Technical white paper

HPE Virtual Lock—Build a resilient defense against ransomware

Solution overview and benefits

Contents

Executive summary

Ransomware has been taking over our news feeds like never before. Each article describes the story of an organization whose business continuity has been compromised due to mission-critical data being held hostage by ransomware. Ransomware has evolved from a primitive cyborg Trojan (Aids Info Disk [AIDS]) distributed through floppy disks to a full-fledged ransomware as a service (RaaS) employing intricate infiltration techniques. These have damaging consequences for individuals and businesses alike.

Backups are one of the most important defenses against ransomware. However, advanced ransomware is now targeting backups—modifying or completely wiping them out—and eliminating the last line of defense against ransomware and forcing organizations to succumb to huge payouts for recovery of their data. Hence, it is crucial to incorporate a data protection architecture built on hardened, immutable storage infrastructure for a holistic ransomware response plan.

Hewlett Packard Enterprise offers a wide range of solid multi-tier storage products that can be effectively utilized to build a robust and secure 3-2-1-1 data protection architecture (extension of 3-2-1 rule, with three copies of your data on two different media types, with one copy off-site but still online, and at least one other copy that is immutable). This paper focuses on the implementation details of HPE Virtual Lock software that can help protect your enterprise data from ransomware and accidental mishaps. The software is currently available as a feature in the HPE Alletra Storage MP B10000 storage array—a Tier 0 enterprise storage solution that delivers the extreme resiliency and performance of high-end storage with the agility of the cloud. This paper also illustrates the simplicity of plugging the HPE Virtual Lock feature into an automated workflow with Veeam Data Platform for the creation of application-consistent immutable snapshots.

Target audience

This paper is intended for information security and data protection technologists who are responsible for the protection of enterprise data. It is assumed that subjects such as storage area networks, encryption, malware, and backup are understood.

Ransomware mode of infection and prevention

Typically, ransomware is delivered as a payload to targeted consumers, government agencies, or even large enterprises in the form of malicious code or a dropper. As shown in Figure 1, the payload eventually starts encrypting files or remains dormant until the activation of the communication path that is used for exchanging information with the victim. Hackers have been refining and increasing the complexity of attacks by using advanced cryptographic techniques, deploying rootkits that enable unauthorized access, disabling antimalware programs, and destroying the backups that act as a last line of defense in the business continuity plan of an organization.

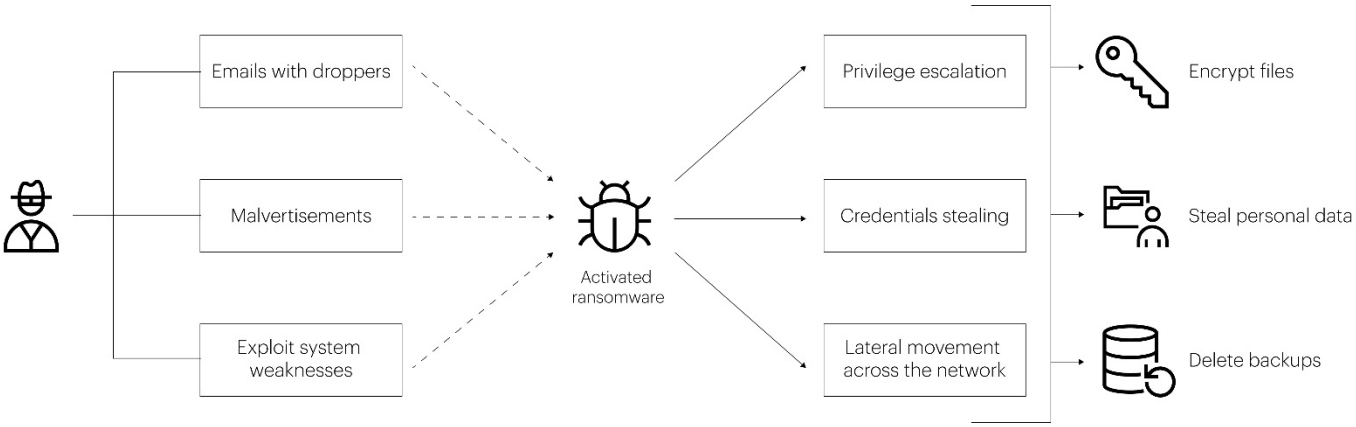

Figure 1. Ransomware mode of infection

Prevention is an important step to reduce the opportunity for a ransomware infection. Building cybersecurity awareness, keeping operating systems and software up to date with patches, reinforcing antivirus software protection, and hardening the systems by enabling only the required services and ports are some measures that can reduce the likelihood of a ransomware attack. However, these solutions are reactive by nature and can only defend against a known variant. It is imperative to include data protection within a comprehensive security strategy to circumvent the damage caused by ransomware.

Minimize data loss and application downtime with immutable snapshots

From an attacker's perspective, the success or failure of an attack depends on your ability to restore trustworthy data after it has been compromised. As a result, attackers often delete or encrypt backups and snapshots in particular to limit your ability to recover lost data quickly by forcing you to fall back upon secondary backups, which can prove tedious and result in a huge amount of potentially sensitive data being lost.

A SOPHOS report on ransomware trends in 2022 states that on average, organizations that paid got back only 61% of their data. Similarly, only 4% of those who paid the ransom got all their data back in 2021. This clearly illustrates that paying the ransom does not offer any guarantee of complete recovery. Therefore, a solid data protection solution such as described herein is essential.

A reliable data protection plan must incorporate the creation of immutable backup copies including unalterable snapshots on primary storage arrays. By storing data in native format in immutable snapshots that cannot be encrypted or deleted, applications can be restored and made available almost immediately. HPE provides several fast, efficient, scalable, and secure storage options in its storage portfolio to build a backup infrastructure that can remediate a ransomware attack with confidence.

Strengthen your data protection strategy with HPE Virtual Lock

HPE Virtual Lock software provides ongoing protection for mission-critical data by safeguarding individual virtual volumes and virtual copies (snapshots) on HPE Alletra Storage MP B10000 storage arrays from accidental or unauthorized deletion. HPE Virtual Lock is an integral part of the HPE Alletra operating system and does not require any software or agent installation at the host level.

HPE Virtual Lock allows the user to specify a desired virtual volume retention period (retention time) while creating snapshots and virtual volumes that make them tamper proof and impervious to ransomware for the set retention duration. The maximum retention time can be specified as high as 1825 days (five years). Until the expiration of the set retention time, the snapshots are immutable; that is, they can only be read. Hence, the virtually locked snapshots can neither be encrypted by a malicious attacker nor be deleted—even by a system administrator with the highest privileges—thus aiding the enterprises to comply with strict auditory requirements. A set of immutable snapshots of the production volumes with HPE Virtual Lock applied to them form the most basic clean room. In the event of a ransomware attack, the infected systems can rapidly be reverted to their state prior to the infection using HPE Virtual Lock snapshots in the clean room with minimum data loss to comply with demanding recovery time objective (RPO) and recovery point objective (RTO) requirements, as shown in Figure 2.

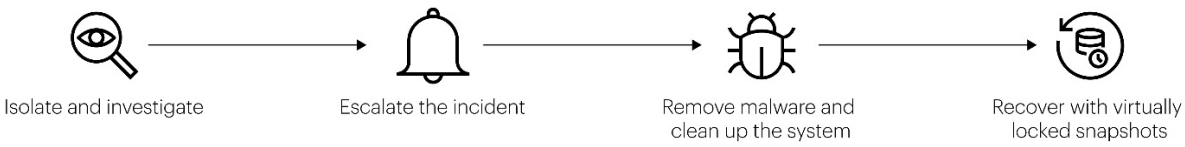

Figure 2. Recover data using immutable HPE Virtual Lock snapshots after a ransomware attack

Additionally, HPE Virtual Lock enables the user to specify an expiration-time duration for the virtual volumes and their snapshots. After the elapse of the set expiration duration, the virtual volumes and snapshots get automatically deleted during the subsequent cleanup cycle. This avoids the accumulation of orphaned snapshots and provides an automated way of reducing the snapshot footprint in the storage array. The retention- and expiration-time durations can be set through simple-to-use CLI commands and REST application programming

interfaces (APIs) that can be seamlessly integrated with any data protection software for automated creation of immutable snapshots. Figure 3 is an example of setting a retention time. For more details on the commands to enable HPE Virtual Lock on snapshots or virtual volumes, see the HPE GreenLake for Block Storage: CLI reference guide.

```
4UW0003299_Alletra660 cli%
4UW0003299_Alletra660 cli%
4UW0003299_Alletra660 cli%
4UW0003299_Alletra660 cli% createsv -ro -exp 30d -retain 14d VirtualLockSnapshot2 BM15Vol
Warning: The retention time cannot be removed or reduced once it is
set. This volume cannot be removed until its retention time expires.
Are you sure you want to set the retention time?
select q=quit y=yes n=no: y
4UW0003299_Alletra660 cli%
4UW0003299_Alletra660 cli% showvv -showcols Id,Name,VSize_MB,CreationTime,RetentionEndTime,ExpirationTime VirtualLockSnapshot2
  Id Name                VSize_MB CreationTime               RetentionEndTime           ExpirationTime
6655 VirtualLockSnapshot2   563200 2022-08-26 04:53:50 MDT 2022-09-09 04:53:50 MDT 2022-09-25 04:53:50 MDT
-------------------------------------------------------------------------------------------------------------
   1 total                  563200
4UW0003299_Alletra660 cli%
```

Figure 3. Enabling HPE Virtual Lock on snapshots by setting retention time through CLI commands

Moreover, HPE Virtual Lock operates at the block level in the storage array; it is agnostic of the host initiator attributes: the flavor of the host OS, the type of application running on the primary storage volumes, host connectivity protocol, and so on. The process for creating virtually locked snapshots is similar to that of regular read-only snapshots—it does not create any overhead in terms of capacity or performance. Any workload running on any platform backed by HPE Alletra Storage MP B10000 storage volumes can be immunized against any form of ransomware attack or unintended mishaps through the proprietary HPE Virtual Lock software.

HPE Virtual Lock integration with backup applications

Veeam Data Platform

Veeam Data Platform is fully integrated with the HPE Virtual Lock feature of HPE Alletra Storage MP B10000 storage arrays. When HPE Virtual Lock is applied to a snapshot, it becomes read only and cannot be altered or deleted by ransomware or by an administrator or attacker with system-level privileges. Veeam's support of backup immutability includes both on- and off-premises storage snapshots and backups, as well as those stored in Amazon Web Services (AWS) cloud object storage. Veeam supports AWS S3 Object Lock to provide immutability that even system administrators cannot alter. Additionally, Veeam supports strong immutability for backups saved to HPE StoreOnce, HPE Alletra Storage Server 4000, or S3 object storage on Scality ARTESCA and Scality RING.

Figure 4 shows the Backup Job configuration page, highlighting the option to make snapshots immutable and choose the duration of immutability. Snapshots cannot be altered or deleted until the immutability period has expired.

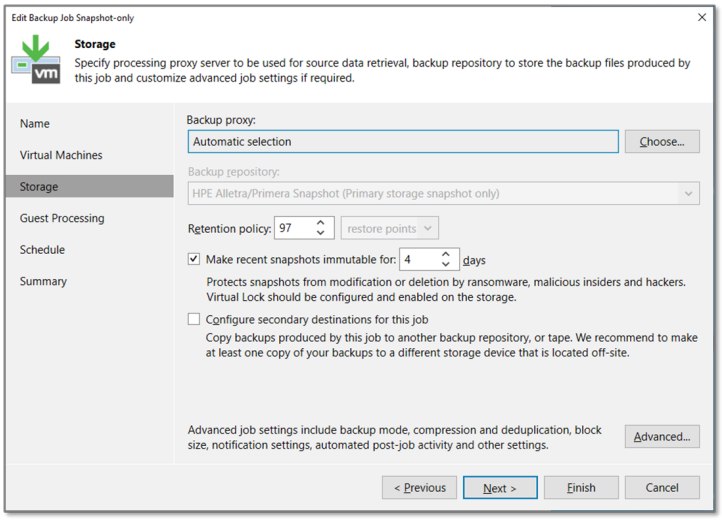

Figure 4. Veeam Backup Job with Immutable option selected for creating virtually locked snapshots

Figure 5 shows the page in the Veeam user interface where you can see the immutable snapshots listed, and the end date and time when the HPE Virtual Lock will expire, and the snapshots will be released from their immutable status.

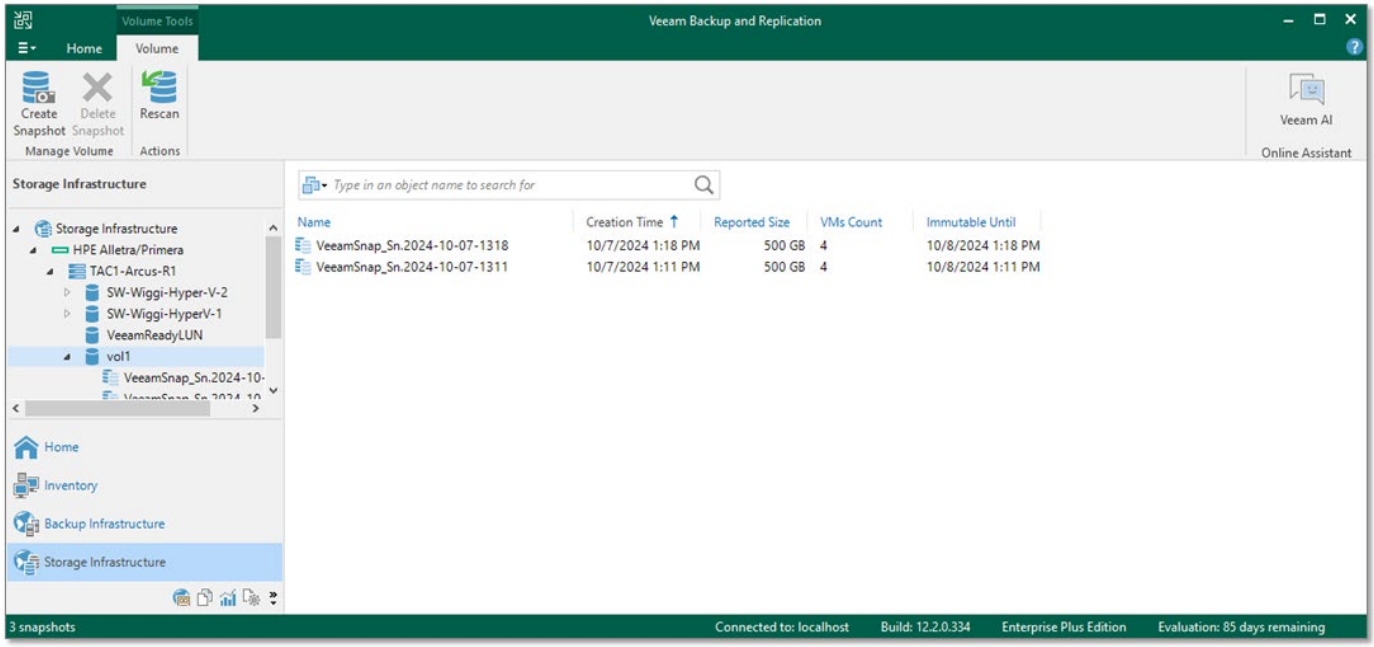

Figure 5. Veeam user interface showing snapshots with HPE Virtual Lock enabled

In addition to immutable snapshots orchestrated by Veeam Data Platform, a robust solution to protect against ransomware also can include Veeam ONE. Veeam ONE is a powerful monitoring and analytics tool that uses real-time monitoring to sense when a host is exhibiting behavior consistent with files being encrypted by ransomware. If such activity is detected, Veeam ONE will raise an alarm so an administrator can take action. With Veeam ONE, organizations can document the immutability of their backup data for regulatory compliance or other internal purposes.

Veeam SureBackup is another useful tool that can scan backup files offline for the detection of malware. In addition, it can use backup files or replicas to deploy machines in an isolated environment so they can be tested with various tools or scripts. Using Veeam SureBackup enables organizations to automate and schedule recovery testing and receive reports regarding the health of their virtual machines, as well as OS and application-level backups.

3-2-1-1-0 backup rule

Immutable snapshots are only one part of a complete data protection solution. Other elements are necessary as well. Veeam strongly recommends adhering to the 3-2-1-1-0 backup rule for a robust data protection solution that can help protect against all threats:

3—Have at least three copies of all data. This should include the primary (production) data and at least two backups

2—Data should be kept on at least two different types of storage media

1—At least one copy should be kept off-site

1—One copy should be offline, air gapped, or immutable

0—Veeam SureBackup should be used to verify that backups can be recovered with zero errors

Veeam supports immutable backups on HPE StoreOnce and immutable storage snapshots on HPE Alletra Storage MP B10000 storage arrays, enabled by HPE Virtual Lock, which cannot be discovered by ransomware. Veeam's support of backup immutability includes both on- and off-premises backups and those stored in AWS cloud object storage. Veeam Hardened Repository with Linux® provides immutability for backups, both on- and off-premises. For backups stored in cloud object storage, Veeam supports AWS S3 Object Lock, which provides immutability that even a system administrator cannot change or remove.

Summary

With a rampant increase in the number and complexity of ransomware attacks and their consequences, information security professionals across organizations are promoting a defense-in-depth approach. This includes creating employee awareness, timely deployment of patches, a solid backup and recovery plan, and so on. In this paper, we describe the importance and simplicity of HPE Virtual Lock software in protecting mission-critical data with immutable snapshots that aid in reliable recovery from ransomware attacks with minimal downtime and data loss. HPE Virtual Lock software can be effortlessly leveraged by the Veeam Data Platform for the automated creation of application-consistent immutable snapshots of workloads hosted on HPE Storage arrays. Incorporating immutability with HPE Virtual Lock software completes and boosts a data protection plan that provides customers peace of mind that when they need to, they can always access the impervious virtually locked snapshots to recover from such debilitating ransomware attacks.

References

HPE Alletra Storage MP B10000

Virtual lock software for HPE Alletra Storage MP B10000, HPE Primera, and HPE Alletra 9000 systems

Learn more at

HPE.com/us/en/Storage/Alletra.html

a00127331ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com