Cyber Protection and Recovery for VCF

Key Cyber Resilience Challenges

- Security alert overload with manual triage
- Lack of visibility into network traffic
- Inconsistency of security policies across the infrastructure
- Inability to implement policies and remediate drifts at scale
- Reliance on traditional backup and DR for cyber recovery
- Recovery infrastructure setup and maintenance
- Manual integration of cyber recovery components across replication, orchestration, restore point validation and networking isolation

$10.5 T

projected global damage from cyberattacks in 2025[1]

Cyber resilience continues to be a daunting problem for organizations worldwide. End-to-end cyber resilience requires a holistic approach that starts at the infrastructure level and spans across strong distributed lateral security and cyber recovery as a crucial last line of defense. The VMware Cloud Foundation offers uniquely differentiated value to our customers in this space, especially as the threats they face continue to evolve and they need additional layers of protection to secure their infrastructure.

Cyber threats are not what they used to be—they have evolved over time to strategically bypass traditional security and response measures, infiltrate critical infrastructure and maximize damage. Data exfiltration has also become increasingly common, as cyber criminals attempt to inflict double or triple extortion to their victims and maximize the chances and size of their ransom payouts.

In an attempt to shield their data from these ever-evolving threats, organizations struggle in more ways than one. SOC teams face a security alert overload that they have to manually triage, have limited visibility into what's going on in their networks and workloads, and struggle to implement remediation measures at scale. Infrastructure teams are challenged as they look to preserve consistent hardening and security policies across the infrastructure as applications are moved, changed or deleted. In addition, their cyber recovery capabilities are thwarted because they continue to operate under the misconception that immutable/air-gapped backups and traditional file scanning will help them recover if their data is encrypted.

The VMware Cloud Foundation technology stack is uniquely designed to address these challenges. It brings together out-of-the-box hardened infrastructure, strong distributed lateral security with vDefend and secure cyber recovery with VMware Live Recovery.

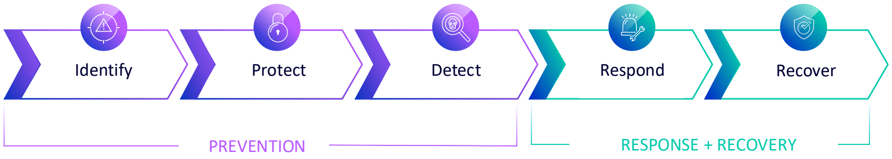


Figure 1: NIST Cybersecurity Framework.

[1] McKinsey & Company

75%

of SOC admins triage 100+ alerts daily

25%

of SOC admins triage **1000+** alerts daily

10X

reduction of alerts to triage with Intelligent Assist

75%

faster restore compared to traditional measures

Up to 24X

faster cyber recovery with local vSAN snapshot manager integration

1-minute

RPOs with enhanced vSphere replication

VMware vDefend Distributed Firewall + Advanced Threat Prevention

VMware vDefend Distributed Firewall and Advanced Threat Prevention enable zero-trust security for VCF sites on-premises and in the cloud through:

- GenAI-powered assistance, remediation, and simplified triage with Intelligent Assist
- Microsegmentation to prevent lateral movement of malware
- Intrusion Detection and Prevention Systems (IDS/IPS) to spot malicious behavior across network conversations and stop data exfiltration
- Network Traffic Analysis (NTA) and Network Detection and Response (NDR) to correlate threat campaigns based on similar indicators of compromise
- Zero-day threat prevention with malware sandboxing
- To learn more about vDefend Distributed Firewall and Advanced Threat Prevention, visit VMware Cloud Infrastructure

VMware Live Recovery

As robust as prevention and detection methods may be, even state-of-the-art security solutions aren't effective 100% of the time, so it is essential to have cyber recovery as a last line of defense. The biggest challenge organizations face is having to manually stitch together multiple point products to successfully recover from a ransomware attack. This use case leverages foundational capabilities of DR such as replication, orchestration, immutability and air-gapping, but requires additional key components:

- **Isolated clean room infrastructure:** an air-gapped site used to power on VMs and run advanced detection techniques for validation before restore to production
- **Embedded Next-Gen Antivirus/Behavioral Analysis:** aggressive detection analysis applied to running VMs in the isolated clean room
- **Deep history of immutable snapshots:** a deep snapshot library is crucial given that ransomware dwells within the environment before encrypting data and therefore requires IT teams to roll back days or weeks to a pre-infection restore point.
- **VM network isolation:** VMs must be isolated from each other during validation to prevent lateral movement of malware and reinfection.
- **Rapid restore point iterations:** cyber recovery is an iterative process, as different recovery point candidates will be evaluated until an uninfected snapshot is identified. This iteration needs to be fast and non-disruptive.

VMware Live Recovery integrates all these components into a guided, automated workflow that spans across identification, validation and restore of workloads at scale. Customers can choose between VCF isolated clean rooms on-premises or in the cloud, provision recovery sites just-in-time from the product UI and benefit from consumption-based pricing.

Cyber Recovery is more than DR

Recovery point selection

Cyber recovery requires a deep history of immutable, air-gapped copies with AI/ML-powered validation and goes beyond traditional DR requirements

Snapshot validation

Cyber recovery scenarios involve data encryption which requires advanced capabilities to analyze and restore, DR requires no validation

Recovery infrastructure

Cyber recovery requires an air-gapped, isolated clean room to safely test workloads before restore, DR does not require embedded security and network isolation

16-24x faster cyber recovery with vSAN local snapshots

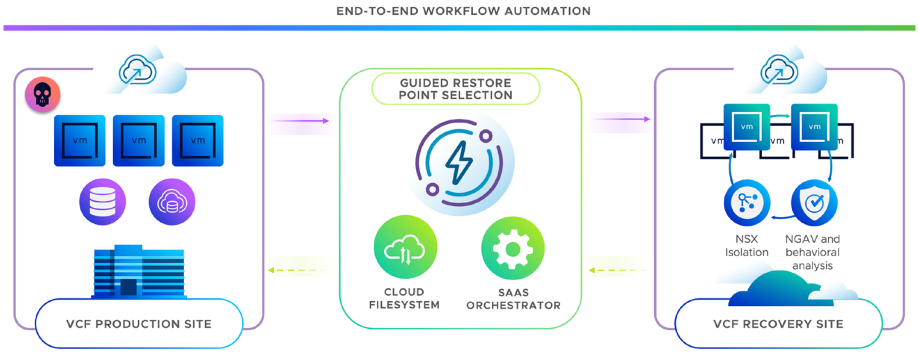


Figure 2: Cyber recovery to a VCF isolated clean room in the cloud (recovery to on-premises sites also supported).

Once the recovery site has been provisioned, the workflow provides recovery point selection guidance. Users can visualize a snapshot timeline along with advanced insights such as VMDK rate of change, file entropy and file deletion/creation/modification to select good snapshot candidates for validation.

For recovery point validation, VMware Live Recovery goes beyond traditional file scanning. Once restore point candidates are running in the isolated clean room, they undergo behavioral analysis with a Next-Gen Antivirus to spot fileless malware. A comprehensive vulnerability analysis as well as a file signature scan are also done to cover all bases. To prevent lateral movement during this process, push-button VM network isolation is integrated into the workflow.

Once clean snapshots are identified and the production site has been fortified and remediated, workloads undergo delta-based failback to minimize data transfers and speed up recovery.

All steps and feature integrations in the guided workflow are delivered through a single VMware Live Recovery subscription at no additional cost to the customer.

Customers can also choose to recover from local vSAN copies once they've identified uninfected restore points in the isolated clean room, as VMware Live Recovery tightly integrates with vSAN snapshot manager in VCF production sites. Restore from local vSAN snapshots lowers failback data transfers by orders of magnitude, which can speed up cyber recovery by 16-24x.[1]

VMware Live Recovery also includes disaster recovery, and both use cases are delivered through a unified management experience, with a single subscription and flexible licensing. Customers can recover from ransomware and other disasters and leverage on-premises or cloud VCF sites. Users can also deploy hybrid topologies for application tiering and customize replication schedules for different applications with RPOs as low as 1 minute

2. ESG Technical Validation of VMware Live Recovery

End-to-End Cyber Resilience for VCF

Infrastructure Hardening

- Identity federation
- Automated patch management
- Data at-rest and in-transit encryption
- Compliance monitoring

East-West Security

- Strong distributed lateral security
- Signature and behavior-based detection
- Data exfiltration avoidance
- Zero-day threat detection

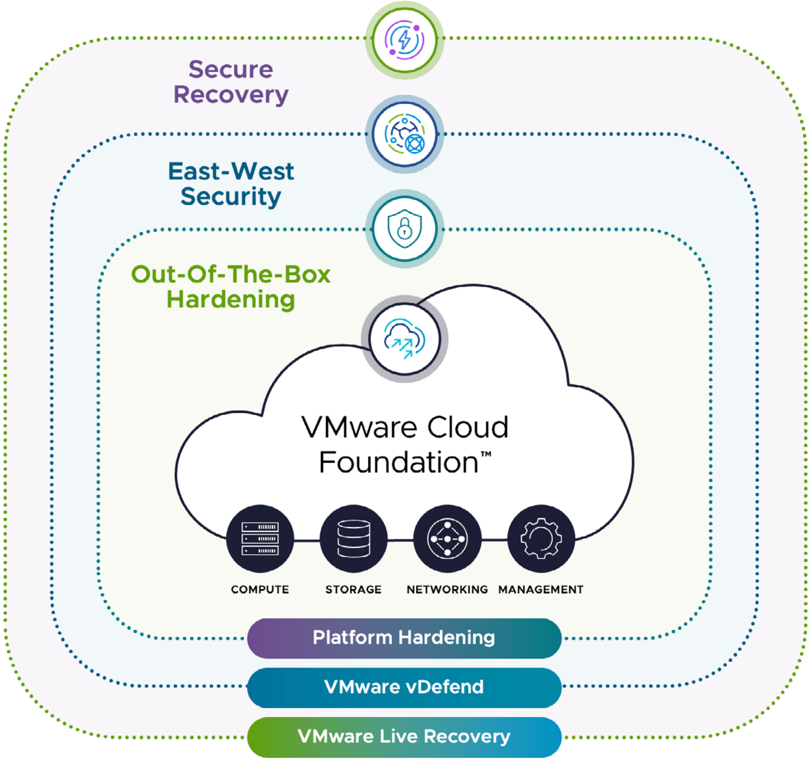
Cyber Recovery

- Confident recovery from existential threats
- Quick recovery with guided automation
- Simplified recovery operations

Learn more about VCF, vDefend and VMware Live Recovery at VMware.com and keep up with the latest innovations in cyber resilience through our VCF blog.

A Cyber Resilient Platform

The ability to prevent, withstand and recover from cyberthreats and other disasters has become an essential need for the modern organization, and the VCF platform helps enable this outcome end-to-end. With VMware Cloud Foundation, best-of-breed solutions and frictionless operations are no longer mutually exclusive.


Secure Recovery
East-West Security
Out-Of-The-Box Hardening
VMware Cloud Foundation™
COMPUTE
STORAGE
NETWORKING
MANAGEMENT
Platform Hardening
VMware vDefend
VMware Live Recovery