Commvault kyndryl Everpure

SOLUTION BRIEF

The Resilience Imperative: Beyond Compliance

An innovative partnership with Kyndryl and Everpure to help enterprises simplify compliance and minimize the risk of regulatory fines.

OVERVIEW

As nations worldwide adopt and enforce cyber regulations, businesses across all industries must adapt their security and cyber resilience strategies to incorporate these new compliance requirements and mandates focused on being able to recover from cyberattacks. Smart organizations recognize that proactive compliance with these mandates isn't just about avoiding penalties—it's about transforming regulatory requirements into competitive advantages. Through our strategic partnership with Kyndryl and Everpure, Commvault helps enterprises build the cyber readiness and resilience foundation that powers sustainable growth and continuous business.

THE RISE IN CYBER REGULATIONS

Today, enterprises operate in an increasingly complex digital ecosystem where data flows across multiple clouds, on-premises infrastructure, and edge environments. This distributed landscape creates unprecedented security and resiliency challenges that governments and regulators are trying to address with cyber resilience mandates. These regulations go beyond traditional compliance checkboxes. They hold enterprises and their leadership directly accountable for cybersecurity investments and resilience testing that extend throughout their operations and supply chains. For global organizations, the challenge intensifies as they must navigate multiple regulatory frameworks—each similar yet distinct in their requirements.

THE RESILIENCE IMPERATIVE

#1 CONCERN

of business and IT leaders is **cyberattacks**, followed by **evolving regulations**

55% OF BUSINESS & IT LEADERS

find navigating the **frequency and speed of regulatory challenges** a significant challenge

2 IN 3 CEOS

are concerned their **IT tools or processes are outdated** or close to end-of-life

1 IN 4 BUSINESS & IT LEADERS

have experienced challenges to modernization by **relying on outdated security protocols**, leading to a data breach or cyberattack

Source: Kyndryl Readiness Report, June 2025

GAIN AN EDGE ON EVOLVING REQUIREMENTS

Forward-thinking organizations know that strategic investments in data protection and recovery capabilities deliver benefits far beyond regulatory compliance. By preparing for emerging regulations like DORA, NIS2, APRA CPS 230, and RBI, these companies establish resilient data management foundations that become lasting competitive differentiators and improve their ability to recover following inevitable cyberattacks.

The cost of delay is significant. Organizations that don't invest in a cyber resilience strategy now risk falling behind competitors, possibly losing revenue and reputation due to downtime following a cyberattack, breach, or operational issue, in addition to possible fines for non-compliance with regulations.

Our partnership with Kyndryl and Everpure addresses this challenge head-on, helping companies strengthen defenses against cyber threats and enable rapid, clean recovery of mission-critical data. Together, we modernize legacy infrastructure for enhanced performance and security, while strengthening enterprises' capabilities to meet evolving compliance obligations.

COMPLIANCE SOLUTION BENEFITS

Accelerate compliance with legal and industrial regulations

Reduce risk of regulatory fines and penalties

Lessen burden on ITOps and SecOps

Minimize exposure and risk of data loss after breach

Enhance performance and flexibility

DEFINING MINIMUM VIABILTY & STRENGTHENING RESILIENCE

Everpure, Commvault, and Kyndryl unite to help companies maintain continuous business operations before, during, and after cyberattacks or unplanned disruptions. Our combined strengths include Everpure's high-performance secure storage platform, Commvault's industry-leading cyber resilience solutions, and Kyndryl's expert advisory and managed services for mission-critical enterprise technology.

Kyndryl, a leader in cybersecurity services, brings comprehensive cyber resilience strategy and regulatory compliance expertise to help organizations improve their security and cyber readiness. Their experts help clients identify security and resiliency gaps, then determine the minimum viable components that are essential for maintaining business operations during cyberattacks or unplanned disruptions. These insights drive the development and implementation of solutions that support operational resilience and institutionalized compliance measures.

Commvault and Everpure combine for an integrated cyber resilience platform that serves as the foundation for this fully managed service. This platform, architected to align with Zero Trust principles, includes network isolation and immutable, indelible storage capabilities that secure backups and enable confident recovery of clean data at petabyte scale following cyberattacks, data loss, or corruption.

Why Minimum Viability?

A minimum viability strategy defines the essential systems, data, and processes your organization must have operational to continue serving customers and meeting critical obligations during a crisis. This foundational approach focuses recovery efforts on what matters most first, enabling faster restoration while meeting regulatory requirements for operational continuity.

Read more about minimum viability >

To address resilience testing requirements, Commvault and Everpure provide automated, continuous cyber recovery testing that gives you the ability to validate data in a secure, clean recovery zone before restoration to production environments. This includes on-demand testing in cloud-isolated tenants via Commvault® Cloud Cleanroom™ Recovery or within an isolated recovery environment (IRE) on-premises using Commvault® Cloud software and Everpure FlashArray™ or FlashBlade™ systems, enabling rapid, highly efficient recovery of data.

AI-assisted threat detection technology, powered by Commvault Cloud Metallic AI®, continuously scans data to identify anomalies and malware with Commvault quarantining affected data when discovered to prevent reinfection during recovery and allowing for deeper forensic investigation. The integrated Everpure and Commvault solution allows these critical detection and quarantine processes to operate at enterprise scale with the performance and reliability mission-critical operations demand. Aligned with security frameworks like ISO 27001, NIST, and PCI DSS, the Commvault Cloud platform in partnership with Everpure, delivers cyber resilience capabilities by enabling testing and reporting on the status of data protection and recovery.

ESSENTIAL CAPABILITIES FOR REGULATORY SUCCESS

Kyndryl Incident Recovery Services combine with Commvault and Everpure solutions to form a holistic solution that helps clients mitigate risk, avoid the high cost of downtime and regulatory fines, improve cyber resilience, and enable continuous business in the face of cyber threats.

MISSION-CRITICAL DATA RECOVERY

Comprehensive data protection with cloud infrastructure as-a-service, clean point recovery, and the ability to isolate compromised copies, supporting access to critical data when you need it most.

DATA SECURITY

AI-assisted anomaly and threat detection, efficient integration with third-party security tools, and comprehensive data access controls to enhance data security.

SCALABILITY AND PERFORMANCE

Everpure delivers petabyte-scale cyber recovery, enabling rapid restoration of enterprise datasets within critical recovery time windows during ransomware incidents.

SECURE AND ISOLATED RECOVERY

Commvault offers isolated cloud tenants and on-premises recovery environments with immutable air-gapped backups, secure access controls, and pave/repave capabilities for clean data recovery.

AUDIT TRAILS AND REPORTING

Detailed audit trails and reporting capabilities that simplify compliance demonstrations to auditors and regulators while providing visibility into your data protection posture.

MANAGE AND CLASSIFY SENSITIVE DATA

Commvault's data governance tools help organizations manage and classify data so it can be handled according to regulatory requirements. This includes data discovery and classification, metadata management, and access and retention policy enforcement.

SIMPLIFIED COMPLIANCE WORKFLOW

Customizable workflows that can be tailored to specific compliance requirements, aligning data management processes with regulatory standards.

READY TO TRANSFORM COMPLIANCE INTO A COMPETITIVE ADVANTAGE?

In today's regulatory landscape, cyber resilience isn't optional—it's a business imperative that can define your organization's future success. Our partnership provides a proven foundation, recognized industry expertise, and advanced capabilities to not just meet compliance requirements, but turn them into competitive advantages that drive growth and innovation. When compliance is not an overwhelming burden for teams and a robust infrastructure is in place, organizations can focus their resources on initiatives that drive business forward.

THE POWER OF PARTNERSHIP

Together, Everpure, Commvault, and Kyndryl help organizations unlock their data's full potential, drive operational excellence, address compliance obligations, and gain the competitive edge that comes from true cyber resilience. In an era where data protection and regulatory compliance have become business imperatives, our partnership provides the comprehensive solution enterprises need to thrive.

LEARN MORE

DORA Compliance with Confidence Solution Brief

Commvault and Everpure Alliance

Kyndryl's Cyber Resilience Services