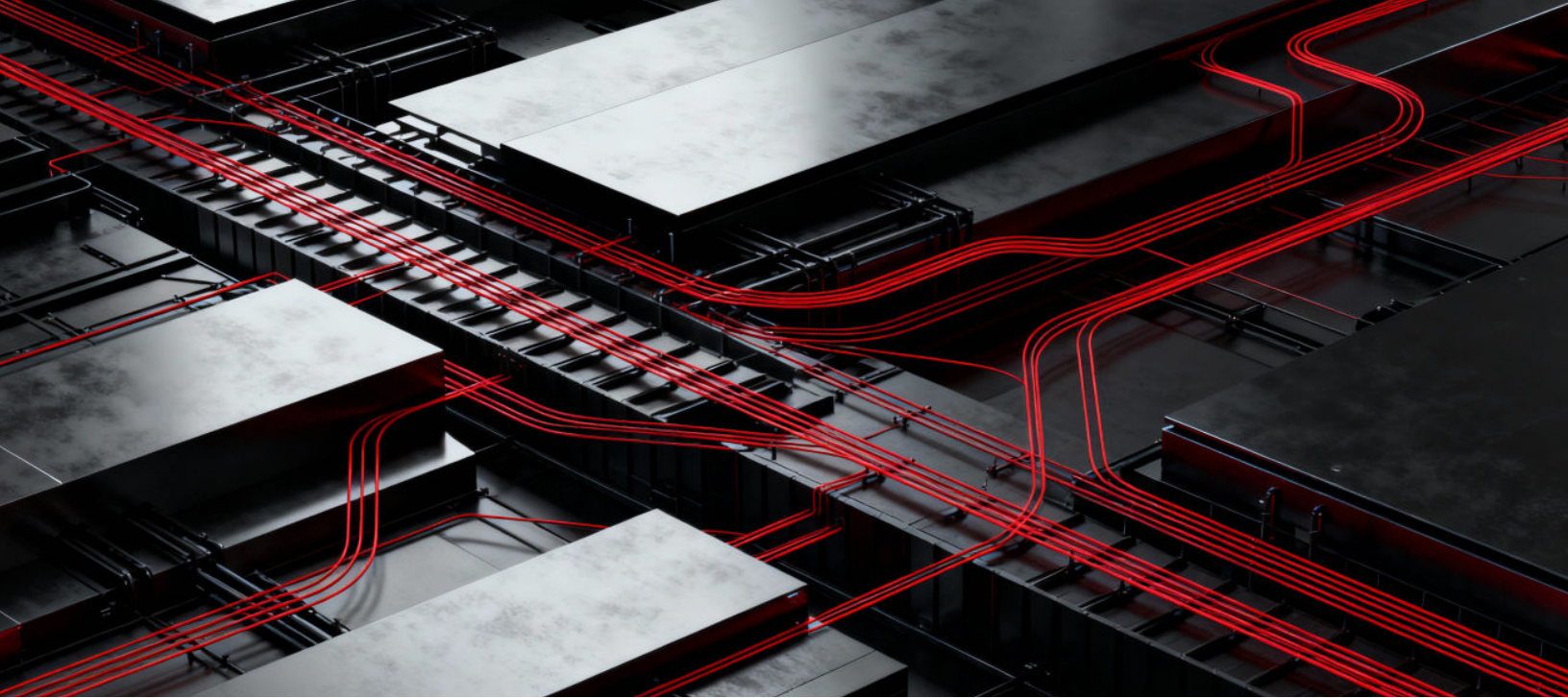




Modern Private Cloud: Balancing Operational Agility with Data Sovereignty



Introduction

For more than a decade, the technology industry has operated under the assumption that the public cloud is the ultimate destination for all IT infrastructure. However, a significant shift is underway. While public cloud adoption has driven agility, it has also exposed critical shortcomings regarding sovereignty and control. Today, organizations are realizing that the original promise of the public cloud – simplification and unfettered agility – often conflicts with the hardening reality of geopolitical risks and strict regulatory requirements.

Modern private cloud platforms have emerged as the definitive answer to this dilemma. Far from a return to legacy infrastructure, these platforms deliver the agility associated with the public cloud while securing the data control and sovereignty that have become non-negotiable for global enterprises.

The Public Cloud Reality and the Sovereignty Gap

The original vision of cloud computing centered on the ability to offload infrastructure management to drive agility. However, for many organizations, the reality has diverged from this promise. As digital footprints have expanded, data control has shifted from an optional consideration to a non-negotiable requirement.

Global hyperscalers, structured to prioritize massive scale, often face difficulties in meeting the strict data, operational, and jurisdictional requirements of specific regions. Their standardized, one-size-fits-all service models frequently conflict with European regulatory mandates, including GDPR, DORA, the EU AI Act, and NIS2.

A critical distinction must be made between data residency, where the data is physically stored, and data sovereignty, which refers to the legal jurisdiction governing that data. While hyperscalers can address residency requirements through local availability zones, they often struggle to guarantee total immunity from extraterritorial laws, such as the US CLOUD Act, which conflict with European regulations.

However, the industry's understanding has evolved significantly beyond this jurisdiction-centric definition. The modern concept of 'digital' or 'cloud sovereignty' now encompasses a broader strategic imperative: autonomy of action. This expanded framework demands more than just legal protection; it requires structural independence to ensure business continuity and strategic choice.

True cloud sovereignty is now understood to include four additional pillars:



Reduced Technological Dependence: Mitigating the risks of foreign export controls, price volatility due to tariffs, and the potential threat of remote 'kill switches'.



Operational Independence: A reduction in vendor concentration and lock-in, ensuring organizations retain the ability to seamlessly move workloads and develop their own platforms independently.

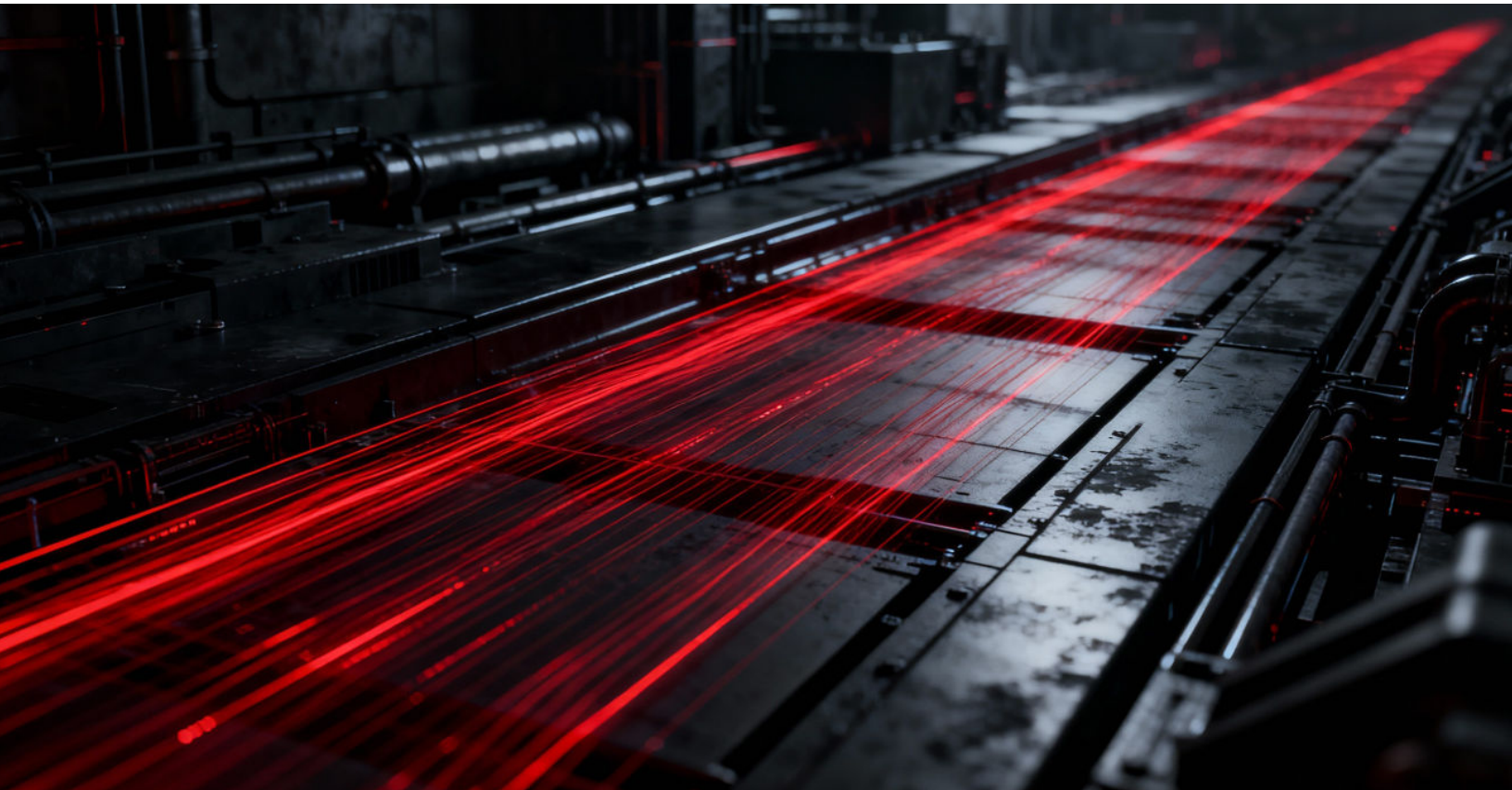


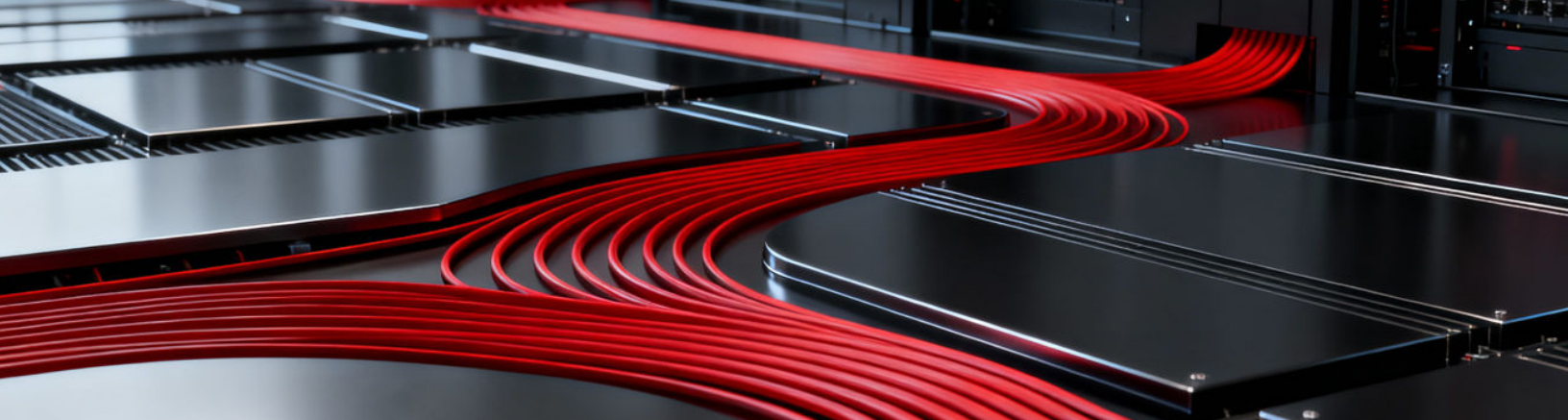
Local Security Control: The implementation of specific national security standards (such as C5 or SecNumCloud) and capabilities such as Bring Your Own Key (BYOK) encryption.



Economic Contribution: A positive impact on the local economy, fostering skills development and supporting the creation of a resilient local industrial base.

Consequently, the regulatory and strategic landscape is driving a need for service providers that can ensure this holistic level of sovereignty – a degree of jurisdictional and operational isolation that global public cloud providers struggle to fulfill completely.





The AI Factor: Amplifying the Need for Control

The rapid ascendancy of AI has further complicated the infrastructure decision-making process. While few enterprises are training foundation models from scratch, most are aggressively pursuing model customization and inference strategies – specifically fine-tuning and Retrieval-Augmented Generation (RAG).

These workloads amplify the criticality of data control. In a RAG architecture, for instance, proprietary corporate data is retrieved and fed into the AI model to generate accurate, context-aware responses. If this process occurs in a public environment, sensitive intellectual property and customer data must traverse public APIs, introducing significant risk.

For enterprises, the priority is sovereign inferencing: the ability to run pre-trained open source or licensed models directly adjacent to where the data resides. This approach shifts the paradigm from 'moving data to the model' to 'bringing the model to the data'. By keeping the inference engine and the data repository (such as vector databases) on a private cloud platform, organizations minimize latency and egress costs while ensuring that sensitive inputs and generated outputs never leave their sovereign boundary. In this context, regulatory compliance is not merely a checkbox, but a prerequisite for safely unlocking the value of AI.

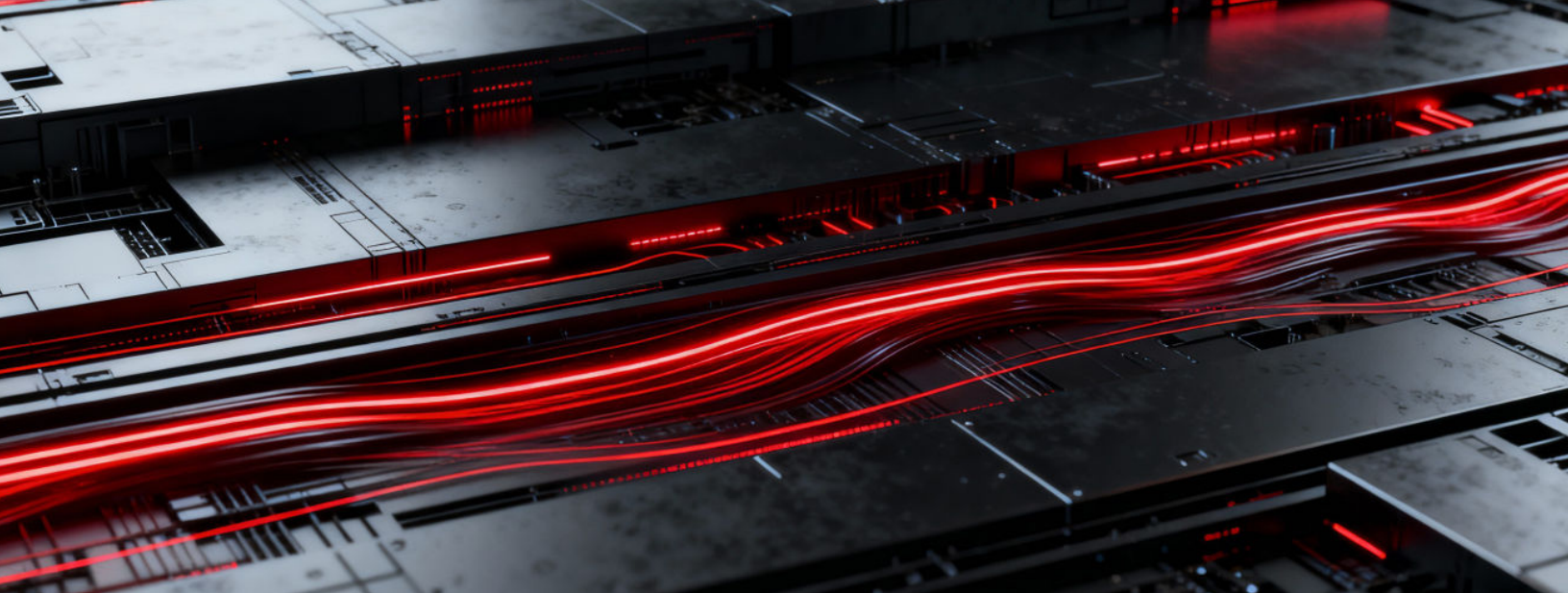
The Economics of Repatriation and Market Drivers

The market for private cloud is growing, driven not only by technical needs but also by significant economic and strategic factors. A key trend is cloud repatriation – the movement of workloads from public cloud back to on-premises or private environments that may be hosted or managed by third-party service providers.

Two primary drivers are fueling this trend:

- 1 Regulatory and Geopolitical Pressure:** As noted, evolving requirements and geopolitical uncertainty are forcing the repatriation of sensitive workloads that cannot legally reside in shared public environments.
- 2 Hyperscaler Lock-in:** Organizations are increasingly seeking alternatives to the commercial and technical lock-in associated with hyperscalers. The unpredictable costs of public cloud consumption, particularly for stable, predictable workloads, have led CIOs to re-evaluate the total cost of ownership (TCO).

Modern private cloud deployments now offer competitive economics without the sovereignty compromises inherent in hyperscale offerings. For businesses, this translates into faster deployment and adoption compared to building custom alternatives, positioning them to repatriate sensitive workloads efficiently.



The Modern Private Cloud: Speed Without Sacrifice

Contrary to the perception that private cloud equates to legacy IT, modern platforms utilize architectures that integrate private, hybrid, and public cloud capabilities. The objective is to offer enhanced security, complete data control, and jurisdictional compliance without sacrificing operational velocity.

However, the value extends beyond just speed and compliance; it directly addresses the broader strategic imperatives of sovereignty. Modern private cloud architectures provide a critical hedge against vendor lock-in. By standardizing on a platform that abstracts the underlying infrastructure, organizations avoid the deep lock-in associated with proprietary hyperscale APIs. This decoupling ensures operational independence, granting enterprises the freedom to move workloads between providers or back on-premises without facing prohibitive refactoring costs or technical barriers.

Furthermore, this model actively fosters a local ecosystem. Unlike the hyperscale model, which often centralizes economic value with a single global provider, modern private cloud platforms are frequently deployed and managed by a network of local partners. This approach ensures a positive contribution to the local economy by developing regional skills and maintaining a robust industrial base. It allows organizations to leverage local security standards and support structures, ensuring that their infrastructure strategy strengthens, rather than hollows out, national digital capabilities.

Unlocking Business Outcomes Through a Unified Operating Model

Broadcom's VMware Cloud Foundation (VCF) is designed to support a unified cloud operating model that simplifies IT infrastructure. By consolidating complexity across fragmented environments, it provides a single platform for managing private, hybrid, and cloud workloads. This unified approach breaks down organizational silos by aligning IT operations with business units through standardized infrastructure, application management, and license portability, accelerating time-to-value for cloud-native and AI applications.

This operating model extends beyond efficiency to deliver strategic resilience. By abstracting the infrastructure layer, VCF protects organizations from vendor software and hardware lock-in, granting them flexibility to diversify their underlying

physical infrastructure. It further reduces technological dependence by supporting fully air-gapped environments, enabling critical systems to operate without reliance on external connectivity.

Unlike rigid public cloud shared-responsibility models, this approach empowers organizations to deploy based on their own specific security architectures and risk appetites. When combined with support from an ecosystem of local providers, these features significantly reduce overall supply chain risk. This alignment of technological independence and local support directly addresses the operational resilience mandates of regulations such as DORA and NIS2, ensuring that compliance is an inherent outcome of the infrastructure strategy.

Market Opportunity and the Partner Ecosystem

This shift is supported by various deployment paths. Cloud service providers are building VCF-based local sovereign cloud offerings specifically for customers, while system integrators and resellers are deploying private cloud solutions for organizations moving workloads back on-premises. Professional services are also playing a role, focusing on workload migration and operational transition. Broadcom's strategy leverages partnership-based deployment models to facilitate these transitions, utilizing a European ecosystem that contrasts with the consolidated models of US-centric hyperscalers.

The Ecosystem Approach to Sovereign Infrastructure

The positioning of VCF against hyperscalers extends beyond technical specifications to address the broader definitions of digital sovereignty. This comparison focuses on three primary areas: strategic control, operational agility, and economic partnership.



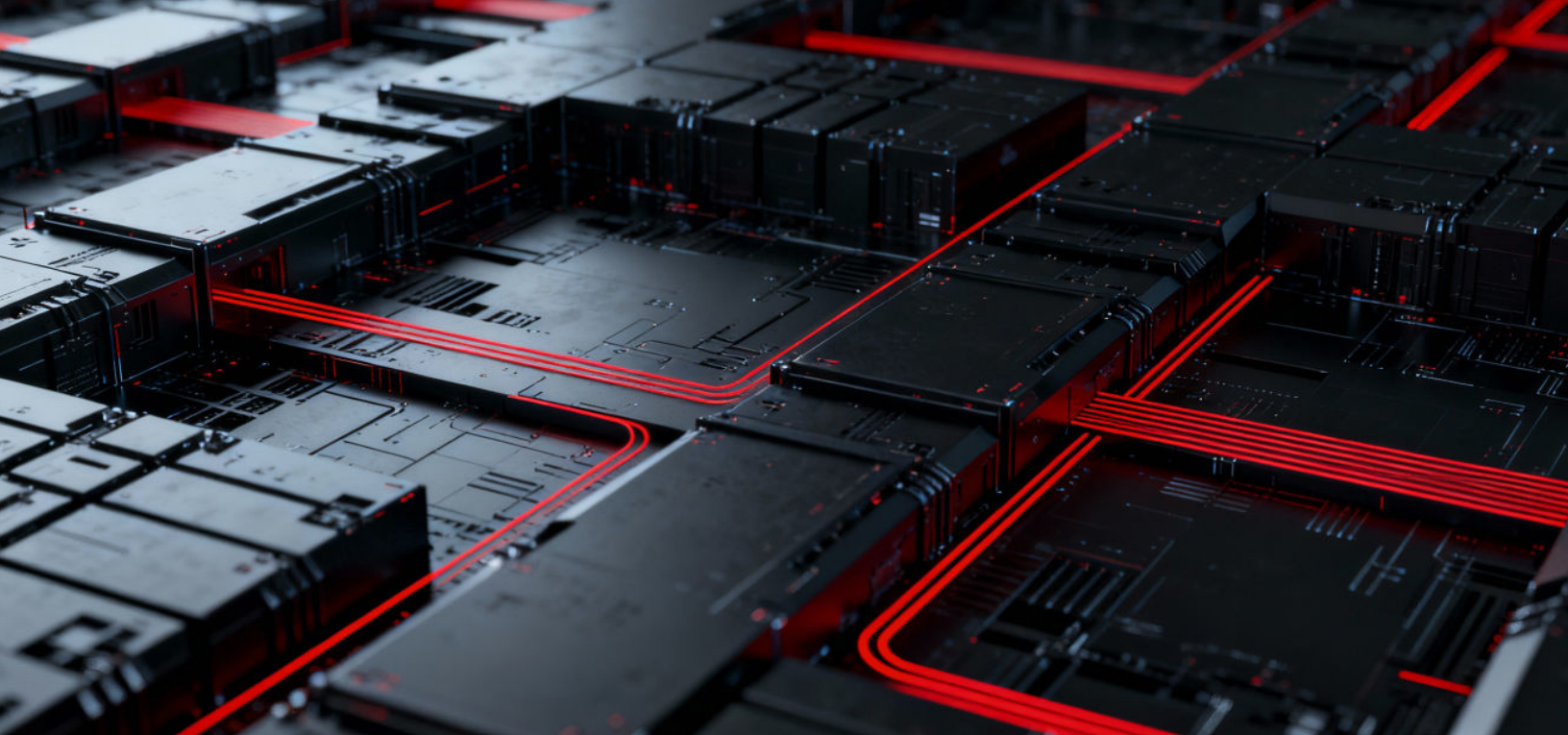
Strategic Control and Autonomy: Unlike hyperscalers' global scale, VCF prioritizes national control and 'autonomy of action'. Keeping critical workloads on-premises and within national borders ensures immunity from extraterritorial laws and reduces reliance on foreign technology. Platform ownership mitigates risks from export controls, tariffs, or remote 'kill switches', maintaining resilience against geopolitical shifts.



Agility and Freedom from Lock-in: VCF offers public cloud speed with reduced vendor concentration. Unlike hyperscalers' deep API integrations that create high exit barriers, modern private cloud prioritizes portability. This avoids vendor lock-in, enabling seamless workload movement and independent tool development, ensuring agility without sacrificing long-term flexibility.



Partnership and Economic Contribution: Broadcom's partner-led strategy contrasts with hyperscalers' direct consolidation, supporting the economic pillar of sovereignty. By fostering a local ecosystem, it supports skills and a robust national industrial base, aligning infrastructure strategy with national economic interests rather than centralizing revenue globally.



Conclusion: The Strategic Shift to Sovereign Resilience

The infrastructure market has reached a critical inflection point. The era of 'cloud first' – where the public cloud was the default destination for all workloads – is yielding to a more nuanced strategy. Organizations are no longer willing to accept the binary trade-off between the agility of the cloud and the sovereignty of their data.

This shift is driven by a realization that true resilience requires more than just uptime; it requires greater control over data and applications and jurisdictional and geopolitical certainty. As enterprises integrate AI and generative models into their core operations, the cost of losing control over data or the broader supply chain has become a compliance and an existential risk. This infrastructure strategy acknowledges that for sensitive, mission-critical, and AI-driven workloads, the operational risks of the public cloud now outweigh its convenience.

Furthermore, this transition validates the importance of a federated, partner-led ecosystem. Sovereignty is inherently local; it cannot be fully delivered by a centralized, global monolith. It requires a network of national and regional providers who understand the specific regulatory fabric of their markets and help develop the local industrial base.

In this context, technology platforms such as VCF serve not as the destination, but as the essential common language that binds this ecosystem together. By providing a consistent technical standard, they enable European enterprises to build modern, sovereign cloud environments that deliver public cloud velocity without compromising national or corporate independence.

Important Information About This Report

AUTHORS

Nick Patience

Vice President & Practice Lead,
AI Platforms | Futurum Research

PUBLISHER

Futurum Research

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

This document, including any supporting materials, is owned by The Futurum Group. This publication may not be reproduced, distributed, or shared in any form without the prior written permission of The Futurum Group

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.



ABOUT BROADCOM

[Broadcom Inc.](#) is a global technology leader known for its high-performance semiconductor products and enterprise infrastructure software, serving critical markets in cloud, networking, storage, and security. The company's acquisition and ongoing development of VMware Cloud Foundation has positioned it as a major force in the modern private cloud, enabling enterprises to run, manage, and secure workloads at scale with flexibility and efficiency. Broadcom has been actively integrating AI-native capabilities into its private cloud platform—such as built-in AI services for model management, GPU support, and optimized infrastructure—so organizations can deploy and govern AI workloads on their own terms. In both hardware and software, Broadcom's innovations aim to accelerate AI adoption while maintaining control, privacy, and cost-effectiveness for businesses worldwide.



ABOUT THE FUTURUM GROUP

[The Futurum Group](#) is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.



CONTACT INFORMATION: The Futurum Group LLC | [futurumgroup.com](https://www.futurumgroup.com) | (833) 722-5337