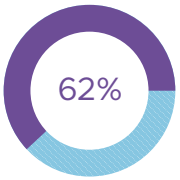
Security, Compliance and Operational Resilience

VMware Cloud Foundation

High breach rates persist



62% of enterprises estimated they experienced one or more breaches in the past year.[1]

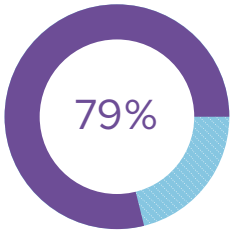
Data breaches are getting pricier

The global average cost of a data breach in 2024 is $4.88 million (10% increase from 2023).[2]

Outages are the new normal

On average, companies report 86 outages per year—translating to 324 minutes of weekly downtime.[2]

Regulatory risks can't be ignored



79% of organizations admit not being prepared to comply with operational resilience regulations, risking hefty punitive fines and penalties.[3]

1. Forrester's 2024 Security Survey
2. Cost of a Data Breach Report 2024, IBM
3. The State of Resilience 2025, Cockroach Labs

Security should not be an afterthought - it must be intrinsic to the platform itself. Customers today need a secure-by-default infrastructure that ensures the availability, integrity, and confidentiality of data while keeping pace with evolving cybersecurity threats. In addition, they need to secure the infrastructure, comply with industry regulations, and build resilience into systems to ensure continuous operation and data protection in the face of challenges such as hardware failures, network outages, and cyberattacks.

Comprehensive, intrinsic, enterprise-grade security

VMware Cloud Foundation delivers a resilient infrastructure and eases the customer's journey through integrated compliance, consistent governance, and seamless control.

VMware Cloud Foundation is hardened out-of-the-box as it delivers in-depth defense at both the host and hypervisor level. Some of the key built-in capabilities for infrastructure hardening are:

- Centralized Identity Management: Enables the infrastructure to take advantage of modern identity providers and their security features through a unified console
- Data-at-rest and data-in-transit encryption features run throughout the stack, to protect data and metadata stored either by the infrastructure or as part of a workload
- Lifecycle Management, vMotion, and DRS: Enables organizations to quickly and automatically remediate infrastructure security concerns without disrupting workloads

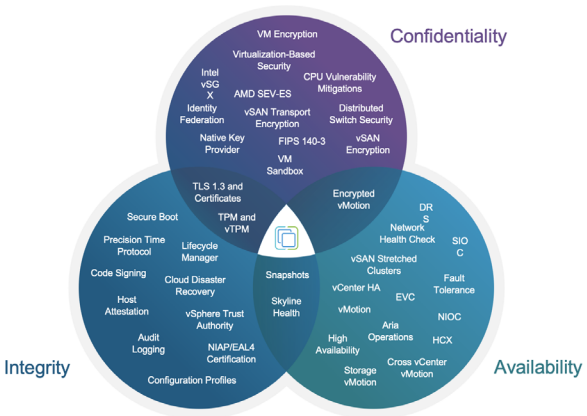


Figure 1: Comprehensive security built into the platform

vmware by Broadcom

Security: Much More Than Just Confidentiality

The central tenets of the field of information security are known as the **CIA Triad:** confidentiality, integrity, and availability.

Confidentiality involves protecting systems and data from unauthorized parties

Integrity entails preventing unauthorized modifications of data by groups or systems.

Availability ensures that data is accessible to authorized parties when needed.

Often, when considering security, the focus is on preventing breaches of confidentiality; however, this is only one third of the story.

Viewed through the lens of the CIA Triad, every feature in VMware Cloud Foundation is aligned with one or more of these principles. This means that every feature in VMware Cloud Foundation is a security feature, contributing to the overall resilience of the platform and the workloads you entrust to it.

VMware Cloud Foundation provides built-in resiliency with features such as:

- **Stretched Clusters:** This capability allows to stretch a vSAN cluster in a workload domain across two availability zones (AZ) within a region so that in the event of a failure at one AZ, workloads can automatically failover to the AZ.
- **vSphere Replication:** It is a hypervisor-based data protection and disaster recovery solution that is fully integrated with VMware vCenter Server and VMware vSphere Web Client, that provides host-based, asynchronous replication of VMs.
- **vSAN Snapshots:** These snapshots capture the state and data of a virtual machine (VM) at a specific point in time and make a copy of data on the same storage media that is actively running the workloads.
- **vSAN Data Protection:** With vSAN Data Protection in vSAN 8 U3, administrators can easily protect and recover VMs from accidental deletions and ransomware attacks through policy-based protection groups, thus providing streamlined snapshot management.
- **vSphere HA:** vSphere HA provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.
- **vSphere Fault Tolerance (FT):** This capability provides continuous availability for applications (with up to four virtual CPUs) by creating a live shadow instance of a VM that mirrors the primary VM. If a hardware outage occurs, vSphere FT automatically triggers failover to eliminate downtime and prevent data loss. After failover, vSphere FT automatically creates a new, secondary virtual machine to deliver continuous protection for the application.

Hardware security

VCF is well integrated with hardware security features such as Trusted Platform Module (TPM) and confidential computing technologies like AMD SEV-ES. Additionally, secure boot, code signing and host attestation features offer multiple layers of defense.

- **Authentication and identity management:** VCF integrates Role-Based Access Control (RBAC) to ensure that only authorized individuals have access to specific resources. It provides unified identity management with Identity Federation Support capability so that Azure AD and Okta identity federation support is integrated within VCF. Also, VCF allows administrators to create new workload domains configured using either a single shared SSO instance or a separate isolated SSO instance.
- **Data Security:** VCF's storage architecture provides encryption of data at-rest and in-transit throughout the stack.

Network security

- **Adaptable networking and security policies:** As applications are moved, changed and retired, their networking and security policies are automatically adjusted, which prevents the sprawl of stale firewall rules and lowers network outages.

Key Benefits: VMware vDefend

No blind spots: Get complete coverage across L4-L7 flows and across workloads, and gain visibility into user behaviors, processes, workload context to identify and block threats.

No network changes: Radically simplify firewall deployment and operations by eliminating changes to the network and avoiding traffic hair-pinning.

Security as code: Deliver "security as code" that provides policy recommendations, automates deployment, configuration, and operationalization.

Dynamic policy orchestration: Pre-create policies before workloads are deployed, and ensure workloads maintain policies throughout their lifecycle.

- **Continuous monitoring:** VCF Operations for networks, an integrated component of VCF, tracks virtual network traffic, offering excellent visibility to detect network traffic patterns and potential risks. It also centrally gathers and analyzes audit and system logs from infrastructure and workloads facilitating prompt reactions to potential security breaches or compliance issues.

Advanced Networking and Security

Advanced services for VCF such as VMware vDefend Firewall and VMware vDefend Firewall with Advanced Threat Prevention (ATP) provide comprehensive zero trust lateral security.

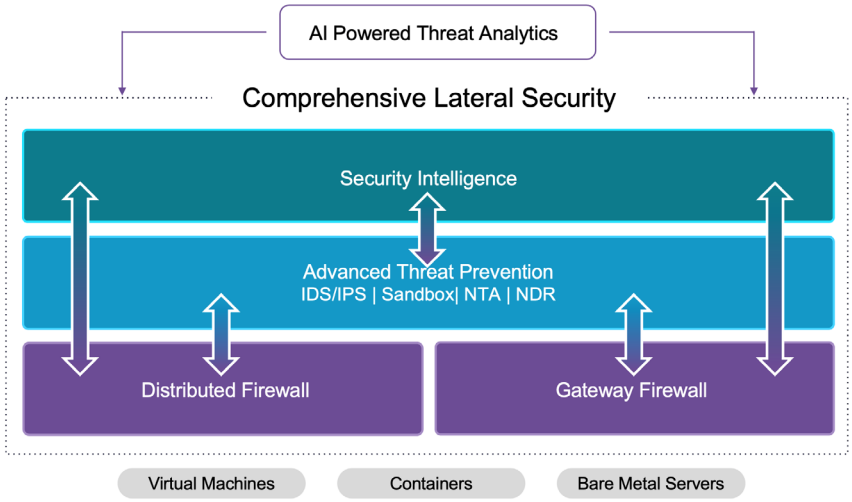


Figure 2: vDefend: Fully Integrated Security Stack

VMware vDefend Firewall: VMware vDefend Firewall is a software-defined Layer 2-7 firewall purpose-built to secure virtualized workloads in VMware Cloud Foundation. It provides stateful firewalling capabilities that can be used by organizations to protect against the lateral movement of threats. VMware vDefend Firewall includes a comprehensive suite of security features such as:

- **Distributed Firewall (DFW):** A software-defined Layer 2-7 firewall integrated into the hypervisor that delivers scale-out micro-segmentation. A Distributed Firewall can be deployed at each vSphere workload.
- **Gateway Firewall (GFW):** A software-only L2-7 firewall designed and deployed for use cases such as zone-based controls for application workloads or policy controls for traffic entering and/or existing VCF workload domains. A Gateway Firewall can be deployed on a vSphere host, either as a Virtual Machine (VM) or as an ISO image on a physical server.
- **Security Intelligence:** A distributed analytics platform that provides network traffic visibility across virtualized environments – every host and every workload – and automated rule recommendations for micro-segmentation.

Benefits in Numbers

- 40% reduction in risk[1] (VMware vDefend)
- 50% reduction in CapEx compared to hardware firewalls[2] (VMware vDefend)
- 75% faster downtime resolution[3] (VMware Live Recovery)

1. Forrester TEI Study of vDefend, March 2025
2. Internal VMware Study: VMware Value Modeling, 3rd party customer interviews
3. IDC Business Value of VMware Live Recovery, March 2024

VMware vDefend Firewall with Advanced Threat Prevention: VMware vDefend Firewall with ATP is a software-defined Layer 2–7 firewall purpose-built to secure virtualized workloads in a private cloud. It provides stateful firewalling with threat prevention capabilities that protect organizations against advanced threats. ATP combines multiple detection technologies—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).

- Distributed Intrusion Detection and Prevention System (IDPS): It inspects network traffic for malicious activities and security vulnerabilities and simplifies compliance audits.
- Network Sandboxing: It provides advanced malware analysis of artifacts by deconstructing malicious behavior engineered into a file or URL.
- Network Threat Analytics (NTA): It detects anomalous activity and malicious behavior by identifying protocol anomalies (unusual protocol activity), traffic anomalies (unusual traffic activity), and host anomalies (unusual workload behavior).
- Network Detection and Response (NDR): It enables the security team to visualize attack chains by condensing massive amounts of network data into a handful of "intrusion campaigns." It achieves this visualization by aggregating and correlating security events such as detected intrusions, suspicious objects, and anomalous network flows.

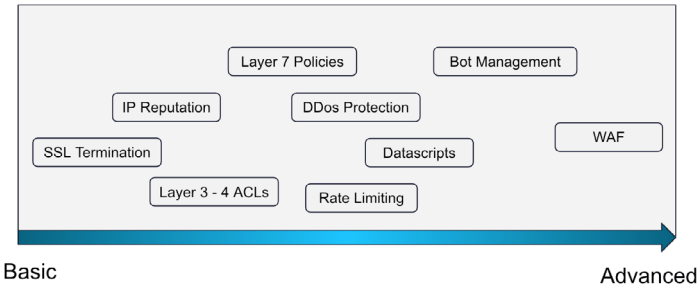


Figure 4: Avi delivers a full application security suite

VMware Avi Load Balancer: Industry's first and only software-defined load balancer - offered as an advanced service to VCF - allows customers to implement centrally managed elastic load balancing for application workloads within VCF. Avi provides enterprise grade load-balancing, global server load balancing (GSLB), web application security, and container ingress services in a single platform. It has four primary functionalities for application availability and resilience- local and global load balancing, SSL termination, web application firewall (WAF) that provides OWASP Top 10 protection to in-line application traffic, deep application visibility including analytics for VMs and container applications, an ingress controller and load balancer for Kubernetes workloads. The built-in WAF is a crucial component for PCI compliance, as it can filter malicious traffic and prevent unauthorized access to cardholder data. Also, Avi's WAF includes support for the Core Rule Set (CRS), which provides a comprehensive set of rules for detecting common web application vulnerabilities.

Key Benefits: Avi Web App and API Security

- Point-and-click simplicity for security policies with central control
- Elastic scale with high performing, load based automatic scale-out architecture
- Granular security insights on traffic flows and rule matches for precise policies
- Automated threat updates through Cloud Services
- Real-time app security insights and analytics
- Protects applications from DDoS attacks and OWASP Top 10 threats

VMware Live Recovery: VMware Live Recovery offers protection from modern ransomware and disaster situations for VMware-based servers and workloads within a managed cloud or on-premises environment to ensure the availability and recoverability of your critical assets.

VMware Live Recovery makes it easier to protect and recover data using a single deployment method and flexible licensing model, so admins can provision and manage VMware Live Cyber Recovery and VMware Live Site Recovery from one interface.

- **VMware Live Cyber Recovery** is an easy-to-use, just-in-time ransomware and disaster recovery (DR) solution, delivered as SaaS, with cloud economics.
  VMware Ransomware Recovery provides an isolated recovery environment (IRE) on a VMware Cloud recovery SDDC that allows you to inspect, analyze, recover, and validate that infected VMs are safe to restore them to a production environment.
- **VMware Live Site Recovery**
  VMware Live Site Recovery is an end-to-end disaster recovery solution that uses array-based, VMware vSphere Replication host-based, or VMware Virtual Volumes (vVols) replication along with VMware Live Site Recovery orchestration.

Figure 3: Compliance Packs in VMware Cloud Foundation

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. Defined benchmarks can be one of more of the following:

- Pre-defined VMware benchmarks which monitor the environment against various VMware defined security recommendations.
- Build-your-own custom benchmarking policies which check the environment against the custom defined policies.
- Out-of-the-box regulatory compliances, specifically: CIS Security Standards, DISA Security Standards, FISMA Security Standards, HIPAA, ISO Security Standards, and PCI DSS Compliance Standards.

Key Benefits: 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

Learn More

To learn more about security, regulatory compliance, and ransomware protections within VMware Cloud Foundation visit:

https://bit.ly/vcf-security

https://bit.ly/vcf-ransomware

https://bit.ly/vcf-compliance

Product Resources:

VMware Cloud Foundation

VMware vSAN

VMware vDefend Firewall

VMware vDefend ATP

VMware Avi Load Balancer

VMware Live Recovery

How to get started

Learn more about how VCF can help you build a secure, resilient, and compliant modern private cloud infrastructure on-premises or at edge sites. Whether you're looking to scale seamlessly, enhance security, or simplify your IT operations, VCF provides the flexibility and power you need.

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 and start your journey toward a future-proof IT infrastructure.

Summary

VMware Cloud Foundation (VCF) is the ideal solution for building and operating private cloud infrastructure on-premises or at the edge. It combines the scale and agility of public cloud with the security and performance of private cloud, enabling faster time to market, increased innovation, and lower TCO.

VMware Cloud Foundation stands out as a leader in securing critical workloads and data. Its robust security measures are deeply embedded within the infrastructure, providing a solid foundation for protection. This thorough approach not only safeguards against threats but also simplifies regulatory compliance efforts. As a result, VMware Cloud Foundation is the choice for businesses worldwide seeking security, compliance, and resilience for their IT operations.

For more information, please visit VMware Cloud Foundation.

vmware by Broadcom

Item No: Use Case 3.3 - Security, Compliance and Operational Reliance 5/25