

Everpure and Rubrik for cyber resilience and recovery

Helping banks restore trusted data and critical services faster

Financial institutions depend on the data and services that support payments, core banking, trading, digital banking, customer access, and other critical services. When a cyberattack disrupts these services, the incident moves beyond cybersecurity and becomes an operational resilience and business continuity issue.

Traditional recovery assumes a viable restore point exists. A cyberattack creates uncertainty about which recovery points are safe, which services must return first, and how quickly a bank can safely resume operations.

For banks, recovery is a sequencing problem as much as a technology problem. Teams must identify trusted data, prioritize critical services, and restore them fast enough to sustain the business.

The recovery question is no longer simply, “How fast can we restore?”
It is, “What can we safely restore, and how quickly can we get the bank operating again?”

The banking recovery challenge

Recovering from a cyberattack in a banking environment presents unique challenges. Banks must restore critical services while maintaining confidence in data integrity, meeting regulatory expectations, and preserving customer trust.

Operational disruption

Cyber incidents can interrupt payments, trading, digital banking, customer access, and other critical services. Extended disruption increases financial exposure and threatens business continuity.

Recovery uncertainty

Banks need confidence that the data they restore is trusted and will not reintroduce compromised data into the environment.

Recovery at scale

Tier 0 and Tier 1 banking services depend on large volumes of interconnected structured and unstructured data. Recovery must work at banking scale without becoming a bottleneck.

Regulatory pressure

Across regions, requirements such as the EU's Digital Operational Resilience Act (DORA); guidance from the Federal Financial Institutions Examination Council (FFIEC), Office of the Comptroller of the Currency (OCC), and New York Department of Financial Services (NYDFS) in the US; guidelines from the Office of the Superintendent of Financial Institutions (OSFI) in Canada; and Australia's CPS 230 standard reinforce expectations around continuity, recovery readiness, testing, and resilience under disruption.

Customer trust

When customers cannot access accounts, move money, or complete critical transactions, a technology disruption quickly becomes a trust issue.



Operational continuity

Restore priority banking services faster under pressure.



Recovery confidence

Know which recovery data is trusted before restoration.



Recovery at scale

Restore Tier 0 and Tier 1 workloads without making scale the recovery bottleneck.



Regulatory readiness

Support repeatable, testable recovery processes and resilience evidence.



Customer trust

Reduce disruption to critical services and customer access.

Banking cyber recovery by the numbers¹

Nearly 70%

of financial services organizations planning to increase cyber recovery investment cited limitations in their current recovery solution as a top-two driver.

1 in 4

financial services organizations reported losses from a successful cyberattack in the previous 12 months.

Around 30%

identified compliance and cyber insurance requirements as their primary driver for increased cyber recovery investment.

Trusted recovery requires resilient infrastructure and intelligent cyber recovery

Banks need both confidence in what they restore and the ability to restore it quickly at scale.

Everpure™ and Rubrik combine protected recovery data, cyber recovery intelligence, and high-performance infrastructure to help banks identify trusted recovery points and return priority workloads to operation with confidence.

Everpure: Resilient recovery foundation

Everpure provides the high-performance, resilient infrastructure required to protect and rapidly restore critical banking data. Technologies such as DirectFlash® Modules and metatag-based snapshots, combined with best-in-class disaster recovery and resilience capabilities, help banks reduce backup times and, more importantly, accelerate recovery times.

- Protect recovery data with default immutable and indelible protection.
- Minimize data loss with policy-driven protection and near-zero recovery time objectives.
- Restore Tier 0 and Tier 1 banking workloads at scale.
- Support rapid, high-performance recovery.
- Protect structured and unstructured banking data across critical environments.

Rubrik: Intelligent cyber recovery

Rubrik provides the intelligence to understand the impact of a cyberattack and determine what can be safely recovered.

- Detect threats and analyze recovery data.
- Identify and validate trusted recovery points.
- Use sensitive data intelligence to support recovery prioritization.
- Orchestrate precise, granular recovery.

Better together: From threat intelligence to trusted recovery

Rubrik identifies compromised and trusted recovery points. Pure1® Workflow Automation, within the Everpure Platform, applies that recovery intelligence to Everpure snapshots and volumes.

Together, this helps teams identify trusted recovery data and recover it quickly while reducing the risk of reintroducing compromised data.

Restore trusted data. Restore the bank.

1

Everpure protected recovery data

Immutable and indelible protection: Protect critical structured and unstructured banking data.

2

Rubrik Security Cloud

Identify trusted recovery points: Analyze threats and determine which recovery data can be safely restored.

3

Everpure Platform

Pure1 Workflow
Automation: Apply Rubrik recovery intelligence to Everpure snapshots and volumes, and recover trusted data fast and at scale.

4

Minimum viable bank services

Return priority banking services to operation (payments, core banking, trading, digital banking, and regulatory operations).

Bank back in operation: Restore what matters first

Minimum viable bank

Recovery is not complete when infrastructure comes back online. Banks must restore the systems, data, applications, and dependencies required to sustain critical operations. A **minimum viable bank** defines what must return first so recovery teams can prioritize the services that keep the institution operating.

Priority banking services

- **Payments:** Restore transaction processing and movement of funds.
- **Core banking and deposit access:** Restore access to accounts and core banking functions.
- **Trading and settlement:** Return critical capital markets and settlement operations.
- **Digital banking and customer access:** Restore customer-facing channels and account access.
- **Regulatory operations:** Restore services and data required to maintain regulatory and operational obligations.

Cyber resilience is measured by recovery

A cyberattack tests more than whether a bank has backups. It tests whether the organization can identify trusted recovery data, restore priority workloads, and return critical services to operation under pressure.

Everpure and Rubrik combine resilient recovery infrastructure with intelligent cyber recovery to help banks recover trusted data faster, reduce recovery uncertainty, and restore the services that keep the bank operating.

Banking proof: Frost Bank

Frost Bank, the banking, investment, and insurance subsidiary of Cullen/Frost Bankers, operates more than 130 branches and 1,200 ATMs throughout Texas. Its environment includes business-critical banking applications, transaction processing, databases, analytics, and customer-facing systems.

Frost Bank uses Rubrik for data management and backup, with archive data stored on Everpure FlashBlade®. Its deployment demonstrates how banks can protect and recover critical data at scale while ensuring continuity of critical services.

30TB

Data warehouse environment protected

3:1

Data reduction compared to legacy solution

16 hours → 2.5 hours

Backup time reduction compared to legacy solution

100% uptime

on the Everpure Platform, including during software and controller upgrades

Learn how Everpure and Rubrik can strengthen cyber recovery and operational resilience for your bank.

[Explore Banking Solutions](#)

¹ | IDC, "Operational Resilience in Banking: From Disaster Recovery to Minimum Viable Bank" August 2026.

[Visit Our Website](#)

800.379.PURE

