Addressing the Top MSP Challenges

verge.io

EXECUTIVE SUMMARY

Managed Service Providers (MSPs) and Cloud Service Providers (CSPs) face unique business and technical challenges. They compete with customers' internal data center operations and larger public cloud entities like Amazon AWS, Microsoft Azure, and Google Cloud Platform. They must deliver a higher IT service quality and a lower price than internal IT operations or the public cloud.

The top MSP challenges include:

- Maintaining Profitability / Eroding Margins
- Keeping up with and adequately integrating technological enhancements
- Dealing with compliance risks
- Defending against and recovering from ransomware threats
- Managing the scaling challenges that come with success
- Differentiating from the Public Cloud and Other MSPs

This paper will detail these challenges and provide ways to resolve them using VergeOS.

VergeOS for MSPs/CSPs

VergeOS is an infrastructure software solution ideally suited to meet the challenges of MSPs. It is an alternative to products like VMware, dedicated all-flash arrays, and proprietary networking that all increase MSP's cost of service delivery. VergeOS is an UltraConverged Infrastructure (UCI) solution that fulfills and expands on the promise of hyper-converged infrastructure (HCI) solutions like those from Nutanix and VMware (vSAN, vSphere, NSX), offering a more flexible, cost-effective alternative.

VergeOS is unique in that it is a software platform that efficiently integrates virtualization (VergeHV), networking (VergeFabric), and storage (VergeFS) into a unified codebase. With VergeOS, there is a single package to install and support, reducing customer onboarding times and simplifying operations. Its capabilities seem custom-designed for MSPs looking to address the above challenges.

ADDRESSING THE TOP MSP CHALLENGES

MAINTAINING MARGINS

If the MSP is not profitable, it can't service its customers, so profitability is the top priority. The problem is that every aspect of running a data center for profit creates a series of cost containment issues that threaten the MSP's ability to retain existing customers and attack new ones. Profitable MSPs must constantly be looking for ways to improve profitably. Since many MSP's infrastructures are built on VMware, which has a very high cost, finding a suitable alternative has the highest potential for increasing profits.

Increasing Profitability with VergeOS

Most MSPs will find that a VergeOS license is 55% less than a VMware license. However, the potential to increase profitability goes well beyond less expensive licensing costs. VergeOS' efficiency and flexibility, which we will detail later, means that most MSPs can eliminate or reduce their next two or three years' worth of server purchases while getting more performance and higher availability from their existing servers. Further, VergeOS' licensing model is priced per server, rewarding IT for investing in more powerful servers with more CPUs, RAM, and storage.

The VergeOS storage services capabilities, VergeFS, include Global Inline Deduplication (GID), which delivers an average 5:1 increase in storage efficiency. In other words, 50TB capacity can typically store 250TB of data. However, unlike most deduplication algorithms, VergeOS' GID is an efficient, lightweight algorithm requiring only modest CPU and RAM. As a result, GID increases profitability by enabling MSPs to buy less storage capacity without overcompensating by buying more CPU power or RAM capacity than necessary.

The simplicity and narrow AI automation capabilities of VergeOS mean that fewer people are required to administer the environment. Not only does simplified operation lower headcount requirements, but it also means that MSPs don't have to suffer from the skills shortage that others face

MANAGING TECHNOLOGICAL HARDWARE ADVANCEMENTS

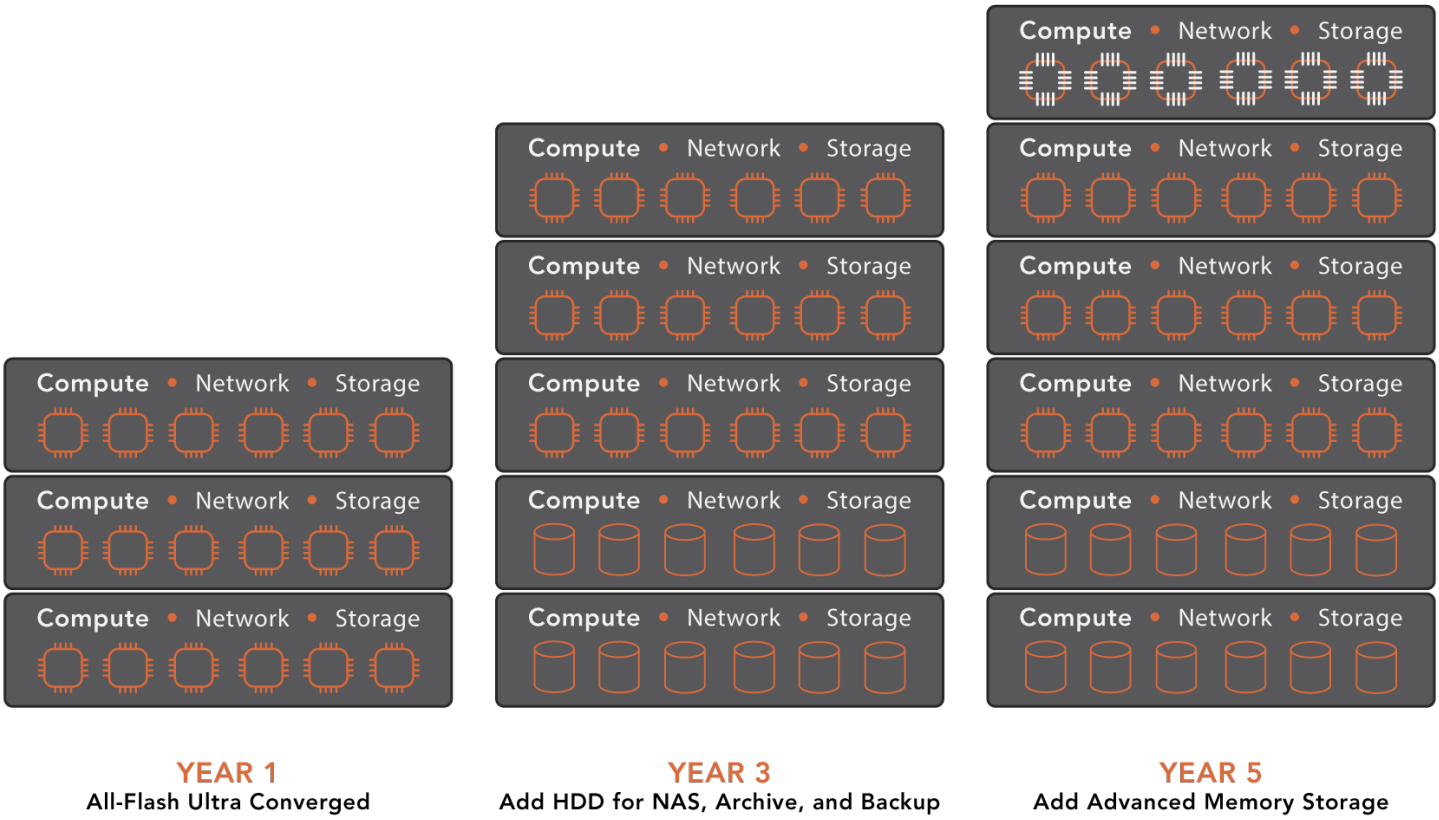
Another challenge for MSPs is managing technological advancements in hardware. For an MSP, new hardware promises more performance while consuming less data center floor space. Implementation of this new hardware, however, is the challenge. First, the infrastructure software company must support this new hardware. Also, the licensing costs of that software must not punish the use of the advanced multi-processor and multi-core hardware. That software must also enable the mixed use of next-generation and previous-generation hardware within the same instance.

MSPs are burdened with thoroughly testing new hardware before exposing their customers to it. This burden incurs additional costs of creating and moving test data to a separate testing environment. After verifying the new hardware, because of VMware's complexities, MSPs must implement a separate VMware instance, which must be independently managed, lowering overall efficiency.

VergeOS Enables Rapid Adoption of New Hardware

VergeOS fulfills all of the requirements for testing and certifying new hardware. It can support servers from different CPU generations and even brands within the same instance. VergeOS is licensed by the physical server, not by the number of CPUs, cores, amount of RAM, or storage capacity. MSPs can invest in their chosen servers without fear of exponentially increasing software licensing costs.

Because of its high level of abstraction, new hardware can be inserted directly into the existing VergeOS environment and does not require the MSP to create a new instance for each hardware advancement. VergeOS' Virtual Data Center (VDC) technology makes testing and approving new hardware technology much more streamlined.



VDCs encapsulate the entire data center like a virtual machine (VM) encapsulates a physical server. Each VDC contains all the VMs, network, and storage settings for a given workload or customer. VDCs can be moved, copied, or cloned, enabling the MSP or the customer to create DR instances, safely test patches, or spawn new environments. VDCs also enable MSPs to hard-allocate specific resources to specific customers to deliver the ultimate quality of service.

VDCs assist in verifying new technology by enabling the MSP to implement the new hardware into the existing VergeOS instance instead of creating a separate lab environment. MSPs can clone their, or other customers', VDCs and isolate the new hardware to that cloned VDC—enabling them to perform an accurate test of the new hardware against a near-production environment. As a result, they can speed up the time to implement new hardware while maintaining and potentially increasing profitability.

DEALING WITH COMPLIANCE RISKS

Another challenge that MSPs face is dealing with their customers' compliance and regulatory requirements. MSPs must comply with data protection and privacy laws, cybersecurity regulations, intellectual property rights, disaster recovery requirements, and cross-border data access and transfer. These laws vary between governing bodies, and some organizations may have even higher requirements than those of governments.

Beyond the challenge of knowing about these regulations is how to implement them consistently over time without slowing down customer adoption and onboarding. The chances for a mistake during the deployment of a customer's environment are high, as are the penalties for non-compliance.

VergeOS Provides Secure Multi-Tenancy

VergeOS VDCs enable MSPs to template an entire data center virtually and then clone it for future use, essential to creating golden masters of the various data center types. For example, if the MSP has a set of customers dealing with PCI data, other customers dealing with HIPAA data, and other customers with no specific compliance concerns, they can create golden master VDCs of each type. They can then clone those golden masters as they on-board a customer. A VDC clone takes milliseconds to create and does not impact performance. The advantage to the MSP is that once they have done the work to create compliant VDCs, all clones are perfectly compliant every time. VDC cloning means that client onboarding accelerates, as does time to revenue.

CYBERSECURITY THREATS

As providers of IT services, MSPs must not only protect their clients from cyber threats and safeguard their own internal systems. A breach in the MSP's system can have cascading effects on all of its clients. While they should leverage all possible means to limit ransomware infection, MSPs are uniquely exposed to attacks because they don't always control the customer's operating environment. MSPs need to ensure that they can stop ransomware from spreading and be able to assist their customers with recovery.

Another vital element of a ransomware resiliency strategy is protecting the operating environment itself. We've seen applications, operating systems, and infrastructure platforms all compromised so bad actors can access customer data or bring down the environment and hold it hostage.

VergeOS Provides Infrastructure-wide Ransomware Resilience

Regarding ransomware, VDCs ensure that a malware file or other exploit introduced into the MSP business operations environment or one of their customer's environments can't spread across the MSP's data center. Each VDC is essentially a "walled garden," and, by default, multiple VDCs are not connected. VDCs eliminate the ability of ransomware to spread across the environment. Even if there is a need for VDC interconnectivity, because VergeOS' VergeFabric provides complete Layer 2 and Layer 3 networking, the MSPs can create very secure tunnels between VDCs. The result is that it is nearly impossible for ransomware to spread across multiple VDCs that the MSP is operating.

The combination of VDCs and VergeFabric also means that MSPs can further isolate customers under attack, effectively quarantining them and eliminating the need to physically scramble to the data center to unplug switches and servers. VergeFabric allows remote network administration, including isolation of a particular VDC if necessary.

While VDCs enable you to stop ransomware from spreading, VergeFS storage capabilities enable rapid detection and recovery from a ransomware attack. As mentioned above, VergeFS is innately deduplicated. Its GID algorithm enables VergeFS' snapshot technology to behave more like clones than snapshots that are available from other vendors. Most other snapshot technologies on the market today are highly dependent on each other.

For example, if you had a policy that triggered a snapshot every hour and retained those snapshots for a day, snapshot 24 would be dependent on snapshot 23, and 23 would be dependent on 22, etc… All 24 of those snapshots would be dependent on the primary volume. As that snapshot quantity continues to increase, it impacts storage performance negatively. As a result, most vendors' best practice is to have no more than 32 active snapshots. The result is a data protection house of cards unsuitable for almost any form of data recovery, especially recovery from ransomware.

VergeOS snapshots are essentially clones and are independent of each other. They are complete copies, yet because of deduplication, they take milliseconds to create and initially require almost no additional space. They are also immutable by default. Because of the efficiency of VergeOS and its deduplication algorithm, customers can take snapshots as frequently as they need or want to with no impact on performance and minimal impact on capacity utilization.

As mentioned earlier, VDCs make it impossible for malware to spread between VDCs. VergeOS' unique snapshot capabilities enable the last known good copy to be a few minutes old and uncompromised by the ransomware. The final ingredient is to help the MSP realize that they or one of their customers is under attack. VergeOS' IOfortify functionality can alert customers of a potential attack. It works by analyzing deduplication historical information to monitor if a VM or VDC shows a statistically significant increase in net new data creation. Since ransomware penetrates a VM and walks its file system, encrypting data as it goes, VergeOS detects this behavior as a drop in deduplication efficiency. This anomaly triggers VergeOS' IOfortify into action, alerting customers of a potential attack within 5 to 10 minutes of the attack starting.

VergeOS itself is also resilient to attack or compromise. When an MSP implements VergeOS, the software installs as read-only. As a result, it can't be compromised. As the MSP starts to create VDCs, a read-write version of the software is injected into each VDC. While it hasn't happened yet, this design protects against an attack directly on VergeOS. Suppose the copy of VergeOS in a VDC is somehow compromised. In that case, all the MSP IT team needs to do is refresh that VDC, and instantly, a new copy

of VergeOS is reinjected into that VDC from the read-only copy at the core, erasing all remnants of the attack while keeping the data in the VDC intact.

With VergeOS snapshots, MSPs can frequently protect their and their customers' data, trust that the protected copies are secure, and know within minutes that they are under attack. Most VergeIO customers experiencing an attack could recover in less than 30 minutes without losing data or paying a ransom. Meeting the ransomware challenge means VergeOS can meet all other data protection requirements, including backup and disaster recovery (DR). VergeOS enables the MSP to increase profitability further by eliminating the need for separate backup, recovery, high-availability, and disaster recovery tools from other vendors.

MANAGING THE SCALE THAT COMES WITH SUCCESS

As the MSP grows, it must add more resources to meet customer demands. The scale requirement is more than how large the environment can scale. It is also how small and how wide it is. Scaling small is important because many customers want to have local services in addition to MSP-hosted services. Scaling down and creating two-node pods is sometimes a critical requirement.

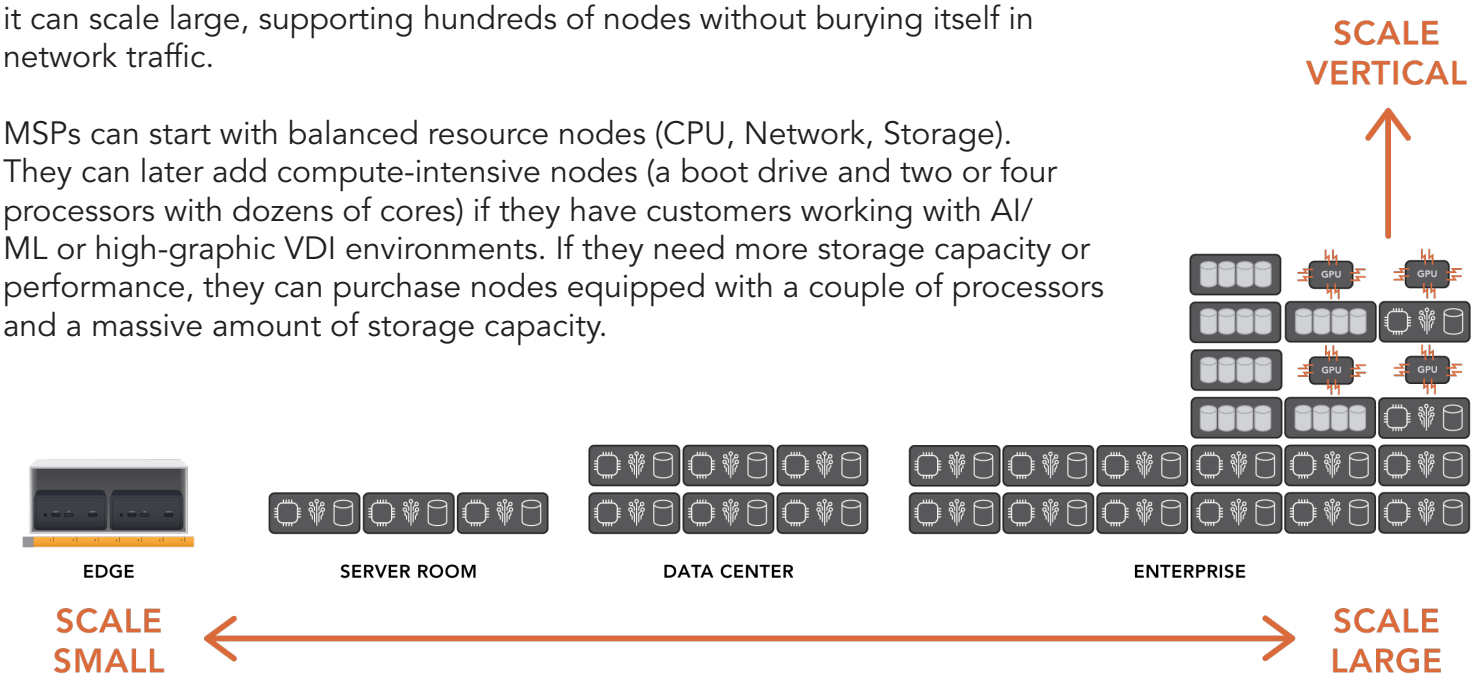
Scaling wide means having the flexibility to mix and match nodes from different server vendors with CPU brands and storage types. It enables the MSP to respond to customer demand quickly with the most readily available hardware. It also allows the MSP executive team to move between hardware vendors for cost savings or efficiency gains.

Scaling large may seem self-explanatory, but a rapidly growing MSP may need hundreds of nodes, not just dozens. Only recently, VMware announced the ability to scale to high double-digit node counts and has not broken into triple-digit instances. Most MSPs, because of the overhead of VMware and its network inefficiencies, do not scale a single VMware instance beyond a dozen nodes.

VergeOS Provides Three-Dimensional Scale

Its efficiency enables MSPs to use VergeOS to scale small, set up two-node clusters in remote offices or Edge locations, scale wide so a single instance can run for decades, and support various hardware platforms. Additionally, it can scale large, supporting hundreds of nodes without burying itself in network traffic.

MSPs can start with balanced resource nodes (CPU, Network, Storage). They can later add compute-intensive nodes (a boot drive and two or four processors with dozens of cores) if they have customers working with AI/ML or high-graphic VDI environments. If they need more storage capacity or performance, they can purchase nodes equipped with a couple of processors and a massive amount of storage capacity.



DIFFERENTIATION FROM THE PUBLIC CLOUD AND OTHER MSPS

MSPs face an unusual set of challengers. Their potential customers may already have internal IT services, and bringing more of those back in-house is always possible. Their potential customers may also look at the public cloud as an option. Finally, their potential customers may also look at other MSPs.

VergeOS is the Difference Maker
Differentiating from the wide variety of MSP competitors is critical for the organization to keep existing customers and attract new ones. VergeOS enables the MSP to provide cloud-like services at rates far less expensive and far more profitable than those provided by public clouds.

VergeOS' recipe engine allows MSPs to build self-service provision capabilities that rival cloud offerings. Complete workloads can be deployed with the click of a button, ranging from various VM templates to sophisticated environments like LAMP Stack, Object Storage, Kubernetes, and Docker.

Competing MSPs that continue to count on VMware or even those that attempt to move to an open-source solution still won't match the efficiency and profitability of a VergeOS-powered MSP.

CONCLUSION

VergeOS presents a comprehensive and efficient solution for MSPs, addressing their unique operational challenges in a highly competitive environment. Its integrated approach, scalability, and focus on security and efficiency make it a valuable tool for MSPs seeking to maintain a competitive edge and grow their businesses.