THE QUANTUM SCALAR SECURITY FRAMEWORK:
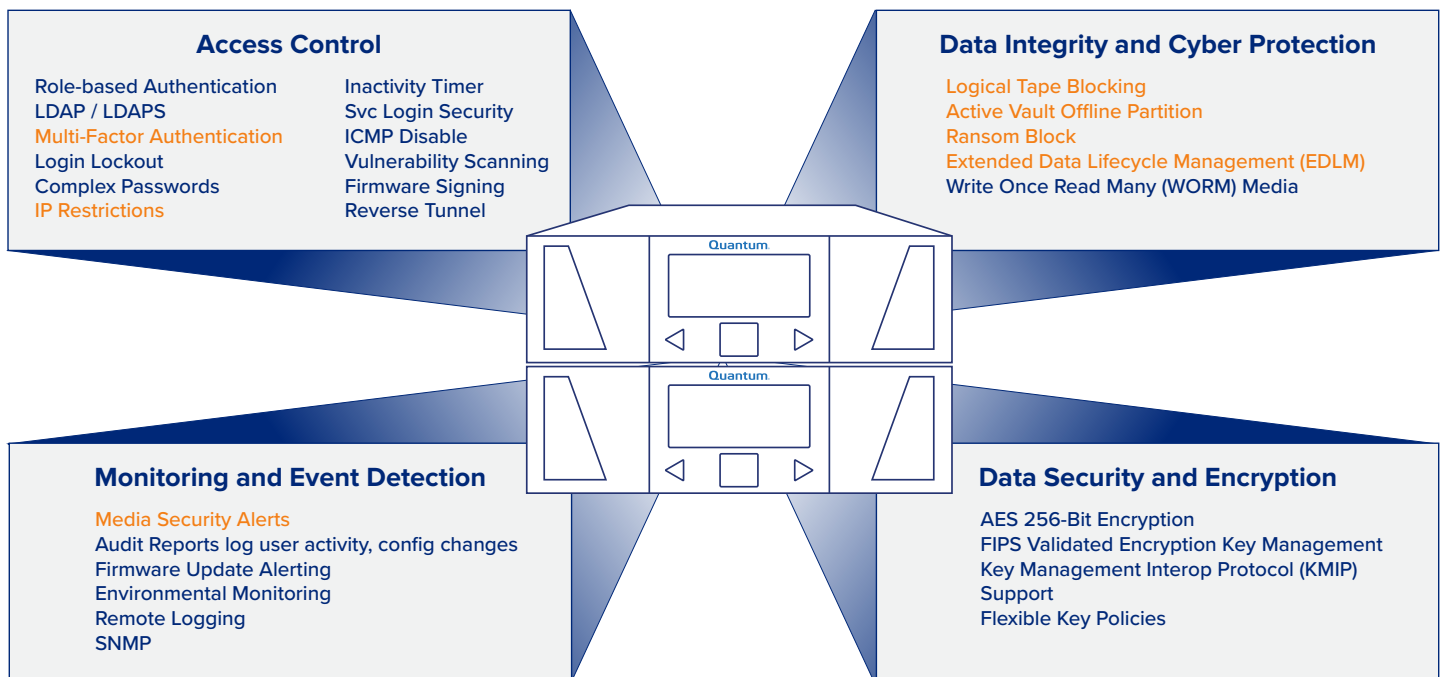
A TECHNICAL BRIEF

Introduction

Security isn't something you can buy. It's not a product, or a feature, or any one thing in isolation. Security is better described as an approach, a way of doing things, or even an attitude or state of mind. Security comes from leveraging the right tools and techniques in the right ways at the right times, and from constantly evaluating opportunities to improve security, because adversaries are constantly evaluating ways to get around your defenses.

Quantum Scalar Tape Libraries are used by everyone from small nonprofits to the world's largest hyperscalers. Organizations rely on them to protect their data, and Quantum takes that responsibility seriously. Scalar libraries are developed with security in mind.

This Tech Brief will provide an overview of the Scalar Security Framework, a combination of tools, features, and methods of operation – many of them unique in the industry – that make Quantum Scalar Tape Libraries the most secure tape storage systems available.

The Scalar Security Framework

The Scalar Security Framework consists of four pillars, each equally critical to achieving and maintaining a secure system. None stands alone, all are interrelated, comprising a layered approach to security. Features marked with an (*) below are exclusive to Quantum Scalar Tape Systems. Certain features may not be available in all Scalar library models.

Access Control

Role-based Authentication	Inactivity Timer
LDAP / LDAPS	Svc Login Security
Multi-Factor Authentication	ICMP Disable
Login Lockout	Vulnerability Scanning
Complex Passwords	Firmware Signing
IP Restrictions	Reverse Tunnel

Data Integrity and Cyber Protection

Logical Tape Blocking
Active Vault Offline Partition
Ransom Block
Extended Data Lifecycle Management (EDLM)
Write Once Read Many (WORM) Media

Monitoring and Event Detection

Media Security Alerts
Audit Reports log user activity, config changes
Firmware Update Alerting
Environmental Monitoring
Remote Logging
SNMP

Data Security and Encryption

AES 256-Bit Encryption
FIPS Validated Encryption Key Management
Key Management Interop Protocol (KMIP) Support
Flexible Key Policies

Orange indicates a feature that is unique to Quantum Scalar® Tape Systems.

Access Control

Maintaining data integrity and data security rely upon maintaining the security of the system, which relies on controlling access to administrative interfaces. Robust access control prevents accidental or malicious changes to the system configuration which could weaken data integrity or data security. Quantum Scalar Tape systems provide a comprehensive set of Access Control features as listed in the table below:

Feature	Description
MFA	Multifactor authentication option for library UI login using standard MFA apps
IP Restrictions	Limit which IPv4/v6 addresses may access the library UI
LDAP/LDAPS	User authentication using LDAP directory services, including secure LDAP
Complex Passwords	Support for long (up to 64 character) and complex passwords
Login Lockout	15-min lockout after 5 failed login attempts thwarts brute-force attacks
Inactivity Timer	Users logged out after a configurable period of inactivity
RBAC	Multiple roles and options to limit user access to specific partitions or functions
Svc Login Security	Option to restrict service access to local on-device UI only
Svc Access Window	Set a time-limited window for service personnel access
Svc Access Disable	Option to completely disable service account
Reverse Tunnel	Configurable time-limited reverse tunneling for remote Support access
ICMP Disable	Option to disable ICMP to prevent discovery of library via 'ping'
Vulnerability Scanning	Every firmware release tested with multiple security scanners. Cloud-Based Analytics (CBA) portal scanned weekly
Firmware Signing	New library firmware is automatically authenticated prior to being installed

Monitoring and Event Detection

Constant monitoring is key to ensuring that the security design of a system is maintained. In addition to damage from attacks, security can be eroded accidentally or unintentionally over time, especially if a system is shared or subject to administration by multiple individuals. Event detection involves detecting and logging important changes to the system, and where applicable, alerting an administrator or other trusted party to the occurrence of an event.

Feature	Description
Media Security Alerts	Library alerts on expected and/or unexpected media removal events
Environmental Monitoring	Monitoring and logging of temperature and humidity. Library alerts if values fall outside safe range for media
Audit Reports	Log all user activity, library configuration changes, and more
Firmware Update Alert	Library alerts operator when updated firmware is available
Remote Logging	Support for sending log events to a remote syslog server
SNMP	Security and health information may be monitored via SNMP

Data Security and Encryption

Maintaining data security involves ensuring that the information stored on the tape media in the library cannot be stolen or viewed by unauthorized parties. Even if individual tapes or the entire library are stolen, data encryption ensures that the information is safe. Robust data security thwarts data breaches, blackmail, and the associated regulatory compliance complications that come with them.

Feature	Description
AES 256-bit Encryption	Support for hardware-based LTO tape encryption – no performance degradation
Encryption Key Management	Support for application-based or centralized SKM or KMIP encryption key management
Flexible Key Policies	Choice of one encryption key per tape, per partition, or per library

Data Integrity and Cyber Protection

Maintaining data integrity means ensuring that data stored in the library has not changed unexpectedly. Unexpected data change can be dramatic, or intentional (on the part of a nefarious actor), such as being encrypted by ransomware. Just as dangerous, and even harder to detect, is data change that's subtle and unintentional, such as those caused by media wear, bit rot, or environmental degradation. Protecting data integrity means safeguarding data from destruction or loss.

Feature	Description
Active Vault	Secure, isolated in-library vault partition not visible to applications or network
Logical Tape Locking	Software-based lock prevents media from leaving the magazine until the magazine is physically removed and re-inserted into the library by an operator.
Ransom Block	Partial eject of magazine puts media physically out of reach of the robot until operator re-inserts the magazine. Media is still visible to the barcode scanner for inventory validation.
Extended Data Lifecycle Mgmt (EDLM)	Monitors data/media health, alerts, and proactively takes action on suspect media.
WORM	Support for hardware-enforced immutability using LTO WORM media

To Learn More

For more information on all of these features and capabilities, read the Scalar Security Framework White Paper.

Quantum.