The Data Protection, Security, and Governance Needs of a Modern Infrastructure and Data-Driven Enterprise

Organizations are faced with rampant data growth and cost, complex infrastructures, compliance regulations, and the increasing risk of data loss from ransomware attacks. Data is at the core of intelligent organizations, and their successful digital transformation (DX) relies on their ability to develop a unified data management and protection architecture for modern multicloud infrastructures.

This series of three blogs written by IDC outlines how enterprises can boost data resilience and compliance in hybrid cloud by leveraging modern data platforms, data protection, and archiving capabilities. This first blog describes some challenges and requirements for modern data protection architectures. The second and third blogs will explore the limitations of traditional data protection strategies and the business value of modern data approaches.

Our sincere thanks to Archana Venkatraman, associate research director of IDC's European cloud data management research, for this blog.

We're at the tipping point of becoming a digital economy.

IDC predicts that by 2022, 65% of global GDP will come from the products and services of digitally transformed organizations. The race to the digital economy has been accelerated by the COVID-19 pandemic, as back in 2019, IDC expected around 50% of GDP to be delivered by digital companies by 2023.

In a digital economy, enterprises require new competencies such as resilience, embedded intelligence, faster innovation cycles, automation, and modern security to deliver continuous value to customers.

Data drives these new competencies. For 87% of CXOs, becoming an "intelligent organization" by 2025 is a top business priority. This vision needs a strong foundation to deliver high standards of protection, security, availability, and data mobility.

IDC's research shows that as much as 68% of data goes untapped today. That means only 32% of data is effectively utilized.

Complexities such as hybrid cloud, data fragmentation, data growth, and new security threats are barriers to deriving value from data.

Let's assess why these trends require modern data protection.

New security vulnerabilities. With more endpoints proliferating, thanks to remote working at scale, cyberattacks have increased. Ransomware was cited as the top data protection concern in IDC's multicloud research, and for 47% of organizations, preventing data loss or leakage was a top security priority. A study by VMware Carbon Black found that there was a 238% surge in attacks from February to April 2020, with 27% of those targeting regulated industries such as healthcare and finance (source: *VMware Carbon Black: Modern Bank Heists 3.0, 2020*).

In addition to malware, internal threats such as accidental deletion, bad actors, and datacenter accidents (such as the OVH fire) also increase the risks. Traditional backup environments do not

provide high levels of data protection due to a lack of immutability or "air gap" features. Air gap protection uses snapshots, replication, and automation to create backup copies that are stored offsite. Immutability provides protection in the form of read-only copies of data for recovery. At a time when malware attackers are targeting backup data first, additional layers of security such as air gaps and immutability in data protection design are a must.

Hybrid, multicloud, and distributed infrastructures. Cloud is the engine of DX. IDC's research shows that 85% of companies run hybrid cloud environments with workloads spread across these infrastructures. Hybrid cloud data is more complex to protect because it includes external networks and many IT components that are beyond IT's control. But at the same time, data, regardless of where it resides, is fully the user's responsibility.

Data is distributed from edge to core to the cloud with core datacenters hosting only 29% of data, according to our research. Data at the edge already accounts for 18% and will see accelerated growth in the future. Protection and intelligent management of all this data is necessary to make hybrid cloud successful.

Data mobility. The value of hybrid and multicloud depends on data mobility. Without a cloud-connected, unified data management strategy, organizations struggle to move data across cloud and edge locations at scale and with security measures such as encryption. Neither can they leverage cost-effective storage tiers for cold data and use enterprise-grade storage services for critical data. A third of organizations admit that data migration and data placement in hybrid cloud are key challenges.

SaaS protection. Use of SaaS such as M365, Slack, and Salesforce is proliferating. Aggressive adoption of SaaS tops the list of planned IT strategy changes in the new normal. For regions with high SaaS adoption such as the U.K. and the U.S., SaaS data protection concerns have risen to the top. Without adding SaaS data to backup strategy, organizations cannot ensure availability, business continuity, disaster recovery, and effective governance at all times.

Archiving efficiencies and compliance. Flexibility to define retention periods, integration with cheaper media such as tape for long-term archiving, and automated processes are all hallmarks of modern archiving. Backup admins need to leverage modern WORM functionalities for compliant archiving. Long-term preservation of data — including unstructured data — needs to be realized in data collection platforms for data reuse, as in analytics and AI. Using a tiered automated HSM approach to further reduce costs for longer-term retention of data is becoming more appealing to businesses amid tighter budgets.

Cloud-native workloads and databases. The digital economy will see more types of data, containerization, new databases, and new regulations. There will be rising costs and greater complexity if data is not managed effectively.

Ensuring data protection and recovery is integral to digital resilience. 42% of respondents admit that greater automation in data protection and management will be critical for resilience.

Modern trends require a paradigm shift in data protection, and C-suites need to see it as an enabler of data-driven projects. Data protection is paramount but needs to be adapted for the modern world with tight integration between storage, cloud, and backup ecosystems.

In the subsequent blogs, IDC will address how organizations can modernize data protection architectures, and look at the benefits and business outcomes of a modern, hybrid cloud-friendly data protection environment.

Veritas and Fujitsu have been global strategic partners since 1992. Our 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.

Guest 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.