**∩ NetApp**

# NETAPP CYBER VAULTING:
# MULTILAYERED DATA PROTECTION

Isolate your most valuable data with secure hardening technology to minimize your attack surface and keep your most critical data confidential, intact, and readily available.

In today's digital landscape, safeguarding your organization's critical data assets is not just a best practice—it's a business imperative. Cyberthreats are evolving at an unprecedented pace, and traditional data protection measures are no longer sufficient to keep your sensitive information secure. That's where cyber vaulting comes in. NetApp's cutting-edge solution combines advanced logical air-gapping techniques with robust data protection measures to create an impenetrable barrier against cyberthreats. By isolating your most valuable data with secure hardening technology, cyber vaulting minimizes your attack surface so that your most critical data remains confidential, intact, and readily available when needed.

With NetApp® cyber vaulting, your data is protected by the highest standards of security. Our solution offers a range of benefits, including enhanced breach protection, rapid recovery capabilities with immutable and indelible copies, and seamless scalability to accommodate your growing data volumes. Whether you're safeguarding intellectual property, customer data, or mission-critical systems, cyber vaulting gives you the peace of mind that comes with knowing that your information is secure. With our flexible deployment and cost-effective storage options, cyber vaulting is an ideal solution for organizations of all sizes and industries.

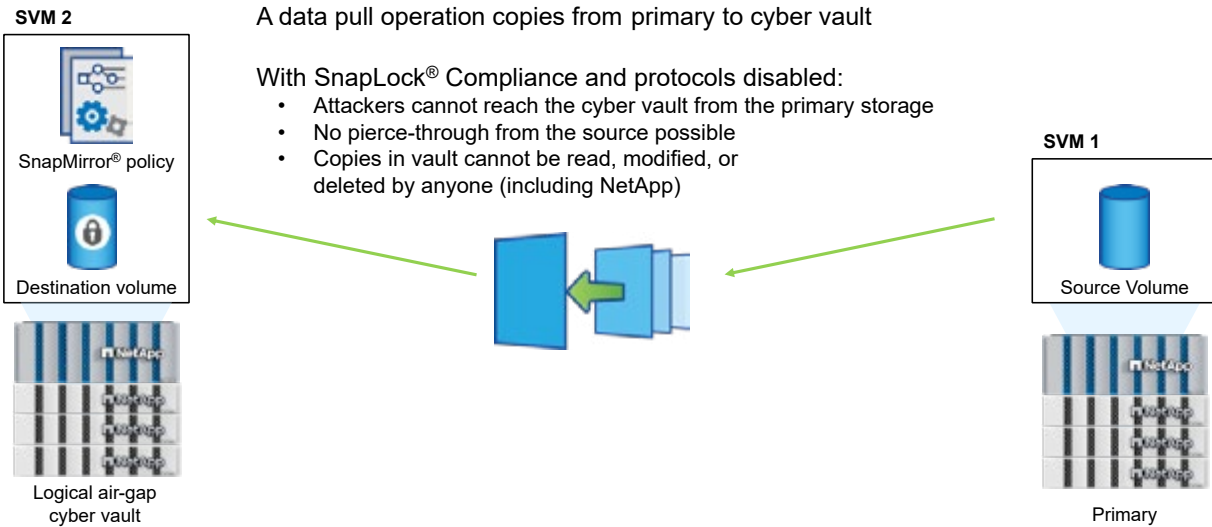**Logical air gap**
Isolated data plane without silos

**SVM 2**

SnapMirror® policy

Destination volume

Logical air-gap
cyber vault

A data pull operation copies from primary to cyber vault

With SnapLock® Compliance and protocols disabled:
- Attackers cannot reach the cyber vault from the primary storage
- No pierce-through from the source possible
- Copies in vault cannot be read, modified, or deleted by anyone (including NetApp)

**SVM 1**

Source Volume

Primary

Figure 1: Logical air gapping with NetApp SnapLock Compliance.

# NetApp logical air gapping

NetApp cyber vaulting empowers organizations to create logically air-gapped environments using NetApp ONTAP® software (Figure 1).

With ONTAP, you can:

- Create isolated storage systems that are logically separated from other networks and systems.

- Implement strict network segmentation and access controls to limit communication between storage and external networks.

- Use NetApp SnapLock® Compliance to create immutable and indelible, write-once-read-many (WORM) storage volumes that prevent data modification or deletion.

At the heart of an effective cyber vaulting strategy lies the ability to create immutable, tamper-proof backups that can withstand even the most sophisticated attacks. This is where NetApp SnapLock Compliance technology plays a pivotal role in the cyber vaulting equation.

SnapLock Compliance is a powerful data protection feature of the NetApp ONTAP unified storage operating system, designed to safeguard critical data against deletion, modification, or encryption. With SnapLock Compliance volumes, your backup data remains indelible and immune to tampering, even by privileged users or administrators—and even by NetApp Support.

When combined with ONTAP Snapshot™ technology, SnapLock Compliance enables the creation of logically air-gapped cyber vaults—secure, isolated storage repositories that house your organization's most valuable data. These cyber vaults are not merely passive repositories, but rather dynamic, resilient, and rapidly recoverable data safeguards.

With ONTAP cyber vaulting, NetApp SnapMirror® policies and rules are managed from the vault, further protecting the vault from service disruptions. See the reference architecture in Figure 2.

**Further hardening the air gap**
For the most critical data assets, NetApp cyber vaulting offers physical air-gapping options that completely disconnect storage systems from networks. With physical air gapping, you can:

- Deploy dedicated, isolated storage systems for maximum protection against external threats.

- Implement secure data transfer processes, with strict security protocols for scanning and handling media.

- Use SnapMirror to replicate data efficiently from production systems to air-gapped storage, enabling secure data transfer and recovery.

- Leverage NetApp AFF and FAS on-premises systems with hardware-based encryption for secure, high-performance storage in air-gapped environments.

**Robust hardening with NetApp ONTAP**

With NetApp ONTAP security hardening requirements, you can further safeguard your data when cyber vaulting in the following ways.

On both primary and cyber vault backup data:

- **Multi-admin verification.** The MAV security feature of ONTAP means that certain operations, such as deleting volumes or Snapshot copies, can be executed only after approvals from designated administrators. This feature prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.
- **Multifactor authentication.** The MFA feature of ONTAP enhances security by requiring users to provide two authentication methods to log in to an admin or data storage virtual machine (SVM).

Between primary and secondary storage:

- Isolate management networks
- Different credentials
- Separate administrators
- Dedicated replication network
- Separate data centers (optional)

NetApp cyber vaulting offers organizations a comprehensive and flexible solution for protecting their most critical data assets. By combining logical and physical air-gapping options with robust hardening methodologies, NetApp enables you to create secure, isolated storage environments that are resilient against evolving cyberthreats without creating knowledge or skills silos. With NetApp, you can be sure of the confidentiality, integrity, and availability of your data while maintaining the agility and efficiency of your storage infrastructure.

NetApp's multilayered cyber resilience capabilities help you protect your data, detect threats in real time, and rapidly recover from cyberattacks.

**Solution components**

- See how to get started with this cyber vaulting how-to blog on the NetApp Community site.
- AFF on-premises storage: NetApp AFF A-Series
- FAS on-premises storage: FAS storage: Seamless, efficient, trusted
- SnapLock Compliance software: Retention and rapid retrieval
- Security hardening guide for NetApp ONTAP

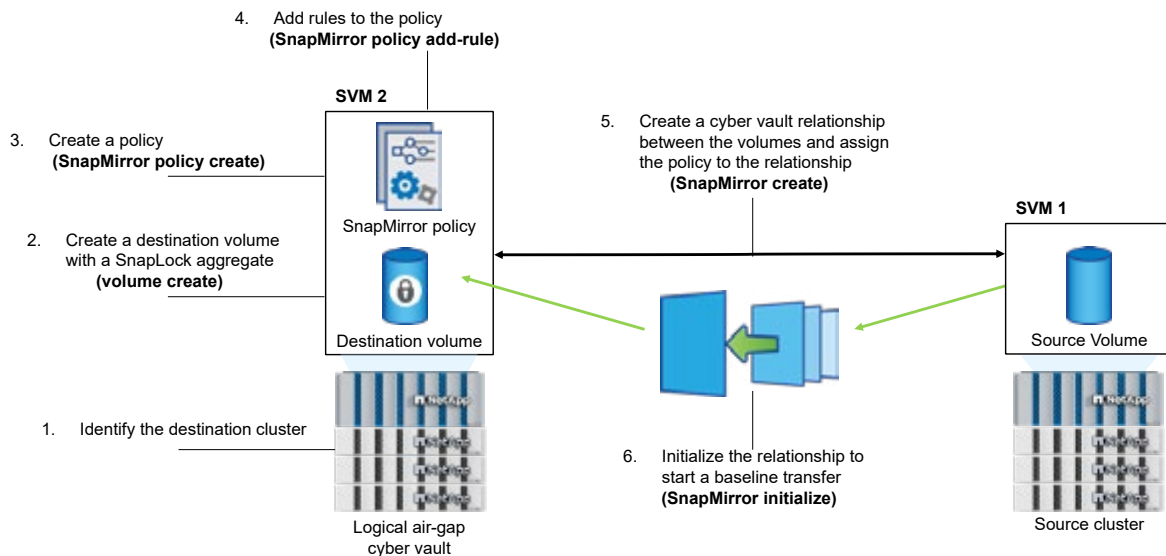Figure 2: NetApp cyber vaulting reference architecture.