CIO FROM IDG SPONSORED CONTENT kyndryl

The Best of Both Worlds:
The Case for Harmonizing Public and Private Cloud Platforms

Despite steady growth, public cloud isn't the answer for every industry. For healthcare, financial, and public sector organizations facing compliance regulations, private cloud IaaS is a better option.

ENTERPRISE ADOPTION OF PUBLIC CLOUD continues to leap ahead, with Gartner forecasting global spending on infrastructure as a service (IaaS) to grow nearly 40% this year. But public cloud isn't the answer to every problem, and in some cases, it never will be.

Some regulated industries may never move their mission-critical applications to the public cloud, because of data locality, ownership, privacy, and other requirements. Latency-sensitive applications may also need to stay in an on-premises data center, because of the inherent limitations of long-distance networks.

Public cloud presents particular challenges to regulated industries. Restrictions may apply regarding where data is physically located, who can access it, and how it is governed. Privacy laws apply in some jurisdictions, as do rules about specific forms of encryption and data protection. In addition, there have been numerous recent incidents of data's being inadvertently left in the open due to human errors such as misconfiguring cloud servers or making simple mistakes. Such oversights are among the biggest sources of cloud-based data exposure, accounting for 82% of vulnerabilities analyzed by security software vendor Outpost24.

Despite the excellent reputation of public cloud providers in this area, many financial firms prefer to keep data tightly controlled.

These issues are magnified in global institutions that must comply with a growing slate of privacy and disclosure regulations that are specific to individual countries and even US states.

Adopting cloud infrastructure can help with data residency issues in particular, says Stanley Wood, IBM distinguished engineer and chief technology officer for the company's Kyndryl Private Cloud offerings. "It gives companies the opportunity to have infrastructure in different jurisdictions which are, in many cases, already tailored to support local regulations," he says. In these larger jurisdictions, public cloud often gives companies the tools to comply with local regulations. Private clouds enable organizations to control their data and comply with regulations in more places and at a more granular level.

The public cloud conundrum is particularly relevant to three vertical industries:

Financial services firms are heavily regulated, due to the large amount of confidential customer data they possess. Security is a top concern, and despite the excellent reputation of public cloud providers in this area, many financial firms prefer to keep data tightly controlled. For firms that do business internationally, data residency requirements may dictate that data be kept in certain physical locations. Network speed is also an issue in segments of this market where milliseconds can translate into millions of dollars. On-premises private clouds have the advantage of reducing the latency inherent in transferring data to and from public clouds.

Healthcare companies often use public cloud as a platform for new services such as telehealth, remote patient monitoring, and remote robotic surgery. They also see opportunities in the cloud OpEx model to reduce costs, which is a major issue in the US in particular. Leading private cloud service providers can offer the same cloud OpEx model in hosted or even on-premises private cloud environments. These are among the reasons many healthcare organizations have adopted a hybrid mix of cloud services with public cloud used for customer-facing applications while back-office technologies and latency-sensitive use cases such as patient monitoring remain on-premises.

Healthcare is perhaps the world's most heavily regulated industry, particularly when it comes to patient privacy. Despite the generally strong track record major public cloud providers have achieved in this area, the risk of unintentional data exposure due to human error is a major impediment to moving more workloads to the public cloud.

The public sector is laden with legacy applications and infrastructure that hold agencies and municipalities back from realizing the potential of smart cities and customer-facing applications that are more functional.

A private cloud also provides an additional measure of protection against misconfiguration and other human errors.

Budget-constrained public agencies also see the cloud's promise of reduced capital expenditures as appealing. However, compliance with privacy, disclosure, environmental, and tax regulations is a significant issue in this sector—as is the need to secure data about citizens and businesses. Many legacy applications also can't easily be transformed for cloud platforms.

Private cloud is here to stay

For all these reasons, private clouds will be an essential part of the cloud computing mix for years to come. In addition to providing a scalable, standardized platform with high levels of automation and availability, private cloud platforms create a foundation for modernization, by enabling organizations to outfit and test legacy applications with cloud-native extensions before moving them into public view.

For organizations that are in regulated industries or that deal with sensitive personal information, a private cloud also provides an additional measure of protection against misconfiguration and other human errors that Gartner estimates are the cause of 95% of cloud security failures.

The need to install and administer on-premises infrastructure can be a drain on budget and IT staff, however. Cloud administration requires different skills than those of legacy data centers, making talent acquisition a challenge that hits particularly hard in industries that are budget-constrained.

"Cloud operations tend to be conducted by site reliability engineers who treat infrastructure as code and use a software development approach to management," Wood says. "That's different from traditional data centers, which are typically based on physical infrastructure management."

The managed service approach

A managed service approach can help resolve these issues by transferring management of the private resource to a service provider with a track record of experience in cloud administration. Service providers in this space offer various levels of capability, ranging from advisory services to operating fully Kyndryl Private Cloud with self-service automation and orchestration.

Organizations that need a combination of solutions can choose to transition their on-premises infrastructure to a private cloud model to gain the benefits of elasticity and self-provisioning while creating a foundation for application migration and modernization. Data remains under the organization's control, and staff can be transitioned from low-value infrastructure management to applications that are more strategic for the business.

Managed private cloud has many of the same benefits and conveniences as public cloud.

Managed private cloud has many of the same benefits and conveniences as public cloud, such as elastic scalability, self-service provisioning, automated workload balancing, and OpEx pricing. Data resilience is built in or available as a service, and data and applications can be selectively migrated to the public cloud on a schedule and terms that meet the needs of the customer.

Adding a distributed cloud or local cloud as a service such as IBM Cloud Satellite Infrastructure Service can make private cloud even more compelling, by bringing aspects of public cloud into the data center. That gives organizations a private cloud solution that seamlessly integrates with public cloud infrastructure, providing management from a single pane of glass, platform services, comprehensive visibility into applications, low latency, integrated security, and incremental migration of workloads and data across private and public platforms.

Modernizing applications in Satellite before migrating to public cloud is a great strategy for mitigating application interdependencies that could undermine cloud migration, Wood says. IT organizations often find that legacy applications talk to each other in ways that aren't well understood. When one application moves to public cloud, it can throw the remaining applications into disarray.

"We've helped a lot of clients move to the cloud, and it is not unusual to need to move some things back on-premises because of that problem," he says. "That leaves a bad taste in the application owners' mouth. With distributed cloud, you can modernize parts of the stack in your data center without breaking that affinity to legacy applications. When the entire stack has been modernized, it can be migrated to public cloud all at once."

The bottom line

Enhanced options for Kyndryl Private Cloud,[1] along with distributed cloud, provide an expanded set of services that will meet the needs of more enterprises. In all cases, it's important to put management and operations in the hands of a seasoned services provider such as Kyndryl.

With decades of managed services experience and more than 21,000 clients, Kyndryl is well positioned to deliver Kyndryl Private Cloud as a flexible usage-based consumption model offering a variety of compute, storage, and network services. Customers can specify their choice of products, from the operating system level to the hypervisor and through the orchestration platform. Kyndryl also offers a wide variety of in-house talent, deployed across 115 countries and having delivered for hundreds of clients for years at scale.

For more information on Kyndryl Private Cloud, visit https://bit.ly/kyndrylprivatecloud.

[1] Kyndryl was spun-off of IBM IT infrastructure services in 2021. Kyndryl's global base of customers includes 75 of the Fortune 100 companies. With 88,449 skilled professionals operating from over 100 countries, Kyndryl is committed to the success of our customers, collaborating with them and helping them to realize their ambitions. .