



# HITACHI

---

**LATAM Partner  
Summit FY26**  
Built to Grow. Powered by Data.

## Redefining Resiliency

Boards and Regulators are Demanding



**Tested & Predictable**

Tested, proven, and predictable cyber recovery.



**Catastrophic Scenarios**

Under catastrophic scenarios (control plane loss).



**Enterprise Scale**

At enterprise scale for functional business services (MVCs).



**End-to-End Workflow**

For all steps of the cyber recovery workflow.

**BUSINESS GOALS**

- Lower RPOs
- Lower RTOs
- Evidence of recoverability
- Lower Cost
- Automation
- True Isolation
- Leverage Existing Investments

Cyber Recovery Workflow

Isolate



Identify



Recover



Eradicate



Harden



Reconnect

**When a ransomware attack strikes, two questions are front and center:**

---

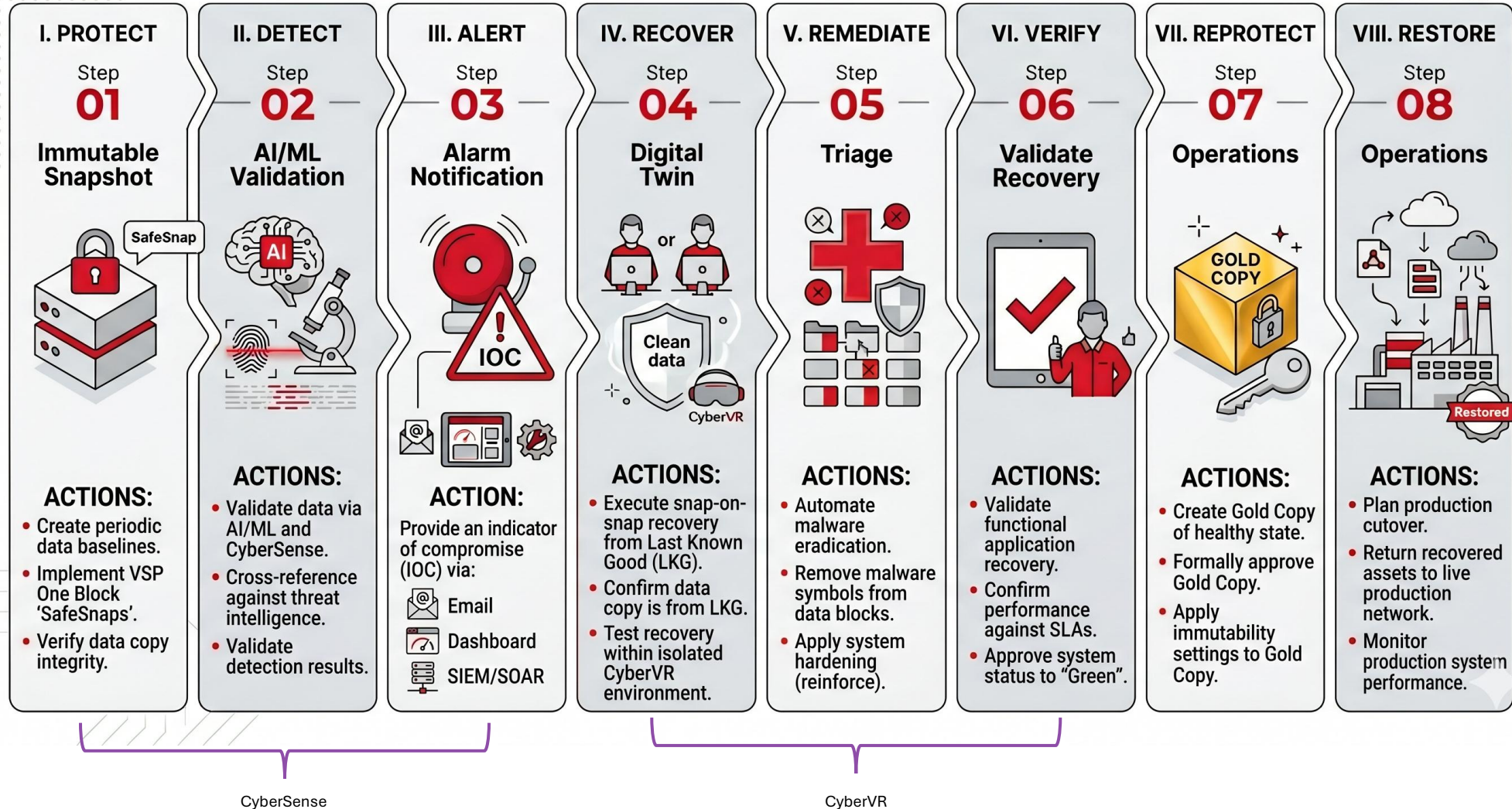
**01**

**Can we trust that our data is clean to restore?**

---

**02**

**How quickly can we resume operations?**

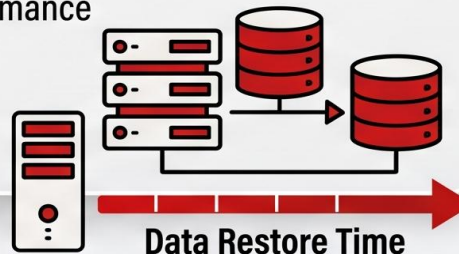


### RTO: RECOVERY TIME OBJECTIVE



#### THE DOWNTIME TARGET

- ✓ **TARGET DOWNTIME** duration for a single component, data set, or specific service.
- ✓ **MAXIMUM ALLOWABLE TIME** to restore data from a specific point (e.g., backup restore).
- ✓ **MAXIMUM ALLOWABLE TIME** to restore data from a business state to a specific point (e.g., backup restore).
- ✓ **OPERATIONAL METRIC** for backup and restore performance (e.g., IT restore process).
- ✓ **DEFINED IN SLAs** and business continuity plans for distinct items.

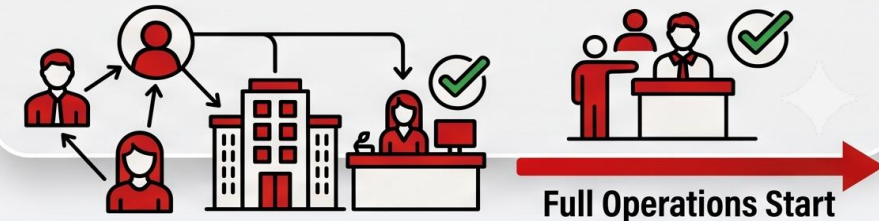


### RTO: RETURN TO OPERATIONS



#### THE BUSINESS READY STATE

- ✓ **ACHIEVING FULL OPERATIONAL STATUS** for the entire business, not just data restore.
- ✓ **SECURING END-USER ACCESS** and restoring access to all business critical applications and interfaces.
- ✓ **RE-ESTABLISHING CRITICAL WORKFLOWS** and restoring employee access to systems for daily tasks.
- ✓ **SERVING CUSTOMERS** and ensuring all customer-facing systems and support channels are functional.



*Recovery is not time to first byte restored — it is the time until business services are clean, hardened, and back in users' hands.*

# What is CyberSense?

## Data Validation Engine

CyberSense doesn't ask “did something change?” It asks, “*is this data still clean?*”

- Inspects actual content inside files, databases, and VMs at the byte level
- Uses comparative analysis of 200+ content-based statistics to identify how files change from snapshot-to-snapshot
- Validates whether data has been corrupted by ransomware
- 99.99% accuracy** in determining whether a snapshot is clean or corrupted

### Snapshots

| STATUS | HOST     | POLICY   | SNAPSHOT  | CREATED |
|--------|----------|----------|-----------|---------|
| Clean  | vmfs     | Sid-2605 | CS_VMFS_2 | 18:30   |
| Clean  | sid-win  | Sid-2605 | CS_VMFS_3 | 10:27   |
| Alert  | sid-sles | Sid-2605 | CS_VMFS_4 | 10:27   |

### Alerts

Pending 9

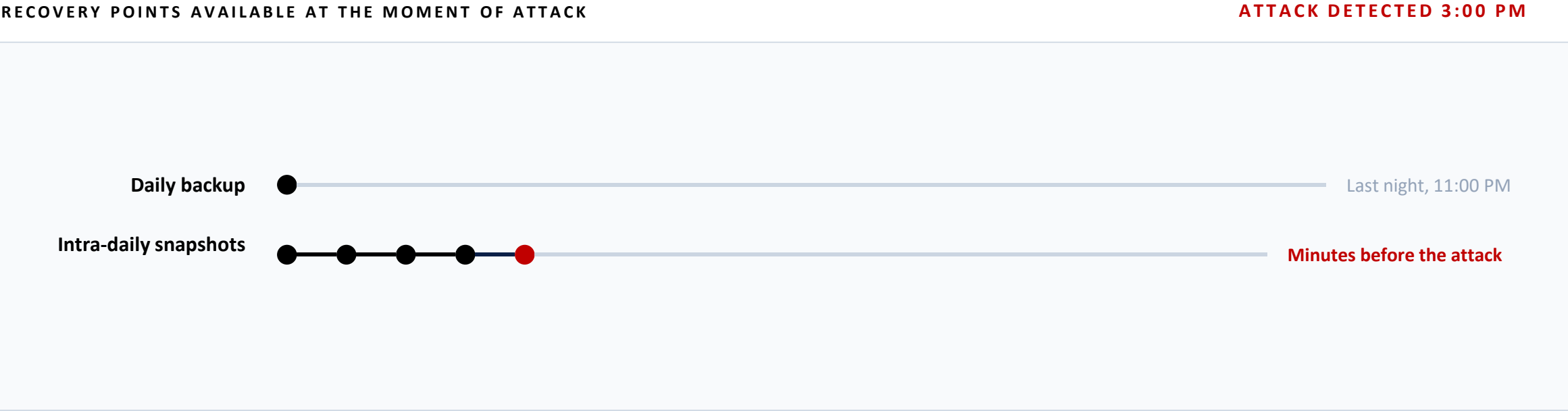
Cleared 1

| SEVERITY                                                                                                                                                                                                                               | TYPE            | POLICY        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---------------|
| Critical                                                                                                                                                                                                                               | Infection Found | Sid-2605-VMFS |
| <div><div></div><div>Infection found in Snapshots</div><div>The file's contents has been encrypted and the file extension has changed to a known ransomware extension.<br/>Policy Name: Sid-2605-VMFS</div><div>Show Files</div></div> |                 |               |

# Closing the Recovery Point Gap

## Recover From the Freshest Copy You Can Prove Is Good

If you're only scanning backups, you're only as good as your last backup and you're data loss can be up to 24 hours! With granular snapshots, that are continuously validated, not only do we improve MTTD (Mean Time to Detect), but we also mitigate data loss. And because the recover points are on production equivalent storage, restore times are dramatically faster than backup-based recoveries!



200+

Content-based analytics inspect every snapshot and backup at the byte level.

99.99%

SLA-backed ransomware corruption detection.

30 sec

Clean data recovery per validated, immutable snapshot.

## What is CyberVR?

### Operational @ Scale Recovery

HITACHI



#### Isolate & Protect

Continuous replication and high-frequency immutable snaps for low RPOs



#### Scan & Detect

Scanning of immutable snapshots, pre-encryption copies quickly identified



#### Blast Radius

Correlate runbooks and scan results to identify the affected runbooks and recovery points



#### Investigate (DFIR)

Instant hunting across index history, faster RCA and latent malware detection at scale, BYO DFIR tools



#### Recover Workloads

Single click workload recovery automation, from snap-clones, reduces RTO dramatically



#### Eradicate

Automated pre-power-on malware eradication, prevents re-infection upon recovery



#### Harden

Automated promotion to semi-connected zones for SME patching of vulnerabilities



#### Validate

Application validations ensure workloads are operational post eradication & hardening



#### Reconnect (MVB)

Automated promotion of clean workloads to functional networks – true end of RTO

# Hitachi, Index Engines & VM2020

## Delivering Confidence, Speed, and Predictability

| CAPABILITY             | AVAILABILITY-ONLY APPROACHES                              | INDEX ENGINES+ VM2020 + HITACHI VANTARA                 |
|------------------------|-----------------------------------------------------------|---------------------------------------------------------|
| Detection Accuracy     | Miss deep content corruption                              | 99.99% SLA-backed, AI-driven detection                  |
| Recovery Speed         | Days to weeks of manual testing                           | At scale recovery; e.g.: 1500 VMs in 70 minutes         |
| Reinfection Risk       | High — difficult to identify clean data points to restore | Dramatically reduced with automated malware eradication |
| Recovery Confidence    | Hope-based approach                                       | Guaranteed with Hitachi’s Cyber Resiliency Guarantee    |
| Testing and Validation | Time-consuming and error-prone                            | Continuous data validation with automated recovery      |
| Business Continuity    | Extended downtimes, uncertain timelines                   | Improved RTO (Return to Operations)                     |



# Gracias