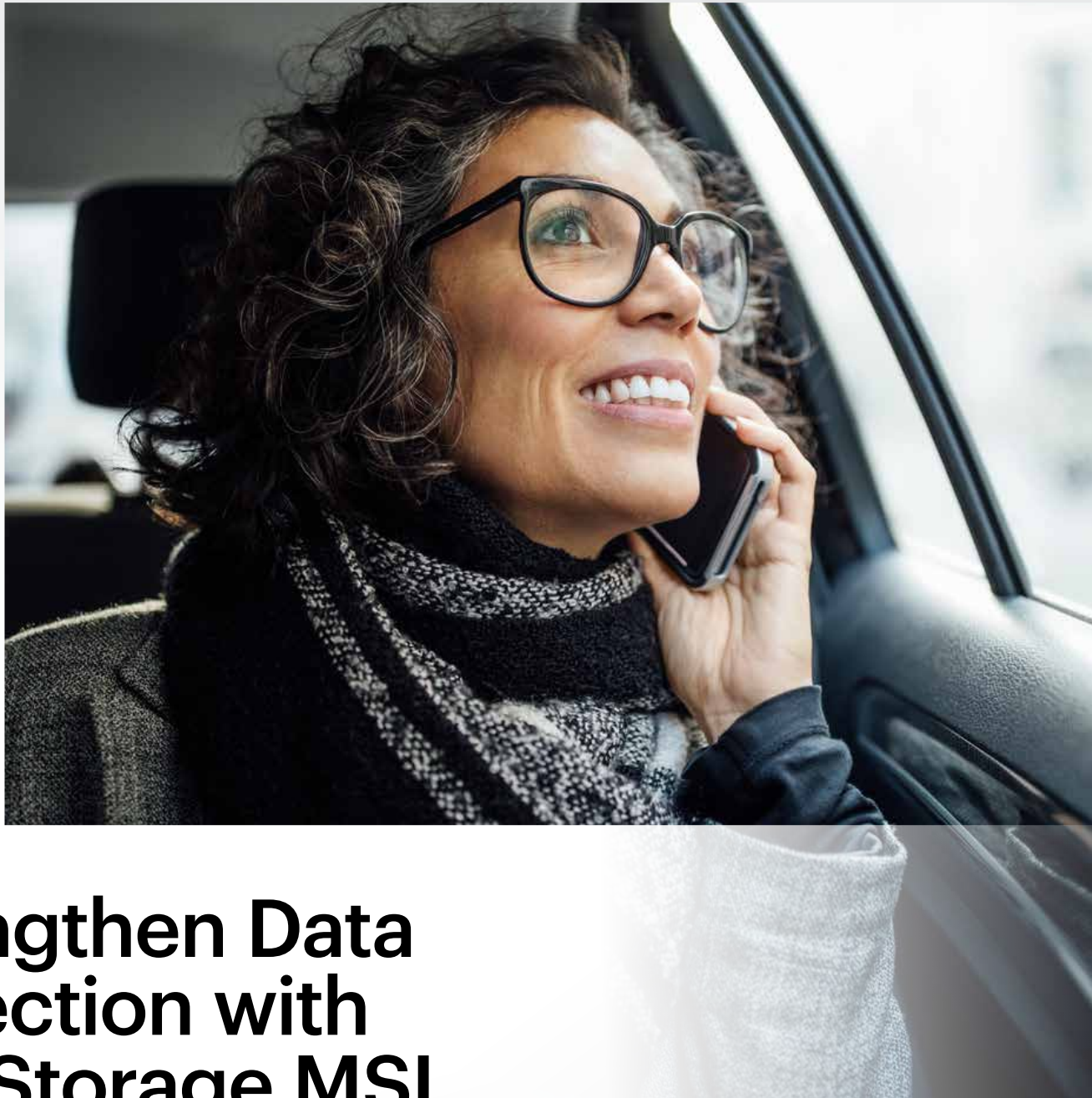




Strengthen Data Protection with HPE Storage MSL Vault Partition

Protect your data from evolving threats

Organizations today face increasing risks from ransomware, insider threats, and compliance violations. Traditional backup systems, especially those online or disk-based, are vulnerable to attack and accidental modification. HPE Storage MSL Vault Partition introduces a new layer of defense by creating isolated, air-gapped partitions within tape libraries that are invisible to applications and more secure with multi-factor authentication (MFA). This secure architecture ensures that backup data remains protected, even if primary systems are compromised.

Achieve secure, air-gapped protection without physical media handling

The HPE Storage MSL Vault Partition creates hidden, drive-free partitions inaccessible to host communication. Only administrators with Security-level access and MFA enabled can manage vaulted media through the Remote Management Interface (RMI), minimizing manual tape handling and ensuring data remains secure.

1. Secure, Isolated Architecture:

Vaulted media is hidden from backup software, inaccessible to host systems, and protected by a drive-free design that prevents read/write operations.

2. Role-based access control:

Only administrators with security-level privileges and MFA enabled can access or manage the MSL Vault Partition.

Layered Security for Long-Term Data Protection and Compliance

Enhance long-term data integrity by layering the HPE Storage MSL Vault Partition with Command View for Tape Libraries (CVTL) – Data Verification and encryption features. This integrated approach strengthens protection against evolving threats and supports regulatory compliance and strengthens protection against evolving threats.

1. Security-Level Access Control:

Only administrators with security-level privileges and MFA can access or manage the MSL Vault Partition.

2. Data Verification: The optional CVTL feature verifies media health without disrupting operations. Media must be removed from the MSL Vault Partition for verification.

3. AES-256 Encryption: Works with the HPE Storage MSL Encryption Kit or any KMIP-supported encryption solution to safeguard data.

4. WORM (Write-Once, Read-Many) Protection: Ensures data written to tape cannot be altered or overwritten, providing immutable retention for compliance, audit integrity, and ransomware resilience.



Get started with HPE Storage MSL Vault Partition

HPE Storage MSL Vault Partition is included at no additional cost with new HPE MSL3040 and MSL6480 Tape Libraries or can be enabled via firmware upgrade for eligible systems. It offers a secure, automated, and cost-effective solution for data protection - helping you safeguard against ransomware, reduce operational overhead, and ensure your data remains protected, accessible, and resilient.

Learn more at

hpe.com/storage/tape

Visit 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.

a00155512enw

HEWLETT PACKARD ENTERPRISE

hpe.com

