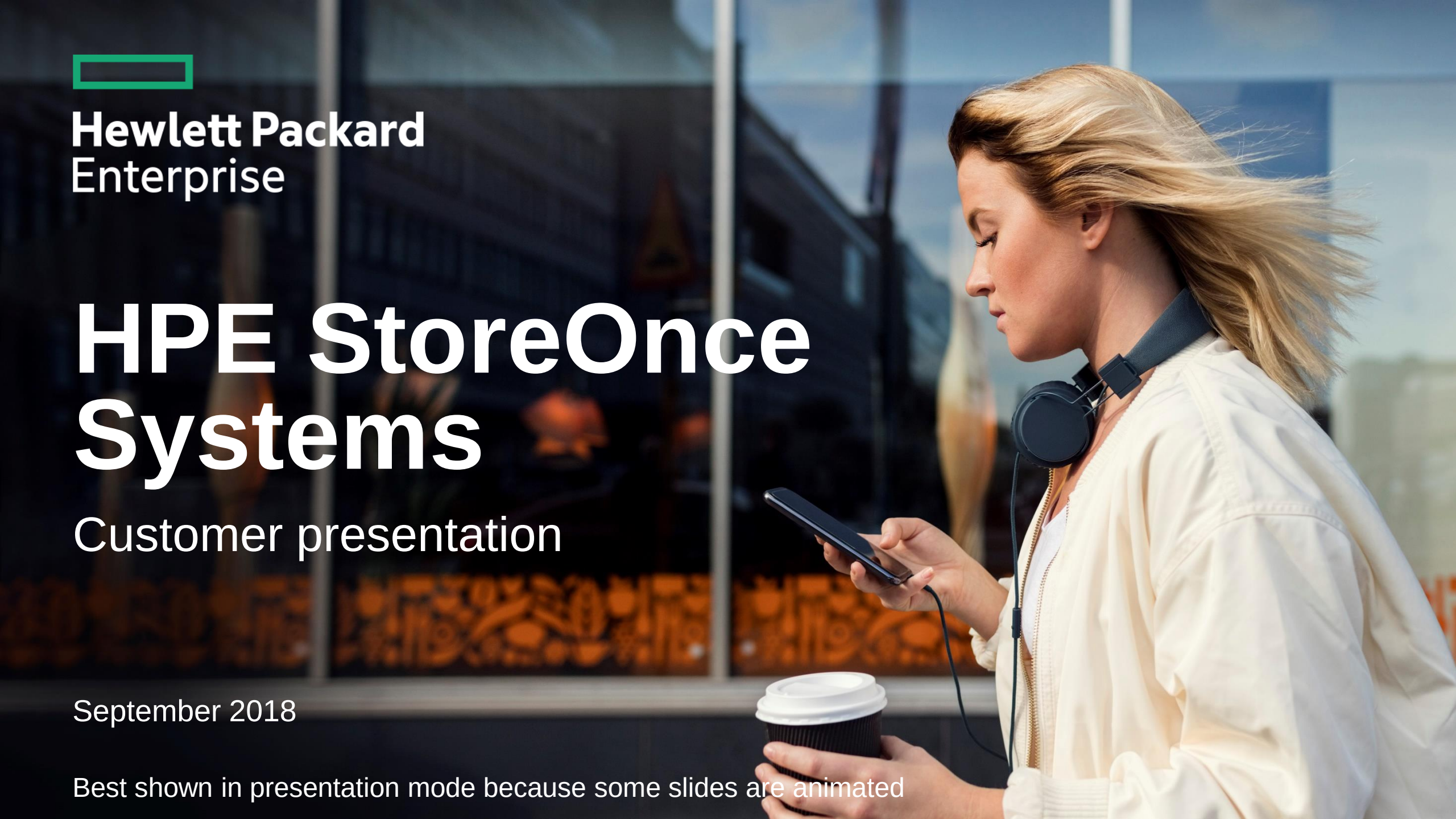


Hewlett Packard Enterprise

HPE StoreOnce Systems

Customer presentation

September 2018

Best shown in presentation mode because some slides are animated

Hewlett Packard Enterprise

HPE StoreOnce Systems

HPE StoreOnce

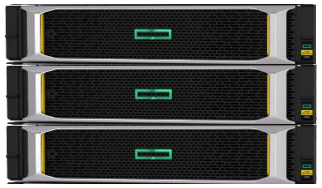
What is it?

- HPE StoreOnce is a stand-alone, disk-based data protection appliance that can be implemented as hardware or deployed as a software virtual storage appliance on VMware vSphere or Microsoft Hyper-V
- The key features of StoreOnce are deduplication, compression, encryption, remote replication, and direct application-managed integration
- Backup applications use StoreOnce backup systems as targets or they can be unified with HPE 3PAR by using HPE Recovery Manager Central (RMC)
- The StoreOnce portfolio spans from entry to enterprise and can expand into the cloud with HPE Cloud Bank Storage, tripling usable capacity

VSA

VSA series
4–500 TB usable
+1 PB with CBS

3620
16–31.5 TB local/usable
+63 TB with CBS



3640
108 TB local/usable
+216 TB with CBS

5200
216 TB local/usable
+512 TB with CBS

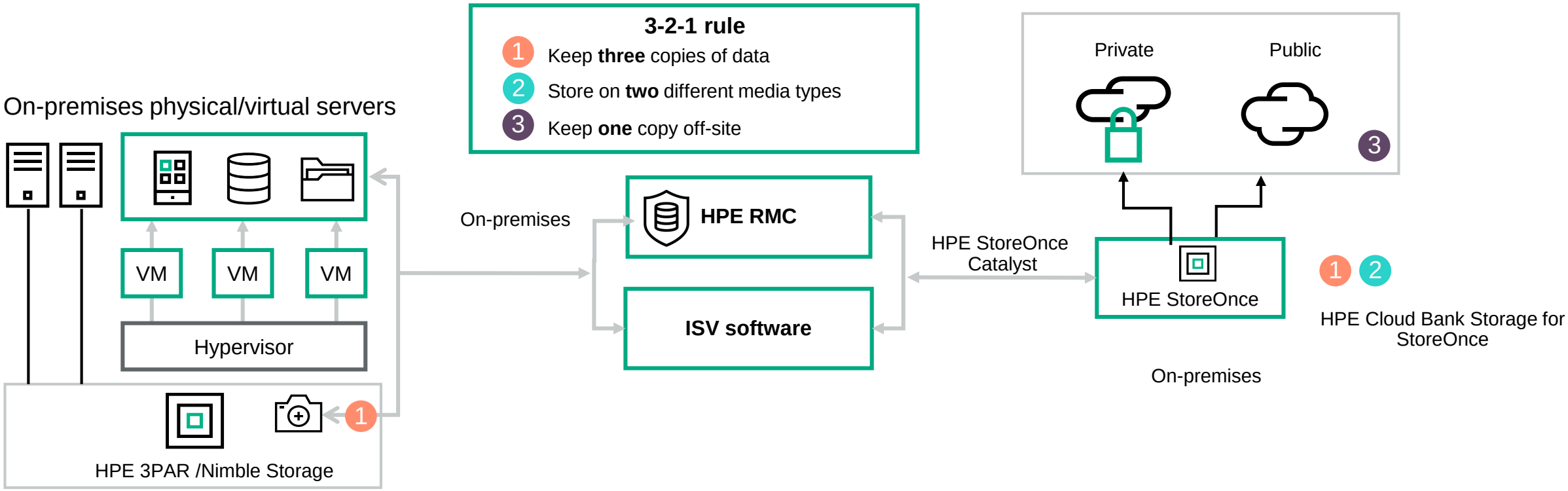
5250
864 TB local/usable
+1728 TB with CBS

5650
1.7 PB local/usable
+3.5 PB with CBS

Hewlett Packard Enterprise

Data protection for Hybrid IT

HPE solution overview

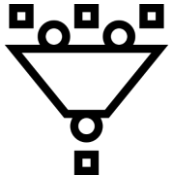


Services

HPE Pointnext and partners
Consulting, support, and education

HPE Financial Services
Flexible capacity and technology refresh

HPE StoreOnce advanced features



Federated deduplication
Multiple appliances use a single dedupe store for capacity savings

Assessment tools
Improve your understanding of your backup environment

Virtual storage appliance
Deduplication in a VM is ideal for ROBOs and virtualized environments

Cloud Bank Storage
StoreOnce deduplication with the cost benefits of cloud storage

Recovery Manager Central
Implement fast, cost-effective protection of HPE 3PAR StoreServ and HPE Nimble*

Hewlett Packard Enterprise

* Available in early 2019

Architecture and interface

HPE StoreOnce uses a flexible, modular architecture

Enables flexible deployment and integration

– Modular 64-bit architecture

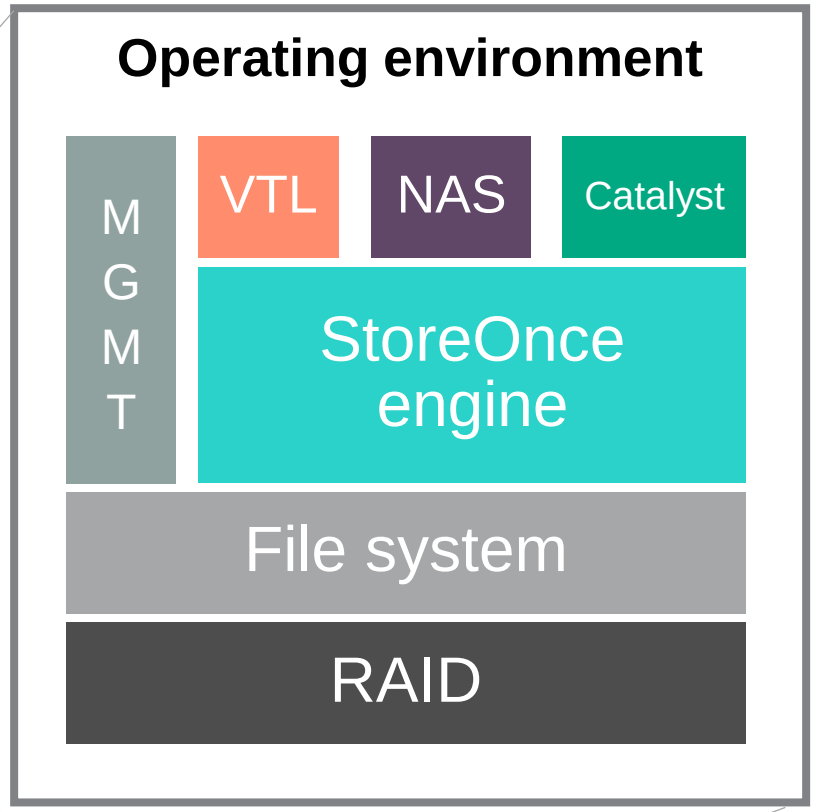
– Lightweight Linux environment

– Well-defined target interfaces

– StoreOnce engine developed by HPE Labs
  – More than 50 patents

– Proven blend of industry-standard components
  – HPE ProLiant DL380 servers
  – HPE disk storage
  – HPE RAID controller

– No dependencies, no compromises
  – Complete HPE stack



Hewlett Packard Enterprise

Nodes and enclosures

Server node

The server node is an HPE ProLiant based server that handles management and data processing

The 3600 series has either 6 or 12 x 4 TB 7200 RPM hard drives used as data disks

These disks are protected using RAID 6

The 5000 series hosts two mirrored small disk drives used as operating system disks

These disks are protected using RAID 1

Disk enclosures

StoreOnce storage capacity can be expanded by adding disk enclosures* (not applicable to 3620)

Value-based enclosures are ideal for low-cost, high-capacity, mid-tiered environments

Dense and data-intensive enclosures are ideal for enterprise environments

*The number of enclosures added depends on the server node

StoreOnce VSA

Virtual storage appliance

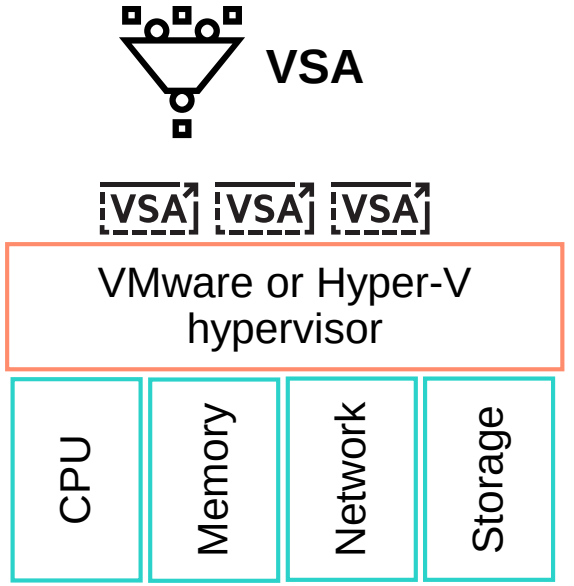
- Maximum write performance: 36 TB/hour (Catalyst)
- Maximum number of concurrent data streams: 256
- Maximum number of backup targets: 32 stores
- Fan-in ratio: 8 sources
- 90-day demo license

Resource minimums and maximums

- vRAM: 24 GB / 320 GB
- vCPU: 2 / 36
- IOPS: 600 / 10,800
- Dedicated hard drives: 4 / 72

Capacity

- Minimum configuration: 4 TB
- Maximum configuration (with expansion): 500 TB
  - Attain maximum storage capacity by adding licenses
- Cloud Bank Storage (licensed) maximum capacity: 1 PB



Next Generation StoreOnce models – StoreOnce 3620 BB954A

BB954A base unit

Without bezel

BB960A 6 x 4TB expansion disks

StoreOnce 3620 (minimum configuration 16 TB)

- Based on HPE ProLiant Gen10 hardware
- Two Intel Xeon 4110 Skylake CPUs (8-core)
- Six 4 TB LFF disks
- 2U form factor based on ProLiant DL380
- Four 1GbE LoM modules
- iLO 5
- Optional 10GbaseT, 10/25GbE, 16/32 Gb Fibre Channel
- HPE p1224 SAS RAID controller
- HPE P408i Smart Array (for boot disks)
- Two 600 GB SFF operating system disks (at rear)
- SAS expander
- Dual redundant power supplies
- Optional six 4 TB disk expansion kit (max. useable 31.5 TB)

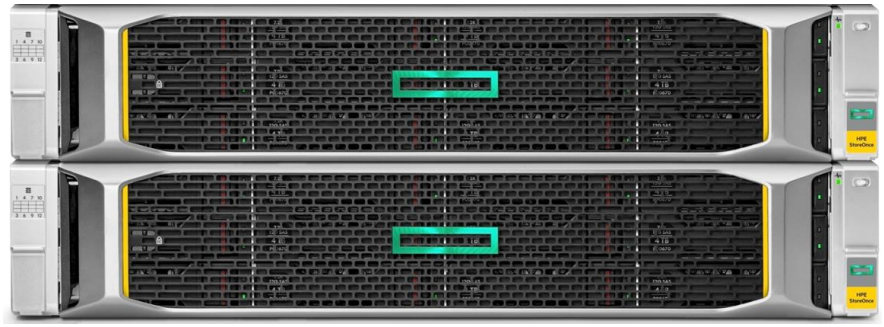
Notes:

- Expansion shelf JBOD is not supported on this model
- No hot spare on this model

Hewlett Packard Enterprise

Next Generation StoreOnce models – StoreOnce 3640 BB955A

BB954A base unit

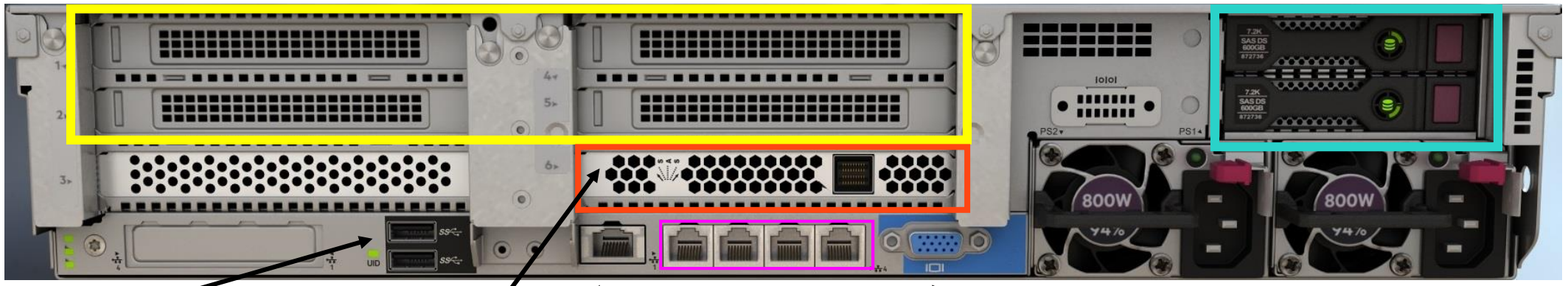


BB962A expansion shelves

StoreOnce 3640 (minimum configuration 36 TB usable)

- Based on HPE ProLiant Gen10 platform
- Two Intel Xeon 4110 Skylake CPUs (8-core)
- Twelve 4 TB LFF disks
- 2U form factor, 6U with max expansion
- Four 1GbE LoM modules
- iLO 5
- Optional 10GbaseT, 10/25GbE, 16/32 Gb Fibre Channel
- HPE p1224 SAS RAID controller
- HPE P408i Smart Array (for boot disks)
- Two 600 GB SFF operating system disks (at rear)
- SAS expander
- Dual redundant power supplies
- One or two D3650 JBOD storage shelves each with 12 x 4TB can be added
  - These connect via 12 Gb/s SAS to the RAID controller in the 'head' unit
- One 'hot' spare in head unit and expansion shelves
- License required; provided with hardware
- Requires additional 2U or 4U of rack space
- Fully expanded = 108 TB of capacity

Next-generation StoreOnce 3620 and 3640 rear view



StoreOnce 5200

BB956A

Based on ProLiant DL380 LFF disk Gen10 server

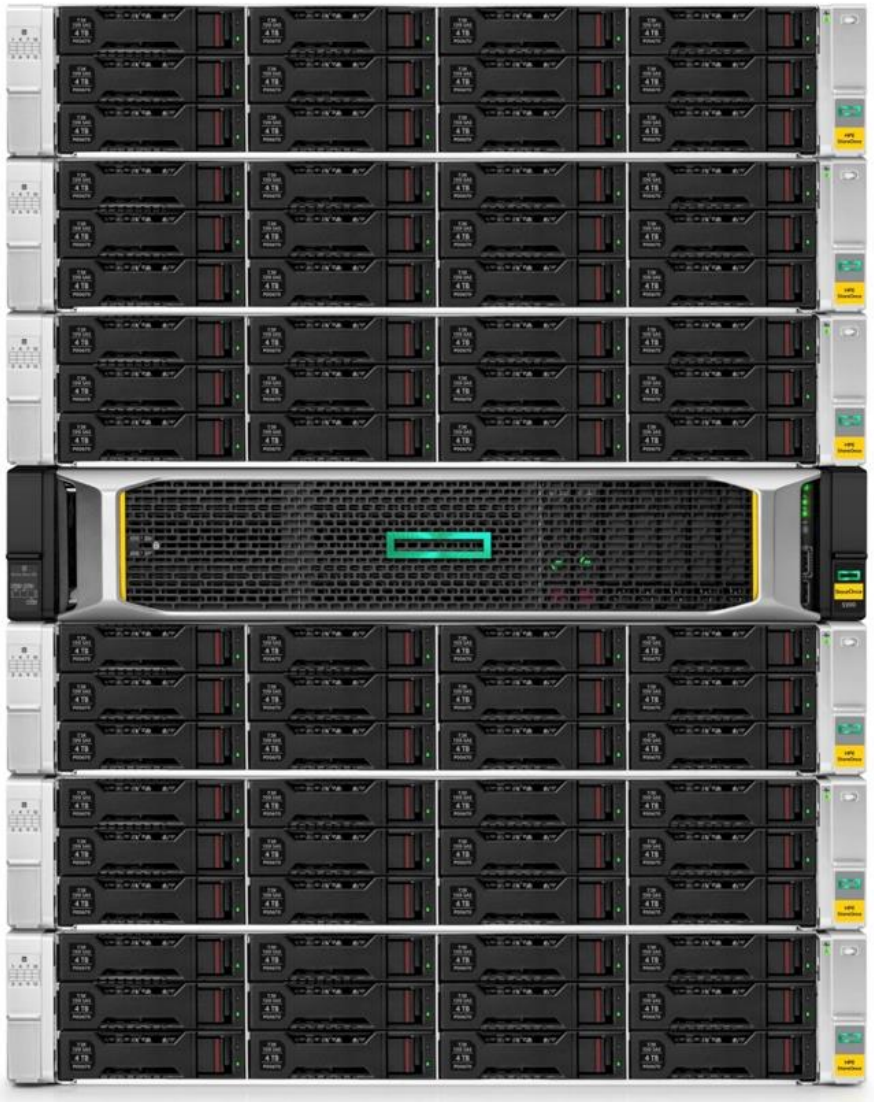
- Two Intel Xeon 5118 Skylake CPUs (12 cores)
- Maximum write performance: 33 TB/hour (Catalyst)
- Maximum number of concurrent data streams: 512
- Maximum number of data stores: 64
- Maximum fan-in or backup targets: 32
- Redundant 800W PSUs standard
- Dedicated, redundant operating system drives (front drive bays)

Flexible I/O configurations

- Supports one to four I/O HBAs in any combination
- Four types available:
  - 10 base-T
  - 10 Gb or 25 Gb Ethernet
  - 16 Gb Fibre Channel (Note: There is no 8 Gb HBA)
  - 32 Gb Fibre Channel

Storage

- Minimum configuration: 36 TB
- Maximum configuration (with expansion): 216 TB
  - Attain maximum storage capacity by adding up to five disk enclosures (BB964)
- Shelf data disk RAID 6 (9+2) plus hot spare
- Cloud Bank Storage (licensed) maximum capacity: 432 TB



StoreOnce 5250

BB958A

Based on ProLiant DL380 disk Gen10 server

- Two Intel Xeon 5118 Skylake CPUs (12 cores)
- Maximum write performance: 41 TB/hour (Catalyst)
- Maximum number of concurrent data streams: 512
- Maximum number of data stores: 64
- Maximum fan-in or backup targets: 32
- Redundant 800W PSUs standard
- Dedicated, redundant operating system drives (front drive bays)

Flexible I/O configurations

- Supports one to four I/O HBAs in any combination
- Four types available:
  - 10 base-T
  - 10 Gb or 25 Gb Ethernet
  - 16 Gb Fibre Channel (Note: 8Gb/s Fibre Channel HBA discontinued)
  - 32 Gb Fibre Channel

Storage

- Minimum configuration: 36 TB
- Maximum configuration (with expansion): 864 TB
  - Attain maximum storage capacity by adding up to one additional (fully populated) storage enclosure (BB976A)
- Data drive RAID 6 (9+2) plus two roaming hot spares (each drawer)
- Cloud Bank Storage (licensed) maximum capacity: 1728 TB

StoreOnce 5650

BB959A

Based on ProLiant DL380 Gen10 server

- Two Intel Xeon 6130 Skylake CPUs (15 cores)
- Maximum write performance: 47 TB/hour (Catalyst)
- Maximum number of concurrent data streams: 1024
- Maximum number of data stores: 192
- Maximum fan-in or backup targets: 50
- Redundant 800W PSUs standard
- Dedicated, redundant operating system drives (front drive bays)

Flexible I/O configurations

- Supports one to four I/O HBAs in any combination
- Four types available:
  - 10 base-T
  - 10 Gb or 25 Gb Ethernet
  - 16 Gb Fibre Channel (Note: There is no 8 Gb HBA)
  - 32 Gb Fibre Channel

Storage

- Minimum configuration: 36 TB
- Maximum configuration (with expansion): 1728 TB
  - Attain maximum storage capacity by adding up to three additional (fully populated) storage enclosure (BB976A)
- Data drive RAID 6 (9+2) plus two roaming hot spares (each drawer)
- Cloud Bank Storage (licensed) maximum capacity: 3456 TB

D6020 disk expansion units for StoreOnce 5250 and 5650

Rear view

Drawer 2 Drawer 1

Mini-SAS HD cables

- Interface 12Gb/s SAS
- Managed SAS cables only (supplied with product)
- Internal SAS and disks run at 6Gb/s

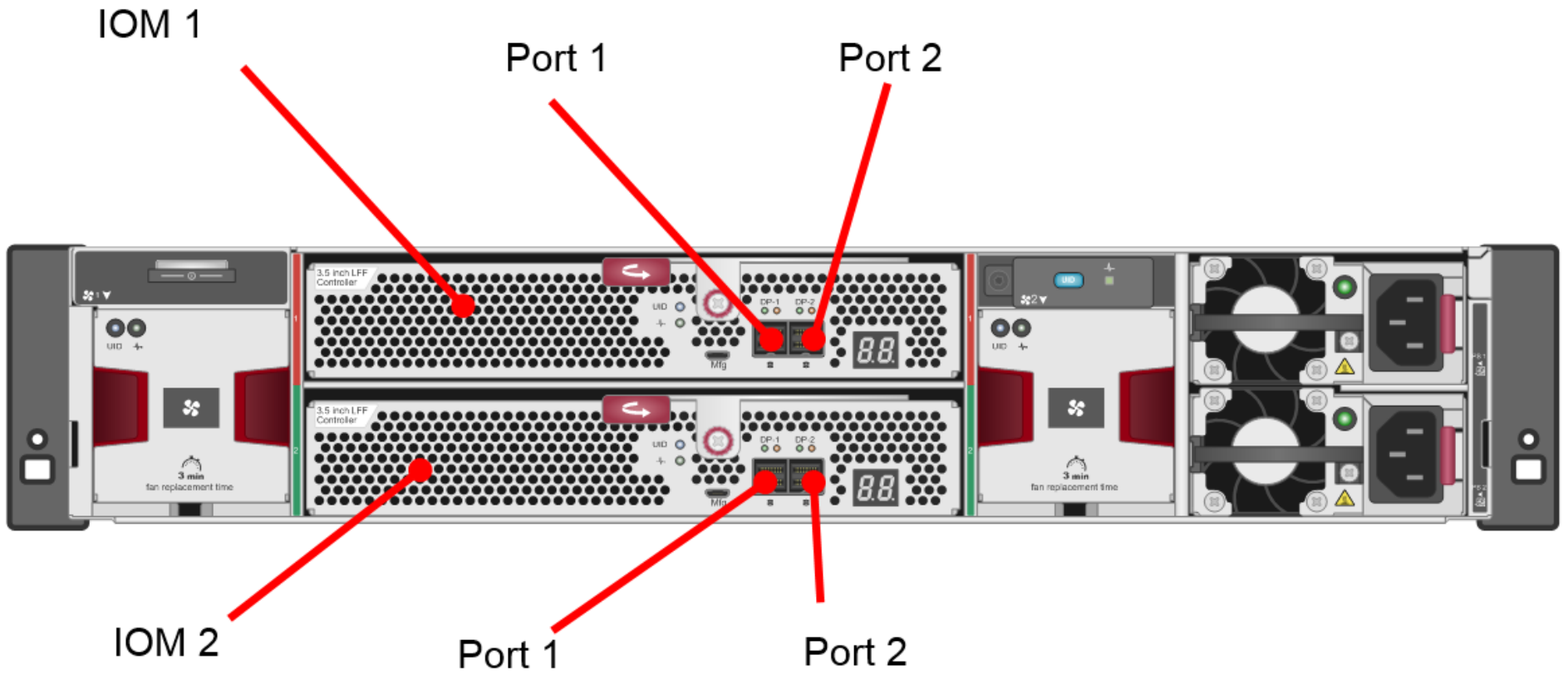
Hewlett Packard Enterprise

D6020 disk expansion units for StoreOnce 5250 and 5650

Drawer 1 extended

D3650 disk expansion shelf for StoreOnce 5200

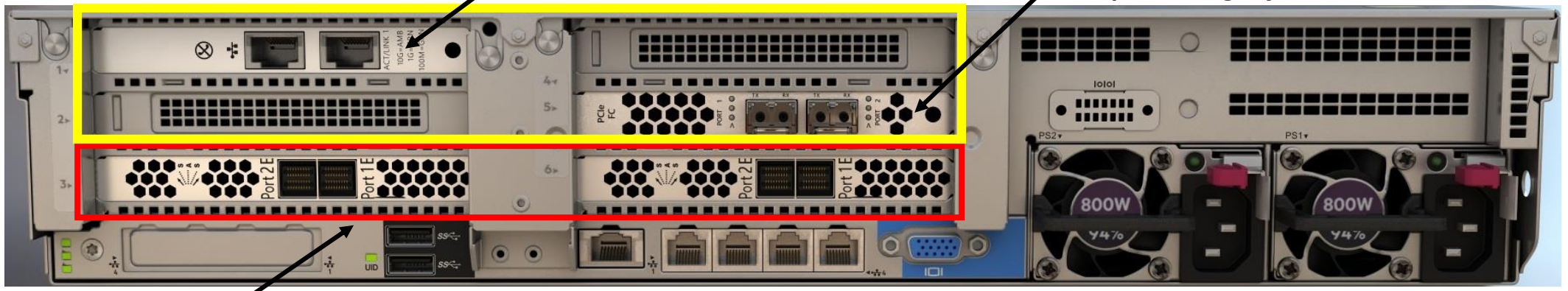
Rear view



Dual I/O modules (12 Gb/s SAS)

Next-generation StoreOnce 5250 and 5650

Rear view

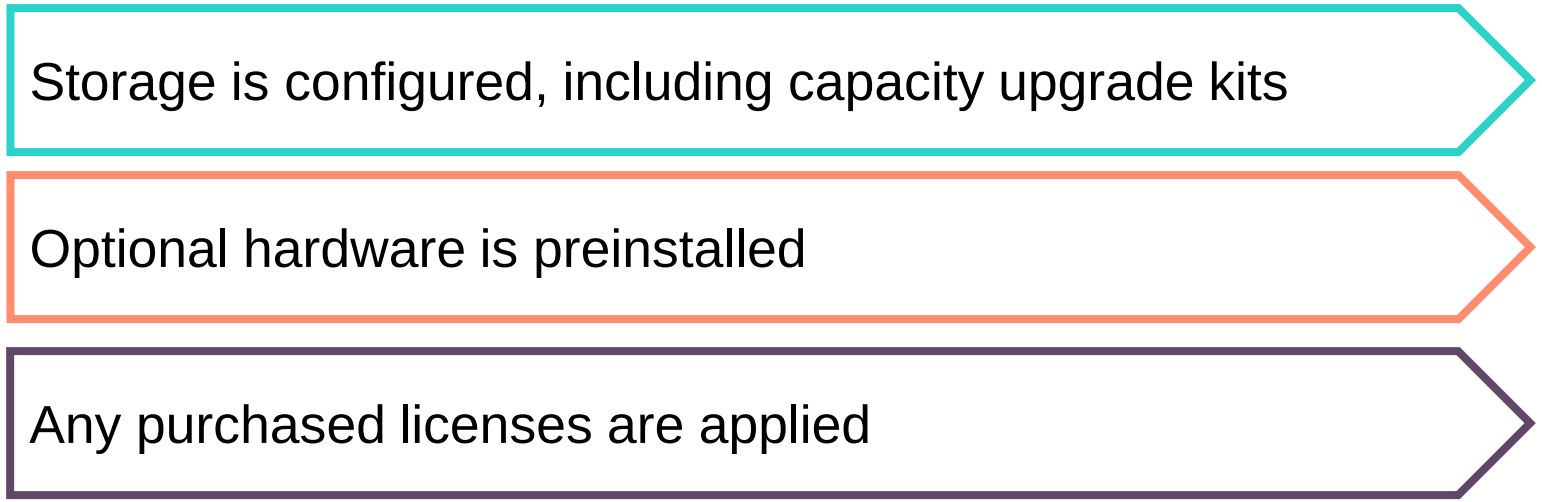


- Install network HBAs in slots 1, 2, 4, and 5 in that order with BB982A (10/25GbE) in slots numbered lower than BB984A (10GBaseT)
- Install Fibre Channel HBAs in slots 5, 4, 2, and 1 in that order with BB986A (16 Gb FC) in slots numbered lower than BB990A (32 GB FC)

What arrives from the factory?

– HPE StoreOnce products provide customers the flexibility to factory-configure their entire order

– From the factory:

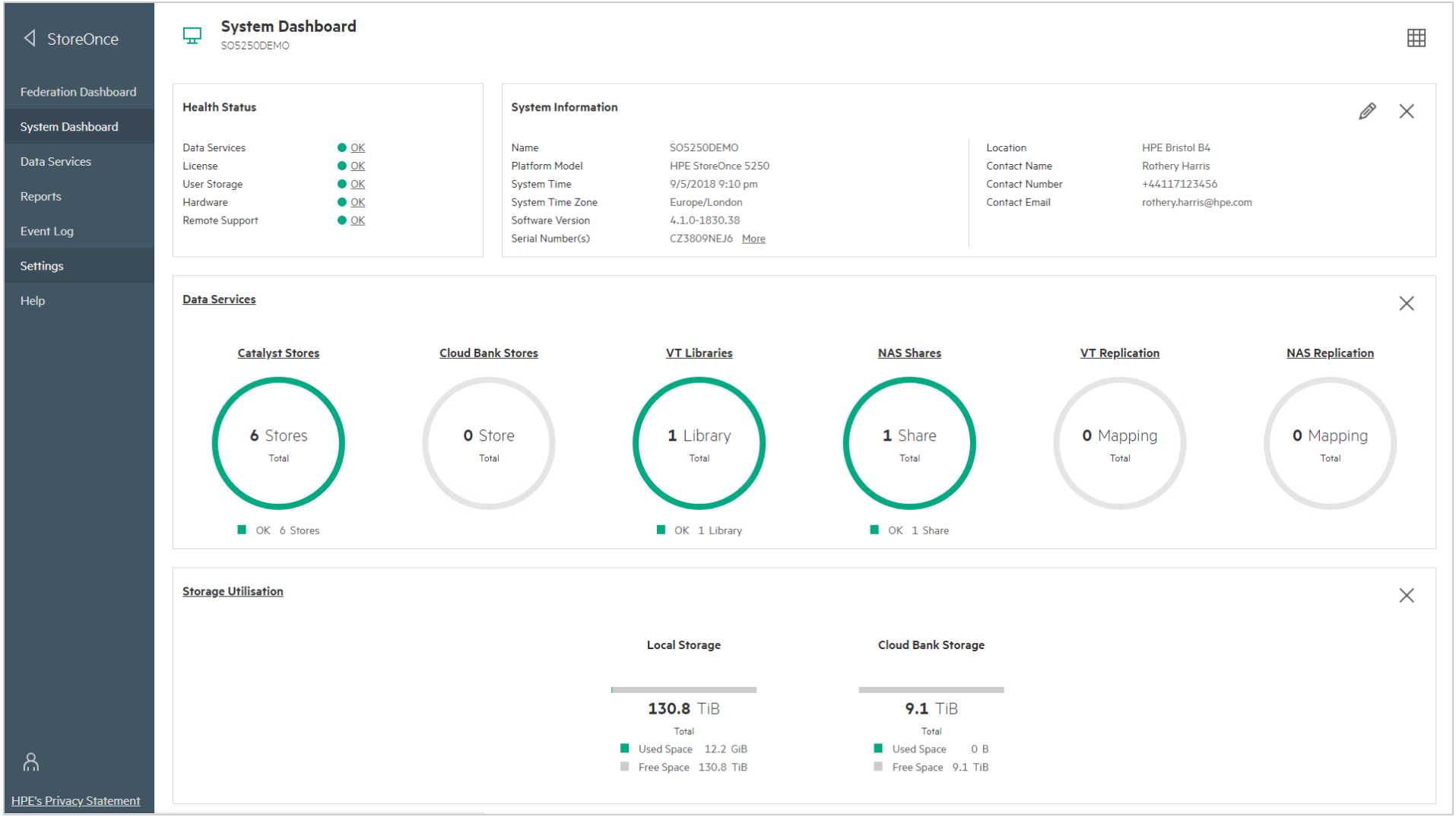


Management

Working with the StoreOnce GUI

Hewlett Packard
Enterprise

StoreOnce GUI dashboard

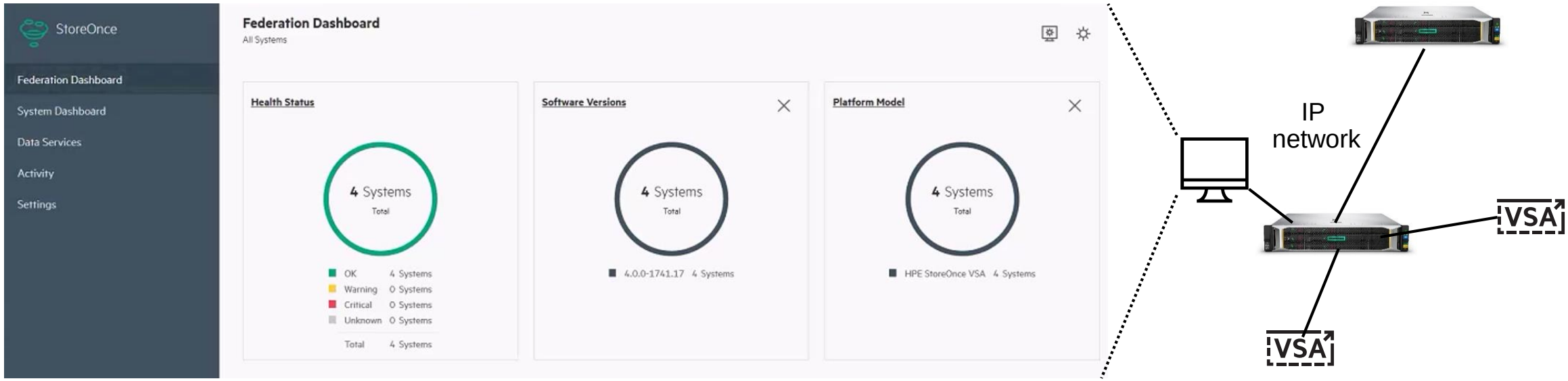


Management federation

- Management federation allows you to manage multiple StoreOnce systems from a single appliance
- The managing system in a federation is called the *lead system* and the other systems in the federation are called *member systems*
- When logged in to a lead system, you can manage not only that system but also any of the member systems in the federation
  - For example, from the lead system you can create StoreOnce Catalyst stores on any member systems in the federation
- The Federation Dashboard screen on a lead system displays aggregated information
- When logged in to a member system, you can manage the system as usual
  - However, you cannot manage other systems in the federation from a member system
- The Federation Dashboard on a member system indicates that the system is part of federation
- Multiple federations can be configured where StoreOnce systems can be leads, members, or both within overlapping federation domains

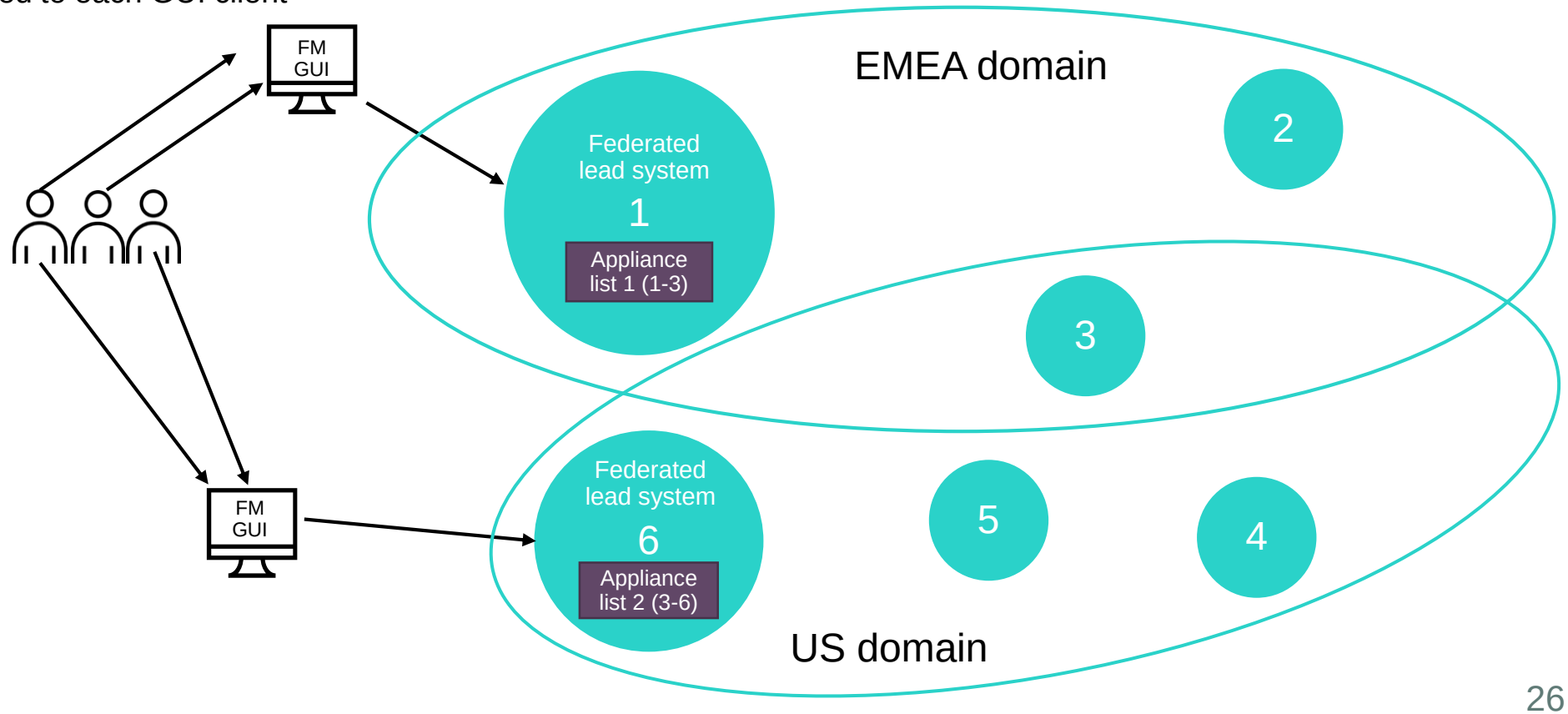
Federated management

– Single view for management and reporting for up to 20 systems (up to 100 by request)
  – VSA and physical systems
  – Federation domains within federation domains or overlapping federation domains
– Concept is a lead system and connected systems
  – Any system can be the lead system
  – Data pushed from connected systems to lead system where it is aggregated



Simple federation: Multiple managed federations can overlap

– Multiple federations can be configured where StoreOnce systems can be leads, members, or both within overlapping federation domains
  – Systems can be managed by two domains if required
  – In this case, system 3 is providing information to lead system 1 and lead system 6
  – Users can be assigned to each GUI client



Role-based access control

Role	Description
Administrator	Read-write permissions across the whole UI
Observer	Read-only permissions across the whole UI
Security Officer	Read-write permissions for security-related items such as user management, key manager management, and log offloads as well as read-only permissions across the UI
Backup Admin	Read-write permissions for all Data Services sections of the UI as well as read-only permissions for certain sections of the UI such as reporting and event logs
Backup Operator	Read-only permissions for all Data Services sections of the UI as well as read-only permissions for the same sections of the UI as the Backup Admin
Support	Read-write permissions across the whole UI with additional support-only access for troubleshooting and debugging such as file system repairs

- A freshly installed system has a single preconfigured user with the administrator role (username Admin)
- Customers can create new users:
  - Locally on box
  - Externally using Active Directory and LDAP
- Assign users one of the first five roles listed in the table
- The support role is hidden from UI users and new user accounts cannot be assigned this role
  - The support role is only used for HPE support engineers

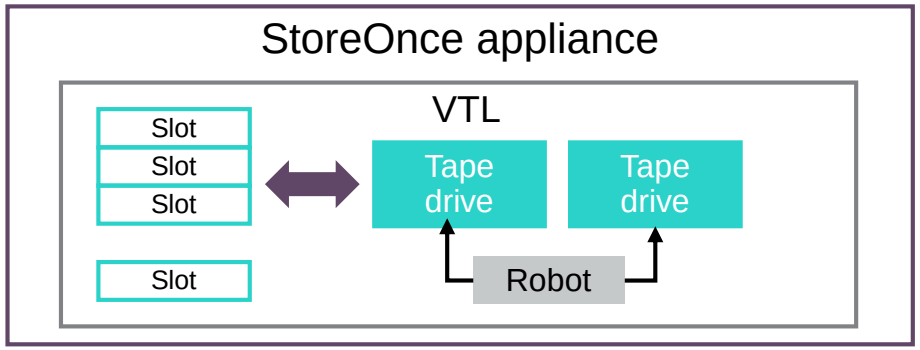
Networking and connectivity

Connectivity: VTL and NAS

StoreOnce has three connectivity types used with leading backup applications; each type can coexist on the same appliance

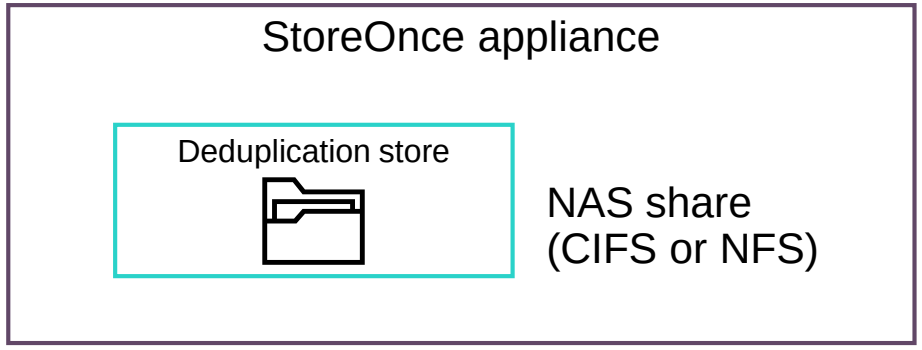
Virtual tape library

- A virtual tape library emulates traditional physical tape and library characteristics
- Tape library targets contain:
  - User capacity specified tapes
  - One or more tape drives
  - Numerous slots to hold tapes
  - Barcode reader to identify tapes
  - Automation for loading and unloading tapes (a robot)
- Customers commonly use VTL based on compliance requirements
- VTLs can connect using iSCSI or Fibre Channel (SAN)



Network attached storage (NFS/CIFS) for backup

- NAS shares:
  - Are created to be used in specific environments that do not support tape emulation backup or when backing up directly to disk is preferred
  - Can be easily configured and viewed by the operating system
  - Can be integrated with Active Directory
  - Use CIFS for Windows and NFS for UNIX/Linux
- **Important:** StoreOnce network share should **only** be used by backup applications that back up to disk
  - Do not use the NAS target device as a drag-and-drop general file store
  - One exception is when using the NAS share to seed an appliance for replication



HPE StoreOnce Catalyst

What is Catalyst?

Catalyst:

– Is a backup protocol developed by HPE

– Is enhanced for disk-based backup data protection

– Makes it simple to create and manage stores

– Provides greater performance by shifting some of the deduplication process to the client

– Allows for flexibility by offering local storage and cloud storage through HPE Cloud Bank Storage in combination with HPE StoreOnce

– Offers additional protection against ransomware and malware with its unique API and encryption

HPE StoreOnce Catalyst benefits

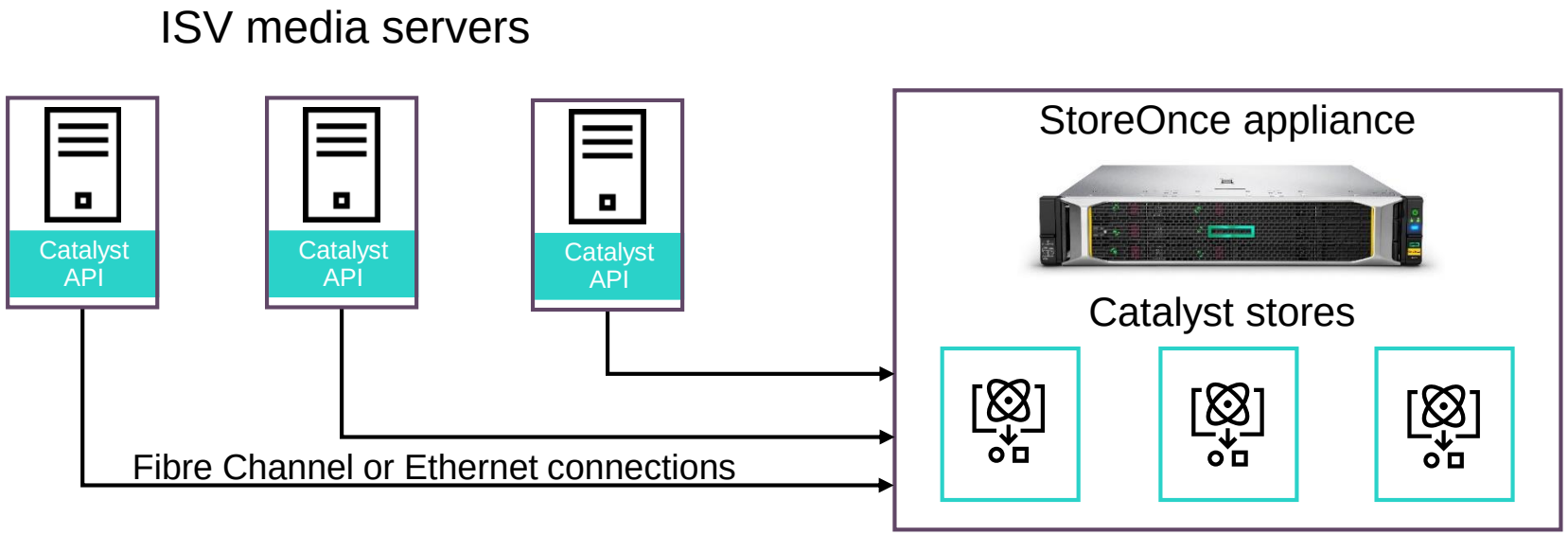
- HPE StoreOnce Catalyst is a storage target and protocol for data protection when using HPE StoreOnce systems
- HPE StoreOnce Catalyst operates a ‘client-server’ model to enable applications (typically ISV data protection software) on host servers to have a much richer interaction
  - Traditional Virtual Tape and NAS stores are limited by their commands and protocols
- As part of StoreOnce Catalyst, some of the deduplication process can be offloaded to the ‘client’
  - This enables what is known as *low-bandwidth* transfers because only new data is transmitted to the StoreOnce appliance
- Catalyst can be extended to duplicate backups on other StoreOnce appliances moving data offsite but still making efficient use of bandwidth
- Catalyst technology has enabled HPE to deduplicate data in the public or private cloud
  - This technology is known as HPE Cloud Bank

Connectivity: HPE StoreOnce Catalyst

A data protection interface unique to StoreOnce systems

Benefits

– Unrestricted feature enabled by default
– Higher performance through client-side deduplication
– Quicker restores
– Simplified management of data movement
– Flexible control compared to traditional emulated tape (VTL) targets or NAS shares
– Can be either Fibre Channel or Ethernet connections

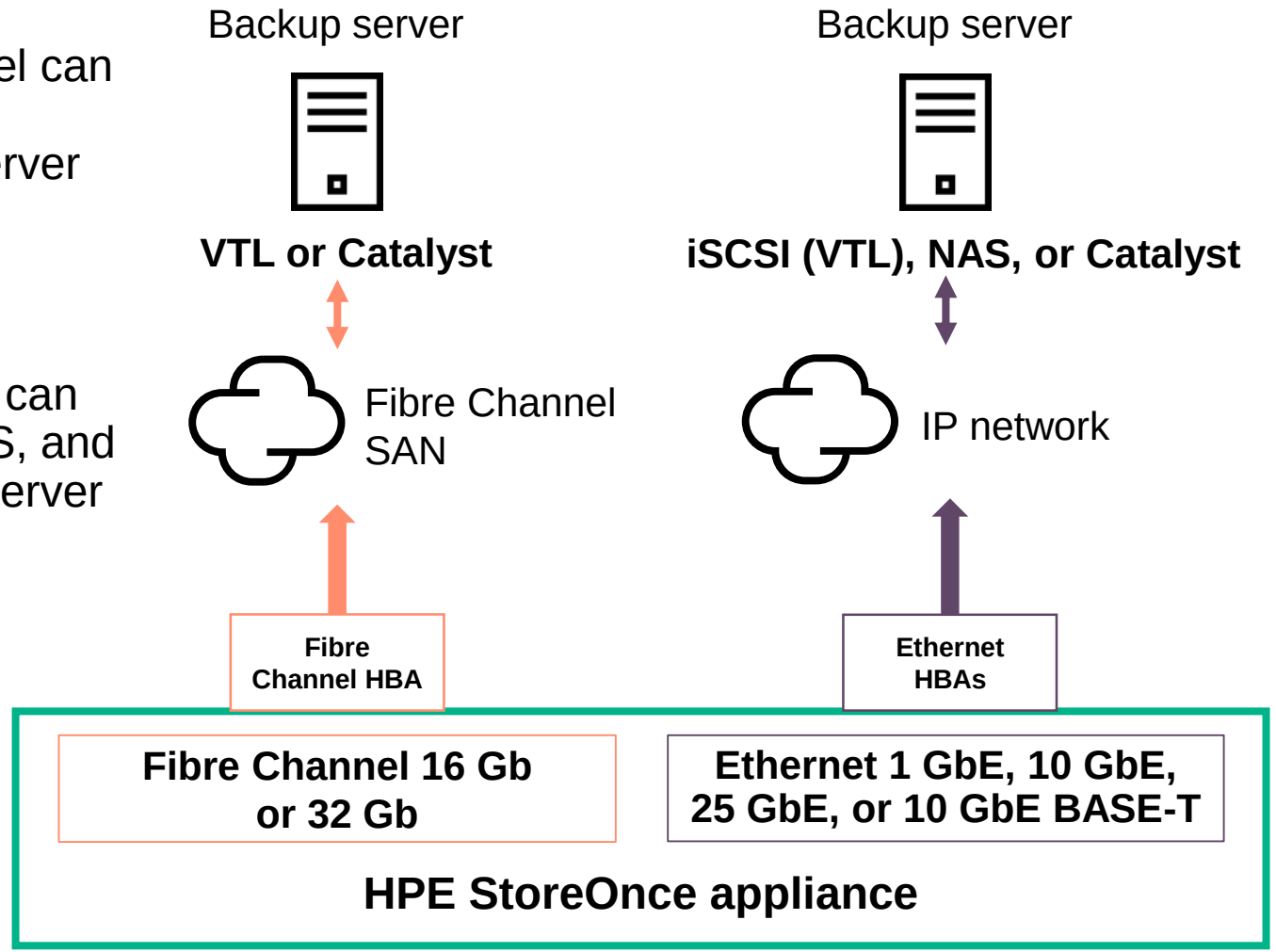


– Client-side deduplication is performed on the backup server using Catalyst API before it is sent to StoreOnce
– This saves network bandwidth while reducing backup windows

Hewlett Packard Enterprise

Networking and connectivity

- 16 Gb or 32 Gb Fibre Channel can be used to connect a VTL or Catalyst store to a backup server
- 1 GbE, 10 GbE, and 25 GbE can be used to connect VTL, NAS, and Catalyst stores to a backup server



Security

Key management

Using local and external key managers

- StoreOnce supports local and external key management
  - Migrating from the local key manager to an external key manager is supported
    - The encryption keys are migrated from the local key manager to the external key manager and data is not lost
    - When the keys are migrated, they are no longer persisted on the StoreOnce appliance
  - Migrating from the external key manager to the local key manager results in data loss, because the keys are not migrated back to the appliance
- The key manager runs as a service on the system and includes its own key store
  - When in Local Key Manager mode, the key store contains the keys that are used by the various subsystems (VTL, NAS, Catalyst, and so forth)
  - When in External Key Manager mode, the key store contains the certificates and credentials of the external key manager that are used to establish the connection
- The connection to the external key manager is protected by HTTPS
- A license is not required to use either the local or external key manager
  - However, without a license, data-at-rest encryption or data-in-flight encryption cannot be used

Data-at-rest encryption

Securing data that is written to disk

- Software-based encryption
- Licensed software feature
  - Stand-alone license SKUs for all platforms:
    - BB994A (HPE StoreOnce Encryption LTU)
    - BB994AAE (HPE StoreOnce Encryption E-LTU)
  - Enterprise server license SKUs:
    - BC007A (HPE StoreOnce VSA Svr Encrypt LTU)
    - BC007AAE (HPE StoreOnce VSA Svr Encrypt E-LTU)
- Encryption for VTL, NAS, and StoreOnce Catalyst stores
  - Encryption domain is VTL, NAS share, or StoreOnce Catalyst store
  - Encryption must be enabled when creating the VTL, NAS share, or StoreOnce Catalyst store
    - It cannot be enabled after creation of the device
- Protecting data at rest helps ensure it cannot be accessed on stolen, discarded, or replaced disks
  - It is not intended to protect a running appliance from being hacked
- Same solution across StoreOnce portfolio—hardware platforms and VSA

How data-at-rest encryption works

- Encryption algorithm meets the AES-256 standards
- Data is encrypted postdeduplication
  - Encryption has no impact on deduplication ratio
- Data is unencrypted as it is read from disk for restore, replication, or copy jobs
- A single key per appliance is obtained from the key manager
  - This key is used as a key wrapping key (KEK) for the data encryption key (DEK)
  - The DEK is persisted on disk after it has been wrapped by the KEK
  - The KEK is only persisted in the key manager store
    - If the system is configured to use an external key manager, then the KEK is not persisted within the appliance

Data-in-flight encryption

Securing data while it is in transit

- Encryption of data-in-flight between two StoreOnce appliances using IPsec
- Licensed software feature
  - Stand-alone license SKUs for all platforms
    - BB994A (HPE StoreOnce Encryption LTU)
    - BB994AAE (HPE StoreOnce Encryption E-LTU)
  - Enterprise server license SKUs
    - BC007A (HPE StoreOnce VSA Svr Encrypt LTU)
    - BC007AAE (HPE StoreOnce VSA Svr Encrypt E-LTU)
- Supported for low-bandwidth replication and low-bandwidth copy jobs
  - Not recommended for backup up jobs because of performance
- The Data Services section has no visibility of data-in-flight encryption
- A standard open-source IPsec package is used
- Support for preshared keys only
- Same solution across StoreOnce portfolio—hardware and VSA
- Not applicable to Fibre Channel traffic
- No hardware accelerators are used
- Does not support certificate-based authentication

Secure Erase

Secure deletion of data

- Protects against recovery of deleted data by allowing customers to erase data securely
- Removes user data backed up to a VTL, NAS, or Catalyst store
- Can delete entire VTL, NAS, or Catalyst store
- Cannot be used on the operating system partition
- Works by overwriting the data
  - Allows user to choose to overwrite the data with one, three, five, or seven passes
- Can only be configured when modifying the VTL, NAS, or Catalyst store
- Impacts performance because of increased I/O as a result of the overwrites
  - Is strongly recommended that Secure Erase is not enabled indefinitely

Secure Erase implemented in housekeeping engine

- Secure Erase is implemented in the deduplication housekeeping engine
  - The housekeeping engine securely erases the data by overwriting it using the specified number of passes
- Only housekeeping jobs that have been created after Secure Erase was turned on are securely erased
  - Any housekeeping jobs created before enabling Secure Erase or any previously deleted data are not securely erased
- Only dedupe chunks that are not referenced elsewhere can be securely deleted
  - If another dedupe item exists that requires that chunk, then it will not be erased
- Secure Erase occurs on deleted data
  - HPE recommends triggering deletions through your ISV (for example, by formatting cartridges)

FIPS 140-2 Level 1

StoreOnce and FIPS validation

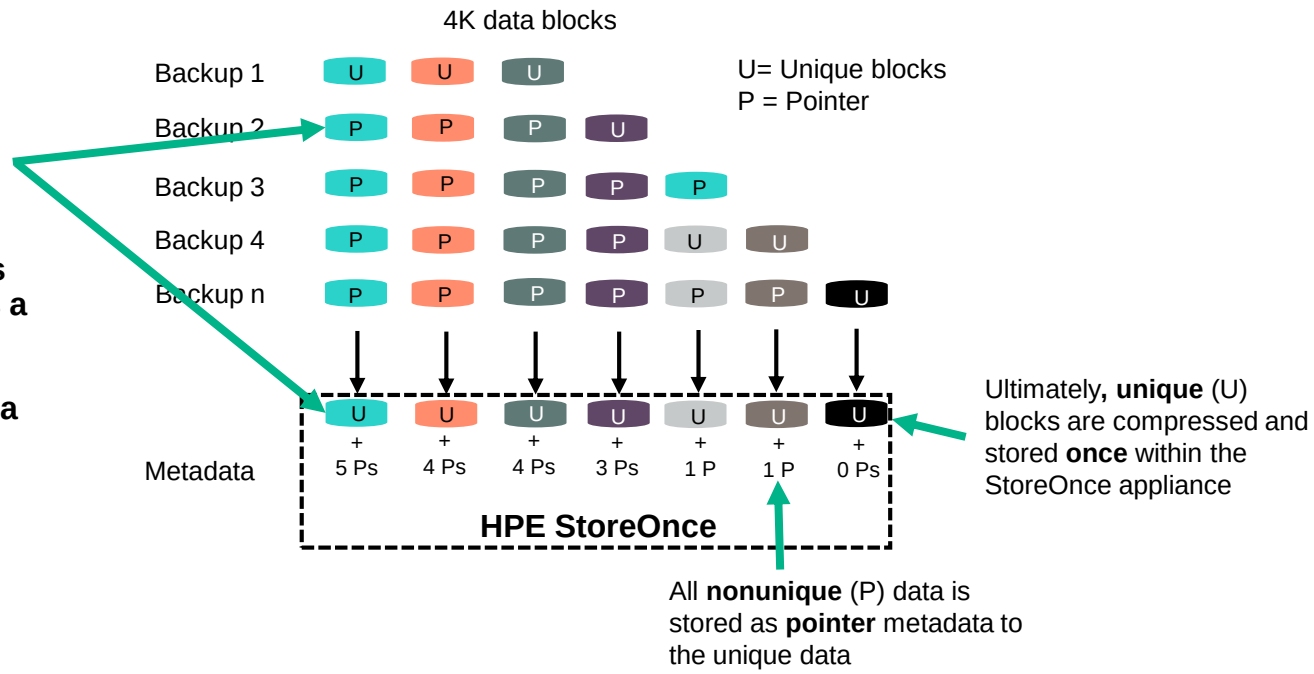
- Federal Information Processing Standard 140-2 (FIPS 140-2) defines the technical requirements to be used by federal agencies when cryptographic-based security is required for protection of sensitive or valuable data
- HPE StoreOnce 4.1.0 or later uses cryptographic algorithms and modules that have completed a FIPS 140-2 (Cryptographic Algorithm Validation Program / Cryptographic Module Validation Program [CAVP/CMVP]) validation
  - These validated modules are active when the product is configured in FIPS mode
- HPE StoreOnce meets FIPS 140-2 level 1 requirements by:
  - Integrating NIST validated cryptographic modules so that critical cryptography uses the modules to provide cryptographic services
  - Using approved entropy sources
  - Using FIPS-validated cryptographic ciphers and functions
- Certificate: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3018

Key technology benefits

Deduplication

- Deduplication removes duplicate copies of repeating data, improving storage capacity while providing longer retention periods before moving data off to archive
- The deduplication process can be explained in simple terms
- Deduplicated data is rebuilt whenever there is a read request
- Depending on the data type, deduplication ratios can vary, but the process works the same:
  - SQL Server: ~10:1
  - Oracle: ~12:1
  - Virtual machines: ~35:1
  - Images: ~1:1
  - Flat files: ~20:1

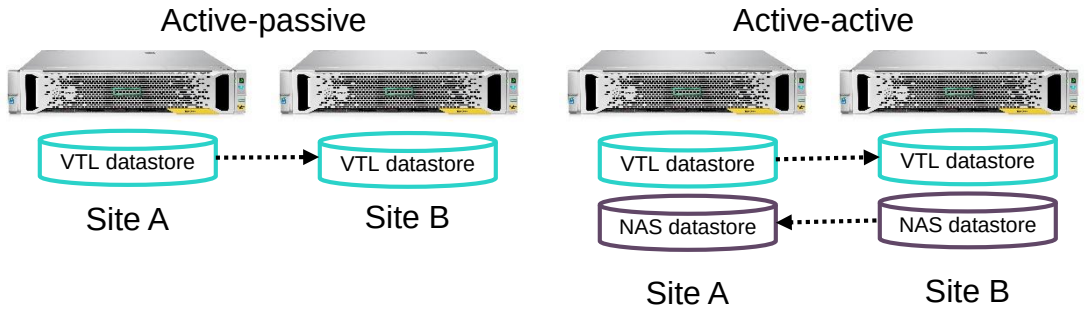
1. **Backups are run and unique data is stored**
2. **As backup data arrives, it is compared against previously stored data blocks**
3. **If duplicate data is found, it becomes a pointer to the original data and stored as metadata**
4. **The process continues, improving dedupe ratios over time**



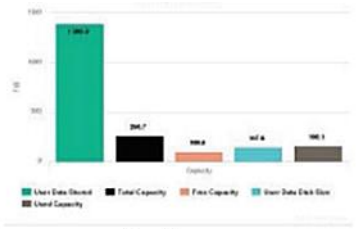
Replication and Catalyst Copy

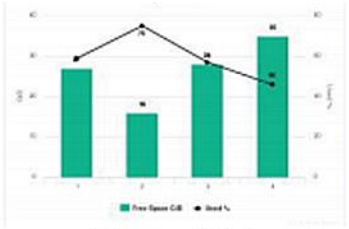
- **Replication** is the process of encoding information so that only authorized parties who possess the proper decryption key can access it
- StoreOnce supports two methods to help secure data:
  - Data-at-rest encryption prevents unauthorized access to data stored on disk that was lost, stolen, or discarded and data being transmitted between devices; it also offers Secure Erase functionality that completely sanitizes data by overwriting all data on disks using random binary ones and zeros
  - Data-in-flight encryption is used to secure links and data that are sent between data centers when using StoreOnce replication; in-flight encryption is only supported with Catalyst

- **Catalyst Copy** is a term used to describe a way of synchronizing data between hardware in two physical locations
- It is the process of creating an exact match on the target appliance of the specified data from the source appliance
  - Catalyst Copy can be directly controlled by StoreOnce or by backup software that supports Catalyst
  - Catalyst Copy can be performed over 1/10/25 GbE networks or Fibre Channel with Catalyst
  - NAS, VTL are replicated (controlled by StoreOnce)
  - Catalyst stores can all be Catalyst Copy
  - There are many Catalyst Copy use cases: active to passive, active to active, many to one, and N-way copy (many to many)

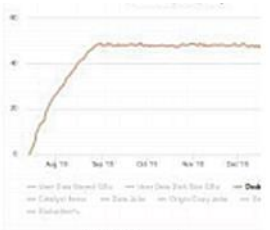


Remote support with Service Tools and Technical Support


Capacity usage


File systems distribution


Dedupe ratio (percentage)


Catalyst performance

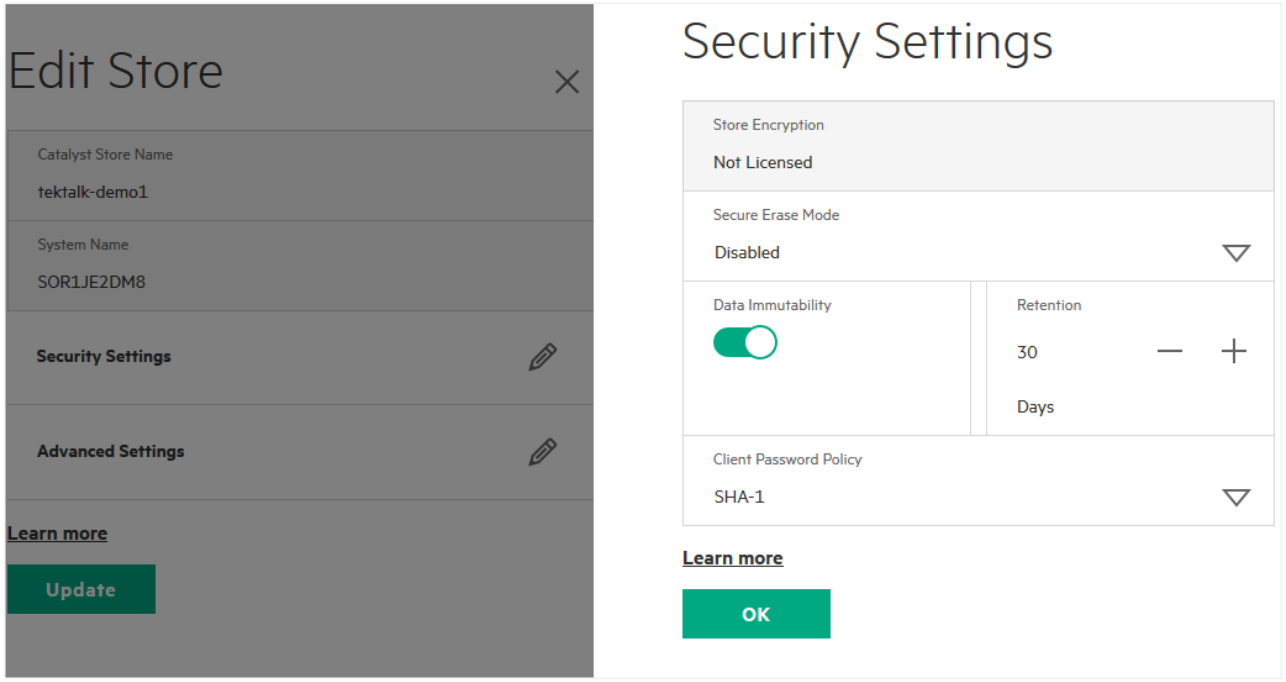
- StoreOnce remote support uses STaTS to monitor StoreOnce systems; the appliance proactively contacts HPE if issues occur
- Site-specific data is used both proactively and reactively with real-time monitoring and information extraction tools
- Connecting to StoreOnce remote support offers enhanced security
  - Remote connectivity leverages the industry-standard HTTP protocol over Secure Sockets Layer to facilitate external communications with HPE StoreOnce remote support
  - All transmissions are encrypted
- What is required for StoreOnce remote support?
  - Customers must register their StoreOnce system in STaTS
  - StoreOnce 3.11.X or later firmware is required
- What are the customer benefits of remote connectivity?
  - Proactive fault detection alerts customers of potential issues
  - Time to resolution is faster
  - Historical data collection improves operational efficiency

Catalyst data immutability

– Catalyst stores can be configured with a data immutability period

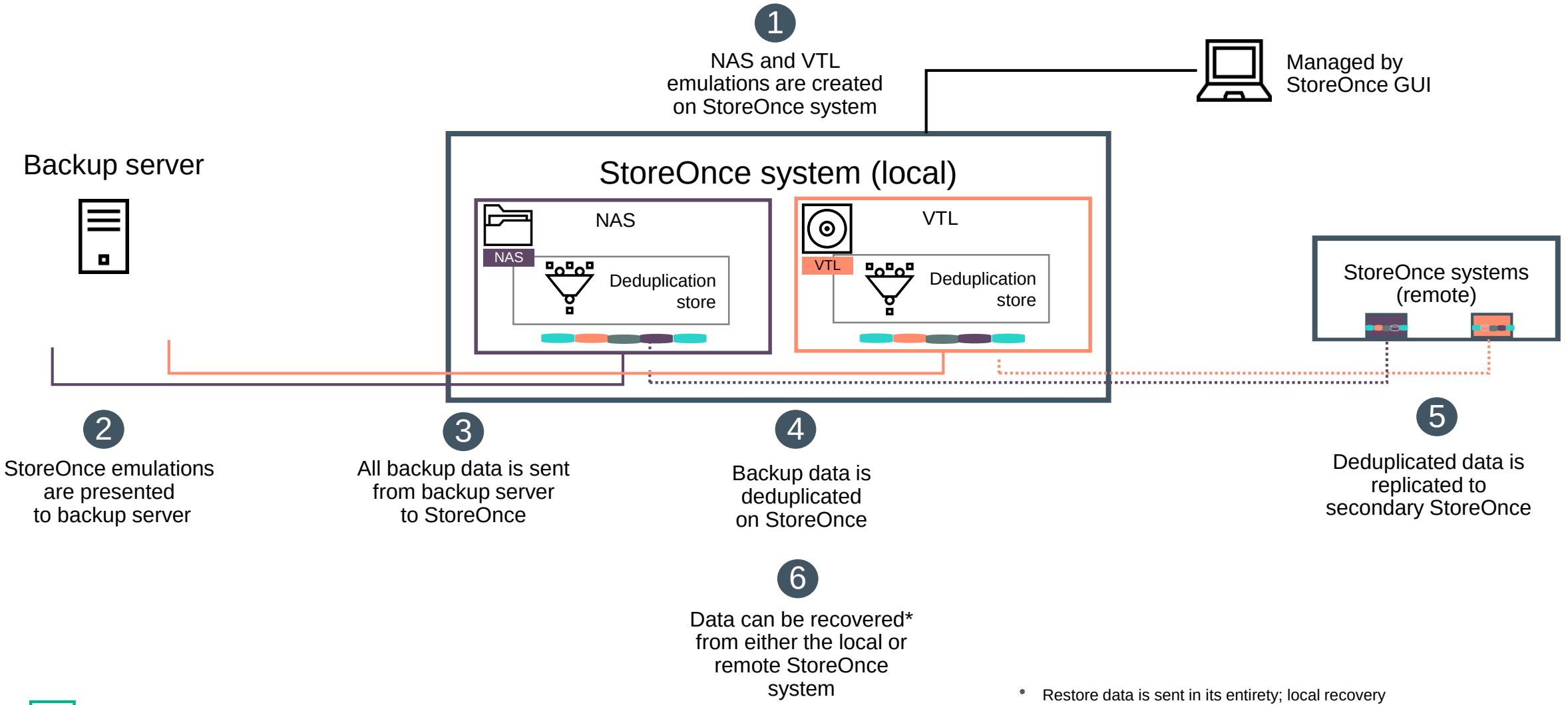
– During the specified period, the backup applications accessing the store cannot delete backups that have been retained for less than this specified period

– This provides additional protection against malicious or unintended backup data deletion when different people are serving as backup application administrator and StoreOnce system administrator



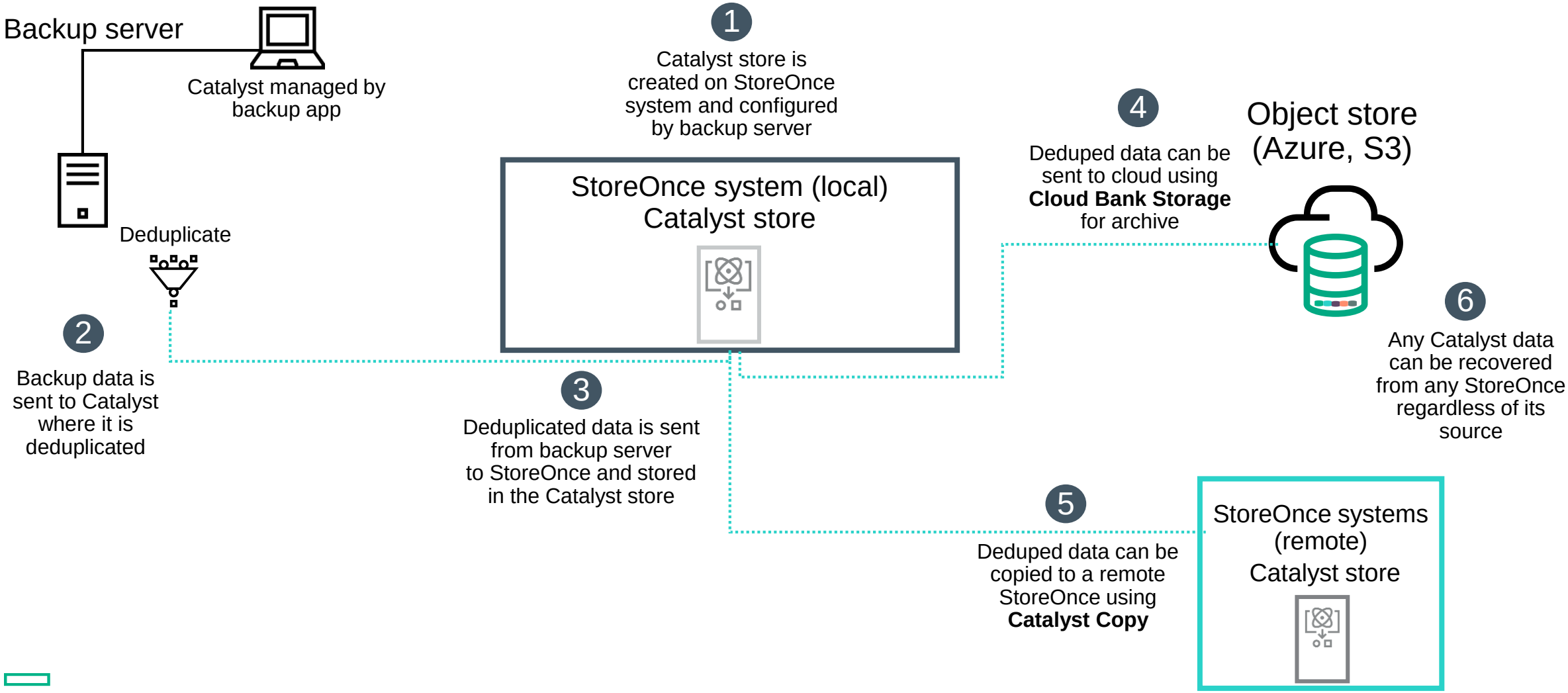
Use cases

NAS and VTL deduplication and replication



* Restore data is sent in its entirety; local recovery is always faster than remote unless using Catalyst

Catalyst, Catalyst Copy, and Cloud Bank Storage



Important HPE StoreOnce details

Partners

- Interface supported:
  - NAS
  - Catalyst

- Interface supported:
  - NAS
  - VTL
  - Catalyst

- Interface supported:
  - NAS
  - VTL
  - Catalyst

- Interface supported:
  - NAS
  - VTL
  - Catalyst

- Interface supported:
  - NAS
  - VTL
  - Catalyst

- Interface supported:
  - Catalyst

For all supported backup applications, reference the StoreOnce Support Matrix

Data considerations and best practices

- StoreOnce is a backup appliance tuned to reduce the storage footprint of backups
- But not all data (or backups) are created equal and considerations must be made when evaluating customer backups
- These considerations include:
  - **Identify the backup and data types:** Understanding the backup data and data types within the backup is critical, and not all data deduplicates the same; this is important to know when sizing the product—there are tools available to help analyze customer data
  - **Deduplication ratios increase over time:** As more data is stored and retained for long periods, deduplication ratios increase; most deduplication ratios maximize when data is stored for longer than three months
  - **Recovery can be tricky:** If recovery times need to meet service level agreements, recovery methods must be clearly understood; recovery times depend on the interface used:
    - Data recovered using VTL or NAS is reassembled on the StoreOnce and sent in its entirety across the network
      - Recovery can take a lot of time and consume network bandwidth
    - Data recovered using Catalyst is reassembled at the backup server, decreasing both recovery time and using less network bandwidth, but this can put more I/O stress on the Catalyst server
  - **Apply the 3-2-1 rule for data protection:** StoreOnce meets all the 3-2-1 data protection requirements
    - Three copies of data, two copies on two different types of media (or location) and one copy off-site

HPE Storage Assessment Foundry tools

Backup assessment tools have been developed to help evaluate a customer's environment and are part of the Storage Assessment Foundry:

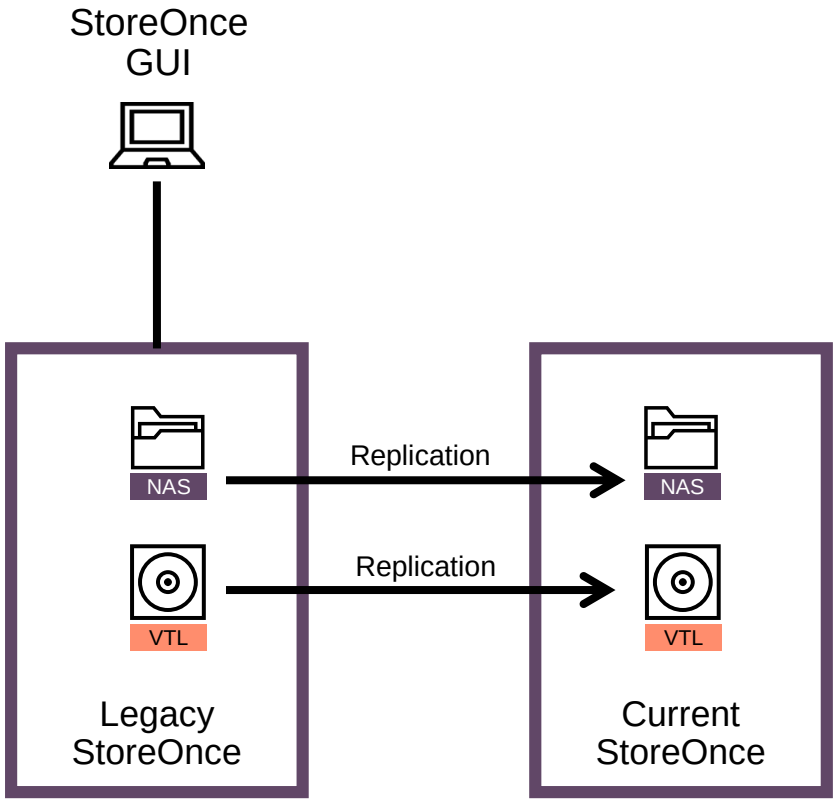
- **HPE NinjaProtected+** is a data protection analysis tool for users of the most popular backup and recovery software applications
  - It is run nondisruptively in customers' environments to capture key metadata (no backup data is accessed) to produce a backup assessment report

- **Data Domain Analyzer** allows the automated creation of EMC Data Domain swap-out configurations, thereby saving countless hours of work when trying to replace an EMC DD array
  - It takes the EMC DD autosupport file and turns it into a comprehensive report, including a StoreOnce solution architecture and price comparison

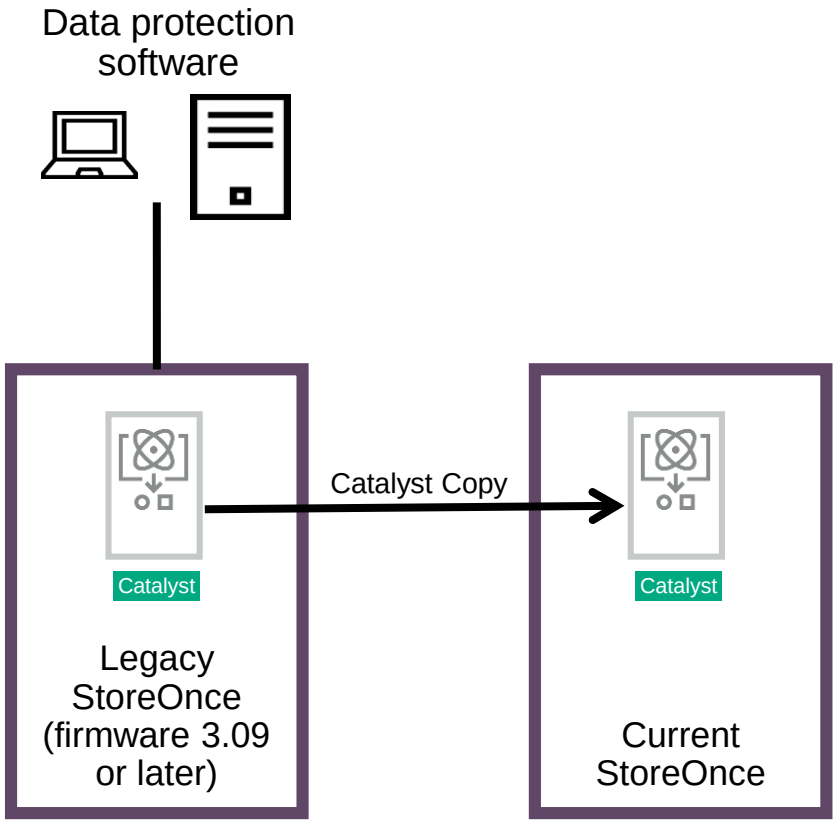
- **HPE Storage Sizer** is a downloadable sizing tool that helps to design a storage infrastructure to help meet customers' needs

Migrating data from legacy to current StoreOnce appliances

Use replication for NAS or VTL



Use Catalyst Copy for Catalyst stores

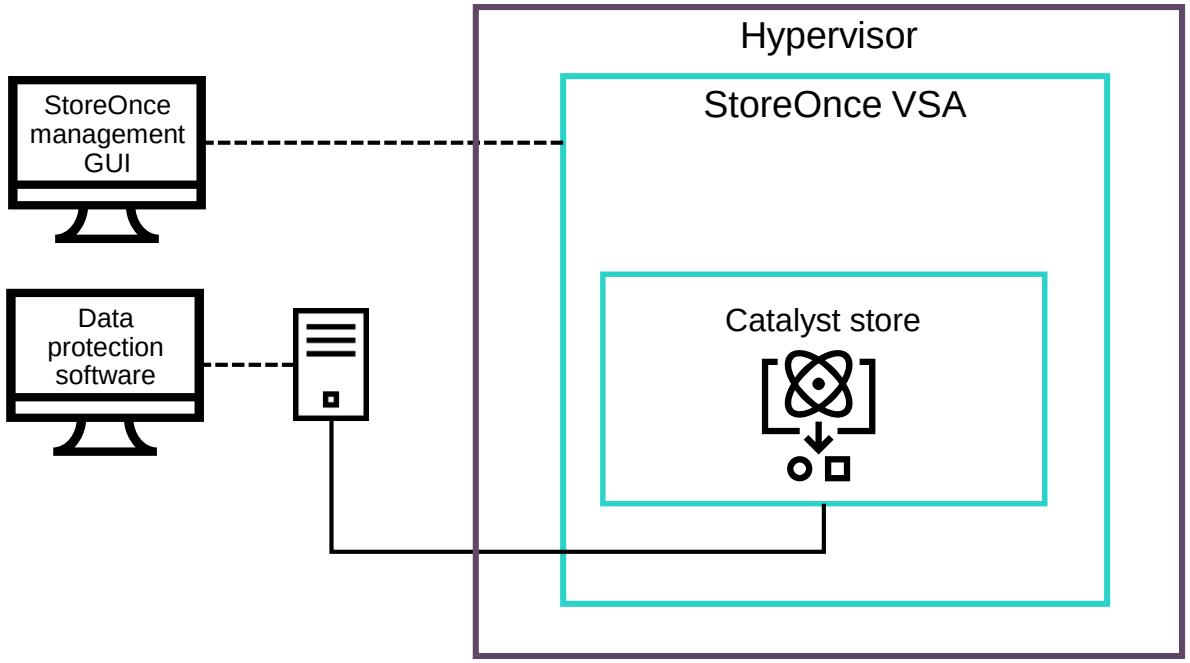


Hewlett Packard Enterprise

HPE StoreOnce Virtual Storage Appliance

VSA architecture overview

- StoreOnce VSA extends the StoreOnce family to enable cost-effective data protection for virtualized environments
- By deploying StoreOnce in a software-defined form factor, customers can increase flexibility and cut storage costs compared to deploying purpose-built appliances
- StoreOnce VSA is a virtual appliance that delivers fast, efficient, and scalable backup in Hybrid IT environments
- A virtual appliance increases deployment flexibility and reduces costs through improved use of storage resources, compute resources, rack space, and power
- VSA capacity licensable up to 500 TB



Features with HPE StoreOnce VSA 4.x

Feature	Description
Capacity	Up to 500 TB per instance
Licensing	– Per instance or through license server – Perpetual, stackable in 1 TB increments
Support	Includes three-year Next Business Day response and HPE Pointnext software update services to extend and upgrade
Resource requirements	Defined to deliver required capacity and performance
Maximum performance	Up to 36 TB/hr for 500 TB product (Catalyst low bandwidth, multistream)
Efficiency	322 GB RAM, 36 vCPU, 10,800 IOPS for maximum performance
Bulk management	Single console reporting and federated management
Freeware and trialware	– 1 TB freeware (perpetual) – 90-day trialware

HPE StoreOnce VSA value

Reduce cost

– No dedicated hardware required
– Use existing resources in remote sites

Cloud ready

– Cloud Bank Storage
– Hosting of VSA in Microsoft Azure Marketplace (up to 32 TB)

Reduce complexity

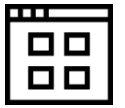
– Centrally managed solution without dedicated infrastructure to install and maintain

Efficiently back up and rapidly recover

– Backup performance of up to 36 TB/hr with StoreOnce VSA

Store and safeguard your data

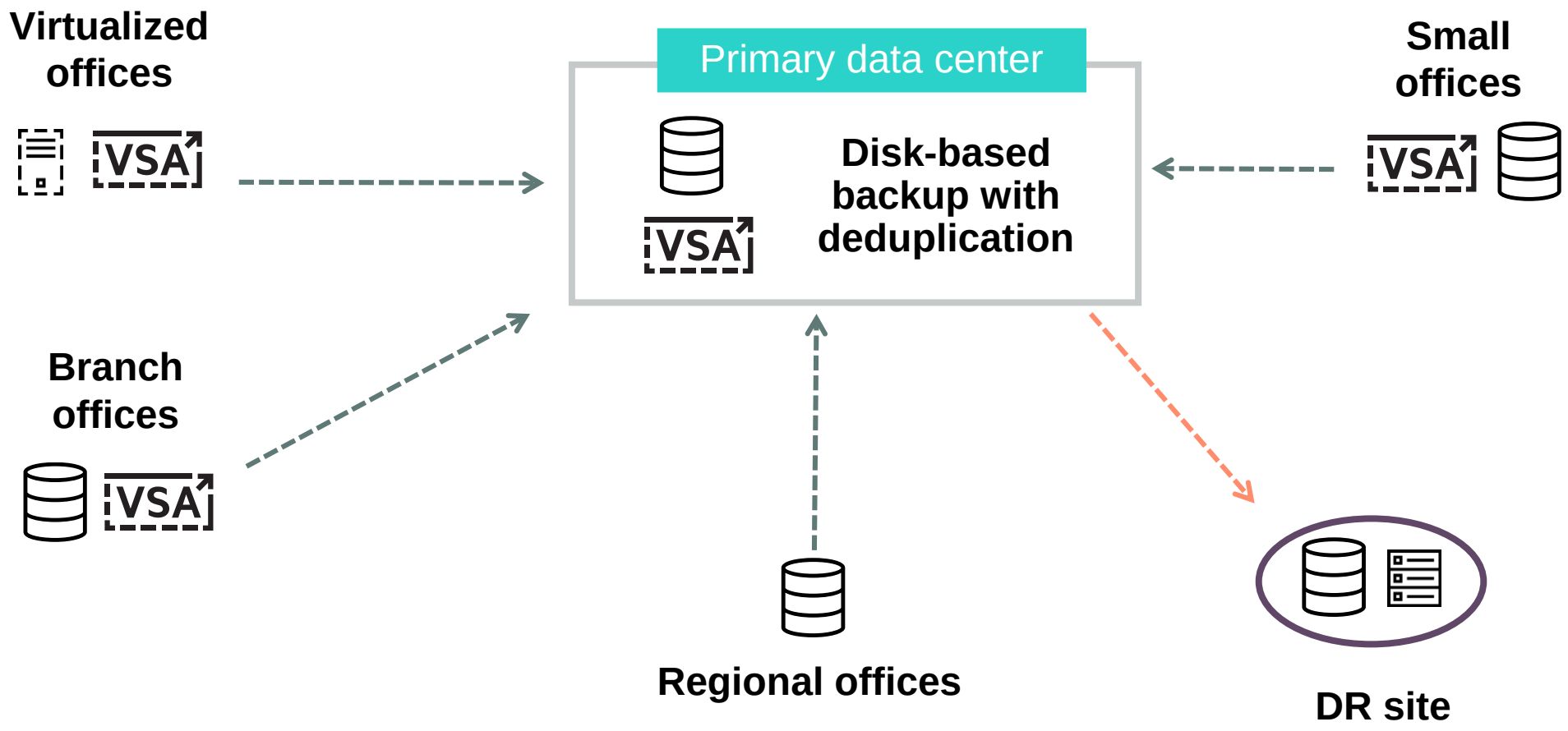
– StoreOnce security pack with data in flight, data at rest, and Secure Erase included at no charge



Broad platform support

– Installed on any x86 server
– Hypervisor support for Hyper-V and VMware

HPE StoreOnce VSA use case



HPE StoreOnce VSA on Microsoft Azure

HPE StoreOnce VSA offers simple, reliable backup with replication in Microsoft Azure cloud

Simplicity and reliability
Easily back up data while reducing unexpected downtimes

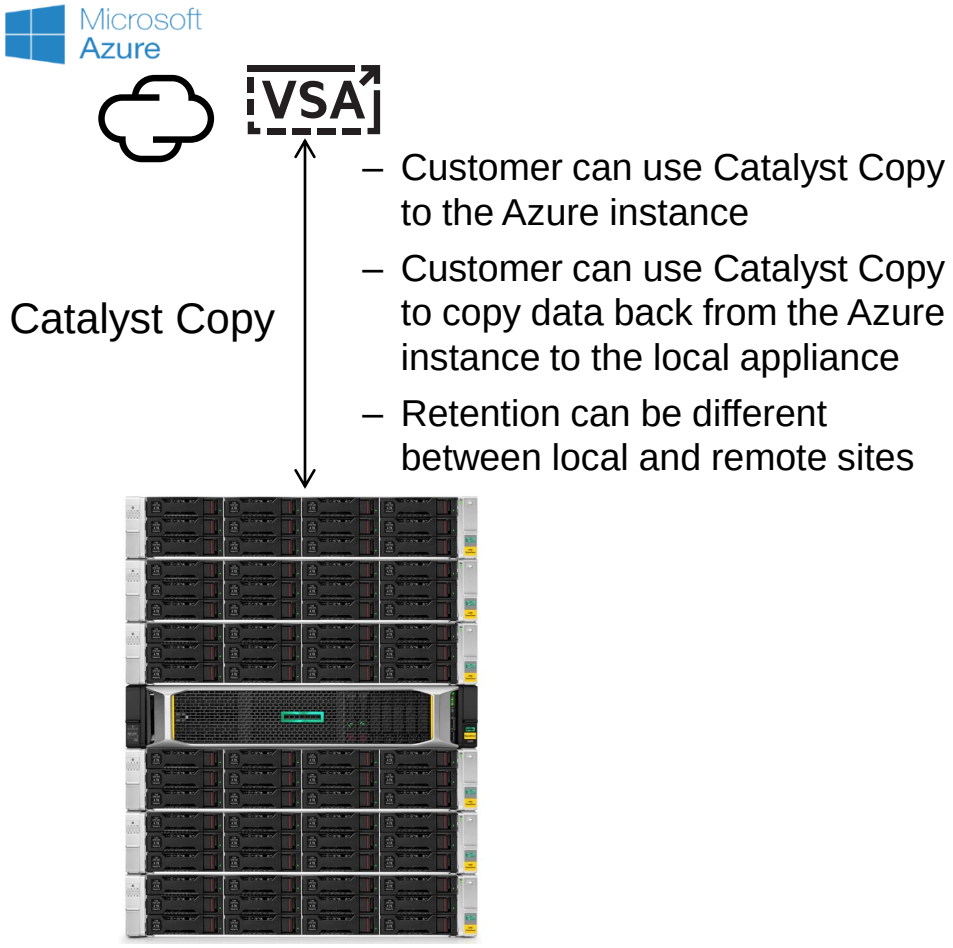
Flexibility
Choose between multiple capacity options to protect data in an Azure cloud

Cost savings
Avoid capital expenses for storage hardware and media, and reduce operational costs

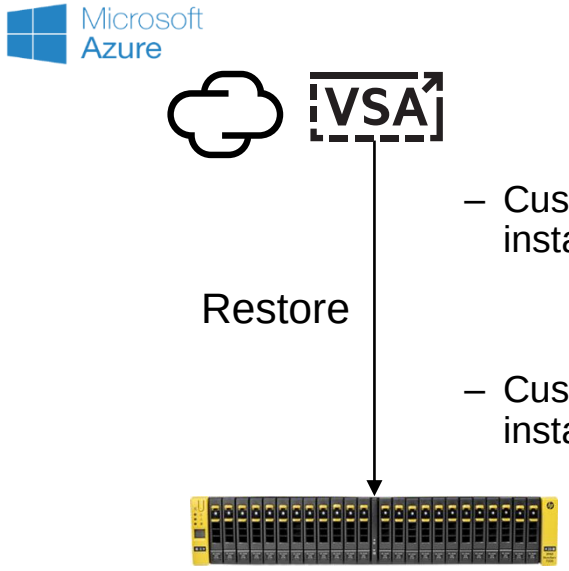
Protection
Restore data and applications with near zero data loss

Bringing the benefits of a hybrid backup solution to ROBOs

Catalyst ISV copies from or to on-site appliance



– Customer can use Catalyst Copy to the Azure instance
– Customer can use Catalyst Copy to copy data back from the Azure instance to the local appliance
– Retention can be different between local and remote sites



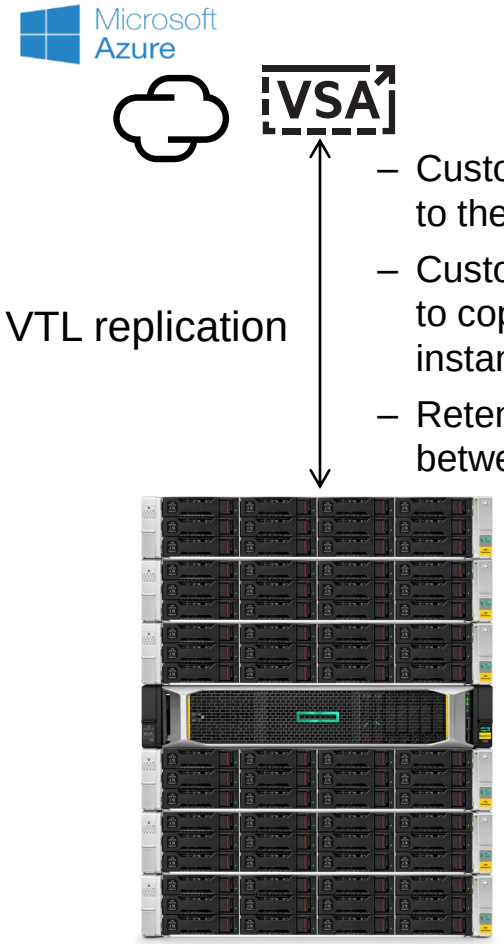
– Customer can restore from the cloud instance to any local primary storage

OR

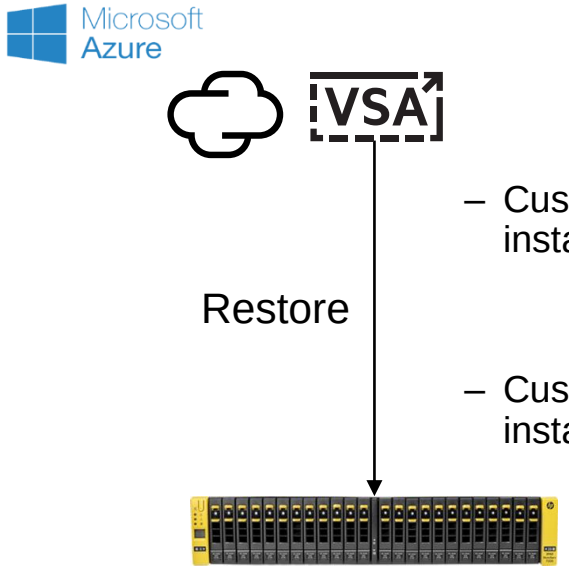
– Customer can restore from the cloud instance to other Azure cloud storage

Note: Supports any Catalyst ISV or application plug-in, along with RMC

VTL replication from or to on-site appliance



- Customer can use VTL replication to the Azure instance
- Customer can use replication to copy data back from the Azure instance to the local appliance
- Retention must be the same between local and remote sites



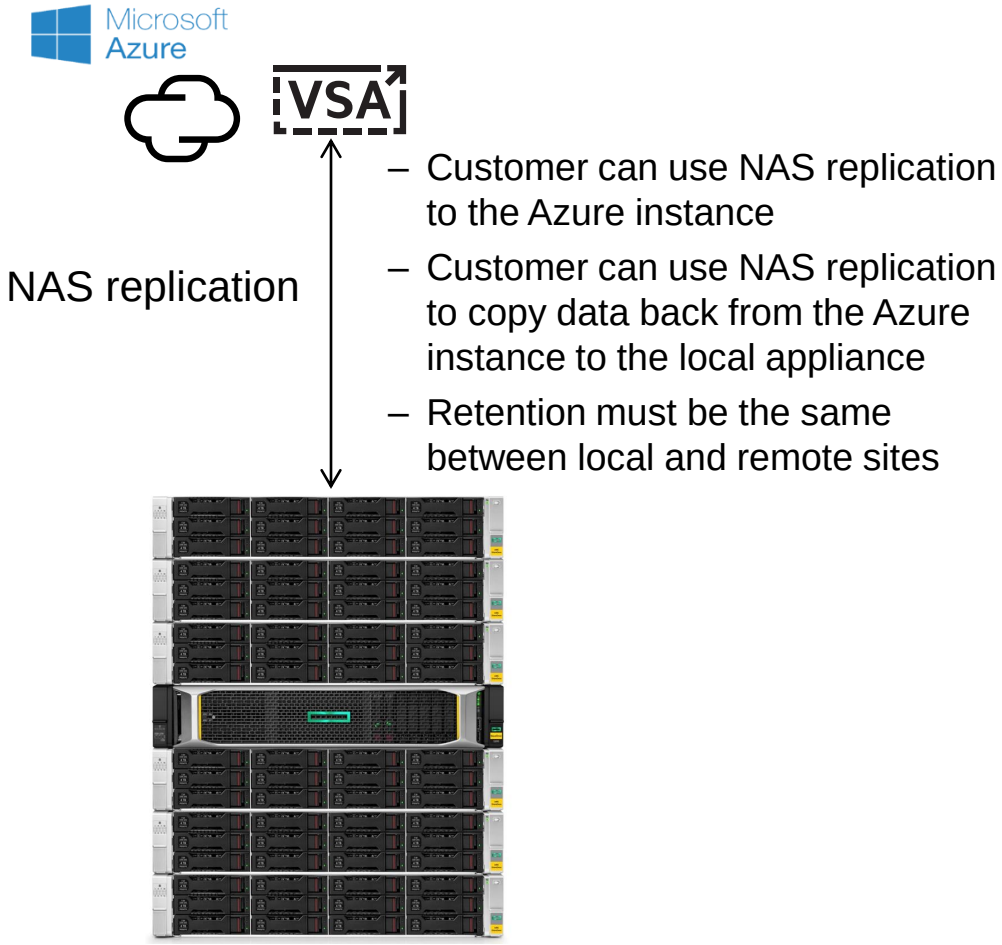
- Customer can restore from the cloud instance to any local primary storage

OR

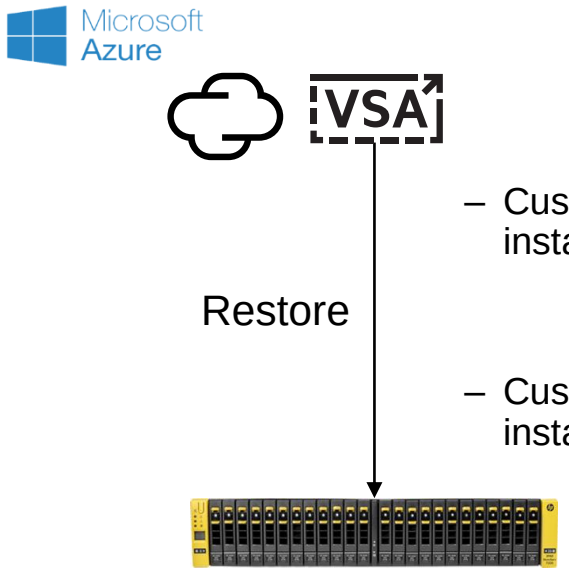
- Customer can restore from the cloud instance to other Azure cloud storage

Note: Supports any Catalyst ISV or application plug-in, along with RMC

NAS replication from or to on-site appliance



- Customer can use NAS replication to the Azure instance
- Customer can use NAS replication to copy data back from the Azure instance to the local appliance
- Retention must be the same between local and remote sites



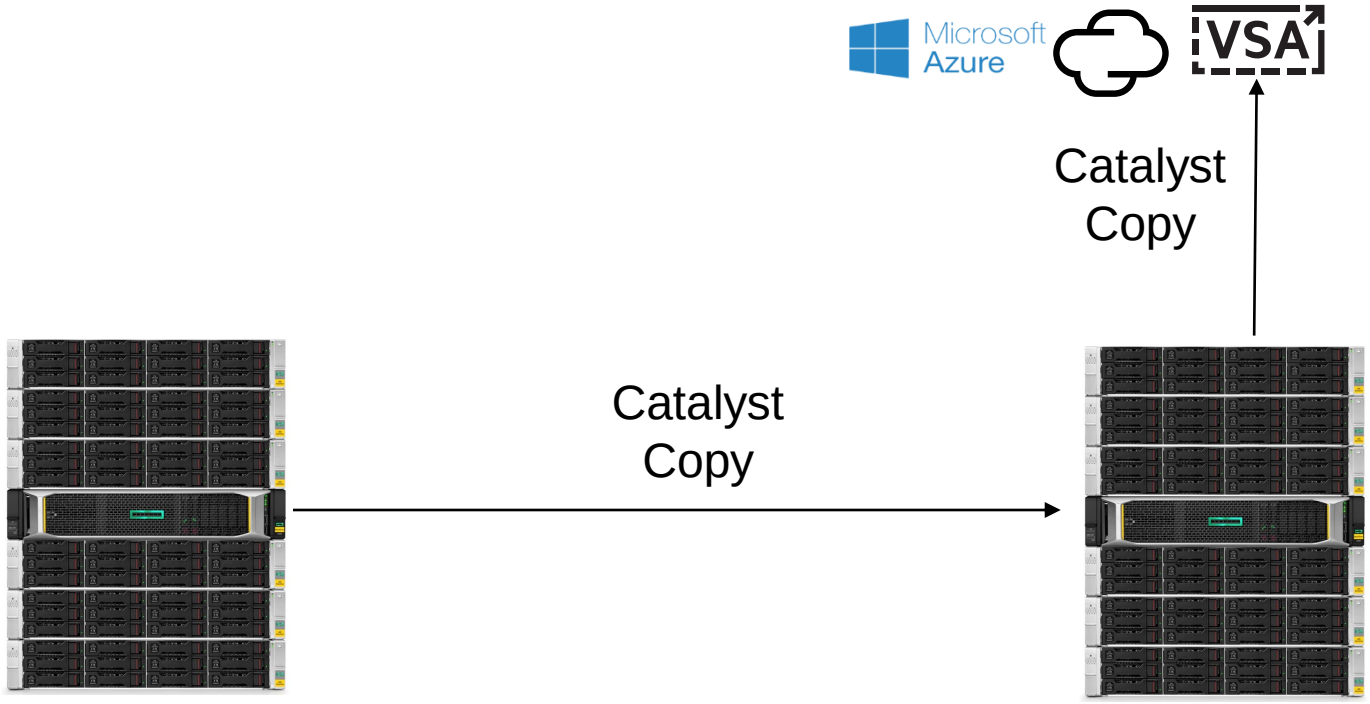
- Customer can restore from the cloud instance to any local primary storage

OR

- Customer can restore from the cloud instance to other Azure cloud storage

Note: Supports any Catalyst ISV or application plug-in, along with RMC

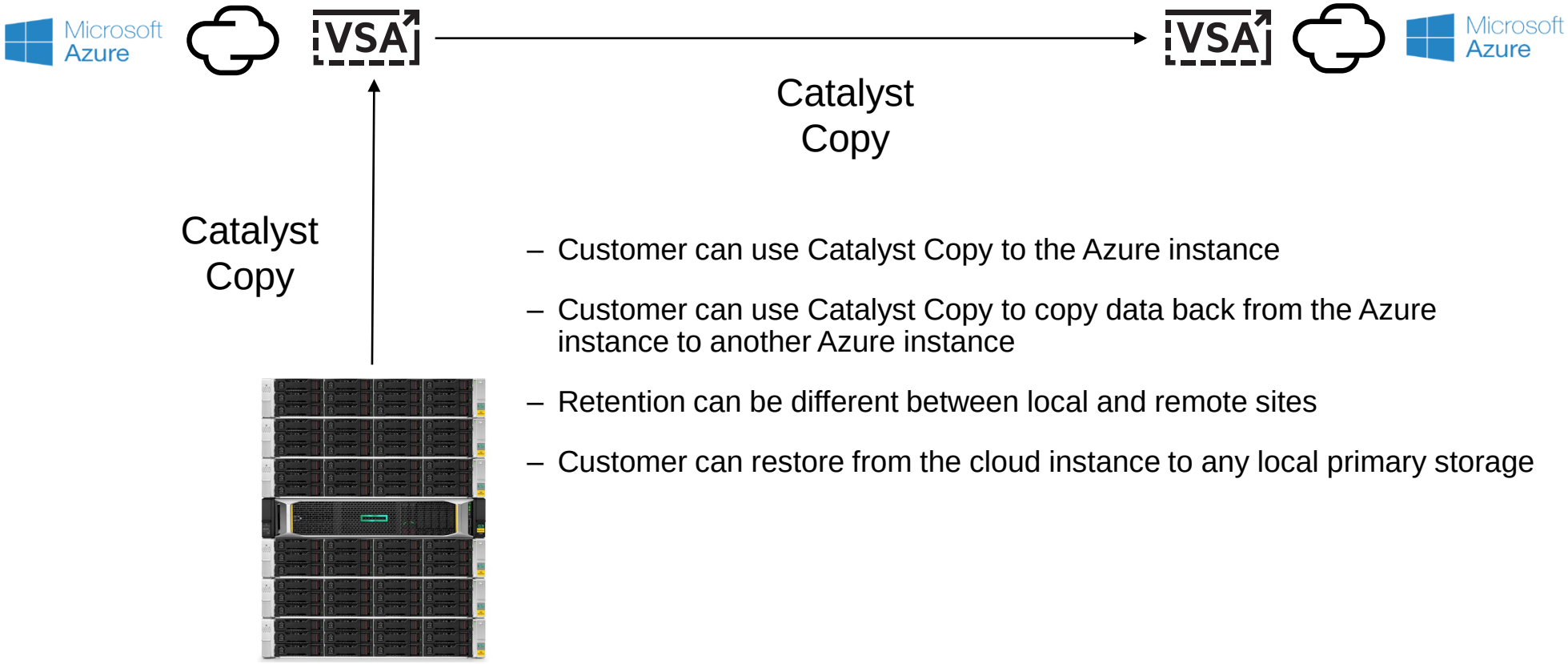
Catalyst multihop (on-premises to on-premises to cloud)



- Customer can use Catalyst Copy to the Azure instance
- Customer can use Catalyst Copy to copy data back from the Azure instance to the local appliance
- Retention can be different between local and remote sites
- Customer can restore from the cloud instance to any local primary storage

Note: Supports any Catalyst ISV or application plug-in, along with RMC

Catalyst multihop (on-premises to cloud to cloud)



- Customer can use Catalyst Copy to the Azure instance
- Customer can use Catalyst Copy to copy data back from the Azure instance to another Azure instance
- Retention can be different between local and remote sites
- Customer can restore from the cloud instance to any local primary storage

Note: Supports any Catalyst ISV or application plug-in, along with RMC

HPE StoreOnce Catalyst plug-ins

Hewlett Packard Enterprise

StoreOnce Catalyst plug-ins

- StoreOnce Catalyst plug-ins are designed for direct backup of business applications to StoreOnce systems, enabling advanced protection for Veritas OpenStorage Technology, Oracle, Microsoft SQL Server, and SAP HANA databases
- The plug-ins leverage Catalyst and provide key advantages:
  - Increased deduplication: Catalyst plug-ins have intelligent data stream analysis, which boosts deduplication ratios and storage savings
  - Increased backup speed: Using multiple backup streams to a Catalyst store improves throughput performance with no impact on data deduplication ratios
  - Increased availability of server resources: During backups, less server compute and bandwidth resources are used than with a native daily full backup
- No cost
  - No data protection software is required and plug-ins are free to download for StoreOnce customers

HPE Cloud Bank Storage

Hewlett Packard Enterprise

What is Cloud Bank Storage?

- Enables StoreOnce to use public and private cloud services for long-term retention and disaster recovery
- Combines the efficiency of StoreOnce deduplication with the cost benefits of cloud storage
  - Is designed to reduce cloud storage and access costs
- Offers single management point for copy control by using the existing backup application
- Supports public and private cloud service providers including AWS S3, Microsoft Azure, and Scality
- Enables recovery from cloud to any StoreOnce system
- Scales up to 2x the capacity of the associated StoreOnce system

Cloud Bank Storage support

- Catalyst Copy controlled and initiated by ISV software, Catalyst plug-in, or RMC
  - Veritas NetBackup using Storage Lifecycle Policy (SLP)
  - Micro Focus Data Protector using object copy
  - Commvault using object copy (Catalyst clone)
  - Catalyst plug-in copy options initiated from the configuration script and using copy commands
- RMC Catalyst copy configured in the RMC GUI copy policy section
- Enhanced restore allows data recovery when needed
- Local metadata storage to reduce amount of data restore from cloud storage provider
- Catalyst Copy from normal Catalyst store to Cloud Bank Storage store enables the data stored on cloud to be deduplicated (cost saving)

Data protection software	Supported
HPE Recovery Manager Central	✓
Micro Focus Data Protector	✓
Commvault	November 2018
Veritas NetBackup	OST plug-in
SAP HANA	Catalyst plug-in
Microsoft SQL Server	Catalyst plug-in
Oracle Database	Catalyst plug-in

What do I need to use Cloud Bank Storage?

– StoreOnce appliance or VSA that supports Cloud Bank Storage

– Catalyst license **only** for older Generation 3 StoreOnce systems (running 3.18.5)

– Next-generation StoreOnce systems support Catalyst as a standard feature

– Encryption license recommended

– Cloud Bank Storage read/write license and optional Cloud Bank Storage detach license

– Microsoft Azure, Amazon S3, or Scality object store

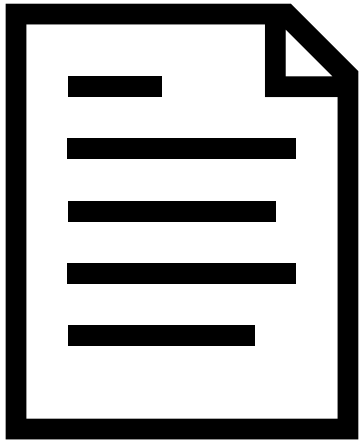
– ISV software that supports Catalyst, HPE RMC, or StoreOnce Catalyst plug-in

HPE StoreOnce Cloud Bank Storage capacities

Model	Maximum local storage	Maximum Cloud Bank Storage
StoreOnce 5650	1.7 TB	3.5 TB
StoreOnce 5250	864 TB	1728 TB
StoreOnce 5200	216 TB	512 TB
StoreOnce 3640	108 TB	216 TB
StoreOnce 3620	31.5 TB	63 TB
StoreOnce VSA	500 TB	1 PB

Cloud Bank Storage licensing overview

Cloud Bank Storage license



– Enables read/write connection from licensed system to external object storage

– Allows read-only connection from other systems

– Applied in 1 TB multiples to the StoreOnce system, up to the system maximum

– Locked to system; consumed by all hosted read/write Cloud Bank Storage stores

Cloud Bank Storage detach license

– Optional extension to enable Cloud Bank Storage stores to be disconnected and reconnected

– Applied in 1 TB multiples to the StoreOnce system; no maximum

– Locked to the system; on detach, the license for capacity of detached store is decremented from system and locked to detached store

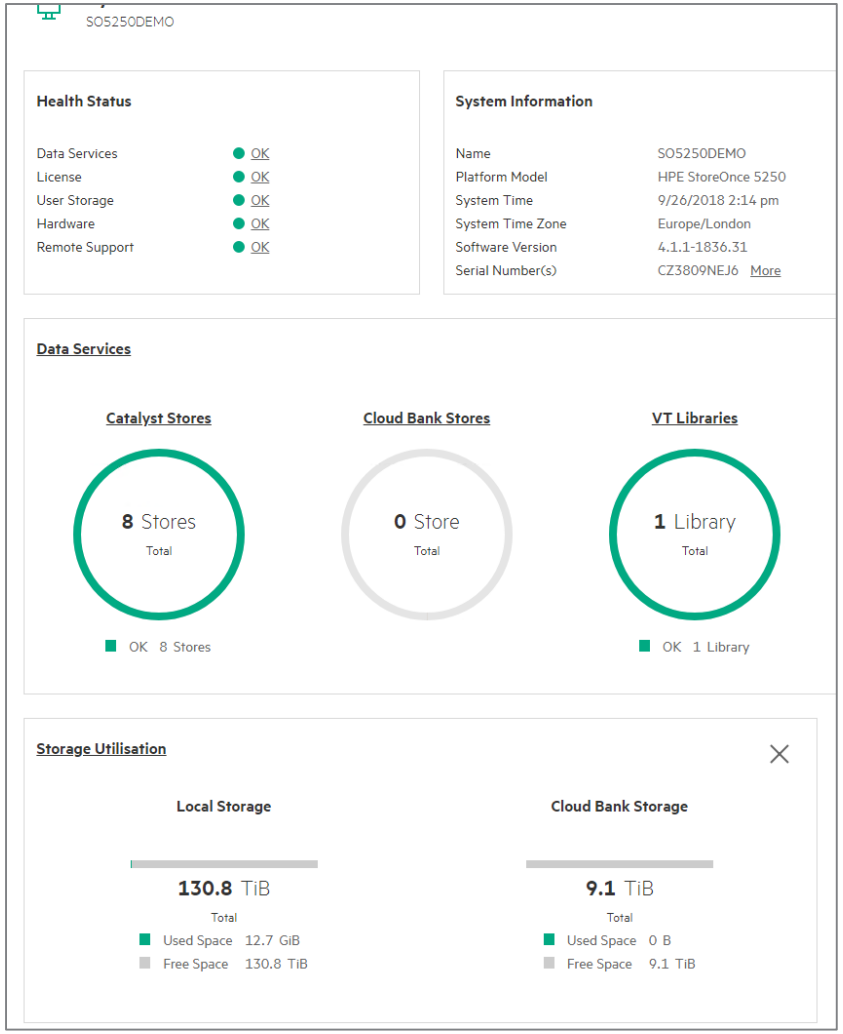
Cloud Bank Storage licensing notes

- All Next-Generation StoreOnce systems (Generation 4 and later) can connect to Cloud Bank Stores
  - Legacy Generation 3 StoreOnce models require a Catalyst license
- Cloud Bank Storage licenses are not needed on a system to connect to Cloud Bank Storage store in read-only mode
  - Disconnected store with detach license can be read without needing or consuming Cloud Bank Storage licenses
  - Cloud Bank Storage stores hosted on other systems can be connected to for read access without needing or consuming Cloud Bank Storage licenses
- Disconnected stores
  - Disconnected stores can be reconnected to any StoreOnce system with sufficient Cloud Bank Storage license capacity in read/write mode up to 60 days after disconnection
    - With StoreOnce systems with firmware updated to revision 3.18 or later, any disconnected stores with a detach license can be reconnected to any StoreOnce system at any time
    - Disconnected stores without a detach license cannot be reconnected to any StoreOnce system after 60 days without HPE intervention
  - Stores cannot be reconnected less than 24 hours from disconnection to avoid issues with eventual consistency of the object storage

How much Cloud Bank Storage capacity can be licensed?

– Check the GUI on the appliance for guidance

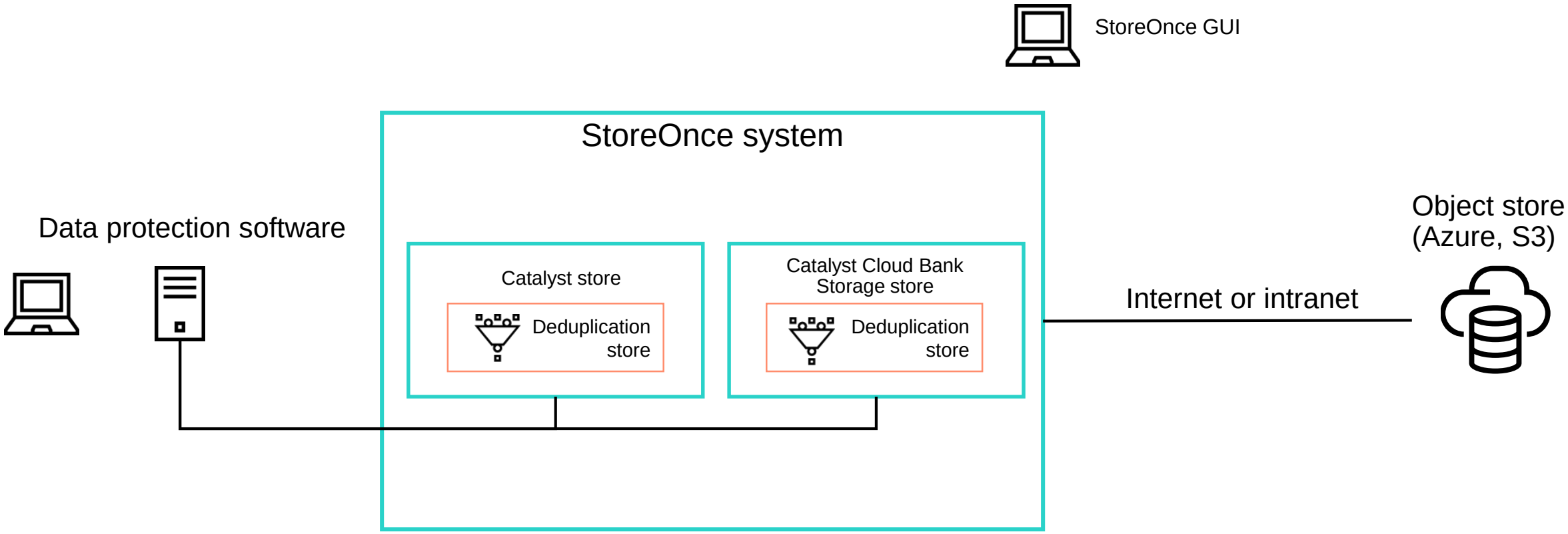
– Note that local storage reduces the amount of Cloud Bank Storage read/write storage that can be used



HPE Cloud Bank Storage in use

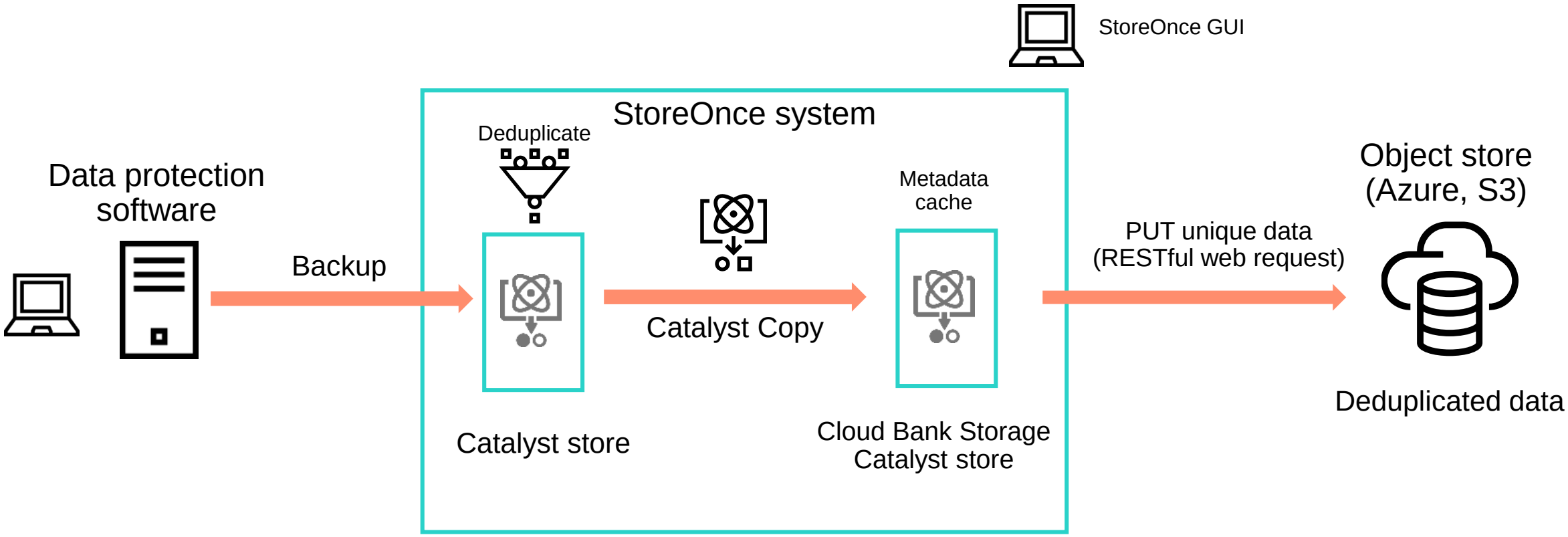
How does it work?

Cloud Bank Storage setup

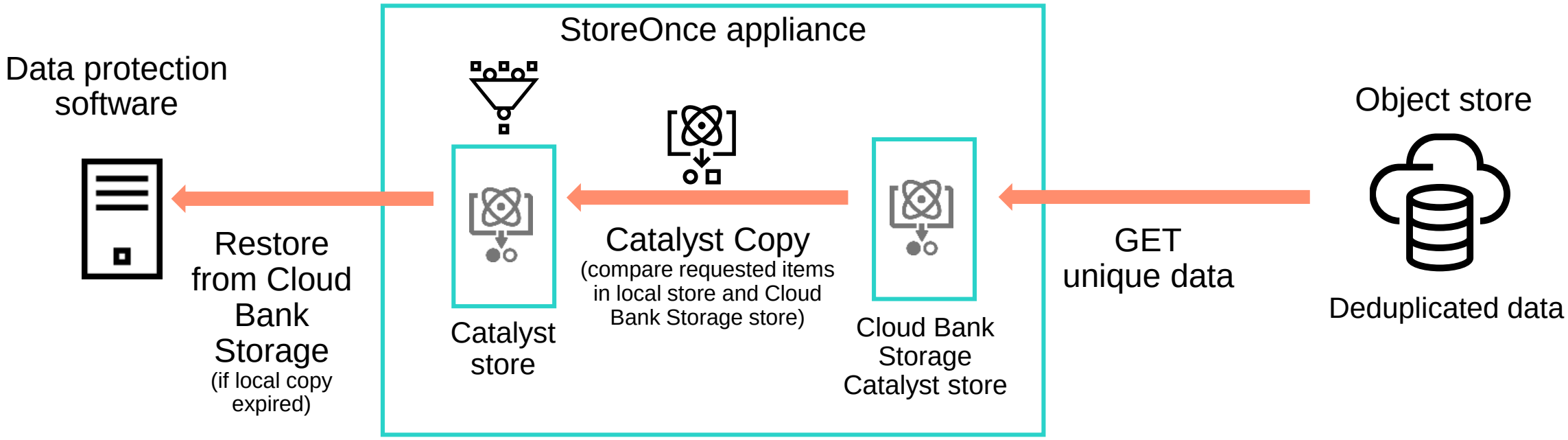


1. Create a Catalyst store by using the StoreOnce GUI
2. Create a Cloud Bank Storage store and enter credentials of the Azure or S3 object store
3. Configure the data protection software for both stores
4. Configure a backup job to the Catalyst store and a copy job (object copy and SLP) to the Cloud Bank Storage store

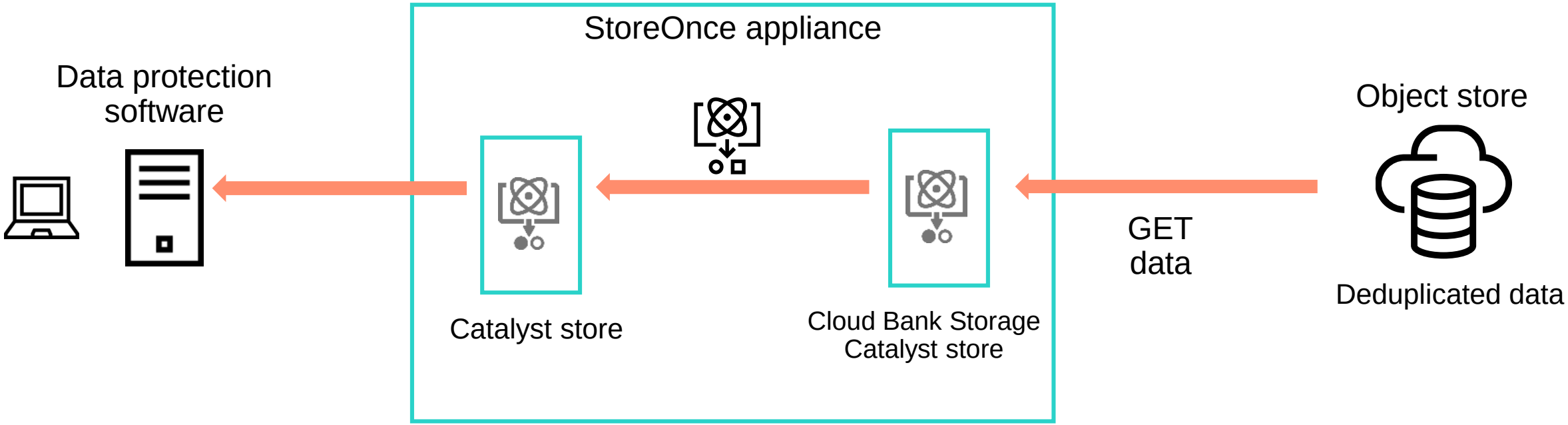
Cloud Bank Storage—Backup and copy



Cloud Bank Storage—Enhanced restore



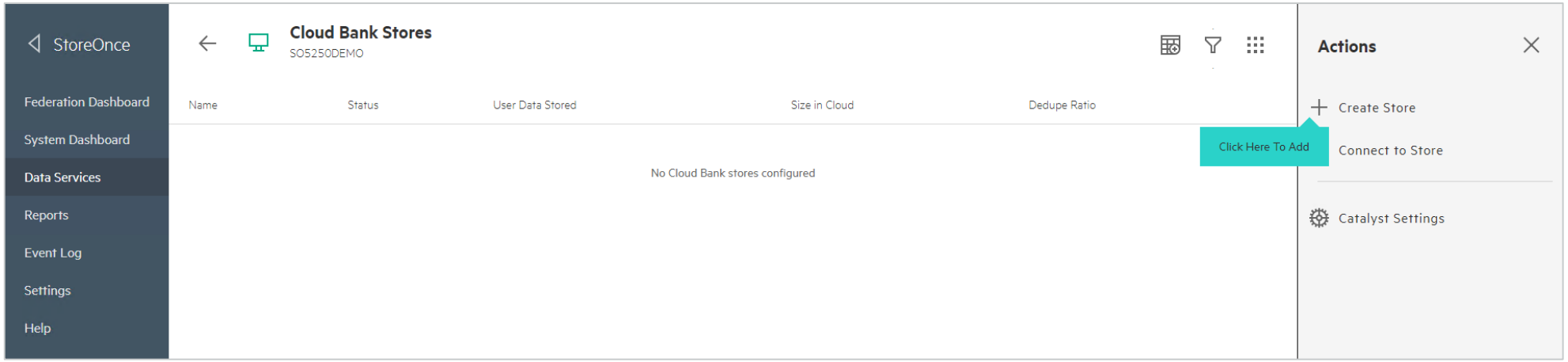
Cloud Bank Storage—DR restore



1. Install new StoreOnce appliance (can be VSA)
2. Use the StoreOnce GUI to create a new Catalyst Cloud Bank Storage store and reconnect to the external object store (requires credentials and encryption key)
   a. Use the connect key; store will be read-only for 24 hours
3. Create a new local store and reconfigure ISV software
4. Initiate Catalyst Copy to local store
5. Restore data to original locations

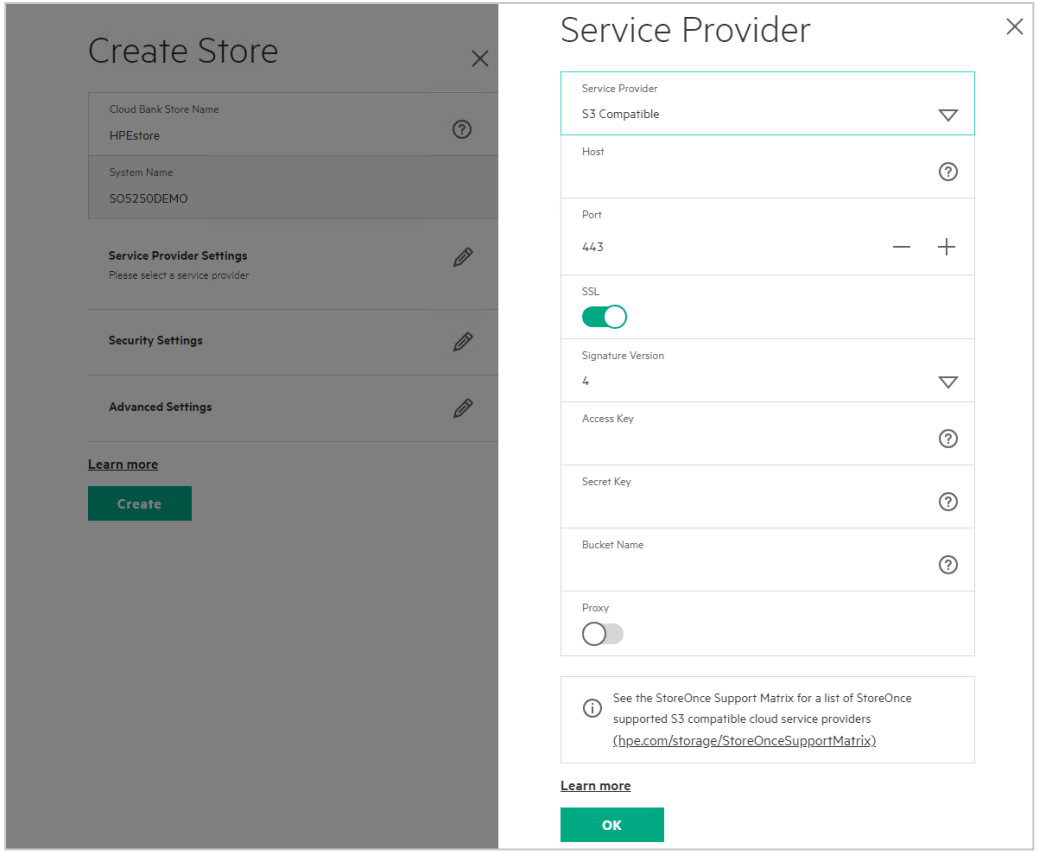
Creating a Cloud Bank Storage store—StoreOnce GUI

– From the StoreOnce GUI, navigate to **Cloud Bank Stores** and then select **Create Store**

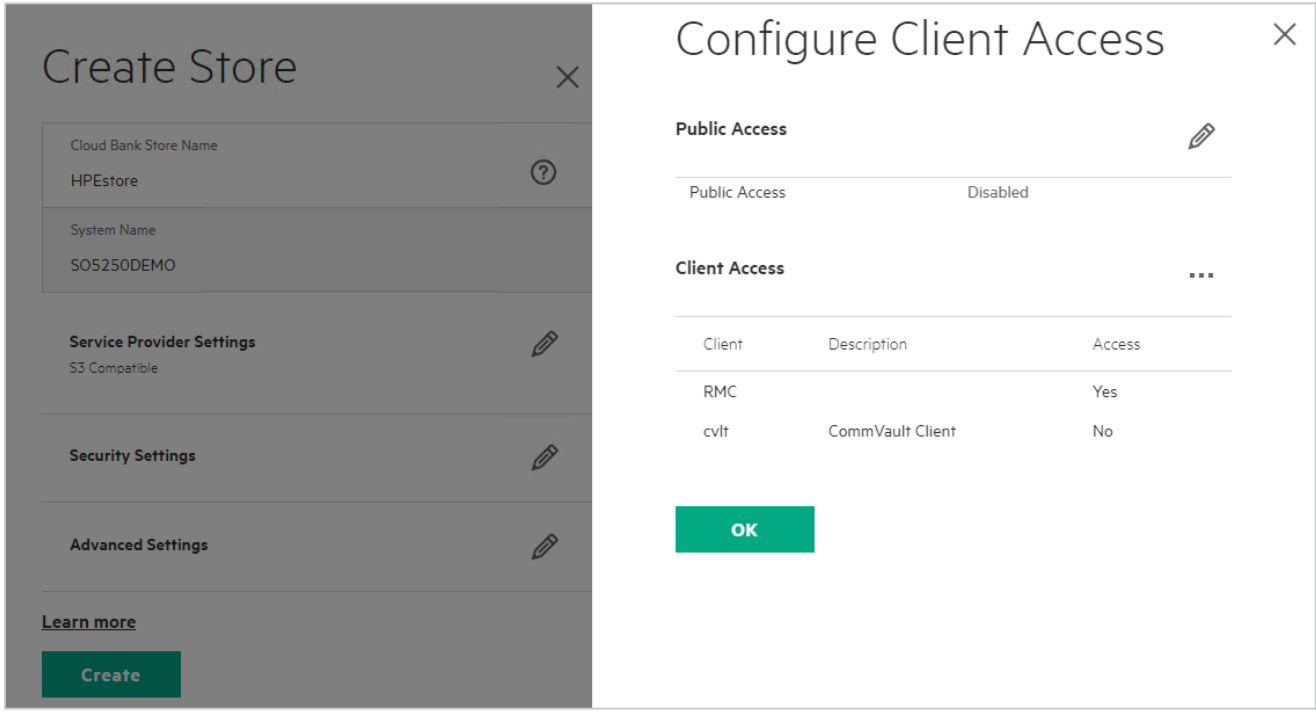


Creating a Cloud Bank Storage store

Configure the service provider

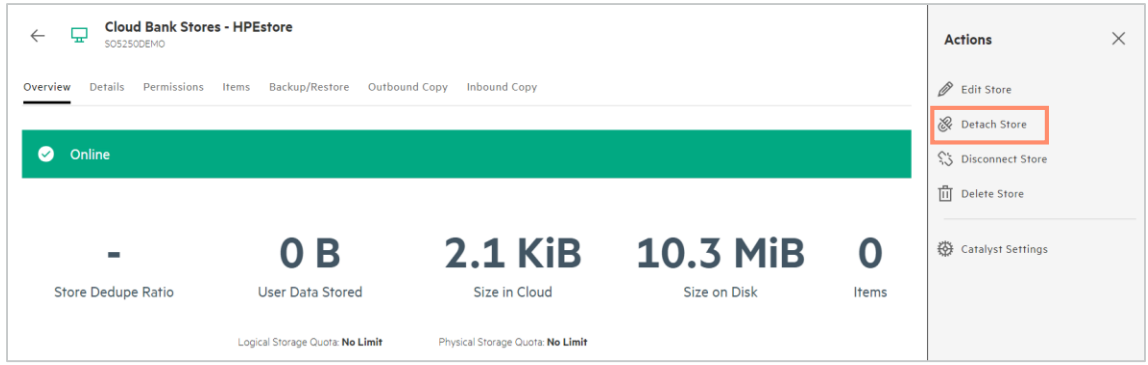


Configure the client access

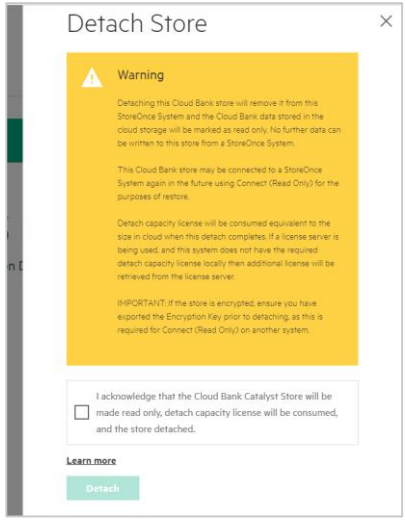


Detaching a Cloud Bank Storage store

From the StoreOnce GUI, navigate to the Catalyst store and select **Detach Store**

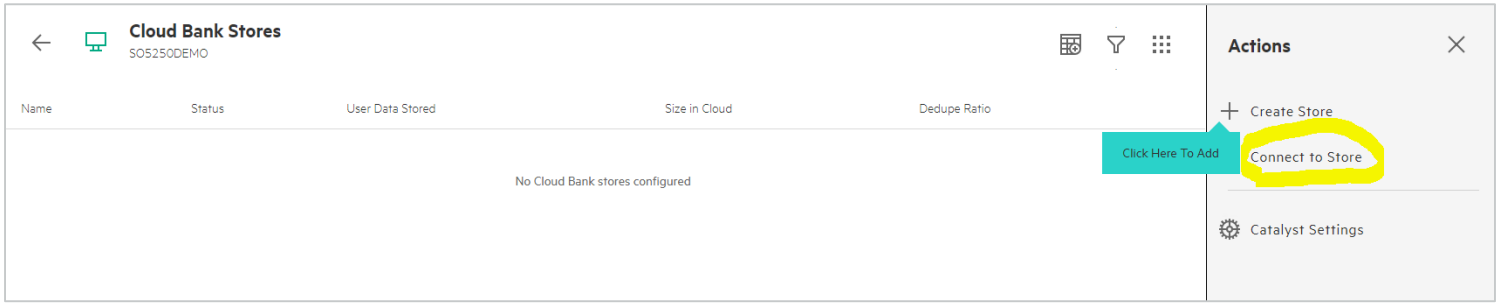


Read and acknowledge the warning and click **Detach**



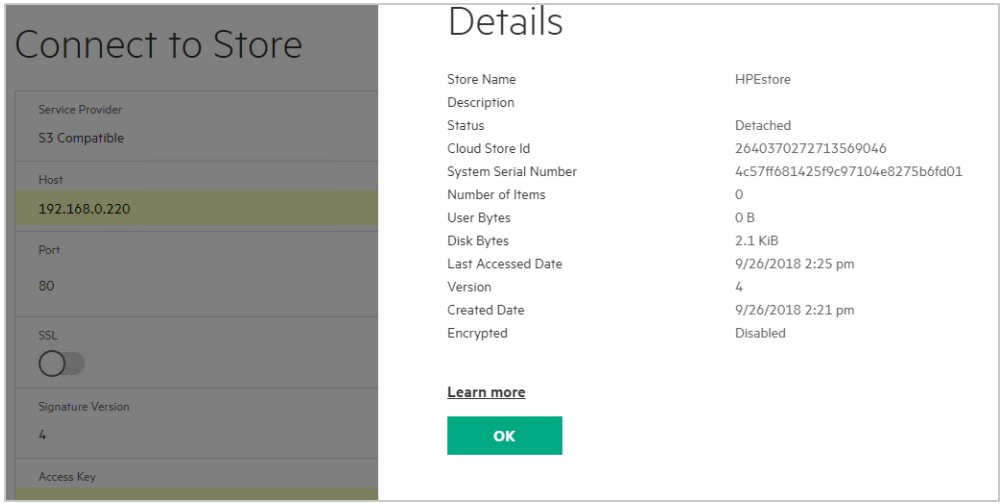
Reconnecting to a Cloud Bank Storage store

From the StoreOnce GUI, navigate to the Cloud Bank Storage store and select **Connect to Store**



Provide the host details and access key information and select **Connect**

The store will reconnect but remains in a read-only state for 24 hours



Multireader functionality

– Cloud Bank Storage enables DR testing, restore testing, and other use cases to validate data integrity

– StoreOnce system connects in read-only mode to the Cloud Bank Storage Catalyst store on the host StoreOnce system

– Multiple systems can connect to a Cloud Bank Storage Catalyst store hosted on a StoreOnce system

– Operation

1. From StoreOnce GUI, navigate to **StoreOnce** → **StoreOnce Catalyst** → **Stores**
2. Click the **Connect** button and select the CSP used to store the Cloud Bank Storage store
3. Provide the required CSP details including the container or bucket name for the Cloud Bank Storage store

   StoreOnce then runs a connectivity check to validate the CSP details (SSL certificate can be authenticated, credentials are valid, the container or bucket exists, and PUT, GET, LIST and DELETE operations function)
4. When the connectivity tests succeed, verify that the read-only attach process displays the details of the Cloud Bank Storage store in the container/bucket

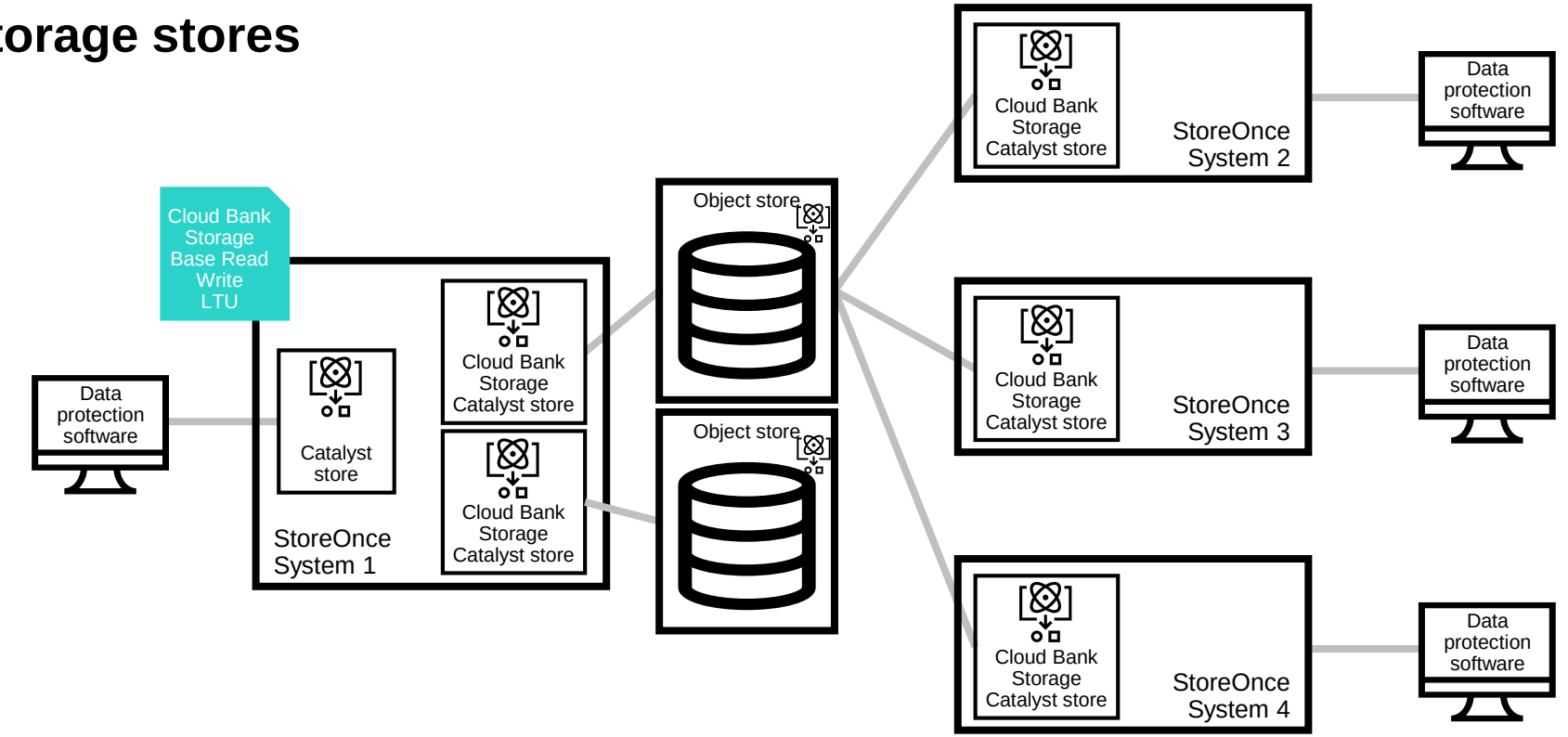
   These details are accessible by the connecting StoreOnce system if the key manager has the encryption key or an encryption key can be entered
5. Confirm that data protection applications are linked to the connected Cloud Bank Storage store to restore the data

– After these steps are complete, the connected Cloud Bank Storage store periodically checks for new or removed Catalyst items and updates the Catalyst store database

Cloud Bank Storage use cases (multireader)

Multireader Cloud Bank Storage stores

- StoreOnce Catalyst Cloud Bank Storage stores support multireader functionality
- This allows many StoreOnce systems to connect in read-only mode to the Cloud Bank Storage store
- No license is required but the data is read only

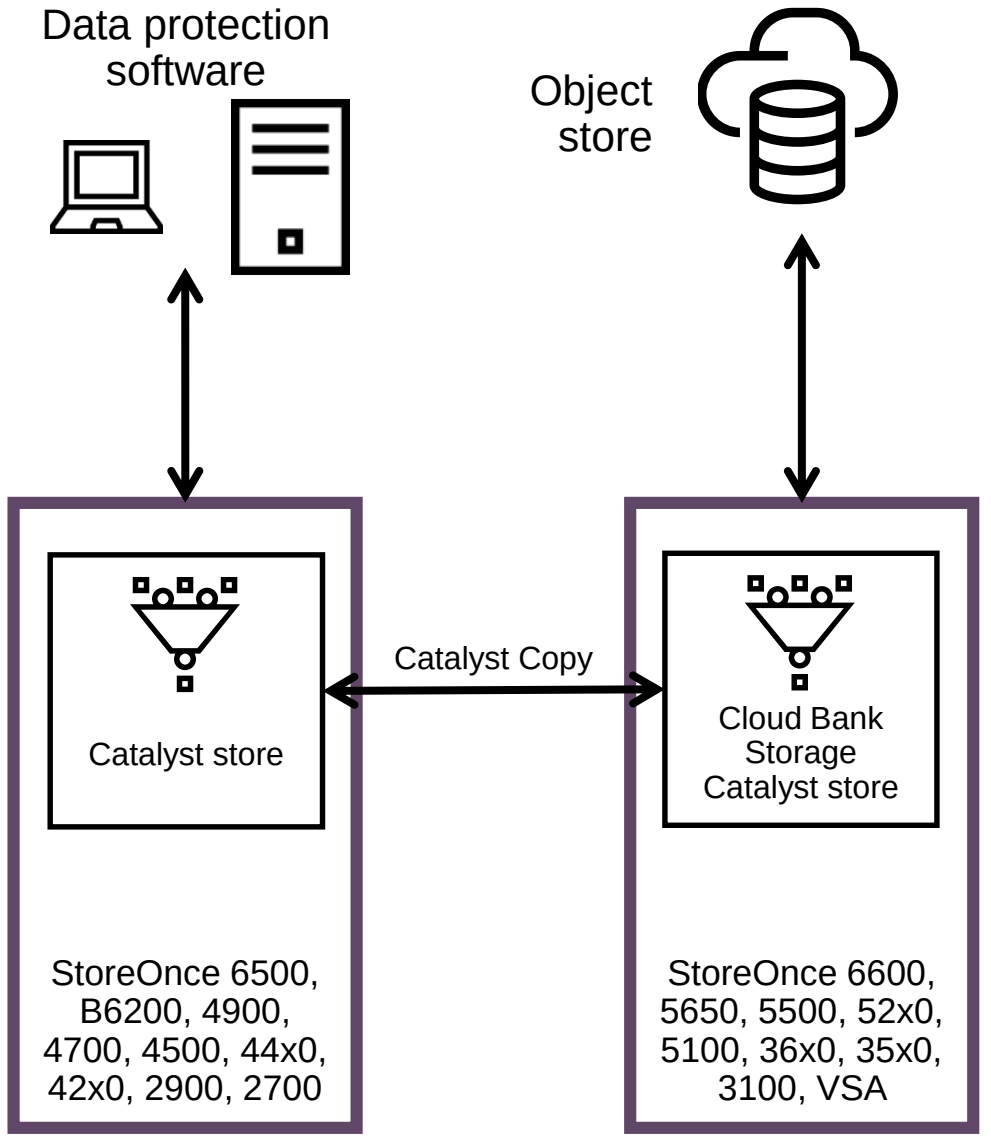


Cloud Bank Storage improvements

- Both Catalyst and the dedupe processes have been enhanced
  - Catalyst database is held in the Cloud Bank Storage store with a local copy to reduce transactions with the cloud and quickly respond to matching and other queries
  - Sparse index for Cloud Bank Storage has twice the sparseness of a regular Catalyst store to enable high Cloud Bank Storage capacity with the available memory
  - Cloud Bank Storage entities are up to 2 MB, compared to 128 KB, to enable larger objects for increased object storage performance
  - Cloud Bank Storage housekeeping deletes entire entities when all chunks in the entity have no references to them; chunks within an entity are not deleted because this is a costly cloud operation
  - ZStd compression is used on Cloud Bank Storage to minimize entity size
    - This provides better performance compared to the LZO compression used on Catalyst stores

Cloud Bank Storage in use with legacy systems

- Older StoreOnce models can use Cloud Bank Storage together with newer models
  - Cloud Bank Storage is configured on a compatible system
  - Catalyst Copy is used to move data from a store on the older model to the Cloud Bank Storage store on the new model
- All Catalyst Copy options are supported with Cloud Bank Storage
  - One compatible system can be the cloud connection for multiple older systems

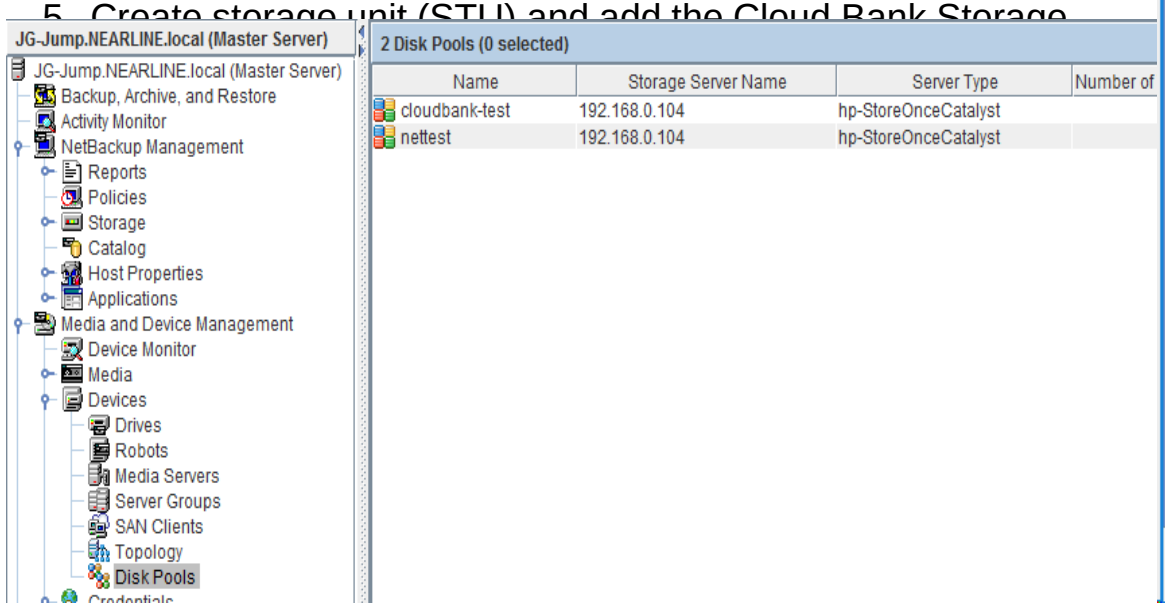


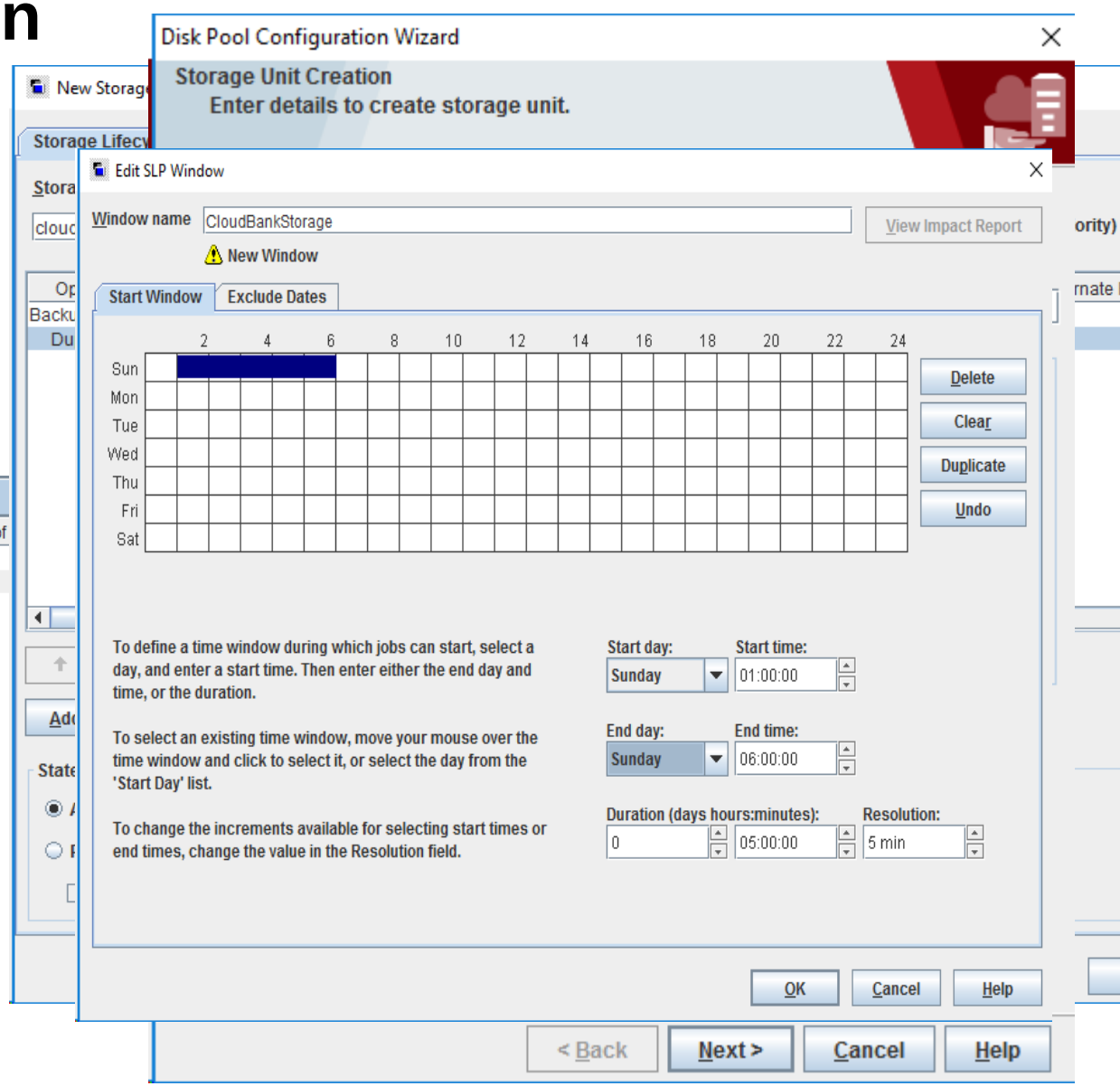
HPE Cloud Bank Storage

Veritas NetBackup configuration

Veritas NetBackup configuration

1. Create two Catalyst stores on the StoreOnce system, with one store connected to the cloud service provider
2. StoreOnce Catalyst OST plug-in must be installed
3. Add the StoreOnce system as a storage target to NetBackup
4. Click **Disk Pools** and select the Cloud Bank Storage Catalyst store
5. Create storage unit (STU) and add the Cloud Bank Storage



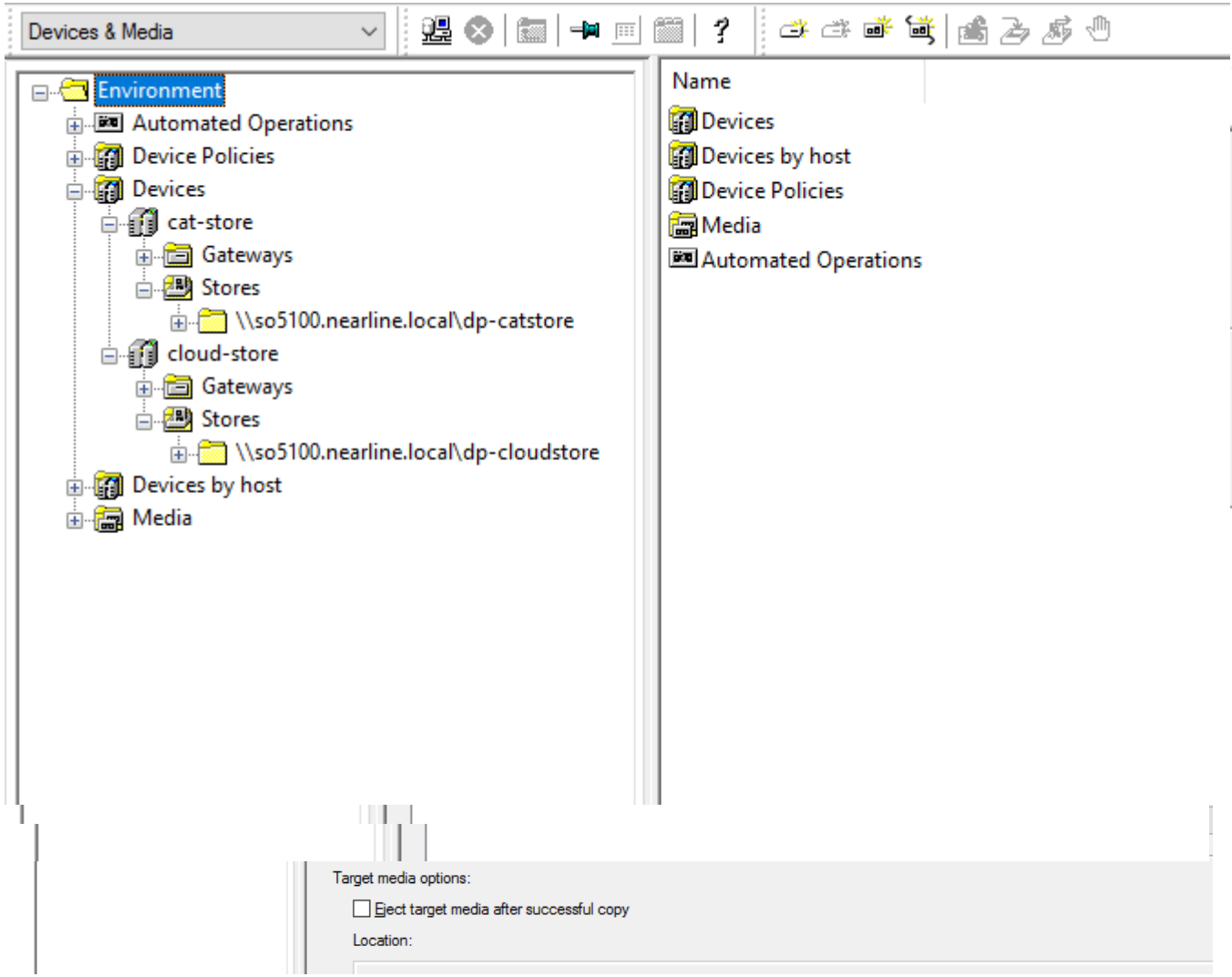


HPE Cloud Bank Storage

Micro Focus Data Protector configuration

Micro Focus Data Protector configuration

1. Create two Catalyst stores on a StoreOnce system and configure one as a Cloud Bank Storage Catalyst store
2. From the main drop-down menu, select **Object operations**
3. Select the source device
4. Click the target device
5. Change the options if needed
6. Select the source media
7. Check the summary and then click **Finish**
8. The copy starts automatically if data has already been backed up



HPE Cloud Bank Storage

HPE StoreOnce Catalyst plug-in configuration for Microsoft SQL Server with copy to Cloud Bank

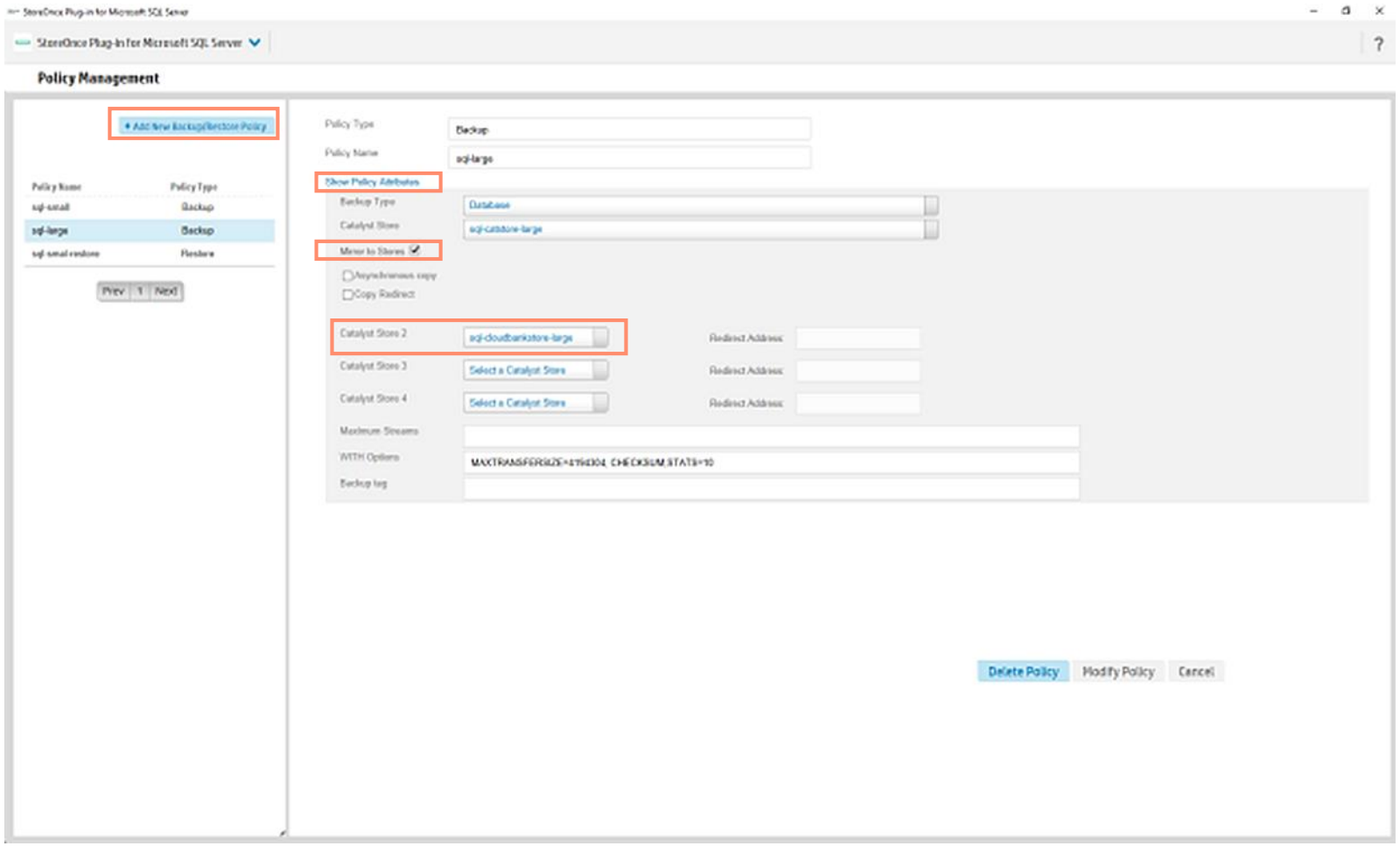
HPE StoreOnce Catalyst Plug-in for Microsoft SQL Server

1. Catalyst Copy is managed through the GUI plug-in

2. Register the Cloud Bank Storage Catalyst store with the Catalyst store manager in the StoreOnce GUI
3. In Policy Management, click **Add New Backup/Restore Policy**
   - Alternatively, select existing policy and attributes and add Cloud Bank Storage

4. Select **Mirror to Stores**

5. Select the Cloud Bank Storage Catalyst store from the drop-down menu
6. Catalyst Copy runs automatically after backup has run



HPE Cloud Bank Storage

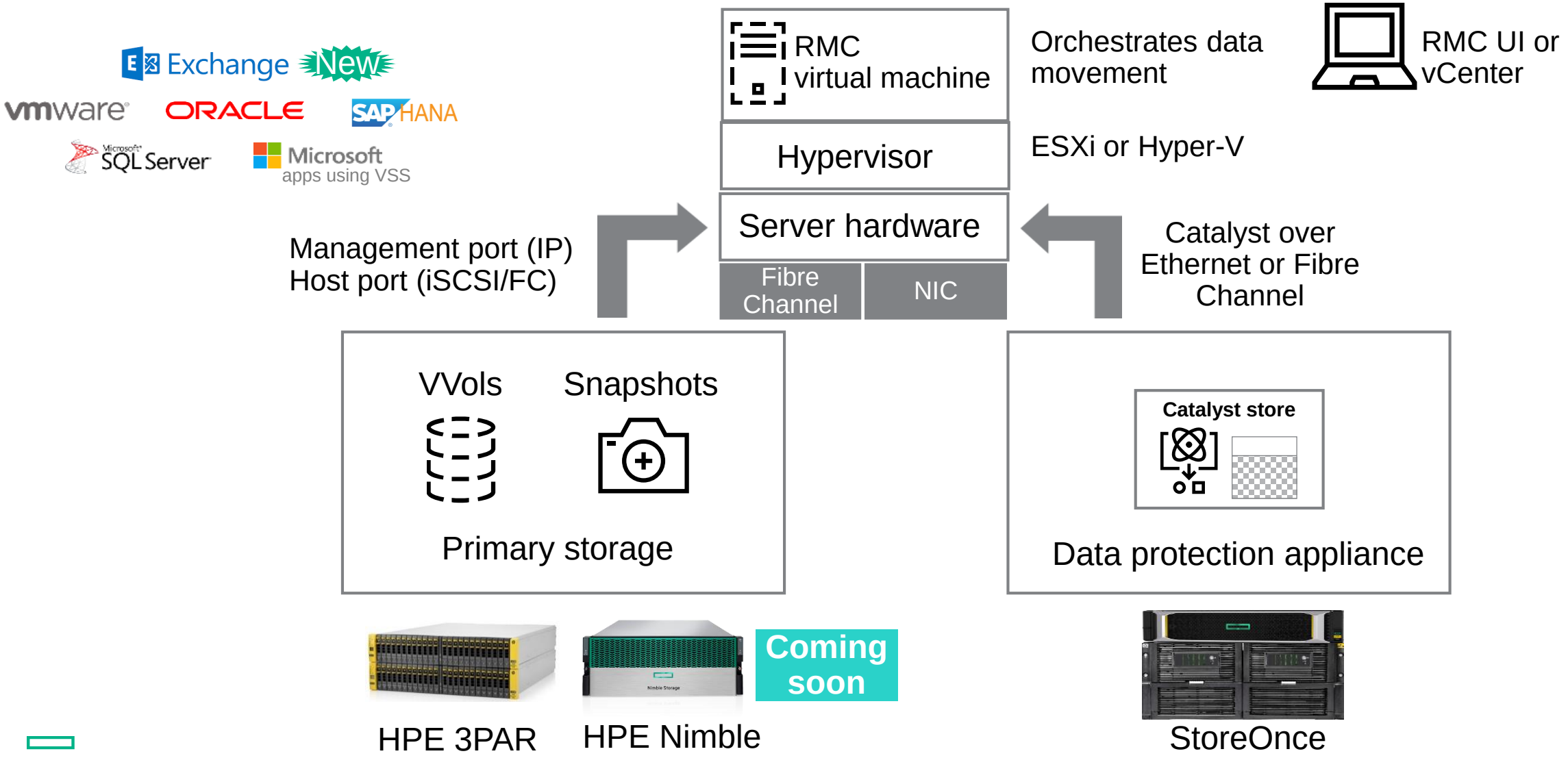
HPE RMC configuration

What is HPE Recovery Manager Central?

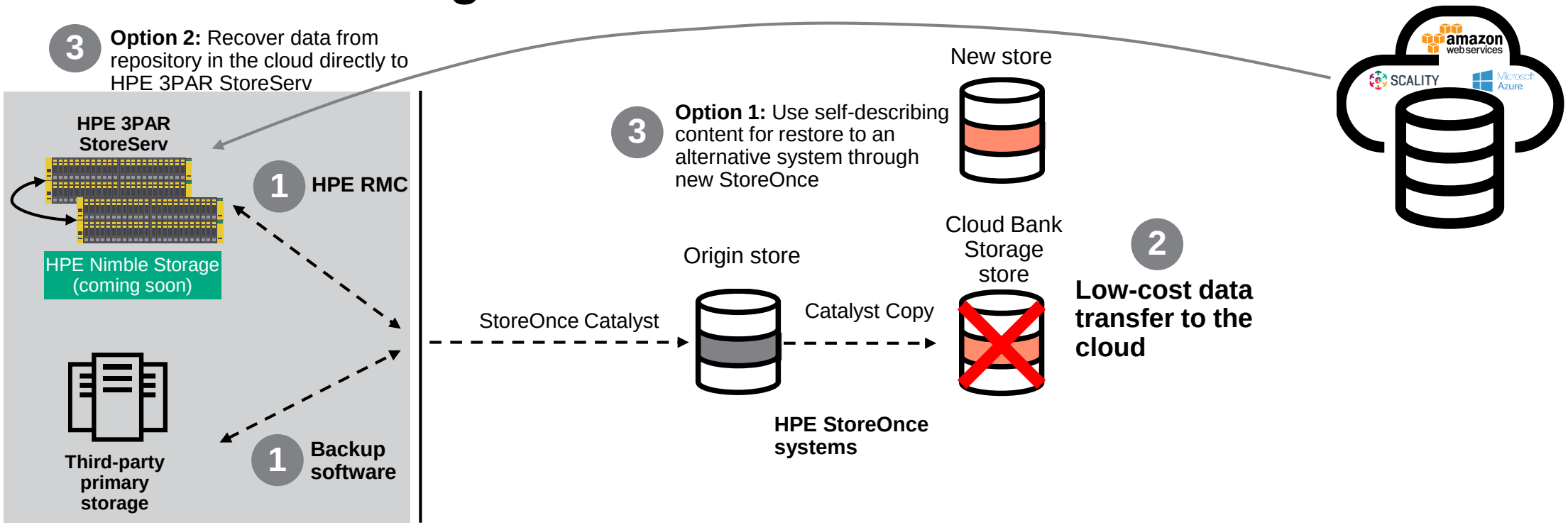
Single integration and control point for data protection of multiple HPE Storage platforms and critical applications

- Leverages primary storage snapshots and StoreOnce Catalyst backup
  - Facilitates direct backup from primary to backup storage, without backup software or media server hardware
- Combines the simplicity and performance of snapshots with the reliability and efficiency of deduplicated backups
  - Creates and manages reservation-less, space-efficient snapshots for fast, low-bandwidth backups
- Manages snapshots, backups, and replicated data copies through a single GUI
  - Helps customers overcome copy data management challenges and meet demanding SLAs

RMC architecture



Cloud Bank Storage and RMC



1 Seamless cloud enablement

Leverage existing data protection software in the current environment without any additional changes for complete cloud protection

2 Efficient transfer and storage

Apply proven StoreOnce Catalyst and dedupe technologies to minimize bandwidth for data transfer and for cloud storage; new dedupe data structures cache metadata locally to improve data transfer process

3 Disaster recovery

Option 1 (recommended): Use self-describing content for restore using an alternative system

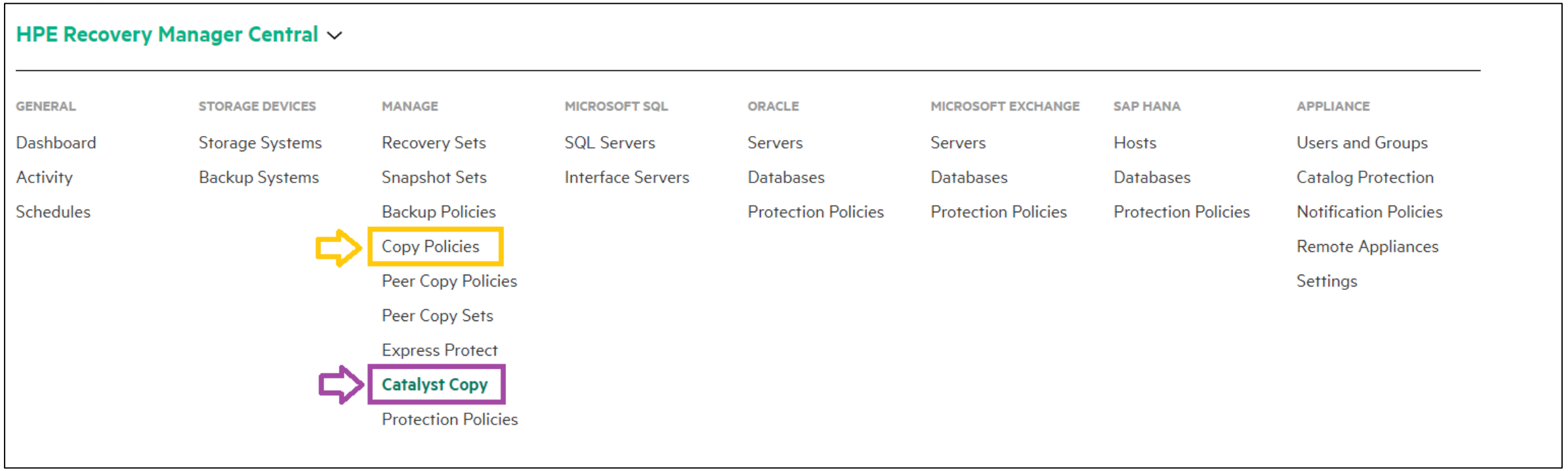
Option 2: Recover data from repository in the cloud directly to HPE 3PAR StoreServ

Using RMC with Cloud Bank Storage

HPE RMC can use Cloud Bank Storage

1. RMC performs Express Protect to a standard Catalyst store and then automatically copies to the Cloud Bank Store on a policy-based action
2. The StoreOnce appliance then moves the data off to the Cloud Storage
   – Cloud Storage can be on-premise S3 compatible, Azure Blob Storage, or AWS
3. RMC highlights the Cloud Bank Store
4. User must create a Catalyst store and Cloud Bank Store (can be on the same StoreOnce appliance or another StoreOnce)
5. User creates a backup policy and also a copy policy
6. Then uses Catalyst Copy to set up a copy to Cloud Bank

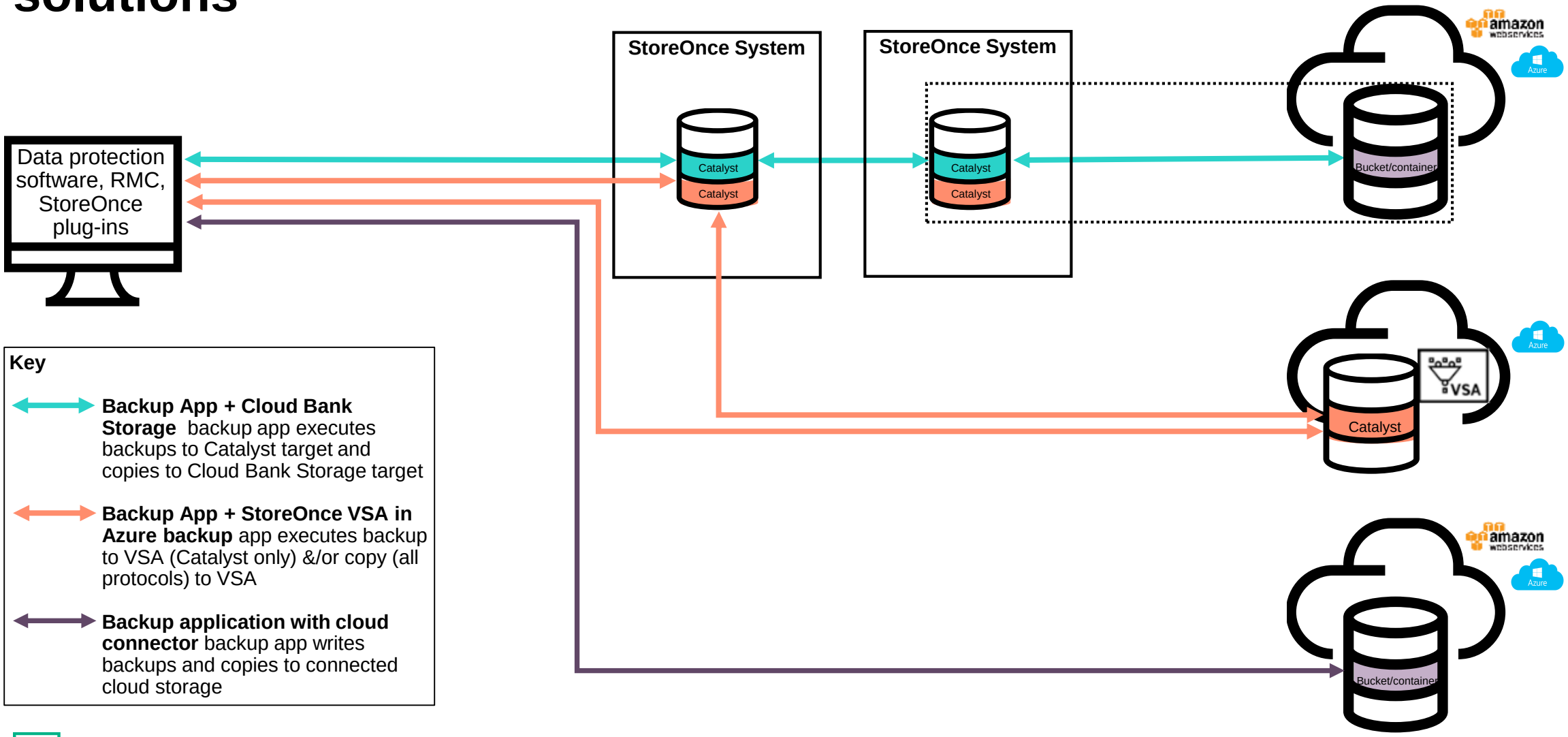
Using RMC with Catalyst Copy and Copy Policies



RMC drop-down menu highlighting Catalyst Copy and Copy Policies

HPE Cloud Bank Storage and other cloud-integrated data protection solutions

Cloud Bank Storage and other cloud-integrated data protection solutions



Cloud Bank Storage ecosystem

Vendor	Services	Supported	Notes
Amazon Web Services	Simple Storage Service (S3) Standard	●	– Reduced redundancy storage is not supported – Cross Region Replication is not supported
	Simple Storage Service (S3) Infrequent Access	●	
	Glacier	●	Cloud Bank Storage does not attach to Glacier*
HPE and Scality	S3 server	●	
Microsoft Azure	Page blob service Hot	●	– Replication must be locally redundant (LRS) – ZRS, GRS, and RA-GRS replication options are not supported
	Page blob service Cool	●	
	Page blob service Archive	●	Cloud Bank Storage does not attach to service Archive*

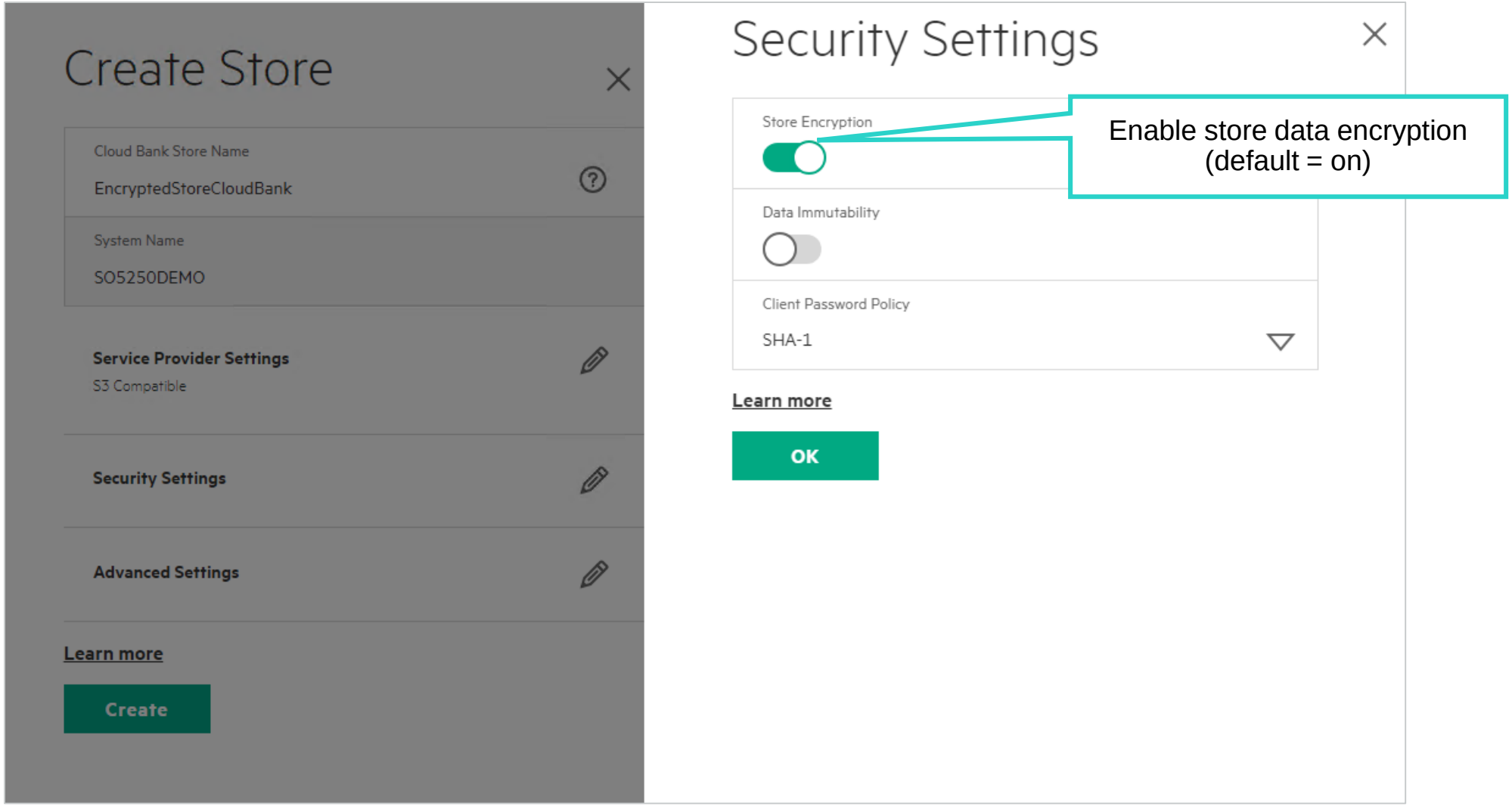
* Although Cloud Bank Storage does not directly connect to some services, administrators can manually move **detached stores** to services such as Glacier or service Archive

Encryption

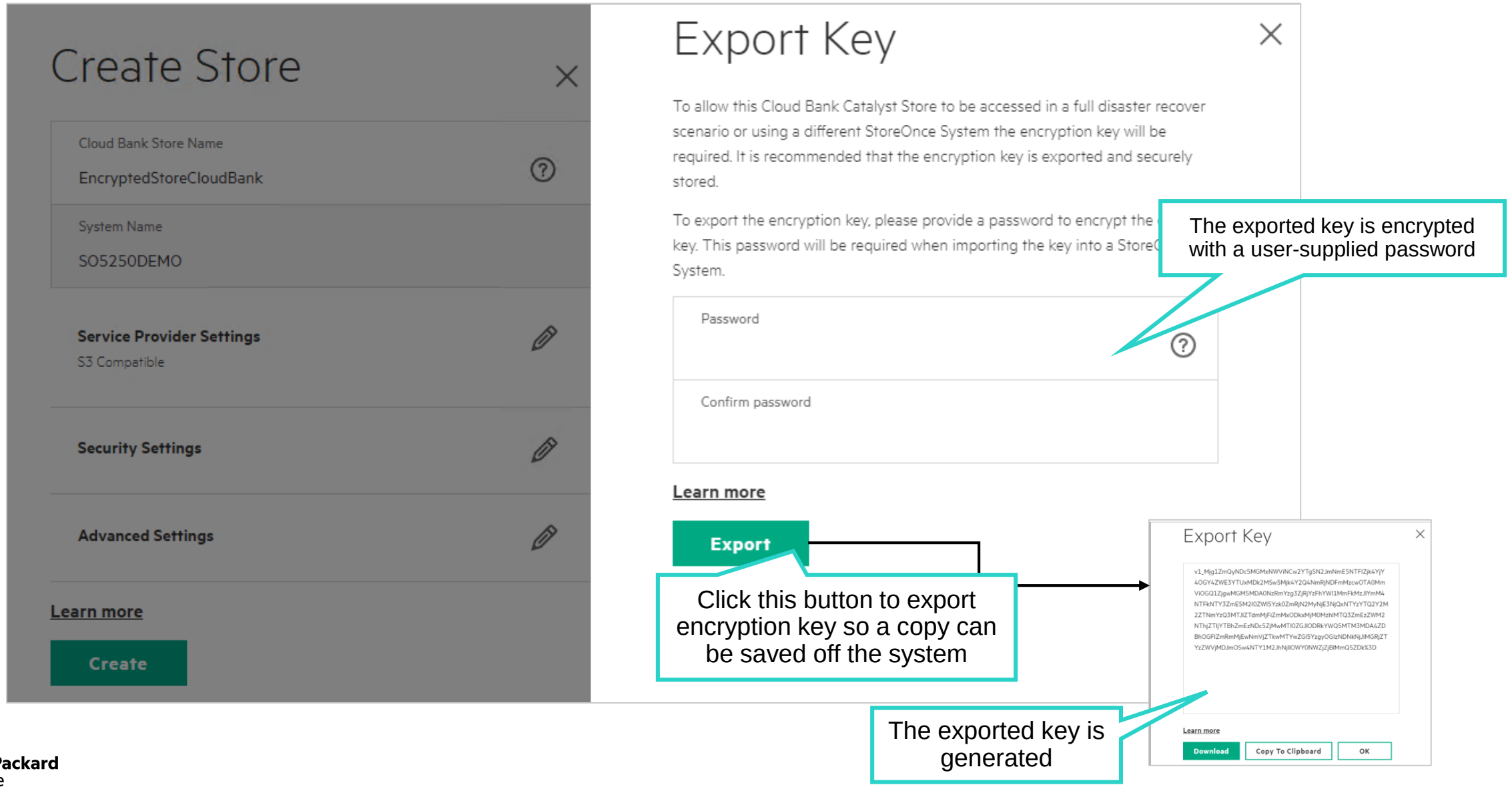
Cloud Bank Storage stores are encrypted for security of data

- Encryption is the default and recommended setting for Cloud Bank Storage stores
  - Encryption settings are configured at store creation time and then fixed
  - Cloud Bank Storage stores use the same encryption process as regular Catalyst stores with keys stored on the system or in an external key manager
  - Encryption is a licensed feature on StoreOnce
- All encryption keys written to the object store are encrypted with a key encryption key (known as the KEK)
  - This is only stored locally or in a central key manager (ESKM)
- The object storage credentials are also encrypted on the system
- When restoring or recovering to a different system without a central key manager, the KEK and its password must be entered
- Prompts to export and save a copy of the KEK are given when a Cloud Bank Storage store is created and detached
  - On export, the user supplies a password to encrypt the KEK
  - An encoded KEK is presented to the user to save in case of loss of appliance

Cloud Bank Storage encryption security settings



Cloud Bank Storage exported key



Hewlett Packard Enterprise

Hewlett Packard
Enterprise

Thank you