verinext

SOLUTION BRIEF

TOP 7 WAYS TO MAKE THE MOST OF THE HYBRID CLOUD

The allure of the cloud is obvious. When public cloud services became available, many organizations moved workloads from on-premises systems in a headlong rush. But as the volume of data and the number of applications multiplied, problems arose. Some brought workloads back in house and others decided to put a halt to the sending any more workloads to the public cloud.

65% of respondents to the Uptime Institute Global Survey of IT and Data Center Managers 2023, for example, are not hosting any mission-critical applications in the public cloud. Why? Costs spiraled out of control in many cases. For others, the cloud became difficult to manage. The hybrid cloud model emerged as a way to optimize the use of the cloud and on-premises systems.

But even in a hybrid setting, complexity lurks. Organizations now have so many cloud services in operation that they typically utilize multiple cloud services from different providers, from multiple public clouds to the growing prevalence of cloud services including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service solutions. These cloud services interchange data and workloads with private cloud infrastructure. Additionally, organizations are more global than ever. Hence, they have cloud services of different flavors and from different vendors functioning in many regions.

Faced with such complexity and geographical dispersal, how can organizations cope? Here are seven ways to make the most of the hybrid cloud.

1 ESTABLISH A SECURE CLOUD

Cloud insecurity haunts the enterprise. The average data breach in the U.S. goes undetected for 206 days and misconfigured cloud services are often the culprit. According to 451 Research, nearly half of organizations have experienced a cloud-based data breach or failed audit in the past 12 months. The bad guys gain access through a cloud email service or to an exposed application and use that foothold to penetrate more sensitive and lucrative systems. Further, they are making malware that is smarter and more effective. Beep malware, for example, can operate at massive scale and infect thousands of targets in a short time. This botnet implant malware employs anti-analysis and detection-evasion techniques that make it difficult to detect. Once inside, it enables adversaries to remotely deploy ransomware and other payloads onto compromised systems. Hence data security comes up as the top reason why enterprises are wary of the cloud. They have either been burned personally or know others who have been ravaged by ransomware and other forms of malware.

Too often, security has been implemented as an afterthought. Organizations rushed to the cloud and THEN considered how they could add security measures. Inevitably, gaps appeared and systems became difficult to proof against attacks. It is essential, therefore, to put security front and center when architecting hybrid cloud infrastructure.

2 ENSURE A COMPLIANT CLOUD

Compliance is another barrier to hybrid cloud adoption and success. Many industries face regulatory oversight. They must ensure their systems meet the standards and best practices mandated in various regulations. But compliance is no longer the province of only very large enterprises, public companies or those in verticals such as financial services and insurance. These days, most companies must now demonstrate responsible use of private, sensitive or confidential information and comply with regulations such as the EU's GDPR and California's privacy law. Other regions are following suit. Anyone violating these rules is subject to millions and sometimes billions in fines (Facebook got a 2 billion Euro fine a few months ago from Europe).

It's no surprise that regulation and compliance scored high in the Uptime Institute's survey as reasons why IT managers tended to avoid putting applications into the cloud. Anyone running a hybrid cloud infrastructure or considering adding one, therefore, must take care to ensure that it does not violate the labyrinth of regulations and privacy mandates that now exist across the world. This entails paying close attention to data movement and the various ways cloud systems pass data around as they transact their business.

3 ARCHITECT A COST-EFFICIENT CLOUD

For some, the perception may be that the cloud reduces costs. But dump too much data indiscriminately into the cloud and costs can soon escalate. Further, there are hidden expenses such as fees to take data from the cloud back in house, region to region, as well as the cost of managing a cloud infrastructure that often sprawls due to lack of reasonable limits from on-premises systems to multiple clouds on several continents and providers.

It takes careful planning to build a cost-efficient cloud and manage it to ensure high return on investment. Low cloud costs are underpinned by the right architectural design. In addition, tools are available to help organizations keep a tighter rein on overall cloud costs. A discipline known as FinOps, for example, helps organizations to add control to cloud budgeting, forecasting and even obtain lower cloud costs globally via a procurement centralization strategy.

Bear in mind, too, that the cloud isn't going away. According to Forrester Research, the public cloud services market is expected to grow to $1 trillion worldwide by 2026. Thus, there is little point in mandating an in-house only policy. Business units will invariably go rogue and deploy their own cloud applications. Good economics and better functionality are available in the hybrid cloud if architected and governed intelligently.

4 IDENTIFY THE BEST PLACE FOR WORKLOADS

Some workloads belong in the cloud. Others don't. Hence, we are seeing companies pull data and applications back in house. An Enterprise Strategy Group (ESG) survey found that 60% of companies have repatriated some workloads from the cloud to on-prem. Understand, though, that there is no stopping the unrelenting growth of the cloud. Some workloads are being repatriated to the data center but many more are being sent to the cloud.

What is needed is clear policy on what goes where and an underlying infrastructure with the flexibility to support a hybrid model. Certain workloads or data transfers may have time-sensitive requirements that demand in-house systems to keep latency down to the millisecond or even sub-millisecond level of response. If latency is an issue, keep data in-house served by top-of-the-line equipment and place your systems as close to users as possible. However, few applications require that level of performance. The cloud can ably support most workloads without showing users any noticeable level of latency. Factors such as cost, security, compliance and data privacy should also factor into the discussion of which applications belong in the cloud and which should be retained close at hand.

5 AVOID ARCHITECTURAL COMPLEXITY

The Uptime Institute Survey made it clear that the main barriers to large-scale cloud adoption are security, compliance, cost and return of investment. But a couple of other favors scored high in the survey: architectural complexity, resiliency and lack of in-house cloud skills.

Most clouds evolved organically. The organization added a cloud service, then another and another. Pretty soon, a sprawling Rube Goldberg tangle develops that is difficult to manage and far more expensive than originally envisioned. These clouds, in turn, suffer on two fronts. As they are poorly planned, they lack the resilience and flexibility that modern business demands. Outages are not uncommon. Latency remains a thorn in IT's flesh. Endless troubleshooting must be done to keep the show on the road. In addition, most organizations lack the internal talent to keep up with the traffic generated by cloud infrastructure inefficiency, never mind bring order and simplicity to the cloud.

6 EMBED OBSERVABILITY

With increased complexity comes the need for greater visibility into what is going on within the walls of a cloud environment. Here, it's worth noting that the tools used for observability on prem are often not the same ones used in the public cloud or for SaaS providers. While some can provide amazing visibility into the health, latency and accessibility of public cloud services, others may not be optimized as they should to deliver the required insights across a hybrid infrastructure.

This need for increased observability is giving rise in popularity to Application Performance Management tools (APM) which can help empower organizations with the information they need into application behavior, infrastructure health and user experiences, irrespective of the deployment location. This proactive approach empowers organizations to identify and resolve issues promptly, ensuring the reliability and efficiency of their hybrid cloud deployments. By integrating observability tools, businesses can enhance their agility, mitigate risks and ultimately deliver a seamless and responsive users experience across diverse hybrid cloud environments.

7 ENSURE RESILIENCY

To safeguard the integrity and availability of data within a hybrid cloud environment, it's necessary to apply reliable backup and recovery solutions. Using state-of-the-industry Backup-as-a-Service (BaaS) and Disaster Recovery-as-a-Service (DRaaS) solutions will ensure that hybrid cloud environments are protected with resiliency in the event of accidental deletions, data corruption or system failures. These data resiliency solutions will also deliver recovery readiness in the event of ransomware or other forms of cyberattacks.

While cloud providers may provide resilience for their infrastructure, they don't provide protection for the data retained in the cloud. It's best to apply disciplined practices for a shared responsibility model to protect data across on-premises and cloud infrastructures and leverage a comprehensive strategy for business continuity by enabling the replication, in multiple regions, for reliable recovery of entire applications and data with minimal downtime.

verinext

ARCHITECTING ENTERPRISE CLOUDS WITH PURPOSE

At Verinext, we believe adopting the use of the hybrid cloud should be done with intent and purpose.

True enterprise cloud architecture should be specifically designed to meet the goals of the business it serves, fostering agility and ensuring optimal performance, scalability and efficiency for workloads that span environments. This is where Verinext excels. Verinext has an experienced, multi-disciplinary team of enterprise cloud architects that will help you navigate the conflicting ideals of greater capabilities and simplified operation via infrastructure modernization. We will help you design, implement, and support hybrid infrastructure with automation and management solutions across all platforms – with purpose.

The end result is an integrated, flexible and agile environment that enables businesses to digitally transform effectively. For more information, visit verinext.com.