VMware Live Recovery

Cyber and Data Resiliency for VMware Cloud Foundation

VMware Live Recovery At-a-Glance

VMware Live Recovery is powerful Cyber and Data Resiliency for VMware Cloud Foundation. It provides protection against ransomware and other disasters on-premises or in the cloud with a unified management experience, accelerated recovery, and simplified consumption with flexible licensing across use cases.

Why VMware Live Recovery?

- ✓ Ransomware and Disaster Recovery across VMware Cloud in one unified management experience
- ✓ Confident, Accelerated Recovery from Modern Ransomware
- ✓ Flexible Licensing across use cases and clouds

Embracing a cloud strategy enables organizations to leverage a diverse range of options, ensuring that applications and data are optimally placed. However, as the landscape expands, so do the challenges of safeguarding critical data against ransomware attacks and other cybercrime.

Increasing sophistication and cost of cyberattacks

Ransomware and other cybercrime is vastly different than merely a few years ago. More attackers are moving away from traditional malware – in fact, most attacks today exclusively use fileless techniques. A fileless attack is one in which the attacker uses existing software, legitimate applications, and authorized protocols to carry out malicious activities. Examples include embedding malicious code directly into memory and hijacking native tools such as PowerShell to encrypt files.

These attacks are costly. According to IBM's Cost of a Data Breach 2024[1], the global average cost of a data breach increased 10% in just one year, reaching USD 4.88 million - the biggest jump since the pandemic. Business disruption and post-breach response activities drove most of this yearly cost increase.

Data is Fragmented

Complex environments often lead to data fragmentation, as data becomes dispersed across distributed data centers, public clouds, and edge devices. This dispersion makes it challenging to maintain centralized visibility and exposes the data to various vulnerabilities.

Inconsistent operating models

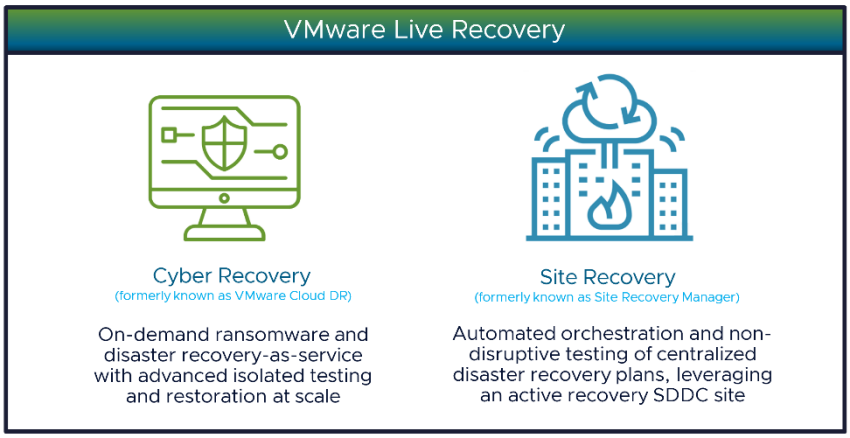
Each data center and cloud provider has its own operating model and services, creating a complicated landscape. The lack of consistency across these entities forces companies to protect their infrastructure using disjointed tools and processes. When a ransomware attack or other disaster occurs, recovery is long and unpredictable due to the many tools and manual processes involved.

VMware Live Recovery

VMware Live Recovery addresses these challenges by providing ransomware and disaster recovery across VMware Cloud Foundation in one unified management experience. It provides confident, accelerated recovery for all VMs across on-premises and public clouds. All of this is simplified by allowing consumption via a flexible licensing model across use cases and cloud infrastructure.

One + One = More

Customers may choose between recovery models – Cyber Recovery and Site Recovery – while still maintaining a single offering, and the ability to add functionality as business needs change. VMware Live Recovery combines these proven VMware technology solutions into a unified management experience, licensing model, and support structure to ensure consistent orchestration and workflows without multiple point solutions.



Cyber Recovery

VMware Live Recovery provides Ransomware and Disaster Recovery across VMware Cloud with advanced isolated testing and restoration at scale.

Managed Recovery Environment
Enable a safe, controlled recovery with an environment secured, built, and managed by VMware.

Push-Button VM Network Isolation
Isolate VMs from one another at restore to prevent lateral movement of ransomware and reinfection of the production environment.

Live Behavioral Analysis
Identify fileless attacks with embedded Next-Gen AV and Behavioral Analysis of powered-on workloads.

Guided Restore Point Selection
Inform selection of restore point candidates with insights such as VMDK rate of change and file entropy.

Ransomware Recovery Workflow
Leverage a step-by-step guided workflow that integrates identification, validation and restore of recovery points within a single UI.

Immutable, Air-Gapped Recovery Points
Store snapshots in a secure, VMware-managed Scale-Out Cloud File System to preserve data integrity at the time of recovery.

Site Recovery

Site Recovery automates orchestration and non-disruptive testing of centralized recovery plans for all virtualized applications

Built-in nondisruptive testing ensures your recovery time objectives (RTOs) are met. Site Recovery Manager integrates with a vast ecosystem of underlying replication technologies, providing maximum flexibility. VMware vSphere Replication provides VM-based replication, supporting a large variety of underlying storage solutions with recovery point objectives (RPOs) ranging from 1 minute to 24 hours.

Simple, Policy-Based Management	Compatible With Any Storage	Next Generation vSphere Replication
Use policy-driven automation to protect thousands of virtual machines easily using centralized recovery plans managed from the vSphere Web Client.	Experience flexibility and choice through native integration with vSphere Replication, Virtual Volumes (vVols), and array-based replication solutions from all major VMware storage partners.	Achieve increased RPO granularity with recovery points as frequent as just 1 minute

"When it comes to cybersecurity, we can sleep soundly and continue to bring joy to our customers"

- Gregory Schurgast
CTO, Vente-unique

"We now have the ability to move critical workloads across data center sites based on any contingency"

- C. K. Prasad
Regional GM & Head - IT
RailTel Corporation

The Impact of Cyber Crime

It's not *if* - it's *when*

✓ Ransomware attacks are proliferating to become the #1 cause of disaster recovery events today. 59% of organizations were attacked by ransomware in 2024, and 70% of them had their data encrypted (*Source: Sophos*).

Backups are Targeted

✓ Astaggering 94% of victims said attackers targeted their backups – and 57% of backup attempts were successful (*Source: Sophos*).

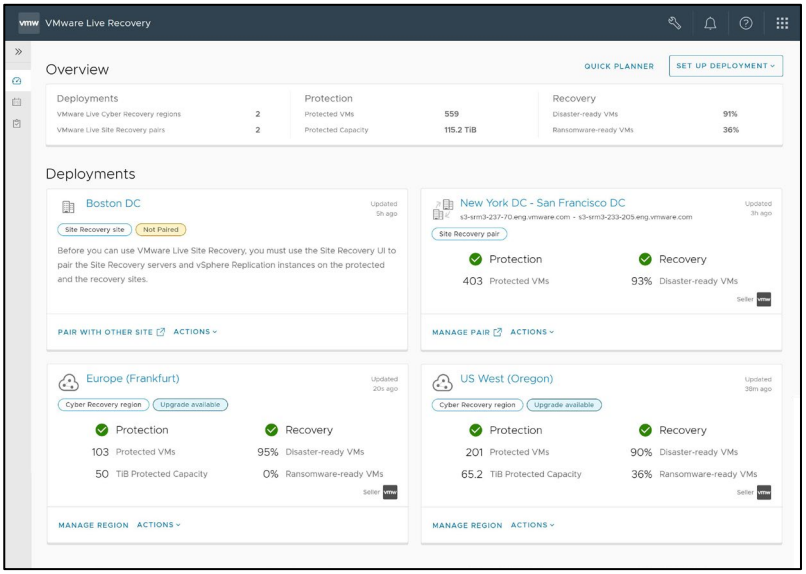
The cost beyond Ransom

✓ The average cost of a ransomware attack (not including the ransom itself) is $4.88M (*Source: IBM*). As a result, the need for organizations to better protect and recover their data has become an urgent business imperative.

[1] IBM Cost of a Data Breach Report 2024

VMware Live Recovery Management Console

Centralized SaaS console enables complete control over all aspects of data collection, Ransomware recovery, Site recovery, automation and execution of disaster recovery on-prem or in the cloud.



Licensing Flexibility

Simplified subscription licensing for VMware Live Recovery helps organizations achieve complete VMware cyber and data protection quickly by centralizing the licensing under a single subscription. While a customer may use one element of the solution, they may add another and further expand their functionality. For example, customers using Cyber Recovery on one VM node can use another VMware Live Recovery license to enable Site Recovery on the same node and take advantage of the benefits of both.

VMware Live Recovery delivers powerful cyber and data resiliency for VMware Cloud Foundation. It provides unified protection for ransomware and disaster recovery across the cloud in one unified console, secure cyber recovery, and simplified consumption with flexible licensing across use cases and clouds.

To learn more about how **VMware Cloud Foundation** and **VMware Live Recovery** can help you protect your business, visit **https://www.vmware.com/** or contact your VMware representative

vmware by Broadcom

Item No: VMware Live Recovery - Solution Overview May-25