

3 steps to improve storage resiliency

Data must flow, but it must
also be stored, securely

Data drives just about every aspect of our modern economies, it yields insights and drives decisions that create value. It is both a resource and an asset, and it must be protected. Not just because it represents monetary value, but because it is also a critical factor of an organisation's DNA as well as the identities of each individual that interacts with its operations.



IBM
Platinum Partner


Computacenter



Storage is key to an organisation's ability to leverage the value of its data. It should be available instantly, to be combined with different datasets to spark innovation, as well as deliver accurate real-time information. Without proper security, data is eminently vulnerable, and there are legions of bad actors out there who want to steal, corrupt, or lock-it up for ransom.

Computacenter partners with IBM to enable an organisation's data to flow freely and securely. That's the way it can be used to deliver services, create products, enhance lives and communities, and deliver what people want and need; products and services that we all take for granted. Our services prioritise data security and privacy, areas which are heavily regulated. That regulation is necessary not only to protect the integrity of each organisation – private or public – but also to protect each one of us as individuals. It's why the regulations are strict and why the penalties for breaches are severe.

The challenges:

Cybercrime, complexity, skills shortages and inadequate storage

Research and strategy specialist, ESG, pointed out that as data becomes more transformative, so the threats rise and the challenges multiply. More and more investment is going into leveraging the value of data, for instance by applying fast-evolving AI tools, but there are still gaps in how organisations store their data securely.

Good storage enhances the value of data, not just because it protects it but because it enables the data to be readily available for use and combination. And resilient storage practices means that data can flow safe in the knowledge that it is protected from attack as well as intelligently stored for quick and easy access.

Resilience is all about creating a range of protocols and systems that work together to protect data, back it up, and ensure that all systems are compliant with an evolving regulatory landscape. Too often, storage is seen as being all about backup, and often backups aren't as well protected as primary datasets. In fact, backups have to be just as protected. They must also be dynamic, that is, constantly updated to ensure they are current.

Cybercriminals target both primary and backup datasets. They know that if the backups are secure their attack won't come to anything. That's why they try and attack every element of an organisation's IT system.

IT complexity is also a problem. Complex systems are hard to understand, which means it's more likely there will be gaps, errors, and vulnerabilities which hackers can exploit to disable an organisation. The attack could start with the backup and infiltrate primary datasets.

First objective should be to create different layers of protection without creating complexity. That's why it's important to work with partners that can deliver a balance between a smooth flow of actionable data whilst creating a resilient architecture that can protect both the data and the operations and activities which depend upon its integrity.



Step 1:

Implement multi-layered data protection

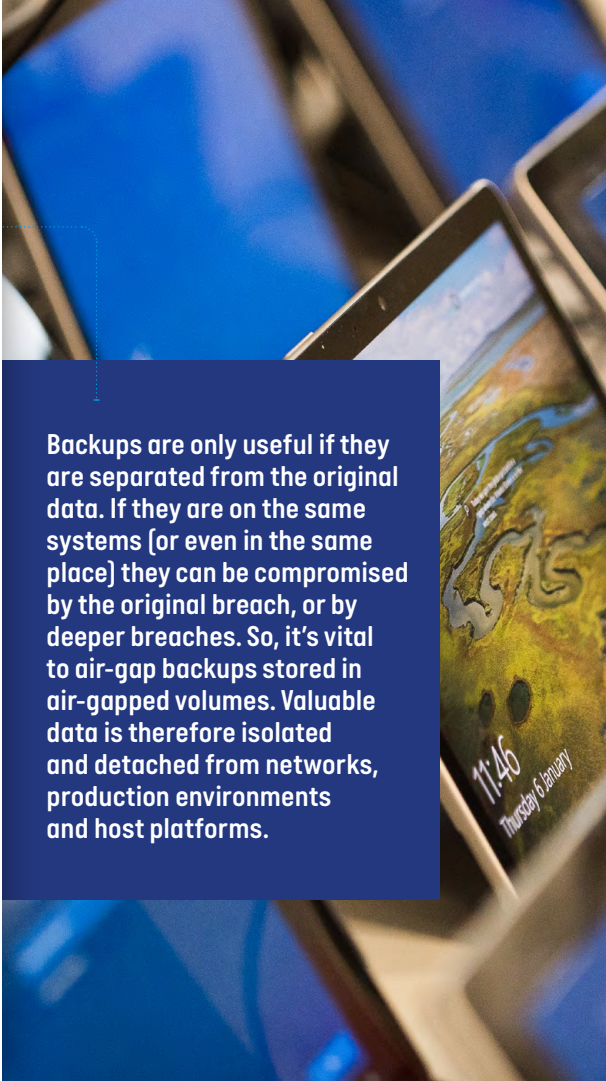
The ability to prevent data loss while maintaining data integrity is integral to the ability to recover faster from an event or breach that compromises access to vital data. Minimising downtime and disruptions to services means organisations can protect people and customers as well as the value of business. That's also important in terms of reputation and governance.

The ability to have multiple data recovery options depends on multi-layered data protection. Organisations need good data discovery, copy management and access control, but there are three core technologies which deliver greater resiliency. Adding more layers to data protection – without adding to complexity – means making life harder for the hackers. They have to break through more layers of security which are physical, administrative, and technical. The goal is to organise them so that they overlap without interfering with the operation function.

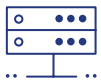
Encryption is at the core of data security.

Multi-factor authentication, data backup, and recovery systems all work together to secure data from bad actors whilst making it available to people and customers. Intelligently scrambling data so it becomes a secret code which can only be used by approved (and proven) individuals or organisations is the vital layer of protection.

Immutable data snapshots differ from traditional ones because they can't be modified. That means it can be trusted as an authentic reference point for data recovery. Time after time, any time it's needed. Once recovered there's no chance that it could turn out to be infected with malware and undermine data or operations.



Backups are only useful if they are separated from the original data. If they are on the same systems (or even in the same place) they can be compromised by the original breach, or by deeper breaches. So, it's vital to air-gap backups stored in air-gapped volumes. Valuable data is therefore isolated and detached from networks, production environments and host platforms.



Step 2:

Leverage advanced storage technologies

Resilience in a fast-moving world means working to stay ahead of not just emerging technologies like Gen AI, but working with partners who are driving that change. It's how organisations can focus on core objectives without the need to attract IT skills at a time when they are in short supply and expensive.

Computacenter's more than three-decade relationship with IBM delivers the best IT skills and intelligence so organisations can leverage the power of proven technologies now, while staying ahead of change.

IBM's FlashSystem delivers industry-leading performance and cost-efficiency. Critically, its hybrid flash arrays simplify hybrid cloud storage so that if attacked, recovery is achieved as quickly as possible. Backups are constant and done in a 'flash'. That speed enables streamlined data management, optimise storage and networking with AI-powered predictive analytics. Organisations can operate with confidence knowing that simple operation is combined with high performance.

Critically, storage resiliency is improved because data is replicated across hybrid environments and constantly kept up-to-date.

The principle to storage resiliency is 100% data availability combined with total confidence in the ability to recover quickly from any outage or attack, confident in the knowledge that immutable snapshots and air-gapped backups will enable organisations to keep running while they recover.



Step 3:

Conduct regular storage assessments

Regularly assessing an organisation's data storage arrangements is just as important as deploying the best technologies. It might sound mundane, but it's one of the top five issues for IT leaders.¹

Computacenter works with organisations to conduct assessments and ask the most pertinent questions at the right times. And it's important to conduct that exercise regularly. Cyberthreats evolve constantly so it's important to be agile in adapting existing technologies and adopting new ones to ensure data protection.

Computacenter stresses the need to examine data storage infrastructure regularly to check that it's not just efficient but also resilient. Can it protect over the long term? Does it need to be adjusted, added to, or changed for something new? It's important to take a long view of the threat landscape, as well as the data needs of organisations.

Computacenter assess the location of data. Where it's stored is just as important as how it's stored. Backups should be as protected as original datasets; they also need to be current and accurate. Data is the engine of modern organisations, so it should be constantly managed as well as protected.

We also ensure that the way organisations store and protect data is compliant to an array of regulations in different territories. Compliance is vital because it helps create a security-first mindset, improves governance, sustainability, and protects vital data assets. Being on the wrong side of data storage protocols not only threatens data but could lead to reputational damage.



Computacenter provides services to check organisations' cloud configuration to ensure they are in good shape to achieve data recovery if needed, and on a more practical level, ensures that storage capacity is sufficient for swift data recovery.

¹ 10 data storage questions for enterprises to ask, TechTarget.com, October 2023.

Resilient storage is the foundation for dynamic data

Data is the engine of modern organisations. The way they store data can either hinder its use or speed its transformation into value.

Computacenter's ability to leverage the power of IBM's FlashSystem technologies means organisations can achieve the resiliency needed to use their data with confidence. Data is easy to access because it's stored intelligently. It can be constantly updated and added to whilst being protected, backed up and managed so that it becomes a dynamic resource to rely on.

Resilience is the power to bounce back as well as protect. When an organisation knows where its data is, and that it is being intelligently and securely backed up, then it can operate with confidence. Protect business, reputation, and empower people to deliver objectives and serve customers confidently.



Computacenter's long experience in harnessing the power of data whilst ensuring its integrity through IBM's market-leading solutions, is a resource that every organisation needs to take advantage of. We can assess current storage arrangements, identify needs and improvements, and get to work so that data storage becomes an asset to an organisation.

Discover more

Computacenter and IBM implement resilient, secure, and high-performance storage systems that protect your data and keep your operations running smoothly.

To find out more about how Computacenter and IBM can help you optimise your organisation's storage solutions, contact your Computacenter Account Manager, call **01707 631000** or email **enquiries@computacenter.com**.

About Computacenter

Computacenter is a leading independent technology and services provider, trusted by large corporate and public sector organisations. We are a responsible business that believes in winning together for our people and our planet. We help our customers to Source, Transform and Manage their technology infrastructure to deliver digital transformation, enabling people and their business. Computacenter is a public company quoted on the London Stock Exchange (CCC.L) and a member of the FTSE 250. Computacenter employs over 20,000 people worldwide.

www.computacenter.com



Computacenter