50 Years of Growth, Innovation and Leadership

Is Your Data Center Protection Strategy Putting Your Business at Risk?

Five Misperceptions You Want to Avoid

A Frost & Sullivan Executive Brief
Sponsored by Lenovo

FROST & SULLIVAN

INTRODUCTION

Artificial Intelligence. Big Data Analytics. Internet of Things. Chances are your company has invested a lot of resources in recent years transforming to a data-centric organization. You're not alone: in a survey of global IT leaders, 77% told Frost & Sullivan that investments in data analytics are critical to their business's digital transformation success over the next 5 years; and 47% said investments in Big Data and Analytics are more important than other technologies. Overall, less than 1% of businesses reported not having some sort of digital transformation strategy; and less than 20% report being behind their industry peers in implementing a digital transformation.[1]

But how are you protecting the growing data pools that fuel your business? Have you collaborated with your Chief Security Information Officer or Compliance officer on a data protection plan that extends across your critical applications? Or are you relying on your cloud service provider or storage solution to provide the protection you need?

If you're like many of your colleagues, perhaps you don't think about data protection enough.

Your business applications must be able to access increasing volumes of data around-the-clock, regardless of outages, human error, and cyber threats. You need protection from cyber security breaches that can cost almost $4 million each, and can result in business shut downs, lost revenue, and stiff fines and penalties in regulated industries.[2]

The truth is, your data-centric business requires a sustainable, consistent, and complete data availability and protection approach—one that automates and streamlines data protection to enable dependable business recovery and protection processes, especially in critical down times, ensuring that your databases are both protected and compliant. An intelligent data management solution integrates storage with robust data management and backup & recovery platforms that enable you to ensure that your data is secure and protected, no matter where it is housed. Best-in-breed solutions facilitate management tasks, with intuitive portals that help your team see what data is protected, where it resides, and how much infrastructure it requires.

Unfortunately, many companies risk their businesses by not adequately protecting their data. In this brief, we'll highlight five common misperceptions related to data protection, and offer better solutions for protecting your business.

1 Frost & Sullivan 2019 IT Decision Makers' Survey, June 2019

2 2018 Cost of a Data Breach Study, Ponemon Institute LLC, July 2018

MISPERCEPTION #1:

"MY DATA IS STORED IN MY ON-PREMISES DATA CENTER, SO IT'S SECURE"

One of the biggest misperceptions about data protection is that if it remains on the business premises, the data will be safe. In fact, 77% of businesses responding to the 2019 Frost & Sullivan Global Cloud User Survey cite improved security as a reason to keep data on the business's premises instead of moving to the public cloud.

Unfortunately, constantly evolving cyber threats target all kinds of business and consumer data, regardless of where it resides or what security measures have been deployed—any Internet-connected infrastructure is vulnerable. Cyber criminals continue to devise new means to breach corporate data. Fileless threats, one of the newest varieties of cyber threats, rose by more than 800% in 2018.[3] On their own, even the most advanced premises-based systems weren't designed to handle the rapid updates needed to respond to the latest threats. Software-based security added later but not integrated with your storage system won't provide the consistent, integrated benefits you require for ongoing success: application and hardware awareness, and the ability to adjust accordingly. Legacy systems typically don't incorporate machine learning and analytics, which help the system to recognize potential threats and stop access before it occurs.

> Fifty-one percent of businesses say maintaining their security profiles across their complete environment is a challenge

Hybrid IT environments—where data may reside on the premises or in a cloud or hosted environment—require a security approach that clarifies the value of different data stored across diverse locations, and allows consistent data management throughout. User authentication, policies and governance must be extended consistently across numerous infrastructures, sometimes with different protocols. To achieve this, management requires a high level of manual intervention. Fifty-one percent of businesses say maintaining their security profiles across their complete environment is a challenge.

The Data Availability Solution Payoff

No system, layer, physical security device, or process can stop every intrusion; but you can mitigate the effects of a breach or natural disaster on your business. Using an intelligent storage management platform mitigates security risks by ensuring that clean copies of data are always available to any application that needs it. Modern data availability platforms give businesses the ability to parse old copies of data, find last "clean" copy not infected with malware or ransomware, and restore the environment using the clean copy—without having to pay the "ransom" for data to be returned. This enables fast recovery, particularly from ransomware attacks.

3 Caught in the Net: Unraveling the Tangle of Old and New Threats, Trend Micro, February 26, 2019

MISPERCEPTION #2:

"MY PROVIDER IS PROTECTING MY PUBLIC CLOUD DATA"

Many business leaders assume that, if their data is in a cloud or hosted environment, the provider's replication practices will cover their data. But is that true across all your data or all your enterprise applications? In reality, most providers have "shared responsibility clauses" in their cloud subscription contracts. In general, providers take responsibility for security and backup of the infrastructure itself. Specific platforms, applications, workloads or services that subscribers load onto their instances are not the responsibility of the provider. Businesses are responsible for their own data and server-side encryption; network traffic security (encryption of data, data integrity); operating system, network and firewall configurations; platforms, applications, and identity and access management; as well as the backup and security of their customers' data.

Businesses are responsible for their own data and server-side encryption; network traffic security (encryption of data, data integrity); operating system, network and firewall configurations; platforms, applications, and identity and access management; as well as the backup and security of their customers' data

Shared responsibility models have impacts on disaster recovery and security strategies. Businesses can't assume that a provider's replication practices will cover their data—most of the time, it's an incorrect assumption, and data may be left unprotected. According to Frost & Sullivan's 2019 Global Cloud User Survey, as many as 69% of businesses had not fully implemented their portion of shared responsibility protections; and 34% had not protected any of the data left uncovered by such a clause.

The Data Availability Solution Payoff

At their core, today's data availability solutions must be able to replicate and restore data to mitigate risk in the event of a loss of data, regardless of where the data is stored. The best data availability platforms automate and orchestrate the replication of data and the ability to recall it—even at a very granular level and regardless of location, whether that the data is stored in a remote office, data center, or the cloud. Also critical is the ability to manage this process consistently—from replication through any necessary recovery—with minimal business disruption, if any at all.

MISPERCEPTION#3:

"MY DATA IS REPLICATED, SO IT SHOULD BE EASY TO RESTORE"

If you have backup copies of your data—even if these are magnetic tape backups that must be physically mounted to new hardware to make operational—you may assume that your business is "safe" when it comes to protecting your data. In reality, data and applications may be pulled "off line" for lengthy replication or backup processing, leading to lost productivity. When data changes faster than a backup service can replicate it, there will be a lack of synchronization between data copies. Since the business continues to generate data even as it attempts to restore a failed storage node from a backup copy, data integrity issues can arise. It may also be a challenge to locate all pertinent databases and synchronize data copies that are located in different places, such as in a hybrid environment.

The Data Availability Solution Payoff

The right data availability solutions makes data available across your business's complete hybrid environment, enabling applications located anywhere within the network to access it. In order to achieve this goal, the latest availability solutions integrate highly efficient, flexible, and scalable storage infrastructure with sophisticated automation and intelligence tools.

In the case of an outage, these modern storage solutions facilitate faster recovery by using storage snapshots to reconstitute data before the storage array is assessed. Additionally, the best storage solutions use updated, non-disruptive cloning techniques that enable multiple backups per day, without interruption to the application or business.

MISPERCEPTION #4:

"IF MY PRIMARY STORAGE IS COMPLIANT, THE BACKUP COPIES WILL BE COMPLIANT ALSO"

Today's businesses face new, global regulatory requirements that entail strict penalties for non-compliance. Furthermore, compliance requirements are becoming global—no longer solely applicable to one country where the data is headquartered, but across any country within which the company operates. Whether subject to industry-specific globally applicable regulations like HIPAA or HI-TRUST, certifications like ISO and PCI, or privacy regulations such as the GDPR, businesses must ensure that all data—both production and backup copies—is protected and processed in accordance with regulatory requirements. Automation can ensure that policies and governance are consistently applied to all storage and infrastructure environments and processes.

Ordinarily, ensuring that data handling requirements are met is largely an onerous manual process. IT staff must configure each storage and backup platform individually, making governance difficult. In addition, primary and replicated data are subject to the same standards, and IT teams must be prepared to provide audit reports for all copies of the data. Forty percent of businesses say inability

to meet compliance requirements is a key concern. Additionally, 46% say they have inadequate governance or processes to handle their infrastructure.

The Data Availability Solution Payoff

The right data availability platform allows businesses to set compliance policies about how sensitive data is handled. These policies govern every storage infrastructure managed by the updated storage system, and ensure that both production and backup data are compliant with applicable regulations. This enables your business to maintain—and prove—compliance of both production and replicated data, regardless of what application generates the data or where it resides.

> Forty percent of businesses say inability to meet compliance requirements is a key concern. Additionally, 46% say they have inadequate governance or processes to handle their infrastructure

MISPERCEPTION #5:

"MY TEAM HAS OUR BACKUP POLICIES CONFIGURED; WE DON'T NEED TO REVISIT THEM"

Configuration of traditional storage environments is highly manual, requiring custom integration and high-touch tasks for things like data migration, storage integration, backup & recovery. As a result, some businesses fall into the "I've already set my backup and retention policies" trap, and don't revisit those policies to ensure their effectiveness—which can be an issue when disparate infrastructures are introduced into the environment. Most platforms—even new "software-defined" solutions—don't seamlessly operate across all components of a hybrid storage environment. In fact, Frost & Sullivan's most recent global cloud user survey found that 47% of businesses find ensuring that their backup and recovery processes cover hybrid environments is a challenge. Additionally, if your backup fails or you can't find the files you need at the time that you need them, restoring service within an acceptable timeframe will be a challenge.

The Data Availability Solution Payoff

Today's data-heavy organizations require increased automation, which spans multiple infrastructures, to ensure consistent management of data wherever it resides within a hybrid environment, and whether it is primary or backup data.

Critical to the success of the data-driven organization is the ability to streamline routine operations and tasks—leaving more time, energy, and resources for innovation and development of new services that support the business. By automating policies, you ensure that, regardless of what storage infrastructure or how many volumes of data are added, they are covered by the same security policies

and regulatory governance that your existing environment uses. Doing so ensures that your data remains safe and within the confines of applicable regulatory requirements.

New, integrated storage and data availability solutions reduce the storage footprint via compression and deduplication technologies. This allows your business to store more for less. Some newer storage hardware systems enable both file and block storage on a single system, reducing the need to procure and maintain different systems for different types of storage. Automation and cross-infrastructure policies enable multiple infrastructures to be managed using a single platform and set of policies, ensuring that storage rules are implemented consistently, and with less human intervention.

INTEGRATED DATA AVAILABILITY: THE RIGHT APPROACH FOR YOUR BUSINESS

Data is of growing importance in today's competitive enterprise. Among businesses surveyed regarding their perceptions about big data and analytics, 81% stated that solving big data and privacy issues were a key strategic focus; while 71% cited overall data governance as a prime focus.[4] As a result, new ways to store and manage critical business data are needed more than ever. "Set it and forget it" procedures are no longer adequate to protect these key corporate assets. And yet, constant, manual processes to ensure appropriate backup, security and compliance practices are too inconsistent, labor intensive and time-consuming for most companies. Instead, businesses require scalable, systemic, and universal, methods to handle data management.

To support today's IT environments, data availability and management need to be simpler and more consistent, offering both higher availability and effectiveness as a result. Integrated data availability services provide a comprehensive, end-to-end solution encompassing storage, backup and replication, disaster recovery, data archiving, and availability. Look for providers that offer software designed to manage your entire hybrid storage environment, from remote office to data center. A comprehensive solution should provide all aspects of data management, from load balancing and scaling to security and compliance. The solution you choose should also integrate all functions into a single, intelligent platform that is both application- and hardware-aware, and can adjust accordingly. Additionally, your chosen provider should validate and optimize the solution across servers, networking and storage, regardless of location, to ensure a high-performance storage environment that can reduce your business's costs.

Using such a solution, your business will be able to enhance its data capabilities; improving data availability as well as disaster recovery, while streamlining management and driving new data insights not available with legacy systems. You'll also be able to free your IT staff for greater innovation, while realizing significant ROI on your data availability investment. This approach also provides sustainable support for the business, as well as recognition of the value of employees, reducing turnover.

For more information on integrated data availability solutions offered by Lenovo and Veeam, visit: **https://www.lenovo.com/us/en/data-center/software/c/software**.

4 Frost & Sullivan 2018 Big Data and Analytics Survey, March 2018

FROST & SULLIVAN

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Floor 3 - Building 5, Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
TEL +44 (0)20 8996 8500 | FAX +44 (0)20 8994 1389

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?