HPE Innovation Day

How to protect against cyber crime

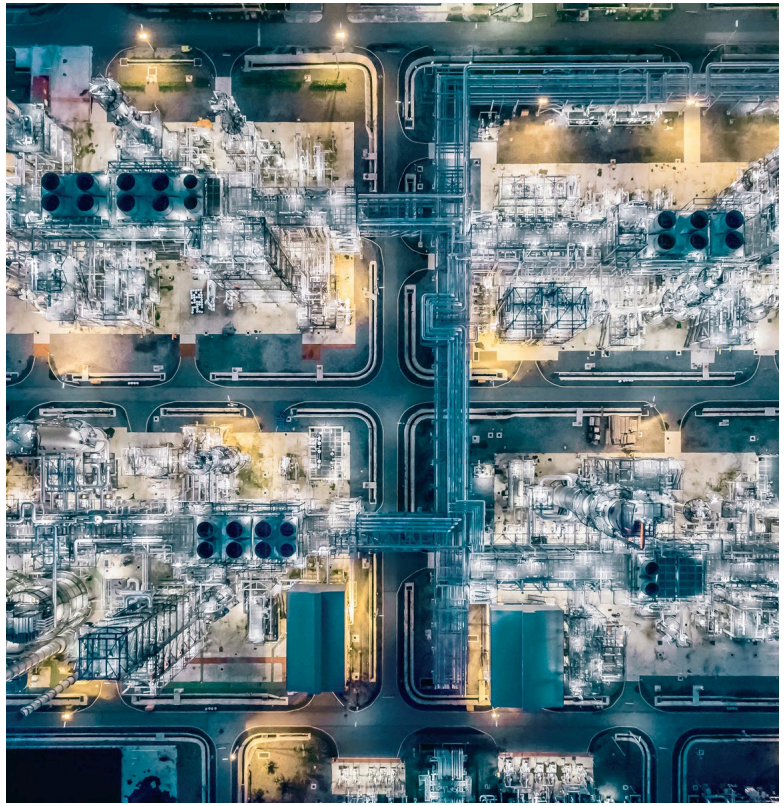
and recover fast after an attack

Egon van Dongen

Manager Sales Engineering EMEA – Zerto a Hewlett Enterprise company

Hewlett Packard Enterprise | NVIDIA

The current cyber-threat landscape

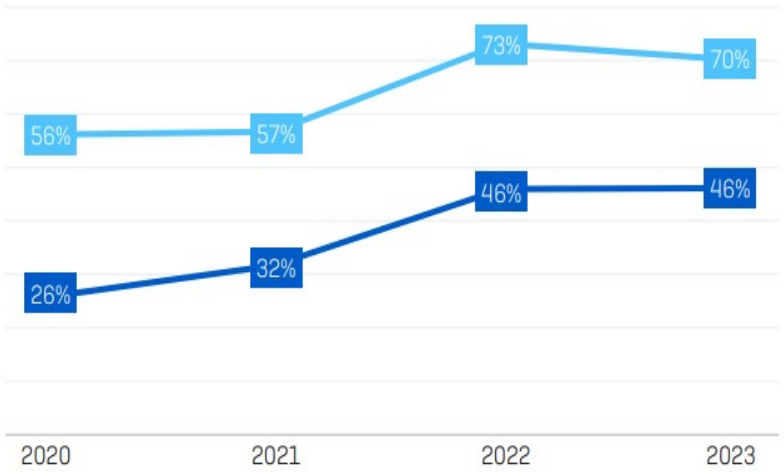


Rapid rise in use of **AI** in cyber-threats

Cyber-threats growing hugely

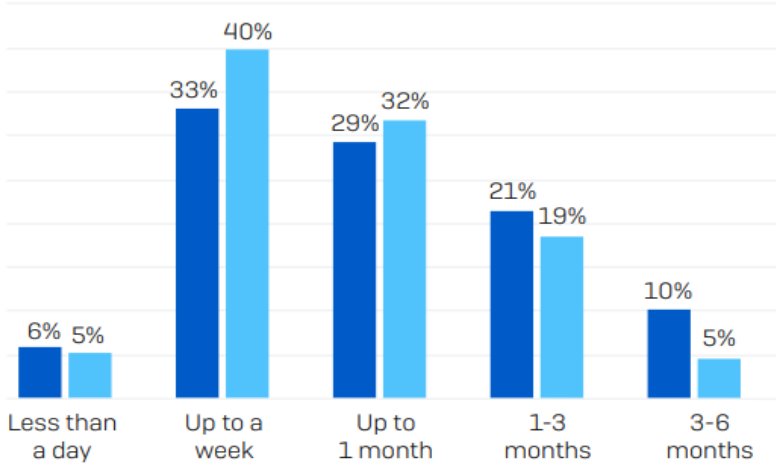
Ransomware most significant and serious cybercrime threat

Still not winning the ransomware battle



Used backups to restore data	Paid the ransom & got data back
46%	46%

Fewer people are using backups to recover than a year ago

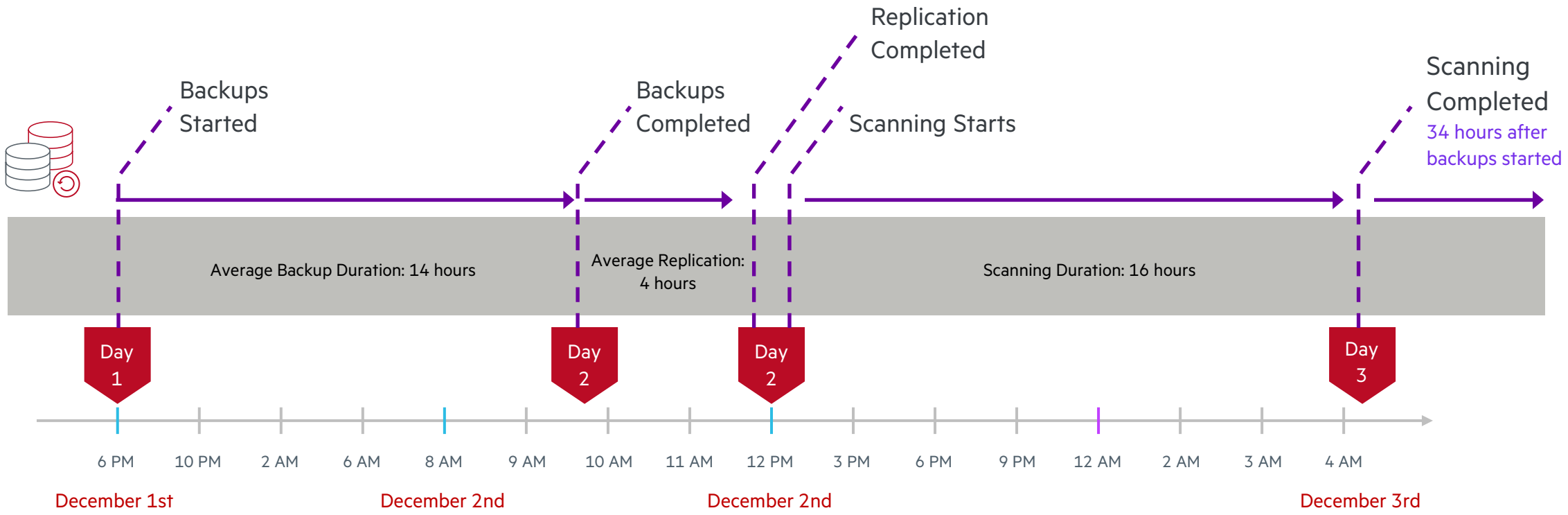


Used backups	Paid the ransom
56% took over 1 week	60% took over 1 week

Time to restore is still an issue, and still costs significant amounts of money

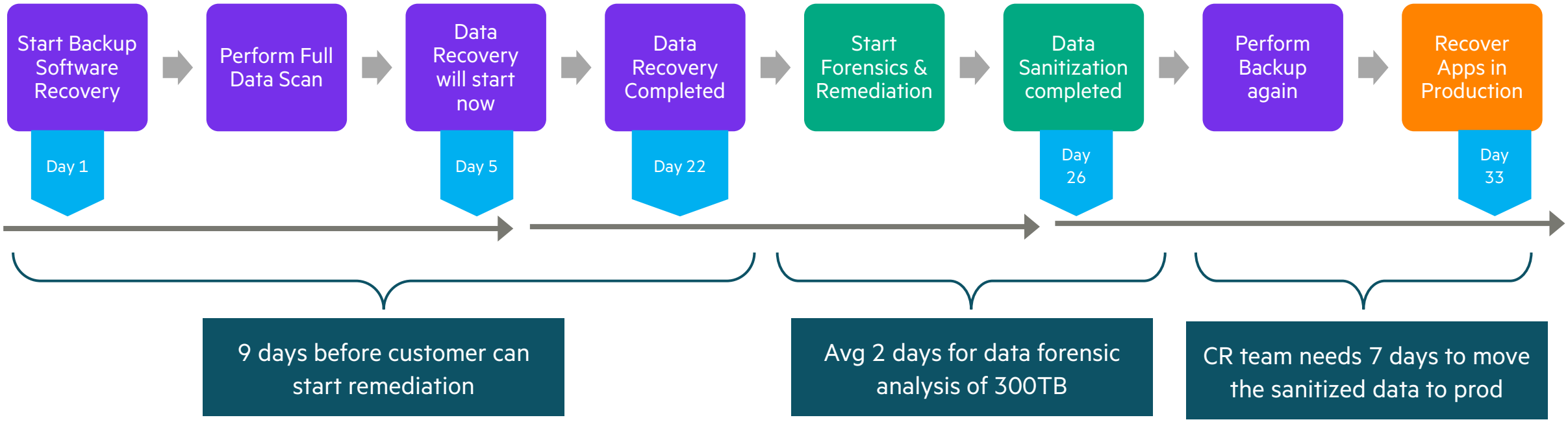
Backup cyber protection timeline

RPO = Minimum 34 hours to protect



Backup cyber recovery timeline

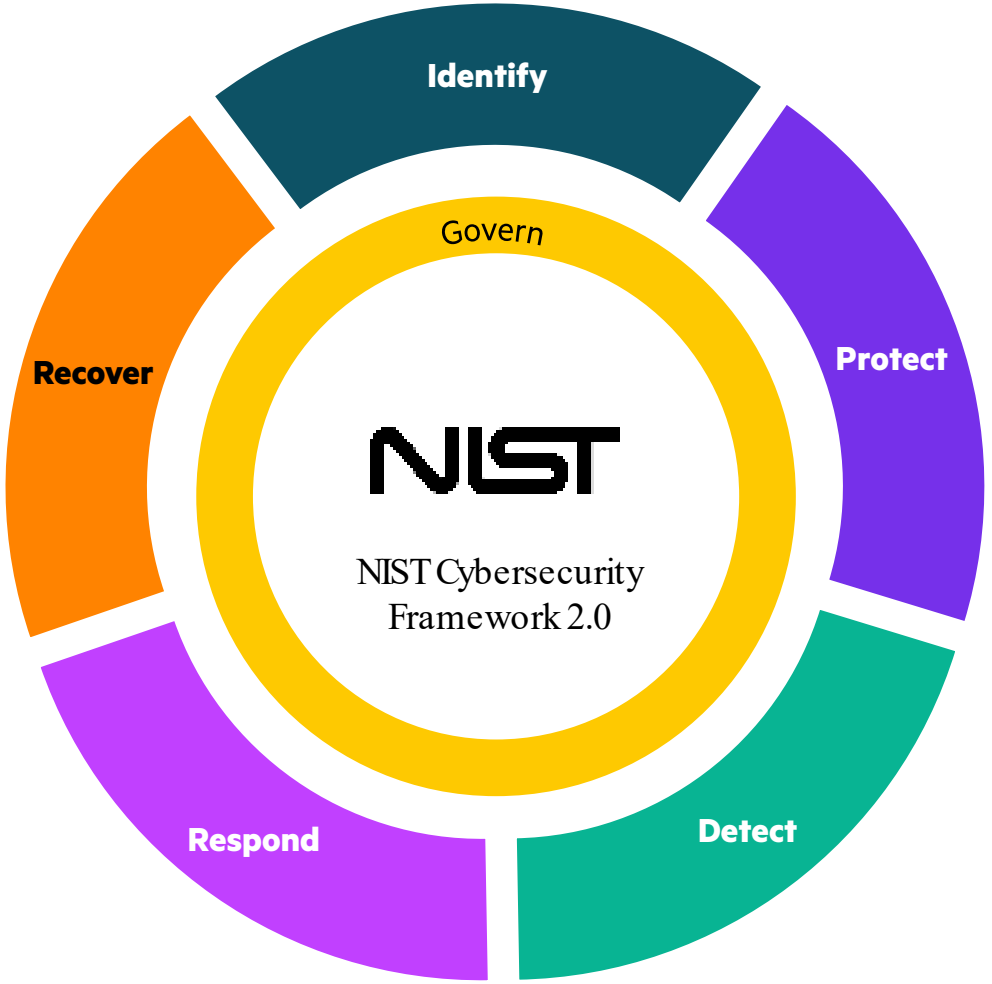
RTO = Minimum 30 days to recover

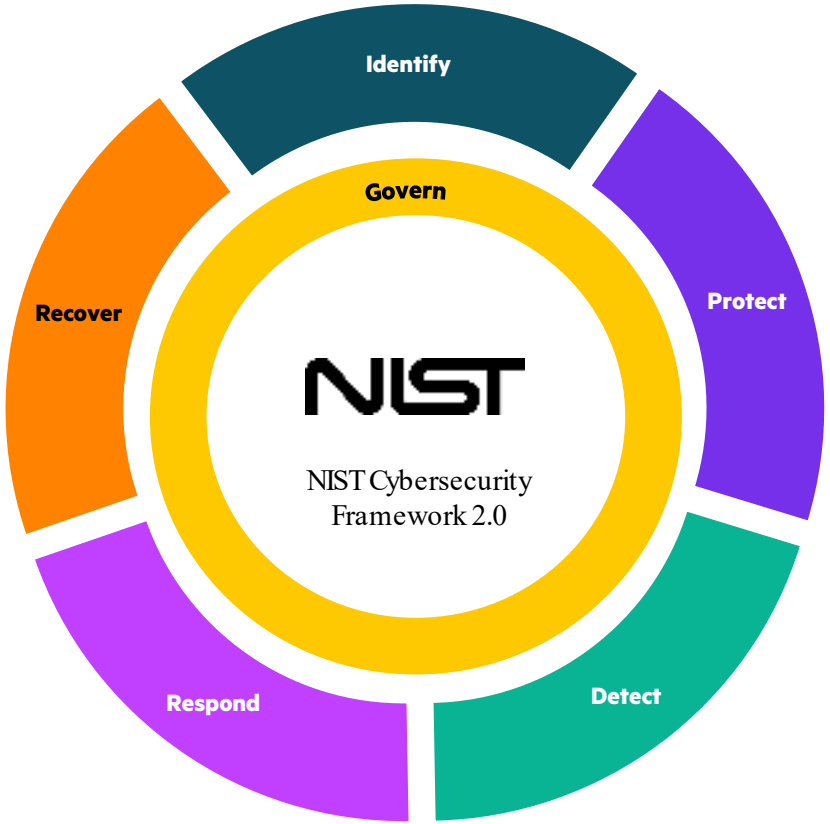


* Example using 300 TBs of front-end data

Cyber is the ~~security~~ team's issue

Cybersecurity across the whole organization





- **Govern**: Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy
- **Identify**: Help determine the current cybersecurity risk to the organization
- **Protect**: Use safeguards to prevent or reduce cybersecurity risk
- **Detect**: Find and analyze possible cybersecurity attacks and compromises
- **Respond**: Take action regarding a detected cybersecurity incident
- **Recover**: Restore assets and operations that were impacted by a cybersecurity incident

Challenges with cyber recovery

Unique problem domain with key differences from DR and backup

Unpredictable attack patterns

Since each attack can vary so much, how can we prepare for unknown unknowns and fold data protection into larger security stack?

Unknown blast radius

How can we determine what's been compromised and how extensive the lateral movement is?

Unclean recovery points

Which points in time are better to revert to and how do I know this as soon as possible?

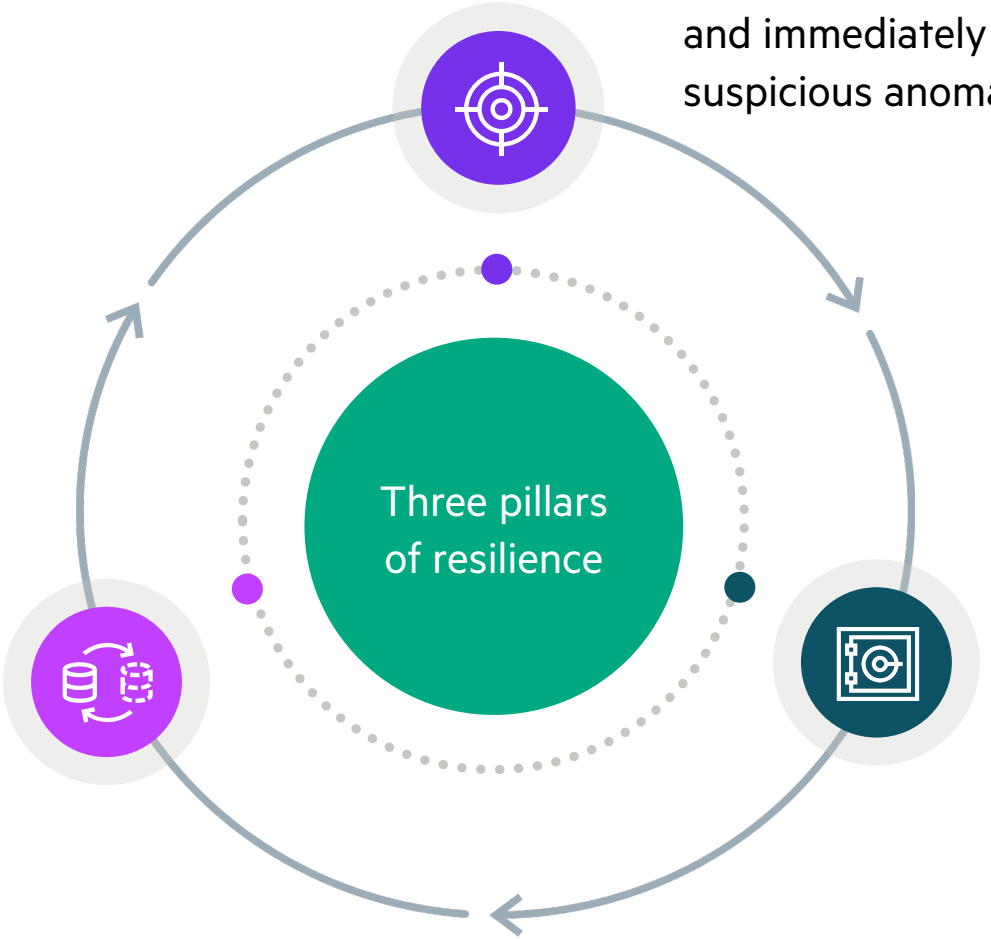
Unacceptable data loss and downtime

How do I minimize how much we lose and how long we're down? Are days and weeks of RPO and RTO an inevitability?

Three pillars of cyber resilience

#1 Replicate and detect

Streaming near synchronous data replication protects every production write in real time and immediately detects and alerts on any suspicious anomalies.



#2 Isolate and lock

Separated vault is fully air gapped and stores immutable data copies on secure, high-performance, FIPS-validated hardware.

#3 Test and recover

Easily identify clean restore points and then quickly recover entire multi-VM apps onto high-performance storage—all while maintaining cross-VM consistency.

Continuous availability from edge to cloud

Orchestration | Automation | Analytics

Disaster Recovery

Radically reduce data loss and downtime with lowest RTOs and RPOs

Ransomware Resilience

Real-time detection, protection, and cyber recovery

Multi-Cloud Mobility

Freedom to move and protect across clouds

Continuous Data Protection

vmware by Broadcom

aws

Microsoft Azure

HPE GreenLake

ORACLE CLOUD

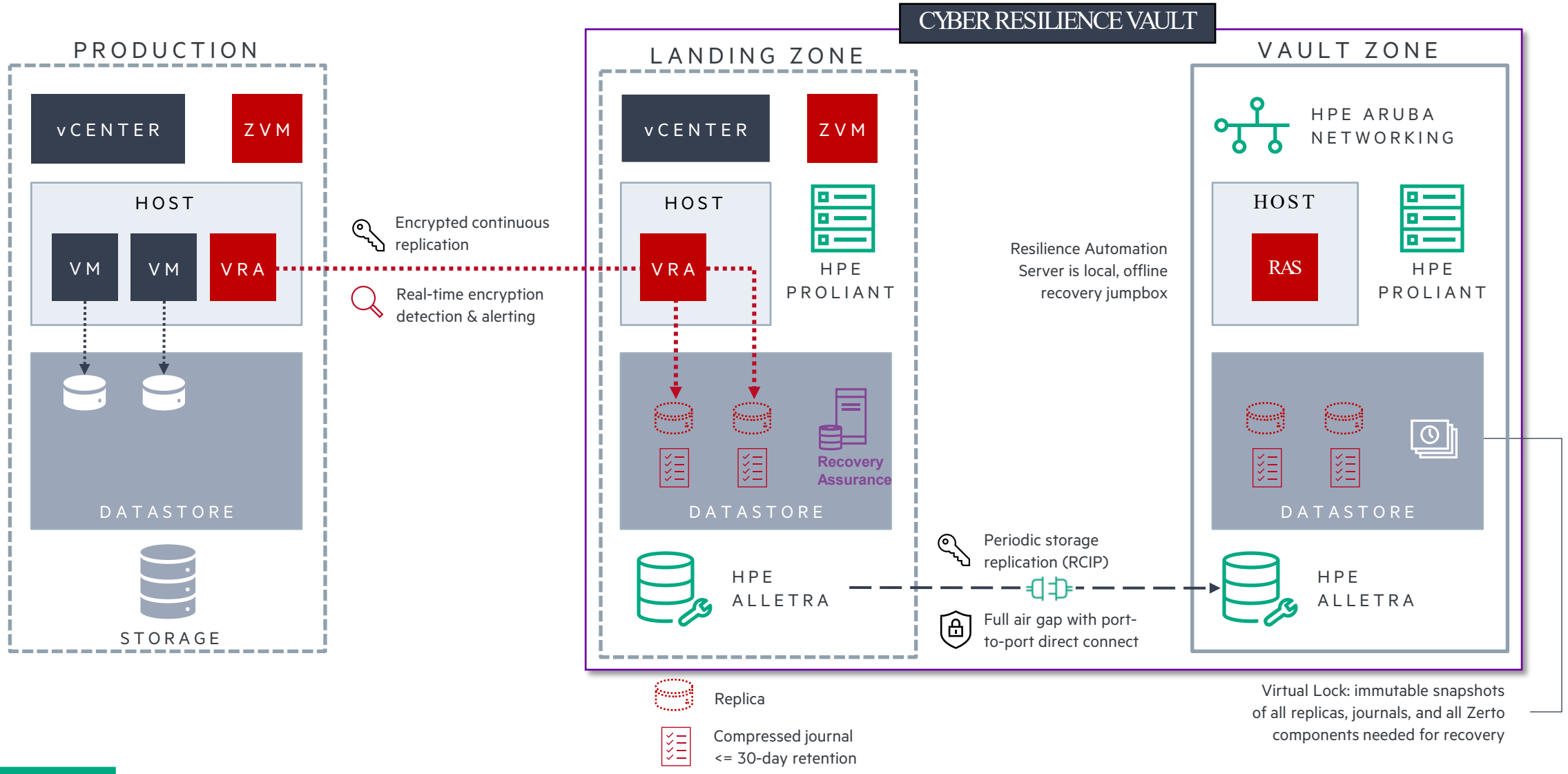
IBM Cloud

Google Cloud

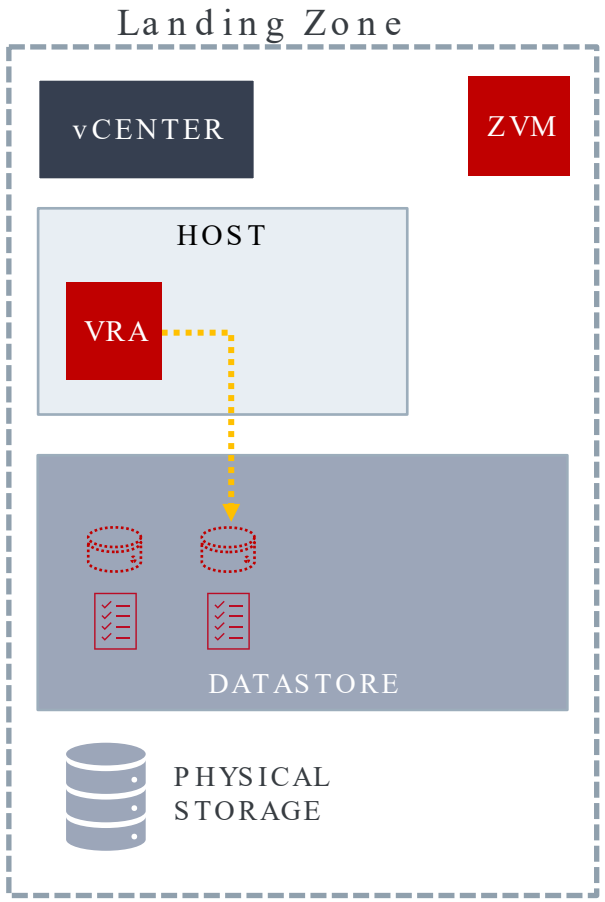
Microsoft Hyper-V

MSP

Isolate and Lock: Zerto Cyber Resilience Vault



Unique components in Zerto Cyber Resilience Vault

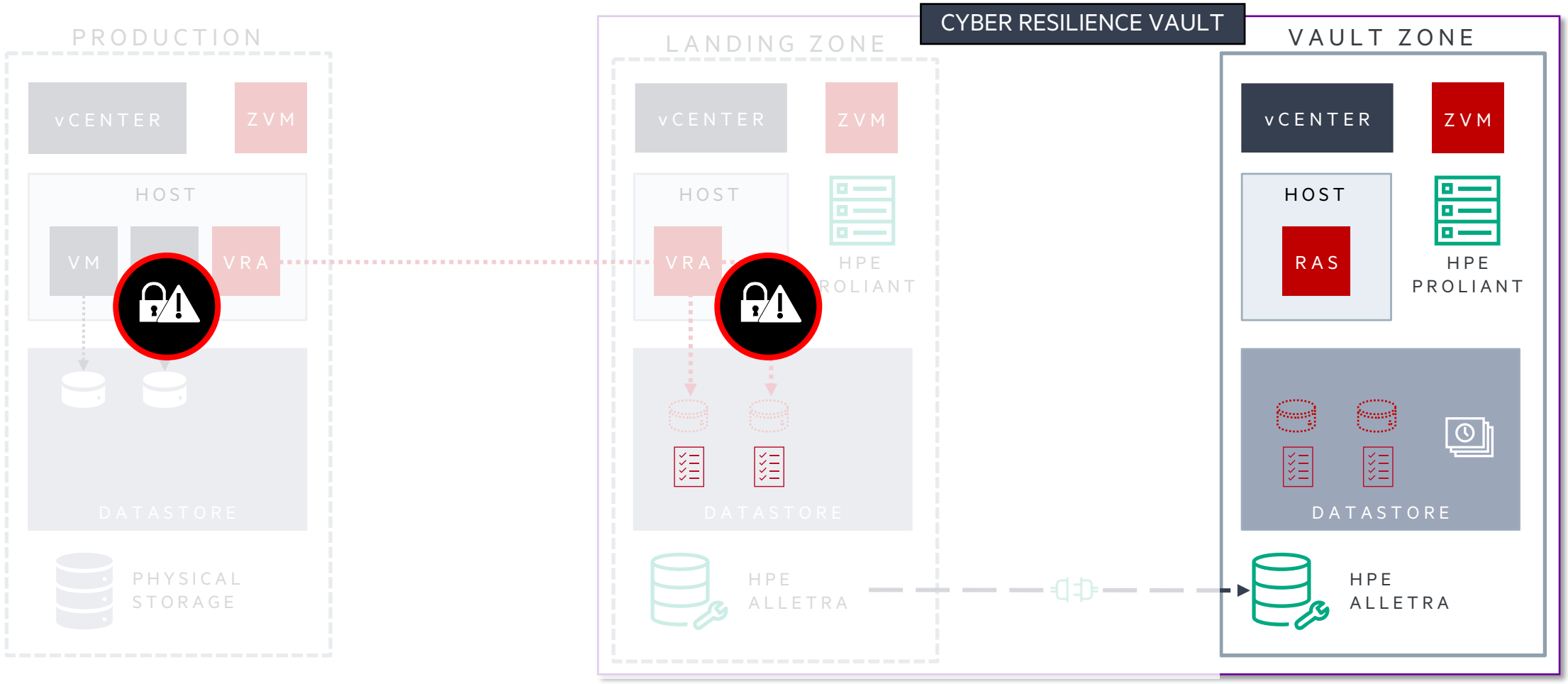


Cyber recovery from a Vault needs at minimum the following:

Immutable snapshots of the following:

- From Zerto:
  - ZVM Configuration
  - VRA Configuration
  - Replica's
  - Journal
- From VMware:
  - ESXi configurations
  - vCenter configation
- Automation and orchestration tools
- Scanning tools

Test and recover



1. Select apps or VMs to recover
2. Select clean checkpoint from journal
2. Mount VMFS from immutable snapshot
2. Power on vCenter, ESXi and Zerto VMs
3. Non-disruptively test and validate clean restore point
3. Recover from ZVR journal using clean checkpoint
4. Recover all infected workloads within minutes

Zerto Cyber Resilience Vault ROI

Rapid recovery = less ransomware impact

	Leading Backup-Based Cyber Vault *	Zerto a Hewlett Packard Enterprise company	Zerto Benefits
Last Good Copy (RPO)	2 days	4 hours or less	>87% Reduction
Time to Restore (RTO)	22+ days	2 hours	>99% Reduction
Total Ransomware Impact	3 – 5 Weeks	6 hours or less	>99% Reduction
Journal-Based Recovery	NO	YES	Only journal-based solution for cyber recovery

* Real-life example based on customer protecting 300 VMs and 300 TBs

Zerto Cyber Resilience Vault

Unlocking rapid air-gapped recovery

Fast and Secure
Air-gapped and immutable data copies on secure, high-performance, all-flash hardware.

Full Stack Solution - Combines isolated recovery environment with secure data vault using unique zero trust architecture.

Security Over Convenience - No centralized control plane: the vault has *no* exposed management port and *no* single point of compromise.

Achieve compliance at lower TCO

HPE Cyber Security Services

Deployment for HPE Storage Cyber Resilience Vault – activities and deliverables

Phase 1	Phase 2	Phase 3	Phase 4
Project coordination	**Discovery and Design**	**Implementation**	**Testing and Handover**
• Schedule a service planning session to confirm the scope, the customer requirements and desired schedule • Provide a timeline of activities to be provided during the engagement	• Discuss and agree the pre-requisites and requirements for the solution with the Customer. • Review the environment to be protected by the HPE Storage Cyber Resilience Vault solution. • Create the detailed solution design document. • **Deliverable:** Detailed Solution Design.	• Implement the Zerto software for a single VMware vCenter in the production environment. • Implement the Landing Zone environment, including the hardware components and the VMware and Zerto software environments. • Implement the Vault Zone environment, including the hardware components and the VMware software environment. • Establish replication between the environments. • Establish immutable snapshot schedules.	• Create the configuration, operational procedure and recovery procedure documents • Complete point-in-time Zerto recovery testing using a single application (one or more virtual machines) • Handover of the HPE storage cyber resilience vault solution from HPE: • Provide a knowledge transfer session. • **Deliverable:** Updated Detailed Solution Design • **Deliverable:** Operational Procedures • **Deliverable:** Recovery Procedures

Phase 1
Project coordination
• Discuss the customer responsibilities to ensure successful completion
• Organize follow-up and status meetings during the term of the service
• Coordinate delivery of the service activities
Phase 2
Discovery and Design
Phase 3
Implementation
Phase 4
Testing and Handover

Key Takeaways

1. **Ransomware** is among the **biggest threats** to data integrity today
2. **Regulators & governments** worldwide are **mandating cyber vaults** as the best approach to protect data
3. Traditional data protection approaches and vaults **aren't secure enough** and cannot recover fast enough to meet the growing threat
4. Zerto Cyber Resilience Vault provides **data immutability** and rapid **air-gapped** recovery using unique, **zero trust** architecture
5. Rapid recovery with Zerto can radically **reduce the impact** of ransomware vs. the competition—and at **lower TCO**

Thank you for joining HPE Innovation Day!

We value your feedback – would you please rate our event?

Hewlett Packard Enterprise | NVIDIA