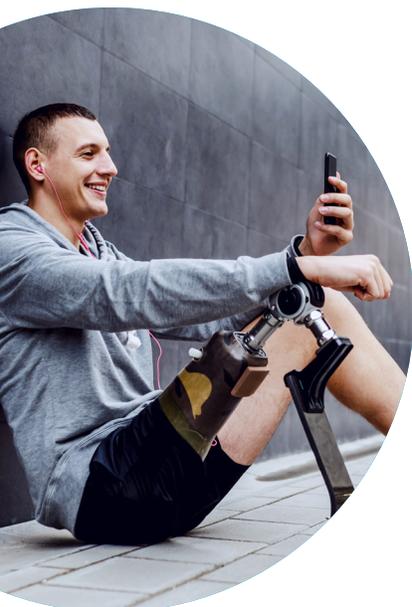
Infrastructure automation is critical to operating at cloud scale and efficiency, and a slightly larger number of surveyed organizations (49%) reported automation deployment. This is an area where there has traditionally been underinvestment. When compared with overall cloud use, there is a striking difference in the adoption of infrastructure automation. Of those organizations with only a single public cloud in use, 39% said automation was deployed. Those with more than 10 clouds in operation reported much higher levels of automation deployment – 55%. This is an indication

that automation is becoming mandatory to manage growing hybrid cloud complexity. Tools that leverage automation – such as IT operations platforms delivered as a cloud-based service that support infrastructure lifecycle management – can further help make sense of the complexity in hybrid cloud.

At the same time, survey respondents are also looking for more efficient operations, with a strong interest in predictive capabilities using telemetry and AIOps. This is a maturation of operational mindsets, as they move from reactive models to predictive ones on the way to being fully proactive. Almost half of surveyed organizations (45%) are using some form of AIOps technology today, and 49% are expecting to deploy it in the next year.

There are strong signals in the study about interconnection and the importance of access to data. Data fabrics can ensure that data is available across a hybrid environment, and 88% of respondents either have that capability in place today or expect to have it within two years. Building performant infrastructure to access the applications that are handling all that data is also seen as critically important, and private 5G wireless networks are expected to be utilized by 91% of respondents in the next two years. Hybrid environments depend on effective data distribution and access capabilities.

Bottom line: Hybrid cloud models are driving the adoption of emerging technologies, including AIOps, infrastructure automation, and edge computing. Infrastructure that aligns these capabilities and provides effective data access and distribution is vitally important.

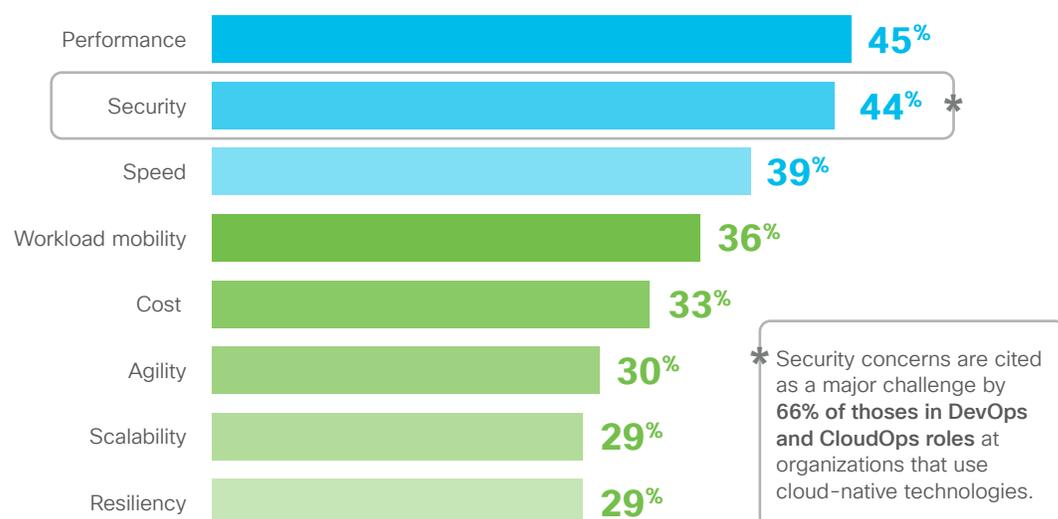


Accelerating cloud-native

The transition to cloud-native application architectures is accelerating as organizations look to these technologies to support better performance and security of their applications. Most survey respondents (91%) are actively moving or planning to move or refactor production workloads and

applications using cloud-native technologies. When you look at the considerations that are driving use of cloud-native technologies, requirements around performance (45%), security (44%), and speed (39%) are among the top responses from those in DevOps and CloudOps roles.

Figure 6. Performance and security are top drivers for using cloud-native technologies



Q. You indicated previously that you were aware of your business' plans for using cloud-native technologies. What requirements would you say are driving these plans?

Q. What are the main challenges to your organizations use of cloud-native technologies?

Base: Respondents in DevOps or CloudOps roles (N = 1,286)

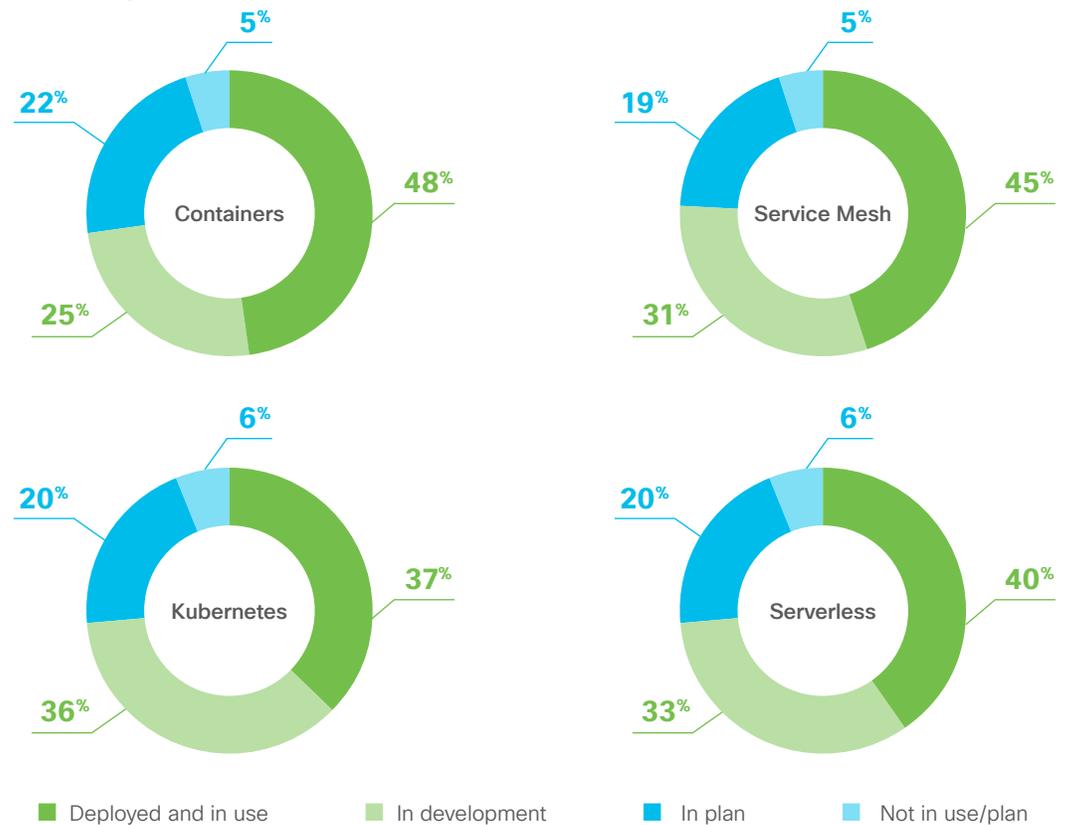
Source: Cisco 2022 Global Hybrid Cloud Trends Report

Survey respondents in CloudOps and DevOps believe that cloud-native technology has had a positive impact...

Nearly half of survey respondents at organizations using cloud-native technologies tell us that their organization has containers deployed and in use (48%), while 45% use service mesh, 40% use serverless technologies, and 37% have

deployed Kubernetes. Fewer than 5% of respondents do not currently use or plan to use any of these cloud-native technologies, and many organizations are in the planning or development stages.

Figure 7. Nearly all organizations currently use or plan to use cloud-native technologies



Q. Which of the following cloud-native technologies are being considered or are already in use?
Base: Respondents that use cloud-native technologies (N = 1,165)
Source: Cisco 2022 Global Hybrid Cloud Trends Report

Improved security is a critical outcome of IaC use, particularly among respondents in cloud operations roles...

While survey respondents are optimistic about the potential of cloud-native technologies, they are also acutely aware of the challenges their organizations face when it comes to effective implementation. Two-thirds (66%) of respondents in DevOps and CloudOps roles indicate that security concerns are the main difficulty in using cloud-native, followed by process and tools integration (57%) and budget constraints (52%) as other key challenges.

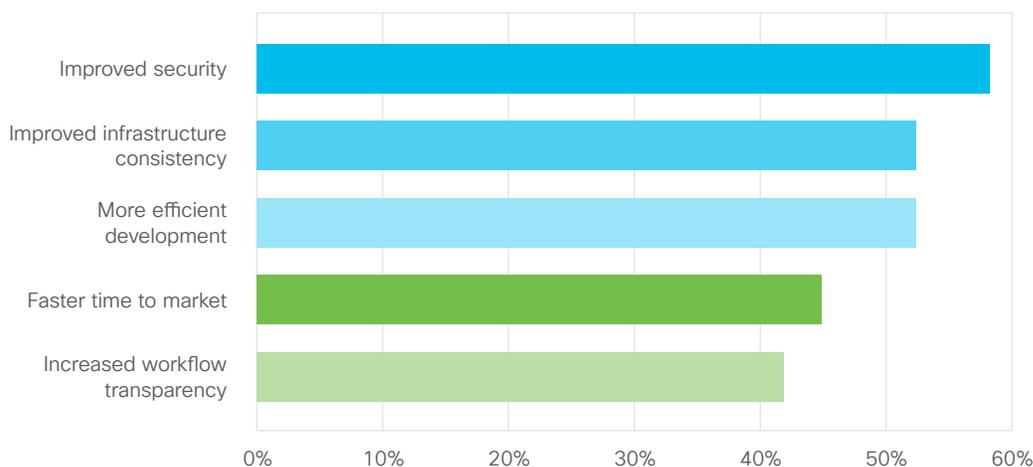
These security concerns are likely exacerbated by a lack of skills and budget in many organizations, which can lead to a lack of adequate data and workload protection in cloud-native environments – where development happens faster. In addition to influencing an organization’s security strategy, the use of cloud-native application architectures also affects networking strategy. Survey respondents

in CloudOps and DevOps believe that cloud-native technology has had a positive impact, making networking more automated (24%) and more secure (25%).

Using infrastructure as code (IaC)

Developers and CloudOps professionals that leverage cloud-native applications can further build on an organization’s automation and security capabilities using infrastructure as code (IaC), which enables the management of infrastructure through code instead of manual processes. Improved security is a critical outcome of IaC use, particularly among respondents in cloud operations roles, 68% of whom said that security improvements are a key driver of IaC, compared with 48% of DevOps respondents. Managing cloud security

Figure 8. Top reasons for adopting Infrastructure as Code (IaC)



Q. What are the most important drivers of your use of Infrastructure as Code (IaC)?

Base: All respondents (N = 1,286)

Source: Cisco 2022 Global Hybrid Cloud Trends Report

DevOps and CloudOps respondents are split on how they built existing IaC functionality...

is also among the dominant use cases of IaC for 69% of DevOps and CloudOps respondents. IaC is crucial in helping to manage complex applications (61%), especially among organizations that use more than 10 public clouds (72%).

Survey respondents in DevOps and CloudOps roles also value IaC for its ability to deliver more efficient development (52%) and improved infrastructure consistency (52%). Geographically, over half of organizations in Latin America indicate that reducing risk (52%) is the key driver of IaC use, compared with 34% of surveyed organizations in North America.

DevOps and CloudOps respondents are split on how they built existing IaC functionality, or how they expect to build it – either by extending existing management systems

(36%), using a SaaS-based IaC offering (34%) or building new development environments (30%). When looking at the steps necessary to secure IaC, DevOps and CloudOps respondents focused on identifying vulnerable settings and scanning IaC configurations for vulnerable settings as their leading imperatives (55% each). It is a preference that could be tied to expectations of broader cloud security issues. Interestingly, these vulnerability concerns were prioritized over two areas that are also common security issues with cloud-based infrastructure – identity and access management (41% of respondents) and embedded secrets (47%). It is clear that all these security issues are of significant concern to survey respondents.



Bottom line: Nearly all organizations are moving or refactoring their applications using cloud-native technologies, or they have plans to do so. Infrastructure as code (IaC) can help accelerate application development processes while improving security.



Conclusion

Hybrid and multicloud models have become the enterprise norm. When executed properly, these models enable organizations to improve security, performance, business agility, and operational resilience. They help support the adoption of a range of leading-edge technologies that enhance application development and operational efficiency. The organizations we surveyed are advanced users of technology that rely on multiple clouds for delivery. What sets them apart is a more mature approach to cloud use and operations. They are looking to capitalize on agility, scale, and technology advances, while expecting to leverage SaaS operations platforms, automation, and AIOps to manage costs and complexity.

Even the most effective hybrid cloud approaches increase challenges related to security and operational complexity. Hybrid-cloud environments require collaboration between stakeholders that

can identify the implications of technology decisions on other areas of the business and the overall hybrid cloud strategy. This requires a unified cloud operating model that supports a wide range of users and cloud frameworks. Proactive and consistent collaboration between cloud operations, networking, and DevOps teams can help ensure security, efficiency, and agility. These operational challenges will remain as the organization pursues new paths and looks to foster innovation.

There are significant benefits to hybrid cloud and multicloud models. However, organizations must master the skills and build the operational capabilities to capitalize on them. They must realize that hybrid cloud environments have profound implications for their infrastructure. They will risk their competitive position if they are not able to secure and manage these models effectively and efficiently.



To learn more, visit cisco.com/go/hybridcloud.



Methodology

Survey data referenced in this report was collected by 451 Research, part of S&P Global Market Intelligence, as part of an independent web survey of more than 2500 global IT decision-makers and professionals in cloud computing, DevOps, and enterprise networking roles. It was commissioned by Cisco. The Cisco 2022 Global Hybrid Cloud Trends Report was completed between April 11 and May 6, 2022. The survey was conducted in 13 countries across North America, Latin America, APAC and Western Europe (U.S., Canada, Brazil, Mexico, Australia, China, Indonesia, South Korea, Japan, Singapore, U.K., France, and Germany).

The survey was designed to examine trends in hybrid cloud as they relate to enterprises' overall infrastructure and global networks strategy. This report explores the progress of organizations around the globe as they work to achieve the promise of hybrid cloud through new technologies and processes, and makes recommendations to help organizations marry expectations with reality of hybrid cloud and complementary and emerging technologies.



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) 08/22



The bridge to possible

SECURE
AGILITY

www.secureagility.com



CISCO
Partner

Gold Certified