Gartner®

Hype Cycle for Storage and Data Protection Technologies, 2023

Published 13 July 2023 - ID G00790904 - 82 min read

By Analyst(s): Julia Palmer

Initiatives: I&O Platforms

This Hype Cycle focuses on emerging innovative storage and data protection technologies and assesses their business impact, adoption rate and maturity level to help I&O leaders build adaptable, future-ready storage and data protection platforms for changing business needs.

Strategic Planning Assumptions

By 2026, large enterprises will triple their unstructured data capacity across their on-premises, edge and public cloud locations, compared to 2023.

By 2026, 60% of I&O leaders will implement hybrid cloud deployments, which is a significant increase from 20% in 2023.

By 2026, 25% of external enterprise storage arrays deployed to support primary storage workloads will adopt nonvolatile memory express over fabric (NVMe-oF), compared with less than 10% in 2023.

By 2026, more than 40% of enterprise storage will be deployed at the edge, which is a significant increase from 15% in 2022.

By 2028, consumption-based STaaS will replace over 35% of enterprise storage capex, up from less than 10% in 2023.

Analysis

What You Need to Know

The storage and data protection market is evolving to address new challenges in enterprise IT. Exponential data growth, public cloud integration, talent acquisition challenges, new workloads and cyberthreats are demanding changes in storage platforms and operational models. Requirements for robust, secure, simple and performant storage are on the rise. In addition, the storage and data services must be scalable and sustainable. As data centers are no longer the centers of data, I&O leaders expect to deliver storage services and data platforms capable of hybrid cloud data flow at the edge and in the multiple public clouds.

As technology continues to advance, it's crucial to stay informed about the latest trends and innovations in storage and data protection. In this research, Gartner has assessed 23 of the most hyped storage and data protection technologies that are reshaping how we store and manage data, offering faster performance, scalability, cloud integration and enhanced flexibility.

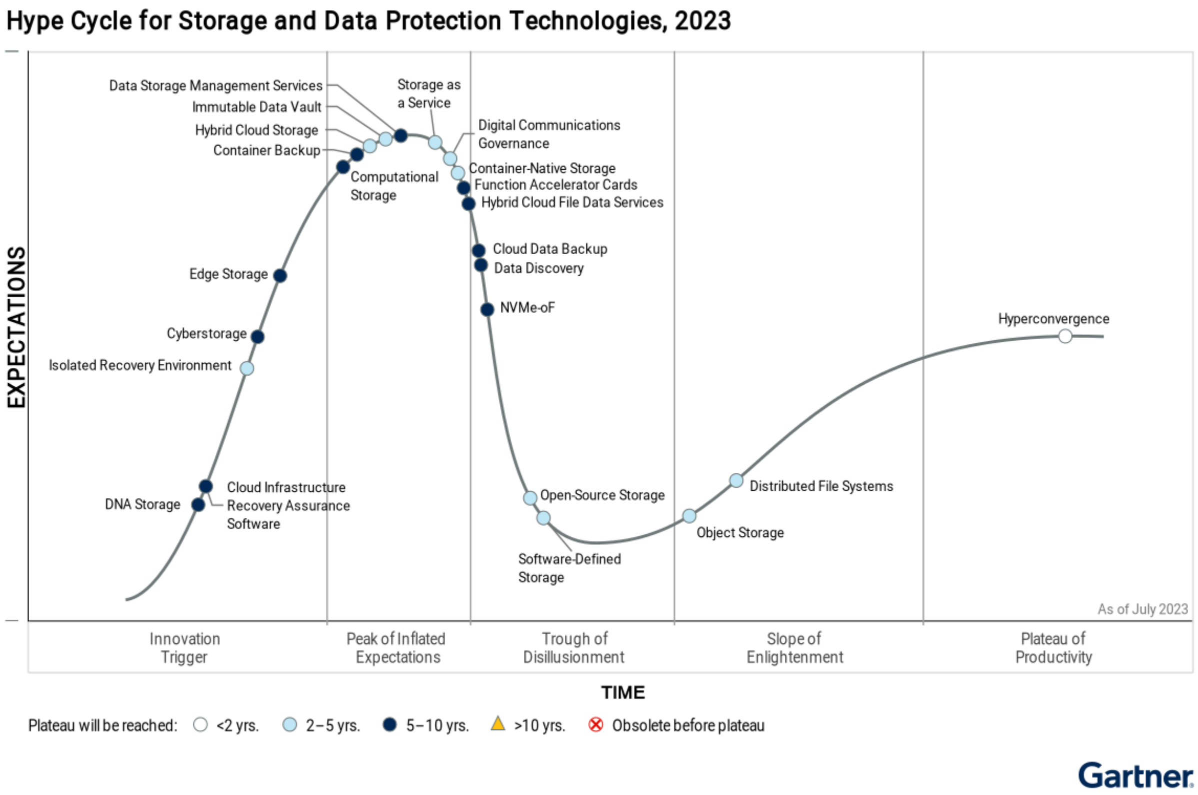
The Hype Cycle

I&O leaders responsible for storage and data protection are reacting to the changing requirements of digital business, unpredictable data growth, introduction of new workloads and the desire to leverage public and hybrid cloud that include core-to-edge capabilities. This research informs I&O leaders and infrastructure technology vendors about innovative storage technologies and assesses their business impact, maturity level and how quickly enterprises are adopting them.

More than half of the technologies reviewed in the 2023 Hype Cycle are poised to mature during the next five to 10 years. At the same time, 65% of technologies have the potential to deliver major benefits if driven and justified by genuine business requirements. To provide clearer, more focused research to support your analysis and planning, we have only included a subset of the most innovative technologies and removed those that are well-adopted and understood.

In 2023, Gartner observed a high concentration of technologies at the peak of the hype addressing the most prominent market trends such as hybrid cloud, containers support, data management and as-a-service offerings. This year, enterprise information archiving and copy data management were dropped as they are well understood and adopted. Storage-class memory SSDs and persistent-memory DIMMS were dropped as they are no longer hyped or promoted. Fast-moving technologies include function accelerator cards and hybrid cloud storage. This year, Gartner introduced five new profiles: DNA Storage, Cloud Infrastructure Recovery Assurance Software, Isolated Recovery Environment, Digital Communication Governance and Storage-as-a-Service.

Figure 1: Hype Cycle for Storage and Data Protection Technologies, 2023



The Priority Matrix

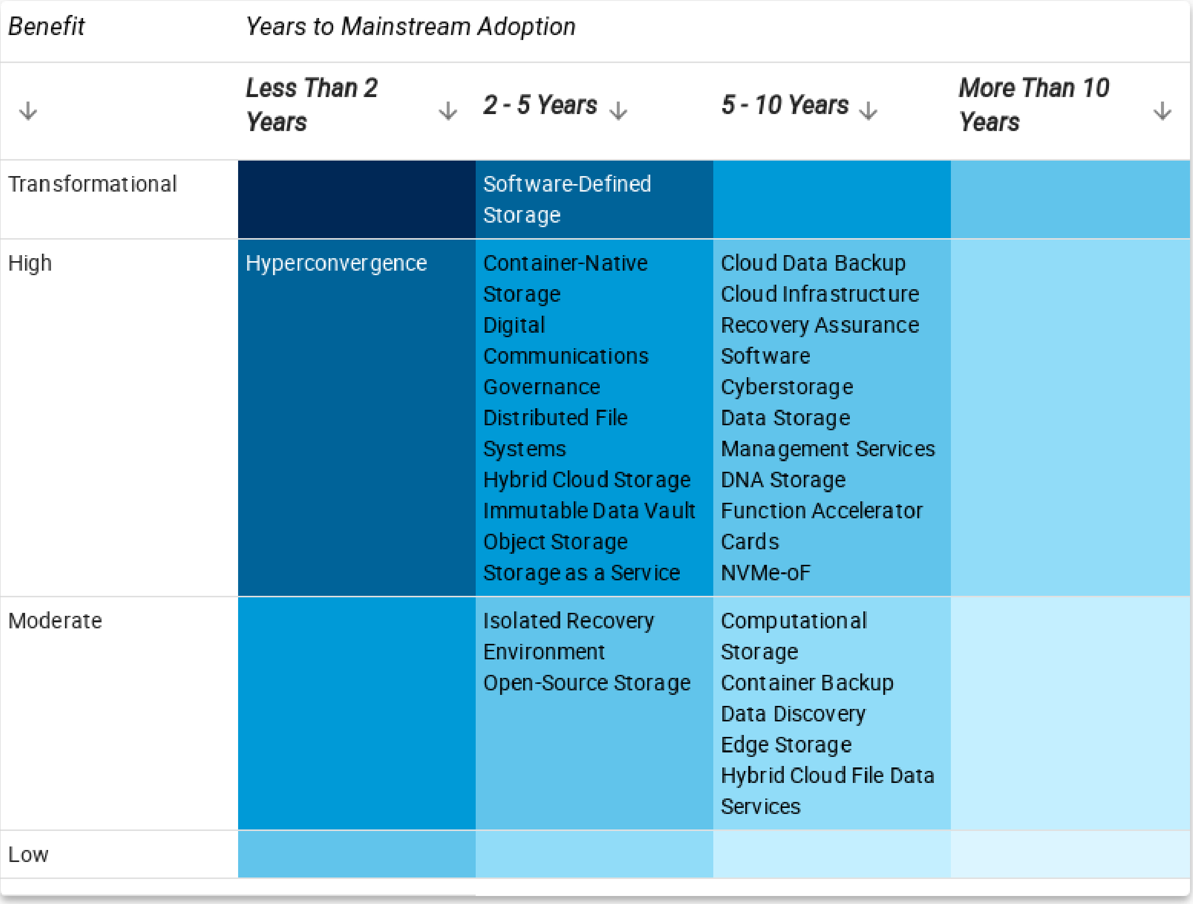
The Priority Matrix maps the benefit rating for each technology against the length of time before Gartner expects it to reach the beginning of mainstream adoption. This alternative perspective can help users prioritize their storage hardware; software and data protection technology investments; and adoption.

In general, companies should begin with fast-moving technologies that are rated transformational or high in business benefits and are likely to reach mainstream adoption quickly. These technologies tend to have the most disruptive impact on business processes, revenue or cost-cutting efforts. After these transformational technologies, users are advised to evaluate high-impact technologies that will reach mainstream adoption status in the near term.

Organizations that have not already done so should evaluate and implement hyperconverged infrastructure, distributed file systems and object storage. I&O leaders should consider implementing hybrid cloud storage, edge storage, cloud data backup and hybrid cloud file data services to address the growing needs of data on-premises and in the cloud. Due to the increased focus in storage security, I&O leaders are increasingly evaluating Cyberstorage, Isolated Recovery Environment, Immutable Data Vault products and capabilities that are designed to detect, prevent and recover from ransomware attacks.

Table 1: Priority Matrix for Storage and Data Protection Technologies, 2023

(Enlarged table in Appendix)



Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		Software-Defined Storage		
High	Hyperconvergence	Container-Native Storage Digital Communications Governance Distributed File Systems Hybrid Cloud Storage Immutable Data Vault Object Storage Storage as a Service	Cloud Data Backup Cloud Infrastructure Recovery Assurance Software Cyberstorage Data Storage Management Services DNA Storage Function Accelerator Cards NVMe-oF	
Moderate		Isolated Recovery Environment Open-Source Storage	Computational Storage Container Backup Data Discovery Edge Storage Hybrid Cloud File Data Services	
Low				

Source: Gartner (July 2023)

Off the Hype Cycle

The following technologies have been removed because they have reached maturity and are no longer hyped:

- Copy Data Management
- Enterprise Information Archiving
- Storage-Class Memory SSD
- Storage-Class Memory DIMMS

On the Rise

Cloud Infrastructure Recovery Assurance Software

Analysis By: Jerry Rozeman, Michael Hoeck

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cloud infrastructure recovery assurance software (CIRAS) solutions help cloud infrastructure as a service (IaaS) customers improve backup and disaster recovery (DR) posture by automating the capture of cloud IaaS and platform as a service (PaaS) configurations, integrating with its own or cloud-native replication capabilities and providing orchestrated backup and DR of homogeneous cloud services, in or across different locations and accounts.

Why This Is Important

Applications that use cloud IaaS and PaaS typically use a complex web of multiple service elements, each of which has its own configurations. Due to the dynamic nature of the cloud and their failures, most customers are unlikely to declare a regional failover without having invested in continuous dependency mapping/graphing, configuration management and automation. CIRAS solutions help organizations address these needs by capturing and orchestratiing recovery as part of the protection strategy.

Business Impact

Backup, DR and continuous availability are not provided “automagically” in public cloud IaaS and PaaS. CIRAS solutions’ application-infrastructure-centered approach orchestrates protection of the associated configuration files and automates recovery across different cloud services. The goal is the recovery of the entire application environment, rather than discrete, individual application components and their data.

Drivers

- Cloud adoption for critical applications continues to grow, as does the realization that DR isn’t provided automagically for those implementations.

- Cloud configuration drift — due to the ease of adding applications to the cloud — results in complexity and the inability to restore to a well-known state. In addition, sprawl occurring to cross-cloud configurations might create even more complexity.

- Cloud services providers lack comprehensive, plug-and-play orchestration and resilience features to easily fail over a complete application.
- Enabled by the self-service capabilities of CSPs, application developers do not consistently implement complete backup/DR solutions.
- Leading backup vendors traditionally focus on protection of an application and its data, not cloud configuration management or application dependence.

Obstacles

- Only a handful of new vendors have solutions aimed at addressing this complexity.
- CIRAS solutions face similar challenges as cloud management platform (CMP) providers experienced years ago in terms of being able to support the range of services provided by any cloud provider.
- The lack of industrywide recognition for this problem complicates the addressability of this risk.
- Mature customers who have already addressed the problem by adding configuration capabilities might not see the need to invest or will build the capabilities themselves.
- A significant percentage of organizations will continue to take recovery of cloud workloads for granted, or overestimate their ability to execute a failover.
- Customers with aggressive recovery time objective (RTO) requirements might need different solutions to address warmer standby capabilities.
- CSPs might build these capabilities themselves.

User Recommendations

- Ensure that internal stakeholders understand the need for recovery capabilities and appreciate the complexities associated with it.
- Build a recovery strategy to holistically protect and recover cloud applications, their configurations and related services.

- Document cloud application implementations, including all dependency services and their configurations for recovery perspectives.
- Evaluate CIRAS vendors as to the degree they support the cloud providers and associated services you leverage, including virtual instances, databases and load balancers, as well as PaaS, identity and access management (IAM), etc.
- Document RTOs and recovery point objectives (RPOs) and assess against CIRAS capabilities.
- Evaluate CIRAS vendors, in addition to your existing data protection tools, and make this a build-or-buy decision.

Sample Vendors

Appranix; Arpio

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

9 Principles for Improving Cloud Resilience

Quick Answer: Can My Disaster Recovery Plan Also Address Ransomware Recovery?

Market Guide for Disaster Recovery as a Service

DNA Storage

Analysis By: Matthew Brisse

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Deoxyribonucleic acid (DNA) data storage is the process of encoding and decoding binary data to and from synthesized strands of DNA. Any binary sequences can be encoded in DNA sequence, which can then be synthesized and stored. To retrieve the data, the DNA molecule must be sequenced and decoded. DNA is emerging as an increasingly attractive medium for the archiving of data, due to its superior density, durability and sustainability.

Why This Is Important

- DNA data storage is important, due to its density, durability and sustainability; it addresses long-term data retention and sustainability needs.
- DNA performs error checking and self-repair, making it an ideal data storage medium and computing platform for applications.
- DNA data storage has a long-term, cost-reduction impact on physical data center space, carbon-dioxide emissions and the avoidance of operating expenditures (opex), by not having to refresh the technology every five to 10 years.

Business Impact

As DNA storage matures, its impact could be transformational for data storage, parallel processing and computing. Adoption of a complete DNA ecosystem as a consumable enterprise product is likely to occur at approximately eight years for data-intensive industries that are often first movers among new technology. The domains include healthcare banking, finance, insurance, utilities and government. The defense, research and intelligence communities are the most likely to be early adopters.

Drivers

- Future DNA data storage use cases will focus on power and space-sensitive, long-term storage requirements.

- Once DNA storage is written to, synthetic strands of DNA digital data require minimal storage space and almost no power. In theory, they can be accessed for thousands (if not millions) of years by a variety of devices in a future-proof manner, with no necessity of data migration.

- Long-term operational costs are reduced, because data migrations due to technology obsolescence or data degradation will not be issues with DNA-based storage.

- The business drivers for DNA-based data storage are density, stability, durability, sustainability and long-term operational cost.

- The world creates several hundred petabytes of new data every day, and a single gram of DNA could store all of it. One gram of DNA can store approximately 215 petabytes of data with a minimum life span of hundreds to, theoretically, thousands of years.

- DNA data storage will have a power efficiency profile that could significantly reduce the physical infrastructure space and the carbon-dioxide footprint over the life of the data.

- Data in DNA storage can endure for thousands of years and remain unchanged, free from degradation or drive failure, compared with current technologies.

- In the future, DNA data storage will be used in combination with DNA computing for extremely large, massively parallel, processing use cases.

Obstacles

- DNA technologies face many of the same challenges as any other startups early in their life cycles: speed, time to market, standards and cost.
- DNA data storage patents are likely to cross industry segments, making patents and licensing agreements challenging. IP submissions accelerate when a market matures, so expect increased numbers of investors.
- The creation of synthetic DNA, the medium that will store data as DNA, needs to become efficient and cost-effective.
- Access speeds and throughput rates for DNA data storage must dramatically improve to compete with classical approaches. DNA self-assembly and other similar processes are essentially chemical reactions, which are much slower, compared with today's classical approaches.
- Data security and regulatory challenges will be an issue, because DNA will someday store personal, sensitive and classified materials.
- The industry needs to develop and accelerate standards on the automation of DNA data storage and the associated retrieval processes.

User Recommendations

- Prepare for increased hype as technologies mature, realizing that DNA data storage is nascent. Savvy organizations will see through the hype to the practical use-case initiatives DNA storage offers.
- Focus on due diligence of startup companies, and align risks with the justification of use-case returns.
- Avoid long-term lock-in with early providers. Startups will emerge and fail until technologies mature, and winners and losers are identified.
- Anticipate difficulties in the development of DNA data storage. Explore the promise of near-infinite, enterprise-grade, reliable, durable capacity at a fraction of the cost of conventional enterprise-grade media.
- Prioritize DNA storage for early use cases, when available, focusing on write-once, read-never or write-once, read-seldom, if ever large-scale datasets.
- Evaluate DNA data storage viability by gauging when storage prices fall to three to four orders of magnitude the cost of tape archival, and when write speeds reach the megabit/second range.

Sample Vendors

Ansa Biotechnologies; CATALOG; DNA Script; Helixworks Technologies; Iridia; Kilobaser; Molecular Assemblies; Spectra Logic; Twist Bioscience

Gartner Recommended Reading

Emerging Tech Impact Radar: Compute and Storage

Top Trends in Building a Digital Future: Next-Gen Computing

Isolated Recovery Environment

Analysis By: Jerry Rozeman, Michael Hoeck

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

An isolated recovery environment (IRE) is a dedicated and secure environment equipped with resources to verify and recover operating systems, applications and data from an immutable backup copy. The IRE is used to recover data in a secure environment, independent of the production environment, because hackers may still have access to the latter.

Why This Is Important

Ransomware attacks are destructive because they take down production, encrypt critical data and may steal sensitive data, resulting in massive financial and reputational damage for organizations. IREs are an essential part of cyberresilience initiatives, since they help in performing analysis and recovery of operating systems, application code and data in secure isolation.

Business Impact

Organizations can leverage IRE to:

- Accelerate recovery from ransomware attacks by allowing restored activities to begin before the production environment is deemed ready for restoration.
- Utilize the opportunity to clean infected data following restoration, minimizing the risk of reintroducing the attack into production.
- Provide the highest level of security and recovery against insider threats, ransomware and other forms of hacking by combining IREs with immutable data vaults (IDVs).

Drivers

- By 2025, at least 75% of IT organizations will face one or more ransomware attacks, as free-rein researchers continue to show a dramatic increase in such attacks since 2020, pointing to sevenfold, or higher, rate of growth.

- The time it takes to recover from a cyberthreat, such as ransomware, is unacceptable for most organizations. To address this, many organizations are prioritizing recovery processes as part of cyberresilience initiatives.

- Ransomware response plans may prohibit access to and recovery of impacted systems during forensic investigations, slowing efforts to begin restoration and cleansing efforts.

- Extensive planning and implementation of new recovery strategies for ransomware attack is a requirement based on the frequency of such attacks (if it is high) and the catastrophic impact of a single attack on an organization.

- Recovery from ransomware is complex and requires a dedicated recovery plan, which is different from traditional disaster recovery.

- Traditional backup and recovery plans and runbooks are not designed for ransomware recovery.

- Cyberattacks purposely target traditional backup and recovery solutions to prevent recovery efforts.

Obstacles

- Dedicated IREs can become very expensive due to the equipment, software, skills and additional resources needed to operate.

- IREs are not a single technology, they require a unified solution approach where multiple technologies need to be integrated and operated to deliver the expected quality and outcomes.

- While an IRE offers an additional layer of protection, recovery processes can be complex without extensive planning.

- IREs are not meant for recovery at scale but for the recovery of most-critical systems.

- Scoping which critical systems to include in the IRE is a challenge as stakeholders vie for priority.

User Recommendations

- Create a dedicated ransomware recovery strategy, in addition to your traditional disaster recovery plans.
- Create a secure, isolated and dedicated recovery environment that prioritizes restoration of data and services as part of organizationwide cyberresilience.
- Align expectations and acceptable risks to the current backup and recovery solution capabilities by conducting a thorough risk assessment.
- Prevent overengineering when selecting an IRE by evaluating benefits, challenges and alternatives first, as the solution will require significant additional investment and broad expertise to implement and manage.
- Implement an IRE selectively by choosing it for the most critical business applications only and complement it with modern backup solutions.
- Optimize recovery speed by implementing IREs in close proximity to production systems.
- Confirm the effectiveness of your recovery environment by conducting exercises that test your environment's performance amid the conditions of an attack.

Sample Vendors

Cobalt Iron; Dell Technologies (Dell EMC); Veritas; VMware

Gartner Recommended Reading

Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware

Quick Answer: Can My Disaster Recovery Plan Also Address Ransomware Recovery?

Restore vs. Rebuild — Strategies for Recovering Applications After a Ransomware Attack

Designing and Implementing a Ransomware Defense Architecture

How to Build a Secure Environment to Recover From Ransomware and Other Cyberattacks

Cyberstorage

Analysis By: Jerry Rozeman, Julia Palmer

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Cyberstorage offers an active defense of the storage systems and their data against cyberattacks through prevention, early detection and blocking of attacks, and aids in recovery through analytics and storage-specific recovery capabilities. Cyberstorage can be a dedicated storage solution containing all capabilities, a platform solution containing multiple products offered as an integrated solution, or independent products that add cyberspecific capabilities toward storage vendors.

Why This Is Important

Ransomware attacks are increasingly common and disruptive, requiring the adoption of cybersecurity tools for active defense and recovery. Although numerous solutions are available for endpoint protection, object, file system and block storage systems provide inadequate protection from malicious downloads, deletion, destruction, or encryption of data. Cyberstorage provides active defense and recovery against cyberattacks on storage systems and their data.

Business Impact

The impact of a cyberattack can be enormous and destructive. Ransomware attacks can completely wipe out or encrypt all your systems, taking down all productivity. Cyberstorage aids in prevention and recovery capabilities to protect storage systems against these disasters minimizing the impact and dependency on full recovery from backup systems.

Drivers

- Tripling of unstructured data capacity across on-premises, edge and public cloud locations increases the need for better protection by implementing cyberstorage against cyberthreats such as ransomware.
- Large file repositories are the easiest to attack for both ransomware and data extortion as hackers leverage elevated credentials to access standard network access protocols such as Server Message Block (SMB) and Network File System (NFS).
- Protecting and recovering from a ransomware attack requires a multifaceted strategy that includes multiple market solutions such as endpoint protection, immutable enterprise backup, and data storage infrastructure detection analytics and recovery as part of cyberstorage solutions.
- Overall security management for file and block storage infrastructure can improve for both capability, and management from a governance perspective as it is the backdoor for hackers.
- Storage being the backdoor for hackers, requires improved overall security and enhanced cyberprotection.
- Encryption at rest does not solve the issue for ransomware through data extortion as data remains unencrypted on the storage access site driving the need for better storage security.

Obstacles

- Ideally, cyberstorage features should be integrated into the data storage system. However, this requires organizations to switch to another storage vendor as the most widely deployed products do only offer limited cyberstorage capabilities.
- Switching data storage vendors is not an option for many companies because of complexity and existing investments.
- Most advanced cyberstorage solutions are offered by smaller and younger companies where existing enterprises have to deal with the challenge of dealing with startups.
- Add-on software solutions or appliances will offer less physical protection to the unstructured data solution but are an easier add-on to the existing environment.

User Recommendations

- Prioritize active protection and security of unstructured and structured data storage systems because limiting or blocking an attack is more effective than recovering from one.
- Review storage vendors' cyberstorage features such as ransomware detection, blocking the attack, advanced recovery and analytics functions and improved overall security hardening into their storage products. Ask for the vendors' roadmap and validate if they support the National Institute of Standards and Technology (NIST) framework standard.
- Watch cyberresilience products and capabilities carefully. Do not see cyberresilience products and capabilities as an alternative to backup or disaster recovery; they are an additional layer of protection.

Sample Vendors

BullWall; Cohesity; Continuity; Dell Technologies; IBM; NetApp; Nutanix; ProLion; RackTop Systems; Superna

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Innovation Insight for Cyberstorage Solutions to Protect Unstructured Data Against Ransomware

2022 Strategic Roadmap for Storage

Edge Storage

Analysis By: Julia Palmer

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Edge storage enables the creation, analysis, processing and delivery of data services at, or close to, the location where the data is generated or consumed, rather than in a centralized environment. Edge storage can be deployed at regional or remote data centers, aggregation points, edge servers and edge gateways. Edge storage is not being delivered by a single technology, because it must be tailored to the specific edge computing use cases.

Why This Is Important

Infrastructure and operations (I&O) leaders are beginning the process of laying out a strategy for how they intend to manage data at the edge. Although I&O leaders embrace infrastructure as a service (IaaS) cloud providers, they also realize that a significant part of the infrastructure services will remain on-premises, and would require edge storage data services.

Business Impact

I&O leaders are changing up their storage strategies as edge computing becomes a critical part of an overall cloud-connected data center transformation. This is driving I&O leaders to change their role from the providers of infrastructure to providers of data services everywhere. With that in mind, I&O leaders are resetting their storage strategies and vendor selections for all deployments outside the public cloud infrastructure, focusing on specific data services for the edge.

Drivers

- As cloud migration continues, the infrastructure and operations team is transforming from the provider of data center infrastructure to the provider of the data services everywhere, focusing on select use cases that require storage at the edge. The four most popular use cases at the edge are distributed cloud/data center, data processing at the edge, content collaboration and access, and data ingest and streaming.

- Data services at the edge require many factors that preclude deployment in the public cloud: data gravity, cloud and bandwidth costs, application-specific data latency, and the effects on throughput of the speed of light. This is in addition to data security, data autonomy and data governance.

- Edge storage services are emerging for latency sensitive and bandwidth-intensive workloads that aren't ideally suited for the public cloud or the core data center. Examples of such workloads include real-time data processing, collaboration and the synchronization of massive amounts of data with online storage.

Obstacles

- I&O organizations struggle to determine what actions should be taken now, as opposed to taking a wait-and-see attitude and planning to optimize their IT operating models to mitigate risks and avoid pitfalls that may jeopardize efforts at the edge.

- The diversity of use cases, workloads, volume of data and unique infrastructure requirements at the edge introduces the potential for issues in system management, costs, security and resilience factors.

- Edge storage is not a single technology, because it needs to be tailored to the specific use cases.

User Recommendations

- Create edge storage platform initiatives by identifying edge-centric workloads, use cases and data service management methods.
- Choose an edge storage topology and platform approach by addressing unique workload requirements that are self-healing, software-defined and power-efficient, and can be elastically scaled up and down cost-effectively.
- Prepare for any new enterprise data center storage deployment to be edge-ready, by prioritizing requirements for the edge operating model and public cloud integration.
- Select edge storage products and technologies that focus on addressing key challenges, such as autonomous operations, centralized data management, performance density and data transfer optimization.

Sample Vendors

AWS; Dell; Hivecell; HPE; LINBIT; Microsoft Azure; Nutanix; SoftIron; StorMagic; VMware

Gartner Recommended Reading

Innovation Insight: Rethink Your Enterprise Storage and Cloud Data Services Strategies for the Edge Awakening

Competitive Landscape: Hyperscale Edge Solution Providers

Market Guide for Hybrid Cloud Storage

Predicts 2023: Edge Computing Delivery and Control Options Extend Functionality

At the Peak

Computational Storage

Analysis By: Jeff Vogel, Julia Palmer

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Computational storage (CS) is a storage architecture involving sophisticated processing capabilities on the storage device. It provides storage functions to offload host processing or reduce data movement from the main memory of the CPU to the storage device. CS products employ greater processing power through field-programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs) with low-power CPU cores on the solid-state drive (SSD).

Why This Is Important

CS is a class of storage architecture that provides consistent performance for latency-sensitive applications, such as AI and machine learning (ML), high-performance computing, immersive and mixed reality streaming, and high-frequency trading on-premises and at edge workloads. The CS architecture enables parallel computation and alleviates existing compute memory, storage and input/output (I/O) constraints. CS solves the data movement issue associated with storage.

Business Impact

The low-power footprint of CS improves the performance-per-watt ratio and decreases power consumption costs for edge applications supporting distributed processing and power efficiency. By using a more powerful compute engine with the SSD controller, CS systems can increase storage efficiencies and lower application costs. They can be a great green initiative with edge applications. CS engines can substantially reduce processing time, and improve compression and other critical drive functions.

Drivers

- Reduces performance inefficiencies, energy consumption and latency-sensitive issues in the data movement between storage and application compute resources.

- Processes and analyzes where data is generated and stored, thus empowering users to extract actionable insights at the device level.
- Reduces latency with edge workloads as data volumes increase and data movement becomes a bottleneck or increases complexity.
- Eliminates application performance issues that require data movement when the dataset size exceeds memory.
- Allows for a set of applications and tasks to be run without host involvement.
- Removes bottlenecks in data-intensive applications such as AI and ML, databases, high-performance computing, analytics, high-frequency trading, and immersive- and mixed-reality streaming.

Obstacles

- CS systems are based on a fundamentally new architecture that is complex and may require applications to be recompiled.
- The services provided by the CS system may require additional APIs or increased awareness of the host system.
- Operational tasks will need to be offloaded into the SSD drives, so host applications must be able to adequately communicate with CS storage drives.
- CS systems require a software framework that enables a host server application to interact with a CS device. This software must be based on an open and standard framework that is being actively worked on.
- CS systems are still relatively nascent. The value of what’s being offered is sometimes difficult to justify.
- Several leading vendors are startups and depend upon outside funding to scale. The lack of established, leading SSD vendors remains problematic for widespread adoption.

User Recommendations

- Explore potential benefits provided by specific use cases such as encryption, video encoding, and AI and ML facial recognition. However, calculate the cost versus performance gains against operating expenditure (opex) savings and the amount of work required for deployment and management. This is especially important where workloads are very input- and output-bound and would benefit the most from processing in storage.
- Determine which compression or decompression engines enable the drive to store more data per gigabyte of flash and maintain high performance within a narrow band, regardless of the read or write mix.
- Perform sufficient vendor due diligence, as each vendor has a slightly different approach to design and implementation.
- Determine whether the selected vendor can support your requirements, as the vendor landscape may include small startups not sufficiently funded or staffed to support large-scale application demands.

Sample Vendors

Arm; Eideticom; IBM; NETINT Technologies; NGD Systems; Pliops; Samsung; ScaleFlux

Gartner Recommended Reading

Emerging Tech Impact Radar: Compute and Storage

2022 Strategic Roadmap for Storage

Container Backup

Analysis By: Jerry Rozeman

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Container backup helps back up persistent volumes of containerized application data and Kubernetes configuration data like K8S objects. Container backup solutions are offered either as part of a traditional backup solution, as part of the primary storage solution or as a containerized application.

Why This Is Important

Container backup is an emerging and largely nascent technology that protects organizations against data and configuration loss in a containerized environment. It is different from a physical or virtual machine (VM) backup as there is no direct mapping between the application and the underlying storage.

Business Impact

Container backup can help:

- Business owners responsible for application data in addressing the data and application configuration loss risk associated with containerized application environments, because such protection is not available by default.
- Platform and application engineering teams in protecting their data as they become the new owners responsible for containerized application data protection.

Drivers

- Containerized application adoption will increase at a rapid pace during the next few years primarily driven by the rapid growth of cloud adoption, application modernization leveraging containerization and the need for application mobility. This will fuel the need to protect data in these environments.
- There is a steady increase in use of containers to run stateful applications — the 2022 CNCF Annual Survey shows that over 63% of respondents are running stateful applications in containers in production (an increase from 55% in the 2020 CNCF Annual Survey).
- DevOps processes require tight integration with backup tools that support Kubernetes and can be embedded in the continuous integration/continuous delivery (CI/CD) workflow. Container backup solutions can deliver on this need by delivering data management features that are configured with declarative and immutable artifacts.
- Recovery strategies designed for physical infrastructure and virtual machines (virtualization) don't work well with containers and Kubernetes.

Obstacles

- Data protection of new workloads has always been an afterthought and that especially applies to container-based applications.
- While container technology seems like the next evolution of server virtualization, the technology and operating model are completely different compared to operating and protecting VMs and hypervisors.
- Container technology requires new buyers in application or DevOps teams who do not see backup to be as high a priority as the infrastructure team does.
- It will still take a long time for the majority of organizations to move away from traditional hypervisors and VMs to container technology in production. This limits the growth potential of container technology and as such it will limit the growth of data protection in containerized environments.
- The current ecosystem for container backup is quite overcrowded with a lack of standards, while demand is running behind.

User Recommendations

- Determine the need for container backup based on application criticality as not every containerized app requires backup.
- Invest in container knowledge to understand the need for backing up Kubernetes objects like namespaces, secrets, keys and configuration maps, in addition to just persistent volumes.
- Align container backup requirements with the organizational structure as, unlike traditional infrastructure, container backup operations will be performed by the platform or application engineering teams.
- Dedicate budget for protecting containers as it requires additional investments in backup solutions and infrastructure.
- Adopt a strategy for container backup just as with every other data source in your enterprise.
- Select specialized container backup solutions first while traditional backup solution capabilities mature over time.

Sample Vendors

Catalogic Software; Cohesity; Commvault; Dell Technologies; Druva; IBM; Pure Storage; Rubrik; Trilio; Veeam Software

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Innovation Insight for Backup and Recovery for Kubernetes-Based Containerized Applications

Comparing Backup and Disaster Recovery Approaches for Kubernetes

Solution Path for Cloud-Native Infrastructure With Kubernetes

Hybrid Cloud Storage

Analysis By: Julia Palmer

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Hybrid cloud storage aims to enable seamless data services among disparate data centers, edge and the public cloud infrastructure. It encompasses many deployment patterns with varying underlying technologies covering a variety of data types. Hybrid cloud storage solutions can be delivered by purpose-built hybrid cloud storage platforms, data transfer appliances, hyperconverged solutions, storage arrays, software-defined storage products or data management solutions.

Why This Is Important

Data and storage services are now delivered everywhere. Integration with cloud infrastructure and platform services (CIPS) providers is becoming a critical selection criterion for storage platforms as many I&O leaders are looking for better efficiency and agility of services. Hybrid cloud storage products are enabling multiple use cases to improve data resilience, life cycle management and operation excellence while leveraging flexibility and scale of the public cloud infrastructure resources.

Business Impact

As data services are increasingly expanding toward the edge and the public cloud, on-premises data centers are no longer considered the center of data. This is pushing I&O leaders to look for new approaches to handle the data on-premises, in the cloud and at the edge. Although hybrid cloud storage can deliver on multiple use cases, disaster recovery and burst for capacity and storage standardization are the most commonly understood and funded by I&O leaders.

Drivers

- Provides data disaster recovery and business continuity by snapshotting or copying datasets, both structured and unstructured, from on-premises or edge storage to public cloud storage.
- Brings data closer to cloud compute and big data infrastructure for purposes of processing or analytics.
- Allows modernization of unstructured data services, as they are more applicable to hybrid cloud storage workflow.
- Standardizes the underlying storage platform for any deployment scenario — edge, core data center or public cloud infrastructure as a service (IaaS) — to provide consistent operational use of storage services.

Obstacles

- Complete disaster recovery requires coordination and integration of more moving parts than hybrid cloud storage solutions often claim.
- There are far greater inefficiencies in moving data closer to the compute operations rather than moving compute operations closer to data; the latter is substantially more efficient.
- Capacity expansion of on-premises storage brings with it unexpected consequences when data is unintentionally recalled or repatriated from the cloud or migration of data is required.
- The use cases for a common storage substrate across disparate and hybrid environments are still nascent; the resulting benefits are not broadly applicable or achievable.
- Available bandwidth and large egress costs limit the continuous movement of data between the on-premises data center and the cloud.

User Recommendations

- Select the data and storage services that require hybrid cloud capabilities.
- Select use cases that will benefit most from leveraging public cloud infrastructure and platform services.
- Build a business case for hybrid cloud storage beyond just a cost-benefit analysis by establishing a value-based analysis on specific business outcome or KPI improvement in the areas of resilience, scale, mobility and operational excellence.
- Choose a hybrid cloud provider by its ability to deliver additional services such as data analytics, cyber resilience, life cycle management, global access and other value-added services.
- Run a thorough proof of concept to validate the capabilities, performance, latency and costs of hybrid cloud storage solutions.

Sample Vendors

Amazon Web Services (AWS); CTERA; Hammerspace; LucidLink; Microsoft; Nasuni; NetApp; Panzura; Peer Software; Qumulo

Gartner Recommended Reading

Market Guide for Hybrid Cloud Storage

Modernize Your File Storage and Data Services for the Hybrid Cloud Future

Critical Capabilities for Distributed File Systems and Object Storage

Data Storage Management Services

Analysis By: Michael Hoeck, Chandra Mukhyala

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Data storage management services (DSMS) are designed to orchestrate the life cycle of data residing in multicloud, hybrid, SaaS and on-premises environments. Through tagging and other classification methods, they provide insights on existing sources of data to better manage data compliance and security, create storage efficiencies, optimize costs and enable analytics workflows.

Why This Is Important

DSMS enable organizations to identify data value and orchestrate the life cycle of data to reduce risk exposure and maximize costs to value of data. Organizations are managing an explosive amount of data across on-premises, hybrid, multicloud and SaaS application environments. The perceived easy path of continuing to add more storage is leading organizations down a path of unsustainable growth in capacity, siloed data, and increased regulatory and security threats.

Business Impact

DSMS solutions offer multiple benefits:

- Improves visibility to the organizations' data through metadata and content-based analytic analysis.
- Categorizes and classifies data to align with storage optimization, improved data life cycle and governance/compliance outcomes.
- Optimizes storage utilization of on-premises, cloud and SaaS applications by tiering, relocating, archiving or deleting data.
- Reduces blast radius of breach, ransomware and cyberattacks through proactive management of data.

Drivers

- The constant and uncontrolled growth of data and the resulting investments in storage capacity and cloud entitlements.
- Increasing number of storage resources and the resulting challenges of managing infrastructure and data across on-premises, hybrid, multicloud and SaaS application environments.
- The threat of security breaches and the understanding of “not if, but when” requires organizations to proactively reduce the blast radius for cyberattacks and ransomware exfiltration.
- Enablement of smarter business outcomes and faster analytics workflows using insights from the data content.
- Increasing number of regulatory requirements to manage data retention life cycles, often aligned to privacy legislation.
- Requirement to balance risk versus reward of retaining too much data.
- Aging storage infrastructure and application assets create technical debt that needs to be eliminated.
- I&O teams’ increasing effort to collect data from unmanaged sources at request of legal and compliance to support e-discovery, public record requests and subject rights requests.

Obstacles

- DSMS strategy is easily overlooked for the "simple path" of acquiring more storage infrastructure and cloud entitlements which compounds the problem.
- Collaboration is required to establish expected outcomes, ownership and budgeting among IT, security, privacy, data and analytics, legal and compliance teams.
- Challenges of gaining executive sponsorship and stakeholder buy-in to a proactive data storage management program.
- Agreement on data classification and related retention policies is critical for successful deployments, but may be difficult to obtain.
- Establishing new skill set to effectively manage DSMS solutions to attain expected outcomes such as data discovery, tiering, archive, migration, disposition and other life cycle management processes.

User Recommendations

- Include DSMS technology options as part of your storage purchase decision process to allow proper analysis of existing storage utilization and introduce alternatives to improve total cost of ownership and organizational data risk position.
- Clearly define scope of data and the outcomes the organization wants to achieve.
- Engage business process owners to align value and use of data to the appropriate retention policy.
- Gain executive team commitment to create or update and, most importantly, enforce data retention policies.
- Compare and contrast vendor offerings for their scope of supported data sources and types, and the remediation capabilities to act on the data.

Sample Vendors

Archive360; Atempo; BigID; Commvault; Congruity360; Data Dynamics; Dell Technologies; Komprise; NetApp; Solix Technologies

Gartner Recommended Reading

Market Guide for Hybrid Cloud Storage

Modernize Your File Storage and Data Services for the Hybrid Cloud Future

Immutable Data Vault

Analysis By: Michael Hoeck, Jerry Rozeman

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Immutable data vault (IDV) solutions provide an immutable, air-gapped and independent copy of the backup in a secure environment for safeguarding backups against ransomware and insider attacks. Deployed on-premises or in the cloud, they are often delivered as packaged or hosted solutions by a variety of vendors, including backup and recovery software manufacturers, systems integrators and managed service providers. IDVs may or may not be part of an isolated recovery environment (IRE).

Why This Is Important

Against the backdrop of cyberattacks increasing in numbers and sophistication, organizations are expanding their efforts to prepare for the need to recover from an attack. With the latest round of attacks targeting backup systems, backup solutions are improving their ability to prevent backup data from being compromised. IDVs provide additional levels of protection and security of backup data to ensure backup data is available after an attack.

Business Impact

IDVs safeguard backup copies by:

- Creating a copy of backup data, independent from production and disaster recovery copies, which is isolated in a physically separate and secure environment.
- Restricting administration to physical console access to remove remote access.
- Using immutable storage to protect copies from being altered.
- Implementing physical or virtual air gap to separate vault copy from production environment.

Drivers

- Threats and sophistication of ransomware attacks, and the potential risk associated with rogue administrators, are increasing.
- Ransomware-as-service offerings are being sold, increasing the threat of new attackers and variants of malware.
- Work-from-home demands have significantly increased the risk of attacks via unsecured or poorly secured endpoints.
- Some attackers take over backup console operations to expire and delete backup data.
- There is an increased focus on new backup strategies to protect, detect and recover from the evolving threats of ransomware.
- Industry-led initiatives, such as Sheltered Harbor (financial services), have created awareness and demand for adding IDVs and IREs to improve cyber resilience.
- Industries such as the government, education and healthcare have had a higher rate of reported ransomware incidents.
- The number of regulatory and executive orders advising implementation of additional, highly protected copies of backup data is growing. Cyber insurers are adding requirements for air-gapped copies of backup data.

Obstacles

- Implementing another solution to store backup data amounts to additional cost that may not be budgeted.

- IDVs not only require additional backup storage, but also are recommended to be physically separated within or outside a data center. This requires additional infrastructure, such as a new cage, an area with limited physical access or at an off-site-managed storage location and air-gapped from the production network.

- The backup environment has become more complex due to the addition of a new isolated copy of data, additional technologies like advanced networking and data scanning, requirement of new procedures and runbooks, and potentially limited staff to operate it.

- Vendors have created confusion over the definition and implementation of “immutable” and “air gap,” due to a lack of standards. Therefore, it’s important to understand what each vendor means by “immutable” and “air gap” and how its functionality is implemented to assess the risk of hackers to override it.

User Recommendations

- Plan for when, not if, an attack will occur in the cost-benefit analysis to gain management buy-in to phase in costs. All new backup implementations should require immutability of the backup store.

- Conduct a thorough cost-benefit and risk assessment to align expectations and acceptable risks to the current backup and recovery solution capabilities. Leverage IDVs for your most critical applications to minimize investments.

- Align recovery time objectives (RTOs) and cost considerations in the selection and deployment of cloud or on-premises IDV solutions.

- Be mindful that the data stored within an IDV may also contain the agent or infectious code, as well as infected or encrypted data. Therefore, incorporate other requirements to scan, cleanse and repair backup data into the environment to prevent the reinfection of other systems during the recovery and restoration process.

Sample Vendors

Cohesity; Commvault; Dell Technologies; IBM; Kyndryl; Microsoft; Rubrik; Unisys; Veritas; Zerto

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

2022 Strategic Roadmap for Storage

Quick Answer: Can My Disaster Recovery Plan Also Address Ransomware Recovery?

Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware

Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware

Storage as a Service

Analysis By: Jason Donham, Philip Dawson

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Storage as a service (STaaS) is a managed service that provides a way for organizations to manage and consume storage without the overhead costs of upfront capital for storage assets and staff time. STaaS provides managers with flexibility, resilience and efficiency. STaaS solutions include both on-premises storage and cloud storage.

Why This Is Important

Infrastructure and operations (I&O) leaders struggle to leverage on-premises cloud operating model benefits while their environment becomes more complex and less agile to business demands. STaaS provides many benefits such as improved asset management through aligning costs to utilization, higher levels of operational efficiency through outsourcing hardware administration and support, and cost savings through a consumption-based as-a-service model with increased levels of automation.

Business Impact

Budget and spend (capex) inefficiencies are driving higher total cost of ownership (TCO) compared to consumption-based (opex) spending that is much more in line with storage needs.

STaaS solutions enable organizations to:

- Shift from capex to opex to eliminate IT budget inefficiencies.
- Improve workload asset management and reduce capitalization costs.
- Eliminate life cycle management issues and technology refresh cycles.
- Reduce cyber liabilities and threat exposure through data services offerings.

Drivers

- Infrastructure managers need options when reconfiguring and resizing storage environments to meet the rapidly changing demands of applications.
- Threats of ransomware and other cyberattacks require higher levels of data security.
- Traditional storage is inflexible when deployed in a hybrid operating model.
- STaaS can increase labor costs on the back of intensive budgeting cycles.
- Inefficient life cycle management and constant infrastructure turnover conspire to create an inflexible environment that hampers innovation and ability to respond to business demands.
- The lack of subject matter experts (SMEs) or staff attrition issues (offset by moving responsibility and accountability to vendors) around critical elements of the infrastructure lead to a less resilient platform and exposure to untenable events.

Obstacles

- Finance or procurement members believe they are better stewards of capex assets or don't fully understand the indirect cost savings or benefits afforded by STaaS.
- Vendor sales and marketing narratives and selling strategies are reluctant to promote or advocate the benefits of as-a-service models over capex-related product features.
- Vendor business models are immature in terms of backend operations — metering, billing — and integration with supply chain and logistics.
- Vendor channels are not fully equipped to enable or support the transition to an as-a-service consumption model.

User Recommendations

- Implement consumption-based STaaS to reduce or eliminate capex budgets and IT refresh cycles.
- Add SLAs to drive critical requirements such as ransomware protection to improve security posture.
- Utilize artificial intelligence for IT operations (AIOps) combined with STaaS to create an intelligent infrastructure platform that proactively and dynamically responds to IT operating model outcomes and business priorities.

Sample Vendors

Amazon Web Services (AWS); Backblaze; Dell Technologies; Hewlett Packard Enterprise (HPE); IBM; Microsoft Azure; NetApp; Pure Storage; Wasabi Technologies; Zadara

Gartner Recommended Reading

Leverage Storage as a Service Platform SLAs and Capabilities to Transform IT Outcomes

Container-Native Storage

Analysis By: Julia Palmer, Arun Chandrasekaran

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Container-native storage (CNS) is designed specifically to support container workloads and focus on addressing unique cloud-native architecture, granularity and performance demands, while providing deep integration with the container management systems. CNS is aligned with microservices architecture principles and adheres to the requirements of container-native data services, including being hardware-agnostic, API-driven and based on distributed software architecture.

Why This Is Important

CNS solutions are specifically designed to provide persistent storage to cloud-native applications. The common foundation is typically based on a distributed, software-defined and unified pool of storage and has container-level granularity of data services, while providing enterprise data management features. In addition, the entire stack is most often orchestrated with Kubernetes to manage container life cycle integration and enable self-service operations for developers.

Business Impact

- CNS enables the deployment of stateful cloud-native applications; this enhances elasticity, availability and multicloud integration.
- Infrastructure and operations (I&O) leaders require storage that can adhere to principles of container-native infrastructure as they support stateful applications, share application data and provide advanced data services.
- CNS eliminates bottlenecks to achieving portable infrastructure agility when building and deploying modern, cloud-native applications.

Drivers

- Organizations are building new cloud applications using cloud-native principles and rearchitecting traditional applications on Kubernetes platforms, both of which are driving significant momentum in the adoption of CNS.
- Due to the increased popularity of deploying and operating container environments by orchestration platform, most IT leaders require a persistent storage solution that can be tightly integrated with container orchestrators, such as Kubernetes.
- I&O leaders require new tools and processes for data management to provide storage services accessed by stateful applications running in containers and orchestrated by Kubernetes.
- CNS solutions can be deployed on-premises or in the cloud, making them optimal for hybrid and multicloud deployment infrastructure. Because CNS functions are based on software, they can be implemented in containers, enabling them to be managed with the same orchestration functions as containerized applications.

Obstacles

- A CNS solution will not be adopted by every enterprise, because it remains most appropriate for new deployments of cloud-native applications, or for applications that will be revised with significant refactoring.
- Although embracing the CNS paradigm will yield agility benefits, adopting a CNS solution is likely to increase operational complexity in the short term for traditional enterprise environments.
- CNS vendor landscape and technology is constantly evolving with a mix of early- and late-stage startups. During the past year, we have observed few acquisitions and product repositioning in the CNS market.
- Given the fragmented nature of the vendor ecosystem, I&O leaders risk creating a technology silo with CNS solutions, which is a common obstacle to large-scale adoption.

User Recommendations

- Choose storage solutions that align with microservices architecture principles and adhere to the requirements of container-native data services, such as being hardware-agnostic, API-driven, based on distributed architecture, and can support edge, core or public cloud deployments.
- Align storage solutions with cloud strategies, making sure you take into consideration CNS applicability in the public cloud and hybrid cloud scenario of your choice.
- Select storage products closely aligned with the developer workflow tools that can be directly integrated with the application layer for portability, scaling and data protection.
- Validate your vendor's capability of continuous innovation delivery, quality customer support and a consistent pricing model, given that the container ecosystem is rapidly evolving with unproven vendor business models.
- Ensure that the CNS solution is tested and qualified for specific Kubernetes platforms.

Sample Vendors

DataCore Software; Diamanti; IBM; ionir; Pure Storage; Red Hat; SUSE; VMware

Gartner Recommended Reading

A CTO's Guide to Navigating the Cloud-Native Container Ecosystem

Solution Path for Cloud-Native Infrastructure With Kubernetes

Market Guide for Container Management

2022 Strategic Roadmap for Storage

Digital Communications Governance

Analysis By: Michael Hoeck

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Digital communications governance (DCG) solutions provide methods to monitor and enforce corporate governance and regulatory compliance across a growing number of communications tools available to employees. For the various communications tools in use, DCG solutions enable consistent policy management, enforcement and reporting capabilities such as data retention, surveillance, supervision, behavioral analytics, auditing, and e-discovery.

Why This Is Important

DCG solutions are critical to an organizations' efforts to meet a growing number of regulatory and organizational compliance requirements. They facilitate the collection of multiple communication channels to retain them, accurately classify the data, consistently apply retention policies, improve timely response to audits and e-discovery requests, surface organization insights, and help effectuate data use policies.

Business Impact

DCG solutions help manage regulatory and organizational use policies for the growing volumes and types of digital communications. They enrich communications data for behavioral analytics to surface insights, such as employee sentiment, misconduct risks, and industry-specific conduct assessments. DCG improves e-discovery efforts supporting legal hold, search, review and export requirements. It is used for consistent application and use of retention policies across various communication channels.

Drivers

DCG solutions enable businesses and organizations to utilize information within digital communications data sources to:

- Comply with regulatory requirements for highly regulated industries such as financial services, healthcare and public sector.
- Consolidate, centralize and simplify access to the multiple channels of digital communications in use by employees, including text-, voice-, and video-based content.
- Assess effectiveness of compliant-use policies for digital communications tools.

- Identify behavioral attributes and business intelligence within digital communications, such as employee sentiment and conduct and risk assessment, based on the use of sentiment analysis and data models.

- Capture and retain mobile device communications, including SMS/Multimedia Messaging Service (MMS) and other mobile application messages, such as WhatsApp, WeChat, and Signal.

- Respond to public records requests, such as Freedom of Information Act (FOIA) and Public Records Act (PRA).

- Simplify e-discovery and access across multiple communication channels driven by litigation, audits, internal matters, and other investigations.

- Respond to subject rights requests of privacy regulations, such as General Data Protection Regulation (GDPR) and California Privacy Rights Act (CPRA).

Obstacles

- DCG solutions may require use of multiple vendor offerings to connect the variety of communication channels with the appropriate archive offering.

- DCG requires an organizationwide strategy of supervising or surveilling employee communications, which may run into barriers of adoption based on a “big brother” perception.

- Executive sponsorship and stakeholder buy-in to data classification and related retention policies is critical for successful deployments, but may be difficult to obtain.

- Ensuring clear understanding of organizations’ data residency requirements for archived data and proper alignment to vendor solutions can be challenging.

- Transitioning or migrating existing data, including previous archives, to a new archive can be time-consuming, complex and costly.

User Recommendations

- Mitigate potential compliance and regulatory violations by shifting from a reactive to a proactive posture using DCG solutions.
- Shortlist solutions that best align scope of digital communications sources to required use cases, such as data retention, e-discovery, supervision, surveillance, and business intelligence.
- Differentiate vendor solutions by assessing use of AI/ML as a critical component of their offering's use of analytics to automate and accelerate business processes.
- Improve e-discovery and supervision/surveillance outcomes by using solutions that reduce false positives.
- Negotiate exit strategy terms upfront to create transparency and minimize future costs for data export/extraction processing.
- Focus attention on SLAs, which obligate SaaS/platform as a service (PaaS) vendors to support the defined performance levels as the data volume grows.
- Scope migration of legacy communication archives, including export from old, import to new and ongoing storage during the selection phase.

Sample Vendors

CellTrust; Global Relay Communications; Mimecast Services; Movius; Proofpoint; Shield; Smarsh; TeleMessage; Theta Lake; Veritas Technologies

Gartner Recommended Reading

Magic Quadrant for Enterprise Information Archiving

Critical Capabilities for Enterprise Information Archiving

Function Accelerator Cards

Analysis By: Anushree Verma

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Function accelerator cards (FACs) are a class of devices that have dedicated hardware accelerators with programmable processors to accelerate network, security and storage functions — known as DPUs/IPUs and/or SmartNICs. FACs improve data operations and services, server availability, and network performance and security, besides enabling connectivity to a network. They have onboard memory and peripheral interfaces, and can run independently.

Why This Is Important

FACs can improve server performance by up to 50%, via offloading functions such as virtual switching, security and application delivery controller (ADC). They can host dedicated network appliances, including firewalls. They can also improve security by placing security functions onto a securely booted, locked-down environment. Today, FACs are primarily adopted by hyperscalers and large cloud providers, and we estimate they will grow at a five-year CAGR of 65% through 2027.

Business Impact

FACs enable cost-efficient and energy-efficient data center environments, while improving performance. By offloading high overhead functions, they allow the server to host more workloads, which reduces the direct cost of additional servers and, in some cases, infrastructure software. In addition, they can facilitate data transmission between remote resources — primarily for HPC and artificial intelligence/machine learning (AI/ML) workloads.

Drivers

- Hyperscale cloud providers such as AWS, Microsoft Azure and Tencent, and other large cloud providers are using FACs today, and growing their implementation to achieve price/performance improvements.
- Vendors are aggressively marketing FACs, which are also referred to as data processing unit (DPU), infrastructure processing unit (IPU), SmartNICs, distributed services card (DSC) or programmable NICs.
- The rise of AI/ML workloads, solid modeling, seismic analysis and advanced analytics has created unprecedented demand on storage and network, resulting in latency and bandwidth issues.
- FACs can reduce the number of servers and hypervisor licenses by 10% to 30%, and may also decrease the number of application software licenses.
- Pulling security out of the server reduces the software-based surface area for attack.
- Telecommunication networks are moving toward virtualizing the network edge with 5G adoption, which leads to offloading 5G user plane function (UPF) and 5G network slicing to the FACs to achieve low latency and high throughput.
- FACs are increasingly bundled in high-performance solid-state storage systems to boost IOPS and minimize latency.
- FACs provide an alternative platform to host network appliances, such as firewalls and ADCs, with price/performance benefits in specific usage scenarios.
- Vendors with a large enterprise-installed base, including Hewlett Packard Enterprise (HPE) and VMware, have invested heavily in the technology and marketed it to organizations with specific usage scenarios until 2022. However, there has been a slowdown in the past few months.
- Increased consolidation in the market with AMD acquiring Xilinx and Pensando Systems, and Microsoft acquiring Fungible.

Obstacles

- Enterprises perceive FACs as a disruptive and dramatic departure from typical data center networking patterns, which limits adoption due to concerns over risk.
- There is confusion in the market due to vendors using different terminology, and providing different capabilities and architectures.
- Data plane programmability is high-risk, and has limited value and interest for enterprises.
- Hyperscale CSPs are able to justify the incremental price with the large-scale order and customization benefits they get by adopting FACs. However, enterprises are so far unable to do so, thereby hindering rapid adoption.
- Form factor and power consumption can impact rack, power and cooling budget, or occupy a full-size PCIe slot.
- Broadcom's pending acquisition of VMware creates uncertainty for potential buyers because Broadcom doesn't currently offer a FAC.

User Recommendations

- Use FACs for specific use cases, such as acceleration of NVMe-oF and AI/ML.
- Engage your existing data center infrastructure vendors on their plans for multivendor interoperability for offload on FACs, prior to your next server refresh.
- Investigate FACs to replace legacy components like physical firewalls and reduce the number of application licenses.
- Pilot FAC offerings to improve scale/security needs in the context of a large-scale data center network (1,000 switches), or to support extremely network sensitive workloads.
- Select FAC-based storage offerings, if you are an enterprise with applications that require microsecond latency performance when processing large datasets.
- Use a cross-functional team that includes networking, compute, storage and security personnel to evaluate FAC offerings.
- Focus on management and orchestration when evaluating FACs, as they are key differentiating factors.

Sample Vendors

AMD; Ethernity Networks; Intel; Kalray; Microsoft; Napatech; Nebulon; NVIDIA; Pliops; VMware

Gartner Recommended Reading

Emerging Technologies: Adoption Growth Insights — Function Accelerator Cards (Next-Gen SmartNICs, DPUs, IPUs)

Your Server Is Eating Your Network — Time to Rethink Data Center Network Architectures

Market Trends: Arm in the Data Center: Act Now to Develop Plans to Address This Shifting Market

Hybrid Cloud File Data Services

Analysis By: Chandra Mukhyala

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Hybrid cloud file data services (HCFDS) deliver seamless file data services across disparate data centers, edge locations and public cloud infrastructure. The most popular use cases for HCFDS are disaster recovery, burst for capacity, burst for processing, data transport, global data orchestration and storage standardization. HCFDS can be native to the underlying storage product or a stand-alone offering that is agnostic to the underlying storage.

Why This Is Important

Organizations are increasingly creating and accessing data at multiple locations beyond on-premises, including the public cloud and edge locations. In addition, modern application workflows span multiple locations using data services from multiple locations. HCFDS addresses this situation by making file data services available anywhere that access or creation of files is required.

Business Impact

Businesses can benefit from better data resilience, capacity management, on-demand flexibility, data portability, resource optimization and operational excellence through the six use cases of HCFDS. These six use cases are disaster recovery, burst for capacity, burst for performance, data transport and computation, global data orchestration and storage standardization across disparate data center locations.

Drivers

- Existing and new unstructured data workloads require hybrid cloud file capabilities in order to be able to use public cloud for elasticity, operational simplicity, processing and data longevity.
- HCFDS address the challenges that arise as a result of data generated from multiple locations and public cloud migration initiatives.
- HCFDS are expanding from being providers of storage to providers of platform services, such as data insights, cyber resilience, life cycle management and data mobility across public cloud and on-premises deployments.
- Increasing application analytics tools for business insights is creating more data across edge locations that must be connected with AI services in the public cloud.
- Knowledge workers are distributed across geographic locations, but need to collaborate on the same set of data.

Obstacles

- There is a limited number of mature solutions for global data orchestration leads.
- Current solutions based on caching architectures have performance and scalability limitations.
- Existing investments in file or object storage products may limit exposure to modern HCFDS offerings.
- Funding from business is limited to disaster recovery and burst for capacity use cases.

User Recommendations

- Take advantage of public cloud infrastructure and platform services by identifying workloads, data types and use cases that will benefit from integration with public cloud.
- Choose a hybrid cloud provider by its ability to deliver additional services, such as media rendering, data analytics, cyberstorage, data life cycle management, performance acceleration, cloud-native access and other value-added services that enterprises require.
- Build a comprehensive hybrid cloud data services catalog to define and maintain global hybrid cloud storage services and to ensure standardization and customer transparency.
- Build a business case for hybrid cloud data services by putting a value on the new capabilities and outcomes delivered as a result of using public cloud for disaster recovery, burst for capacity, burst for processing, global data orchestration and storage standardization.

Sample Vendors

Atempo; CTERA Networks; Hammerspace; IBM; Komprise; Nasuni; NetApp; Peer Software; Qumulo

Gartner Recommended Reading

Modernize Your File Storage and Data Services for the Hybrid Cloud Future

Market Guide for Hybrid Cloud Storage

Sliding into the Trough

Cloud Data Backup

Analysis By: Jerry Rozeman

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Cloud data backup tools back up and restore production data generated in the cloud. Data can be created by SaaS tools (e.g., Microsoft 365); platform as a service (PaaS) tools (e.g., Amazon Relational Database Service [RDS]); or infrastructure as a service (IaaS) tools (e.g., Amazon Elastic Compute Cloud [EC2]). Backup copies can be stored in the same or a different cloud location, or on-premises in the data center, where restore granularity/recovery location options should be offered.

Why This Is Important

Public cloud providers typically offer infrastructure resilience and availability to protect their systems from server, site or region failures, and generally provide shared responsibility for the data. When data is lost due to user or administrator error, configuration and patching changes, development issues, software corruption, or malicious attacks, user organizations are responsible, rather than the cloud provider. Cloud data backup tools address these deficiencies.

Business Impact

Adopting cloud data backup tools will deliver:

- Confidence in routine data backup of critical computing and application data
- The ability to comply with data protection policies
- Improved availability of data to recover after infrastructure failure, user or administrator errors, software corruption, or malicious attacks

Drivers

- As more production workloads migrate to the cloud (in the form of SaaS, PaaS or IaaS), it has become critical to protect the data generated natively in the cloud.

- Cloud providers focus on infrastructure high availability and disaster recovery (DR), but are not responsible for application or user data loss.

- Most SaaS applications' natively included data protection capabilities are not true backup, and lack secure access control and consistent recovery points to recover from internal and external threats.

- As Microsoft 365 is widely adopted, the need for better protection is growing rapidly, which is especially driven by Microsoft's inconsistent and incomplete use of recycle bins, the requirement for retention policies, and lack of intuitive recovery processes.

- Backup of Salesforce data is the second-most-addressed workload by vendors in this space.

- Native backup of IaaS and PaaS data usually resorts to cloud-based snapshots and scripting, which may lack application consistency, restore options, data mobility, storage efficiency and policy-based automation, and do not provide a secure, independent external copy of the data.

- Interest in providing backup for Azure AD, Azure DevOps and GitHub is rising.

Obstacles

- Deploying data protection for cloud-based workloads is often an afterthought, because it is not part of the original business case for cloud-based workload deployment or migration.

- In-depth review of each cloud vendor's SLAs is another obstacle that customers have to overcome, because it limits them in their speed of cloud adoption.

- The outcome of the SLA review might block the cloud service adoption because the SLA might not meet company requirements.

- Besides Microsoft 365 and Salesforce, most SaaS-based applications do not support third-party, external backup solutions that limit customers in protecting these workloads.

- Adopting cloud data backup tools will require significant investments in software, services and/or infrastructure, knowledge and processes.

- Establishing partnerships by IT with apps, DevOps and other teams to structure data protection can be a challenge.

User Recommendations

- Ensure that an enterprise-class data backup and recovery strategy is part of every cloud deployment or migration, which aligns with organizational compliance requirements.
- Evaluate and thoroughly understand cloud-native backup and recovery capabilities, and compare them with your company protection policies before migrating applications to SaaS, PaaS or IaaS data infrastructure solutions.
- Ensure that contracts with cloud providers clearly specify the capabilities and costs associated with the backup solution, including exit fees, and understand the limitations of such solutions.
- Factor in the cost of cloud backup application, in addition to the cost of hosting the production application in the cloud.
- Focus on ease of deployment, ease of management, data mobility, storage efficiency and flexible options in terms of backup/recovery granularity and location when selecting third-party backup tools.

Sample Vendors

AvePoint; Cohesity; Commvault; Druva; HYCU; Keepit; OwnBackup; Rubrik; Veeam; Veritas

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Market Guide for Backup as a Service

Innovation Insight: Backup for SaaS Applications

Quick Answer: Should I Back Up Microsoft 365?

Data Discovery

Analysis By: Michael Hoeck

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Data discovery solutions discover, analyze and classify structured and unstructured data to create actionable outcomes for security enforcement and data life cycle management. Using elements of metadata, content and contextual information, combined with expression- and machine-learning-based data models, data discovery solutions provide actionable guidance and processes to advance data management and security initiatives.

Why This Is Important

Data discovery solutions improve organizations' ability to manage ever-expanding repositories of structured and unstructured data in on-premises, hybrid and cloud infrastructures. They increase visibility of disparate and unorganized sources of information. They enable compliance teams to improve insight into policy adherence and sensitive information, including personal data (PD); and enable security teams to improve visibility of sources of data access risk.

Business Impact

Data discovery solutions can have the following business impacts:

- Accelerate the identification of sensitive data to improve the outcomes of an organization's security controls and privacy initiatives.
- Advance data life cycle management activities by assigning retention policies with data discovery categorization and classification results.
- Reduce business risk through advanced capabilities to eliminate and quarantine sensitive information, and identify data lineage and access permissions issues.

Drivers

- Organizations want to mitigate business risks associated with data processing activities (including data breach, data exfiltration, PD and intellectual property exposure, auditing and regulatory fines), identify sensitive data and implement effective data life cycle initiatives
- There is a need to minimize the blast radius of a cyberattack's access to sensitive information through data classification coupled with security controls, defensible deletion and minimization efforts.
- Organizations want to be able to align and monitor proper data access based on categorization and classification of all data.
- Retention policies can be difficult to establish, refine and consistently enforce without clear data inventory knowledge and awareness of potential sensitive data risk.
- The demands associated with the growing number and complexity of compliance and privacy regulations, such as the EU's General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, and financial services compliance, have greatly increased interest in, and awareness of, data discovery software.
- The potential value of contextually enriched data is capturing the interest of data and analytics teams.

Obstacles

- For its broad set of use cases, capabilities and benefits, funding and budget for data discovery solutions may require a collaborative effort across multiple departments, including security, privacy, compliance, legal and IT teams.
- Successful results of using data discovery software may be affected by a lack of data life cycle management policy buy-in or consensus from key internal constituencies, including executive sponsorship.
- Action-oriented retention policies are required to defensibly delete data identified by data discovery software.
- It can be challenging to get the organization to commit to aligning administrative costs for data discovery solutions and their management with an ongoing business program and investment, rather than a singular project-based activity.

User Recommendations

- Use data discovery software to enable IT, security operations, privacy, compliance and line-of-business (LOB) teams to make better informed decisions regarding classification, data management and content migration.
- Use data discovery software to better grasp the risks of data footprints, including where data resides and who has access to it, and to expose another rich dataset through subsequent classification and content analysis to drive business decisions.
- Develop strong data life cycle management principles by establishing, updating and enforcing retention policies using the information gathered and remediation actions from data discovery software.
- Identify the potential risks of unknown data stored in structured database repositories often associated with applications that enable the storage of free-form text.
- Create data visualization maps to better identify the value of data and the risks to it, including the data owner, using data discovery software.

Sample Vendors

ActiveNav; BigID; Concentric AI; Congruity360; Data443; DataGrail; Netwrix; Securiti.ai; Spirion; Varonis

Gartner Recommended Reading

How to Succeed With Data Classification Using Modern Approaches

State of Privacy: The Privacy Tech Driving a New Age of Data Wealth

2022 Strategic Roadmap for Storage

Market Guide for E-Discovery Solutions

NVMe-oF

Analysis By: Jeff Vogel, Joseph Unsworth

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Nonvolatile memory express over fabrics (NVMe-oF) is a network protocol that takes advantage of the parallel-access and low-latency features of NVMe Peripheral Component Interconnect Express (PCIe) devices. It is a protocol interface designed for high-performance fabric technologies, including remote direct memory access (RDMA) over Fibre Channel, InfiniBand or Ethernet with RoCE v2, iWARP or TCP. NVMe-oF uses the NVMe protocol to extend access to NVMe devices.

Why This Is Important

NVMe-oF addresses use cases where low-latency application requirements are critical when in combination with NVMe drives. Although it requires continuous infrastructure changes and upgrades, the benefits provided by NVMe-oF are triggering high performance and the use of scalable architectures that can capitalize on the underlying networking capabilities in combination with NVMe flash media. NVMe-oF protocols enhance the capabilities of storage in distributed and disaggregated platforms.

Business Impact

NVMe-oF enables organizations to create a high-performance storage network. NVMe-oF storage targets can be dynamically shared among workloads, thus providing an on-demand or composable storage resource that provides flexibility, agility and greater resource efficiency. NVMe-oF runs on both traditional Fibre Channel (FC) and IP switches. NVMe/TCP offers additional choices for IT connectivity infrastructure and is a good match for organizations without legacy FC infrastructure.

Drivers

- The NVMe-oF protocol takes advantage of high-speed networks and accelerates the adoption of next-generation storage architectures.
- Storage as a service (STaaS) adoption will rival Internet Small Computer System Interface (iSCSI) and low-end FC storage area network (SAN) bandwidth requirements.
- NVMe-oF can scale out to high-capacity levels with high-availability features and be managed from a central location, serving dozens of compute clients.
- The release of VMware vSphere 7.0 Update 3 for mainstream usage, an NVMe-oF over TCP storage protocol, opens up a path for TCP/IP to be a popular data center transport mechanism of NVMe-oF.
- Most storage array vendors have already debuted at least one NVMe-oF-capable product as an alternative protocol for primary storage.

Obstacles

- Depending on the existing infrastructure, the implementation of end-to-end NVMe-oF could require substantial changes to and increase costs of storage platforms, networks and servers.
- Infrastructure and operations (I&O) leaders struggle to justify ROI for end-to-end NVMe-oF deployments. Only a small percentage of workloads will see clear performance benefits from such an uplift.
- The cost and complexity of infrastructure elements, such as host bus adapters (HBA) and switching devices, impede the adoption of NVMe-oF solutions in mainstream enterprises.
- Some NVMe data storage products on the market deliver only a small fraction of NVMe's potential performance improvements. This is due to end-to-end differences in how NVMe-oF is implemented.
- Software support for NVMe-oF is relatively nascent.

User Recommendations

- Select workloads where the scalability and performance of NVMe and NVMe-oF justify the costs and complexity of such deployment. Target it for AI and machine learning (ML), high-performance computing (HPC), in-memory databases or transaction processing.
- Define which type of implementation will be used — host-to-controller or controller-to-NVMe media. Consult suppliers for which type they support against performance requirements.
- Investigate potential infrastructure bottlenecks, such as applications, servers or networks. Consult suppliers on potential performance and total cost of ownership (TCO) gains to justify the ROI.
- Assess potential storage platform, network interface controller, HBA and network fabric suppliers to verify that interoperability testing has been performed and references are available.
- Verify the availability and support of NVMe-oF networks for hypervisor and operation systems to ensure compatibility and performance improvement.
- I&O leaders must either deploy NVMe-oF with RDMA RoCE v2 or NVMe-oF over TCP/IP-based products to ease the transition and provide investment protection.

Sample Vendors

Dell Technologies; Hewlett Packard Enterprise (HPE); Hitachi Vantara; Huawei; IBM; Lightbits Labs; NetApp; Pure Storage

Gartner Recommended Reading

Magic Quadrant for Primary Storage

2022 Strategic Roadmap for Storage

Quick Answer: How Can I Use Storage as a Service to Reduce IT Spend?

Open-Source Storage

Analysis By: Julia Palmer, Arun Chandrasekaran

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Open-source storage is a form of software-defined storage, for which the source code is made available to the public through a distribution license that complies with open-source definition. It supports many of the same features as proprietary storage, including support of structured and unstructured data, as well as heterogeneous management.

Why This Is Important

Although open-source storage has been around for over a decade, it has been adopted mainly by hyperscalers, managed service providers and large organizations. Recent innovations in x86 hardware and flash technology, combined with an innovative open-source ecosystem, are making open-source storage and its licensing models practical for cloud and big data workloads. This makes it a potential alternative to proprietary storage.

Business Impact

Open-source storage adoption among technology firms and service providers, and in research and academic environments, underscores the benefits of leveraging the broader open-source storage developer ecosystem across disciplines. Big data, analytics and private cloud use in enterprises are other promising use cases. Open-source storage will enable customers to innovate rapidly in key storage areas, such as data management at a lower acquisition cost, with “good-enough” availability, performance and manageability.

Drivers

- Open-source storage is playing an important role in enabling cost-effective, scalable platforms for new cloud and big data workloads.
- Customers are actively evaluating open-source storage products across block, file and object protocols.
- More than 90% of enterprises worldwide use open-source technology in support of their mission-critical IT workloads, leading to use of open-source options across the technology stack.
- Cloud computing, microservices application architectures, big data analytics and information archiving are pushing the capacity, pricing, and performance frontiers of traditional scale-up storage architectures. This has led to a renewed interest in open-source software as a means to achieve high scalability in capacity and performance at lower acquisition costs.
- The emergence of open-source platforms, such as Kubernetes and TensorFlow, is backed by large, innovative communities of developers and vendors, such as DataDirect Networks (Lustre), IBM and Red Hat (Ceph Storage). Collectively, they provide enterprises with a broad selection of options to consider for use cases such as cloud storage, big data, stateful microservice workloads and archiving.
- There is also an influx of open-source storage projects for container-based storage, such as Longhorn, MinIO, OpenEBS and Rook.

Obstacles

- Onboarding open-source storage software will require more subject matter experts, as some IT leaders overestimate the benefits, and underestimate the costs and risks. Although open-source storage requires less upfront investment than proprietary storage, IT leaders need to weigh the benefits, risks and costs carefully.
- It is difficult to predict cost and ROI of ownership of open-source storage. Pragmatic, long-term open-source investment strategy must include a balance of cost, flexibility and innovation to yield successful results.
- For mature open-source storage projects, leaders may turn to the community as a knowledge base to augment their self-support efforts. Unfortunately, these communities do not come with a contracted SLA, and there is no guarantee of quick and reliable support.
- Open-source storage licensing can be challenging due to myriad license types and governing copyright conditions. Interpretation of legal risks can be complex and requires rigorous due diligence.

User Recommendations

- Allocate resources to invest in participating and contributing to open-source storage initiatives to support ecosystem activities.
- Actively deploy pilot projects, identify internal champions, train storage teams and prepare the overall organization for this disruptive trend.
- Use a commercial distribution and obtain support through a vendor, as opposed to downloading the source code for free. Open-source storage requires significant effort and expertise to install, maintain and support.
- Carefully evaluate any downsides of lock-in against the perceived benefits attained when deploying “open-core” or “freemium” storage products. The proprietary software version often comes in the form of add-on modules, retained features or management tools that function on top of open-source storage.
- Conduct legal license risk due diligence, and assessment of usage and compliance. Ensure compatibility with distribution of your product or service.

Sample Vendors

DataCore Software; DataDirect Networks; iXsystems; MinIO; Openfiler; Red Hat; SoftIron; SUSE

Gartner Recommended Reading

A CTO's Guide to Open-Source Software: Answering the Top 10 FAQs

How to Manage Open-Source Software Risks Using Software Composition Analysis

Critical Capabilities for Distributed File Systems and Object Storage

Magic Quadrant for Distributed File Systems and Object Storage

Competitive Landscape: Chinese Infrastructure Software-Defined Storage Vendors

Software-Defined Storage

Analysis By: Chandra Mukhyala

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Software-defined storage (SDS) abstracts storage software from the underlying hardware, providing common provisioning and data services across IT infrastructures, regardless of locality and hardware technology. It can be deployed as a virtual machine (VM), a container or as storage software on a bare-metal, industry-standard server, providing flexibility to deploy storage wherever the application demands — on-premises, at the edge or in the public cloud.

Why This Is Important

SDS provides flexibility to support applications across the hybrid cloud from on-premises, the edge or the public cloud, with consistent storage service across these locations at a lower total cost of ownership (TCO). SDS vendors target a broad range of workloads. These include general-purpose file storage, backup, archiving, analytics, high-performance computing (HPC) and artificial intelligence (AI), supporting structured/unstructured data services for VMs, containers and bare-metal workloads.

Business Impact

- SDS breaks the dependence on proprietary storage hardware, supporting lower acquisition costs.
- SDS enables choice of storage compute, flash, memory and networking hardware options to align with application needs.
- Some Gartner customers report as much as a 40% TCO reduction from the use of standard hardware, lower-cost upgrades and maintenance.
- Increased hybrid cloud deployment flexibility and the ability to have common provisioning and data services on-premises, at the edge and in the public cloud.

Drivers

- Build a storage solution at a low acquisition price point on common platform hardware.
- Decouple storage software from hardware to standardize data center hardware platforms to scale compute and capacity independently.
- Build an agile “infrastructure as code” architecture, enabling storage to be a part of software-defined data center automation and orchestration framework that integrates with the public cloud.
- Take advantage of the latest innovations in storage hardware before they are available and supported in traditional external controller-based (ECB) storage arrays.
- Ability to run the same storage services across on-premises, at the edge and in the public cloud.

Obstacles

- I&O leaders often struggle to navigate SDS vendor solutions as a result of the variety of SDS product offerings, with established and emerging vendors delivering differentiated value propositions and product capabilities.
- Hybrid cloud IT operations is an emerging use case for SDS, because tomorrow's data center landscape is expanding to include edge and public cloud, Hence, adoption often requires multiple products and complex integration.
- I&O leaders need to invest in personnel with specialized skills to effectively develop and manage SDS in the enterprise. Therefore, the potential cost savings obtained from reduced capital expenditures (capex) requires a cost-benefit analysis for improved operating flexibility.
- Performance and TCO, along with other business value factors, must be considered contemporaneously, creating a more-complex assessment that slows deployment.

User Recommendations

- Recognize that SDS is a growing deployment model that will be focused primarily on web-scale storage architectures, but has applicability at the edge and public cloud deployments.
- Select SDS vendors that provide support for multiple deployment options, and offer validated hardware reference designs that minimize performance and scalability trade-offs.
- Grade SDS products by their ability to be truly hardware-agnostic, API-driven, based on distributed architectures, flexible pricing models and hybrid cloud deployment flexibility.
- Deploy SDS as part of a cohesive software-defined infrastructure (SDI) design, with an emphasis on delivering uniform storage platforms across on-premises, public cloud and edge environments.
- Before embarking on SDS deployments, recognize that SDS may involve substantial work sizing the underlying hardware and building the total solution on your own, versus a plug-and-play appliance.

Sample Vendors

DataCore Software; IBM; NetApp; Nutanix; Qumulo; Red Hat; Scality; StorMagic; VMware; WEKA

Gartner Recommended Reading

Magic Quadrant for Distributed File Systems and Object Storage

Market Guide for Hybrid Cloud Storage

Modernize Your File Storage and Data Services for the Hybrid Cloud Future

Climbing the Slope

Object Storage

Analysis By: Chandra Mukhyala

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Object storage refers to a system that houses data in structures called "objects," and serves hosts via APIs such as Amazon Simple Storage Service (Amazon S3). Conceptually, objects are similar to files, in that they are composed of content and metadata. Object storage uses a flat namespace, compared with treelike structures seen in file systems. Object storage offerings are available as software-based storage, virtual machines, traditional hardware appliances or as a managed service.

Why This Is Important

With unstructured data doubling every few years, the need for scalable, resilient and cost-effective storage becomes a critical requirement. A single data lake that captures all of an organization's unstructured data for analysis to provide insights to the business is a key technology enabler. Object storage satisfies those needs through a flat namespace housing key-value pairs with rich metadata, all protected with erasure coding.

Business Impact

Object storage can help businesses take control of their data management strategy by attaching rich metadata to objects, into a scalable and cost-effective storage that is more developer-friendly. Object storage is helping businesses replace tape systems for backups with an online storage that is easily searchable for compliance and regulatory purposes. In addition, object storage is being frequently used for discovering business insights by running various analytics on the underlying data.

Drivers

- The primary driver for object storage continues to be the explosive growth in unstructured data, resulting from digital transformation across all industry verticals.

- Organizations are managing larger objects and a larger number of objects, leading to the need for scalable and cost-effective storage. Photos and videos are captured in higher resolution and for more use cases than in the past.
- There is more application- and machine-generated data that is captured for analytics purposes.
- The need for application developers to consume storage through a simple programmatic interface. Modern application developers prefer the programmatic nature of object storage over traditional file-based storage.
- The default storage in the public cloud being object storage leads to more applications preferring object storage over other forms of storage.
- The rise of ransomware is driving the demand for immutable storage, and object addresses that requirement with S3 object locking for protecting backup data.

Obstacles

- Majority of legacy applications are still dependent on file-based interfaces like NFS and SMB.
- Modern distributed file systems are highly scalable, and are available as hardware-agnostic, software-based deployment models that can run on any standard server hardware, on-premises or in the public cloud, making them cost-effective and flexible.
- Most file-based storage offerings also support S3 protocol for accessing files as objects.
- Increasingly vendors are offering a unified platform for all unstructured data that provide both file and object services, minimizing the need for a stand-alone object storage offering.
- Modern file systems can satisfy the vast majority of requirements for which object storage is considered. Exceptions are when an application depends heavily on the metadata associated with the object or when scaling to several billion objects.

User Recommendations

IT leaders that require highly scalable, self-healing and cost-effective storage platforms for unstructured data should:

- Evaluate the suitability of object storage products, but not when the primary use case requires processing or editing of file-based data. Use cases for object storage are expanding from backup and archiving to primary storage for applications where data processing is done in server memory.
- Evaluate the product's API support for dominant public cloud providers, when building on-premises object storage repositories so that workloads can be extended to public cloud, if needed. Amazon's S3 has emerged as the dominant API over vendor-specific APIs and OpenStack Swift (which is in precipitous decline).
- Select object storage vendors that offer a wide choice of deployment (software-only versus packaged appliances versus managed hosting) and licensing models (perpetual versus subscription) that can provide flexibility and reduce total cost of ownership.

Sample Vendors

Backblaze; Cloudian; Dell EMC; Hitachi Vantara; Huawei; IBM; MinIO; NetApp; Scality; Wasabi

Gartner Recommended Reading

Magic Quadrant for Distributed File Systems and Object Storage

Critical Capabilities for Distributed File Systems and Object Storage

Voice of the Customer for Distributed File Systems and Object Storage

Distributed File Systems

Analysis By: Chandra Mukhyala

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Distributed file systems (DFSs) use a single file system to cluster multiple storage nodes together, presenting a single namespace and a storage pool to provide aggregated bandwidth for multiple hosts in parallel. Data and metadata are distributed over multiple nodes in the cluster to handle availability and data protection in a self-healing manner. DFSs can be expanded nondisruptively by adding new nodes horizontally, thereby increasing cluster capacity and performance.

Why This Is Important

Building scalable and cost-effective distributed storage platforms for unstructured data is an imperative for infrastructure and operations (I&O) leaders. The accelerated growth of existing file datasets and the introduction of new file-based workloads are bringing distributed scale-out storage architectures to the forefront of IT infrastructure planning. DFSs are designed to address performance and scalability limitations in traditional, scale-up, network-attached storage (NAS) environments.

Business Impact

- DFSs are based on scale-out architecture that scales performance and capacity linearly and nondisruptively, as required by business demands.
- Many of the file system products are being deployed as software-only, which provide better flexibility and a lower total cost of ownership (TCO), compared with integrated storage appliances.
- The introduction of a DFS will significantly improve private cloud services for unstructured data, which require highly scalable, resilient and elastic infrastructure.

Drivers

- To address exponential unstructured data growth, I&O leaders are increasingly replacing scale-up NAS appliance systems with distributed scale-out file system products to benefit from the linear scaling of capacity and performance.
- Enterprises are preparing for exponential growth of unstructured data and seeking data insights, as well as integration with cloud storage for long-term, data life cycle management.
- Analytics, artificial intelligence (AI) and machine learning (ML) applications are generating more data and increasing demand for DFSs.
- Simulation and data modeling, the traditional use cases for DFS, continue to be major drivers of DFS.

Obstacles

- DFS deployments are often complex, requiring careful planning and a lengthy proof-of-concept (POC) process to validate operational requirements.
- Many DFSs are designed to be deployed in a single, large data center and cannot efficiently scale down for small deployments at the edge.
- Some DFSs are designed for performance and still require separate tools to do data management, cyber protection and analytics.
- DFSs are not often selected when I&O leaders are looking for hybrid cloud file platforms, because they are designed for on-premises data residency requirements.

User Recommendations

- Establish clear workload performance indicators relevant to business and validate all performance claims with POC deployments, with an emphasis on protocol type, file sizes and your choice of underlying hardware.
- Increase agility by integrating DFSs with data insights and life cycle management options. This approach will enable you to get a better handle on data management and provide actionable insights to the business.
- Shortlist vendors with the ability to integrate with the public cloud and enable hybrid cloud storage deployments with tiering, archiving and bidirectional data flow for data processing. This emerging paradigm is experiencing positive, early traction with enterprises.
- Prioritize vendors that include support for Amazon S3, along with Network File System (NFS) and Server Message Block (SMB), in a multiprotocol manner.

Sample Vendors

Cohesity; Dell Technologies; Huawei; IBM; Inspur; Nutanix; Pure Storage; Qumulo; VAST; WEKA

Gartner Recommended Reading

Magic Quadrant for Distributed File Systems and Object Storage

Voice of the Customer for Distributed File Systems and Object Storage

Critical Capabilities for Distributed File Systems and Object Storage

Entering the Plateau

Hyperconvergence

Analysis By: Philip Dawson, Jeffrey Hewitt

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Hyperconvergence combines storage, computing and networking into a single system that reduces data center complexity and increases scalability. Multiple servers can be clustered together to create pools of shared compute and storage resources (or nodes), designed for convenient consumption. Delivery models include physical and virtual appliances, reference architectures, as a service or public cloud.

Why This Is Important

Infrastructure and operations (I&O) leaders seeking a cost-effective solution with a single management interface that excludes proprietary, external hardware controller-based storage should consider hyperconvergence as a viable option. Possible use cases include virtual desktop infrastructure (VDI), edge/Internet of Things (IoT), hybrid cloud and cloud-native.

Business Impact

Hyperconvergence enables IT leaders to be responsive to new business requirements in a modular, small-increment fashion, avoiding the large-increment upgrades typically found in three-tier infrastructure architectures. It is of particular value to midsize enterprises that can standardize on hyperconvergence and to the remote sites of large organizations that need cloudlike management efficiency with on-premises edge infrastructure.

Drivers

- Hyperconvergence provides simplified management that decreases the pressure to hire hard-to-find specialists. Adoption is greatest in dynamic organizations with short business planning cycles and long IT planning cycles tied to hybrid cloud delivery. The hyperconverged infrastructure (HCI) market is now trifurcating, focusing on the data-center-led “hybrid cloud” management use case with cloud-native applications, the VDI use case and the “edge/IoT” remote management use case.

- Hyperconvergence leads to lower operating costs, especially as it supports a greater share of the compute and storage requirements of the data center.

- Nutanix, an early innovator in hyperconverged integrated system (HCIS) hardware appliances, has largely shifted to a Hyper Converged Infrastructure (HCI) software revenue model and continues to increase its number of OEM relationships and partners.

- Larger clusters are now in use, and midsize organizations are considering hyperconvergence as the preferred alternative for on-premises infrastructure for block storage.

- Hyperconvergence vendors are achieving certification for more demanding workloads, including Oracle and SAP, and end users are beginning to consider hyperconvergence as an alternative to integrated infrastructure systems for some workloads.

- As more vendors support hybrid and public cloud deployments, hyperconvergence is a stepping stone toward public cloud agility as suppliers are expanding hybrid cloud deployment offerings for cloud-native applications.

- A number of niche hyperconvergence suppliers offer scale-down solutions to address the needs of remote office/branch office (ROBO) and edge environments.

Obstacles

- Applications designed for scale-up architectures (as opposed to scale-out ones) are unlikely to meet cost or performance expectations when deployed on hyperconverged infrastructure.

- The acquisition cost of hyperconvergence may be higher, and the resource utilization rate lower than for three-tier architectures.

- While HCI has somewhat matured from a hypervisor compute and storage function, software defined in networking is split between the obsolete software-defined networking (SDN) and networking around software-defined WAN (SD-WAN), driving edge deployments.

- For large organizations, hyperconverged deployments will remain another silo to manage.

User Recommendations

- Implement hyperconvergence for hybrid cloud infrastructure and cloud-native applications when agility, modular growth and management simplicity are of greatest importance.
- Establish that hyperconvergence requires alignment of compute, network and storage refresh cycles; consolidation of budgets; operations and capacity planning roles; and retraining for organizations still operating separate silos.
- Test the impact on disaster recovery and networking under a variety of failure scenarios, as solutions vary greatly in performance under failure, their time to return to a fully protected state and the number of failures they can tolerate.
- Ensure that clusters are sufficiently large to meet performance and availability requirements during single and double node failures, and require proofs of concept to reveal any performance anomalies.

Sample Vendors

Cisco; Dell; Microsoft; Nutanix; Sangfor; Scale Computing; StorMagic; VMware

Gartner Recommended Reading

Market Guide for Full-Stack Hyperconverged Infrastructure Software

Gartner Peer Insights 'Voice of the Customer': Hyperconverged Infrastructure Software

Market Guide for Integrated Systems

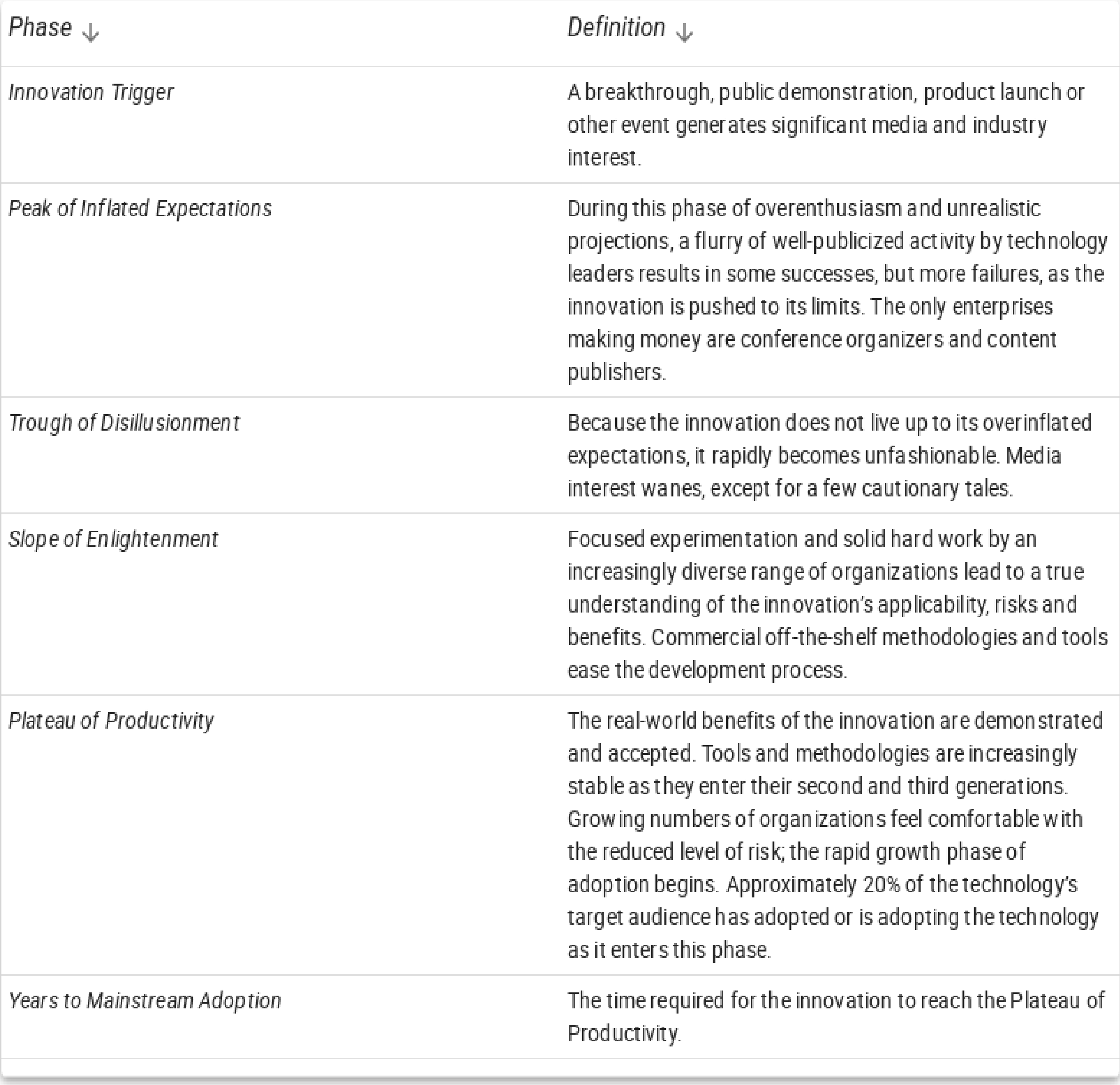
Appendixes

See the previous Hype Cycle: Hype Cycle for Storage and Data Protection Technologies, 2022

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)



Phase ↓	Definition ↓
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

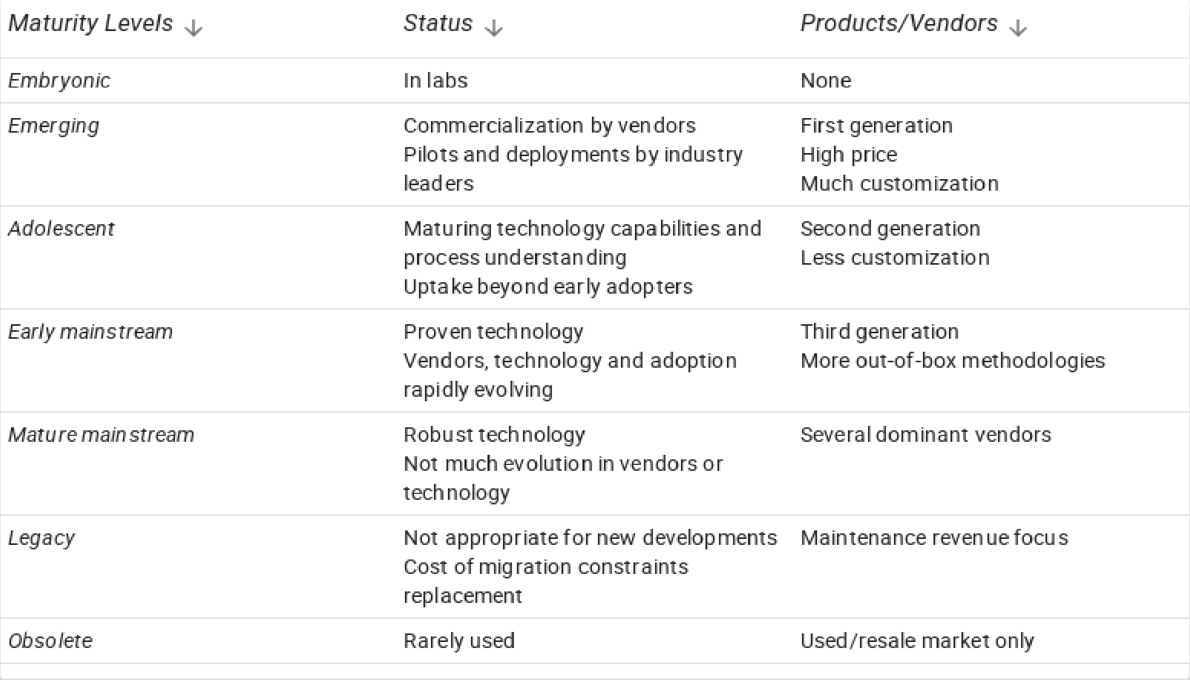
Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)



Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constraints replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Document Revision History

Hype Cycle for Storage and Data Protection Technologies, 2022 - 1 July 2022

Hype Cycle for Storage and Data Protection Technologies, 2021 - 22 July 2021

Hype Cycle for Storage and Data Protection Technologies, 2020 - 6 July 2020

Hype Cycle for Storage and Data Protection Technologies, 2019 - 11 July 2019

Hype Cycle for Storage Technologies, 2018 - 13 July 2018

Hype Cycle for Storage Technologies, 2017 - 19 July 2017

Hype Cycle for Storage Technologies, 2016 - 5 July 2016

Hype Cycle for Storage Technologies, 2015 - 13 July 2015

Hype Cycle for Storage Technologies, 2014 - 23 July 2014

Hype Cycle for Storage Technologies, 2013 - 24 July 2013

Hype Cycle for Storage Technologies, 2012 - 5 July 2012

Hype Cycle for Storage Technologies, 2011 - 26 July 2011

Hype Cycle for Storage Technologies, 2010 - 13 July 2010

Hype Cycle for Storage Hardware Technologies, 2009 - 17 July 2009

Hype Cycle for Storage Hardware Technologies, 2008 - 11 June 2008

Hype Cycle for Storage Hardware Technologies, 2007 - 19 June 2007

Hype Cycle for Storage Hardware Technologies, 2006 - 24 August 2006

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Modernize Your File Storage and Data Services for the Hybrid Cloud Future

Emerging Tech Impact Radar: Compute and Storage

Magic Quadrant for Distributed File Systems and Object Storage

Market Guide for Hybrid Cloud Storage

Innovation Insight: Rethink Your Enterprise Storage and Cloud Data Services Strategies for the Edge Awakening

Leverage Storage as a Service Platform SLAs and Capabilities to Transform IT Outcomes

Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware

Top Trends in Enterprise Data Storage 2023

Table 1: Priority Matrix for Storage and Data Protection Technologies, 2023

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		Software-Defined Storage		
High	Hyperconvergence	Container-Native Storage Digital Communications Governance Distributed File Systems Hybrid Cloud Storage Immutable Data Vault Object Storage Storage as a Service	Cloud Data Backup Cloud Infrastructure Recovery Assurance Software Cyberstorage Data Storage Management Services DNA Storage Function Accelerator Cards NVMe-oF	
Moderate		Isolated Recovery Environment Open-Source Storage	Computational Storage Container Backup Data Discovery Edge Storage Hybrid Cloud File Data Services	
Low				

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase ↓	*Definition* ↓
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase ↓	*Definition* ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constraints replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)