TechTarget | Custom Media
White Paper

Multi-tenancy Everywhere: The Evolution of the Modern IT Department

The adoption of remote and hybrid work throughout the pandemic accelerated the digital transformation that IT organizations had already been undergoing by months, even years. However, as organizations shift between public and private clouds, the rise in data breaches and ransomware has prioritized the need for data protection and security.

pogo | Western Digital

The distribution of information workers coupled with the reliance on software-as-a-service means remote workers access the same data across different regions and domains.

Now that data is stored everywhere – data centers, public clouds, private clouds, applications, containers, file shares – the lack of control over corporate and private data is unprecedented, as IT departments are juggling a multitude of priorities for prevention and preparedness at the same time.

As a result, object storage has become widely-deployed in security-sensitive domains such as financial services, health care (hospitals and biosciences), government agencies and more.

The Rise of Object Storage

As workers accessed data between home and office locations throughout the pandemic, the need for greater control over data has increased. The immutability architecture of object storage, meaning data cannot be updated in place unlike with a file system, protects data from threats that can change data.

In addition, the ability of object storage to group resources from different SAN/NAS appliances together, gives IT decision makers the flexibility to modify corporate policies while maintaining compliance.

- **Unstructured Data** – Given the rapid growth of unstructured data content, object storage has become a common cornerstone of modern enterprise IT environments.
- **Multi-tenancy** – To service distinct users (or "tenants"), multi-tenant environments pack more customers on shared storage arrays, allowing IT directors to maintain access control and restrictions to virtualized applications or containers for AI/ML.
- **Authentication** – Strong authentication control-access and object-level encryption makes user data useless to criminals, while allowing it to be accessed by anyone, from any location.
- **Backups and Disaster Recovery** – Disk and tape have been the most popular media types for backups. But object storage is quickly becoming the preferred option, especially to organizations with large remote workforces.

The Increase in Ransomware Attacks

Ransomware attacks have become a threat beyond the industries with data privacy laws and backup regulations, and no sector is excluded. From agricultural producers to oil pipelines, ransomware attacks have increased exponentially since the start of the pandemic.

According to a recent study by Cybersecurity Ventures, attacks now occur globally every 11 seconds on average with ransomware and companies are paying – average payouts have exceeded $1.85M.

A key finding of a February 2022 Veeam Data Protection survey reported that 9 out of 10 respondents could not recover applications or restore data quickly to meet specified service-level agreements (SLAs)[1].

As recent data breaches have demonstrated, even companies that aren't directly attacked can be impacted. And that means no organization can ignore the rise of ransomware.

Based on these findings, 90% of organizations could not recover applications or data as quickly as they wanted, nor recover all the data they wanted.

Any organization with outdated security plans that don't address the overall shift toward cloud-based services to support flexible work environments are susceptible.

While ransomware attacks can take many forms, a common type involves encrypting user data with the threat that the data will be released (decrypted) or deleted if a ransom is not paid. Additionally, attackers continuously innovate their approach, which makes the prevention of ransomware an on-going challenge.

[1] "2022 Data Protection Trends Report", According to 3000+ business and IT leaders on their IT and data protection strategies surveyed by Veeam, February 22, 2022

How multi-tenancy assists the digital transformation

Technology departments experienced a boost in productivity through the adoption of public cloud methodologies, where storage, compute, and applications can be deployed on-demand. This increased agility has IT organizations looking for ways to deliver that same agility in their hybrid-cloud environments.

At the same time, diligence in security is needed to compartmentalize departments within larger organizations as "tenants", similar to how the public cloud operates, as this provides greater security and provides a mechanism for charge-back accounting to departments based on their use of compute and storage resources, just like the public cloud.

These two driving requirements for greater agility and security come together under the umbrella of multi-tenancy. In this white paper, we're going to focus mostly on the storage technologies that enable IT teams to implement multi-tenancy for their organizations.

What is multi-tenancy and how does it improve security and agility?

Multi-tenancy is a data center architecture approach that enables the hardware resources (compute, storage, networking) of a storage appliance to be easily shared between organizations and departments.

When deploying multi-tenant environments in object storage, resources can be divided into separate namespaces, or separate access to specific networks when deploying file and block storage.

To make multi-tenancy work there are key technologies that come into play at the network, storage, and compute level to bring it all together.

How does multi-tenancy play into the network architecture?

Large cloud service providers divide up customers into their own VLAN(s) so that all of their network traffic is separated from other customers (tenants) in the shared network and server environments.

When setting up the networking infrastructure for multi-tenancy it's important to choose switches with solid VLAN feature sets that'll scale efficiently with the datacenter.

How does multi-tenancy work with object storage?

Object storage systems generally provide Amazon S3™-compatible object storage so that applications written to use the S3-protocol can work using the exact same APIs using dedicated S3-compatible storage that's more cost-effective and performant.

One of the benefits of Ceph-based object storage systems used with platforms like OSNexus QuantaStor is that each tenant has their own namespace for all of their S3 “buckets”. This makes it easy to keep the storage for different customers and departments completely separate.

How does object locking in object storage feature protect against ransomware?

In a typical ransomware hack, attackers take over and encrypt an organization’s data, then charge a ransom to decrypt the data.

To protect their data, IT leaders need to make sure that hackers are unable to change their data. In object storage, object locking is a built-in immutability feature which prevents data from being changed or deleted.

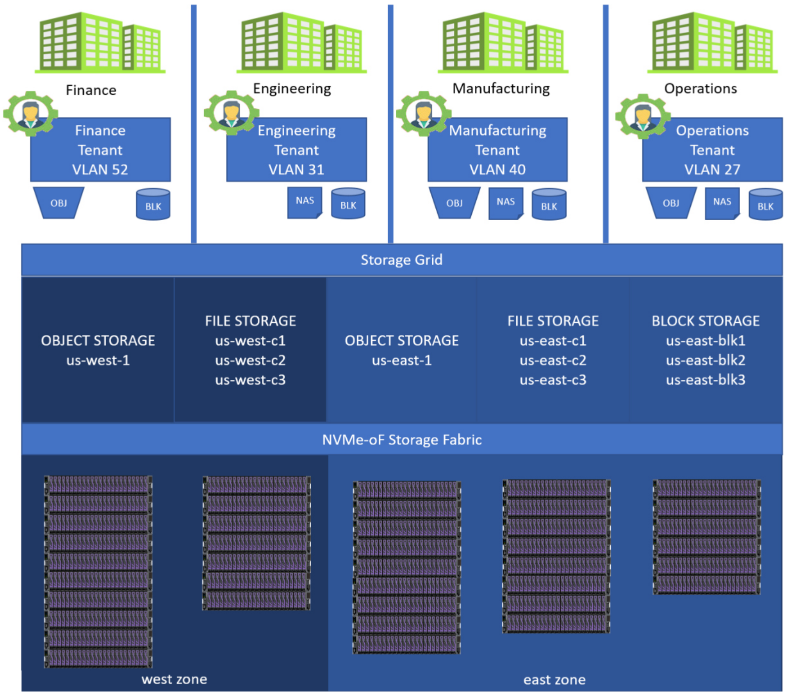
An important feature to enable for backups, object locking is configurable on a per “bucket” basis. Backup products like Veeam® leverage the object locking to ensure that your backups are not modified by hackers.

What is QuantaStor?

QuantaStor is a scale-out SDS platform that runs on all major server platforms. OSNexus is a member of the Ceph Foundation and incorporates open-source Ceph technology into QuantaStor as the basis for how it delivers object storage. QuantaStor extends the capabilities of Ceph by delivering a suite of security features, load balancing, hardware integration, monitoring, and many other features to deliver turn-key scale-out object storage, NAS, and SAN capabilities without the need for Ceph or Linux® expertise.

What key security features does QuantaStor bring as a SDS platform?

QuantaStor integrates with KMIP servers so that security keys for data encryption-at-rest can be stored centrally and separately from the storage cluster. QuantaStor supports both hardware (SED/Opal 2.0) and software encryption.


Finance
Engineering
Manufacturing
Operations
Finance Tenant VLAN 52
Engineering Tenant VLAN 31
Manufacturing Tenant VLAN 40
Operations Tenant VLAN 27
OBJ
BLK
NAS
BLK
OBJ
NAS
BLK
OBJ
NAS
BLK
Storage Grid
OBJECT STORAGE us-west-1
FILE STORAGE us-west-c1 us-west-c2 us-west-c3
OBJECT STORAGE us-east-1
FILE STORAGE us-east-c1 us-east-c2 us-east-c3
BLOCK STORAGE us-east-blk1 us-east-blk2 us-east-blk3
NVMe-oF Storage Fabric
west zone
east zone

QuantaStor is now FIPS 140-2 L1 certified and has features that help organizations comply with multiple security standards including NIST SP800-53, SP800-171, HIPAA and CJIS so that systems can be deployed in a broad spectrum of regulated environments.

Lastly, QuantaStor has a patented RBAC system that makes it easy to create custom roles for specific administrators so that IT teams can easily apply the 'principle of least privilege'.

QuantaStor integrates with LDAP and Active Directory for single-sign-on and SMB based NAS file sharing making it easy for IT teams to incorporate QuantaStor into their existing authentication systems.

How does QuantaStor deliver multi-tenancy?

QuantaStor provides multi-tenancy with S3-compatible object storage that can be logically separated into namespaces for each tenant. This enables complete separation of the S3 buckets so that different tenants are not able to access the data of another tenant or even list names of the buckets of another tenant.

Combined with object locking this enables IT teams to deliver secure object storage for a range of applications from backups, archive, AI/ML, and CDNs.

How does composable disaggregated infrastructure hardware play into implementing multi-tenancy?

As end-user or service requirements change, multi-tenant configurations have kept pace, benefiting from advances in storage innovation.

Secure multi-tenant environments that prevent ransomware or data loss must be processed and stored on the right hardware. Pogo Linux hardware solutions powered by Western Digital high-performance, low-latency NVMe™ storage and NVMe™-over-Fabrics networking technologies maximize the benefits that OSNexus QuantaStor can deliver.

Composable disaggregated infrastructure (CDI) enables IT organizations to dynamically add hardware resources (compute, storage, networking) on-demand as needs grow.

As a result, data center administrators no longer need to worry about available HDD slots in the servers, as additional capacity from NVMe-oF™ JBOFs can be added to any rack in the data center. This media can then be sent to any given storage cluster to easily expand those specific clusters as needs grow.

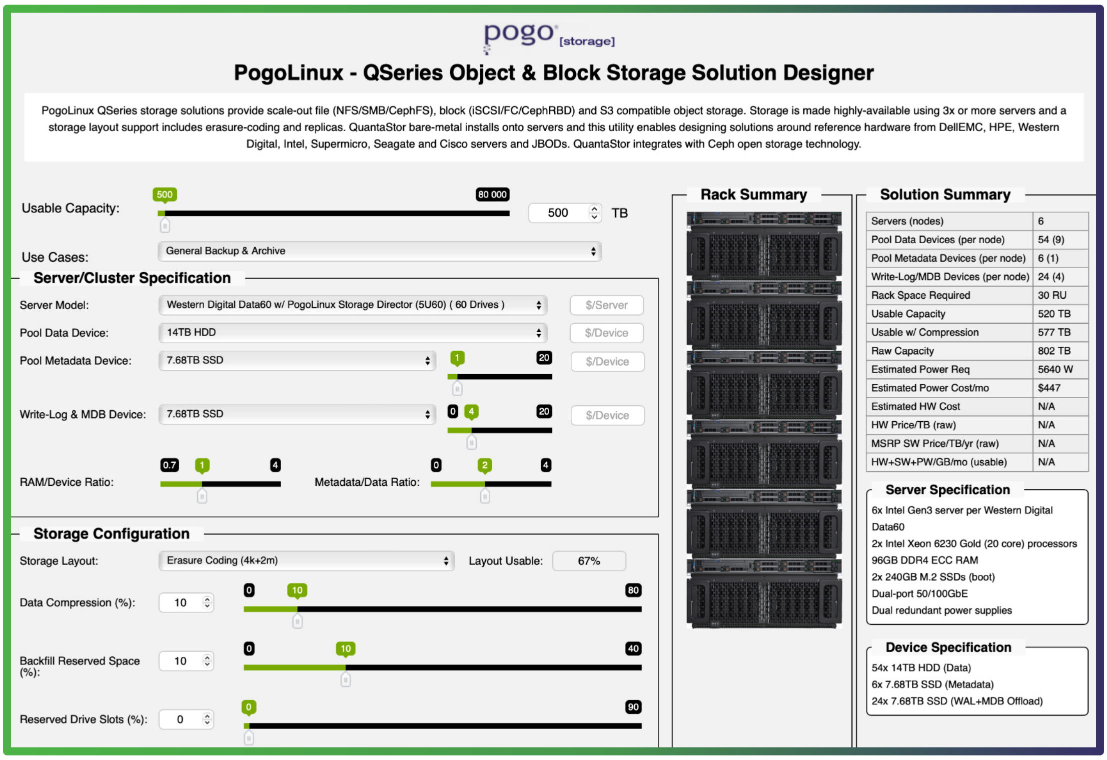
Western Digital is a leader in this space with the new OpenFlex™ Data24 . The Data24 is an ethernet attached all-flash NVMe-oF™ storage enclosure that enables one to dynamically expand the storage of any server on the network without having to reconfigure the servers.

How to design a multi-tenant object storage solution

Pogo Linux provides design assistance and a dedicated sales team as well as customized design tools to design reliable, scalable QuantaStor storage clusters on a variety of hardware platforms. A specialized version of the online design utility that includes the Western Digital Data24 as well as the other Western Digital disk enclosures like the Data60 and Data102.

QuantaStor object storage clusters can be deployed using all-flash media or a hybrid mix of NVMe™ and HDDs for greater cost efficiency at scale. For hybrid configurations about 2% to 3% of the total capacity of the cluster must be flash based with NVMe™ media preferred. The design utility ensures that the correct amount is allocated by showing a warning if the selected amount of flash storage is insufficient.

The best way to start with the design utility is to select the amount of usable capacity required, then select a use case from the available list. From there the hardware selection and other settings can be adjusted to optimize the solution for any given application.



PogoLinux - QSeries Object & Block Storage Solution Designer

PogoLinux QSeries storage solutions provide scale-out file (NFS/SMB/CephFS), block (iSCSI/FC/CephRBD) and S3 compatible object storage. Storage is made highly-available using 3x or more servers and a storage layout support includes erasure-coding and replicas. QuantaStor bare-metal installs onto servers and this utility enables designing solutions around reference hardware from DellEMC, HPE, Western Digital, Intel, Supermicro, Seagate and Cisco servers and JBODs. QuantaStor integrates with Ceph open storage technology.

Usable Capacity: 500 TB

Use Cases: General Backup & Archive

Server/Cluster Specification

Server Model: Western Digital Data60 w/ PogoLinux Storage Director (5U60) (60 Drives)

Pool Data Device: 14TB HDD

Pool Metadata Device: 7.68TB SSD — 1

Write-Log & MDB Device: 7.68TB SSD — 4

RAM/Device Ratio: 1

Metadata/Data Ratio: 2

Storage Configuration

Storage Layout: Erasure Coding (4k+2m)

Layout Usable: 67%

Data Compression (%): 10

Backfill Reserved Space (%): 10

Reserved Drive Slots (%): 0

Solution Summary

Servers (nodes)	6
Pool Data Devices (per node)	54 (9)
Pool Metadata Devices (per node)	6 (1)
Write-Log/MDB Devices (per node)	24 (4)
Rack Space Required	30 RU
Usable Capacity	520 TB
Usable w/ Compression	577 TB
Raw Capacity	802 TB
Estimated Power Req	5640 W
Estimated Power Cost/mo	$447
Estimated HW Cost	N/A
HW Price/TB (raw)	N/A
MSRP SW Price/TB/yr (raw)	N/A
HW+SW+PW/GB/mo (usable)	N/A

Server Specification

6x Intel Gen3 server per Western Digital Data60
2x Intel Xeon 6230 Gold (20 core) processors
96GB DDR4 ECC RAM
2x 240GB M.2 SSDs (boot)
Dual-port 50/100GbE
Dual redundant power supplies

Device Specification

54x 14TB HDD (Data)
6x 7.68TB SSD (Metadata)
24x 7.68TB SSD (WAL+MDB Offload)

Access the online design tool at https://www.pogolinux.com/scale-out

Pogo Linux Brings the Power of Multi-tenancy to Meet Data Center Agile and Secure System Needs

To accelerate the adoption of multi-tenant environments in the data center, OSNexus has partnered with Pogo Linux and Western Digital to provide organizations with an integrated hardware and software solution. Within minutes, data center users with a diverse range of data protection and security breach protection requirements can quickly deploy highly-scalable, high-performance QuantaStor object storage cluster solutions and expansion nodes on industry-standard hardware.

The Pogo Linux StorageDirector appliances deliver a turn-key unified cluster management solution that's optimized for QuantaStor to ensure fluid business continuity and peace of mind without sacrificing performance and scalability. While Ceph replicates data to make it fault-tolerant for migration purposes, QuantaStor's integrated hardware management actively-monitors key Pogo Linux hardware elements, including HDD and flash storage health, power supply, fans and thermal temperature.

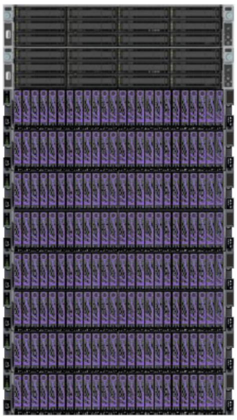
Scale-Out StorageDirector

Western Digital
OpenFlex Data24 NVMe
Based scale out architecture

QuantaStor with SAS, NVMe and NVMe-oF

Scale-Up StorageDirector

Western Digital Data60/102
based scale-up architecture



Western Digital Data24 NVMe
based composable architecture

QuantaStor with SAS, NL-SAS and NVMe

The StorageDirector's deep hardware integration with Intel's third-generation Cascade Lake Xeon processors, DDR4 memory and high-capacity Western Digital NVMe™ flash SSDs and NVMe-oF™ technologies, provides mass storage capability that can be easily expanded when needed. Pogo Linux StorageDirector scale-out and scale-up solutions can be configured for high-availability using three (or more) QuantaStor appliances in a storage layout that's designed to support erasure-coding.

Wherever users access data or wherever the data is stored, the Pogo Linux Storage Director delivers purpose-built security for backups and recovery to prevent security breaches in the post-pandemic data center.

To learn more about the Pogo Linux multi-tenancy object storage solutions, visit:

https://www.pogolinux.com/products/osnexus/overview

This content was commissioned by Western Digital and produced by TechTarget Inc.