Hitachi Vantara

World‘s Fastest Automated Ransomware Recovery

Cyber Resiliency with Ops Center Protector and CyberVR

Andrej Gursky
Solutions Consultant CEE, Hitachi Vantara
April 2024

Resiliency Challenges

Proactive

Change Management

Accelerating new technology initiatives and modernization, without increasing cyber risk, while ensuring application reliability

Cyber Assurance

Understanding the true risk of vulnerabilities, validating the efficacy of existing tools against real attacks, and accelerating the time it takes to remediate and mitigate

Reactive

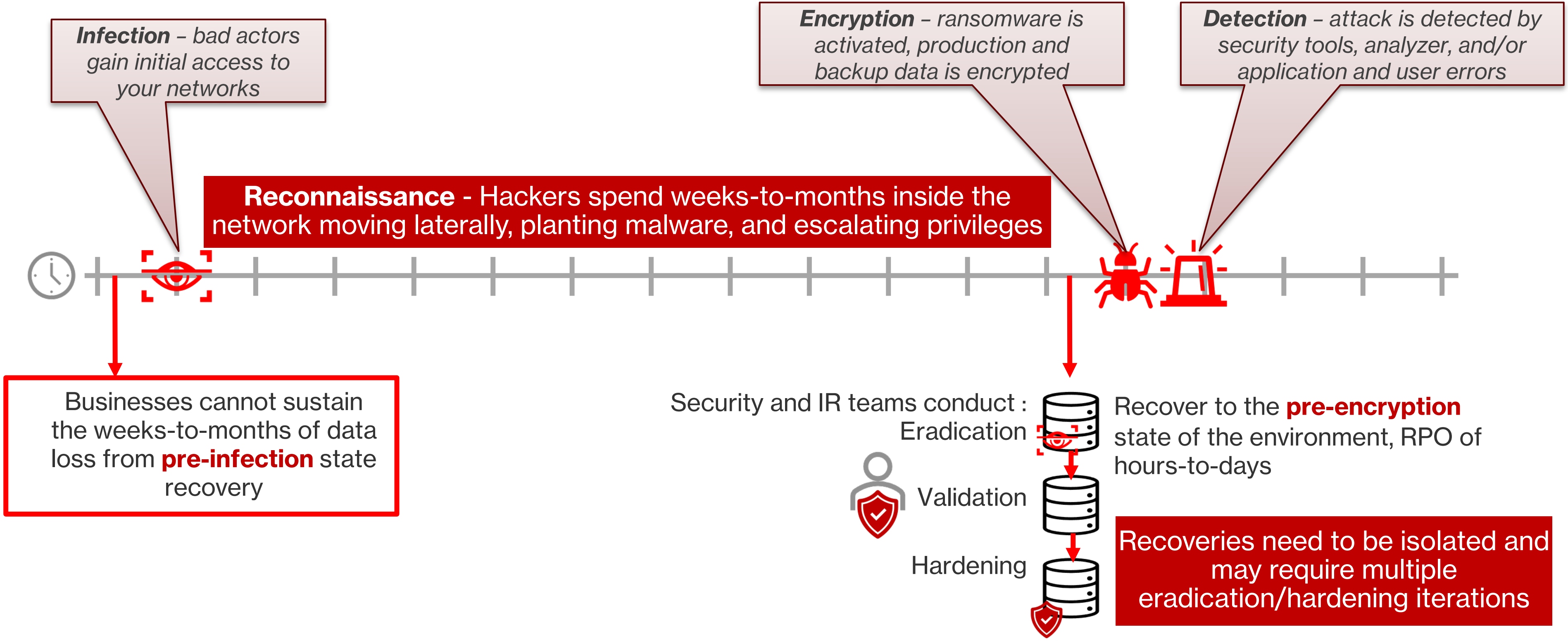
Data Immutability

Ensuring that all snapshots are immutable to changes by bad actors and/or compromised administrator credentials, without loosing recovery agility

IR Training

Hands-on training of ransomware recovery scenarios including multi-point-in-time recovery, network isolation, and hardening to prevent attack reoccurrence

Infection vs Encryption – Ransomware Timeline



Infection *– bad actors gain initial access to your networks*

Reconnaissance - Hackers spend weeks-to-months inside the network moving laterally, planting malware, and escalating privileges

Encryption *– ransomware is activated, production and backup data is encrypted*

Detection *– attack is detected by security tools, analyzer, and/or application and user errors*

Businesses cannot sustain the weeks-to-months of data loss from **pre-infection** state recovery

Security and IR teams conduct : Eradication

Validation

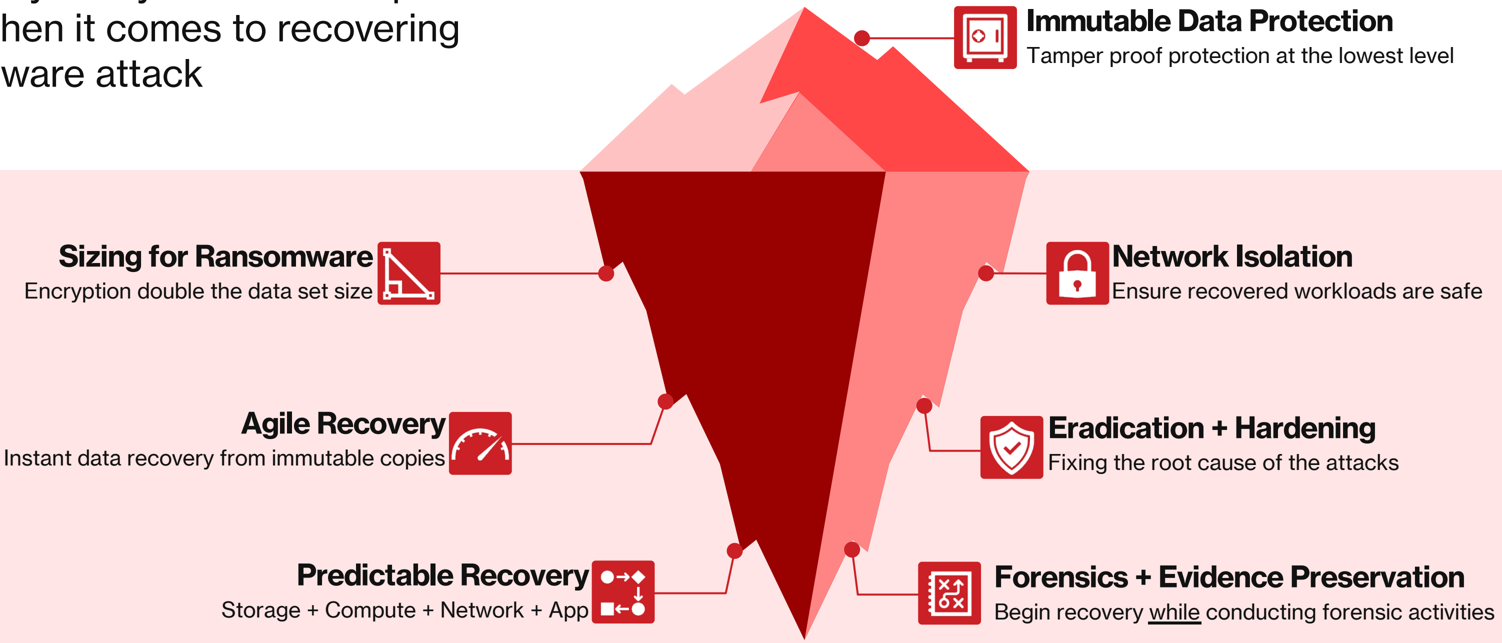
Hardening

Recover to the **pre-encryption** state of the environment, RPO of hours-to-days

Recoveries need to be isolated and may require multiple eradication/hardening iterations

Ransomware Recovery Challenges

Data immutability is key but it’s the “tip of the iceberg” when it comes to recovering from a ransomware attack



Immutable Data Protection
Tamper proof protection at the lowest level

Sizing for Ransomware
Encryption double the data set size

Network Isolation
Ensure recovered workloads are safe

Agile Recovery
Instant data recovery from immutable copies

Eradication + Hardening
Fixing the root cause of the attacks

Predictable Recovery
Storage + Compute + Network + App

Forensics + Evidence Preservation
Begin recovery while conducting forensic activities

Ransomware Resiliency Requirements

Gartner

At a minimum a ransomware protection solution must include:

1. Immutability
2. Air gap technology
3. Instant recovery capability
4. Isolated recovery capability
5. Automated data restoration and deployment capabilities
6. Ransomware detection capability

Let's explore how we can achieve the resiliency requirements in a cost-effective manner, with proven and predictable results, that can be applied to a large portion of the technical infrastructure

Meeting these requirements with backup-based technologies results in expensive, unpredictable, and un-sustainable solutions

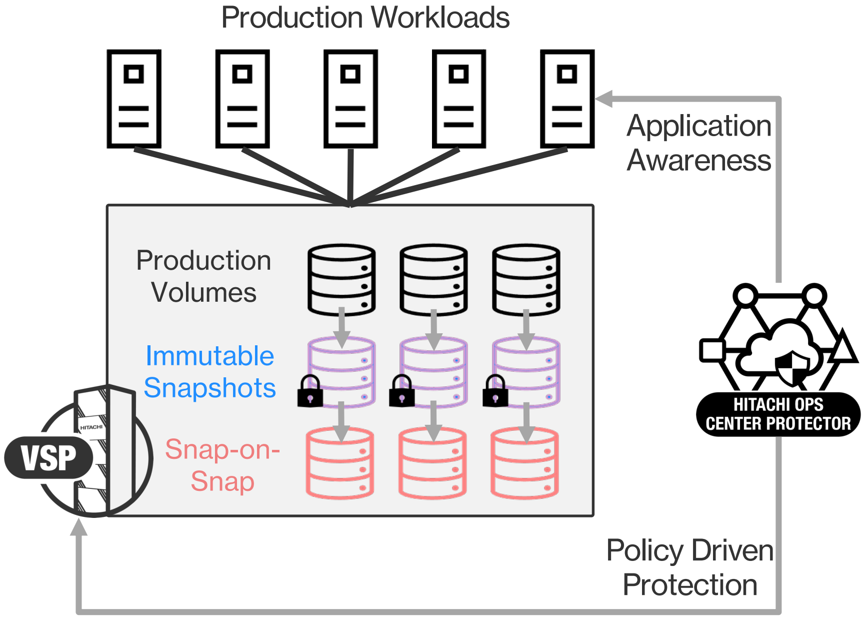
Gartner: Research Roundup for Improving the Protection of Backup Infrastructure and Recovering From Ransomware Attacks
Published 1 April 2022 - ID G00768084

Hitachi Vantara

CyberVR and Ops Center Protector

Solution

Protector Snapshots



Data immutability at the hardware layer

Capacity-efficient and near-instant snapshots

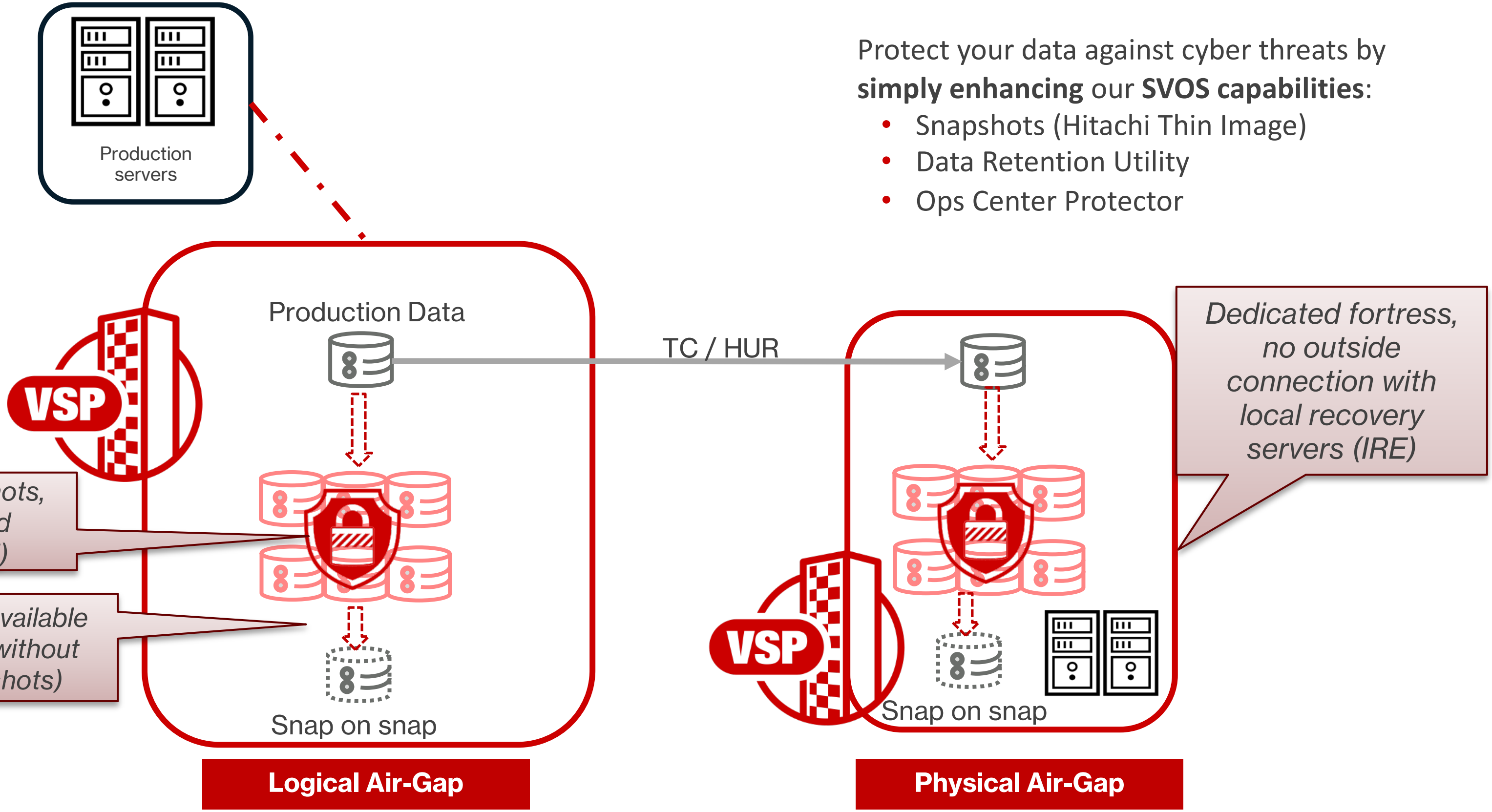
Instant restores from immutable snapshots

Zero risk or impact to data integrity

Hitachi Cyber Resiliency – Example

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

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

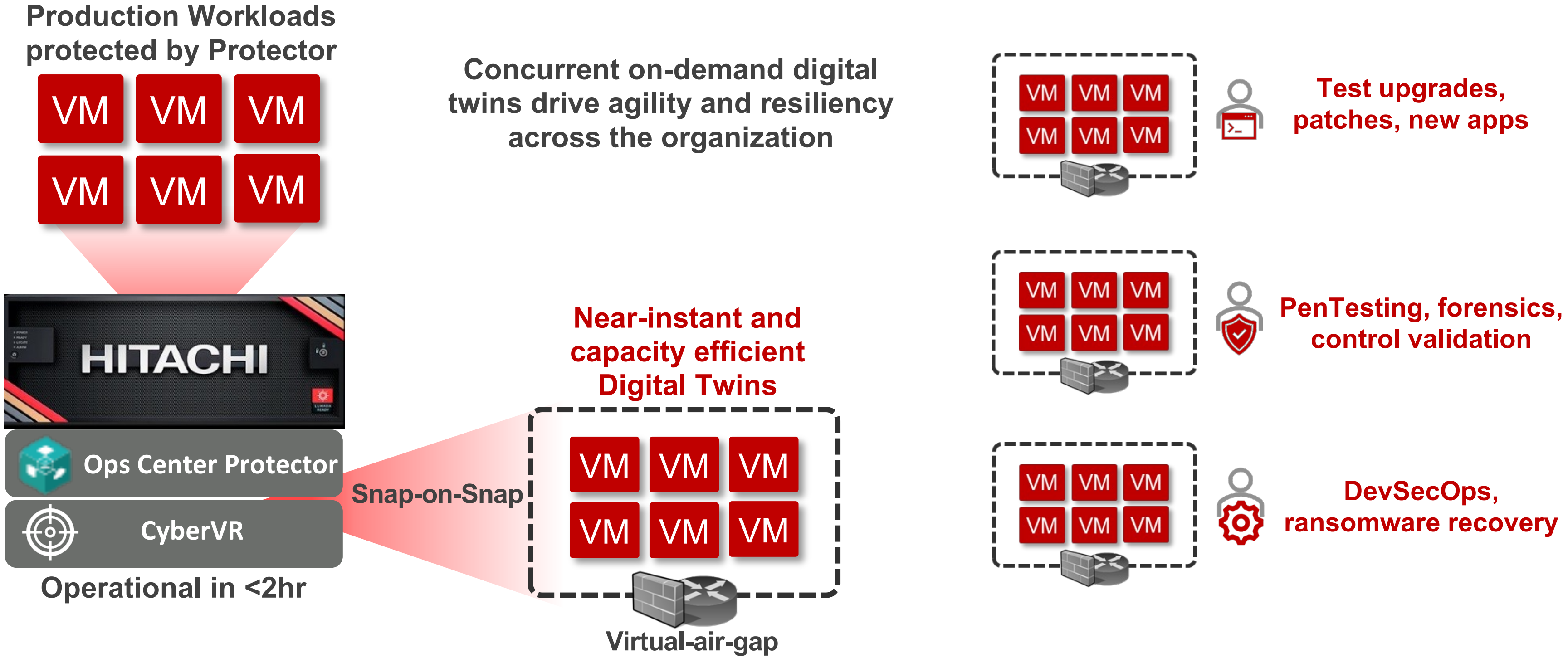


Immutable snapshots, with guaranteed retention (DRU)

Ability to make any snap available for test or forensic (RW, without modifying original snapshots)

Dedicated fortress, no outside connection with local recovery servers (IRE)

CyberVR & Ops Center Protector



Production Workloads protected by Protector

Ops Center Protector

CyberVR

Operational in <2hr

Snap-on-Snap

Concurrent on-demand digital twins drive agility and resiliency across the organization

Near-instant and capacity efficient Digital Twins

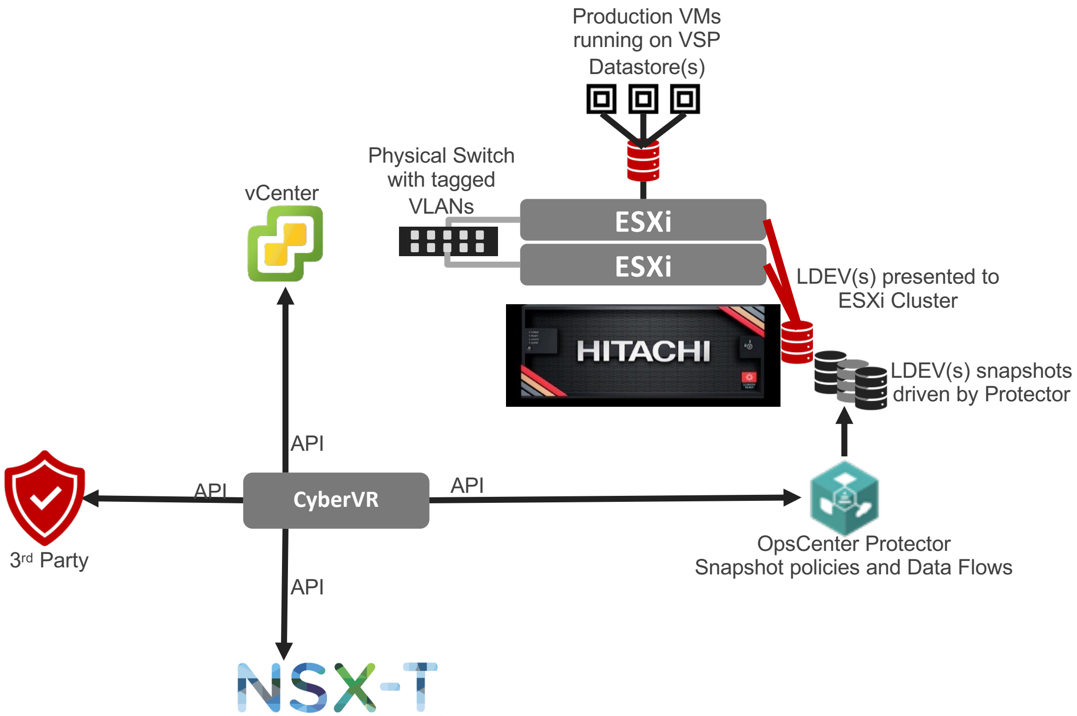
Virtual-air-gap

Test upgrades, patches, new apps

PenTesting, forensics, control validation

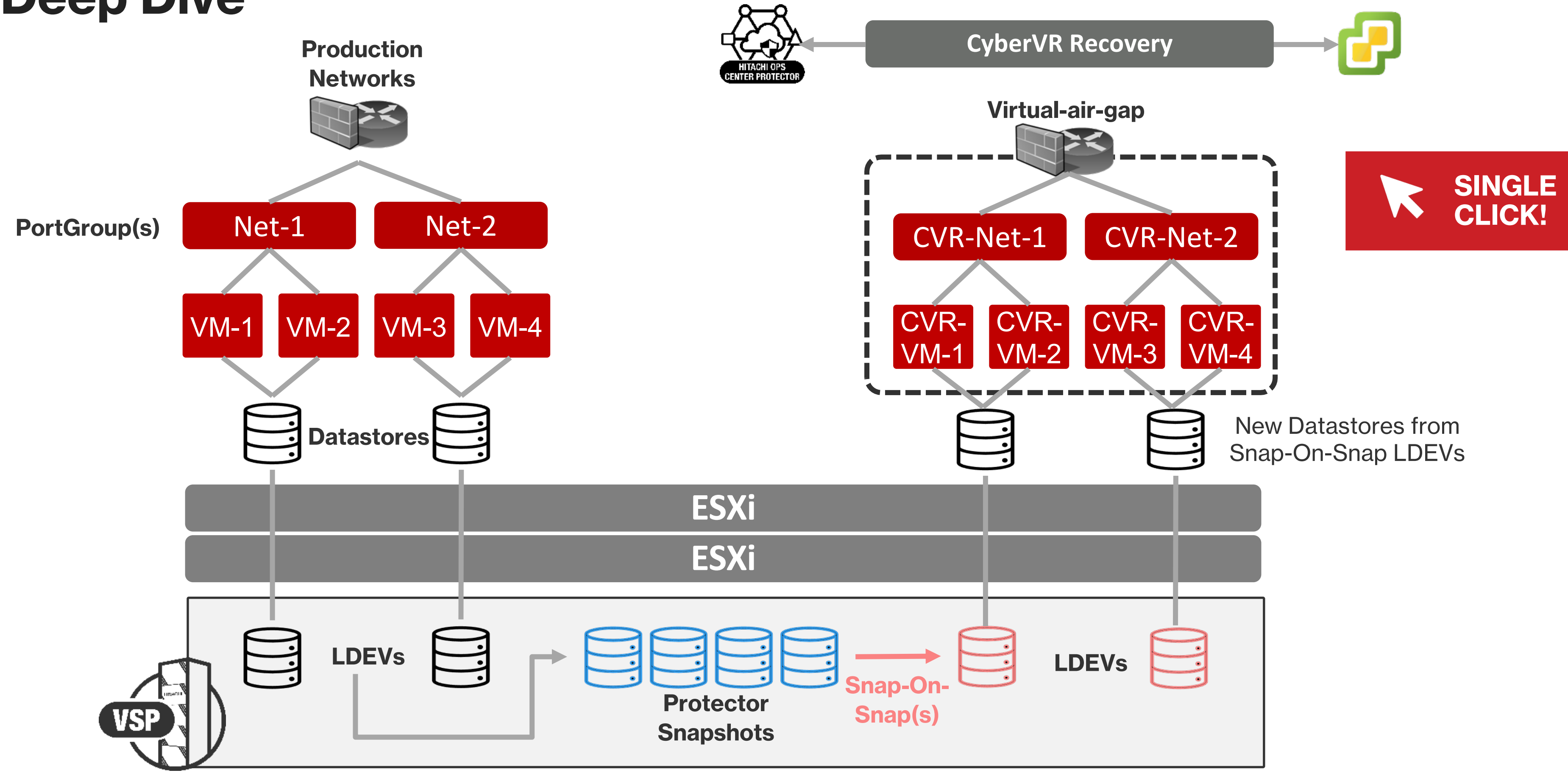
DevSecOps, ransomware recovery

Integration


Production VMs running on VSP Datastore(s)
Physical Switch with tagged VLANs
vCenter
ESXi
ESXi
HITACHI
LDEV(s) presented to ESXi Cluster
LDEV(s) snapshots driven by Protector
API
API
CyberVR
API
3rd Party
OpsCenter Protector Snapshot policies and Data Flows
API
NSX-T

- VMware
  - ESXi Cluster
  - vCenter Server
- OpsCenter Protector
  - LDEV/VM Snapshots
  - Application license for consistent VMware protection (recommended)
- Networking
  - Pool of available VLANs on the physical switch
  - (optional) VMware NSX-T
- Authentication
  - vCenter service account
  - OpsCenter Protector service account
  - (optional) NSX-T service account

Deep Dive

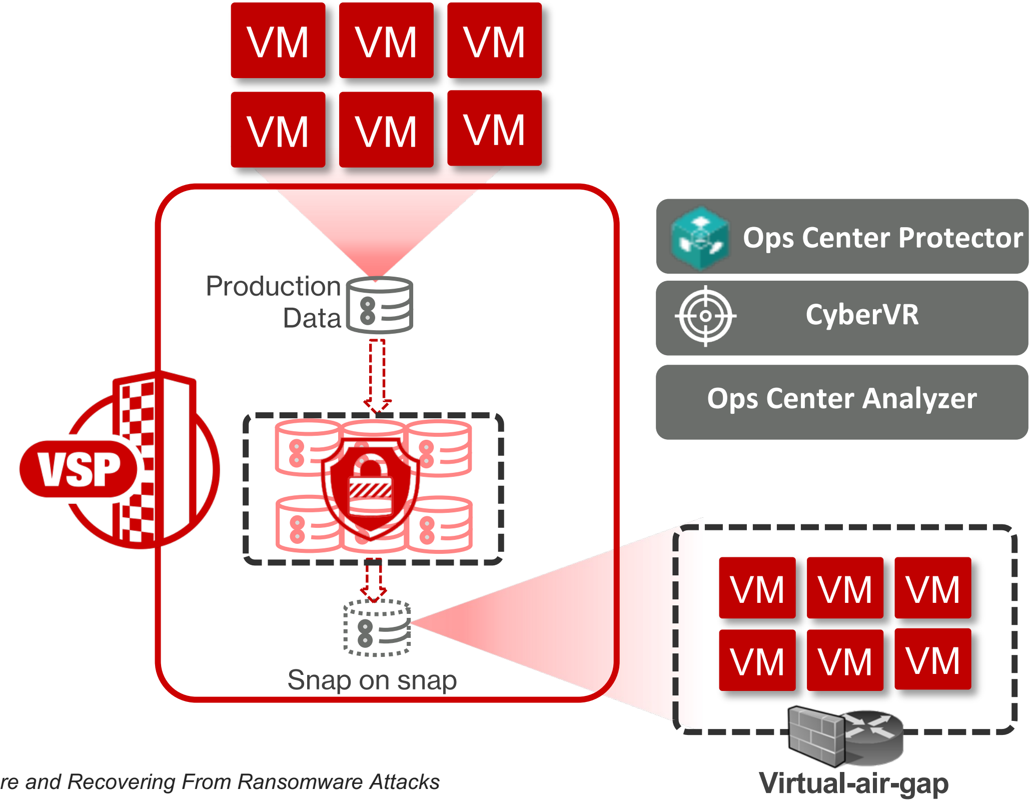

HITACHI OPS CENTER PROTECTOR
CyberVR Recovery
Production Networks
Virtual-air-gap
SINGLE CLICK!
PortGroup(s)
Net-1
Net-2
CVR-Net-1
CVR-Net-2
VM-1
VM-2
VM-3
VM-4
CVR-VM-1
CVR-VM-2
CVR-VM-3
CVR-VM-4
Datastores
New Datastores from Snap-On-Snap LDEVs
ESXi
ESXi
LDEVs
Protector Snapshots
Snap-On-Snap(s)
LDEVs
VSP

Ransomware Resiliency Requirements

Gartner

At a minimum a ransomware protection solution must include:

1. Immutability
2. Air gap technology
3. Instant recovery capability
4. Isolated recovery capability
5. Automated data restoration and deployment capabilities
6. Ransomware detection capability



Gartner: Research Roundup for Improving the Protection of Backup Infrastructure and Recovering From Ransomware Attacks Published 1 April 2022 - ID G00768084

Hitachi Vantara

Ransomware Recovery

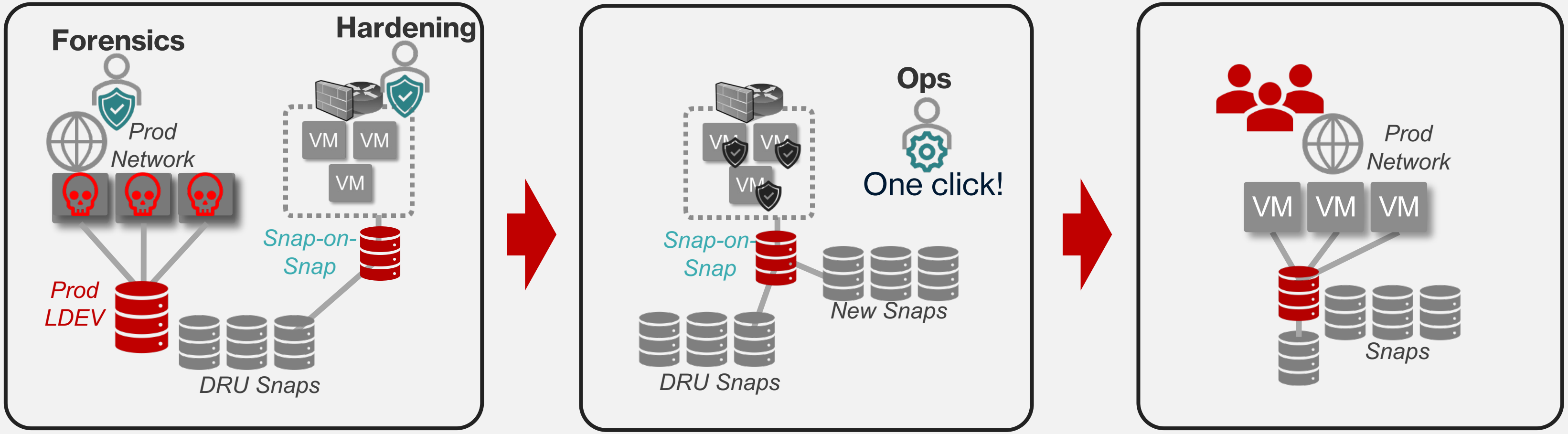
With Ops Center Protector and CyberVR

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

Isolated Recovery & Triage

Re-protection

Re-Connection



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

Recovered VMs are re-protected before re-connecting users

Recovered VMs switched from virtual air-gap to production networks

Measured in Minutes for Thousands of VMs

(1500 VMs in 70 min)

Backup vs Protector and CyberVR

Need/Feature	Backup	Protector + CyberVR
Data protected under 3,2,1 rule to different media	✓	X
Long term retention of data (months/years)	✓	X
File/object scanning, indexing, and alerting	✓	X
Immutable data protection at the lowest level (hardware)	✓	✓
Predictable and proven RTO of 100s-1000s of VMs/TB	X	✓
End-to-end recovery automation (storage/compute/network)	X	✓
Data copy required for recovery -> hardening -> eradication	At Least 1X	0
End-to-end failback automation (storage/network)	X	✓
Data copy required for failback	3X	At most 1X
Ease of testing	Manual	Single Click

Scalability

Recovery times depend on the number of volumes, hosts, and VMs – **NOT** on the size of the data

5X 5X 5X

	12 VMs	60 VMs	300 VMs	1500 VMs
Virtual-air-gap Creation	5 min	5 min	5 min	8 min
Storage snap-on-snap	1 min	1 min	8 min	21 min
VMware snap mount	2 min	2 min	3 min	6 min
VM recovery and boot	1 min	2 min	8 min	25 min
VMware Tools Validation	2 min	6 min	6 min	10 min
TOTAL RTO	**9 min**	**15 min**	**30 min**	**70 min**
Per VM RTO	**45 (s)**	**15 (s)**	**6 (s)**	**3 (s)**

Data Recovery is NOT Enough

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

Follow Us

Hitachi Vantara

@HitachiVantara

Hitachi Vantara

Hitachi Vantara

Thank You