Brought to you by Informa Tech

Publication date:
19 Sep 2023
Author(s):
Dennis Hahn, Principal Analyst, Data Center Storage

On the Radar: NetApp provides a data protection solution to thwart ransomware

Summary

Catalyst

Ransomware attacks pose a significant threat to primary storage, as they can encrypt and hold data hostage, rendering it inaccessible until a ransom is paid. To deal with ransomware attacks that breakthrough preventative cyber defenses, regular backups have been the go-to strategy for data restoration, allowing for the recovery of primary data from the most recent unaffected backup. However, a newer option is to use the features built into the primary storage itself to detect and recover from a ransomware attack that damages data. Point-in-time copies or storage snapshots have long been a mainstay of primary storage to create a history of data images for disaster recovery. These enhanced snapshots are now being used to restore data in a failsafe way in the event of a ransomware attack that corrupts data.

NetApp has recently come out with a complete ransomware solution using its storage snapshots to remediate and recover data from breakthrough ransomware attacks that get to the data level and start to encrypt and alter data on primary storage.

Omdia view (user needs)

- Most storage snapshots are inherently immutable, but this does not mean they are ready to be used for ransomware protection. Careful attention needs to be paid to ensure that certain

aspects of the snapshots are fail-safe against ransomware attacks, leading to new capabilities such as indelibility (prevention of deletion).

- A complete ransomware storage solution goes beyond immutable snapshots. It takes into consideration all the other aspects to protect and harden the storage within an environment (see below section: ***Primary storage ransomware self-protection capabilities***).
- From Omdia's point of view, when protecting against ransomware, organizations should use a layered or multipronged approach. The best protection uses two logically separated mechanisms to make data copies, as ransomware tries to shut down data recovery mechanisms and typically corrupts or deletes all copies it can find unless the copies are immutable and/or indelible.
- Beyond being simple to use, a complete ransomware storage solution also needs the proper tools to provide insight into how well the environment is protected. Artificial intelligence and machine learning (AI/ML) based tools can greatly help in this regard.
- The process for recovery from a ransomware attack needs to be considered in any solution. The quicker and faster critical operating environments can be brought back online, the less money and reputation will be lost by the organization.

Why put NetApp's primary storage ransomware protection on your radar?

Ransomware has been a significant scourge for IT. Effectively thwarting ransomware requires innovation and well-thought-out deterrents and data recovery protection. When recently researching this space, NetApp's solution approach and capabilities seemed to address the key requirements.

Organizations should always have a strong detection and prevention aspect to their cybersecurity counter-offensive, but when those security measures fail, guaranteed remediation from an attack is critical for not incurring data loss. Omdia believes that guaranteed recovery requires organizations to use a layered approach to recover attacked mission-critical data. The NetApp solution to ransomware data recovery is a good example of this layering and provides some advantages over just using backups to provide protection.

Storage snapshots have historically been very effective for recovering data from accidental file deletion and can be very helpful as part of a disaster recovery strategy, but when it comes to protecting against intentional attacks on data, basic snapshots fall well short of being effective. Omdia believes the new NetApp ransomware recovery feature serves as a good example of the extended capabilities that must be added to basic snapshotting to make a fool-proof ransomware solution.

Market context

In this new data-driven economy, data has become the foundation for how firms run, compete, and prosper. Corporate data must therefore always be protected, whether it is stored on-premises, in the cloud, at the edge, or as part of a multicloud architecture. The first line of defense to secure data center data should always be cyber-secured networking and access restrictions.

However, as a crucial second line of defense, ransomware-free, versioned data copies that can be utilized in the case an attack manages to bypass frontend preventative security measures and comprise primary

storage are a must. To effectively thwart ransomware, this second line of defense must guarantee data recoverability under all and any circumstances, or else the bad people have won. While ransomware prevention is better than remediation, all organizations need to be always ready to recover ransomware-corrupted data because eventually preventative ransomware protections will enviably fail.

Ransomware attacks continue to evolve, with new variants emerging frequently. No single security solution is likely to provide a fool-proof guarantee against all ransomware attack approaches, which is why Omdia suggests a layered data protection strategy. This proposed strategy is something like the longstanding 3-2-1 backup strategy but altered for this new world of ransomware. A best practice ransomware recovery strategy should be to keep multiple ransomware-clean copies created from two independent mechanisms, with at least one physically air-gapped. New ransomware variants are becoming increasingly clever at turning off data protection mechanisms, reconfiguring protections, corrupting backup data, gaining unauthorized access to copies, or tampering with backup storage devices. While most of the ransomware recovery implementations Omdia has reviewed go to great lengths to protect in these scenarios, it only takes one administrative misconfiguration to create a vulnerability, and who knows what these well-funded and admittedly clever attackers will come up with next?

Last year, data centers experienced increasingly sophisticated cyberattacks, so it is now a must-have requirement to have immutable data copies as a fallback against such attacks. Immutably stored data copies cannot be altered by writing to them. They are locked in time and cannot be deleted through typical administrative actions, so they are great for recovering data. Increasingly, Omdia has been witnessing companies develop capabilities embedded into primary storage which can recover data from immutable copies. These mechanisms often involve snapshots that cannot be altered.

Companies can no longer afford to lose even little bits of data if this data was important enough to protect in the first place. So, immutable traditional backups are likely still a must, even when the primary storage has internal ransomware recovery. Traditional backups have broad coverage capabilities that can protect data anywhere it lives in increasingly distributed data estates, and they do a great job providing a required second set of independent copies that can be logically air-gapped or even physically air-gapped to, for example, tape.

Complete ransomware protection requires upfront data protection, detection with lock-down action, and fast recovery upon an incident. Protection starts with ensuring there is an uninfected, usable copy version available well before the ransomware attack occurs. Upon any attack, an automated response to limit damage to the stored data should then be initiated. Finally, once the attack has been contained, any data that has been compromised should be recovered so the organization can quickly return to business as usual.

An acceptable initial step for primary storage is just having array-based immutable volumes, especially if the storage is additionally protected by an excellent backup procedure that is intended to guard against ransomware. Beyond that, the following list of key capabilities needs to be taken into account to completely resist ransomware in the primary storage.

Primary storage ransomware self-protection capabilities

- **Recovery as a feature of storage software:** It is becoming more common for storage array software to include ransomware capabilities. Right now, network-attached storage (NAS) or file arrays are probably the ones with the most internal or integrated ransomware security. Storage area networks (SANs) or block arrays can also support internal ransomware protection, but it is less common. Object storage is typically based on versioning, so it inherently has the basics for

protection, but it is less often used as primary storage in data centers. Today, an area that is more nascent, but badly needed, is ransomware protection for cloud primary storage. This is an especially intriguing area, as primary cloud storage deployments (i.e., AWS EBS) often lack strong native data protection options. Ransomware protection for the cloud is now emerging as a feature of software-defined storage (SDS) services running on the cloud from independent vendors. Ultimately, most storage software supports some kind of point-in-time image, with some touting those as effective against ransomware. However, careful thought should be given to whether the offering provides complete ransomware protection or if it is merely a checkbox item that is minimally effective when it comes to recovering ransomware-attacked data.

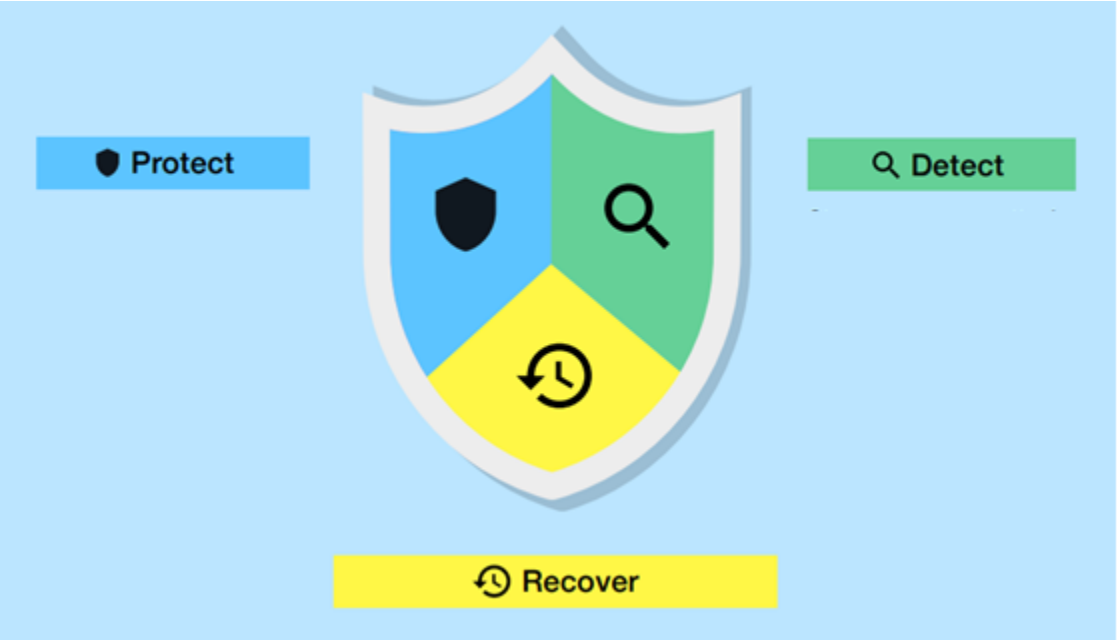
- **Immutable (failsafe) volumes and file copies:** Most storage array snapshots are inherently immutable to a degree. Therefore, numerous companies have come out with claims of providing immutable volumes and files in the last couple of years. Storage snapshots are used to maintain a history of data images in an unalterable state, enabling the restoration of data to various points in time so as to restore data that has been encrypted and damaged by ransomware. Immutable snapshot copies typically cannot be altered or deleted until they reach their timestamped retention period. Most companies use space-efficient snapshots to support these multiple recovery points. Two important considerations of snapshot capabilities are how many can be held at one time and how often snapshots can occur. The closer together the snapshots, the better for achieving the best RPO (recovery point objective—the amount of data lost between a snapshot and incident). An intriguing recent snapshot function is to initiate a snapshot upon ransomware detection in order to capture the state of the stored data and lessen the effects of a ransomware assault by minimizing the RPO.
- **Solution hardening and protected controls:** Ransomware attackers often attempt to disable data recovery and remediation mechanisms by deleting copies and reconfiguring copy capabilities so they are no longer protecting the data. Therefore, the protection software needs to detect any non-normal system changes and alert operators to changes that jeopardize future recoveries. To neutralize these attackers' efforts, the administrative controls need to be secured and the storage operating software updated to the latest versions. It is important that the software supports the ability to continuously scan the protected environment for administrative configuration gaps and misconfigurations attackers might be able to exploit for their attacks. For NAS storage implementations, it is important that the storage software not let hackers gain control over file admin rights and internal file registries and continually scan for configuration gaps in protection. In addition to the usual access controls and privilege management practices, it is a good idea to require two administrator approvals for major configuration modifications and copy deletions.
- **Attack detection and its containment:** An important feature of a complete ransomware solution is the proactive detection of ransomware operating on the stored data set. The array is a good place in a storing architecture to monitor the rate at which data is changing in the storage, possibly because of encryption modifications brought on by a ransomware assault. The intelligence in an array can also run sophisticated data anomaly detection with the use of ML detection techniques. The use of ML can even allow the detection software to learn over time what are actual attacks versus false alarms in detection. Once an attack is detected, time is of the essence, so automated user protection policies need to kick in to contain the damage an attack can have on the stored data. Most frequently, this involves delaying writes to the affected storage area until an administrator can verify or clear what triggered the event.

- **Centralized detection alerting and status:** Monitoring for incidents with immediate alerting and reporting to a centralized dashboard are essential for any ransomware solution. The solution should be configurable to send prompt warnings of important items whenever any suspicious activity or potential ransomware issue is discovered. For quick investigation and action, these notifications should be forwarded to designated security professionals or a security operations center (SOC). There should be an ability to export event listings and logs to security information and event management (SIEM) tools for higher level reporting, further analysis, and company-wide reporting.
- **Failsafe ransomware attack data recovery:** Incident response and recovery are complex processes that require expertise and system coordination. However, using primary storage snapshots taken in the context of the storage environment is highly helpful for speedy restoration and can be easily verified for overall simpler data recovery. Analyzing the scope of the attack and locating the compromised files and affected systems are crucial before beginning any recovery. According to best practices, it is preferable to create a recovery environment that is isolated from the rest of the data center network so the incident cannot spread further. The next step in a recovery is to identify snapshots that were unaffected by the attack; sophisticated systems are beginning to do this by utilizing AI/ML technologies. One of these unaffected snapshots should then be used to restore the affected systems to a known state by converting the snapshot into a read and writeable data volume. Before the restore is permanently implemented, the restored environment should be scanned with antivirus software, and the data of these recovered systems should be verified to be in a good state and one with an acceptable recovery point objective.
- **Assisted recovery point selection:** Ransomware recovery solutions must assist businesses in recovering with the least amount of damage. A strong recovery capability will display a timeline of snapshots and advise the operator of the best options for a ransomware-free recovery. When using easily restorable array snapshots, numerous data images can be restored and investigated because the recovery of snapshots will be nearly instantaneous. Ransomware in recent years has gotten very crafty by spreading across an environment for a few weeks and infecting the stored data but delaying the start of the encryption process and actual data attack. It is essential to have a lengthy history of snapshots to recover the data from the most recent unaffected copy. Therefore, the ability of array snapshot software to store hundreds of recovery images with excellent space efficiency is an important feature.
- **Automated and quick data recovery:** Automation is crucial to the user experience because identifying the ideal recovery point and verifying it requires knowledge and time. Given that the recovery time for a complete data center environment can be lengthy, the system should be able to prioritize recoveries of the most crucial systems first. The automated recovery of array snapshots will typically result in the fastest recovery of ransomware-corrupted data because array snapshots can be quickly converted into a writeable volume inside the array without a lengthy copy-back process. Most snapshots will restore the data to a historical recovery point, which will require a roll-forward from application logs so as to not lose the last written data. For applications like databases that have the capability, automation should include the ability to fully roll-forward for a complete up to the last write data recovery.

NetApp cyber resilience overview

NetApp has recently released enhancements to the NetApp solution for ransomware, including ONTAP features that deliver cyber resilience directly on NetApp primary data storage. The NetApp solution provides various effective tools for visibility, detection, and remediation, helping users spot ransomware early, prevent this spread, and recover quickly, if necessary, to avoid costly downtime. Traditional layered defense solutions remain prevalent, as do third parties and partner solutions for visibility and detection. Effective remediation remains a crucial part of the response to any threat. The unique industry approach leveraging the immutable NetApp Snapshot technology and SnapLock logical air gap solution is an industry differentiator and the industry best practice for ransomware remediation capabilities. These are also complemented by NetApp's Cloud Insights Storage Workload Security features that address threats that may come in from valid but compromised user accounts.

1. Figure 1: NetApp's approach to safeguarding data from ransomware



Source: NetApp

NetApp ONTAP: Protect, detect, and recover

NetApp's internal storage cyber resilience solution is based on the storage continually storing immutable copies of the data at different points in time, detecting threats to minimize the attack impacts, and then being able to recover quickly any data that was compromised in the attack. Most of this capability at its core is based on NetApp's historically sound snapshot technology but with significant and important enhancements to create a complete solution. Omdia sees the NetApp cyber solution as one of the more complete embedded primary storage solutions on the market today.

The protect part of NetApp's solution starts with the ongoing creation of immutable, space-saving snapshots, which need to be taken before a cyber incident occurs. The protection of the solution also extends into the administrative and management aspects of the storage. As NAS file storage, it also blocks malicious file types. An important aspect of the complete NetApp cyber resilience solution is to stop

malicious attackers from altering admins' credentials, changing protection configurations, and even deleting snapshots so there is no longer recovery data available. And as most storage should do today, it supports end-to-end encryption of the data held in the storage out to the accessing client (protecting data both in transit and at rest).

The detect part of the NetApp solution continually watches the data within the storage to detect anomalies. This needs to be automated within the detect software to offload human efforts and ensure it is constantly being done. Once an anomaly is detected, the event has to be handled appropriately. Part of that is making sure there are as few false alarms as possible, and the other part is strongly signaling an attack to administrators as soon and accurately as possible.

Another interesting part of the NetApp solution is the interaction with the Storage Workload Security (mentioned above), which combines real-time file system activity analytics with an AI-generated baseline behavior model for each authorized user. If there is a valid user who is engaging in anomalous behavior (access or activities to repositories that are both out of baseline and potentially harmful—even if these would not trigger encryption or entropy-based ransomware protections), the solution will detect, alert, and block further activity from the suspect account and trigger the recovery point. This type of functionality reflects the (noted above) layering approach to the best solutions.

The recover part of the solution uses protective data copies inside the storage to make it easy and fast to complete a recovery. A restore from a local copy to the storage secure snapshot typically only takes minutes.

The suite of cyber capabilities embedded in NetApp storage

NetApp solutions

- For on-premises data center storage arrays:
  - NetApp AFF and FAS running ONTAP (see below)
- For public cloud storage:
  - NetApp Cloud Volumes ONTAP (see below)
  - Amazon FSx for NetApp ONTAP (see below)
- General solutions:
  - NetApp ONTAP (with support for tamperproof, immutable, and indelible snapshots, Autonomous Ransomware Protection, and Policy)
  - NetApp BlueXP
  - NetApp Cloud Insights (Storage Workload Security)

Company information

Background

NetApp is focused on data management and data center storage. They claim to be focused on one thing, "helping your business get the most out of your data." The transition from being very storage-focused to being a broader data-centric software company that includes storage has been a journey for NetApp.

The transition toward becoming more software-focused on the world outside of storage appliances required NetApp to invest more heavily in data management. After advancing toward becoming one of the leading data management companies, it appears it is time for NetApp to enter into a more balanced storage and data management investment approach. NetApp is in a good position to deliver on the data-related industry-leading solutions the market is demanding, whether that be in the cloud or on-premises.

Cybersecurity use case

The NetApp ransomware protection solution was installed by an Electrical Equipment Engineering and Manufacturing company so they do not have a repeat of the cyberattack they endured before the protection deployment. As is often the case, the company had cyber resilience in place, but it was not enough. After a recent cyberattack, the customer decided to secure their IT by setting up a Disaster Recovery Plan, outsourced in one of their subsidiary data centers. The all-in-one ransomware protection solution provided the complete protection they were seeking for their primary storage. This customer offers expert services, critical power, power control, and safety and energy efficiency to data centers around the world as its business. Deploying this ransomware solution allowed them to focus on delivering and optimizing power consumption for the industry and not worry about ransomware data recovery.

Current position

As far as cyberattacks go, an organization cannot have too much protection. Making primary storage more cyber resilient is a major strategy for storage vendors. NetApp and a couple of others seem to be at the forefront for providing ransomware protection embedded into primary storage products.

Omdia believes this will be a growing trend, and in fact, several others also provide interesting capabilities inside their storage, but NetApp, with its advanced snapshot technology and complete coverage, provides a good example of where the industry is going. While several file-only vendors offer solution choices, NetApp has extended its offering to also cover block or SAN storage as part of its unified and SAN-only storage arrays. NetApp has also worked hard to provide the functionality for both on-premises and in the cloud deployments, leveraging its strength in hybrid cloud and data management offerings.

Key facts

Table 1: Datasheet: NetApp and its ransomware solution

Product name	NetApp ransomware solution	**Product classification**	Innovation management software
Version number	Starting with the ONTAP 9.13.1 version	**Release date**	May, 2023
Industries covered	All industries represented in the customer base focus on knowledge-intensive industries (finance, insurance, professional services, etc.)	**Geographies covered**	Worldwide
Relevant company sizes	All company sizes represented in customer base (startups to Global Fortune 500), focus on medium to large organizations (300–10,000 employees)	**Licensing options**	Included with storage purchase
URL	https://www.netapp.com/cyber-resilience/ransomware-protection/	**Routes to market**	Sold with capability
Company headquarters	San Jose, California, US	**Number of employees**	12,000 worldwide

Source: Omdia

Analyst comment

The first line of defense in cybersecurity is networking and access controls, but those in charge of the data center have quickly realized that having up-to-date, ransomware-free, versioned data copies is a crucial fallback for data recovery in the event the frontend defenses are breached. In addition to protecting data against corruption and accidental loss, storage array snapshots located inside primary storage are now playing a crucial role in thwarting malicious activity and recovering data in the event of a data-damaging attack. Despite claims made by some storage vendors that their array snapshots may be used for ransomware attack data recovery, simple snapshots fall far short of being the complete cybersecurity solutions required to truly secure mission-critical data. In addition, with ransomware data thefts and data ransoming on the rise, Omdia now holds that stored data should always be encrypted with well-thought-out key management to protect against theft and the threat of exposing company information for ransom. This includes all data that is secret, contains a competitive advantage, or might just be embarrassing if it was released to the public.

As prevalent as ransomware attacks have become, Omdia now believes all data worth keeping needs to be protected against ransomware. Comprehensive protection of all enterprise data has become especially important as data environments have become more distributed with multicloud, remote workers, analytics data collection, and edge computing data. Additionally, mission-critical data now absolutely must have at least two immutable copies made by two different backup processes to guarantee that at least one ransomware-protected copy would survive a ransomware assault, given the increased sophistication of cyberattacks observed by Omdia in 2022. A layered protection strategy should also be considered to move

the recovery closer to the data inside the storage system, allowing for a speedy shutdown in the event of an attack and quick data recovery afterward.

Inside a primary storage system is a great place to deploy other important capabilities that can thwart ransomware attacks. The storage system can instantly recognize and respond to abnormal system data being stored. It can then respond to these occurrences with automatic procedures to make sure the stored data is affected as little as possible. It can also scan the storage for data protection security gaps and misconfigurations that can be exploited by ransomware software that tries to change configuration settings to shut down data recovery measures.

It is important to complete any ransomware solution with centralized monitoring and timely notifications. Since immutable backups continue to be a crucial component of any layer protection strategy, Omdia advises that storage-level protection be coupled with the broader backup vendor technology to obtain centralized monitoring and possible integrated application recovery management.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Author

Dennis Hahn, Principal Analyst, Cloud and Data Center – DC Storage

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com