Enterprise Strategy Group™

TECHNICAL VALIDATION

Cyber Recovery With VMware Live Recovery

Cyber and Data Resiliency at Scale for VMware Cloud Foundation

By Tony Palmer, Practice Director
Enterprise Strategy Group

August 2025

Contents

Introduction

This Technical Validation from Enterprise Strategy Group documents the detailed evaluation of the VMware Live Recovery (VLR) and vSAN data protection integrated solution, focusing on the key benefits of simplified operations, accelerated ransomware recovery, and efficient recovery at scale.

Background

Ransomware is widely considered a critical threat to the viability of any business. Given the high frequency of attacks and the impacts of successful ones, many organizations are left with damages that have an effect well beyond IT. Attackers often go beyond valuable data assets by undermining key infrastructure components and exposing significant gaps, including those in the backup infrastructure itself.

Enterprise Strategy Group research shows that 75% of organizations report experiencing an attempted ransomware attack within the past 12 months, with 27% indicating that attacks happened on at least a weekly basis (see Figure 1).[1]

Figure 1. Ransomware Attacks Continue to Be Pervasive

Source: Enterprise Strategy Group, now part of Omdia

Cyberattacks have evolved over recent years and become particularly deceptive. Modern cyberthreats are fileless in nature and cannot be detected through the traditional file scanning methods that organizations typically use, which increases the chances of reinfection of the production environment if these remain undetected and directly hinders their confidence in recovery. The best way to identify *and contain* fileless threats is to power the workloads on in a secure, isolated environment (commonly referred to as isolated recovery environment or isolated clean room) and analyze how the data within the workloads behaves over time to detect potential indicators of compromise.

[1] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023. All Enterprise Strategy Group research references and charts in this technical validation are from this research report, unless otherwise noted.

Considering this paradigm shift in ransomware attacks, cyber resilience has become top of mind to CIOs and IT professionals worldwide who recognize immediate action must be taken, and cyber recovery acts as a last line of defense when all else fails. Recovering from a ransomware attack presents its own unique challenges, which are widely different from those presented by traditional disaster recovery. In addition, provisioning, securing and managing an isolated clean room is a complex task requiring expertise across multiple disciplines.

Cyber recovery requires a few key capabilities:

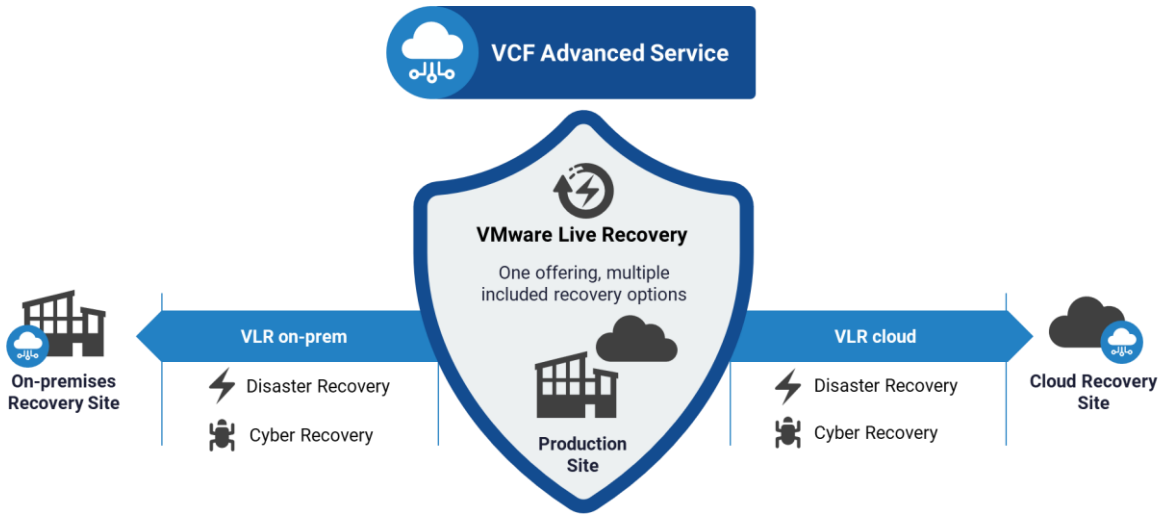
- **Guidance to identify recovery point candidates** by using data and metadata-based parameters that inform the changes across recovery snapshots. Otherwise, IT teams are left with numerous recovery points and no clear guidance as to where to start. Ransomware tends to dwell within the environment undetected for some time, which requires a rollback of days or even weeks to find a viable restore point.
- **Integration of vulnerability, signature, and behavioral analysis** to validate recovery point candidates and ensure they are not infected before restoring. Network isolation must also be embedded in the isolated clean room to prevent the spread of malware through lateral movement should an infected copy be powered on.
- **Orchestration** at scale usually requires extensive manual integration that has a direct impact on IT resource allocation, time to recovery, and damage caused by the cyberattack.

VMware Live Recovery Solution Overview

VLR delivers cyber and data resiliency for VMware Cloud Foundation (VCF). Specifically, the solution integrates cyber recovery and disaster recovery (DR) across a wide range of VCF topologies into a unified offering. The solution enables organizations to choose between recovery models, with a single subscription and a flexible licensing model.

VLR integrates cyber and disaster recovery into a unified management experience across on-premises and cloud VCF sites. VLR is designed to accelerate recovery from cyberattacks and other disasters using end-to-end guided automation, embedded recovery point selection, built-in validation, and turnkey isolated clean rooms with push-button network isolation. Figure 2 illustrates key recovery topologies for VLR. While the focus of this validation analysis is cloud cyber and disaster recovery, readers should note that VLR supports restoring to both on-premises and cloud VCF sites.

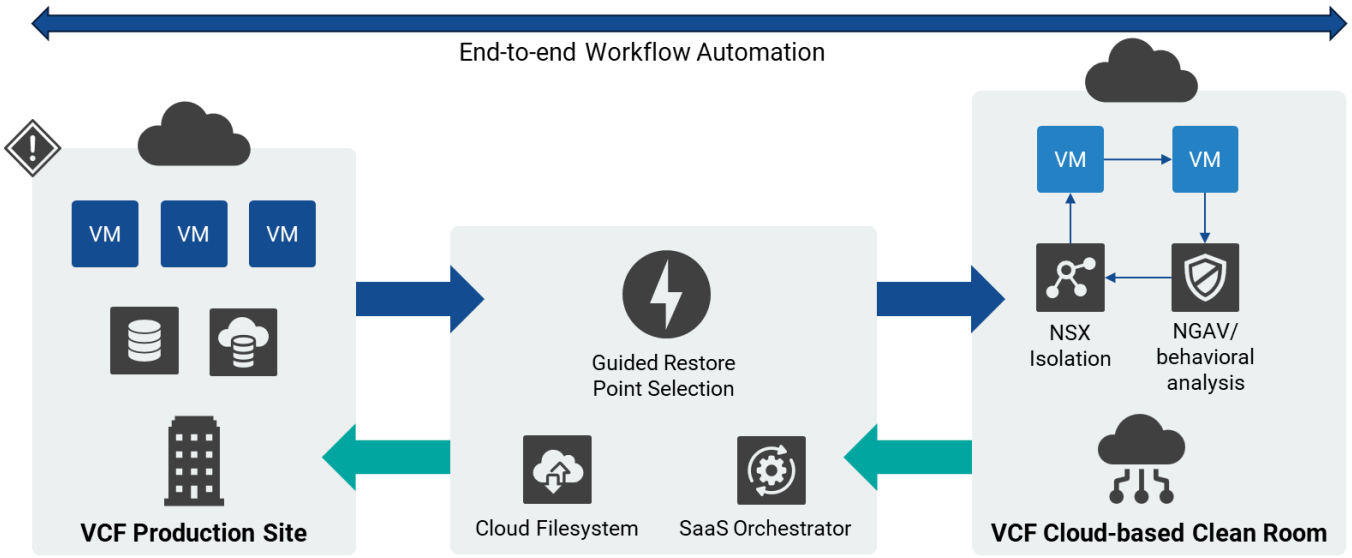
Figure 2. VMware Live Recovery Across On-premises and Cloud Environments



Source: VMware and Enterprise Strategy Group, now part of Omdia

For cyber recovery to a cloud VCF isolated clean room (see Figure 3), VLR integrates end-to-end capabilities for users to select, validate, and recover workloads using a cloud-based VCF isolated clean room. This eliminates the need for manual integration across cyber recovery components such as backup, replication, orchestration, infrastructure, network isolation, and EDR. IT teams can run fully-orchestrated cyber recovery with a single solution.

Figure 3. Cyber and Disaster Recovery to the Cloud – End-to-end Workflow Automation



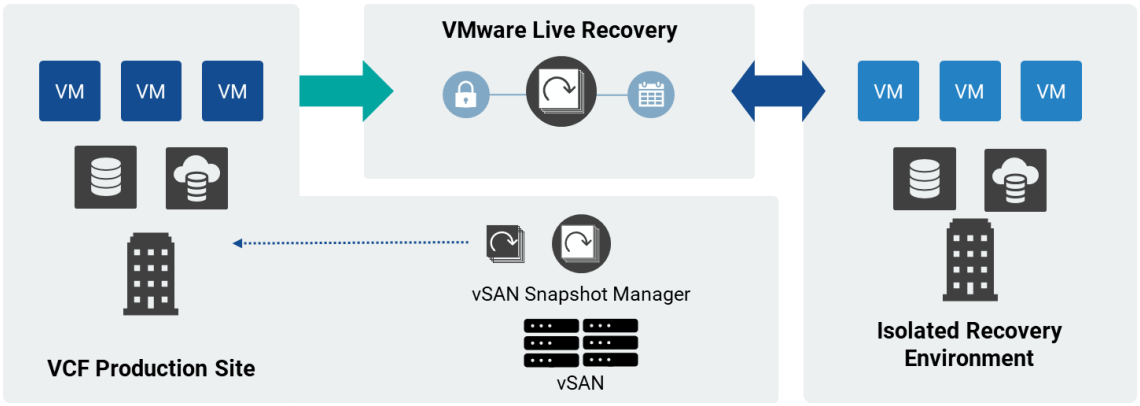
Source: VMware and Enterprise Strategy Group, now part of Omdia

VMware by Broadcom has recently announced an integration between VLR and vSAN snapshot manager, a step forward in its platform-level strategy. This is one of the key areas of focus in this validation study.

The integration between VLR and vSAN snapshot manager is meant to deliver accelerated recovery both from cyberattacks and operational disruptions by enabling users to invoke recovery from local vSAN copies, which dramatically reduces data transfers from the isolated clean room back to production.

Using the embedded validation of powered-on workloads in the isolated clean room, organizations will be able to identify a pre-infection restore point. However, given the rollback in time, the delta between the pre-infection snapshot and what was in production may be significant. The integration between VLR and vSAN snapshot manager adds value here, as it enables users to restore directly from a local copy instead of bringing back the entire VM from the cloud. This reduces data transfer at failback significantly and, therefore, enables much faster recovery. The vSAN snapshot manager operates under a different vCenter than the rest of production, which allows for separation to prevent tampering of local stored snapshots.

Figure 4. VMware Live Recovery Integration With vSAN snapshot manager



Source: VMware and Enterprise Strategy Group, now part of Omdia

Enterprise Strategy Group Technical Validation

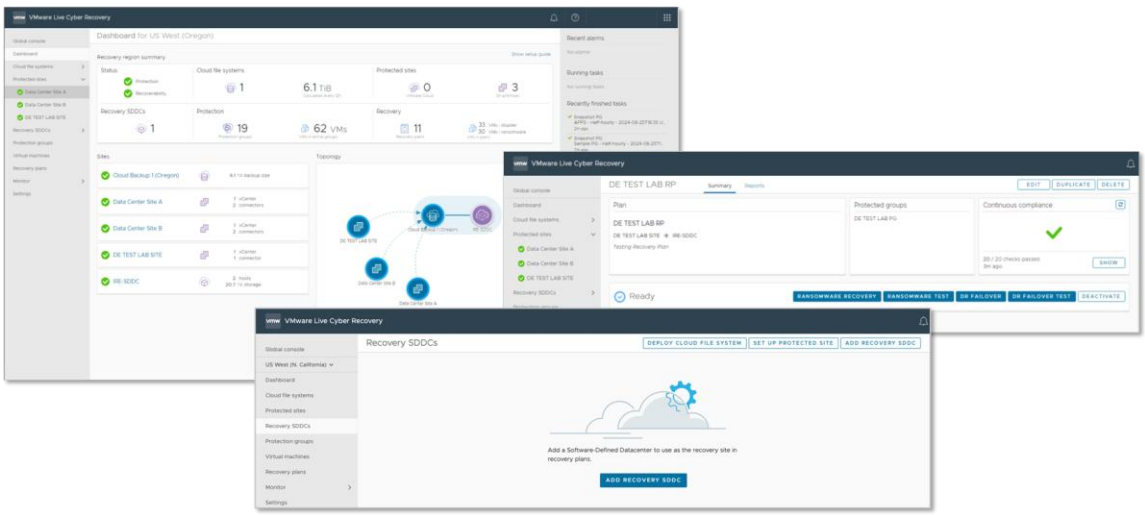
Enterprise Strategy Group validated how the VLR and vSAN data protection integrated solution can help organizations recover from threats at scale faster and more efficiently.

Simplified Operations

Enterprise Strategy Group reviewed the ease of use of VLR for the use case of cyber and disaster recovery to a cloud site. VLR allows users to provision an isolated clean room with embedded push-button network isolation in a just-in-time fashion. This clean room can be flexibly scaled up or down, which optimizes infrastructure spending and removes the need for IT teams to build, secure, and manage this environment themselves.

Isolated clean room provisioning, along with restore point selection, validation with built-in tools, and restore at scale, are all integrated into a step-by-step guided cyber recovery workflow that takes users through all needed steps.

Figure 5. Cyber Recovery Workflow



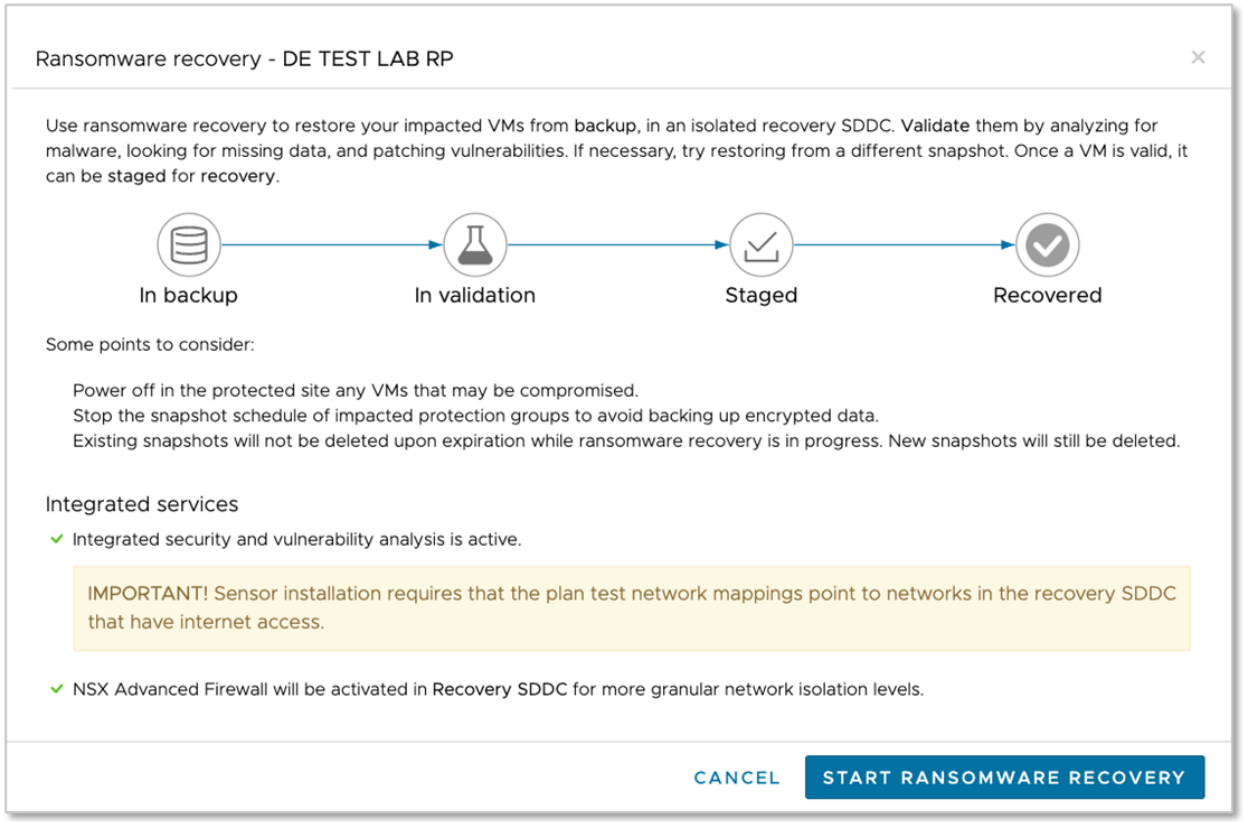
Source: VMware and Enterprise Strategy Group, now part of Omdia

Centralized visibility also helps streamline the way teams run their restore operations, and VLR allows them to monitor, control, and manage their recovery sites, protected VMs, protection groups, and health status of recovery plans.

IT teams can also choose between running failover or testing operations for both cyber and disaster recovery from the same control panel. Customers also benefit from non-disruptive testing of recovery plans and rapid recovery point iterations, as VLR can instantly power on VMs in the isolated clean room without data rehydration or VM format conversions.

Figure 6 shows how infrastructure teams are guided through a step-by-step cyber recovery workflow that spans across identification, validation, staging, and restore of recovery points at scale.

Figure 6. Cyber Recovery Steps



Source: VMware and Enterprise Strategy Group, now part of Omdia

Users have a centralized view of all the steps of the workflow as they go through the recovery process. The first step of the workflow is Guided Restore Point Selection. This feature presents the user with a snapshot timeline paired with insights such as virtual machine disk rate of change, file entropy, and advanced metrics to help inform good snapshots to consider for recovery.

Once recovery points are selected, they are powered on in the VCF isolated clean room and undergo live behavioral analysis, a vulnerability analysis, and a signature scan. The suggested time for behavioral analysis is eight hours, but users can customize this according to their application requirements and risk tolerance.

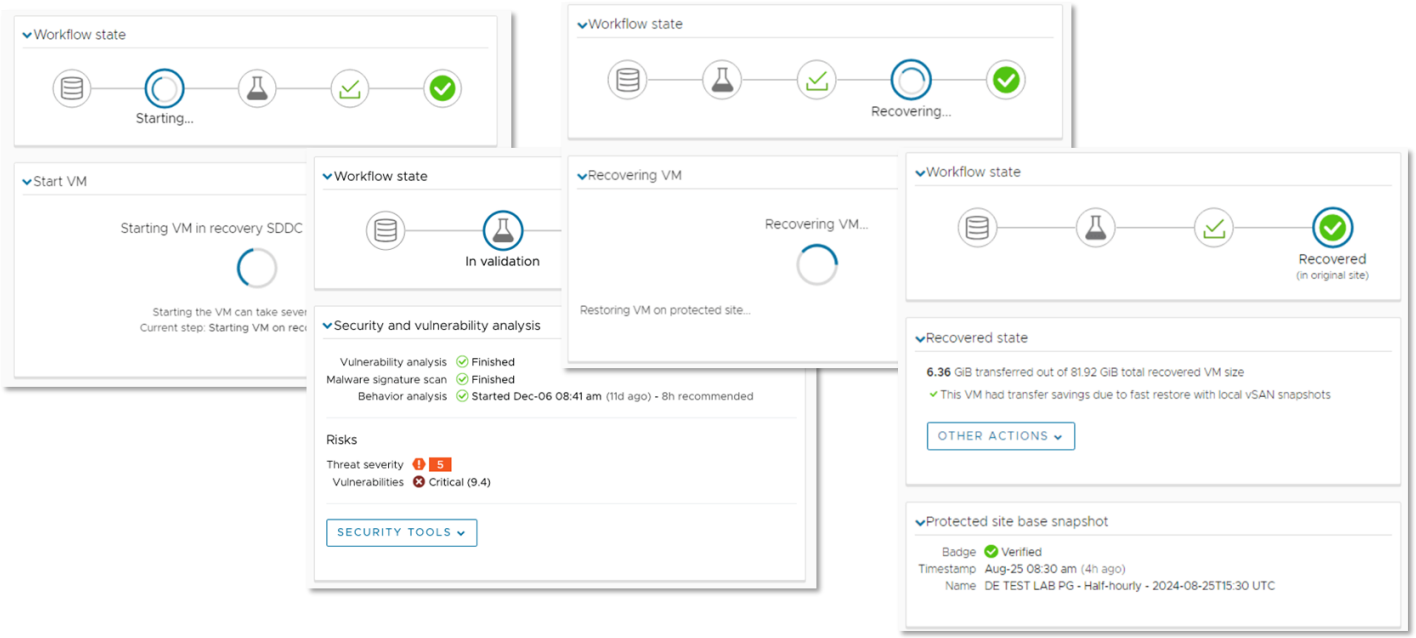
These three detection tools help identify both file-based as well as fileless attacks, which have become increasingly common, cause widespread damage if not caught in time, and cannot be detected through traditional file-scanning methods.

To prevent lateral movement of malware across VMs when these are powered on and prevent potential reinfection of the production site, VLR offers customers the ability to provision turnkey isolated clean rooms with “push-button” network isolation. Users can either select pre-configured isolation configurations or customize their own as needed.

Once recovery points are validated, they undergo delta-based failback to production, where only the changed blocks of data are transferred back instead of the entire VM. If the user has vSAN snapshot manager set up in the production site, they can also recover from a local copy and speed up the restore process. VLR provides full visibility into the status of each VM across the workflow and supports recovery operations for dozens of VMs at a time. It also supports snapshot badging, as these can run the validation process to streamline collaboration across infrastructure and security teams.

Given the nature of cyberattacks, the initially selected restore point candidates may be infected and, therefore, not viable to bring back to production. In this scenario, it is critical for IT teams to be able to quickly and non-disruptively iterate and select new restore points to validate. VLR supports instant restore of recovered VMs in the isolated clean room, given that neither data rehydration nor VM format conversions are required.

Figure 7. Cyber Recovery In Action



Source: VMware and Enterprise Strategy Group, now part of Omdia

Why This Matters

Operational challenges in cyber recovery operations span multiple disciplines that can impact costs and limit an organization's ability to effectively test recovery. The manual integration of disparate components and diverse support models across different products from separate vendors increases complexity and costs, which can result in a justified lack of confidence in recovery.

What is needed is a solution that not only streamlines cyber recovery but also minimizes complexity, with a combination of integration of components, enhanced collaboration between infrastructure and security teams, and repeatable, automated workflows.

Enterprise Strategy Group validated that VLR solves these challenges with a single solution that integrates all components into a guided, automated workflow experience that enables simplified, confident, secure recovery at scale.

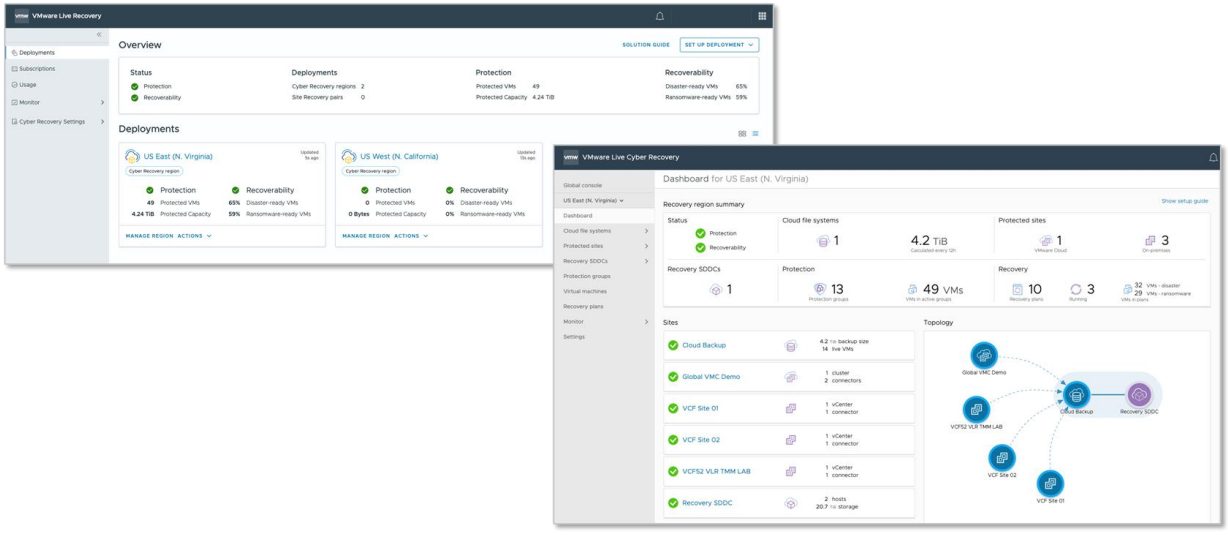
The VLR workflow enables bulk VM restore and obviates the need for IT teams to select, validate, and recover workloads manually on a per-VM basis. The time to recover production operations for large scale environments with hundreds to thousands of VMs is further reduced by minimizing the data transfer from the cloud with recovery from local snapshots. VLR provides granular capabilities that, taken together, provide exceptionally efficient recovery at scale.

In combination, VLR's end-to-end workflow automation, ready-to-run isolated clean rooms with zero-effort network isolation, built-in validation of recovery points, non-disruptive recovery testing, and fast iteration of restore points in cyber recovery solve key problems for organizations attempting to accomplish all of this with disparate tools and techniques.

Accelerated Cyber Recovery At Scale

Enterprise Strategy Group reviewed VLR's ability to accelerate cyber restore leveraging local vSAN copies, as well as its ability to do so at scale. The VLR dashboard shows consolidated information that enables IT teams to monitor their protected and recovery site mappings, overall protection and recovery health status, protected capacity, deployed file systems, and recovery plans. Visibility into what's protected and what isn't, how topologies are configured and the overall recovery health status of the environment is closely tied to an organization's ability to recover quickly from a cyberattack, as seen in Figure 8.

Figure 8. VMware Live Recovery Dashboard



Source: VMware and Enterprise Strategy Group, now part of Omdia

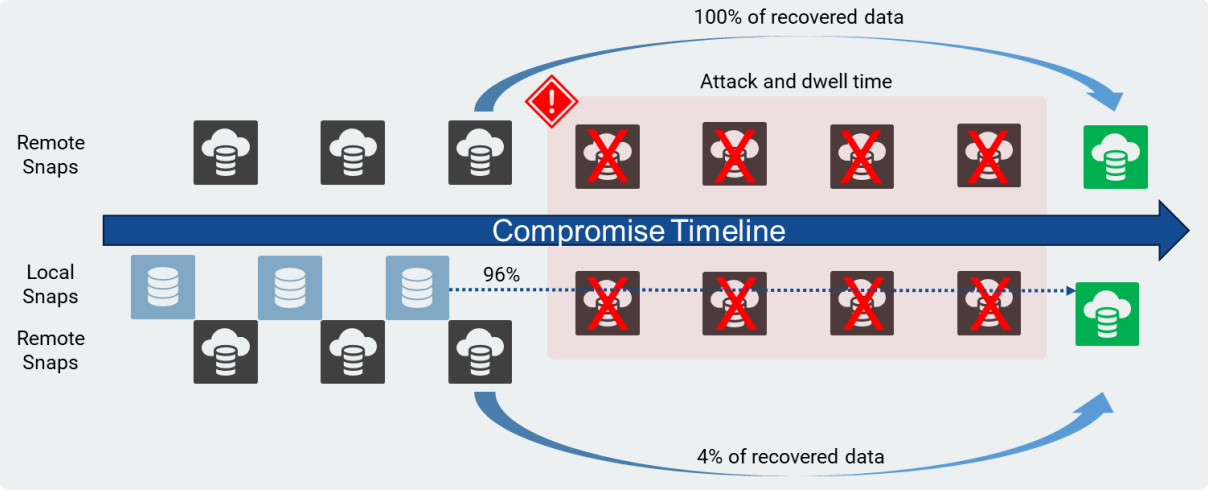
In order to quantify how much faster recovery can be when leveraging the integration between VLR and vSAN snapshot manager, we ran recovery tests with delta-based failback, as well as with restore from local snapshots to compare the differences in the amount of data transferred and determine how that would impact time to recovery. First, we'll illustrate the concepts and explain how it works before walking through the validation results.

The integration between VLR and vSAN snapshot manager enables IT teams to create recurring, on-premises snapshots for VMs within protection groups and invoke restore from these local copies in the event of a cyberattack or operational failure. In a ransomware recovery scenario, once a pre-infection restore point is identified in the isolated clean room, the local snapshot is automatically matched to it and restored, with a minimal data delta transferred from the cloud file system to complete the restore process.

VLR automatically discovers vSAN ESA VMs protected with vSAN data protection (i.e., with local replication to the vSAN snapshot manager) and enables accelerated ransomware recovery with no configuration required. Users can create protection groups, which are collections of VMs that the solution protects together, and one or more protection groups can be included in a recovery plan. A recovery plan specifies how the solution recovers the VMs in the protection groups that it contains. The combination of snapshot schedules and retention timeframes are user-defined and highly flexible. Users can also set up recovery plans to have all the necessary steps for completing a ransomware recovery, ransomware test, DR failover, and a DR failover test.

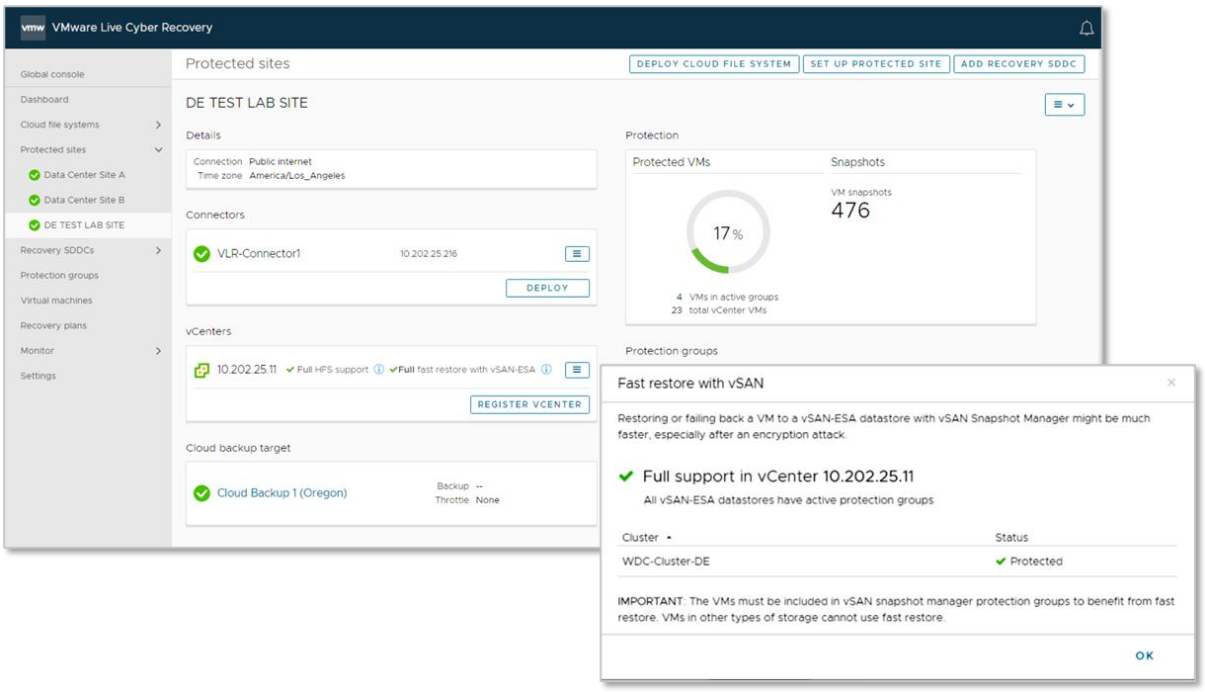
Figure 9 shows a simple example of how the integration between VLR and vSAN snapshot manager can reduce data transfers from the cloud to the protected site dramatically by combining the most recent known good local snapshot with the most recent remote snapshot.

Figure 9. Reducing Data Transmission From the Cloud With VMware Live Recovery



Source: VMware and Enterprise Strategy Group, now part of Omdia.

Figure 10. Restore From Local vSAN Copies With VMware Live Recovery



Source: VMware and Enterprise Strategy Group, now part of Omdia

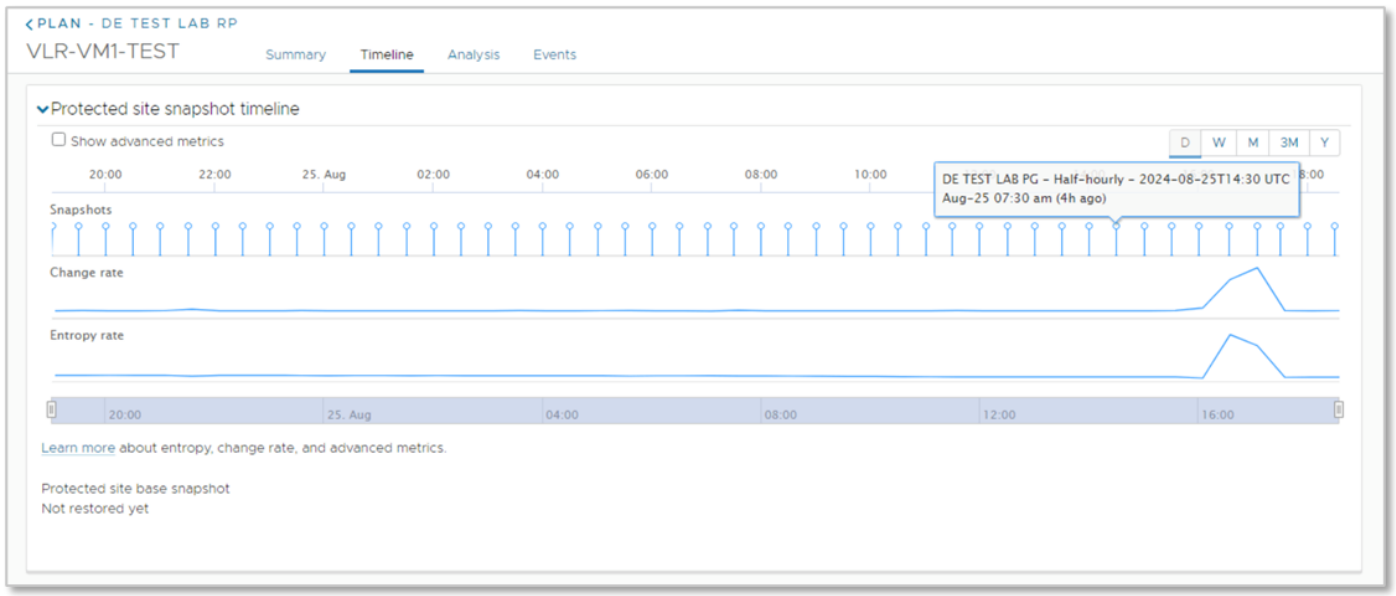
Figure 10 shows VLR, including the protected sites and the fast restore with vSAN data protection.

We evaluated VLR integration with vSAN data protection via testing conducted using two pairs of Windows VMs, made up of one small and one large data set. One pair was configured with local VMware data protection snapshots and the other was not. Testing was designed to compare the amount of data transferred from the cloud and enable a calculation of the potential impact on time to recover.

Each of the four Windows VMs had a 40 GB OS drive (C:\) and a separate data disk (X:\). The smaller instance had a 60 GB data drive, and the larger instance had a 150 GB data drive. The data drives were populated with 50 GB and 120 GB of initial data, respectively, using the fio workload generation utility. For this testing framework, the snapshots were scheduled at hourly intervals, with approximately 30 minutes of skew between the local vSAN data protection snapshots and the remote VLR snapshot cycles. The fio workload was used to generate 5-6% of data change per snapshot interval. Multiple iterations of tests were run to ensure repeatability.

To generate a simple and easily observable initial attack point, each VM had its data drive encrypted with the BitLocker utility available within the Windows OS. After waiting a number of hours to simulate dwell time and allow the capture of additional local and remote snapshots, we determined that the VMs could not access their data drives if rebooted without the BitLocker encryption key. At this point, the workload generator was halted and the recovery process was started. From the VLR snapshot selection screen, it was easy to spot malicious activity across consecutive snapshots, as seen in Figure 11.

Figure 11. Guided Restore Point Selection



Source: VMware and Enterprise Strategy Group, now part of Omdia

A pre-infection snapshot candidate was selected for validation, and VLR validated and restored to the production site.

Table 1 shows the measured data transferred from the cloud for restores across the four VMs we tested with.

Table 1. Data Transfer Reduction with VMware Live Recovery

VM Disk Capacity	vSAN data protection	Data Affected	**Cloud Data Egress (GiB)**	**Delta**
150 GB	Yes	120 GB	8.29	-93%
150 GB	No	120 GB	133.36	+11%
100 GB	Yes	50 GB	2.15	-96%
100 GB	No	50 GB	53.52	+7%

Source: Enterprise Strategy Group, now part of Omdia

Enterprise Strategy Group validated that VLR, in combination with vSAN data protection (i.e., integration with vSAN snapshot manager), can drastically reduce the amount of data transfer from the cloud for disaster or cyber recovery by 93% to 96%, depending on the size of the VM and the rate of change for each workload. For a real-world organization with hundreds to thousands of VMs, this would add up quickly, reducing data transfer from the cloud by tens to hundreds of terabytes, representing tremendous savings in both egress fees and time to recovery.

The ability to run these accelerated cyber recovery operations at scale was also validated. VLR supports accelerated cyber and disaster recovery at scale with several key capabilities. First, the step-by-step cyber recovery workflow allows simultaneous restore for large numbers of VMs, which removes the need for manual, per-VM analysis to select, validate, and bring back to production.

In addition, VLR allows users to provision the VCF isolated clean room in the cloud just in time directly from its centralized UI. This isolated clean room can be immediately scaled up or down as needed, depending on the amount of VMs that need to be restored, whether for a recovery plan test or an actual cyber event response. This solves a major pain point, as IT teams can flexibly provision, scale, and decommission their recovery site to support the scale of their operations without cost inefficiencies.

Finally, VLR supports up to four filesystems per cloud recovery site, which delivers a snapshot storage capacity of up to 1.75PB. The ability to have multiple datastores mounted to a single recovery site delivers improved replication performance, simplifies topology design and VM network configurations, and drives down cost by reducing the number of cloud recovery sites required. To further increase scale, each cloud filesystem can be paired with its own dedicated source site and then subsequently recovered to a single target VCF cloud site.

Why This Matters

More than half of the organizations surveyed by Enterprise Strategy Group struggle with long recovery times. 54% of respondents believe it would take their organization more than three days to fully recover from a ransomware event, while 84% of those who've been hit with a cyberattack report not being able to fully restore their data.

Numerous factors contribute to these issues slowing down—and sometimes preventing—recovery. Both the incessantly growing volume of data organizations need to protect[2] and the rising complexity in IT environments[3] contribute to a lack of knowledge of precisely what organizations really need in order to recover from modern ransomware. Other critical factors include: manual integration of multiple solutions from different vendors adding friction to workflows and leaving gaps; lack of a ready-to go isolated clean room when cyber recovery is needed increasing delays and the risk of human error; the inability to run rapid non-disruptive cyber recovery iterations injecting more delay; relying exclusively on signature-based scans to validate restore points increasing risk of reinfection, forcing a restart of the whole recovery process; and errors in protection group setup and retention schedules can result in missing data or even a failed recovery.

Enterprise Strategy Group validated that the integration between VLR and vSAN snapshot manager delivers accelerated recovery by reducing data transfers at failback from 93% to 96%. Additional capabilities in VLR that support accelerated restore include guided workflow automation, which streamlines the way IT teams operate and removes friction that delays the recovery process; the ability to flexibly provision a turnkey isolated clean room, which removes the need for IT teams to build, secure, and manage one themselves; and the end-to-end integration of cyber recovery components that eliminate manual integration across backup, EDR, networking, infrastructure, and orchestration. In addition, VLR enables rapid recovery point iterations and non-disruptive testing of recovery plans as it instantly powers on VMs in the isolated clean room with no data rehydration or VM format conversions. All of these benefits can be scaled to support thousands of VMs and deliver successful cyber resilience outcomes.

[2] Source: Enterprise Strategy Group Research Report, *Navigating the Cloud and AI Revolution: The State of Enterprise Storage and HCI*, March 2024.
[3] Source: Enterprise Strategy Group Research Report, *2025 Technology Spending Intentions Survey*, December 2024.

Conclusion

Ransomware is a significant threat that can potentially devastate organizations. Nearly two-thirds (65%) of respondents surveyed by Enterprise Strategy Group consider it one of the top three most serious threats to the viability of their organization.[4] To address this issue, it's crucial to first comprehend its impact. In the same survey, more than half (54%) of organizations report it would take their organization more than three days to fully recover from a ransomware event and resume operations, with a quarter of respondents saying it would take more than a week, woefully longer than would be tolerable for most outages. Enterprise Strategy Group research found that the business and financial impacts from attacks can be significant. While only 23% of respondents indicated a loss of revenue following an attack, impacts indirectly affecting the bottom line were common. Specifically, 38% reported application downtime, 34% cited infrastructure cost overruns, 32% reported negative customer experiences, and 27% pointed to a negative impact to shareholder value or brand standing.[5]

When ransomware strikes, the main goal is obviously to recover data and minimize losses. This is because data losses not only lead to non-compliance but also pose significant business risk. Unfortunately the current reality is that 84% of organizations that have been the victims of at least one successful ransomware attack reported that they were *not* able to fully restore their data after the cyber event. This highlights the need to reengineer recovery processes to enable confident protection from modern cyberattacks.

Organizations struggle with the manual integration of multiple tools to enable cyber-resilience and protect and recover their data from ransomware attacks. Manually managing infrastructure hardening, security, backup, orchestration, isolated clean room provisioning, networking, and recovery is operationally daunting. This helps explain why organizations don't generally test their cyber-resilience and recovery plans because the products they're relying on make it cumbersome and disruptive to do so.

VLR is solving these problems with a broad array of capabilities rarely seen in a single product. From optimizing the use of IT resources—both technological and human—enabling close collaboration between disparate teams, to guiding users through the entire recovery workflow and automating the end-to-end process to eliminate the complexity inherent in operations of this nature.

Based on our evaluation and analysis, VLR simplified and accelerated cyber recovery at scale by enabling concurrent bulk recovery for dozens of VM's concurrently. Guided workflows with built-in validation tools to identify and help clean sophisticated strains of malware minimized manual intervention and reduced the risk of reinfection. In addition, we saw how VLR provides the ease of use and flexibility needed to recover data from cyberattacks with centralized visibility and monitoring of all components of the recovery operation. Recovery testing of VLR validated how the integration with vSAN data protection (vSAN snapshot manager) drastically reduced data transfer for recovery from cloud-based snapshots by up to 96%, offering a significant reduction in time to recovery and data egress costs.

If your organization is looking to accelerate its digital transformation and implement efficient and effective cyber- and data-resiliency, Enterprise Strategy Group recommends you take a close look at VMware Live Recovery.

For more information, please visit VMware Live Recovery.

[4] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.
[5] Source: Enterprise Strategy Group Research Report, *Balancing Requirements for Application Protection*, April 2025.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com