Technical Insight Report

Combatting Ransomware with Primary Storage

By Krista Macomber, Senior Analyst

March 2022

Evaluator Group

Enabling you to make the best technology decisions

Introduction

It is no secret that ransomware attacks are continuing to rise in count and become more severe in of their impact to enterprises. Evaluator Group sees customers investing in order to respond to this threat; in our Ransomware Pulse Survey 2021, 87% of respondents indicated that they plan to spend, or have budgeted to spend, money on technologies for ransomware protection and prevention over the next 12 months. Specifically, we see customers spending on data protection technologies, in order to ensure their ability to recover. In our study, 56% of respondents indicated having spent money on data protection over the preceding 12 months due to the rise in ransomware attacks.

While in some instances it may be possible to recover from ransomware using backups, backups are not the bulletproof, end-all be-all insurance policy they are often positioned as. Attackers understand that, if the customer can recover, they do not need to pay the ransom, so they have modified their approach to target the backup environment. Additionally, recovering from backups comes with some tradeoffs; it takes time to locate the last known good copy, it takes time to execute the recovery, and the backup copy might result in data loss by not offering a suitable recovery point. For these reasons, ransomware resiliency also should be addressed in the primary storage environment itself.

Addressing Ransomware Resiliency with Primary Storage

Especially considering these threats to and challenges in recovering from backups, Evaluator Group advises customers to build a comprehensive strategy for ransomware resiliency that extends beyond recoverability to include the ability to protect against and to detect a ransomware attack.

Core Pillars of Ransomware Resiliency

- Prevent
- Detect
- Recover

Addressing ransomware resiliency with primary storage can help to more quickly identify that a ransomware attack is happening, and to speed time-to-recovery from an attack.

Preventing a ransomware attack from occurring centers on obtaining visibility into who is accessing data, how are they accessing data, and why – with the goal of uncovering nefarious users and preventing them from accessing the environment. Additionally, IT may receive insight into how the various elements of the IT environment interact, throughout the data lifecycle, in order to discover areas of risk that may be compromised. This visibility is complemented by strong access control measures, to oversee who has access to what components of the IT environment. Data encryption and the ability to set data or objects as immutable (locked in a read-only mode so that they cannot be altered), and indelible (locked so that they cannot be deleted) are important so that, even if a bad actor is able to penetrate the environment, they cannot take control over data.

Visibility and analytics also play a role in ransomware detection, by helping to identify malicious activities as they are happening. In a backup environment, insights are retroactive, based on changes that have already occurred in the production environment and then been backed up. Data typically needs to be pulled of the backup system in order to be analyzed, as well. There is a performance penalty for scanning production systems, but this tradeoff can help to uncover sooner that a ransomware attack is occurring when compared to scanning and analyzing backup data. Integration with other tools such as IBM Qradar, SecureX, and Splunk allows these insights to be rolled into the broader context of the IT environment as a whole.

Fast time-to-recovery is critical to getting the business back up and running as quickly as possible, as a result reducing the business impact of a ransomware attack. This is especially true when it comes to core applications and services such as Active Directory. Recovering from backups can lengthen the achievable recovery time, especially if a file system becomes corrupted and as a result requires IT to search for and identify the last known good backup copy.

Using NetApp Storage for Ransomware Resiliency

For its part, NetApp's architecture follows a philosophy of "data-centric security" – that is, protecting data in use, at rest and in transit, across core, edge and cloud environments. The following section will explore what this means in terms of specific technical capabilities and through the lens of ransomware resiliency – preventing, detecting, and recovering from ransomware.

Prevention

In an effort to prevent ransomware attacks from occurring, NetApp employs a zero-trust security architecture, multiple levels of intelligence and verification, and logging and auditing capabilities to prevent malicious actors. Additionally, its FPolicy file access notification framework monitors and manages file access events across the SMB and NFS v3 and v4.0 access protocols. FPolicy serves as a control layer for file, user and storage volume access. It allows IT to block or restrict certain users, and to control read and write activity on file systems and at the storage volume level. FPolicy can feed third-party vendor's tools, including security information and event management (SIEM) products such as Splunk, to provide IT with additional visibility into malicious activity across the entire infrastructure. These capabilities are complemented by boot and upgrade image validation.

To further prevent access to backup data by bad actors, NetApp uses secure administration features including role-based access control (RBAC) and multi-factor authentication (MFA). It also supports a REST Open API Framework and offers a "plug and play" software development kit (SDK) so that partners can integrate into the NetApp security framework.

NetApp applies a number of technologies to encrypt data at rest and in flight. These include:

- Data at rest encryption, facilitated through:
  - NetApp Storage Encryption (NSE), which provides nondisruptive, hardware-based full-disk storage encryption for data at rest.
    - Specifically, NSE uses FIPS 140-2 level 2 self-encrypting drives (SEDs) for network-independent and system-independent encryption of data at rest.
  - NetApp Volume Encryption (NVE), a software-based encryption feature for data-at-rest that allows customers to bypass the need for SEDs.
    - NetApp Secure Purge "scrubs" data on a NetApp Volume Encryption (NVE) volume by cryptographically shredding files so that they cannot be recovered from the physical storage media. This prevents data spillage from occurring and provides "Right to Erasure" functionality.
  - The usage of NSE and NVE in conjunction with each other to feed extra protection through NetApp Aggregate Encryption (NAE). NAE allows encryption keys to be shared for the aggregate volumes as well as for deduplication to be applied across the aggregate volumes, in order to increase storage and management efficiency.
  - The usage of NetApp CyptoMod, a module that provides cryptographic operations for NSE and the onboard key manager.
  - The usage of the Intel AES New Instructions (Intel AES-NI) SMB encryption set.
  - Internet Protocol security (IPsec) can be invoked, which provides data authentication, integrity, and over the wire encryption between two endpoints over an IP network.
- TLS 1.2 Protocol support for transferring data and management plane usage, including for:
  - NetApp's SnapMirror data replication capability.
  - NetApp SnapVault, through which read-only snapshots from multiple systems to be backed up to a central, secondary storage system.
- Challenge Handshake Authentication Protocol (CHAP) is supported for iSCSI for user or network host authentication.
- Support for the Key Management Interoperability Protocol (KMIP), the de facto communication protocol for managing encryption keys, is included.

NetApp creates snapshot copies that are read-only and immutable, and its SnapLock feature meets customer requirements for indelibility. SnapLock has two modes that it can function in:

- Enterprise Mode, which offers customers some flexibility in terms of duration of the lock period, with the admin being able to control and alter retention settings.
- SnapLock Compliance Mode, which addresses immutability, indelibility and retention requirements of legislation such as HIPAA. Once it is set, the retention period cannot be changed by any user, or even by NetApp employees.

To get operations back online quickly, SnapMirror can replicate immutable snapshot copies to another site.

Detection

NetApp uses workload file activity patterns, data entropy calculations, and a custom built on-box analytics engine to identify and block malicious users. It also evaluates data entropy to understand if the data being leveraged in a nefarious way. Specifically, this functionality is embedded in the following capabilities/offerings:

- NetApp's Active IQ application for IT operations monitoring that uses AI/ML based in telemetry data. From a data protection standpoint, Active IQ can provide customers with prescriptive guidance/recommendations as well as automated actions/remediations to improve availability and reduce the organization's risk posture.
- FPolicy which is a file access notification framework for monitoring and managing file access events across the SMB and NFS v3 and v4.0 access protocols.
- NetApp Cloud Secure, which integrates with FPolicy to analyze and detect abnormal user behavior – specifically, file/data access patterns. This capability helps to identify ransomware and other cyberattacks as they are occurring, and it helps to ensure compliance. When an anomalous event is identified, Cloud Secure automatically triggers a storage snapshot and blocks user account access to prevent data exfiltration. It is a feature of NetApp Cloud Insights, which is a SaaS-based solution for monitoring on- and off-premises IT infrastructure.
- Cloud Data Sense, which identifies, maps and reports on a wide range of file systems and object storage solutions, both on- and off-premises. Cloud Data Sense is controlled via NetApp Cloud Manager. It applies AI and automation for data discovery, mapping, classification/categorization, and governance tasks (e.g., data deletion and data access requests, ensuring that data is in compliance with data privacy requirements).

Recovery

NetApp offers several capabilities to help customers expedite the ransomware recovery processes. Customers can perform granular file recoveries, allowing specific files to be quickly pinpointed and recovered as opposed to requiring, for example, an entire image to be recovered. Additionally, rapid restores can be executed from local or remote snapshot copies.

Identifying the last known good data copy is a challenge that Evaluator Group hears consistently from IT operations. To address this need, NetApp augments its own data forensics capabilities with partnerships with vendors such as Catalogic and ProLion. Catalogic's CryptoSpike technology identifies infected users and files, and blocks infected users' ability to further access NetApp file shares. ProLion also monitors threat indicators to identify and block malicious users and attacks.

Prioritizing data recovery based on its value to the organization is important to getting the business back up and running as quickly as possible following a ransomware attack. NetApp Active IQ allows IT to find volumes that are most readily used within the organization, for instance looking a the highest read and

write activity. Additionally, Cloud Insights provides IT with insights such as the most frequently accessed data. Both of these tools can help to narrow down the organization's most useful data. With SnapMirror, customers can then execute fast, snapshot-based, granular recoveries.

Conclusion

Architecting the storage environment for ransomware resiliency – that is, preventing, detecting, and being able to recover from ransomware – is a complex and multi-pronged process. Positioning the production storage environment as a core component of the ransomware resiliency strategy can arm IT operations to better prevent and more quickly detect and recover from ransomware attacks.

For its part, NetApp primary storage checks a number of important boxes for ransomware resiliency:

- Zero-trust architecture with auditing and logging
- Multi-faceted access control
- Encryption (data at-rest and in-flight)
- Immutability, including replication of immutable data points
- Indelibility
- AI/ML to uncover and stop nefarious activity.
- Granular file recoveries
- Rapid recoveries from snapshots

About Evaluator Group

Evaluator Group Inc., an Information management and data storage analyst firm, has been covering systems for over 20 years. Executives and IT Managers rely upon us to help make informed decisions to architect and purchase systems supporting their data management objectives. We surpass the current technology landscape by defining requirements and providing an in-depth knowledge of the products as well as the intricacies that dictate long-term successful strategies.