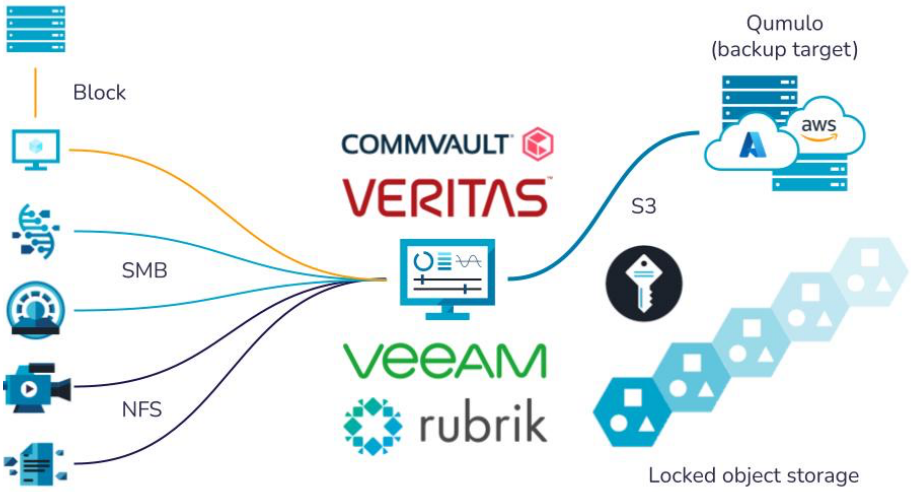
Qumulo

Solution Brief

Immutable data protection with Qumulo S3 storage

Data protection has always been a critical function of any enterprise – ensuring that business data can be recovered from hardware failure, site failure, inadvertent or intentional tampering or deletion. In the past few years, however, protecting data against ransomware attacks has become another critical component of any backup strategy, and modern backup solutions have been largely successful in minimizing data theft and business impact from cyberattacks.

Many ransomware vectors have now taken to attacking backup datasets directly – particularly backup images hosted on NFS or SMB storage – either deleting them outright or encrypting them and blocking any data recovery. Many backup vendors are now discouraging the use of file-based backup storage, recommending that enterprises use object storage instead for its stronger resistance to ransomware attacks.



Secure object storage with Qumulo

The Qumulo data platform's object support includes the enhanced security features encouraged by backup vendors: object locking to prevent backup datasets from inadvertent or malicious deletion; object versioning to prevent new backup data from overwriting older versions, and bucket-level controls that simplify the management of data retention at scale.

Limitless scalability

Whether on-premises or in the cloud, any single Qumulo data platform instance can scale to an exabyte or more or capacity, ensuring that you can meet the demands of even the longest retention periods. On-premises storage performance gets better as more capacity is added, while cloud-based Qumulo instances can scale to virtually any throughput level independent of used capacity.

Vendor compatibility

While Qumulo is well known as a large-scale file data platform, its support for object storage means that it's fully compatible as a backup target for enterprise backup software such as Commvault, Rubrik, and Veeam.

Object locking

Qumulo's object storage implementation includes the ability to lock data at the object level or at the bucket level, as well as object versioning, in which older versions of object data are retained even if the object itself changes. Since ransomware often targets enterprise backups as well as production data, these features prevent backup datasets from being compromised even in the event of a successful ransomware attack.

Store your backup data wherever you need it

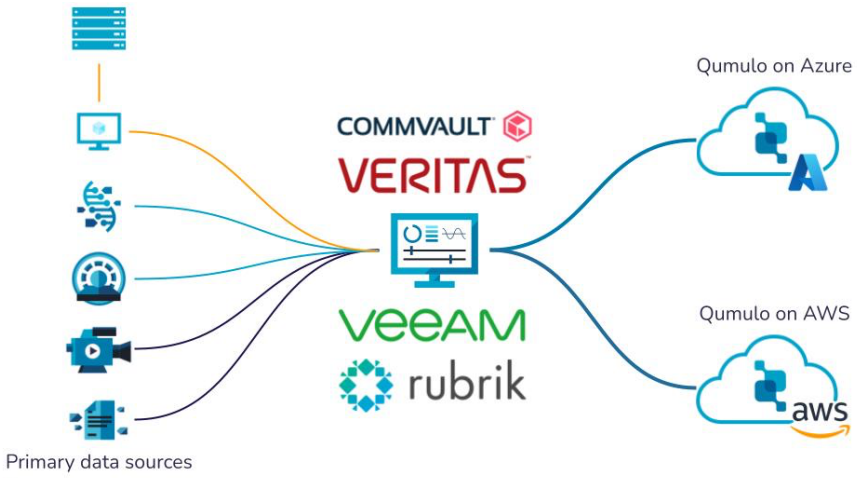
Whether you prefer to store your backup data on-premises or in the cloud, Qumulo is the only platform that combines the same secure, feature-rich object storage with the ability to scale to hundreds of petabytes on Azure, on AWS, or in the data center

High-performance data recovery

No matter where your Qumulo is deployed, it can easily support the throughput that your backup software needs – whether from the multiple concurrent backup streams needed to protect all your critical data sources, or when running high-speed restore operations to quickly recover lost data.

Azure Native Qumulo runs as a managed service. Cloud Native Qumulo can run on either Azure or AWS. Any cloud instance can be deployed and ready for use within minutes and offer the same support for file and object storage as an on-premises Qumulo cluster.

Every Qumulo cloud instance can scale to over 100GBps of throughput or over four million IOPS, so you can recover hundreds of TBs at high speed whether in the cloud or back to your on-premises storage.



According to a recent study by Veeam, an enterprise hit by ransomware in 2023 lost an average of 41% of production data to encryption or deletion. In the event of a successful ransomware attack, even a medium-sized enterprise could lose hundreds of terabytes of data that will need to be restored quickly.

For high-speed recovery of lost data, an on-premises Qumulo cluster sized to support a 1PB production data footprint can deliver over 50GBps across all nodes, ensuring ample throughput to recover lost data from backup while still leaving enough bandwidth to support any other active workloads that share the cluster – including active backup streams.

[1] "Ransomware Trends 2024: Lessons learned from 1,200 victims and 2,500 cyberattacks". Available at https://go.veeam.com/wp-ransomware-trends-report-2024.