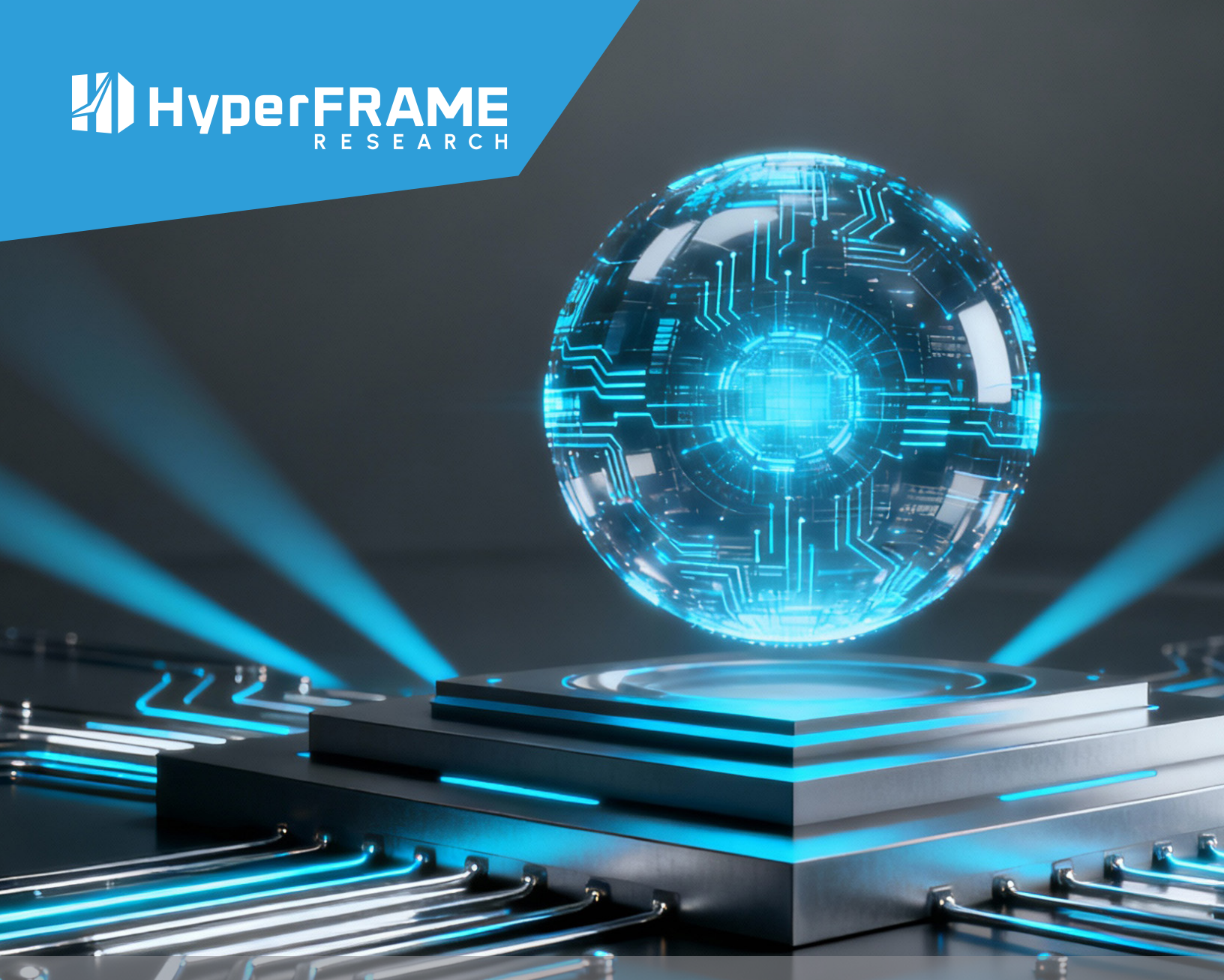




WHITE PAPER

Future-Proofing IT Infrastructure: A Decision Framework for Enterprise Architects

Aligning Technology Choices with Business Goals for Enterprise Success

Authors:

Stephanie Walter

Practice Leader - AI Stack

Steven Dickens

CEO and Principal Analyst

OCTOBER 2025



Executive Summary

The enterprise infrastructure landscape is evolving rapidly as modern technologies, including the demands of AI, ripple through global enterprises and put pressure on existing IT environments. HyperFRAME Research has designed this paper for IT leaders and enterprise architects tasked with guiding infrastructure evolution. This paper is particularly relevant for larger, more complex organizations. While complexity is not necessarily a function of organizational size, the two often go hand in hand. For the purposes of this paper, a large, complex organization would likely have several thousand employees, hybrid infrastructure footprints, and deeply virtualized install bases built over years or even decades. For such enterprises, the challenge is beyond just keeping pace. These types of organizations need to make smart decisions about how to future-proof their infrastructure without abandoning what already works.

“To be a leader in our industry, we have to be constantly innovating and focusing on digital transformation. And part of that process is to be able to arm our sales team with the tools they need, collecting data, and feeding that into AI and machine learning models in order to determine what the best course of action is to take... VMware Cloud Foundation lays that groundwork.”

Rodney Lee Barnhardt
Server Administrator, Charlotte Pipe and Foundry

The focus of this paper is not simply on comparing infrastructure options. It's about helping organizations understand how to use their existing investments, skill sets, and processes while incorporating modern technologies like containers, microservices, and hybrid cloud platforms. Organizations need to navigate trade-offs between virtualization and containerization, using a practical decision framework tailored to highly virtualized organizations with thousands of employees.

VMware Cloud Foundation is a unified private cloud platform that combines the scale and agility of public cloud with the security and performance of private cloud, delivering increased productivity and lower TCO. VMware Cloud Foundation accelerates innovation with a self-service IaaS platform and Kubernetes runtime. It delivers a modern cloud interface to run apps built on VMs, containers, and AI workloads with security and resiliency.

VMware Cloud Foundation seamlessly combines the benefits of VM operations with modern container orchestration through a single declarative API that streamlines operations, reduces complexity, and speeds up application delivery. This simple approach eliminates silos as well as the need for separate infrastructure for VMs and containers.



This paper offers a structured rubric to align technology choices with business goals, workload needs, and non-functional requirements (NFRs). Virtualization offers maturity, stability, operational simplicity, control, and efficiency, delivering lower Total Cost of Ownership (TCO). Containers provide agility and portability while also providing a path to cloud-native transformation and microservices adoption. Crucially, these options are not mutually exclusive. Further complicating decision-making are hybrid cloud complexity, vendor shifts, and emerging technologies like AI and edge computing. This paper addresses this complexity by focusing on:

- Establishing a clear baseline of current infrastructure
- Evaluating team skills, processes, and tooling
- Defining NFRs and ranking their importance
- Mapping platforms to workload patterns
- Analyzing operational and financial trade-offs
- Aligning infrastructure with long-term cloud and application strategy

“With VMware Cloud Foundation, we’ve built a secure, private cloud environment that allows us to quickly and efficiently implement AI technologies.”

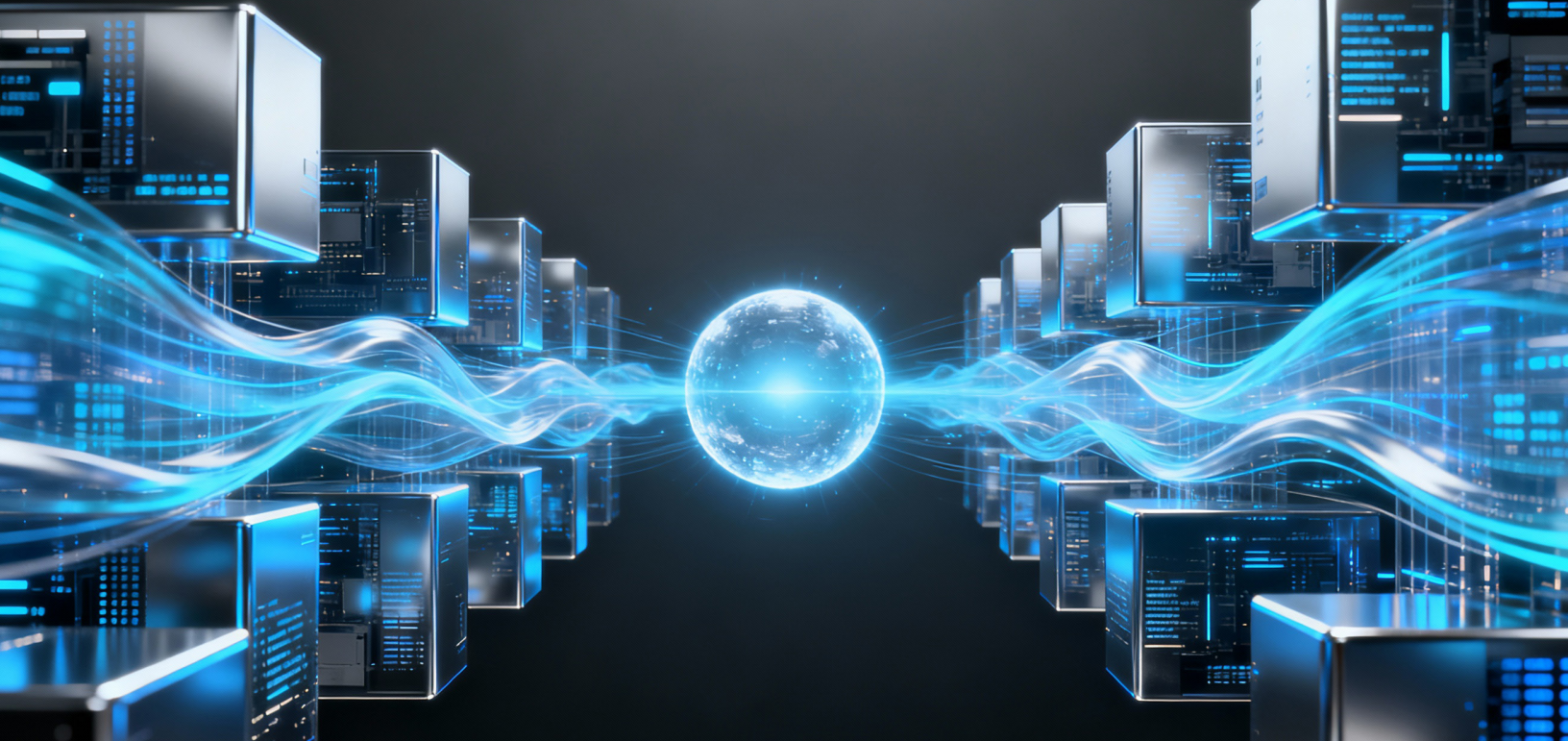
Mark Fournier
CIO and CTO, United States Senate Federal Credit Union

We also explore the role of platforms as enablers of hybrid cloud and container orchestration. Organizations increasingly want to simplify and streamline infrastructure operations by adopting platforms that can support both traditional VM-based applications and modern container-based workloads. Put simply, infrastructure evolution is a prerequisite for digital competitiveness, operational resilience, and regulatory compliance. This paper guides decision-makers through that evolution, balancing agility with stability, and innovation with risk control. The intent is to arm enterprise architects with a pragmatic framework for continuous modernization.

Who is this Paper For?

This white paper is intended for infrastructure decision-makers, enterprise architects, and IT strategists at large enterprises, specifically organizations that

- Have several thousand employees
- Maintain a hybrid infrastructure
- Operate a deeply virtualized environment as their baseline



Introduction: The Need for Infrastructure Evolution

Banks, telcos, retailers, government agencies, and other large enterprises face constant pressure to deliver digital services at speed and scale. Digital transformation, data proliferation, and AI workloads are stretching infrastructure to its breaking point. Customers expect seamless digital experiences. Regulators demand tighter compliance. Business leaders want faster innovation at a lower cost. The demands on the underlying IT infrastructure are constant and ever-changing.

Yet legacy systems remain, and virtualized environments continue to serve as the foundation for many enterprise IT operations. Many enterprises depend on established virtual machine (VM) estates that were initially deployed as long as 20 years ago because they continue to prove their value in stability, security, and resource efficiency. While they remain well-suited for many workloads, including next-generation workloads such as GenAI and big data analytics, these longstanding VM environments face evolving demands around elasticity, automation, and integration with modern development practices. Meanwhile, containerization, edge computing, and AI workloads require new infrastructure paradigms.

Hybrid cloud adds another layer of complexity. On-premises systems coexist with private and public clouds. Workloads span multiple environments. Network, identity, and data integration become harder to manage. Infrastructure

teams must also navigate shifting vendor roadmaps and commercial models. Acquisitions and divestitures also reshape the technology landscape.

This white paper is written for enterprise architects tasked with evolving infrastructure in this dynamic environment. We provide a step-by-step decision framework grounded in operational reality. The framework accounts for technical constraints, organizational dynamics, and business priorities. While this white paper is written with enterprise architects in mind, the guidance is equally relevant for CIOs, infrastructure leaders, and other IT executives shaping future infrastructure strategy and evaluating effective modernization approaches.

“VMware Cloud Foundation is at the core of our Digital Application Platform. Using VCF we have expanded our on-prem delivery capabilities while improving operational efficiency. At IPZS we feel that we are now on the right track to continue supporting Italy’s digital transition with a modern private cloud that enables full use of our competences to deliver cloud-native applications.”

Paolo Bazzica
Chief Information Officer, IPZS



Step 1: Inventory the Current Infrastructure

Successful modernization begins with understanding the current infrastructure paradigm. Decisions made without a complete picture of existing infrastructure carry the risk of investing time and resources in the wrong solution. To deeply understand the environment, organizations should inventory workloads, deployment patterns, and any supporting platforms.

The three infrastructure approaches that enterprises typically rely on for workload placement are: bare metal, virtualization, and containerization. Most environments contain a mix. Each approach represents a different architectural model, and each has distinct performance, scalability, and operational characteristics.

- **Bare metal:** This is still widely used for high-performance computing. Bare metal offers dedicated resources with minimal overhead. Bare metal is typically used for tasks where low latency is vital. High-frequency trading, performance-hungry transactional databases, or carrier-grade NAT in telco networks are good examples of when bare metal may be preferred.
- **Virtualization:** VMs continue to be the backbone of enterprise IT. They support general-purpose workloads and provide benefits such as logical isolation, resource pooling, and snapshotting. VMs are primarily managed via platforms like VMware, although alternatives exist that are less widely adopted.
- **Containerization:** Containers are orchestrated by Kubernetes and are the preferred choice for cloud-native applications and DevOps-driven teams. Containers offer lightweight deployment, rapid scaling, and portability across environments.

“Right now, we are moving more and more workloads on Kubernetes environments... it’s like a revolution where we migrate legacy solutions to a modern platform... We selected VMware Cloud Foundation because we were looking for a project with high automation. We love automation. We really love automation.”

Jean-Michel Blanc
Group Head of System Engineering, Loomis

While all three play important roles, this paper focuses primarily on virtualization and containerization because they support the vast majority of enterprise workloads. Bare metal is essential for specific high-performance use cases, but is typically used in more specialized scenarios.

Enterprises should consider these key questions when analyzing current infrastructure:

- How many workloads run on VMs, containers, and/or bare metal?
- Which applications require specific hardware or hypervisors?
- Where is underutilization occurring?
- Are workloads being co-located with similar performance and security profiles?
- What are the wider network, storage connectivity, and management issues that are adjacent to the compute requirements?
- What are the recovery point and time objectives (RPO/RTO)?

Map these findings to business functions to reveal alignment gaps. For instance, a latency-sensitive analytics engine might be deployed on bare metal without sufficient failover or automation capabilities, leading to operational fragility. Additionally, development teams may lack access to container-based environments, slowing innovation.

Several trends are shaping how enterprises manage their infrastructure portfolios. One is the growing practice of running containers within virtual machines. Doing so has the advantage of operational consistency while allowing the use of existing VM management tools. This approach effectively leverages the mature security and isolation capabilities of hypervisors and provides an additional boundary around containerized applications. This is particularly appealing for workloads with stringent compliance or multitenancy requirements. It also enables organizations to introduce container technology incrementally and use established virtualization practices. This layered strategy offers a pragmatic balance between embracing cloud-native patterns and maintaining robust, well-understood operational controls.

Edge computing is another trend and is seen particularly in sectors like telco and retail. Edge computing needs localized processing and is employed in use cases like fraud detection and real-time analytics. Additionally, the trend of widespread adoption of CI/CD pipelines influences platform decisions. CI/CD pipelines accelerate deployment cycles and require infrastructure that supports automation and integration. Enterprise architects must take applicable trends into consideration as they plan any infrastructure modernization.

Understanding your infrastructure footprint is not a one-time task. It should be an ongoing analysis that enables organizations to leverage existing investments while bringing modernization opportunities to light. Examining emerging trends and asking the right foundational questions can help enterprise architects uncover inefficiencies and prioritize critical modernization areas. That way, their infrastructure choices are aligned with the operational and strategic goals of the business.

“The more we learned about VMware Cloud Foundation, the more we saw it could address all our problems. It was the desired single pane-of-glass, and a route to new levels of automation... VMware Cloud Foundation enables us to do more with less. We have the same team, but we’re able to cover so much more.”

Michael Miller

Technical Architect, Mary Washington Healthcare

Step 2: Evaluate Organizational Structure and Team Skillsets

Technology can only succeed if the organization is ready for it. The second step is to evaluate people, processes, and tools. For people, start with skills mapping. Identify expertise across core infrastructure domains such as virtualization platforms, Kubernetes-based container orchestration, hyperconverged infrastructure, and infrastructure-as-code automation frameworks. Determine any knowledge gaps and then figure out the cost and time to close them. This is a step that many organizations overlook, but doing so has huge ramifications.

Retraining and skills gaps are underappreciated barriers to infrastructure transformation. Moving to new tools doesn't stop at installing new software. An entire operating model must be redefined. For example, a team proficient in virtualization faces a steep learning curve when shifting to container orchestration or adopting infrastructure-as-code. Familiar methods for provisioning, monitoring, and troubleshooting no longer apply.



“With VMware Cloud Foundation, we can offer our customers a private cloud operating model from our own data center. VCF offers a significantly more flexible and easier-to-manage IT infrastructure with its automation, advanced security features, dynamic networking capabilities, and comprehensive cloud management.”

Michael Heier
Head of Managed Workplace, Ratiodata

Next, take a look at workflows. Modern infrastructure requires modern workflows. Are teams following GitOps principles? Is CI/CD in place? Are incident response and change management processes aligned with development cycles? Finally, investigate tooling. Inventory current tools for monitoring, automation, configuration management, and orchestration. Assess whether these tools integrate with any new platforms being considered.

Evaluating the organization structure and the team’s skills often reveals notable risks. One common issue is operational

silos between infrastructure and development teams that can hinder collaboration and modernization. Another challenge arises when organizations adopt new technologies without ensuring that the team is skilled in these technologies. For example, a team that decides to adopt Kubernetes without Kubernetes skills is going to be in for a rough and expensive ride. Additionally, supporting multiple infrastructure platforms without unified tooling increases complexity and overhead. This stretches both human and financial resources.

Enterprises often underestimate the effort required to build new competencies. Traditional I&O (infrastructure and operations) organizations often lack the operations skills required to manage single-platform solutions based on Kubernetes for containers and KubeVirt for virtualization. They must be ready to invest in significant training and hiring to gain the deep Kubernetes skills required to be successful with such platforms. Training alone is not enough. Embedding new practices and technology requires sustained investment, process reengineering, and leadership support.





Step 3: Determine Non-Functional Requirements

Non-functional requirements (NFRs) are incredibly important, yet they are often overlooked when making infrastructure decisions. Functional requirements define and determine what a system does, like processing payments or insurance claims. However, NFRs shape how it performs under pressure, scales with demand, and survives in the face of failure. Enterprise architects must evaluate any infrastructure approach with NFRs in mind.

System Performance - Performance is one of the most visible and critical NFRs. Low latency and high throughput are mandatory in environments such as transaction processing systems in financial services or real-time analytics in retail. Infrastructure must be architected and tuned to meet performance demands consistently, no matter what the performance goals are. System performance directly impacts customer experience and transaction reliability. This is especially true in verticals where milliseconds and transaction integrity matter. Failure to meet performance expectations or lost transactions can lead to lost revenue, user dissatisfaction, and operational bottlenecks.

Ability to scale - Scalability is also important, especially in the current era of AI-driven applications. Infrastructure must be able to expand or contract without disrupting services, whether growth is linear, seasonal, or spiky. Infrastructure that can scale both vertically and horizontally offers the flexibility required by large enterprises. Without scalable infrastructure, organizations risk downtime or even performance during peak usage. This can undermine trust and stall digital growth.

Security posture - Security and compliance must be considered in any enterprise system. Infrastructure must be able to support data isolation, encryption, access controls, and auditability to comply with mandates like DORA, GDPR, HIPAA, and PCI-DSS. Taking security into account in infrastructure decisions should be done by default. Modern platforms must deliver security by design, not as an afterthought. Robust security reduces the risk of breaches and fines, as well as builds customer trust and ensures business continuity.

Total Cost of Operation - TCO remains a constraint in both capital expenditures and operational overhead. But it's not just the cost of servers and software. It's also the labor cost of administration, patching, scaling, and securing these environments. TCO must consider long-term licensing models, support contracts, and skills investment. A thorough

understanding of TCO helps prevent budget overruns and supports long-term financial planning. It also ensures that infrastructure decisions deliver sustained value.

RAS - Reliability, Availability, and Serviceability; while this acronym dates back to the mainframe days, its mantra still remains true today. Manageability is about keeping control. Systems must be observable, automatable, and recoverable. When infrastructure sprawls across on-premises data centers, public clouds, and edge locations, the ability to govern it all from a unified console becomes non-negotiable. These attributes make sure that systems are resilient and support high service levels. They also reduce the risk of prolonged outages and operational surprises.

“VMware Cloud Foundation has enabled us to execute on our private cloud strategy by breaking down IT silos, removing technical debt, and allowing teams to shift from focusing on keeping the lights on to higher value projects that move our business forward. By delivering an ‘everything as code’ private cloud platform, we simply do everything faster and more securely now. Security patches are easier to implement, new applications are deployed in minutes rather than months, and services are updated and rolled out to customers in a fraction of the time. These are all benefits people only thought were possible in the public cloud. We are doing these things in our modern private cloud.”

Roger Joys
Principal Technology Strategy Advisor,
Cloud & Data, GCI Communications

Backup and Recovery - RPO (Recovery Point Objective) and RTO (Recovery Time Objective) are critical metrics in IT environments, defining the maximum tolerable data loss and the maximum acceptable downtime, respectively, ensuring business continuity and minimizing the impact of disruptions. By establishing clear RPO and RTO targets, organizations can develop effective disaster recovery plans that align with their business needs and risk tolerance. Inadequate recovery planning can result in extended downtimes or data loss,

meaning severe consequences for compliance, reputation, and revenue.

Flexibility - Portability and integration also carry weight. The best infrastructure is not a silo. It works with existing tools and accommodates new ones. It supports container registries, CI/CD pipelines, and monitoring platforms. It integrates with the broader IT ecosystem. Infrastructure that supports a variety of tools and platforms accelerates innovation while allowing enterprises to adapt quickly to changing business needs or market demands.

Taken together, these NFRs allow architects to go beyond surface-level feature comparisons and assess whether a solution is truly fit for purpose in the context of their enterprise. Any modernization initiative that ignores NFRs does so at its peril.

Step 4: Compare Virtualization and Containerization Options

Now that the organizational context and infrastructure needs are defined, the next step is to assess which foundational compute model best aligns with the workload demands and objectives of the business. Virtualization and containerization each serve a purpose and coexist in most large enterprises. The key is to understand when and where each model fits best.

Virtualization - Virtual machines continue to serve as a foundation for enterprise IT environments. Hypervisors offer efficient use of computing resources while enabling strong isolation between workloads. These platforms come with integrated tools that support critical enterprise functions like monitoring, security enforcement, and disaster recovery planning. These platforms also have long-standing and tight integrations with observability and ITSM environments. Virtualization remains especially relevant for established applications that require stability, compliance, and predictable resource use, such as ERP systems and enterprise databases. While there may be minimal performance overhead compared to bare metal, the operational benefits and rich ecosystem typically outweigh the drawbacks. For most customers, the performance loss of low single-digit percentages is barely noticeable, whereas the benefits of virtualization provide a huge upside. In addition, applications that are architected to scale out generally perform better when virtualized than on bare metal because a more granular approach can be taken. Any consideration of shifting away from virtualization must also factor in the organizational cost of retraining teams and adopting new toolsets.

Containerization - Containers are optimized for cloud-native workloads and DevOps delivery models. They allow teams to build and scale microservices architectures with agility because they are lightweight, portable, and fast to deploy, especially when orchestrated via Kubernetes. That being said, containers do introduce new complexity. The shared kernel model, networking layers, and dynamic scheduling present unique security and operational challenges. They also require a steep learning curve along with new tools for orchestration, observability, and policy enforcement.

Hybrid Approach - Most enterprises adopt a blended model. Containers often run inside VMs for added isolation and compatibility with existing infrastructure. Increasingly, platforms like VMware Cloud Foundation enable organizations to run both VMs containers within a single operational environment. The one platform approach reduces complexity by consolidating tooling, management practices, and governance models. Teams can support both legacy and cloud-native workloads without fragmenting their infrastructure strategy. This layered architecture allows organizations to use the strengths of each model while balancing risk and operational complexity.

Choosing the right model is not about declaring a winner. It's about mapping workload characteristics to platform capabilities, as shown in the table below:



Virtualization

Use for compliance-heavy, stable, and general-purpose enterprise applications.



Containerization

Use for scalable, rapidly iterated, cloud-native services that benefit from automation and horizontal scaling.

By clearly evaluating the trade-offs and operational realities of each model, architects can build a compute fabric that supports today's workloads and tomorrow's transformation goals.

Step 5: Evaluate Platform Capabilities and Integration

The enterprise IT environment rarely presents as a neat, tidy picture. It's almost always a hybrid affair, a real tapestry of on-premises systems, dedicated private clouds, and services pulled from the public cloud. This kind of mixed setup certainly

brings flexibility to the table, but also introduces significant challenges to platform capabilities and integration. This step means looking beyond just the individual building blocks of virtual machines and containers to really size up the platforms that orchestrate them into some kind of coherent whole. The ultimate goal is for everything to work together smoothly.

Examining these platforms quickly demonstrates that there are different core philosophies at play. Some vendors will push for a full-stack integration. Think of this as a pre-packaged deal where compute, storage, networking, and management are all tightly interwoven. The promise here is simplicity and a degree of predictability because it's a known, validated technology stack.

"We had to completely change how we provided our IT services to the researchers. It had to be fast, easy and reliable...VMware Cloud Foundation provides everything we need: compute, storage and networking as well as load balancing and flexibility. With VCF Automation we're providing a public cloud-like user experience while maintaining security, compliance and control."

Philippe Morel
Director of IT Operations and Infrastructure, EPFL

Open source Kubernetes orchestration providers champion a more open flexibility. These platforms offer a consistent layer for running containers, no matter what lies beneath, i.e., bare metal, different virtual environments, private clouds, or the big public cloud providers. The driving idea here is giving enterprises a choice and trying to steer clear of being too dependent on one infrastructure supplier. Hyperconverged infrastructure providers offer yet another angle. They've steadily built HCI into a broader play for hybrid multicloud, complete with their own virtualization and container tools, always with an eye on making life simpler for IT operations. Digging deeper into these platforms tends to zero in on several make-or-break areas:

- 1. The Management Experience:** How easy or how convoluted is it to actually run the infrastructure day to day? Is there a unified command center with real visibility across different environments and workloads? A platform that genuinely simplifies complexity directly translates into efficient operations.

- 2. The Developer Experience:** Modern applications get built because developers can get what they need from the infrastructure. Does the platform give them self-service capabilities? Robust APIs to work with? Tooling for CI/CD already baked in? Can it handle a variety of application designs? Empowering developers speeds up innovation.
- 3. Ecosystem and Tooling Alignment:** How well does a new platform play with the existing tools? Think about the existing monitoring systems, security information and event management, identity systems, and automation scripts. Compatibility here is huge because it helps avoid creating new, isolated silos of operation.
- 4. Workload Support and Hybrid Configurations:** Can the platform adeptly handle both legacy virtualized applications and newer, container-based ones? Can it manage them together, maybe even allowing containers to run inside VMs for specific security or isolation needs? For most established businesses, being able to bridge that gap between the old and the new is absolutely essential.

Trying to run these hybrid environments is not without its headaches. HyperFRAME Research sees the following challenges pop up across many large enterprises:

- **Interoperability:** Just getting applications and data to move without friction, and ensuring management tools work consistently across VM platforms and container systems, is a persistent hurdle. True seamlessness takes a commitment to standards and some very solid APIs.
- **Security:** Applying security policies and keeping an eye on threats in a consistent way when your systems are scattered everywhere is a huge challenge. Container security, with its shared kernel model and questions about image sources, needs its own dedicated focus and specialized tools. What you want is a security posture that's reliably strong, no matter where the workload lives.
- **The Skills Gap:** Managing Kubernetes and all the cloud-native technologies that go with it requires skill sets that are often in short supply. Organizations need a plan for upskilling their current people or bringing in new talent who understands DevOps, container orchestration, and how to manage a hybrid cloud. This gap can seriously slow things down.
- **Vendor Lock-in:** Enterprises should prioritize platforms that offer flexibility across infrastructure choices, whether open source or proprietary. While participation

in open source communities, such as CNCF, and support for technologies like Kubernetes are strong indicators of openness, the broader goal is interoperability and portability. Ultimately, the focus should be on platforms designed for heterogeneous environments to maintain control, reduce switching costs, and retain the freedom to adapt infrastructure strategy as requirements and market conditions change.

- **Monitoring and Governance:** Getting a clear, comprehensive view of how applications are performing, what resources are being used, and whether you are meeting all your compliance obligations across the sprawling hybrid estate is difficult but essential. Robust frameworks are needed for monitoring, logging, and governance that can span all your different environments to stay in control and optimize effectively.

Tackling these issues isn't about finding a magic bullet; it requires a proactive plan. HyperFRAME Research recommends pushing for standardized tooling where it makes sense, looking seriously at hybrid cloud management platforms that provide unified control across different infrastructures, and generally taking a phased approach to adoption. Starting with pilot projects lets teams build up their expertise and smooth out the processes before rolling things out more broadly. Ultimately, a careful evaluation of platforms, with specific attention paid to integration, how consistent management is, and how well they support both VMs and containers, is the bedrock for dealing with the complexity of modern IT infrastructure and being genuinely ready for whatever comes next.

"Integrated Kubernetes, however, is VCF's best-kept secret, despite VMware consistently ranking in the top 3 contributors to Kubernetes over the past decade, securing a prominent place as a top-tier contributor in the ecosystem. Lack of headlines aside, VMware continues to play a pivotal role in shaping the future of Kubernetes, underlining its deep commitment to continuous innovation and leadership in container technology."

CIO.com, "Breaking down silos: A holistic approach to running Virtual Machines and Containers on the same platform at scale." Jul 21, 2025



Step 6: Analyze Total Cost of Ownership and Operational Overhead

Cost inevitably plays a major role when discussing infrastructure evolution. Yet, Total Cost of Ownership (TCO) is often viewed too narrowly, focusing on obvious items like licenses and hardware. The real story, however, frequently lies in the less visible but substantial costs of operational overhead and the sheer complexity involved in managing or, more significantly, migrating today's sophisticated platforms. A true TCO analysis digs deeper.

Operational complexity is a significant factor. This is the daily grind of upkeep: patching, tuning, compliance checks, and troubleshooting. Different platforms impose different burdens. An integrated stack might simplify some aspects but demand niche skills, while a looser collection of tools might require more integration effort. Honestly assessing your team's skills, automation maturity, and the actual time spent on maintenance versus value-add work is crucial. This operational drag heavily influences real TCO.

Migration is often positioned as a path to lower TCO. And yes, shifting virtual machines between hypervisors is, technically, largely solved since about 2008 using standard replication and automation. It's become routine. Migrating an entire

“By removing a lot of the operational burden, VMware Cloud Foundation allows us to focus on our application developers and provide new functionality to our customers and increase business value.”

Jeremy Mayfield
Senior Solutions Architect, GCI Communication Corp.

software-defined data center (SDDC), however, is another matter entirely. The VMs themselves aren't the problem. The challenge is untangling the complex web woven around them: the networking, security policies, compliance controls, and orchestration workflows. This deep integration, common in established VMware SDDC environments using vSphere, vSAN, NSX, VCF Operations, and VCF Automation, is incredibly difficult to replicate wholesale elsewhere. There's no single 'migrate SDDC' tool that captures that integrated operational reality. Platforms sometimes perceived as simpler, like HCI providers in certain contexts, often start with a less encompassing initial scope compared to such a deeply layered stack.

This reality dramatically impacts the financial equation. At enterprise scale, the projected savings from moving off a deeply embedded platform can quickly evaporate when confronted with the actual cost, risk, and effort of an SDDC level migration. The strategic calculus has changed. Migrating primarily for cost savings often no longer makes sense. The disruption and effort demand a more compelling, broader strategic driver, perhaps a fundamental gain in agility, a critical new capability, or significant risk mitigation. Cost reduction alone is rarely sufficient justification.

So, when evaluating vendor TCO claims, maintain a healthy skepticism. Their assumptions might not match the organization's reality. Rigorous internal due diligence is essential. Analyze your specific licensing, hardware cycles, operational capabilities, and realistically estimate transition costs and risks. Comparing notes with industry peers or using independent benchmarks adds valuable perspective.

In essence, TCO analysis goes far beyond list prices. Operational overhead and the true complexity of migration are critical, often underestimated factors. Strategic business goals, not just potential cost savings, must guide these significant infrastructure decisions.

“Compared to more traditional on prem setup, we saw a steep IT manual tasks reduction by up to 70% through automation while improving our business resilience.”

Paolo Bazzica
Chief Information Officer, IPZS

Step 7: Consider Future Trends and Technologies

Future-proofing an enterprise means not just planning for the known evolutions but also building in the capacity to adapt to technologies and practices that are still taking shape. It's about understanding the trajectory of change. A few significant technology waves are already making their presence felt, and their impact on infrastructure choices will only grow:

- **Edge Computing's Ascent:** This is not just a niche anymore. Edge computing is rapidly becoming mission-critical, especially in sectors like telecommunications for network functions or in banking for things like real-time fraud detection, right where transactions happen. This necessitates a shift in thinking about infrastructure. It needs to be more distributed, inherently resilient, and capable of delivering low-latency processing far from centralized data centers. An enterprise's platform choices need to account for managing and securing these far-flung deployments effectively.
- **The AI/ML Infrastructure Puzzle:** The reality is that the ideal infrastructure for AI/ML workloads is still a moving target. The demand for specialized hardware, like advanced GPUs and custom silicon, is intense. Furthermore, how data is managed, moved, and processed for complex model training and widespread inference is constantly being reevaluated. Infrastructure needs to be incredibly agile to keep pace.
- **Serverless Architectures Finding Their Place:** Serverless, or functions as a server, isn't going to consume every workload. However, it is firmly establishing itself as a potent complement to containerized and virtualized



environments. For event-driven applications, for gluing services together, or for handling unpredictable, spiky workloads, serverless offers compelling efficiency. The key is how well your chosen platform can integrate with and use serverless capabilities where they make sense, without forcing an all-or-nothing approach.

It's not just about new kinds of "boxes" or "services," however. The way enterprises manage and secure infrastructure is also in flux, and these evolving practices are just as important.

- **GitOps and IaC are Maturing:** Managing infrastructure through code (IaC) and employing Git repositories as the single source of truth (GitOps) is well beyond the early-adopter phase. These techniques aren't just about automation. They're about bringing version control, auditability, and declarative control to the entire infrastructure lifecycle. Platforms that inherently support or seamlessly integrate with these practices gain a distinct advantage.
- **Zero Trust as a Guide Principle:** With perimeters becoming increasingly irrelevant in the hybrid, multicloud world, the adoption of Zero Trust security models is gaining serious momentum. When this approach is applied to every user, device, and application, there are profound implications for network architecture, identity management, and how security is embedded within infrastructure platforms. The paradigm shifts.

Strategically, this all means recognizing that standing still is falling behind. Continuously evaluating infrastructure strategy in light of these trends is paramount for staying competitive.

It also shows the importance of architecting for flexibility. Infrastructure must be built to gracefully incorporate new technologies and adapt to evolving operational models without requiring a complete tear-down and rebuild every few years.

Step 8: Define a Phased Implementation Strategy

Translating infrastructure strategy into reality demands a structured implementation plan. Attempting a complete transformation at once carries significant risk. A phased execution methodology allows for learning, adaptation, and risk mitigation, ensuring outcomes align with strategic goals.

"With VMware Cloud Foundation, University of Bristol has built a modern private cloud that completely revolutionizes the way we operate and deliver services to our academic community. VCF enables us to run our AI jobs. It gives us the sovereignty we were seeking. And we know there's hidden benefits in the VCF platform that we're only just starting to discover."

Keith Woolley
Chief Digital and Information Officer, University of Bristol



A well-structured phased approach typically includes these three stages:

Assess and Prioritize: This initial phase needs careful analysis and stakeholder participation. Identify the enterprise's critical workloads and map them against the previously identified NFRs. Build consensus on priorities by collaborating across business units, security, compliance, and application teams. Which applications offer the most value from modernization? Which poses the greatest risk? Understanding these factors guides targeted efforts.

Pilot and Validate: Before large-scale commitment, use focused pilot projects or proofs of concepts (PoCs) to test assumptions and validate solutions for specific use cases. This might involve containerizing a server to test a Kubernetes platform or migrating a stable application to modern virtualization. Pilots provide hands-on experience, uncover integration issues, refine cost estimates, and build confidence before broader investment. It's about learning in a controlled manner.

Scale and Optimize: Successful pilots pave the way for gradual production rollouts. Start with less critical applications or business units and expand incrementally. Integrating with existing systems and processes requires careful planning. This phase also involves continuous optimization of performance, security, and cost based on real-world usage data collected from the new hybrid infrastructure.

Within this framework, technology selection can often follow pragmatic guidelines based on workload needs:

- **Virtualization**

Often the suitable default for stable, well-understood applications, especially those with significant compliance requirements.

- **Containerization**

The primary choice for cloud-native development, microservices, and applications needing rapid scaling. Requires robust orchestration (like Kubernetes).

Defining success metrics up front is crucial. Key Performance Indicators (KPIs) like deployment speed, application uptime, cost savings, or performance provide objective measures of

progress. Track these KPIs to demonstrate business value and ensure the modernization effort stays aligned with the strategy.

Lastly, successful execution depends heavily on critical organizational enablers. Invest in training teams on necessary technologies like container orchestration and hybrid cloud management. Adapt operational models, embracing DevOps principles and CI/CD pipelines, particularly for containerized environments. A methodical approach supported by informed technology choices, organizational readiness, and clear metrics offers the most reliable path to successful and sustainable infrastructure modernization. This structured approach transforms strategic intent into tangible operational improvement.

Building on the Incumbent: VMware's Role in the Evolving Enterprise

To achieve visibility and automation across a hybrid landscape with both VMs and containers, large, complex organizations often find value in unified platforms like VMware Cloud Foundation (VCF) to offer a holistic path for managing traditional and cloud-native workloads. VCF can offer a cohesive and cost-effective approach for managing traditional and cloud-native workloads when factored against the cost and risk of a wholesale migration to another platform alternative.

While the acquisition of VMware by Broadcom occurred in late 2024, the shift has prompted many enterprise architects to look beyond their current architectural choices for the first time in a long time. This period of change, however, also brings into focus the critical need for platforms that can cohesively manage both established VM estates and burgeoning containerized applications. For organizations seeking such a unified approach, VMware Cloud Foundation emerges as a contender as it integrates comprehensive Kubernetes orchestration capabilities directly. Beyond general-purpose virtual machines and Kubernetes, VCF is also engineered to support the increasingly critical demands of AI and high-performance computing (HPC) workloads. Enterprises can use its infrastructure for GPU accelerated applications, complex machine learning model training, and AI-driven analytics.

“VMware vSphere Kubernetes Service enables us to deliver a unified platform for both VM and containerized apps, while VMware Private AI allows us to securely harness AI capabilities across this infrastructure. Increased server performance and superior VM density will reduce our total number of servers, lowering power consumption and costs by an estimated 25–30%.”

Michael Heier
Head of Managed Workplace, Ratiodata

Under new stewardship, VCF continues its evolution as an integrated software-defined stack for private and hybrid clouds. While adapting to the new licensing and portfolio structure requires careful assessment, the underlying technological capability remains. For organizations deeply invested in vSphere, VCF presents a path towards a more managed, cloud-like operational model without abandoning familiar tooling and expertise.

Extending the deployment and leveraging the broader capabilities of VCF, moving beyond its use as a point solution for virtualization that supports container-based workloads as well, stands as a viable alternative to potentially disruptive and costly platform migrations. Organizations considering migrating away from VMware, a complex endeavor with significant hidden expenses, should weigh the opportunity cost. Resources consumed by untangling a deeply integrated SDDC and retraining staff could potentially be directed towards innovation if extending the existing platform aligns with strategic goals.

VCF is a significant platform that warrants objective evaluation within any comprehensive infrastructure decision framework. It may be particularly attractive when balanced against the substantial risks, costs, and operational upheaval associated with large-scale migration projects.

With VCF, VMware offers a single platform with a built-in Kubernetes runtime and a CNCF-certified Kubernetes distribution for organizations to run modern containerized applications alongside traditional VMs on the same infrastructure. VCF was designed to simplify Kubernetes deployment and management while unifying compute, storage, networking and security – which VMware says reduces total cost of ownership and operational complexity. VMware is touting VCF as a major offering following the Broadcom acquisition. CIOs and anyone involved in DevOps operations should at least give it a strong look as a platform to standardize on.”

**TheNewStack, “Has VMware Finally
Caught Up With Kubernetes?”**
April 2, 2025





Final Thoughts on Infrastructure's Path Forward

Plotting a course through the evolving maze of enterprise IT infrastructure is no small feat. The ground shifts constantly, and the sheer number of variables within any large organization can feel overwhelming. The purpose of this framework has not been to offer a single map but rather to equip you with a better compass for the journey. Bringing a measure of disciplined thought to this undeniable complexity is, in itself, a powerful advantage.

When the dust settles on any major infrastructure decision, success or failure rarely hinges on a single piece of technology. Instead, it's the work done up front that makes the difference: a truly granular grasp of what each specific workload demands, the definition of those critical non-functional requirements, and a brutally honest look at what the organization can actually absorb and manage in terms of change. These aren't just checkboxes; they are the very footings upon which durable strategies are laid.

If there are overarching truths to be gleaned, they might be these: First, the notion of a "one size fits all" infrastructure solution is a dangerous mirage. The optimal configuration, the right blend of virtualization and containers, or the most suitable platform vendor, will always be bespoke and tailored to unique business pressure and application characteristics. Second, the hybrid world, with its inherent levels of interoperability, its constantly shifting security frontiers, and its relentless cost pressures, isn't a temporary state. It's the new operational norm. Vigilance and adaptability are not optional. Thirdly, inching forward with pilot programs and phased rollouts isn't timid, it's

shrewd risk management. It's how to learn, adapt, and let new systems take root organically and ensure they actually deliver before more costly investments.

The real task for enterprise architects in large, complex organizations is to rise above the noise and hype. It's about leading with conviction, armed with a robust framework for analysis and decision, with an eye to build on what you already have today to deliver what you need tomorrow. The path of infrastructure evolution is a continuous one and is a series of informed choices rather than a single grand design. Making those choices with clarity and with relentless focus on delivering genuine, measurable value back to the business is the core of the architect's charge in this dynamic era.

"Through this containerization process, First Bank has successfully built a more agile and more resilient cloud native platform. It has enhanced the usability and flexibility of our applications and has laid a solid foundation for large-scale adoption in the future. This result is a critical step in our journey towards our core values as an enterprise—which is the vision to make our products and service processes software-defined, data driven, and AI enabled."

Dr. Pei-Wen Liu
Executive Vice President and Chief Information
Security Officer, First Bank



ABOUT HYPERFRAME RESEARCH:

HyperFRAME Research delivers in-depth research and insights across the global technology landscape, spanning everything from hyperscale public cloud to the mainframe and everything in between. We offer strategic advisory services, custom research reports, tailored consulting engagements, digital events, go to market planning, message testing, and lead generation programs.

Our industry analysts specialize in rigorous qualitative and quantitative assessments of technology solutions, business challenges, market forces, and end user demands across industry sectors. HyperFRAME Research collaborates closely with your Analyst Relations, Product, and Marketing teams to build and amplify your thought leadership, positioning your expertise to enhance brand and product recognition. Through content that engages readers, viewers, and listeners alike, we ensure your voice resonates across channels.

CONTACT HYPERFRAME RESEARCH:

Steven Dickens

CEO & Principal Analyst | HyperFRAME Research

Email Address:

steven.dickens@hyperframeresearch.com

Telephone Number:

+1 845 505 1678

X: [@StevenDickens3](#)

LinkedIn: [Steven Dickens](#)

BlueSky: [Steven Dickens](#)

CONTRIBUTORS

Steven Dickens

CEO & Principal Analyst

Stephanie Walter

Practice Leader - AI Stack

INQUIRIES

Contact us if you would like to discuss this report and HyperFRAME Research 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 "HyperFRAME Research." Non-press and non-analysts must receive prior written permission by HyperFRAME Research for any citations.

LICENSING

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

DISCLOSURES

HyperFRAME Research 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.

