Understanding the BYOC Deployment Model

How does the Bring Your Own Cloud (BYOC) model achieve data privacy and sovereignty of self-hosting with the ease and scalability of fully managed services?

Dunith Danushka · Follow
Published in Tributary Data
6 min read · Sep 26, 2023

Photo by Zbynek Burival on Unsplash

In today's fast-paced digital landscape, maintaining data privacy within an organization is paramount. Data breaches have far-reaching consequences, both

financially and reputationally. According to statistics from the Ponemon Institute, the average cost of a data breach in 2020 was $3.86 million, and the average number of records exposed per breach was 25,575. These incidents result in financial losses, erode customer trust, and can lead to legal and regulatory penalties.

That presents organizations with a dynamic challenge: how to harness the boundless potential of cloud computing while maintaining control over their data, infrastructure, and costs. Enter "**Bring Your Own Cloud" (BYOC)**, a concept that empowers organizations to tailor their cloud strategies to their unique needs.

In this article, I give you a general introduction to the BYOC deployment model, covering its very foundations, the reason for its existence, its operational model, and some practical use cases. Please note that this is not tied to a specific technology domain. So, feel free to study the basics and apply it to your own domain.

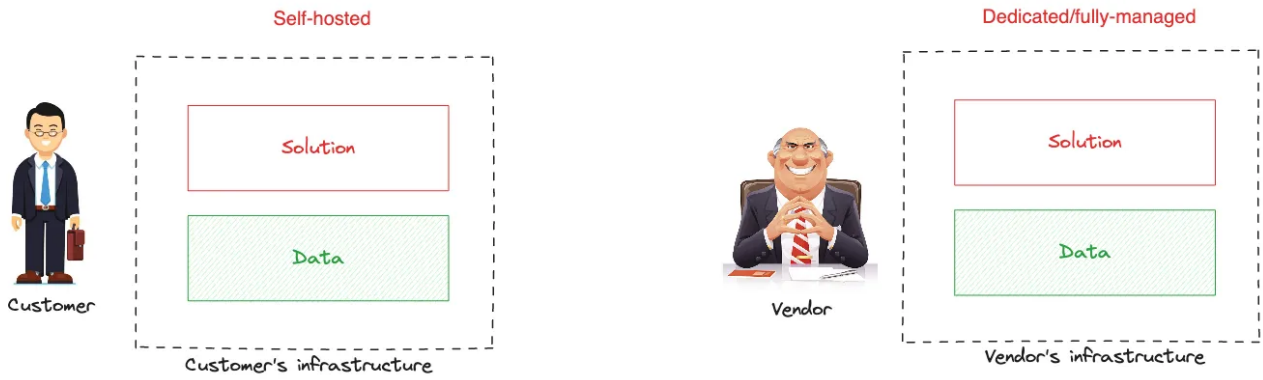
What is BYOC?

Suppose you represent an organization that wants to buy a technology solution that solves a business problem. The solution can be anything that works with data, such as a database, a message broker, or a data analytics system, designed, engineered, and delivered to you by a technology vendor.

When it comes to solution deployment, there are several options.

- **Self-hosted deployment** — Buy the solution distribution from the vendor, install and manage it on your own hardware infrastructure — on-premise data center or cloud.
- **Fully-managed/dedicated deployment** — The solution is provisioned and managed in the vendor's cloud infrastructure.

Both models have their pros and cons. Typically, a self-hosted deployment requires a significant upfront investment for hardware, and you're responsible for planning the necessary infrastructure and human resources to keep everything up and running. However, it offers full control over your data, making it an attractive option for organizations focused on data privacy, security, and sovereignty.

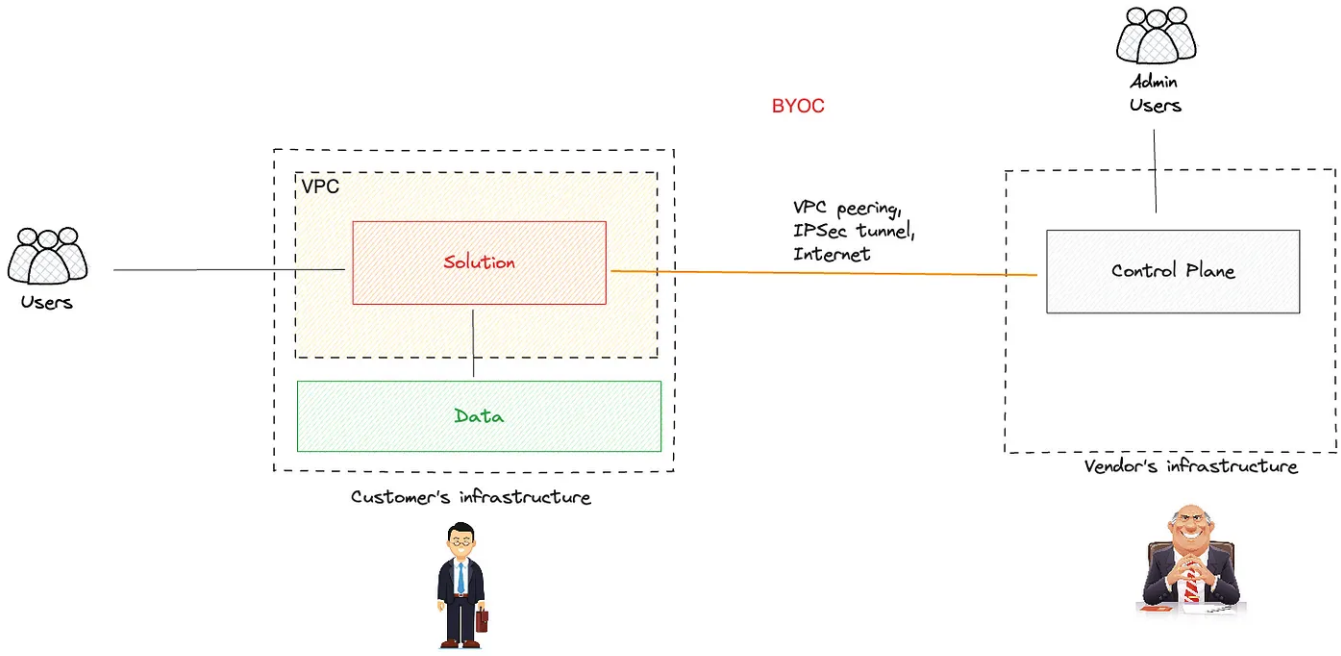


Self-hosted and Fully managed deployment models

Conversely, a fully managed deployment is where everything is managed for you by the vendor in the vendor's cloud. It's like a one-stop-shop where setup, monitoring, maintenance, and scaling are all taken care of. However, not every organization trusts third parties with their data, and the lack of transparency, access control, and residency can be a major deal-breaker.

So, we need to find a compromise between these two. That is where the Bring Your Own Cloud (BYOC) model shines.

In BYOC, the vendor provisions the solution in your cloud infrastructure, typically inside a VPC you created for them and manages it remotely. It's like having the best of both worlds — your data never leaves your cloud while enjoying the benefit of offloading operations and maintenance to the vendor.



BYOC in a nutshell

Why BYOC?

The primary motivation for organizations to consider BYOC is data sovereignty, enabling organizations to have greater control over the physical location and storage of their data. Data sovereignty refers to the concept that data is subject to the laws and regulations of the country or region in which it is physically located.

BYOC offers organizations a choice of cloud region, allowing them to select specific cloud regions or data centers in the cloud provider of their preference. That ensures that their data is stored within the geographic boundaries that align with their data sovereignty requirements. For example, if a country has strict data residency laws, BYOC enables organizations to store data within that country's borders.

Apart from that, BYOC also offers the following benefits:

- **Control and Customization**: BYOC empowers users with greater control over their cloud infrastructure. They can configure, customize, and manage their cloud environment according to their specific requirements. This level of control is particularly beneficial for organizations with unique security, regulatory, or performance needs.
- **Data Portability**: BYOC allows users to move their data and workloads more easily between different cloud providers or environments. This flexibility can be advantageous when data sovereignty, compliance, or cost optimization are crucial considerations.
- **Vendor Lock-In Mitigation**: One of the primary motivations behind BYOC is to reduce or mitigate vendor lock-in. When organizations use a single cloud provider for all their services, they can become dependent on that provider's technologies and pricing structures. BYOC can help avoid this dependency by diversifying cloud providers or adopting open standards.
- **Cost Optimization**: Users can optimize costs by selecting the most cost-effective cloud resources and services from various providers. They can also leverage spot instances, reserved instances, or other pricing models that best fit their budget.

BYOC operational model

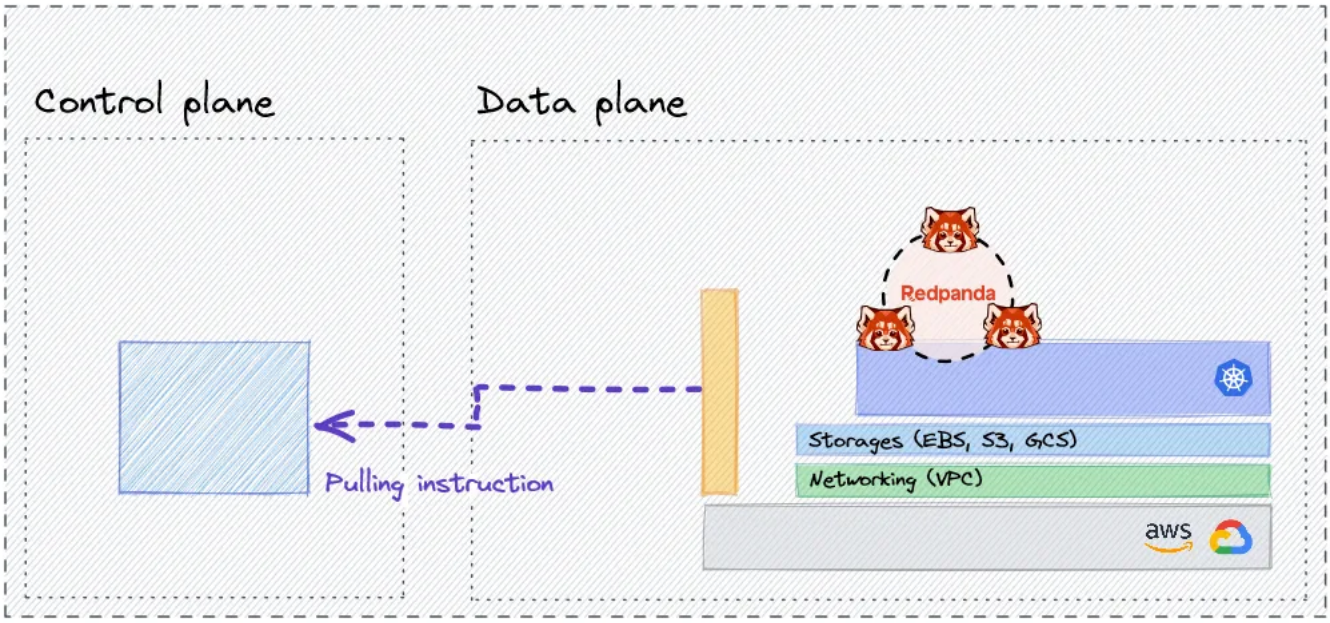
The benefits of BYOC are impressive from a business standpoint. But, a technologist like me would explore BYOC under the covers to understand how it works.

In the BYOC operational model, the terms "**data plane**" and "**control plane**" are often used to describe distinct architectural functions. These terms are also

commonly associated with networking and cloud computing in general. In general, the control plane is responsible for managing, governance, and orchestrating resources and policies, while the data plane handles the actual processing, analysis, and storage of data.

The nice thing with BYOC is that it provisions the data plane within the customer's VPC, granting them full control over underlying storage, computing, and networking infrastructure. The control plane is typically provisioned in the vendor's cloud and connected with the data plane via an IPSec tunnel or over the public Internet.

The data plane has an agent that pulls instructions from the control plane and configures the cloud infrastructure accordingly. It also takes care of the bootstrapping of the data plane. The pull approach is preferred over the push approach as it ensures the control plane has no exposed credentials or excessive permissions on the vendor side. Lastly, the agent doesn't collect or distribute any metrics since the metrics are all collected via the cloud provider's API endpoint.



The BYOC operational model — Redpanda deployment for a reference. Image credits — Christina Lin

Administrative users of the organization are given access to the control plane to perform tasks like user account management, policy setting, and accessing metrics related to the solution.

BYOC use cases and existing solutions

BYOC model is increasingly becoming popular among organizations that ingest, store, and process customer data.

The financial industry frequently employs BYOC to address stringent regulatory requirements and data privacy concerns. It allows financial institutions to choose the most secure and compliant cloud solutions while maintaining control over sensitive customer data. Healthcare organizations and life sciences companies use BYOC to ensure compliance with healthcare regulations like HIPAA. They can store and process patient data in compliance with data sovereignty laws and strict security requirements. Finally, the government and public sector agencies often use BYOC to maintain data sovereignty and adhere to government-specific compliance regulations. This approach allows them to leverage public or private cloud resources while retaining control over sensitive data.

Apart from that, technology companies and startups often use BYOC to have more control over their infrastructure and to leverage different cloud providers for specific services. This approach allows them to optimize costs, maintain flexibility, and meet the performance demands of their products and services.

If we take the data infrastructure market as an example, several vendors already offer BYOC support as a core product offering.

Redpanda Data BYOC: Enables you to provision a Redpanda cluster within your VPC, stream data to it, and manage it by the Redpanda team.

StarTree Cloud: Allows you to provision an Apache Pinot cluster within your VPC.

Decodable — Allows you to build streaming data pipelines with Apache Flink.

Data Streaming | Data Engineering | Data