On-Premises Ransomware Recovery for VMware Cloud Foundation on Lenovo ThinkAgile VX

Solution Brief

Executive Summary

Recover business-critical workloads with confidence, validate, cleanse, and restore inside an isolated recovery "clean room" that keeps your data on infrastructure you control.

The solution with VMware Cloud Foundation on Lenovo ThinkAgile VX powered by Intel Xeon 6 and AMD EPYC processors results in a platform that helps organizations reduce licensing complexity, streamline operations across VMware Cloud Foundation, and strengthen recovery readiness from day one..

Business Challenge

Ransomware has become one of the most disruptive threats to enterprise IT, and the rapid adoption of AI is raising the stakes. As organizations use AI to modernize operations, cyber adversaries are also using AI to automate reconnaissance, accelerate phishing campaigns, exploit stolen credentials, and move faster toward mission-critical data. For example, in 2025 AI-enabled adversaries increased their attacks by 89%. In this environment, conventional defenses, immutable backups, and traditional disaster recovery are no longer enough. Protecting business-critical VMware Cloud Foundation workloads requires a tested cyber recovery strategy designed for the moment when prevention fails: one that can identify, validate, cleanse, and restore trusted workloads with confidence.

What makes ransomware uniquely difficult to recover from is not just the encryption event itself, but the combination of attacker dwell time, credential-based compromise, and increasingly stealthy malware-free attack techniques. Attackers often operate undetected for weeks or months using stolen credentials, moving laterally through the environment while targeting critical assets such as backup and recovery infrastructure.

By the time a breach is discovered, recent backups and replicas may already be compromised, and simply restoring the latest snapshot can reintroduce malware, malicious configurations, or unauthorized access into production. Modern ransomware also frequently employs fileless techniques that evade traditional signature-based scanning. According to CrowdStrike, 82% of detections reported in 2025 were malware-free, making it essential to validate recovered workloads using behavioral analysis, Next-Generation Antivirus (NGAV), and Endpoint Detection and Response (EDR) controls within an isolated clean-room environment before recovery. This challenge is compounded by the operational complexity of coordinating recovery workflows across multiple security, infrastructure, networking, and orchestration tools, increasing the risk of delays, reinfection, and recovery failures.

A sound recovery strategy must therefore assume that malware is embedded in the snapshot data and that snapshots should never be restored directly to production. Recovery points must first be brought up in a safe, controlled space, then inspected, cleansed, and validated before any workload returns to service.

For regulated organizations, such as financial services, healthcare, federal agencies, and other compliance-driven enterprises, the challenge is even greater. Requirements associated with DORA, HIPAA, federal cybersecurity mandates, and operational resilience expectations increase the need to prove that recovery processes are controlled, auditable, and capable of restoring trusted operations after a cyber event. For organizations with data-sovereignty or privacy requirements, this also means recovery data and recovery operations may need to remain on infrastructure they own and govern, making on-premises cyber recovery a strategic requirement for VMware Cloud Foundation environments.

The Solution

The **Lenovo Solution for On-Premises Ransomware Recovery for VMware Cloud Foundation** pairs VMware Advanced Cyber Compliance (ACC), a VCF Advanced Service, with Lenovo ThinkAgile VX hyperconverged infrastructure. It provides well-architected, validated guidance for recovering on-premises business-critical workloads within an Isolated Recovery Environment (IRE) in the event of a ransomware attack on the protected instance. VMware ACC helps customers replace fragmented point products with integrated workflows, continuous drift remediation, and secure recovery validation. Customers gain stronger resilience, simpler operations, faster recovery, and potentially 3–5× lower software costs.

Business-critical workloads are continuously replicated from a **protected VCF instance** to a separate **recovery VCF instance**. When an attack occurs, impacted workloads are brought up not in production, but inside an isolated workload domain (the IRE) where the infrastructure team in collaboration with the security and the cyber-response team can verify, cleanse, and recover them safely before failing them back to production.

Why on premises? Recovery data, compute, the Isolated Recovery Environment, and the vSAN recovery datastore all remain within customer-controlled VCF infrastructure, rather than being replicated to a cloud file system and recovered in a cloud-based SDDC. Your recovery operations stay close to home; on hardware you govern directly.

Delivered on Lenovo ThinkAgile VX, a co-engineered, integrated HCI platform purpose-built for VMware Cloud Foundation. The solution provides the compute, vSAN ESA storage, and lifecycle management needed to stand up both the protected and recovery instances with confidence. The ThinkAgile servers are based on our ThinkSystem portfolio. Lenovo ThinkSystem ranked the most reliable x86-based server platform in the ITIC 2025 report extending that claim to 12 consecutive years (ITIC 2025 report).

The diagram below provides a conceptual view of how protected VCF instance replicates business-critical workloads to a recovery VCF instance through VMware Advanced Cyber Compliance. The recovery instance hosts the Isolated Recovery Environment (IRE) and connects to an Endpoint Detection and Response (EDR) portal for security analysis.

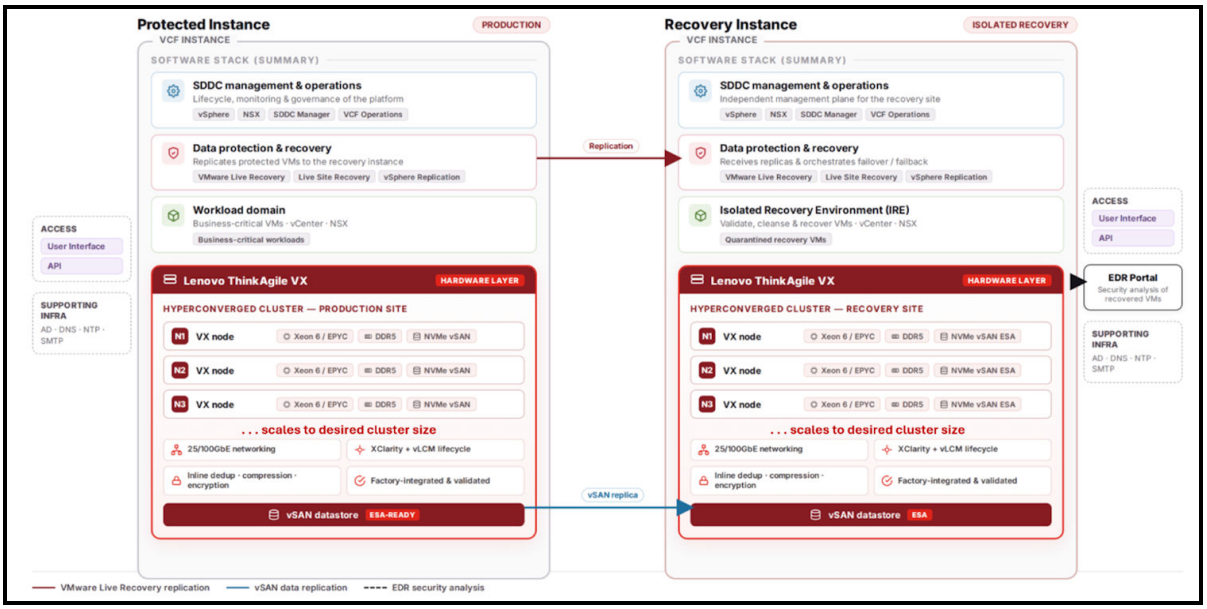

Figure 1. Ransomware Recovery Architecture.

How it works

Recovery follows a guided, iterative workflow built around a single principle: nothing returns to production until it has been proven clean. The process moves through identification, isolated validation, remediation, and controlled failback

1. **Continuous, point-in-time replication**Workload VMs replicate from the protected instance to the recovery instance using VMware Live Recovery with vSphere Replication. The validated design enables multiple point-in-time instances so responders can reach behind the dwell period to a recovery point taken before the infection began.
2. **Identify a clean recovery point**Because recent replicas may be compromised, responders use data-driven signals, such as entropy rate (a measure of likely encryption) corroborated with abnormal CPU-usage trends, to select replicas from before the attack.
3. **Validate inside the Isolated Recovery Environment**The selected replica is powered on as a test VM inside the IRE, never in production, under a quarantined network-isolation policy. Because VMs can be started directly in the IRE without data rehydration or VM format conversion, responders can iterate through candidate recovery points much faster to identify a pre-infection state. As each VM is brought online, an EDR sensor integrated into the workflow is automatically installed to perform behavioral analysis, which is essential for detecting fileless threats, along with signature-based scanning and vulnerability analysis. Customers can validate restore points with their preferred EDR, Carbon Black by default, or CrowdStrike Falcon with customer-provided licenses integrated into ACC's guided cyber recovery workflow.
   The resulting insights are surfaced to users so the team can validate, cleanse, and promote only trusted workloads. This same non-disruptive workflow also makes it easier to regularly test cyber recovery plans, improving recovery readiness before an actual incident occurs.
4. **Cleanse, then Restore**Once the workload is verified clean, the workflow stages VMs and restores workloads back to production, closing the loop safely.

The diagram below provides a conceptual view of the **solution logical design** flow.

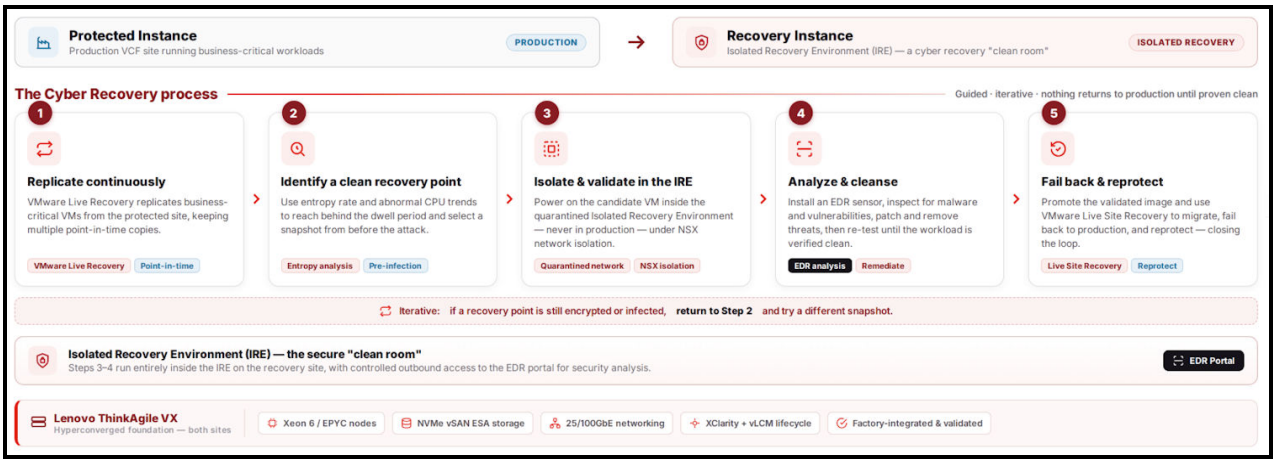

Figure 2. On-Premises Ransomware Recovery Logical Design.

The Isolated Recovery Environment

Central to any cyber recovery strategy is an Isolated Recovery Environment, a cyber recovery "**clean room**" disconnected from the production data center and used as an isolated place to safely power on, inspect, and recover ransomware-infected workloads. The IRE is dedicated to recovery and is not used for test/development, burst capacity, or any other purpose.

The solution is built on two VMware Cloud Foundation instances running on Lenovo ThinkAgile VX, each with its own management domain:

- **Protected instance**. The production VCF environment hosting business-critical workloads (management domain + workload domain).
- **Recovery instance**. Alternative VCF infrastructure that receives the replicated workloads and hosts the IRE as a dedicated, isolated workload domain.

Within the recovery instance, the IRE comprises a **compute cluster** with NSX edge clusters, providing a network-restricted environment in which to safely power on potentially infected VMs, and an **ESA vSAN storage cluster** that stores the replicas on a datastore remotely mounted to the compute cluster. An NSX Tier-1 gateway and IRE network segment isolate the recovered test VMs, while controlled outbound access reaches the EDR portal for sensor installation and security analysis.

In the following sections, we take a deeper dive:

Core software components

The Lenovo ThinkAgile VX solution with VMware, is design around the following software components:

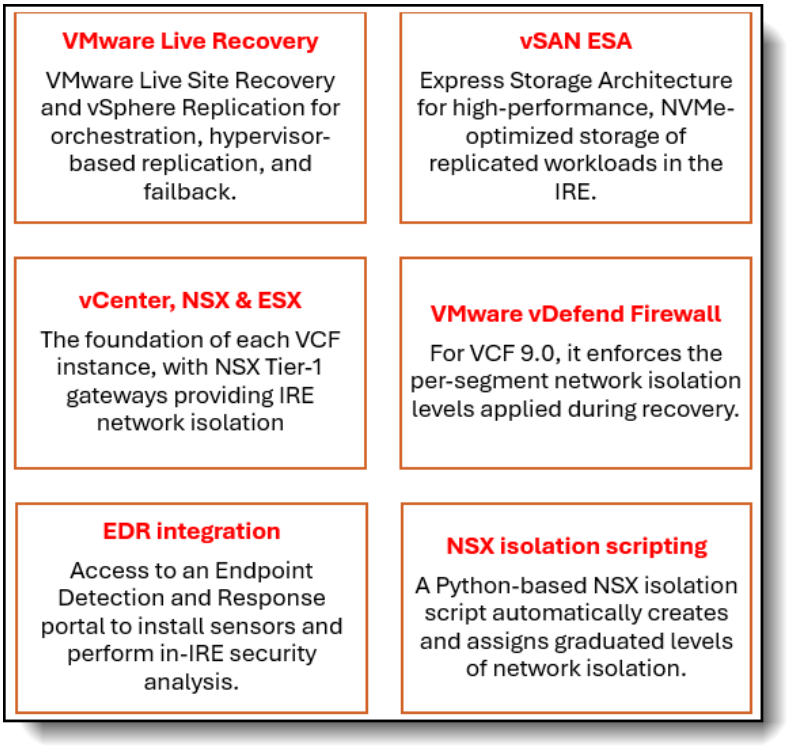

Figure 3. Core software components.

Network isolation levels

NSX-backed isolation policies let responders precisely control what a VM under examination can reach, preventing lateral spread of malware while enabling granular behavioral analysis at each phase of recovery.

The following table lists the network isolation levels.

Table 1. Network Isoalation levels

Isolation level	Behavior
Isolated / Quarantined	VM fully cut off; no inbound, outbound, or east-west traffic permitted.
Quarantined + Analysis	Permits DHCP, DNS, and NTP plus access to the EDR cloud portal, while blocking general outbound, inbound, and east-west traffic, the working mode for safe forensic analysis.
External Outbound / Internal Inbound / Internal	Intermediate levels that selectively re-enable connectivity as a workload is progressively validated.
Open	Full connectivity restored, used once a workload is confirmed clean and ready to return to service.

vSAN Cyber Recovery Profiles

These profiles are tailored for cyber recovery workloads, requiring fewer compute resources than a comparable vSAN ReadyNode, while enabling the use of high-capacity TLC or QLC storage devices.

Table 2. Network Isoalation levels

Description	CyberRecovery SM	CyberRecovery MED	CyberRecovery LRG
Minimum CPU (#Cores) Per node	16	24	32
Minimum Memory per Node (GB)	128	192	256
Minimum nodes per cluster	4	6	6
# of Storage devices for the base configuration	4 - 8	4 - 18	4 - 24
Networking GbE (min)	10	25	100
Replication Throughput (node, up to)	150 MB/s	225 MB/s	300 MB/s

By leveraging reduced CPU requirements and high-capacity QLC storage, organizations can build cost-effective recovery repositories without overprovisioning infrastructure.

These profiles are integrated into Lenovo DCSC for ThinkAgile VX to streamline the selection process.

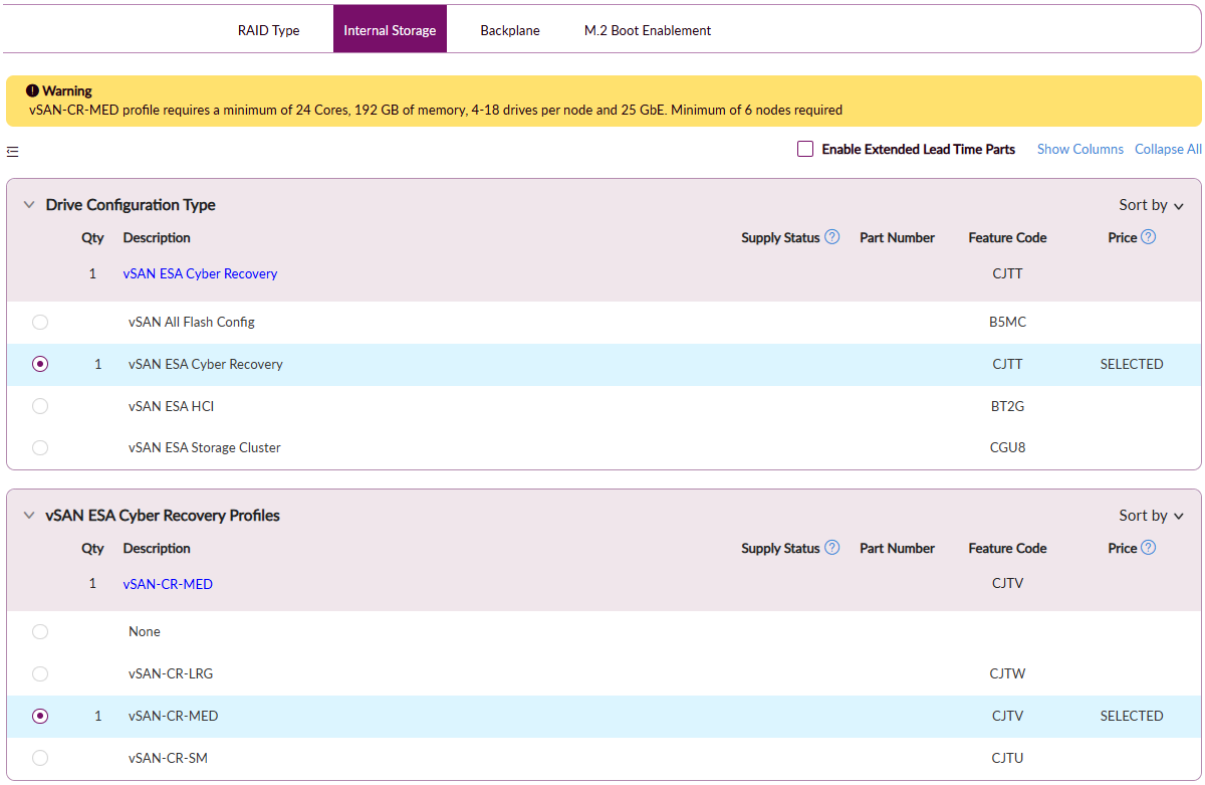

Figure 4. vSAN ESA Cyber Recovery Profiles in Lenovo DCSC

QLC NVMe drives deliver greater storage capacity at a lower cost, making them ideal for capacity-oriented workloads such as backup and cyber recovery repositories. Today, ThinkAgile VX only supports TLC drives, with plans to enable QLC drives by the end of CY 2026.

Notes on the QLC drives:

- NVMe QLC drives, when enabled, are supported exclusively for the Cyber Recovery use case.
- They require 4K IU (Indirection Unit) devices

- Minimum of 4 devices per host
- QLC support requires ESXi 9.1 or later

Table 3. Attributes specifications

Attribute	Specification
Type	NVMe QLC
Performance Class	F (100 K – 349 K writes/s) or higher
Capacity	15.36 TB or 30.72 TB
Min Devices per Host Supported	4 (4K IU devices only)
Minimum ESXi Version	9.1+
Supported Use Case	Cyber Recovery only

Sample Bill of Materials (BOM)

The following table lists the bill of materials (BOM) for the CyberRecovery-MED profile using ThinkAgile VX650 V4.

Table 4. Attributes specifications

Machine Type/Model Component	Description	Qty
7DG6CTO1WW	CyberRecovery-MED: ThinkAgile VX650 V4	6
C68E	ThinkAgile VX650 V4 24x2.5" Chassis	6
C5QQ	Intel Xeon 6505P 12C 150W 2.2GHz Processor	12
C3QR	ThinkSystem 2U V4 Performance Heatsink	12
C0U9	ThinkSystem 32GB TruDDR5 6400MHz (1Rx4) RDIMM	48
C0BA	ThinkSystem 2.5" U.2 CD8P 3.84TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	108
C46P	ThinkSystem 2U V4 8x2.5" NVMe Backplane	18
CC7G	ThinkSystem M.2 RAID B550i-2i SATA/NVMe Enablement Kit	6
C286	ThinkSystem M.2 VA 480GB Read Intensive NVMe NHS SSD	12
C1YK	ThinkSystem SR650 V4/SR630 V4 x16 OCP Cable Kit	6
BN2T	ThinkSystem Broadcom 57414 10/25GbE SFP28 2-Port OCP Ethernet Adapter	12
C0U3	ThinkSystem 2000W 230V Titanium CRPS Premium Hot-Swap Power Supply	12
6400	2.8m, 13A/100-250V, C13 to C14 Jumper Cord	12
C3RD	ThinkSystem 2U 6056 20K Performance Fan Module	36
BPKR	TPM 2.0	6
C3K9	XClarity Platinum Upgrade v3	6
SCJD	XClarity One - Standard, Per Endpoint w/3 Yr SW S&S	6

Key Benefits

The following chart provides a high level of the key benefits.

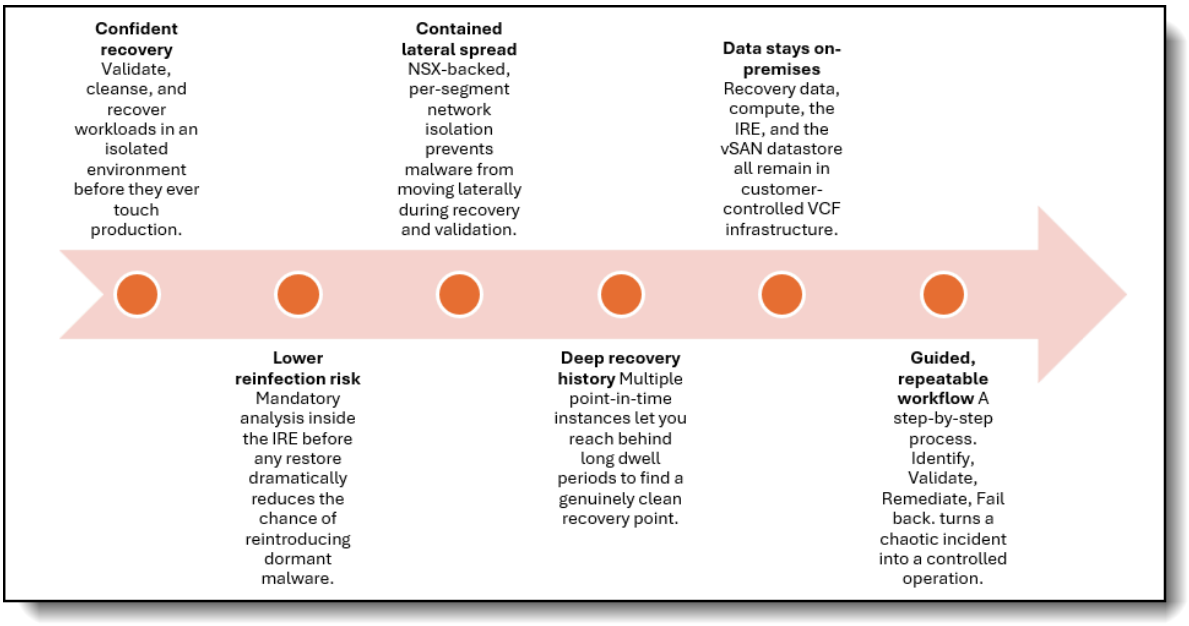

Figure 5. Key beneftis

Target Use Cases

Here are some customer use cases for this solution.

Ransomware recovery for business-critical workloads
Restoring on-premises VMs after an attack on the protected VCF site, entirely within customer-owned infrastructure.

Isolated forensic analysis
Safely powering on and examining potentially infected VMs in a dedicated isolated workload domain before any restore to production.

Clean recovery-point identification
Iteratively selecting a malware-free recovery point using entropy, CPU-usage trends, and multiple point-in-time replicas.

Controlled failover, failback, and reprotection
Returning cleansed workloads to production and re-establishing protection through an orchestrated workflow.

Data-sovereignty-conscious recovery
Meeting governance and compliance requirements that mandate keeping recovery data and operations on premises.

Why Lenovo ThinkAgile VX

Lenovo ThinkAgile VX is a co-engineered solution with VMware, purpose-built to deliver an enterprise-grade private cloud using VMware Cloud Foundation. It arrives fully tested, validated on Lenovo's industry-leading server platforms, giving you a proven, consistent foundation for both the protected and recovery instances without the risk of integration of building it yourself.

High-performance vSAN ESA storage
High-density NVMe storage optimized for vSAN ESA, with inline deduplication, compression, and encryption, ideal for the recovery instance's isolated datastore.

Broadest platform choice
Support for Intel Xeon 6 and AMD EPYC processors across 1U and 2U form factors, with storage-dense and GPU-optimized configurations. Customers can get the assurance that their systems are tested, certified, and validated to support VCF, reducing risk and downtime.

Unified lifecycle management
Integrated into vSphere Lifecycle Manager (vLCM) through the Lenovo XClarity Integrator, with validated ThinkAgile VX Best Recipes that streamline full stack solution updates and keep environments compliant.

Scale on your terms
SStart small and scale seamlessly as protection needs grow, with cloud-like economics available through Lenovo TruScale.

VMware alignment without lock-in
Stay aligned with VMware roadmaps while preserving flexibility across hardware refresh cycles.

Services and support

Our comprehensive services accelerate time to value, minimize downtime, and free your IT staff to focus on driving innovation and business growth:

- **24x7 Single Point of Support**. Premier Support delivered by Lenovo experts who specialize in ThinkAgile solutions, covering both Lenovo server hardware and VMware by Broadcom software, with rapid resolution and no finger-pointing.
- **Comprehensive services portfolio**Deployment and migration services, hybrid-cloud and modernization assessments, managed services, proactive health checks, and Technical Account Management (TAM)
- **Flexible warranty**Three- or five-year hardware warranty options, with optional service upgrades including Enterprise Server Software Support, YourDrive YourData, and Health Check.

Get started

Ransomware recovery is the last line of defense. and the one that matters most when prevention fails. With the Lenovo Solution for On-Premises Ransomware Recovery for VMware Cloud Foundation on ThinkAgile VX, you can recover business-critical workloads quickly and confidently, validate them in true isolation, and keep your data on infrastructure you control.

To learn more, contact your Lenovo representative or Business Partner, or visit lenovo.com/thinkagile.

For More Information
For more information about Lenovo solutions, contact your Lenovo representative or Business Partner, or visit Lenovo servers.

Related publications and links

For more information, see these resources:

- VMware by Broadcom, VMware Validated Solutions 9.X: On-Premises Ransomware Recovery for VMware Cloud Foundation (overview, design objectives, detailed design, IRE design, and recovery process). Figures 1–3 reproduced from this document): https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vvs/9-X/on-prem-ransomware-recovery-for-vmware-cloud-foundation.html
- VMware, Ransomware Recovery for VMware Cloud Foundation: Solution Brief: https://www.vmware.com/docs/ransomware-recovery-for-vmware-cloud-foundation-solution-brief
- Lenovo, ThinkAgile VX Series Datasheet: https://lenovopress.lenovo.com/datasheet/ds0104-thinkagile-vx-series
- Lenovo, VMware Cloud Foundation on Lenovo ThinkAgile VX: https://lenovopress.lenovo.com/lp1533-vmware-cloud-foundation-on-lenovo-thinkagile-vx-fx-reference-design
- CrowdStrike 2026 Global Threat Report: https://go.crowdstrike.com/2026-global-threat-report.html

Authors

Alejandro Perez is a WW Enterprise IT Solution Manager within Lenovo's Infrastructure Solutions Group (ISG). He leads the adoption and integration of Enterprise Infrastructure solutions, serving as the Subject Matter Expert for targeted solution architectures. He collaborates with organic and 3rd party SW ecosystem partners to drive innovation and contribute to the company's success. With over 20 years of experience in the IT industry, he has a strong background in Edge Computing, Business Development, and SAP HANA. He is passionate about bringing new technologies to the market and developing new solutions for regional markets.

Related product families

Product families related to this document are the following:

- ThinkAgile VX Series for VMware

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document, LP2491, was created or updated on August 17, 2026.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP2491
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP2491.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
Lenovo TruScale®
ThinkAgile®
ThinkSystem®
TruScale®
XClarity®

The following terms are trademarks of other companies:

AMD and AMD EPYC™ are trademarks of Advanced Micro Devices, Inc.

Intel®, the Intel logo and Xeon® are trademarks of Intel Corporation or its subsidiaries.

Other company, product, or service names may be trademarks or service marks of others.