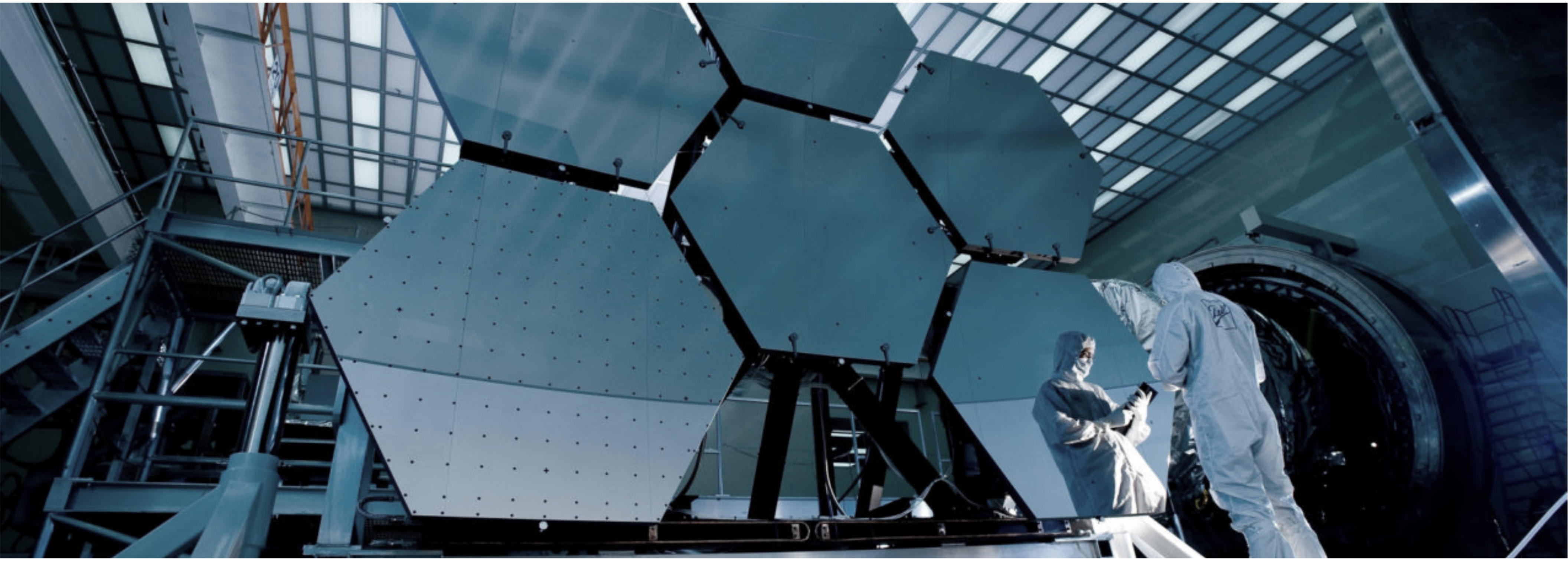
A DATA BACKUP AND PROTECTION POLICY COST ANALYSIS REPORT

Researched by:
Kevin Bailey
Chief Analyst
Synergy Six Degrees

3-2-1 no longer fit for purpose with high hidden costs for today's "always available" needs.

Prepared for:

cybrilliance
Empower Your Business with Cyber Resilience.



SYNERGY
SIX DEGREES

TABLE OF CONTENTS

Synergy Six Degrees

71-75 Shelton Street
Covent Garden
London WC2H 9JQ
United Kingdom

INTRODUCTION

Report Purpose

Synergy Six was commissioned by Cybrilliance[*], Inc to analyse the capabilities of the existing recommended 3-2-1 backup & recovery policy for today's needs.

The report request was driven by recognition of the evolved value of data as one of the most critical availability elements of business continuity - and it being a primary target for cyber attacks.

Method

Synergy Six delved into the implementation, effectiveness and data protection of current backup and recovery capabilities. Where applicable Cybrilliance asked for evidence where existing 3-2-1 policy was unfit for purpose - and what the alternative is.

Backup Providers

Cloud-native and on-premises backup & recovery providers were sampled.
NB: Any current providers in these environments could have been considered.

Costs

Standard published list pricing was applied.

3-2-1 Policy

The generic policy was analysed for the purpose of this report. Organisations can substitute their specific implementation of the 3-2-1 policy.

Recovery

Estimates of time to recover a second data copy from disk (not immutable) was calculated using sustained transfer rates.

[*] - Cybrilliance is a global master distributor for cyber resilience tools. www.cybrilliance.com

Executive Summary

The value of data to businesses and its monetization by cyber criminals, combined with the growth in government, industry and privacy regulatory compliance has changed the way that data is managed and protected over the past 20 years. These elements were not accounted for when the 3-2-1 policy was first introduced.

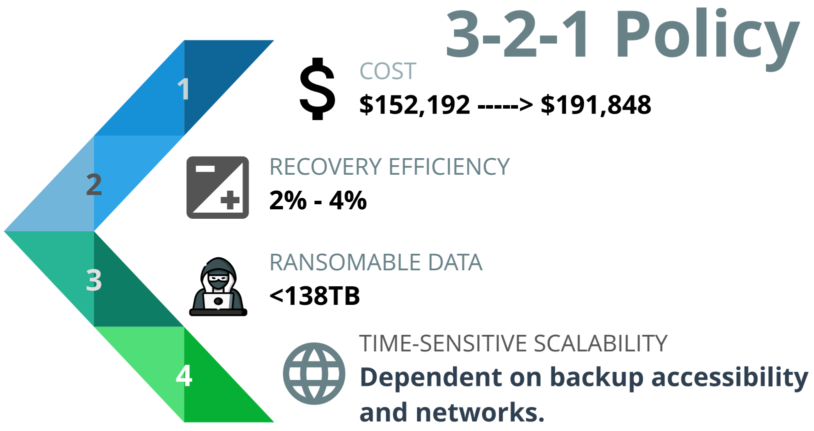
- The 3-2-1 policy replicates and retains data “just in case” it may be needed. This replication and retention accumulates 54 times the original and growth data in one year. Once data has been secured as a backup copy, an equally critical task is to recover the data in a realistic timeframe following an incident. Our research uncovered that during a recovery window of 5 hours, for 5TB of data, only 4% (230GB) of the data was available at the end of the 5-hour recovery window.
- Initial costs of ~$10-$26k to deliver data backups, did not represent the real costs for tamper proof data protection and realistic data recovery times. The hidden costs will only become visible during turbulent incident recovery activities, and these can climb to 17 times ~$150-$190k of the initial costs.

Digital businesses have a responsibility to provide “always available” devices and data to their customers, partners and employees.

Intensive research focused on the objectives of this report found that the 3-2-1 backup and recovery policy is no longer fit for purpose.

Synergy Six propose an evolution of the 3-2-1 policy to a 1-1 policy. This means a move towards all active data recovery being performed immediately ‘on-device’ and immune from compromise without restrictive dependencies. A 1-1 policy only requires one copy of data that is kept on immutable technology (off-site) to prevent malicious or inadvertent data tampering.

- Modelling storage costs: The NeuShield Data Sentinel product for 1-1 shows that only 2.02TB of additional data storage was required. The 3-2-1 policy required 270TB .
- Modelling recovery costs: NeuShield recovered all 5TB of data in less than one hour and the cost of the 1-1 policy was $22,387 (including immutable storage cost). The cost saving (when compared to 3-2-1) was between $127k-$168k per year.



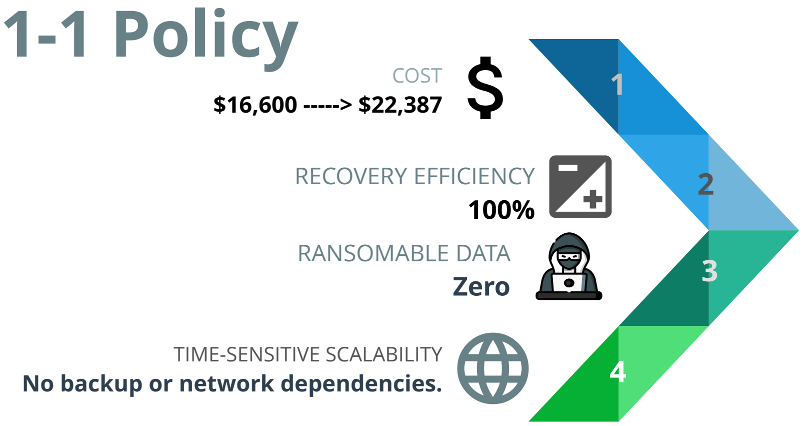
3-2-1 Policy

COST
$152,192 -----> $191,848

RECOVERY EFFICIENCY
2% - 4%

RANSOMABLE DATA
<138TB

TIME-SENSITIVE SCALABILITY
Dependent on backup accessibility and networks.



1-1 Policy

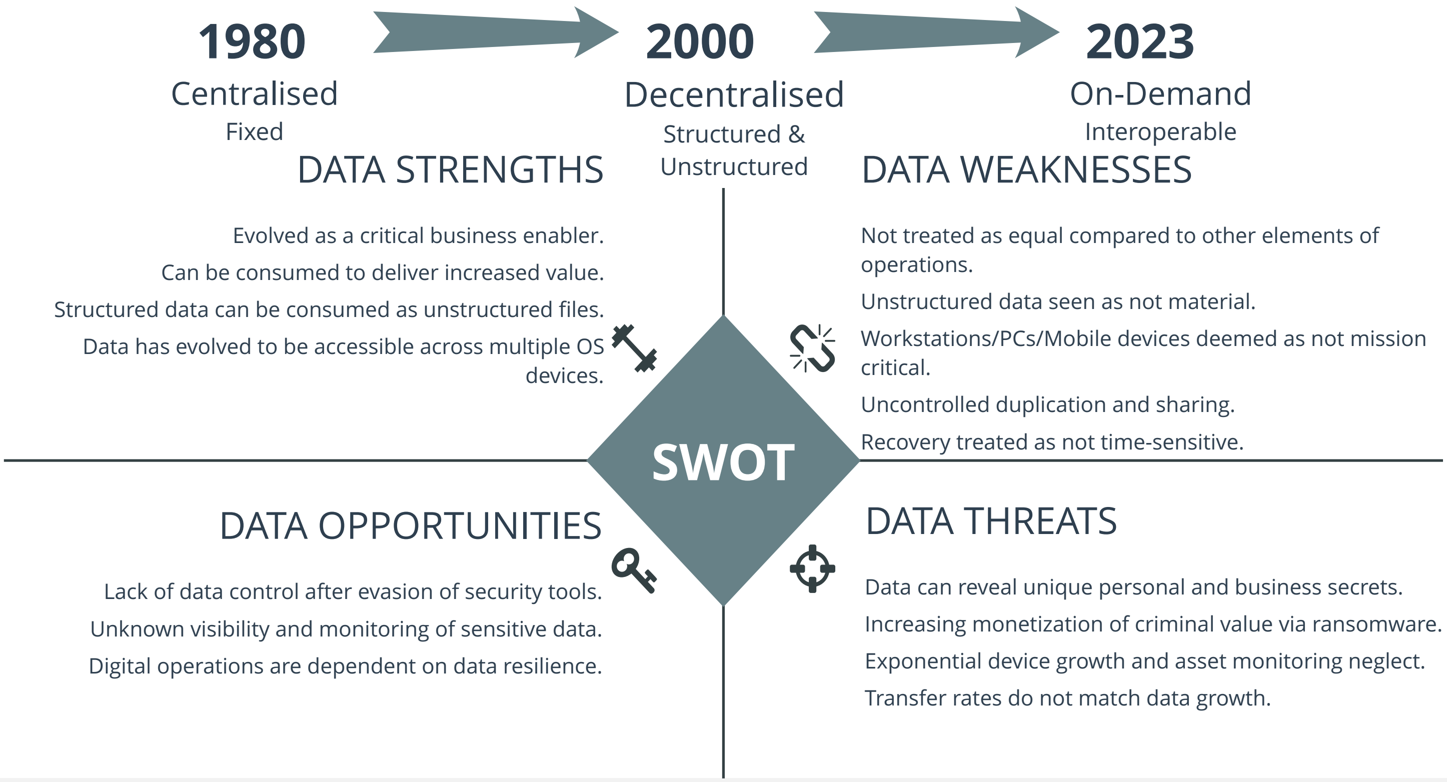
COST
$16,600 -----> $22,387

RECOVERY EFFICIENCY
100%

RANSOMABLE DATA
Zero

TIME-SENSITIVE SCALABILITY
No backup or network dependencies.

DATA EVOLUTION ANALYSIS



1980
Centralised
Fixed

2000
Decentralised
Structured & Unstructured

2023
On-Demand
Interoperable

DATA STRENGTHS

Evolved as a critical business enabler.

Can be consumed to deliver increased value.

Structured data can be consumed as unstructured files.

Data has evolved to be accessible across multiple OS devices.

DATA WEAKNESSES

Not treated as equal compared to other elements of operations.

Unstructured data seen as not material.

Workstations/PCs/Mobile devices deemed as not mission critical.

Uncontrolled duplication and sharing.

Recovery treated as not time-sensitive.

SWOT

DATA OPPORTUNITIES

Lack of data control after evasion of security tools.

Unknown visibility and monitoring of sensitive data.

Digital operations are dependent on data resilience.

DATA THREATS

Data can reveal unique personal and business secrets.

Increasing monetization of criminal value via ransomware.

Exponential device growth and asset monitoring neglect.

Transfer rates do not match data growth.

3-2-1 Policy

Peter Krogh introduced the 3-2-1 backup rule when he published his book, “The DAM Book: Digital Asset Management for Photographers” in **2005.**[1]
The 3-2-1 evolution was based on the need to lessen the impact of a single point of failure, i.e., where a disaster wipes out your on-site backups, your off-site cloud-based backup (2nd copy) can save the day.

Time-Sensitive Data

Peter’s original purpose for a 3-2-1 policy never needed to appreciate **‘time-sensitive’** recovery of compromised data and the devices that hold the data.
Data value variability and its impact (financially, legally, and in your operations) means that time-sensitive recovery cannot accept the past reality of 3-2-1 data and device recovery in days, weeks, or months to restore operations for the business, employee and/or consumer.

[1] - https://www.uschamber.com/co/run/technology/3-2-1-backup- rule#:~:text=Peter%20Krogh%2C%20a%20photographer%2C%20writer,3%2D2%2D1%20strategy.

3-2-1 ANALYSIS

What is 3-2-1[2]

3-2-1 is a backup policy that increases an organisation's capability of recovering lost or corrupted data.

- **3 –** Keep three copies of any important file: one primary and two backups.
- **2 –** Keep the files on two different media types to protect against different types of hazards (disk, immutable storage, tape, etc.).
- **1 –** Store one copy off-site (e.g., outside your business facility).

Why was the 3-2-1 policy introduced?

The increased redundancy of deploying multiple backup copies helped ensure that disk drive errors, stolen devices or data loss from database migration, software corruption, ransomware attack or human error will be recoverable.

Accordingly, the Cybersecurity and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), and other government cyber agencies subsequently realized the benefits and recommended that individuals and businesses adopt the 3-2-1 strategy.

What and how is data backed up?

Critical data maintains an organisation's business. This material data can be termed as either sensitive or essential. Data may be located on desktops, laptops, servers, and even mobile devices - and can be a mixture of unstructured and structured formats.

Data is backed up (copied) using specific software that executes and stores the data copies on-premises or on cloud storage (or a mixture of both).

To ensure that a specific recovery point objective (RPO) can be achieved, backups are taken periodically on a daily, weekly, monthly, and quarterly basis. The amount of data captured during each backup period is influenced by the mixture of full, incremental, differential and snapshot replications.

[2] https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf

3-2-1 DATA ACCUMULATION ANALYSIS

How much backup data will you accumulate?

Growth in data lakes (where such data has an immediate or believed future material value to the business) is commonplace, always ensuring that the data owner has permitted its use.

Retaining data "just in case" or because it is located on a device, creates a data swamp. Neglecting visibility and control of the swamps opens the business to regulatory inspection, complex housekeeping, cyber exposure and spiralling costs.

The 3-2-1 policy can fall into both pools of data - Data Lake - the data is of continued value to restore in the event of an incident; Data Swamp - where data is collected as part of the backup schedule, without knowing the nature of every data copied.

When a cyber criminal attacks an organisation the intention is to create as much damage as possible to gain the maximum return for the attack. Do not be fooled into thinking you will be dealing with recovering GB files. You should plan to be confronted with recovering the entirety of your data lakes, swamps, device folders and applications.

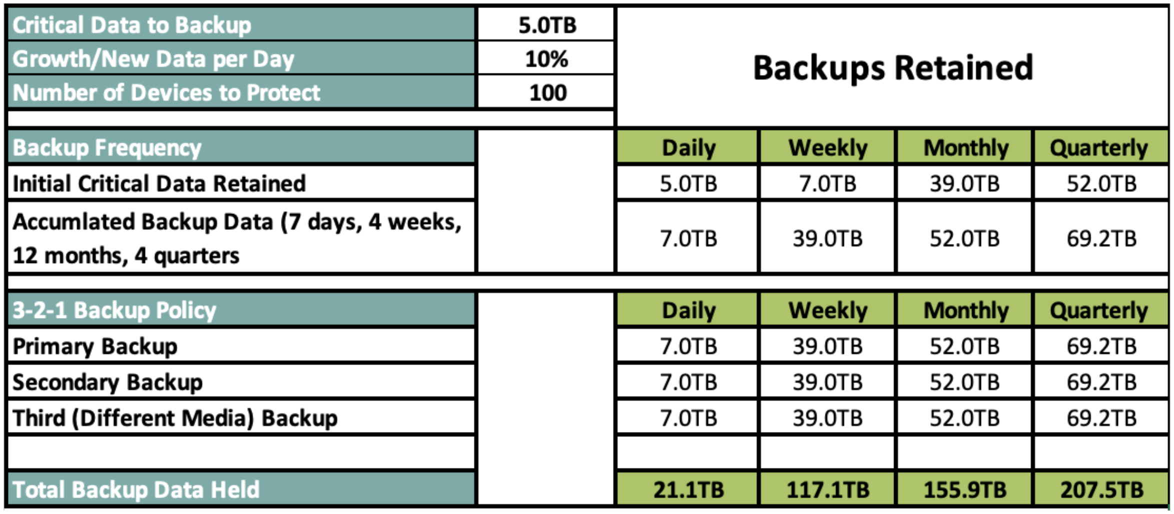
Table 1 shows a random sample for an organisation that has 5 terabytes (TB) of data on Day 1 of the backup cycle, adhering to the 3-2-1 backup policy for a single year of operations.

The example assumes a full backup is taken at the start of any given period (daily, weekly, monthly, quarterly) and then only the incremental changes (data changes including new files) are retained (along with the original full backup) until the start of the next period.

In summary, **5TBs** of unique critical data on Day 1, with 10% daily change/new data/files created will result in **69.2TBs** by the end of the year 1[3].

Enforcing a 3-2-1 backup policy requires the organisation to retain a total of **207.5TBs** of backup data across three copies.

Table 1 - Backup Data Retained



Critical Data to Backup	5.0TB	Backups Retained			
Growth/New Data per Day	10%				
Number of Devices to Protect	100				
Backup Frequency		Daily	Weekly	Monthly	Quarterly
Initial Critical Data Retained		5.0TB	7.0TB	39.0TB	52.0TB
Accumlated Backup Data (7 days, 4 weeks, 12 months, 4 quarters		7.0TB	39.0TB	52.0TB	69.2TB
3-2-1 Backup Policy		Daily	Weekly	Monthly	Quarterly
Primary Backup		7.0TB	39.0TB	52.0TB	69.2TB
Secondary Backup		7.0TB	39.0TB	52.0TB	69.2TB
Third (Different Media) Backup		7.0TB	39.0TB	52.0TB	69.2TB
Total Backup Data Held		21.1TB	117.1TB	155.9TB	207.5TB

[3] No storage compression, decompress or vendor suggested optimisation product features have been used in the calculations.

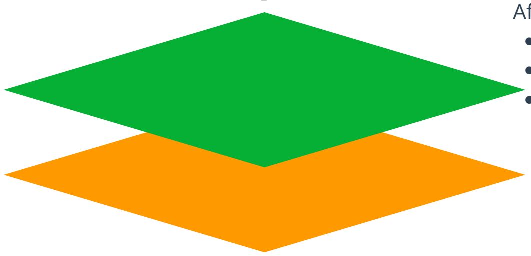
3-2-1 PROVIDER ANALYSIS

Example Vendors

This research looks at two providers of backup and recovery products. Although the vendor landscape offers fixed or hybrid implementation options, the analysis focus is on an on-premises vendor and a cloud-native based provider.

The reasoning for choosing these two vendors was based purely on their market consideration, presence, feature set and adoption. Any of the other vendors listed below could be supplemented in place of those chosen.

- **On-Premises** - The list of enterprise class on-premises vendors is substantial and could come from any of the following example list: Acronis, Veeam, Dell, Rubrik, Commvault, Veritas, Zerto, Barracuda, IBM, OpenText, etc.
- **Cloud-Native Provider** - The list of enterprise class cloud-native provider vendors is substantial and could come from any of the following example list: Arcserve, Druva, Microsoft, Google, AWS, Unitrends, etc.



ON-PREMISES VENDOR - Veeam

Veeam Data Platform - Essentials

Affordable data protection and management for small businesses.

- All-encompassing small business data protection from a single UI.
- Protection from ransomware and other cyber threats.
- Flexible licensing that gives you the freedom to change and grow.

CLOUD-NATIVE VENDOR - AWS

AWS Centralised Backup

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services in the cloud as well as on premises using the AWS Storage Gateway.

3-2-1 BACKUP COMPROMISE ANALYSIS

Retaining an appropriate number of backups (copies of data) is an essential element of an organisations data protection strategy. The accessibility, viability and condition of the material (sensitive) data held across these data copies can never be taken for granted.

The following examples outline operational and exceptional events occurring regularly in today's complex operations. The majority of these examples did not exist when 3-2-1 was introduced. Therefore, they did not need consideration at that time.

Misconfiguration

An incorrect or sub-optimal configuration of the backup system and all of its chained dependencies may lead to vulnerabilities in the capture and recovery of data.

Incomplete

As data grows the window to complete your backups gets shorter. This can create invalid restore points and missing data in your backup cycle.

Loss of Database

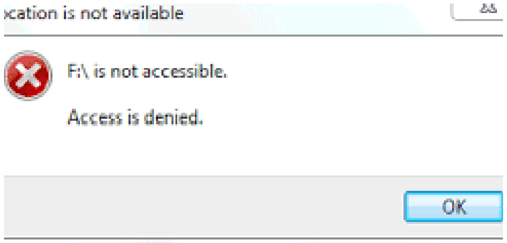
Corruption of the backup database prohibits the execution of scheduled backups and incapacitates all data recovery capabilities.

Embedded Malware

Attackers often try and succeed in implanting malware months before a ransomware attack to infect the backups.

Compromised

Backups (and shadow copies) are a first stage target as part of an attack. The data will be deleted or encrypted to disable the victim's capability to restore the data.



ιcation is not available

F:\ is not accessible.

Access is denied.

Inaccessibility

The ability to transfer or recover data into or across the business depends on a functioning network. During a cyber incident networks will be disabled to protect the business.

Human Error

Many cases of genuine mistakes are exacerbated by overworked, distracted and under trained users.

3-2-1 DATA RECOVERY ANALYSIS

Can you guarantee a clear runway?

Cyber tabletop exercises will test against expected cyber incident scenarios and operational anomalies. When planning for - and even simulating recovering (rebuilding) data during operational hardware failures or planned disaster recovery tests and [cyber] tabletop exercises, you will define agreed service-levels for recovery time (RTO) and recovery point (RPO) objectives. This will access data available from the traditional 3-2-1 policy. These operational scenarios will be undertaken in a controlled manner, with the purpose of ensuring a clear runway for the activities.

Usually these tests are conducted when it is calm and there is time to observce and think. However, when an active incident is encountered, this calm is replaced with anxiety, agitation, nervousness, fury, and legal influence.

The unpredictability of interference on your RPO and RTO during a cyber incident will be influenced by the attack type(s) and without warning. Interference will cause delays due to inaccessibility of backup media, availability of 2nd or 3rd backups, backup database, availability of hardware, network connectivity and its sustained performance.

Recovering the 2nd copy

3-2-1 is enforced to ensure that operations have additional copies of data, when the 1st copy is unavailable. This is normally due to backup accessibility, cyber compromise, or incomplete backups. Adhering to the 3-2-1 backup policy, Table 2 shows the amount of data recovery achievable where recovery of the 2nd copy (off-site) is available. Only one other common variable factor is included: sustained network performance.

Table 2 provides five RTO windows for an organisation that must recover the original Day 1 5TB of data during the first week of operations.

Table 2 – 3-2-1 Policy scenario for recovering 5.0TB of critical data

Device Types	Provider	Day 1 Data to Backup	Addt. Data Storage Required per Year[1]	How much data is Ransomable[2]	Min. Data Recovery Required[3]	Recovery Time Objective[4]				
						1 Hr	2 Hrs	3 Hrs	4 Hrs	5 Hrs+
Microsoft: 50 x Windows PCs 40 x Servers 10 x SQL Servers						Data Recovered @~100Mbps[5]				
	Veeam	5.0TB	207.5TB	138.3TB	5.0TB	0.0461TB	0.0922TB	0.1382TB	0.1843TB	0.2304TB
						Data Recovered @~51Mbps[5]				
	AWS	5.0TB	207.5TB	138.3TB	5.0TB	0.0230TB	0.0461TB	0.0691TB	0.0922TB	0.1152TB

Notes:

1. The cumulative data being stored from daily, weekly, monthly, and quarterly 3-2-1 backups.
2. Data that is unusable for recovery purposes due it being compromised and used for ransomable purposes.
3. The minimum amount of data to recover during the disaster/incident.
4. Target recovery time objective policy windows.
5. Sustained network data transfer speed measured in megabits per second. Data transfer speeds are either contracted commitments or end user measured rates.

3-2-1 DATA RECOVERY ANALYSIS

Recovering the 2nd copy cont.

Meeting the RTO

Table 2 clearly highlights that the capability to deliver a reasonable RTO is strikingly woeful, even when a clear runway for data recovery is available.

Speed is critical when striving to meet an RTO. The flexibility of native-cloud providers to offer immediacy to turn on additional bandwidth should be available for businesses storing data in their cloud.

Table 3 reflects the same data points as Table 2 with one addition. AWS (as do other native-cloud providers) allows customers to add bandwidth on-demand.

The base data transfer model for AWS was increased from 51Mbps and multiplied by a factor of 39 to achieve a bandwidth capability of 1.99Gbps. This multiplier example was used to respond to organisations that can run at this speed with their 2.0Gbps network interface cards (NIC). Every good network administrator will know there are many 'runway' caveats (blockers) that will affect gaining full sustained bandwidth capability. These will not be discussed in this paper.

The increased bandwidth provision comes close to meeting the Day 1 RPO, but still requires a further 25 mins to recover the remaining 39GB of data waiting to be restored during the 5-hour RTO window.

Table 3 – Increasing sustained data transfer speeds

Device Types	Provider	Day 1 Data to Backup	Addt. Data Storage Required per Year[1]	How much data is Ransomable[2]	Min. Data Recovery Required[3]	Recovery Time Objective[4]				
						<1 Hr	2 Hrs	3 Hrs	4 Hrs	5 Hrs+
Microsoft: 50 x Windows PCs 40 x File Servers 10 x SQL Servers						Data Recovered @~100Mbps[5]				
	Veeam	5.0TB	207.5TB	138.3TB	5.0TB	0.0461TB	0.0922TB	0.1382TB	0.1843TB	0.2304TB
						Data Recovered @~51Mbps[5]				
	AWS	5.0TB	207.5TB	138.3TB	5.0TB	0.0230TB	0.0461TB	0.0691TB	0.0922TB	0.1152TB
						Data Recovered @~2Gbps[5]				
	AWS	5.0TB	207.5TB	138.3TB	5.0TB	0.92TB	1.84TB	2.76TB	3.69TB	4.61TB

Notes:

1. The cumulative data being stored from daily, weekly, monthly, and quarterly 3-2-1 backups.
2. Data that is unusable for recovery purposes due to it being compromised and used for ransomable purposes.
3. The minimum amount of data to recover during an incident.
4. Target recovery time objective policy.
5. Sustained network data transfer speed measured in megabits per second. Data transfer speeds are either contracted commitments or end user measured rates.

IS 3-2-1 STILL FIT FOR PURPOSE?

Has backup & recovery kept pace?

Over the past 20 years security tools have evolved in delivery and multifaceted innovation. They have transformed from simple anti-virus protection into a portfolio of complex detection and remediation solutions that cover all known ingest and egress points across mobile, data centre and cloud architectures.

Over the same period, backup and recovery (data protection) solutions have become more fragmented. Features have been introduced that identify, segment, clean and secure data - and this has resulted in increased complexity.

While the majority of security tool actions pro-actively mitigate damage in real-time, data protection (backup and recovery) never moved from its reactive position - until now.

Data protection solutions need to become proactive, as well as being ready to respond to data incidents, if they are to increase their relevance in assisting today's "always-available" digital operations environments.

Dependencies

Backup and recovery of data is increasingly dependent.

- Identifying suitable windows to backup data and take periodic snapshots during the day is a challenge with the need to maintain maximum up-time for system availability.
- You must also ensure that you can identify specific recoverable data quickly and that target devices are operational for the data to transfer from and to.
- Network connectivity is critical. Data cannot be transferred without an active or sustainable network.

Evolved Disruption

Complexity of computing over the last 20 years has continued to evolve due to the need to deliver "always-available" interactions. In addition, hardware and software has introduced complexity to deliver interoperability to take advantage of processing across multi-disciplinary systems, including the foundation architectures of individual products.

Historically, primary external business disruptions came from macro level disruptors such as political, economic, social, and technological (PEST) factors. The criminology joined the cyber revolution. Businesses have now acknowledged that extensive and various cyber attack vectors and the resultant cyber incidents must be considered and managed to maintain business operations and keep data secure.

IS 3-2-1 STILL FIT FOR PURPOSE?

3-2-1 Summary

Our research data points prove that backup and recovery and the associated 3-2-1 policy is not fit for purpose. There is a bias towards capturing data (RPO), with little or no consideration of recovery (RTO). Innovation of products to tackle this issue has been lacking. Vendors continue to accumulate increased revenue from licensing and the business of recovery costs.

Focus

It is evident that the focus of backup and recovery and its associated 3-2-1 retention policy is heavily motivated on delivering and achieving the 1st phase; number of variable data periods and copies of data that help to identify a required RPO.

- *The growth in material data in our research has meant that organisations can accumulate immense volumes (270TB) of data, just in case it may be required. Two-thirds of this data can be compromised and nullified for recovery.*

The equally important critical second phase, recovery time, cannot adequately meet the needs of organisations immaterial of their market segmentation.

- *Delivering only 4% (230Gb) of the material data required will incur substantial cost implications to a business.*

Innovation

Product vendors have not delivered any initiatives to accelerate advanced RTO functionality over the past 20 years. Cloud residency remains dependent on connectivity for data transfer.

The two considerations available to protect backup copies from cyber compromise are encryption (software) and immutable (hardware) technologies.

- ***Encryption** - Encrypting all backup data will secure its contents from compromise, but this feature is a hammer approach that will introduce management and accessibility complexity.*
- ***Immutable** - This is a viable consideration, while also factoring in cost, performance, accessibility and protection from acts of God (fire, flood and destruction) that confine this feature to an off-site location.*

Cost

While not part of the primary objectives requested for this research project, Synergy Six was alarmed at the hidden costs being consumed in the execution of the backup and recovery process. Current economic conditions and budget challenges highlight the need to raise this concern in our summary analysis.

- ***Licensing and Storage** - Immaterial if you have a 3-2-1 or derivative policy, the cost of base licenses, paid necessary features, management resources and storage of data appear to be spiralling, with the vendor appearing to hold their customers to ransom for a critical process.*
- ***Recovery** - Very little support appears to be provided by the vendors to size bandwidth that enables a clear runway to recover the data. This results in a business incurring hundreds of thousands in unbudgeted costs at impact.*

Our research is further validated with the continual news coverage of cyber incidents (ransomware, data breach, etc.) where business operations are paralysed for weeks and months due to being unable to recover and rebuild data to an operational level within an acceptable recovery window.

IS THERE AN ALTERNATIVE TO 3-2-1?

Cybrilliance asked for an alternative to the 3-2-1 backup policy if the conclusion of our research was that 3-2-1 is no longer fit for purpose.

Synergy Six Opinion

The variability of data value and its impact financially, legally, and within your operations means that retaining “just in case” material data (and the need for time-sensitive recovery) cannot accept the past reality of 3-2-1 data and device recovery in days, weeks, or months to restore operations for the business, employee and/or consumer.

When John Kindervag[4] introduced Zero-Trust (ZT) in 2010, its mantra: “never trust, always verify” focused on an organisation’s operational policies, processes, and design concepts. A decade later the core principle [never trust] remains intact but has been widely adapted by industry analyst groups and vendors to include products and infrastructure (ZTNA, ZTA, ZTS, ZTDP, ZTXEP[5]) as well as viable alternatives to the ZT framework.

“Whether a company loses a factory in a fire – or millions of files in a cybersecurity incident – it may be material to investors.” SEC Chair Gary Gensler.

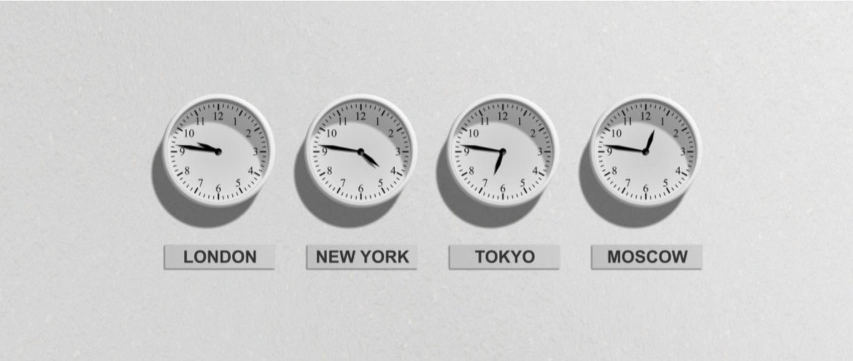
Eighteen years ago, Peter Krogh’s original purpose for a 3-2-1 policy never needed to appreciate the “always-available” world that we expect today. **‘Time-sensitive’** recovery of compromised data and the devices that hold the data was never a factor. Back then, compromised data related incidents were primarily initiated by internal events that could be resolved in a calm, scheduled, and ordered manner.

No longer is data a commodity treated equally just to be retained in case of future needs. Data collection, function, confidentiality, and value (to the business and cyber-criminal groups) are and will continue to be unique assets and must be treated accordingly.

[4] https://www.illumio.com/news/illumio-appoints-john-kindergav-chief-evangelist

[5] See Appendix A

What is Time-Sensitive Recovery



The capability to immediately and simultaneously re-establish active data and associated device(s) combined with real-time data compromise protection.

This can only be delivered if data recovery is device focused, delivering both RPO and RTO with the absolute minimum of fulfilment dependencies.

Similar to Zero Trust, RPO and RTO windows should be established against real-life scenarios using “never trust, always verify”.

Backup vs Active Data

Backed up data is the combination of periodic copies of complete, partial or incremental changes of critical/material data that is retained for the purpose of rebuilding any portion - or entirety - of the data when the primary data and associated devices have been lost or compromised.

Backup data is not active data.

It is an historical representation of the active data stored externally from the primary device. Nor can it be deemed as time-sensitive because backups have variable dependencies that inhibit the clear runway for an organisations dependency as “always available”.

Active data is not a backup.

It is the primary critical/material data, including critical services, plus incremental changes over a designated period in use on a device. This data includes the instances of the active operating system and applications.

THE 1-1 STRATEGY FOR TODAY'S ALWAYS AVAILABLE DATA, OPERATIONS, RECOVERY AND PROTECTION REQUIREMENTS

1-1 is the strategy of adopting **Active Data** protection and recovery (**1-***) accompanied with an **Immutable** [storage] / Air-gap copy of the data **(*-1**).

1-* Active Data Protection & Recovery

All critical/material data resides on the operating device. Data is protected in real-time from unauthorised data compromise (encryption, deletion) and amendment, immaterial if endpoint/network and other security tools have been evaded or not by cyber malware.

Recovery of data, dependent operating systems and applications should be immediate. Where data has been compromised across multiple devices, this should occur simultaneously.

*-1 Immutable Storage

The element of the existing 3-2-1 policy where one copy of data is stored on a different media type. Immutable storage is a broad term referring to data storage that is impervious to ransomware attacks and other cyber malfeasance. In other words, it is in suspended animation, unalterable and undeletable.

Immutable can also be classified as 'Air-gap' storage that utilises disk or magnetic tape technology, normally located at a secondary location, or in the cloud. Although organisations have the flexibility to locate the immutable [historical] copy of data on-site, Synergy Six advises organisations not to retain this data on-site.

The purpose of the immutable copy of data is for typical non time-sensitive recovery activities such as device and disk failures and disaster recovery. If the immutable copy is retained on-site and the location is compromised by fire, flood or other destruction you will lose the capability to recover data.

The 1-1 Strategy

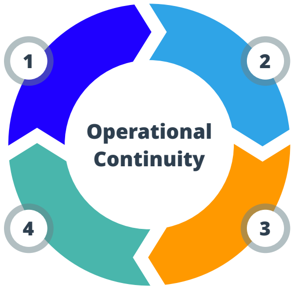
Advancing Operational Continuity

Organisations currently follow a synchronous process to ensure that their systems remain operational as required and are resilient to known and unknown risk.

- **Stage 1** - Businesses have a variety of cyber **security tools** implemented to defend and mitigate cyber attacks.
- **Stage 2** - When an incident occurs the risk management process invokes **Incident Response** to contain the incident, eradicate identified attack vectors and initiate recovery of systems, applications and data.
- **Stage 3** - Backup and recovery tool(s) are executed to **rebuild data** for a given RPO aligned to the target RTO.
- **Stage 4** - Once all system hardware and software have been deemed clean of malware, senior management will **re-establish business operations**. This stage can be undertaken in full or partially as each element of infrastructure is available.

Synergy Six proposes that organisations adjust their current operational resilience process and introduce an additional stage.

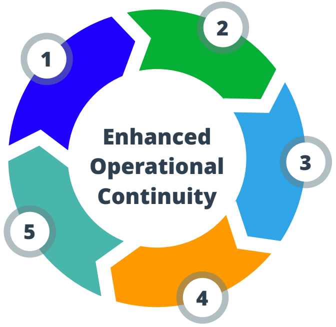
The introduction of this new stage - **Active Data Protection** - should be placed between security tools and Incident Response. The Active Data Protection stage will ensure that data cannot be compromised, lessen the impact on Incident Response and negate the need to rebuild/recover data from backups.



Current Stages of Continuity

1. Security tools to mitigate cyber attacks.
2. Incident Response reacting to a successful incident.
3. Reactive Backup & Recovery to rebuild compromised data.
4. Business continuity process to re-establish operations.

Active Data Protection and Recovery



Proposed Stages of Continuity

1. Security tools to mitigate cyber attacks.
2. **Proactive - Active data protection to mitigate data compromise.**
3. Incident Response reacting to a successful incident.
4. Reactive Backup & Recovery to rebuild data for non-cyber attack scenarios.
5. Business continuity process to re-establish operations.

Applying Active Data Protection & Recovery

Theorising needs to be transferred from paper into reality. Synergy Six researched the viability of this evolution to help organisations take immediate action and plan for changes to increase the resilience and recovery capabilities of their data.

1-1 Vendor Selection

The breadth of data protection and security vendors that will profess to provide an offering that meets the description for 1-1 selection will be enormous.

Achieving only partial alignment to the 1-1 policy will create recovery and cost implications down the line. So, when considering vendors it is essential that organisations evaluate and test due diligence for how the product/service can fully align to the 1-1 policy, including the organisations existing and planned technology, tactics and policies (TTPs).

Vendor selection should focus on both elements of the 1-1 policy (1-*/*-1). While many technical leaders have a goal to reduce their product stack, this should never compromise the tighest security measures. Excellence in one element should be prioritised over a vendor that has 'good-enough' functionality.

Vendor Categories

Backup and Recovery

Existing providers of this category do not meet the first element of the 1-1 policy. The purpose of this category is to retain copies of data to enable recovery in the future. This labels the retained data as historical and not active.

A vendor should be chosen to meet the needs of the second element (an Immutable copy) of the 1-1 policy. Accessibility of this data copy is critical and any vendor selection should consider the off-site location of the technology. Organisations should also factor data residency requirements where sovereignty of such data may have implications in compliance where the data is stored out of country/region.

Endpoint Detection and Response

EDR vendors will profess to provide the capability to deliver the first element (**Active Data** protection and recovery) of the 1-1 policy, via their ability to take regular snapshots of data. This claim is flawed in a few areas:

- EDR snapshot is a feature of Microsoft VSS. It allows IT administrators to rollback files following data compromise. Unfortunately, this is a very simplistic view of a cyber incident process flow.
- In access of 90% of attacks the attacker will inspect an organisations infrastructure, to identify data and response capabilities. One of the first stages of an attack is to nullify all copies of data including backups, snapshots, image copies.
- Attacks will not only compromise an organisations data and response capabilities, it will target and encrypt device operating systems and applications, rendering the device inoperable. Nullifying the capability to access/execute any features in the EDR product.

Active Data Protection

A new category delivering the first element (**Active Data** protection and recovery) of the 1-1 policy, from new or established data protection or security vendors.

1-1 Example Vendor

Utilising the depth of Synergy Six vendor briefings, we identified only one that could meet the needs of the first element (**Active Data** protection and recovery) of the 1-1 policy.

Synergy Six expects that other vendors will deliver this level of architecture over the next 3-5 years. In many cases Synergy Six predicts that the independence of new (start-up) organisations will be short lived as they will likely be acquired by existing backup and recovery and security vendors looking to transition their existing portfolio's.

NeuShield, Inc has taken a different approach to traditional security by offering **data protection**. Rather than trying to detect and block threats one-by-one the company takes a new patented approach that uses **Mirror Shielding™**, **One-Click Restore** and **Data Engrams™** which shield data to prevent threats from modifying it.

NeuShield
How much is your data worth?

Product Features and Support

✓ Solution

NeuShield Data Sentinel

- **Home** Edition
- **Business** Edition
- **Datacenter** Edition

Dependencies

- Microsoft OS Only
- No Networks Required
- No Backups Required
- No Malware Engine

Key Functionalities

- Active Data Protection.
- Instant Data Revert -RTO.
- Anti-Ransomware, Exfiltration, Tampering.
- Multiple Data and OS RPOs.
- Files, SQL Database, Apps, OS and Critical Services.
- Anti-Wiper and Boot DIsk Protection.
- MFA Access.
- SaaS Monitoring Portal.
- Multi-Tenant Support.
- Microsoft - PCs & Servers.

Unfair Advantage

At the time of this report, the NeuShield technology is the only provider that can protect the actual 'active' data on the device from an attack.

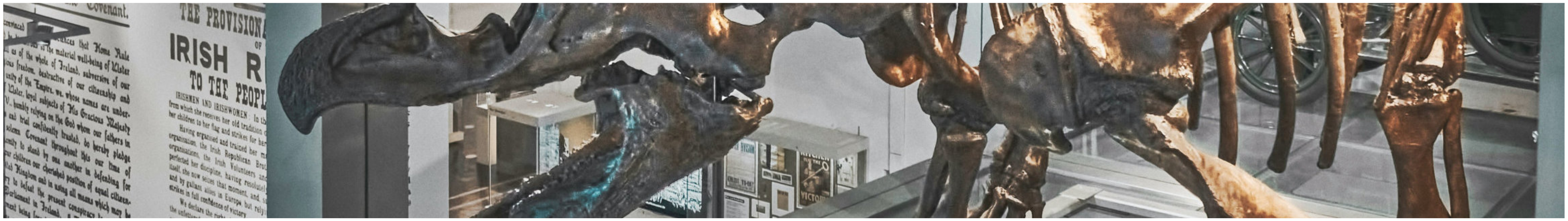
The core patented technology of the NeuShield product portfolio:

- Prevents real-time unwanted changes to protected files, folders and SQL databases.
- Has virtually zero impact on device performance
- Preserves existing user workflow and behavior for local and cloud data.
- Is compatible with and does not replicate functionality of existing security applications.

Challenging the 3-2-1 backup Policy

3-2-1 Backup Policy Issues	NeuShield 1-1 Strategy Value Proposition
1. **Accumulated Storage**	1. NeuShield states that they require an average of 10% active data additional storage.
2. **Recovery Time Objective**	2. NeuShield claims to revert data to a "last good known state" in minutes.
3. **Backup Compromise**	3. NeuShield claims to prevent malware compromise of active data.
4. **Protect Active Data**	4. NeuShield claims to prevent data compromise in real-time.
5. **Malware Free Data Copies**	5. NeuShield claims that when embedded malware has infected templates, they can to revert to a malware free version.
6. **Network Availability**	6. NeuShield can be operated without any network/Wi-Fi connectivity.
7. **IT Resourcing**	7. NeuShield is installed using standard tools and its revert function operates simultaneously, reducing IT resource administration.
8. **Complex Configuration**	8. NeuShield claims to install and configure in 10 minutes across an organisation, working seamlessly with existing tools, requiring no integration.

Transitioning 3-2-1 into 1-1



Synergy Six included NeuShield's Data Sentinel Business Edition to the example vendor data models researched in the previous 3-2-1 analysis.

Our primary analysis purpose was to deliver comparative data points for Data Accumulation and speed of Data Recovery. In addition, due to the disturbing incremental and hidden costs observed during our initial research findings, we have included the cost differential between each of the three providers.

Table 3 shows an amended example of Table 2 including the Active Data Protection & Recovery product, NeuShield Data Sentinel.

The purpose of the table remains consistent with Table 2, showing the accumulated storage requirements, time and amount of data recoverable within a specific RTO window for an organisation that has 5TB of data and adheres to the 3-2-1 backup policy.

We have retained the two AWS backup offerings to visualise the required sustained bandwidth to recover an RPO aligned to the Day 1 5TB.

In our analysis we used the following features of the NeuShield Business Edition product to achieve the first element (1-*) of the proposed 1-1 data protection continuity policy, delivering time-sensitive recovery.

- **Mirror Shielding**™ - Real-time data protection
- **One-Click Restore** - Instant OS & application recovery
- **Data Engrams™** - Instant data revert

The second element (*-1), Data Backup Copy, for non time-sensitive recovery would be achieved using an organisation's existing backup and recovery vendor to retain a single [immutable] copy of data stored in a secondary off-site or cloud location.

1-1 Policy with NeuShield

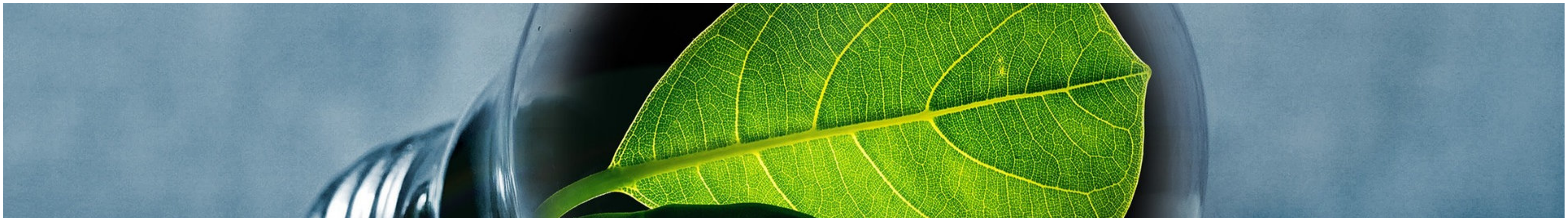
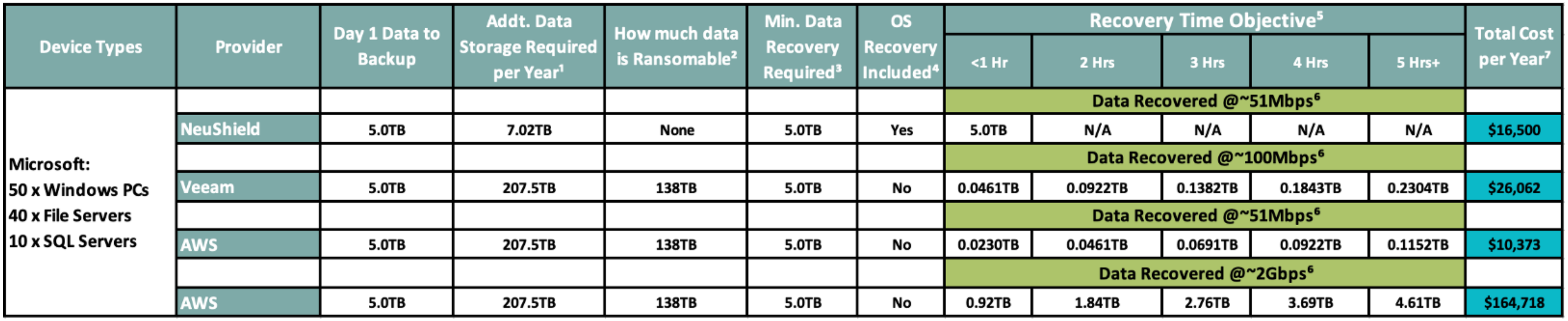


Table 4 – 3-2-1 backup and 1-1 active data protection providers



Device Types	Provider	Day 1 Data to Backup	Addt. Data Storage Required per Year[1]	How much data is Ransomable[2]	Min. Data Recovery Required[3]	OS Recovery Included[4]	Recovery Time Objective[5]					Total Cost per Year[7]
							<1 Hr	2 Hrs	3 Hrs	4 Hrs	5 Hrs+	
Microsoft: 50 x Windows PCs 40 x File Servers 10 x SQL Servers							Data Recovered @~51Mbps[6]					
	NeuShield	5.0TB	7.02TB	None	5.0TB	Yes	5.0TB	N/A	N/A	N/A	N/A	$16,500
							Data Recovered @~100Mbps[6]					
	Veeam	5.0TB	207.5TB	138TB	5.0TB	No	0.0461TB	0.0922TB	0.1382TB	0.1843TB	0.2304TB	$26,062
							Data Recovered @~51Mbps[6]					
	AWS	5.0TB	207.5TB	138TB	5.0TB	No	0.0230TB	0.0461TB	0.0691TB	0.0922TB	0.1152TB	$10,373
							Data Recovered @~2Gbps[6]					
	AWS	5.0TB	207.5TB	138TB	5.0TB	No	0.92TB	1.84TB	2.76TB	3.69TB	4.61TB	$164,718

Notes:

1 - 6 As per Tables 2 & 3.

7. Total cost per year for protection and recovery. Does not include support costs or other costed features not used in model.

Table Summary

NeuShield: Additional 'on-device' storage of 1.92TB will increase total storage to **6.92TB. Zero** data is ransomable. Recovery of all 5TB of data (and device OS) is completed in **less than 1-hour**. NeuShield license cost estimate is **$16,500** (including 2TB of new device storage). In addition, the costs for a data copy stored on immutable storage (via backup product) would require approximately c**$5,787,** taking the total 1-1 policy strategy to c**$22,287**.

Veeam: Data points remain consistent with Table 3. To meet the 5-hour RTO additional bandwidth would need to be accessible. We have estimated that an additional bandwidth one-time budget of c**$100,000** and a maximum of c**$5,787** for a data copy stored on immutable storage, taking the total Veeam cost to backup and recover c**$131,849**.

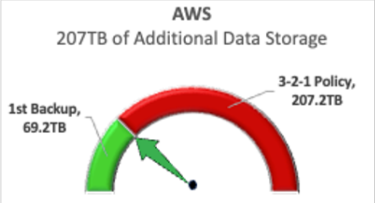
AWS: Data points remain consistent with Table 3. To meet the 5-hour RTO additional bandwidth would need to be accessible either via an on-demand request or contracted on a monthly basis. Using AWS published guideline (1Mbps bandwidth costing an extra $6.60 per month under contract), we have estimated that an additional bandwidth one-time budget of c**$154,345** is required. In addition, the costs for a data copy stored on immutable storage would require approximately c**$27,130**, taking the total AWS cost to backup and recover c**$191,838.**

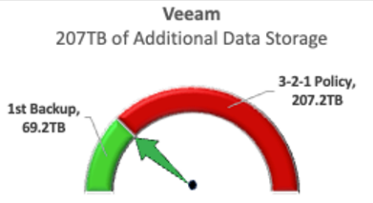
Evolving 3-2-1 into 1-1 with NeuShield

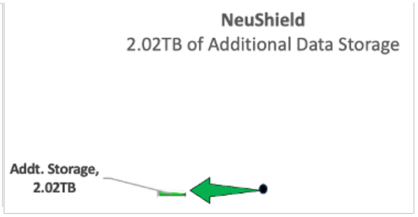
Conclusion

3-2-1 Data Accumulation

The two 3-2-1 providers will generate 69.2TB of primary backup data over a 1-year period. An additional 138TB of data is retained in case primary backup data is unavailable. In total an organisation will have 276TB of active and copied data. NeuShield required 2.02TB in the same 1-year period. No additional backup data is required for NeuShield to deliver its functionality. In total NeuShield will require 7.02TB of Active data.



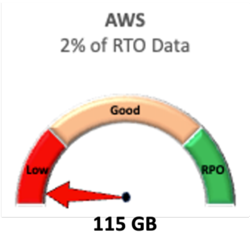


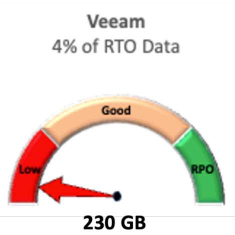


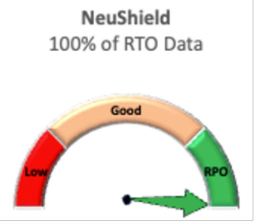
Data Recovery (5TB)

The 3-2-1 providers gravely fail to deliver full data recovery required to achieve a 5-hour RTO. The figures derived from the analysis show both AWS and Veeam only achieved 2-4% of the RPO within the required RTO. No OS recovery was included.

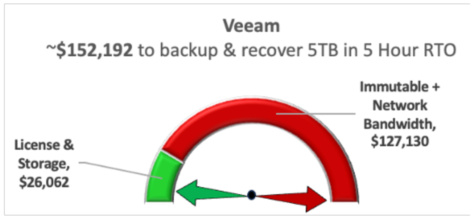
NeuShield met 100% of the RPO and RTO within 1 hour, including the device OS and applications.

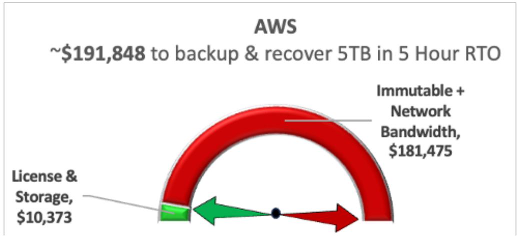




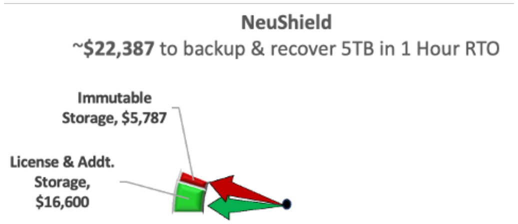


3-2-1 Backup and Recovery Costs





1-1 Data Protection and Recovery Costs



'3-2-1 Data Recovery is like paying $150 a month for a health plan with a $10,000 deductible'

Synergy Six believes that organisations can evolve from 3-2-1 to 1-1 with no impact on their ability to restore data operational continuity, immaterial of incident cause (cyber incident, hardware failure, user file deletion, bad patching).

We acknowledge that some risk averse CIOs may prefer a staging approach such as 1-2-1, Active Data Protection & Recover (**1**), plus two backup copies (**2**) (one copy in a secondary location or in the cloud) and one on a different media (**1**) (immutable), until the 1-1 strategy is proven.

Appendix A

Zero Trust Bibliography

- **Zero Trust** - Introduced in 2010 by John Kindervag as part of his zero trust model; *a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised*
- **Zero Trust Network Architecture** - *Zero trust network access (ZTNA) is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities.*
- **Zero Trust Architecture** - *an enterprise's cyber security plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.*
- **Zero Trust Security** - *Zero Trust security is a framework requiring all users, whether in or outside the organisation's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.*
- **Zero Trust Data Protection** - *Zero Trust Data Protection is the concept of not inherently trusting any user, device, application, or service with given access to one's data.*
- **Zero Trust eXtended Ecosystem Platform** - Introduced in 2019 by Forrester to extend its original ZT strategy; *Zero Trust platforms include integrated products from a single vendor's portfolio and third-party vendor technology integrations to form a Zero Trust technology ecosystem.*

Appendix B

Table 4 - Detailed Analysis

Additional 'on-device' storage is a maximum of ~10% of original in-use data storage, ***6.92TB.***

Zero *NeuShield protected data is ransomable, as all active and data engrams are protected with Mirror Shielding™.*

5TB of data resides across 100 individual devices, no dependency on network bandwidth or sequential movement of backup data via networks is required.

Completion of all reverts for operational data, applications, and OS prior to the incident is achieved simultaneously by users or IT administrators (centrally). e.g. ***1TB of data and OS/Application revert takes ~6 minutess per device****.*

NeuShield cost estimate ***$16,500*** *is priced by the type of device (PC/WorkStation/File Server/DB Server). No additional pricing uplifts are necessary for features or amount of data under protection.*

Additional storage of ***207.5TB*** *is calculated with 10% change/new files for 12 months, using daily, weekly, monthly, and quarterly backup periods. One copy of the backups is immune from being held for ransom,****leaving 138TB at risk****.*

A sustained network transfer rate of 100Mbps was modeled. A maximum of ~230GB was recoverable within a 5-hour RTO, ***leaving 4.77TB of data yet to be recovered****. No consideration was modeled to include the separate time required to recover device OS/Applications.*

To achieve the recovery of all 5TB of data, within a 5-hour time window, an increase of ~27 x original sustained network transfer rate (100Mbps) would be required either under contract or invoked (on-demand) during incident response.

Veeam cost estimate $26,062 is priced using the Veeam cost calculator using number of devices and size of data to be backed up. No additional pricing uplifts were added for product features such as advanced, premium, NAS Storage, MS365, Salesforce, etc.

*Including the additional bandwidth to recover all 5TB within the 5-hour RTO window, we estimate additional one-time budget of c****$100,000 allocation of budget****, taking the Veeam cost to recover c****$126,000****.*

Additional storage of 207.5TB is calculated with 10% change/new files for 12 months, using daily, weekly, monthly, and quarterly backup periods. One copy of the backups is immune from being held for ransom, ***leaving 138TB at risk****.*

In this model, AWS contracted network bandwidth of 51Mbps could achieve a maximum of ~115.2GB of data recovery within a 5-hour RTO, ***leaving 4.85TB of data yet to be recovered****. No consideration was modeled to include the separate time required to recover device OS/Applications*

To achieve the recovery of all 5TB of data, within a 5-hour time window, an increase of ~39 x original sustained network transfer rate (51.2Mbps) would be required either under an existing monthly contract or on-demand during incident response. We estimated the capability to recover 4.61TB within a 5-hour RTO window. The remaining 39GB would require an additional 25 minutes to recover.

AWS cost estimate $10,373 was the lowest priced using the AWS cost calculator using number of devices and size of data to be backed up. No additional pricing uplifts were added for product features such as data residency, subsequent data movement, etc. The cost per MB to recover data was not factored in.

*Including the additional bandwidth to recover all 5TB within the 5-hour RTO window, we estimate an additional one-time budget of c****$154,345 allocation of budget,*** *(using AWS published guideline of 1Mbps bandwidth costing an extra $6.60 per month under contract). taking the AWS cost to recover c****$164,718.***