arcserve®

WHITE PAPER

the end of data protection as we know it?
defining a next generation architecture

by Christophe Bertrand, VP of Product Marketing

My friends, the end is near. Good news/bad news: backup and data protection architectures as we know them are about to undergo a drastic set of changes in the next few years.

The backup and recovery market is quickly morphing as end users weather a perfect storm hitting their infrastructure, affecting the efficiency of their operations.

There are many factors. Let me share my short list:

- The use of multiple point solutions, for data protection and high availability, from multiple vendors. This creates inconsistent data protection infrastructures for larger end users
- Added complexity partially caused by the wide adoption of virtualization
- The increased adoption of multi-tier business applications with complex data protection schemas
- The exponential growth of structured and unstructured data
- Increasing requirements to demonstrate compliance and data stewardship
- Lack of data and system recovery predictability
- Strained resources in terms of systems, people and funding
- Lack of measurability and control of key metrics such as Recovery Point Objective (RPO) and Recovery Time Objective (RTO). If you don't know where you are at, at any given point in time, how can you control it?

Across many of these challenges is the consumerization of IT, which compounds the level of expectations placed on the data recovery team, as users demand **"we want our data back, and we want it now!"**

Having extensively surveyed the CA arcserve customer base, we were able to confirm these trends and challenges. There is a crisis that is now fueling an unprecedented and dramatic review of best practices in data protection, with a fundamental shift towards more measurability... and a keen focus on recovery. This is a time for change, and a time for a new type of solution.

Market Outlook

We observe from analyst reports that this vast and well established market is growing at a nice pace, and seeing major investments from vendors competing in it. However, many solutions are limited in scope – what we like to call point or niche solutions. Industry observers agree: there is a strong need for solution completeness (offering a broad feature set) in order to meet current challenges and improve efficiencies across the board. These limited solutions may also lack in ease of use and scalability capabilities, further limiting the ability of IT to deliver a consistent quality of service.

Fueled by data growth and technology advancement such as virtualization, current architectures come up short in a number of areas and essentially perpetuate data protection islands or silos. Today's IT is about the interdependence of systems and applications in the context of service delivery. Understanding and proving that you can recover in a business-reasonable amount of time with a business-acceptable currency of data is crucial. Metrics such as RPO and RTO have become synonymous with business availability. Current architectures make overall poor use of their resources due to a lack of ability to measure process inefficiencies, obsolete solutions with expensive licensing, or niche data protection solutions that only compound the problem, by adding complexity on top of complexity.

This all results in a lack of Service Level Agreements (SLAs) – and without those, how can one demonstrate value back to the business? Users find it very difficult to define SLAs in the first place, since most approaches are manually intensive. In this context, recovery performance can't be tested frequently enough to determine what the realistic SLA should be. In addition, this context also affects the ability to scale – and we know one thing: data is going to keep on growing and critical systems are never going away. Assuring recoverability of these systems is essential.

Requirements for the next generation architecture

A fundamental change is necessary to fix data protection. It requires the adoption of a modern architecture that has been designed to solve today's complex problems, as well as provide a highly scalable platform for the future.

The next generation of data protection products cannot compromise when it comes to features: completeness is essential. What this means is a solution that combines all the core technologies of data protection and recovery: image backup, file-level backup, advanced scheduling, physical, virtual, tape, replication, high availability, deduplication etc. It's a long list, and one that only a few vendors can successfully handle. This is what we call the "solution stacking" phenomenon.

Another way to look at this is that every organization should be able to benefit from the best levels of protection and recoverability, something that until recent innovations was only reserved to the largest enterprises. Innovation is about offering what was limited to the few to a broader audience, and that's exactly what next generation architectures need to do: innovate by delivering enterprise-level features at a fraction of the cost, and with ease of use.

The use of a specific technology like backup or replication is a "conclusion", not a starting point.

What matters is to map the data/system protection or recovery level to the business need. Reverse engineering requirements to match a technology is a sure way to miss the mark. A modern solution lets customers or service providers easily create plans on the basis of their RPO and RTO, as simply as if they were using a dial. Let the right technology kick in based on requirements.

Key to this endeavor is the abstraction of what can be complex tasks or workflows that happen "behind the scenes". Therefore, the next generation of solutions has to unify many technologies in a way that is still easy to configure, yet still provides fine tuning capabilities. A modern unified architecture is needed, one that combines backup, high availability, replication, advanced reporting, on-premise, off-premise or in the cloud, for physical or virtual systems.

A modern unified architecture has to be designed on the core tenants of usability and flexibility. Ease of use has become a de facto requirement in light of the complexities associated with data recovery infrastructures. Simplifying does not mean taking capabilities away, on the contrary, it means empowering users to do more with less, to do better with less, to prove it, to help ensure that it is more reliable rather than merely hope that it works.

Virtualization: a double-edged sword

Virtual environments have become prevalent in many organizations and offer great capabilities that can be leveraged by a data recovery solution. In addition, supporting multiple hypervisors and delivering advanced data protection, migration and recovery capabilities in a heterogeneous fashion is critical. In a modern unified data protection solution, support for virtualization has to be built-in from inception, while at the same time still providing flawless support for physical servers.

Data Protection and Recovery is about Business Protection and Resilience, or the ability for a business to handle interruption events or disasters in a way that minimizes disruptions. It's also about optimizing IT operations. Operational efficiency can be vastly improved with unified architectures, and can lead to operational resilience. Operational efficiency is really about being in control of your key metrics, being able to optimize and streamline processes, workflow and resources. The next wave of technology in data protection, contrary to some beliefs, is not about narrow specialization in one aspect of data recovery, or say one or two virtualization platforms – but about abstracting complexity across the entire data protection and recovery landscape. Efficiency with data is also critical. Leveraging technologies that limit the amount of data being transferred and stored has a direct impact on operations.

As data volumes keep growing exponentially, as organizations' commercial successes and mergers and acquisitions make them larger in terms of locations or volume of transactions, the obvious infrastructure impact is on performance and scalability.

From a data recovery perspective you need a solution to not only adapt to higher volumes of data, but to also maintain service levels agreements such as RPO and RTO, backup window performance, and overall management efficiency. Scalability is a fundamental design element, its DNA. It's not a patch or a convoluted workaround.

It has to be built-in in a way that provides modularity and flexibility, and work across a wide variety of platforms, with disk or tape, on-premise, off-premise or in the cloud.

Introducing CA arcserve® Unified Data Protection

In order to alleviate the shortcomings of current architectures, our teams have developed a truly unified solution that leverages not only proven technologies from the CA arcserve portfolio but also great innovations to enhance data protection and recovery.

CA arcserve Unified Data Protection delivers comprehensive Assured Recovery™ for virtual and physical environments with a next generation unified architecture and an unmatched ease of use. This feature-rich solution enables users and service providers to scale easily, while delivering against their recovery point and recovery time objectives, on-premise, off-premise or in the cloud.

CA arcserve Unified Data Protection combines industry-proven image backup, tape, replication, high availability and true global deduplication technologies within one, simple solution.

Innovative technologies include a new unified, scalable architecture, simple task-based data protection plans, Assured Recovery capabilities and true global deduplication. CA arcserve UDP covers a broad spectrum of enterprise-level functionality typically found in multiple discrete point solutions such as imaging, replication and high availability, yet is easy to deploy, use and scale, on-premise, off-premise or in the cloud, for a variety of virtual and physical platforms.

Its unified management interface provides ease of use and deployment, significantly improving data and system protection and recovery operations compared to point solutions. It improves the operational efficiency of data and system protection recovery.

In combination with a broad set of features for deploying advanced data protection and recovery strategies, CA arcserve UDP enables the automated disaster recovery testing of business-critical systems, applications and data, without business downtime, or impact to production systems.

In many ways, data protection as we know it is not dead, at least not yet... but it is rapidly morphing into a more efficient and unified solution that leverages a continuum of technologies to deliver more control over data protection operations and metrics.

Don't be left behind with an aging and inefficient infrastructure. Our next generation architecture is available now.

It's easy to use, it's unified...and it just works!

arcserve®

Assured recovery™

For more information on CA arcserve UDP, **please visit arcserve.com**