The Rise of Cloud Application Infrastructure Recovery (CAIRS)

Why Gartner's New CAIRS Category Signals a Shift in Enterprise Disaster Preparedness

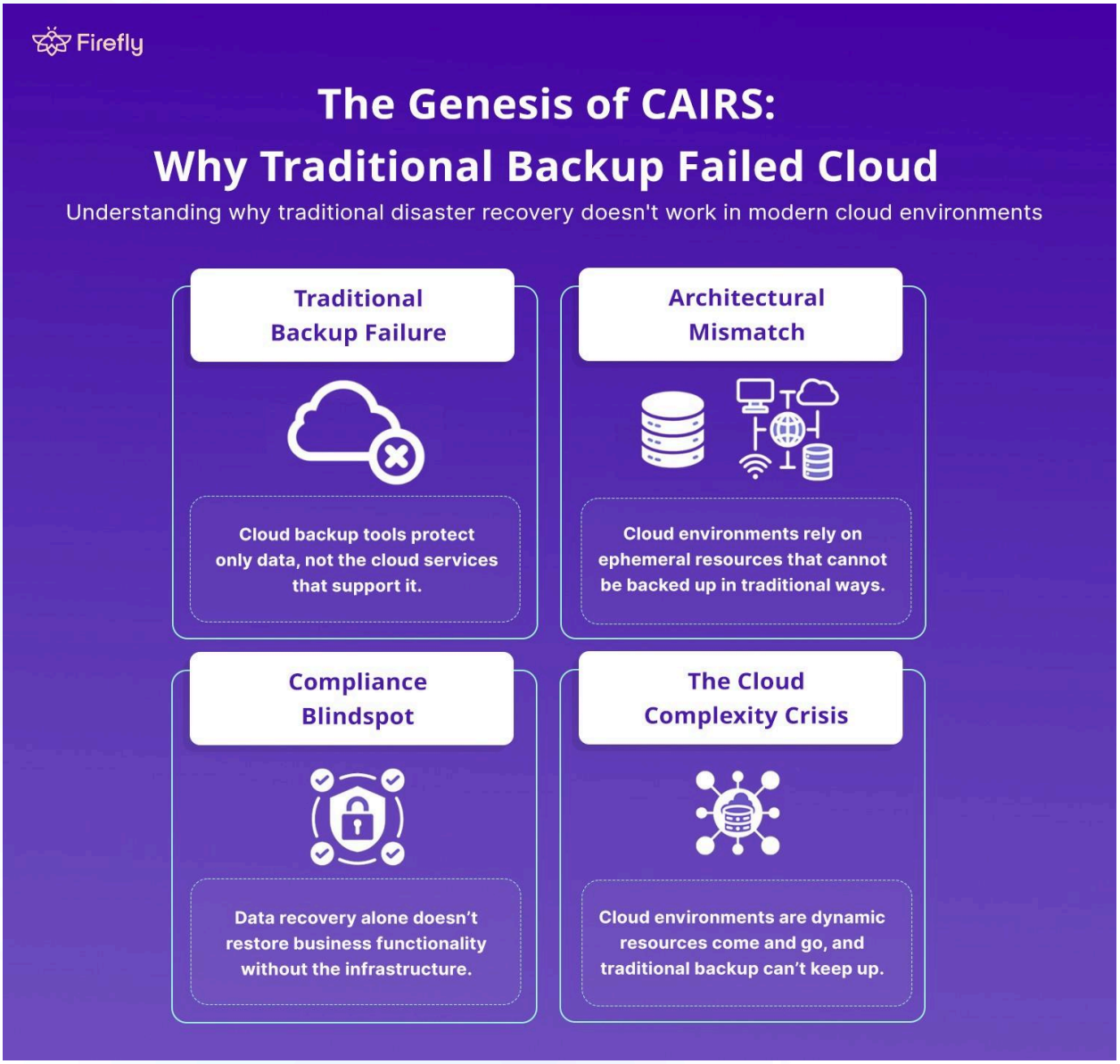
Executive Summary

The enterprise disaster recovery landscape has reached a critical inflection point. Gartner's new Cloud Application Infrastructure Recovery (CAIRS) category in their 2025 Hype Cycle for Backup and Data Protection Technologies signals that traditional backup approaches are fundamentally inadequate for modern cloud environments.

This white paper examines why Gartner established this category and how leading organizations are moving beyond data backup to comprehensive infrastructure recovery through Infrastructure-as-Code (IaC). With only three vendors recognized by Gartner in the category (including Firefly), CAIRS represents both a market opportunity and an urgent call to action for enterprises whose cloud infrastructure remains vulnerable to failure in the face of disaster.

Table of Contents

The Genesis of CAIRS: Why Traditional Backup Failed Cloud



Gartner's creation of the Cloud Application Infrastructure Recovery category emerged from harsh reality: one where traditional disaster recovery has fundamentally broken down in cloud environments. Gartner's research shattered the illusion that traditional data protection works in modern cloud environments:

"Cloud and third-party backup tools typically protect only the underlying data of an application, but not all dependent cloud services."

Modern applications exist as complex ecosystems of ephemeral resources that appear and disappear based on demand. When disaster strikes, database backups mean nothing if auto-scaling groups and security policies have disappeared.

Gartner identifies the core problem:

"Organizations' use of multiple clouds has complicated efforts to consistently enforce and apply proper data protection strategies."

Businesses spend millions recovering databases while ignoring the infrastructure required to run applications.

When disaster strikes, they discover that data means nothing without the auto-scaling groups, load balancers, and security policies that make applications function.

The Hidden Crisis in Modern Cloud Disaster Recovery

Recent high-profile failures (Think: Microsoft Azure's automation failures, Google Cloud deleting UniSuper's entire account, GitHub breaking critical workflows, or the AWS outage) all reveal the same fundamental problem: organizations cannot reliably recover complex cloud infrastructure.

Crisis #1: The Scale of Cloud Dependency

Enterprise cloud dependency has reached critical levels. Multi-cloud deployments create fragmentation and complexity, while 90% of companies use IaC but lack resources to implement it successfully. These aren't operational challenges. They're existential risks where infrastructure failures eliminate entire business capabilities.

Crisis #2: The Recovery Time Disconnect

Gartner identifies a critical disconnect between expectations and reality. One Accenture client cut recovery time from 26 days to 16 hours using automated, IaC-based rebuilds: a 38x improvement. The key insight? The prerequisite for fast rebuild: a trusted, executable blueprint of every asset kept outside the blast radius. IaC is that blueprint.

Crisis #3: The Ransomware for Infra Problem

Modern ransomware targets infrastructure, not just data. Response requires re-instantiating clean environments quickly, reliably, and securely. Traditional backup approaches, designed for data restoration, are completely inadequate for rebuilding entire infrastructures from scratch.

CAIRS Defined: Beyond Data to Infrastructure

Gartner defines Cloud Application Infrastructure Recovery as solutions that "automate the discovery of application blueprints to identify the dependencies of all cloud services, data, and configurations required to rebuild, replicate, and recover applications." This represents a fundamental shift from data-centric to infrastructure-centric recovery.

The Four Pillars of Effective CAIRS

1. **Comprehensive discovery** maps dependencies between services, applications, and data across multi-cloud environments. This includes continuous visibility into infrastructure relationships, tracking configuration drift in real-time, and maintaining awareness of external dependencies that traditional backup ignores.
2. **Infrastructure codification** converts live infrastructure into executable IaC rather than backing up ephemeral resources. This generates clean, deployable code for complex patterns while maintaining version control and supporting multiple IaC frameworks.
3. **Automated recovery** enables rapid rebuild capabilities through push-button deployment, cross-cloud recovery support, CI/CD integration, and comprehensive rollback verification: separating CAIRS from traditional disaster recovery.
4. **Governance and compliance** ensures infrastructure recovery meets enterprise requirements through consistent policy enforcement, comprehensive audit trails, and support for regulatory requirements increasingly focused on infrastructure resilience.

The Business Case for Infrastructure Recovery

DR-as-code treats disaster recovery as a software engineering problem rather than backup and restore, representing the most significant evolution in disaster recovery thinking since automated backup systems. Traditional disaster recovery asks: "How do we restore our systems to their previous state?" DR-as-Code asks: "How do we rebuild our systems to an optimal functional state?"

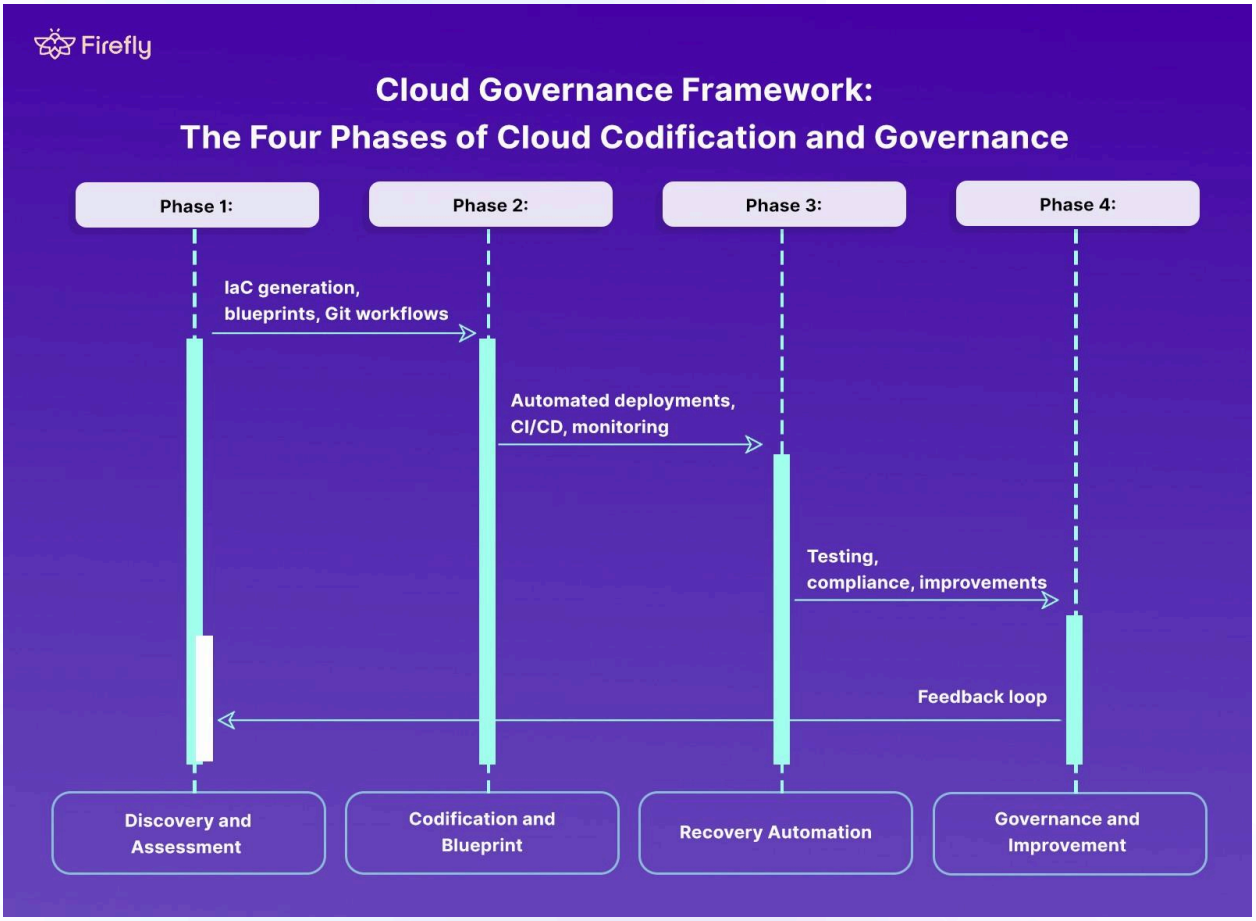
The implications of inadequate cloud disaster recovery create a perfect storm of increasing dependency, complexity, and inadequate protection that threatens enterprise viability.

Organizations face unprecedented risks from cloud infrastructure failures while continuing to rely on disaster recovery approaches designed for a different reality.

- **Revenue Protection and Business Continuity:** Cloud infrastructure failures eliminate entire business capabilities instantly, halting revenue streams. Years of infrastructure configuration disappear when traditional backup cannot protect these critical assets.
- **Regulatory and Compliance Requirements:** Auditors now scrutinize cloud deployments for disaster recovery capabilities. SOX, GDPR, and industry standards increasingly require infrastructure resilience that traditional backup cannot address.
- **The Cost of Inaction:** Recovery times measured in weeks represent threats to customer relationships. Clean data backups mean nothing without the ability to rebuild infrastructure, creating competitive disadvantages that grow as operational gaps widen.

The Implementation Framework: From Backup to Recovery

The transition from traditional backup to comprehensive infrastructure recovery requires a structured approach addressing technical, operational, and organizational challenges.



Phase 1: Infrastructure Discovery and Assessment

- **Comprehensive Asset Discovery** scans all multi-cloud resources with configuration details, security policies, and operational metadata. Discovery must be continuous.
- **Dependency Mapping** identifies relationships between infrastructure components and business applications, including technical and business dependencies.
- **Application-Centric Organization** structures infrastructure around business applications rather than technical components, enabling recovery focused on restoring business capabilities through comprehensive tagging and priority classification.

Phase 2: Infrastructure Codification and Blueprint Creation

- **Automated Code Generation** converts existing infrastructure into clean, deployable IaC using Terraform, Pulumi, CloudFormation, etc. Code must be maintainable with modular components and reusable patterns.
- **Blueprint Development** creates comprehensive deployment procedures for each application, including dependencies and validation. Blueprints require regular automated testing through complete and partial deployment scenarios.
- **Version Control Integration** manages infrastructure code through Git-based workflows with automated testing and deployment pipelines.

Phase 3: Recovery Automation and Integration

- **Automated Deployment Systems** provide push-button recovery with cross-account, cross-region, and cross-cloud capabilities, and validation of deployed infrastructure.
- **Workflow Integration** connects recovery with existing CI/CD pipelines and GitOps processes, enabling self-service recovery capabilities for development teams.
- **Monitoring Enhancement** implements continuous infrastructure state monitoring with automated alerting for configuration drift and policy violations.

Phase 4: Governance, Testing, and Continuous Improvement

- **Regular Testing** validates recovery capabilities through automated, scheduled deployment testing and application functionality verification.
- **Compliance Maintenance** ensures regulatory requirements through detailed logging of infrastructure changes, recovery procedures, and testing activities.
- **Continuous Improvement** establishes procedures for reviewing and updating recovery capabilities as infrastructure evolves, incorporating industry best practices and lessons learned.

Firefly, CAIRS, and The Future of Cloud Resilience

Gartner's creation of the CAIRS category signals several transformative trends that will reshape enterprise infrastructure management over the next decade, and perhaps farther.

The future of cloud resilience will be characterized by organizations that treat infrastructure as software, recovery as deployment, and disasters as opportunities for improvement. Those that continue to rely on traditional backup approaches will find themselves increasingly set back by operational complexity, reliability challenges, and recovery capabilities that comprehensive automation platforms like Firefly solve elegantly and efficiently.

Learn more about Firefly's CAIRS capabilities here.