



**HPE Virtual Lock software  
and data-adaptive  
ransomware work together  
to protect electronic  
healthcare data**

Ransomware attacks are all too common, as they present a get-rich-quick opportunity for criminals who have no respect for the privacy of the impacted businesses and their customers. In these attacks, access to critical data is blocked through encryption and/or deletion before the attackers attempt to extort large amounts of money from the company in exchange for the encryption keys or to prevent stolen data from being published online.

In a recent example, a large healthcare provider was subjected to a cyberattack that resulted in encrypted and stolen data, disrupting drug services nationwide for weeks. Even after paying the extortion, decrypting the data was slow and resulted in additional weeks of downtime.

These types of cyberattacks are on the rise: the US Office of the Director of National Intelligence [reported](#) that ransomware attacks worldwide increased by 77% in 2023 (4,591 attacks) compared to 2022 (2,593 attacks). These numbers continued to rise in 2024 with a 15% increase to an unprecedented 5,289 attacks. The healthcare sector was targeted more than twice as much in 2024 compared to 2022.<sup>1</sup> The results have included delayed medical procedures, strained acute-care resources, and other patient-care disruptions.

The nature of the healthcare industry makes it particularly susceptible to ransomware attacks. Healthcare involves highly sensitive data, including personally identifiable information and personal health information, and requires continuous operation as a critical requirement. With the need for facilities to be connected over the internet, the data and operation requirements make healthcare facilities a prime target for ransomware attacks.

The rise of ransomware as a service (RaaS) and initial access brokers (IABs) has streamlined the process for bad actors to carry out attacks. An IAB will gain access to victims' networks and then sell that access to attackers. The attackers then use RaaS software to carry out the attack. With most technical work completed by IABs and RaaS core operators, ransomware attackers need to be less technically savvy to have a successful attack.

## The 3-2-1-1 rule for data protection

A comprehensive security strategy includes data protection incorporating live snapshots, data replication, and a solid backup solution. The 3-2-1-1 rule specifies that a data protection policy should include the following:

- Keep at least three copies of data.
  - Minimum requirement example: Primary, snapshot, and remote backup
  - Common configuration example: Primary, snapshot, local backup, remote backup
- Store the copies on two different and independent storage devices: tape, disk, disk arrays, or cloud.
- There is consensus that replicated primary storage arrays are not considered independent and do not comply with the rule.
- Keep one backup copy off-site in the event of a site-wide issue, or local hazards or infections within the network.
- Keep at least one air-gapped backup copy.

The air-gapped backup copy is a recent extension to the 3-2-1 rule aimed at protecting against cyberattacks such as ransomware. Nobody can alter or delete this copy of data, even if they have administrative credentials and a remote connection to the backup console or the storage repository.

The classic example of an air-gapped solution is tape media that has been extracted from the library and stored in a vault. A newer approach is based on a backup copy marked as immutable on the storage device, so even an administrator with remote access cannot alter the data, the immutability attribute, or the immutability expiration date. Hewlett Packard Enterprise recommends [HPE Virtual Lock software](#) to meet the air-gap requirement for any existing or new data protection solution for Epic Systems environments.

<sup>1</sup> ["Worldwide ransomware, 2024: Increasing rate of attacks tempered by law enforcement disruptions,"](#) CTIIC, February 2025.

## HPE data-adaptive ransomware detection on HPE Alletra Storage MP B10000

To help protect healthcare data from ransomware attacks, HPE has introduced its new data-adaptive ransomware detection feature for the HPE Alletra Storage MP B10000 with the 10.5.0 release, and it does not require a license. It is built on the advanced encryption detection technology in HPE Zerto Software and provides real-time encryption detection on any block storage workloads.

Data-adaptive ransomware detection uses two independent algorithms. This allows for dynamic trigger calculations and trigger thresholds. This is an essential improvement over hard-coded thresholds that ransomware has learned to avoid. The result is enhanced detection accuracy and fewer false positives.

Data-adaptive ransomware detection runs as an in-line process, analyzing data before it is written to disk and before any compression, deduplication, or on-drive encryption. The performance impact is negligible, and it can be used in disconnected or air-gapped environments.

When a ransomware incident is detected, the HPE Alletra Storage MP B10000 takes three actions:

1. The volumes are marked as degraded
2. An immutable snapshot is created for forensic investigation
3. Alerts are sent to:
  - a. Security syslog
  - b. Data Services Cloud Console
  - c. HPE support (if call home is enabled)

When data-adaptive ransomware detection is combined with HPE Virtual Lock, critical backup data is safe from deletion or encryption, and recovery from a ransomware incident can be quick and efficient with minimal data loss or downtime.

## HPE Virtual Lock software as part of a comprehensive security strategy for Epic Systems

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 to limit recovery of lost data quickly by forcing the target to fall back on secondary backups, which can prove tedious and result in a huge amount of potentially sensitive data being lost.

HPE Virtual Lock software provides ongoing protection for mission-critical data by safeguarding snapshots on [HPE Alletra Storage MP B10000](#), [HPE Alletra Storage 9000](#), and [HPE Primera](#) storage arrays from accidental or unauthorized deletion or modification. HPE Virtual Lock software is an integral part of these storage array operating systems and does not require any software or agent installation at the host level.

In an Epic Systems environment, array-level snapshots should be an integral part of a comprehensive security strategy. HPE Virtual Lock software should be used, at a minimum, on the consistency groups that include the production ODB filesystems. This will allow for rapid recovery in the event of a cybersecurity attack.

HPE Virtual Lock allows for snapshots to be immutable for a defined period. This makes them tamper-proof and impervious to ransomware for a set retention duration of up to five years. The immutability of the snapshots can never be decreased, removed, or altered. Hence, the virtually locked snapshots can neither be encrypted by a malicious attacker nor deleted—even by a system administrator with the highest privileges.

## Scheduling snapshots with HPE Virtual Lock

### Create a schedule for immutable snapshots with Data Services Cloud Console

A protection schedule can be created that uses HPE Virtual Lock for an entire volume set through the Data Services Cloud Console by selecting the volume set and then navigating to the Policies tab. Click the + icon to launch the Add Protection wizard.

This wizard allows the creation of a snapshot schedule that includes how often the snapshots will be taken, how long they will be immutable, how long before they expire, and if the snapshots should be coordinated between the local and a remote system.

In Figure 1, a protection policy named Epic\_VirtualLock\_Schedule is created that will create an immutable snapshot every day at 8:00 a.m. The snapshots are immutable for 7 days and expire after 14 days.

The screenshot shows the 'Add Protection' wizard interface. At the top, it says 'Add Protection' with a close icon. Below that is a section for 'Schedule 1'. The configuration fields are as follows:

- \* Schedule Name**: Epic\_VirtualLock\_Schedule
- \* Take Recovery Point**: Every 1 Days
- Time (in hours)**: 8
- \* Days**: Su, M, Tu, W, Th, F, Sa
- \* Expire after**: 14 Days
- Virtual lock**: 7 Days
- Remote Protection**

At the bottom, there are three buttons: 'Cancel', 'Back', and 'Add'.

Figure 1. Adding a protection policy in the Add Protection wizard

## Create a schedule for immutable snapshots with the command line interface (CLI)

A script is required to run a protection policy through the CLI, so this section describes the CLI commands required for the script.

To view the virtual volumes (vvs) in the virtual volume set (vvset), run the command **showvv set: <set name>**, where set name is the name of the existing Epic Systems production database vvset, as shown in Figure 2.

```
4UW0004475 cli% showvv set:Epic_vvset
  Id Name      Prov Compr Dedup Type CopyOf  BsId Rd -Detailed_State- Rsvd(MiB) VSize(MiB)
89487 Epic_ODB.0 tdrv v2   Yes  base ---   89487 RW normal      525    153600
89488 Epic_ODB.1 tdrv v2   Yes  base ---   89488 RW normal      525    153600
89489 Epic_ODB.2 tdrv v2   Yes  base ---   89489 RW normal      525    153600
89490 Epic_ODB.3 tdrv v2   Yes  base ---   89490 RW normal      525    153600
89491 Epic_ODB.4 tdrv v2   Yes  base ---   89491 RW normal      525    153600
89492 Epic_ODB.5 tdrv v2   Yes  base ---   89492 RW normal      525    153600
89493 Epic_ODB.6 tdrv v2   Yes  base ---   89493 RW normal      525    153600
89494 Epic_ODB.7 tdrv v2   Yes  base ---   89494 RW normal      525    153600
-----
      8 total                                4200    1228800
4UW0004475 cli% █
```

Figure 2. Output of showvv set command

The following command is an example for creating immutable snapshots of all volumes in a volume set:

```
createsv -ro -exp 8h -retain 1d @vvname@_VirtualLock set:Epic_vvset
```

Here is the breakdown of the command:

- **createsv** is the CLI command to create snapshot volumes.
- **-ro** tells the system to create a read-only snapshot.
- **-exp 8h** tells the system to make the snapshot immutable for 8 hours (m=minutes, h=hours, d=days).
- **-retain 1d** tells the system to keep the snapshot for 1 day (m=minutes, h=hours, d=days).
- **@vvname@\_VirtualLock** tells the system to name the snapshot volumes using the parent volume's name with **\_VirtualLock** appended.
- **set:Epic\_vvset** tells the system to use all volumes in the **Epic\_vvset** vvset.

After the snapshots have been created, the attached vcopy volumes and the retention and expiration times can be seen by running the command as shown in Figure 3:

```
showvv -showcols Id,Name,VSize_
MB,CreationTime,RetentionEndTime,ExpirationTime Epic*
```

```
4UW0004475 cli% showvv -showcols Id,Name,VSize_MB,CreationTime,RetentionEndTime,ExpirationTime Epic*
  Id Name                               VSize_MB CreationTime           RetentionEndTime           ExpirationTime
89487 Epic_ODB.0                          153600 2024-08-12 09:50:51 MDT --
89582 Epic_ODB.0_VirtualLock              153600 2024-08-12 13:01:37 MDT 2024-08-12 21:01:37 MDT 2024-08-13 13:01:37 MDT
89488 Epic_ODB.1                          153600 2024-08-12 09:50:51 MDT --
89583 Epic_ODB.1_VirtualLock              153600 2024-08-12 13:01:37 MDT 2024-08-12 21:01:37 MDT 2024-08-13 13:01:37 MDT
89489 Epic_ODB.2                          153600 2024-08-12 09:50:51 MDT --
89584 Epic_ODB.2_VirtualLock              153600 2024-08-12 13:01:37 MDT 2024-08-12 21:01:37 MDT 2024-08-13 13:01:37 MDT
89490 Epic_ODB.3                          153600 2024-08-12 09:50:51 MDT --
89585 Epic_ODB.3_VirtualLock              153600 2024-08-12 13:01:37 MDT 2024-08-12 21:01:37 MDT 2024-08-13 13:01:37 MDT
89491 Epic_ODB.4                          153600 2024-08-12 09:50:52 MDT --
89586 Epic_ODB.4_VirtualLock              153600 2024-08-12 13:01:37 MDT 2024-08-12 21:01:37 MDT 2024-08-13 13:01:37 MDT
89492 Epic_ODB.5                          153600 2024-08-12 09:50:52 MDT --
89587 Epic_ODB.5_VirtualLock              153600 2024-08-12 13:01:37 MDT 2024-08-12 21:01:37 MDT 2024-08-13 13:01:37 MDT
89493 Epic_ODB.6                          153600 2024-08-12 09:50:52 MDT --
89588 Epic_ODB.6_VirtualLock              153600 2024-08-12 13:01:37 MDT 2024-08-12 21:01:37 MDT 2024-08-13 13:01:37 MDT
89494 Epic_ODB.7                          153600 2024-08-12 09:50:52 MDT --
89589 Epic_ODB.7_VirtualLock              153600 2024-08-12 13:01:37 MDT 2024-08-12 21:01:37 MDT 2024-08-13 13:01:37 MDT
-----
 16 total                               2457600
4UW0004475 cli% █
```

Figure 3. Output of the showvv -showcols command

With immutable snapshots of the Epic production database and journal allow for a basic clean room, so data can be restored easily after the cybersecurity threat is neutralized.

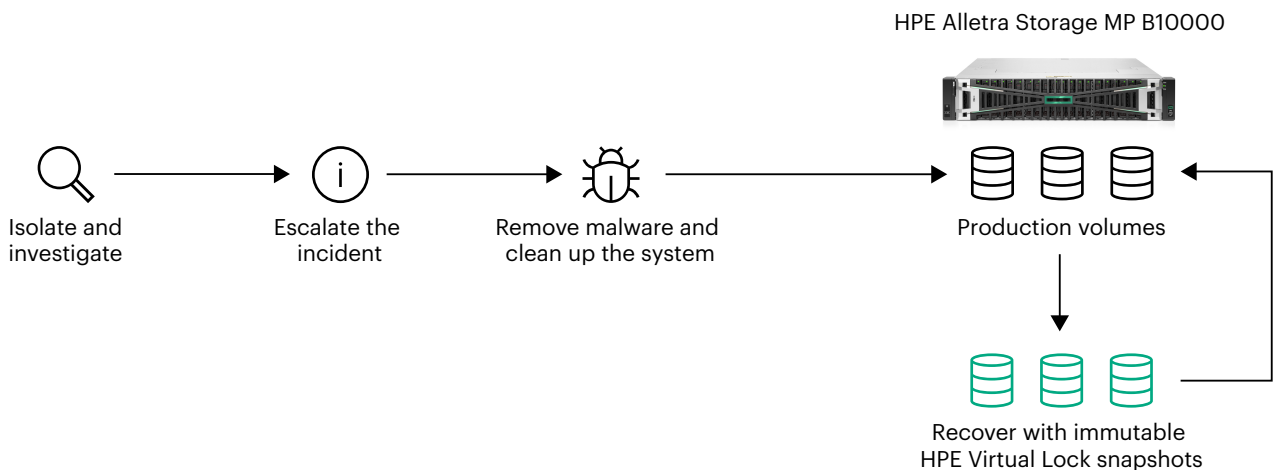


Figure 4. Immutable HPE Virtual Lock snapshots can be used to recover data after a ransomware attack



**For additional information, see the following:**

[HPE Alletra Storage MP B10000: Cyber resilience with data-adaptive ransomware detection](#)

[Advance your cyber resilience against ransomware with HPE Alletra Storage MP B10000](#)

[HPE Alletra Storage MP B10000 Data-adaptive ransomware detection](#)

[HPE Virtual Lock Software—Product Information Reference](#)

[HPE 3PAR Virtual Lock Software](#)

[Ransomware: Ensuring protection from an increasingly complex threat](#)

[Ransomware data recovery architectures](#)

[HPE Virtual Lock—Build a resilient defense against ransomware](#)

**Learn more at**

[HPE.com/us/en/storage.html](https://hpe.com/us/en/storage.html)

Visit [HPE.com](https://hpe.com)

[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00142754ENW

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://hpe.com)

