verge.io

A COMPREHENSIVE GUIDE TO A VMWARE EXIT FOR MULTI-SITE ORGANIZATIONS

Prepared by
Verge.io

www.verge.io

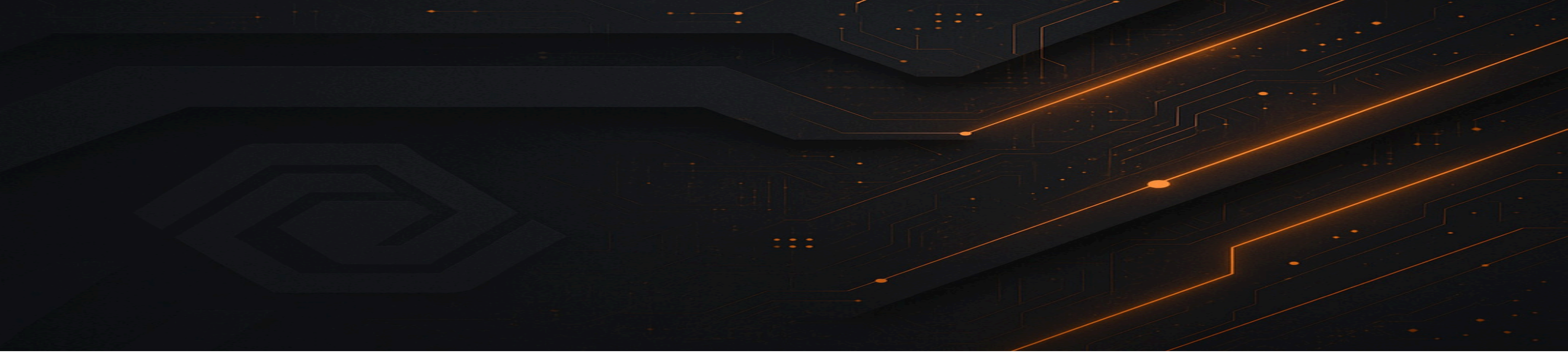
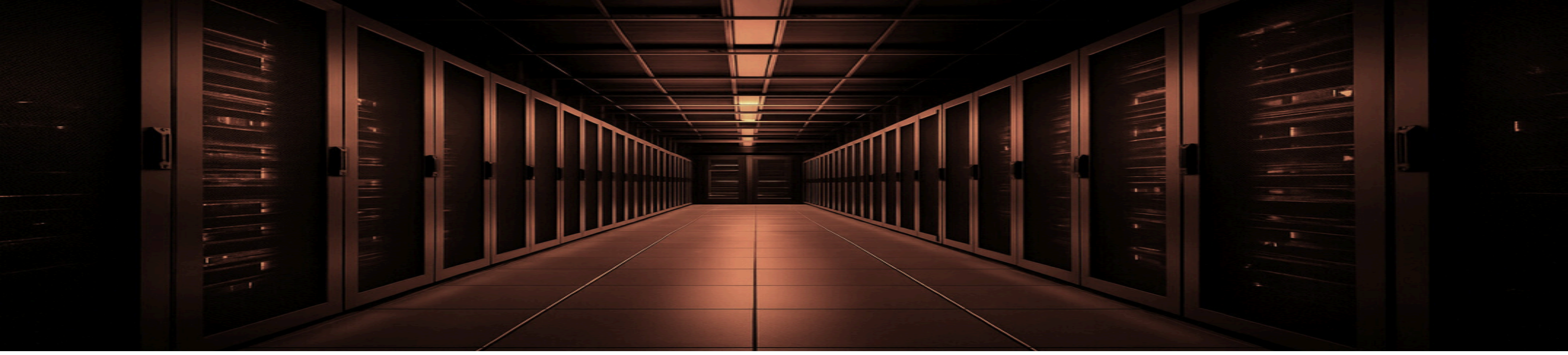


Table of Contents



Organizations operating across multiple venues, branch offices, or edge locations need a multi-site VMware Exit Strategy. VMware's licensing changes under Broadcom ownership have made their current virtualization strategy financially unsustainable. In addition these organizations were running into technical limitations in VMware's ability to provide an infrastructure solution for this use case. This document provides a systematic approach to evaluate, test, and select an alternative platform that meets distributed infrastructure requirements.

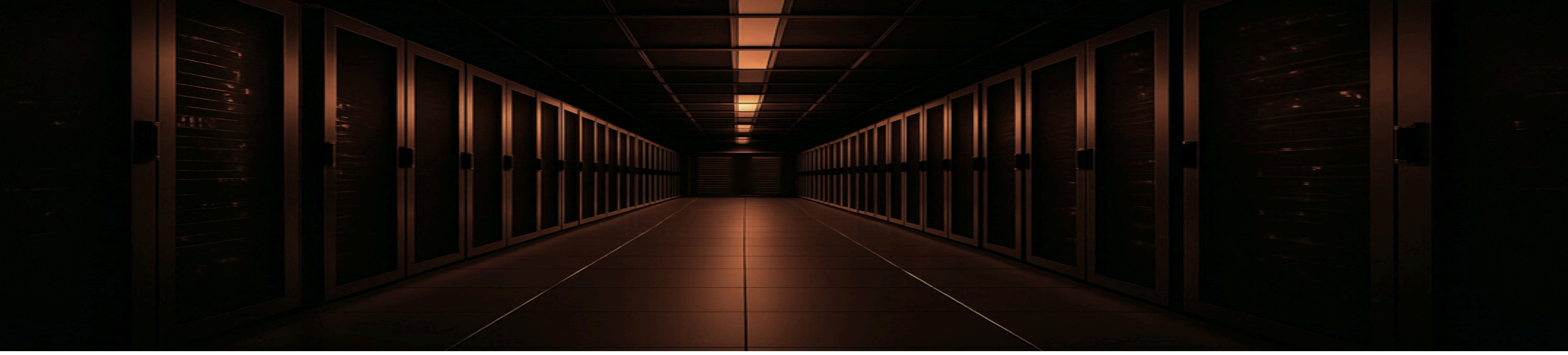
What is Multi-Site IT?

Multi-site IT refers to technology infrastructure that supports operations across multiple distinct locations under a single organization. These locations typically fall into three categories—branches, edge sites, and venues—each with unique requirements.

- **Branches** are often smaller office locations or retail outlets that rely on centralized systems but still need local services for productivity.
- **Edge sites** process data closer to where it's generated, often to support real-time analytics or reduce latency, making them critical for workloads like AI inference, manufacturing control, or IoT.
- **Venues** are specialized locations—such as entertainment centers, stadiums, or casinos—where local IT must support high volumes of customer interactions and transaction processing. Across all three, core IT requirements include operational independence during WAN or cloud outages, centralized visibility and management, local performance for critical workloads, and integrated capabilities for networking, storage, and data protection.

Define Your Multi-Site Requirements

Start by documenting the specific needs of distributed operations. Multi-site organizations share common requirements that differ from traditional data center deployments.



Operational Independence: Each location must continue functioning when WAN connectivity fails. Point-of-sale systems, manufacturing controls, security systems, and local databases cannot depend on constant network access to headquarters or the cloud.

Remote Management: Sites lack dedicated IT staff. The infrastructure must be manageable from a central location with minimal on-site intervention. This includes routine maintenance, updates, troubleshooting, and capacity planning.

Consistent Architecture: Running different virtualization platforms at different sites creates operational complexity. The same software stack should work at a two or three node retail location and a 50-node core data center.

Hardware Flexibility: Avoid platforms that lock you into specific server brands or proprietary hardware. Standard x86 servers should support your virtualization platform without vendor restrictions.

Built-in Resilience: Small sites cannot justify separate backup appliances, disaster recovery tools, or complex storage arrays. The platform must include data protection, replication, and recovery capabilities.

Evaluate Total Cost Impact

VMware alternatives vary in their cost structure. Look beyond the hypervisor licensing to understand the full financial impact.

Software Licensing: Avoid platforms that charge by socket, core, or storage capacity. Vendors will combine all three metrics, creating unpredictable costs as you add CPU cores, memory, or storage to existing servers. Look for solutions with simple per-node licensing that rewards organizations for investing in dense hardware. This approach makes capacity planning predictable and eliminates penalties for choosing high-performance servers.

Hardware Costs: Calculate whether the platform requires proprietary servers, minimum node counts, or specific hardware configurations. Some platforms mandate four or six-node clusters when a more efficient solution enables two or three nodes to meet the needs of that location.

Third-Party Tool Elimination: The right platform should replace backup software, monitoring tools, and disaster recovery solutions. Each eliminated tool reduces both licensing costs and operational complexity.

Operational Expenses: Estimate the labor cost of managing multiple platforms, backup tools, and management interfaces. Complex environments require more staff time for routine tasks, updates, and troubleshooting.

For a detailed analysis of how these cost factors impact real deployments, see our comprehensive examination of The Infrastructure Problem facing modern organizations.

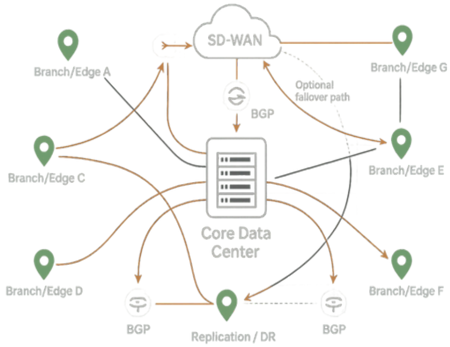
Research Platform Capabilities

Focus your research on platforms designed for distributed environments rather than traditional data center solutions adapted for edge use.

Architecture Approach: Look for platforms that integrate virtualization, storage, networking, and data protection in a single software stack. Avoid solutions that require separate software modules for each function.

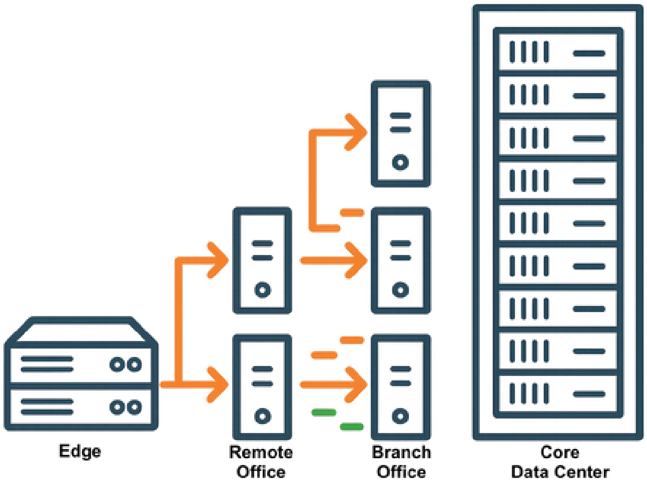
Management Model: The platform should provide centralized visibility and control across all sites while maintaining local autonomy. Single-pane-of-glass management is not just convenient, it is necessary for distributed operations.

Network and Connectivity: The platform should provide advanced networking capabilities that work across distributed sites. Look for integrated software-defined networking that can create secure tunnels between locations, handle network segmentation, and optimize traffic flow. The solution should support bandwidth optimization for replication and backup traffic, especially over constrained WAN connections. Consider platforms that can integrate with existing SD-WAN solutions or provide their own overlay networking capabilities.



Migration Capabilities: Evaluate the platform’s ability to simplify and accelerate migration from VMware. Look for integrated migration tools that can move workloads with minimal downtime and without requiring extensive manual processes. The platform should support automated tools for bulk workload movement. Avoid solutions that require third-party migration tools or complex manual procedures that extend migration timelines and increase risk.

Update Mechanisms: Rolling updates should occur without downtime or manual intervention at each site. The platform should handle patching, security updates, and feature upgrades centrally.



Scaling Characteristics: Verify that the platform provides full functionality in small deployments. Avoid solutions requiring large clusters to access advanced features, making them unsuitable for branch offices.

Integration Capabilities: The platform should integrate with standard data center automation and observability tools. Look for support for infrastructure-as-code platforms like Terraform, monitoring systems like Grafana, and an API-first philosophy that allows integration with existing workflows.

AI Readiness: Modern platforms should support GPU workloads for inference and analytics. This capability positions your infrastructure for future AI requirements without architectural changes.
A comprehensive discussion of these requirements and why traditional approaches fall short can be found in Rethinking ROBO and Edge architectures.

Test Methodology

Structure your testing to simulate real-world conditions rather than laboratory scenarios.

Multi-Site Simulation: Deploy test clusters that mirror your actual site configurations. Include sites with different server types, network conditions, and workload characteristics.

Migration Testing: Run parallel environments to test workload migration from VMware. Measure performance, compatibility, and any application modifications required. Test the platform's migration tools for speed, reliability, and ease of use. Validate that migrations can occur during business hours with minimal service disruption. Assess the learning curve for staff to operate migration tools and processes.

Failure Testing: Disconnect sites from the network and verify that local operations continue. Test hardware failures, power outages, and connectivity issues. The platform should maintain service

availability during these events.

Management Validation: Confirm that you can monitor, configure, and troubleshoot remote sites from a central location. Test the platform during simulated network outages to verify local management capabilities.

Operational Workflows: Test backup, restore, replication, and disaster recovery processes. Verify that these functions work without additional tools or manual processes.

Selection Criteria Framework

Use these criteria to evaluate platforms systematically.

Functional Completeness: The platform should replace VMware plus backup software, storage management tools, and network management systems. Partial solutions create vendor sprawl and operational complexity.

Proven Scale: Look for platforms with documented deployments across hundreds of sites. References should include organizations with similar site counts, geographic distribution, and operational requirements.

Migration Simplicity: The platform should provide integrated tools that streamline VMware migration without requiring separate software or complex procedures. Look for solutions that can migrate workloads with minimal downtime and provide automated validation of migration success.

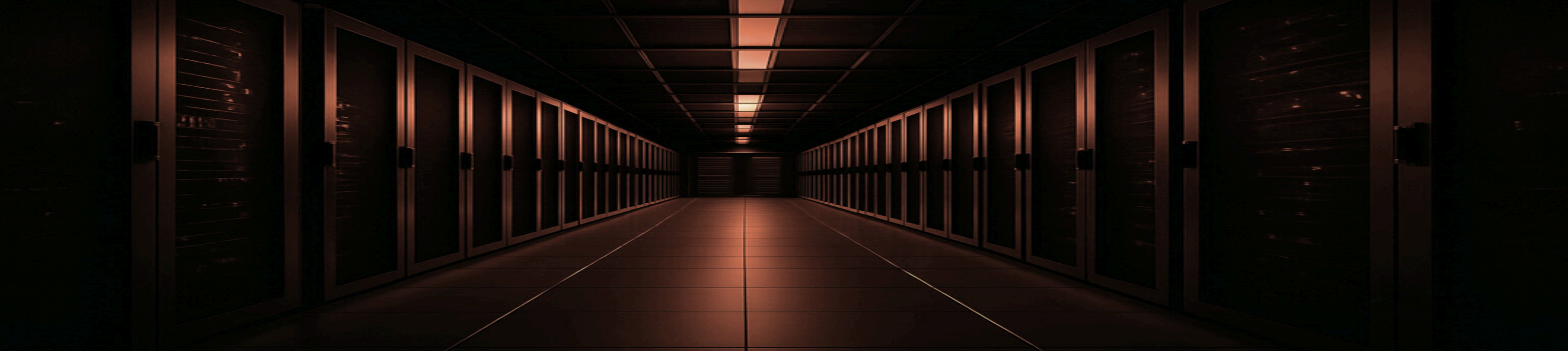
Professional Services: Evaluate migration services, training programs, and technical support quality. Distributed deployments require vendors that can support complex rollouts and ongoing operations.

Future Capabilities: The platform should support emerging requirements like AI workloads, container orchestration, and advanced networking without architectural changes.

Implementation Strategy

Plan your migration to minimize risk and operational disruption.

Pilot Deployment: Start with a representative site that includes typical workloads and connectivity patterns. Run the pilot for at least 30 days to validate performance and operational procedures.



Phased Rollout: Deploy sites in groups based on geography, criticality, or operational windows. This approach allows you to refine processes and address issues before full-scale deployment.

Staff Training: Train your team on the new platform before beginning migration. Include both technical training and operational procedures for managing distributed deployments.

Cutover Planning: Plan migration windows that minimize business impact. Some platforms support live migration from VMware, while others require scheduled downtime.

Rollback Procedures: Maintain the ability to revert to VMware if critical issues arise. Keep VMware licenses active until the new platform proves stable in production.

Vendor Evaluation Process

Structure vendor discussions to gather the information you need for decision-making.

Reference Calls: Speak directly with customers who have completed similar migrations. Ask specific questions about deployment challenges, ongoing operations, vendor support, and cost savings achieved.

Proof of Concept: Insist on hands-on testing before making a selection. The vendor should provide hardware support, software, and technical support for a comprehensive evaluation.

Total Cost Modeling: Request detailed cost comparisons that include software, hardware, services, and operational expenses over three to five years.

Support Model Assessment: Understand response times, escalation procedures, and geographic coverage. Multi-site organizations need vendors with global support capabilities.

Roadmap Alignment: Verify that the vendor’s development roadmap aligns with your infrastructure requirements and timeline.

VergeOS: Purpose-Built for Multi-Site Infrastructure

VergeOS represents a platform designed to meet distributed infrastructure requirements. It addresses the challenges outlined in this strategy through integrated capabilities that span from edge locations to core data centers.

Unified Code Base: VergeOS delivers storage, networking, hypervisor, and AI capabilities from a single, tightly integrated software stack. The platform eliminates the need for separate operating systems, storage controllers, or network appliances. The first virtual machine customers deploy runs their applications, not infrastructure components. This unified approach reduces complexity, eliminates compatibility issues between software layers, and simplifies updates across all infrastructure functions. The single, tight code base improves efficiency, delivering better performance on the same hardware.

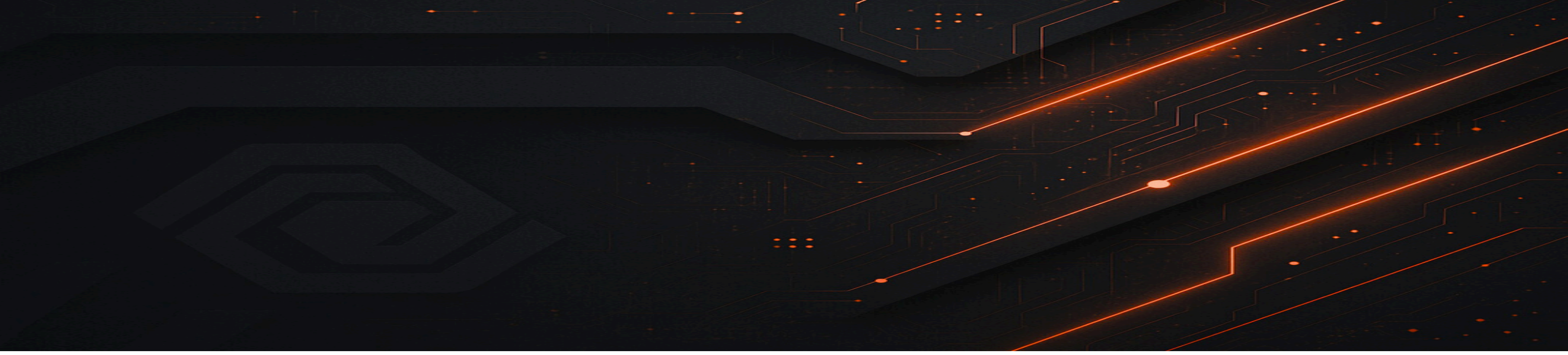
Disconnected Operations: Each VergeOS site operates independently when network connectivity fails. Local systems continue running applications, processing transactions, and maintaining data protection without dependency on headquarters or cloud resources. The platform automatically synchronizes changes when connectivity returns, ensuring no operational disruption during network outages.

Site's Dashboard: VergeOS Site Dashboard provides centralized oversight across hundreds of locations through a single interface. IT teams can monitor site health, deploy updates, and manage configurations without logging into individual systems. The platform maintains visibility even during network interruptions, queuing management tasks for execution when connectivity returns.

Global Inline Deduplication: VergeOS includes integrated global inline deduplication that operates across all infrastructure functions. The technology reduces storage requirements for virtual machines, snapshots, backups, and replication traffic. Deduplication works at the block level and is WAN-aware, optimizing data transfer between sites, and within the site, by only transmitting unique data blocks. This integration means every aspect of the infrastructure benefits from storage efficiency without requiring separate deduplication appliances or software. While deduplication effectiveness will vary, VergeIO customers consistently report improved deduplication rates even when compared to dedicated storage arrays.

Virtual Data Centers (VDCs): Multi-tenancy through VDCs allows logical separation of workloads, users, and policies within the same physical infrastructure. Organizations can create tenant boundaries by geography, business unit, or compliance requirements while maintaining centralized management.

ioMigrate: VergeOS includes integrated migration capabilities through ioMigrate, enabling direct workload movement from VMware environments without requiring separate migration tools or appliances. ioMigrate is built into the core VergeOS code base, providing rapid migration capabilities that minimize downtime during the transition. The technology handles VM conversion, storage migration, and network configuration automatically, reducing migration complexity and accelerating



deployment timelines. Organizations can migrate production workloads during business hours with minimal service interruption, eliminating the need for extended maintenance windows or complex cutover procedures.

ioMetrics: Built-in observability through ioMetrics eliminates the need for separate monitoring tools. The system provides real-time performance data, capacity trending, and predictive analytics across all sites. Integration with external monitoring platforms like Grafana occurs through native APIs without additional licensing.

ioClone: Data protection through ioClone delivers crash-consistent snapshots that consume minimal storage space. The technology supports unlimited snapshots per virtual machine with instant recovery capabilities. This eliminates backup software licensing and simplifies disaster recovery workflows across distributed sites.

ioReplicate: Site-to-site replication through ioReplicate enables disaster recovery between locations without separate tools. The platform replicates virtual machines, applications, and data at the block level, providing near real-time protection with configurable recovery points.

Infrastructure as Code: Native Terraform support enables automated deployment and configuration management across all sites. The platform's API-first design integrates with existing DevOps workflows and CI/CD pipelines without custom scripting.

Hardware Agnostic: VergeOS runs on standard x86 servers from multiple vendors, avoiding hardware lock-in and reducing procurement costs. The platform scales from two-node edge deployments to large data center clusters using the same software stack.

VergeFabric: VergeOS includes integrated software-defined networking through VergeFabric, enabling secure connectivity between distributed sites without requiring separate overlay networking solutions. VergeFabric creates encrypted tunnels between locations, handles traffic optimization for WAN connections, and provides network segmentation capabilities. The technology integrates with existing network infrastructure while adding advanced routing, switching, and security capabilities. Organizations can establish site-to-site connectivity for replication, management, and application traffic without deploying separate SD-WAN appliances or complex VPN configurations.

VergeIQ for AI at the Edge: VergeOS includes integrated AI infrastructure through VergeIQ, enabling organizations to run inference and analytics workloads directly at venues and edge locations. The platform supports GPU resources for real-time processing without requiring separate container orchestration or AI platforms. Organizations can deploy machine learning models for customer analytics, predictive maintenance, or operational intelligence while keeping sensitive data

local. This capability eliminates the latency and connectivity dependency of cloud-based AI services. It also eliminates token costs.

These integrated capabilities allow organizations like Topgolf to replace VMware while simplifying operations, reducing tool sprawl, and preparing for future AI workloads. The platform eliminates the need for separate backup, monitoring, and disaster recovery solutions while providing the automation and visibility required for distributed infrastructure management.

Real-World Validation

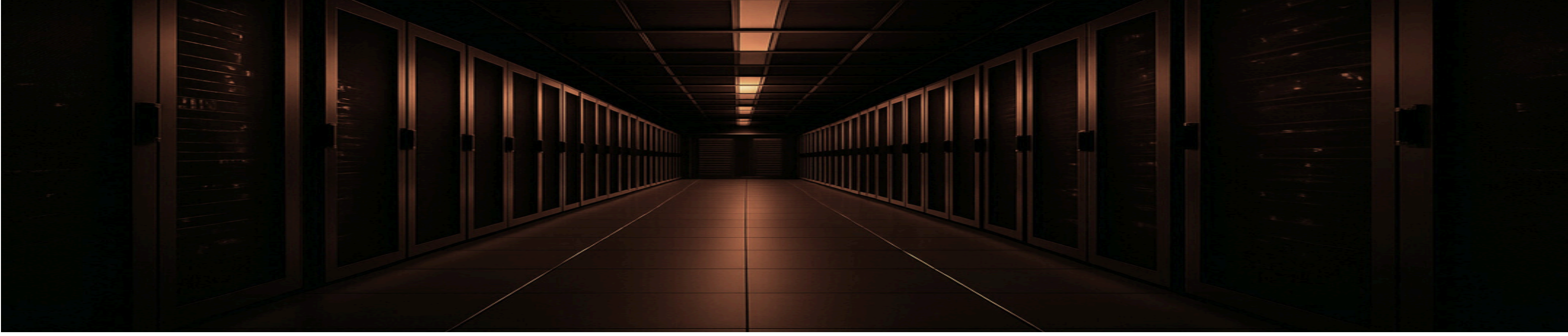
Theory and vendor demonstrations only provide part of the picture. Look for actual deployments that demonstrate success at scale.

Topgolf provides an excellent example of how a global organization with 100+ venues approached this challenge. Their infrastructure team evaluated multiple platforms before selecting VergeOS to replace VMware across their entire footprint. The deployment reduced their hardware footprint from six-node to three-node clusters while eliminating third-party backup software. Read the complete analysis in Topgolf is Choosing VergeOS.

Conclusion

Multi-site infrastructure decisions have long-term consequences. Take time to evaluate alternatives thoroughly rather than rushing to replace VMware with the first available option. The right platform will simplify operations, reduce costs, and position your infrastructure for future requirements. The wrong choice will create new problems that persist for years.

VergeOS represents one platform designed specifically for these requirements. It provides integrated virtualization, storage, networking, and data protection in a single software stack that scales from edge locations to core data centers. Organizations like Topgolf have deployed VergeOS across hundreds of venues to replace VMware while simplifying operations and reducing costs.



VMware Alternative Evaluation Checklist

Multi-Site Organizations Replacement Guide

Phase 1: Define Requirements

Current State

□ Document site count and growth plans

□ Calculate VMware licensing and support costs

□ List backup, monitoring, and DR tools in use

□ Identify sites requiring WAN-independent operation ■ Assess current hardware configurations

Future Needs

□ Define AI workload requirements at edge

□ Identify automation tool integrations needed

□ Document compliance requirements by location

Phase 2: Research Platforms

Licensing Model

□ Per-node pricing (not socket/core/capacity)

□ No penalties for dense hardware

□ Backup/DR/monitoring included

□ Transparent support costs

Architecture

□ Single software stack edge-to-core

□ Full functionality in small deployments

□ Integrated virtualization, storage, networking

□ API-first design for automation

Vendor Assessment

□ Roadmap alignment

□ Multi-site customer references

□ Global support coverage

Phase 3: Test and Validate

Proof of Concept

□ Deploy clusters matching site configurations

□ Test disconnected operations during network outages

□ Validate backup/restore without third-party tools

□ Test centralized management capabilities

□ Verify rolling updates without downtime

Migration Testing

□ Test VMware workload migration

□ Measure performance differences

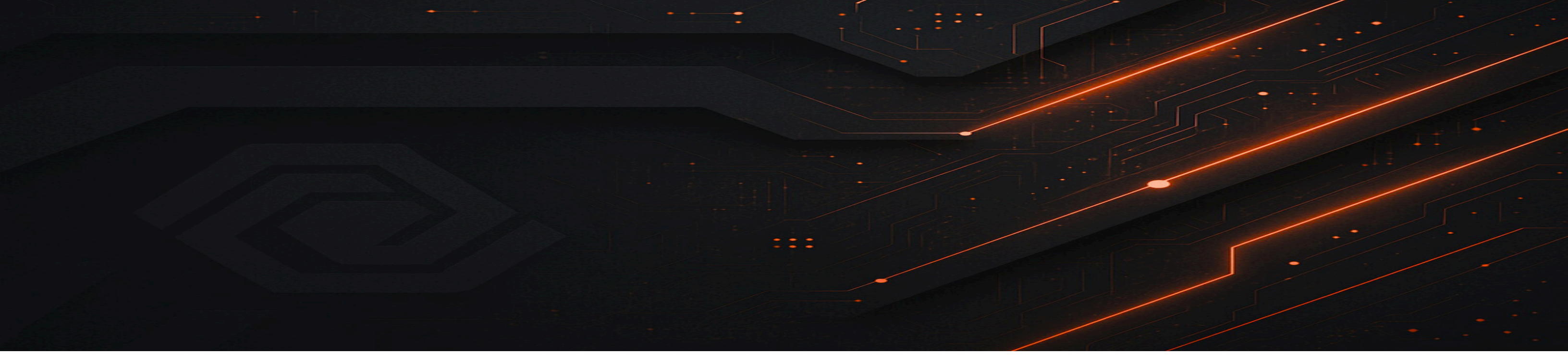
□ Validate data integrity during migration

Integration Testing

□ Test Terraform/Iinfrastructure-as-Ccode integration

□ Validate monitoring platform connectivity

□ Verify API functionality



Phase 4: Financial Analysis

Cost Modeling

□ Calculate 3-5 year software licensing costs
□ Model hardware savings from efficient architecture
□ Estimate operational savings from tool consolidation
□ Include migration and training costs

Reference Validation

□ Interview customers with similar deployments
□ Verify performance and operational claims
□ Understand implementation challenges

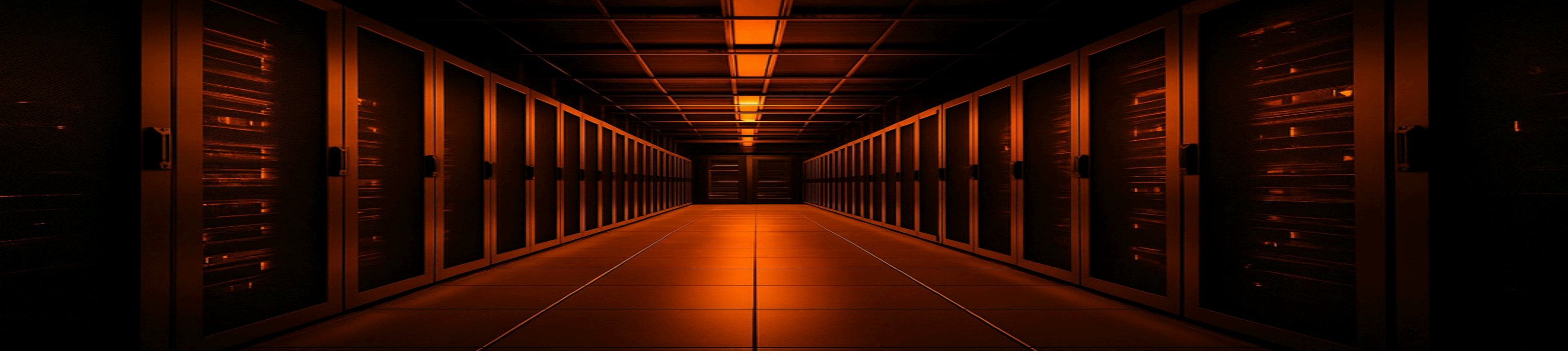
Phase 5: Implementation

Migration Planning

□ Select representative pilot site
□ Define phased rollout by geography/criticality
□ Plan staff training before migration
□ Develop rollback procedures
□ Create stakeholder communication plan

Success Metrics

□ Define migration success criteria
□ Establish baseline performance measurements
□ Plan cost savings reporting



VergeOS Specific Validation

If evaluating VergeOS, confirm these integrated capabilities:

- □ **Sites Dashboard**: Single-pane management across locations
- □ **Global Inline Deduplication**: Integrated across all functions
- □ **VDCs**: Multi-tenant separation by geography/compliance
- □ **ioMigrate**: Integrated VMware migration without separate tools
- □ **ioClone**: Snapshots eliminate backup software needs
- □ **ioReplicate**: Site-to-site DR without additional tools
- □ **ioMetrics**: Built-in monitoring and observability with external integration
- □ **VergeFabric**: Software-defined networking across sites
- □ **VergeIQ**: AI workloads from edge to core without separate platforms
- □ **Disconnected Operations**: Full autonomy during outages
- □ **Hardware Agnostic**: Works with preferred server vendors

Key Success Factor: Choose platforms designed for distributed operations, not data center solutions adapted for edge use or edge solutions stretched to data center use.