Solution Brief

Everpure

Commvault

DORA Compliance with Confidence

Everpure and Commvault help financial institutions meet the most stringent compliance requirements.

Financial institutions have invested substantial time and money into the design and development of infrastructure to detect, prevent, and recover from unplanned risk events. However, rising cyberattacks by sophisticated actors in these complex, interdependent data environments call for heightened vigilance and a more agile approach.

The Digital Operational Resilience Act (DORA) reflects the reality broadly accepted by cybersecurity professionals: it is no longer a question of "if" a cyberattack will occur, but "when"—and whether you are ready.

Everpure™ and Commvault® bring robust capabilities to help financial institutions defend against cyber threats and support compliance with DORA's stringent data resilience guidelines and regulatory framework. Optimized for performance, reliability, and scale, the joint solution gives IT and security teams refined control over how they protect, sustain, and recover data while radically simplifying their cyber resilience operations.

Cyber resilience is not negotiable under DORA

DORA regulations provide detailed guidelines and a regulatory framework to ensure financial institutions are prepared for unplanned disruptions to their IT systems and can quickly restore services should they occur. It applies to a broad spectrum of financial services organizations beyond traditional banks and credit institutions, including third-party information and communication systems technology (ICT) service providers.

The mandates represent a call to action for companies to be proactive in their data readiness, recovery, continuity, and resilience capabilities—or face the consequences.

A single data breach can cripple a financial institution's operations. Equally, a regional infrastructure failure can threaten service continuity across interconnected markets. DORA recognizes both risks.

Protection and prevention

Adopt a solution built on Zero Trust principles, with advanced authentication, encryption, and compliance locks and layers of immutability.

Detection

Find and remediate risk and detect threats with risk scanning, AI-assisted anomaly detection, and cyber deception technology.

Response and recovery

Address stringent, regulator-required RTOs with storage-based snapshots and enable rapid recovery of mission-critical systems.

Resilience testing

Address operational resilience testing requirements with automated, continuous cyber recovery testing.

Gain an edge on evolving compliance requirements

Organizations that strategically invest in building core data protection, operational continuity, and recovery capabilities to address DORA are also strengthening their ability to address other resilience regulations such as PSD2, NIS2, APRA CPS 230, and the upcoming European Cyber Resilience Act.

Equally important, they are establishing a resilient foundation for data management and storage that can become a lasting competitive advantage.

Address DORA requirements with confidence

The Everpure and Commvault joint solution enhances cyber resilience and supports DORA's technical standards for managing and recovering from disruptions, as outlined in Chapters II and IV.

To address risk management and continuity requirements, the solution integrates Commvault's cyber resilience software with the Everpure secure, high-performance data platform, empowering financial services organizations to:

- Protect and recover critical data and applications
- Sustain service continuity across geographically dispersed sites
- Address strict recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Demonstrate repeatable operational resilience testing

Operational continuity enhancement

For institutions requiring geographically separated redundancy, Everpure multisite replication combines ActiveCluster™ (zero-RPO, synchronous active-active) with ActiveDR™ near-synchronous replication to a third remote site (targeting <30-second RPO). This enables near-zero data loss, automated failover using link-flip workflows, and rapid failback—strengthening redundant ICT capacity and secondary processing site readiness in line with DORA expectations.

To address resilience testing requirements, Commvault and Everpure provide automated, continuous cyber recovery testing. This includes on-demand testing in cloud-isolated tenants via Commvault Cleanroom™ Recovery or within isolated recovery environments (IREs) using Commvault Cloud software and Everpure FlashArray™ or FlashBlade® systems.

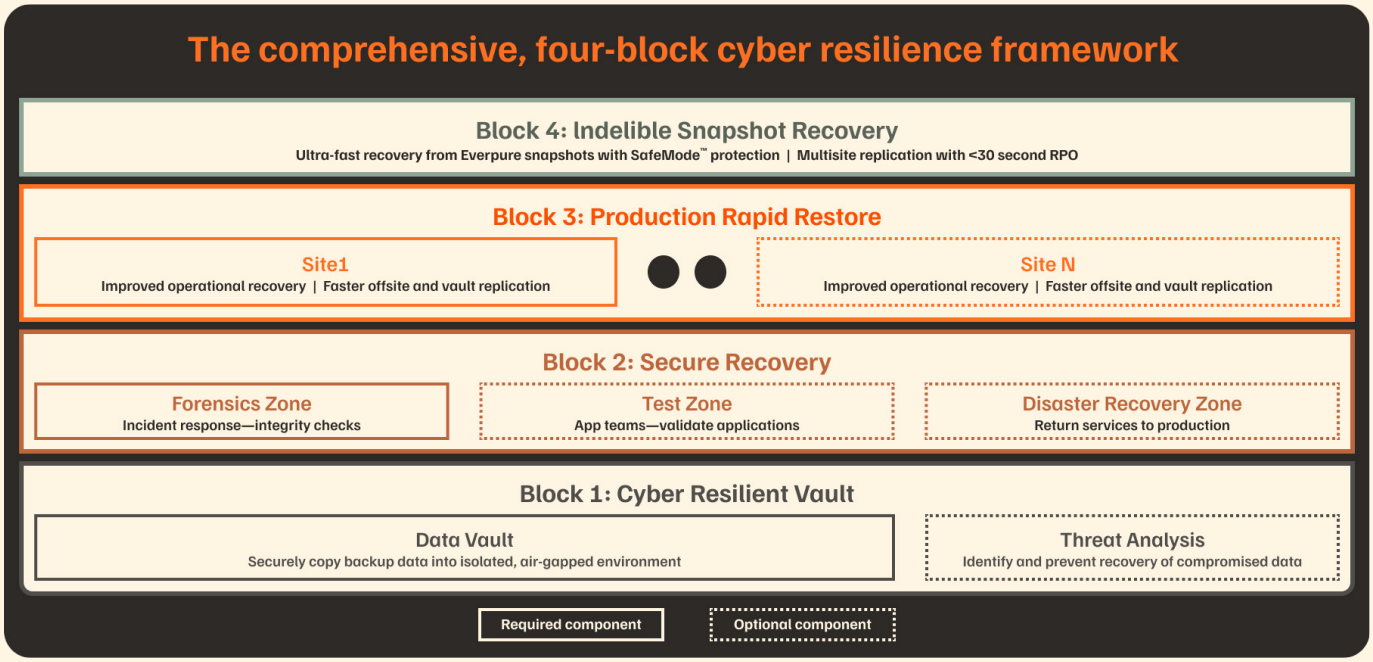
A solution designed for flexibility and scale

Given the depth and breadth of DORA requirements and the systems that institutions already operate, the Everpure and Commvault solution is modular and highly scalable.

Financial institutions can:

- Add multisite replication for operational continuity
- Extend into hybrid-cloud environments
- Scale across block and file workloads
- Automate disaster recovery runbooks using Everpure Fusion™ presets
- Continuously validate RPO/RTO objectives

This layered approach empowers organizations to strengthen both **continuity and clean recovery** capabilities without disrupting existing infrastructure.



The solution retains its four foundational layers—now strengthened with multisite operational continuity.

Block 1
Cyber Resilient Vault to safeguard backups

The logically air-gapped Cyber Resilient Vault is the required foundation for the solution. It provides an isolated, indelible repository that safeguards critical data. Data vault controls are isolated from the production environment to reduce the risk of credential leak and unauthorized access.

Commvault Threat Scan runs additional scans of replicated production backup data, enabling clean recovery in the Clean Recovery Zone.

This layer ensures integrity and immutability—essential for recovery from cyber incidents.

Block 2
Secure Recovery to recover and test applications

The solution decouples forensic analysis from business-critical restoration using an air-gapped IRE. This can operate on premises or via Commvault Cloud Cleanroom Recovery.

This layer ensures restored systems are trusted and free from compromise before returning to production.

Block 3
Everpure Production Rapid Restore to speed and simplify data transfer

Everpure FlashBlade indelible object storage serves as the high-performance target for Commvault backups. FlashBlade enables fast, secure, and reliable restores of large data sets to address regulatory recovery targets.

S3 Object Lock and SafeMode™ ensure backup data cannot be altered or deleted once written.

Block 4
Indelible Snapshot Recovery and multisite operational continuity

For critical Tier 1 systems such as payments, storage-based snapshots enable the fastest restoration workflows.

Everpure FlashArray supports:

- Indelible SafeMode Snapshots
- Application-consistent replication
- Synchronous ActiveCluster between sites
- Near-synchronous ActiveDR replication to a third site
- Automated failover with link-flip
- Instant reverse replication for failback
- Encrypted replication traffic
- Defined RPO/RTO alignment

Important distinction: Multisite replication sustains operational continuity during site-level disruption. The Cyber Resilient Vault and Clean Recovery Zone ensure clean recovery following cyber compromise. Together, they address both uptime and integrity—complementary pillars of digital operational resilience.

Global operational resilience

The principles of operational resilience are universally applicable across industries. Governments worldwide recognize their importance and are actively developing or implementing regulations to ensure business continuity and resilience for critical sectors.

While DORA applies specifically to financial institutions, the need to withstand, respond to, and recover from ICT disruptions extends across energy, healthcare, telecommunications, and digital infrastructure sectors.

Working with Commvault and Everpure, organizations can move more confidently to address today's and tomorrow's data resilience requirements. By combining multisite operational continuity with isolated clean recovery and indelible backup protection, organizations strengthen their ability to protect the value of their data—even in the face of sophisticated cyber threats and infrastructure disruptions.

The Everpure and Commvault partnership

Everpure and Commvault have partnered since 2010 to solve real-world challenges in securing, managing, and recovering data of all types.

The combination of Commvault's industry-leading cyber resilience software and the high-performance, secure Everpure Platform allows organizations to:

- Sustain service continuity across geographically dispersed sites
- Minimize data loss with defined RPO/RTO objectives
- Restore trusted systems following cyber incidents
- Continuously test and validate recovery readiness
- Address evolving operational resilience and regulatory requirements

By choosing Commvault and Everpure, financial institutions can unlock the full potential of their data, drive operational excellence, address compliance obligations, and gain a competitive edge in an increasingly complex threat landscape.

Additional resources

- Learn more about strengthening operational resilience in financial services.
- Understand the requirements of the Digital Operational Resilience Act (DORA).
- Find out more about the Everpure and Commvault partnership.
- Explore Commvault's cyber readiness and recovery solutions.

Visit Our Website | **800.379.PURE**

ID18466-01-en-03/26