PLATFORM9

Executive Decision Guide

Critical considerations for your Virtualization alternatives

- Top ten questions to consider
- Self-assessment: Determine your readiness to migrate
- Understand the risks and requirements
- Private cloud vision: Beyond virtualization replacement

Table of Contents

Introduction

The virtualization world is at a crossroads. Broadcom‘s acquisition of VMware has sent ripples through the industry, leaving enterprises questioning their dependence on VMware—especially with the massive price hikes they are facing. If you‘re an IT leader, you‘re likely weighing your options, not just to cut costs but to future-proof your infrastructure.

But here‘s the catch: migrating from a platform as ingrained as VMware isn‘t a walk in the park. It‘s a complex journey filled with technical challenges, business considerations, and strategic decisions that could make or break your IT operations.

This guide is your compass. We‘ll dissect the critical questions you need to ask, explore viable alternatives, and help you assess your organization‘s readiness to make the leap. Let‘s navigate this transition together, ensuring your virtualization strategy aligns seamlessly with your business goals.

10 critical questions to consider

Before you chart your migration path, tackle these essential questions to ensure a smooth transition.

1. What are the total costs, including hidden costs?

Look beyond licensing fees

While licensing is a significant expense, hidden costs can stealthily inflate your budget. Selecting a platform with user-friendly management tools and resource controls helps mitigate unforeseen expenses. Ensure your target environment minimizes additional training and provides cost-management features to keep your budget on track.

Consider:

- **Training costs:** New platforms may require your IT staff to learn new skills. Factor in training programs and potential certification expenses.
- **Process changes:** Operational shifts might necessitate changes in workflows, documentation, and standard operating procedures.
- **Hardware compatibility:** Assess whether your current hardware supports the new platform or if upgrades are necessary.
- **Downtime costs:** Plan for potential downtime during migration and how it might affect productivity and revenue.
- **Operational systems and tooling:** Day 2+ operations require, at minimum, monitoring and logging and ideally proactive remediation and automation. Assess what you need to monitor and how your teams or your systems will respond to triggers.

Creating a comprehensive cost analysis now can save financial headaches later. Especially if you intend to scale beyond just VM-based applications towards private cloud agility, scalability, and ease-of-use.

2. How will migration impact business continuity and DR operations?

Safeguard your operations

Business continuity is non-negotiable. Depending on your DR strategy, you may need to choose a platform that supports live migration and/or integrates with your existing DR solutions so you can maintain your desired uptime and data recovery objectives after the transition. Ensure your target environment has the required capabilities to minimize risks.

Evaluate:

- **Disaster recovery tools:** Identify DR products that are compatible with both your current and target platforms. Solutions like Zerto or Veeam offer multi-platform support, but verify their specific coverage in your target environment.
- **VMware-specific solutions:** If you're using VMware Site Recovery Manager (SRM), you'll need to find alternatives or plan for significant adjustments.
- **Replication and failover:** Ensure that your new platform supports your required replication methods and failover processes without compromising Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs).

Preparation here is key to maintaining uptime and data integrity during and after the migration. Ask your vendor how they will help handle migration of virtual machines, what their backup and disaster recovery features are, and what the effects on RTOs and RPOs will be during and after the transition.

3. What level of expertise and resources are needed?

Assess your team's readiness

Your IT staff are the linchpin of a successful migration. Assessing your team's readiness helps in selecting a platform that aligns with their skill set. Platforms offering integration with existing tools and providing robust support can reduce the learning curve. Ensure your target environment is user-friendly and well-supported to leverage your current resources effectively.

Consider:

- **Skill gaps:** Identify areas where your team lacks experience with the new platform.
- **Training programs:** Develop a timeline and budget for upskilling your staff.
- **External expertise:** Determine if bringing in consultants or partnering with vendors is necessary to fill knowledge gaps.

- **Resource allocation:** Ensure you have enough personnel to manage the migration without neglecting day-to-day operations.

Investing in your team's capabilities now sets the stage for long-term success. Related to this, make sure your platform vendor will empower your team with comprehensive support resources for migration and ongoing operations. Look for a platform that can provide proactive support and operational tooling with built-in monitoring, alerting, and troubleshooting capabilities.

4. What are the integration challenges with existing tools and processes?

Ensure seamless operations post-migration

Integration issues can cause significant delays and disruptions. Selecting a platform that supports your current networking and automation tools minimizes these challenges. Ensure your target environment offers compatibility with your existing systems to facilitate a smooth transition.

Key areas to scrutinize:

- **Networking configurations:** Network virtualization differs across platforms. Evaluate how your current virtual switches, VLANs, and network policies will translate.
- **Storage compatibility:** Examine whether your storage solutions (SAN, NAS, SDS) are supported by the new platform. Incompatibility could require significant investment in new storage technologies.
- **Customized scripts and automation:** Your existing scripts and automation tools may not be compatible. Plan for rewriting or adapting them.
- **Third-party integrations:** Tools for monitoring, backup, and security might need reconfiguration or replacement. Engage with vendors to understand compatibility and support.
- **Partner support:** Collaborate with partners experienced in both VMware and your target platform to navigate these complexities.

Addressing these challenges upfront minimizes operational disruptions. Even in cases of complex networking setups (e.g., using VMware's networking features), alternative platforms should offer software-defined networking (SDN) and virtual firewall policies compatible with your existing network infrastructure.

5. What are the security and compliance implications?

Protect your enterprise at every stage

Security and compliance are non-negotiable. Choosing a platform with built-in security features and compliance support ensures you meet industry standards. Verify that your target environment can uphold your security policies and regulatory obligations.

Consider:

- **Pre-migration vulnerabilities:** Identify any security gaps that could be exploited during the transition period.
- **Compliance requirements:** Ensure the new platform meets industry regulations like GDPR, HIPAA, or PCI DSS.
- **Security features:** Evaluate built-in security features of the new platform, such as encryption, access controls, and auditing capabilities
- **Integration with security tools:** Check compatibility with your existing security solutions like firewalls, intrusion detection systems, and SIEM tools.
- **Staff training:** Educate your team on new security protocols associated with the platform.

A secure migration protects your data and maintains customer trust. Make sure that a potential solution has the necessary identity management, federation, access controls, and audit capabilities to meet regulatory requirements.

6. How robust are the data protection and backup capabilities?

Don‘t leave data protection to chance

Data loss isn‘t an option. Ensure that your new platform offers robust backup and recovery features to protect your information assets. Confirm that your target environment can integrate with your existing storage solutions and provides reliable data protection mechanisms.

Investigate:

- **Backup solution compatibility:** Verify that your backup software supports the new platform.
- **Storage solutions:** Ensure your storage platforms are compatible. Incompatibility might necessitate data migration to new storage systems.

- **Historical data migration:** Plan how to transfer existing backup archives and workload images without data loss.
- **Backup windows and schedules:** Adjust backup strategies to align with the new platform‘s capabilities and limitations.

Protecting data during migration safeguards business operations and compliance. Will your new platform need special drivers and integrations? Ask your vendor if those drivers are available, and are being maintained. Data protection and data migration requires a full understanding of your business and technical requirements by your vendor.

7. What is the scalability of the new platform?

Future-proof your infrastructure

Your organization will evolve—your platform should too. Scalability ensures your platform can grow with your business. Selecting a solution that offers flexible resource allocation and high availability features supports future expansion. Make sure your target environment can scale efficiently to meet your evolving requirements.

Evaluate:

- **Vertical and horizontal scaling:** Determine how easily you can add resources (CPU, memory, storage) and nodes.
- **Operational models:** Understand how the new platform‘s architecture affects scalability. For instance, hyper-converged infrastructures scale differently than converged or traditional designs.
- **Cost implications:** Analyze how scaling up or down affects licensing and operational costs.
- **Private cloud potential:** Consider platforms that offer private cloud capabilities, enabling on-demand scaling similar to public clouds but within your control.

Choosing a scalable platform ensures long-term adaptability and cost efficiency. Modern hosting platforms should also support virtual machine High Availability (HA) and GPU to be prepared for AI and ML workloads.

8. What is the vendor's roadmap and long-term viability?

Choose a partner, not just a product

A vendor's future impacts yours. Choosing a platform with a solid roadmap and commitment to innovation ensures continued support and relevance. Verify that your target environment's provider is stable and forward-thinking.

Research:

- **Technical roadmap:** Does the vendor plan to develop features that align with your strategic goals, such as containerization, AI integration, or edge computing support?
- **Market experience:** Evaluate the vendor's track record in delivering reliable solutions and supporting enterprises during transitions.
- **Support services:** Assess the quality and availability of customer support, including response times and expertise levels.
- **Community and ecosystem:** A strong user community can be a valuable resource. Check forums, user groups, and third-party integrations.
- **Financial stability:** Ensure the vendor is financially sound to avoid disruptions due to company instability.

A vendor aligned with your vision becomes a strategic ally. Aim to find a platform from a provider with a strong market presence and a clear roadmap focusing on modernization needs like containerization and self-service API-driven automation. Ensure your vendor has a commitment to ongoing innovation to increase long-term viability and alignment with your technological goals.

9. How will licensing and support models change?

Understand the new financial landscape

Financial surprises can derail even the best-laid plans. Understanding licensing and support changes helps prevent financial surprises. Selecting a platform with clear pricing and flexible support ensures you can manage costs. Ensure your target environment offers a licensing model that aligns with your budgetary needs.

Consider:

- **License types:** Transitioning from perpetual to subscription-based licenses can affect long-term costs.

- **Support levels:** Different platforms offer varying levels of support—basic, premium, or enterprise. Match the support level to your operational needs.
- **Community support:** With shifts in technology focus (e.g., towards cloud and Kubernetes), community support for some platforms may wane. Ensure there's a robust community or vendor support to rely on.
- **Contract terms:** Scrutinize the fine print for clauses on price increases, renewal terms, and SLAs.

Being financially informed helps in negotiating favorable terms. Look for a platform with a straightforward subscription model and flexible support options. The solution should include features like quota management to control usage and costs effectively. Transparent pricing and customizable support plans are optimal for managing expenses predictably.

10. What are the risks of vendor lock-in and future flexibility?

Keep your options open

Avoiding another lock-in scenario is crucial. Flexibility safeguards your future. Choosing a platform that avoids proprietary constraints allows for easier migrations down the line. Ensure your target environment supports open standards and offers the adaptability your organization may require.

Strategies include:

- **Open standards:** Opt for platforms that adhere to open standards, facilitating easier migration in the future.
- **Data portability:** Ensure that you can export and move your data without proprietary restrictions.
- **Interoperability:** Choose solutions that play well with others, supporting a mix of technologies and platforms.
- **Code escrow:** Consider agreements where the source code is held in escrow, providing access in case the vendor goes out of business.
- **Vendor relationship:** Select partners who prioritize your long-term success over short-term gains.
- **BYO:** Choose a platform where you can bring your own compute (BYOC), storage (BYOS), and networks (BYON) providing flexibility and choice.

Evaluate workloads to migrate

Making the decision to migrate applications and workloads away from VMware is the beginning of the process. Evaluating which workloads to migrate off VMware and when is critical to minimizing risks and maximizing the value of your new platform.

Here's a step-by-step approach to help you identify and prioritize workloads for migration:

1. Categorize workloads by criticality and complexity

Critical workloads: Business-critical applications that are essential to operations, such as ERP systems, databases, and customer-facing applications. These may be the last to migrate due to their complexity and impact on the business.

- **Non-critical workloads:** Development, test, and non-production environments. These workloads are ideal for early migration because they provide a low-risk way to validate the new platform.
- **Legacy applications:** Applications with dependencies on older operating systems or specific VMware features. These may require re-architecture and should be carefully evaluated for migration feasibility.

2. Assess workload dependencies and integration needs

Map out dependencies between applications, storage, networking, and security configurations. Ensure that these dependencies are fully supported or can be adapted to the new platform without significant disruption.

3. Evaluate resource utilization and performance requirements

Analyze resource usage patterns to determine if the new platform can provide equal or better performance. Workloads with predictable resource requirements are often easier to migrate early in the process.

4. Consider data protection and compliance needs

Identify workloads that are subject to strict compliance regulations or have complex data protection requirements. These may need additional planning to ensure that security and compliance standards are maintained during and after migration.

5. Prioritize workloads based on business impact and migration complexity

Start with low-risk, high-reward migrations to build confidence and experience with the new platform. Pilot migrations with less critical applications will provide valuable insights into potential challenges that can be addressed before moving more sensitive workloads.

6. Plan phased migrations and set clear milestones

Develop a phased migration strategy with clear milestones to measure progress and identify issues early. This approach allows for controlled, incremental changes rather than large-scale disruptions.

7. Containerize some workloads

Greenfield applications can be started with the cloud-native approach and the platform should support that. By establishing the availability of this pattern early, new application development can be accelerated. No need to slow down new development while the migration continues.

8. Monitor, test, and optimize post-migration

Continuously monitor performance, test functionality, and optimize workloads post-migration to ensure they meet operational expectations. Address any gaps or performance issues promptly to maintain business continuity.

Self-assessment: Determining your readiness to migrate

Understanding your starting point is half the battle. Based on your readiness and resources, you may fall into one of three categories. Identifying where you stand helps tailor your approach for a successful transition.

1. **Actively planning/implementing migration**
    - **Characteristics:** You have a clear strategy, timelines, and resources allocated.
    - **Actions:** Conduct detailed planning, engage with vendors and partners, and begin pilot migrations.
2. **Renewing with a plan to migrate**
    - **Characteristics:** You're extending your VMware contract but have a migration roadmap.
    - **Actions:** Use this time to train staff, test new platforms, and refine your migration strategy.
3. **Renewing but needing further understanding**
    - **Characteristics:** You're renewing without a clear migration plan but are exploring options.
    - **Actions:** Gather information, attend workshops, and conduct a thorough assessment using this guide.

Tailor your approach based on where you stand to ensure an effective transition:

- **Identify your category:** Use the above characteristics to determine where your organization fits.
- **Customize your plan:** Align your migration strategy with your readiness level and resource availability.
- **Engage stakeholders:** Involve leadership, IT teams, and business units to build consensus and support.

By understanding your position on the readiness spectrum, you can craft a migration plan that aligns with your organization's capacity for change. Whether you're eager to move forward or need time to prepare, acknowledging your starting point is essential for a successful journey.

Understanding the risks and requirements

Migration comes with its share of risks:

- **Technical risks:** Compatibility issues with hardware, software, and networks can cause delays or failures.
- **Operational risks:** Inadequate planning may lead to downtime, affecting business operations.
- **Financial risks:** Unforeseen costs can strain budgets and affect other projects.
- **Time constraints:** Underestimating the time required can compress schedules, leading to rushed decisions.

Mitigation strategies:

- **Comprehensive planning:** Leave no stone unturned in your preparation.
- **Pilot programs:** Test migrations on non-critical systems to identify potential issues.
- **Expert partnerships:** Leverage vendors and consultants who specialize in migrations.
- **Clear communication:** Keep all stakeholders informed to manage expectations and facilitate collaboration.

Understanding these factors helps in crafting a realistic and effective migration plan.

The private cloud vision: Beyond virtualization replacement

As enterprises look beyond traditional virtualization, the need for a full private cloud experience becomes paramount. A true private cloud delivers more than just a replacement for vSphere; it provides a fully integrated platform that combines the best of cloud-native technologies with on-premises control, agility, self service usability, control and security.

The private cloud experience encompasses self-service capabilities, multi-tenancy, and scalability, all packaged as a single, cohesive platform. It moves beyond mere VM management, enabling organizations to deploy, manage, and scale applications seamlessly across their infrastructure.

- **Self-service and automation:** Empowers users with on-demand access to resources, reducing IT overhead and accelerating time to market.
- **Multi-tenancy and security:** Supports multiple business units, applications, and user groups within a single platform, with built-in security and isolation features to protect sensitive data.
- **Scalability and elasticity:** Designed to scale resources up or down based on demand, providing the flexibility needed to meet fluctuating business requirements without over-provisioning.
- **API automation and integration:** Seamless integration with DevOps pipelines and third-party tools, enabling automated workflows, CI/CD processes, and rapid deployment of applications.
- **Cloud-native architecture:** Leverages containers, microservices, and Kubernetes orchestration to modernize application delivery and management.
- **Software-defined networking (SDN):** Provides advanced networking capabilities, such as micro-segmentation and virtual routing, enabling secure, efficient network configurations that adapt to your needs.

This private cloud approach appeals to enterprises that need the agility of the public cloud but require the control, security, and compliance of on-premises infrastructure. It's designed for organizations that want to consolidate their IT operations into a unified, automated platform, driving efficiency and strategic value.

Unlike many virtualization alternatives, a private cloud platform is purpose-built to be part of a holistic IT transformation. It aligns with strategic business goals by enabling innovation, reducing operational complexity, and providing a robust foundation for digital transformation efforts.

What are your next steps?

The decision to migrate from VMware isn't just about reacting to market changes—it's about proactively shaping your organization's future. By addressing the critical questions outlined in this guide, you're equipping yourself to make informed decisions that align with your strategic objectives.

Conduct an internal assessment

Use the self-assessment to understand your readiness and identify gaps.

Engage stakeholders

Involve all relevant departments—IT, finance, operations—to gather diverse insights.

Select migration partners

Look for vendors and consultants with proven expertise in migrations similar to yours.

Develop a detailed migration plan

Outline timelines, resources, budgets, and risk mitigation strategies.

Invest in training

Ensure your team is prepared to manage and operate the new platform effectively.

Pilot and iterate

Start with non-critical systems to test your plan and make necessary adjustments.

Remember, the goal isn't just to migrate—it's to position your organization for agility, innovation, and sustained success in an ever-evolving technological landscape.

It’s possible, and proven in production

Thank you for reading Executive Decision Guide. We understand the challenges you are facing, and have proudly helped many organizations successfully transition away from VMware.

Our approach to enterprise private cloud has been proven at scale, with our Always-On Assurance™, while reducing costs by 30-50%.

Schedule your personalized 1-hour expert insights session with Platform9

- **Learn from real-world use cases** about migration and management.
- **Explore detailed case studies** from companies similar to yours.
- **Explore your virtualization and private cloud needs with an exclusive pilot program** to test Platform9 in your environment.

Contact us

Platform9's comprehensive private cloud platform offers built-in automation and ease of use with the flexibility to bring your own compute, storage, and network—delivering a public cloud-like experience. Founded by a team of cloud pioneers from VMware, Platform9's private cloud platform has powered over 20,000 nodes in production across some of the world's largest enterprises like Cloudera, EBSCO, Juniper Networks, and Rackspace. With a comprehensive SaaS-based control plane, Always-On Assurance™, and decades of experience, Platform9 helps businesses embrace the future of private cloud with ease and confidence.

Follow us on:

Headquarters: 84W Santa Clara St Suite 800, San Jose, CA 95113.
India office: 7th Floor, Smartworks M Agile Building, Pan Card Club Road, Baner Pune, 411045 Maharashtra, India.

Website:
https://platform9.com

Email:
info@platform9.com

Phone:
+1 650-898-7369