



011010101
101101010
001
010
100
010

Tectrade

Your Data Protection Partner

Spectrum Protect step-by-step

Your guide to planning a better
back-up strategy in the Age of Data

Meeting the challenge of the Age of Data

If you've been in IT for any length of time, you'll know today's landscape is a completely different one to that of only a few years ago. In the Age of Data businesses are doing more than just storing information, they're focusing on how they can use it to deliver meaningful, profitable insights about their businesses and their customers.

Today, the critical importance of data to a business's success means availability and data protection are more in the spotlight than ever before. And if you're a Tivoli Storage Manager (Spectrum Protect) user, this has a direct impact on how you safeguard your business.

The increasing price of valuable data

Like many companies, you're probably finding the data you're protecting with Spectrum Protect is growing at a phenomenal rate. And this massive data growth is having a significant effect - increasing costs, consuming resources and narrowing back-up windows to name just three. In fact, by 2020, it's expected the average enterprise will manage 50 times more information than it does today but with only 1.5 times more IT staff.

The result? Many companies have quickly realised they need to re-evaluate how they approach backing up and protecting their critical data as it becomes more valuable by the day.

Sadly, however, some users on older versions of Spectrum Protect are being left behind, simply unable to keep up with the demands of enterprise back-up in the Age of Data.

Backing-up for the future

In this short guide, we're going to look at how you can begin to plan more effective back-up strategies for your business by highlighting the four key areas of concern we see regularly when working with new clients.

Step 1: Match capacity constraints to business demands

In today's Age of Data, IT professionals are faced with a significant challenge: how to quickly protect data as it accelerates in multiple directions with diminished physical resources. Continuing to fill your traditional tape library is not an option as many enterprises are faced with the real possibility of running out of physical space in the next few years.

So step one is about getting a better view of the problem, using your Spectrum Protect reports to audit and identify the main culprits in your data explosion

High value vs. Low value data

In our experience, running an audit often reveals low-value and rarely used servers taking up more resources and incurring more costs than they should.

By clearly identifying which data sources are consuming the most resources, you can make a informed decision on whether you have the capacity (and are willing) to support and protect data which is of low value to your business.

Alternatively, you may choose to either adjust your back-up schedule for this type of data or archive some of it completely.

“Step one is about getting a better view of the problem.”

Key learning:

Not all data is equal. Identify the biggest data consumers and assess value of the data vs. the cost of managing it.

Step 1: Match capacity constraints to business demands

Checklist

Get a clear picture of all the servers, apps and data silos you need to back up

Arrange them in descending order in terms of data volume to be backed up

Speak to the relevant stakeholders for that data to understand its importance to your business

Identify which data is high volume but low importance and identify whether it can be treated differently to avoid impacting on the security of your core back-ups

Step 2: Identify dangerous bottlenecks

Although much of the discussion on backing up data revolves around volume and capacity issues, 'time' is always the key focus when there is a problem. Simply, you need to know how quickly your business can get back up and running after an incident. Will it take seconds, hours or days?

Your back-up strategy more than likely has established Recovery Time Objectives (RTOs) in place which identify how quickly any lost data must be recovered in an emergency. You will also have Recovery Point Objectives (RPOs) outlining the amount of data your business is prepared to lose in any single event. But for both RTOs and RPOs, if you're to achieve aggressive targets, you need to make full use of the back-up windows you have available.

The problem is: With the exponential growth in data, these back-up windows are becoming ever tighter and if your critical data misses its slot, your RTO and RPO targets could be placed in serious jeopardy. And that's why step #2 focuses on identifying bottlenecks.

Get close up to the back-up process

To get a clear picture of any real or potential bottlenecks, whether related to data, systems or people, you need put the entire back-up process under scrutiny.

The data volumes audit from step #1 will help, but you also need to track each step of the back-up process to see where time is being lost and where new approaches could reduce or eliminate bottlenecks, helping to protect your business.

For example, the latest version of Spectrum Protect provides a 10x improvement on Spectrum Protect-based deduplication. So less data needs to be backed up which will save you a significant amount of (often critical) time.

Put mission-critical data first

By auditing the entire back-up process, you can take active steps to ensure your most important data is always backed up without fail (even if this comes at the expense of other less mission-critical information). Because, ultimately, nothing should compromise your ability to back-up the right data at the right time.

"If you're to achieve aggressive targets, you need to make full use of the back-up windows you have available."

Key learning:

It's not just how much data you need to back up that's important, but which data gets priority.

Step 2: Identify dangerous bottlenecks

Checklist

Take a long hard look at whether you're able to meet your RTOs and RPOs within your current back-up window

Understand how much time is being spent on each step (again, both by people and systems)

Project this forward six months - will you still be able to meet those objectives when data volumes have risen?

For each of these stages, first identify any areas that can be eliminated (e.g. by archiving a set of data)

Break down the entire back-up process by its constituent steps. Make sure you include both machine and human activity

Then look at where time-saving efficiencies can be found (eg better deduplication, reconfiguring hardware, upgrading systems, etc.)

Step 3: Ensure your back-up strategy supports your business strategy

Yes, a key focus of most back-up strategies is to protect the business's data. But all too often, this leads to companies adopting a hoarding approach – treating all data the same, no matter what its level of importance, and then retaining it forever. Or else they develop very granular policies that create high levels of complexity – consuming more IT resources than necessary and increasing opportunities for costly mistakes.

A better solution is to create a back-up strategy that supports and protects your core business. To do this you need a clear view of the data within your business and how it should be treated. This is where a back-up catalogue has infinite value.

Get clarity with a back-up catalogue

At its core, a back-up catalogue matches the needs of your business with the critical recovery times for key data sets – both for onsite and offsite data whether structured or unstructured. In essence, it needs to document not just what you're backing up but why and for how long.

Your back-up catalogue should begin with identifying the key business objectives related to different data sets. It should specify meaningful RTOs and RPOs for each data type together with any specific retention rules (e.g. where your business needs to comply with industry regulations on data retention). With this foundation in place, you can create specific data back-up policies focused on serving the core needs of your business and make realistic investments based on both tangible business value and compliance requirements.

“With this foundation in place, you can create specific data back-up policies focused on serving the core needs of your business.”

Key learning:

Use a back-up catalogue to align your data protection strategy with your wider business strategy.

Step 3: Ensure your back-up strategy supports your business strategy

Checklist

Use the list of data sources you assembled in step #1 as a master list of data to be backed up

For each group, assign an RPO, RTO and retention period

Putting the data groups in order of RTO should mean the most important data to the business comes at the top of the list

If all data groups have the same RTO and RPO, you're probably giving low-value data too high a prominence (which could potentially compromise the performance of your back-up regime)

Look for any data groups that don't conform to this priority rating - do they deserve their rank?

Re-assign RTOs and RPOs in line with the data's real importance to the business



Step 4: Take advantage of Spectrum Protect innovations

Spectrum Protect has been trusted by many of the world's most demanding organisations for decades. Because of its longevity, some businesses have been content to remain on older versions (e.g. 5x). But as data has grown in size and importance, these older versions haven't moved with the times, limiting these users' options.

Stay on track to get ahead

You can't afford to be complacent. You need to review your business's back-up strategy on a regular basis (at least yearly). Or when there's a major event, like a merger or a new site, which will have a material impact on your data volumes. By doing so, many organisations have identified key changes which have resulted in them re-evaluating their Spectrum Protect solution.

Spectrum Protect 7.X – back up for the age of data

Newer versions of Spectrum Protect, like Spectrum Protect 7.x, tackle the Age of Data head on with new capabilities totally aligned to the daunting levels of data

enterprises must deal with today. Since Spectrum Protect 5.x, the internal database has been re-architected from the ground up to deliver far greater performance and better support for today's apps and operating systems, including virtual machines and cloud-based environments.

The current version's deduplication and node replication capabilities also decrease the amount of data you must back up, lessening capacity pressures and reducing costs.

Which all begs the question: If you're on an older version of Spectrum Protect, shouldn't you be re-evaluating whether it's still the best option for your business today?

“Shouldn't you be re-evaluating whether it's still the best option for your business today?”

Key learning:

Enterprise data has moved on, make sure your Spectrum Protect solution keeps pace.

Step 4: Take advantage of Spectrum Protect innovations

Checklist

Check which version of Spectrum Protect you are currently using (be aware that if you are on 5.x, it's no longer supported by IBM)

Assess the improvements you could achieve with an upgrade to the latest version (greater capacity, reduced bottlenecks, better performance, support for the latest applications, storage deployment models, etc)

Look at whether this could deliver the protection you need at an acceptable ROI

Book your Spectrum Protect Healthcheck

Data is the life force that drives your business, so it's imperative to ensure your Spectrum Protect configuration is as healthy as it should be!

Luckily, the Tectrade experts have the tools, experience and knowledge to help diagnose your unique data challenges and provide consultative advice on what to do next.

We'll help you find a solution that helps meet your business goals, and turn Spectrum Protect into a more powerful tool than you've ever realised.

It's easier than you think.

[Find out more](#)



We will take personal responsibility for ensuring you achieve your data goals

The current explosion in volume, velocity and variety of data has left many organisations battling to realise data's value, and minimise its cost.

Tectrade works with complex organisations, with ambitious aims and modern data requirements. It's complicated, demanding work. But it's work we love.

However great your data challenge, we will never walk away. It's simply not in our

character. We relish tackling new problems, and positively thrive on delivering the almost-impossible.

Tectrade provides global expertise in data management. With international operations, over 20 years of experience and 50+ technical specialists, Tectrade has helped hundreds of clients to gain comprehensive control of their data, and manage it effectively as their organisation grows.

At Tectrade, we live and breathe data. It's in our DNA. And we're relentless in finding the solution that's right for your business. With teams in Europe, and the US, we can deliver projects and managed services on a truly global scale.

[Tectrade.com](https://www.tectrade.com)

UK

River Court, Mill Lane
Godalming, Surrey GU7 1EZ
+44 1483 861448
info@tectrade.com

US

1460 Broadway
New York, 10036
+1 646 493 9811
info@tectrade.com

011010101
101101010
001
010
100
010

Tectrade
Your Data Protection Partner