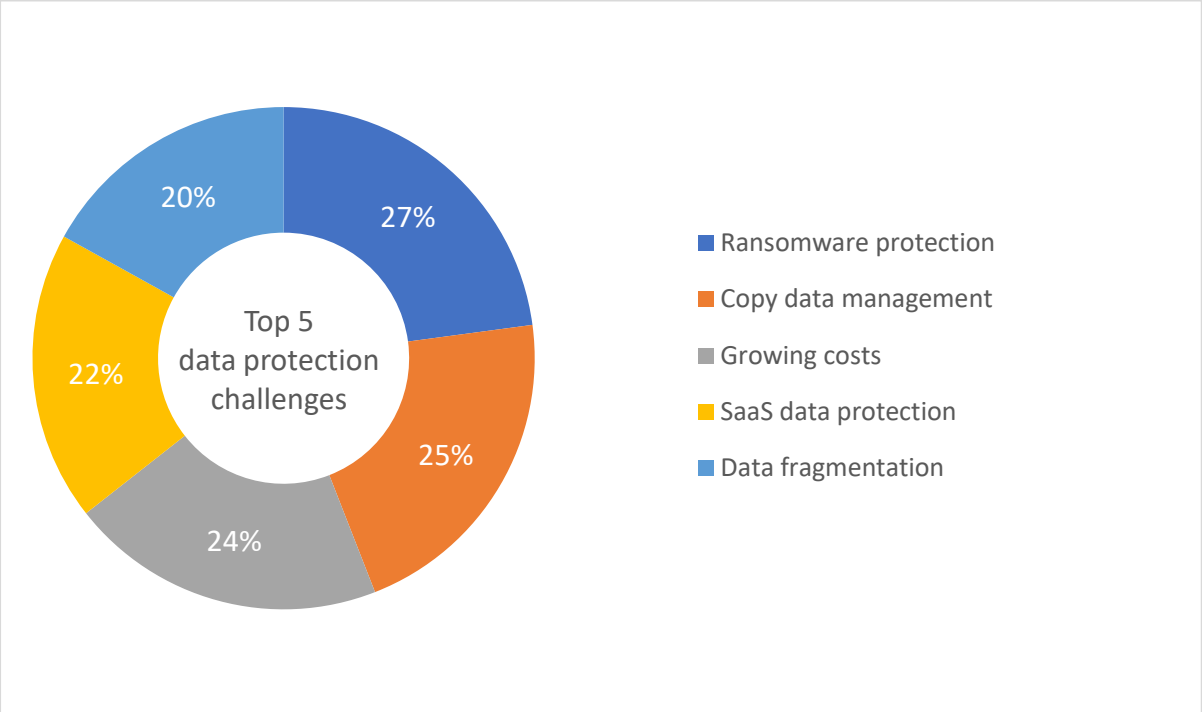
How Traditional Data Protection Strategies Increase the Risk for Your Business

In the first in this series of blogs, IDC highlighted how modern enterprise IT trends such as hybrid cloud adoption, data fragmentation, and ransomware bring new data protection requirements. In this second blog, IDC will analyze the limitations in traditional data protection strategies in meeting the new requirements.

Rapid data growth across core, cloud, and edge repositories is resulting in data silos. Traditional data protection environments do not have the features to deliver data protection, data governance, and data security in a simple, unified, and automated way. As a result, data protection challenges remain key concerns for IT.

So, what are the most challenging areas of data protection in traditional environments?



Source: *IDC Multicloud Survey, 2020*

In conversations with IDC, IT teams say their recovery time objects (RTOs) and recovery point objects (RPOs) run in hours and backup environments are the weakest link in their disaster recovery and business continuity strategies. They also complain about data loss, lack of data visibility, and an inability to consistently meet SLAs.

These concerns indicate that organizations are not confident in the ability of their existing data protection architectures to manage modern challenges such as ransomware, SaaS data management, or data sprawl across different repositories.

Limitations of Legacy Data Protection Environments

They are confined to the datacenter perimeter. Traditional data protection environments were primarily set up to protect datacenter environments and traditional data sources such as structured data.

But IDC's research shows that only 29% of data is currently in core datacenter environments, with the rest spread across secondary datacenters, cloud, edge, and endpoint environments. Aggressive cloud adoption, growing edge projects, and SaaS usage are all contributing to data sprawl beyond the core datacenter.

Legacy backup environments do not give IT teams 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.

They don't expand coverage to modern data sources or needs. Modern enterprises building cloud-native apps and containerized workloads use unstructured databases. IDC research shows that for large enterprises, unstructured data management is one of their top 5 data protection challenges.

These data-driven businesses have a number of needs, such as using secondary data for test/dev and analytics purposes without creating multiple copies of the same data.

Legacy data protection environments are static environments focusing more on complex and time-consuming backups rather than being application centric, availability centric, or recovery centric. These environments do not leverage new technologies such as artificial intelligence or machine learning to monitor or detect anomalies and help remediate them.

Management complexities. Traditional data protection platforms do not rely on modern features such as automation, unified policies, or a single pane of glass to view, protect, and recover datasets from edge to core to cloud.

Over the years, IT organizations have added multiple, redundant point solutions tactically to overcome individual problems. This amplifies the complexities in traditional datacenter environments, adds risks, and increases costs. IDC's research shows that **64%** of large organizations spend more than 10% of IT budgets on data protection, compared with **just 17%** in 2019.

Traditional environments do not combine the strengths of tape and disks with policy-based and automated management of the various targets to bring efficiencies. IDC believes that tighter integration of storage, data protection, and applications can enhance automation, orchestration, and consistency.

They don't deliver multiple tiers of protection. Multilayered data protection is an imperative, as it brings flexibility to meet the unique needs of each application and ensures complete data life-cycle protection and compliance.

Existing data protection architectures are rigid and hardware defined and do not deliver immutability or air gaps for multilayered protection. These are essential for cyber resilience or recovery from ransomware attacks.

A tiered approach delivered via integrated storage and backup software includes robust availability; faster, granular recovery; compliance capabilities; and cost-efficient storage options for long-term retention and archiving. This includes a tape environment to retain backups for longer as an "offsite" copy.

They are inefficient. IDC believes that data preservation (such as long-term retention or archiving) needs to occur within the data collection platform. Legacy backups don't deliver this flexibility. Nor do they deliver the cloud-like economics and scale or deep levels of pre-engineered integration from storage to backup to availability.

They are perceived as a cost center rather than a security and compliance enabler. Data protection is less about backups and more about instant recovery, ensuring always-on needs, and safeguarding data integrity for a business. Legacy backups don't bring the flexibility for organizations to select their backup and restoration destinations.

What Modern Businesses Need

- Unified data management — end-to-end data protection from the core to the cloud, and ensuring availability for key applications
- Access to a consistent set of data management capabilities suitable for hybrid environments including physical, virtual, and cloud
- A data protection platform that is core to the organization's resilience, compliance, and data availability objectives

Enterprises need new competencies such as always-on availability and exemplary compliance and digital trust capabilities. Traditional data protection environments cannot meet these modern requirements. Reset the data protection foundation and boost resilience.

In the final blog in this series, we will evaluate the business value and outcomes of a modern, intelligent, and integrated data protection strategy.