Business Outcomes and Value of Modern Data Protection Strategies

In the previous two posts in this series of IDC blogs on data protection, we highlighted how modern enterprise IT trends such as hybrid cloud adoption, data fragmentation, and ransomware challenge organizations to become resilient and trusted. We also highlighted the limitations in traditional data protection strategies in meeting the new requirements.

In this blog, we will highlight how a modern data protection strategy can overcome the challenges but also help deliver digital business outcomes.

As data-driven strategies become front and center for C-suites everywhere, it's time to think about data protection as strategic to meeting broader business outcomes. In conversations with IDC, IT leaders identify their top priorities as follows:

- **Digital resilience.** A laser-sharp focus on digital resilience continues during the COVID-19 recovery journey.
- **Digital trust and compliance.** Modern security capabilities, adhering to privacy and data protection regulations, and following a governance model are integral to digital trust and competitive differentiation.
- **Data control.** At least 5%–10% of revenues for verticals such as the financial sector are likely to be based on data monetization and data-driven products, making data control an imperative.
- **Data mobility and cloud migration.** The ability to move data to/from core, edge, and cloud repositories, as well as legacy migration, are essential for successful cloud migration and digital transformation.
- **Cost optimization.** Organizations believe they are wasting at least 15% of their public cloud spending and are aiming to cut cloud waste in half using insights to optimize their use.
- **Capitalizing and monetizing data.** Data capitalization is a top business goal; organizations have set themselves a four-year horizon to achieve this and have started assessing data life-cycle management roadblocks.

A modern data protection paradigm is needed to deliver on these six business outcomes. Organizations should treat all valuable business data as "first-class citizens" to create a strong first line of defense and to ensure last-mile security.

A modern data protection paradigm can ensure that no data is left behind — data on premises, data in SaaS environments, data in the cloud, and new data at the edge.

How?

1. A modern data protection strategy is all about unifying data management. This can help to eliminate complexities and increase visibility of data — resulting in better protection. It can also help organizations succeed in a dynamic world of hybrid cloud, edge, containers, and SaaS applications.

> ***By 2024, net-new production-grade cloud-native apps will increase to 70% from 10% of all apps in 2020, due to adoption of technologies such as microservices, containers, dynamic orchestration, and DevOps, according to the IDC FutureScape: Worldwide Future of Digital Innovation 2021 Predictions, European Implications.***

2. For a digital business, data and application availability can make or break brands. SLA requirements are becoming tighter with a push to zero downtime and zero data loss. An integrated data protection solution can help deliver robust availability and recovery.

> ***The current best practice for recovery point object (RPO) is 15 minutes, down from 1 hour, and the current best practice for recovery time object (RTO) is down to seconds from 2 hours.***

3. When it comes to cyber resilience, having multilayered protection capabilities is an imperative. Capitalizing on immutable storage targets, encrypting backups, and anomaly detection as part of modern data protection strategies are crucial to building continuous cyber resilience.

> ***53% of organizations see investments in security, privacy, and compliance technologies to improve the organization's risk posture as a priority over the next two years to build resilience.***

4. Capitalizing on new features and technologies such as insights, automation, policy-engine, metadata management, data discovery and cataloging, data movement, protection, governance, and security is key.

> ***The top 3 areas that savvy organizations have identified for "greater automation" in IDC's Future Enterprise Resilience Survey (February 2021) are data protection (42%); network/endpoint security (32%); and infrastructure resources (compute, storage) optimization (30%).***

5. To deliver on data-driven business ambitions, it is critical to address data management bottlenecks. Limitations in traditional data protection are forcing organizations to transform their data protection strategies.

> ***Spiraling costs, SaaS data protection, implementing modern databases, disjointed data management, ensuring rapid recovery, lack of data visibility, and complexity are all top IT pain points today.***

If the broad six business outcomes are on your radar too, it's time to embark on these five best practices. It's time to reassess and introduce a modern, unified, and automated data protection foundation. It's time to make data protection a business enabler.

To learn more about how enterprises can boost data resiliency and compliance in hybrid cloud by leveraging modern data platforms, data protection, and archiving capabilities access the recent IDC webinar, 'Reset today for what matters the most – data protection, compliance and resilience'.

Veritas and Fujitsu have been global strategic partners since 1992. The proven, long-term partnership with Veritas extends Fujitsu's vendor- and platform-agnostic Data-Driven Transformation Strategy (DDTS) to optimize and monetize organizations' data assets.

Fujitsu's datacenter offerings, such as PRIMERGY server, PRIMEFLEX Integrated System, and ETERNUS storage, together with Veritas' Enterprise Data Services Platform, boost resilience, compliance, and protection of data residing on premises and in the cloud. The joint ecosystem helps customers to reduce cost, increase efficiency and productivity, and meet compliance requirements.

Author: Archana Venkatraman, IDC

Archana Venkatraman is associate research director for cloud data management at IDC Europe. Her primary research coverage is cloud data management, covering multiple topics such as data protection, edge to cloud data trends, application and data availability, compliance, data integration, intelligent data management, DataOps, data quality, and multicloud priorities and trends. She is also a co-lead of IDC's cloud practice and an active contributor to IDC Europe's DevOps and AI research practices.