Title tag: Cloud Vendor Lock-In | Transcenda
Meta description: Learn what cloud and vendor lock-in can mean for your digital infrastructure and find out how to mitigate the possible disruption of these issues.

Navigating Cloud and Vendor Lock-In When Designing Data Infrastructure

When designing digital infrastructure to manage data or other essential resources, companies today turn to third-party vendors for cloud resources and managed service offerings. This is a standard and effective way to build a business's capabilities, but it comes with risk — the organization can become overly dependent on service providers or cloud vendors.

This effect is known as lock-in, and it can have serious consequences, especially when a business feels the need to change its infrastructure approach and finds itself trapped by technical dependencies.

Some level of lock-in is likely inevitable due to the central role cloud platforms and managed services play for companies. It's also worth noting that staying with the same vendors isn't wholly negative and there are advantages to relying on a few key technologies. It is important, however, to be aware of the full picture and plan around the risk of excessive lock-in.

What Are the Effects of Cloud and Vendor Lock-In?

Forming a clear-eyed strategy to manage the risk of cloud and vendor lock-in at your own organization is easier when you know both the positive impact of vendor loyalty and the downsides that come with excessive lock-in.

The pros of deeply integrating with vendors' tools for cloud infrastructure and managed services include:

- **Efficiency:** Heavy use of managed services and reliance on third-party cloud vendors can come with operational efficiency gains, largely because work that would go to in-house experts remains with the third party. Ease of management, enhanced automation and lower skill demands are a few of the factors at play.
- **Reliability:** Using third-party resources for key data infrastructure elements may lead to improved uptime, data durability and disaster recovery ability. This is due to vendors' capabilities outstripping what's possible with internal resources.
- **Scalability:** Using outside cloud resources or managed services allows businesses to easily increase or decrease their resource access as needed, without the capital expenses associated with in-house infrastructure.
- **Access to features:** Vendors are always adding new features and capabilities to their products, which means companies that invest deeply in third-party infrastructure gain access to these advanced features.

- **Predictable costs:** Spending on cloud resources and managed services is a month-to-month capital expenditure. This makes it easier to plan and predict than the operational expenditure model built around making large upfront investments for in-house hardware and software.

While those notable advantages can encourage your business to make heavy use of cloud resources and managed services, it's important to understand the downsides of becoming too locked in with vendors or services.

Notable downsides of vendor and cloud lock-in include:

- **Difficult, lengthy migration:** Perhaps the most common and notable issue associated with vendor lock-in is the difficulty of choosing a new cloud or managed service provider. Becoming too dependent on one external vendor's offerings means that no matter the reason for a proposed switch — savings, the ability to save money or another motive — the move takes excessive time and effort.
- **High migration costs:** In addition to hard, labor-intensive migration processes, switching vendors in a heavy lock-in situation means spending money. Recreating the same level of performance on the new system, safely transferring all the data and meeting other requirements becomes costly when a company is deeply invested in one vendor's offerings.
- **Compliance issues:** Some data storage projects come with special stipulations. For example, if your organization is tasked with keeping health care data or personally identifiable financial information, you may need to use fully controlled on-premises storage for governance reasons. Third-party cloud resources and services would not help in these cases, or make it very expensive to do so. Niche add-ons come at a higher cost.
- **Susceptibility to product changes or shutdowns:** If vendors decide to make significant changes to a service offering — or to shut it down entirely — heavily locked-in users can find themselves scrambling for answers. If key processes are bound up with the vendor's technology, those may break, causing major functionality issues.
- **Security liability:** Security threats affecting major cloud resources or managed services also affect companies that have committed to using those offerings. An unpatched vulnerability or known issue with a third-party service can be beyond an internal IT team's ability to fix or mitigate, so users must wait for the vendor to take action.

These potential issues show the importance of thinking about lock-in during the early days of purchasing cloud resources or third-party services. You should inspect the balance between upsides and downsides for any offerings you pursue, and make sure your company is receiving an overall positive experience.

What Are Some Risk Factors Leading to Lock-In?

There are a few key factors to monitor when choosing to work with cloud vendors and add managed services to your company's technology stack. By paying attention to these variables, you can minimize the risk of excessive vendor and service lock-in, giving yourself a simpler path forward.

You should make sure to monitor:

- **Volume of data stored:** The more information a company commits to a third-party cloud or service offering, the harder it will be to move or extract that data, and thus the greater the risk of lock-in. This issue can quickly snowball when companies aren't selective about what data they retain and store. This can be seen in cloud providers having no ingress fees to data, only hosting charges — but then begin charging egress fees to download data following a very small free-tier amount, which can be as little as 1GB.
- **Depth of integration:** Creating multiple points of connection and dependencies between third-party services and a company's own systems is a major potential source of lock-in. In many cases, these integrations are functionally beneficial and thus worth pursuing, but it's also worth knowing the risks.
- **Use of proprietary vendor features:** Using technologies and tools that are specific to one vendor, rather than open standards, leads to complications when changing away from that provider. Machine learning, for example, is a highly proprietary field, and often requires a rewrite to pivot away from a given provider. As with integrations, taking advantage of these features can be advantageous, but it should be done with knowledge of the possible consequences.
- **Length of service usage:** The longer a business engages with a vendor, the more entwined they will likely become. In the natural course of working with a service provider, the number of connections between a company's in-house systems and the third-party offerings will increase, increasing lock-in and making a change more difficult.

Some of these risk factors are inevitable, and others come with valuable benefits for the company buying in. The point is not to avoid these issues at all costs, but rather to be aware of them and make sure you're comfortable with the amount of vendor lock-in you're incurring.

What Are Some Examples of Vendor Lock-In's Impact?

When businesses end up with an excessive amount of vendor lock-in, the results can bring both short- and long-term difficulties in terms of IT management and overall performance. Avoiding these outcomes is the primary reason for planning around the risk of lock-in.

Examples of these problems include:

- **Sudden cost increases:** Managed services and cloud products can increase in price for several reasons. For instance, an external vendor that has recently gone public may be seeking more income to please shareholders. These rate hikes can cause budgetary issues for locked-in users who can't easily renegotiate their contracts or change vendors.
- **Product shutdowns:** Managed services and cloud offerings occasionally shutter, meaning that companies too locked into their ecosystems will be forced into a complex, costly

migration with little warning. This is especially likely when a product is acquired by a new owner.

- **Version lag in managed services:** It's common for managed services offerings to be a few versions behind when compared to the software companies can run locally. Users of the managed offering will therefore miss out on using the latest patches and features while they're still new.
- **Need for compliance:** Businesses locked into public cloud and managed services contracts may find their chosen providers don't have the necessary credentials to comply with regulations governing specific kinds of data. These organizations have to work hard to build alternative systems that can provide this capability.

How Can Your Business Mitigate the Risk of Vendor Lock-In?

Considering the consequences of excessive lock-in, as well as the potential benefits and the inevitability of some level of dependence, you can devise strategies that will help you select a suitable range of services and infrastructure. Best practices include:

- **Relying on open formats and industry standards:** By avoiding proprietary options wherever possible, you're giving yourself an easier job when it's time for cloud migration. If your IT network is replicable on another provider's infrastructure, the level of lock-in is low.
- **Constantly evaluating alternatives:** best practices around data storage and other key IT functions may change considerably over the years. By consistently monitoring the industry, you may find valuable new services before becoming too locked into your current solutions.
- **Monitoring costs and usage:** Avoiding an "auto-pilot" approach to storing data in the cloud and ignoring the way you use and pay for cloud services and infrastructure, you can sidestep issues such as placing large volumes of unnecessary content into cloud storage.
- **Ensuring data is exportable and replicable:** If you can explicitly manage your data in an exportable form, you're ideally prepared to move to a new external vendor at any time. This flexibility is the antithesis of excessive lock-in.

How Can an Expert Engagement Help with Vendor Lock-In Issues?

Sometimes, the best way to mitigate vendor lock-in is to seek assistance. Expert consultants and third-party contributors can help at a number of points, including when you're designing infrastructure and when you're undergoing a migration to a new service.

Transcenda's experts have worked with companies of all sizes and descriptions and can draw on their industry knowledge to suggest approaches that will minimize unnecessary cloud vendor lock-in and mitigate the related risk.

Contact us to learn how your business can benefit.