



 **kascade**® x **druva** 

## Building a Resilient Data Protection Strategy



# The data protection landscape of today

**Technology has rapidly evolved, most recently moving from server backups to backing up virtual machines. Those straightforward days are long gone.**

**Now, as we embrace a multi-cloud strategy, the data protection landscape has drastically changed—data is no longer centralised but scattered across various platforms, complicating our backup strategies considerably.**

But that's not all. Data protection today is about so much more than just safeguarding against system failures or natural disasters. We are under constant threat, and attackers are becoming increasingly savvy. It's alarming, but people are actively seeking out vulnerabilities in backup and disaster recovery technologies. Cyber-attacks, data theft, and ransomware are now part of our everyday conversations about security. This reality demands a vigilant and robust approach to data protection—because having the right technology isn't enough.

What's surprising is that while many organisations are quick to update their IT strategies to keep up with these changes, their protection strategies often fall by the wayside. Sure, quick fixes can solve immediate problems, but they don't tackle the root causes that a comprehensive data protection strategy can.

That's where this guide comes in! We're here to walk you through the essentials of modern data protection and help you develop a strategy that's not just effective but resilient. No matter where you currently stand with your data protection, use this guide as a roadmap to assess and improve your approach. Let's start on this journey together to build a backup plan that meets the demands of today's dynamic technology landscape—because your data's safety is more important than ever!

# Why it's time to rethink data protection

**Too often, we create these plans, only to put them to one side when the daily grind kicks in.**

**But here's the reality:** with the rapid pace of change and the escalating threats we face today, it's time to wake up and take a hard look at your strategies. Ignoring data protection is a gamble you can't afford to take. The consequence of not acting can be devastating and can result in data loss, downtime, and irreversible damage to your reputation. Now is the moment to rethink your approach, refine your strategies, and strengthen your defences.







# Backup

**In today's fast-paced digital landscape, backup technology has evolved far beyond just being a safety net for your files and virtual machines.**


It's now a vital component of your overall data protection and security strategy. Think of it as your last line of defence against cyber incidents.

However, we're living in a world where users are constantly on the move, using multiple SaaS applications and generating data at an unprecedented rate. For many, the response to these modern work practices has been to put together quick fixes for their backup needs, often leading to a mishmash of systems to manage different types of data. While this approach may provide temporary relief, it can create chaos down the road—think more alerts, more complexity, and a frustrating lack of standardisation.

Here's the harsh reality: during the early stages of a destructive ransomware attack, cybercriminals often target backups and infrastructure. They'll try to delete or destroy backup data, making it significantly harder for you to recover and potentially pushing you towards paying the ransom.


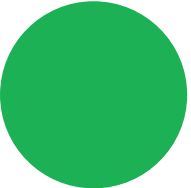
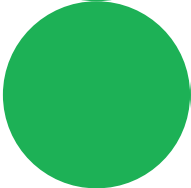
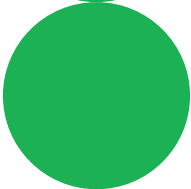
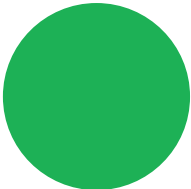
This makes on-premises backup services particularly vulnerable unless you take the necessary steps to strengthen it. And don't forget with many SaaS applications and services, you have likely agreed to their Shared Responsibility Model. That means you still have a key role in protecting and backing up your data! It's a common misconception that SaaS providers handle everything, but the reality is, security is a team effort. Both you and the provider have responsibilities to ensure your data stays safe. We've seen people get caught off guard by this, so it's definitely something to keep in mind!

Let's be honest, while you totally understand the importance of effective backups, it's all too easy to let this crucial area slip through the cracks when you're caught up in the day to day. It's tempting to push it aside, especially when everything seems to be running smoothly. But here's the thing: when that moment arrives and you need to restore your backup, you'll find yourself wishing you hadn't overlooked it.



# So, what does a robust backup strategy look like today?

Here are some key principles and recommendations to help you assess the resilience of your backup approach:



## Be resilient

Ransomware attacks are designed to undermine your recovery efforts, and that's why your backup service must be resilient against these threats. It's crucial that your backups are immutable, meaning they can't be altered or deleted once created. This way, your data remains true to its original state, providing you with peace of mind. And don't forget about encryption—your backups should be encrypted by default, adding an extra layer of protection!

## Multiple copies

You've likely heard about the 3-2-1 backup strategy: where you need at least three copies of your data, on at least two different media, and at least one copy offsite. And that is just the minimum standard. Even in a cloud-centric world, this principle is still relevant. However, remember that your copies should be independent of one another; they shouldn't be linked in a way that could jeopardise your data's integrity.

When considering your backup strategy, think about frameworks like the Grandfather-Father-Son approach. You'll want to make sure technology allows you to restore earlier versions of your data even if the latest ones are corrupted. It's all about having the right tools in place to safeguard your valuable information! The right tools will even help you to identify and recover good clean data, even if it means restoring from multiple backups.

## Utilise Insights

Attackers often hope their attempts to compromise your data go unnoticed, which can be a sign of a broader attack on your organisation. A good cloud backup service should be able to detect anomalies and unusual changes and raise alerts when something doesn't seem right. Imagine getting notified about mass deletion requests, unusual file activity, or changes to retention periods—all crucial indicators of potential threats. Ask yourself; if someone was changing invoicing details in my organisation, would my backup technology be able to alert me of this?

In addition to this, it is important to make sure that your backup system includes alert mechanisms that remain effective even if your infrastructure is compromised. For example, if an administrator account is involved in a suspicious change, you should receive immediate alerts about those accounts. And if the worst happens and one of these accounts is compromised, having features like an immutable recycle bin can be a lifesaver—ensuring that anything deleted isn't lost forever.

With these considerations in mind, now's the perfect time to evaluate your backup technology and strategy. Does your current setup effectively tackle these challenges? Modern cloud-based backup solutions integrate all these essential elements into a single platform. Your backup should be a source of clarity, providing standardised insights into the health of all your backups—all in one place.



# Disaster Recovery

**Disaster Recovery (DR) is a cornerstone of any robust data protection strategy, but let's face it, the DR landscape has changed dramatically in recent years!**

Gone are the days of maintaining costly physical DR sites that lead to double the expenses, double the maintenance, and double the headaches. Today's challenges are multifaceted and require us to rethink how we approach disaster recovery.

As organisations increasingly adopt hybrid cloud strategies, data is becoming more fragmented. Whether you're moving parts of your environment to the cloud, or making the leap from one hypervisor to another, DR isn't just about replicating one on-premises site to another anymore. It's a whole new ball game!

And to add to these changes, the need to test DR never stops. So ask yourself, when did I last test my DR strategy? We know it can be time consuming and one of those activities that just keeps getting bumped down the list, but when disaster strikes and you need that plan, you'll be much more calm and composed if you know that recovery will work as you only tested it recently. Surely that peace of mind is priceless?





# So, how can you revamp your DR strategy to tackle these modern challenges?

Here are some key considerations and recommendations to elevate your DR game:

## Embrace the cloud

A cloud-based approach to DR has rapidly become the gold standard! By using a cloud solution, you can cut costs significantly. No more paying for double the hardware—you only incur costs when you activate your site. Plus, maintenance becomes a breeze! Say goodbye to the headache of managing version upgrades on your hardware. With cloud-based DR, you can secure all your data in one central location, even if you're operating on a hybrid cloud model. Your technology should facilitate seamless replication of data from both on-premises and cloud environments, giving you a single platform to monitor everything with ease.

## Plan for every scenario

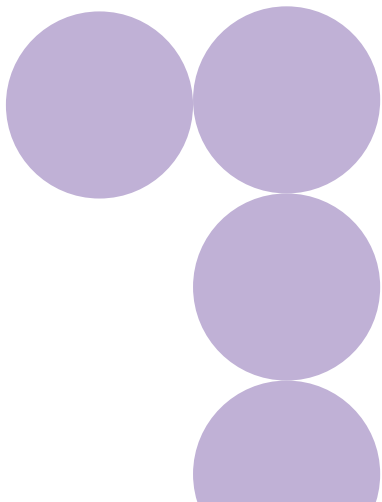
A flawless DR strategy must account for all possible scenarios. There's no shortcut here; you need to invest time and effort to consider every potential situation and make sure your DR plan is flexible. As you develop your strategy, remember to test various recovery scenarios—full recoveries and partial recoveries. And don't forget that part of your planning needs to include the users and you need to make sure you have a solid communication plan in place for users during a DR event. Many organisations dive straight into planning for a full failover but neglect the equally important partial failover strategies. When a real incident occurs, being caught off guard can be a recipe for disaster!

And let's not forget about failback planning! It's crucial to have a plan for returning to normal operations once the dust settles. Don't let this become another source of panic—use this as an opportunity to evaluate your strategy. Are you confident in its flexibility, or is it time to revisit and refine your approach?

## Involve the business

While DR often falls under the IT umbrella, it's truly a business solution. Engaging business leaders in the process is vital for creating a solid DR strategy. Together, you can determine your Maximum Tolerable Downtime (MTD) and Maximum Tolerable Data Loss (MTDL). These are critical metrics that should be defined by business leaders and your IT team. This collaboration makes sure that your team can establish appropriate Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) that align with the organisation's real needs. Without this valuable insight, IT might misjudge the actual business impact of an incident.

Rethinking your disaster recovery strategy isn't just a nice-to-have—it's a necessity. By embracing cloud solutions, meticulously planning for every possible scenario, and involving business leaders in the conversation, you can create a DR strategy that not only protects your organisation but also strengthens its resilience. Remember, a robust disaster recovery plan is not merely a safety net; it's a strategic advantage that can empower your organisation to bounce back quickly and effectively. So take the time to assess and refine your approach—your business's future may depend on it!



# Where to start?

**You should now understand what gaps you may have in your data protection strategy and how to improve your resilience.**

Now it's time to roll up your sleeves and get to work on your data protection strategy. And if you already have a plan in place, think of this as a fantastic opportunity for a little spring cleaning—time to review, refine, and strengthen your current approach!

## Step 1



### Understanding your data landscape

First, let's identify exactly what data you need to protect. Ask yourself: What kind of data am I safeguarding? Where does this data live? What threats am I guarding against? Clarifying these points will help you tailor the perfect strategy for your organisation and pinpoint where to focus your attention.

How do you start gathering this intel? Kick things off by creating a service catalogue. This should be a team effort between IT and your users. Approach it from a user's perspective—list all the services in use, the type of information they handle, and how they're utilised. Map these services to your systems for a comprehensive view of all the systems at play and the data they contain.

## Step 2



### Identify your crown jewels

Next, let's define what 'sensitive data' means for your organisation. This will be personal to your business and the data you hold. For some, it might be personally identifiable information (PII). For others, it could be confidential materials like IP, designs, or even those secret family recipes (looking at you, culinary empires!).

Understanding what your 'crown jewels' are, where they're stored, who can access them, and how they're protected is crucial for a solid strategy. And once you're confident you know what your crown jewels are and where they reside, make sure you understand the process you need to follow if there is a breach.

## Step 3



### Map out your protection tiers

With your sensitive data pinned down and a clear view from your service catalogue, it's time to structure your data protection tiers—think Bronze, Silver, Gold. This setup will help you prioritise your recovery efforts, whether you're restoring from a backup or activating your disaster recovery (DR) plan.

Make sure your tiers align with your Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) to make sure your business can bounce back swiftly and effectively, recovering the right information in the right order.





# Test, test and test again

**Your data protection strategy is only as good as your last test.**

Be honest with yourself—when was the last time you tested your strategy? Would you be confident if a disaster struck? If the answer is yes, you're ahead of the game!

However, we recommend testing your data protection strategy at least every quarter. If you're currently doing it bi-annually or annually, consider how you can increase that frequency to further strengthen your resilience. You'd be surprised to hear how many people tell us their DR test is overdue when we ask!

Don't just run the same test each time—explore different recovery scenarios. Test partial Virtual Machine recoveries, full DR tests, and single-item recoveries. Remember to think about it from a business perspective, too. For example, if you have externally hosted services, how will these function within your DR environment? Engage your users in the testing process—they'll quickly point out anything that doesn't feel right!

## **After testing, document everything**

What worked? What didn't? What improvements are needed? Assign actions and review them during your next test. Remember, data protection is a continuous cycle of improvement, and if you're not actively working on improvements, we start to worry on your behalf!

# Ready your response

Now that you've considered your data protection strategy and completed the steps outlined, it's time to make sure you're fully prepared.

**Here's what we've covered:**

- ✓ **Know what data you're protecting—create a service catalogue.**
- ✓ **Define your crown jewels.**
- ✓ **Create your backup tiers (Bronze, Silver, Gold).**
- ✓ **Define your RTO and RPO.**
- ✓ **Test and document your test results.**

It's time to compile all this information into a comprehensive recovery plan. Think of these documents as the holy grail of your data protection strategy. If you're aiming for ISO accreditation, this documentation is essential!

While it might seem tedious, the more detail you include, the better. Consider scenarios where a disaster strikes while you're on holiday or asleep with Do Not Disturb on. How will your team know what to do without you?

**Make sure your documentation includes:**

- ✓ **Partner details for those responsible for your systems.**
- ✓ **Step-by-step guides for launching your disaster recovery environment.**
- ✓ **A prioritised recovery plan (using your RTO's to define this) and remember to consider any dependencies that may be required to get certain applications back.**

Also, think about where these documents will be stored. You need to ensure that the documents are accessible to those that need it, even during a cyber attack. As such, your file server or SharePoint repository may not be the best option.

Lastly, remember to review these documents regularly. They are only as accurate as the last time you reviewed them. When you need your DR plan, you want to avoid the stress of realising it hasn't been updated in three years and is lost in your overflowing inbox!

## Why Kascade?

**At Kascade, we've been reviewing and implementing data protection strategies for over 25 years.**

We know this area is crucial for every organisation, yet it's often overlooked with the day-to-day.

That's where we step in! While you focus on the day-to-day, our data protection services are here to take the weight off your shoulders. We understand the challenges you face, and we're dedicated to making your life easier. With Kascade's experts on your side, you can enjoy transparency and peace of mind knowing that your backups are being regularly checked and your disaster recovery strategy is being tested. So when the time comes, you can be rest assured that everything has been thoroughly taken care of—no details overlooked!



## Kascade Backup

**Our next-generation backup service is as versatile as a Swiss Army knife.**

On-premises? We've got it. In the cloud? Absolutely! SaaS data protection? You bet! With Kascade Backup, powered by Druva, you can consolidate your backup strategy into one central hub, eliminating the fragmentation of your critical data.

No more worrying about accidental deletions or the looming threat of ransomware—we've got your back! Our team continuously monitor, manage, and troubleshoot your backups, allowing you to focus on your core business while we make sure your data is safe and recoverable. The best part? It won't break the bank! Our patented global deduplication technology streamlines backups, reducing storage requirements and cutting costs.

### What's included

- ✓ Proactive monitoring and remediation.
- ✓ Zero infrastructure—cloud-based platform.
- ✓ A single platform for all your needs.
- ✓ Data encryption and immutability.
- ✓ Regular testing.
- ✓ Ransomware protection.
- ✓ Peace of mind with support from the Kascade team.



## Kascade Recover

**Kascade Recover provides you with a tailored DR strategy that takes the stress off your plate.**

We run and maintain your recovery infrastructure, fully managing a system designed specifically for your needs through the world-leading Microsoft Azure. And no matter if your VM's are on-premises, in vSphere, Hyper-V or in the Cloud with Azure, Kascade Recover is there to help.

With Kascade Recover using Azure Site Recovery, your business continuity and disaster recovery plans gain the benefits of minimal upkeep and flexibility—plus, it's budget-friendly! Our solutions are designed to fit your business, offering flexible managed services and a fully configured cloud infrastructure.

### What's included

- ✓ Regularly scheduled failover tests.
- ✓ Unplanned failover support.
- ✓ Reporting and post-failover reviews.
- ✓ Annual service reviews.
- ✓ Monitoring of replication.
- ✓ Remediation of replication faults.
- ✓ Peace of mind with support from the Kascade team.



# So, in conclusion

In today's fast-paced and ever-evolving digital landscape, having a robust approach to safeguarding your data is not just a necessity—it's a vital part of your business resilience. Remember, data protection is a continuous journey that requires regular assessment, testing, and adaptation to keep up with new threats and technologies. By understanding your data landscape, defining your sensitive information, and implementing effective backup and disaster recovery strategies, you're not just protecting your organisation; you're empowering it to thrive.

At Kascade, we're here to support you every step of the way, ensuring that your data is not only safe but also recoverable when you need it most. Let's make data protection a priority together, and pave the way for a secure and successful future!

[kascade.co.uk](https://kascade.co.uk)



**Ready to embark  
on your journey  
to data protection  
peace?**

Book a data protection workshop with the experts at Kascade and discover how you can improve your strategy today!