

Everpure and Commvault Anomaly Workflows

Turn early storage anomaly signals into faster, workload-aware cyber response and recovery.

Cyberattacks can surface first as subtle changes in storage behavior: shifting data reduction rates, unusual IOPS, abnormal latency, unexpected capacity changes, or changes in snapshot activity. These signals may appear before an event is fully understood as a security incident.

Everpure™ Pure1® anomaly detection, Pure1 Workflow Orchestration, and Commvault Cloud Threat Scan help turn those early storage signals into workload-aware cyber recovery context. The Pure1 workflow uses Everpure Fusion™ to bring together the Pure1 anomaly signals and Commvault IntelliSnap metadata to identify affected workloads and raise Commvault Threat Scan events.

The result is a faster path from storage anomaly to recovery action.

From anomaly to action

Detection alone is not resilience. Security, infrastructure, and recovery teams do not just want to see anomalies. They need to be alerted to act, with accurate signals, fewer false positives, and a direct path from signal to investigation and recovery planning.

Too often, storage-layer warnings stay trapped at the storage layer. An unusual pattern on an array may tell teams that something is wrong, but not which applications, databases, file systems, or virtual machines (VMs) may be affected. During a cyber event, manually correlating storage alerts, protected workloads, backup jobs, snapshots, and recovery options across disconnected tools can slow triage and increase risk.

Everpure and Commvault help close that gap. Using the Everpure Enterprise Data Cloud architecture as the blueprint, the Commvault anomaly workflow connects Pure1 anomaly detection, Everpure Fusion fleet information, and Commvault IntelliSnap metadata. The workflow helps identify the affected FlashArray™, map the anomalous volume to protected clients or VMs, and raise anomaly events in Commvault Cloud Threat Scan so teams can investigate faster and make more informed recovery decisions.

In simple terms: Pure1 detects. Everpure Fusion enriches. Commvault operationalizes.



Detect earlier

Spot storage anomalies before threats fully emerge.



Map impact faster

Link anomalies to affected apps, VMs, and data.



Recover with confidence

Use enriched insights to speed recovery decisions.

How the workflow works

The Pure1–Commvault anomaly workflow automates the multistage process shown in Figure 1, moving from storage telemetry to workload-aware anomaly events in Commvault Cloud.

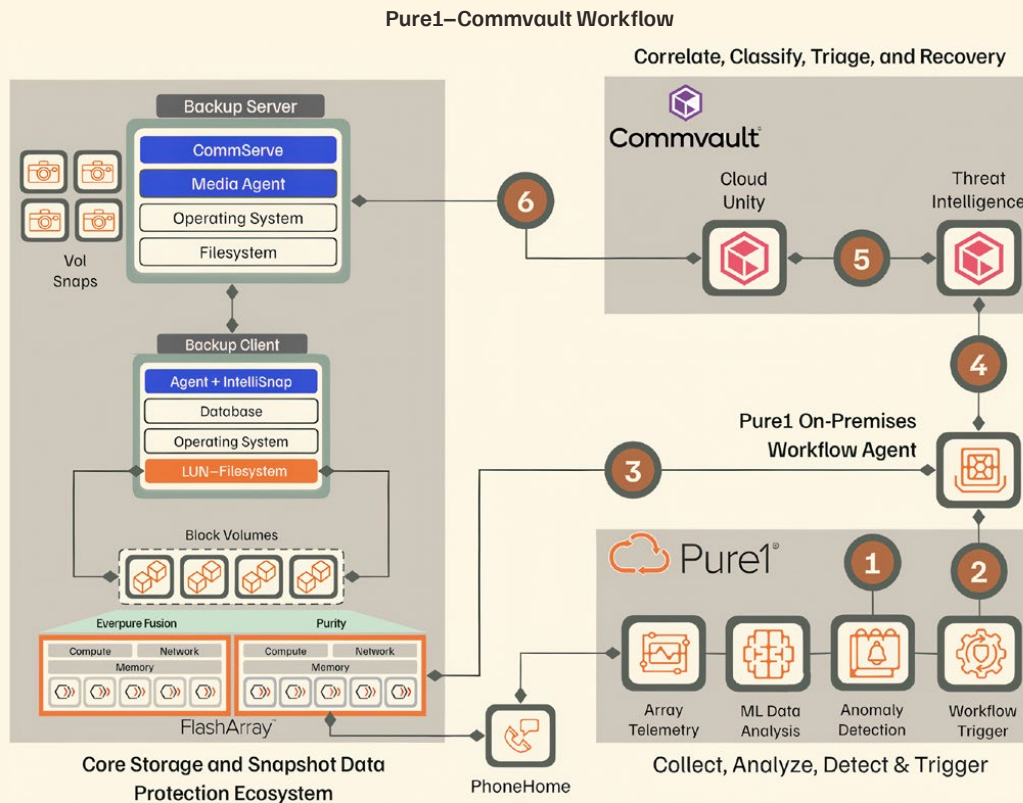


FIGURE 1 Pure1 detects and enriches the anomaly, Everpure Fusion provides fleet context, and Commvault correlates the signal to IntelliSnap-protected workloads for triage and recovery action.

Stage 1: Anomaly detection

Pure1 collects and analyzes FlashArray telemetry to identify abnormal storage behavior. Machine learning baselines key signals such as latency, IOPS, bandwidth, data reduction ratio, capacity, volume count, and snapshot count, automatically detecting unusual activity at the storage layer.

Stage 2: Workflow trigger

When Pure1 detects an anomaly, Pure1 Workflow Orchestration triggers the workflow and reaches the customer environment through the Pure1 on-premises workflow agent. This prevents the anomaly from remaining an isolated storage alert.

Stage 3: Gather volume details

The workflow uses Everpure Fusion fleet context to identify the affected array and retrieve details needed to match the anomaly to Commvault's FlashArray snapshot inventory.

Stage 4: Gather client details

The workflow identifies the clients and VMs associated with the IntelliSnap-based snapshots. This brings storage context and protection context together so the signal can be mapped to Commvault-managed workloads.

Stage 5: Anomaly events in Commvault

After correlation, the workflow raises anomaly events in Commvault Cloud Unity for affected protected clients or VMs. The alert is no longer just a storage-side symptom; it is part of a threat profile for the workload.

Stage 6: Recovery orchestration

With affected workloads identified, teams can use Commvault threat intelligence, Threat Scan workflows, and point-in-time snapshot data to prioritize investigation and evaluate recovery options with more confidence. The workflow supports cleaner recovery decisions, but does not independently certify that a recovery point is clean.

Cyber response with more confidence

When threats surface first in storage behavior

Ransomware and other disruptive activity can change how data compresses, how volumes grow, how snapshots behave, and how workloads perform. Pure1 anomaly detection learns normal behavior and surfaces deviations early, helping teams spot unusual storage behavior before it becomes a larger operational or cyber resilience event.

When manual response takes too long

Manual triage can leave storage, backup, security, and recovery teams working from different views of the same threat. Pure1 Workflow Orchestration helps connect storage telemetry, Everpure Fusion fleet information, and Commvault IntelliSnap metadata to build a clearer picture of affected assets and protected workloads.

When teams need to know how workloads may be affected

A storage anomaly without workload context slows investigation. By correlating anomalies to Commvault-protected clients, backup jobs, and IntelliSnap snapshots, the joint workflow helps responders identify which VMs, databases, file systems, or other protected workloads may be under threat. Commvault's risk profiles help focus investigations and determine the best course of action.

When recovery decisions matter

Restoring from the wrong point can increase risk or extend downtime. Anomaly events in Commvault Cloud, enriched with Pure1 and Everpure Fusion context, help teams understand where to focus investigation, which workloads may require closer review, and how to evaluate point-in-time recovery options with better context. Commvault Threat Scan reduces the chance of bringing an infected workload back online and reinfecting production.

Built for workload-aware cyber recovery

The Pure1–Commvault anomaly workflow is designed to help teams move from a storage anomaly to a clearer understanding of which protected workloads may be affected and how to best address the situation.

By connecting Pure1 anomaly detection with Everpure Fusion and Commvault IntelliSnap metadata, the workflow helps translate unusual storage behavior into workload-aware recovery context. Instead of investigating arrays, volumes, snapshots, jobs, and clients separately, teams get a more connected view of where to focus attention.

This helps security, infrastructure, and recovery teams reduce manual correlation, prioritize investigation, and make more informed recovery decisions during a cyber event.

From signal to action

The value is not just detecting anomalies—it is making them actionable for recovery teams.

Early anomaly intelligence

- ML-driven baselines across latency, IOPS, bandwidth, data reduction ratio, and capacity
- Visibility across performance, capacity, snapshot activity, administrative behavior, system metrics, and unusual logins
- Fleet-scale correlation across arrays

Workload-aware recovery context

- Anomaly events raised in Commvault Cloud
- Commvault IntelliSnap correlation to protected clients, jobs, and snapshots
- Added context for threat investigation, Threat Scan workflows, and recovery planning

Automated signal-to-action

- Pure1 Workflow Orchestration recipes
- Low-code/no-code workflow automation
- Broad ecosystem integrations, RBAC, and audit trails

Additional resources

Explore how Commvault and Everpure help teams strengthen cyber resilience and test our joint solutions:

- [Explore Commvault and Everpure Cyber Resilience Solutions](#)
- [Test Drive Commvault and Everpure](#)

Visit Our Website

800.379.PURE

