Inside Track
Executive Brief

FREEFORM DYNAMICS

IN ASSOCIATION WITH

FUJITSU

Modern Data Protection Revisited

Business advantage is all about ensuring access to data

Freeform Dynamics, 2020

Introduction

When IT systems first entered commercial use, the focus was on the transactions and getting them processed quickly, rather than on the data that was being created and stored. But things changed quickly, partly due to external regulation and legislation, but mainly thanks to a growing recognition that the data itself was important.

Today, many organizations understand very well that the data they hold has great value. Indeed, many also say that they could get even more value from the data than they currently extract. So as the perceived value of data and enterprise information ramps up, it is an excellent time to look again at how such data should be protected.

What's modern about data protection?

As the importance of data has increased, so too has the business requirement to protect that data. In the past data protection was seen as a type of insurance, for example, it was there to help recover the data should there be a physical problem with the storage device, data becoming corrupted, or if a user accidentally deleted files.

But as with most forms of insurance, it was regarded as a necessary evil, rather than something of value. And, just as importantly, the data frequently centered on protecting the device, not protecting the data. Today, things need to change.

New storage needs new protection

In recent years both the business and IT worlds have undergone dramatic change. On the technology side, new technologies, such as solid-state (Flash) storage, data replication and snapshot services, have been introduced. As well as providing faster response, they can deliver additional data resilience, redundancy and availability.

There is also a new way to build storage systems, namely Software Defined Storage (SDS). This implements storage systems in software, using industry standard servers, each with their own local storage. These can be used as if they were storage arrays, with the added benefit of being easy to scale up or out as demand ramps up. However, without attention to detail, SDS could make it harder to ensure data protection.

More data locations

Another change is the growing number of locations where valuable data may be stored. Data requiring protection can now be found on a range of distributed systems, such as:

- Public clouds
- Software as a Service (SaaS) applications
- Internet of Things (IoT) platforms and edge gateways
- Artificial intelligence (AI) and machine learning (ML) systems

Then there is the data held by workers on the personal systems they use, such as PCs, laptops, tablets and smartphones, with different operating systems, storage capacities and connectivity. In addition, many of these users, and their devices, are based outside of central corporate offices. Already we find many users are working remotely, often from home, and this is unlikely to change.

New business models

Organizations want to become more flexible and agile, so they can respond faster to customers, competition and opportunity. Combined with the huge growth in the amount of data that organizations routinely generate, this has forced storage to the front of IT considerations.

Demands for constant data access

As business evolves, it is no longer adequate to rely on quarterly reviews based on historical data. Instead, progressive organizations want two inter-related things: they want to make real-time decisions using accurate live data, with real-time analytics embedded into business operations, and they want to include more historical data in their future-looking analyses.

However, with data stored in such a wide range of different systems, formats and physical locations, the challenges are non-trivial. Then there is the fact that many organizations also want to use the vast quantities of data generated by their IoT systems to inform decision making. Add in the potential for using information held by suppliers and partners, and the picture becomes even more complex.

All these factors are coming together to make fast access to information held in data protection and archiving systems a necessity, not merely desirable.

New threats and security challenges

It is not just new technologies and business models that are changing the demands on data protection: the threat landscape is evolving too. The wide range of new data sources and data locations has greatly increased the potential ‘attack surface’ for malicious actors. And today’s attacks on information systems often reflect the value that data holds – value that is clear to a financially motivated cyber-crime industry.

Most notably, in recent years cyber-criminals have perfected the ransomware attack, where an organization’s data is encrypted by malware. Once data is encrypted, the effect is almost identical to a total system failure. And if such data is critical to the organization’s operations, there are usually only two options available:

- Pay the ransom and hope the encryption key will be provided in return
- Restore the data from a secure, air-gapped data protection repository that has not been similarly compromised and encrypted by the cyber-criminals.

The second response is the only one that makes sense and can guarantee a full return of data ready for use. Ironically, it can also be cheaper than paying a ransom – but only if it was funded and executed before the attack took place. This makes the ability to restore data essential in order to minimize disruption and lost business.

Taking a fresh look at data protection

Taken as a whole, business and technology change means that storage is no longer an afterthought. Indeed, in many organizations the cost of storage is the biggest single item in the IT budget. That, on its own, strongly suggests that data protection needs to be looked at afresh. The importance of data means that data protection cannot be viewed merely as a form of compulsory insurance. More importantly, it tells us that organizations today must re-evaluate how they protect data.

The need to make real-time decisions based on live data adds another dimension to the importance of data protection. Data must be available, whenever required, from whatever source that generated it, almost instantly. Clearly this means it would be an advantage to have all data, from whatever source, pooled and held in a central location or in a public cloud repository.

Protecting data, not devices

Fortunately, data protection solutions have matured greatly in recent years. Data protection is no longer a system-focused one-size-fits-all solution, where backup copies of system data are stored on a second storage device or on tapes, ready to be recovered only in the event of an emergency.

Instead, sophisticated modern solutions focus on protecting the data wherever it is, whatever its format, regardless of its host device or system. This alone offers an excellent business case to justify investment in innovation, but modern data protection also has other measurable benefits.

For example, such systems can reduce the CPU and memory overhead on production server systems by offloading data protection processes to dedicated appliances. This can in turn reduce the need to update primary server systems, often with considerable cost benefits.

And modern systems can consolidate data, working hand-in-hand with primary storage systems to make it available whenever and wherever it is needed. In that way, modern data protection systems can also allow analysis of historical and/or archived information to inform forward-looking business decisions.

Taken together, the use of modern data protection systems makes data protection no longer just a cost. Instead, it can become part of the value-generating side of the business, while mitigating risks and enhancing business agility.

In order to achieve all this, these modern data protection systems need to be able to:

- Make data available in the case of IT outages
- Restore data following data loss and / or corruption
- Restore data rapidly following a cyber-attack
- Restore to multiple sites, and to differing storage platforms
- Provide rapid access to historical data for analysis

This, in turn, requires the data protection solution to be able to:

- Speedily ingest data from multiple sources and restore data quickly on demand
- Scale to cover long-term data growth
- Integrate with existing infrastructure management tools
- Deliver all data services, e.g. snapshots, replication, dedupe, compression etc.
- Integrate with commercial and open-source data protection software tools
- Be a central repository of data for new projects with no impact on primary data
- Provide long-term archiving capabilities

Such breadth of capabilities often requires solutions to be built using components from multiple, established data protection hardware and software providers. But to make life easier, one way to obtain such benefits is to look for integrated platforms that are built with modern data protection in mind.

Data protection approaches

There are two common approaches taken by data protection appliances. Target-based appliances are designed to hold protected data and allow freedom to use the most preferred backup application. Integrated appliances are pre-configured with bundled data protection software and are delivered fully functional.

Appliances, both target-based or Integrated, are designed to simplify and consolidate backup data with the goal of simplifying and optimizing data protection and data recovery. Clearly it is essential that such appliances function well with the primary storage platforms you run, preferably using the same management tools in everyday administration.

Another important fact to bear in mind is that protected historical data is increasingly being used in business analytics operations and forward planning. This makes it essential that such modern integrated data protection systems have resilience built in to ensure that data is always available.

Although it might seem counter-intuitive, this could mean that you need to take a copy of the protected data and store it at another site on a similar appliance, or perhaps copy it to a modern tape system. A single modern tape media can store huge volumes of data, is easy to transport, and has a very long lifetime. A third option may be to replicate the protected data to a public cloud service.

Appliances should also incorporate policy-driven data movement engines to automate routine operations wherever possible. And many industries will benefit from built-in data classification capabilities, to ensure sensitive information is secured appropriately.

Benefits and opportunities

If data protection is done well, not only does it mean the organization can continue to function efficiently and effectively in case of disaster, loss or failure, but it can also deliver additional business benefits. For example, it can:

- Provide a central repository of enterprise data from across locations, cloud services and IoT edge systems
- Make historical and current data available for future usage in new projects
- Act as the source from which real-time business analytics and AI/ML solutions using multiple data sources can be constructed with effective governance
- Satisfy external regulatory and compliance obligations
- Form the basis of an effective enterprise data lifecycle management platform

Things to think about

With so much potential benefit, as well as the historically understood requirements, there is a lot to think about when you look to update your data protection systems. Here are a few questions to consider as starting points when you talk to your current supplier or start talking to new suppliers:

- Do they have a range of solutions with the operational characteristics you need to support the range of data sources, locations and platforms you run today?
- Will they keep up to date with industry developments to ensure your solution can meet the demands you have tomorrow as well as those of today?
- How comprehensive are the data protection capabilities they provide?
- Do they have rapid 24x7, local-language support wherever you have systems that require protection?
- Does their data protection management integrate with the tools that currently run and monitor your infrastructure?
- Do they understand your specific needs, not just those of a general customer?
- Do they have a partner community that includes those suppliers with whom you already work?
- Can they provide flexible ways to finance your data protection needs?

In summary

The data protection needs of modern organizations have evolved rapidly in recent years, yet for many their data protection systems have not evolved to match. This is partly explained by the fact that data protection is often regarded as insurance and is almost invisible to the organization until the need for it strikes.

However, when you combine the rapidly expanding range of locations where data is produced with the sheer growth in the amount of data being created, it is obvious that both the data protection strategy and technology need to be updated. At the same time, it has long been a challenge for organizations to get full value from the data that they hold – a challenge that is made harder today by rapid data growth.

Fortunately, modern data protection solutions can keep data continuously available to the organization and, if done well, can also help generate new business value. Modern data protection solutions could therefore have a very effective role to play ensuring the business gets value from primary, backup and archive data.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we help busy IT and business professionals get up to speed on the latest technology developments and make better-informed investment decisions.

For more information and access to our library of free research, please visit www.freeformdynamics.com or follow us on Twitter @FreeformCentral.

About Fujitsu

Fujitsu is the leading Japanese information and communication technology (ICT) company offering a full range of technology products, solutions and services. Approximately 140,000 Fujitsu people support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers.

For more information, please visit www.fujitsu.com

Fujitsu Data Protection, www.fujitsu.com/dataprotection

Terms of Use