Hewlett Packard
Enterprise

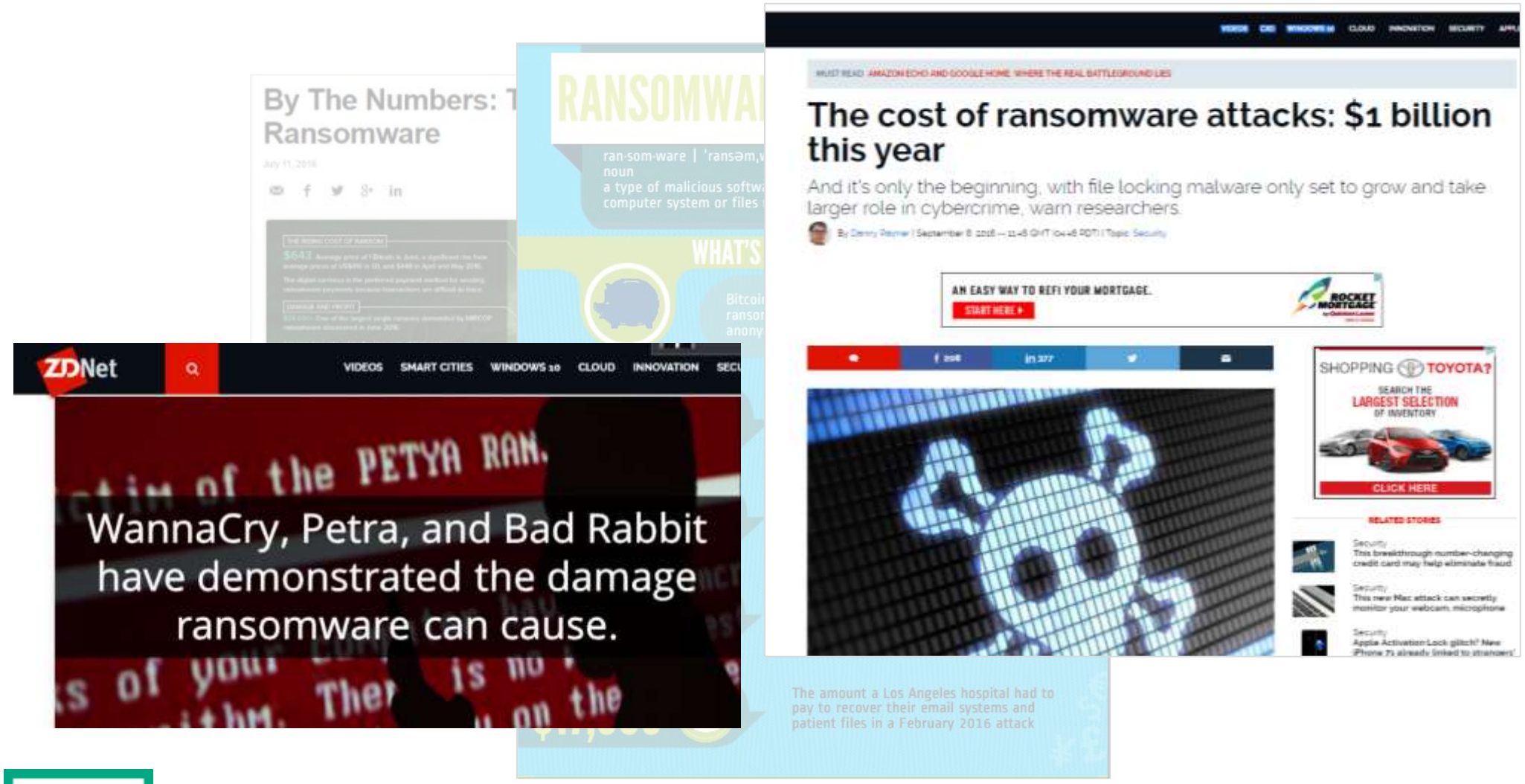
«БЕЗПЕКОВІ АСПЕКТИ ТЕХНОЛОГІЙ СУЧАСНИХ СХД, ЯКІ МОЖУТЬ БУТИ ЗАСТОСОВАНІ ДЛЯ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

Василь Візгін

Категорійний менеджер по системам збереження даних

ВАРТІСТЬ АТАК RANSOMWARE

Не тільки IT та фінансові збитки, але й імідж компанії



ЯК МОЖНО ЗАПОБІГТИ RANSOMWARE АТАЦІ ТА МІНІМІЗУВАТИ НАСЛІДКИ

1. Обізнаність користувачів (тренінги), вчасна установка патчів на ПЗ (з менеджментом процесу), управління обміном файлів та інше. (Але мене це не обходить☺)
Моя парафія - Захист даних та Резервне копіювання!

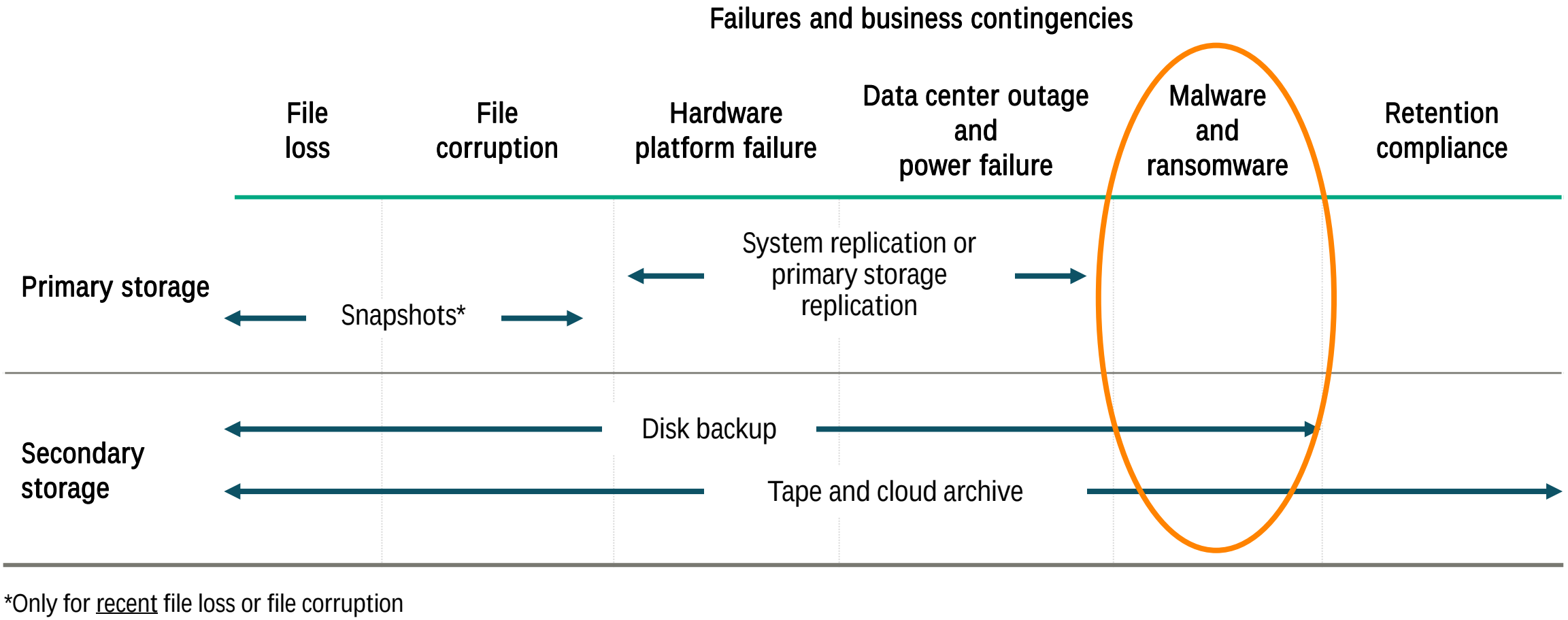
2. Видалення ransomware після заподіяння пошкодження важко. У більшості випадків видалення інфекції потребує повної перебудови системи з останнього перевіреного бакапу.
Основний технічний метод контроля – це забезпечити регулярне виконання резервного копіювання, проте можливо, що частина бакапів буде містити ransomware.
Подрібно розуміти recovery time objective (RTO) та recovery point objective (RPO)
Розробити стратегію резервного копіювання — використовуючи топологію зберігання 3-2-1
Використовувати спеціалізовани пристрої резервного копіювання як частину стратегії 3-2-1
Використовувати повни бакапи з версіями—це забезпечує доступність перевіреного бакапу, що був зроблений до інфікування. Ransomware може буди скритим тижнями.

ЯК МОЖНО ЗАПОБІГТИ RANSOMWARE АТАЦІ ТА МІНІМІЗУВАТИ НАСЛІДКИ

3

Маючи повні бакапи давніші за 30 днів покращують вірогідність відновлення.
Потрібно розуміти бакап-оточення—коли бакапляться сервери, не забути про робочі станції, ПК, laptops та інші кінцеві пристрої
Реалізувати захист бакапу від змін – не забути також захистити після того, як вони збережені offline та off-site.
Регулярний тест (аудит) бакапів.
Комбінувати миттєві знімки та бакапи. Знімки – не бакапи.
Деякі ransomware будуть намагатися вимкнути підсистему знімків ОС та стерти всі зроблени знімки (наприклад, Volume Shadow Copy (VSC) на Windows). Тому використовуємо їх разом – знімки для швидкого відновлення, бакапи – для довгострокового відновлення після катастроф.

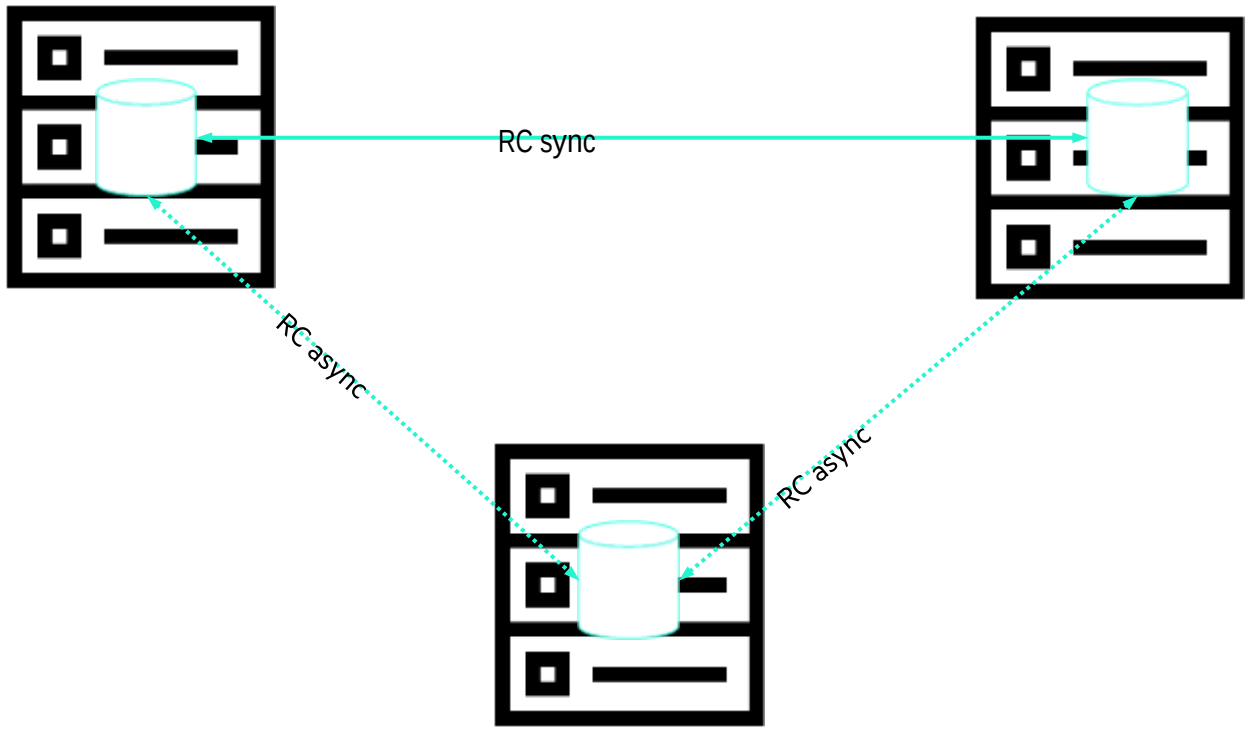
ЗЛІПКІВ ТА РЕПЛІКАЦІЇ НЕДОСТАТНЬО ДЛЯ ЗАХИСТУ ВІД RANSOMWARE (НО Є НЮАНСИ☺)



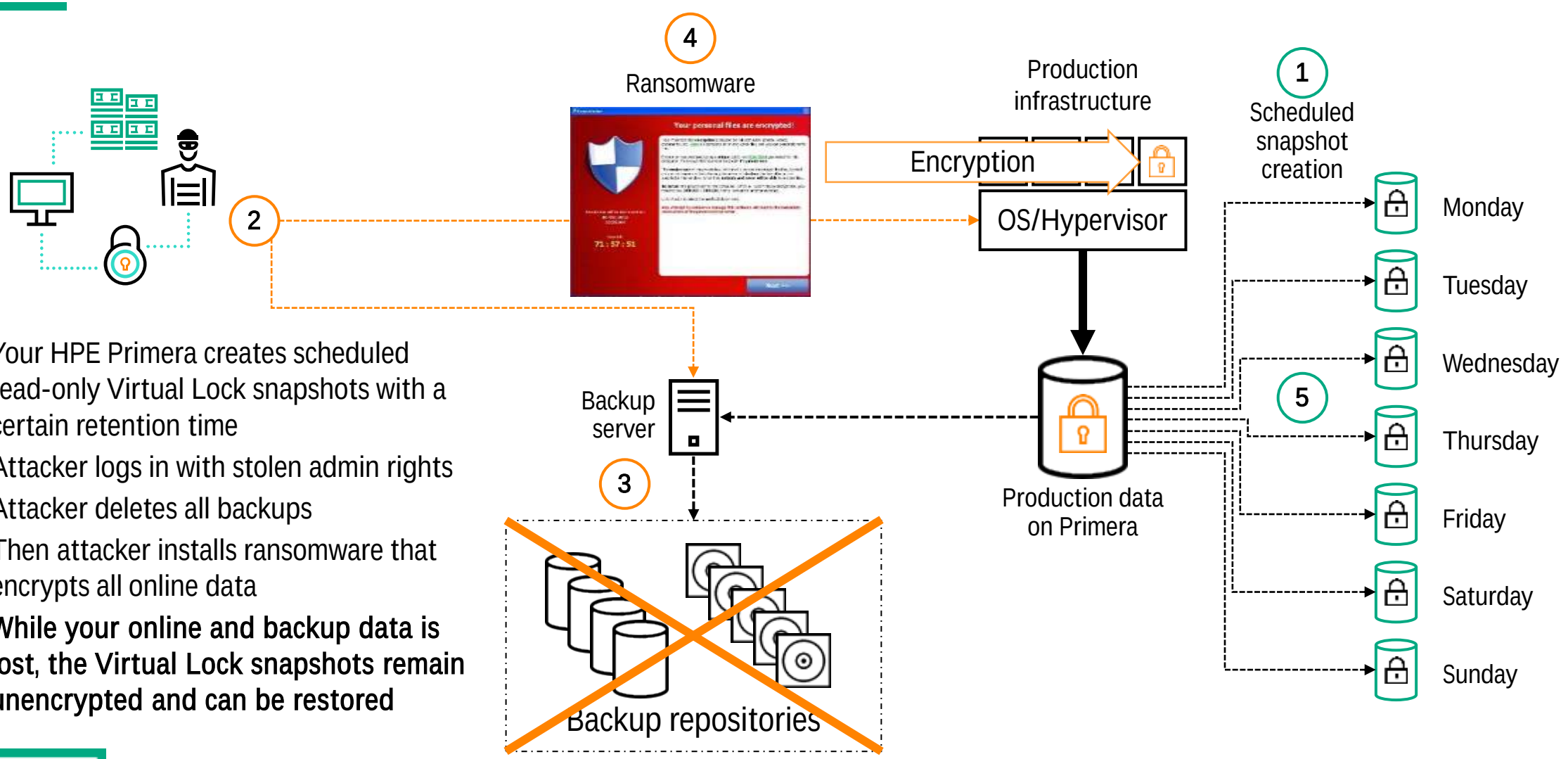
*Only for recent file loss or file corruption

РЕПЛІКАЦІЯ

3DC



CUSTOMER EXAMPLE: CYBER-ATTACK
And how HPE Virtual Lock saves your data



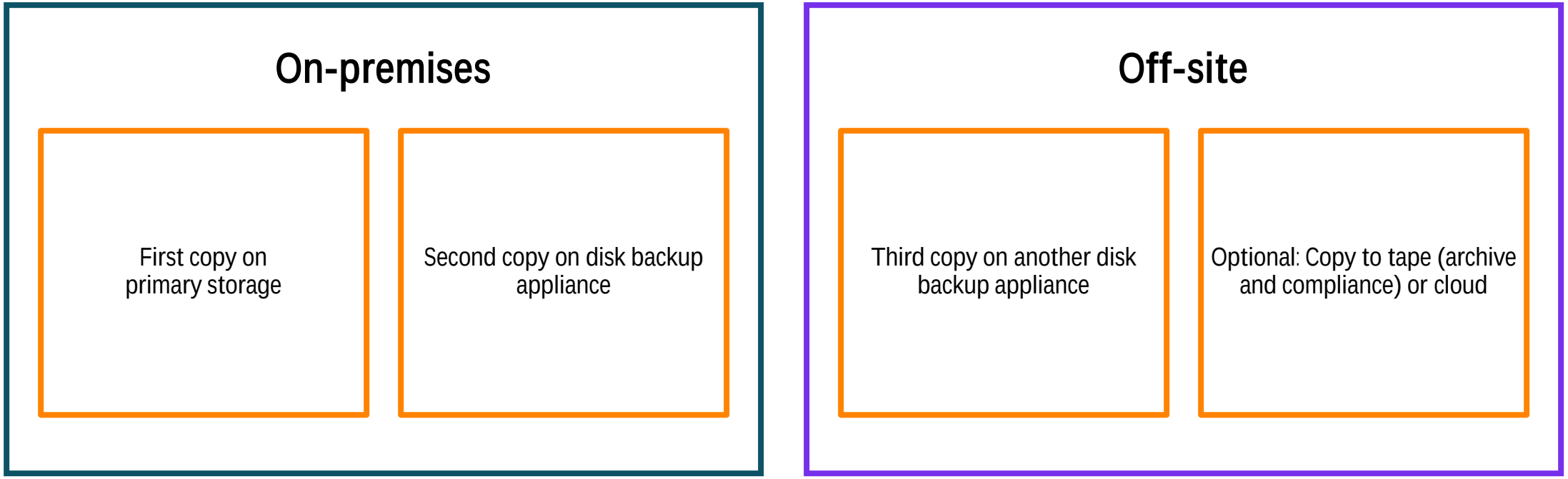
1. Your HPE Primera creates scheduled read-only Virtual Lock snapshots with a certain retention time
2. Attacker logs in with stolen admin rights
3. Attacker deletes all backups
4. Then attacker installs ransomware that encrypts all online data
5. **While your online and backup data is lost, the Virtual Lock snapshots remain unencrypted and can be restored**

ДО РЕЧІ:
ЗЛІПКИ ТА ДЕДУПЛІКАЦІЯ МОЖУТЬ ДОПОМОГТИ ВИЯВИТИ ПРОЦЕС ШИФРУВАННЯ

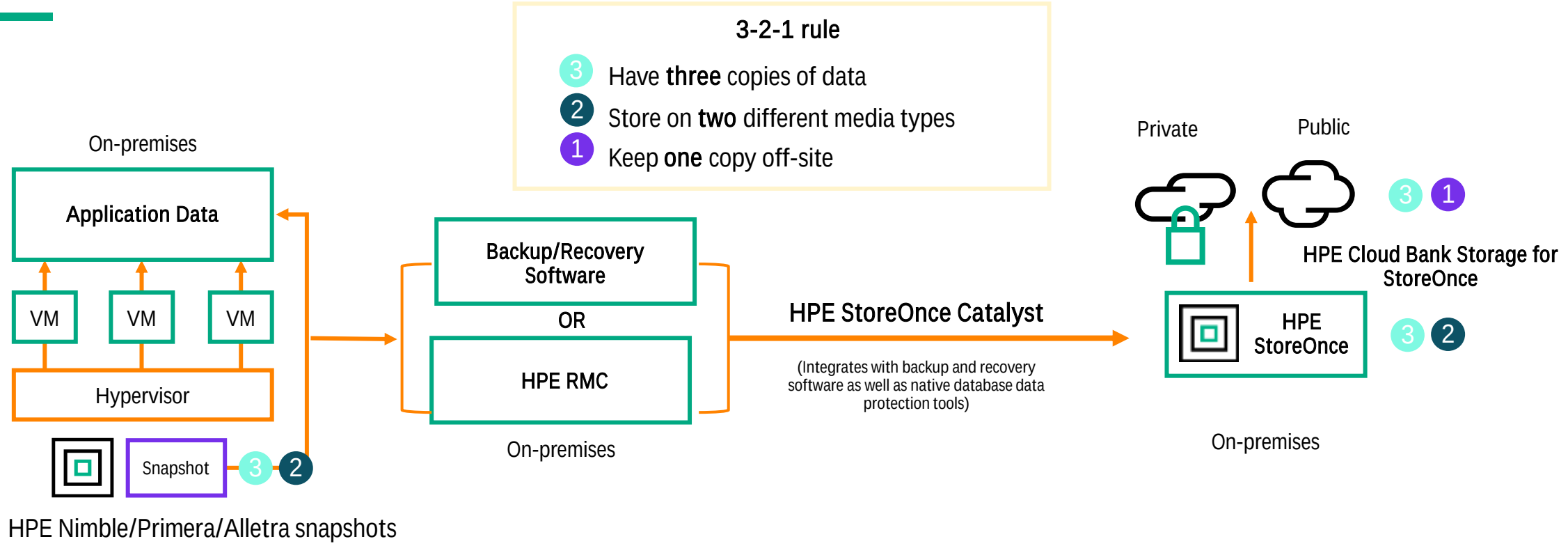
THE 3-2-1 RULE FOR BEST PRACTICE DATA PROTECTION

Protecting data against any failure…wherever it lives

3-2-1 best practice: **Three** copies of data, **two** copies on **two** different types of media, **one** copy off-site



HPE SOLUTION OVERVIEW FOR DATA PROTECTION AGAINST RANSOMWARE

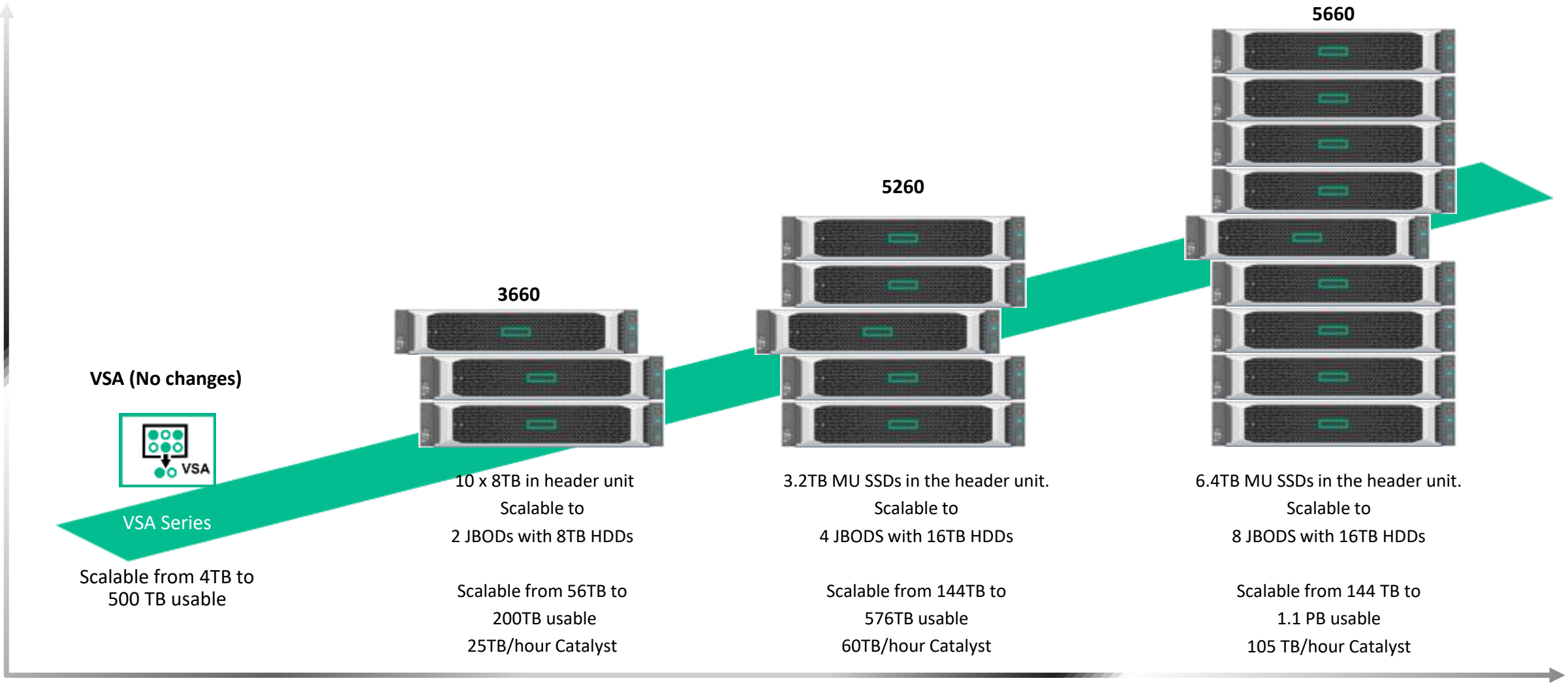


Services

HPE Pointnext and partners Consulting, support, and education

HPE Financial Services
Flexible capacity and technology refresh

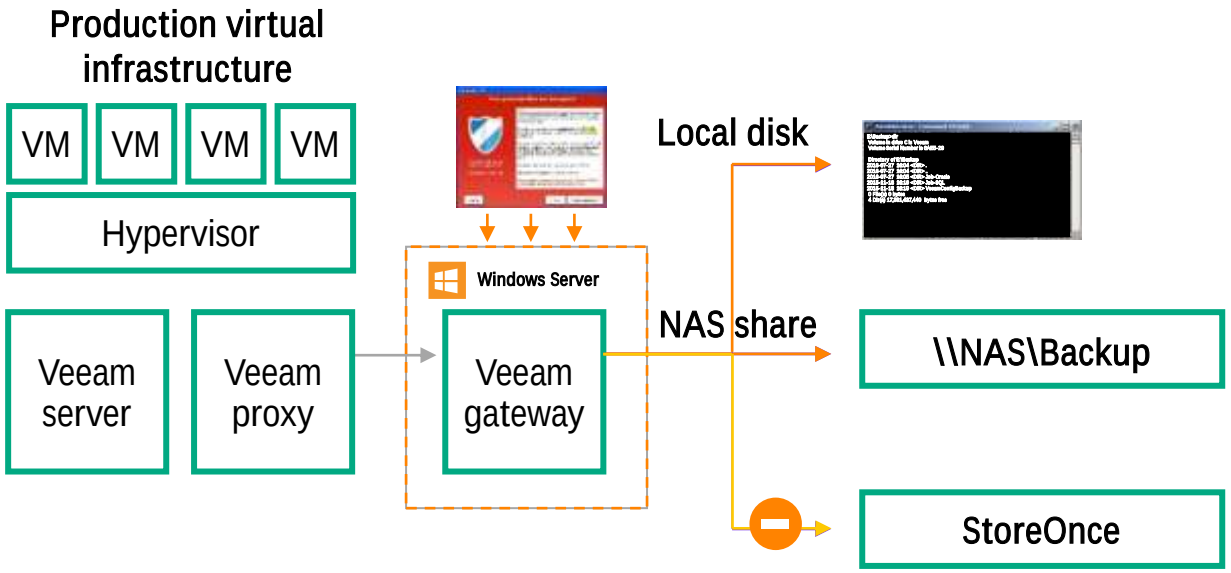
HPE STOREONCE GEN4 + PORTFOLIO



HPE STOREONCE CATALYST DENIES ACCESS TO BACKUPS
Example: Veeam backup and recovery software

Secure

Benefit: Your backup repository is protected against viruses



Access is denied to virus—repository is visible only using Catalyst API

Backup repositories

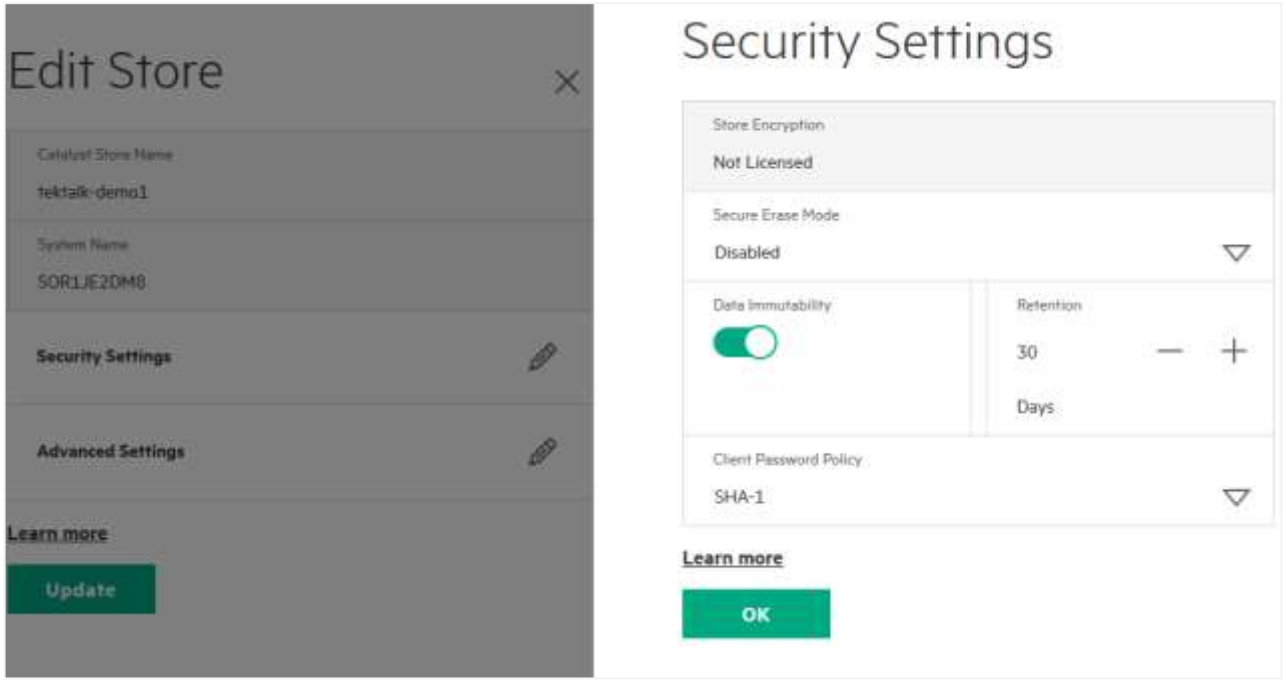
Oracle.VM.vbk
SQL.VM.vbk
DC.VM.vbk
All restore points are lost !

Oracle.VM.vbk
SQL.VM.vbk
DC.VM.vbk
All restore points are lost !

Oracle.VM.vbk
SQL.VM.vbk
DC.VM.vbk
All restore points are HEALTHY !

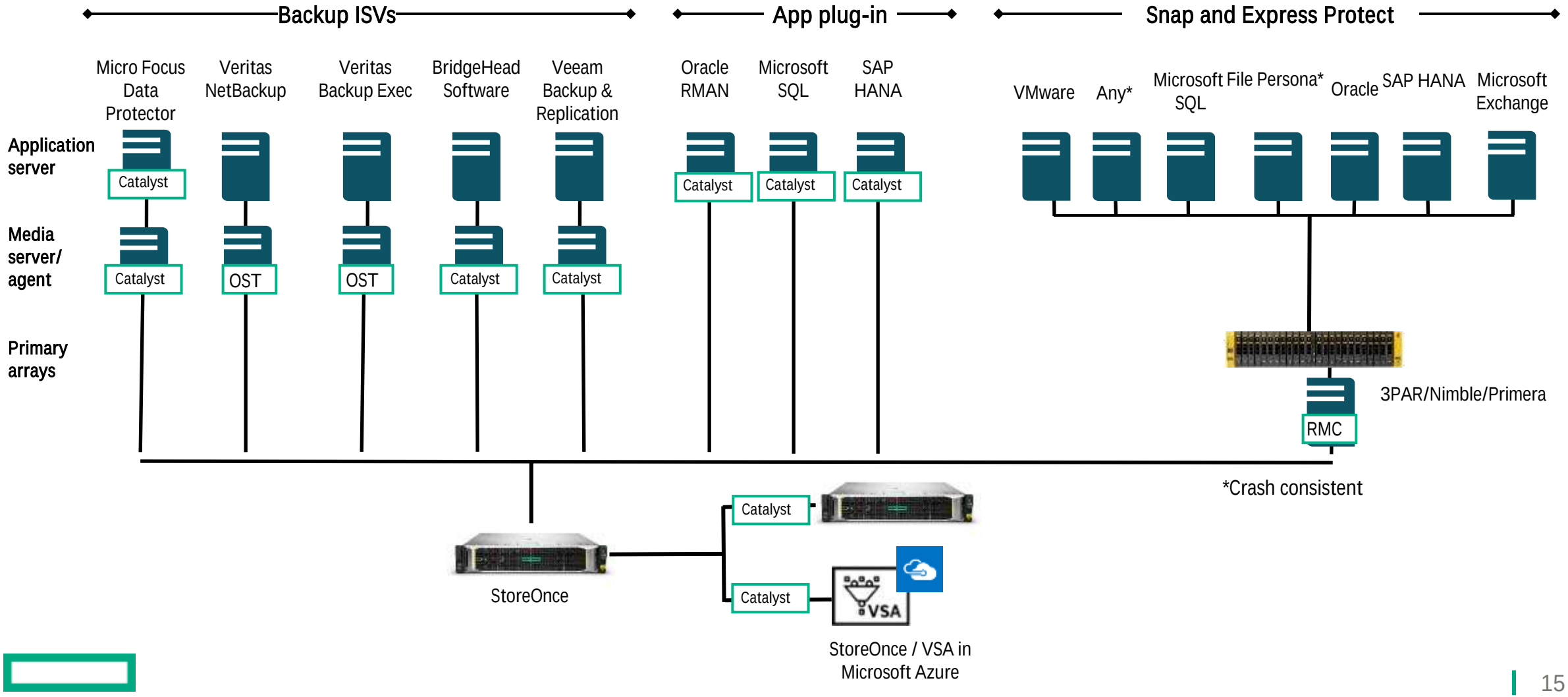
CATALYST DATA IMMUTABILITY

- 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



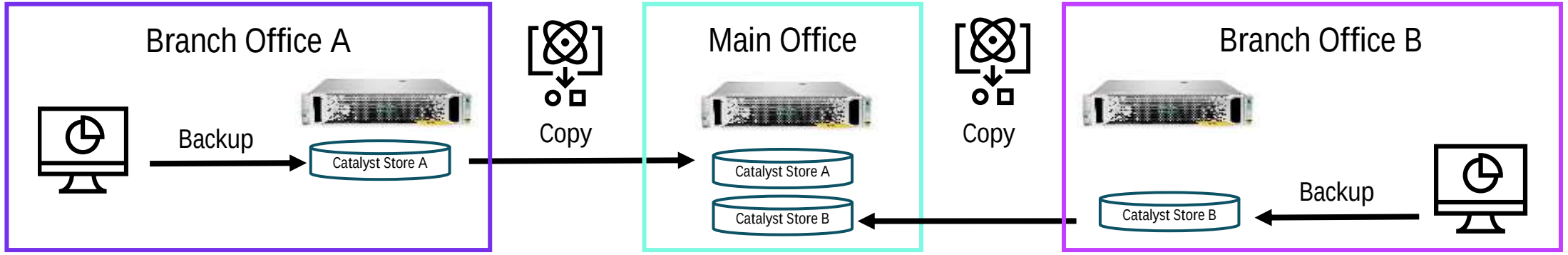
STOREONCE CATALYST AND RMC INTEGRATE WITH APPLICATIONS AND BACKUP SOFTWARE

Simple



CATALYST COPY AND REPLICATION

- Catalyst Copy
  - Is a way of making copies of specific Catalyst items between Catalyst stores
  - Can be directly controlled by the Catalyst Copy Utility or by backup software that supports Catalyst Copy
    - When supported, backup software is aware of all copies and manages lifecycle of all copies; for example, allows local backups to be managed independently from remote copies
  - Uses StoreOnce deduplication to significantly reduce the amount of data that needs to be replicated
  - Can be performed over 1/10/25 GbE networks (CoETH) or over Fibre Channel (CoFC)
  - Supports a range of flexible configurations that enable the concurrent movement of data from one site to multiple sites
    - One to one, many to one, and N-way copy (many to many)
  - Can cascade data around the enterprise (multi-hop)



RMC RESTORES DATA QUICKLY AFTER A RANSOMWARE ATTACK TO MEET STRINGENT RPOS AND RTOS

Fast

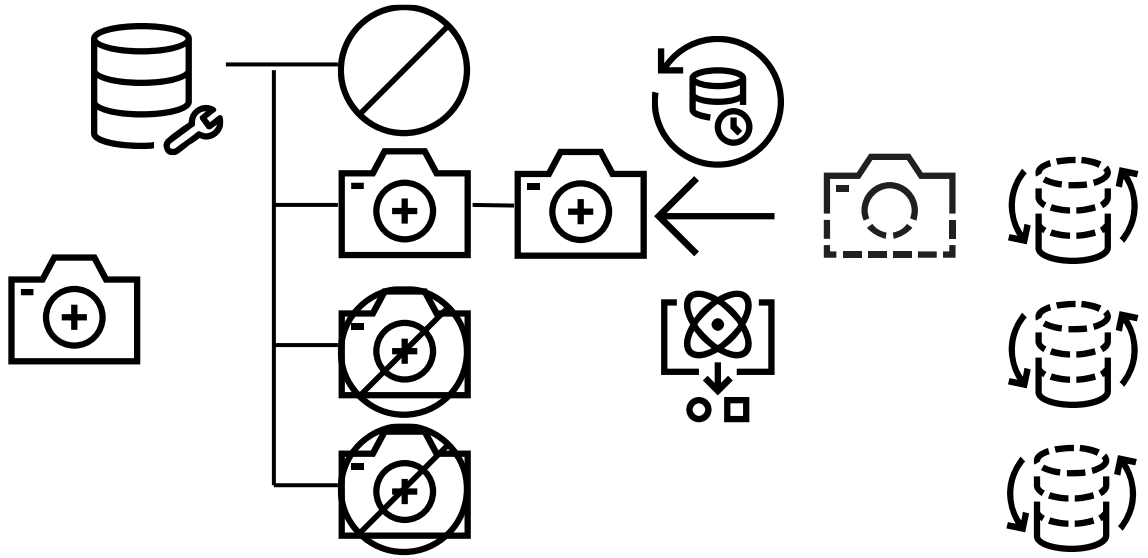
Recover at the speed of flash by only sending unique changed data from StoreOnce to array

Deliver on SLAs with 15x faster recovery* than traditional backup applications

Reduce cost and complexity of traditional recovery approaches with direct restore from 3PAR to StoreOnce

*Compared to traditional server-based backup environments

15x faster restore*



RMC reads only the backup differentials from StoreOnce and moves only the changed blocks from StoreOnce to a target snapshot on 3PAR

HPE RMC AND HPE CLOUD BANK STORAGE
Optional cloud backup

Retain 100 PB[1] + data from $0.001/GB/month[2]

Economic
Low-cost, scalable, long-term retention

Efficient
Ability to send, store, and retrieve **only unique** data for lower TCO

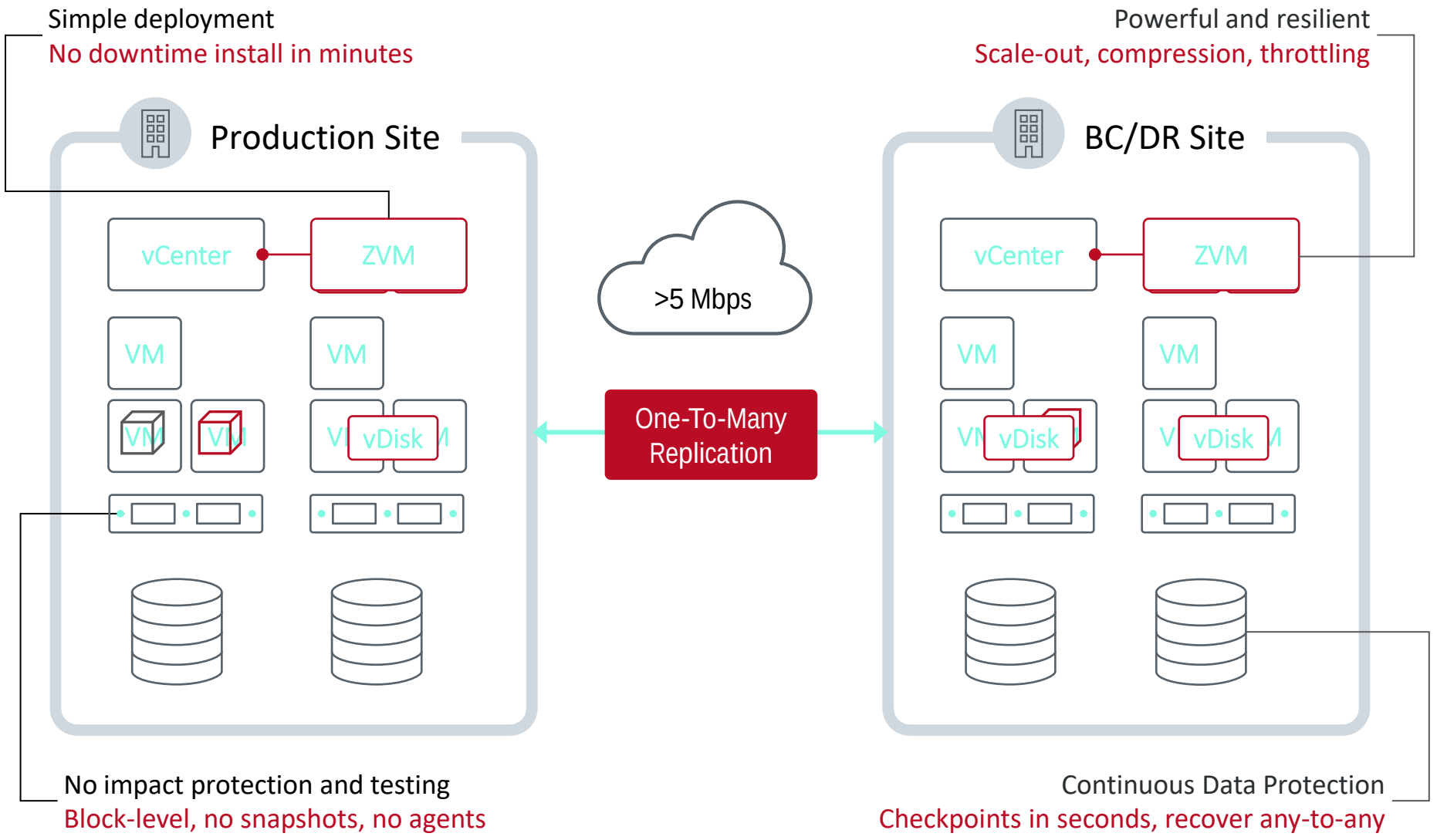
Flexible
Automated, native tiering of backup data to the cloud platform of your choice

Secure
Simple, encrypted, and reliable cloud disaster recovery

[1]Assuming dedupe ratio of 20:1 and the maximum logical capacity of StoreOnce 6600 of 34 PB

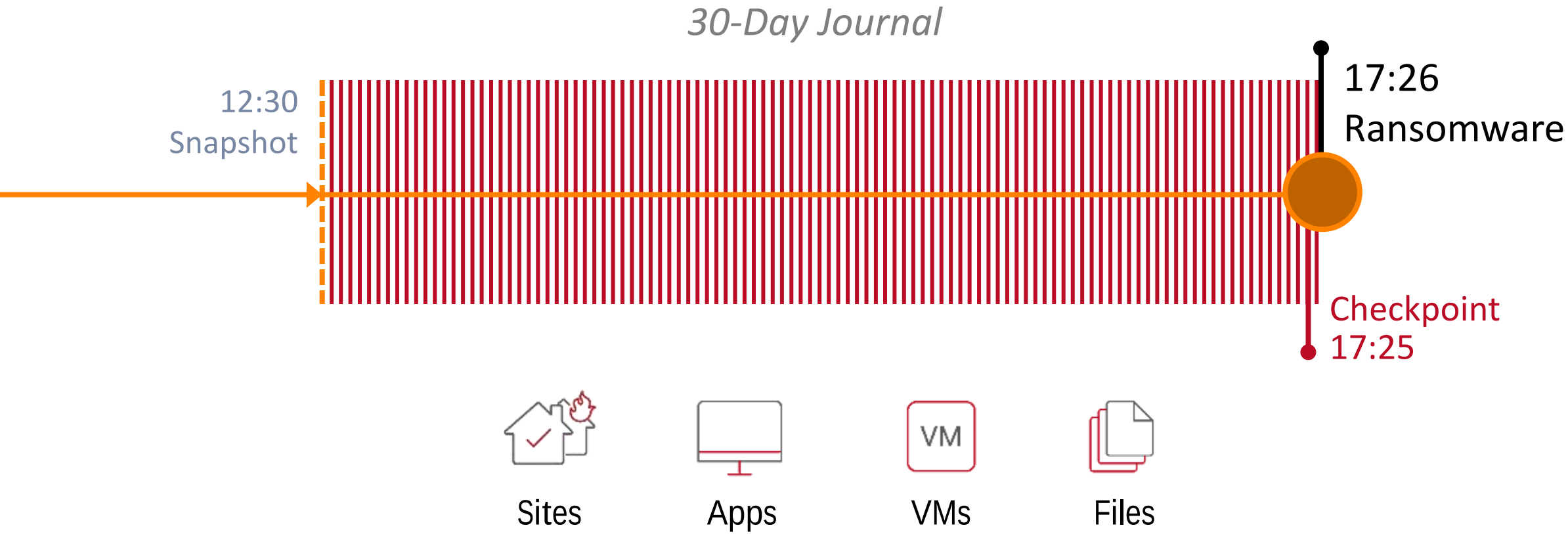
[2]Assuming dedupe ratio of 20:1 and AWS (S3) standard object storage pricing of $0.02 per GB per month

ZERTO CONTINUOUS DATA REPLICATION+AUTOMATED DISASTER RECOVERY

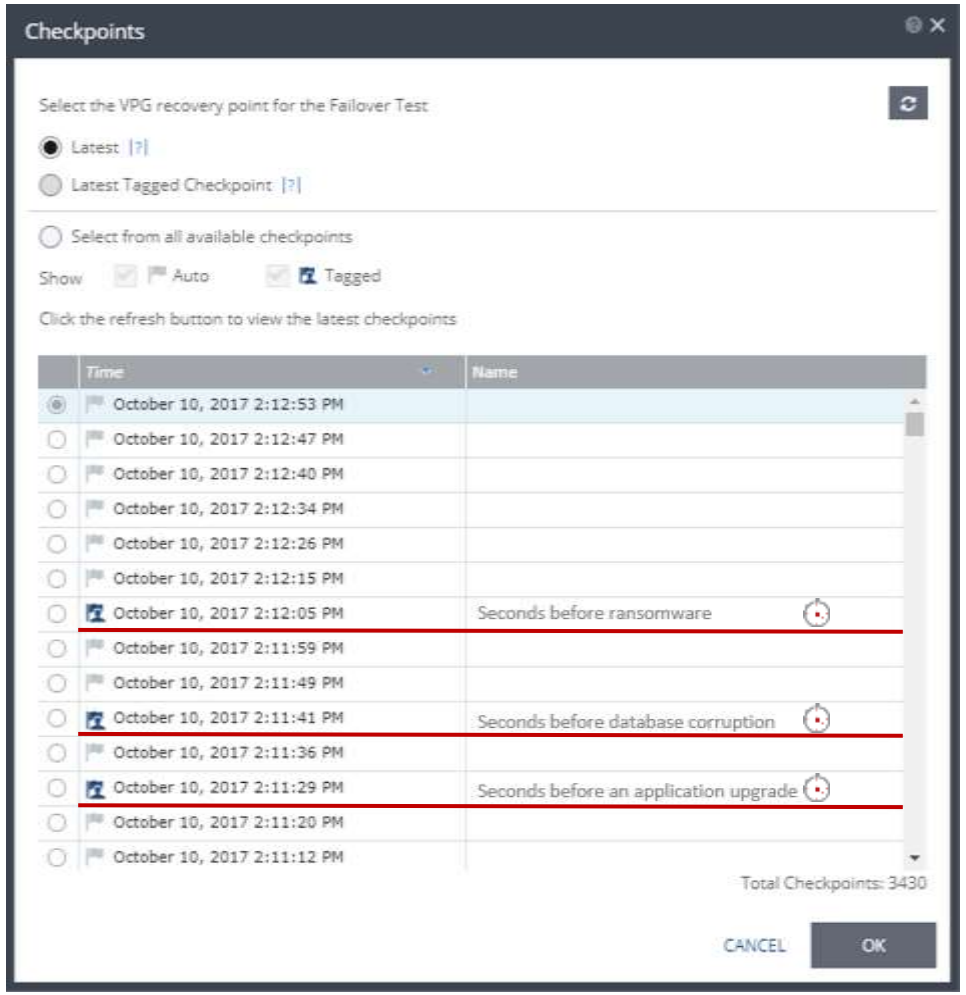


ZERTO JOURNAL-BASED RECOVERY

Rewind and recover from any point in time

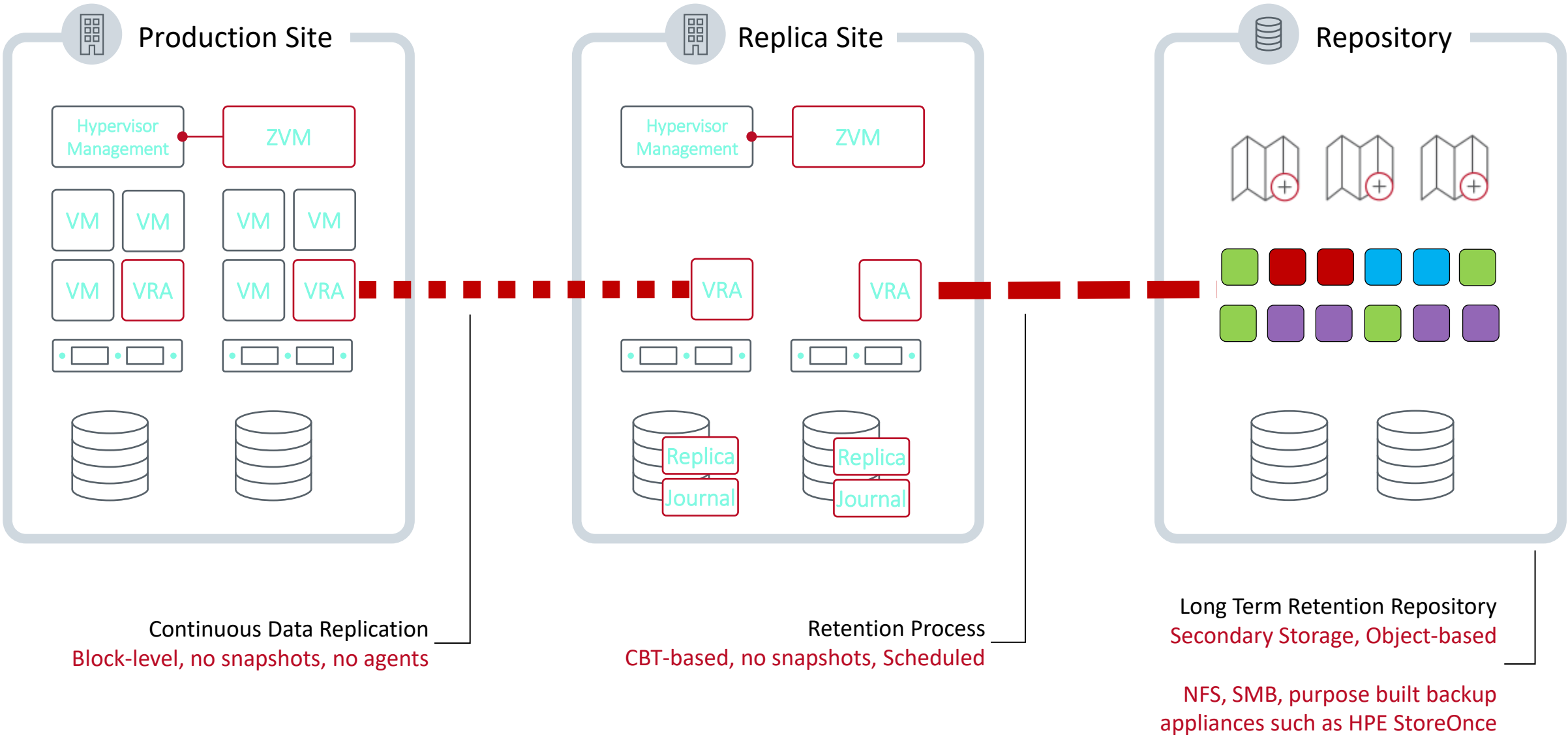


ZERTO JOURNAL-BASED RECOVERY



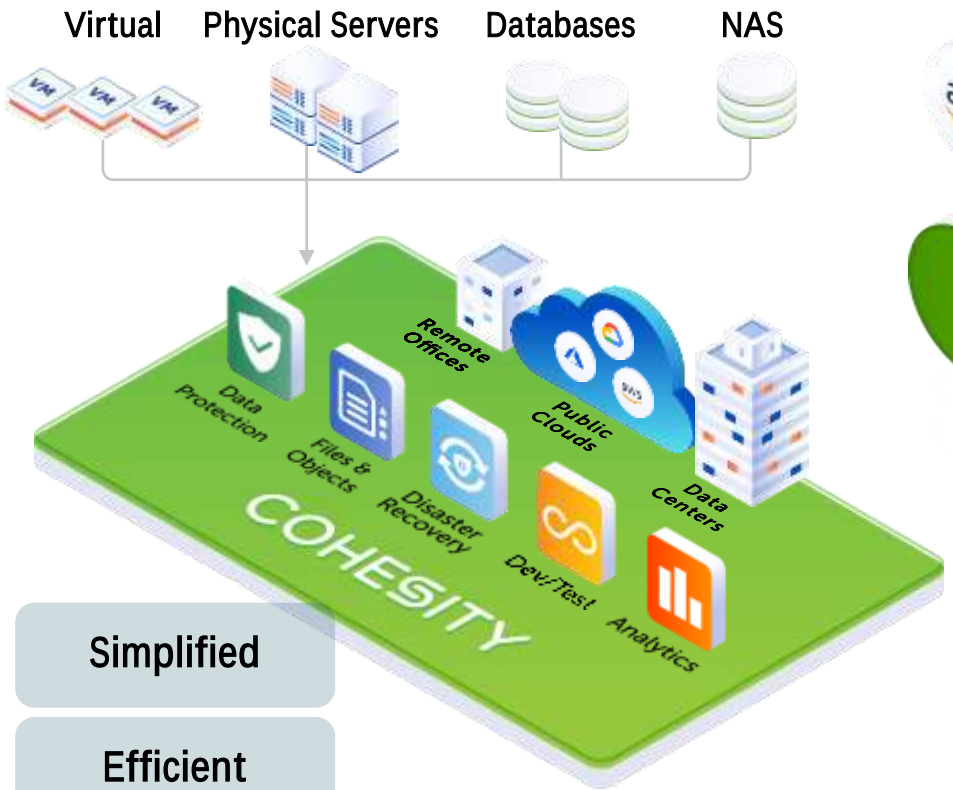
- Simply rewind to any point in time
- Protection against logical failures
  - Not just disasters
- Recover from seconds ago
  - Not the last backup or snapshot
- Application consistency
  - With write-order fidelity
- Recover multi-VM apps consistently
  - Down to the second

ZERTO ELASTIC JOURNAL - ARCHITECTURE



COHESITY - REDEFINING BACKUP AND DATA MANAGEMENT

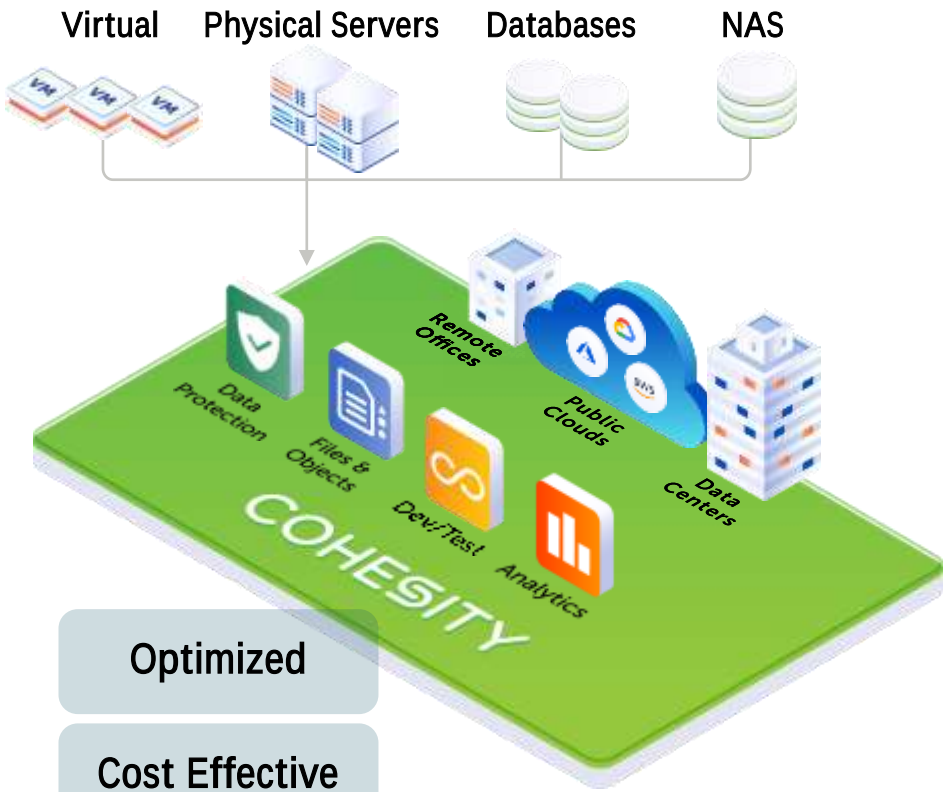
Production



- Simplified
- Efficient
- Immutable

Hybrid & Multi-Cloud

Disaster Recovery



- Optimized
- Cost Effective
- Scalable

COHESITY'S APPROACH TO ANTI-RANSOMWARE

ARCHITECTURE MATTERS

1 DEFEND BACKUP

- Immutable backup
- WORM (DataLock)
- RBAC/MFA
- Encryption framework
- Data isolation

2 DETECT

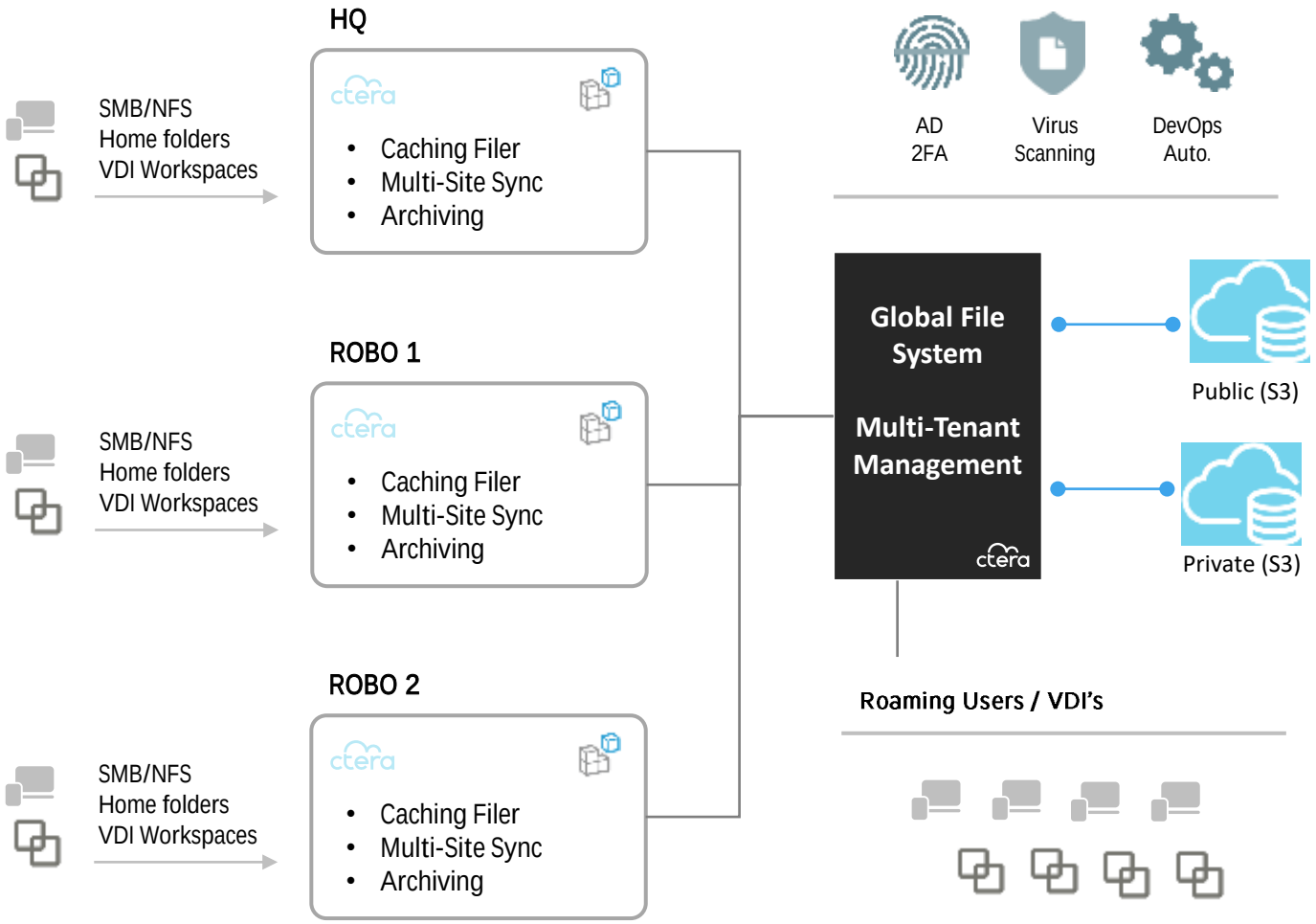
- Machine learning-based detection

3 REDUCE DOWNTIME

- Machine learning-based recommendation
- Discover vulnerabilities (CyberScan)
- Restore at scale

CTERA - MODERN DISTRIBUTED FILE SERVICES

- Unified Solution for HQ, ROBO, Roaming Users & VDI
- Replaces Legacy NAS & Backup Systems
- Perfect for VDI File Storage
- Scalable to Thousands of Sites & Users
- Maximum Security
- Centrally Managed

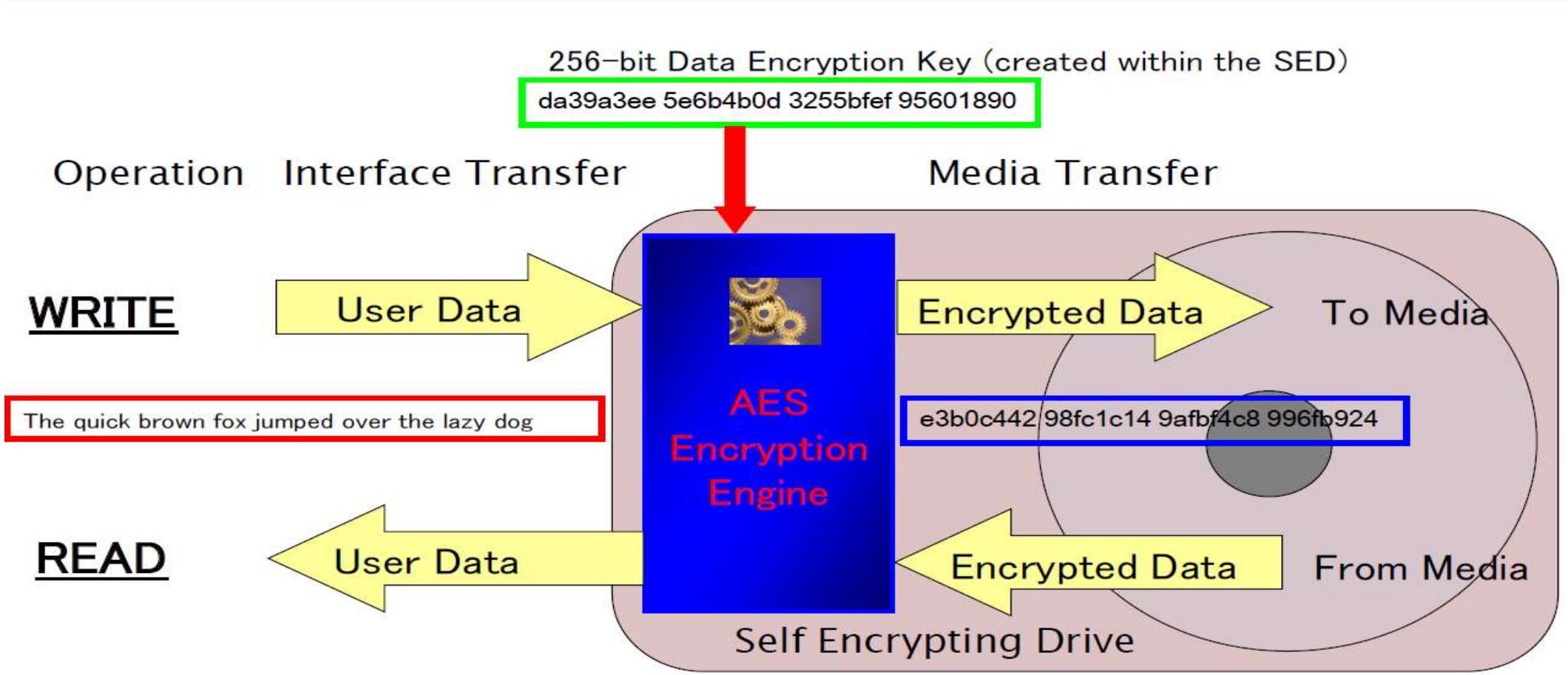


SELF ENCRYPTING DRIVES IN STORAGE AND SERVERS

Encryption keys

- Self-Encrypting Drives contain special firmware and an ASIC that provides encryption.
- The ASIC on the drive provides for full interface speed encryption so there are no data delays.
- The drives are Closed Encryption Devices
  - Each drive has it's own encryption key that never leaves the drive, but can be changed
  - The drive exposes an open interface (datastore) for authentication key management which is handled at the array level
  - All data on the disk is encrypted (full disk encryption)
  - Uses AES 256 encryption standard
  - Enables instant and secure erasure of the SED (cryptograpic erase)
    - Accomplished by changing the drive encryption key rendering the data unintelligible

SELF ENCRYPTING DRIVES



СЕРВІС DMR – DEFECTIVE MEDIA RETENTION

- Диски та, опціонально, інші носії інформації залишаються у вас після заміни.

ЧОМУ HPE ДЛЯ БОРОТЬБИ З RANSOMWARE?

Secure

Operating system

Secondary storage

StoreOnce with Catalyst

Simple

ISV and app integrations

RMC and StoreOnce Catalyst

vmware · ORACLE · SAP HANA · Microsoft SQL Server · Microsoft apps using VSS · VEEAM · MICRO FOCUS · VERITAS

Management integration

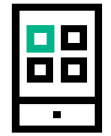
RMC and 3PAR SSMC

HPE PRIMERA

HPE Nimble**

Fast

15x faster restore*



Minimal application impact

Move to object storage (on-premises or cloud)

ДЯКУЮ!

Vasyl.Vizgin@hpe.ua