Secure and Resilient Platform with VMware Cloud Foundation

Key requirements of a secure and resilient platform

- **Platform security** – Maintain robust security at every layer of an infrastructure.
- **Cybersecurity** – Safeguard against threats like data breaches, ransomware and cyber-attacks.
- **Cyber recovery** – Quickly restore operations and protect and recover critical data after a cyberattack.
- **Disaster recovery** – Ensure continuous operations after a disaster with effective failover mechanisms.

A *secure and resilient platform* refers to an infrastructure designed to protect data and apps from security threats and ensure continuous, reliable service—even during cyberattacks, system failures, or disasters. But delivering a secure and resilient infrastructure platform involves several critical challenges that can lead to prolonged infrastructure downtime, data breaches, financial losses, reputation damage, and increased vulnerabilities to threats:

- **Rapid threat evolution** makes it difficult to keep infrastructure security up-to-date.
- **Increasing costs of cyberattacks** can lead to substantial financial strain.
- **Integration of multiple security tools** can be complex and costly.
- **Siloed infrastructure and security teams** can delay cyber responses.
- **Lack of disaster recovery preparedness** and compliance gaps can lead to infrastructure downtime.

The solution: VMware Cloud Foundation

VMware Cloud Foundation™ (VCF) is a comprehensive private-cloud platform that combines the scale and agility of public cloud with the security and performance of private cloud, offering industry-leading TCO. Purpose-built to modernize infrastructure and accelerate innovation, VCF delivers integrated, enterprise-class compute, networking, storage, management, and security across all endpoints such as private cloud, public cloud, partner clouds, sovereign clouds, edge, and co-location facilities.

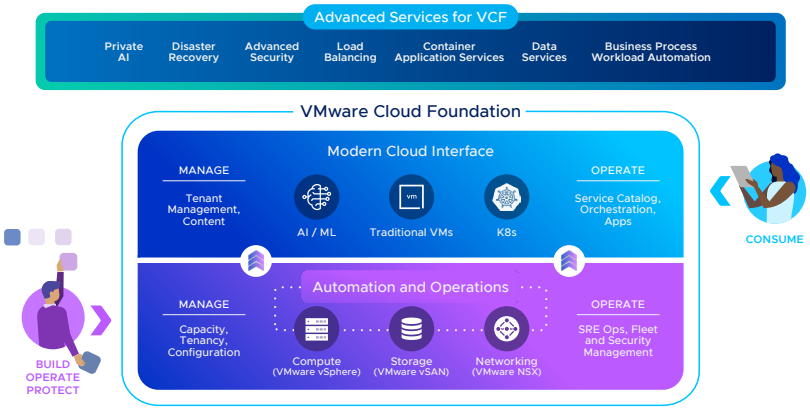
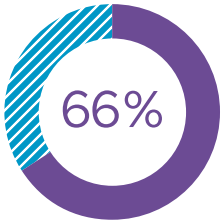


Figure 1: Deliver a secure and resilient platform with VMware Cloud Foundation.

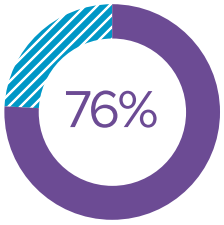
vmware® by Broadcom

Key benefits of using VCF for protecting and recovering from ransomware

- A modern Ransomware Recovery as a Service solution
- Fewer annual data loss incidents
- Faster and confident recovery from cyberattacks
- Reduced infrastructure downtime
- A reduction in lost staff productivity due to data loss incidents



66% quicker to resolve data loss incidents[1]



76% less staff productivity lost from data loss incidents[1]

$24,000
average annual benefit per VMware Live Recovery-supported application[1]

"I think it took us a little bit under two days. All in. And we literally have a completely isolated environment that we didn't have to set up. I really have yet to see a recovery product for ransomware that works as well as VMware's."

Alaa Elbanna
Global Director, Infrastructure, VanEck

Providing a secure and resilient platform

VCF delivers end-to-end protection, detection and recovery that includes out-of-the-box infrastructure hardening, integrated compliance and risk management, strong distributed lateral security, and cyber and disaster recovery. It offers consistent security policies to protect workloads and infrastructure from lateral cyberthreats while meeting corporate compliance, industry, and government requirements. It also includes capabilities to create custom compliance rules and checks to help keep your organization running smoothly. In addition, VCF delivers distributed network-based context-aware security capabilities, along with market-leading live recovery capabilities and workflows to protect and recover critical apps and data after a cyberattack or other disaster event.

Use case: Implement ransomware protection and recovery

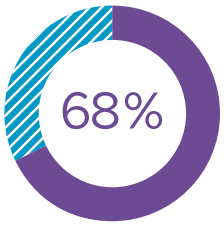
VCF helps your organization safeguard critical business data and ensure operational continuity by deploying security measures to detect and block ransomware in real time and creating recovery protocols to quickly restore compromised systems and data. Here are some key features and capabilities:

- **Cyber Recovery** – One of the technologies in VMware Live Recovery™, this service enables a confident, accelerated restore from modern ransomware. An advanced offering that needs to be purchased separately, it features the following key capabilities.
  - **VMware-managed Isolated Recovery Environment (IRE)** – Enable a safe, controlled recovery from ransomware in this secure environment, built and managed by VMware.
  - **Embedded behavioral analysis of powered-on workloads** – Identify and contain both file-based and fileless attacks within a secure, quarantined environment that can be provisioned directly from the product UI.
  - **End-to-end workflow** – This step-by-step guided workflow integrates identification, validation and restore of recovery points within a single UI.
  - **Push-button VM Network Isolation** – Isolate VMs from one another at restore to prevent lateral movement of ransomware and reinfection of the production environment.
  - **Guided restore point selection** – This feature enables informed selection of restore point candidates with insights such as VMDK rate of change and file entropy.
  - **Immutable, air-gapped recovery points** – Preserve data integrity at the time of recovery with snapshots restored in a secure, VMware-managed cloud file system.
- **Speed up recovery with VMware vSAN™ snapshots** – VMware Live Recovery now integrates with vSAN snapshot manager to enable recovery from a local vSAN snapshot, eliminating the need for full failback of the data from the IRE back to production, significantly reducing data transfer volume and speeding up the cyber recovery process.

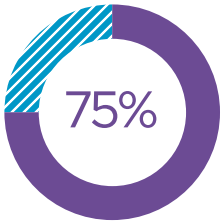
vmware® by Broadcom

Key benefits of using VCF to implement disaster recovery

- Less unplanned downtime
- Faster, more efficient disaster recovery
- Improved DR team productivity
- Simplified DR management
- Enhanced reliability



68% more productive DR teams[1]



75% quicker to resolve downtime events[1]

98% less unplanned downtime[2]

- **Minimize attack surface with VMware vDefend™ Firewall** – Protect application workloads with a multi-layer defense that includes the following capabilities:
  - **VMware vDefend Distributed Firewall (DFW)** – This software-defined Layer 2-7 firewall is integrated into the hypervisor and delivers scale-out micro-segmentation, helping you isolate the environment while the last-known clean recovery point is being identified.
  - **VMware vDefend Gateway Firewall (GFW)** – This is a software-only Layer 2-7 firewall designed and deployed for use cases such as zone-based controls for app workloads, policy controls for traffic entering and/or existing VCF workload domains.
  - **VMware vDefend Advanced Threat Prevention (ATP)** – Detect threats within the network with an array of advanced technologies:
    - » **Sandbox** – The network sandbox looks deep inside every artifact and uses advanced AI and machine learning (ML) to identify potentially malicious files and prevent them from executing.
    - » **Distributed Intrusion Detection/Prevention System (IDS/IPS)** – Inspect traffic at every workload using industry-leading signature sets and protocol decoders to find and block known threats.
    - » **Network Threat Analytics (NTA)** – Detect malicious behavior by identifying protocol anomalies, traffic anomalies, and host anomalies.
    - » **Network Detection and Response (NDR)** – Enable your security team to visualize attack chains by condensing massive amounts of network data into a handful of "intrusion campaigns."

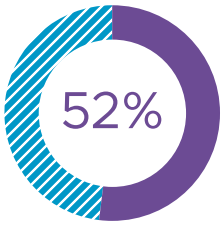
Use case: Implement disaster recovery

VCF enables your organization to deploy a comprehensive disaster recovery plan to restore critical systems, apps and data after a major disruption such as a natural disaster or system failure. Here are some key features and capabilities:

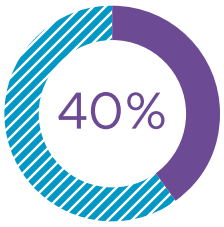
- **Site Recovery** – A component of VMware Live Recovery, this solution automates orchestration and non-disruptive testing of centralized recovery plans for all virtualized apps, ensuring your recovery time objectives (RTOs) are met. Here are some highlights:
  - **Enterprise-grade orchestration**
    - » Simple, policy-based management and automation help protect thousands of VMs using centralized recovery plans managed from the VMware vSphere® Web Client.
    - » VMware NSX® integration eliminates the need to manually remap networking.
    - » Non-disruptive testing of centralized recovery plans for all virtualized apps helps ensure a predictable RTO.
    - » Automated failback at scale enables you to return to regular operations with ease using centralized recovery plans.

Key benefits of using VCF to integrate security, compliance and resiliency

- Reduced downtime
- Improved security posture
- Simplified compliance management
- Enhanced customer and stakeholder trust
- Reduced risks and financial losses



52% improved security team efficiencies[2]



40% reduced risk of security breaches and associated costs[3]

$750,000
savings in security hardware costs per data center deployed[3]

>11x more
east-west network traffic secured[4]

  - **Compatible with any storage**
    - » Native integration with vSphere Replication, Virtual Volumes (vVols), and array-based replication solutions from all major VMware storage partners provides flexibility and choice.
  - **Next-generation vSphere Replication**
    - » Recovery points as frequent as just one minute help increase RPO granularity.
    - » Integration with a vast ecosystem of underlying replication technologies provides maximum flexibility.
- **Simplified disaster recovery with NSX Federation** – NSX unifies the network across racks and data centers with centralized federated management and resource pooling for active-active and active-standby deployments. Centralized policy configuration and enforcement across multiple locations from a single pane of glass enables network-wide policy consistency, operational simplicity, and a simplified disaster recovery architecture. In the NSX Federation, configuration changes are made on the active Global Manager—these changes are then synchronized with the relevant Local Managers and the standby Global Manager (if there is one).
- **Cost-effective, multi-site AZ and DR with VMware Avi™ Load Balancer License Portability** – The modern, software-defined Avi Load Balancer, an advanced service for VCF, simplifies and accelerates private-cloud app availability and resiliency. With Avi Load Balancer's Global Server Load Balancing (GSLB) capability and support for multi-AZ, it intelligently routes traffic across geographically dispersed data centers, ensuring app availability even if one site experiences an outage. In a DR scenario, a license can be assigned in Avi Cloud Console from an active site to a DR site without the need for idle capacity standby, **optimizing resource utilization and saving up to 50% in costs**.

Use case: Integrate security, compliance and resilience

VCF provides robust security measures, regulatory compliance, and resilience built into your IT infrastructure to protect sensitive data, meet legal obligations, and maintain infrastructure uptime for business continuity. Key features and capabilities include the following:

- **Out-of-the-box infrastructure hardening** – VCF delivers in-depth defense at both the server and hypervisor level with capabilities such as these:
  - **Identity Federation** enables you to take advantage of modern identity providers and their security features.
  - **Data-at-rest and data-in-transit encryption** helps protect data and metadata stored either by the infrastructure or as part of a workload.
  - **Lifecycle Manager, vMotion, and DRS** enable your organization to quickly and automatically remediate infrastructure security.
- **Hardware security** – VCF includes hardware security features such as TPMs and confidential computing technologies like AMD SEV-ES. In addition, secure boot, code signing, and host attestation features offer multiple layers of defense.

"By ensuring our critical clinical applications are protected and always available with vDefend security solutions, we advance St. John's Health's reputation as a trusted partner with the community."

Tyler Wertenbruch
IT Technical Manager, St. John's Health

- **Authentication and identity management** – VCF integrates Role-Based Access Control (RBAC) and Identity Federation to support Azure AD and Okta, as well as a single shared SSO instance or a separate isolated SSO instance.
- **Data security** – The VCF storage architecture provides encryption of data at-rest and in-transit throughout the stack.
- **Network security** – VCF includes a host of network security features and capabilities including the following:
  - **Adaptable networking and security policies** – As applications are moved, changed and retired, their networking and security policies are automatically adjusted, preventing the sprawl of stale firewall rules and reducing network outages.
  - **Continuous monitoring** – VCF Operations for networks, an integrated component of VCF, tracks network traffic across both virtual and physical networks, providing enhanced visibility and helping to detect potential risks.
  - **Advanced networking and security features** – These include the following:
    - **VMware vDefend Firewall** – This advanced service is a software-defined Layer 2-7 firewall purpose-built to secure virtualized workloads in VCF, providing stateful firewalling capabilities to protect against the lateral movement of threats. VMware vDefend Firewall is available in two form factors: Distributed Firewall (DFW) and Gateway Firewall (GFW). It also offers network traffic visibility into every host and workload across virtualized environments, and automated rule recommendations for microsegmentation.
    - **VMware vDefend Advanced Threat Prevention** – This advanced service delivers a software-defined Layer 2–7 firewall with threat prevention capabilities such as Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis (NTA)—with aggregation, correlation, and context engines from Network Detection and Response (NDR).
    - **VMware Avi Load Balancer** – This is an advanced service that provides enterprise-grade load balancing, global server load balancing (GSLB), web application security, and container ingress services in a single platform.
- **Integrated compliance** – VCF Operations, an integral component of VCF, provides alerts, policies, and reports to validate VCF resources against defined benchmarks, delivering continuous compliance checking with alerts. Choose from pre-defined VMware benchmarks, custom benchmarks, or out-of-the-box regulatory compliances like CIS, DISA, FISMA, HIPAA, ISO, and PCI DSS. Compliance drift alerts and auto-remediation are also embedded, helping to lower business risk, avoid hefty fines and reduce unplanned downtime.
- **Built-in resilience** – VCF offers a plethora of built-in resiliency features including the following:
  - **Stretched Clusters** – This capability enables you to stretch a vSAN cluster in a workload domain across two AZs within a region, so that in the event of a failure at one AZ, workloads can automatically failover to the other.

Helpful resources

VCF website

VMware Live Recovery website

VMware Security Solutions

Private Cloud Modernization Program solution brief

VCF TCO white paper and infographic

VMware Live Recovery business value white paper

VMware Live Recovery technical documentation

VMware Live Recovery Hands-on Lab

VCF blogs

Follow us on X

Follow us on LinkedIn

Watch latest videos on YouTube

- **vSphere Replication** – This hypervisor-based data protection and disaster recovery solution is fully integrated with VMware vCenter® Server and VMware vSphere Web Client, providing host-based, asynchronous replication of VMs.
- **vSAN Snapshots** – These capture the state and data of a VM at a specific point in time and make a copy on the same storage media that is actively running the workloads.
- **vSAN Data Protection** – Included in VMware vSAN 8 U3, this capability provides streamlined snapshot management by enabling admins to easily protect and recover VMs from accidental deletions and ransomware attacks through policy-based protection groups.
- **vSphere HA** – Ensure high availability for VMs by pooling the VMs and the hosts they reside on into a cluster. Hosts in the cluster are monitored, and in the event of a failure, the VMs on a failed host are restarted on alternate hosts.
- **vSphere Fault Tolerance (FT)** – This capability provides continuous availability for apps with up to four virtual CPUs by creating a live shadow instance of a VM that mirrors the primary VM.
- **Dual DPU support** – This capability enables Active/Standby configurations to ensure continuity and protection against DPU failures or uplink loss.

Get started

Learn more about how VCF can deliver a secure and resilient platform for your organization. Want help in your cloud journey? Our Private Cloud Modernization Program is designed to guide you through every step, no matter where you are in the process. Please contact your Broadcom representative to learn more.

Sources:

1. IDC white paper, sponsored by VMware by Broadcom. "The Business Value of VMware Live Recovery." Doc #US51113923. November 2023.
2. IDC white paper, sponsored by VMware by Broadcom. "The Business Value of VMware Cloud Foundation." Doc #US52312224. August 2024.
3. A Forrester Total Economic Impact of Broadcom VMware vDefend, Commissioned By Broadcom VMware, March 2025.
4. IDC white paper, sponsored by VMware by Broadcom, "The Business Value of Networking and Lateral Security for VMware Cloud Foundation." Doc #US52148724. June 2024.

vmware® by Broadcom

Item No: FY25-7866-BC-VMW-VCF-SECURE-RESILIENT-SO-USLET-WEB-20250409 4/25