Solution Brief

The NetApp Solution for Ransomware

Empowering customers to protect their data, finances, and reputation

Abstract

This solution brief covers the growing threat of ransomware and how to identify, thwart, and remediate this threat using NetApp® Snapshot™ technology. This brief serves as a companion to the technical report TR-4572: The NetApp Solution for Ransomware, which provides a guide to help organizations meet prescribed security objectives for information system confidentiality, integrity, and availability.

Key Benefits

Leverage the Security Functions of Snapshot Copies

- Snapshot copies are a built-in feature of the NetApp ONTAP® storage management software.
- They enable rapid recovery in a matter of seconds, which can dramatically improve recovery time objectives.
- You can take Snapshot copies on a customized schedule.
- Snapshot copies create pointers to original data, making recovery simple and easy.
- You can make nearly instantaneous copies of your valuable data while applications are running.

Recover From Ransomware

- Recover data and information from across the enterprise; up to 1,023 Snapshot copies per volume can be created.
- Read-only copies prevent ransomware corruption.
- You can streamline recovery point objectives from uninfected data points.
- Snapshot copies can serve as a disaster recovery and business continuity plan solution.

The Challenge

The growing threat of ransomware

Organizations continue to face the challenge of ransomware, notably WannaCry, Samsam, and Cerber, and attacks can cost a business time, resources, and reputation. There is tremendous pressure to address this problem and minimize losses from these attacks. With this growing threat, security is on the mind of most businesses regardless of size or industry.

In 2017 there was an increase of 327 new ransomware families, which is a rise of 32% from 2016. Many companies use detection software; however, these technologies cannot stop an attack. Detection software finds and reduces the amount of damage ransomware can accomplish, but it cannot reverse the effects of an attack. Threats continue to change and become more difficult to detect by traditional techniques. A ransomware attack is no longer a matter of if it will happen but rather a matter of when.

An organization typically has two options after it has encountered ransomware: pay the ransom or restore from backups. A ransom payment does not guarantee that your files will be restored, and restoration from backups can be a tedious process that takes additional time and resources. NetApp Snapshot technology brings a third recovery option to the table.

The Solution

The NetApp ONTAP Snapshot solution for ransomware

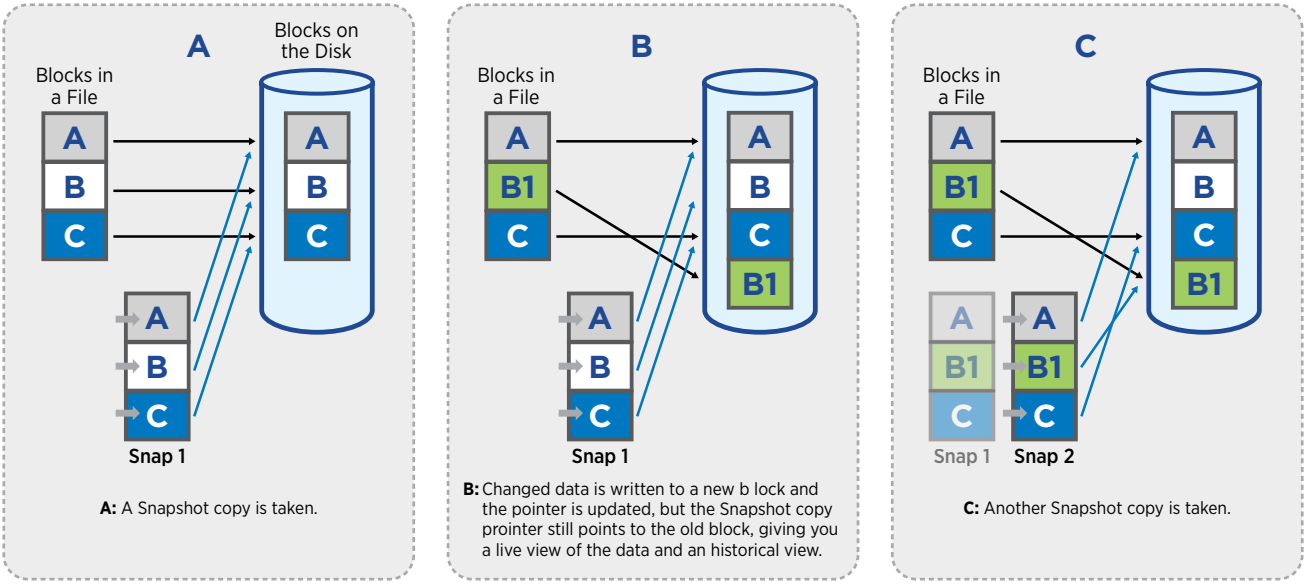
NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

NetApp recommends that organizations identify all data sources at risk for ransomware exposure (for example, file shares). Managers can then create or adjust recovery point objectives (data recovery procedures) so that these sources are backed up regularly.

What is a NetApp Snapshot copy?

A NetApp Snapshot copy is a point-in-time file system image. Low-overhead Snapshot copies are made possible by the unique features of the NetApp WAFL® storage virtualization technology that is part of the ONTAP software. Like a database, WAFL uses pointers to the actual data blocks on disk, but, unlike a database, WAFL does not rewrite existing blocks. Rather, it writes updated data to a new block and changes the pointer. A NetApp Snapshot copy simply manipulates block pointers, creating a frozen read-only view of a WAFL volume that lets applications access older versions of files, directory hierarchies, and/or logical unit numbers (LUNs) without special programming. Because actual data blocks aren't copied, Snapshot copies are extremely efficient both in the time needed to create them and in storage space.

NetApp®



You now have access to three generations of data without taking up the disk space that three unique copies would normally require. Live: Snapshot copy 2 and Snapshot copy 1 (in order of age).

Figure 1) NetApp Snapshot copy.

A NetApp Snapshot copy takes only a few seconds to create (typically less than one second) regardless of the size of the volume or the level of activity on the NetApp storage system. After a Snapshot copy has been created, changes to data objects are reflected in updates to the current version of the objects, as if Snapshot copies did not exist. Meanwhile, the Snapshot copy of the data remains completely stable, and a Snapshot copy incurs no performance overhead. You can comfortably store up to 1,023 Snapshot copies per WAFL volume (previously, 255 copies were supported), all of which are accessible as read-only, online versions of the data.

These point-in-time copies of data protect the most valuable resource of businesses and their customers with no performance effect and minimal storage space consumption. Using the tools already available through the NetApp solution, businesses can defend their most precious assets from the destruction of ransomware.

Restoring from uninfected Snapshot copies

NetApp Snapshot technology vastly improves the frequency and reliability of backups, because it incurs minimal performance overhead and can be safely created on a running system. NetApp Snapshot copies allow near-instantaneous, secure, user-managed restores. Users can directly access Snapshot copies to recover from accidental deletion, corruption, or other unfavorable modifications of their data. This is critical in the case of a ransomware attack, because recovery from a point where data was uninfected can save a company from costly damage. Because the security of the file is retained in the Snapshot copy, the restoration is both secure and simple.

Additionally, there is an active remediation component in the Snapshot solution called NetApp SnapRestore® data recovery technology. For more information, see the NetApp SnapRestore page on the NetApp portal.

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation, and optimize their operations. For more information, visit www.netapp.com. #DataDriven