# VMware Live Recovery

Cyber and Data Resiliency for VMware Cloud Foundation

## VMware Live Recovery At-a-Glance

VMware Live Recovery delivers powerful cyber and data resiliency for VMware Cloud Foundation. It provides ransomware and disaster recovery in a unified management experience, accelerated recovery, and simplified consumption with flexible licensing across use cases and clouds.

## Why VMware Live Recovery?

- ✓ Ransomware and Disaster Recovery across VMware Cloud Foundation in one Unified Management Experience
- ✓ Confident, Accelerated Recovery from Modern Ransomware
- ✓ Flexible Licensing across use cases and clouds

Safeguarding critical data against ransomware attacks, cybercrime and other disasters is critical to the ongoing success of modern organizations.

VMware Live Recovery complements the powerful features of VMware Cloud Foundation by providing advanced data resiliency and site protection capabilities. VMware Live Recovery is a critical last line of defense against cyber threats, to deliver confident, accelerated recovery.

## Increasing sophistication and cost of cyberattacks

Ransomware and other cybercrime is vastly different than merely a few years ago. Attackers are moving away from file-based malware – in fact, 80% of attacks today[2] use exclusively 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.

Even the common approach of immutable, air-gapped backups is not enough. To ensure threats are identified, contained, and not reintroduced, it's important to power on a potential restore point in a fully isolated recovery environment to run behavioral analysis tests before putting the system back into production.

These attacks are costly. The recent IBM Cost of a Data Breach[1] report indicates that the average cost of a ransomware attack is $4.45M, an increase of more than 2% from the previous year.

## What is needed for Modern Recovery?

When a ransomware attack or other disaster occurs, recovery is long and unpredictable because the nature of cyber-attacks. Recent recovery points will almost certainly be infected, so it's crucial to balance between selecting an uninfected point in time without going too back historically. In addition, the process of recovery point selection can be time consuming, with repeated resource-intensive testing that (if not entirely separated from the main data center) could reintroduce infections to the wider network through lateral movement. To prevent this, isolated recovery environments are necessary to fully separate production workloads. And lastly, each of these strategies need to be orchestrated at scale.

## Introducing VMware Live Recovery

VMware Live Recovery brings together the power of VMware's proven solutions to allow customers to extend their on-premises DR to the public cloud and also integrates cyber-recovery into a centralized management experience. It provides confident, accelerated recovery from cyber-attacks and other disasters across on-premises and public clouds. All of this is simplified by allowing consumption via a flexible licensing model with a single subscription across use cases and cloud infrastructure. VMware Live Recovery uniquely enables a cyber and data resilient private cloud.

vmware by Broadcom

**" I have yet to see a recovery product for ransomware that works as well as VMware's."**

Worldwide Director of Infrastructure
US-Based Global Asset Management Firm

## One + One = More

VMware Live Recovery combines two proven VMware technology solutions into a unified entry console, licensing model, and support structure.

- **VMware Live Cyber Recovery**
  (formerly VMware Cloud Disaster Recovery + VMware Ransomware Recovery)
- **VMware Live Site Recovery**
  (formerly VMware Site Recovery Manager)

Customers may choose between recovery models while still maintaining a single subscription, with the ability to add functionality with its flexible licensing model.

## VMware Live Cyber Recovery

VMware Live Cyber Recovery provides Ransomware and Disaster Recovery as-a-service across VMware Cloud Foundation with advanced isolated testing and restoration at scale.

VMware Live Cyber Recovery leverages a step-by-step guided workflow that integrates identification, validation, and restore of selected recovery points within a single UI. Its immutable, air-gapped snapshots are stored in a secure cloud file system to ensure data integrity at the time of recovery. Guided restore point selection delivers insights such as VMDK rate of change and entropy to help customers identify snapshot candidates. Live behavioral analysis of powered-on workloads and embedded next-gen anti virus identify and contain both file-based and fileless attacks within a secure, quarantined environment that can be provisioned directly from the product UI. This eliminates the need for IT teams to build, secure and manage that environment on their own.

Finally, the VMware Live Cyber Recovery guided workflow also integrates push-button VM network isolation levels to prevent lateral movement of ransomware should a compromised snapshot be powered on in the Isolated Recovery Environment (IRE).

## VMware Live Site Recovery

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

Built-in nondisruptive testing ensures recovery time objectives (RTOs) are met. VMware Live Site Recovery integrates with a vast ecosystem of underlying replication technologies, providing maximum flexibility. Enhanced vSphere Replication delivers RPOs as low as 1 minute and supports a large variety of underlying storage solutions.

VMware Live Site Recovery enables simple, policy-based automation that enables the protection of thousands of virtual machines easily through 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.

## 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. Two thirds of organizations were attacked by ransomware in 2022, and 76% of them had their data encrypted[3]

### No Guarantees for Ransom

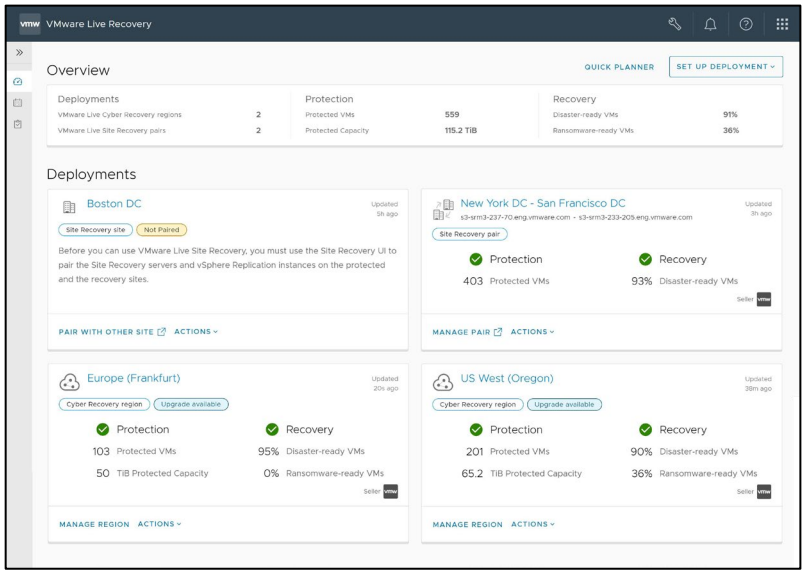
- ✓ Paying the ransom has no guarantees—a staggering 96% of organizations who paid the ransom did not regain full access to their data

### The cost beyond Ransom:

- ✓ The average cost of a ransomware attack (not including the ransom itself) is $4.54M[1] As a result, the need for organizations to better protect and recover their data has become an urgent business imperative.

## Unified Management Experience

A centralized SaaS console enables complete control over all aspects of data collection, ransomware recovery, site recovery, automation, and execution of disaster recovery on-premises 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 to further expand their functionality. Customers no longer must choose between using on-premises and cloud DR on the same node.

## In Summary

By bringing these powerful VMware solutions together, customers can recover from threats to their infrastructure of choice across on-premise and cloud environments. VMware Live Recovery is the industry's first solution that combines purpose-built cyber recovery with enterprise-grade DR in a single management experience across private and public cloud

**Accelerated, Simplified, and Unified – that's VMware Live Recovery.**

For more information about VMware Live Recovery, visit vmware.com/products/live-recovery or reach out to your sales representative

Sources:
1. IBM Cost of a Data Breach
2. CrowdStrike Cyber Intrusion Services Case Book
3. Sophos State of Ransomware 2022