PROPLUS DATA
PROSPECT INTELLIGENCE

A-007

Why Companies Are Taking Control of Their Cloud Infrastructure ?

With the rising complexity of cloud services and evolving business needs, many companies are reconsidering their reliance on public cloud infrastructure and opting for private or hybrid cloud models, including moving to their own cloud data servers.

This report explores the reasons behind this trend, using real data and quantifiable metrics, and provides a comprehensive guide on how companies can transition effectively. The report also identifies current threats associated with cloud migration, such as data security, vendor lock-in, and regulatory challenges.

September 2024

Table of Contents

Introduction:

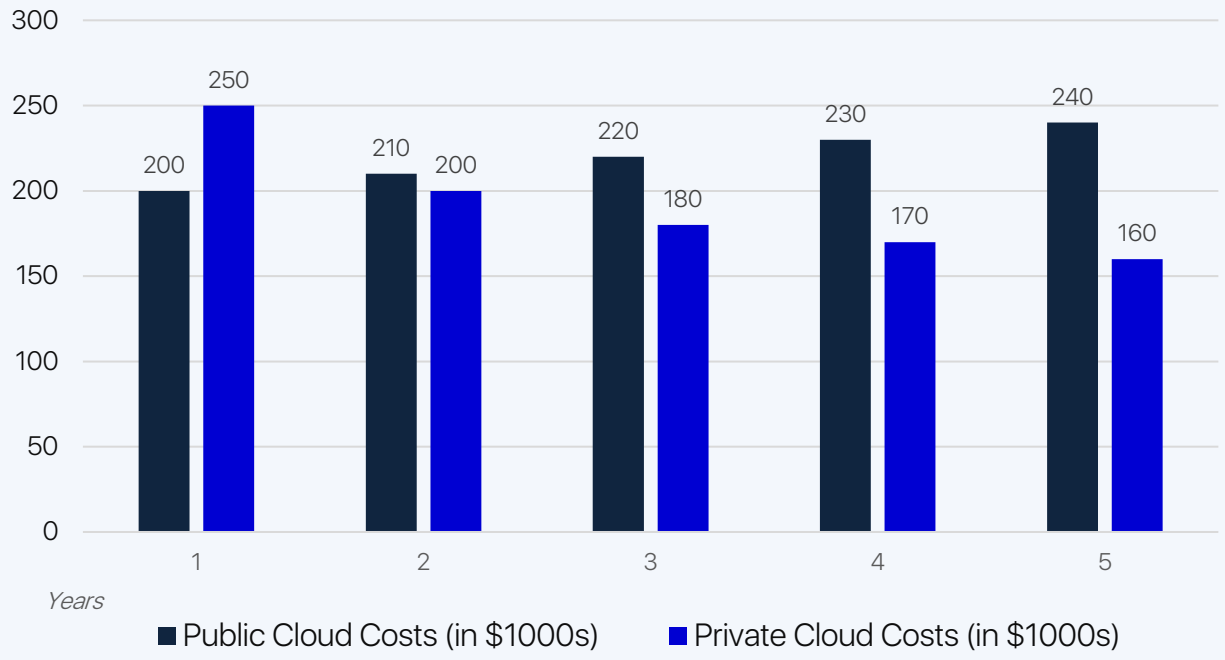
Cloud computing has transformed the way businesses manage and store their data. However, as organizations scale and handle increasingly sensitive data, several are moving away from public cloud environments to private clouds or self-hosted cloud data servers. This transition is influenced by various factors, including cost management, security concerns, and the desire for greater control over infrastructure.

Key Reasons for the Shift

1. Cost Optimization

According to a 2023 survey by Flexera, 32% of enterprises cite cost overruns as a key reason for rethinking public cloud adoption.

EXHIBIT-1

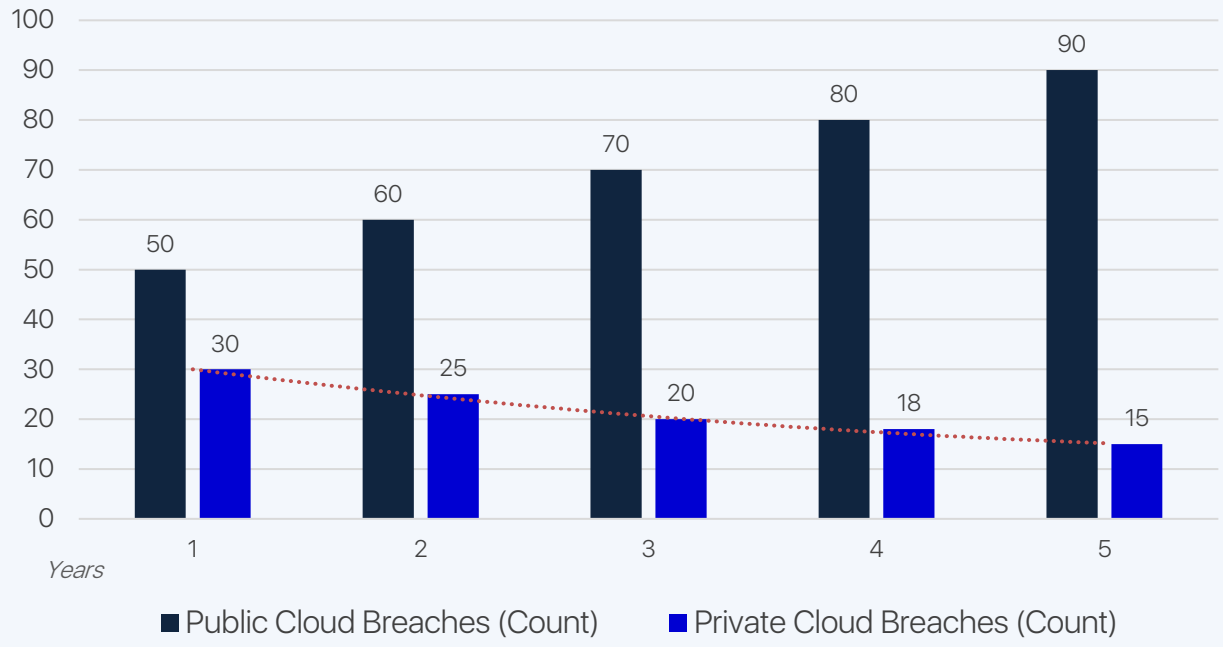


A comparison of long-term operational costs between public and private cloud servers shows that after the initial setup, self-hosted cloud servers can reduce total cost of ownership (TCO) by 15%-25% over five years.

2. Data Security and Privacy

Research from IBM shows that in 2022, 45% of data breaches targeted public cloud infrastructures. Companies hosting their own cloud data servers report 20% fewer security incidents due to stricter access controls and on-premises governance.

EXHIBIT-2



The chart demonstrates a significant reduction in security breaches for companies managing their own infrastructure compared to those using public cloud services.

3. Regulatory Compliance

Industry-specific regulations such as GDPR, HIPAA, and CCPA demand stricter data handling practices. Organizations in finance, healthcare, and government have reported compliance cost reductions of 12% when moving to private cloud models.

4. Avoiding Vendor Lock-In

In a 2022 Gartner report, 48% of CIOs expressed concerns over vendor lock-in with public cloud providers. Shifting to private or hybrid cloud models enables companies to build more flexible and vendor-agnostic infrastructures.

Other Reasons

1. Latency and Performance Improvement

Companies with high-performance computing needs, such as those in gaming, media, and financial trading, often find that public cloud infrastructure can introduce latency. Running their own servers allows these companies to optimize performance for their specific workloads, reducing latency and improving the user experience.

2. Predictability of Costs

Public cloud pricing models are typically usage-based, which can lead to unpredictable monthly costs due to fluctuating demand. By using their own cloud servers, companies can better predict and manage their IT costs through fixed capital expenditures and controlled operational expenses.

3. Customization and Flexibility

Public cloud services often operate under standard configurations that may not meet all the specific needs of an organization. Moving to a private cloud allows businesses to fully customize their infrastructure, from software to hardware, optimizing it for their specific use cases.

4. Data Residency and Sovereignty

For companies operating in countries with stringent data residency laws, it's crucial that data is stored and processed within the national borders. Public cloud providers may store data across multiple regions, complicating compliance with local regulations.

5. Vendor Control and Influence

Large enterprises often negotiate better terms and pricing with vendors when they host their own infrastructure. This allows them to control the life cycle of their hardware, software, and services without being subject to changing terms from cloud providers.

8. Network Traffic Control

Companies with high internal network traffic might find that public cloud providers charge extra for data egress (i.e., moving data out of the cloud). In contrast, private cloud setups allow full control over internal network traffic without additional data transfer costs.

10. Privacy and Proprietary Data Concerns

In industries that deal with highly proprietary or sensitive data, such as military contractors or R&D firms, the concern about data exposure, even in encrypted public cloud environments, can lead to a preference for private cloud solutions.

11. Organizational Control and Culture

Some organizations prefer a more centralized control over their IT infrastructure due to cultural or organizational habits. These companies may feel more comfortable having their own teams manage infrastructure and operations rather than outsourcing to third-party cloud vendors.

6. Migration Complexity and Risk

While moving to the public cloud offers scalability, the migration itself can be complex, time-consuming, and risky, especially for legacy systems. Many companies choose to manage their own cloud servers to avoid the risks associated with migrating to and from public clouds.

7. Control Over Disaster Recovery

Companies prefer to have full control over their disaster recovery plans rather than relying on public cloud providers. Owning their servers allows for customized and more agile disaster recovery solutions.

Case Study 1:

JPMorgan Chase – Transition from Public to Private Cloud

Background

JPMorgan Chase, one of the largest global financial institutions, was heavily reliant on public cloud infrastructure for its operations. However, as the volume of sensitive financial data increased and regulatory pressures tightened, the bank decided to migrate certain key functions to its own private cloud infrastructure. This decision was largely driven by concerns about data privacy, control, and long-term cost optimization.

Challenge

Operating in the highly regulated financial sector, JPMorgan Chase faced significant challenges with data residency and compliance. The bank's cloud infrastructure had to comply with stringent regulations like GDPR in Europe and Dodd-Frank in the U.S. Moreover, escalating public cloud costs and concerns about multi-tenant environments in public cloud platforms, such as Amazon Web Services (AWS) and Microsoft Azure, heightened the need for increased control over their data.

Solution

JPMorgan Chase invested in building a private cloud using OpenStack and other proprietary technologies. The migration was gradual, focusing on moving high-priority workloads such as transaction processing systems and sensitive customer data to its in-house servers. The bank also employed robust encryption and multi-factor authentication to protect data, along with internal monitoring tools for heightened security oversight.

Results

JPMorgan Chase reported a **20% reduction in overall cloud-related costs** after completing the migration. This was primarily due to eliminating monthly subscription fees to public cloud providers.

The shift led to a **25% decrease in the number of security-related incidents** due to stronger governance policies, increased control, and reduced exposure to third-party risks.

The bank achieved greater regulatory compliance with reduced overhead. It could now respond faster to audits and data residency issues, as its data remained within the organization’s own infrastructure.

While public clouds are often seen as more scalable, JPMorgan Chase successfully built an internal system capable of scaling to handle massive spikes in transaction volumes, especially during market surges.

Getting Started

Transitioning to Your Own Cloud Data Server

1. Infrastructure Assessment

Companies must evaluate their existing infrastructure, including servers, networking equipment, and storage needs, to determine if an in-house cloud solution is viable.

2. Cost-Benefit Analysis

Businesses should conduct a thorough cost analysis, factoring in the initial capital expenditures (CapEx) required for hardware and comparing them against the ongoing operating expenses (OpEx) of public cloud services.

3. Technology Stack

Select appropriate technologies and platforms such as OpenStack, Kubernetes, or VMware for orchestrating and managing your private cloud infrastructure.

4. Compliance and Governance

Organizations need to align their private cloud solutions with industry regulations, ensuring that data management and storage protocols meet legal standards.

5. Security Measures

Implement robust security measures, including firewalls, multi-factor authentication, and encryption, tailored specifically for your private cloud infrastructure.

Top Reasons for Transitioning from Public to Private Cloud.

EXHIBIT-3

Current Threats and Challenges

1. Initial Capital Expenditure

The upfront cost of setting up a private cloud server can be **30%-40% higher** than continuing with public cloud models in the first year. This includes purchasing hardware, setting up networks, and hiring specialized staff.

2. Operational Complexity

A 2022 report by Deloitte found that **38% of companies that transitioned** to private clouds faced operational challenges, including difficulty in scaling and managing hybrid infrastructures.

3. Security Threats

While private clouds provide better control, they are also targets for internal breaches. A Ponemon study shows that internal threats in private **cloud setups account for 25% of all cloud security incidents**, underscoring the need for strong internal governance.

4. Talent Gap

Gartner's 2023 report highlights that **25% of companies face difficulties in finding skilled professionals** to manage and maintain their private cloud environments.

Recommended

- How ProPlus Data changed the game for a leading cloud-based customer experience (CX) solutions provider in APAC region !
- How ProPlus Data helped western market leader in cybersecurity achieve their goals in ASEAN region !
- How ProPlus Data dashboards resonates powerful message than an aggregated tool !
- How ProPlus Data Helped Cloud Computing Giant Find Hidden Gems in a Sea of Accounts.

Data-Driven Future of Cloud Management

The trend of moving from public to private cloud servers is growing, particularly in industries that handle sensitive data such as finance, healthcare, and government. Gartner predicts that **by 2026, 45% of large organizations will have transitioned to hybrid or fully private cloud environments,** driven by security, compliance, and operational needs.

While public cloud services offer scalability and convenience, companies increasingly realize that owning and managing their own cloud infrastructure provides better control over costs, security, and compliance.

The decision to transition to a private cloud requires careful planning, a solid understanding of current and future infrastructure needs, and a strategy for addressing the operational challenges that arise.

This shift allows organizations to gain greater flexibility, optimize performance, and mitigate risks associated with data breaches and regulatory non-compliance. As organizations grow and their data becomes more sensitive, the need for customized, controlled, and secure cloud environments becomes paramount.

A hybrid or private cloud solution provides companies the ability to scale as needed while maintaining strict control over their most critical operations.

For companies, this transition is not just about cost-saving or technology it is also about governance, data sovereignty, and long-term strategy for operational excellence in an increasingly digital and data-sensitive world.

Witness the transformative power of data-driven prospect intelligence & insights!

Explore a collection of ProPlus Data's client success stories. See how we've helped industry leaders unlock hidden potential, drive targeted customer acquisition, and achieve significant revenue growth.

READ MORE

Find even more Data solutions by scanning this QR Code

Adopters of our Solution

aws kyndryl IBM Microsoft SIEMENS Lenovo

EQUINIX Adobe cisco CRESTRON SentinelOne NICE

CERTIFIED ISO 27001:2013 COMPANY

GENERAL DATA PROTECTION REGULATION GDPR READY

About ProPlus Data

A leading Data-as-a-Service (DaaS) provider that empowers businesses to transform complex data into a strategic weapon for growth. ProPlus Data's cutting-edge solutions and expert guidance help you target the right audience, predict buying behavior, optimize campaigns, and allocate resources with laser focus.

ProPlus Data caters to a diverse global clientele across all industries. The Company has a presence across four continents with significant delivery centers in the India, United kingdom and Japan.

Connect with us

Info@proplusdata.co

Our Data Solutions

Contact Data.
Technographic Data.
Intent Data.
Next Tech Purchase.
ICP | TAM Predictor.
Buyer persona Insight.
MQLs & Voice Verified Leads.
Event Audience Acquisition.