

Hewlett Packard
Enterprise

HPE aruba
networking

Zerto
a Hewlett Packard
Enterprise company

Fortifying the Future:

The Essential Role of SASE & Cyber Vaults in Data Protection

Jason Fernyc, Consulting Systems Engineer

Chris O'Connor, Solutions Architect

March 2025



VIPSS

Victoria International
Privacy & Security Summit

Your Speakers For the Session



Jason Fernyc, P.Eng., M.Eng., CWNE
Consulting Systems Engineer
HPE Aruba Networking



Hewlett Packard
Enterprise



Chris O'Connor
Solution's Architect
Zerto, A HPE Company



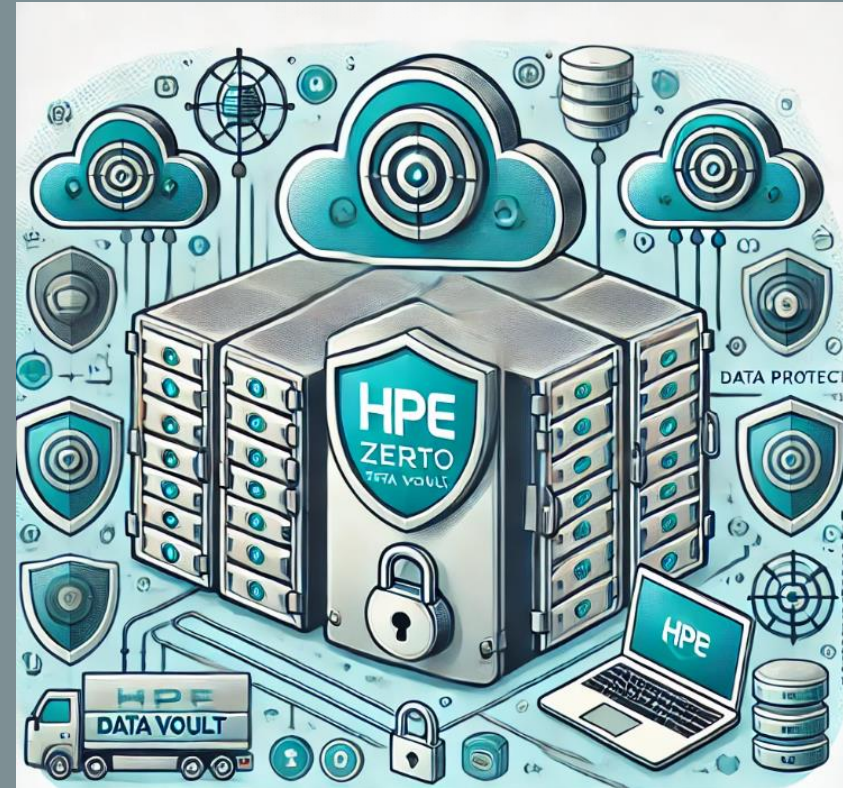
Today's Topics

HPE aruba
networking



Zerto

a Hewlett Packard
Enterprise company



"The best time to plant a tree was 20 years ago. The second best time is now." - Chinese Proverb



What Can HPE Offer You?:

Connectivity, Security & Recovery

1

Unified Connectivity from the HQ, Branch to the Teleworker

Aruba's single platform enables users & devices to connect via scalable & resilient LAN, WLAN, WAN and P5G infrastructure across any environment.

2

Network Zero-Trust & Segmentation

Aruba's platform automatically segments all network users & devices. Zero trust principles are applied across all users & devices. Prevents lateral movement of threat actors.

3

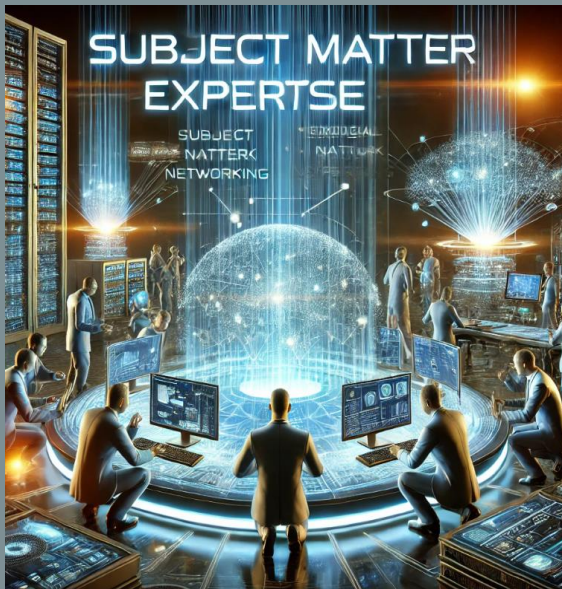
Attack Detection, Prevention & Rapid Recovery

Zerto identifies unusual data changes indicating encryption. Alert triggers automated response workflow. Systems restored to moments before attack. Recovery completed in minutes instead of days.

Our Industry Credentials

HPE **aruba**
networking

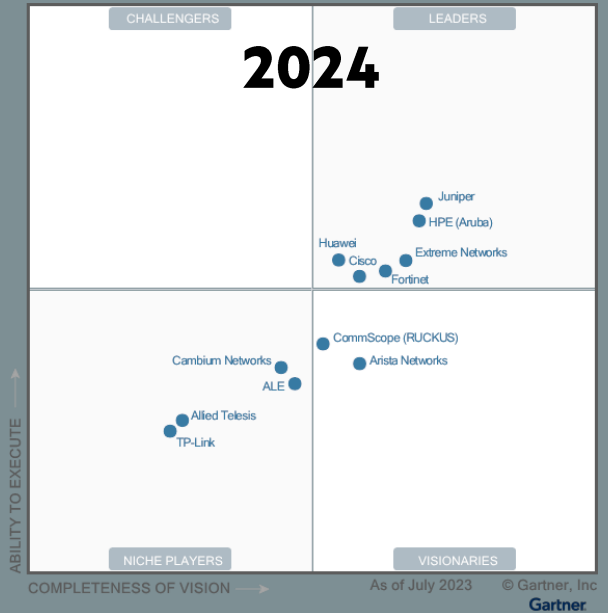
23 years in Industry



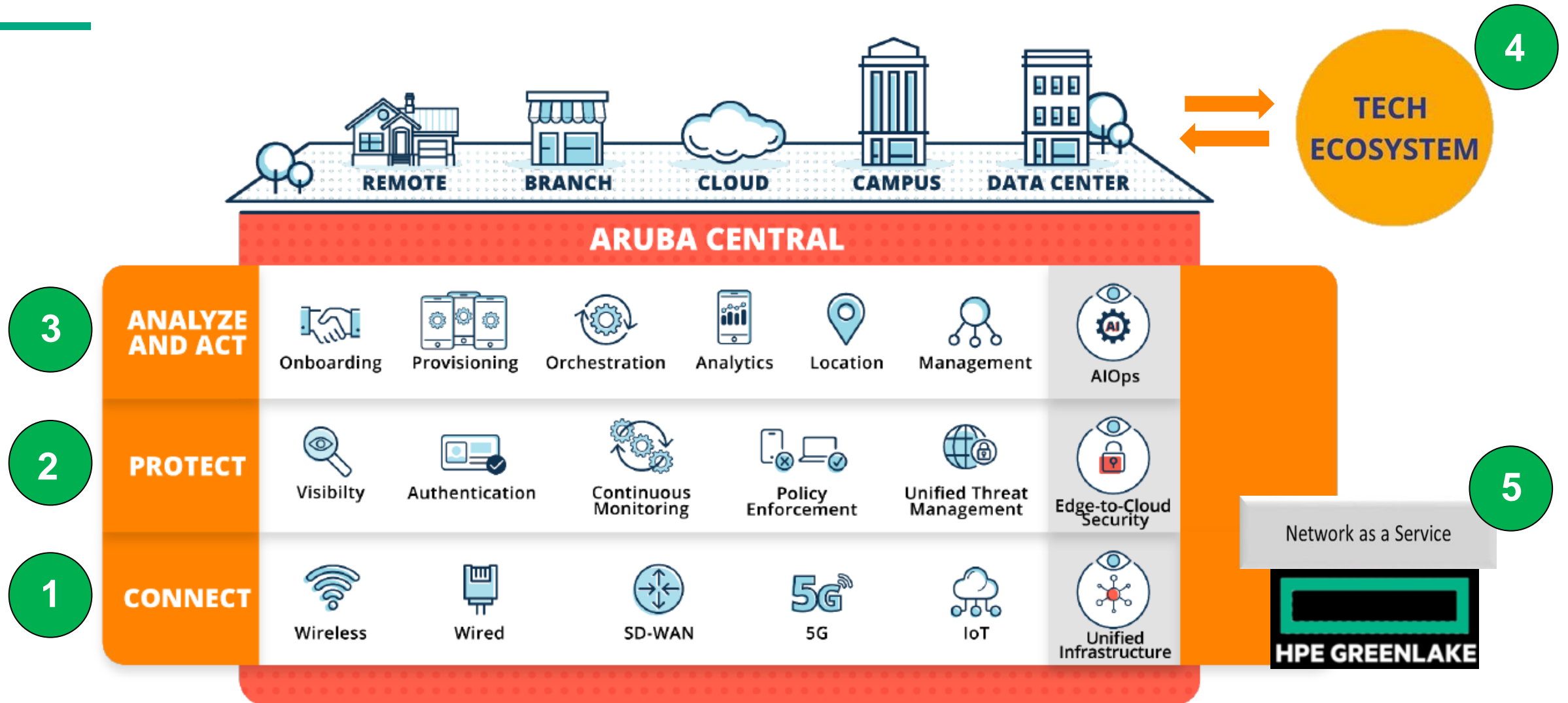
Network Business Unit



Leader 18+ years



Aruba Networking's End-To-End Solution Architecture



Top challenges we hear from customers



Connectivity Needs Expanding

Providing Reliable, Scalable, Ubiquitous connectivity across the business

Evolving Security Needs

Rapid expansion of Bad Actors, Threat landscape & Attack Surface



Managing it All

The applicability of Cloud Management & AI Operations

Affordability Challenges

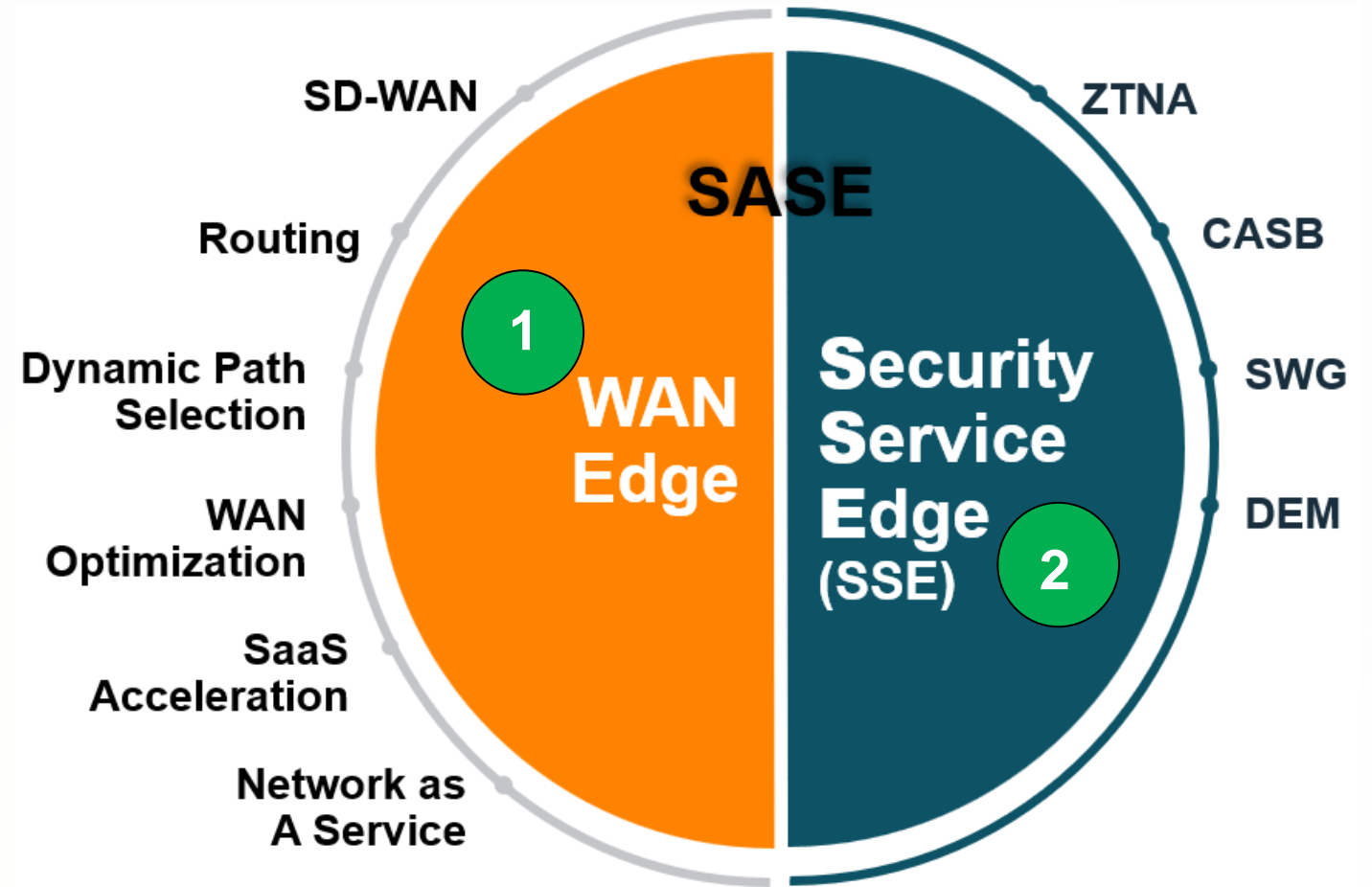
Balancing IT & Security spend against ROI & Risk





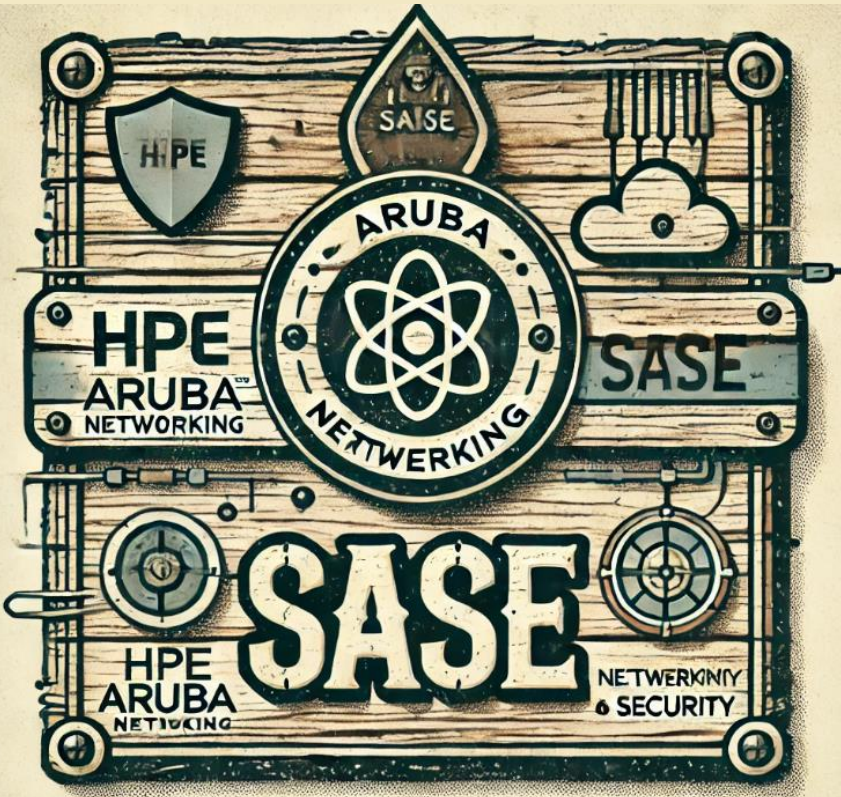
The SASE Framework:

Combining Connectivity & Security



Key Benefits of SASE

Delivering Connectivity & Security



Enhances Your Security

Apply consistent security policies across all locations and users. Eliminate security gaps with a unified control plane and centralized security policies.

Reduces Your Complexity

Consolidate multiple point/silo solutions into a single platform. Simplify management with integrated workflows.

Optimizes Experience For All

Ensure fast, reliable access to applications. Prioritize business-critical traffic with intelligent dynamic routing. Streamline Your Operations.

Future-Ready Scalability

Adapt quickly and efficiently to changing business requirements. Support new locations and users without traditional hardware constraints.



Key Capabilities of HPE Aruba Networking SDWAN

- 1 Performance & User Experience**
Recognizes applications on the first packet. Applies appropriate security and QoS instantly.
- 2 Intelligent Traffic Handling**
Routes traffic based on business priority. Selects optimal paths across multiple WAN connections, Direct Internet Access (DIA) and/or Cloud.
- 3 End-To-End Visibility**
View users, devices & applications across on-premises, data center and Cloud environments.
- 4 Integrated Security**
Leveraging Firewall, IDS/IPS and Advanced behaviour Analytics technologies all in a single platform.
- 5 Built-In WAN Optimization**
Improves application performance. Includes industry unique deduplication, compression, and protocol acceleration.

Key Capabilities of HPE Aruba Networking SSE



- 1 Zero Trust Network Access (ZTNA)**
Enforce least-privilege access to applications. Replaces traditional VPNs with identity-based, context-aware access controls.
- 2 Secure Web Gateway (SWG)**
Protect users from web-based threats. Enforce acceptable use policies and prevents data loss.
- 3 Cloud Access Security Broker (CASB)**
Provide visibility into SaaS applications. Enforce data security policies, implement DLP strategy, and prevent shadow IT.
- 4 Digital Experience Monitoring (DEM)**
Deliver end-to-end visibility of real-time user experience across diverse networks, devices and geographies.



HPE Aruba Networking: **Summary**



Ubiquitous Connectivity

Provide Scalable & Resilient networking for every user, device across a wide range of environments to suit every use case that your organization requires.



Zero-Trust & Segmentation

Respond to increasing threats even before they have an opportunity to manifest. Response protocols activate automatically to contain risks.



AI-Powered Operations

Advanced analytics provide unprecedented network visibility. AI identifies anomalies before they become threats or impact performance.



Hewlett Packard
Enterprise

Zerto Cyber Resilience Vault

Unlocking rapid air-gapped recovery

Chris O'Connor, Solutions Architect

March 2025

Top challenges we hear from customers



Evolving threats

Last year, 61% of disaster responses were triggered by **ransomware**¹



Slow speed of recovery

Average time to recover from ransomware is **one month**²

Ransomware's dilemma

Lose data or pay ransom—and **only 4%** of those who paid got all their data back²



Staying in compliance

Myriad standards & regulations, e.g. GDPR, SOX, HIPAA, DORA, FISMA



1 The State of Ransomware and Disaster Preparedness: IDC
2 Sophos: The State of Ransomware

Cyber vaults are increasingly mandated



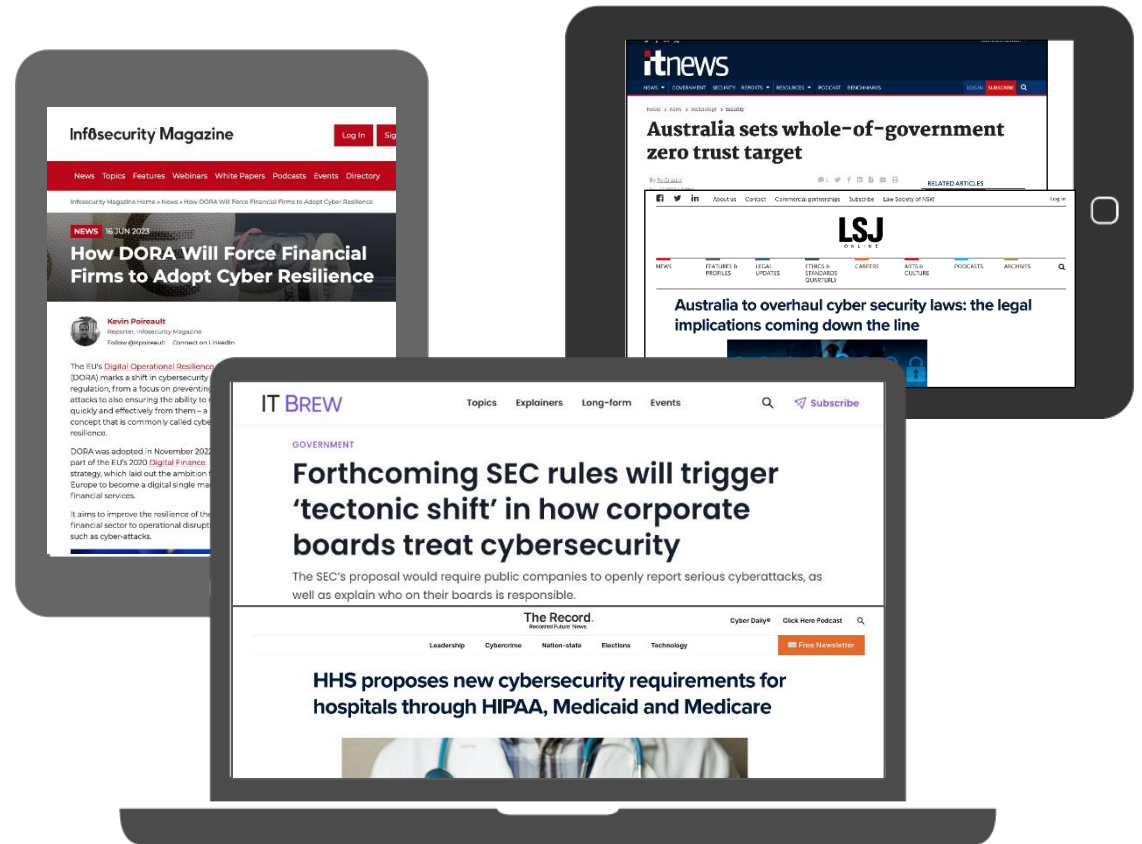
Regulators, legislators, and insurers are requiring vaults as best option to protect against cyber attacks



Need to protect your data protection solution — must plan for what happens if backups are compromised

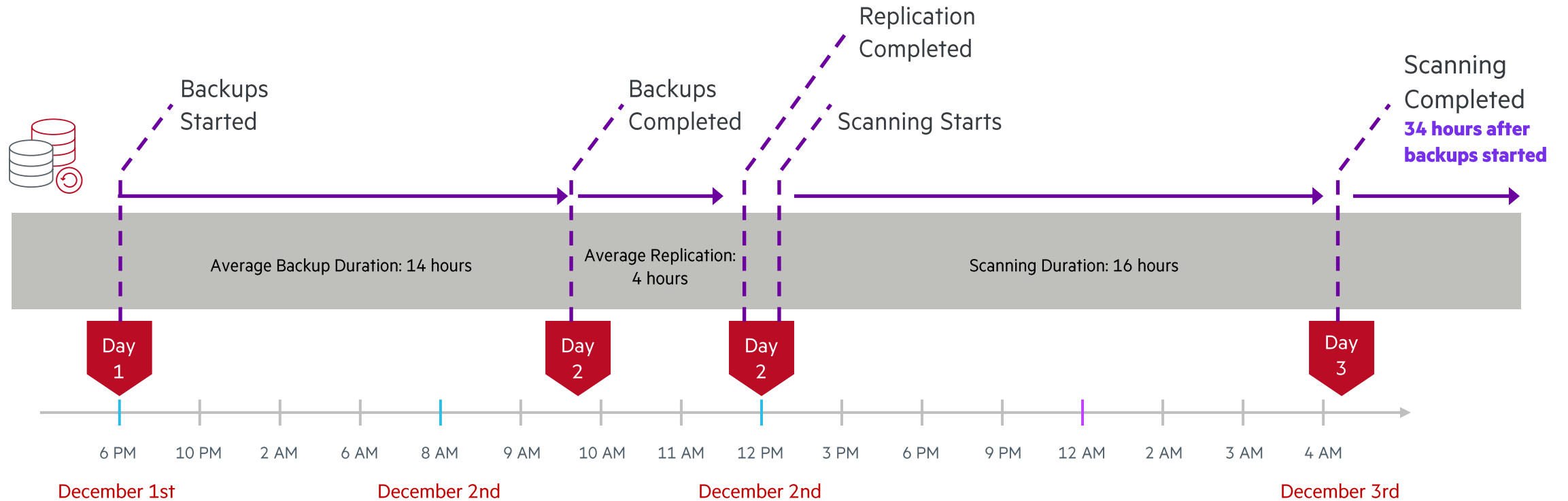


Always need emergency option of last resort in case all else fails; part of defense-in-depth



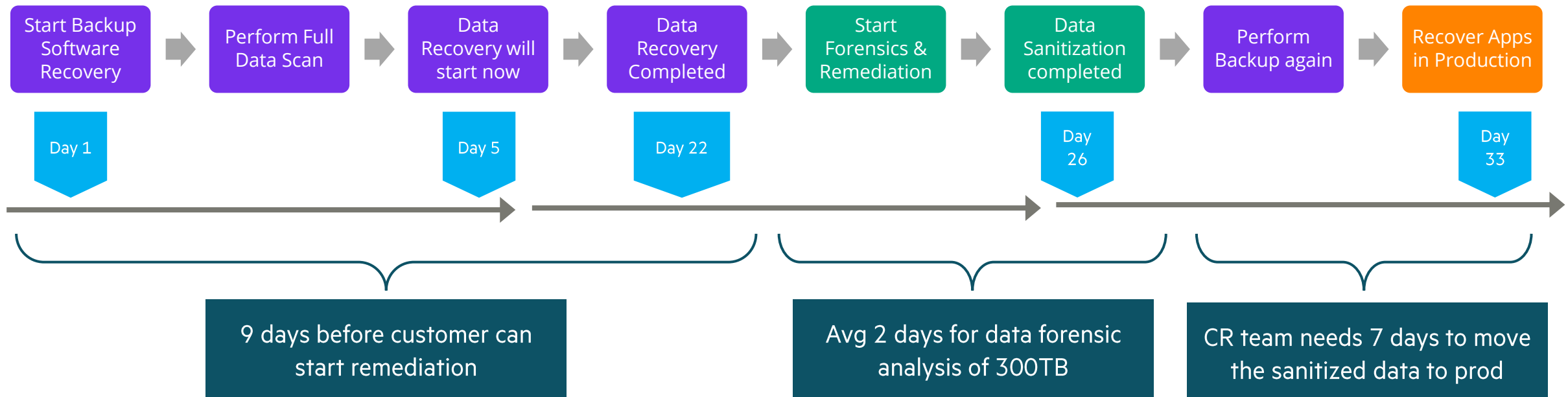
Backup cyber protection timeline

RPO = Minimum 34 hours to protect



Backup Cyber Recovery Timeline

RTO = Minimum 30 days to recover



* Example using 300 TBs of front-end data

Zerto

Continuous availability from edge to cloud



vmware®

aws

Microsoft Azure

HPE GreenLake

ORACLE
CLOUD

IBM Cloud

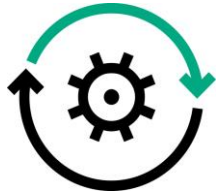
Google Cloud

MSP

Microsoft
Hyper-V

Leader in data protection since 2011

Eliminate data loss and downtime with continuous data protection



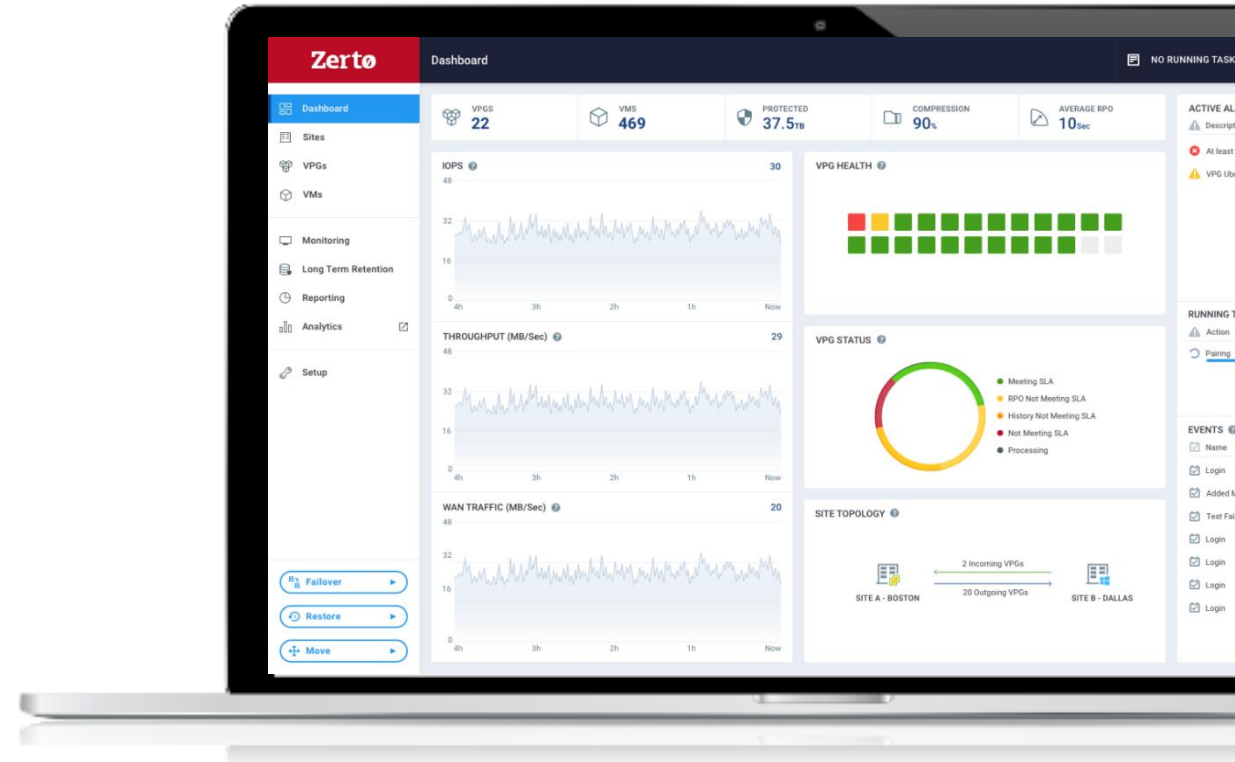
Software-only, hypervisor-based replication for flexible, always-on protection without storage lock-in



RPOs of seconds and RTOs of minutes to quickly restore operations by rewinding and resuming from any point in time from the past

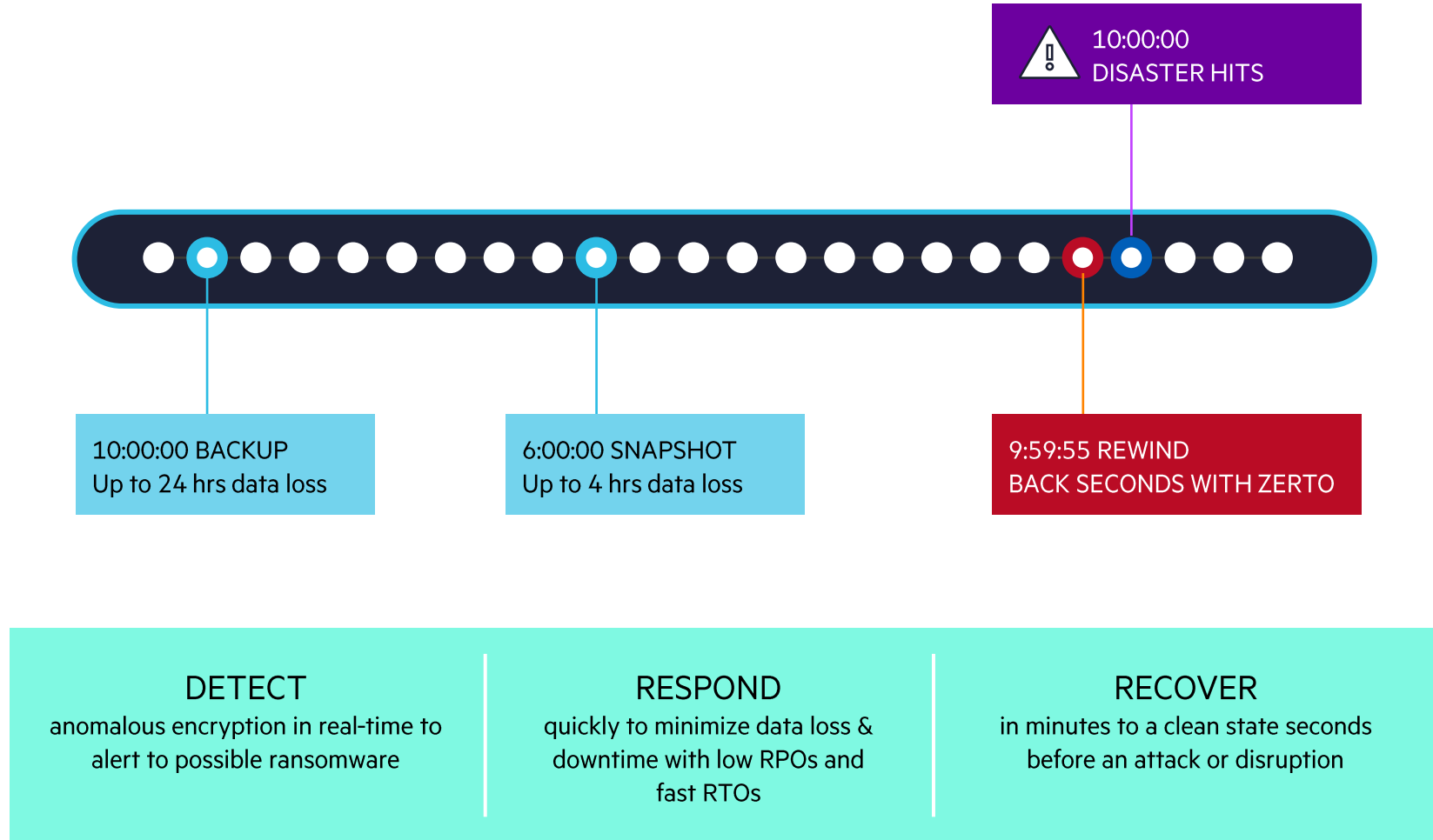


Orchestrated failover, failback, and non-disruptive testing to easily recover files, VMs, or multi-VM app stacks



Replicate and detect

Granular, point-in-time recovery with the dynamic Zerto journal



Replicate and detect

Replicate every change and log as recovery checkpoints every 5-15 seconds

The screenshot shows a window titled "Zerto Journal" with a list of recovery checkpoints on the left and a detailed view of a suspicious anomaly on the right. The checkpoints are listed with timestamps from 05/18/24 9:54:55 down to 05/18/24 9:53:26. The detailed view shows a yellow warning icon and the text "Suspicious anomaly".

Timestamp	Event
05/18/24 9:54:55	
05/18/24 9:54:51	
05/18/24 9:53:45	Suspicious anomaly
05/18/24 9:53:38	
05/18/24 9:53:31	
05/18/24 9:53:26	

Detect suspicious writes as they stream in and flag for admins to investigate

“[Zerto’s] real-time ransomware detection puts us in a much stronger position to both identify and mitigate ransomware attacks. This gives us confidence that we can proactively meet the risks presented by ransomware.”

– Network admin at manufacturing customer

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

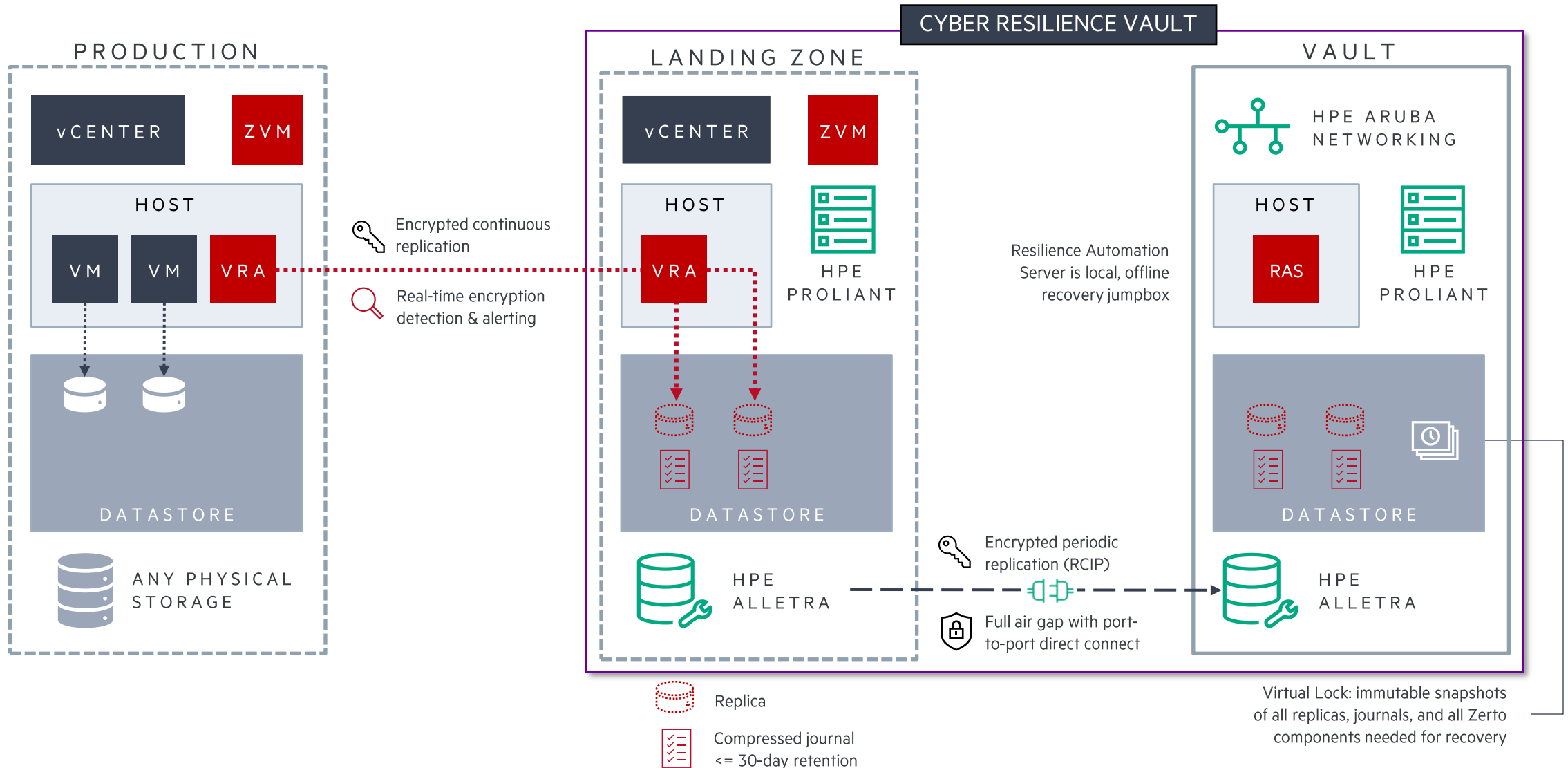
Separated vault is fully air gapped and stores immutable data copies on secure, high-performance, FIPS-validated hardware.

#3 Test and recover

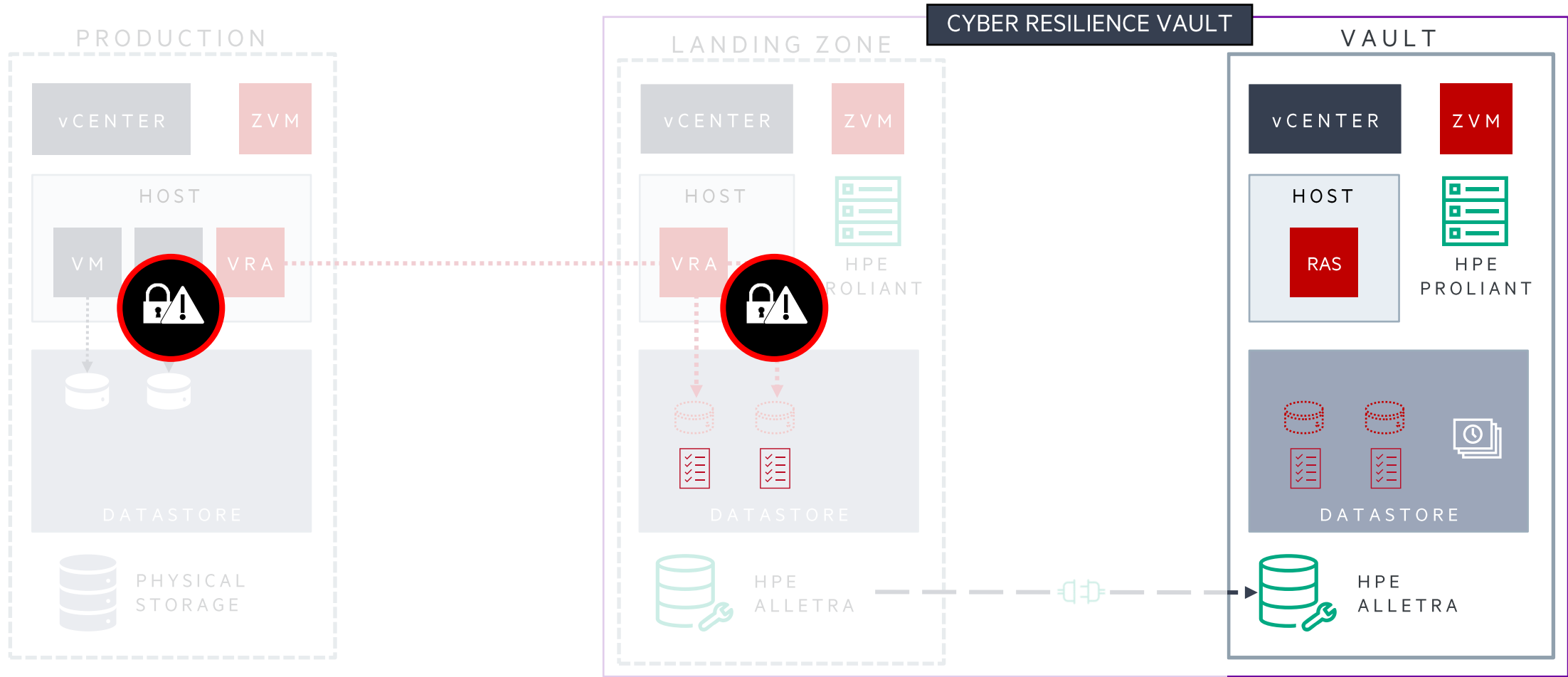
Easily identify clean restore points and then quickly recover entire multi-VM apps onto high-performance storage—all while maintaining cross-VM consistency.



Isolate and Lock: Zerto Cyber Resilience Vault



Test and recover



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



Zerto Cyber Resilience Vault ROI

Rapid recovery = less ransomware impact

	Leading Backup-Based Cyber Vault *	Zerto <small>a Hewlett Packard Enterprise company</small>	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



Thank you

