WHITE PAPER

The technical case for the Lumen® Validated Design for Cyber Resilience with Commvault

Validated using Lumen as the operational environment

July 2026

LUMEN®

Table of contents

Executive summary 3
Introduction 4
Customer profile 5
Business challenges 6
Design overview 8
Architecture and design 11
Deployment strategy and validation 14
Results and metrics 17
Lessons learned 18
Outcomes and recommendations 19
Why Lumen? 21
Appendix 22

Executive summary

Cyber resilience is no longer achieved through backups alone. As ransomware attacks and data integrity risks increase across hybrid and multi-cloud environments, enterprises require an integrated approach that protects data in motion, secures data at rest, and enables fast, confident recovery.

The **Lumen Validated Design for Cyber Resilience with Commvault** delivers a proven architectural blueprint that integrates secure, high-performance network connectivity with policy-driven backup and recovery workflows. This design reflects the architectural principles behind the Lumen Cyber Resiliency Solution and demonstrates how resilient networking and advanced recovery orchestration work together to reduce risk and operational complexity.

This validated design was proven in Lumen's own operational environment using Commvault Cloud software and recovery workflows for real-world validation. Results included approximately 90% consolidation of legacy backup platforms, $3.5 million in annual cost savings and significantly reduced recovery times.

The Commvault capabilities validated in this design are operationalized for customers through Lumen® Data Protect, Lumen's managed data protection service built on Commvault technology.

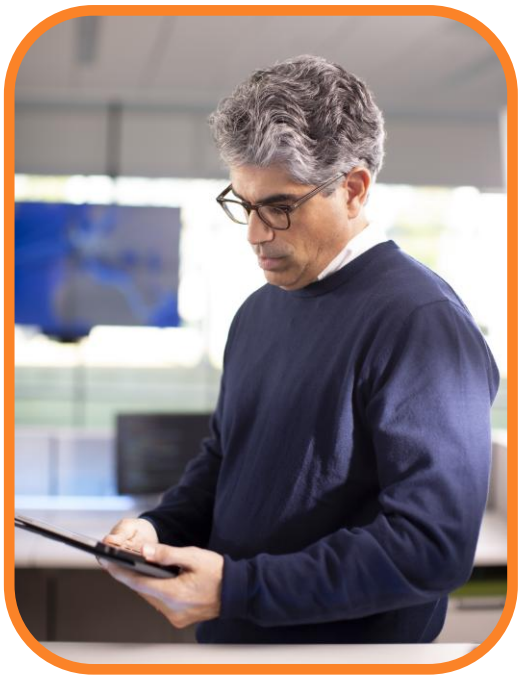
Designed to meet Lumen's stringent operational and regulatory requirements, this Lumen Validated Design for Cyber Resilience demonstrates measurable results in resilience, scalability and enterprise-grade recovery assurance across edge, core and multi-cloud environments. Key components of the design include:

- **Zero-trust enforcement**: Provides continuous verification and validation of all access.
- **Air-gapped storage**: Isolated backup copies for protection against tampering and deletion.
- **Anomaly detection**: Identifies unusual patterns that may indicate a security breach.

This white paper presents an overview of the design, deployment and validation of a Lumen Validated Design for Cyber Resilience with Commvault in a production environment. It represents one possible design configuration within the broader Lumen Cyber Resilience solution, which may be implemented using different combinations of components depending on customer requirements. This document provides practical guidance for enterprise architects, security leaders and infrastructure teams seeking to design and implement their cyber-resilient data protection strategies.

Introduction

Organizations today face escalating cyberthreats and regulatory demands that challenge traditional approaches to data protection, cyber resilience, and recovery. As attack surfaces expand across hybrid environments, maintaining service continuity and compliance has become increasingly complex.



For companies like Lumen that operate across hybrid environments and provide critical services to essential industries, a single incident can result in significant financial, reputational and legal consequences.

The Lumen Validated Design for Cyber Resilience, created in partnership with Commvault, addresses this need by delivering a validated architectural blueprint for cyber-resilient data protection. The design demonstrates how secure, high-performance networking and policy-driven recovery workflows can be combined to reduce operational risk and improve recovery outcomes across hybrid environments. It was first deployed within Lumen's own infrastructure, enabling real-world validation prior to external adoption.

Purpose and scope

This white paper details the design, deployment and validation of the Lumen Validated Design for Cyber Resilience with Commvault, proven in hybrid environments operated by Lumen. This document is intended to offer practical guidance for enterprise architects, security leaders and infrastructure teams in strengthening cyber-resilient data protection strategies.

Key topics include:

- Business and technical drivers influencing the architecture
- Core design principles such as zero-trust enforcement, air-gapped storage and anomaly detection
- Deployment strategy across hybrid environments
- Governance and observability features such as centralized reporting, alerting and policy management
- Protection of SaaS workloads including Microsoft 365, Salesforce and Active Directory
- Operational outcomes including business continuity, reduced downtime, cost efficiencies and improved time to recover service levels
- Lessons learned from consolidating legacy backup tools into unified platforms
- Recommendations for scaling and adapting this validated design across diverse enterprise environments

Results may vary depending on organizational context, infrastructure maturity and implementation approach.

Customer profile

Target audience

This white paper is intended for technical and strategic stakeholders involved in cyber resiliency planning and implementation. Primary audiences include infrastructure architects, backup and recovery administrators, SOC teams and cloud platform owners. Other audiences may include senior leaders responsible for data protection, risk management and compliance.

Industry vertical and size

This Lumen Validated Design for Cyber Resilience was proven in Lumen's own production environment, providing a strong foundation for use across industries with similar operational, scale, and regulatory requirements. Across sectors, the design supports continuous availability, rapid restoration, reduced downtime and protection of data integrity and reputation, especially in environments with regulatory and operational complexity.

Industries and segments that may benefit include:



Energy/Utilities – Support continuous grid, plant and pipeline availability; protect and centrally manage backups from non-virtualized SCADA and substation systems without infrastructure upgrades. Provide ransomware-resilient recovery following data breaches, cyberattacks or weather incidents.



Media & Entertainment (M&E) – Index, protect and tier massive unstructured media libraries—spanning NAS, object and archive—while supporting granular file recovery across hybrid storage.



Manufacturing/Logistics/Transportation – Securely and efficiently back up and restore distributed edge systems in factories, warehouses, vehicles or terminals using lightweight agents with bandwidth-optimized policies.



Healthcare/Life Sciences/Pharma - Provide audit-ready backup workflows for clinical, research and lab systems. Help maintain access to patient data and research environments during outages or rollback scenarios and help reduce downtime and loss of essential clinical systems and patient data.



Financial Services – Support secure backup of sensitive customer and transaction data in regulated environments. Minimize exposure to data loss and support continuity of financial operations under threat conditions.



Retail and Hospitality - Securely and efficiently back up and restore distributed edge systems in head office and branch locations using lightweight agents with bandwidth-optimized policies.



Telecom/Technology – Scalable, efficient backup across network and business locations. Maintain service continuity and data integrity across geographically dispersed infrastructure.

Existing IT/OT environment

Lumen operates a complex, hybrid infrastructure that spans traditional IT systems and OT environments, making it a representative proving ground for large-scale cyber-resilient architectures. The environment reflects the operational realities of a large-scale enterprise navigating digital transformation, regulatory compliance and evolving cyberthreats. It includes:

- Distributed data centers and cloud integration for backup and recovery
- Edge and core systems
- Centralized control and policy enforcement
- Secure, segmented networks for data protection

This infrastructure is designed to support high availability, rapid recovery and scalable protection across diverse workloads and geographies.

Regulatory and compliance requirements

Organizations operating in hybrid environments are subject to a growing set of compliance frameworks that define required controls for data protection, access management and recovery assurance. The Validated Design described in this white paper incorporates capabilities that meet the standards of the following mandates:

CMMC (Cybersecurity Maturity Model Certification)

Addresses the protection of Controlled Unclassified Information (CUI) in defense industrial base systems. Requires implementation of specific cybersecurity practices and maturity levels to meet Department of Defense expectations. (https://dodcio.defense.gov/CMMC/Resources-Documentation/)

SOX (Sarbanes-Oxley Act)

Mandates accurate financial reporting and enforceable data retention policies. Requires secure, auditable backup systems to support compliance with financial governance standards. (https://www.sec.gov/spotlight/sarbanes-oxley.htm)

FIPS (Federal Information Processing Standards)

Applies to systems handling sensitive but unclassified federal data. Requires use of validated cryptographic modules and secure data handling practices to meet federal cybersecurity standards. (https://csrc.nist.gov/publications/fips)

Business challenges

Industry trends/drivers

Cyber resilience is a strategic priority across industries. As digital transformation accelerates and regulatory scrutiny intensifies, organizations face a convergence of threats and expanding threat surfaces. This reality requires orchestrated, validated recovery strategies that can withstand modern adversaries and operational complexity.

Ransomware: precision-engineered disruption

Ransomware has evolved from blunt-force disruption into a calculated, scalable business model for criminals. In Q1 2025, ransomware attacks surged 126% YoY to an average of 275 incidents per day.[1] Attackers have exfiltrated more than 238 terabytes of sensitive data, a 92.7% increase that reflects a substantial growth of public extortion tactics.[2] The average cost of a data breach is nearly $4.5 million.[3] AI-driven threats and commoditized Ransomware-as-a-Service (RaaS) kits have exacerbated the threat by lowering the barrier to entry and enabling low-skilled actors to launch sophisticated campaigns for as little as $40.[4]

Trends exacerbating the ransomware threat

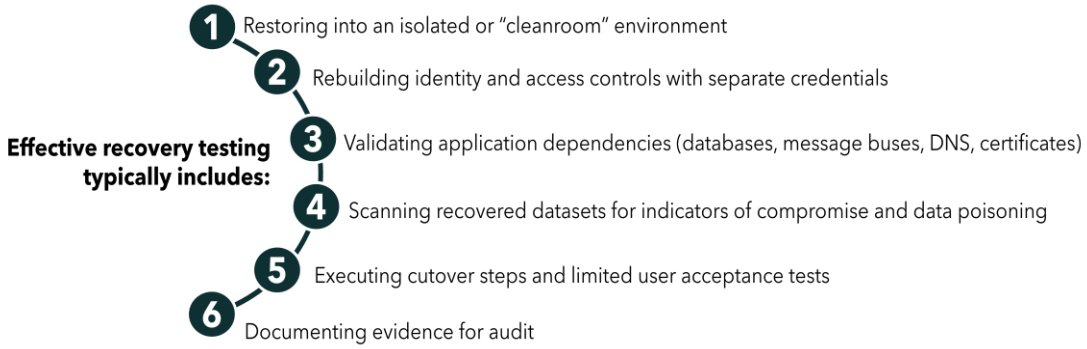
- Commoditization via cheap, simple-to-use RaaS kits
- Public extortion using leak sites
- AI makes threats easier to create and harder to identify

The threat landscape is faster, smarter and more adaptive than traditional defenses were designed to handle.

Data loss and recovery failures

Although data backups are still important defensive tools, they aren't infallible safety nets. Recent studies show nearly one-third of ransomware victims suffered permanent data loss.[5] Recovery rates have dropped from 87.4% in 2021 to 66.3% in 2024, as attackers increasingly target backup infrastructure.[6] In 76% of incidents, adversaries compromised backup repositories before launching their main payload.[7]

These failures expose deeper architectural flaws, especially those lacking segmentation and immutability. Routine backup testing is not enough. Organizations must validate full recovery under adversarial conditions to ensure operational readiness.



Rising demand for AI workloads

Artificial intelligence (AI) is reshaping industries at speed and expanding rapidly across cloud, edge and hybrid environments, driving unprecedented demand for secure, resilient data infrastructure. Model accuracy and business outcomes depend on clean, trustworthy data. Attacks like data poisoning and AI-powered threats can undermine and erode trust.

Secure and resilient AI workloads require:

- Tamper-proof data pipelines with cryptographic validation and immutable storage to help protect data integrity
- Recovery-ready architecture that can restore raw data, model weights, training environments and inference pipelines
- Privacy-first design to meet evolving regulations like GDPR, HIPAA and emerging AI governance frameworks
- Defense against AI-powered threats, including polymorphic malware, deep fake-driven social engineering and automated phishing campaigns

Cloud migration and data sprawl

Hybrid and multi-cloud adoption has introduced fragmentation and risk at scale. According to IDC, 88% of cloud buyers are deploying a hybrid cloud or are in the process of operating one, and 79% are already using multiple cloud providers.[8] Data now resides across various platforms and environments, creating blind spots attackers can exploit and complicating recovery.

Building resilience requires architectural consistency across unified observability, immutable storage tiers, automated failover orchestration and policy-driven data lifecycle management. Recovery plans must be cloud-native in design and address region-wide outages, identity compromise and API abuse.

Compliance pressure and regulatory mandates

Regulatory frameworks such as HIPAA, NIST 800-171, GDPR, and NYDFS 23 NYCRR 500 now require demonstrable recovery capabilities and mature resilience practices. Cyber insurance providers are raising standards, assessing disaster recovery readiness and resilience maturity as prerequisites for coverage.

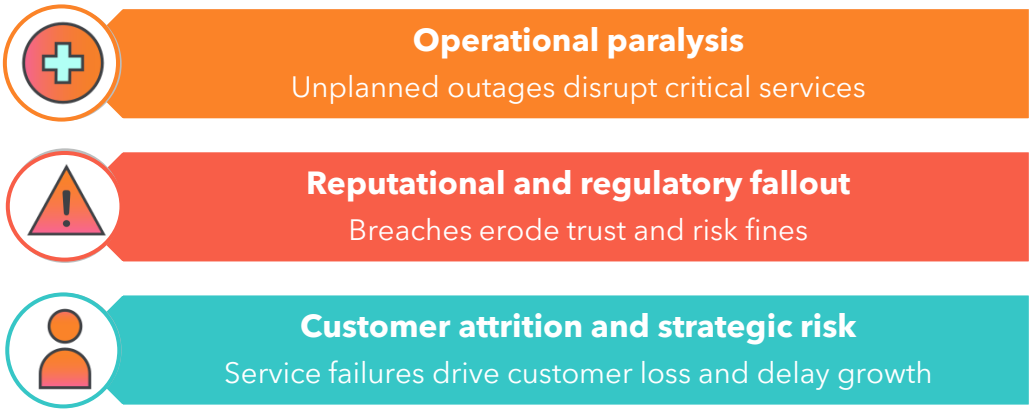
Talent shortages and automation imperatives

The cybersecurity talent gap continues to widen, with more than three million unfilled roles globally.[9] This shortage is driving investment in automation, including automated recovery workflows, playbook-driven incident response and AI-assisted threat detection. Automation enables organizations to reduce mean time to recover, continuously validate recovery readiness and maintain business continuity despite resource constraints.

In a distributed ecosystem, the ability to restore data quickly and coherently is both a technical requirement and a business-critical imperative.

Consequences of inaction

When organizations lack the ability to recover quickly and securely, the impact ripples across operations, revenue, customer trust and regulatory standing. Consequences can include:



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 demonstrates how Commvault's enterprise-grade data protection capabilities, operating over Lumen's secure high-performance network infrastructure can be combined to deliver scalable, secure and automated recovery outcomes.

Validated design principles

This Validated Design applies a defense-in-depth approach to cyber-resilient data protection. It emphasizes rapid, clean recovery across hybrid environments and includes:

- Immutable, air-gapped backups
- Unified platform for on-prem and cloud workloads

- Comprehensive analytics and anomaly detection
- Scalable architecture with 10PB design capacity

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 following components were deployed and integrated as part of the validated architecture within Lumen's hybrid infrastructure. Where applicable, components listed reflect validated use, while others represent supported architectural options within the overall design.

- Commvault Cloud SaaS - provides cloud-delivered backup and recovery for SaaS workloads and cloud environments. These capabilities are delivered to customers through Lumen® Data Protect (LDP).
- Commvault Cloud Software – deployed on-premises to manage backup and recovery for local and hybrid workloads
- Air Gap Protect (AGP) – implemented in Azure, AWS, and GCP, 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, powered by NetApp – supports local primary and remote secondary backup tiers and includes a third air-gapped copy

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 secure tenancies: 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 capabilities leveraged in this design:

- Commvault Cloud Backup and Recovery and Risk Analysis, validated at 10PB in Lumen's environment
- HyperScale X Reference Architecture Software for Hewlett Packard Enterprise (HPE) appliances
- 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 the 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

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® Network Storage

Lumen® Network Storage, powered by NetApp, is supported within the Lumen Cyber Resilience solution as a flexible storage layer that can serve multiple roles depending on customer architecture. At the solution level, it may be used for secure primary storage with capabilities such as anomaly detection and automated immutable snapshot creation to help protect against corruption and unauthorized data modification.

Within this validated design, Lumen Network Storage is used as a secondary storage tier for immutable, air-gapped backup copies to support recovery assurance. The validated architecture is designed to accommodate multiple storage implementations while maintaining consistent recovery behavior.

Lumen products and services included in this design:

- IP VPN
- Wavelength
- Ethernet
- Cloud Connect with IP VPN On-Demand
- Lumen® Network Storage

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 cyber-resilient recovery 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

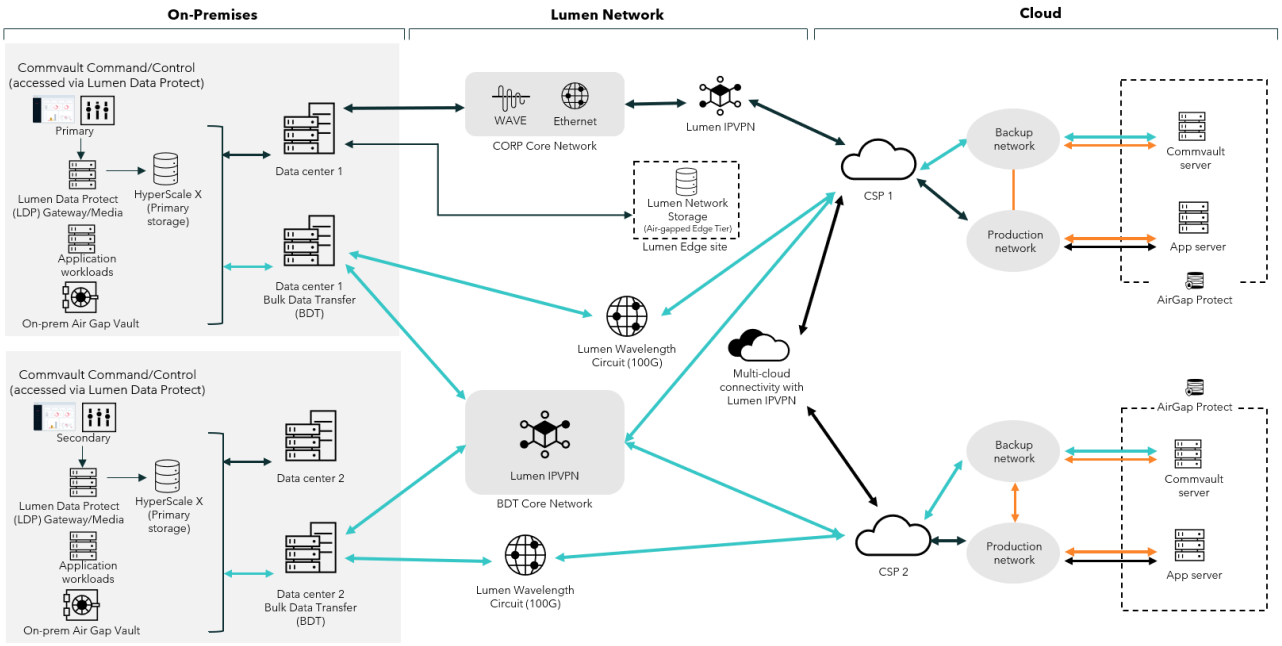
The logical architecture defines how core components interact to enforce policy, isolate trust zones, and orchestrate data movement across cloud and on-premises environments. It enables streamlined cleanroom recovery, anomaly detection, and automated workflows. The following diagram illustrates these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

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-prem and in cloud zones. These vaults are logically isolated and support immutable storage.

Figure 1

Logical architecture of the validated design



◀▶ : ability to backup and restore **Black:** Corporate core network **Teal:** Bulk data core network **Orange:** Cloud network

- Replication pathways:
  - On-prem to cloud replication: Backup data can be replicated from on-prem vaults to cloud vaults using Lumen Wavelength, 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.
- Lumen® Network Storage: Supported architectural option for a third copy of backup data, including air-gapped configurations, complementing primary and secondary backup tiers.

Network components



- Lumen IP VPN (ASN 3549): Provides private transport for backup and recovery traffic across hybrid environments.
- Lumen Wavelength 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 Wavelength 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.

Deployment strategy and validation

Deployment strategy

Deployment followed a phased, infrastructure-aware rollout designed to minimize disruption, accelerate onboarding and provide consistent protection across hybrid environments. The strategy emphasized modular integration, transport optimization and security-first architecture.

Infrastructure alignment

- On-premises deployment: Commvault C2 nodes, media agents and vaulting infrastructure were deployed across six primary data centers. These sites were equipped with HyperScale X appliances to support primary and secondary backup tiers, with Lumen® Network Storage for additional backup copies, including air-gapped configurations.
- Cloud deployment: Commvault Air Gap Protect (AGP) tenants were provisioned in multiple CSPs. Each tenant was configured with 3-2-1 architecture to help provide redundancy and immutability.

Network and transport integration

- Bulk Data Transfer (BDT): High-throughput backup traffic was routed over dedicated Lumen Wavelength circuits between data centers and cloud vaults. This BDT core network was isolated from corporate traffic to help performance and security.
- Lumen IP VPN backbone: All backup and replication traffic was encrypted and routed via Lumen IP VPN (ASN 3549) to help enable secure, multicloud connectivity and consistent transport behavior across CSPs.

Security and access controls

- Authentication enforcement: Commvault Air Gap Protect (AGP) required authentication for every read/write operation to help prevent unauthorized access and provide zero-trust compliance.
- Logical Air Gapping: Immutable vaults were deployed with separate authentication domains and no direct access from production networks, enabling isolation and integrity.

Operational coordination

- Commvault SaaS orchestration: Deployment and policy management were coordinated via Commvault's SaaS platform, which resides in the cloud and interfaces with Media Agents across all environments. While deployment and validation were performed using native Commvault Cloud SaaS, the same product and capabilities are available to customers through Lumen® Data Protect for organizations preferring a managed procurement and support model.
- Standardized retention policies: Backup retention was standardized across all environments to help simplify governance and help maintain consistent recovery point objectives.

Validation

Validation of the deployment was conducted across eight key dimensions to check that the solution met enterprise-grade standards for reliability, scalability and operational excellence.

Functional validation

- Infrastructure setup: Two virtual CommServe instances (primary and DR) were configured with LiveSync replication to support high availability and disaster recovery.
- Client deployment: Silent push installations were initiated for approximately 20,000 hosts.
- Proof of Concept (POC) execution: A proof-of-concept test was conducted with ~20 different client types to validate compatibility and operational readiness.
- SQL cluster configuration: Automatic discovery and configuration of SQL clusters were validated as part of operational checks, confirming reliable support for clustered environments.
- Knowledge transfer and task testing: All major tasks were tested and verified, with knowledge transfer sessions conducted to secure operational continuity.

Performance and scalability

- Node deployment: 72 HPE HSX nodes were successfully configured across six geographically distributed sites.
- Stream optimization: Stream limits were adjusted dynamically (from 1,500 to 1,800) to accommodate job volume, demonstrating elastic scalability.
- CommServe optimization: SQL memory allocation was increased to improve LiveSync job performance.

- Tomcat heap tuning: Memory allocation was increased to maintain User Interface (UI) responsiveness.
- Deduplication Accelerated Streaming Hash (DASH) copy reliability: DASH copy operations were validated for performance and reliability, with configuration tuning applied to maximize throughput and service stability.

Resilience and high availability



- Network bonding issues: Misconfigured Link Aggregation Control Protocol (LACP) bonding on Cisco Nexus switches was corrected to restore expected throughput.
- Node configuration failures: Installation issues caused by conflicting network bonds were resolved through targeted configuration changes and reboot procedures.
- Disaster Recovery (DR) execution: CommServe DR backups were performed, followed by service suspension and cumulative updates to validate recovery protocols.

Security and compliance

- Credential management: SQL cluster credential required customization to maintain reliability.
- Certificate handling: Certificate import was required for NetApp StorageGrid integration, highlighting compliance with secure storage protocols.

Manageability and monitoring

- CommCell console performance: Socket/core allocations were increased in line with environment growth to maintain UI performance.
- Anomaly reporting: Custom reports were built to focus on monitoring indicators.
- Alerting and Service Level Agreements (SLA) tracking: Alerts were configured for failed jobs and SLA compliance was reviewed and adjusted where necessary.

Interoperability and compatibility

- Multi-platform support: Customizations were deployed to provide wide supportability across Windows, Linux, Solaris, HP-UX and Oracle RAC environments.
- Legacy system integration: Specialized feature flags were deployed to support integration with older systems.

Deployment repeatability

- Standardized procedures: Silent install scripts and plan association reports were used to streamline deployment across thousands of hosts.

Workload simulation

- POC testing: Simulated workloads across ~20 client types validated system behavior under varied conditions.
- Backup load testing: Synthetic full backups and LiveSync jobs were monitored and optimized to simulate production-scale operations.

- Restore scenarios: Multiple restore tests—including SQL, guest file, VM—were executed to validate recovery under stress.

Results and metrics

The deployment of the Lumen Validated Design for Cyber Resiliency with Commvault has delivered measurable improvements in operational efficiency, cost savings and cyber resilience across Lumen's hybrid infrastructure. Examples include:

Tool consolidation, operational streamlining and efficiency gains

- Achieved approximately 90% consolidation of legacy backup platforms, reducing complexity and streamlining operations across hybrid environments.
- Centralized policy enforcement and orchestration across all backup domains, supported by unified control plane and automation features from Commvault.
- Edge-optimized infrastructure and high-throughput connectivity, provided by Lumen, to help eliminate data center bottlenecks and accelerate backup and recovery across remote sites.

Staffing and coverage efficiency

- Reduced administrative overhead by consolidating backup operations into a single control plane.
- Automation and elastic scaling expanded coverage to CSPs without increasing staff by utilizing managed services and consumption-based delivery models from Lumen and Commvault.

Financial impact

- Achieved approximately $3.5 million in annual savings through reduced licensing, infrastructure and operational costs.
- Consumption-based service models from Lumen and Commvault contributed to predictable budgeting.

Downtime and recovery improvements

- Reduced recovery time objectives (RTO) through features like Commvault IntelliSnap®, Live Mount and Direct-to-Cloud Recovery.
- High-speed Lumen IP VPN and dedicated Wavelength circuits supported rapid data movement and multi-cloud integration.

Ransomware protection enhancements

Using Commvault's security features, cyber resilience improved with immutable and indelible storage, logical air-gapping across hybrid environments, honeypot detection and cleanroom recovery, Security Information and Event Management (SIEM)/ Security Orchestration, Automation, and Response (SOAR) integration for real-time alerting and forensic analysis.

- The secure Lumen network backbone and strategic technology partnership with Commvault supports advanced protection and rapid recovery from ransomware threats.

From operational and staffing efficiencies to financial savings, downtime and recovery improvements, to ransomware protection, the Lumen Validated Design for Cyber Resiliency with Commvault has delivered measurable benefits.

Lessons learned

Through deployment of this Commvault-based Lumen Validated Design, Lumen documented several keys to success, challenges and mitigation strategies.

Key success factors

From this Validated Design, Lumen has determined the following keys to success:

- **Immutable storage and cleanroom recovery**: These features were central to achieving cyber resiliency goals. They performed reliably under simulated compromise scenarios and enabled secure recovery workflows.
- **Policy-driven Automation:** Commvault's workload discovery and policy orchestration helped streamline protection across diverse environments. This reduced manual effort and improved consistency.
- **Infrastructure stability:** The Lumen platform provided a dependable foundation for distributed deployment, with consistent high performance, throughput and availability across edge and core locations.

Challenges and mitigation strategies

The major challenges and subsequent solutions included:

Hybrid environment complexity

- Challenge: Managing distributed workloads across on-premises and cloud environments introduced configuration variability and operational overhead.
- Mitigation:
  - Commvault's unified platform simplifies hybrid data protection by consolidating backup and recovery operations across environments.
  - Lumen hybrid cloud infrastructure supports seamless workload mobility and secure data exchange, reducing the need for custom integrations.

Visibility and monitoring

- Challenge: Achieving unified observability across diverse infrastructure layers can be difficult, especially in multi-cloud and edge deployments.
- Mitigation:
  - Commvault's reporting capabilities and APIs were utilized to tie into the configuration management database used by Lumen for self-service visibility and metrics, as well as enhancing management capabilities and executive readout with dashboards.
  - Lumen infrastructure supports centralized logging and telemetry aggregation, enabling consistent monitoring across edge and core systems.

Security and resilience across platforms

- Challenge: Ensuring consistent security controls and rapid recovery across cloud and on-premises components requires specialized tooling.
- Mitigation:
  - Commvault's Auto Recovery and cloud portfolio delivered multi-layered protection and automated recovery workflows across hybrid environments.
  - Lumen's secure network backbone and edge compute capabilities reinforced data sovereignty, regulatory alignment, and recovery isolation, which is particularly relevant in highly regulated industries.

Outcomes and recommendations

Summary of outcomes

The deployment of the Lumen Validated Design for Cyber Resilience with Commvault has delivered measurable improvements across operational resilience, recovery and cost efficiency. These outcomes validate the design's ability to meet enterprise-grade requirements across hybrid environments.

Beyond technical success, the implementation reinforced strategic alignment between infrastructure and security teams, accelerated modernization of legacy backup workflows and established a replicable model for cyber-resilient architecture.

For organizations navigating complex regulatory landscapes and rising threat vectors, this design offers a proven foundation for scalable, policy-driven data protection.

Recommendations

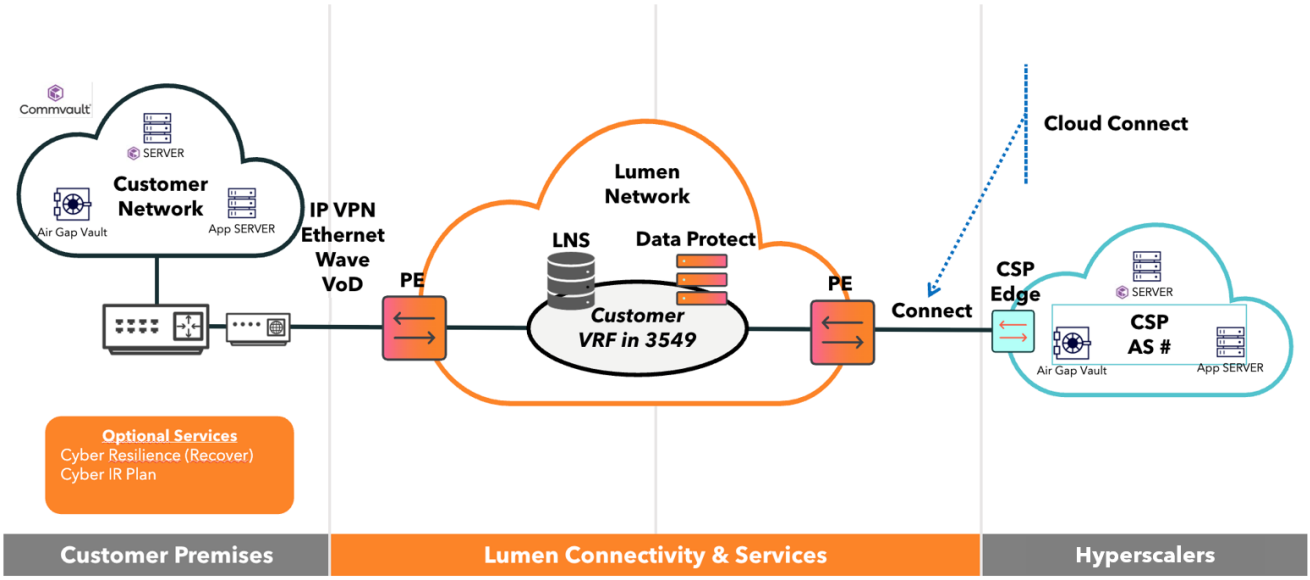
The Lumen Validated Design described in this white paper can be adapted to suit a range of infrastructure profiles using the following best practice configurations:

Private-premise customers

- Use Lumen IP VPN, Ethernet, Wave and VoD/Ethernet Fabric Connect for secure transport.
- Deploy Commvault HyperScale X and Air Gap Vaults on-premises.
- Extend protection to cloud via Cloud Connect (e.g., AWS Direct Connect, Azure ExpressRoute, and Google Cloud Interconnect).

Figure 2

Suggested architecture for private premise

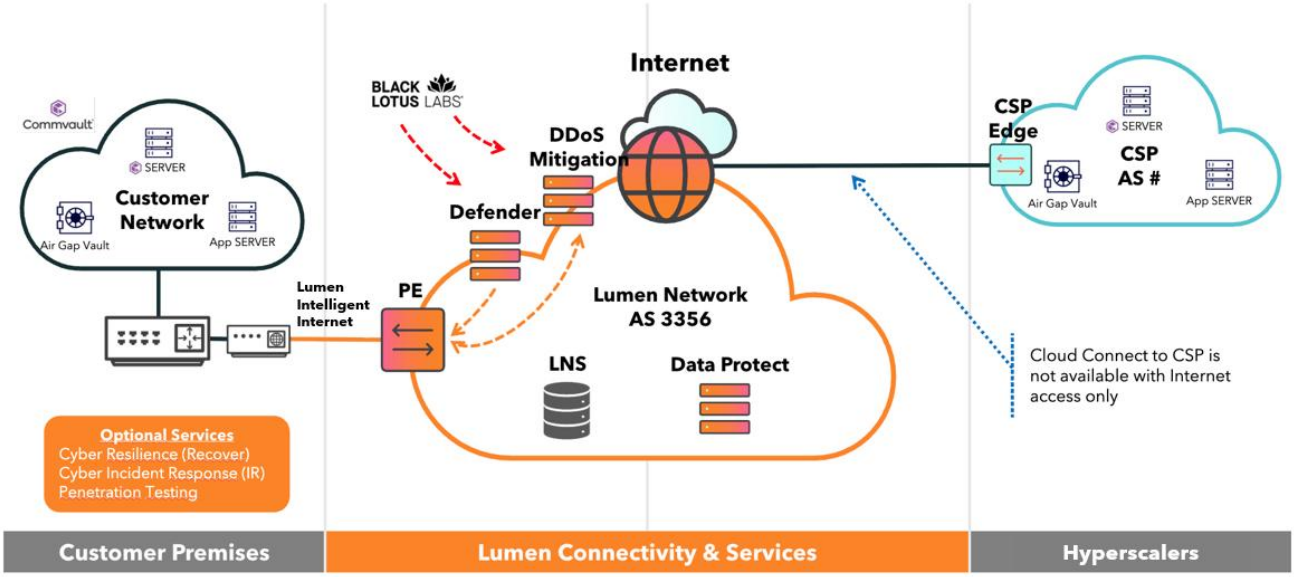


Public cloud-centric customers

- Use Lumen® Intelligent Internet for access and Defender/DDoS Essentials for edge protection.
- Deploy Commvault AGP in CSP environments for immutable cloud backups.
- Leverage Lumen® Network Storage (LNS) and Lumen® Data Protect for secure, air-gapped cloud backup and recovery.

Figure 3

Suggested architecture for the public cloud scenario

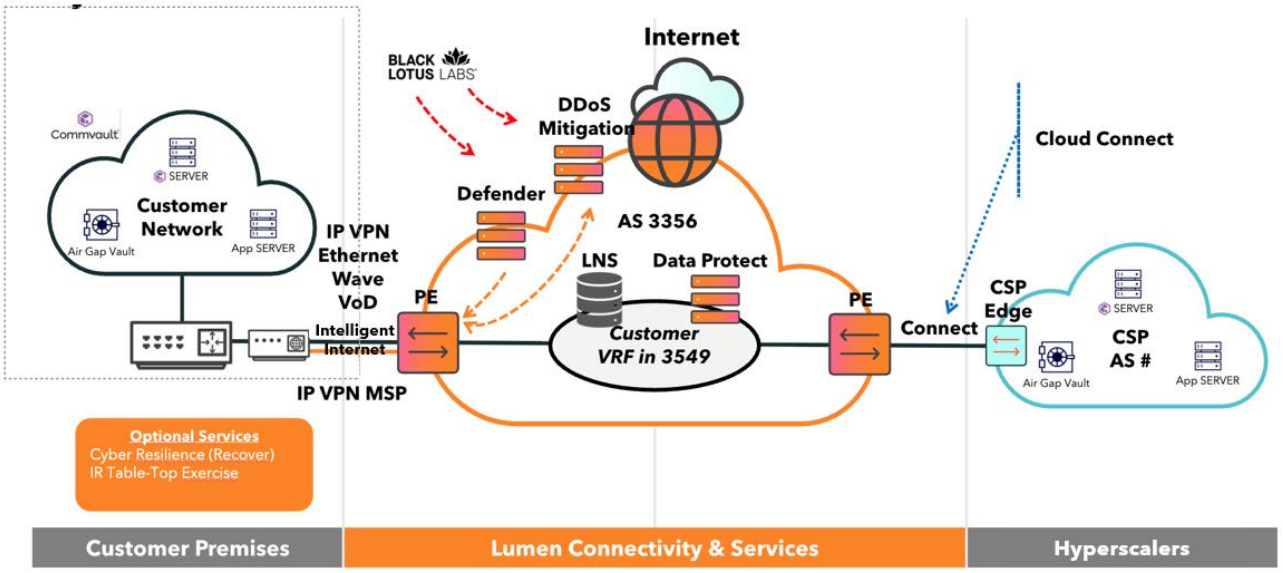


Hybrid customers

- Use Lumen® IP VPN MSP, Ethernet and Cloud Connect for multi-cloud integration.
- Deploy Commvault AGP in cloud zones and HyperScale X on-premises.
- Add optional services like Lumen® Professional Security Services Penetration Testing, and next-gen Web Application Firewall.

Figure 4

Suggested architecture for the hybrid-both scenario



Fully managed customers

For organizations seeking a fully managed experience, Lumen offers a suite of managed services that complement this validated design. These services provide end-to-end operational support, including deployment, monitoring, patching and lifecycle management of the backup and recovery environment.

Customers who want to implement this Validated Design in their environment can choose Lumen® Data Protect (LDP) as a managed model to access Commvault Cloud capabilities through Lumen. Lumen® Data Protect is Lumen's branded SaaS offering, powered by Commvault Cloud, and delivers the same robust features and security controls as native Commvault SaaS. Lumen Data Protect is ideal for organizations seeking simplified operations, unified billing and seamless integration with Lumen's secure network infrastructure.

Why Lumen?

Trusted partner in digital transformation

Lumen is architecting the future of enterprise connectivity and resilience. The company's mission to "ignite business growth by connecting people, data, and apps quickly, securely and effortlessly" is reflected in every aspect of the Lumen Validated Design for Cyber Resilience. This architectural approach simplifies adoption, accelerates time-to-value and delivers repeatable outcomes for organizations navigating transformation.

The validated design documented in this white paper was first deployed internally. It led to the consolidation of more than 90% of legacy backup systems into unified platforms, reduced operational overhead and provided cost savings. This internal-first approach shows that what is offered to customers is proven, resilient and optimized for scale.

Proven network and security infrastructure

Lumen's infrastructure is engineered for performance, resilience and scale. With ~340,000 global route miles of fiber, the network is built to support the demands of AI, hybrid cloud and edge computing. Services like IP VPN and Wavelengths form the backbone of this Lumen Validated Design for Cyber Resilience, enabling secure, high-performance connectivity across distributed environments.

Security is foundational to Lumen's architecture. Central to this security posture is Black Lotus Labs®, Lumen's proprietary threat intelligence team and 2024 winner of the Cybersecurity Breakthrough Award for Threat Intelligence Company of the Year. Operating across one of the world's most peered global networks, Black Lotus Labs identifies and disrupts threat actor techniques by analyzing traffic across Lumen's backbone, often detecting threats up to seven days before competitors. Their research is shared with the broader security community, including leadership roles in the Joint Cyber Defense Collaborative (JCDC), and has led to the takedown of nation-state malware networks in partnership with U.S. federal law enforcement.

Black Lotus Labs' visibility and proactive defense posture make Lumen's infrastructure secure, predictive and capable of adapting to evolving threats while protecting customers at scale.

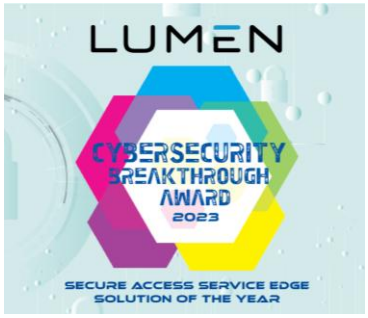
Co-validated with Commvault for repeatable outcomes

This Lumen Validated Design for Cyber Resilience with Commvault is the result of a deep technical collaboration between both organizations. This partnership integrates Commvault's enterprise-grade backup and recovery platform with Lumen's infrastructure to deliver a unified, policy-driven framework for cyber-resilient data protection. The co-validation demonstrates that the architecture and recovery workflows are robust and replicable, ready to be deployed with confidence and speed across enterprise environments.

The solution is designed to support AI workloads from training to inference, with tamper-resilient data pipelines and cleanroom recovery environments. As AI adoption accelerates, Lumen's infrastructure is positioned to be the trusted backbone of the AI economy—delivering the connectivity, security and scalability that modern enterprises require.

Lumen has won three straight Cybersecurity Breakthrough Awards, including the 2024 Threat Intelligence Company of the Year for Black Lotus Labs.







Appendix

How this Validated Design is used

This Lumen Validated Design serves as a technical reference architecture demonstrating how cyber resilient recovery workflows can be designed, implemented, and validated using Commvault as the recovery orchestration platform within the broader Lumen Cyber Resilience solution.
The design represents one possible configuration of the Lumen Cyber Resilience solution, focusing specifically on validated backup, recovery, and cleanroom workflows. The broader solution supports additional components and deployment models that may be incorporated based on specific requirements, infrastructure profiles, and operational objectives.

The principles and validated recovery patterns described in this document reflect implementation and validation within Lumen's hybrid environment and may be used as a reference when evaluating cyber-resilient data protection architectures.

Bill of materials

Note: The components listed below represent the technologies and services that support or complement the validated architecture described in this white paper. Availability and procurement options reflect current commercial offerings and may include managed delivery models in addition to the configurations validated in Lumen's operational environment.

Component	How to Buy
IP VPN	https://www.lumen.com/en-us/networking/ipvpn-on-demand.html
Wavelength	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
Lumen® Network Storage	https://www.lumen.com/en-us/services/lumen-network-storage.htm
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 Terabyte CVLT 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

Footnotes

[1]Firch, Jason, *The Average Cost of Ransomware Attacks*, May 2025. https://purplesec.us/learn/average-cost-of-ransomware-attacks/
[2] Stone-Gross, Brett. Bates, Heather. Dodia, Rajdeepsinh. Barajas, Yesenia. *Ransomware Surges, Extortion Escalates: ThreatLabz 2025 Ransomware Report*. July 2025. https://www.zscaler.com/blogs/security-research/ransomware-surges-extortion-escalates-threatlabz-2025-ransomware-report
[3]Ponemon Institute and IBM, *Cost of a Data Breach Report 2024*, 2024. https://www.ibm.com/reports/data-breach
[4]World Economic Forum, 3 Trends set to drive cyberattacks and ransomware in 2024, February 2024. https://www.weforum.org/stories/2024/02/3-trends-ransomware-2024/
[5]Hornetsecurity, *Ransomware survey reveals nearly a third of businesses suffered data loss in 2024,* October 2024. https://www.hornetsecurity.com/us/blog/nearly-a-third-of-businesses-suffered-data-loss-in-2024
[6] Hornetsecurity, Ransomware survey reveals nearly a third of businesses suffered data loss in 2024, Oct 15, 2024 https://www.hornetsecurity.com/us/blog/nearly-a-third-of-businesses-suffered-data-loss-in-2024
[7]Hashedout, *20 Ransomware Statistics You're Powerless to Resist Reading*, October 2024. https://www.thesslstore.com/blog/ransomware-statistics
[8]IDC, *Ten Trends That Shaped the Cloud Market in 2024*, February 2025. https://blogs.idc.com/2025/02/05/ten-trends-that-shaped-the-cloud-market-in-2024/
[9]World Economic Forum, *3 trends set to drive cyberattacks and ransomware in 2024*, February 2024. https://www.weforum.org/stories/2024/02/3-trends-ransomware-2024/

This content is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen products and offerings as of the date of issue.

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

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice. ©2026 Lumen Technologies. All Rights Reserved.

LUMEN®