

Protecting VergeOS

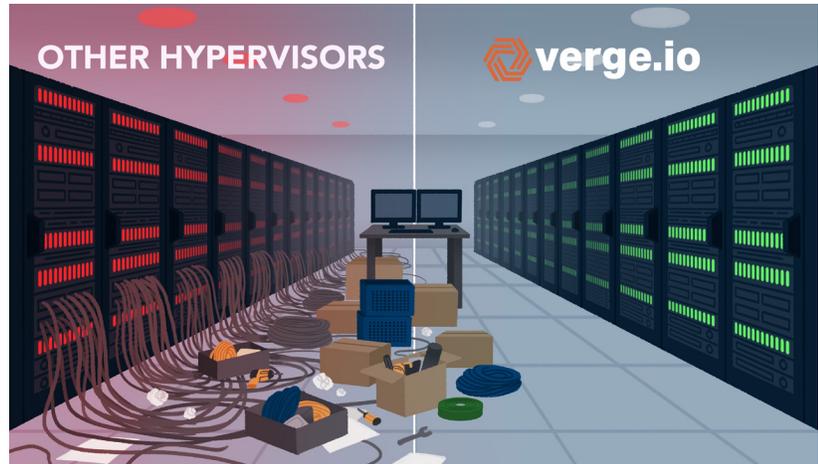


As customers transition from VMware, they typically want to continue using their backup software for various reasons. VergeOS can work with almost any backup application. When combined with VergeIO's integrated data protection and application availability, you can rest assured that your data and applications are always available, leading to unprecedented infrastructure resiliency.

VergeIO's Data Protection and Application Availability

First, it is essential to understand VergeIO's integrated data protection and application availability features. VergeIO's UltraConverged Infrastructure (UCI) integrates virtualization, storage, and networking into a cohesive operating environment and provides infrastructure-wide availability at no additional charge.

Most hypervisors must piece-part their way to data protection, application availability, and disaster recovery. These components add complexity and increase the price. VergeOS provides all these capabilities within a single piece of code for one price.



Automated High Availability

VergeOS guarantees complete high availability. In case of a server failure, all the virtual machines (VM) running on that server will migrate to other servers within the instance. VergeOS leverages a narrow AI algorithm that predictively determines the best possible node to relocate the impacted virtual machines, ensuring a seamless transition and optimal performance even during a failed state. If administrators put a server into maintenance mode, VM migration is seamless, and thanks to VergeOS' live migration capabilities, there is no downtime. VergeOS will automatically restart the VMs on the remaining nodes if the server crashes. The only outage is the time it takes for the server to power on.

Unmatched Data Protection

decades old and were written in an era of small drive capacities and expensive costs per TB. They add significant overhead to the storage hardware, often requiring dedicated hardware to help lower the potential performance impact. Besides increasing cost, this hardware also means another point of failure must be protected against, so customers must buy multiple controllers. Another concern is that algorithmically recovering from a drive failure can take hours, if not days, even with flash drives as drive density increases.

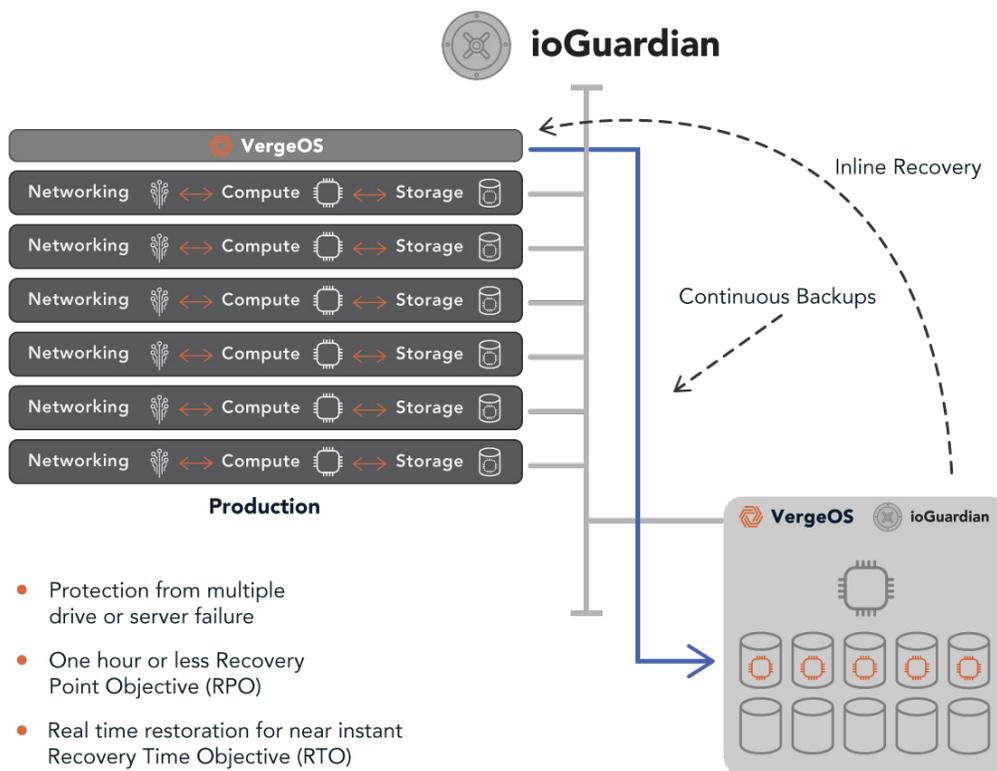
VergeOS delivers always-on global inline deduplication, integrated at its core, allowing customers to achieve significant storage capacity savings with minimal performance impact. As applications or users write data to the VergeOS instance, before actually writing the data, the deduplication algorithm examines it in segments for uniqueness. Only the remaining unique segments are written to physical media, and to protect from drive failure, they are written synchronously to two different nodes in the instance. This redundancy ensures a virtual machine can access its data even if a drive or server fails. The broad data distribution without a complex algorithm improves performance and eliminates hot spots.

Protection from Multiple Drive or Server Failures

Most storage systems use dual parity RAID or Erasure coding to protect against multiple drive failures, which only exacerbates the performance problems mentioned above.

VergeOS' [ioGuardian](#) takes a different approach and delivers missing data segments to virtual machines (VMs) in real-time when multiple drives or servers fail. This inline data delivery ensures that even if the primary VergeOS instance suffers from multiple drive failures, VMs can continue operating without any downtime.

There is no additional software to buy with ioGuardian, as its capabilities are integrated directly into VergeOS. This integration simplifies the data protection process for customers and lowers costs. Only an additional server, configured and licensed as the ioGuardian target, is needed. This server can be an older server or storage system capable of running VergeOS. VergeOS' global inline deduplication minimizes capacity planning for the ioGuardian server, making it a cost-effective solution for businesses of all sizes. The asynchronous data transfer allows for using hard disk drives instead of flash, further reducing costs without compromising reliability.



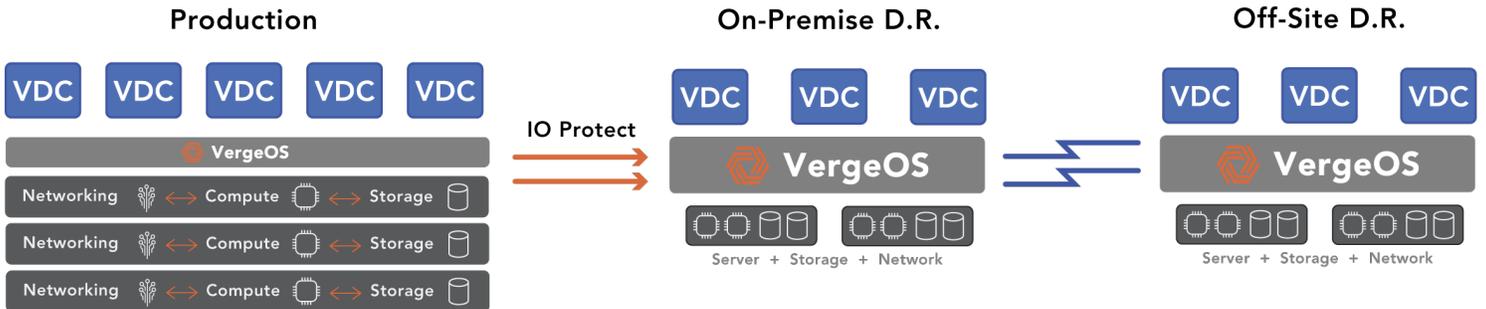
Several backup vendors offer instant recovery, where a VM can be re-instantiated on a backup appliance. While impressive, this approach requires downtime for the VM restart on the backup appliance, which may provide suboptimal performance. IT intervention is also necessary during the recovery process. Additionally, even with change block tracking technologies, most customers do not protect their entire environment every hour, resulting in an actual recovery point objective (RPO) of typically four to eight hours.

ioGuardian's inline recovery does not cause downtime, assuming the data is on the ioGuardian server. Instead, it provides missing data segments to the VM in real time without IT intervention. It delivers an instant recovery time objective (RTO) and an RPO measured in minutes instead of hours. Furthermore, the VM continues to execute from the primary instance, not on a potentially degraded backup appliance.

Holistic Disaster Recovery

Most storage systems use dual parity RAID or Erasure coding to protect against multiple drive failures, which only exacerbates the performance problems mentioned above.

VergeOS' ioGuardian takes a different approach and delivers missing data segments to virtual machines (VMs) in real-time when multiple drives or servers fail. This inline data delivery ensures that even if the primary VergeOS instance suffers from multiple drive failures, VMs can continue operating without any downtime.

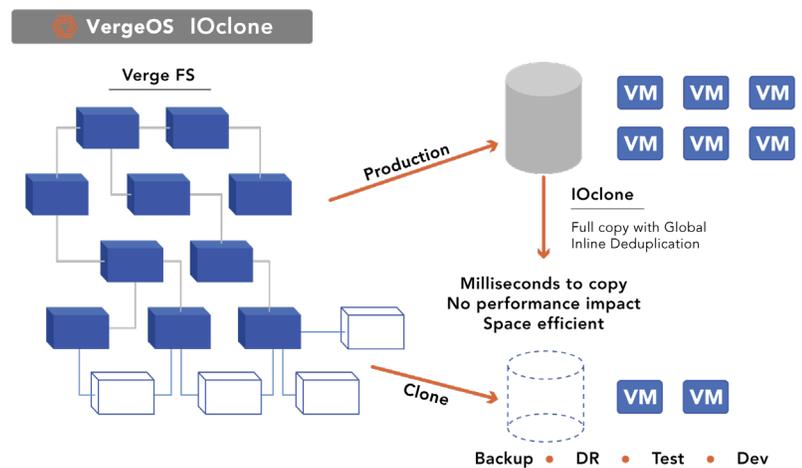


Implementing VDCs in disaster recovery strategies involves copying the VDC to a DR site and establishing asynchronous replication. In a disaster, the DR site's VDC contains a replica of the original data center, ensuring functionality even on different hardware. VergeOS customers have reported significant reductions in time spent and increased success rates in their DR tests, achieving a 100% success rate in rapid disaster recovery.

Snapshots That Act Like Clones

VergeOS offers unlimited snapshots through its IOclone technology. Unlike traditional snapshot technology, which is used on dedicated storage arrays and other hypervisors, manipulate inode tables to create snapshots. Each snapshot depends on the snapshot before it, and all snapshots depend on the original.

VergeOS snapshots act more like clones, creating independent, standalone copies. Because deduplication is integrated into the operating system's core, there is almost no immediate capacity impact when taking a snapshot. Customers can take snapshots as frequently as needed and retain them indefinitely without impacting performance. This independence is crucial for meeting the 3-2-1 rule of backup, setting VergeOS apart from traditional snapshot solutions, which can't fulfill the requirements of that rule. VergeOS snapshots can be used to recover the entire instance, a virtual data center, a virtual machine, or even individual files and copy them back to a virtual machine.



Ransomware Resilience

VergeOS also provides unprecedented protection from a ransomware attack. First, each VDC is isolated from the others, meaning if ransomware gets into a particular VDC, it can't spread beyond that VDC, eliminating the attack's blast radius. Second, VergeOS snapshots are, by default, read-only, which means a ransomware attack can't alter them. These snapshots can be taken frequently, without adversely impacting performance, to lower the potential of data loss. Finally, using VergeOS subscriptions, you can enable our ioFortify capability, alerting you of an attack within minutes of it starting.

Elevate Data Center Resilience with VergeOS

With its UltraConverged Infrastructure, VergeOS revolutionizes high availability, data protection, and disaster recovery. Its unique features, such as automated high availability, advanced data protection, and innovative snapshot technology, ensure operational continuity and data integrity.

The holistic approach to disaster recovery through virtual data centers simplifies replication and guarantees functionality, even on diverse hardware. Embrace VergeOS for streamlined data management and disaster recovery, ensuring your organization's resilience and success.

Integrating Backup Solutions

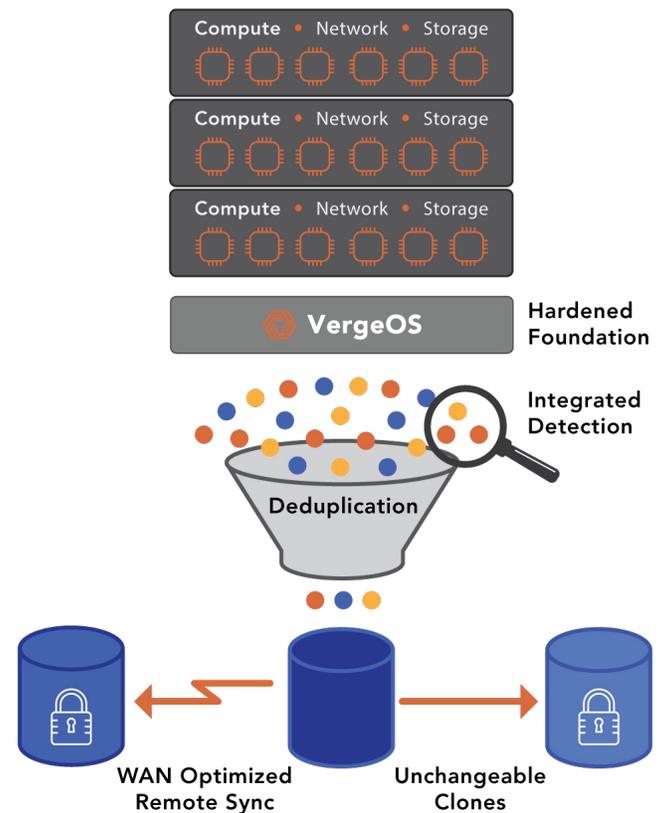
VergeOS' Data Availability Services combined with ioGuardian capabilities lessen IT dependency on the backup infrastructure for most recovery efforts, and many customers decide that is all the protection they need. VergeOS also provides an in-guest agent to quiesce VMs to deliver application-consistent snapshots. Still, some customers want to use third-party backup solutions to meet these requirements:

Backup of Last Resort

Some customers may want a separate copy of data outside VergeOS's control. VergeOS can export the VMs' raw files via an NFS mount point that almost any backup product can browse and back up to meet compliance or vendor-independent data copy requirements to a different storage system, like the public cloud or even tape.

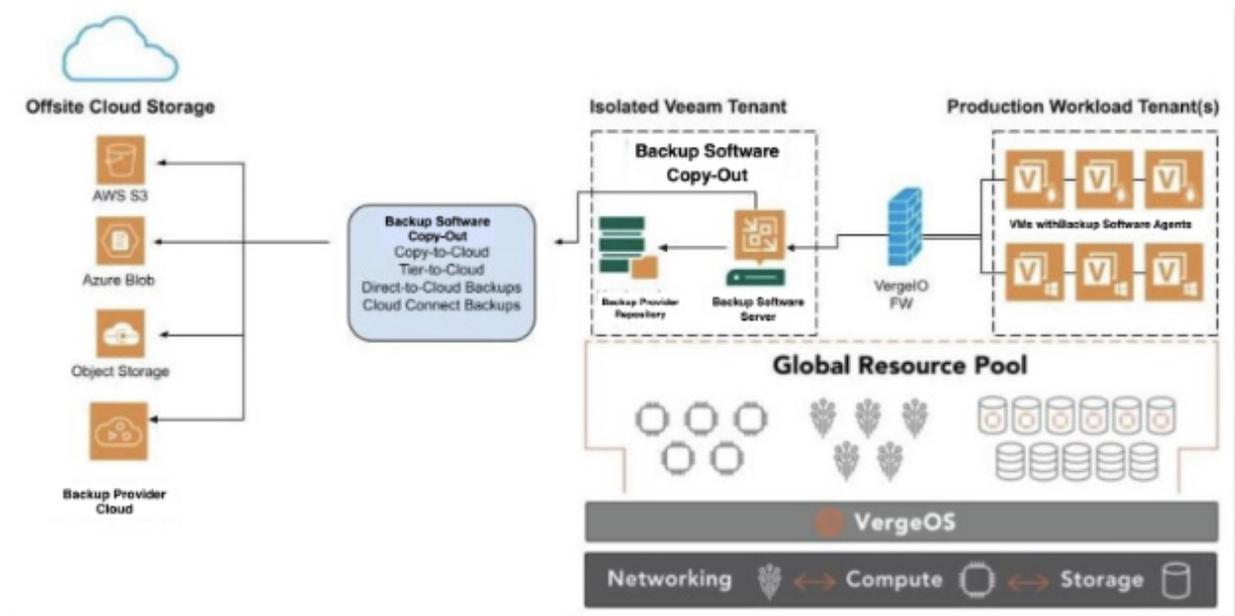
Catalog Restoration

Another need is for browsable single-file restoration. While restoring a single file from within a VergeOS snapshot is possible, customers often want the ability to browse all available backup copies and select a specific version of a file to recover. Customers can install the operating system specific agent into the virtual machine for these situations. Because VergeOS' CPU utilization is 30% more efficient than VMware's, at most, 1% of the consumption of these resources has no impact on application performance. Also, installing the agent inside all VMs is unnecessary since not all VMs need this type of single file recovery.



Firewall Protected Backup Software

A final use case involves using VergeOS and VDC technology to host the third-party backup software. Customers can create a VDC specifically for the backup software and its storage repository, including immutable functions. The customer can then open specific ports in the VDC to back up other VDCs or external, non-VergeOS data sets. Since VergeOS supports multiple types of storage, administrators can direct the backup repository to hard disk drives to keep costs low.



Conclusion

VergeOS presents a robust and versatile platform that offers a cost-effective alternative to VMware and redefines data protection, application availability, and disaster recovery. Its innovative UltraConverged Infrastructure (UCI) seamlessly integrates high availability and advanced data protection, ensuring that virtual environments remain resilient even under the most demanding conditions. By leveraging VergeOS, organizations can enjoy reduced dependency on traditional backup solutions thanks to features like automated high availability, ioGuardian's inline recovery, and holistic disaster recovery capabilities.

Furthermore, the flexibility of integrating with existing backup software and the ability to host third-party solutions within VergeOS' virtual data centers (VDCs) cater to diverse business needs and compliance requirements. With its impressive data protection and disaster recovery tools suite, VergeOS is a comprehensive solution for enterprises seeking to elevate their infrastructure resilience and operational efficiency.

