LOGICALIS
Architects of Change

vmware
by Broadcom

Solution Brief

Cyber Resilience Starts at Infrastructure Layer

How Logicalis and VMware Cloud Foundation build security, recovery, and compliance into private cloud infrastructure



For organizations of every size, cyber attacks are not a question of if, but when, making resilience a key component of every security strategy. Yet many organizations are underprepared, as recent research has shown

78%
of organizations experienced a ransomware attack in 2025[1]

Nearly
40%
of those executives believed their teams were “well prepared” to prevent and recover from the threat[2]

Yet
50%
of affected companies were completely unable to fully restore the data they lost[3]

This resilience gap, dubbed the "Resilience Illusion" by VMware, requires security, recovery, and compliance to be built into the infrastructure layer itself, so every workload, application, and dataset inherits the same protections. In this brief, we'll see how the private cloud provides that foundation.

The Business Case for Resilience by Design

Historically, enterprise security focused on keeping attackers out. Today, however, adversaries increasingly log in with stolen credentials, then move laterally using legitimate administration tools that blend in with everyday network traffic. For most organizations, the core challenge lies in structural, legacy limitations:

- Siloed network, security, and IT operations
- Fragmented toolsets spread across many vendors
- Defenses designed for file-based threats
- Point-in-time compliance checks that lag behind real-time risk

Overcoming these limitations starts with an outcome-centric approach that unites security, compliance, and resilience. When resilience is built into the infrastructure, organizations can contain incidents faster, limit costly downtime, and reduce the expense of recovery. Continuous compliance also lowers audit burden and regulatory risk, since teams can prove at any point in time that controls are actively enforced. The result is a stronger financial position and greater confidence to pursue new initiatives.

1 CrowdStrike, “State of Ransomware Survey,” 2026
2 IBM Institute for Business Value, “AI and Cyber Threat Evolution Analysis,” 2025/2026
3 IBM Security, “Cost of a Data Breach Report,” 2025

Infrastructure-Level Resilience with VMware Cloud Foundation

Organizations that build resilience into their infrastructure can move from reactive incident response to a resilient posture that helps them withstand, contain, and recover from attacks. VMware Cloud Foundation (VCF) builds these capabilities into its private cloud platform, extending consistent protection across VMs, containers, and AI workloads.

Contain Threats

Attackers who gain a foothold typically move laterally in search of high-value systems. Zero Trust segmentation at the hypervisor layer limits that movement by verifying every connection between workloads.

VMware vDefend delivers hypervisor-native Zero Trust lateral security, and VCF 9.1 extends Zero Trust security and resilience across every layer of the platform, from vSphere and NSX to VCF Private AI Services. With these protections in place, security teams can isolate compromised workloads quickly and identify threats early.

Protect Data and Identity

Because data and identities are the assets attackers want most, encryption should protect information at rest, in motion, and in use. Through VMware Advanced Cyber Compliance, VCF supports confidential computing, which runs sensitive workloads in hardware-encrypted memory that remains inaccessible even to the hypervisor.

Identity has grown more complex with the proliferation of AI agents, yet many organizations either have no identity management strategy for AI agents or they rely on predefined human access. Identity Security helps organizations apply consistent access controls across the platform, to both AI agents and humans.

Recover With Confidence

Ransomware recovery depends on a clean, trusted environment for restoration. VMware Advanced Cyber Compliance 9.1 automates cyber and disaster recovery. Recovery points power on instantly inside isolated, on-premises VCF clean rooms, where an integrated EDR sensor is automatically injected into each VM so teams can validate workloads before returning them to production. With these isolated clean rooms, recovery becomes a tested, repeatable process with a verified, clean outcome.

Deliver Proven, Continuous Compliance

Regulators and auditors increasingly expect organizations to demonstrate resilience on demand, through ongoing audits, documented evidence of security controls, and timely incident reporting. Advanced Cyber Compliance uses integrated capabilities in VCF Operations for fully automated compliance monitoring and desired state remediation across the entire VCF stack. Continuous remediation and unified visibility keep environments aligned with policy and give teams audit-ready evidence whenever it is requested.

Built into VCF, these capabilities can help organizations stay resilient across the full lifecycle of an attack, from prevention through recovery and compliance.



Build Resilient Infrastructure

with Logicalis and VMware

With Logicalis and VMware, organizations gain access to the expertise needed to build a more modern, resilient private cloud infrastructure. We provide support across the full lifecycle of design, deployment, and management through our proven approach:

Align

Assessments of recovery readiness, security posture, and compliance requirements.

Transform

Implementation and hands-on support from our teams, from advisory and training to deployment, management, and optimization.

Scale

Ongoing strategy sessions, monitoring, recovery testing, and compliance reporting, so teams can focus on the business.

Together with VMware, we help organizations move from reactive recovery to infrastructure designed for resilience. If you are ready to build a more resilient infrastructure, contact us today to schedule a complimentary assessment.

Schedule Free Consultation

Why Logicalis?

- 7,000+ professionals serving 10,000+ clients across 30 territories
- VMware partner with a highly certified team of VMware technology experts
- Lifecycle services across cloud, connectivity, collaboration, and security
- Cybersecurity Maturity Model Certification (CMMC) Level 2 and ISO 27001:2022 accreditation
- Named to CRN's MSP 500 list for 13 consecutive years

LOGICALIS Architects of Change | vmware by Broadcom