

SURVEY REPORT

WANCLOUDS 2022 CLOUD-NATIVE TRENDS OUTLOOK

wanclouds

The future of cloud computing is evolving at a rapid pace. With the COVID-19 pandemic prolonging most businesses' remote work plans and accelerating their digital transformations, the number of organizations moving to the cloud is exploding. In addition to the broader shift to the cloud, organizations are also adopting cloud-native computing approaches to effectively build and run applications across public, private, and hybrid cloud environments.

Rather than designing solutions for the cloud and then deploying them in legacy data centers, cloud-native approaches focus on building solutions to be engaged in a distributed cloud model. These approaches are now explicitly designed to take advantage of the scale, elasticity, and resiliency of modern cloud environments.

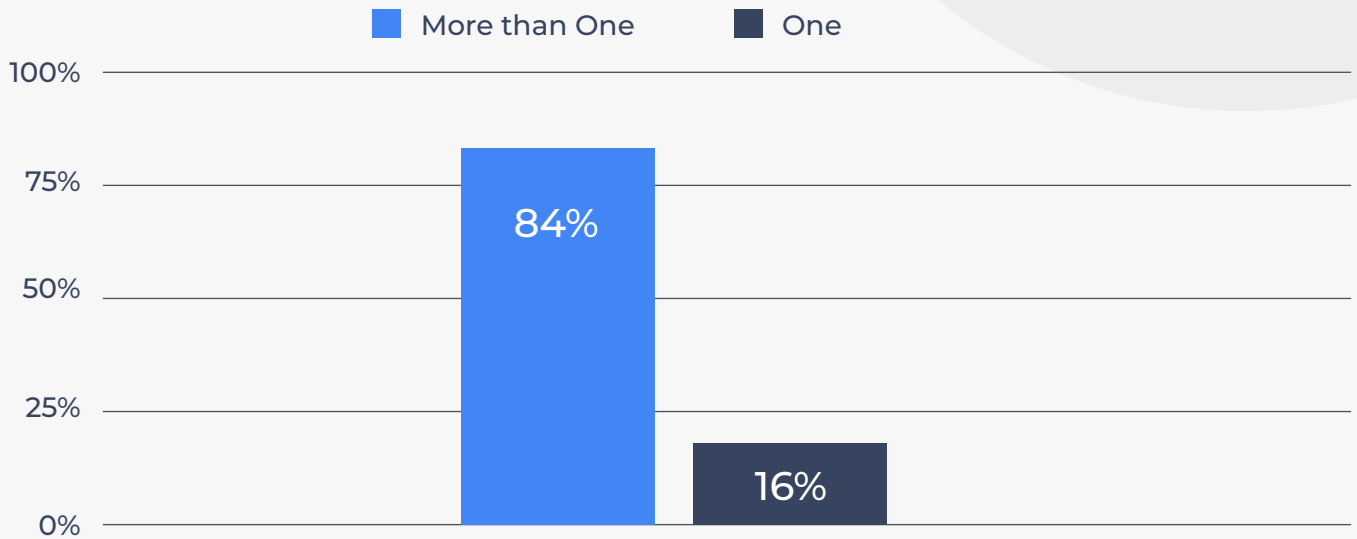
As IT leaders look to capitalize on cloud innovation, they are also increasingly turning to Kubernetes and containers to empower cloud-native application development. Kubernetes use has seen explosive growth over the last year. In fact, according to the most recent State of Cloud Native Development Report by SlashData, over 5.6M developers use Kubernetes today. That is up 67% year-over-year and means that 31% of all backend developers are now using the container service.

To better understand how these developers, IT teams, and the companies they work for are becoming cloud-native, as well as the issues they will face across the cloud in 2022, Wanclouds commissioned a survey to 416 U.S. and UK IT decision-makers in Q4 2021. The results informed the following 2022 Cloud-Native Trends Outlook.

Nearly half (48%) of responding decision-makers said their organization began building and/or deploying applications in the cloud more than 2 years ago, 42% started 1-2 years ago, and 10% noted they started less than a year ago. When asked how far along their organization is in its cloud-native journey, 15% of respondents said less than 20% of their applications are in the cloud, 30% said 20-40% of their applications are in the cloud, 29% said half of their applications are in the cloud, and 22% said more than half of their applications are in the cloud. An additional 5% said their organization was 100% cloud-native.

MULTI AND HYBRID CLOUD FOCUS IN 2022

How many cloud platforms does your company use?



'Flexibility' is an essential aspect of modern workplace environments. Not only are employees demanding more freedom to decide when they work, where they work, and how they work, organizations are pushing for greater mobility in their third-party vendor strategies. The rise in multi-cloud and/or hybrid-cloud adoption exemplifies this. In fact, Wanclouds found that 84% of IT decision-makers say they use more than one cloud platform today. Most commonly, they said they use two (29%) or three (19%) cloud platforms.

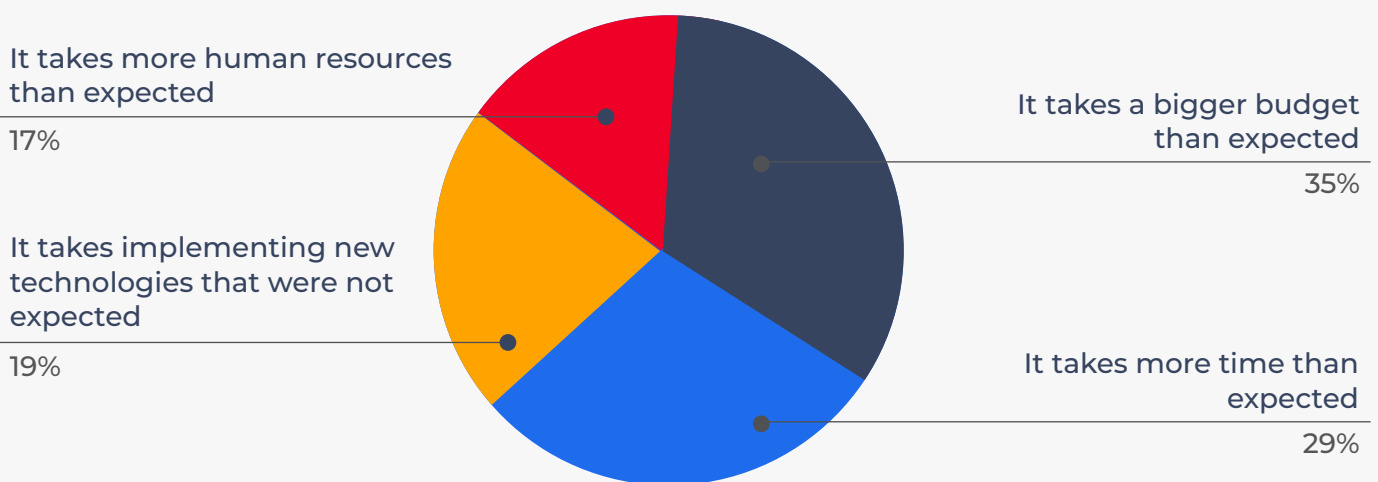
There are plenty of benefits pushing enterprises to go this route. Most notably, companies can focus on using the best cloud environment for the specific needs of each workload. But perhaps the most cited reason by IT executives is avoiding vendor-lock-in with any cloud provider. When Stratoscale polled a group of IT professionals recently, 80% reported medium to high levels of concern about being locked into a single public cloud platform. This concern was particularly prevalent amongst companies with fewer than 100 employees.

But the preference for a multi-cloud approach certainly isn't exclusive to small businesses. Despite several competitors choosing a solo provider, JP Morgan has been vocal about its multi-cloud – or precisely its hybrid cloud – strategy. As its CIO of Global Technology Infrastructure, George Sherman recently told Insider: "A multi-cloud, hybrid strategy is the winning strategy, I don't think it's conservative or cautious — I think it's smart, and I think it's practical."

This is a sentiment shared by most British and American IT decision-makers, it seems, with just under half (48%) telling Wanclouds they use both private and public clouds today. Meanwhile, Wanclouds also found that less than a quarter of respondents (22%) are using only public cloud platforms. Additionally, 15% of IT decision-makers say they're using a mixture of on-premise and public cloud platforms, and another 15% say they're using a blend of on-premise, private, and public clouds.

CLOUD MIGRATIONS ARE TAKING LONGER & BIGGER BUDGETS THAN EXPECTED

When working on Multi-Cloud Migrations for your organization, which of these is most often the case?



With household names like Ford, Boeing, and Adidas expanding their cloud strategies through partnerships with the 'cloud big four', there's never been more focus on how enterprises effectively migrate their data to the cloud and how much it costs them. Indeed, with 2021 highlighting just how costly downtime is to businesses' financial health, companies' migration journeys have become incredibly high stakes. Now more than ever, there's a need to complete the journey quickly, with minimal to no disruption, and in a cost-effective manner. Unfortunately, however, this isn't always the case.

When it comes to the migration length, nearly half (48%) of US and UK companies say the average length of time it takes them to complete a single multi-cloud application migration successfully is 1-2 months. Nearly a quarter (23%) say it takes them up to 6 months, and 9% say it takes them more than 6 months. Only 19% say it takes them less than a month to migrate an application to the cloud.

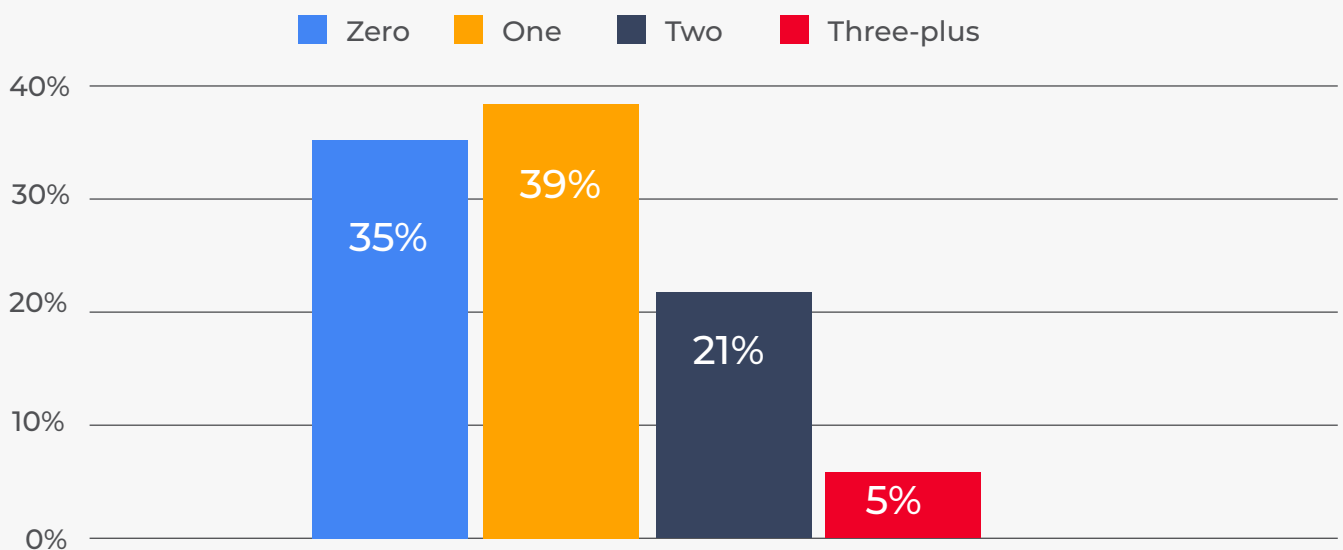
Considering how robust most businesses' application stacks are, that's a lot of time and money that companies have in front of them for migrations. Even companies with fewer than 1,000 employees run an average of 22 custom applications according to McAfee, and large enterprises with more than 50,000 employees run 788, on average.

The number of those applications to migrate and complexities in migrating across multiple clouds are leading to migrations taking a bigger budget than expected. In fact, when asked what challenges they most often faced with multi-cloud migrations, 35% said 'it takes a bigger budget than expected'. That was followed by those who said their biggest challenge was 'it takes more time than expected' (29%), it 'takes implementing new technology or updating existing technology that wasn't expected' (19%), and those that said 'it takes more human resources than expected' (17%).

And the costs keep rolling in even after the migration is complete. In fact, 54% of IT decision-makers say they are getting hit with ongoing cloud costs or spending based on what they planned. As a result, most (37%) have resorted to tracking their cloud spend weekly, while a third say they do so monthly. The pain of getting hit with unexpected costs is a point the Wanclouds team regularly hears from customers, particularly from AWS users frustrated by hidden charges and a lack of company-wide cloud visibility within the platform's billing system.

CLOUD SECURITY RISES IN IMPORTANCE IN 2022

How Many Data Loss Incidents Has Your Company Experienced In The Past Year?



Enterprises worldwide have been battling a cybersecurity crisis and health emergency in tandem. The shift to working from home has left gaps in many businesses' security strategies, while opportunistic cybercriminals increasingly target healthcare and manufacturing organizations under enormous strain. It's hardly a surprise then that 88% of IT decision-makers say they're at least slightly worried – and 15% are apprehensive – about cloud workload security in 2022.

Meanwhile, extreme weather events like the 1-in-500 year rain/flooding in NYC, west coast wildfires, and Storm Christoph in the UK create even more havoc for businesses and threaten downtime. Between cybersecurity and climate warnings, enterprises have a challenge on their hands to protect their cloud environments. A challenge that's proven too difficult for most, with a vast majority of US and UK businesses feeling the wrath of data loss incidents in 2021.

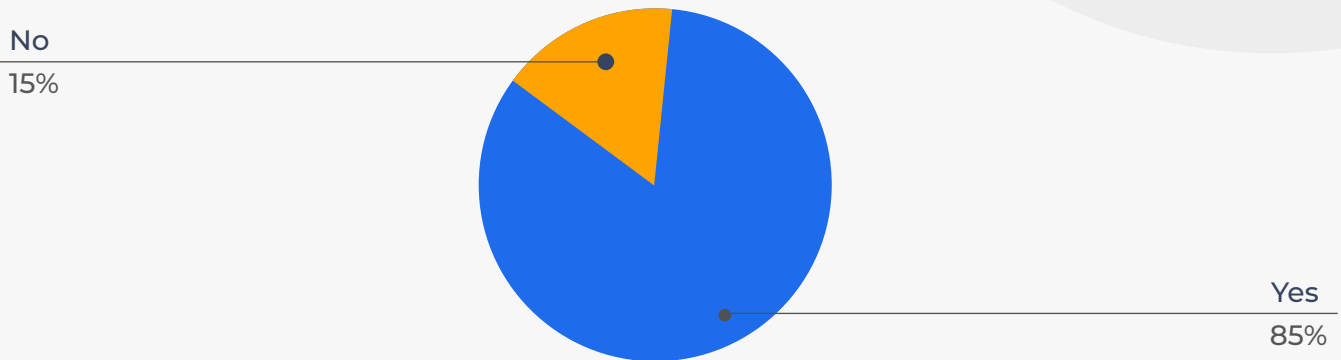
According to Wanclouds, 65% of IT decision-makers say their organization experienced at least one data loss incident last year. Over one-in-five (21%) said they experienced two data loss incidents, and 5% said they lost data in three separate events. Unfortunately, this has been a common theme for a while. But not only is it getting worse, but the severity of data loss is also worsening.

The cost of dealing with a data breach or downtime incident is too much for many companies to overcome. A whopping 60% of small businesses will close after experiencing a data breach. Unsurprising, considering the cost of downtime is \$5,600 per minute. Wanclouds found that of the nearly two-thirds of businesses that experienced data loss in 2021, 31% experienced downtime or unavailability of cloud services for six to 10 hours. That answer was followed by 29% who said their downtime lasted one to five hours, and 17% that noted they were offline for 10 to 15 hours. A further 5% said their cloud services were unavailable for more than a day after they experienced a data loss incident.

Yet, 28% of US and UK IT decision-makers say they still don't have a cloud-based disaster recovery plan in place to respond to these incidents. If the Covid-19 pandemic has taught us anything, it's the importance of cloud-based disaster recovery and business continuity planning. Without one, every business risks losing vital data and having their systems, operations, or services shut down by natural and man-made disasters, security risks, hardware failures, and power outages.

CONTAINER USE WILL INCREASE NEXT YEAR

Will You Be Using A Cloud Container Strategy Next Year?



The pandemic, and IT teams' attempts to create more agile, efficient, and quicker workflows, have undoubtedly accelerated adoption. In a year when more organizations will move to a distributed IT infrastructure spread across multiple clouds, we'll also witness an accompanying increase in containerized applications. According to Wanclouds, 85% of IT decision-makers say they will be using a cloud container strategy next year. This represents significant industry growth, given Gartner previously predicted that only 75% of global organizations would run containerized applications in production by 2022.

Its portability, flexibility, and multi-cloud capabilities have caused the open-source container orchestration platform to increase in popularity. In particular, we're seeing many organizations adopting Kubernetes as their default container orchestration tool. The Cloud Native Computing Foundation data shows that of the 84% of companies using containers in production, an overwhelming 78% were using Kubernetes.

Given the growth in use, there also needs to be a focus on protecting an organizations' Kubernetes applications. Despite their strict security protocols that help block access to components outside of a cluster, Kubernetes are susceptible to attack. A few years ago, hackers hijacked Tesla's Kubernetes console to perform crypto mining and access its AWS environment credentials. Researchers recently detected a series of attacks against Kubernetes clusters via misconfigured Argo Workflows instances. Hackers could access an open Argo dashboard and submit their workflow.

For many IT teams, however, they feel out of their depth. 54% of respondents told Wanclouds that they think it's more challenging to secure Kubernetes environments than legacy cloud environments. Fortunately, this is something the Cybersecurity and Infrastructure Security Agency (CISA) has explored in the face of rising malware and supply chain attacks. It recommends several proactive and hardened security measures including regularly scanning containers and pods for vulnerabilities; running containers and pods with the least amount of privileges possible; using network separation to control the amount of damage a compromise can cause; using firewalls to limit unneeded network connectivity, and using encryption to protect confidentiality.

Looking Ahead

Cloud usage will continue to evolve in 2022. In particular, there'll be much focus on how organizations manage their multi-cloud environments and which cloud providers they'll tap to host their critical resources. It's turned into quite the competition, with the likes of AWS, Microsoft, Google, and IBM fighting for market share in an incredibly profitable industry. And as enterprises continue to realize the value of deploying multiple providers within multi and hybrid cloud environments spending will increase substantially in the New Year.

But that doesn't hide the fact that significant challenges threaten enterprises' cloud-native journeys. While most C-suites are making multi-cloud a strategic priority this year, budgeting, security risks, and even a tools/skills shortage prevent many organizations from enjoying a smooth migration – especially those with lean IT teams.

Wanclouds

Wanclouds is a leading multi-cloud SaaS, solution, and managed service provider. It helps enterprises with cloud deployments, migrations, and protecting their cloud infrastructure in time and cost-efficient ways. The company's cloud Migration as a Service (MaaS) and Disaster Recovery as a Service (DRaaS) reduce the financial investment and remove the technical complexities that halt or delay businesses from migrating on-premise to the cloud, moving across clouds, or setting up backup and restore protection. Its SaaS-based automation suite VPC+ provides a single pane of glass for managing and protecting multi-cloud environments through a centralized cross-cloud solution. Wanclouds is headquartered in Santa Clara, CA.