International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246/ ICRTCSIT-114
Eureka Vision Publication | ICRTCSIT'25-Conference Proceeding

Original Article

Holistic virtualization strategy for balancing risks and costs - Executive and practitioner combined approach

Anand Athavale
Independent Researcher, Decades of Industry experience in Data Management.

Abstract - *Virtualization technologies have brought various challenges over the past few years. All of IT infrastructure is being scrutinized whether it is for a large company, or, a large Managed Service Provider serving IT needs for multiple customers. While emergence of cloud is one of the reasons which is spread over multiple years, VMWare acquisition followed by licensing reset has turned out to be the biggest change driver. However, cost reduction needs to be carefully approached as security, supportability, and supply chain risks must be considered along with regulatory compliance. This article gives a framework for economic and technology buyers and practitioners to approach the buying and deployment decisions to focus on cost reduction while diversifying risk.*

Keywords - *Risk diversification, supply chain risk, total cost of ownership, attack surface*.

1. Introduction

Risk diversification at the core, addresses impact reduction of a single market event. This applies to a repeatable event, or, event of similar types. However, if the diversification is done with a single focus of cost reduction by the economic buyer, other negative consequences such as supportability reduction, increase of supply chain risks and security risk can creep in. Hence, it is important to look at both aspects, the total cost of ownership and the risk analysis. The current event still active in the market is the disruption due to VMWare licensing changes. Most of the IT buying decisions are being redone to counter the impact. These decisions are however strategic and must be considered as such with a holistic look from economical buyers with practitioners of IT and security. Besides the license costs, enterprise application supportability, security risks and supply chain risks need to be factored in, to distribute and reduce those risks while achieving intended cost containment. Besides the license costs, labor costs and skills are additional influencers.

1.1. The goal setting for cost containment

Typically, the IT budgets tend to be higher percentage for small companies while large companies tend to make use of economies of scale to keep IT budget percentage relatively down. On the flip side, small company IT budgets have close to zero wiggle room. The IT budget percentage can change due to technology refresh cycles or digital transformation resulting in temporary increase in the IT budget, sometimes doubling it for the transition period. However, the VMWare licensing impact broke these norms [1]. Some organizations saw increase of 5 to 12 times, for the VMWare license costs. For small companies, this increase was in the range of 25% fixed increase in IT budget, which was non-sustainable or possible even for one year in some cases. SMBs saw increase between 6 to 20%, which meant, for higher level percentages, they had to look for partial absorption of the increase, but also migration, consolidation, or reduction measures to sustain the increase in the costs. Large enterprises also saw an increase, which was either in the vicinity of 2%, where they could absorb the increase, or, toward 15%, which meant again a combination of partial absorption and partial consolidation, migration, or reduction.

2. Characteristics of alternatives

There are a quite few hypervisor technologies which could be considered as alternatives. Besides Hypervisors, there are pure and hybrid containerization options also available. However, for the purpose of this article, containerization is not being considered for two reasons. First, the migration is not always an option and it may not be straight forward. Second, the comparisons parameters may not be the same to have a holistic discussion in a concise manner.

While considering alternatives, VMWare itself remains an alternative as it fulfils important requirement when establishing supportability for some of the enterprise applications [2]. Here is a list of popular alternatives, before we start discussing various characteristics of these alternatives.

- VMWare

- Hyper-V
- Nutanix
- OpenStack & Red Hat OpenShift Virtualization
- AWS, Azure, GCP and other CSP Infrastructure as a Service options (Not strictly virtualized)
- Proxmox VE (Enterprise)
- Verge.io

There are other options beyond this list. However, this list serves good representation of the various characteristics for the cost and risk discussions.

Characteristics of the alternatives can be categorized at a high level as follows:

- Cost
- Adoptability
- Risk

Cost characteristics considered are as follows. These characteristics while serve economic buyer, the know-how resides in the practitioner's area of expertise.

2.1. License costs and meters

Hypervisors have the same purpose of virtualizing the physical resources to "carve" out more independently consumable units, referred as virtual machines, although, some hypervisors may use different terms to represent these units. However, the licensing is not tied to the same meter or measurement unit. VMWare ties the license to CPUs. Nutanix, verge.io and Hyper-V license are sold per node or server. CSPs typically attach the cost to each "runnable" unit but given the Operational Expense model, CSPs charge it per hour.

2.1.1. Labor costs (Skills required vs. skill availability)

Skills required could be bucketed in "easy to learn and use" and "special skills" categories. But, depending on the use of the virtual machines, deeper skills in the hypervisor technology along with outside virtualization technology skills like scripting etc. may be needed and must be considered. VMWare and Nutanix are in the medium level, while Red Hat virtualization and cloud may need high level of skills and attract higher salary premiums.

2.1.2. Migration costs

Migration costs are subdivided into infrastructure and licensing costs. Switching off one technology infrastructure while ending the license term while switching on alternative technology infrastructure and starting a new license term is rare. Often, there is overlap due to evaluation, licensing terms, hardware support terms and similar factors. Migration cost is the cost of running two technologies for the same purpose until the transition is over. Migration cost can also include any development, which aids testing, migration and switch over from process and code perspectives.

2.1.3. Infrastructure costs

Infrastructure costs are typically the power, cooling, networking, rack space costs. If the technology requires hardware for the core technology, or, surrounding support such as backup, recovery, test and development, analysis, monitoring, and similar functions, it also needs to be factored in this cost. No two technologies have the same infrastructure costs [3]. Hence, the infrastructure cost of alternatives needs to be carefully compared. Adoptability characteristics considered are as follows. The veto lies with the practitioner, but it has some aspects where economic buyer must weigh in.

2.2. Runnability

Very few applications are fully operating system agnostic. Further, there may be applications built by system integrators for specific customers, which have strict requirements of operating systems, and sometimes underlying hypervisor technology. Runnability is mainly tied to whether the application will run and function as expected on the given combination of operating systems and alternative hypervisor technology. It is important to note that all operating systems your applications need may not be available on the alternative virtualization technology you choose or evaluate.

2.2.1. Supportability/Certifications

Supportability and certifications are separate from runnability. Enterprise applications such as Oracle, SQL Server and other enterprise databases, SAP, Exchange, Active Directory have strict supportability matrix and certified combinations of versions, operating systems, and hypervisors. As an example, Oracle has published virtualization matrix [4] and non-Oracle cloud supportability [5]. Oracle Real Application Cluster is even more restrictive. SAP publish such certification matrix as well. Outside of which, support can be delayed, even with valid licenses or running application. Microsoft has Server Virtualization Validation Program, which certifies that third-party (non Hyper-V) hypervisors can properly run Windows Server guest operating systems with full Microsoft support. All testing for this program is done by the virtualization product vendors, with the results of the tests submitted to Microsoft for review and approval. These are example considerations for supportability, which practitioners must communicate with the economic buyers.

2.2.2. Scalability, stability, and performance

Hypervisor technologies have different limits on physical and emulating physical resources virtually along with performance variations of virtual machines running on the hypervisors. This is one of the reasons that the migration cannot be a flip of a switch. Load testing, longevity testing and performance verification is needed as inputs to the decision criterion.

2.2.3. Storage Compatibility

VMWare and Hyper-V as an example have integrations with storage array vendors to serve as the virtual machine datastore or repository from the arrays. If organizations have strategically invested in the storage array vendors to serve the virtualization storage needs, this also needs to be factored in, because the investment may go waste if the move is not tied with the array storage hardware and software refreshes. Risk characteristics considered would vary based on industry and may get subdivided into compliance and cyber risk, which sometimes overlap partially. The veto lies with the CIO and CISO, but IT practitioners must be fully made aware of these risk factors and implications of the same.

2.3. Supply chain risk

When switching to anything open source, a thorough evaluation and consideration is needed on current community support and future of that open-source technology. If the open-source technology has a variant or an upgrade with support and continuity, the risk is lower. At the same time, if there is no backing entity ensuring secure practices for the open-source code and tools, it is a risk which needs to be considered by the CISO and CIO. Depending on the alternative, it is vital to check the vendor's "Trust Center" equivalent material which is publicly available [6].

2.4. Single point of failure

IT practitioners and CIO always consider and build for hardware failures. However, they may not necessarily plan for technology provider failure or shutdown. Newer regulations in EU like DORA (Digital Operational Resiliency Act) which applies to Finance and Insurance sectors calls out "ICT Concentration risk" [7] where relying on a single technology provider or technology itself is considered non-compliance. Hence, when choosing the alternative, there needs to be carefully drafted "what-if" scenario for such drastic event. One of the recent providers claims to provide backup and recovery along with virtualization with heavy reliance on snapshots. Not planning for "what-if" the underlying storage fails can get the business from operational and compliance risk.

2.5. Monoclonal risk

This is like single point of failure in that there is a common factor involved. Monoclonal is a medical term which means it is produced by cells derived from a single cell. This translates to using same technology for all tiers of the overall operational infrastructure. If adopting new alternative than a proven and hardened one over the years, it has higher risk of wipe out due to a flaw or a security gap. Rubber is a classic example of such a risk in non-IT world. This risk gives a solid reason to consider risk diversification, discussed in the later portion, where bucketing alternative technologies are discussed.

3. Bucketing the needs to achieve cost objectives with least risk

The three categories of characteristics described previously feed into the diversification decisions aimed to "budget fit" the new virtualization strategy while keeping the risks at minimum. For ease of discussion, the high-level buckets are limited to three. Post the grouping exercise, there are some overarching considerations in terms of cost, compliance, and cyber risks to consider which complements the grouping.

3.1. Highest adoptability risk bucket

As described, certain enterprise applications such as enterprise databases like Oracle, SQL Server, SAP, Active Directory, and the likes have stringent supportability and certifications. Here, the choice is limited because, while you are looking to reduce cost, you are restricted by supportability and validations to switch to the cheapest or the most economical group of virtualization technology. This is compounded by the need to have higher level of certainty in the vendor's business, given these applications are backbone of the organization's own business operations. The representative choices here are Nutanix and may be Hyper-V depending on the "Windows Operating system" heaviness involved in the core enterprise applications. As discussed at the beginning, depending on the volume of the virtual machines involved in this group, VMWare itself may also be an option, assuming the volume is above the threshold of new licensing terms to avoid overpayment or underutilization. This is especially true for large enterprises.

3.2. Moderate adoptability risk bucket

This group primarily covers more common but less stringent supportability consideration applications available on wide variety of Linux distributions like MySQL and similar workloads. While supportability risks may be lower, the load, longevity and performance validations are still needed. Hence, if Nutanix like alternatives are not affordable to offset the costs of highest adoptability risk bucket applications, medium cost bucket alternatives like Citrix or RHOV can be considered. Besides adoptability risk, the criticality should also be considered when selecting the virtualization technology for this group. Any application which is essential for business, ideally should be in the first bucket. But, if cost is a factor, going with more familiar, more mature choice than a new arrival would be advisable.

3.3. Least adoptability risk bucket

This group should contain what is typically referred as "General purpose". This would contain application development, test/dev and similar use which is "easily replaceable". The tools and applications which get used on these virtual machines are off-the-shelf, mostly part of the operating systems and do not have a lot of pre-requisites or dependencies. General purpose web servers, file-based content repositories, proxy servers and similar component hosting virtual machines would be part of these. To balance the higher budget share of high and moderate adoptability risk, the virtual technology here could be cheaper or free and newer. The risk factor here which needs to be considered is the quantities of such virtual machines. Typically, these would be low scale at a virtual machine level but large quantities. Besides the virtualization technology, the in-guest components and tools still bear the cyber threat, especially in large quantities. These risks can be reduced by following the overarching complementary best practices.

3. Best practices to complement the grouped approach for alternate virtualization

Best practices which cut across these three groups for alternate virtualization technology adoption and selection can be sub-divided into two categories. One is compliance and cyber risk and second is the cost. For compliance risk mitigations, each group choice must have a sub-alternative within the group. As an example, if the high adoption risk bucket choice is to go with Nutanix, there should be another 1:1 matching choice, say, AWS EC2 to avoid the risks listed in regulations such as DORA. This is more than a notional choice. The viability of sub-alternative needs to be confirmed for every characteristic described at the beginning of the article just the same, as done for the first choice. The sub-alternative best practice also applies to moderate and low adoption risk groups. For cyber risk or monoclonal risk mitigation, each group of virtual machines should be served for network, identity, and primary storage separately. As an example, have different active directory domains and have different admin users for each group.

If there is a constraint of number of human resources, have varying password requirements which would force the passwords to be different for admin accounts in different active directory domains. In addition to different passwords, the account names and account naming conventions should also be unique to each active directory. This lowers the risk of threat encountered by the virtualization technology within low adoption group spreading into higher tiers. It is important to remember that the idea is not to have active directory VMs and domains deployed on separate virtualization technologies. It would have been ideal, but the active directory supportability may pose limitations toward achieving that. Hence, the idea is to at least cordon off active directory VMs serving three groups from each other as much as possible. For cost considerations beyond the license costs of alternatives chosen, it is important to consider the costs of secondary storage. Here, the choice should be made keeping data reduction, cyber analysis supportability and scale across heterogenous virtualization technologies, not just within specific virtualization technology. If this is not considered, the data reduction savings in secondary storage which were possible because of uniform virtualization technology will be lost creating a new budget issue while solving another.

4. Conclusion

Re-evaluating virtualization technology is a need originating from a budgetary reason. However, selection of alternative depends on more factors than just the budget and is not as simple as going with the cheapest or the lowest TCO option. Looking at more than one technology for there-do can help balance the budget needs with compliance and security risks. Best practices overarching the selected alternatives also help adhering to regulations, diversifying risk, and keeping ancillary costs down, especially for secondary storage choices. Grouping the alternatives help economic buyers and practitioners to make choices together, instead of one of the buying centers dictating the terms.

References

[1] Alexander K, List of awesome VMWare alternatives, [July, 2025], https://github.com/alexgoesgit/awesome-vmware , [September 2025]

[2] ReadySpace, VMware licensing cost post-Broadcom: What Businesses Need to Know, [August, 2025], https://readyspace.com/vmware-licensing-cost-post-broadcom/, [September 2025]

[3] Customer Stories, Nutanix, [October, 2024], https://www.nutanix.com/company/customers/dumont , [September 2025]

[4] Oracle Virtualization matrix, [2025], https://www.oracle.com/database/technologies/virtualization-matrix.html , [August 2025]

[5] Oracle Database support for Non-Oracle Public Cloud Environments, [May 2025], https://support.oracle.com/knowledge/Oracle%20Database%20Products/2688277_1.html, [September 2025]

[6] Amar Chahal, Why Your Organization Needs a Trust Center, [August 2024], https://www.hypercomply.com/blog/corporation-trust-center , [August 2025]

[7] EUR-Lex, Digital Operational Resiliency Act-Article 29, [December 2022], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554#art_29, [September 2025]

[8] K. R. Kotte, L. Thammareddi, D. Kodi, V. R. Anumolu, A. K. K and S. Joshi, "Integration of Process Optimization and Automation: A Way to AI Powered Digital Transformation," *2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)*, Bhimtal, Nainital, India, 2025, pp. 1133-1138, doi: 10.1109/CE2CT64011.2025.10939966.

[9] L. N. R. Mudunuri and V. Attaluri, “Urban development challenges and the role of cloud AI-powered blue-green solutions,” In Advances in Public Policy and Administration, IGI Global, USA, pp. 507–522, 2024.

[10] S. Banala, L. N. R. Mudunuri, G. C. Vegineni, S. Addanki, P. Pulivarthy and G. Vemulapalli, "Enhancing Decision-Making: From Raw Data to Strategic Insights for Business Growth," *2025 International Conference on Computing and Communication Technologies (ICCCT)*, Chennai, India, 2025, pp. 1-6, doi: 10.1109/ICCCT63501.2025.11020024.

[11] V. M. Aragani and P. K. Maroju, "Future of blue-green cities emerging trends and innovations in iCloud infrastructure," in Advances in Public Policy and Administration, pp. 223–244, IGI Global, USA, 2024.

[12] Kothuru, S. K., & Sehrawat, S. K. (2024, April). Impact of Artificial Intelligence and Machine Learning in the Sustainable Transformation of the Pharma Industry. In *International Conference on Sustainable Development through Machine Learning, AI and IoT* (pp. 60-69). Cham: Springer Nature Switzerland.

[13] Sudheer Panyaram, (2023), AI-Powered Framework for Operational Risk Management in the Digital Transformation of Smart Enterprises.