

The hybrid cloud paradox

Byline article

Olivier Delachapelle, Head of Product Line Management, Product Sales Europe at Fujitsu

How business and IT leaders can resolve the tug-of-war between hybrid cloud DX and new security and resilience challenges

Business and IT leaders are being pulled in two directions at once. That is the situation outlined by industry analysts IDC in a [recent campaign*](#)) from Fujitsu alongside our partner Veritas.

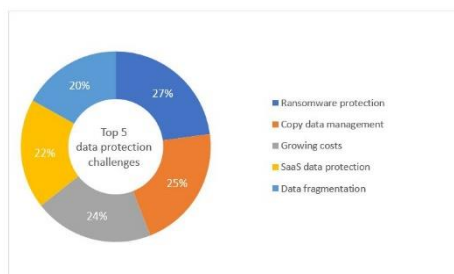
On one side, it's necessary to pull through greater intelligence into the enterprise, with data as the key opportunity. However, IDC's research shows that only 32% of data is effectively utilized today, while at the same time, for 87% of CXOs, a top business priority is becoming an "intelligent organization" by 2025.

On the other side are the practical challenges of mobilizing and leveraging enterprise data. One is added complexity, alongside concerns over security, data protection, and data mobility that come with cloud and SaaS adoption. As IDC puts it: "Cloud is the engine of DX" – with 85% of companies running hybrid cloud environments where workloads are spread across these infrastructures.

Is this an unresolvable conflict of interest? We think not. A modern data protection strategy can overcome the challenges and help deliver digital outcomes. That is, provided you put business value at the top of your strategic objectives and take a risk-based approach to data protection and resilience that directs investment to where the hazards are most prevalent.

Hybrid cloud comes with security and resilience challenges

When it comes to hybrid cloud data protection, IDC argues that traditional responses are failing. As this chart shows, organizations are concerned that existing



data protection architectures are not up to the job of managing challenges such as ransomware, SaaS data management, not to mention data sprawl across different repositories.

The fundamental problem is that legacy backup environments are designed to protect the data center but not beyond. As a result, IT teams lack the flexibility to scale data management functions and meet the data services requirements of all workloads – physical, virtual, and cloud-based applications, including SaaS environments. Attempts to overcome this have had many adverse effects. They have increased management complexity while failing to provide the layered approach necessary for today's needs or the means to fully exploit cloud economics. As a result, they are perceived as a cost center rather than a security and compliance enabler – a piece of technical debt that is being carried forward.

IDC recommends five ways to get on top of this tug-of-war:

1. Unify data management to eliminate complexities and increase visibility.
2. Introduce an integrated data protection solution to push SLAs to current best practice; for recovery point object (RPO) that's now 15 minutes, down from one hour, and for recovery time object (RTO), it's down to just seconds, from two hours.
3. Multilayered protection is imperative.
4. Capitalize on new automation technologies such as insights, automation, policy-engine, metadata management, data discovery and cataloging, data movement, protection, governance, and security.
5. Address data management bottlenecks.

Fujitsu agrees these are highly desirable outcomes. But we prefer to embed them within a larger framework that accentuates adaptability and business value.

Creating an Adaptive Organization

Our take is to emphasize the need to drive intelligence into the enterprise in order to create greater adaptability. And why the difference between this and the buzzwords of an “intelligent organization”? No one is in any doubt, with the pandemic of 2020-21 still disrupting business, organizations must accelerate their data transformation plans to adapt quickly to any circumstances.

However, despite profound changes achieved by IT leaders worldwide in response to the pandemic, Fujitsu’s experience and research show the adaptability to respond to business users’ continuing needs for flexibility is still lacking. We see a growing disconnect between what business users want and what digital leaders think they are delivering. In particular, business users are sending strong warning signals to digital leaders about the continuing inability to leverage data to adapt to emerging needs.

Delivering business value

Our preferred model to achieve this is a data-driven transformation strategy (DDTS). This four-stage methodology embraces the five outcomes recommended by IDC, with an emphasis on delivering business value. Each DDTS layer is critical to the success of the transformation: it is not possible to leapfrog the preliminaries and still hope for excellent outcomes. Business value is a direct result of the proper choice and application of data science and AI. These choices, in turn, are contingent on getting the strategy and architecture right.

For example, while containerization and cloud-native applications currently rank lower in IT teams’ priorities identified by IDC, they are likely to accelerate in two to three years. This means data protection decisions taken today will need to serve emerging requirements, such as tomorrow’s container protection and data persistence.

Channel approach

Fujitsu works closely with its SELECT partners to bring together the right ecosystem to address each customer’s unique needs. This is achieved by integrating the contributions of large and small organizations and aggregating capabilities into an ecosystem. Partners create business value through being empowered to collaborate effectively to realize emerging market opportunities.

Taking a risk-based approach to risk

When it comes to balancing the tug-of-war between hybrid cloud DX and resilience, few organizations can afford to protect themselves against any outage and recover instantly in the event of a failure.

We recommend addressing this in two ways: Automate as much as possible to protect data consistently in hybrid environments, and adopt a risk-based approach to data protection and resilience. Understand the likelihood of different failure scenarios and the expected business impact and invest accordingly.

But don’t do any of this in piecemeal, tactical deployments. As has happened before, these could just increase complexity rather than resolve it. Any moves you make should be part of a holistic approach to hybrid cloud data protection, where business value is your touchstone. As your next step on this journey, find out more about Fujitsu’s DDTS model to achieve precisely that [here](#).

Olivier Delachapelle, Head of Product Line Management, Product Sales Europe at Fujitsu

Brussels-based Olivier creates and implements operational strategies for the Europe Region Products Business Line. He fosters, innovates and leads the product organization and ensures profitable growth – especially for focus topics such as IT-related services and integrated systems.



**) Source: European IDC Fujitsu Veritas Webinar: Reset Today for What Matters the Most – Data Protection, Compliance and Resilience, June 2021*