Top 5 Challenges of Building a Secure and Resilient Platform

And how to overcome them with
VMware Cloud Foundation

› Get Started

vmware®
by Broadcom

Introduction: Key requirements of a secure and resilient platform

A secure and resilient infrastructure is essential for modern organizations to thrive. But what, exactly, do you need to build a secure and resilient platform? Let's take a look:

Platform security

You need to maintain security at every layer of your infrastructure.

Cybersecurity

You need to safeguard against threats like data breaches, ransomware and cyberattacks.

Cyber recovery

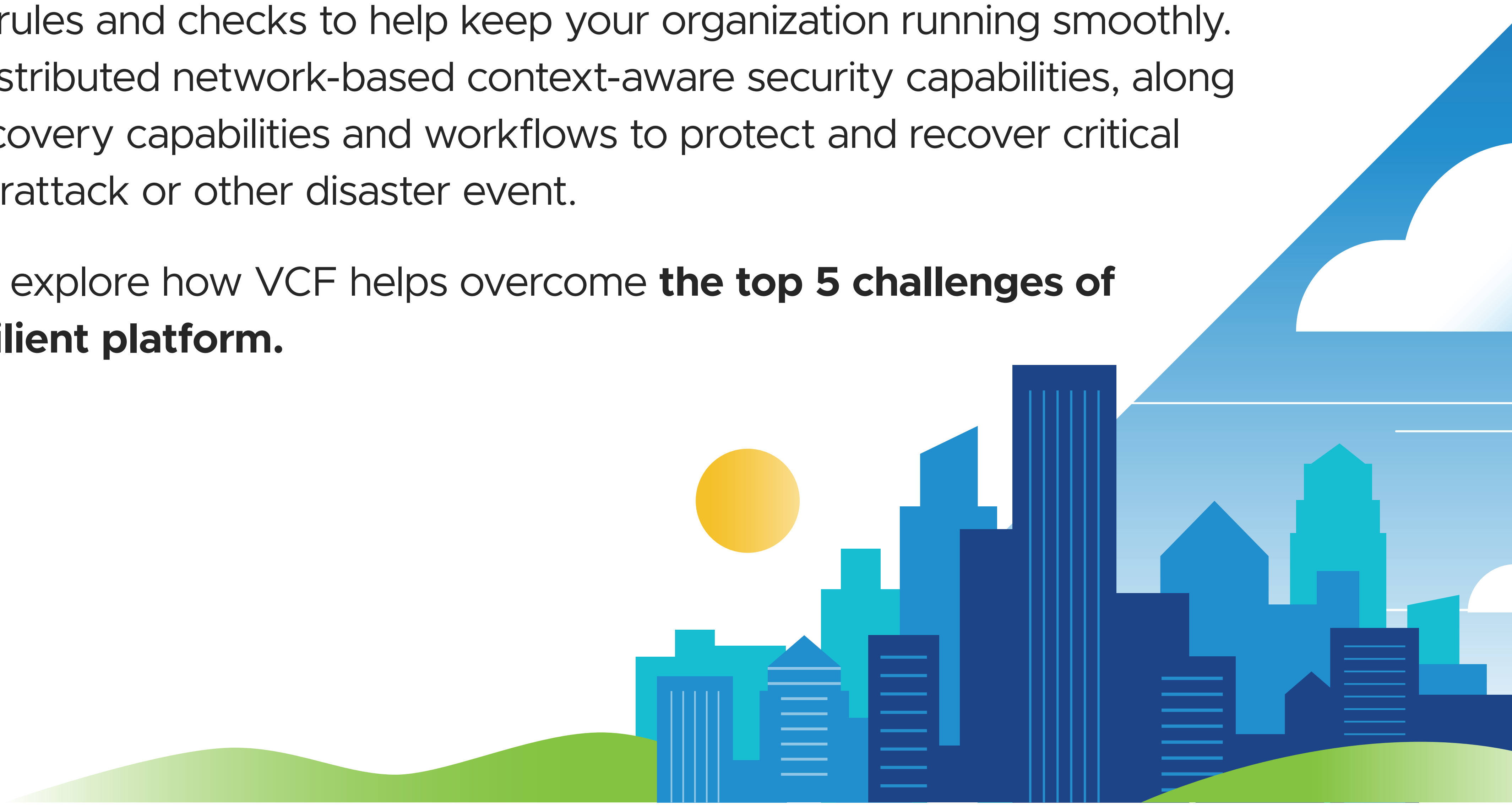
You need to quickly restore operations and protect and recover critical data after a cyberattack.

Disaster recovery

You need to ensure continuous operations after a disaster with effective failover mechanisms.

This is exactly what VMware Cloud Foundation™ (VCF) can do. VCF is a comprehensive private-cloud platform that delivers end-to-end protection, detection and recovery with 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.

In the following pages we'll explore how VCF helps overcome **the top 5 challenges of building a secure and resilient platform.**



Rapid threat evolution

Lateral movement of modern ransomware attacks and new methods of infiltration such as fileless attacks make it difficult to keep infrastructure protections up to date. As a result, conventional endpoint detection and antivirus solutions struggle to identify and stop today's threats.

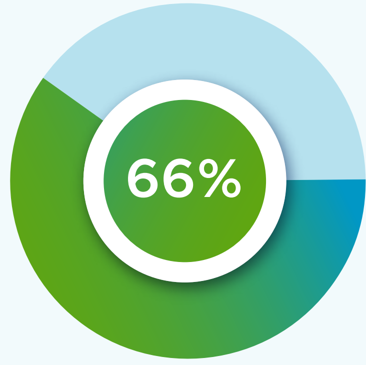
of ransomware attacks are fileless in nature.[1]

The solution: VMware Cloud Foundation

VMware Live Recovery™, an advanced service on top of VCF, provides secure cyber recovery to enable a confident, accelerated restore from modern ransomware. Guided recovery workflows enable you to quickly identify recovery point candidates, validate restore points using embedded behavioral analysis, and restore them with minimal data loss.

VMware vDefend™, another advanced service, delivers a multi-layer defense to protect application workloads by dramatically minimizing the attack surface.

$24K average annual benefit per VMware Live Recovery–supported application.[2]



quicker to resolve data loss incidents.[2]

[1] CrowdStrike, Inc. "2023 Global Threat Report." 2023.

[2] IDC white paper, sponsored by VMware by Broadcom, "The Business Value of VMware Live Recovery." Doc #US51113923. November 2023.

Increasing costs of cyberattacks

The escalating costs of cyberattacks, including recovery efforts, regulatory fines, and reputational damage, can cause substantial financial strain for today's organizations.

Recovery efforts alone—ranging from system restorations and forensic investigations to the implementation of stronger security protocols—can run into millions of dollars.

$2.73M

average recovery cost (excluding ransom payment) to recover from ransomware attack.[3]

The solution: VMware Cloud Foundation

VMware Live Recovery delivers Ransomware Recovery as a Service across VCF with advanced isolated testing and restoration at scale. With capabilities such as VMware-managed Isolated Recovery Environment (IRE), Embedded Behavioral Analysis, end-to-end guided workflows, and Guided Restore Point Selection, it dramatically speeds up the cyber recovery process and minimizes data loss.

76%

less staff productivity lost from data loss incidents.[4]

[3] Sophos Ltd. "The State of Ransomware 2024." April 2024.

[4] IDC white paper, sponsored by VMware by Broadcom, "The Business Value of VMware Live Recovery." Doc #US51113923. November 2023.

Complex security integration

Implementing robust security across every layer of infrastructure and scaling security measures to accommodate growth and changes in infrastructure requires organizations to integrate multiple security tools, which can be complex and costly.

What's more, integrating new security measures with legacy systems and fragmented data across dispersed environments can introduce vulnerabilities and make it harder to achieve consistent resilience across all systems.

The solution: VMware Cloud Foundation

VCF includes advanced security features such as infrastructure hardening, hardware security, microsegmentation, data-at-rest and data-in-transit encryption, and identity and access management (RBAC) integrated directly into the platform.

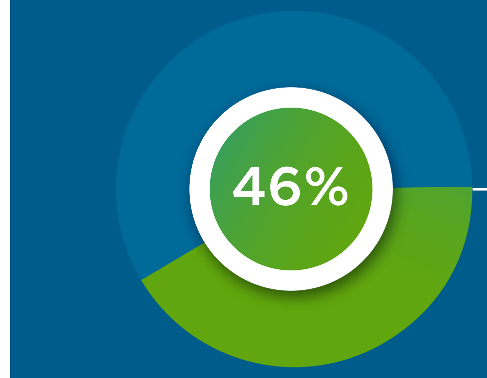
Adding VMware vDefend on top of VCF delivers advanced firewall and threat prevention capabilities to protect your organization against modern threats.

>11x more east-west network traffic secured.[5]

[5] IDC white paper, sponsored by VMware by Broadcom, "The Business Value of Networking and Lateral Security for VMware Cloud Foundation." Doc ##US52148724. June 2024.

Lack of collaboration and inconsistent operating models

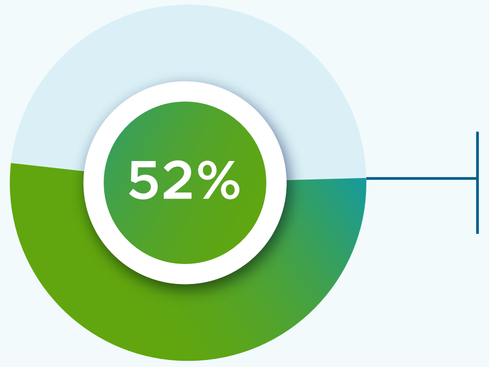
Typically, infrastructure and security teams operate in silos with disjointed tools and processes across different environments, leading to delayed responses to cyber incidents, increased risk of vulnerabilities, and potential data loss.



of respondents complained about lack of an orchestrated process in place between IT, security, and business leaders for responding and recovering from ransomware.[6]

The solution: VMware Cloud Foundation

With VCF, the ability to establish more standardized and repeatable security requirements and approaches across IT environments opens up time for security teams to focus on improving actual security results. With automated vulnerability scanning, security patching and troubleshooting, it reduces the time and effort spent on manual intervention.



improved security team efficiency with VMware Cloud Foundation.[7]

[6] A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024.

[7] IDC white paper, sponsored by VMware by Broadcom, "The Business Value of VMware Cloud Foundation." Doc #US52312224. August 2024.

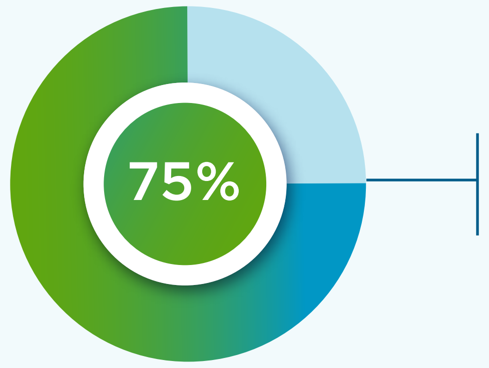
Disaster recovery and compliance preparedness

Effective disaster recovery requires both planning and infrastructure support, which can be resource intensive. In addition, meeting stringent regulatory and compliance requirements and addressing compliance gaps can further complicate infrastructure management.

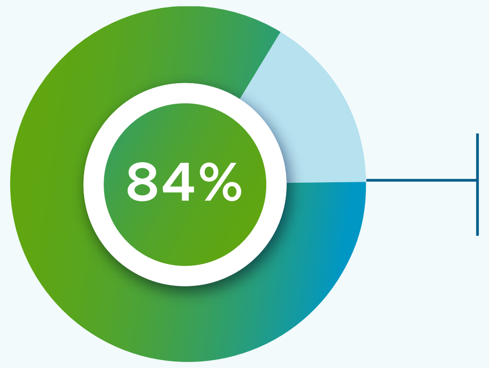
The solution: VMware Cloud Foundation

VMware Live Recovery delivers disaster recovery capabilities across VCF, on-premises and in the public cloud, providing automated orchestration and non-disruptive testing of centralized recovery plans for all virtualized applications.

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.



quicker to resolve downtime events.[8]



less staff productivity lost due to unplanned downtime.[8]

[8] IDC white paper, sponsored by VMware by Broadcom, "The Business Value of VMware Live Recovery." Doc #US51113923. November 2023.

Build a secure and resilient platform for your organization

Deliver end-to-end protection, detection and recovery with VMware Cloud Foundation.

Check out these helpful resources to get started:

VCF website Blogs

VMware:

Live Recovery website Security Solutions

Follow us:

X LinkedIn

Watch our latest videos:

YouTube

vmware® by Broadcom