Achieving Data Layer Agility and Protection

Critical Factors to Consider

storagefabric.io

Contents

https://storagefabric.io
info@storagefabric.io
+1 877 - 7- CIPHER

virtalica

virtalica

Achieving Data Layer Agility and Protection

Critical Factors to Consider

Executive Summary

Modern enterprises comprise a plethora of systems and workloads inherited over time by choice, necessity or sheer inertia. It is not unusual to have tens of on-prem storage solutions including multiple SAN/NAS deployments, last generation object storage vendors, and various other technologies for block and file system data.

These solutions need to be separately integrated into provisioning frameworks, auditing, logging, costing and charge-back, identity management, policy enforcement, and dozens of other critical systems before entering production. It is not unusual to have pre-production cycles exceeding 18-24 months.

Once deployed, this interaction spaghetti results in often unreasonably large overheads and burdens saddled squarely upon enterprise clients needing these services. As a result, provisioning a simple storage volume in a large enterprise can take over 3 weeks!

To address these challenges, emergent smart agile architectures and ways of thinking are empowered by next generation storage technologies and cloud. However, to achieve agility for decades-long horizon designs, multiple critical factors need to be addressed.

To compile this brief, we drew from our experience working with top 10 global financials, Fortune 500 companies, various government agencies and the DoD.

Vendor Lock-In

By far one of the most important factors, the true costs of lock-in are often overlooked and not straightforward: loss of opportunity, loss of leverage and negotiation power (to benefit from the invariably falling costs of Moore's Law driven infrastructure), and the cost of entertaining alternative options – which now are inevitably coming with the significant price tag of having to migrate and also possibly rewrite hundreds of locked-in applications. *Agility inherently requires minimizing lock-in.*

Cloud (Private/Hybrid/Public)

Enterprises increasingly embark on “move to the cloud” mandates driven by promises of increased agility, pay-as-you-go, eliminating large on-prem footprint including staff, etc.

Unfortunately, not all cloud migrations turn out so well. Enterprises often find that many applications end up costing more when outsourced. Further, even when cost benefits pan out, the significant vendor lock-in costs, new associated cyber security vulnerabilities, increased risk surfaces, the architectural challenges of integrating into existing systems (identities, key management, provisioning, etc), and generally scaling out are all non-trivial.

Importantly, the fabric of interacting workloads often spans multiple private, hybrid and public clouds. *Secure and consistent access to data residing on-prem and in-cloud from both on-prem and in-cloud vantage points is critical.*

Cyber Security

Cyber Security is one of the leading challenges of architecting systems involving data and cloud. Unfortunately, as the numerous attacks and breaches [30-39] [42] [44] in the very recent past have shown, public and private clouds constitute a spectacularly attractive target for

global, sometimes nation-state, adversaries with virtually unlimited resources.

Handling these vulnerabilities requires making critical architectural decisions impacting the cyber posture of the enterprise. These include:

Decision #1. Where to place the **protection boundary: enterprise or provider-side?** The real question: what is the *acceptable impact of a provider-side compromise* on the enterprise?

Decision #2. **Who enforces protection**: enterprise data clients or the infrastructure? How cyber-sophisticated are enterprise clients. The real question: what is the acceptable impact of user mistakes on the enterprise?

Further, **conflicting regulation** in different jurisdictions, if not carefully handled, places the enterprise in the untenable position of violating at least some regulatory frameworks. For example, under the Cloud Act, American authorities get access to stored data, regardless of where it is housed. Yet, GDPR contains requirements directly conflicting with these provisions. As a result, in the absence of client-side encryption and maintaining enterprise control (Decision #1) it is simply not possible to use public clouds without being in violation.

Agile cyber-secure architectures *adopt a zero-trust posture where protection boundaries are enterprise-side and enterprise clients do not need to be relied upon for policy enforcement.*

Legacy Systems

Application-driven lock-in and the inertia inherent in large enterprises virtually ensure existing systems may linger around for years, possibly decades. *Agility requires seamless integration and migration capabilities.*

Performance

Geography-spanning infrastructures are often bottlenecked by underlying network fabrics, and performance is usually vantage-point relative. Cloud-hosted applications running in the same East Coast cloud may experience dramatically different numbers than those running on the West Coast or on-prem. Overall, even here, the laws of physics (speed of light, fiber capacity) rule bandwidth and latency.

Yet, while applications vary wildly in their bandwidth and latency sensitivities, **consistency of access and performance is almost always important**. This however is not easy to achieve across numerous vantage points not only because of the underlying networking fabric but often also because of a lack of flexible unifying technology.

Agile unifying designs deploy smartly provisioned abstraction layers to ensure access consistency and improve performance.

Cost and Footprint

Reducing footprint and costs by direct data migration into the cloud may seem straight-forward at first glance. Smart architectures however need to avoid significant potential performance sacrifices and costs. For example, the *cost* of accessing a remote bit may be comparable to the cost of redundantly storing that bit for a month in the cloud. This is not only market-driven but mainly because laying fiber involves digging trenches and actual rubber hitting asphalt and these costs decrease much slower than Moore's law.

Further, the need to access data segments consistently from multiple vantage points (including on prem) requires a careful design using appropriate technology. Optimizing costs to reach an overall 2-5c/GB and *achieving consistent high performance without a high footprint requires specialized workload-tuned transactional and caching technology* judiciously deployed enterprise-wide.

Resilience and Integrity

As increasingly larger amounts of enterprise data are held by third parties, it is critical to consider end-to-end integrity as a first-class citizen and proactively enforce and verify it.

For large peta and exabyte sized data sets, factors ranging from software bugs to cosmic radiation inevitably lead to corruption that is often not detected by basic data checksums.

And, while multi-store redundancy (often provided by clouds) goes a long way in guaranteeing recoverability, it does not ensure integrity. We have **discovered numerous critical data corruption bugs in major on**

prem and cloud providers that went unnoticed for years until advanced end-to-end integrity mechanisms were deployed.

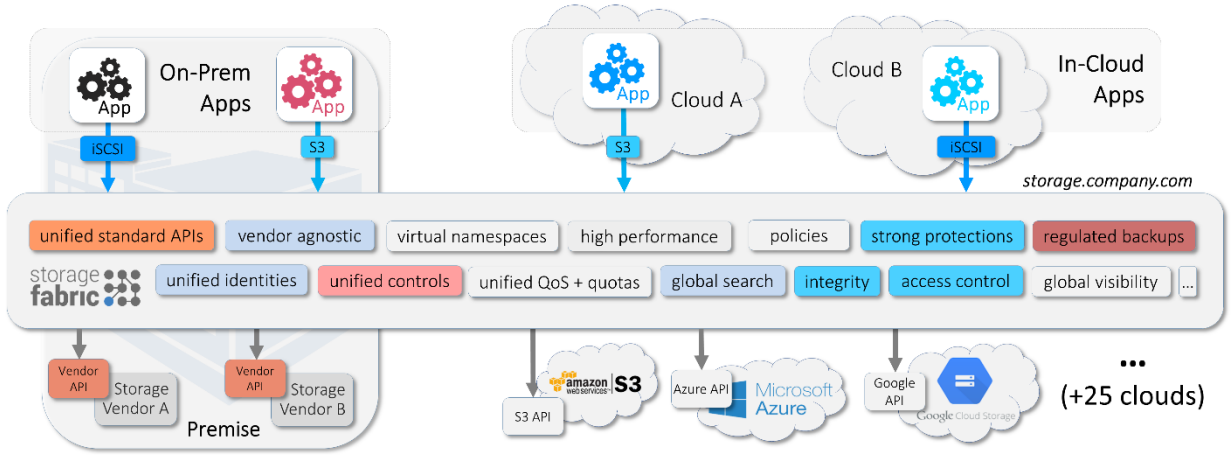
Another obvious yet often overlooked key element is the ability to **operate and fail gracefully** during downtimes. This requires avoiding monoculture architectures and embracing multi-cloud. Because despite the excellent published uptime numbers cloud downtimes happen and when they do, **monoculture architectures** – especially where multiple interacting workloads are hosted on the same platform – can **fail catastrophically**. A major storage service week-long downtime brought thousands of customers to a halt.

Agility requires multi-provider, resilient designs.

Current State

The state of the art is maybe best illustrated by several key facts that emerged from our interactions with F100 enterprises:

- On-prem storage is costlier than cloud but careful designs are needed to truly benefit.
- Footprint is growing, expensive, and not straightforward to securely migrate.
- On-prem vendor projects routinely end up costing more than originally proposed.
- Vendors use risky, expensive and complex transition/onboarding to increase lock-in.
- Storage operations are relatively expensive, and solutions fail expected ROI.
- Scaling globally is non-trivial.
- Most vendors and clouds don't encourage you to use competing services.
- Network traffic is very expensive.
- Once a vendor is chosen after a long and protracted negotiation, the enterprise is very likely locked in for too long.
- Clouds offer deep (50%+) enterprise discounts if viable competition is enabled by multi-cloud technology.
- Multi-cloud architectures are non-trivial.
- Using existing identities and securely enforcing global policies across all services and on-prem providers is challenging.
- Simply hoping users and vendors are reliable is not the best security strategy.
- Current solutions do not easily address legacy storage integration/ migration.



StorageFabric™

StorageFabric™ (https://storagefabric.io) addresses the above critical security, integration and vendor lock-in challenges. It is a *swiss knife for high performance enterprise storage integration and protection* in a multi-vendor, multi-cloud world. It unifies and protects storage across tens of **on-prem and cloud**-based vendors. Breaches do not affect the enterprise. Benefits include:

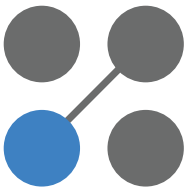
- Escape Vendor Lock-In
- Cyber Protections and Global Visibility
- High Performance
- Immediate Integration of Existing Systems
- Can Eliminate On-Prem Footprint
- Significant Cost Savings

What Our Customers Say

"I am ecstatic of the great work [...] hats off [...] for the work they did and also CTO/Deputy CTO - and I guess Jim - major kudos."

"I'd like to compliment you all on the quality [...] your documentation and install procedures [...] significantly better than other vendors that I have dealt with of late and is a welcome change."

"I cannot thank you all enough for your hard work and dedication to make this happen. [...] often went out of their normal roles and assisted in other areas to ensure success. [...] I look forward to working with you [...] in the future as we continue to grow and evolve the service."



About Virtalica

Virtalica was established by world-renowned experts with many decades of expertise. Our mission is to create next generation high-performance enterprise technology that is secure and easy to use.

Technologies

StorageFabric™ (Storage Integration + Protection Fabric): https://storagefabric.io
SANScaler™ (Zero Footprint 3¢/GB Enterprise FLASH SAN): https://sanscaler.io

Virtalica
164 20 Street, 4th floor
Brooklyn, NY 11232
USA

https://virtalica.com
storagefabric@virtalica.com
+1 - 631 - 731 - 1695
+1 - 877 - 7 - CIPHER