Reference Architecture

Lumen Validated Design for Cyber Resilience with Commvault

Lumen as the Operational Environment

Introduction

Lumen Validated Design (LVD) for Cyber Resilience with Commvault combines Lumen's network innovation with Commvault's advanced data protection to deliver secure, scalable recovery across hybrid environments. This reference architecture demonstrates how integrated threat detection, edge-optimized connectivity, and immutable backups can simplify operations and strengthen business continuity.

The purpose of this document is to provide a proven blueprint for deploying cyber-resilient backup and recovery solutions. It details the roles of both Lumen and Commvault, outlines design principles such as defense-in-depth, and describes how features like air-gapped backups, unified management, and zero-trust security help organizations protect critical data, recover rapidly from cyber incidents, and maintain compliance. Built on Lumen's own production experience, this validated design reinforces real-world performance and market credibility for organizations seeking robust cyber resilience strategies.

The entire validation process has been documented in the White Paper **The technical case for the Lumen® Validated Design for Cyber Resilience with Commvault.**

Design overview

This section outlines the architecture, platform roles and infrastructure components that support cyber-resilient backup and recovery across hybrid environments. The validated design integrates Commvault's enterprise-grade data protection with high-performance transport provided by Lumen to deliver scalable, secure and automated recovery capabilities.

Validated design principles

This validated design applies a defense-in-depth approach to enterprise data protection. It emphasizes rapid, clean recovery across hybrid environments and includes:

- Immutable, air-gapped backups
- Unified platform for on-premises and cloud workloads
- Comprehensive analytics and anomaly detection
- Scalable architecture with 10PB design capacity

High Level Design

Role of Commvault

Commvault serves as the foundational data protection platform and was selected for its ability to deliver scalable, secure and automated backup and recovery across hybrid environments. The solution is designed to support petabyte-scale workloads and enforce multilayered cyber resilience while handling complex backup requirements and a diverse application and server portfolio.

Platform architecture

The core platform components deployed across Lumen's hybrid infrastructure include:

- Commvault Cloud SaaS, delivered as Lumen® Data Protect (LDP) - provides cloud-delivered backup and recovery for SaaS workloads and cloud environments
- Commvault Cloud Software – deployed on-premises to manage backup and recovery for local and hybrid workloads
- Air Gap Protect (AGP) – implemented in Azure and AWS, and providing logically air-gapped, immutable backup copies with separate authentication domains to help prevent tampering, deletion or malicious changes
- HyperScale X appliances and Lumen® Network Storage, with NetApp – supports local primary and remote secondary backup tiers and includes a third air-gapped copy

Services not available everywhere. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.

Operational design

- Unified control plane: Centralized policy management and orchestration for backup, recovery and storage tiering across all environments.
- Elastic consumption model: Storage is provisioned dynamically with pricing aligned to actual usage.
- Automation: Policy-driven orchestration of backup and recovery workflows reduces manual intervention and helps create consistency across platforms.
- Global deduplication: Reduces storage footprint and network bandwidth requirements to optimize performance and cost.

Cyber resilience features

- Immutable and indelible storage in separate tenancy: Production and backup copies are stored in accounts that use different security tenancies. This helps protect against modification and deletion, enforces independent authentication domains, minimizes the risk of lateral compromise and helps create clean recovery points even if primary credentials are compromised.
- Logical Air Gapping: Backups are isolated from production networks and secured with independent access controls.
- Multi-region and cross-cloud recovery: Supports failover and restoration across geographies and cloud providers.
- Zero-trust architecture: Enforces Multi Factor Authentication (MFA), Role-Based Access Control (RBAC), Identity Provider (IDP) integration and encryption in-flight and at-rest to protect backup infrastructure.

Native Application Programming Interface (API) integration:

- Native API integration: Enables efficient, agentless protection of cloud-native services through secure authentication protocols for major public cloud platforms.
- Cross-cloud Disaster Recovery (DR) orchestration: Automates Virtual Machines (VM) conversions and failover between cloud providers. Intelligent copy-management automates data movement to cost-effective cloud storage classes (e.g., S3 to Glacier, Blob Hot to Archive).
- Granular recovery for SaaS applications: Enables item-level restores directly into live environments for applications such as Microsoft 365, Active Directory and Salesforce.
- Kubernetes and container protection: Includes persistent volumes and configuration manifests, supporting full application recovery and migration.

Commvault products and services included in this design:

- 10PB of Commvault Cloud Backup and Recovery and Risk Analysis
- HyperScale X Reference Architecture Software for Hewlett Packard Enterprise (HPE) appliances
- NetApp for 3rd Air Gapped copy
- Air Gap Protect

Role of Lumen

Lumen provides a high-performance transport backbone for Commvault's data protection, enabling fast, movement of encrypted data across hybrid environments. With IP VPN On-Demand and Cloud Connect, Lumen delivers scalable, secure connectivity tailored to workload needs for both proactive protection and rapid recovery.

Bulk Data Transfer (BDT) optimization

For high-volume backup and recovery operations, Lumen uses Lumen® Wavelength Solutions. These connections support:

- High throughput for large-scale data transfers.
- Low latency for time-sensitive recovery operations.
- Dedicated bandwidth for vaulting and replication tasks.

Cloud connectivity via Lumen IP VPN (ASN 3549)

For non-BDT traffic, Lumen leverages Cloud Connect across ASN 3549, its core IP VPN routing platform to provide secure, high-performance connectivity and dynamic provisioning between data centers and major cloud hypervisors. This backbone supports secure routing, traffic isolation and low-latency data movement across hybrid environments.

- Global transit and peering strategies
- High-availability architectures
- Regulatory compliance in cross-border data flows
- Platform evaluations for latency, throughput, and resilience

Services not available everywhere. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.

Encryption and security in transit

Customers may encrypt the data in motion using Transport Layer Security (TLS)-based encryption and Federal Information Processing Standard (FIPS)-compliant cryptographic modules. This helps maintain the confidentiality of sensitive data, integrity of backup payloads, resilience against interception or tampering, and regulatory compliance.

Lumen products and services included in this design:

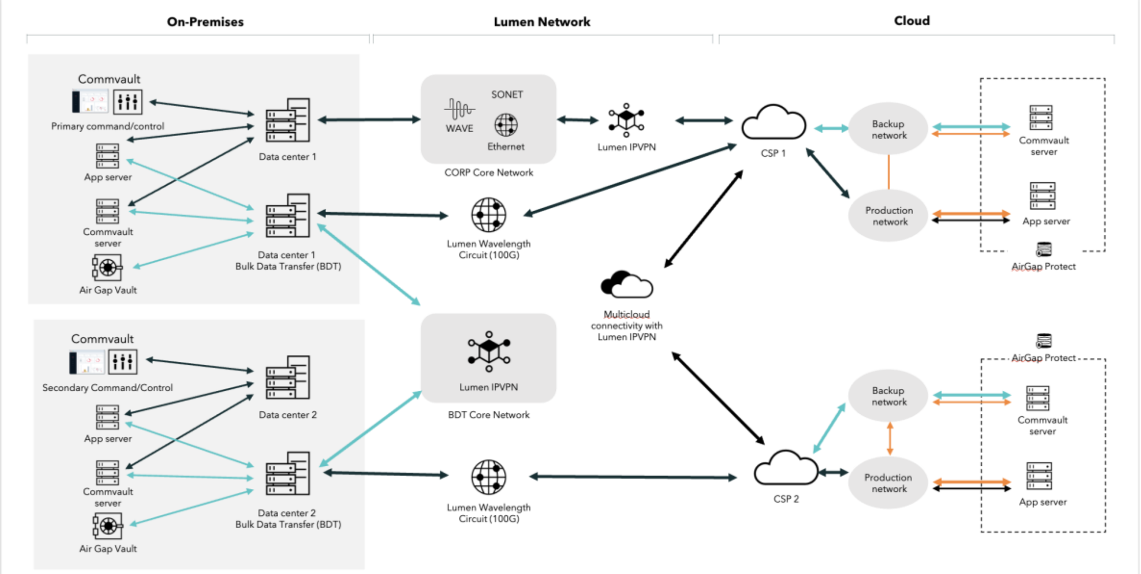
- IP VPN
- Wavelengths
- Ethernet
- Cloud Connect with IP VPN On-Demand

Architecture and design

The Lumen Validated Design for Cyber Resiliency is built on a foundation of architectural clarity and operational rigor. This section outlines the core design elements that enable secure, scalable and automated data protection across hybrid environments. It includes logical architecture, physical deployment models and integration strategies that support cleanroom recovery, zero-trust enforcement and centralized governance.

Logical architecture

The logical architecture defines how core components interact to enforce policy, isolate trust zones, and orchestrate data movement across cloud and on-premises environments. It enables streamlined cleanroom recovery, anomaly detection, and automated workflows. The following diagram illustrates these relationships.



↔: ability to backup and restore

Black: Corporate core network

Teal: Bulk data core network

Orange: Cloud network

Data flow overview

- Primary data flow: Application servers generate production data, which is backed up to local vaults and replicated to an alternate geographical location via Lumen IP VPN and Bulk Data Transfer (BDT) circuits.
- Vaulting operations: Backup data are written to Commvault Air Gap-protected vaults, both on-premises and in cloud zones. These vaults are logically isolated and support immutable storage.
- Replication Pathways:
  - On-premise to cloud replication: Backup data can be replicated from on-premise vaults to cloud vaults using Lumen Wavelengths, Ethernet circuits, and IP VPN.
  - Cross-cloud replication: Data can be replicated between cloud-service providers (CSPs) via the Lumen multi-cloud IP VPN backbone, between regions within a given CSP, or both.
  - Inter-data center replication: Data centers are interconnected via BDT core network and transport layers (Wave, Ethernet, SONET).

Backup and vaulting topology

- Local vaults: Each data center includes primary backup storage targets for immediate backup and recovery, and an air-gapped secondary backup storage target.
- Air Gap Protect (AGP): Commvault's AGP service manages cloud-based vaults with logical air-gapping and separate authentication domains.
- Control plane orchestration: Backup and replication handled by primary and secondary command-and-control (C2) servers, which interface with vault tiers and CSP endpoints.

Physical deployment

This section details how cleanroom recovery zones, air-gapped vaults and policy enforcement layers are physically instantiated across data centers, cloud platforms and edge locations. It highlights how trust boundaries are enforced through network segmentation, how immutable storage is provisioned and how automation is embedded into the deployment to support lean operations and rapid recovery. These deployment patterns are designed to meet the resiliency, compliance and scalability requirements outlined in earlier sections.

Hardware components

- Application servers and backup servers: Distributed across data centers and cloud zones to support workload-specific local backup and recovery, as well as geographical site disaster recovery.
- HyperScale X Reference Architecture Software for HPE appliances: Used for scalable, high-performance backup storage and compute.
- NetApp storage arrays: Support a third copy of backup data, including air-gapped configurations.

Network components

- Lumen IP VPN (ASN 3549): Provides private transport for backup and recovery traffic across hybrid environments.
- Lumen Wavelengths circuits: Dedicated high-throughput links for Bulk Data Transfer (BDT) to Azure and other CSPs.
- BDT core network: Supports large-scale data movement between data centers and cloud vaults.
- Wave, Ethernet, SONET: Additional transport options used for inter-site connectivity and redundancy.

Cloud Components

- Air Gap Protect (AGP): Commvault's cloud-based, isolated, immutable and indelible storage service deployed at multiple CSPs.
- Cloud service providers (CSP 1, CSP 2): Represent multi-cloud targets for backup and recovery, integrated via Lumen IP VPN and Commvault's cloud-native APIs.
- Production and backup networks: Segmented cloud networks for operational workloads and backup data to support isolation and security.

Integration points

- Primary and secondary C2 nodes: These nodes orchestrate backup and recovery workflows across data centers and CSPs.
- Air Gap Vaults: Deployed on-premises and in the cloud, these vaults are logically isolated and managed by Commvault's Air Gap Protect (AGP) service.
- Multi-cloud connectivity: Enabled via Lumen IP VPN, Wavelengths and Ethernet circuits to support seamless data movement between on-premises infrastructure and CSPs.
- Commvault platform integration: Commvault interfaces with Lumen network fabric to manage backup traffic routing, vaulting operations and recovery orchestration.

Security controls

This section details how Lumen and Commvault technologies interlock to automate cleanroom recovery, enforce zero-trust boundaries and maintain compliance across hybrid environments. It focuses on orchestration layers, identity and access controls, and observability mechanisms that check that protection policies are consistently applied—regardless of where data reside or how it moves.

Logical air-gapping

- Air Gap Vaults are deployed on-premises and in the cloud.
- These vaults are isolated from production networks and managed by Commvault's Air Gap Protect (AGP) so that backup copies are immutable and not accessible via standard network paths.

Network segmentation

- The architecture separates production networks from backup networks, both on-premises and in the cloud.
- Segmentation reduces the attack surface and prevents lateral movement of threats between operational and recovery infrastructure.

Encrypted transport

- All data in motion are routed through Lumen IP VPN, which provides private transport across hybrid environments.
- Backup data is encrypted at the application layer during transmission using Commvault's in-flight encryption protocols to provide multilayered protection across hybrid environments.
- TLS-based encryption and FIPS-compliant cryptographic modules are used to secure backup traffic over Lumen's backbone.

Dedicated Bulk Data Transfer (BDT) paths

- Lumen Wavelengths circuits are used for BDT traffic and isolated from general-purpose corporate networks.
- These dedicated paths reduce exposure to secure, high-throughput data movement between vaults and CSPs.

Command and control isolation

- The architecture includes Redundant Control plane, which orchestrates backup and recovery workflows.
- These nodes are logically separated from application servers and vaults, supporting secure orchestration and policy enforcement.

Multi-cloud security integration

- Connectivity to CSPs is managed via Lumen IP VPN, avoiding public internet exposure.
- Backup and recovery operations are executed within segmented cloud networks, maintaining isolation between production and backup environments.

Bill of Materials

Component	How to Buy
IP VPN	https://www.lumen.com/en-us/networking/ipvpn-on-demand.htm
Wavelengths	https://www.lumen.com/en-us/services/wavelengths.html
Ethernet	https://www.lumen.com/en-us/networking/ethernet.html
Cloud Connect	https://www.lumen.com/en-us/edge-cloud/cloud-connect.html
Commvault Cloud Air Gap Protect for Commvault, US & Canada, AWS Infrequent Tier	Available via Lumen Data Protect (https://www.lumen.com/en-us/services/lumen-data-protect.html)
CVLT Sensitive Data Governance for Non-Virtual and File, Unlimited Front-End TerabyteCVLT Sensitive Data Governance for Non-Virtual and File, Unlimited Front-End Terabyte	Available via Lumen Data Protect (https://www.lumen.com/en-us/services/lumen-data-protect.html)
Commvault Sensitive Data Governance, Per Front-End Terabyte	Available via Lumen Data Protect (https://www.lumen.com/en-us/services/lumen-data-protect.html)
Commvault File Optimization, Per Front-End Terabyte	Available via Lumen Data Protect (https://www.lumen.com/en-us/services/lumen-data-protect.html)
CVLT File Optimization for Non-Virtual and File, Unlimited Front-End Terabyte	Available via Lumen Data Protect (https://www.lumen.com/en-us/services/lumen-data-protect.html)
Commvault Cloud Air Gap Protect for Commvault, US & Canada, AWS Frequent Tier	Available via Lumen Data Protect (https://www.lumen.com/en-us/services/lumen-data-protect.html)
Commvault Complete DP, Per Front-End Terabyte	Available via Lumen Data Protect (https://www.lumen.com/en-us/services/lumen-data-protect.html)
Commvault Complete DP, Per Front-End Terabyte	Available via Lumen Data Protect (https://www.lumen.com/en-us/services/lumen-data-protect.html)
CVLT HyperScale X Reference Architecture 24-Drive Node, Per Node	SOW via Lumen or direct from Commvault (SKU: CV-HSRA-24-1N)

Lumen support guides:

- https://www.lumen.com/help/en-us/products.html
- https://www.lumen.com/help/en-us/readiness/prepare-to-activate-your-services-in-north-america.html

Commvault support guides:

- Best Practices for the CommCell Environment - https://documentation.commvault.com/11.40/expert/best_practices_for_commcell_environment.html
- Ransomware Protection - https://documentation.commvault.com/11.40/expert/ransomware_protection_01.html

Why Lumen?

With the rapidly changing marketplace, you need a partner to help you transform your organization. Lumen is committed to being a trusted partner to help you realize your security needs and priorities so you can focus on growing your business. Reach out today for a free consultation with the Lumen team.

866-352-0291 I lumen.com I info@lumen.com