HPE GreenLake

8 steps to achieving the cloud-everywhere vision

If you were to imagine the perfect book to describe IT organizations right now, it might be entitled A Tale of Two Clouds.

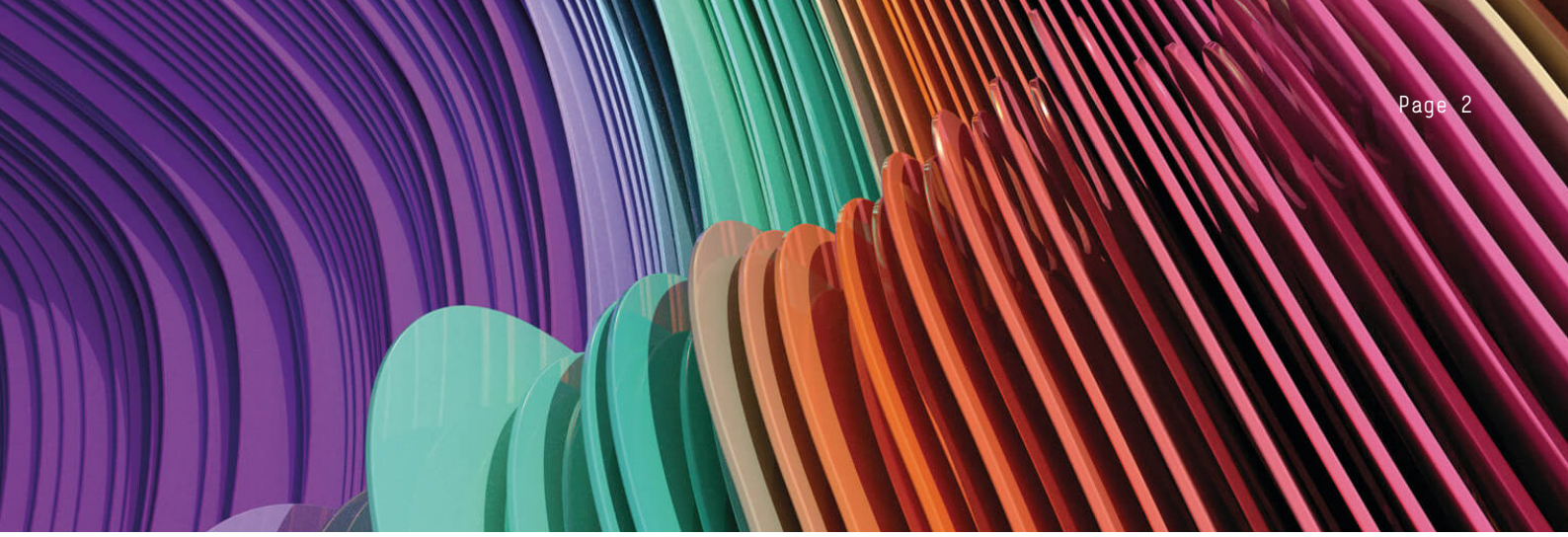
With 30%[1] of new digital workloads being deployed to the cloud as of 2021, organizations are pouring time and money into a mix of both public and private cloud infrastructure. But they're not doing so equally.

What's the holdup? The problem lies in the fact that, like in **A Tale of Two Cities**, the 1859 Charles Dickens novel contrasting London and Paris before the French Revolution, private and public environments have evolved very differently. Private clouds rely mostly on legacy, on-premises infrastructure and personnel. Public clouds use service providers and more modern technology to host and share digital content.

Enterprises know they will ultimately benefit from tapping the best of these two **cities**. And most dream of the day when they will finally be able to move beyond **cloud-first** thinking—which implies they're still headed in that direction—and toward a **cloud-everywhere** mentality. This is where, instead of talking about the silos in which data and applications sit, you can focus on how you'll use your well-oiled hybrid cloud to deliver innovative experiences to customers, partners, and employees.

This obviously will not happen overnight. Too many business, people, process, and technology hurdles stand in the way. Nonetheless, here are eight steps companies can follow to tackle immediate challenges and jump on the path to building cloud-everywhere environments.

[1] Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences—Press Release by Gartner, November 10, 2021.



1. Think security first

Cybersecurity is one of those checkbox items that far too many IT organizations put off until the end of a project. So, we're mentioning it first and suggesting it should top every hybrid cloud to-do list.

According to the 2022 Thales Cloud Security Study,[2] 35% of organizations globally say they have experienced a cloud-based security incident or failed an audit in the past year. Not surprisingly, these security concerns have restricted many businesses, as they consider moving to the public cloud.

Sean Foley, senior director and edge-to-cloud transformation strategist at Hewlett Packard Enterprise, notes that part of the difficulty lies in the fact that many enterprises start with a private cloud, where the security approach changes minimally from on-premises operations. However, once workloads get moved to a public cloud provider, things get more complicated. You need more automation to move data files around, and therefore, you need to adjust your overall security approach.

Foley says success hinges on making improvements across four security disciplines:

1. Strong identity and access control, dictating who or what gains entry to the network
2. Effective logging and monitoring of all network activity to understand typical network traffic and look for anomalies or security incidents requiring remediation
3. Consistently deployed encryption for fortifying private and highly confidential data
4. Automated response mechanisms to douse the flames of security events before they spread

2. Embrace FinOps

The big promise of cloud computing is the speed, agility, and—more than anything—cost savings it can offer when implemented correctly. But surveys suggest companies don't have a tight handle on how much their cloud environments cost on an ongoing basis. As a result, they end up spending too much.

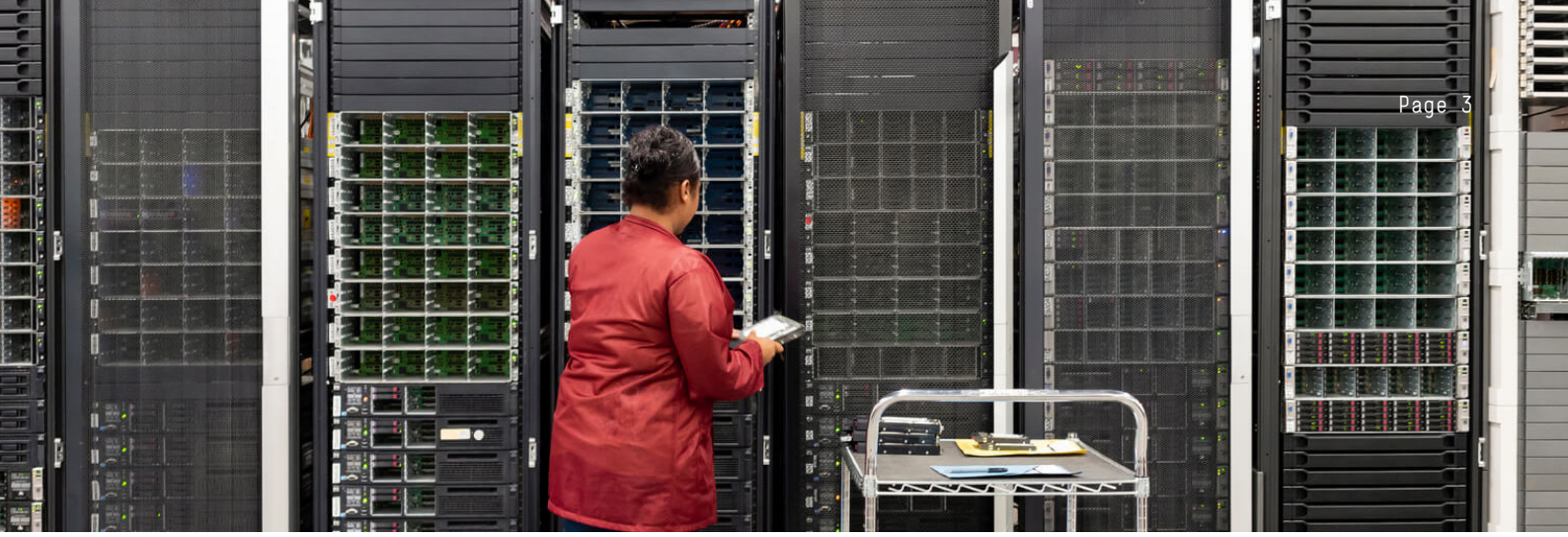
According to the recent Flexera 2020 State of the Cloud Report,[3] IT professionals surveyed said they expect to increase cloud investment by almost 50% this year but still struggle to accurately forecast spending. In fact, they said their organizations exceed this investment by an average of 23% while wasting about 30% of their cloud budgets.

This isn't a new trend. Companies have struggled to understand their economics since hybrid cloud became a reality. But to become cloud everywhere, it will be critical to establish programs, processes, and the technical wherewithal to holistically track, monitor, analyze, and address cost in both public and private infrastructures—and do that in as automated a fashion as possible. Not doing so will continue to hamper and harm even the best hybrid cloud programs.

But to become cloud everywhere, it will be critical to fully embrace FinOps. FinOps is an evolving discipline focused on establishing the program, process, and technical acumen to allow teams to collaborate on data-driven spending decisions.

[2] 2022 Thales Cloud Security Study—Thales, May 2022.

[3] State of the Cloud Report—Flexera, 2022.



3. Know your data

Arcserve says there will be 200 zettabytes of data worldwide by 2025.[4] Some of that will be yours (even if you aren't sure how many bytes are in a zettabyte), but do you know how much? Or where it sits? Or what to do with it? Or how to secure and manage every bit of it?

Good data management begins with having systems in place to troll your public and private networks. You should be performing regular audits to understand the lay of the digital land and issuing reports to keep everyone informed across the organization, from IT to operations, finance, sales and marketing, human resources, and legal.

4. Pay attention to your people

As IT professionals, it's easy to focus on the technical aspects of a hybrid estate. But failing to also address the people and process side of the equation could be tantamount to disaster.

Specifically, it is critical to make sure that employees—existing and new hires—are well versed in what it takes to integrate, manage, and secure both private and public cloud infrastructure successfully and cost-effectively. Unfortunately, most organizations are limited by having experts in only one or the other area.

In fact, 86% of respondents in a Wakefield Research and Logicworks survey[5] believe a shortage of qualified engineers will slow cloud projects, and 63% agree it's harder to find a qualified engineer than it is to locate Bigfoot (seriously).

When marching toward the cloud-everywhere destination, organizations must do their utmost to find and hire talented IT professionals who understand the ins and outs of both private and public environments. If hiring is an issue—and even if it isn't—investing in training to ensure current employees can step up to the hybrid cloud task becomes essential. You cannot succeed if half the team is highly agile and spends its energy on public cloud while the other half is bogged down servicing 20th century technology. If you're going to be agile, just be agile. The technologies and outcomes might be different between Amazon Web Services or Microsoft Azure and on-premises, but the concepts are the same.

5. Peer through a single pane of glass

At one time, software vendors promoted the idea that you're better off being on one platform because you can take advantage of everything the environment offers. Companies bought it for a while, but in the digital age, that **better together** approach has given way to a more multifaceted one.

Rather than putting all of their public cloud eggs in a single basket, 72% of IT organizations are mixing it up across multiple platforms according to the 451 Research January 2020 report, public cloud lock-in concerns incongruent with successes seen in multicloud deployments.[6] Each platform offers its means of monitoring what's going on within that environment, but platforms do not play well together. What's more, they don't provide a view of information or apps being consumed from data warehouses or the network edge.

All of this makes it difficult to get a true picture of activity across the hybrid estate. For this reason, it's important to look for options that provide a single pane of glass for all consumption-based IT. This is a user interface displaying key statistic data for understanding and controlling your entire hybrid cloud. Look for services or solutions with a unified dashboard and features such as consumption analytics, continuous regulatory compliance monitoring, and fast provisioning.

[4] The 2020 Data Attack Surface Report—Arcserve, 2020.

[5] 86% Believe Talent Shortage Will Slow Down 2020 Cloud Projects—Logicworks, 2020.

[6] Public cloud lock-in concerns incongruent with successes seen in multicloud deployments—451 Research, January 2020.

6. Mind your SLAs and CLAs

When you have absolute control over your private cloud, it's fairly simple to ensure high-quality service levels. After all, it's your baby and you don't have to rely on anyone else to keep it running. But when relying on service-level agreements (SLAs) or cloud service agreements (CLAs) with one or more outside providers, this process can become incredibly time consuming and costly.

These agreements need to be in sync and well-orchestrated to ensure the greatest possible user experience, not only for employees but also your customers. At a minimum, take the time to identify who will be responsible for continually overseeing your agreements, know what you can negotiate, and make sure you have alternatives for extricating your company from a relationship if needed.

Again, you have the option to offload these responsibilities. There are plenty of services available today that specialize in SLAs and CLAs, so you can spend your valuable time on higher-level priorities.

7. Ensure high availability and failover through automation

Channeling his inner Yogi Berra, Amazon's Werner Vogels once quipped, "Everything fails all the time."

IT professionals often take that concept to heart when planning their hybrid estates but don't always embrace it as fully as they should. In the ideal world, everything is built in such a way that, if it goes down, it comes back up automatically with little intervention. In practice, however, things don't always go so smoothly.

On-premises, you build backup, redundancy, and failover into physical servers, storage, and other arrays. In the public cloud, you rely on software for automated recovery. By themselves, they work OK. But in hybrid environments, having two inconsistent systems can create service inefficiencies during outages.

Organizations should adjust by pivoting their on-premises operations to be more **cloudy** through microservices, automation, and other modern processes and apps that manage availability and failover.

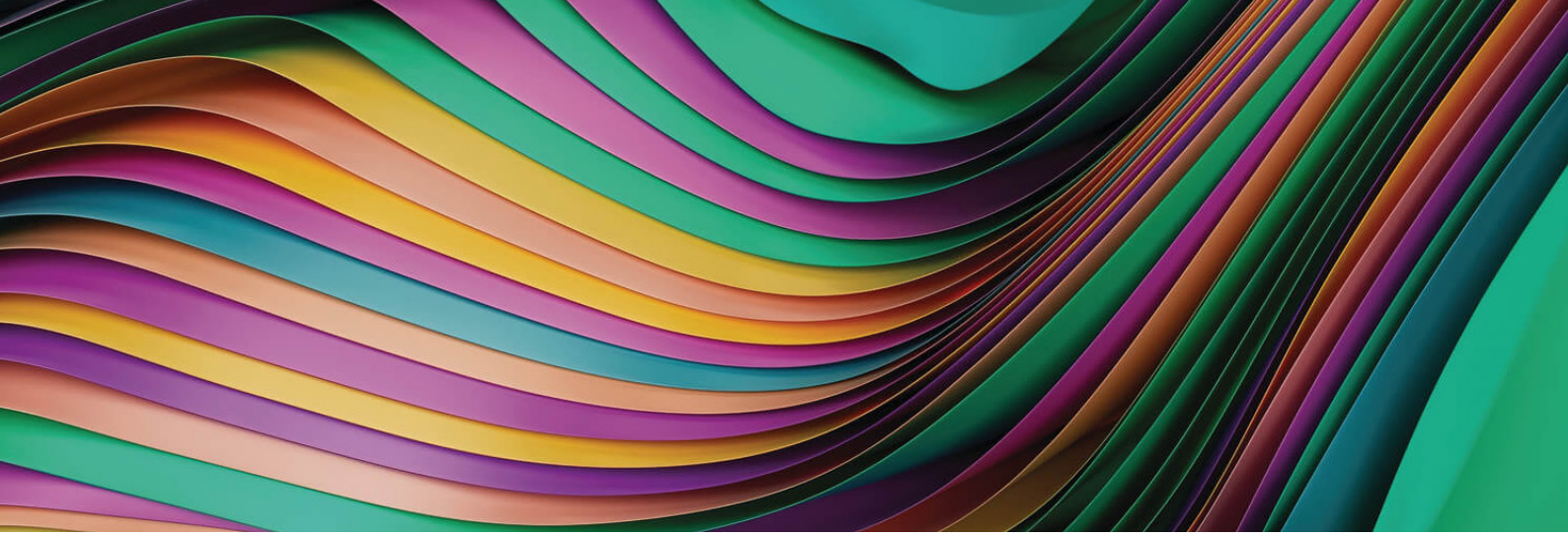
8. Let someone else do it

Reaching the cloud-everywhere panacea is no small task. It takes time, diligence, and expertise.

You may have all those things in-house. If so, great. If not—or if you're unable to commit resources to the long-term task of figuring out how to build, deploy, manage, and automate workloads in your hybrid environment—then outsourcing might make more sense.

Outside advisory services can help you embrace the cloud faster. They typically provide global teams of consultants who can assist you in building the right hybrid clouds for your business while evolving your team's culture and skills. They will handle much of the public and private cloud integration work so you can avoid many of the most common challenges organizations face today. For example, the HPE Transformation Program is designed to do just that. It leverages the HPE Edge-to-Cloud Adoption Framework to accelerate and decrease the risk of transforming to a cloud-like operating model.

The cloud-everywhere vision is within reach for most organizations. But achieving it requires a solid plan, a commitment to making it happen, and a willingness to consider outside consultants. If organizations do all of this, their IT staff can finally close the book on **A Tale of Two Clouds** and bring better experiences to life.



Learn more at

hpe.com/us/en/greenlake/cloud.html

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Explore **HPE GreenLake**

Get updates

Hewlett Packard Enterprise

a50006801ENW