intercity

The essential guide to

BACKUP & DISASTER RECOVERY AS A SERVICE

(BaaS & DRaaS)

Intercity explains what BaaS and DRaaS are, how they work and how they can improve your business.

CONTENTS

WHAT MAKES BAAS THE BEST BACKUP TECHNOLOGY?

BaaS has numerous advantages over other forms of backup:

Resilient

Your data is stored offsite. It is safe, whatever happens to your office. If your office is struck by fire, flood or theft, the data that drives your business will survive.

Technically Secure

Your data is encrypted before it is sent from your offices, while it is stored at the datacentre and before it is sent back to you.

Physically Secure

Physical access to the datacentre that stores your data is controlled and limited to screened and authorised personnel. At Intercity, there are several levels of ID and biometric access controls.

Reliable

The datacentre that stores your data will incorporate numerous levels of systems redundancy. There will be no single point of failure that could prevent you accessing your data. The computer hardware as well as the power, safety and environmental systems will be duplicated. The best datacentres have the capability to perform system updates without any downtime. It is not economically practical for individual businesses to build such redundancy into their own server rooms.

Fast

BaaS is built on frequent, small, incremental backups – they only backup what has changed since the last backup. These can be run over normal broadband connections without interfering with your business' day-to-day activities.

Future proof

Computer and storage technologies evolve. Tape drives develop from DAT to DLT to LTO. Network storage changes from NAS to SAN. New database and communications systems emerge every year. You have to keep your backup hardware and software current with these changes if you run your own backup system. It is complex, expensive and never-ending. With BaaS, that becomes the responsibility of your service provider.

Scalable

As your business grows and its processes become more advanced, the volume of data you want to backup will grow too. BaaS grows with you. You pay for the service per terabyte (TB) of data stored. There is no upper limit. If you maintain your own backup system you have to continually increase capacity and modify processes to accommodate the extra data.

Flexible

A BaaS service can be provided to suit any level of expertise. Self-service suits those organisations with an expert IT department that can handle all aspects of their backup and recovery process. A managed service suits businesses without that level of expertise. The service provider monitors the health of the backup processes and provides human support as necessary.

Automated

BaaS is the ultimate 'fire and forget' service. Once configured, you don't have to change anything. It continues to run even if the volume of data you need backed up changes. There's no need to change tapes and no need to monitor capacity on your network storage.

Identifiable legal safeguards

The data you store on your computers has to be kept protected and private. Even if GDPR didn't insist on it, we all have a moral obligation to respect the privacy of the people about whom we store information. With a UK-based BaaS service, you know that the same laws and ethical standards that govern the way you store data also govern the way your BaaS provider stores it. You can even visit the datacentre that stores you data.

Economical

BaaS and DRaaS protect you from the spikes in costs that happen every time you need to refresh your backup hardware and software. With backup technology and storage volumes evolving so fast, updates need to happen every three to five years. These can be an unwelcome expense to any IT department that's already under pressure to reduce costs and improve services. BaaS and DRaaS avoids the cost.

Reduce Capex

Shifting your backup costs from hardware to an out-sourced service moves it from your CAPEX budget (capital expenditure) to OPEX (operating expenditure). This might be essential if your CAPEX budget has been frozen yet you still need to improve your backup systems. BaaS and DRaaS give you the best backup system without touching CAPEX.

DO YOU REALLY WANT BACKUP, OR IS RESTORING YOUR GOAL?

It seems an odd question. You can't restore data unless you've backed it up first. But the question is more valid than you may think.

Is your goal to backup data? Or, if you think more carefully, is your goal to be able to restore data quickly and easily if you ever need to? Let your answer shape your thinking. A backup that seems to run faultlessly every night is useless if the data is corrupt when you try to restore it.

When assessing backup solutions, whether they are cloud-based BaaS services or local systems, consider the recovery options.

How accessible is the data?

A professional tape-based backup system will store its media in a secure, off-site location. That's safe – but how quickly can you retrieve your media? And how quickly can you find out which media you need to recover? Multi-year archives can be extensive.

Cloud-based backup is more accessible. It is available all day, every day. But does your provider impose limitations on the recovery of data? You need to check.

Can you identify the correct data?

Imagine you backup key databases four times a day. If you need to restore data from four months ago, there could be over 460 instances of the database to choose from. Are they well-managed and logically presented? Does the software make it easy to identify and recover the data you need? Restoring the wrong data can be as disruptive as a hardware failure.

Do you have the skills, staff or service to restore data?

BaaS can be provided as self-service, an assisted-service or a managed service.

Self-service is very popular. It is almost always the cheapest option. But is it right for you? You could discover its limitations when you need it most. You need to consider:

Have your staff gone through the training processes?

Is there an accreditation process so you know you always have staff qualified to restore your data? You don't want them to be learning the processes while the entire company waits for its systems to be restored.

Do your staff understand the business purposes of the data or are they purely technical? For example, is there somebody who understands that if you restore your released software you may also need to restore the appropriate training videos or documentation? Or that restoring design files in CAD means you need to restore corresponding Bill-of-Materials versions in your ERP system? Or that restoring one version of a web form requires a similarly-aged version of a CRM database? BaaS is about business processes, not data. Who understands the interdependency of your data and the systems it serves?

Managed service: If it's a managed service, are staff available 24/7 to assist your recovery?

Are there technical barriers to fast data recovery?

How fast is your broadband connection? Consider this: when you initialise BaaS you have to backup your entire volume of data or server image. The volume of data is so large some service providers send a portable hard disk to collect it.

But what happens when you need to restore?

Do you have to wait for a portable hard disk to be configured and sent back to you? That will be too slow for most organisations facing a crisis.

And remember: **it's the recovery that matters more than the backup.**

Is BaaS the same as "online backup"?

BaaS is sometimes referred to as "online backup". The difference is only one of perception. The concept is the same: the data on your computers is backed up to a cloud service.

The difference is that online backup is usually the type of service you use to backup our home computers whereas BaaS is what our IT departments use at work.

The practical difference is that BaaS makes it easy to backup and restore complex systems such as Exchange databases and entire system images whereas online backup focuses on simpler data files.

What can you backup with BaaS?

BaaS can store anything from simple files such as Word documents, to advanced databases such as Microsoft Exchange to entire virtual machines running VMWare.

The breadth of what BaaS can store explains why it is so closely related to Disaster Recover as a Service (DRaaS). Whereas BaaS tends to focus on the storage and retrieval of files and data, DRaaS focuses on the recovery of entire systems. Only when an entire server is backed up with its operating system, user databases, shares and data can DRaaS be used to help an organisation get running after a disaster.

Although data can be recovered as part of a BaaS programme, it is usually limited to files that have been modified or deleted in error. The volume of data restored is usually limited and specific. It is the type of activity that can happen in the normal course of business.

DRaaS is used when entire systems are inaccessible. It usually follows a major calamity such as a fire, flood or cyber-attack.

What threats does BaaS protect you from?

BaaS protects you from all IT–related threats: accidental deletion, data corruption, hardware failure, natural disasters and cyberattacks.

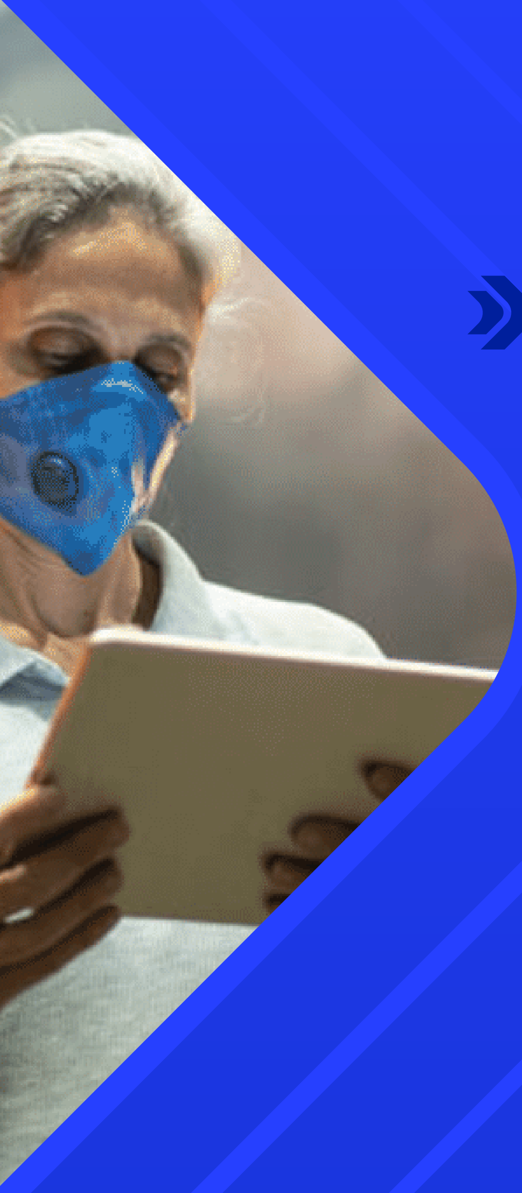
The discipline of backup was born in the 1970s when computer hardware was less reliable than it is today. Hardware failures were common. It was essential that data could be restored from an alternative source.

As computers have become more reliable, humans have become a more common source of contaminated data. We make mistakes and we embed those mistakes in our IT systems. It is now common for backups to be used to recover from human error: a staff member accidentally deletes a document or one staff member overwrites another's work with an older version.

In this situation it must be easy to recover information. If an IT manager has to search through tape archives the recovery probably won't happen. Users will be asked to recreate their work. That's not a productive scenario for the business. BaaS lets the IT manager identify and recover data without leaving their desk.

The same applies to corrupted data. BaaS gives a business an easier and quicker way to recover data than an on–site, physical backup system ever could. When the pricing spreadsheet refuses to open or the deal calculator's database is generating garbage your business' productivity depends on something better than 'start again from scratch'. BaaS gives you the ability to quickly get back to a pristine version of your data.

BaaS and DRaaS deliver business recovery not just data recovery.



BAAS REPRESENTS YOUR LAST LINE OF DEFENCE AGAINST CYBER-ATTACKS SUCH AS A RANSOMWARE LOCK-DOWN.

If user education and anti-virus software have failed, your offsite backups can be used to restore your business to its pre-assault condition.

HOW SECURE IS BAAS?

BaaS is more secure than on-site backup because it has to be. Organisations that send their data off-site demand the reassurance that it is totally safe. This safety comes from four levels: in transit, in storage, in access control and in system redundancy.

In Transit

BaaS encrypts data before it is transmitted from your site to the repository and back again. It is only decrypted once it reaches its destination. If a hacker intercepted the data while it was still in transit it would be indecipherable. The encryption standard adopted by most BaaS systems is AES 256-bit encryption.

In Storage

Once it reaches the repository, the data is re-encrypted as it is stored on the datacentre's servers. In the highly unlikely event that hackers gained access to the repository, the data they would see would not be recoverable. Only an authorised user – the owner or their agent - could decrypt the data.

Access Control

Datacentres adopt a level of physical access similar to military bases. Different measures apply in different service providers but physical access to the building will usually be restricted with even closer control being applied to the datacentre itself. Control measures should include some aspects of biometric identification that cannot be passed between people e.g. fingerprints or iris scans.

System redundancy

Datacentres that offer BaaS services should offer several levels of hardware redundancy. Within the primary site, they will have no single point of failure. The IT systems and components continue uninterrupted if any single part fails. They will even be able to continue during maintenance procedures (for Tier 3 datacentres). The power and cooling systems on which they depend will have redundancy too. The final – but optional – level of redundancy will be to duplicate the backup repository to a different, similarly-equipped datacentre. This would be excessive for most organisations. Under the 3-2-1 rule, the offsite backup is already the second copy of their data.

DO I CHOOSE WHICH SOFTWARE RUNS BAAS?

Normally, no. The software is specified by your BaaS service provider.

The biggest name in the backup industry is Veeam. Veeam software can handle backup to local devices as well as cloud repositories. It is used by so many organisations that the move from on-site backup to BaaS can be achieved within Veeam. The organisation doesn't have to switch software. It just adds a BaaS repository to its existing backup processes.

How do I choose between BaaS suppliers?

- How much does the BaaS service cost to backup data (per TB per month)?
- How much does the BaaS service cost to restore data (per TB)?
- Are there any other charges? If so, how much?
- Are there any setup charges?
- Do you need a managed service?

What is the supplier's service rating e.g. NPS (Net Promoter Score)?

Have you been shown a demonstration of a backup and recovery process in action?

Have you been offered a 30-day trial of the BaaS service?

Can your supplier facilitate the broadband service and equipment your BaaS will need?

Is your data protected by AES 256-bit encryption during backup?

Is your data protected by AES 256-bit encryption in storage?

Is your data protected by AES 256-bit encryption during recovery?

Does the datacentre employ biometric security to restrict access to the datacentre?

Is the datacentre governed by UK law?

Can you visit the datacentre?

What Service Level Agreements (SLAs) does the datacentre offer? Scheduled downtime? Unscheduled downtime?

Does the datacentre have to go offline to perform maintenance procedures or upgrades?

> **"Can you visit the datacentre?"**

HOW DOES BAAS AND DRAAS HELP IT DEPARTMENTS?

BaaS and DRaaS remove a huge workload from your IT department. Too many IT staff are left in the office after normal working hours, changing backup tapes and waiting to see that the backup completes properly.

Their hours extend as our data volumes grow. Such long hours are totally unnecessary. BaaS is not only technically superior, it places a far lower workload on your IT department. Backups become smaller and more frequent. They run several times a day without inconveniencing users or interrupting their day-to-day activities.

Once BaaS is configured and running, IT's only involvement is to check any alerts that are raised. There's no media to check, no capacities to monitor and no logs to read. If BaaS needs attention, it tells the IT staff.

PUBLIC CLOUD OR PRIVATE CLOUD?

"The cloud" is not a single, standardised entity. When storing your critical backup data in the cloud, you need to understand exactly how and where it is being stored.

Public Cloud

Is familiar to most consumers. Examples include Google Drive, Dropbox and OneDrive. Public cloud services are available to anybody, sometimes free and sometimes paid. Services are provided with no customised access or security facilities.

Private Cloud

Offers online storage to businesses under specific, customised agreements with tailored SLAs. Private cloud hosting includes access and security facilities that are tailored to the specific customer or application.

DOES A BAAS PROVIDER NEED ITS OWN DATACENTRE?

Some BaaS providers store your data in their own datacentre. Others provide an interface to the numerous cloud providers who supply online storage.

A BaaS provider with its own datacentre can tell you where your data is stored and the legal jurisdiction that applies to it. This is especially important as data protection and privacy become more important. People want the assurance that GDPR and other UK regulations protect the way their data is used.

A provider with its own datacentre can tell you everything you need to know about the physical and technical measures that are taken to protect your data (subject to security considerations, of course). It can tell you about any planned updates and procedure improvements because it is talking about its own internal updates and procedures. This information would not be so readily available to 3rd party resellers.

The provider with its own datacentre delivers one final benefit that trumps all others: responsibility. There is only one company responsible for the storage of your backup data. There is no question of the provider passing the buck elsewhere.

WHAT'S THE DIFFERENCE BETWEEN BAAS AND DRAAS?

Backup as a Service (BaaS) stores and secures your data files whereas Disaster Recovery as a Service (DRaaS) stores and secures your entire server: operating system, applications and configuration as well as data.

The difference becomes apparent if you have to recover after a total system failure.

> **"Consider what you are trying to protect yourself against."**

BaaS

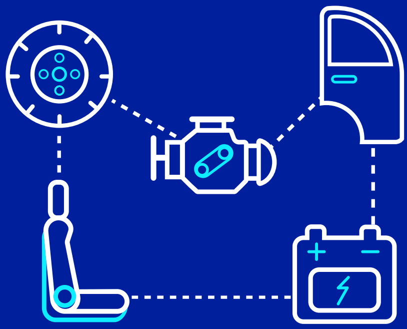
Will give you back your vital data. This will let you restart your business but only after you have procured and configured new servers and their associated operating systems and applications. All your user settings may also need to be recreated. Your business will recover but it will be hard work. Your IT staff will be occupied for weeks. Your general staff will operate below their usual levels of productivity until systems start working the way they were used to them working.

DRaaS

Will restore your servers, your applications, your user configurations and your data in hours or even minutes. Even if your physical server is destroyed, the server image can be restored to a different virtual machine (VM). Your business can be running again so fast very few people would realise just how calamitous the IT failure was.

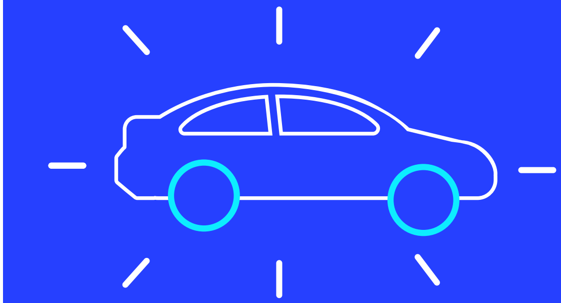
The difference between BaaS and DRaaS can be illustrated with a simple analogy. Imagine your car is wrecked.

BaaS



With a recovery from Baas, you would get your car back but it would be in pieces that you had to reassemble.

DRaaS



With a recovery from DRaaS, the car reappears as if by magic, complete and ready to drive away.

SHOULD YOU CHOOSE BAAS OR DRAAS?

With this in mind, you may wonder why anyone would settle for BaaS over DRaaS. It is a lesser service.

Consider what you are trying to protect yourself against.

If your concern is protection against data corruption or loss, BaaS is a perfectly adequate and appropriate service. Businesses are far more likely to need to restore data because of a user or system error than they are to restore an entire server because of a fire or similar disaster.

Only a tiny fraction of businesses suffer the kind of failure that requires DRaaS. But when a business reaches a certain size, it is the Board's responsibility to prepare for unlikely contingencies. That's when DRaaS is required.

WHO DO YOU WANT TO BE ON THE MORNING AFTER?

If you're still unsure whether BaaS or DRaaS is right for you, ask yourself this. Who do you want to be the day after a disaster?

? The manager who tells his boss "The IT systems are up and running again – let's get the rest of the business back on its feet"

? Or the manager who says "We might have email and core data back sometime next week."

CAN BUSINESSES SURVIVE A MAJOR DISASTER?

Even if you only do basic research on backup strategies, you will have come across the statistic that 80% businesses go bust within a year of a major disaster. Or 70%, Or 40%. Or they close within three years. Or they never reopen at all.

Like most internet 'facts', it is hard find the source of this statistic.

A US Federal Emergency Management Agency (FEMA) report suggests 40% of businesses do not reopen following a disaster. Another 25% fail within one year – **www.accesscorp.com/study-40-percent-businesses-failreopen- disaster/**

Similar statistics from the United States Small Business Administration indicate that over 90% of businesses fail within two years after being struck by a disaster – **www.chamber101.com/2programs_committee/ natural_disasters/disasterpreparedness/Forty.htm**

Or – **www.safety-managementuk.com/70-percent-fail.php**

This is the point at which statistics become unhelpful if not totally irrelevant. No two businesses are the same. A retail business with hundreds of small online transactions per day would suffer more from an IT failure than an art gallery that sells five items a month.

HOW DO RTO AND RPO AFFECT BAAS?

RTO

Recovery Time Objective

RTO is the maximum acceptable time for which an application can be unavailable in a downtime situation.

The shorter the RTO, the faster the recovery needs to be.

RPO

Recovery Point Objective

RPO is the maximum acceptable amount of data loss which can occur in a downtime or data loss situation.

The shorter the RPO, the more frequent the backup or replication of data needs to be.

> **“Who do you want to be the day after a disaster?”**

intercity

LET'S TALK ABOUT YOU

Do you have a goal to digitally transform and enhance your workplace?

Tell us your challenges, so we can find the best IT solutions, digital workplace technologies or managed services together.

Speak to us on **0808 500 1436**
or visit **www.intercity.technology**

Our Offices

Head Office
101 –114 Holloway
Head, Birmingham
B1 1QP

Elstree
Allum Gate,
Theobald St,
Elstree, Herts
WD6 4RS

Bolton
Hallmark House,
Paragon Business
Park, Horwich
Bolton, BL6 6HG