GIGAOM

SONAR REPORT
CLOUD, INFRASTRUCTURE, & MANAGEMENT
RANSOMWARE PROTECTION: BLOCK-BASED STORAGE

Max Mortillaro, Arjan Timmerman

Sep 7, 2022

GigaOm Sonar Report for Block-Based Primary Storage Ransomware Protection

An Exploration of Cutting-Edge Solutions and Technologies

Cloud & Infrastructure

GigaOm Sonar Report for Block-Based Primary Storage Ransomware Protection

An Exploration of Cutting-Edge Solutions and Technologies

Table of Contents

1. Summary

Ransomware is a specific type of malware that encrypts data assets on primary storage systems—including file shares, databases, disk partitions, data volumes, backup systems, and repositories—making them inaccessible unless the victim pays an extortion fee. Ransomware is highly optimized to spread across networks, organizations, and infrastructure systems through methods similar to trojan attacks. The ransomware payload is embedded in a file that looks legitimate and is triggered by an unsuspecting user opening the infected file. Usually, it will spread across the environment by taking advantage of user credentials as well as documented and undocumented exploits, bypassing the limited access scope of a user. As such, ransomware protection is a transversal, cross-stack topic across organizations.

Ransomware attacks can impact file- and block-based primary storage solutions alike:

- **File-based** ransomware attacks are the most pervasive. Advanced file-based ransomware implementations use a combination of techniques to remain unnoticed and spread silently. For example, they start encryption activities a few weeks or months after a system has been infiltrated, or they first target dormant files that haven't been accessed for a significant time.
- **Block-based** ransomware attacks, while less common, can be even more damaging. In this case, ransomware encrypts entire data volumes, making recovery much harder than it is for file-based attacks. The entire volume must be recovered, offering less granularity and fewer recovery prioritization options than for file-based recovery activities. These attacks, however, are quicker and easier to detect because once a volume is encrypted, all read/write operations become impossible.

This report focuses on ransomware protection solutions available for block-based primary storage systems, while a sister report covers solutions for file-based—or network attached storage (NAS)—primary storage systems.

Although dedicated out-of-band ransomware protection solutions exist, organizations should not underestimate the benefits of in-band ransomware protection capabilities that are embedded in block storage solutions. The most effective mitigations include a combination of in-band and out-of-band capabilities, but for smaller businesses or cost-conscious organizations, block storage ransomware protection solutions constitute an important first line of defense.

Benefits of ransomware protection on block storage include:

- **Faster recovery** from a ransomware attack than backup restores can provide, usually measured in minutes instead of hours or days, thanks to snapshots. This is particularly crucial for mission-critical applications that can't withstand prolonged downtimes.
- **Greater ease of use** because reverting to a healthy snapshot takes considerably less effort than identifying and orchestrating data recovery from a data protection platform.
- **Cost-effective** protection and recovery operations: Block storage ransomware protection solutions are usually provided at no cost and deliver a very effective protection layer. Furthermore, fast local recovery from ransomware is cheaper than recovery from data protection systems, both from a recovery time and a human effort perspective. In addition, organizations avoid paying any potential egress transfer fees when restoring from the cloud.

How We Got Here

Ransomware attacks have become a prevalent and persistent threat for all organizations across all industries and sizes of business. While these attacks frequently made headlines a few years ago, they've now become so widespread that only the most spectacular cases are mentioned in the news media today.

Organizations assess business risk by evaluating the probability of an event occurring and correlating this probability with the impact (the extent of possible damage), usually through a risk assessment matrix. The impact can be diverse, ranging from negligible to widespread, but regardless of the physical manifestation, outcomes are generally summed up in three categories: financial (loss of revenue), regulatory (increased scrutiny, fines, and eventually the loss of license for regulated businesses), and reputational (loss of trust from customers).

Ransomware is particularly concerning for organizations because it combines a high probability of happening with a widespread impact, not only in terms of locations and systems affected but also in terms of damage. Ransomware can bring businesses and government agencies to their knees, forcing them to choose between paying a hefty ransom or risk losing production capacity and revenue for weeks, if not months.

Ransomware does not discriminate among infrastructure layers; once in, it will attempt to encrypt all of an organization's assets within reach, which is why proper segmentation of access and networks is important. Organizations usually implement several data protection layers, including data protection (backups and disaster recovery), security at the network layer, and authentication mechanisms to reduce the attack surface. However, relying solely on backups should be avoided for the following reasons:

- Primary data is the most up-to-date data repository available in the organization. Large enterprises can have a significant delta between production data and data backups, especially if the data has elevated change rates.
- Losing primary data and having to restore it from data protection platforms is a time-intensive process, limited by the throughput of the backup media and network bandwidth, especially if protected data resides on the cloud.
- For cloud-based data protection, data retrieval could incur egress transfer fees, which can add up quickly as more data and systems need to be recovered.

Because primary data is the first point of impact for ransomware attacks, it’s advisable to implement primary storage solutions that incorporate ransomware protection. Timely identification, alerting, and mitigation are preferable to dealing with the aftermath of a ransomware attack and its severe impact from a financial, regulatory, and reputational perspective.

ABOUT THE GIGAOM SONAR REPORT

This GigaOm report is focused on emerging technologies and market segments. It helps organizations of all sizes to understand the technology and how it can fit in the overall IT strategy, its strengths, and its weaknesses. The report is organized into five sections:

Overview: An overview of the technology, its major benefits, and possible use cases, as well as an exploration of product implementations already available in the market.

Considerations for Adoption: An analysis of the potential risks and benefits of introducing products based on this technology in an enterprise IT scenario, including table stakes and key differentiating features, as well as consideration on how to integrate the new product with the existing environment.

GigaOm Sonar Chart: A graphical representation of the market and its most important players focused on their value proposition and their roadmaps for the future.

Vendor Insights: This section provides a breakdown of each vendor’s offering in the sector, scored across key characteristics for enterprise adoption.

Near-Term Roadmap: A 12- to 18-month forecast of the future development of the technology, its ecosystem, and major players of this market segment.

2. Overview

To briefly recapitulate, primary storage ransomware protection solutions emerged in response to the growing prevalence and damaging impact of ransomware attacks. These attacks focus on encrypting data at rest that resides on primary storage systems, including file shares, databases, data volumes, and disk partitions—for example, in virtual machines (VMs). The most sophisticated ransomware also goes one step further and actively targets backup systems and repositories as well to cause maximum damage.

This report focuses on ransomware protection capabilities present in block-based primary storage.

Even if block storage systems are not primary vectors of ransomware spread, they are still targets for ransomware:

- Block storage often serves large virtualization environments and mission-critical applications.
- VMs running on block storage can be impacted at the operating system layer by ransomware, with volumes getting encrypted and becoming unreadable.
- Side attacks using credential theft can enable an attacker to gain access to block storage, allowing them to delete snapshots, thus depriving organizations of the ability to revert to a healthy state.

Without proper controls (for example, segmentation of data, least-privilege access, and stringent permissions), block storage repositories become easy targets for the uncontrolled spread of ransomware.

Main Components

The goal of ransomware protection on primary storage is to act as the first line of defense by mitigating threats and ensuring primary data remains protected, thus ensuring continuity of operations. Primary storage solutions can provide ransomware protection in various ways, from very simple capabilities to the most advanced implementations.

Immutable snapshots provide the most basic level of protection. These allow administrators to revert to a healthy state if data is compromised by ransomware. While foundational for ransomware protection, this feature is reactive and doesn't provide proactive insights. It's only after the environment has been hit and the ransomware detected that administrators can use immutable snapshots to recover from the attack.

Combining immutable snapshots with other techniques, such as replication, provides an intermediary level of protection. In this case, snapshot data is replicated to a dedicated, isolated system or to the cloud. Additional capabilities, such as basic detection and snapshot recovery orchestration may also be included.

The most advanced implementations provide sophisticated ransomware identification algorithms trained using artificial intelligence and machine learning (AI/ML) models. They're able to analyze a broad range of patterns and anomalous behaviors and correlate seemingly isolated incidents to identify potentially harmful scenarios. These detection patterns include usual activity times in a given geographic area, data types typically accessed (including user access patterns), as well as large-scale file operations across folders and shares. In addition, advanced solutions implement proactive mitigation strategies, such as the identification of systems and accounts that are the source of these changes, the ability to revoke access of potentially impacted users and systems, and the possibility of cutting off access to parts or all of the affected file systems. Finally, these solutions integrate with monitoring and artificial intelligence operations (AIOps) platforms, providing comprehensive alerting and active mitigation options.

Ransomware creators implement various techniques to avoid immediate detection. For example, ransomware can make its way into an organization's environment but stay dormant for weeks or months. It can also perform staggered activities, affecting only a few files at a time, usually those that haven't been accessed for months or years. However, this focus on old files, unnoticed by humans, is easy for the storage platform to identify.

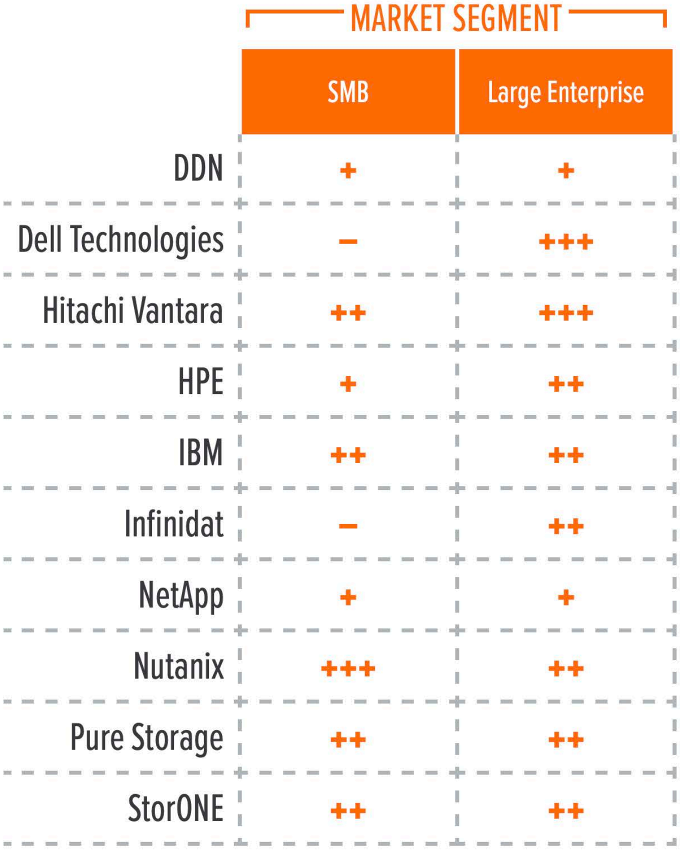
With the growth of ransomware protection solutions and the increased focus on proactive monitoring, the concept of encrypting old files first in an indiscriminate manner is losing its appeal, and may make room for random patterns that are more difficult to identify. On the other hand, AI-based ransomware protection solutions are regularly updated and trained to catch up with new threat models and identify them.

Market Segment

To better understand the market and vendor positioning, we assess how well block-based primary storage solutions with integrated ransomware protection are positioned to serve specific market segments (**Table 1**). Note that we're only looking at ransomware capabilities offered by primary storage vendors, not at dedicated, standalone ransomware protection solutions.

- **Small-to-medium business (SMB):** In this category, we assess solutions on their ability to meet the needs of organizations ranging from small businesses to medium-sized companies, including departmental use cases in large enterprises. For these use cases, the solution should provide a turnkey experience and a complete feature set suited for the IT generalist. The solution should compensate for the limited resources of these organizations and the unavailability of dedicated personnel, whether IT specialists or information security experts.
- **Large enterprise:** Here, offerings are assessed on their ability to support large and business-critical projects. Optimal solutions in this category will focus on the feature set depth, and integration with existing enterprise tools, such as data protection solutions, information security tools, AIOps, and ITSM platforms. Scalability and flexibility are key to successful enterprise adoption.

Table 1. Market Segment



	MARKET SEGMENT	
	SMB	Large Enterprise
DDN	+	+
Dell Technologies	−	+++
Hitachi Vantara	++	+++
HPE	+	++
IBM	++	++
Infinidat	−	++
NetApp	+	+
Nutanix	+++	++
Pure Storage	++	++
StorONE	++	++

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
− Not applicable or absent

Source: GigaOm 2022

3. Considerations for Adoption

The purchase drivers for adopting ransomware protection deployed on block-based primary storage are very clear. The only potential downside is that a storage system embedding advanced ransomware protection may be more expensive than a storage system without such capabilities. On the other hand, the benefits are so overwhelming that organizations should seriously consider whether purchasing a storage solution *without* ransomware protection capabilities makes sense.

Prospective customers should carefully consider the following when evaluating solutions: first, how the primary storage ransomware protection fits within their overall security, threat, and ransomware protection posture; and second, how the solution integrates with their broader threat mitigation strategy.

A primary storage solution that provides only immutable snapshots as a ransomware protection layer would be acceptable for an organization that has invested in advanced, dedicated ransomware protection solutions. However, this would be insufficient for an SMB that can't afford the same investment in a dedicated ransomware solution.

Similarly, a large organization with a heterogeneous storage infrastructure might question the benefits of a deeply integrated and advanced ransomware protection solution that is proprietary to a single storage vendor.

Another consideration is the scope of a given solution compared to the broader infrastructure footprint. If the customer manages other storage types (NAS, for example) and one vendor's solution supports both file and block systems, this could be an advantageous choice for the organization.

In any case, determining the current security posture of an organization, where it plans to go, and the available budget will help further refine the appropriate adoption criteria.

Key Characteristics for Enterprise Adoption

Here we explore the key characteristics that may influence enterprise adoption of the technology based on attributes or capabilities offered by some vendors but not others. These criteria will be the basis on which organizations decide which solutions to adopt for their particular needs. These key characteristics are:

- Architecture
- Proactive identification
- Mitigation and recovery
- Management
- Licensing

Architecture

The design, implementation, and feature set of ransomware protection solutions can impact scalability, performance, and efficiency. Solutions tightly embedded within the storage platform will provide immediate results but will lack the kind of global view that is better able to identify anomalous patterns happening either at scale or in specific locations.

Proactive Identification

Basic ransomware protection features such as snapshots and continuous data protection are now taken for granted. Ransomware infection patterns are nearly imperceptible to IT personnel, who often realize the extent and impact of a ransomware attack only after it's too late to react. Advanced ransomware protection systems are trained on ransomware behavioral patterns that can identify anomalous behavior by analyzing file system changes in real time.

Mitigation and Recovery

Although timely identification of infection patterns is crucial, alerting is not sufficient. The solution should implement techniques to isolate encrypted data and contain the spread; for example, by terminating active connections to the file system or temporarily restricting access. Similarly, it must implement methods to recover the impacted data easily.

Management

Monitoring and alerting capabilities and the ability to visualize threats and their impact are essential. The solution should include a management interface with proactive alerting capabilities, and integrate with enterprise system management solutions, AIOps, and IT service management (ITSM) tools.

Licensing

Regardless of the architecture and deployment model, some ransomware protection features are included in the storage solution feature set at no cost, while more advanced solutions might be licensed separately. However, some vendors do offer advanced protection as an integral part of the storage system.

Table 2 shows the principal features that can affect the adoption of ransomware protection for block-based primary storage systems and how well each is implemented in the solutions assessed in this report.

Table 2. Key Characteristics Affecting Enterprise Adoption

	KEY CRITERIA				
	Architecture	Proactive Identification	Mitigation & Recovery	Management	Licensing
DDN	+	+	+	++	+++
Dell Technologies	++	+++	++	++	++
Hitachi Vantara	++	+++	+++	++	++
HPE	++	+++	++	++	+++
IBM	++	+	++	++	++
Infinidat	+++	+++	+++	++	++
NetApp	++	+	++	++	++
Nutanix	++	++	++	++	++
Pure Storage	+++	–	+++	+++	+++
StorONE	++	++	++	++	+++

+++ Exceptional: Outstanding focus and execution

++ Capable: Good but with room for improvement

+ Limited: Lacking in execution and use cases

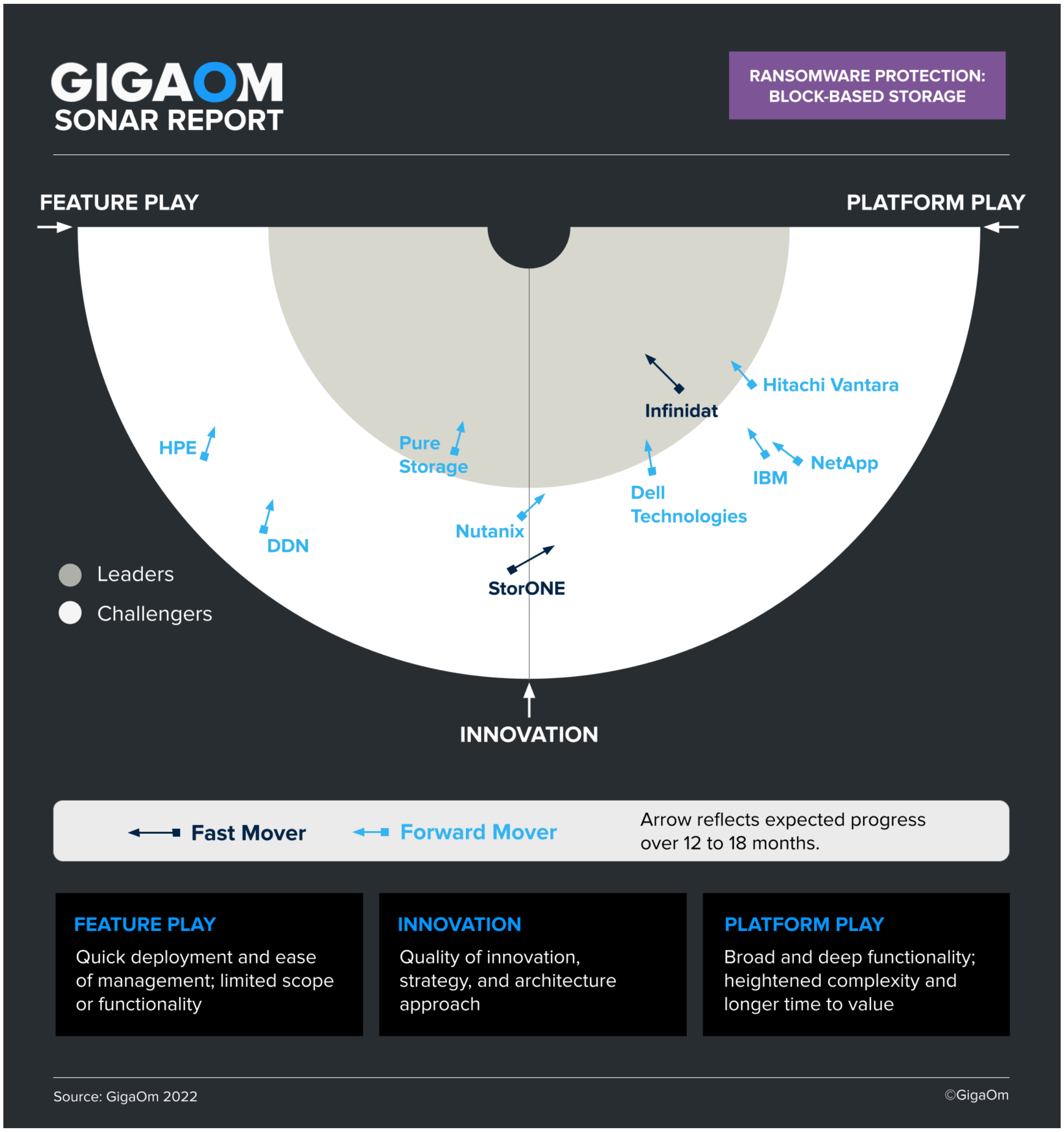
– Not applicable or absent

Source: GigaOm 2022

4. GigaOm Sonar

The GigaOm Sonar provides a forward-looking analysis of vendor solutions in a nascent or emerging technology sector. It assesses each vendor on its innovation and architecture approach, while determining where each solution sits in terms of enabling rapid time to value (Feature Play) versus delivering a complex and robust solution (Platform Play).

The GigaOm Sonar chart (**Figure 1**) plots the current position of each solution against these three criteria across a field of concentric semi-circles, with solutions set closer to the center judged to be of higher overall value. The forward-looking progress of vendors is further depicted by arrows that show the expected direction of movement over a period of 12 to 18 months.



Arrow reflects expected progress over 12 to 18 months.

FEATURE PLAY
Quick deployment and ease of management; limited scope or functionality

INNOVATION
Quality of innovation, strategy, and architecture approach

PLATFORM PLAY
Broad and deep functionality; heightened complexity and longer time to value

Source: GigaOm 2022

©GigaOm

Figure 1. GigaOm Sonar for Block-Based Primary Storage Ransomware Protection

As you can see in the Sonar chart in **Figure 1**, there are three groups of vendors. On the Platform-Play side, the first group contains solutions with a strategic, longer-term approach. Infinidat offers a complete and balanced ransomware protection solution with InfiniGuard Cyber Recovery, which can provide outstanding value to organizations. Dell Technologies deals with a broader solution portfolio and is gradually implementing ransomware protection capabilities within its products. The PowerMax storage platform currently offers a complete implementation, and those features will trickle down to its PowerStore and PowerFlex platforms. Hitachi Vantara has a different approach, based on integration with its rich ecosystem of monitoring and data management software. The company is focusing on adding ransomware capabilities to both block and object storage (although object storage is not in scope for this report). Finally, IBM delivers solid foundational orchestration and recovery capabilities; however, ransomware detection capabilities are currently unavailable for general purpose workloads.

In the middle is the second group, consisting of innovative solutions with a fast time-to-value approach. These are faster to implement than the first group, but the breadth of features is currently incomplete in some areas. Some of the evaluated companies are moving to close this gap. Pure Storage is leading in this area with its SafeMode snapshots, strong multifactor authentication (MFA), and verification mechanisms. Basic proactive detection capabilities are provided through Pure1, but advanced capabilities are still on the roadmap. Nutanix offers comprehensive analytics, hardening and immutable snapshots with instant recovery, with a strong focus on proactive detection at the network layer. StorONE offers a well-balanced solution and has a good roadmap to further improve its feature set.

On the Feature-Play side, the third group consists of vendors with a feature-focused approach. HPE offers strong foundational capabilities (notably on the Alletra 9000) but heavily relies on a building-block approach. It requires skilled architects to properly comprehend features and capabilities across HPE's portfolio and integrate them into a comprehensive solution. NetApp has a strong roadmap for file-based ransomware protection but its scope for block storage ransomware protection is smaller, although some innovations in zero-trust security are worth noting. DDN offers a basic set of ransomware protection features, including immutable snapshots and cloud-based monitoring capabilities, which can be used to indirectly observe potential ransomware activity.

5. Vendor Insights

DDN

Among DDN's storage solutions, the IntelliFlash platform delivers unified file and block storage capabilities and includes features to protect against ransomware attacks: IntelliCare for detection and IntelliFlash immutable snapshots for remediation.

From a detection perspective, IntelliFlash leverages the IntelliCare Cloud Analytics platform to identify unusual storage growth (which can often indicate ransomware activity) and generate alerts.

If a ransomware attack is confirmed, IntelliFlash snapshots can be used to rapidly revert to a prior healthy state. The snapshots can be scheduled and enabled from IntelliFlash's management interface with the capability to land snapshots on-premises, in the cloud, or both, including options to store data at multiple locations.

Both IntelliFlash snapshot capabilities and the IntelliCare Cloud Analytics platform are part of the base DDN feature set.

Strengths: DDN provides a basic set of ransomware protection features on its IntelliFlash platform, including basic monitoring capabilities and immutable snapshots.

Challenges: Detection capabilities are limited and indirect. There is no recovery orchestration.

Dell Technologies

Dell Technologies currently provides comprehensive ransomware protection capabilities on its PowerMax storage appliances. The solution combines immutable snapshots and proactive detection and is complemented by air-gapped backups.

Proactive detection capabilities are delivered through CloudIQ, Dell's AIOps platform. PowerMax provides telemetry data to CloudIQ, which monitors and detects anomalies in near real time, assesses adherence to security baselines, and identifies security incidents such as potential ransomware attacks. Alerts are subsequently generated and pushed to administrators through a variety of methods. The solution also integrates with ITSM and SIEM platforms to automatically create incidents and initiate incident investigation activities.

From a mitigation perspective, PowerMax snapshots are natively immutable (read-only). To prevent their intentional deletion by a malicious user, Dell Technologies added another layer of security with Secure Snapshots, a policy-based feature that prevents accidental or malicious deletion of immutable snapshots (even by administrators) for the entire duration of the defined lock period. PowerMax snapshots can also be replicated to S3 object storage in the cloud, providing additional immutability options. The solution also includes anti-tampering measures to protect against time server drift and premature expiration of the lock duration on Secure Snapshots.

Recovery-wise, organizations can define set-and-forget snapshot policies with frequent intervals, allowing RPOs as low as 10 minutes. Although adjacent to primary storage ransomware protection and not evaluated in this report, it's worth mentioning that Dell Technologies offers integrations with PowerProtect Cyber Recovery, an independent product that can be used with any storage platform. This allows data backup from a PowerMax to a Dell PowerProtect appliance and to have this backup replicated to another air-gapped PowerProtect appliance. Moreover, Dell Technologies also provides the ability to scan and recover last valid data copies with Cyber Sense, a solution that scans vaulted backups performed with PowerProtect Cyber Recovery. In addition, native air gap is also available through SRDF on PowerMax.

Secure Snapshots are a standard PowerMax feature. Dell Technologies CloudIQ is provided as a part of a customer's support contract, at no extra cost. The solution was conceived to support the broadest range of Dell Technologies products, including storage solutions, data protection platforms/ appliances, servers, HCI solutions, and Dell networking products. As such, it offers complete support and visibility across storage systems and geo locations.

Regarding other block storage solutions in Dell Technologies' portfolio, the PowerMax capabilities are expected to gradually come to the PowerStore platform in 2023. The PowerFlex solution also supports Secure Snapshots and PowerProtect Cyber Recovery vault.

Strengths: Dell offers solid ransomware protection capabilities on its PowerMax platform, combining true snapshot immutability with an AIOps platform capable of identifying ransomware attacks.

Challenges: Support is currently limited to PowerMax storage arrays. Some features could be added such as multi-user validation, and proactive termination of access.

Hitachi Vantara

Hitachi Vantara has traditionally targeted its products at medium and large organizations. Those systems use the same OS and expose the same feature set, enabling users to design their infrastructures with consistent characteristics at the core and the edge. And this holds true for its ransomware protection as well, both for block and file storage.

Proactive detection capabilities are delivered through Ops Center Analyzer, Hitachi's AIOps platform. Ops Center Analyzer analyzes I/O patterns and correlates them with threat types, informing administrators via alerts automatically, letting them know whether a ransomware attack is in progress or if a data exfiltration activity is happening.

To mitigate ransomware, the solution uses the Hitachi Data Retention Utility orchestrated through Hitachi Ops Center Protector. This tool is part of the Hitachi storage OS that's included with all Hitachi VSP arrays at no additional cost. It provides options to lock logical storage devices or volumes to prevent any modifications, such as host writes or array management operations. These locks can't be removed before a specified retention period.

From a recovery perspective, organizations can easily set immutable snapshot policies with frequent intervals, enabling low RPOs. Hitachi's OpsCenter Protector offers a full set of copy data management capabilities for snapshots, clones, and more. This allows data to be backed up from a VSP system and have this backup replicated to another air-gapped VSP system. Finally, Hitachi can also scan and recover last valid data copies through CyberVR, a complementary cyber resiliency solution that Hitachi recommends for specific use cases where automated data recovery orchestration from ransomware is required across a large VM environment (hundreds of VMs) or more advanced ransomware security testing and forensics is required.

To protect data from ransomware, and as an overall management interface, Hitachi Ops Center suite is a must. This management suite, which includes Ops Center Protector and Ops Center Analyzer, is bundled in the base software package at no additional cost with each Hitachi VSP storage system. These tools enable protection against ransomware that is effective and scalable and can be increasingly automated.

Hitachi offers a broad range of ransomware protection for its primary storage offerings. The Hitachi Ops Center suite provides the right tooling to analyze and protect data from ransomware while allowing quick recovery from an attack. Although the solution is extensive and effective, it still requires external solutions, like CyberVR, to accomplish a secure environment that can detect and protect the data.

Strengths: Hitachi offers good ransomware protection on its VSP platform, with great snapshot immutability. The Hitachi Ops Center platform can identify and protect against ransomware attacks.

Challenges: Ransomware protection and recovery capabilities are spread across multiple tools; Hitachi could improve manageability through consolidating its toolset, which would be useful for end users.

HPE

HPE takes a layered and modular approach to ransomware data protection, using a blend of features available on its block storage systems, its HPE Infosights AIOps platform, and other portfolio components.

Focusing solely on components in scope for this report, proactive detection capabilities are delivered by HPE Infosight. Though not specifically designed for ransomware protection, it uses sophisticated techniques, including machine learning, to detect and report anomalies that can indicate an active ransomware attack. Although Infosight compares workload characteristics against historical trends, it can also tap into normalized and anonymized baselines for similar workloads that are collected across HPE's entire customer base.

HPE implements a feature branded Virtual Lock, which was originally on 3PAR systems and is now available on Alletra 9000 systems and on HPE Primera storage arrays. The Virtual Lock function, originally implemented for compliance purposes to prevent deletion of volumes, is used to protect snapshots intended for ransomware recovery by locking immutable, read-only snapshots on storage arrays, effectively preventing volume copies or the accidental or intentional deletion of volumes. Organizations can define a custom retention period during which deletion is impossible, even by administrators with the highest privilege level.

In addition, Alletra 9000 includes time-server tampering protection features. A time change can't be forced on the system, which prevents an attacker from prematurely and artificially expiring the immutability period on snapshots. The only way to force a time change is to fully factory reset the Alletra 9000, which would mean an attacker can't access and encrypt the data and demand a ransom for its recovery.

HPE offers various snapshot replication and protection topologies for Alletra 9000 and Virtual Lock, some of which include HPE StoreOnce backup appliances (which also offer immutable snapshots). There are also integrations with third-party data-protection solutions (including HPE Zerto), and some of these solutions can be used to create "clean rooms" that create multiple levels of mitigation and data protection.

On the Alletra 6000 platform, HPE takes a different approach, with strong MFA and multi-user authorization. The Alletra 6000 snapshots are not immutable; however, snapshot deletion can be configured to require two different administrators to authorize the operation. Once enabled, this policy can’t be deactivated or overridden.

All these capabilities are core features of the storage platforms discussed here and do not incur extra licensing.

Strengths: HPE offers a modular and realistic approach to combating ransomware, with a number of built-in capabilities that large organizations can integrate into their broader ransomware protection strategy.

Challenges: Although multi-user authorization provides increased protection on HPE Alletra 6000 systems, snapshots aren’t immutable. HPE’s approach requires an architectural mindset to correctly tie all the building blocks together.

IBM

IBM supports ransomware protection capabilities on its block storage product line that runs IBM Spectrum Virtualize, the operating system that powers IBM FlashSystem appliances, and IBM Storage Volume Controller (SVC).

The solution’s feature set focuses primarily on snapshot immutability, orchestration, and recovery to a healthy state after a ransomware attack. To achieve this goal, it relies on IBM Safeguarded Copy (SGC), a technology that provides immutable copies of data on a FlashSystem or SVC, and on IBM Copy Services Manager (CSM), an external automation and scheduling tool. IBM CSM provides crash consistency and facilitates creating, cataloging, and recovery of SGC snapshots. It’s worth mentioning that SGC is also available on IBM DS8000 storage systems.

The solution is branded IBM FlashSystem Cyber Vault and constitutes a framework for automating the processes required to proactively use SGC to perform data validation and recovery when a ransomware attack has occurred.

Technically, Cyber Vault requires a dedicated FlashSystem environment and is deployed in a dedicated clean room/sandbox environment isolated from production, with CSM handling the scheduling of SGC snapshots. These snapshots are immutable and can't be altered or deleted. Recovery happens on separate recovery volumes, which can be used for data validation, forensic analysis, and restoration of production data.

IBM recently announced the availability of IBM Spectrum Sentinel, a solution that builds on SGC and uses anomaly detection and ML to identify potential threats. Spectrum Sentinel can create immutable application-specific snapshots on primary storage and orchestrate recovery from verified and validated backup copies. In this first release, support is limited to the Caché and Iris databases used by the EPIC healthcare system. IBM plans to support additional workloads with SAP HANA in the second half of 2022 and other major databases in 2023.

For other workloads, early warning signs of an attack can be provided by IBM Storage Insights or IBM Spectrum Control. Both solutions can analyze current I/O workload against previous usage baseline and help provide indications that an attack is in progress. Organizations can set up alerts that indicate an attack may be happening by combining multiple triggers. For example, a sudden drop in data reduction efficiency could indicate vast amounts of data getting encrypted, rendering deduplication and compression ineffective.

IBM also recommends monitoring write change rate for deviations and anomalies as well as integration with SIEM platforms (such as IBM QRadar) for better visibility.

From a licensing perspective, SGC is included in the FlashSystem product line except for the 5000 model.

Strengths: IBM Cyber Vault provides a robust ransomware protection framework focused on data isolation and controlled recovery, with some capabilities to forecast potential attacks.

Challenges: There are currently no AI/ML-based detection capabilities. The solution requires a dedicated FlashSystem or SVC environment to operate, and while this provides increased security, it also increases the cost of the solution. Spectrum Sentinel is promising, but the solution's scope is currently very limited.

Infinidat

Infinidat boasts a modern, AI-based hybrid storage architecture that delivers a no-compromise feature set with compelling $/GB and $/IOPS figures. To achieve this, its InfiniBox storage system takes advantage of a data path designed around a combination of DRAM, flash memory, and hard disk drives associated with sophisticated AI-based caching technology to optimize data placement.

Ransomware protection is delivered through the InfiniGuard solution, which offers modern data protection, backup, disaster recovery, and business continuity features. InfiniGuard offers backup and recovery performance, at scale, covering all data protection needs and is enhanced with InfiniSafe cyber recovery technologies to ensure the customer is ready in the event of a cyberattack. While originally announced on the InfiniGuard platform in February 2022, InfiniSafe was expanded to the InfiniBox and InfiniBox SSA platforms in April 2022.

Branded InfiniGuard CyberRecovery, this technology provides immutable snapshot copies of source data sets that incorporate logical air-gapping—both local and remote. When a customer has a cyberattack, they can move the copies into a secure, fenced network to check for malware or ransomware. Once a known good copy of the data set is identified, the customer can make a near-instantaneous recovery of the known good copy, and in only minutes for petabyte-scale backup datasets.

In August 2022, Infinidat announced InfiniSafe Cyber Storage guarantees for the InfiniBox and InfiniBox SSA platforms. Not only will Infinidat guarantee that the immutable snapshot is immutable, but it will also guarantee recovery of the immutable snapshot in one minute or less, regardless of dataset size.

InfiniSafe brings together the key foundational requirements essential for delivering comprehensive cyber-recovery capabilities with immutable snapshots, logical air-gapped protection, a fenced forensic network, and near-instantaneous recovery of backups of any repository size.

Infinidat offerings are focused on customers with very large datasets. In petabyte-scale environments, ensuring fast and secure data is an enormous undertaking, and InfiniGuard helps customers protect their environments with InfiniSafe technologies, which are included with the InfiniGuard solution at no additional cost.

An area that requires further attention is the ability to deliver better proactive identification of anomalous behavior.

Strengths: InfiniGuard delivers solid cybersecurity features at no extra cost, allowing customers to quickly and securely restore data, even at scale, in case of an attack.

Challenges: Proactive identification is still limited and needs improvement.

NetApp

NetApp implements a comprehensive ransomware protection strategy across its product portfolio, both for on-premises and cloud workloads, with multiple layers of protection.

Most NetApp anti-ransomware capabilities are focused on proactive data identification and recovery, making them particularly suitable for SMB/NFS volumes. For block volumes, organizations can take advantage of ONTAP immutable snapshots. These snapshots can be configured and scheduled via policies and can be replicated either locally or in the cloud (with Cloud Volumes ONTAP). In addition, NetApp includes SnapCenter, a tool that orchestrates the creation and replication of application-consistent snapshots, which can be replicated to a remote location and used to recover from ransomware attacks.

Since May 2022, NetApp has offered multiple-administrator verification for sensitive operations . This can prevent unauthorized changes made by one person to snapshot and replication policies, immutability settings, snapshot deletion, and more.

The capabilities are included in NetApp ONTAP and come at no extra cost.

Strengths: NetApp offers immutable snapshots and flexible replication options to the cloud for block storage ransomware protection.

Challenges: Although NetApp ransomware protection capabilities are significant for file-based storage systems, capabilities for block storage systems remain limited.

Nutanix

Nutanix provides a comprehensive platform with varied storage capabilities that go beyond its initial HCI scope. Its solution, Nutanix Unified Storage, delivers native file, block, and object capabilities through its suite of products. In the context of primary block storage, the solution delivers these capabilities through the Nutanix Volumes service.

Where Nutanix Files leverages integrated ransomware protection and Nutanix Data Lens to proactively detect ransomware, Nutanix Volumes handles block storage, and so uses a different solution to identify ransomware threats. This is done through Nutanix Flow Security Central, a feature of Nutanix Flow. Flow Security Central monitors for network anomalies and malicious behavior as well as common network attacks that propagate and look for vulnerabilities to further infiltrate the network and spread ransomware. Flow Security Central also monitors endpoints such as VMs to identify malicious traffic.

From a mitigation and recovery perspective, Nutanix Volumes provides immutable snapshots, preventing tampering and deletion. Those native snapshots can be easily recovered and organizations can take advantage of a secondary level of immutable storage with Nutanix Objects, which also delivers immutable object storage and support for WORM policies.

Nutanix also implements by default hardening features that can be used to prevent ransomware attacks. Adherence to security best practices and monitoring against baseline deviations are handled through Nutanix Flow Security Central, a security-oriented management platform that allows security monitoring and management across multiple Nutanix deployments. The solution also has strong support for compliance, with several standards supported (FIPS, DoDIN APL, and so forth), and embeds a fully fledged STIG compliance setup.

Nutanix Flow Security Central is an add-on for Nutanix Cloud Infrastructure (NCI), a complete software stack to unify hybrid-cloud infrastructure including compute, storage, network, hypervisors and containers, in public or enterprise clouds.

Strengths: Nutanix delivers comprehensive network analytics, security hardening features, and instant data recovery through immutable native snapshots.

Challenges: Detection happens primarily at the network layer rather than the storage layer. The capability is not very useful for organizations implementing a multilayered threat mitigation strategy with proactive detection capabilities.

Pure Storage

Pure Storage offers multiple storage products. Among these, FlashBlade delivers unified fast file and object storage capabilities, while FlashArray focuses on block and file storage.

To protect against ransomware attacks, Pure Storage implements immutable snapshots in both solutions. However, while the data contained in the snapshots is immutable, the snapshots themselves could be deleted by an attacker with rogue administrative access.

A feature called SafeMode Snapshots, built into both storage array types, locks snapshots and prevents their deletion. Instead of the standard deletion process, objects such as volumes or snapshots are destroyed and moved into a staging “destroyed” area for a predefined period (at least 24 hours, and up to 30 days, with Pure Storage recommending at least 14 days of retention). This incompressible timeframe locks any object in the “destroyed” area and prevents it from being wiped until the timer has expired.

SafeMode is built into the storage solution’s operating system,and enabled by default. The solution includes strong MFA and requires at least two authorized contacts (out of five) to carry out changes to SafeMode configuration, along with the Pure Storage support team via a conference call. Each authorized contact is also provided with a six-digit PIN to enhance security. Though this process may seem cumbersome, it ensures maximum security.

SafeMode snapshots are configured through Pure1, Pure Storage’s management, analytics, and support platform. Pure1 can also assess whether SafeMode snapshots are enabled across all Pure storage arrays.

Strengths: SafeMode snapshots provide thorough protection and recovery capabilities against ransomware attacks by combining strong MFA and identity verification mechanisms with strengthened protection against malicious snapshot deletion across file and block products. SafeMode is included in the base feature set, and Pure1 allows organizations to assess global compliance to SafeMode.

Challenges: The solution lacks built-in ransomware detection capabilities.

StorONE

StorONE’s ransomware protection strategy currently relies on using immutable snapshots on its StorONE S1 software-defined storage platform. No special steps are required to make a snapshot immutable as this is the default state of StorONE snapshots. The solution includes proactive detection, and customers are instantly notified if there is unusual activity on one of their volumes.

StorONE immutable snapshots can be created, either ad hoc or scheduled with policy-based frequency and retention periods, via the management interface or API calls. Immutable snapshots can’t be deleted manually while the retention policy is active, and volumes with active snapshots can’t be deleted either.

The new management interface allows these various policies to be created seamlessly, with a visual understanding of how they overlap and a clear view of how long data is effectively retained. Furthermore, different retention policies and snapshot frequencies can be created per S1 instance.

It's worth noting that StorONE's immutable snapshot technology applies to both file and block volumes. When used with file volumes, the snapshots are browsable at the file level, allowing administrators to verify file integrity and recover a given file or subset of files.

Additional features on the vendor's roadmap for 2022 include partial recovery orchestration and protection against NTP server tampering. All current and future capabilities are part of the solution standard feature set and come at no extra cost to customers.

Strengths: StorONE offers good foundational capabilities to mitigate and recover from ransomware attacks, with incremental roadmap improvements planned in 2022.

Challenges: Proactive detection capabilities were recently introduced and have yet to prove their efficiency in the field.

6. Near-Term Roadmap

There's a clear divide among the evaluated solutions in terms of capabilities: Many solutions are already mature in that they provide a broad set of advanced features, including AI/ML-based anomaly detection and proactive remediation.

Regarding less-mature solutions that offer snapshot immutability and/or continuous data protection, implementing proactive threat detection is a possible roadmap direction, but it largely depends on each vendor's ability and appetite to commit R&D resources. Given the amount of effort and cost involved, it's more likely that these solutions' feature sets will remain the same while the vendors seek strategic partnerships with well-established, general-purpose ransomware protection vendors.

Meanwhile, advanced solutions will continue improving their AI/ML detection and training models. While provided as a part of the primary storage management stack, these solutions will remain adjacent to the storage array itself and may eventually be expanded to support heterogeneous environments. Alternatively, they could be spun off as a stand-alone solution, which could be free to use with the vendor's storage platforms, but licensed for use with external storage solutions.

7. Analysts' Take

Although ransomware protection is not new, the increased attack frequency rate is thrusting this discipline more and more into the spotlight. Until recently, data protection, business continuity, and disaster recovery discussions were the primary drivers for ransomware protection solutions.

Organizations were already aware of the need for deep, layered threat protection strategies that implement threat detection and mitigation mechanisms at multiple levels. Similarly, storage vendors acknowledged the ransomware risk and that production data storage systems were often the primary target.

By implementing ransomware protection on primary storage systems, storage vendors enable organizations to strengthen their security posture with proactive identification and mitigation. The most advanced ransomware protection primary storage solutions ensure that primary data is minimally impacted by ransomware attacks, guaranteeing a normal flow of business operations while also mitigating the consequences of financial, regulatory, and reputational impact.

Furthermore, the existence of ransomware protection on primary storage systems—and its maturity—allows storage vendors to differentiate against their competition and create new business opportunities.

8. Report Methodology

A GigaOm Sonar report analyzes emerging technology trends and sectors, providing decision makers with the information they need to build forward-looking—and rewarding—IT strategies. Sonar reports provide analysis of the risks posed by the adoption of products that are not yet fully validated by the market or available from established players.

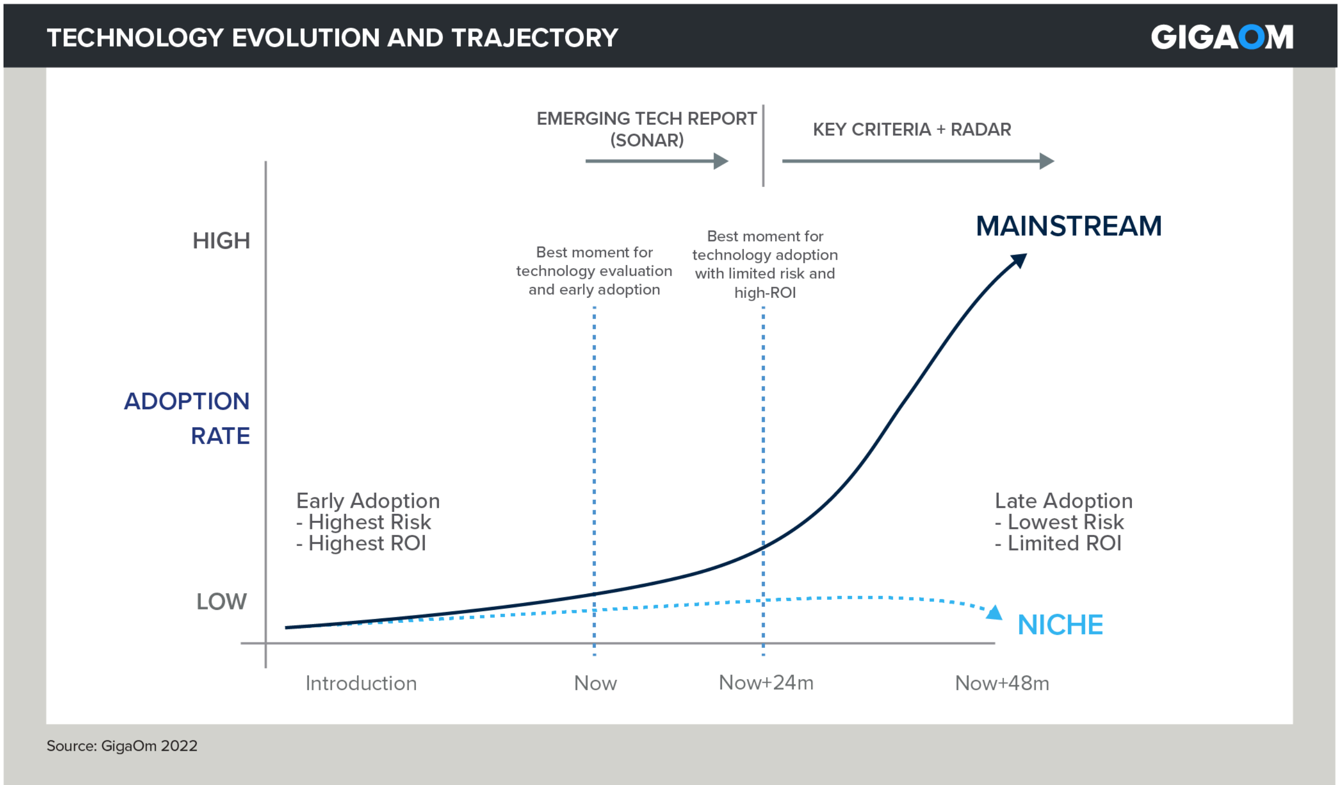
In exploring bleeding-edge technology and addressing market segments still lacking clear categorization, Sonar reports aim to eliminate hype, educate on technology, and equip readers with insight that allows them to navigate different product implementations. The analysis highlights core technologies, use cases, and differentiating features, rather than drawing feature comparisons. This approach is taken mostly because the overlap among solutions in nascent technology sectors can be minimal. In fact, product implementations based on the same core technology tend to take unique approaches and focus on narrow use cases.

The Sonar report defines the basic features that users should expect from products that satisfactorily implement an emerging technology, while taking note of characteristics that will have a role in building differentiating value over time.

In this regard, readers will find similarities with the GigaOm Key Criteria and Radar reports. Sonar reports, however, are specifically designed to provide an early assessment of recently introduced technologies and market segments. The evaluation of the emerging technology is based on:

- **Core technology**: Table stakes
- **Differentiating features**: Potential value and key criteria

Over the years, depending on technology maturation and user adoption, a particular emerging technology may either remain niche or evolve to become mainstream (see **Figure 2**). This GigaOm Sonar report intercepts new technology trends before they become mainstream and provides insight to help readers understand their value for potential early adoption and the highest ROI.



Source: GigaOm 2022

Figure 2. Evolution of Technology

9. About Max Mortillaro

Max Mortillaro is an independent industry analyst with a focus on storage, multi-cloud & hybrid cloud, data management, and data protection.

Max carries over 20 years of experience in the IT industry, having worked for organizations across various verticals such as the French Ministry of Foreign Affairs, HSBC, Dimension Data, and Novartis to cite the most prominent ones. Max remains a technology practitioner at heart and currently provides technological advice and management support, driving the qualification and release to production of new IT infrastructure initiatives in the heavily regulated pharmaceutical sector.

Besides publishing content/research on the TECHunplugged.io blog, Gestalt IT, Amazic World, and other outlets, Max is also regularly participating in podcasts or discussion panels. He has been a long-time Tech Field Day Alumni, former VMUG leader, and active member of the IT infrastructure community. He has also continuously been running his own technology blog kamshin.com since 2008, where his passion for content creation started.

Max is an advocate for online security, privacy, encryption, and digital rights. When not working on projects or creating content, Max loves to spend time with his wife and two sons, either busy cooking delicious meals or trekking/mountain biking.

10. About Arjan Timmerman

Arjan Timmerman is an independent industry analyst and consultant with a focus on helping enterprises on their road to the cloud (multi/hybrid and on-prem), data management, storage, data protection, network, and security. Arjan has over 23 years of experience in the IT industry and worked for organizations across various verticals such as the Shared Service Center for the Dutch Government, ASML, NXP, Euroclear, and the European Patent Office to just name a few.

Growing up as an engineer and utilizing that knowledge, Arjan currently provides both technical and business architectural insight and management advice by creating High-Level and Low-Level Architecture advice and documentation. As a blogger and analyst at TECHunplugged.io blog, Gestalt IT, Amazic World, and other outlets, Arjan is also from time to time participating in podcasts, discussion panels, webinars, and videos. Starting at Storage Field Day 1 Arjan is a long-time Tech Field Day Alumni, former NLVMUG leader, and active member of multiple communities such as Tech Field Day and vExpert.

Arjan is a tech geek and even more important he loves to spend time with his wife Willy, his daughters Rhodé and Loïs and his son Thomas sharing precious memories on this amazing planet.

11. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

12. Copyright