ArkivumLimited
R21 Langley Park Way
Chippenham
Wiltshire
SN15 1GE
UK

+44 1249 405060

info@arkivum.com
@Arkivum
arkivum.com

Arkivum's Digital Archive Managed Service

Service Description

Table of Contents

Introduction

Arkivum Ltd is an established provider of long term, digital data archiving solutions.

The Arkivum digital archiving services are used by organisations that are required to retain and access their valuable data for extended periods of time due to compliance, industry best practice or IT cost saving drivers.

The industry leading A-stor data archiving service, provides a fully-managed and secure service for long-term data retention with online access and a 100% guarantee of data integrity, a Service Level Agreement and backed by worldwide insurance.

Arkivum provides this service by storing and managing three copies of customer data; two copies are near-line using tape libraries in UK data centres, which provides high availability and quick access, the third copy is stored offline on data tape at a third-party data Escrow facility. This Escrow copy provides added customer assurance and security as they are able to retrieve their date in all circumstances (such as the customer wanting to terminate their contract and move their data elsewhere).

As part of the service, Arkivum manages all the media, hardware and software migrations needed to ensure that data is available to the customer in the future in a “bit-for-bit” identical form to the original deposit.   This data integrity is guaranteed and underwritten by a 100% data guarantee. Finally, there are no restrictions on time or volume of data stored, for example many of our clients are storing data within the service for 50 years plus..

All the client data within the service is encrypted for confidentiality, is guaranteed for data integrity and is stored in a high availability infrastructure giving quick data access when needed. Secure UK facilities, ISO27001 policies and procedures, strong data encryption, secure access control, and full audit trails together mean that the Arkivum service meets UK legal requirements for the storage of sensitive data.

The service can be procured using either a Capex model (where a specified storage volume is purchased in one transaction for a defined period of time), or an Opex model (where the storage volume is decided and purchased each year). For added flexibility, both models can be mixed within the same contract. The storage fees cover all elements of the service, for example there are no “extra” fees for data retrieval, calling Arkivum’s support staff or migrating data to new media types.

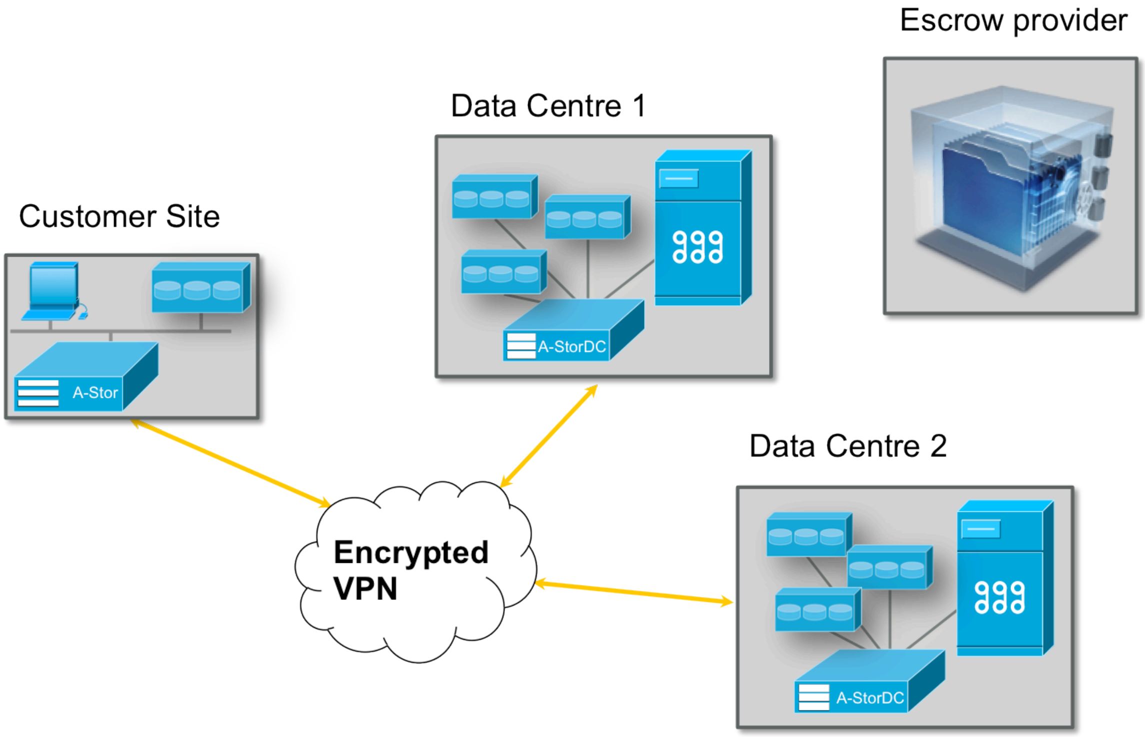
Organisations that use the A-Stor service benefit from increased levels of compliance whilst at the same time reducing the IT spend on storage and administrative overhead.

This document describes the A-Stor service where the data is kept within Arkivum's share managed service. For organisations that cannot allow their data to go off-site, then Arkivum's Oscar, (On-Site Cloud ARrchive managed service), provides a compelling alternative. It has all the all the features and benefits of A-Stor but is run and managed within a client's own infrastructure.

Please contact Arkivum on +44 1249 405060 for further details or visit www.arkivum.com.

How the A-Stor Service Works

Arkivum follows data preservation best practice by storing three complete and independent copies of customer data in three geographically separate locations. Two are stored nearline in colocation Data Centres. The third is stored offline by a third party under Escrow (or at the customer site depending on the agreement with the customer). Each copy is stored on LTO data tape. There may also be additional copies stored on disk caches for performance and access. The creation of all these copies is automatic and transparent to the user of the service. Each copy has its integrity monitored and managed and any corruptions or loss automatically repaired to make the system self-healing. A-Stor only stores encrypted data.



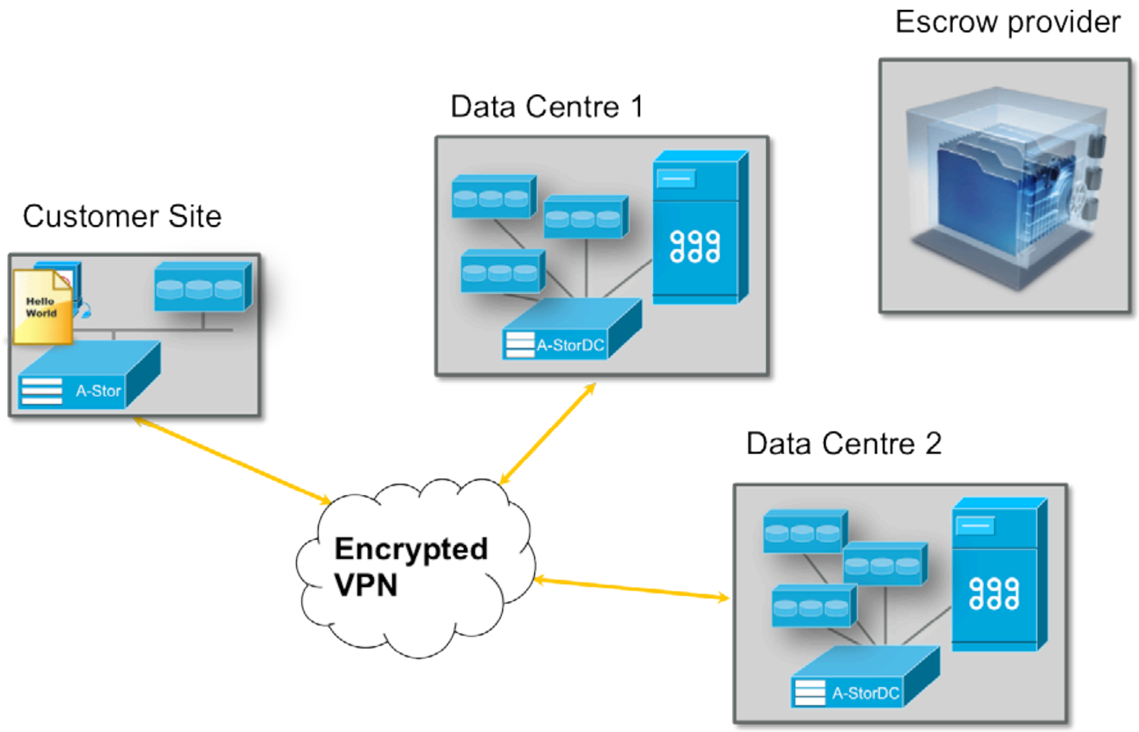
There are six stages that a file goes through to reach the point where it is covered by the 100% data integrity guarantee:

1. File is copied onto the A-Stor appliance
2. A-Stor appliance encrypts the file
3. Encrypted file is copied to Data Centre 1
4. Data Centre 1 transfers copy of encrypted file to Data Centre 2
5. Data Centre 1 generates tape for Escrow
6. The 100% data integrity guarantee for the file is now active.

Throughout these stage the data is easily accessible to the customer. They can go in and get the files back with the same name and path that they used when they originally provided the data.

The following sections show each of the stages.

Stage 1: File is copied onto A-Stor appliance



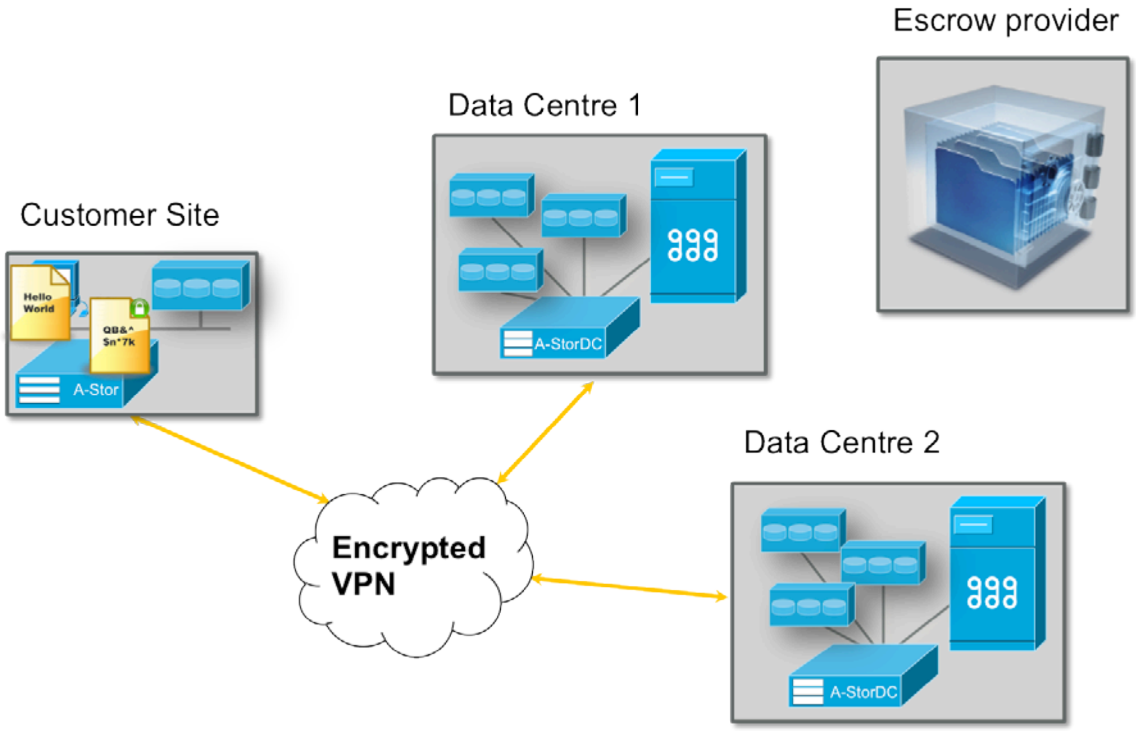
An appliance on a customer site provides a gateway into the Arkivum archiving service. The file is cached on local disk within the appliance.

The appliance can be physical or virtual and exposes a file system, this means getting files into the archive is simply a case of copying them in, just like using any other network file system.

A REST API is available for integration with other systems. An Automated Data Importer utility is available from Arkivum.

See Appendix A for the specification of A-Stor appliances.

Stage 2: A-Stor appliance encrypts the files

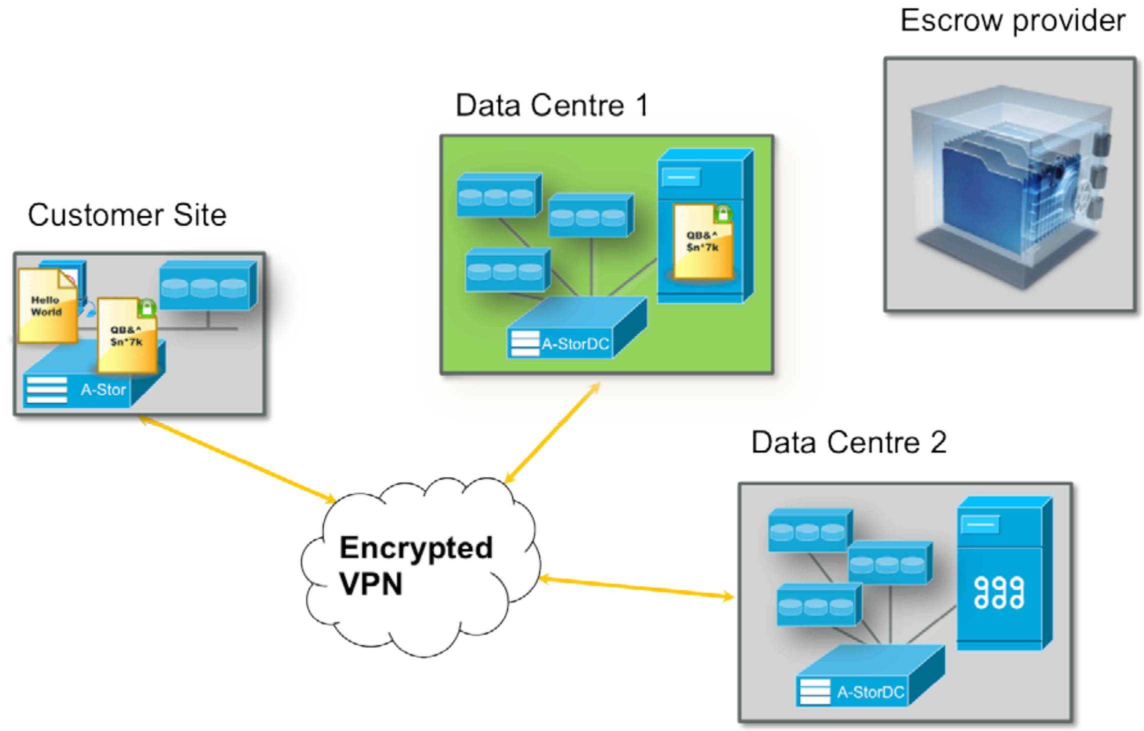


As soon as the files come into the archive onto the appliance, they are immediately checksummed and encrypted, using industry standard mechanisms, and stored locally.

The files are always encrypted before they leave the customer network. The customer holds the encryption key. This means that only the customer can decrypt the data stored within the Arkivum service.

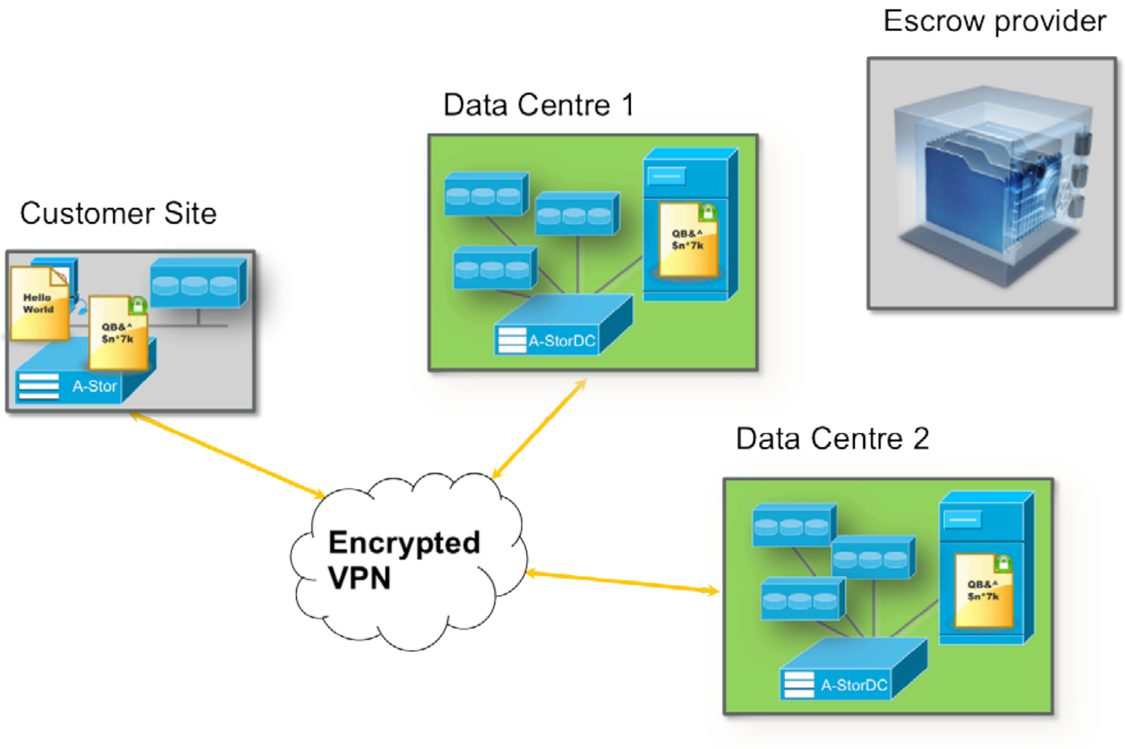
From this stage on, whenever copies of the data are made checksums are used to ensure that the copy has been correctly received and stored.

Stage 3: A-Stor Appliance copies encrypted file to Data Centre 1



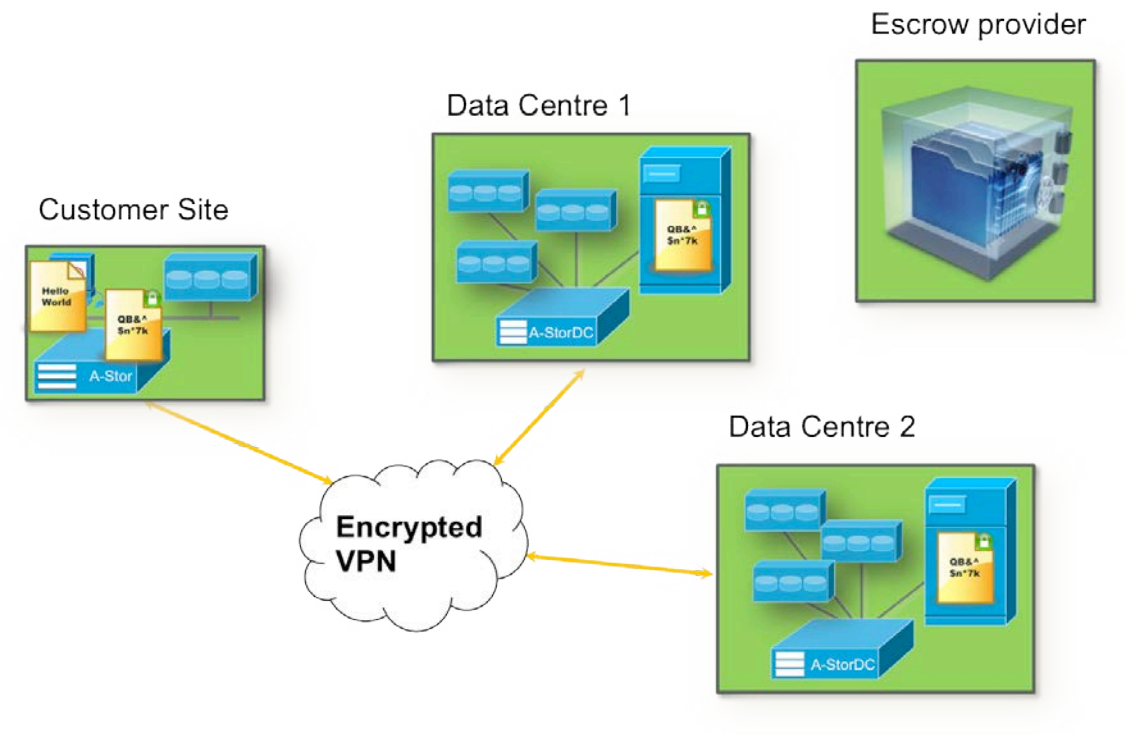
The encrypted file is then replicated to the first Data Centre via secure VPN. At the Data Centre the data is stored on LTO data tape in online tape library for easy access.

Stage 4: Data Centre 1 copies the file to Data Centre 2



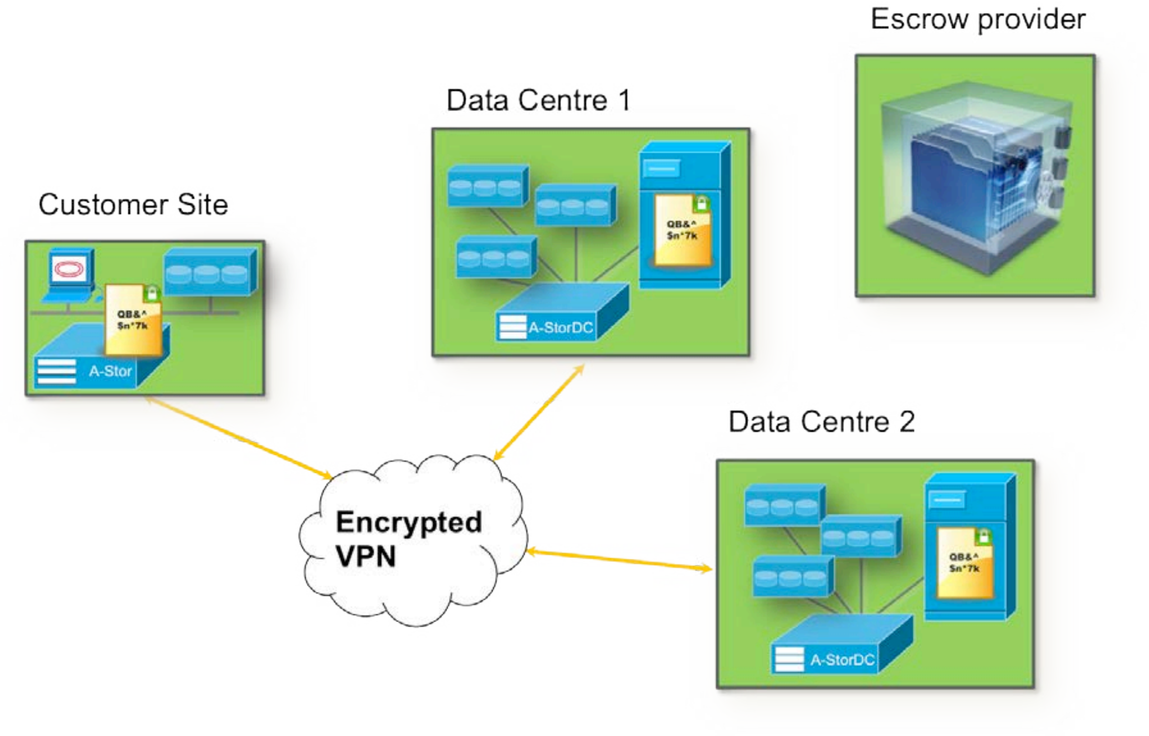
The file is then replicated from Data Centre 1 to the second data centre in a different geographical location. Again it's stored on LTO tape in a library. At this point there are now two copies nearline with a high availability and good resilience.

Stage 5: Data Centre 1 creates tape for Escrow



A third copy is then made and is held offline in a secure independent 3rd party escrow location (or to the customer site depending on the agreement with that particular customer). This copy uses LTFS on data tape along with open source tools so if the customer ever needs to access their data, they can be sure they can do so without having any reliance on Arkivum or the Arkivum service.

Stage 6: 100% data integrity guarantee now applies to the file



When all three copies have been created and are securely stored, A-Stor gives the customer the green light that they can remove their local copy if they need to (for example to free up space). At this point the 100% data guarantee is now in effect for the archived data.

OSCAR – On-Site Cloud ARchive

Recognising that many organisations don't allow their data to go off-site, OSCAR, Arkivum's On-Site Cloud ARrchive, offers all of A-Stor data integrity and management features within a corporate firewall, making it ideal for organisations where confidentiality or regulation requires all information to be stored onsite.

The 'OSCAR' pod solution, which incorporates a tape library and server running Arkivum's A-Stor, is located 'on-site' on the customer's premises, either within a private data centre or alongside other customer IT infrastructure in a co-location facility.

Appendix A: A-Stor Appliance Specification

System Specification	**Micro Edition**	**Mini Edition**	**Enterprise Edition**
Supported Protocols	CIFS SMB	NFS v3 CIFS SMB	NFS v3 CIFS SMB
File Shares Supported	1	3	128
Archive Size Supported	Up to 3TB	Up to 30TB	Unlimited[1]
Maximum Single Ingest	256GB	1TB	2TB Upwards
Useable Disk Cache	500GB	3TB	4TB Upwards
Disk Technology	SATA	SATA (RAID 5)	SAS (RAID 6 inc BBU)
Standard Connectivity	Single GbE	Dual GbE	Quad GbE
Management Interface	-	Remote Management capability over shared network interface	Full Remote Management over dedicated management interface
Optional Connectivity	-	-	Network: • Additional GbE Ports • 10GbE Ports • Infiniband up to 56Gb/s Storage (For Cache): • Fibre Channel up to 8Gb/s • SAS 6Gb/s • iSCSI NIC Other Qualified PCI Devices
Storage Resilience	-	RAID	Dedicated Hardware RAID with BBU
Memory Resilience	-	-	ECC RAM
Physical Specifications			
Form Factor	Compact System	NAS Mini Tower	2u Server

Power	100-240V AC, 50/60Hz, Auto-sensing, 2 Amps	100-240V AC, 50/60Hz, Auto-sensing, 2 Amps	Dual Redundant PSU, Platinum Rated, 100-240V AC, 50/60Hz, Auto-sensing, 10 Amps - 5 Amps
Width	63mm	148mm	444mm (482.4mm inc mount points)
Height	294mm	284mm	87.3mm
Depth	292mm	294mm	723.0mm
Weight (Max)	6.3kg	10.2kg	32.5kg
Environmental Data			
Operating Temperature	10 to 35 °C	10 to 35 °C	10 to 35 °C
Operating Humidity	10-80% relative humidity	10-80% relative humidity	10-80% relative humidity
Warranty Data			
Duration	1 Year	1 Year	3 Years (Extendable to 5)
Type	Return To Base	Advanced Replacement[2]	On Site 4 Hour response