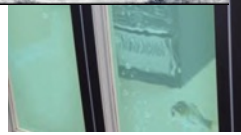
HITACHI
Inspire the Next

Hitachi Vantara Cyber Resilience Solutions

Andrej Gursky
Solutions Consultant CEE, Hitachi Vantara
October 2022

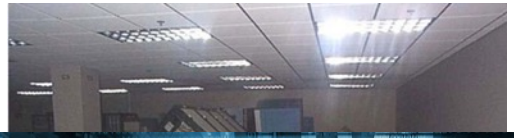
Many things can disrupt your operations

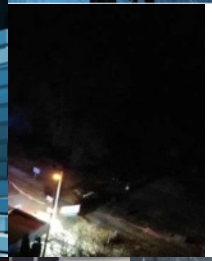
HITACHI
Inspire the Next



Many things can disrupt your operations

HITACHI
Inspire the Next





HITACHI
Inspire the Next

Cyber Resilience
Definition & Approach

Cyber resilience principles

HITACHI
Inspire the Next

Immutability

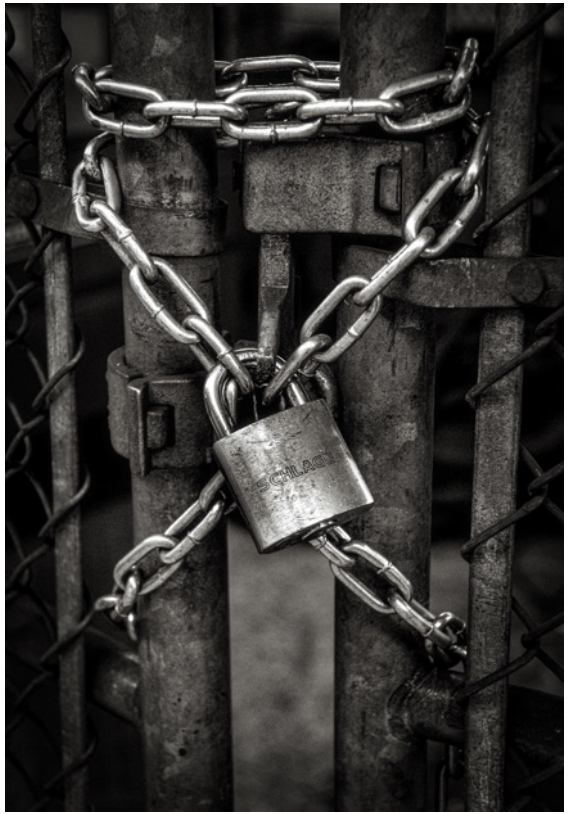
Something that is unable to be changed

Air Gap

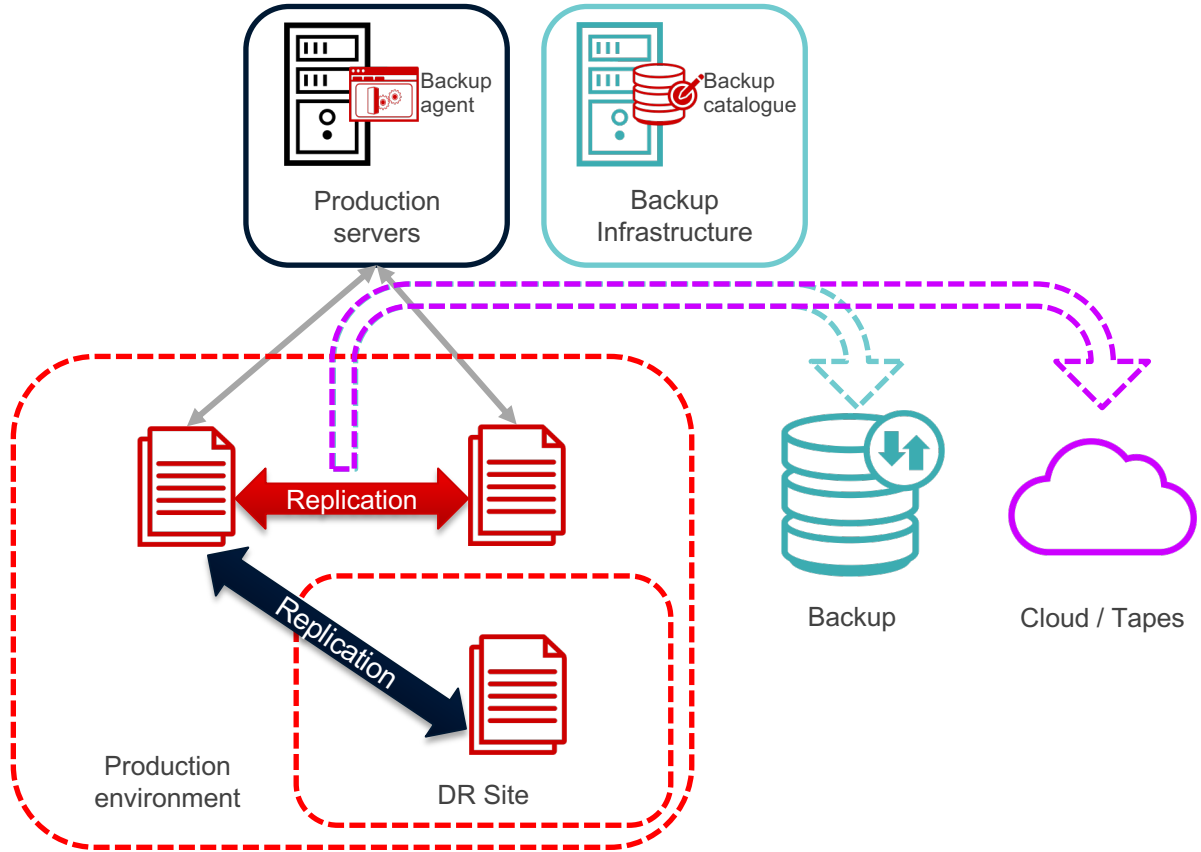
An air gap is the idea of **creating a barrier** between something that has to be protected and a hypothetical cyber threats. An air gap can be either logical or physical

Data Retention

Setting a retention to a data will make **deletion impossible** during the retention period



Traditional Approach



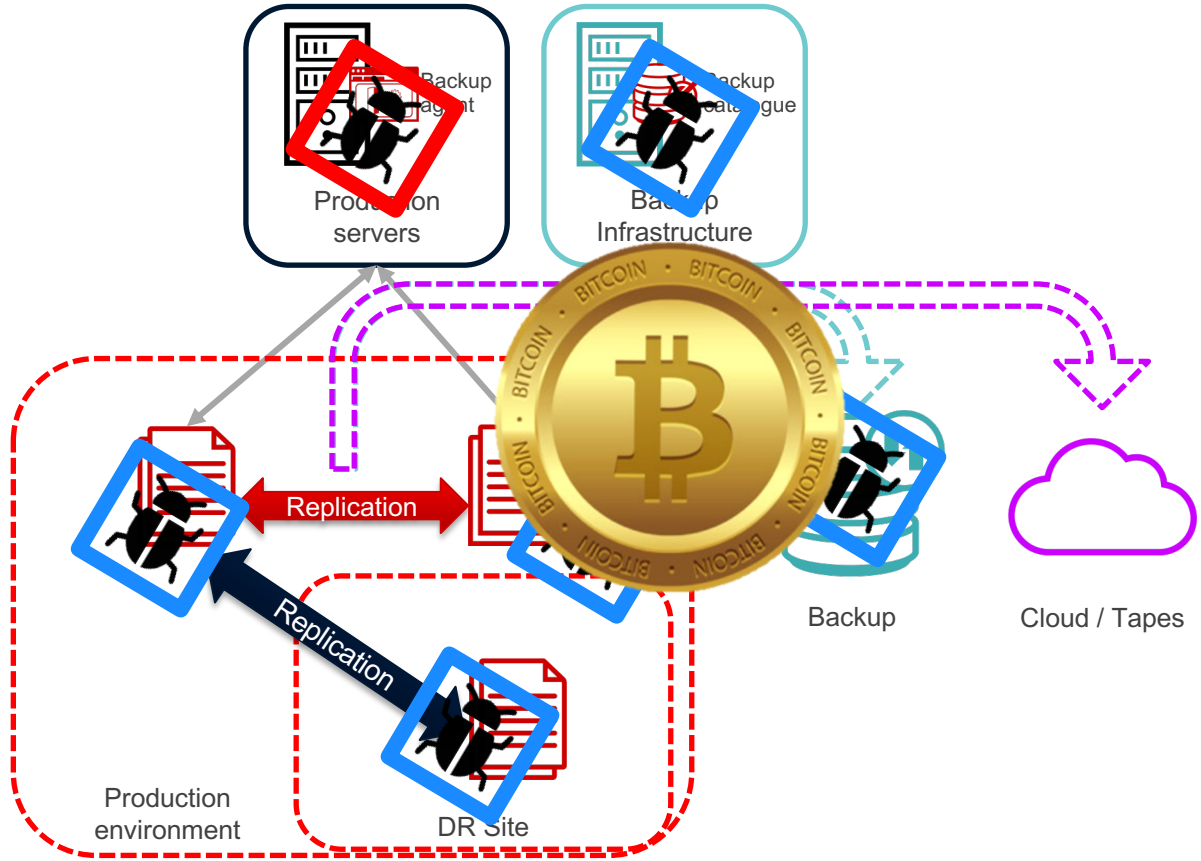
Backup applications usually copy data to cheaper '**secondary storage**'. Sometimes backup data is tiered to even cheaper long-term storage / tape / cloud for **long-term protection**

A **backup agent** is used to gather the data and sometimes quiesce applications to ensure data consistency

The **catalog** is necessary to understand the backup data. It stores metadata such as when the backup was taken, from which host, and metadata about the files themselves

Cyber attack overview

HITACHI
Inspire the Next



Example of a ransomware attack

1. **Campaign**
   Reconnaissance and information gathering
2. **Infection / penetration**
   Gain access to the target
3. **Analysis and discovery**
   Deep comprehension of target's architecture, protections etc.
4. **Spoliation and encryption**
   Alter restore mechanisms
   Encrypt target data
   Wipe archives
5. **Ransom**
   Issue ransom demands

Then we just have to pay, isn't it ?

HITACHI
Inspire the Next

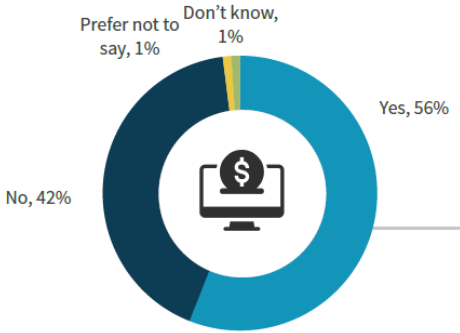
Paying Ransom Doesn't Guarantee Data Recovery

More than half (56%) of organizations that have been victimized by a successful ransomware attack at some point admit to having paid a ransom to regain access to data, applications, or systems. However, it's not necessarily a solution that works effectively as paying the ransom does not guarantee the recovery of data. Indeed, only one in seven reported getting all their data back post payment. So, paying the ransom encourages further "bad behavior" in the form of demanding additional ransoms, and fails to guarantee seamless business resumption overall, including recovering from data loss and other operational consequences.

ONLY 1 IN 7

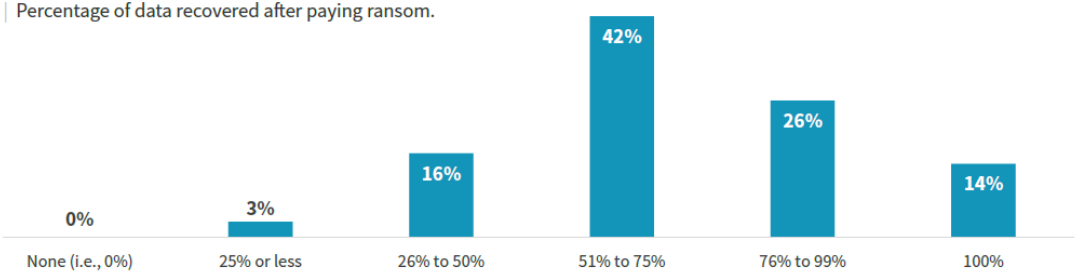
reported getting all their data back post payment.

Have organizations paid ransoms resulting from successful attacks?



More than half of organizations that have been victimized by a successful ransomware attack at some point admit to having paid a ransom to regain access to data, applications, or systems."

Percentage of data recovered after paying ransom.



Back to Contents

Then we just have to pay, isn't it ?

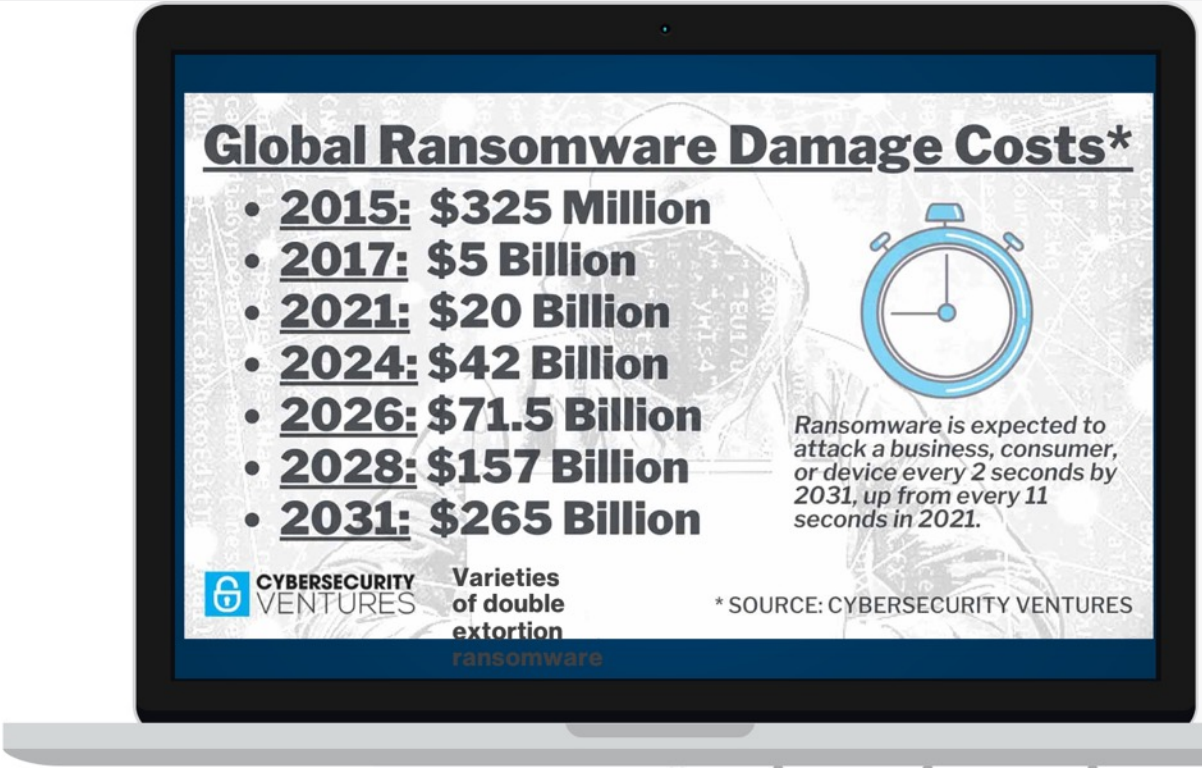
HITACHI
Inspire the Next

Paying Ransom Doesn't Guarantee Data Recovery

More than half (56%) of organizations that have been victimized by a successful ransomware attack at some point admit to having paid a ransom to regain access to data, applications, or systems. However, it's not necessarily a solution that works effectively as paying the ransom does not guarantee the recovery of data. Indeed, only one in seven reported getting all their data back post payment. So, paying the ransom encourages further "bad behavior" in the form of demanding additional ransoms, and fails to guarantee seamless business resumption overall, including recovering from data loss and other operational consequences.

ONLY 1 IN 7

reported getting all their data back post payment.

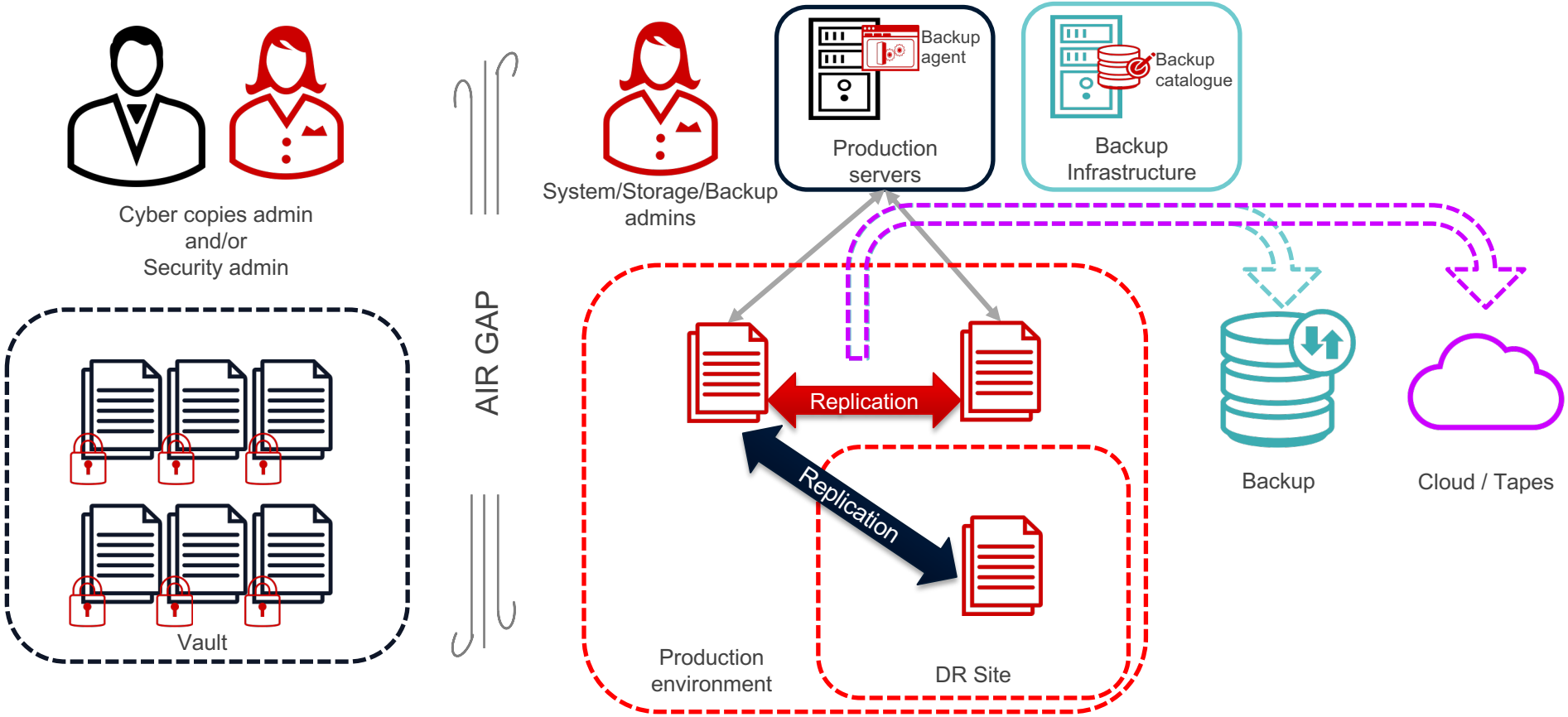


80% of those who paid a ransom experienced another attack

Back to Contents

How to protect data against Cyber Threats ?

HITACHI
Inspire the Next



Hitachi Cyber Resiliency defense approach

HITACHI
Inspire the Next

- Ops Center Analyzer
- Managed Cybersecurity Services

- Identify critical data
- Create protected copies and/or backups
- Air gap isolation

- Data verification and forensics
- Recovery through embedded copy mechanism

Disclaimer

HITACHI
Inspire the Next

- There is **no turnkey solution**, to fit to each organization's needs
- Hitachi Vantara can propose a multi layer approach solution. We have a complete toolbox, so let's be creative !

  - **BLOCK** solutions
  - **FILE** solutions
  - **OBJECT** solutions
  - Automation
  - Managed Services

- It's a multilayer approach, discussion should be started arround protection, backup, etc.

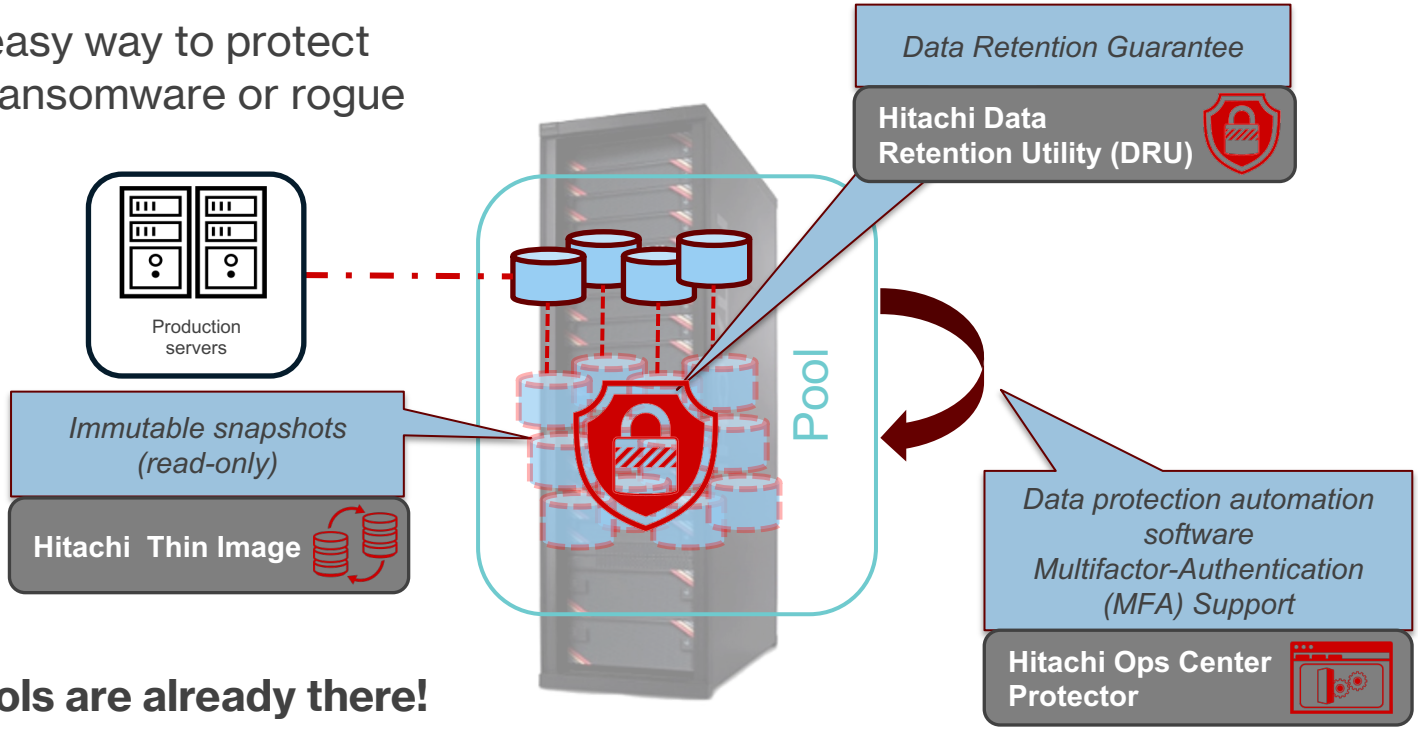
HITACHI
Inspire the Next

Hitachi Cyber Resilience
Examples for Block Storage

Hitachi Cyber Resiliency solution – for Block

HITACHI
Inspire the Next

- If only there were an easy way to protect primary data against ransomware or rogue administrator .....



All the requested tools are already there!

Hitachi Ops Center Protector

HITACHI
Inspire the Next

Simplify Protection and Recovery

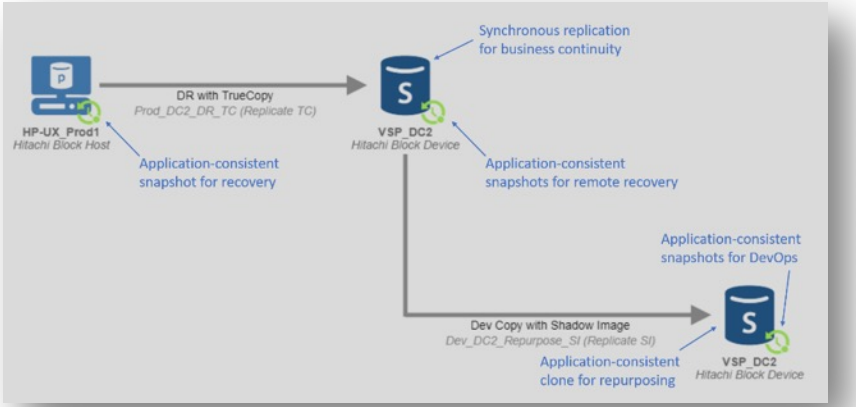
Automate and orchestrate the high-performance snapshot and replication technologies built into all Hitachi VSP arrays

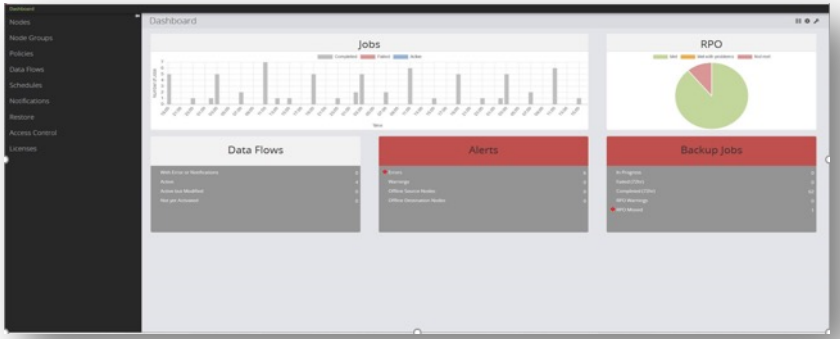
Policy-Based Workflows

Use the right tool for each job and combine them to meet complex service level objectives

Support Secondary Functions

Protector makes it easy to automatically create, refresh, and control copies of production data for DevOps, Finance, and more

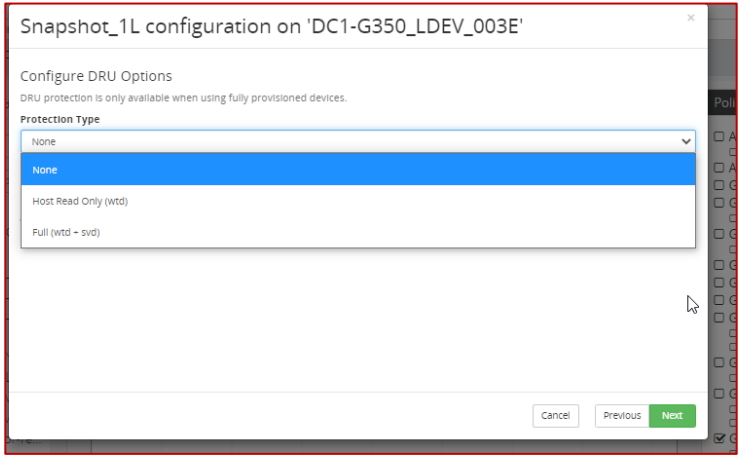


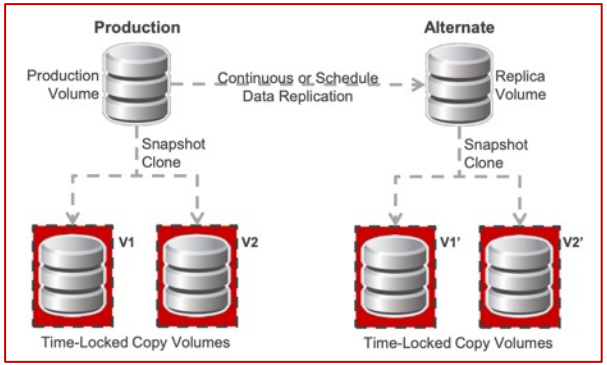


Hitachi Data Retention Utility

HITACHI
Inspire the Next

- Undo damage by ransomware attacks in seconds
- Fully integrated component of all VSP arrays
- Can be orchestrated with Ops Center Protector
- Locks down copies of production data for a defined period of time
- Data cannot be deleted, edited or encrypted during the retention period
- Retention locks cannot be removed prior to a specified retention period even by a system administrator or even by Hitachi engineers

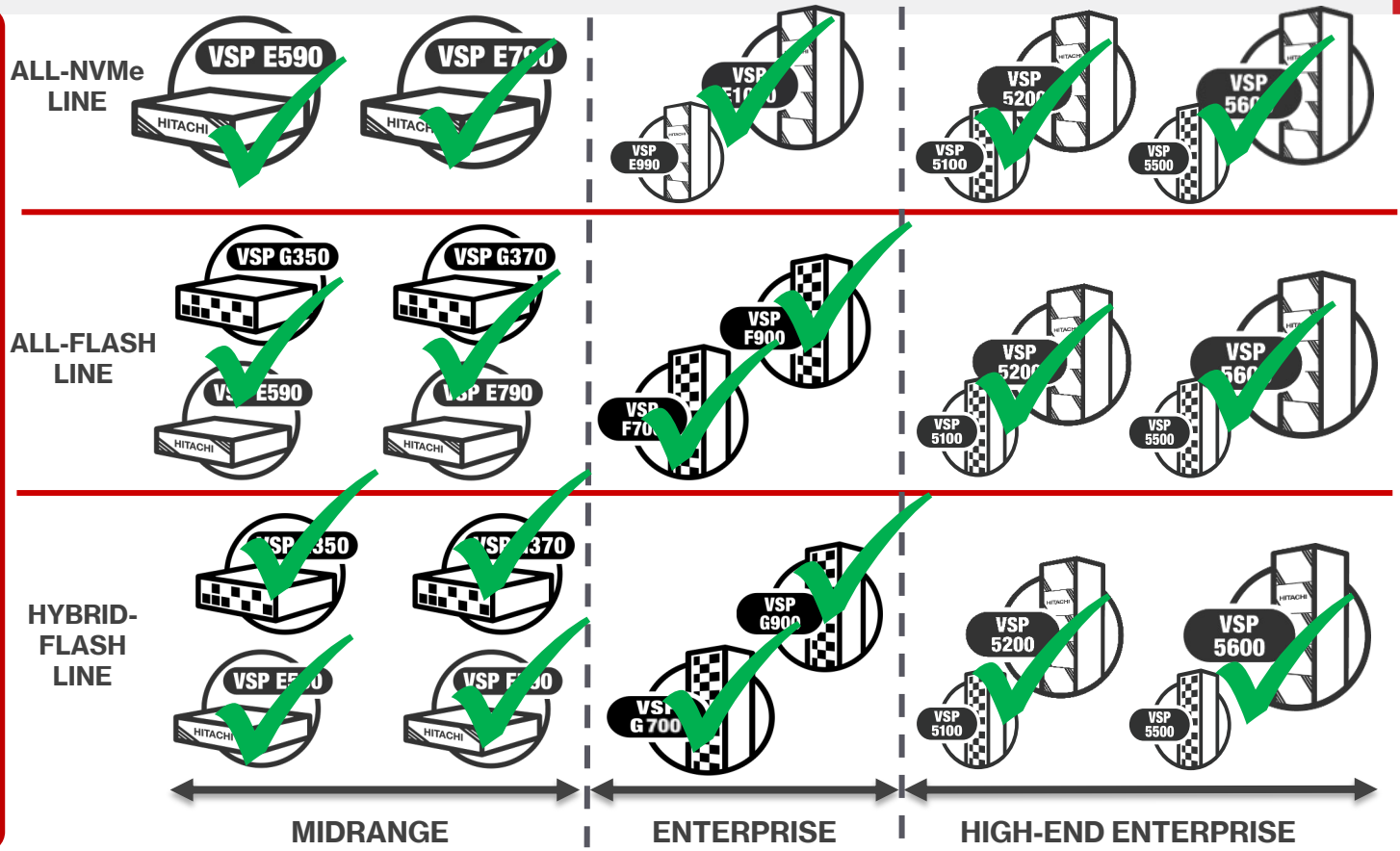




Supported with whole VSP Family

HITACHI
Inspire the Next

Common Operating System
Common Ops Center Software Portfolio

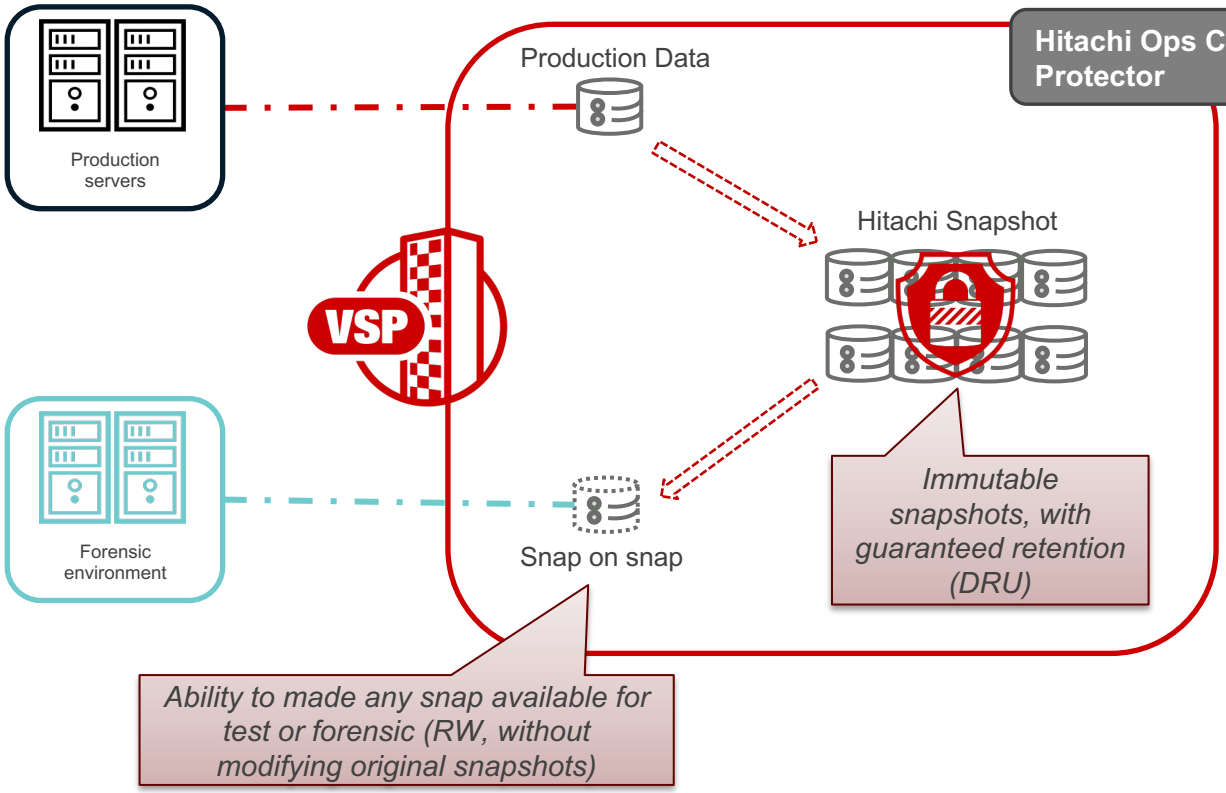


Witch models include ? :

- Hitachi Data Retention Utility
- Shadow image Clone
- Thin Image snapshot
- Virtualization capabilities
- Hitachi Ops Center Protector

→ **ALL!**

Hitachi Cyber Resilience – example 1 for Block

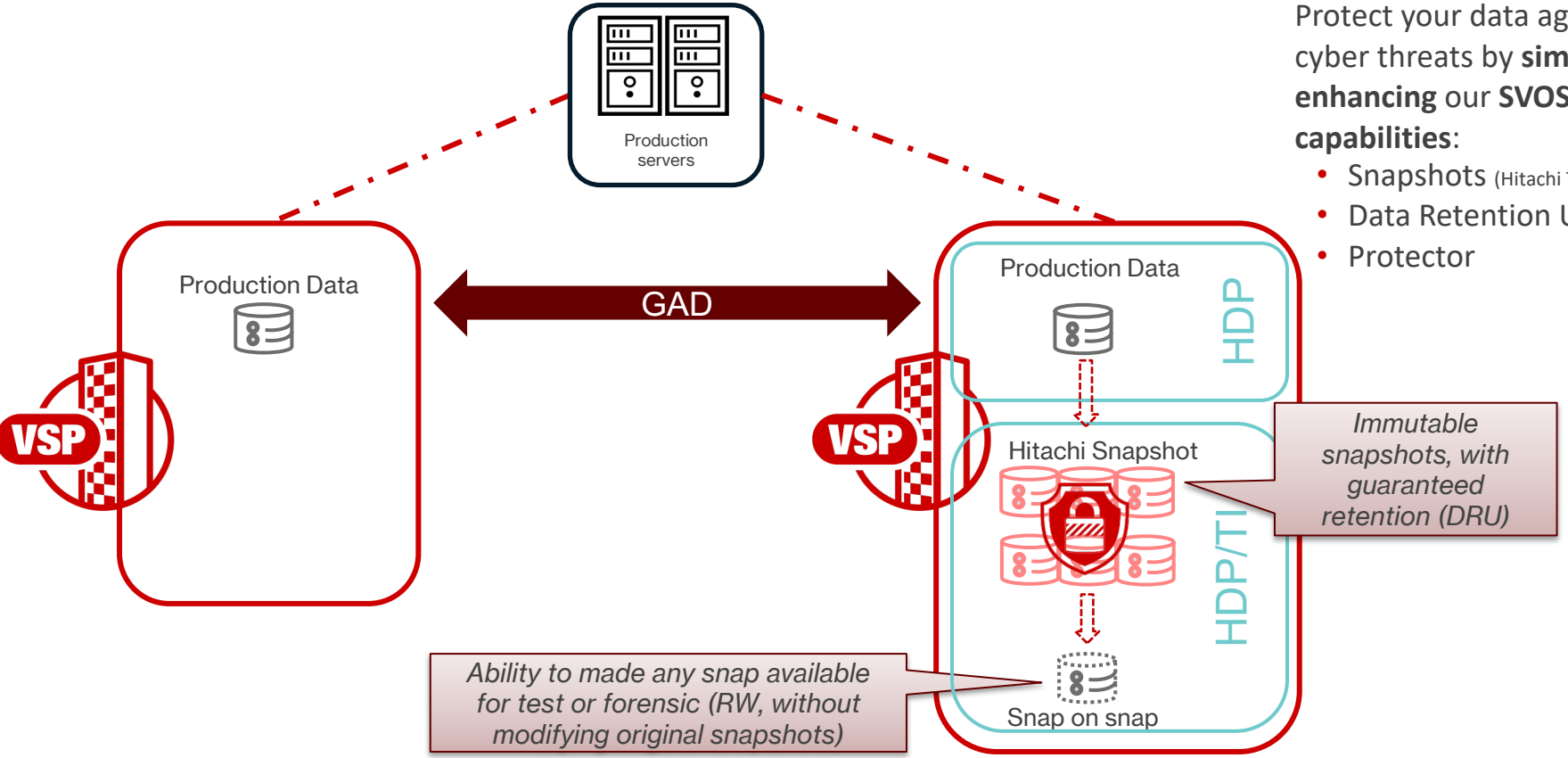


Protect your data against cyber threats by **simply enhancing** our **SVOS capabilities**:

- Snapshots (Hitachi Thin Image)
- Data Retention Utility
- Protector

Use **Hitachi Ops Center** for orchestration (Protector) and alerting (Analyzer)

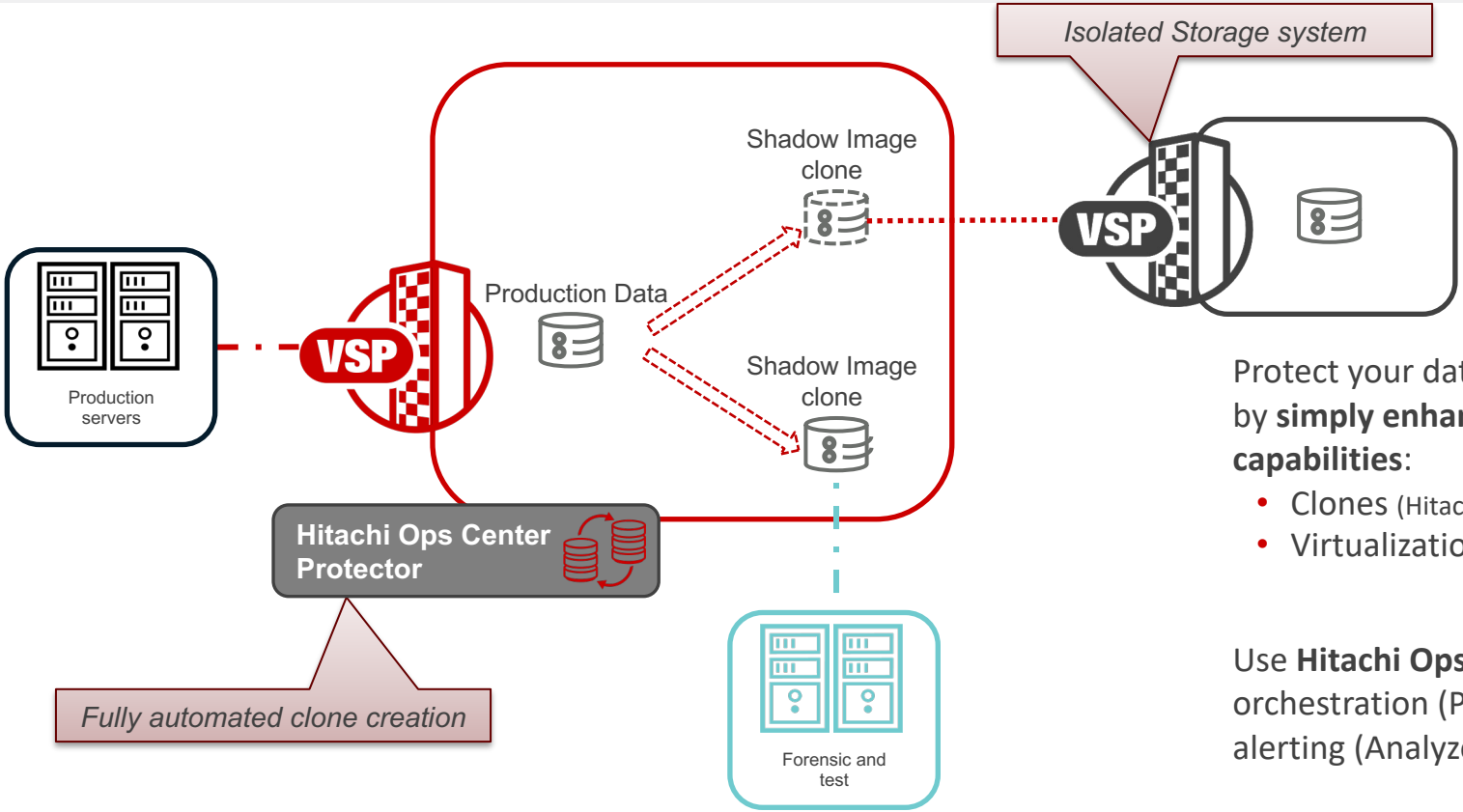
Hitachi Cyber Resilience – example 2 for Block



Protect your data against cyber threats by **simply enhancing** our **SVOS capabilities**:

- Snapshots (Hitachi Thin Image)
- Data Retention Utility
- Protector

Hitachi Cyber Resilience – example 3 for Block



Protect your data against cyber threats by **simply enhancing** our **SVOS capabilities**:

- Clones (Hitachi ShadowImage)
- Virtualization (Universal volume Manager)

Use **Hitachi Ops Center** for orchestration (Protector) and alerting (Analyzer)

Ops Center Analyzer Alerts

HITACHI
Inspire the Next

Ransomware alerting, as outlined below, can be performed via Ops Center Analyzer on any of the above options:

- THREAT : DATA EXFILTRATION
  - Elevated read I/O on LDEVs
  - Elevated read I/O on VMware VMDKs
- THREAT : ENCRYPTION
  - Elevated write I/O on LDEVs
  - Elevated write I/O on VMware VMDKs
  - Elevated write I/O on numerous LDEVs
  - Elevated CPU + write I/O on VM

Be Creative!

HITACHI
Inspire the Next

All the needed pieces are already there.

We just have to put them together, without bringing additional product/software.

HITACHI
Inspire the Next

Hitachi Cyber Resilience
Block Level Automation for VMware

Challenges with Existing Solutions

HITACHI
Inspire the Next

Disaster Recovery

- Replicates malware/encryption
- Lacks network automation/isolation
- Lacks point-in-time recovery

Snapshot Rollback

- Places systems back to vulnerable state
- Erases evidence needed for forensics
- Lacks network automation/isolation

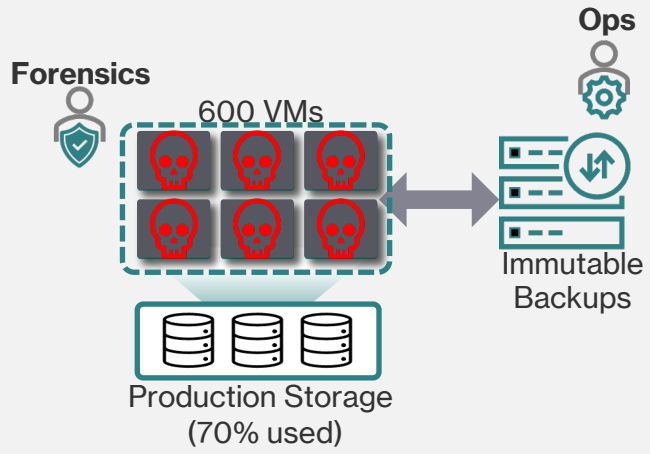
Backup

- Requires massive data copy – SLOW
- Cannot scale to 100s/1000s of VMs
- Manual recoveries and isolation

Ops Center Protector and CyberVR Deliver:

- Single click automation (storage/network/VM)
- Virtual-air-gaps (functional-yet-isolated)
- Multi-point-in-time recovery
- Proven and tested RTOs
- Immutability with recovery agility
- Scalability to 100s-to-1000s of VMs
- Seamless workflows for patching and remediations

Recent Real-World Ransomware Recovery Example



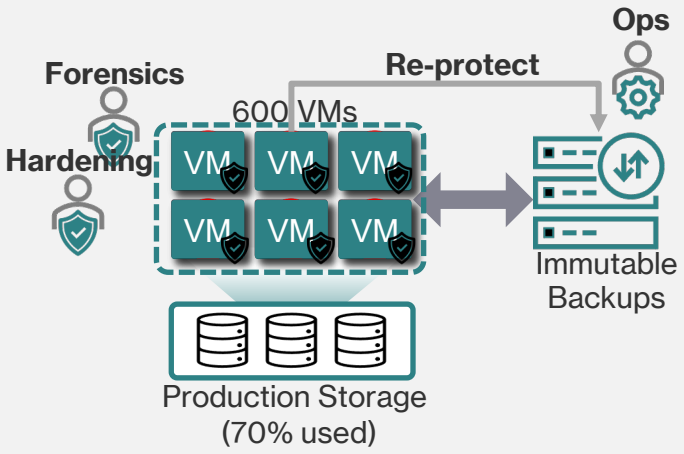
Ransomware encrypts workloads, forensics team investigates

Backup and recovery operations can't begin until storage is freed up

4 days until forensics complete and backup recovery begins

Recent Real-World Ransomware Recovery Example

HITACHI
Inspire the Next



RTA = 10 Days
Recovery Time Achieved

Ransomware encrypts workloads, forensics team investigates

Backup and recovery operations can't begin until storage is freed up

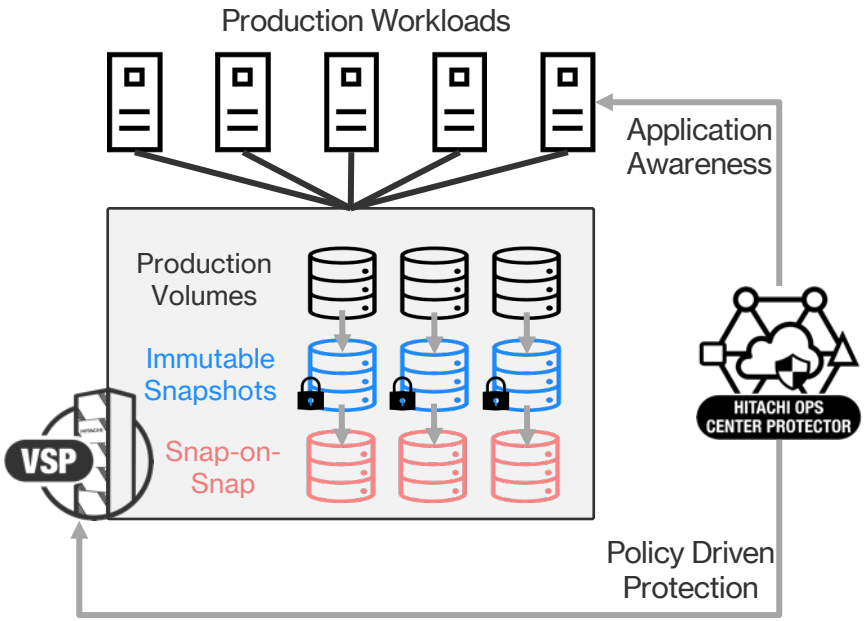
4 days until forensics complete and backup recovery begins

3 days to recover and isolate 600 VMs from pre-encryption backups

1 day to harden and eradicate malware from recovered workloads

2 days to protect hardened workloads before connecting to production

Ops Center Protector Snapshots

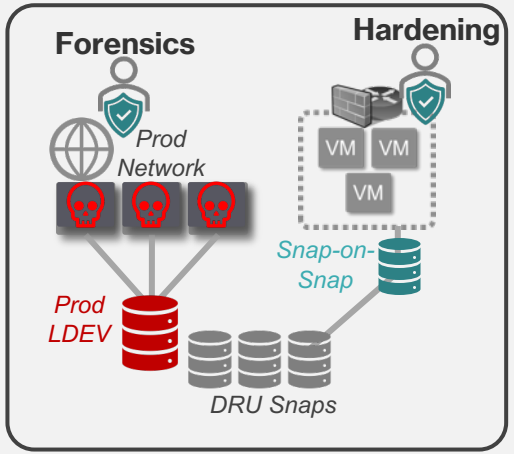


- Data immutability at the hardware layer
- Capacity-efficient and near-instant snapshots
- Instant restores from immutable snapshots
- Zero risk or impact to data integrity

World‘s fastest automated ransomware recovery from storage-efficient immutable snapshots

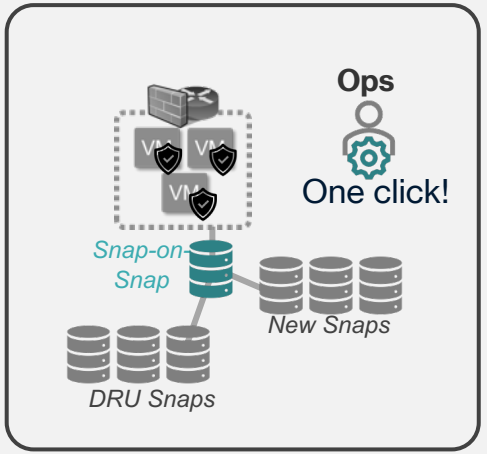
HITACHI
Inspire the Next

Isolated Recovery & Triage



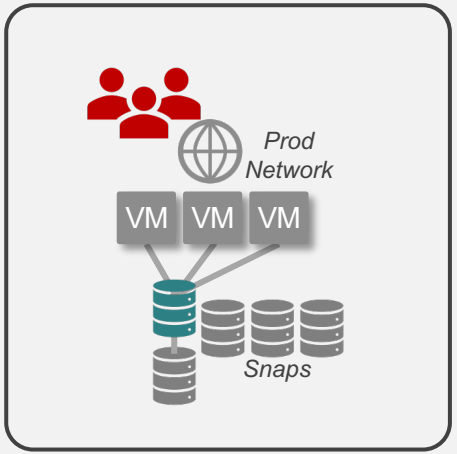
Recovery from immutable snaps to virtual-air-gap on production-equivalent storage

Re-protection



Recovered VMs are re-protected before re-connecting users

Re-Connection



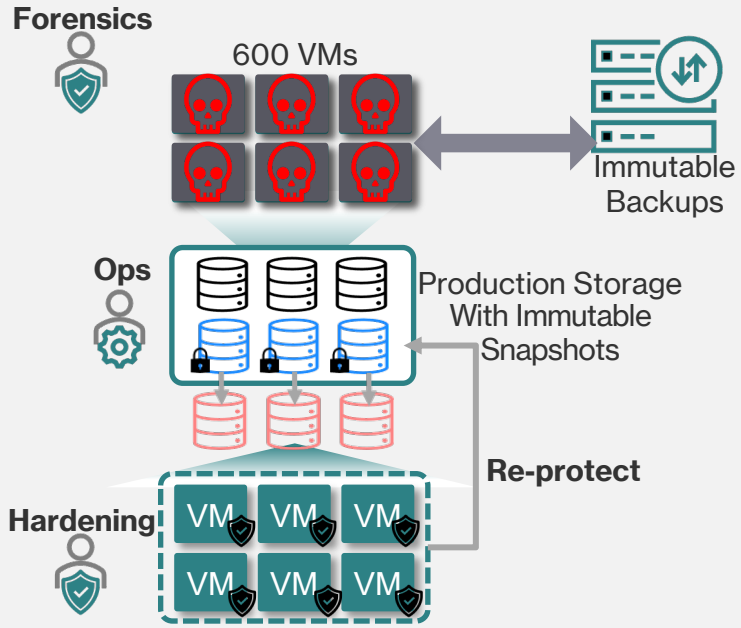
Recovered VMs switched from virtual air-gap to production networks

Measured in Minutes for Thousands of VMs

(1500 VMs in 70 min**)**

Ransomware Recovery with Protector and CyberVR

HITACHI
Inspire the Next



RTA as low as **Hours**

Ransomware encrypts workloads, forensics team investigates

30min to recover and isolate 600VMs from pre-encryption snaps

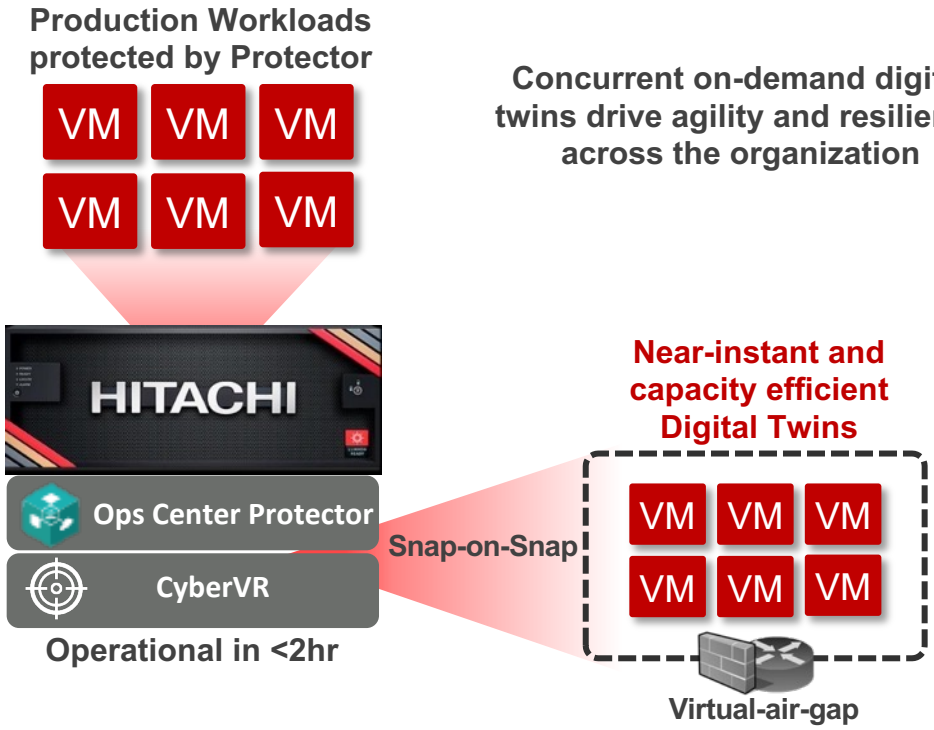
Forensics, hardening, and eradication are done simultaneously

10min to protect hardened workloads with minimal capacity impact

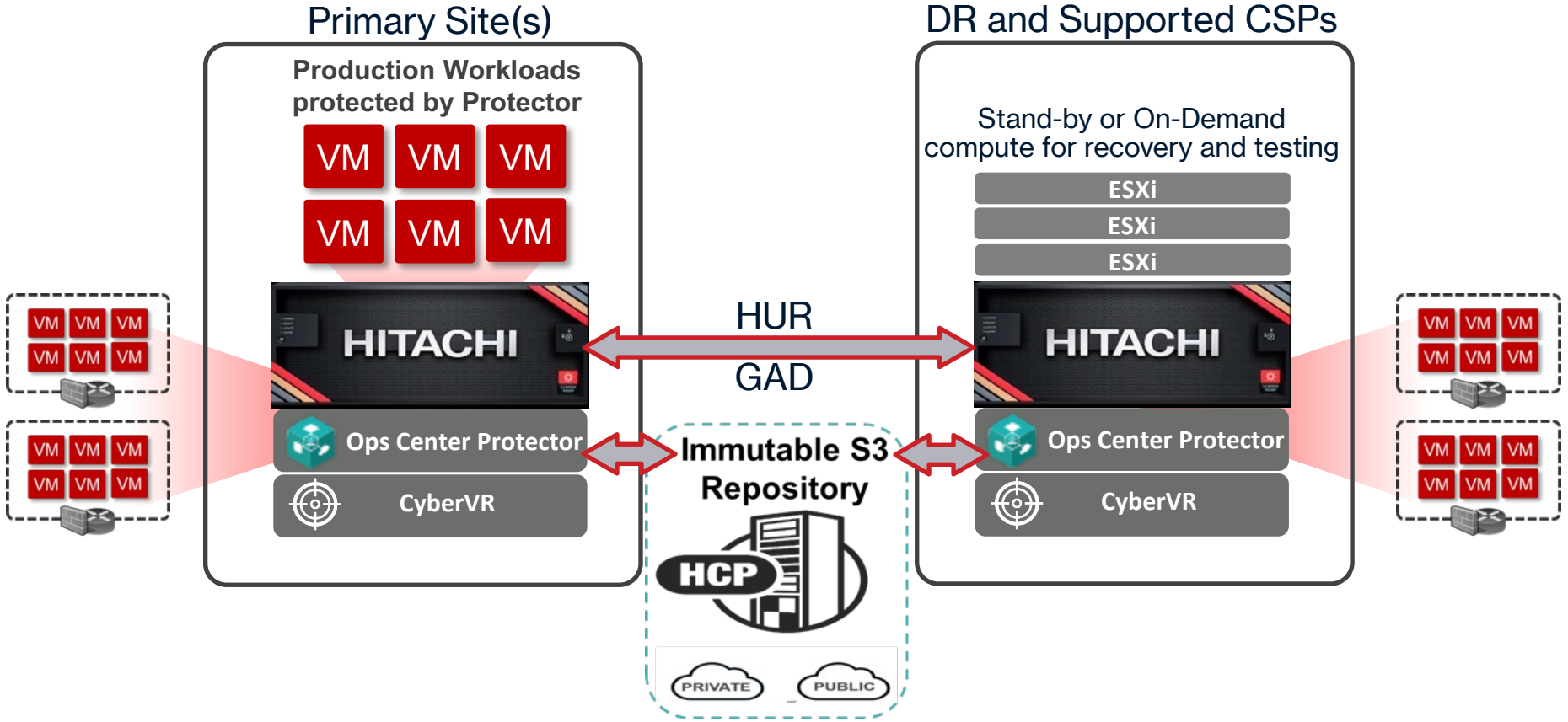
The recovery bottleneck is the time it takes to harden and eradicate, **not** storage/backup/network capacity

CyberVR & Ops Center Protector Snapshots

HITACHI
Inspire the Next



Implementation Options – Local, DR, CSP



Data Recovery is NOT Enough

HITACHI
Inspire the Next

Ops Center Protector:
Simplify the creation and management of policy-based modern data protection and copy data management workflows.

CyberVR:
Storage, compute, network, and application orchestration driving predictable and reliable recovery of data, workloads, and services.

Steps to Applications and Services Recovery	Without CyberVR	With CyberVR
Policy driven replication and immutable snapshots	Ops Center Protector	Ops Center Protector
Discovery of metadata to instantiate VM and networks	Manual	Automated
Instant recovery of data through snap-of-snap	Manual	Automated
Mount and re-signature volumes for consumption	Manual	Automated
Functional network isolation for safe recoveries	Manual	Automated
VM Registration and network/compute configuration	Manual	Automated
Booting VMs in correct orders with delays	Manual	Automated
Validating status of applications and services	Manual	Automated
Number of steps to recover a 300 VM environment	~1500	1 click
Risk of errors/false-starts during an incident	High	Low

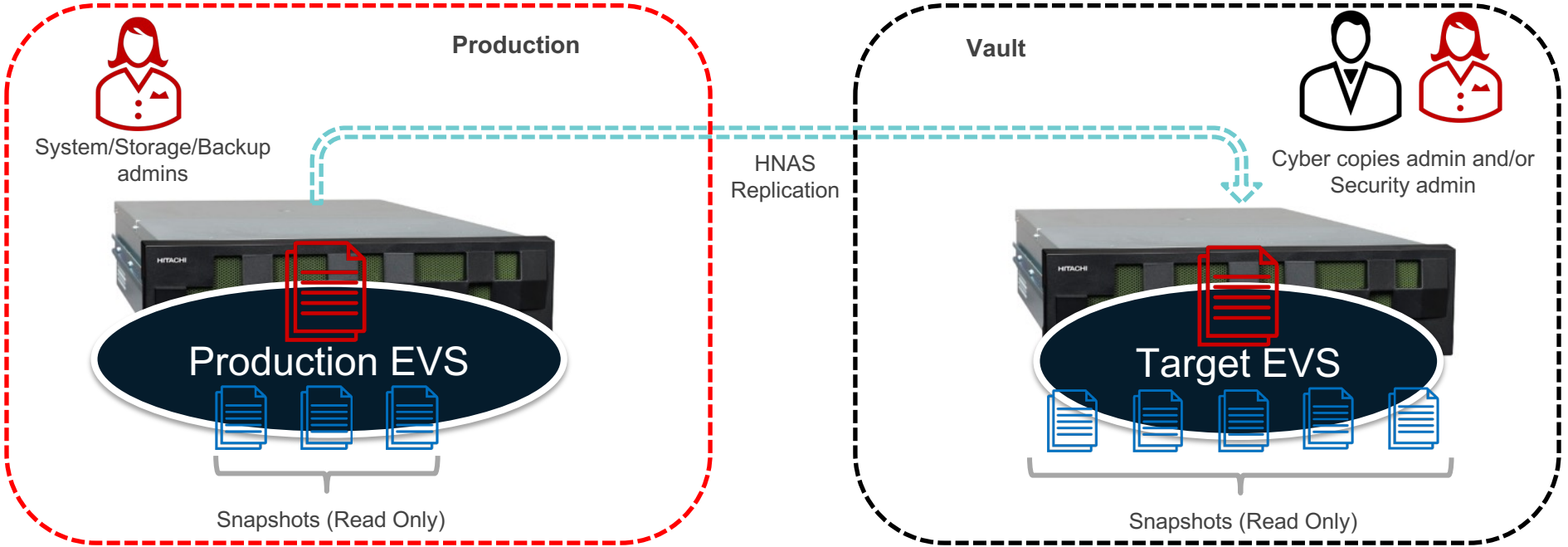
With CyberVR, recovery tests can be conducted continuously, providing proof of resiliency

HITACHI
Inspire the Next

Hitachi Cyber Resilience
Examples for File Storage

Hitachi Cyber Resilience solution – for HNAS

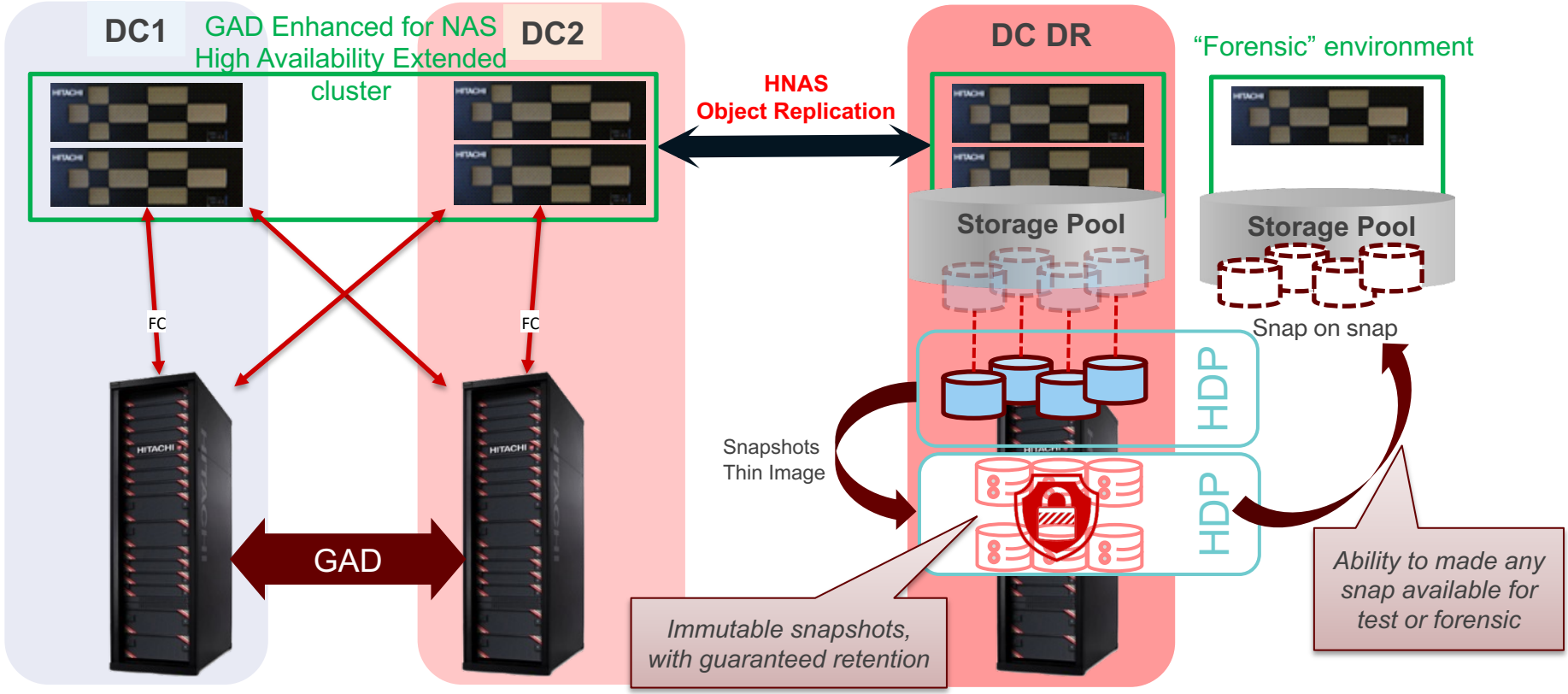
- HNAS snapshots = **immutability**
- Combine Snapshots with Replication
  - Local and Remote Snapshot **Retention are independent**
  - Local and Remote **administration role can be separated**



Hitachi Cyber Resilience solution – for HNAS

HITACHI
Inspire the Next

VSP Block layer protection can benefit to HNAS



HITACHI
Inspire the Next

Hitachi Cyber Resilience
Examples for Object Storage

Hitachi Content Platform - Cyber Resilience for Objects by design

HITACHI
Inspire the Next

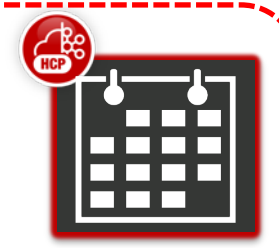
Protect your data against cyber threats by **simply enhancing** our **HCP capabilities**:

Data Protection and Compliance

Immutability & Retention

Protection & Replication

Policy Based Automation



Versioning

Access, Security, Efficiency

Authentication

Encryption

Standard APIs

Dedupe

Compression

Unrivaled Data Resilience

HITACHI
Inspire the Next

HCP is Backup Free

15 nines of data durability

Each data fragment can survive the simultaneous loss of six drives

One bit lost every 1 trillion years

+

10 nines of accessibility

Amazon only offers 4 nines; ~53 minutes of downtime per year

+

2 copies of all metadata

+

Customer-configurable redundant local object copies (2, 3, or 4)

+

Content validation via hashes and automatic object repair

+

Replication – offsite copies with automated repair from replica

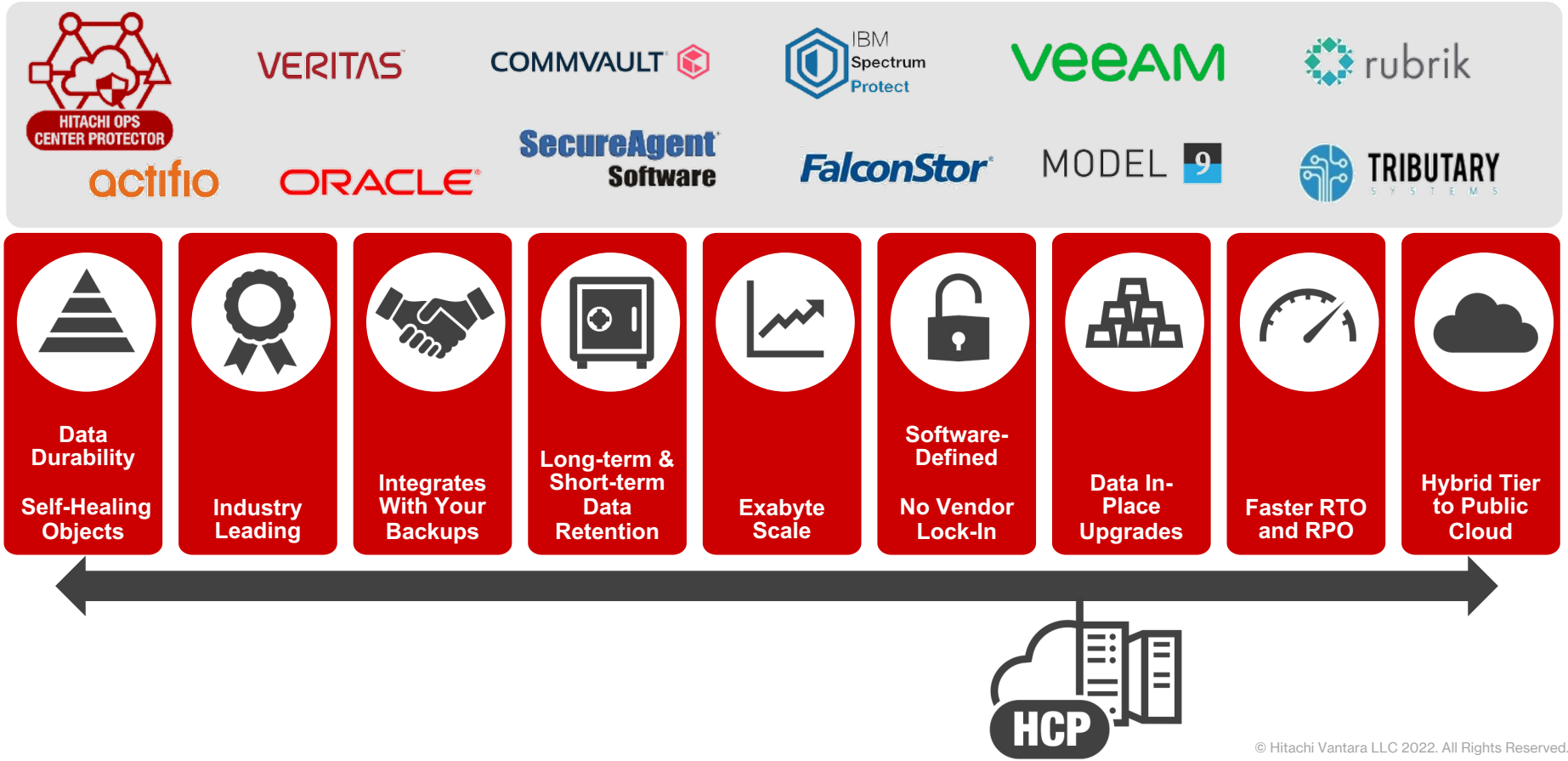
+

Object versioning – protection from accidental deletes and changes

- **1 Million times more available than AWS S3**
- **Exceptional data protection**
- **Much better suited for replacement of tape libraries than any other disk-based backup solutions**

Hitachi Data Protection capabilities with HCP

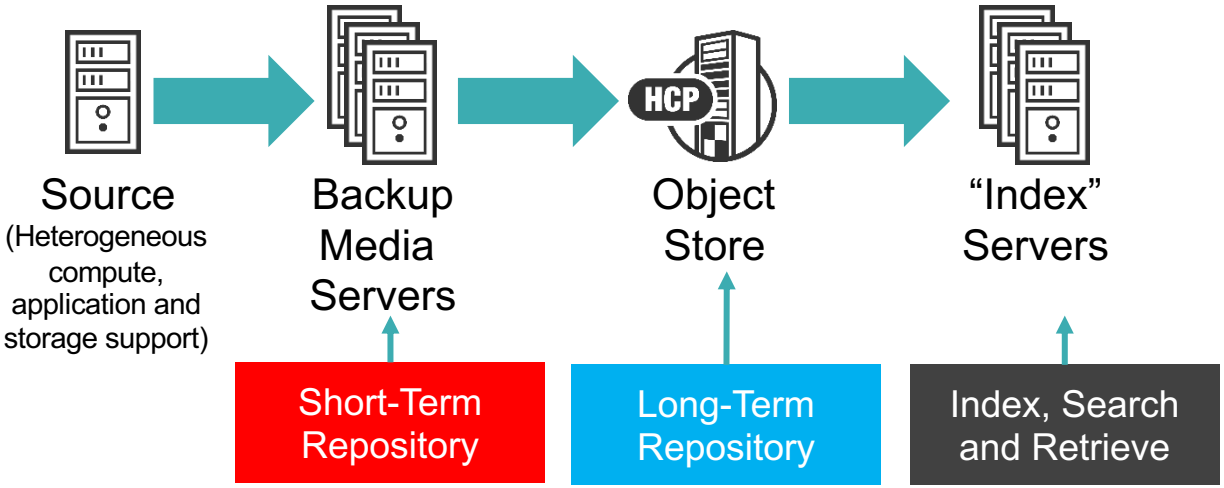
HITACHI
Inspire the Next



Backup to Object Storage

HITACHI
Inspire the Next

For customers looking to reduce or eliminate the use of tape for long-term retention of backup data, and gain greater use from their backup data, supporting several backup software solutions using the S3 protocol.



VERITAS
COMMVAULT
VEEAM
HITACHI OPS CENTER PROTECTOR

Data Recovery for End/Mobile Users

HITACHI
Inspire the Next

Ransomware can make your backups (your “insurance”) a liability.

1. **DATA PROTECTION**
   Real-time Sync and Protects End User Laptop Data
2. **WORM (Write-Once-Read-Many)**
   Makes HCP immutable to ransomware attack.
3. **VERSIONING**
   Recover to the previous good file versions before the ransomware attack

Some of Our Customers

- “milDrive” for the US Department of Defense
- Desktop Data Backup
- File Sharing and Backup for Staffs and Teachers
- File sharing and backup, replaces thumb drives

One Platform for All Services

HITACHI
Inspire the Next

S3 Applications

Capacity Optimization, Protection & Retention
Cloud Ready Applications

S3 Enabled Applications

Cloud File System | S3 Apps | Custom App

VERITAS
COMMVAULT
RUBRIK

Big Data Integration

Offload | Inline Optimize

splunk> teradata. LUMADA

NextGen Applications

Data-driven Business Workload

Parallel Filesystem

GPU Direct Storage

World's Fastest FileSystem

NVIDIA GPUDIRECT

Modernize

HDFS

Spark
presto
S3 Select
Greenplum

File Services

File Services for Edge to Cloud

Cloud Filesystem

on-premises
private or public cloud

Open S3 • Dispose • Categorize • Classify

Hitachi Object Storage Platform

Power Your Data Lake

Secure • Govern • Audit

Tiering

Native Integration

1. **Unified Data Management On-Premise and Public Cloud**
2. **Consume Public Cloud Services On-Demand**
3. **Bring Public Cloud Services to On-Premise**
4. **Policy Based Cloud Service Consumption**

Why Hitachi Vantara

HITACHI
Inspire the Next

Backup solutions and integration **(HDPS**(Commvault)**, NetBackup, Veeam, IBM SP** and more)

CyberVR for Vmware Cyber Resilience, and recovery training

Ops Center Protector for Enterprise Copy Data Management & Automation

VSP storage platform powered by **SVOS RF** with built-in replication, **Retention and Immutability**

HCP with S3 storage, Object lock, WORM and policy-based governance and compliance

HNAS with immutable snapshots, and more to come

Thank You

HITACHI

Inspire the Next