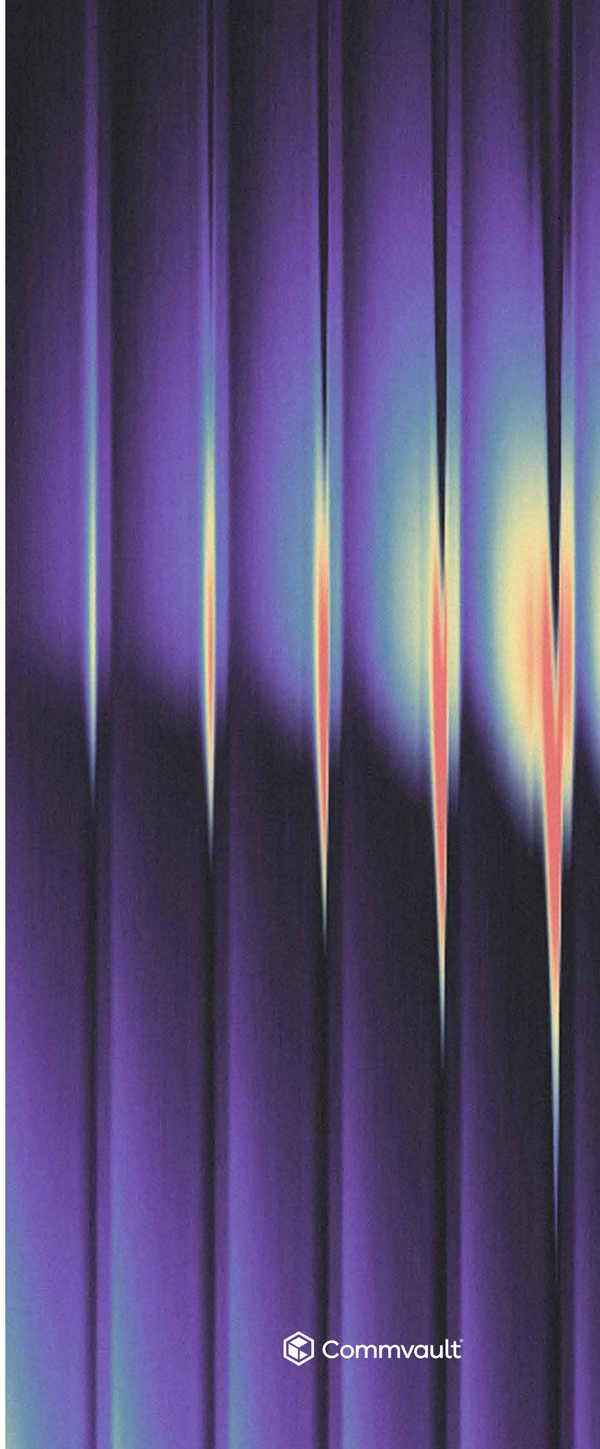
READINESS REPORT ISSUE 3 MARCH 2026

The CISO's Guide to Modern Multi-Cloud Resilience

7 Criteria for Evaluating Cloud Data Protection Platforms

A Readiness Report for CIOs and CISOs



READIVERSE

Commvault

Executive Summary

The CISO mandate has shifted from data protection to business survival. In multi-cloud environments, an adversary who compromises AWS credentials doesn't just access production data. They can delete backups, snapshots, and disaster recovery configurations across your entire cloud ecosystem.

Most organizations exist somewhere between "we have backups" and "we can recover cleanly under attack." Evaluating data protection platforms now requires deep scrutiny of architecture, economics, and operational resilience across heterogeneous cloud ecosystems.

This report examines the foundational build vs. buy decision, alongside seven critical vectors every security leader should evaluate when procuring cloud data protection, from backup cost optimization and recovery architectures to continuous resilience operations (ResOps) and data security posture management.

The First Question: Build vs. Buy

AI coding assistants make building custom backup solutions appear straightforward. However, homegrown tools may face hidden liabilities in multi-cloud environments:

The multi-cloud complexity trap:
A script that works perfectly for one provider's block storage may fail for another's. Building a homegrown tool often requires maintaining separate codebases for every cloud where you operate, multiplying the engineering burden.

Scalability and performance risk:
Internal tools rarely achieve enterprise-grade robustness. A script might work for terabytes, but does it crumble under the performance weight of petabytes? Homegrown architectures may fail to meet strict service-level agreements when data volume spikes.

The market benchmark:
Is what you are building actually superior to specialized products available for purchase? Commercial platforms abstract multi-cloud complexity, offering features like global deduplication and cross-cloud portability that would take years to replicate internally.

Opportunity cost:
Every hour an engineer spends maintaining a backup utility is an hour not spent on revenue-generating innovation.

7 Criteria for Evaluating Cloud Data Protection Platforms

For organizations that determine a commercial platform is the right strategic choice, the following seven criteria form a comprehensive evaluation framework:

1. Cost Control: Avoid Paying to Protect What Doesn't Matter

Legacy platforms can force you to protect everything equally: Dev environments get the same treatment as production data. The result? Unpredictable costs that spiral across cloud providers. Modern platforms give you control through five key capabilities:

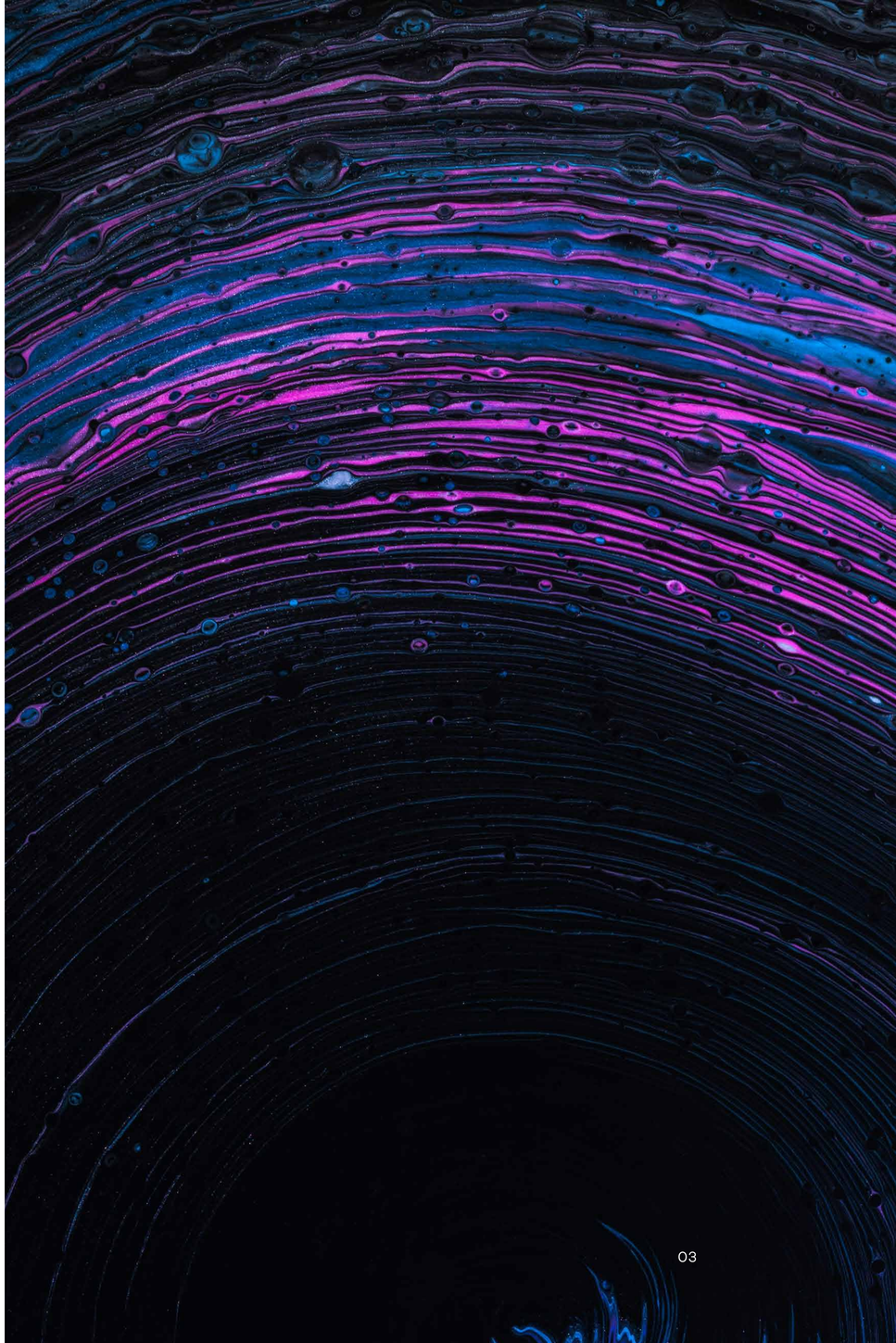
Granularity and unified service catalogs: Ideally, you should not pay to protect dev/test artifacts at the same rate as mission-critical IP. Look for precise selection capabilities – specific prefixes, tables, or partitions – managed through a global service catalog. This should protect the entire data pipeline via a "single pane of glass" by abstracting underlying differences between cloud storage services.

Recovery point objectives (RPO) and modern architecture: In high-velocity environments, critical data change rates can be enormous. To help enable minimal data loss, RPOs must be as low as possible. This stress-tests architecture; only products built on truly modern, scalable cloud-native stacks can handle frequent backups without toppling under multi-cloud footprint load.

Compliance and isolation: Air-gapped and immutable backups are compliance mandates. Most frameworks require isolation of secondary copies from primary data. Cross-region and cross-cloud backup support is strongly recommended. In the face of surging ransomware attacks, storing backups in a completely different cloud provider offers ultimate blast-radius separation.

Application awareness: Applications rarely live in a vacuum. You must protect the "application" as a whole entity, even if its components span multiple zones or clouds. Preserving complex internal dependencies at backup time is critical to enabling the operation of the application when restored.

Optimized total cost of ownership: TCO is the governing constraint. Managing native backup tools for each cloud provider can result in fragmented bills and unpredictable costs. The right platform consolidates this spend, delivering advanced capabilities without runaway costs of managing disparate infrastructure.



7 Criteria for Evaluating Cloud Data Protection Platforms

2. Flexible Recovery: One Size Does Not Fit All

In a crisis, rigidity is the enemy. Recovery requirements vary wildly depending on the incident, and a one-size-fits-all recovery button is insufficient. Your platform must be flexible in the face of different scenarios:

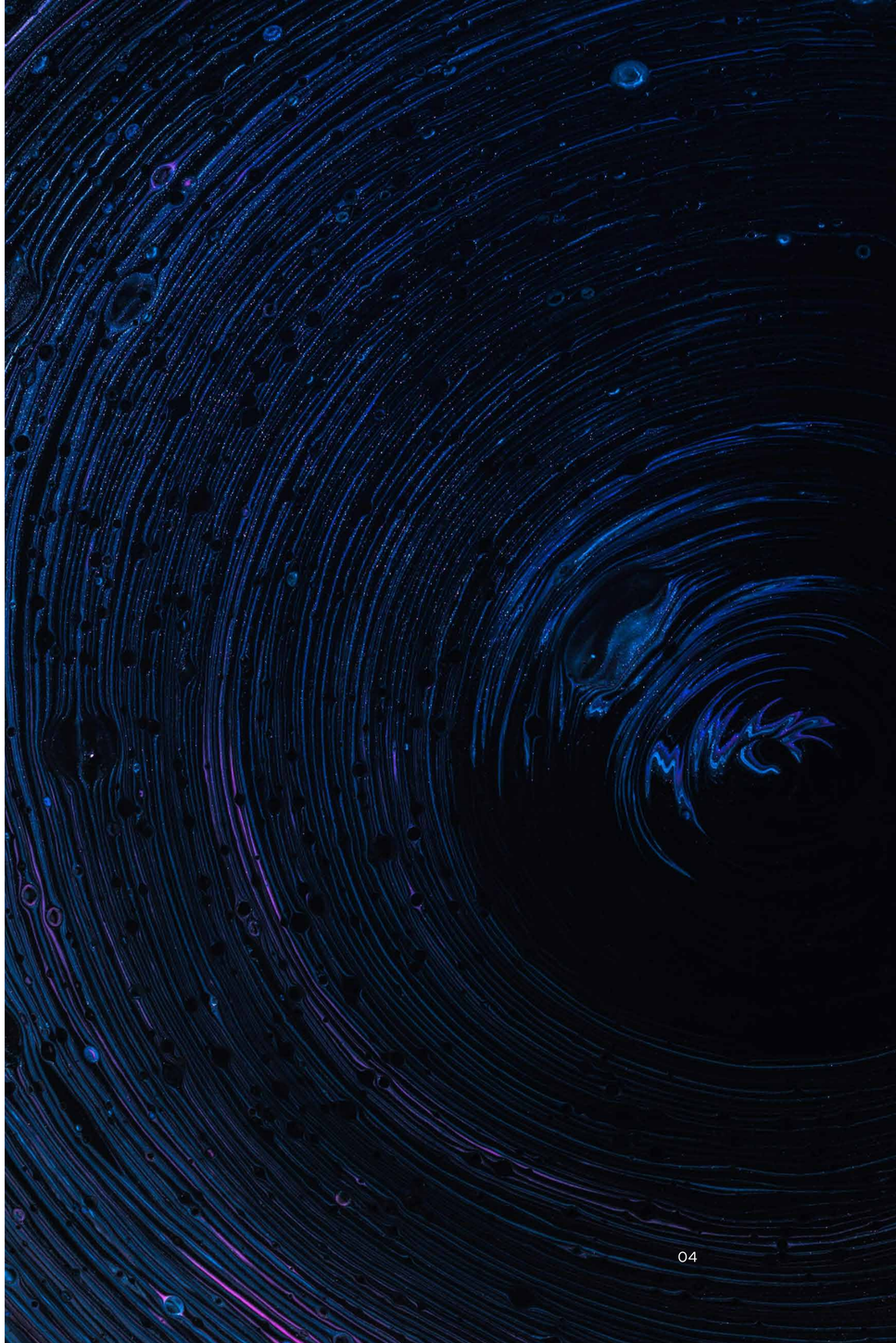
Compliance and audit scenarios: You may need rapid access to a specific dataset to prove recoverability to an auditor without executing a full, time-consuming restore.

Surgical recovery: For recovering portions of your data estate, recovery needs to be granular and not "all or nothing." If a single database partition is corrupted, you shouldn't have to roll back the entire table. Granular recovery allows you to fix only what is broken.

Full application recovery: Recovering raw assets is insufficient if application logic remains broken. Look for application-aware recovery that restores internal dependencies, so that the service comes back online, not just the files.

Cross-cloud portability: In extreme scenarios, such as a total provider outage or account compromise, you may need the ability to restore data from one cloud to another. A platform that avoids proprietary lock-in and supports cross-cloud recovery helps provide protection and flexibility.

Speed and TCO: The platform must support rapid recovery time objectives while providing this flexibility at optimized TCO regardless of the specific recovery scenario.



7 Criteria for Evaluating Cloud Data Protection Platforms

3. Continuous Resilience: ResOps-Ready

Recovery, not backup, determines business continuity. To modernize, we must treat data protection like DevOps: continuous, automated, and tested. This is ResOps.

Resilience as Code: Procurement should focus on platforms that treat recovery plans as code, meaning strategies that are continuously tested and deployed. Crucially, these plans need to be cloud-agnostic, allowing you to apply the same resilience logic to a workload in one cloud as you would in another.

Ongoing testing: A vendor that boasts about backup speeds but is silent on recovery orchestration is missing the objective. Your operational resilience depends on how fluidly you can transition from a "business as usual" state to a "recovery" state across any cloud environment. Annual disaster recovery tests provide false confidence when infrastructure changes daily.

The end-to-end view: Shift the KPI from "successful backup rate" to "successful recovery verification" measured through recovery posture scores that quantify readiness across your estate.

4. Early Warning Systems: Catch Threats Before They Strike

To truly modernize, we must fully embrace ResOps, beyond the reactive cycle of backup and recovery. True resilience starts before an event hits your data estate. This "Left of Bang" strategy requires a platform that acts as an intelligent early warning system across your entire multi-cloud footprint:

Anomaly detection: AI/machine learning (ML) is operationally tailor-made for this use case. ML algorithms excel at establishing baselines and identifying subtle patterns, such as unexpected encryption or spikes in data entropy, far faster than human monitoring. This speed is critical: The quicker the AI identifies the pattern, the faster you can intervene, helping directly minimize the blast radius of data loss.

Threat detection: As for specific threats, the goal is coverage. You should select services that cast a wide net, scanning for the highest possible volume and variety of threats. Because the threat landscape evolves hourly, a backup platform should ideally integrate with specialized, best-of-breed threat detection engines rather than relying solely on a proprietary library.

7 Criteria for Evaluating Cloud Data Protection Platforms

5. Post-Event Orchestration: From Alert to Recovery in Seconds

To round out the ResOps story, we must connect pre-event detection ("Left of Bang") with smooth post-event response. When an incident is confirmed, the recovery workflow cannot be a manual scramble; it must be a precise orchestration:

Integration with external signals: Post-event recovery often relies on intelligence from outside the backup platform. Most enterprises use a fabric of security information and event management tools and observability tools to aggregate logs. Your data protection platform should integrate with them, accepting triggers to initiate recovery the moment a high-fidelity alert is fired.

API framework for automated runbooks: Speed is the currency of recovery. It is crucial to have a robust API framework that allows you to trigger automated recovery "runbooks" programmatically. This removes human latency, allowing your security stack to isolate a compromised account and begin data restoration across regions, accounts, or even clouds rapidly.

Cleanroom capabilities: In the event of a ransomware attack, you cannot simply restore to production; you risk re-infecting the environment. Ideally, the platform will support recovery to an isolated recovery environment (like Commvault® Cloud Cleanroom™ Recovery), automating the restoration of data into an isolated environment for forensics and sanitization before it touches production infrastructure.

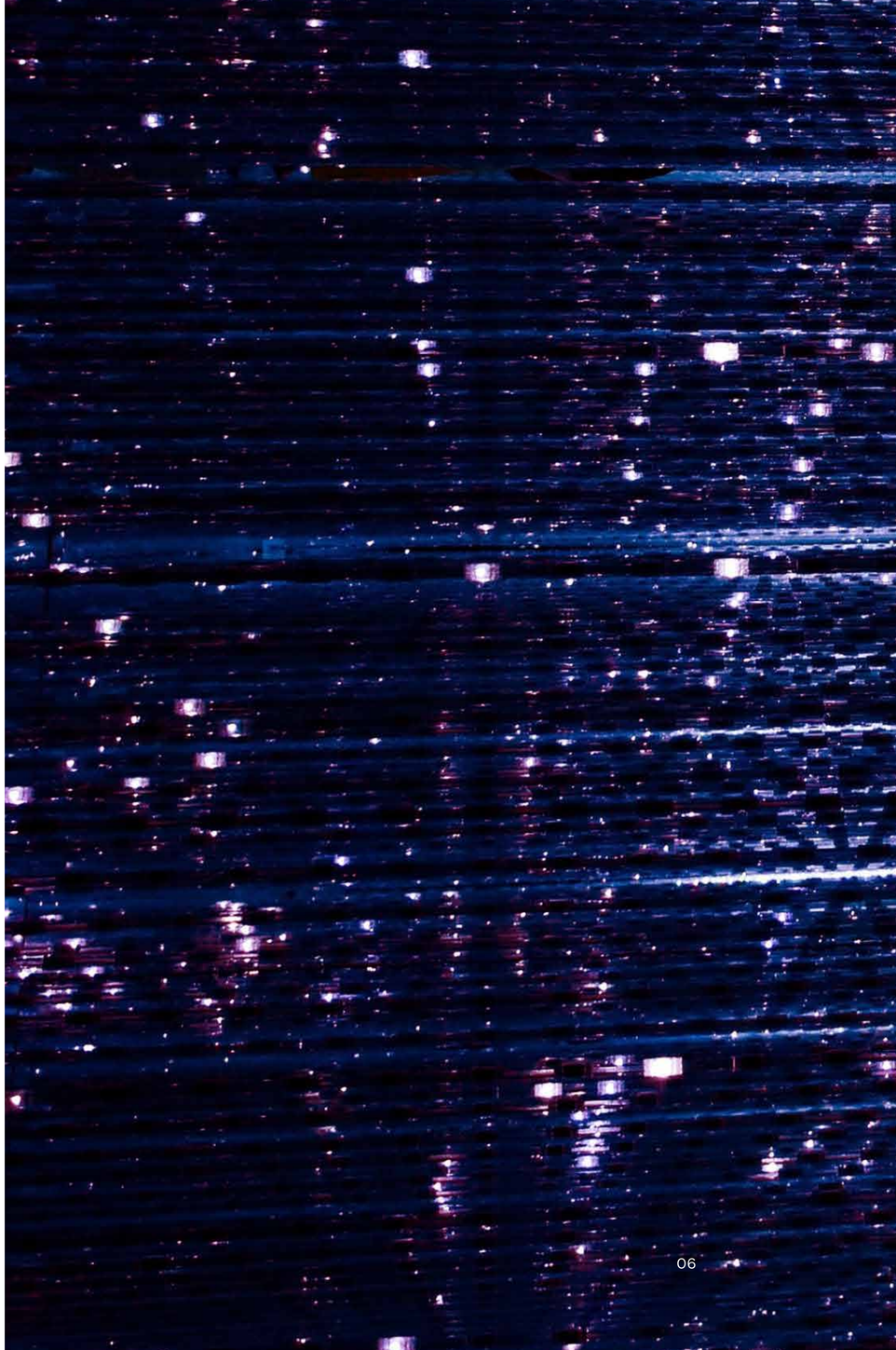
6. Platform Integration: Make Protection Invisible

Companies deal with hundreds of SaaS services daily. To avoid "death by SaaS" and drowning in disparate UIs, your data protection platform should be invisible yet omnipresent. This relies on a mature ecosystem built on three pillars:

Deep integration frameworks: The platform should fit natively into your engineering culture. Look for comprehensive API and SDK frameworks. Whether your developers prefer raw API access or language-specific SDKs, these tools allow them to integrate protection natively into applications. If your organization has standardized on Infrastructure as Code, confirm that backup policies and recovery plans can be fully codified to fit smoothly into CI/CD pipelines.

Agentic workflows: Does the platform support the creation and management of AI agents to automate complex workflows? Crucially, this innovation brings risk: Autonomous agents can create runaway costs. The platform should provide absolute control over the agents you create, so that automation doesn't break the budget.

Transparency: You need a clear window into operations across all clouds. The platform should provide distinct reporting views tailored to specific stakeholders: consumption reports for FinOps to track spend, task reports for admins to monitor health, and compliance reports for governance, risk, and compliance teams to prove governance.



7 Criteria for Evaluating Cloud Data Protection Platforms

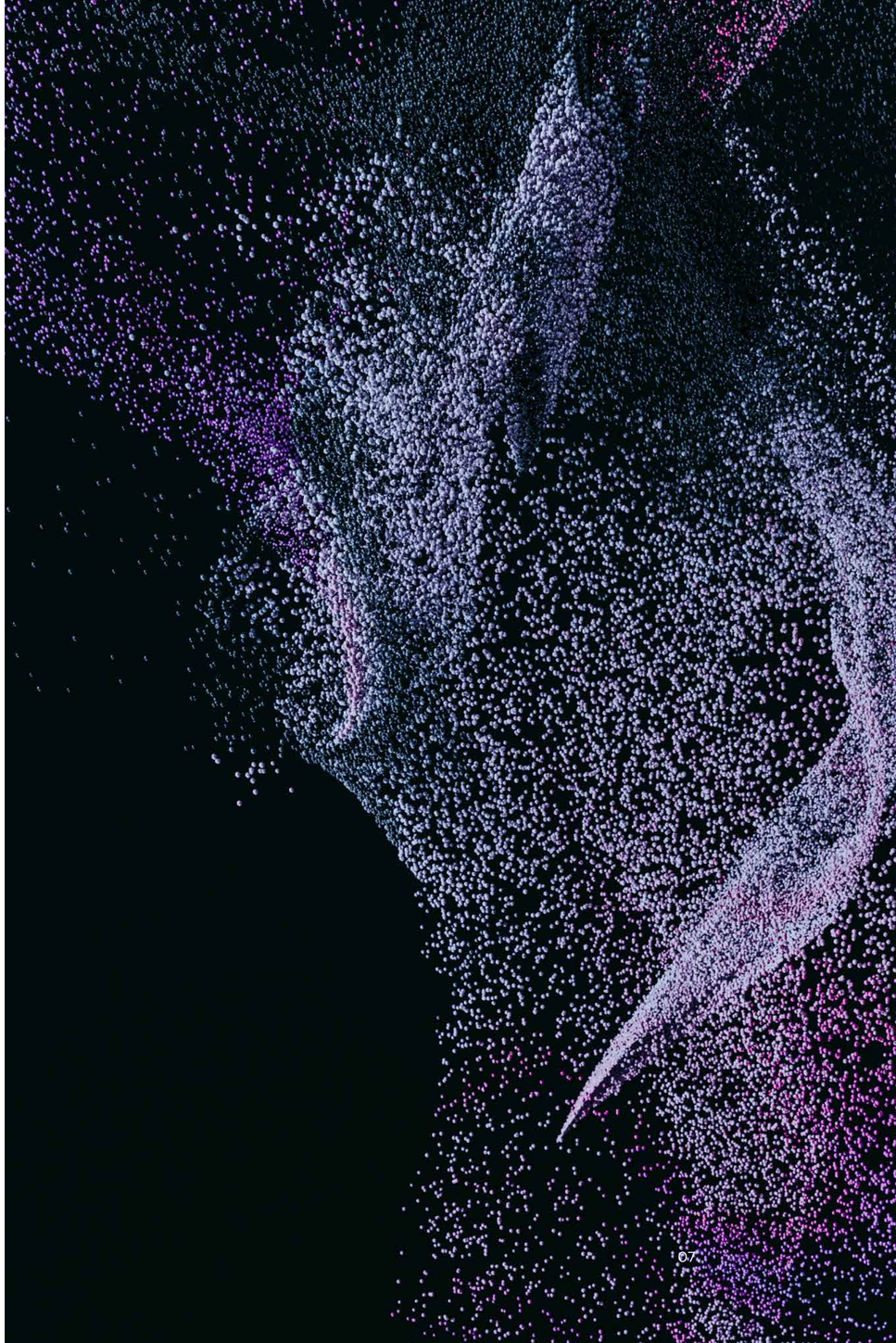
7. Foundational Security: Protect the Protector

Data protection platforms are high-value targets for attackers. CISOs should evaluate the platform's security posture through four distinct lenses:

The compliance matrix: Is the platform compliant with the specific regulatory frameworks relevant to your industry (SOC2 Type II, ISO 27001, HIPAA, PCI-DSS, FedRAMP)? Verify that these certifications apply to the platform globally, helping you maintain consistent compliance whether your data sits in a region hosted by one provider or another.

Encryption and sovereignty: "Secure enough" is not a strategy. Verify that data is strictly encrypted both at rest and in transit. The critical differentiator is Bring Your Own Key support. True data sovereignty also means you control the encryption keys, so that neither the vendor nor a compelled third party can access your data without your explicit authorization. For organizations facing data residency requirements (EU GDPR, financial services, healthcare), evaluate Hold Your Own Key, where keys never leave your infrastructure, and platforms supporting jurisdiction-aligned multi-cloud architectures.

Data Security Posture Management (DSPM): You cannot protect what you do not understand. A modern platform should go beyond simple storage and offer DSPM capabilities to automatically discover and classify sensitive data (personally identifiable information, private health information, payment card industry information) across your multi-cloud ecosystem. Intelligence on data sensitivity helps you make smarter, cost-efficient policy decisions by applying stringent protection to high-value assets while optimizing costs for lower-priority data.



The Cloud Data Protection Checklist

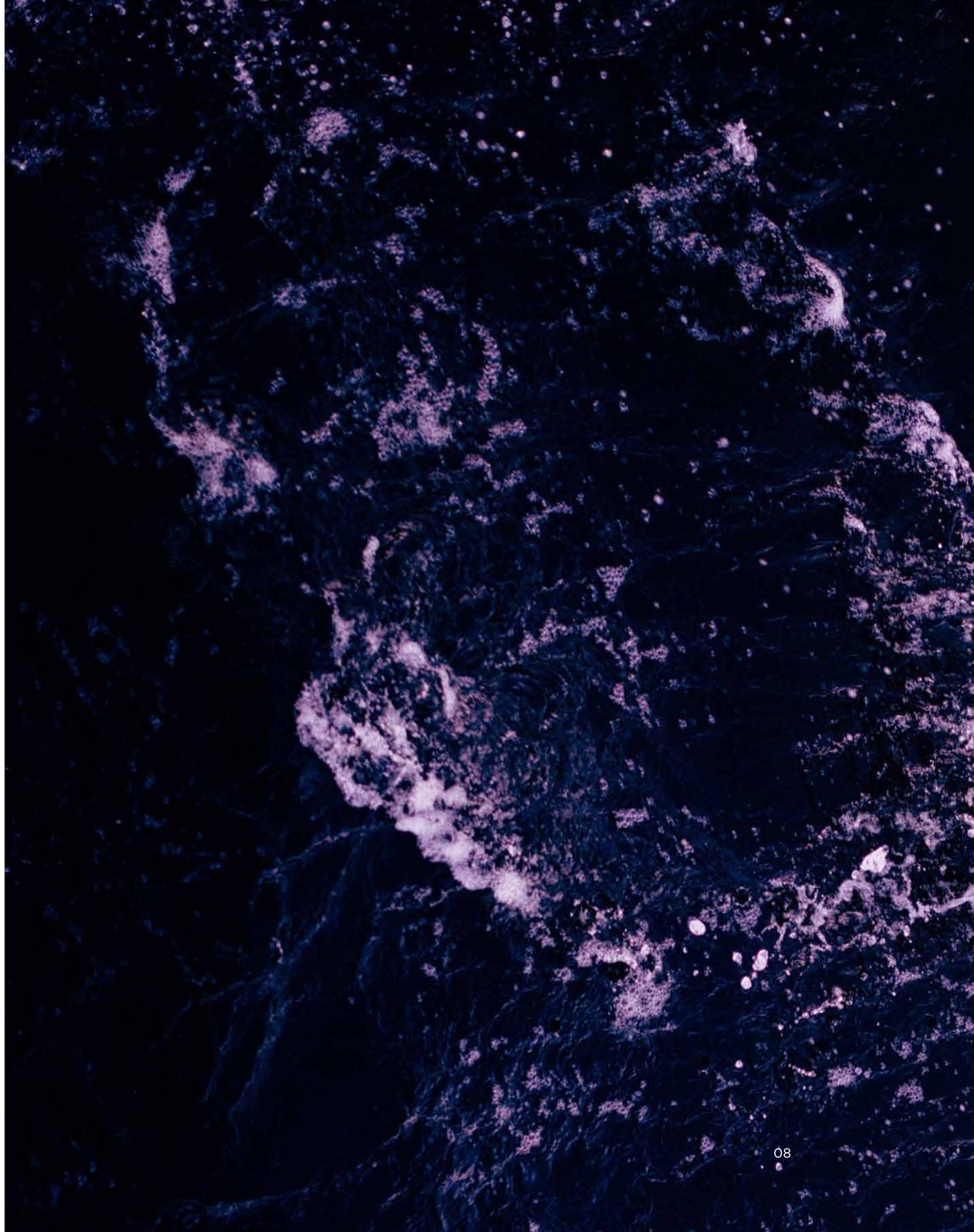
Multi-cloud data resilience has evolved from a tactical IT function into a strategic imperative that demands board-level attention. The seven criteria outlined in this report provide a comprehensive framework to help you when evaluating solutions:

- Backup cost control
- Flexible recovery
- ResOps-ready
- Early warning systems (Left of Bang)
- Post-event orchestration (Right of Bang)
- Platform ecosystem maturity
- Foundational security

Organizations that establish mature resilience practices now will define operational standards for their industries. Those that defer may accumulate technical debt and risk exposure that becomes increasingly expensive to remediate.

The mandate is clear: Multi-cloud environments require multi-cloud resilience. Organizations that move decisively will be better positioned to handle whatever comes next.

To understand where your organization currently stands on the resilience maturity spectrum, download the Multi-Cloud Resilience Maturity Model at **readiverse.com/multi-cloud-resilience.**



Additional Resources

Summary Multi-Cloud Resilience Checklist at **readiverse.com/multi-cloud-resilience**.

Multi-Cloud Resilience Maturity Model:
Assess your current capabilities and identify priority gaps at **readiverse.com/multi-cloud-resilience**.

Join the Readiverse Community – connect with CIOs and CISOs building resilient multi-cloud operations at **readiverse.com**.

This Readiness Report was prepared based on analysis of multi-cloud resilience requirements, procurement best practices, and enterprise security frameworks.

Published: March 2026 | © 2026 Commvault.