

IMMUNIZE DATA FROM RANSOMWARE WITH SCALAR ACTIVE VAULT TECHNOLOGY

NOTICE

This technology brief contains information protected by copyright. Information in this technology brief is subject to change without notice and does not represent a commitment on the part of Quantum.

Quantum assumes no liability for any inaccuracies that may be contained in this technology brief.

Quantum makes no commitment to update or keep current the information in this document, and reserves the right to make changes to or discontinue this document and/or products without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of Quantum.

TABLE OF CONTENTS

Introduction 3

Library Partitions..... 3

Active Vault Security 4

Vaulting Process Flow 5

Putting the “Active” in Active Vault 7

Active Vault Benefits 8

INTRODUCTION

Ransomware isn't going away, and it's an enterprise problem. Government agencies and businesses of all sizes are increasingly targeted. Every organization needs a plan for protecting against this threat.

The key to thwarting ransomware is maintaining a copy of data that is completely inaccessible from any network, a characteristic sometimes referred to as "air-gapped." The most cost effective and secure way to hold data offline is magnetic tape. A tape cartridge on a shelf is completely immune to ransomware. But this approach has inconveniences and potential risks.

Traditionally, moving tapes offline meant physically exporting them from an automated tape library, and having an operator carry them to a shelf or container in a physically secure location. This takes time better spent elsewhere, and because it involves humans, it's error prone. Tapes are easily misfiled or lost. And while tape cartridges are reasonably robust, they do not handle physical abuse well. Drops to the floor can damage them.

This Technology Brief describes how Quantum's unique Active Vault—an optional feature of Quantum's Scalar® tape libraries—enables keeping an ultra-secure, air-gapped copy of data that is also protected from human error.

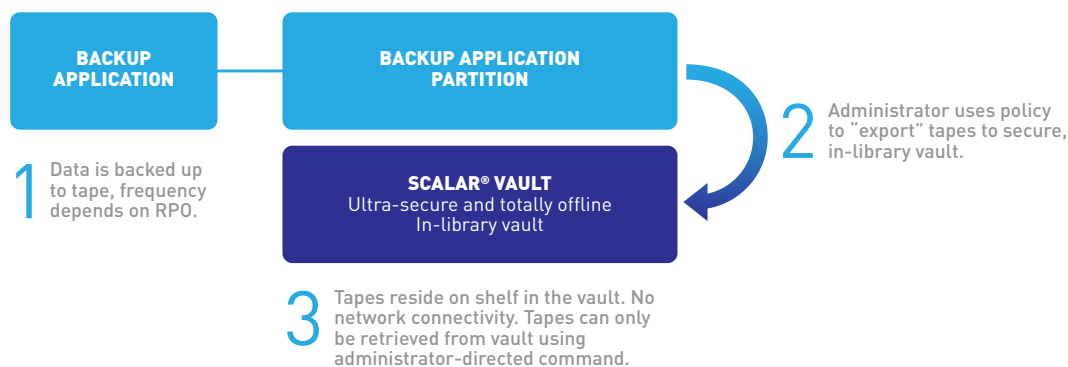


Figure 1. Active Vault At-a-Glance

LIBRARY PARTITIONS

Tape library partitions were invented to share one tape library among several applications. Partitions normally contain dedicated data slots, cartridges, tape drives, and import/export (I/E) slots but share the robot. In Scalar libraries these are known as application-managed partitions. Quantum has evolved the concept of partitions beyond mere application sharing. Scalar libraries may also contain library-managed partitions, which consist of unlicensed slots, are invisible to external applications and are used to enable special features.

One type of library-managed partition is the Active Vault (AV) partition. AV partitions provide a secure storage location within the library that is not accessible to applications, even accidentally. They are configured by the tape library administrator and may be any size required.

Add

Available Resources
Storage: 612 I/E: 6 Drive: 0

Partition Name:

Type:

Vendor Identification:

Product Identification:

Control Interface:

Barcode Reporting:

Number of Drives:

Drive Type:

Storage Slots:

Extended IE Slots:

IE Slots:

AMP Extension:

Figure 2. Adding an Active Vault Partition - note the fields for robotic control and drives are not selectable

ACTIVE VAULT SECURITY

Active Vault provides security for data in several ways. AV partitions may not be exposed externally to applications. The library software simply does not allow it. An operator cannot accidentally put vaulted tapes “online,” exposed to threats. AV partitions also contain no tape drives, providing an additional barrier to access. Finally, because vaulted tapes remain in the library, they are safe from mishandling, damage, and loss.

Access to Active Vault configuration is restricted as well. Only tape library administrators may create, modify, delete, or reconfigure AV partitions. Library operators have “User” privileges only, which may be restricted to specific partitions when a library is shared by multiple applications. For greater security, Scalar libraries may be integrated with Microsoft Active Directory or other LDAP directory services.

Sometimes additional media security is needed, so Active Vault is compatible with other standard Scalar library security features, such as full tape encryption, WORM media, and media security notifications.

VAULTING PROCESS FLOW

Tapes may be moved into an AV partition manually using the library GUI, but usually this movement is controlled by policy, as shown in Figure 3 below. A typical policy might be that when the application that owns application-managed partition “NBU” exports a tape, that tape should move into the AV partition named “NBU-V” instead of the library’s I/E slots. The application believes the tapes have left the library, but instead they have been moved into the secure vault. If there are multiple applications using the library, each one may have a corresponding AV partition of its own.

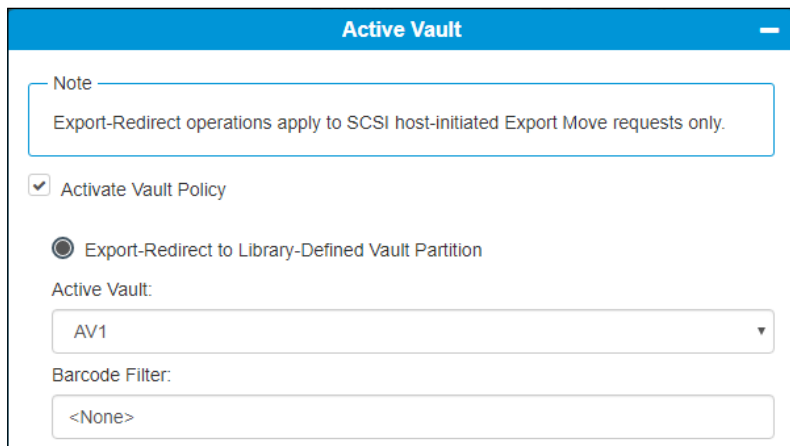


Figure 3. Active Vault Export-Redirect Policy Dialog

Let’s compare the operator experience with manual vaulting vs. Active Vault:

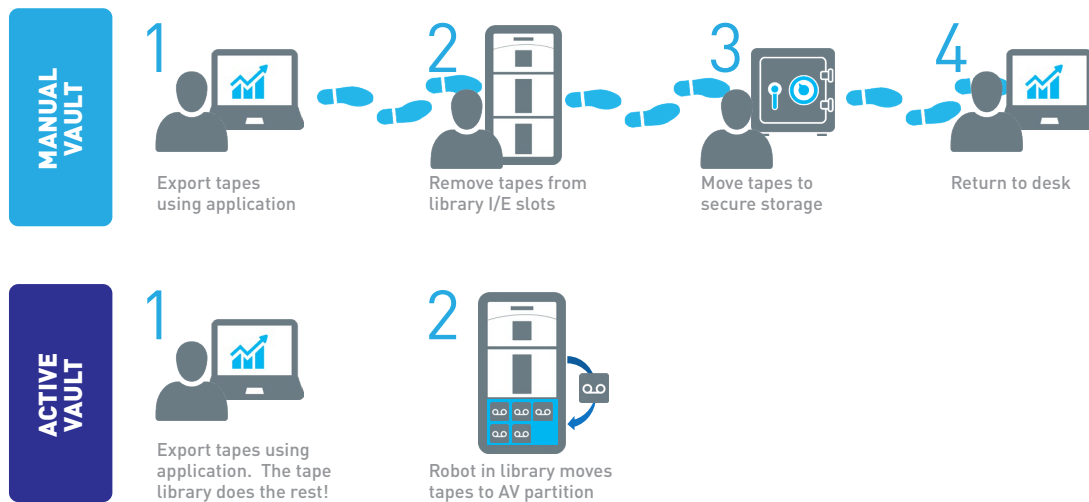


Figure 4. Vaulting Workflow, Before & After Active Vault

With Active Vault, the operator takes no additional steps and does not have to leave their desk to physically interact with the library or media. The library can even be in a lights-out facility thousands of miles away.

Retrieving data from a manual vault is a similar process:

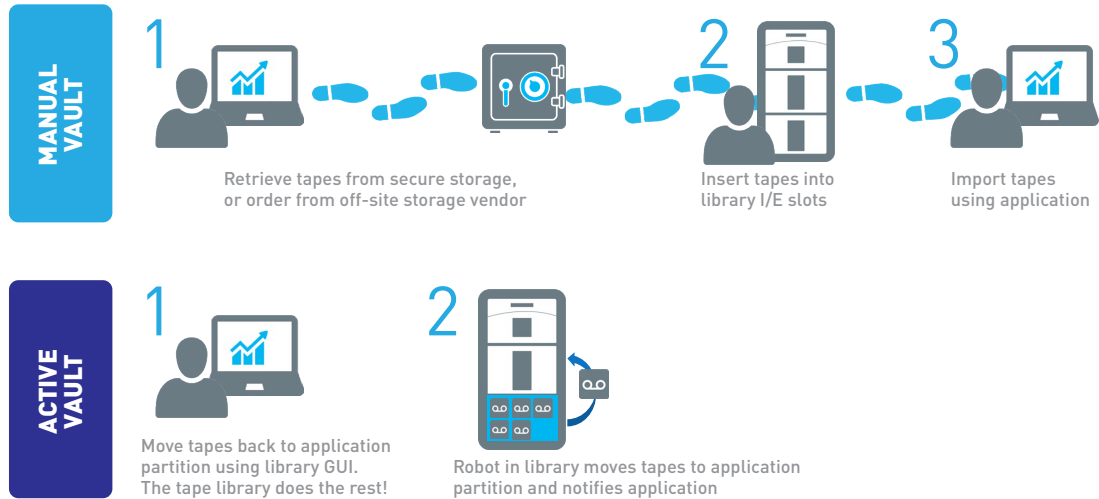


Figure 5. Vault Retrieval Workflow - Before & After Active Vault

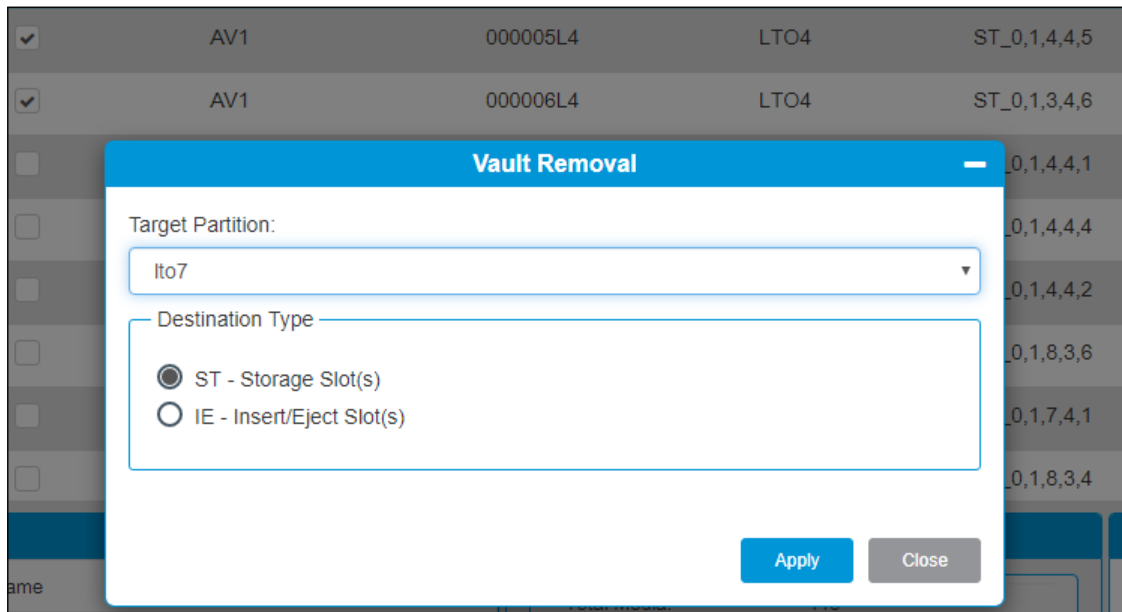


Figure 6. Scalar i6000 Vault Retrieval Dialog

PUTTING THE “ACTIVE” IN ACTIVE VAULT

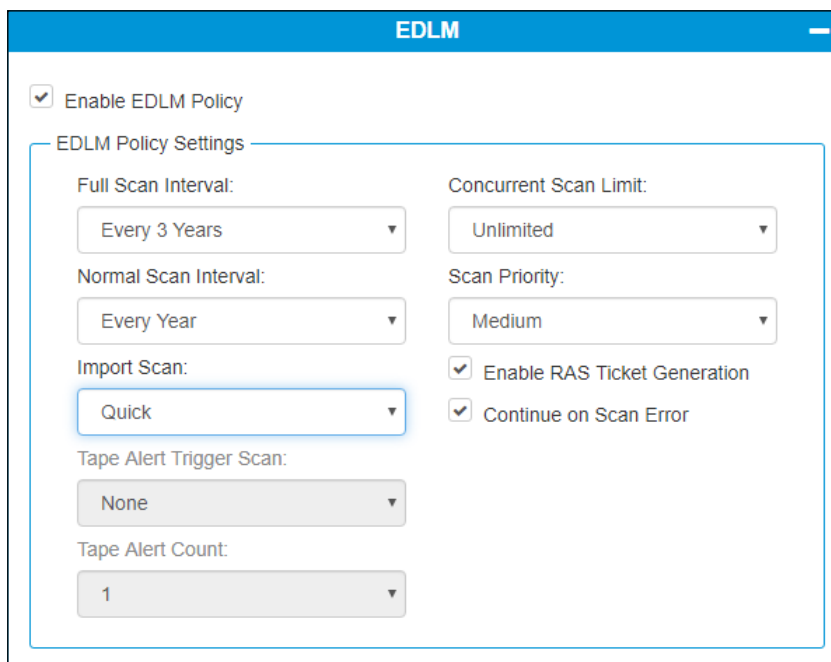
Another danger that can put vaulted data at risk is media degradation. Stored under proper conditions, magnetic tape can last for decades. Real-life durability depends on how and how much the media is used, the cleanliness of the atmosphere in which it runs, and the temperature and humidity of storage locations. Simply put, the only way to know if your data is still accessible is to test it.

Manually vaulted media sitting on a shelf is almost never tested. It's simply too big a hassle. Instead, organizations roll the dice, only learning media has gone bad when needed data is irretrievable.

Automated Media Conditions Monitoring

Years ago, Quantum created Enterprise Data Lifecycle Management (EDLM) to solve this problem. EDLM is an optional feature of Scalar i6 and i6000 libraries that provides policy-based, automated background media validation. It monitors media condition, warning when tapes have degraded while there is still time to act, before any data is lost.

If a customer purchases and configures EDLM, tapes residing in an AV partition will be scanned at programmed intervals, ensuring that vaulted data is kept in good condition. Tape drives used for EDLM scanning have their external data ports disabled, so the integrity of the Active Vault is maintained. Even if these drives are accidentally connected to the storage network, no data may be accessed.



The screenshot shows the EDLM configuration window with the following settings:

- Enable EDLM Policy
- EDLM Policy Settings:
 - Full Scan Interval: Every 3 Years
 - Concurrent Scan Limit: Unlimited
 - Normal Scan Interval: Every Year
 - Scan Priority: Medium
 - Import Scan: Quick
 - Tape Alert Trigger Scan: None
 - Tape Alert Count: 1
 - Enable RAS Ticket Generation
 - Continue on Scan Error

Figure 7. EDLM Policy Configuration on an Active Vault Partition

ACTIVE VAULT BENEFITS

- Provides ultra-secure, offline data storage
- Saves operator time
- Eliminates manual media handling
- Saves storage space
- Transparent to applications
- Enables lights-out and remote vaulting
- Eliminates risk of physical media damage or loss
- Secures media from accidental exposure
- Enables proactive media condition monitoring & alerting