GAPP
SYSTEM

Technická opatření vyplývající z NIS2 v praxi

Petr Dvořák

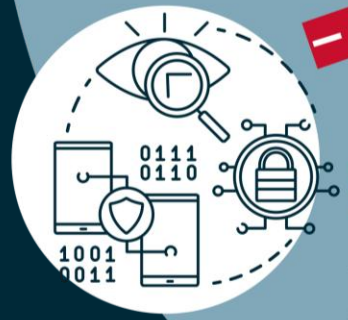
Hotel Jalta, Praha
1. 4. 2025

Ideální IT
JE EFEKTIVNÍ

Každá koruna vynaložená na Vaše IT se Vám musí několikrát vrátit. Infrastruktura navržená na míru bude reflektovat Vaši jedinečnost a Vaše specifika.

Ideální IT
JE AGILNÍ

Ve světě ideálního IT budete dosahovat svých cílů rychleji a snadněji. Klíčem k tomu bude flexibilita Vaší infrastruktury a automatizace rutinních činností.



Ideální IT
JE BEZPEČNÉ

Obavy o bezpečnost budou minulostí. Výrazně zvýšíme míru zabezpečení s využitím těch nejmodernějších technik a zajistíme neustálou dostupnost aplikací.

Ransomware se stále vyvíjí a zdokonaluje

Fáze napadení

Fáze 1: Jak napadaní začíná?

- Kliknutí na přílohu emailu.
- Instalace software obsahující škodlivý kód.
- Využití zranitelnosti některého ze systémů v síti.

Fáze 2: Zašifrování produkčních dat

- Škodlivý kód postupně šifruje data na napadených systémech.
- Dále se snaží rozšířit i na další systémy.
- Šifrovány jsou zpravidla pouze části souborů. Zároveň dochází k dešifrování v reálném čase při jejich čtení, aby celý proces zůstal skrytý.

Fáze 3: Zničení záloh

Pokud umíte data obnovit, nebudete platit výkupné.

- Škodlivý kód šifruje vedle produkčních dat i zálohy.
- Škodlivý kód instaluje keylogger s cílem získat admin oprávnění.
- Hacker přistupuje k systému s admin oprávněním a maže zálohy.

Fáze 4: Požadavek na výkupné.

- Organizace je ve stavu, kdy jsou produkční data zašifrována a zálohy smazány.
- Výkupné je přiměřené velikosti a možnostem organizace.
- Zaplatit ho nedává jistotu, že se vše podaří obnovit. Zároveň může znamenat i reputační dopad.

Co to znamená?

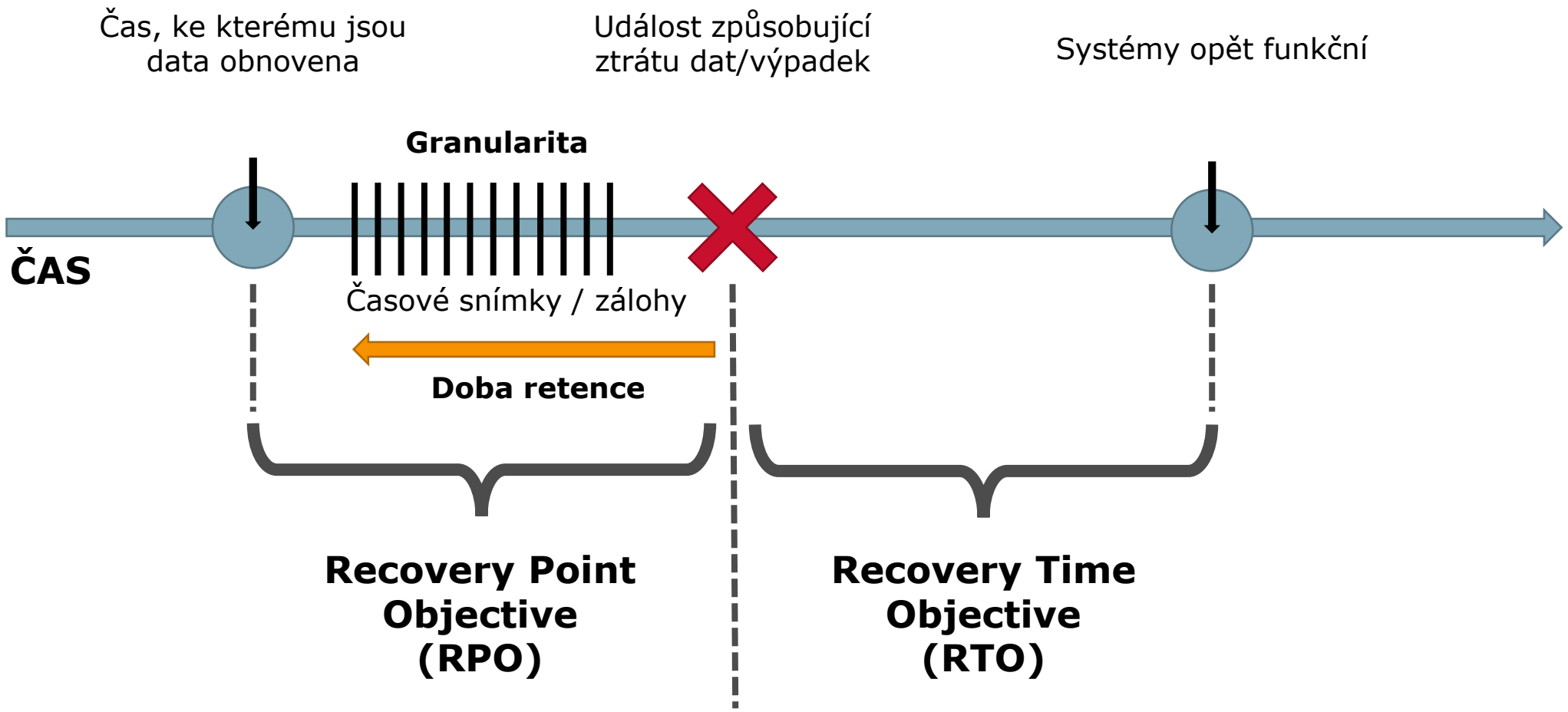
- 100% ochrana je nemožná; každá organizace se může stát obětí.
- Pro úspěšnou obnovu **MUSÍ** být **zálohy a snapshoty adekvátně ochráněny**.
- **Včasná detekce je důležitá**, neboť obnova z příliš starých dat může být nereálná.

Parametry obnovy dat (1)

- **Recovery Time Objective (RTO)**
  - Cílový čas/doba zotavení
  - Čas potřebný k opětovnému zprovoznění systému tak, aby se zabránilo negativním důsledkům spojeným s přerušením jeho chodu
  - Definuje toleranci organizace k zastavení procesů navázaných na systém

- **Recovery Point Objective (RPO)**
  - Cílový bod obnovení/zotavení
  - Čas definující období od incidentu do historie, během kterého mohla být ztracena data
  - Definuje toleranci organizace ke ztrátě dat

Parametry obnovy dat (2)



Východiska pro návrh strategie dle ISO 22301

- 8.2 Analýza dopadů na podnikání a posuzování rizik

  - 8.2.2 Analýza dopadů na podnikání
    - Identifikace činností podporujících „business“
    - Posouzení dopadů v případě jejich nefunkčnosti
    - Stanovení časových rámců pro obnovu činností

  } Recover Point Objective (RPO)
  Recover Time Objective (RTO)

  - 8.2.3 Posuzování rizik
    - Identifikace rizik
    - Analýza rizik
    - Vyhodnocení rizik

} Rizika a jejich ohodnocení

Obnova po incidentu je primárně o tom:

1) mít **kopii dat**, ze které mohu obnovit,

2) mít tato data **kam obnovit**,

3) umět to provést.

GAPP SYSTEM

Dostupná a odolná architektura z pohledu dat

- **Primární infrastruktura**
  - Samostatné servery
  - Hyperkonvergovaná infrastruktura
  - Disková pole

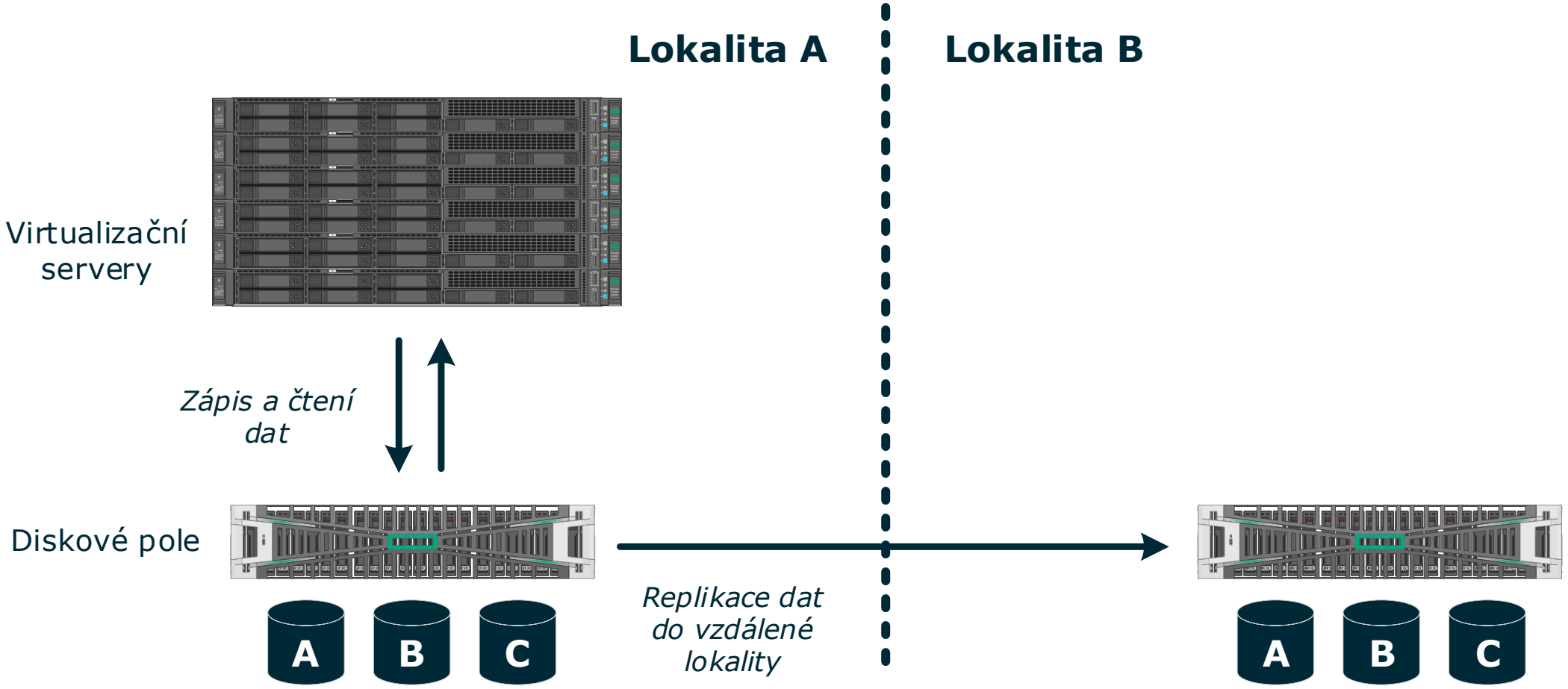
} Technologie přinášející služby zabezpečení dat již v místě jejich primárního uložení

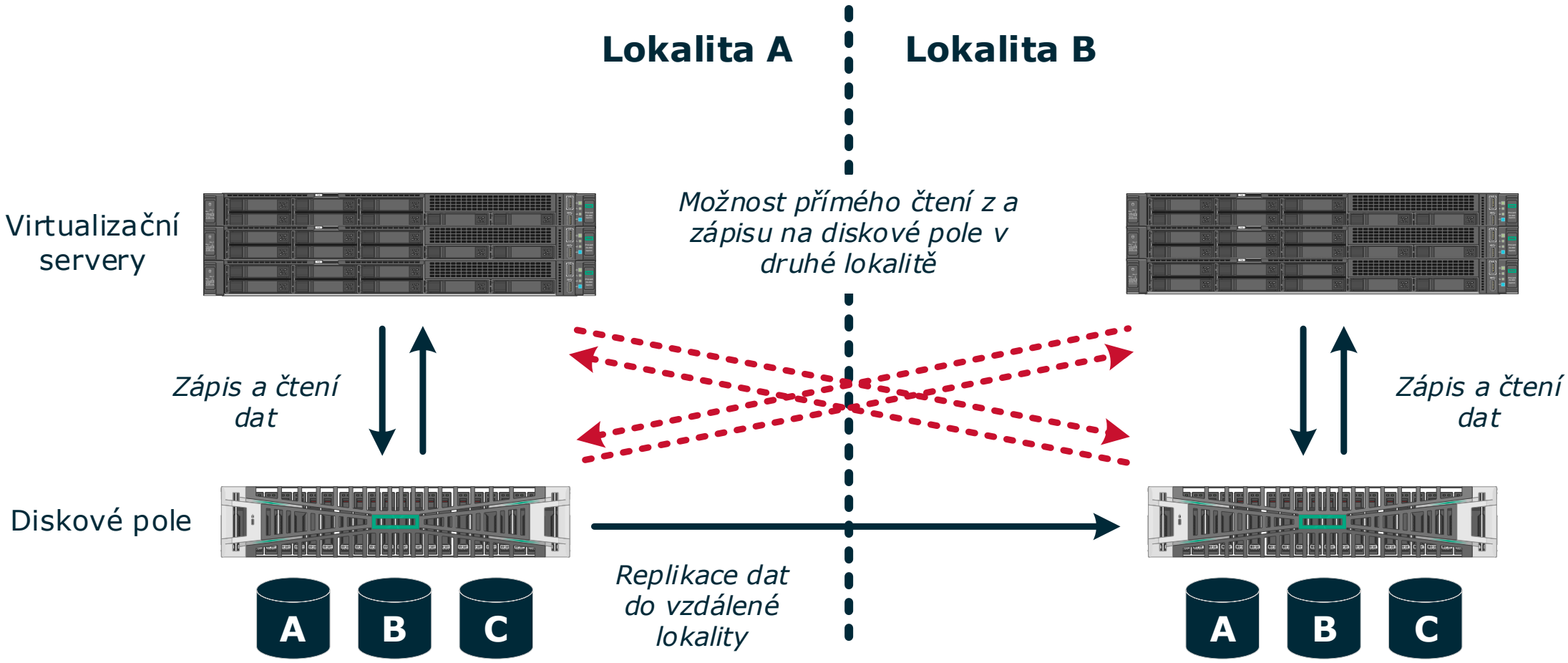
- **Infrastruktura zálohování a obnovy dat** (v širším pojetí)
  - Replikace dat
  - Klasické zálohování dat

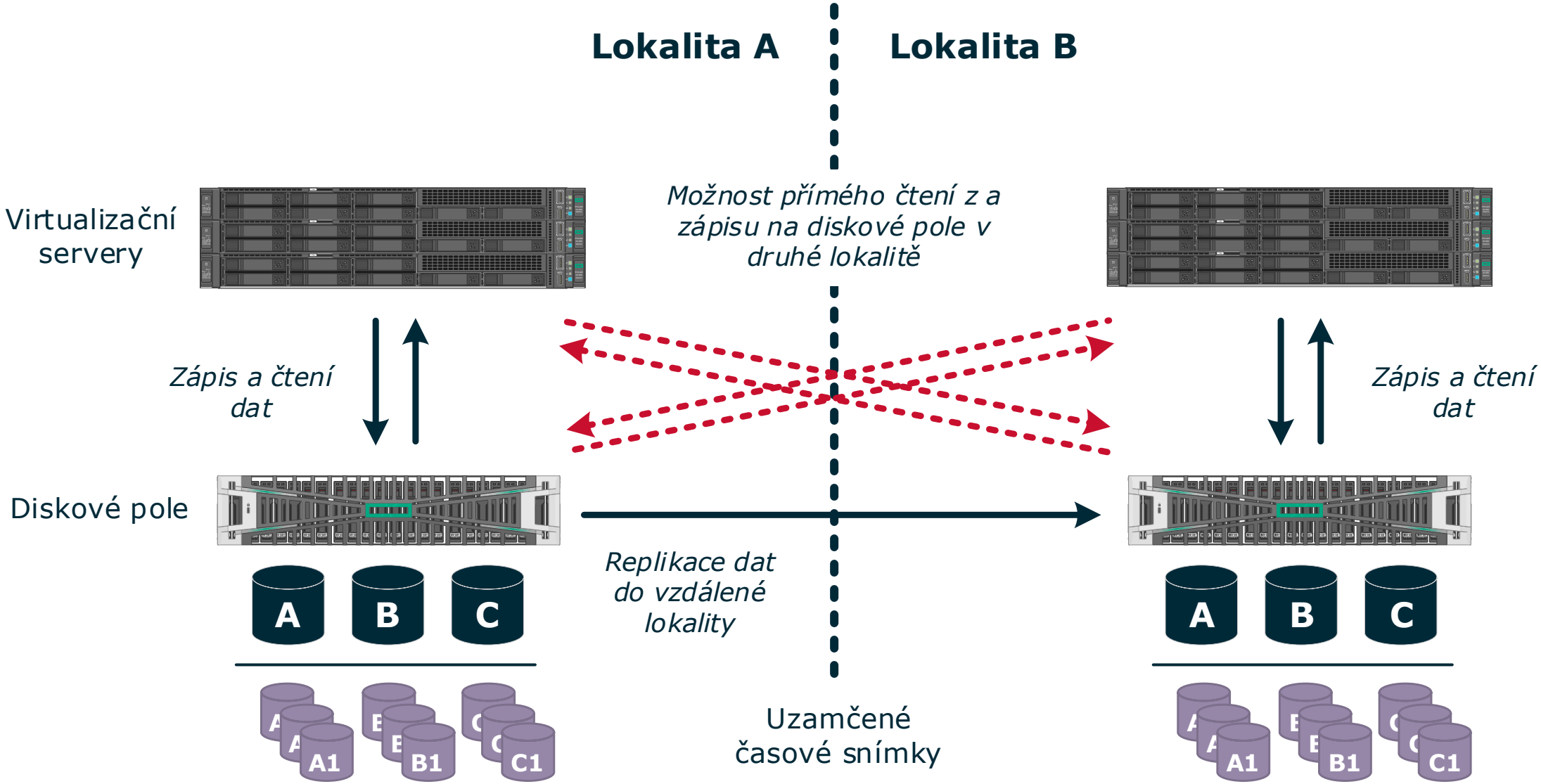
} Technologie pro vytváření kopií dat a jejich zabezpečení

PRIMÁRNÍ ÚLOŽIŠTĚ A ZABEZPEČENÍ DAT

GAPP SYSTEM


Lokalita A
Lokalita B
Virtualizační servery
Zápis a čtení dat
Diskové pole
A
B
C
Replikace dat do vzdálené lokality
A
B
C


Lokalita A
Lokalita B
Virtualizační servery
Možnost přímého čtení z a zápisu na diskové pole v druhé lokalitě
Zápis a čtení dat
Zápis a čtení dat
Diskové pole
A
B
C
Replikace dat do vzdálené lokality
A
B
C


Lokalita A
Lokalita B
Virtualizační servery
Možnost přímého čtení z a zápisu na diskové pole v druhé lokalitě
Zápis a čtení dat
Zápis a čtení dat
Diskové pole
A
B
C
A1
B1
C1
Replikace dat do vzdálené lokality
Uzamčené časové snímky
A
B
C
A1
B1
C1

HPE Alletra MP B10000

- Využitelná kapacita 15 TiB – 5 PiB
- Deduplikace a komprese
- Výkon od 60 000 IOPS (8K Random Mixed 60/40)

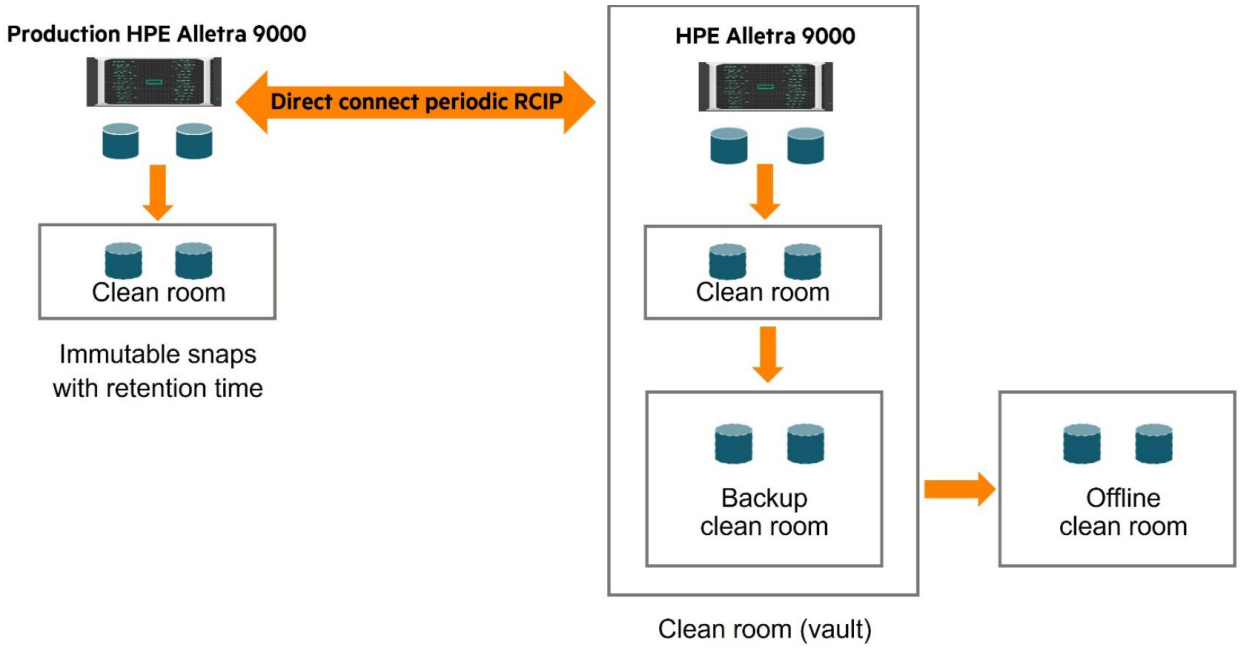
- **Konektivita**
  - Fibre Channel
  - iSCSI
  - NVMeoF/FC

- **Široká škála služeb zabezpečení dat**
  - Synchronní a asynchronní replikace dat
  - **Active Peer Persistance**
  - Snapshoty a klony
  - **Virtual Lock**

Hewlett Packard Enterprise

HPE Virtual Lock

- Optimalizované zabezpečení proti výmazu snapshotů na diskových polích HPE
- Každý Virtual Lock snapshot má definovanou min. dobu retence
- Po tuto dobu není možné snapshot odstranit nebo změnit



Hewlett Packard Enterprise

Zabezpečení na úrovni primárního úložiště

- Vhodný návrh architektury primárního úložiště dat umožňuje zajistit:

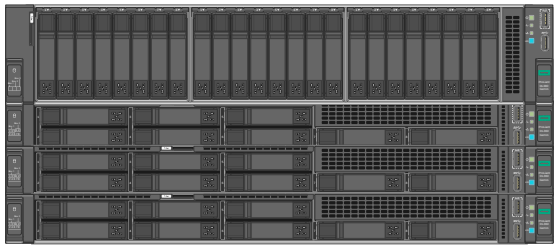
1. **Neustálou dostupnost dat přes více lokalit.**
2. **Vytváření a udržování zabezpečených kopií dat.**
3. **Rychlou obnovu z fyzické i logické chyby.**

- Přesto je nutné mít na paměti, že:
  - snapshoty nejsou plnohodnotnou zálohou.
  - kvalitní a spolehlivý systém zálohování dat má svoji nezastupitelnou roli.

ZÁLOHOVÁNÍ A OBNOVA DAT

GAPP SYSTEM

Virtualizační servery



Řízení systému zálohování dat

Zálohovací server

Bezpečnostní správce

Zálohování dat

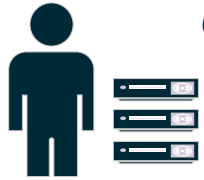
Diskový systém optimalizovaný pro zálohování dat

Replikace záloh do vzdáleného umístění

Datový trezor

Kopie dat na pásky

Pásková knihovna



Odnos fyzických médií do zabezpečené lokality

Kopie dat na pásky

Pásková knihovna

Referenční architektura

- **CommVault Cloud Platform – Backup & Recovery**
  - Complete Data Resiliency Platform
  - Řešení pro zálohování, replikaci a obnovu dat
- **HPE StoreOnce System**
  - Diskový systém optimalizovaný pro ukládání zálohovaných dat
- **HPE StoreEver MSL Tape Library**
  - Magnetopásková knihovna
- **Zálohovací a media agent servery**
  - x86 servery pro řízení řešení a přenos dat

Commvault®

Hewlett Packard Enterprise

Commvault Cloud Platform

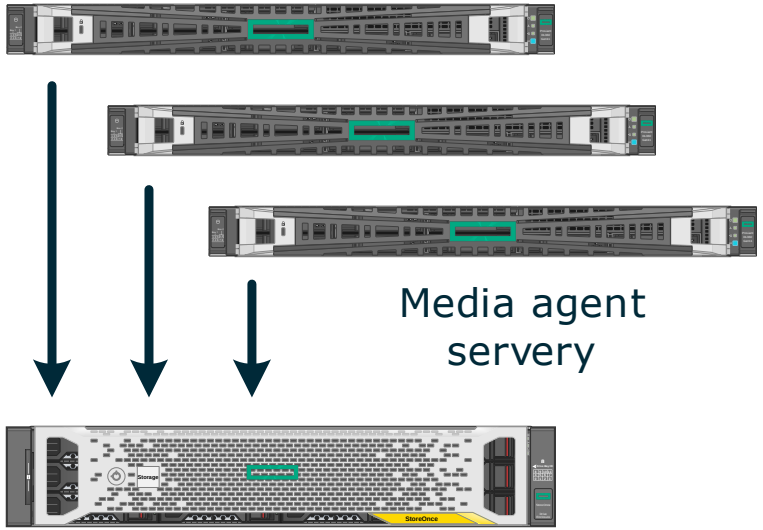
- Komplexní bezpečnostní řešení pro **rychlou obnovu dat a provozu**
- Neobsáhlejší podpora různých platforem, úložišť, operačních systémů a aplikací na trhu
- Poskytuje širokou škálu technologických nástrojů
  - Zálohování a obnova dat
  - Replikace dat
  - Ochrana zálohovaných dat
  - Využití snapshotů diskových polí
  - Identifikace škodlivého kódu

Figure 1: Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Gartner

Commvault®

HPE StoreOnce System



- Datové úložiště **optimalizované pro ukládání zálohovaných dat**
- Od 16 TiB do 1,1 PiB využitelné diskové kapacity
- Inline deduplikace a komprese zálohovaných dat

- **HPE StoreOnce Catalyst**
  - Umožňuje distribuci procesu deduplikace (na zdroji / na cíli)
  - Poskytuje efektivnější integraci úložiště a řešení pro zálohování dat
  - Zvyšuje zabezpečení před napadením datového úložiště škodlivým kódem

HPE Alletra Storage Server 4120

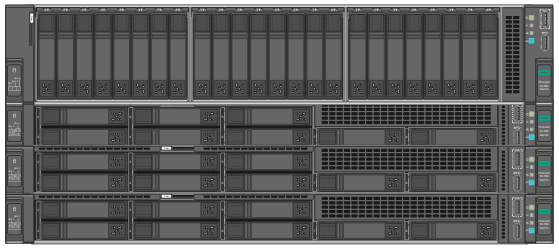
- Ideální server pro **all-in-one** konfiguraci zálohovacího serveru Commvault nebo media server pro uložení další kopie dat

- Stěžejní výhody:
  - Až **24x 3,5" HDD** pro uložení dat
  - **NVMe SSD** pro OS a metadata
  - Až **8x PCIe slot** pro konektivitu

- Při využití 20 TB HDD **až 480 TB v 2U**

Hewlett Packard Enterprise

Virtualizační servery



Řízení systému zálohování dat

Zálohovací server

Bezpečnostní správce

Zálohování dat

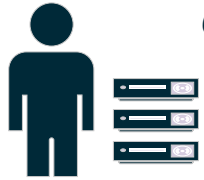
Diskový systém optimalizovaný pro zálohování dat

Replikace záloh do vzdáleného umístění

Datový trezor

Kopie dat na pásky

Pásková knihovna



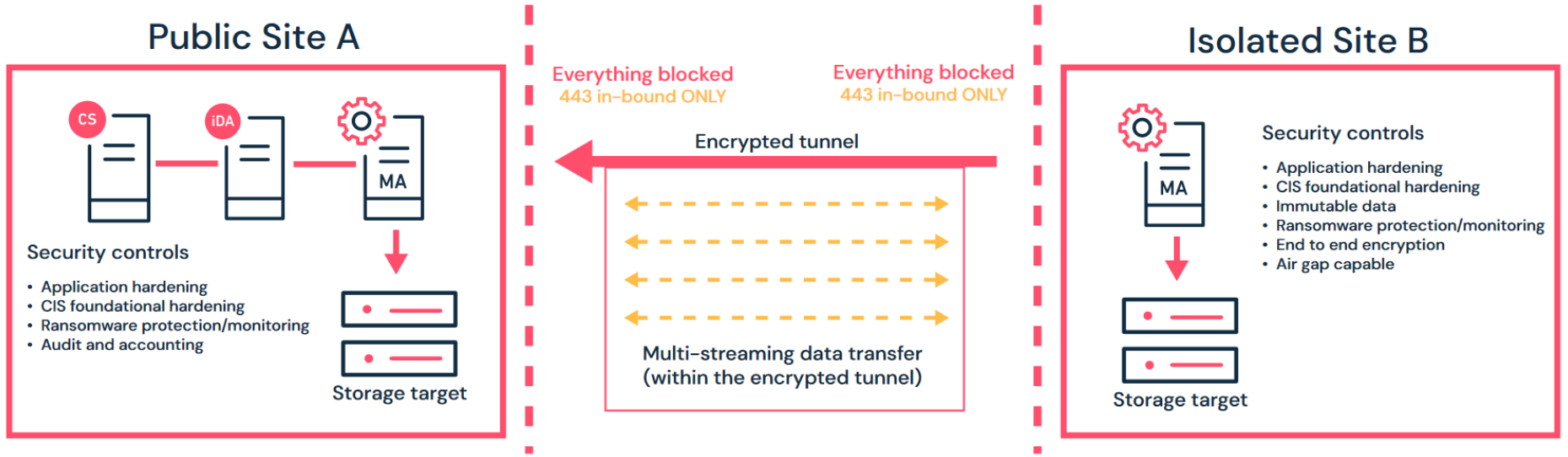
Odnos fyzických médií do zabezpečené lokality

Kopie dat na pásky

Pásková knihovna

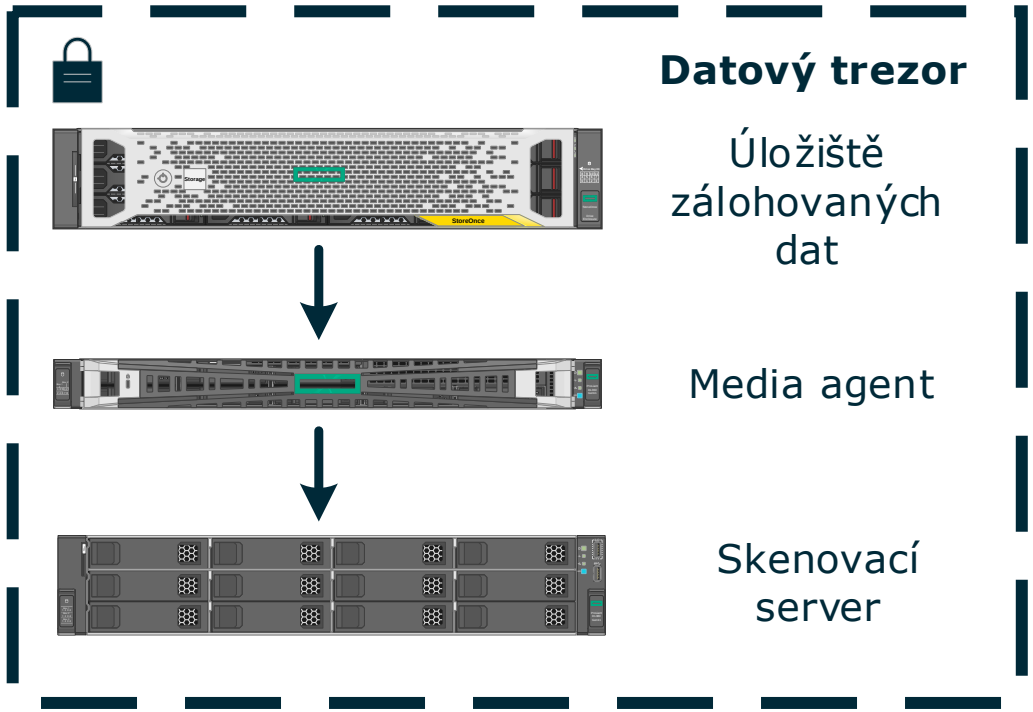
Datový trezor s využitím Air-Gap

- Do datového trezoru nelze navázat **žádné spojení zvenku**
- Datový trezor je umístěn za vyhrazeným firewallem s extrémně restriktivními pravidly
- Všechna spojení jsou navazována z datového trezoru a data jsou přenášena prostřednictvím **šifrovaného tunelu**



Commvault Threat Scan

- Automatizovaná **analýza zálohovaných dat na výskyt malwaru** a dalších podezřelých změn
- Vybraná data jsou obnovena na skenovací server
- Tam je proveden sken na malware, neočekávané šifrování atd.
- V případě výskytu jsou data umístěna do karantény a je reportován výskyt škodlivého kódu



Commvault®

Zabezpečení na úrovni zálohování a obnovy

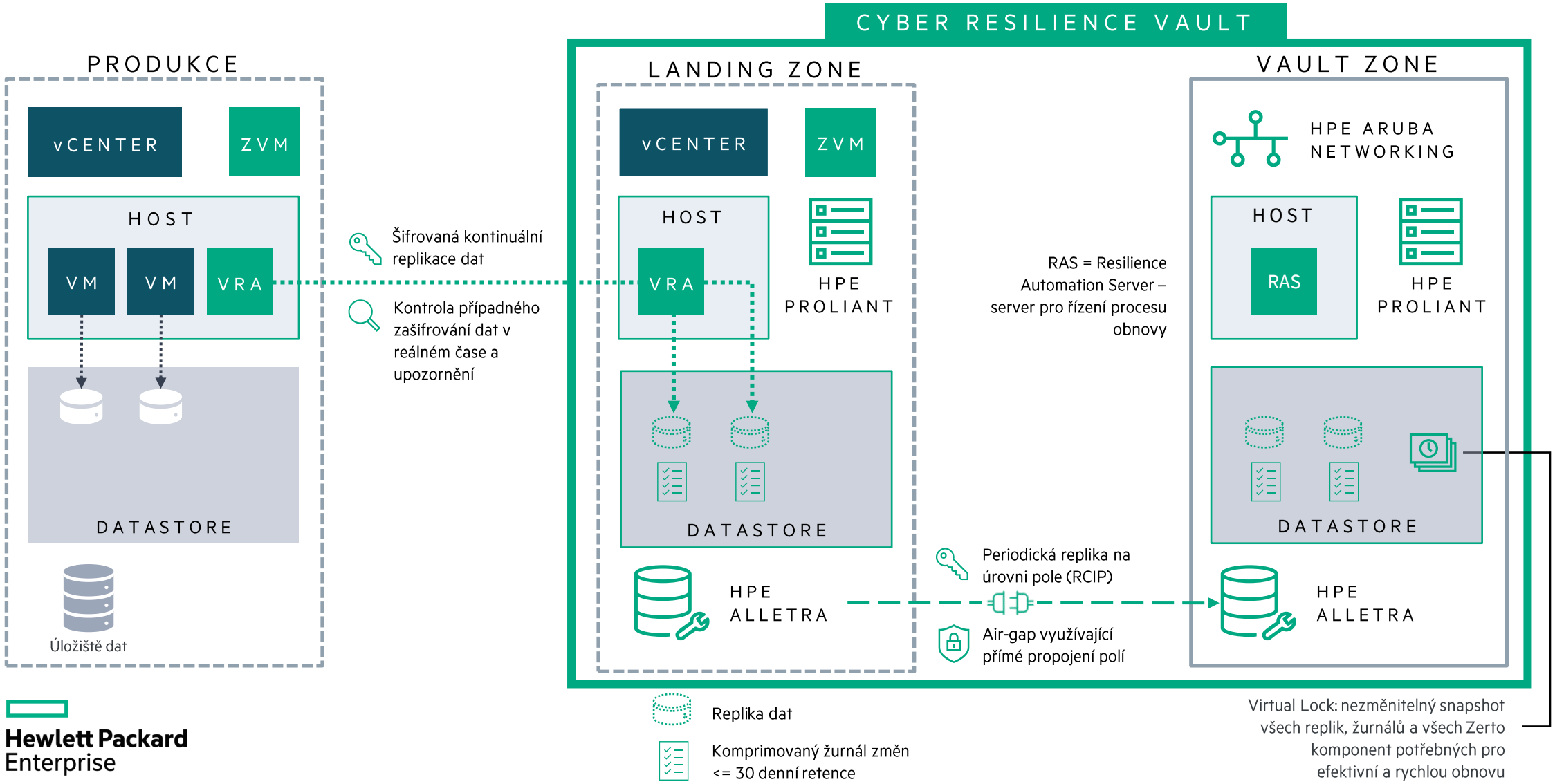
- Vhodný návrh architektury zálohování a obnovy dat umožňuje zajistit:

1. **Garanci, že vždy budeme mít data dostupná k obnově.**
2. **Jistotu, že tato data nebudou kompromitována.**
3. **Komplexní ochranu všech relevantních dat.**

REPLIKACE VIRTUALIZOVANÉHO PROSTŘEDÍ

GAPP SYSTEM

Zerto Cyber Resilience Vault



Hewlett Packard Enterprise

Zabezpečení na úrovni replikace VM

- Vhodný návrh architektury replikace virtualizovaného prostředí umožňuje zajistit:

1. **Garanci, že jsme schopni ihned spustit celé systémy.**
2. **Jistotu, že tato data nebudou kompromitována.**
3. **Vysoce granulární pohyb v čase, ke kterému potřebujeme obnovit.**

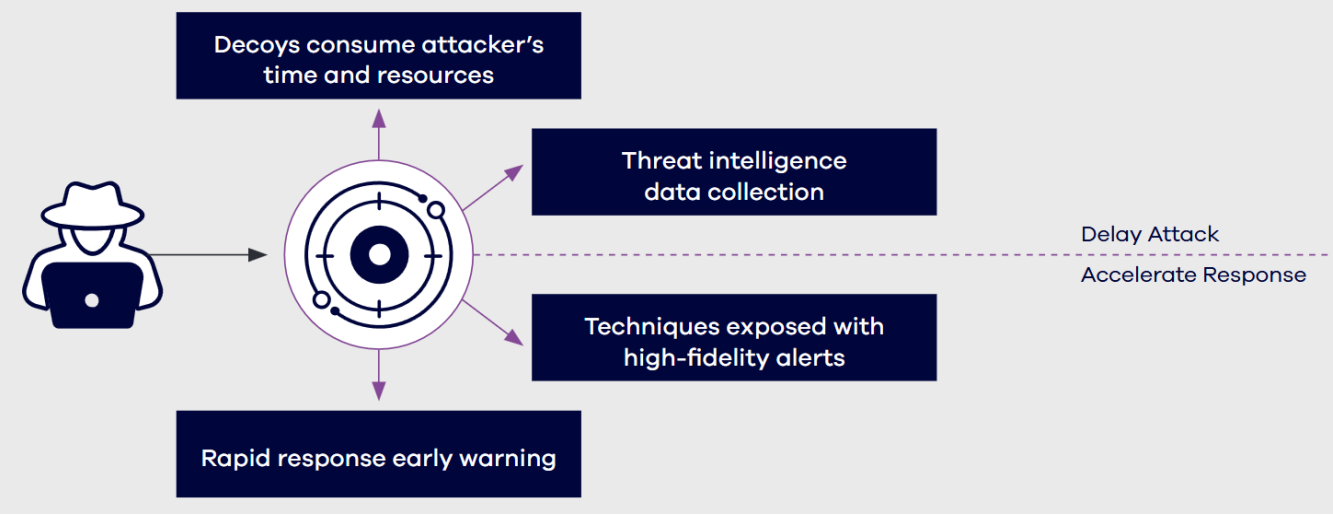
- Přesto je nutné mít na paměti, že:
  - snapshoty nejsou plnohodnotnou zálohou.
  - kvalitní a spolehlivý systém zálohování dat má svoji nezastupitelnou roli.

DALŠÍ OPATŘENÍ PRO ZVÝŠENÍ ODOLNOSTI

GAPP SYSTEM

ThreatWise – zajištění včasné reakce

- Řešení pro včasné odhalení narušení bezpečnosti včetně zero-day útoků na bázi pokročilých honey-potů simulujících reálná zařízení a systémy.
- ThreadWise emuluje nejrůznější zařízení běžně se nacházející v IT prostředí (servery, databáze, přepínače, atd.)
- Následně detekuje pokusy o útoky na ně, ty analyzuje a adekvátně alertuje.



Commvault®

Vydejte se na cestu k ideálnímu IT s námi

Naše společné kroky v realizaci technických opatření pro zvýšení míry bezpečnosti

1. **Příprava celkové strategie zabezpečení.**
2. **Návrh architektury řešení ukládání a zálohování dat.**
3. **Realizace PoC vybraných technologií.**

Standardní služby, které v GAPP System poskytujeme

- **Instalační a implementační služby**
- **Konzultační služby a školení**
- **Služby technické podpory v rozsahu 7x24 včetně podpory proaktivní**

Děkuji za pozornost

Petr Dvořák
+420 602 150 352
petr.dvorak@gapp.cz