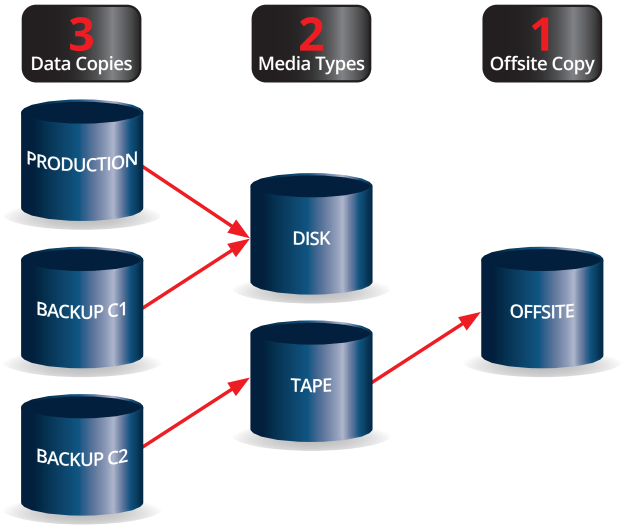
Cloudlake Datasheet

autodata

# The 3-2-1 Cloud Backup Strategy
# (the Autodata 101!)

**The 3-2-1 Backup Strategy has been a mainstay for years in the data-storage space, endorsed by almost every backup vendor at some point and advised by many governments globally. If you don't know what 3-2-1 means, then I hope to enlighten you. If you do, I'd like to give you an insight into the possibilities of 3-2-1 in the modern infrastructure environment. Even if the name is new to you, it's very possible this is still the approach you have taken for many years that industry professionals like myself have continually advised.**

The basic strategy revolves around having **3** copies of your data on **2** different mediums (systems) with at least **1** of those offsite from the primary data source.



Your 3-2-1 setup may look a bit different: you may replicate your primary data storage to a secondary DR site then take a backup from there, or take multiple backups to different disk arrays; or you may use a cloud provider for offsite backup, rather than having tapes collected/taking them home with you. But ultimately most businesses have implemented some kind of similar strategy.

3-2-1 is a well-adopted and sound approach, and traditionally it's a strategy designed to fit into the majority of on-premise infrastructures, offering a good level of protection against traditional threats to data security (both malicious and accidental). **The key question is though: "is it the BEST strategy for your business today"?** I'd argue maybe, at best!

Modern infrastructures are changing with a drive towards cloud adoption across almost every business sector. Data-security policies dictate critical and sensitive business data is not stored in your home office or in the back of your car.

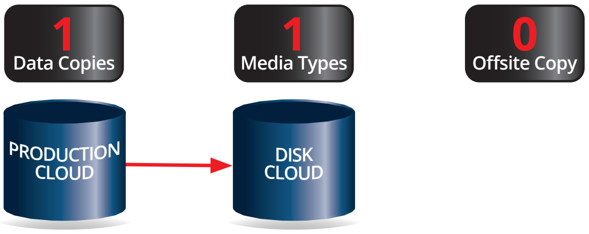
Compliancy across many industries means not only are you required to store your data securely, but you have to be able to retrieve it in a timely manner and/or dispose of all data no longer necessary. As a result, the traditional 3-2-1 strategy may no longer fit the bill.

**To cut to the chase, I'll give you an example of something we discuss daily with clients relating to cloud-based services**, whether it be O365, Azure, AWS, Google Workspace (formerly G Suite) or another cloud platform.

By early 2020, cloud-service adoption was already steadily rising. Throughout the pandemic and beyond, its trajectory will continue. As a result of such rapid implementation, many organisations are increasing, not decreasing, their data risk. This is usually a direct consequence of not installing adequate protection and/or ignoring best practices. This can sometimes be down to budget constraints, but is much more likely to be due to a misinterpretation of the platform responsibilities.

Cloud providers commonly operate a "shared responsibility" model, whereby **THEY** will look after **THEIR** infrastructure but **YOU**, as the user of their service or services, are responsible for **YOUR** data. This is highlighted in Microsoft's own Service Agreement where they clearly state: *"We recommend that you regularly backup Your Content and Data that you store on the Services [...] using Third-Party Apps and Services".*

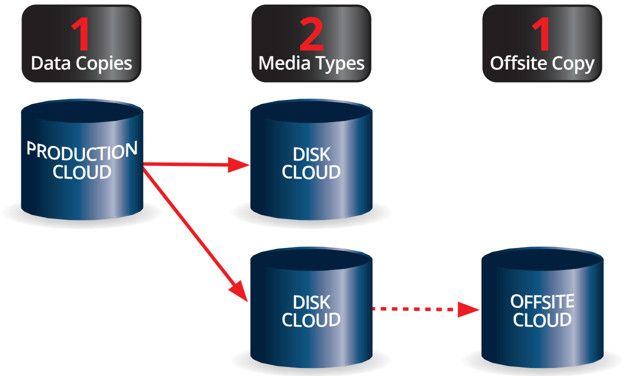
How does this cloud model look without utilising any tools?



THAT'S **NOT GOOD!**

# The 3-2-1 Cloud Backup Strategy (cont/d)

I have heard people say, “but I have Geo-Redundancy and/or retention policies in place for my data”, and it could be argued that the following diagram is an over-estimation of that protection (as the “theory” behind the offsite copy was to provide an air gap between systems) but allowing for the benefit of the doubt:

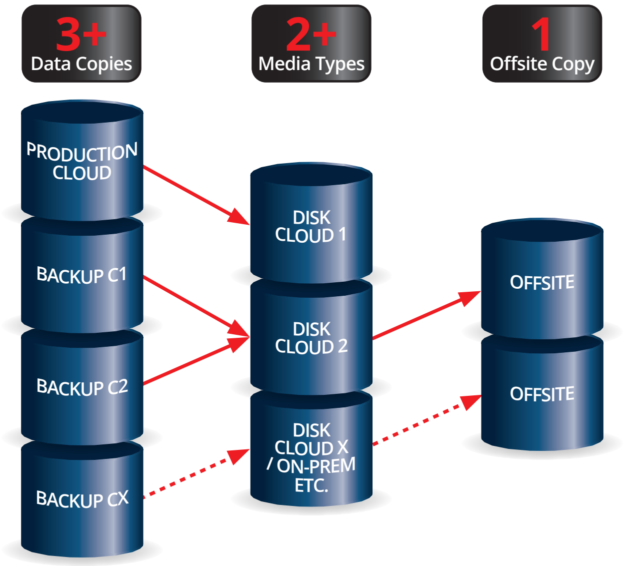


**STILL NOT GOOD!** We can and should do better than this. Moving to the cloud should help mitigate risk, not increase it.

At Autodata, our Cloudlake platform enables us to backup these services to a separate cloud or clouds, in geographically separate locations, across multiple data-capture points, even branching back out to on-premise storage if required.

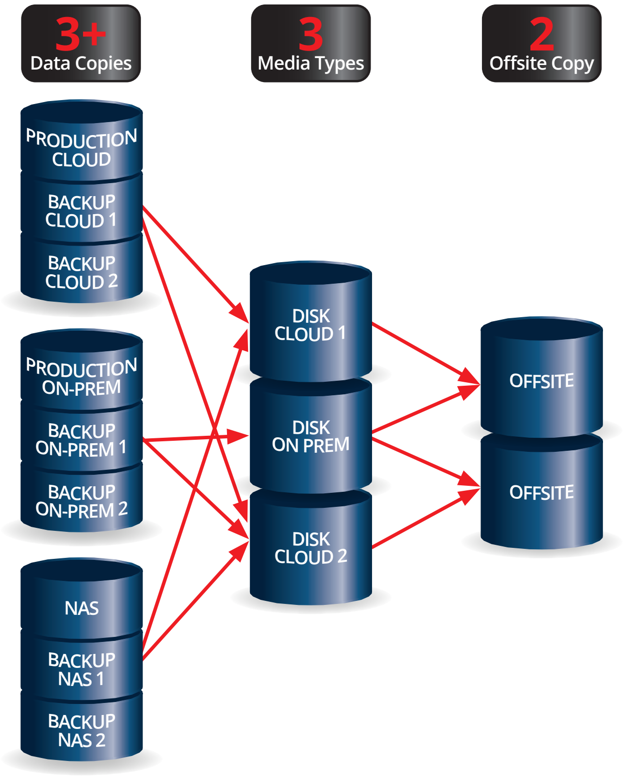
Cloudlake can capture an unlimited amount of data. This ensures that not only the current data is stored and recoverable, but also that historical data can be archived and restored for compliance, statistical or any other requirements, including in the event of any data loss, breach or attack.

This is what a basic Cloudlake backup solution would look like for O365/Azure/AWS/Google etc:



**But what about data stored on-premise?** By utilising the cloud for backup (which you may already do) we can again decrease the risk to your data. Cloudlake can combine both your on-premise backup and your cloud backup - as well as archiving and ‘NAS’ solutions - into one hybrid platform.

Although every environment is unique, here is an example which can be tailored to individual need and risk:



**Ultimately, whether you’re looking to:**

(a) “get back” to the 3-2-1 your organisation operated traditionally or

(b) improve this model either on-premise or in-cloud,

**the solutions exist to help you achieve it SIMPLY, SECURELY and COST-EFFECTIVELY.**

**Get in touch to find more out about CLOUDLAKE today.**

Ant Bucknor, Data Centre & Cloud Specialist
E: ant@autodata.co.uk