Commvault

WHITE PAPER

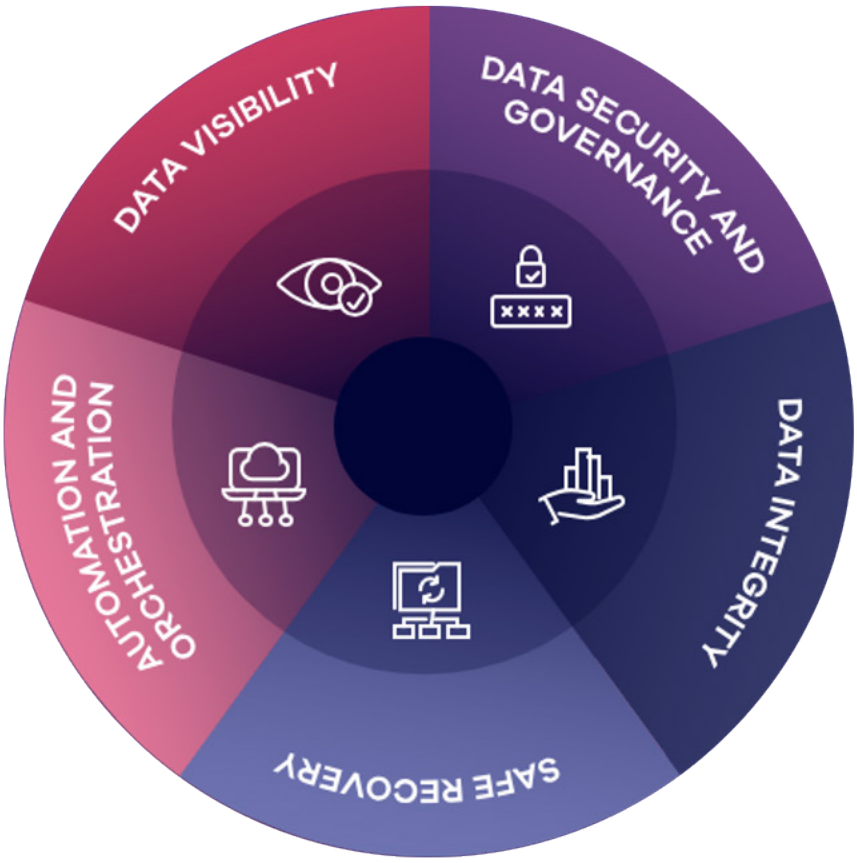
Can You Prove You're Recoverable Right Now?

What cyber resilience looks like in practice when detection and recovery are connected by design – and validated by evidence.

Commvault

Table of Contents

CONTENTS



EXECUTIVE SUMMARY

Cyberattacks are no longer isolated security events. They are enterprise-wide disruptions that expose how well teams can respond and recover amid fragmented tools, signals, and decision-making. As attacks unfold, security and IT teams are often forced to navigate chaos rather than act with clarity.

Cyber resilience requires more than data protection. It demands a coordinated approach that unifies security, IT, and recovery teams around shared intelligence, validated recovery paths, and proven readiness. This is the foundation of ResOps, an operating model that assumes disruption and proves recoverability through evidence.

Commvault Cloud unifies anomaly and threat detection, data protection, and recovery validation and operations on a single platform. By embedding AI-assisted insight directly into the data protection lifecycle, Commvault helps enable organizations to identify trusted recovery points, test recovery paths, and restore critical systems with confidence — even in the face of sophisticated attacks.

THE CHALLENGE

When a cyberattack hits, you're expected to respond immediately — and decisively. Security teams surface alerts, IT teams prepare for recovery, and business leaders want to know how quickly operations can be restored. But too often, you're forced to make critical decisions with incomplete information and disconnected tools, while the clock is already ticking.

Attackers exploit this reality. They move quietly, remain undetected for long periods, and increasingly target backup and recovery environments themselves. By the time you're ready to recover, you may no longer trust your most recent data copies. Without shared visibility across security and IT, you're left choosing between restoring quickly and restoring safely — a tradeoff that leads to prolonged outages, reinfection risk, regulatory exposure, and lost confidence at the board level.

Cyber resilience breaks down when teams can't act as one. And in modern attacks, fragmentation is exactly what attackers count on.

THE SOLUTION

To withstand attacks in the age of AI and respond with confidence, you need an approach that enables teams to act together and recover without guesswork.

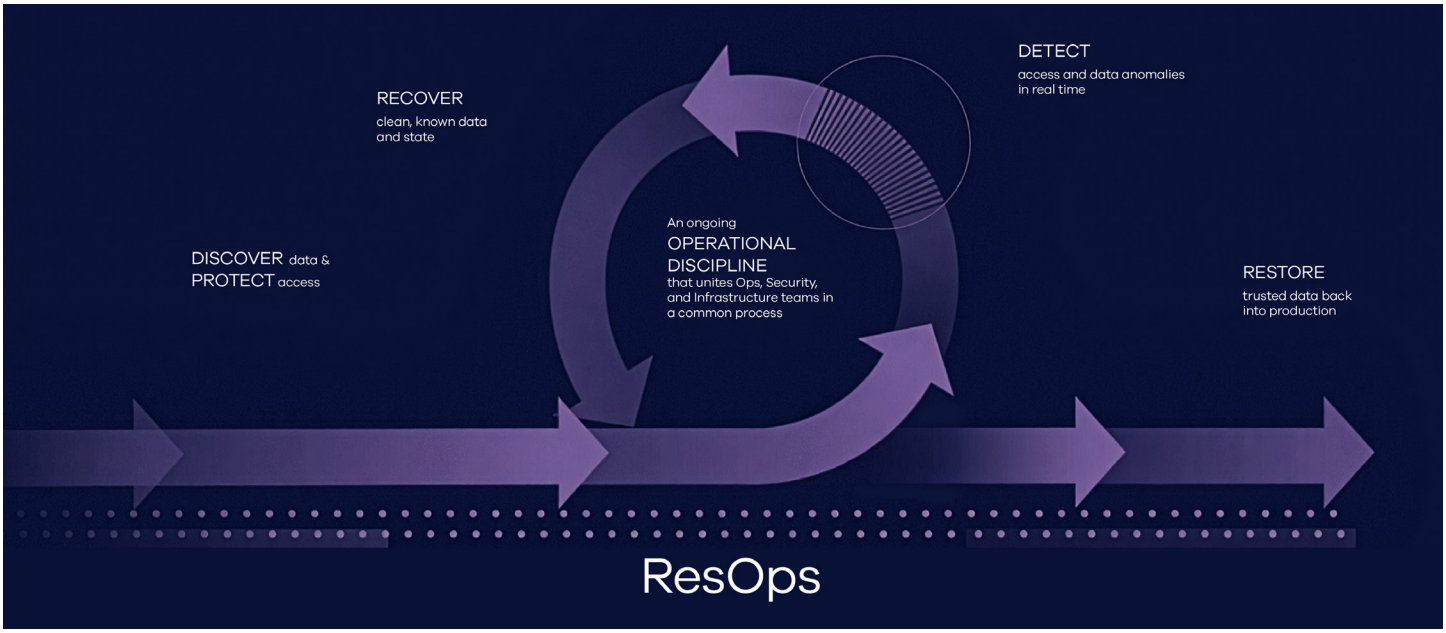
- **Unify security, IT, and recovery around a single cyber resilience strategy**
  Detection, protection, and recovery decisions must be driven by shared intelligence and common evidence — so teams move together under pressure instead of working in silos.
- **Validate recoverability, not just detect threats**
  You need proof that recovery points are clean, intact, and usable before production systems are restored.
- **Protect the recovery process itself**
  Backups, identities, and recovery environments must be isolated, hardened, and designed to withstand attack.
- **Enable fast, clean, and complete recovery at scale**
  Detection signals must translate into recovery decisions everyone trusts, enabling recovery workflows within the required impact tolerances without forcing tradeoffs between data loss and reinfection risk.

THE COMMVAULT APPROACH

Commvault Cloud brings cyber resilience together as a unified platform that aligns with the ResOps operating discipline. Instead of treating detection, protection, and recovery as separate domains owned by different teams, Commvault unifies them, giving IT teams a security-informed, shared view of risk, recoverability, and response.

Anomaly and threat detection are embedded directly into the data protection lifecycle — before data is copied, after it's stored, and during recovery. Behavioral anomaly detection provides early indicators of compromise, while integrated threat detection is designed to scan protected data for malware, ransomware, and encryption artifacts. These signals don't stop at alerting; they can trigger remediation and help establish a common set of facts teams can trust when determining what to recover and how to fast-track recovery safely.

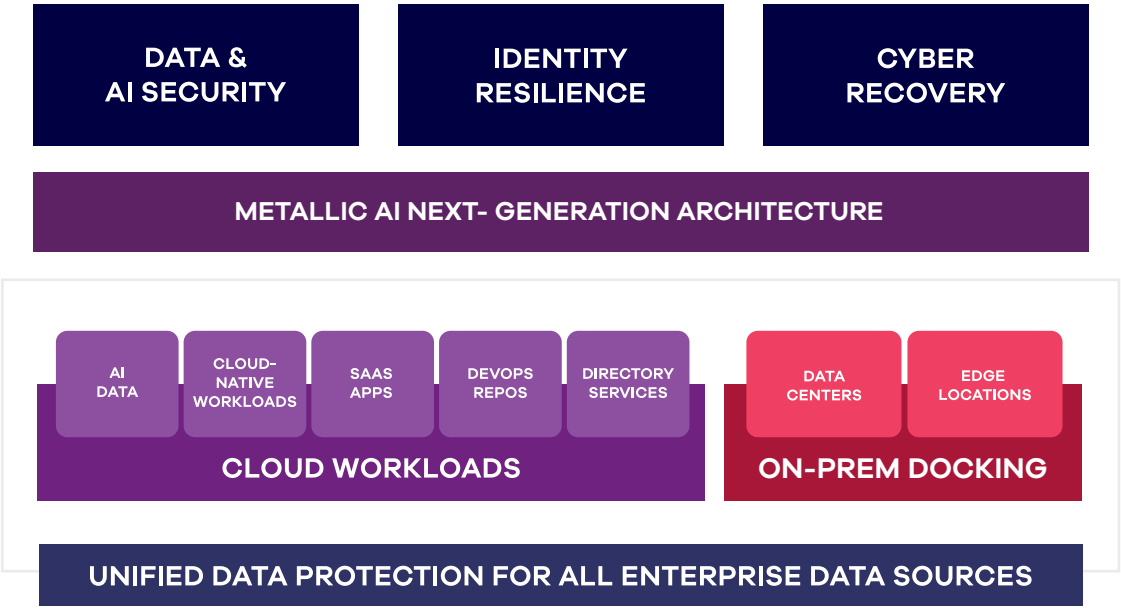
The result is evidence-driven recovery. You can validate clean recovery paths in isolated environments, rehearse real-world scenarios, and restore critical systems with confidence — even when disruption is assumed. By unifying operations, defenses, and recovery on Commvault Cloud, teams can act as one, move decisively under pressure, and emerge from attacks not just operational again, but measurably more resilient.



ResOps Capabilities in Action

ARCHITECTURE MATTERS

Commvault Cloud



Privacy note: Commvault anomaly and threat detection analyze metadata and behavioral signals, not customer data content.

Key Capabilities

PROTECTION & ISOLATION

Limit blast radius and protect the recovery path.

Multi-phase anomaly detection across the data lifecycle

Behavioral anomaly detection monitors live systems, copy operations, post-copy data, and recovery workflows to surface early indicators of compromise – even when malware is unknown or dormant. AI-assisted analytics distill large volumes of backup and operational data into clear, actionable insights, highlighting anomalies and key events to help teams spot issues early, understand what changed, and act with confidence.

Integrated threat detection and encryption analysis

AI-assisted threat scanning inspects protected data for malware, ransomware, and suspicious encryption using signature-based detection, heuristics, machine learning, YARA rules, and advanced encryption analysis.

Threat intelligence and deception-driven early warning

Built-in cyber deception and integrated third-party threat intelligence exposes malicious activity earlier, helping teams identify compromised systems and data before recovery begins.

Hardened and isolated recovery data

Immutable, logically isolated backup copies and recovery environments help prevent attackers from tampering with restore points or pivoting into recovery workflows.

VALIDATED RECOVERY & REBUILD

Recover cleanly, completely, and within business impact tolerances.

Cleanpoint™ recovery validation

Detection signals are correlated with backup metadata and enriched with threat data to identify which restore points are safe to use. Teams receive clear threat summaries, risk context, and recovery guidance directly within recovery workflows, eliminating guesswork during high-pressure recovery decisions.

Synthetic Recovery™ for clean, current restores

Automatically assemble a new recovery point composed only of verified clean data – preserving the most recent good data while excluding corrupted or encrypted elements, with no forced tradeoff between data loss and reinfection risk.

Any-to-any recovery at enterprise scale

Restore applications, data, and infrastructure across on-prem, cloud, hybrid, and SaaS environments without requiring like-for-like infrastructure – supporting rebuild-from-scratch scenarios when environments are fully compromised.

Identity-aware recovery validation

Detect and roll back suspicious Active Directory and Entra ID changes as part of recovery, ensuring identity systems don't reintroduce persistence or privilege escalation.

SCENARIO ORCHESTRATION, TESTING, AND VALIDATION

Turn resilience assumptions into evidence.

On-demand Cleanroom Recovery environments and runbooks

Spin up isolated, air-gapped environments in minutes to validate recovery paths, investigate incidents, and orchestrate real-world response scenarios without impacting production.

Integrated threat scanning during recovery testing

Inspect data during test restores in isolated environments to validate recoverability under realistic conditions, enabling recovery path validation before systems are returned to production.

Repeatable, low-risk recovery validation

Support frequent testing of recovery plans, enabling teams to validate impact tolerances, refine runbooks, and build confidence across security, IT, and business stakeholders.

TECHNICAL DIFFERENTIATION

Commvault anomaly and threat detection is natively embedded across the data protection lifecycle, helping to provide continuous visibility into live systems, data movement, stored copies, and recovery workflows — not just detection at restore time.

Rather than relying on a single technique, Commvault combines behavioral anomaly detection, malware and ransomware analysis, encryption identification, cyber deception, identity-aware signals, and third-party threat intelligence to continuously assess data integrity. These signals are correlated with backup metadata and recovery operations to identify what was impacted, which recovery points remain safe, and how recovery should proceed.

Because detection and validation are integrated directly into protection and recovery workflows, teams can move from alerting to action — validating clean recovery paths, reducing reinfection risk, and accelerating recovery across on-prem, cloud, hybrid, and SaaS environments.

COMPLIANCE & CERTIFICATIONS

Commvault Cloud is designed to help meet the security, privacy, and compliance requirements of enterprise and regulated environments. Our controls, processes, and certifications support global standards across data protection, privacy, and operational security.

Visit Commvault's Trust Center for complete compliance documentation.

CONCLUSION

Cyber resilience isn't achieved by tools operating in isolation — it's delivered when teams can act together with clarity and confidence. By unifying anomaly and threat detection with protection, recovery, and v alidation on a single platform, Commvault Cloud helps enable organizations to move beyond alerting and toward cyber resilience.

With Commvault Cloud, you have a powerful tool designed to help you protect what matters, validate recoverability, and restore critical systems cleanly and quickly — even when disruption is assumed. The result is not just faster recovery, but a more resilient organization that's prepared, coordinated, and ready to emerge stronger after every attack.

Learn more at www.commvault.com.

FAQ

Q: What's the difference between anomaly detection and threat detection?

A: Anomaly detection identifies unusual changes in protected data or behavior that may indicate early compromise, even when malware is unknown. Threat detection actively looks for known malicious activity using intelligence and scanning techniques. Together, they provide early signals and confirmation that directly inform clean, confident recovery decisions.

Q: What is ResOps, and why does it matter for cyber resilience?

A: ResOps, or Resilience Operations, is an operating model that unifies security, IT, and recovery teams around shared evidence and workflows. It assumes disruption will occur and focuses on proving recoverability through testing, validation, and coordinated execution, rather than relying on plans or point tools that operate in isolation.

Q: Why is recovery validation critical after a cyberattack?

A: Because attackers increasingly target backup and recovery environments, restoring data without validation can reintroduce risk. Recovery validation confirms which recovery points are safe to use before systems are restored. This reduces guesswork, prevents reinfection, and allows teams to restore operations with confidence under pressure.

Q: How does Commvault Cloud connect detection to recovery?

A: Commvault Cloud embeds anomaly and threat detection directly into the data protection lifecycle, including before copy, after data is stored, and during recovery. Detection signals are correlated with backup metadata and recovery workflows, turning alerts into actionable recovery intelligence that helps teams decide what to restore and how.

Q: What is Cleanpoint™ recovery validation?

A: Cleanpoint™ recovery validation identifies recovery points that remain trustworthy after an attack by correlating detection signals, threat context, and backup metadata. It is designed to provide teams with clear guidance inside recovery workflows, reducing the need for deep forensic expertise while accelerating safe, evidence-based recovery decisions.

Q: Does Commvault access or read customer data for anomaly and threat detection?

A: No. Commvault does not read or analyze customer data content. Anomaly and threat detection operate primarily on metadata, behavioral signals, and backup characteristics such as changes in size, structure, entropy, and activity patterns. When scanning is enabled, analysis is customer-controlled and performed within protected recovery workflows.

Q: How does AI support anomaly and threat detection without replacing human judgment?

A: AI supports teams by analyzing large volumes of data to surface anomalies, patterns, and risk context that would be difficult to identify manually. It assists with interpretation and prioritization, but decisions remain human-led. This approach reduces noise and effort while improving clarity and confidence during investigation and recovery.

Q: Why is identity resilience critical to cyber recovery?

A: Identity systems are often the fastest path attackers use to gain persistence and escalate privileges. Identity resilience ensures suspicious changes to directories and access controls are detected, validated, and rolled back during recovery. This prevents restored systems from inheriting compromised identities and reduces the risk of reinfection after recovery.

RELATED RESOURCES

Cyber Recovery 101