arcserve®

What You Need to Know **Now** About Next Generation Data Protection Architecture

You don’t need anyone to preach the importance of efficient, effective data protection. You already know that the ability to not only protect, but recover your data from system disruptions and data loss—**and quickly**—are mission-critical components of your business.

Yet, your data protection architecture may very well harbor an Achilles’ heel—**a big one**.

It could be your vulnerable computing and networking hardware and infrastructure that serve as a less-than-rock-solid foundation. Perhaps it’s inflexible data protection silos that mark the death knell of your plan’s efficacy and efficiency. Then, there’s infrastructure exposure to small and large data loss events.

It’s your job to identify everything that could possibly go wrong—and to protect against each eventuality.

The good news for you is that this is an exciting time in the world of data protection architectures. Technology is evolving at an exponential pace, helping you improve operational efficiency, better met the needs of your end-users, and provide more robust data protection, deduplication, and recoverability.

So, what do you need to know about where the industry is headed?

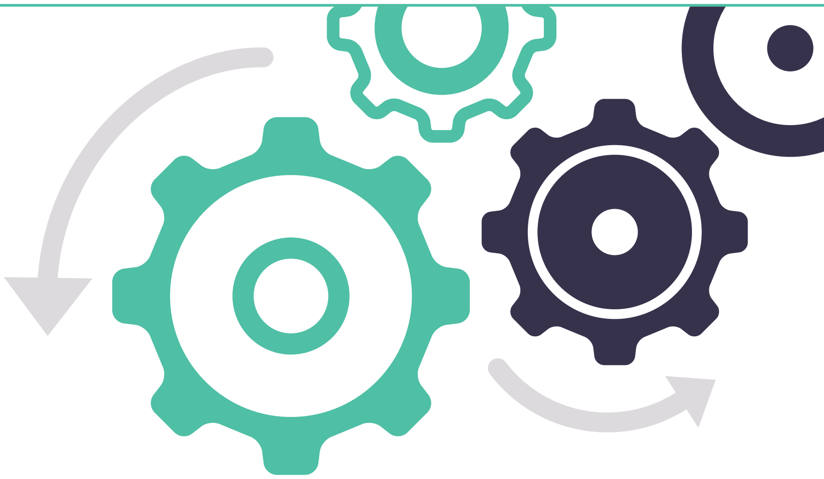
We'll walk you through the driving forces behind these rapidly evolving data protection architectures, the trends you'll want to be keeping an eye on, what we should all demand of next generation architectures, and the state of the current market landscape.

Rest easy. There may be a lot going on in the industry right now, but we're going to boil it all down for you.

Table of Contents

Chapter 1:

What's Driving Changes to Existing Architectures?



To thrive today, data protection vendors like Arcserve must constantly innovate to help customers manage an exponentially greater degree of complexity.

What pressures are driving the market?

Until very recently, there was no one single solution for data protection, deduplication, and recovery. IT departments were forced to employ multiple-point solutions provided by multiple vendors—creating environments that were inherently more complex and labor-intensive to manage.

These situations, undoubtedly, also resulted in inconsistent data protection.

Now, consider the wide adoption of virtualization and multi-tier business applications, each with its own complex data protection schema. It's enough to make your head spin.

Ready for some more? How about heightened public awareness of data loss?

In this climate, highly publicized data failures have tremendous impacts on business profitability and consumer trust. And, so, IT departments are pushed to demonstrate rigorous compliance and data stewardship to C-suite executives, boards, and investors—all while lacking consistent recovery predictability and the ability to measure the key performance indicators which they're expected to report.

As if that weren't enough, IT departments must now also cope with the consumerization of IT, while simultaneously working under strained resources.

It can all seem like an insurmountable challenge. **It's not.**

A shift is coming—and it's about time.

IT today is about the interdependence of systems and applications—all within the context of service delivery.

The vendors that have identified this opportunity for market disruption are reviewing data protection best practices and making the fundamental shifts necessary to align their products with them. And, their next generation products will offer more measurability, greater usability, and improved recovery abilities to their customers.

What current and future trends should you be on the watch for?

Chapter 2:

Trend to Watch: Purpose-Built Data Protection Appliances

The days of purchasing, installing, and configuring backup software on your own servers is giving way to a new trend—a trend that promises a simpler, more straightforward route to data protection.

That is, purpose-built physical appliances that have been preconfigured to run data protection and recovery software.

And, today, those physical appliances are in high demand.

> “Not only do 64% of organizations use PBBA’s somewhere in their environments today, but another 29% either ‘plan to’ or ‘are interested in doing so in the foreseeable future.”
>
> – Jason Buffington, Senior Analyst, Enterprise Strategy Group

What’s fueling the appetite for physical appliances?

To put it simply: **Simplicity**.

These turnkey solutions make data protection architecture easier to price, purchase, setup, and deploy. That means small and mid-sized organizations are able to harness enterprise-level data protection capabilities without big budget IT departments—they can be up-and-running fast.

This fact has greatly accelerated the acquisition and deployment of data protection infrastructure. In fact, according to figures published by IDC*, companies spent $3.26B on purpose-built backup appliances in 2014.

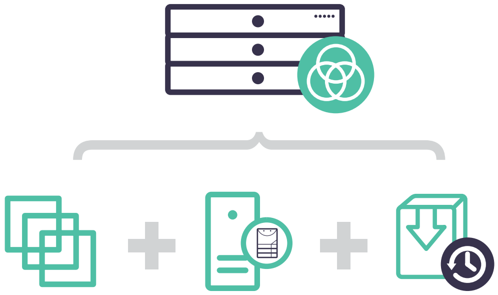
* International Data Corporation (2015, March 20). Worldwide Purpose-Built Backup Appliance (PBBA) Market Revenue Breaks the $1 Billion Mark in the Fourth Quarter, According to IDC [Press release]. Retrieved from here.

The evolution of physical data protection appliances

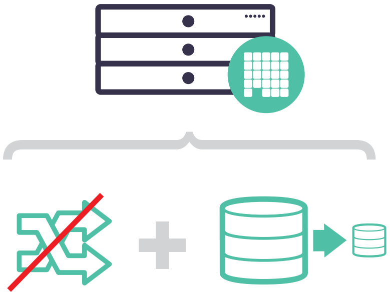
Until recently, if you purchased a traditional purpose-built backup appliance (PPBA), you received a bundled solution featuring retrofitted software and hardware—an afterthought lacking in design elegance, efficiency, and ease of use.

Now, the market is moving toward solutions that have been built with physical appliances in mind from the get-go.

Those appliances include:



Integrated **backup appliances** that natively support multiple applications and ship with both backup software and a server.



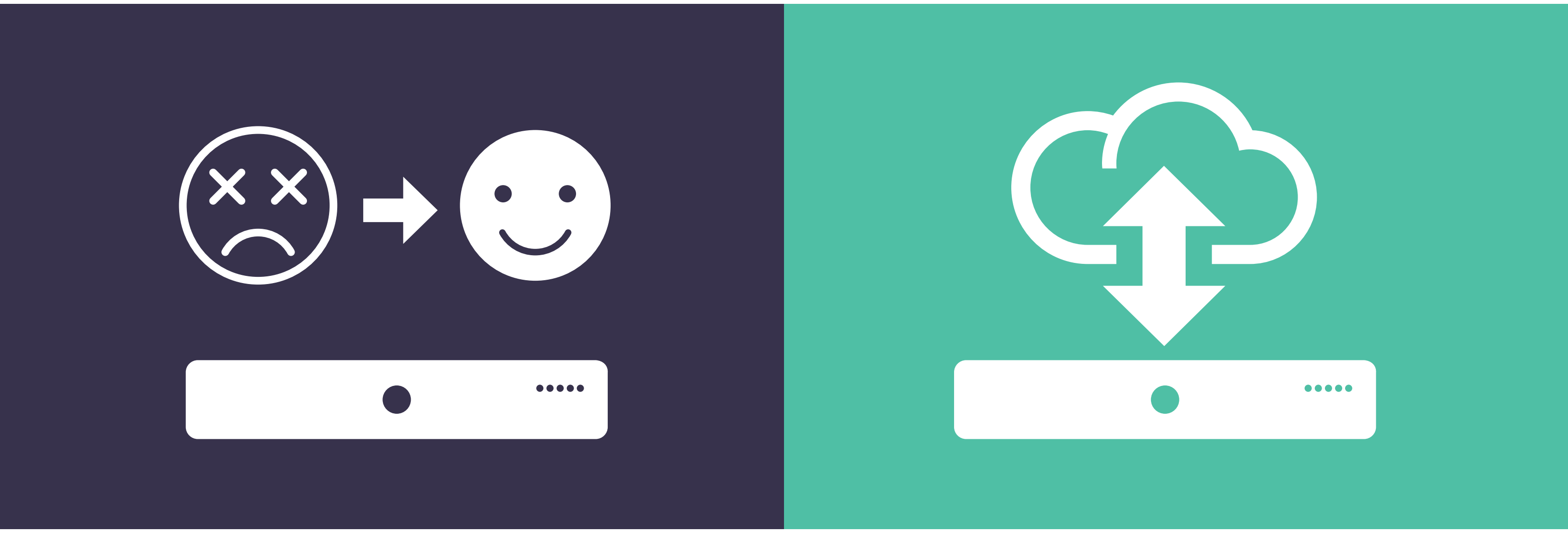
Target-based or more efficient source-side **deduplication appliances** that eliminate duplicate data and compress the data that remains, reducing the total amount of data you must protect.

Typically, deduplication appliances are paired with backup appliances to achieve these tremendous data reductions. However, new options are now entering the market that feature integrated backup and deduplication capabilities in one appliance.

Physical data protection appliances also include failover and cloud-gateway appliances, though these two cloud-native offerings are an emerging trend all their own. As such, we'll cover them in greater depth in our next chapter.

Chapter 3:

Trend to Watch: Failover and Cloud-Gateway Appliances

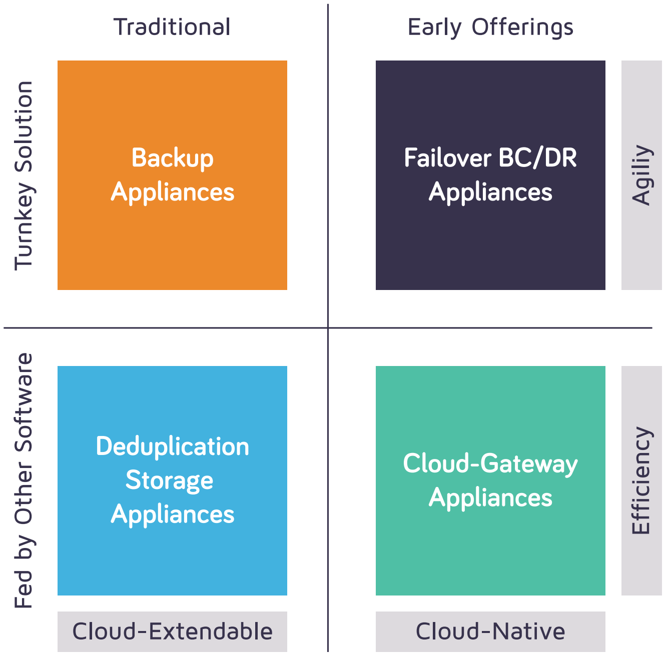


When those in the IT industry speak about purpose-built data protection appliances, they're quite often referring to traditional backup appliances. This is the space where the market has lived for quite some time now.

However, with the explosion of data growth, expanding cloud capabilities, and business users' expectation of anytime, anywhere data access, two emerging, cloud-native categories have entered the mix—and they represent where the market is headed.

They are backup/disaster recovery failover appliances and cloud-gateway appliances.

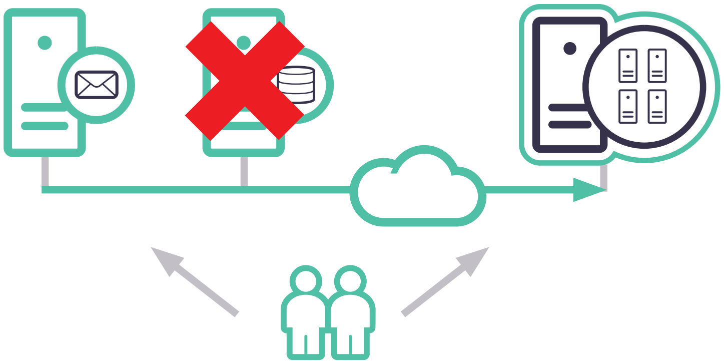
What value do these new categories bring to your data protection infrastructure?



	Traditional	Early Offerings	
Turnkey Solution	Backup Appliances	Failover BC/DR Appliances	Agiliy
Fed by Other Software	Deduplication Storage Appliances	Cloud-Gateway Appliances	Efficiency
	Cloud-Extendable	Cloud-Native	

Source: "Data Protection Appliances are better than PBBAs," Jason Buffington, Enterprise Strategy Group, 2014

Backup/disaster recovery failover appliances



If it's your job to walk the data recovery tightrope, then consider backup/disaster recovery failover appliances your safety net.

These new failover appliances integrate software and hardware, which have been purpose-built to deliver high availability.

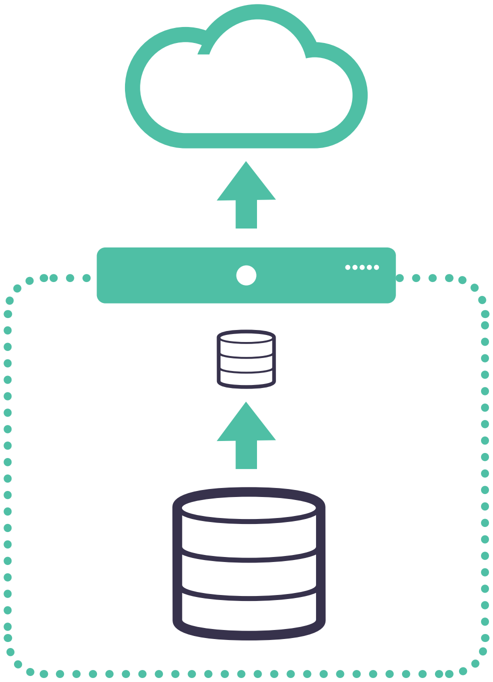
They're typically deployed locally, as well as in secondary locations, so that in the event of a data loss event or systems failure, you can quickly stand up either a virtual machine or a service within the appliance, reducing both system downtime and data loss.

What's more, the backup and recovery of your business-critical applications and data are so seamless your end users won't know they've been pointed to a disaster recovery site.

These failover appliances deliver a high degree of automation to the data recovery process, which is certainly welcome, and they typically offer IT administrators and managed service providers (MSPs) more value when it comes to service level agreements (SLAs), as well.

So, long story, short: If your recovery time objective is a few seconds, this type of disaster recovery, or DR, environment is a must.

Cloud-gateway appliances



Cloud-gateway appliances serve as far more than a data highway to your MSP or cloud service, whether public or private. Rather, they're designed and natively-optimized to replicate your data to the cloud.

What's the benefit?

While not all cloud-gateways are built alike, they may offer some or all of the following:

- Built-in encryption, ensuring your data remains secure
- Local storage, though limited, giving you instant access to recent backups cached locally on your appliance
- Deduplication, reducing the amount of bandwidth necessary to replicate your data to the cloud service—and delivering some serious cost savings, too

There's no question: As more and more organizations take their data to the cloud, these appliances will become increasingly in demand.

Chapter 4:

Trend to Watch: Unified Data Protection Technology

The U.S. Navy hit the nail on the head with its "Keep it simple, stupid" design principle.

Unfortunately, data protection technologies didn't adhere to KISS until very recently. What do we mean by **unified** data protection, exactly?

Essentially, we're talking about a single, lightweight solution that not only delivers all of the functionality you require for both physical and virtual environments, but one that was built from the ground up with that end goal in mind.

What's driving the demand for unified data protection technology?

Until very recently, protecting data required an arsenal of niche products to manage the explosion of data growth and the consumerization of IT—products that didn't talk to each other and resulted in inflexible data silos.

Yes, solution stacking could deliver on the organization's needs for a time, but as additional niche solutions were stitched together, delivering on evolving needs and increasing service levels, a Frankenstein's monster would emerge.

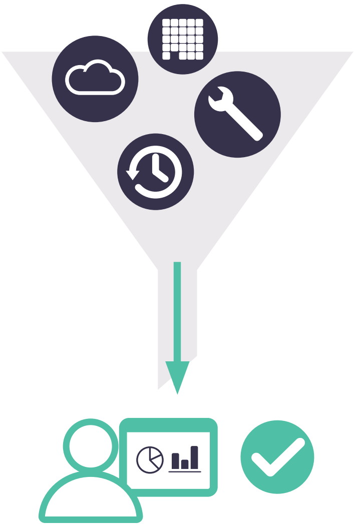
And that presented a unique challenge for small and mid-sized businesses.

While enterprise businesses had deep pools of IT talent to draw from—talent that could be counted on to include very specialized knowledge of particular data protection tasks and technologies, small and mid-sized businesses didn't have that same luxury of mammoth IT departments and budgets.

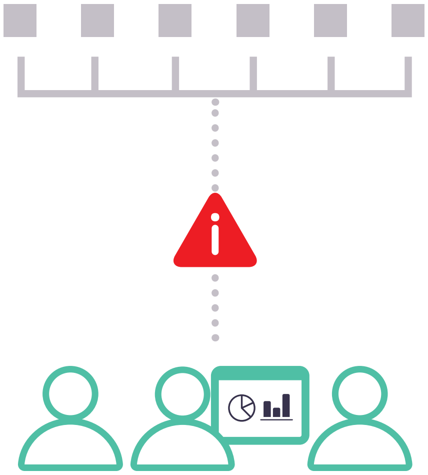
Instead, they had to rely on IT generalists who, now, empowered by the ease of unified data protection technologies and a single management dashboard, are able to deploy enterprise-level data protection capabilities—all with a single, common body of expertise.

Vendor approaches to unified data protection technologies

If you do a bit of digging, you'll find vendors have generally adopted one of two primary approaches to their unified data protection technology "flavor":



They leverage elements of their core backup, deduplication, cloud-gateway, and recovery technologies and rewrite them to create a new solution that's unified on the front and backend. The end result is a lightweight, integrated product that delivers everything you need in one place and a simplified management experience.



They bolt packages of established, complementary backup and recovery products together, which are each accessed through a single management portal. While this approach allows users to select from a broader range of applications and access those applications from a single location, it also results in system bloat, does not always allow for seamless integration and automation of features, and requires added resources to manage.

Keep in mind that this is still an emerging trend and the degree of technology integration and maturity of management interfaces are all in various stages of development, so conduct your research carefully.

Chapter 5:

Trend to Watch: All-Inclusive Licensing

All-inclusive licensing: Myth or reality?

The fact is this trend tends toward hype. In truth, only a very small number of solutions on the market are truly all-inclusive, though the market is starting to shift in this direction.

Why?

Simply put: Pricing is confusing. And, as vendors seek to reduce customer confusion and provide a more positive experience, they're making the switch.

What all-inclusive software licensing options might you find?

Where those licenses exist, they may be based upon:

- Numbers of servers or sockets
- TBs of protected data

And, where they are capacity-based, capacity may be defined further still as data protected before or after deduplication, which can greatly affect your costs.

Still, these pricing structures help you cut through the ambiguity and quickly determine what you can expect to pay for the solution you need.

What about unrestricted licensing?

Yes, it's out there, but it's rare—and the vendor may not be able to provide as much capacity as you want, at the price structure you need, so be wary of creating a false economy.

What are you more likely to see when shopping around?

Vendors are far more likely to license bundles of their most popular features, offering additional specialized features as add-ons. (In short: Nickle and diming.) And, this is a situation that makes determining your final sticker price far more difficult.

Assessing deduplicating backup appliances?

In some cases, you may pay additional fees for extras like encryption, replication, and backup acceleration. And, in a few limited cases, even the deduplicating algorithm or software represents a fee-based add-on. Something you'd most likely expect to be represented in an "all-inclusive" package price.

Researching integrated backup appliances that come bundled with software licenses?

Look closely. According to DCIG*, barely over 20% of integrated appliances ship with all of the features and functionality you need. Yes, they'll arrive with deduplicating software and a console, but you'll have to dig deeper to determine if your license also includes replication, encryption, and OS agent software, as well, or if those features will represent additional costs.

Do your research

Regardless of which type of license is offered—limited or all-inclusive—be sure to do your due diligence and keep an open mind; the best licensing option for your organization may not be the one you first expect.

Speaking of due diligence, we encourage you to read the fine print—**all of it**.

* Arcserve (2014, December 17). Trends in Data Protection with DCIG [Webinar]. Retrieved from here.

Chapter 6:

Requirements for Next Generation Architecture

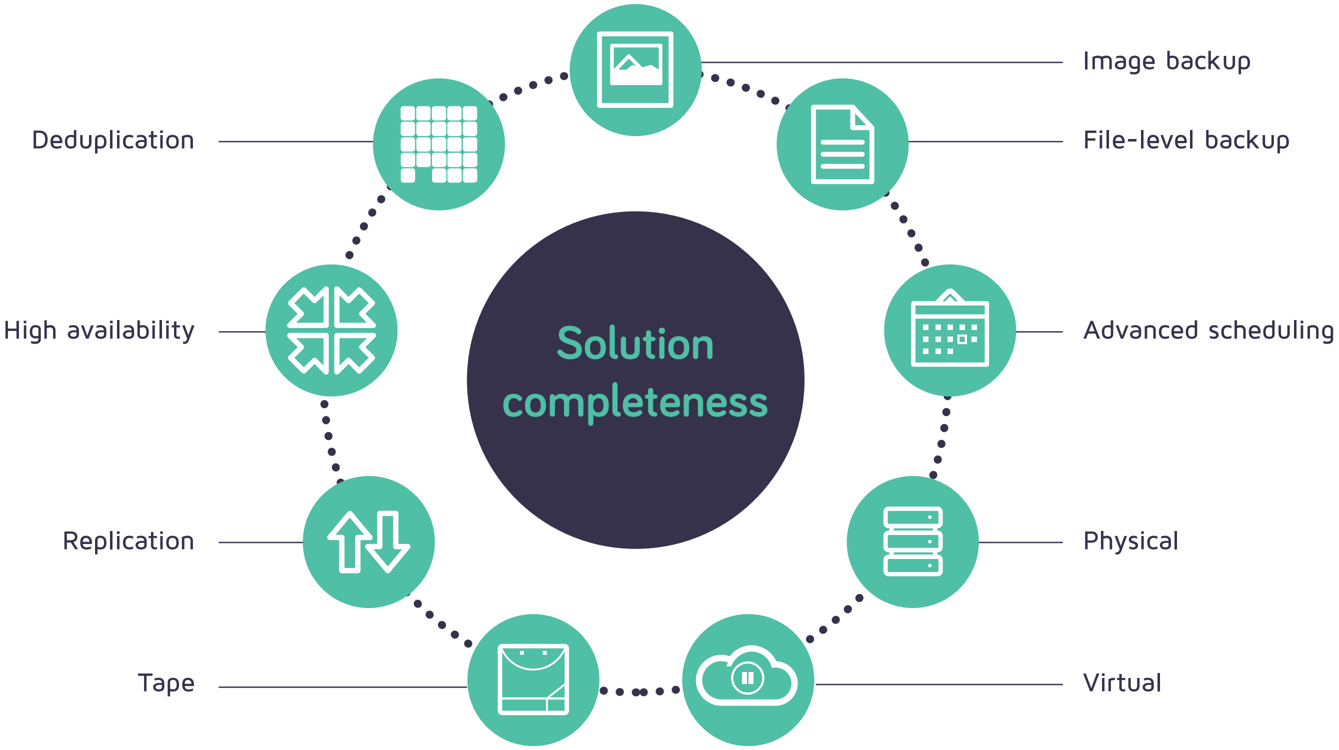
Data protection has become increasingly complex and some solutions out on the market have become obsolete. How can you ensure you're the hero, not the chump?

Next generation data protection architectures are a great place to start. When they deliver on their promises, they make things easy, while making you look good. They'll be affordable and offer both a high degree of scalability and feature completeness, too.

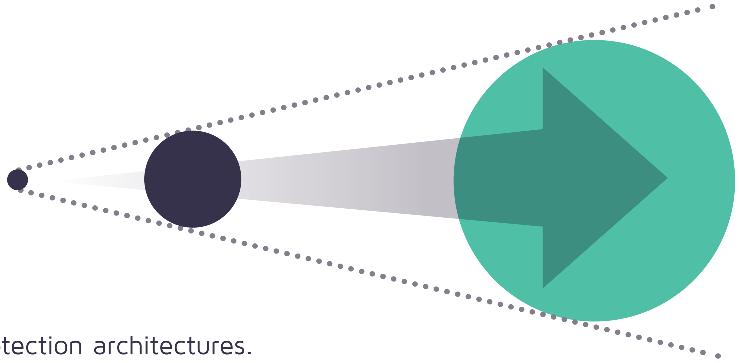
What should you come to expect as these solutions mature?

Solution completeness

Next generation architectures will provide you with all the core data protection technologies you need within a single solution, including:



Currently, only a few vendors can successfully deliver robust solutions like this.



Solution scalability

We expect much more of modern data protection architectures.

Not only must they adapt to handle higher volumes of data, while also maintaining recovery point objective (RPO), recovery time objective (RTO), and backup window performance service level agreements, they must be flexible enough to work across a variety of platforms—with disk or tape, as well as on-premise, off-premise, on the appliance, and in the cloud.

And, as organizations grow, merge, and are acquired, their data protection architectures must be modular and flexible enough to scale—all while delivering high performance.

What does that mean in layman's terms?

While you might begin with data protection software that you install yourself, you might purchase an appliance as your business grows and, ultimately, move some of your data to the cloud as your organization matures.

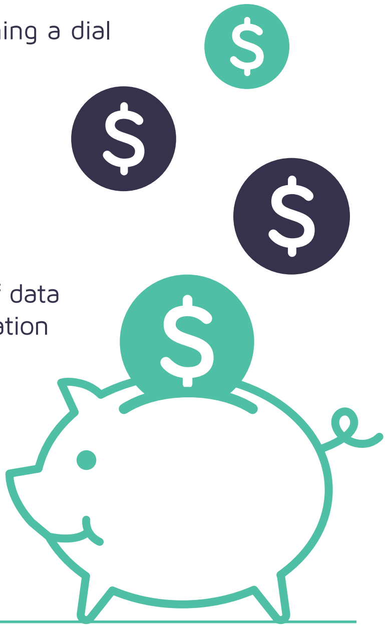
And, a highly scalable solution will allow you to do all three—when and where you need it.

Solution ease of use

Modern data protection architectures must not only be simple to implement, they must also be easy to use. And, any solution that's unable to deliver that degree of simplicity will fall victim to the competitive products that can.

Look for solutions that allow you to:

- Unify a number of technologies in a way that's easy to configure
- Create plans on the basis of your RPO and RTO KPIs, as simply as turning a dial
- Allow complex tasks and workflows to happen "behind the scenes"
- Still provide you with the ability to fine tune capabilities



Solution pricing

There was a time when only the largest enterprises could afford this level of data protection and recoverability. In fact, as recently as two years ago, deduplication and unified management consoles were strictly enterprise-class features.

No longer.

Now, data protection technologies are flexible enough to be deployed in a variety of ways, optimizing operational efficiencies and costs, with licensing that make them affordable.

Chapter 7:

The State of the Current Market Landscape

We've evaluated the state of the market landscape—and we've found it wanting.

Where data protection began with software, it has evolved to offer hybrid infrastructures fed by a strong appetite for appliances and the emergence of the cloud as a destination.

And, that evolution has resulted in legacy products that are now obsolete. Some are coupled with expensive licensing, others are unable to measure process inefficiencies. Then, there are those that don't scale or are weak from a usability perspective. Others still, are niche solutions that must be stitched together with others in order to deliver the robust data protection and recoverability you need, while compounding the degree of complexity you must manage.

In each case, these solutions impede your ability to consistently deliver high-quality IT service to your end users.

How does a vendor deliver a truly next generation solution?

For starters, it means letting go of legacy software and retrofitted solutions.

Instead, forward-thinking vendors are looking at the current data protection landscape as a whole, and building new, integrated technologies that are highly flexible, adaptable, and configurable.

What does the market offer today?

If you're ready to dive into your search for a solution, be forewarned—it's a big pool, and not all vendors have begun to align their solutions to new, pressing demands.

Today:

22	**vendors offer 26 virtual server backup software solutions**
10	**vendors offer 47 deduplicating backup appliances**
14	**vendors offer 72 integrated backup appliance**

And those numbers don't even begin to take into account the deduplicating and integrated backup appliances that are also available as virtual appliances.

Of course, while the entire field of vendors is big, a select few are the clear leaders in the industry.

They are:

- Arcserve® UDP
- CommVault® Simpana®
- Dell® AppAssure
- Symantec Backup Exec™
- UniTrends™
- Veeam®

With a multitude of providers pushing so many solutions to market, it can be difficult to find that just-right-for-you needle in the data protection haystack.

Still, it's a task worth pursuing.

When you do find a next generation architecture that offers solution completeness, scalability, and ease of use, you'll be equipped to meet your current data challenges head-on, while simultaneously improving efficiencies.

Chapter 8:

Shopping for Your Killer Next Generation Solution

When you consider the range of options available on the market—and then dig into the features and functionality being offered by each—making apples-to-apples comparisons becomes a hefty undertaking.

That task becomes especially tricky when vendors aren't abundantly clear about which features are, and aren't, included in their advertised sticker price.

So, what should you keep in mind as you're evaluating your options?

Cut through the hype and determine which features you can count on.

Be sure to ask:

- Is the solution available as a physical or virtual appliance, or both?
- Does the solution offer a unified management console?
    - If it does, how far along is the vendor in its development process?
    - How deeply does its console integrate with the various appliances you'll have to manage?
    - Before you ink a contract, make sure you test drive the integration or see a demo to make sure the solution lives up to the vendor's promises.
- Does the solution feature a cloud-gateway appliance, allowing for backup, data storage, and recovery in the cloud?
- If deduplication is part of the solution's feature set, is it target- or source-side? Or, does it offer both?
- Does the solution feature backup/disaster recovery failover appliances and instant restores?

When it comes to licensing, be sure to read the fine print. Closely.

Ask questions, like:

- Is the license all-inclusive and, if so, can the vendor really deliver?
- Is the vendor licensing a more limited feature set?
  If so, what's the final sticker price after you've added the specialized functionality you'll need?

What should you consider?

We encourage you to pay special attention to the factors that next generation data protection architectures can—and should—deliver.

They are:

- **Platform completeness:** A one-stop-shop for all of your data protection needs
- **Unified technologies:** Seamless integration under the hood, eliminating impenetrable data silos
- **Virtualization:** Virtual machines that allow you to run multiple operating systems and applications on a single physical server
- **Ease of use:** User-focused design that empowers the IT generalist to deploy and manage the solution
- **Instant failover/BMR:** High availability and disaster recovery that ensure business continuity
- **Replication:** Increased fault tolerance through automated data replication
- **Tape/Archive:** Supports replication to tape for added reliability
- **Data reduction:** Target-based or more efficient source-side deduplication which reduce the total amount of data you must protect
- **Cloud service:** Improved ability to move data to the cloud and manage it

Want to know how the heavy hitters stack up?

	Arcserve UDP7000	CommVault	Dell	Symantec Backup Exec 2014	Unitrends	Veeam
PLATFORM COMPLETENESS	●	◕	◕	◕	◑	◑
Unified	●	●	●	◑	◕	◔
Virtualization	●	◕	◕	◕	◑	●
Ease of Use	●	◔	●	◑	◕	◕
Instant Failover/BMR	●	○	◕	○	◕	◔
Replication	●	◕	◕	○	◕	◑
Tape/Archive	●	●	◑	◕	◑	◔
Data Reduction	●	●	◕	◕	◑	◑
Cloud Service	◕	●	◑	◑	●	◔

○ None ◔ Basic ◑ Average ◕ Advanced ● Best

Source: Arcserve

Of course, no solution is right for every organization, so be armed with your architecture requirements and investigate carefully to find the one that's perfect for you.

Chapter 9:

Arcserve UDP

It's your reputation on the line. How much are you willing to leave to chance?

With Arcserve UDP, you can count on the industry's first complete data protection appliance, featuring both Assured Recovery™ and cloud-native capabilities.

> As a Managed Service Provider company that deals with disaster recovery…I'll sleep better at night knowing that my customer sites have the UDP appliance protecting their data.
>
> – Ian Richardson, CEO, Doberman Technologies

What's in it for you?

Arcserve UDP alleviates some of the stressors of your complex job with benefits, like:

- ✓ **A simplified data protection and recovery architecture and a unified management console that offer set-it-and-forget-it ease**
- ✓ **Significantly improved data and system protection and recovery options over legacy point solutions**
- ✓ **Vastly improved operational efficiencies and cost reductions**

What will Arcserve UDP deliver?

Arcserve UDP offers a turnkey data protection and recovery software and appliance architecture with backup, replication, and true global deduplication **standard**. It's the most highly integrated image-based data protection solution on the market, as well.

Arcserve UDP also offers:

- A high availability backup/disaster recovery failover appliance, including capabilities support for three standby virtual machines
- Cloud-native software and appliance capabilities allowing you to seamlessly replicate data to public and private cloud services, as well as MSPs
- Both virtual **and** physical server protection—**the only unified software and appliance solution on the market to do so**
- A highly scalable architecture that grows with you when you leverage the appliance and software together
- A leading-edge software and appliance unified management console
- Software that delivers automated disaster recovery testing of business-critical systems, applications, and data—all without business downtime or impact to production systems
- All-inclusive software licensing, based upon CPU sockets (physical or virtual) or per TB of protected data

And if that wasn't enough, it's also easy to use and simple to deploy. So simple, in fact, that you can unbox the appliance and deploy the solution in 15 minutes.

> “As a long-term Arcserve customer, I'm really impressed with this new breed of appliance. I'm not the IT guy and I set up the Arcserve UDP Appliance myself. It's easy to deploy and has lots of features including the deduplication which is very efficient.”
>
> – Gary Hirschfield, Director, Administration, Sunrise Capital

The fact is your job's not a picnic, but now you can breathe easy. Why? Because Arcserve UDP is exactly that. **A picnic**. (Or perhaps a walk in the park. Either way, you're in the park and not staring at a screen. Enjoy your new-found freedom, my friend.)