Whitepaper

Safeguarding your assets in a data-driven world

Backup as a Service **BUaaS**

YOUR DIGITAL TRANSFORMATION PARTNER FOR GROWTH

M247

The importance of data

It is data rather than money that makes the world go round these days. That's because for most modern businesses and enterprises, data is money. It is the most valuable asset they own; central to operations, vital for business growth, crucial for innovation, and essential for compliance.

The business landscape is increasingly competitive, and success in today's digital economy means being able to keep your secrets close to your chest and leverage data to your organisation's advantage. Every competitive advantage an organisation might have, whether that's the partner relationships being nurtured, the behind-the-scenes innovation, or a bank of intellectual property, brings with it a staggering amount of valuable data.

It's no wonder, then, that data has become the primary target for cybercriminals looking to make a quick and relatively easy buck.

A growing threat

According to the National Cyber Security Centre (NCSC), over the past three years there has been a huge increase in the number of ransomware attacks on businesses. Cybercriminals are well aware that organisations and businesses cannot operate without access to their data, and they are exploiting system vulnerabilities to gain access to it so they can hold it hostage until a ransom is paid.

A recent report by Forbes suggests that, since 2016, more than 4,000 US businesses have been targeted with ransomware attacks every day, in a trend that continues to grow. The average ransom payout for these data thefts is $154,108.

But of course it's not just about the money. Each ransomware attack results in an average downtime of 21 days, impacting on business operations and bottom lines, as well as causing reputational damage that can drive customers and partners away for good.

In this landscape, failure to detect, respond to and evade ransomware attacks becomes an issue of business continuity.

$3.86m average total cost of data breaches

10% increase since 2014

Ponemon Institute, 2020

53% of malicious breaches were financially motivated

Ponemon Institute, 2020

51% of downtime damaged customer relationships

Veeam Report, 2021

Business continuity management

All organisations have certain facets and functions that are critical to their day-to-day operations. Things like staff, offices, technology and supply chains are vital, and if they are impacted by a disaster, or interrupted in some other way, the entire business can be brought to a halt.

Business continuity is about having a plan in place to mitigate the impact of a disaster, whether that's a flood in the office or a ransomware data breach, and allow organisations to continue to function with as little disruption as possible.

> Business continuity management is about identifying those parts of your organisation you can't afford to lose, and planning how to maintain these if an incident occurs

A good business continuity plan recognises the potential threats to an organisation, analyses what impact they would have on day-to-day operations, and puts in place a framework that allows key functions of the organisation to continue, even if the worst should happen.

A business continuity plan should cover:

Offices and premises

- Loss of utilities
- Loss of access
- Quarantine

Partners and suppliers

- Storage of supplies
- Penalty clauses
- Alternative suppliers

Staff and contractors

- Skill set
- Geography and travel
- Use of third parties

Data and technology

- Loss of systems
- Data access and recovery
- Loss of connectivity

For most modern organisations, data and technology is the biggest area of concern. Connectivity outages, technology failure, system breaches and data theft pose a significant threat to business continuity, with interruption in any one of those areas representing an almost wholesale loss of function. That's why having a thorough and robust backup plan in place is absolutely critical.

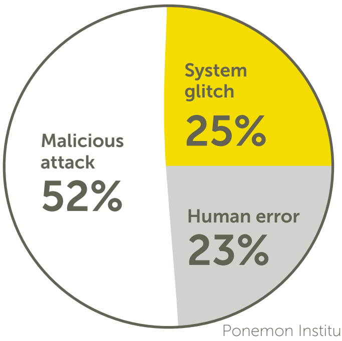
Backup and restore

While maximising the potential of data will be a priority as the world moves into an increasingly digitalised way of working, protecting the data they already have needs to be at the top of the list.

Warp-speed changes in the ways and places attacks now happen makes it difficult to prevent each potential breach, but an all-encompassing and proactive defence strategy will ensure organisations are as protected as possible. Backing up global data is the first, last and best line of defence for every organisation, and whether individual organisations opt for on-premise, cloud-based or hybrid solutions, it's never been easier to implement a robust strategy for backing up and restoring data.

Causes of data loss

All it takes is human error, a ransomware attack or virus and all your business critical information could be lost.



Ponemon Institute, 2020

Data backup - the simple objective

In essence, backing up data means keeping a copy of all or selected data somewhere else, so that if the original data is compromised or can no longer be used, there is a replacement ready and waiting to be mobilised.

Robust and proactive data management is critical for a good backup and restore strategy, because that is what will ensure all data is accessible, available, accurate and up to date at all times. There's no good restoring data that is out of date, incomplete or obsolete, so backup and recovery need to be built into a wider strategy for creating, collecting, storing and managing data.

Data management

A good data management plan will :

Increase productivity

Quick and easy access
to all data, at all times

Reduce data loss

Backed up data in
immutable snapshots

Improve operations

Streamlined processes
and overview global data,
faster response time

Lower costs,

Eliminate redundant
capacity and storage
and free-up IT teams

Minimise risk

Secure personally
identifiable information (PII)

Improve decision-making

Centralised data
that's easily accessible

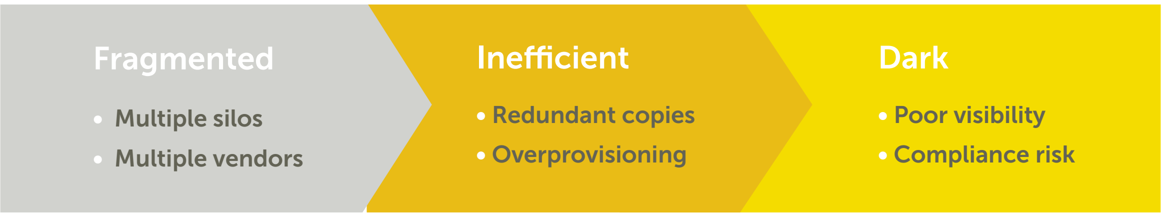
Legacy systems, new threats

As we enter a new era of hybrid working, many organisations find themselves and their data exposed through complex infrastructure and sprawling IT estates.

Data and applications are no longer confined to a single server, and backup is no longer a simple case of downloading everything to a removable drive at the end of each day and taking it offsite. In the age of remote working and co-located teams, data is increasingly spread across data centres and clouds through file shares, shared storage and even SaaS-based platforms.

Not only is it increasingly difficult for IT managers to get an overview of their entire data estates, the tools designed to backup on-premise file shares and applications simply cannot perform the functions they need to. They are costing companies time and resources, while failing to adequately protect data.

The problem with complex infrastructure



Fragmented

- Multiple silos
- Multiple vendors

Inefficient

- Redundant copies
- Overprovisioning

Dark

- Poor visibility
- Compliance risk

54% of organisations consider the ability to move data to the Cloud a defining aspect of data management

Veeam Report, 2020

The data challenge

General Data Protection Regulation (GDPR)

There are several laws governing the collection, storage, disposal and destruction of data, and in the UK, as a part of Brexit, GDPR was written into law under the Data Protection Act 2018.

GDPR is one of the most wide-ranging pieces of legislation ever enacted by the European Union and affects how every organisation, business and individual collects and transfers data. It puts the onus on companies to ensure they know exactly what personally identifiable information (PII) they hold, where it is stored, and how long it has been there, and requires all organisations to be able to quickly access and delete a user's PII from all systems, and provide an accurate audit log.

Becoming and remaining GDPR compliant has been a challenge for many organisations; it is difficult to know what data they hold and where it is, because personal information is so often collected and stored in different formats, in different locations, and in different systems.

But failure to comply with the legislation leaves organisations open to a range of sanctions, including:

- A warning in writing in cases of first and unintentional noncompliance
- Regular periodic data protection audits
- A fine of up to £20 million or 4% of annual worldwide turnover of the preceding financial year in the case of enterprise, whichever is greater, for breaches of special conditions

The key principles of GDPR

Information must be:

- **Used fairly, lawfully and transparently**
- **Used for specified, explicit purposes**
- **Used in a way that is adequate, relevant and limited to only what is necessary**
- **Accurate and, where necessary, kept up to date**
- **Kept for no longer than is necessary**

Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Ransomware

Ransomware attacks are evolving at an alarming rate, and whether they are targeting on-premise or cloud-based data and applications, the impact on organisations can be massive. Initially designed to encrypt or destroy primary data and hold it for ransom, this type of attack has evolved in recent years to target backed-up data as well. They don't just attack systems once, or from one angle; they can take control of an organisation's global data environment, halting all operations, causing untold reputational damage, and leaving businesses liable to sanction.

Legacy backup systems are especially vulnerable to ransomware. These tend to be mounted on backup servers, which leaves them detectable by cybercriminals and particularly vulnerable to attack. Furthermore, legacy systems often run in a degraded state with seriously reduced recovery time objectives (RTO), making recovery of valuable assets a trickier and more lengthy process. And in a legacy system, it is much more likely that ransomware can be targeted to specific data streams, allowing attackers to capture the most valuable data, cause the most harm, and elicit the biggest payout from victim organisations.

None of this is good for business continuity, operational resilience or indeed organisational reputation. The question for most organisations becomes, how much is the business worth?

Complex IT estates

Many organisations are embracing digital transformation on an ad hoc basis. The distribution of the workplace, which has been necessary over recent months due to COVID-19, has led to a reactionary and piecemeal adoption of new technologies, platforms, workstreams and data storage.

With users now spread far and wide, networks are more open than ever, and a bring-your-own-device model of working has left data vulnerable.

It used to be that cloud solutions offered a streamlined environment, but we are seeing the same complexities that affected traditional data centres being replicated there too, with mass data fragmentation across an increasingly complex IT environment.

Organisations that are keen to maintain computer, network and storage functions in a physical data centre while spinning up various cloud solutions are finding it increasingly difficult to maintain oversight of their data and ensure compliance.

The data solution

While cybercriminals continue to push the boundaries of what, where and when they attack, the technology to combat ransomware and protect the critical and valuable data held across organisations is also evolving. With the right strategy and approach, even backed up data can be protected.

Consolidate your platforms

You can't protect what you can't see, and key to any data security measure, is consolidation of the environment into one, easy-to-use platform.

Most organisations need a centralised system for data backup but are using applications and generating data across multiple sites and platforms. This leads to enormous data silos across a range of corporate and cloud environments, making it hard for IT managers to have a holistic view of an organisation's assets.

Employing a single data-management platform puts organisations in a better position to protect their valuable assets and brings all workloads and data into the same environment. A single platform for workloads and data, and a simple-to-use, intuitive user interface enhances environmental oversight, security and compliance.

With all data in one place, organisations are able to take a multi-layered approach to data protection to better safeguard both primary and backed-up assets against ransomware.

Prevent, detect and respond to ransomware

Prevent
Take proactive steps, such as two-factor authentication and an immutable file system, to make data a less attractive proposition for attackers.

Detect
Harness the full power of machine learning and in-built cloud analytics to detect attacks, continuously monitoring primary sources and identifying anomalies.

Respond
Quickly locate and delete infected files across the global data footprint for fast recovery from attacks and bring back all data through an instant mass restore

Scale for security

Many organisations have systems that trap data in propriety formats and systems. With a hybrid cloud solution like M247 Backup as a Service (BUaaS), data becomes more agile, flowing from site to cloud and cloud to cloud without restriction or limit.

An inherent benefit of almost any cloud or hybrid solution is the ability to scale at will, and this means organisations can ensure data security even when there are heavier-than-normal volumes of data being generated.

That means organisations with annual or monthly peaks and troughs of data ingest are able to maintain the same level of oversight and compliance throughout the year, with an immutable system that allows for unlimited scaling of PetaBytes and beyond, and greater budgetary control.

Modern backup for modern workloads

M247 pay-per-usage BUaaS includes:

- Immutable file system to ensure backed-up data cannot be encrypted, modified or deleted
- Cloned backup, making it presentable for restore, thus creating an airgap
- RBAC, airgap and multi-factor authentication to prevent backup data from becoming a target
- Machine learning to establish patterns and automatically scan for and detect data ingest/change-rate anomalies, which signal a potential ransomware attack
- Simple search and instant recovery to any point in time, to get the business quickly back up and running again

GDPR and searchable data

In the event of a breach, loss or corruption of assets, organisations need to be able to retrieve data within minutes. Backup as a Service solutions make this instantly achievable, with powerful global search functions making it easy to locate and recover the right files, every time. With all secondary storage converged, personal data can be searched for and located almost instantly.

COHESITY

M247 BUaaS solution is supported by Cohesity and includes a Google-like global index and search functionality that supports critical-use cases, including fully automated and scheduled threat analysis and compliance monitoring to save IT teams time. Cluster-wide content scanning allows for searches of clear text files based on various criteria, including name, phone number or credit card information,to ensure all files can be instantly located, restored or deleted, and the necessary audit trails generated.

National Cyber Security Centre Guidelines and Backup as a Service

• Integrated cybersecurity

While ransomware attacks are on the rise and cybercriminals are becoming increasingly skilled at breaching the security of even the world's biggest corporations, BUaaS solutions are upping the ante and integrating cybersecurity measures as standard.

The National Cyber Security Centre's guidelines on data protection cover everything from automation to access controls, and M247's BUaaS products are designed to meet these measures head-on.

• 3:2:1 Guidelines

NCSC states that three copies of an organisation's data should be held at all times, on two different media, one of those being at an off site location.

M247 BUaaS replicates to another location within the same organisation or to the public cloud of your choice.

• Automated data protection

NCSC states that critical data held for recovery must be regularly protected.

M247 BUaaS automates protection by discovering new workloads and distributing backups across the platform, enabling more-frequent backups and quicker recovery.

• Immutability

NCSC states that one copy of data should be stored off-site or offline, or be immutable online.

BUaaS supports Write-Once-Read-Many (WORM) to protect files against being deleted, corrupted or altered, even by administrators.

• Administrative access controls

NCSC states there should be administrative controls in place to control access to data.

This is easily achieved with a BUaaS solution, through role-based access controls to limit both access to and authorisation of the environment. Multi-factor authentication across the environment ensures enhanced security in the event of a compromised user account.

The future is data

As data grows exponentially in influence and value, it has never been more important for organisations across the board to safeguard theirs with a solid plan for backup and recovery.

While Backup as a Service solutions alone won't remove the threat of increasingly sophisticated ransomware, they can play a critical role in an organisation's defenceagainst attack. With the right solution and the right partner, BUaaS can be an insurance policy for data and a lifebelt for business.

If your organisation needs a backup solution that's built for the future, and the connectivity to maximise its potential, contact our expert team today.

To find out how our technology can transform your business get in touch

- ✉ 0808 301 9688
- ☎ sales@m247.com
- 🌐 m247.com
- in M247

M247