How to unify and control your

Hybrid Cloud

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"

While industry analysts predict 75 percent of all databases will be deployed or migrated to a cloud platform by 2022, what that actually means is really up for debate. Organizations are undoubtedly investing time and money into a mix of both public and private cloud infrastructure. But they're not doing so equally. Indeed, Hewlett Packard Enterprise CEO Antonio Neri noted at the company's Discover Virtual Experience event in July 2020 that more than 70 percent of enterprise apps and data still operate outside of public clouds.

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.

Enterprise organizations know they will ultimately benefit from tapping the best of these two "cities." And most dream of the day when they're finally 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. Think security first

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

According to the State of Cloud Security 2020 survey from Sophos, nearly three-quarters (70 percent) of organizations have experienced a public cloud security incident in the past year. Not surprisingly, the same percentage of IT leaders say security concerns have restricted their move to the public cloud.

Sean Foley, director of cloud delivery at HPE, notes that part of the difficulty lies in the fact that many enterprises start with a private cloud where the security approach changes minimally. 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, need to adjust the 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. Understand your economics

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.

In fact, in the recent Flexera 2021 State of the Cloud Report, IT professionals surveyed said they expect to increase cloud spend by almost 39 percent this year but still struggle to accurately forecast spending. In fact, they said their organizations exceed cloud spend an average of 24 percent while wasting about 30 percent of their cloud budgets.

This isn't a new trend. Companies have struggled to understand their economics since hybrid cloud became a thing. 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 program.

3. Know your data

IDC says there will be 175 zettabytes of data worldwide by 2025. 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.

"Everything fails all the time"

- Werner Vogels, Amazon

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 staffs are limited by having experts in only one or the other area.

In fact, 86 percent of respondents in a recent Wakefield Research and Logicworks survey believe a shortage of qualified engineers will slow cloud projects this year, and 63 percent 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 (AWS) and on-prem, 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 percent of IT organizations are mixing it up across multiple platforms, according to 451 Research's January 2020 report, "Public cloud lock-in concerns incongruent with successes seen in multicloud deployments." Each platform offers its own 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 thisreason, 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.

6. Mind your slas and csas

When you have absolute control over your own 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 (CSAs) 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 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 CSAs 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, it's not always so smooth.

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 process and apps that manage availability and failover.
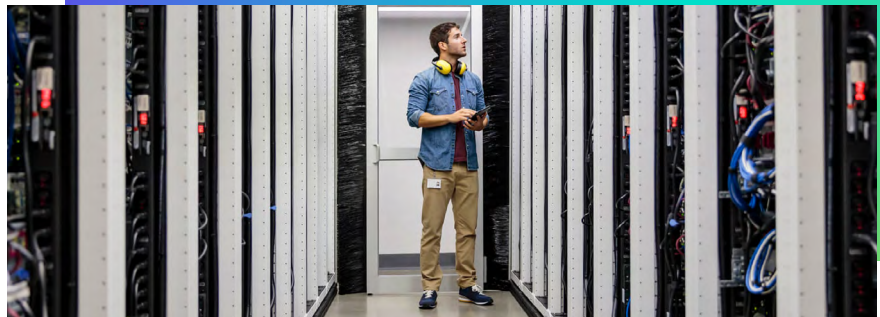
8. Let someone else do it

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. But 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 seek the help of trusted advisors to help guide you.

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.

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 staffs can finally close the book on "A Tale of Two Clouds" and bring better experiences to life.

How companies can take control of their multicloud investments

Maintaining a solid view of your hybrid estate requires Standardized procedures and processes throughout the enterprise

If you're like the vast majority of companies, according to the Flexera 2020 State of the Cloud report, you are accelerating your hybrid cloud strategy. You might still keep your mission-critical apps and data on-premises, but most likely you're moving several of your workloads to the public cloud. And if you're like many IT organizations, the road hasn't been easy. You're struggling to manage costs, meet government regulatory compliance requirements, and ensure maximum visibility into what's consumed across your public and private cloud environments.

Sound about right?

According to Flexera's survey of cloud decision-makers, 87 percent of organizations now have hybrid cloud strategies in place, and 59 percent say their cloud use is higher than before COVID-19 hit. At the same time, IT organizations are running into difficulties managing all of their data and applications across their private and public cloud infrastructure.

Had everything remained on-premises and, maybe, one public cloud environment, things might have been different. Most companies, however, want to avoid getting locked into any one service provider, with 72 percent saying they use a mix of public cloud platforms.

Part of the problem with that approach lies in the fact that each cloud provider's environment is proprietary. On their own, they function quite well, offering the visibility, metering, and analytics you would want to efficiently manage and secure your data environments. But they do not interoperate. Not really. So it becomes almost impossible for IT, operations, and financial leads to get an accurate sense of how much data and other resources are regularly consumed by individuals or departments across the enterprise.

The result of all of this, according to the Flexera study, is that organizations often find themselves over budget on cloud an average of 23 percent and wasting an estimated 30 percent of their cloud spend. And, as for on-premises environments, businesses typically find that they overprovision by almost 70 percent in order to avoid running out of capacity. Additionally, they are running into compliance and security issues as their apps and data become more distributed and complex.

But it doesn't have to be this way. By adhering to the following guidelines, IT organizations can gain better control and insights across their hybrid estate.

1. Prioritize visibility into usage and spending

Visibility—or the difficulty gaining it—is easily the most pressing problem for most organizations after migrating to multicloud environments. It's not that IT professionals can't use native tools offered by each cloud solution. Some of them are actually rather good. But when overseeing multiple private and public cloud environments, the process can be painfully tedious, time consuming, and inefficient.

This is where a unified software platform designed for hybrid environments can help. The best of the bunch will provide a central console offering an incredibly clear line of sight into how, when, where, and by whom data, applications, and other resources are being consumed across the enterprise. This is no small accomplishment when you stop to think about it.

2. Apply consistent tagging methodologies

Visibility into your consumption data is one thing, but can you gain insights from that data that make sense to your stakeholders? This is relevant because, in all likelihood, you pay for services as you consume them, and you want to make sure that you're paying for services that are a) being used, and b) meet the needs of the business.

This is where resource tagging comes into play. Whether it's storage, compute, virtual machines, containers, or any other resource you're consuming, proper tagging methodologies let you add business context to your consumption data so that you can report usage and spend in meaningful ways. But if each cloud has its own proprietary tags, and you are operating in multiple environments, gaining a holistic view becomes impossible. Adding to the complexity: 30 percent of organizations with more than 1,000 employees say they have different business units using different cloud vendors, according to the 451 Research report "Public cloud lock-in concerns incongruent with successes seen in multicloud deployments."

This is where unified consumption analytics platforms offer particular value. By aggregating usage and cost data across the hybrid estate and enabling you to apply consistent tagging methodologies, they can drive more accurate cost and forecasting reporting along with deeper insights into your hybrid estate's activities.

3. Design automatic triggers to identify opportunities

Applying rules to the consumption data you collect helps identify any important cost and compliance improvement opportunities. Then, with the right unified software platform, you can set up automatic triggers that let you know it's time to take some recommended action.

For example, looking across the entire cloud estate, the service provider could flag which departments are getting the most out of their cloud access, which ones are hardly using it at all, and which ones might be leaving the virtual meter running while away from the office, costing the organization unknown dollars. Similarly, the provider's holistic visibility could expose costly system anomalies or issues that need to be addressed.

4. Automate controls for consistent compliance

Another area of particular significance is compliance. Businesses are increasingly under pressure to comply with a variety of compliance frameworks, such as the NIST Cybersecurity Framework, HIPAA, and GDPR, with stiff penalties for noncompliance—not to mention the impact on a company's brand should a breach occur. One of the most significant benefits unified software platforms provide is that they make it easier to manage IT security and compliance across hybrid estates through rich tools and expertise.

According to the Flexera survey, 83 percent of enterprises point to cybersecurity as the top challenge they face with their hybrid cloud environments. Data governance, which relates to all of the back-end work supporting regulatory compliance efforts, was cited as a top concern by 79 percent of participants.

5. Partner to optimize cost, compliance—and more

The trouble many organizations face in both of these regards is that, while they tend to be highly skilled at fortifying their own data centers and tracking private data within them, they're not as experienced at holistically optimizing hybrid cloud environments to achieve greater visibility and manage budgets and overall spending or regulatory compliance. Even when they are, they typically benefit from offloading many of those responsibilities to a qualified third party.

"Paper-based records are more than an inconvenience. We have to change our approach, to digitize project management. All parties want it: contractors, regulators, suppliers, and management."

- Henrik Andersson, Supervisor, Interoc

For instance, Interoc, a Swedish construction firm, wanted to ensure industry compliance and better management of numerous projects by switching to an all-digital cloud solution. It knew from experience that paper-based record-keeping could be time consuming and inefficient, especially in its industry. Any lack of accurate record-keeping could have created a huge regulatory issue.

"Increasingly, we're being asked to show environmental or regulatory compliance," says Henrik Andersson, a supervisor at Interoc. "We need to be able to show live updates or to attach video or photo evidence. Paper-based records are more than an inconvenience. We have to change our approach, to digitize project management. All parties want it: contractors, regulators, suppliers, and management."

By turning to a managed service, however, Interoc was able to reduce project management reporting time by 60 percent and uncover potential regulatory hurdles before they became bigger issues.

Some unified software platforms can help companies detect provisioned resources that are out of compliance. The better ones do that across the entire hybrid cloud estate. They promote faster and easier gathering of relevant data across the network in preparation for regulatory audits. And they make it possible to holistically implement, manage, and enforce process-rule compliance. In a nutshell, they provide complete visibility and real-time alerting for governance, risk, and compliance data.

The trend toward hybrid cloud environments doesn't appear likely to subside anytime soon. If anything, it's accelerating and giving rise to a host of visibility, business context, and security and compliance challenges. By turning to a unified software platform, however, organizations can achieve the level of continuous cost and compliance they need to keep everything running smoothly, safely, and securely.

Delivering your hybrid cloud and workloads as a service to help optimize cost, control, and business agility. Annodata with HPE GreenLake.

Learn more at

kyocera-annodata.co.uk

annodata
A KYOCERA GROUP COMPANY