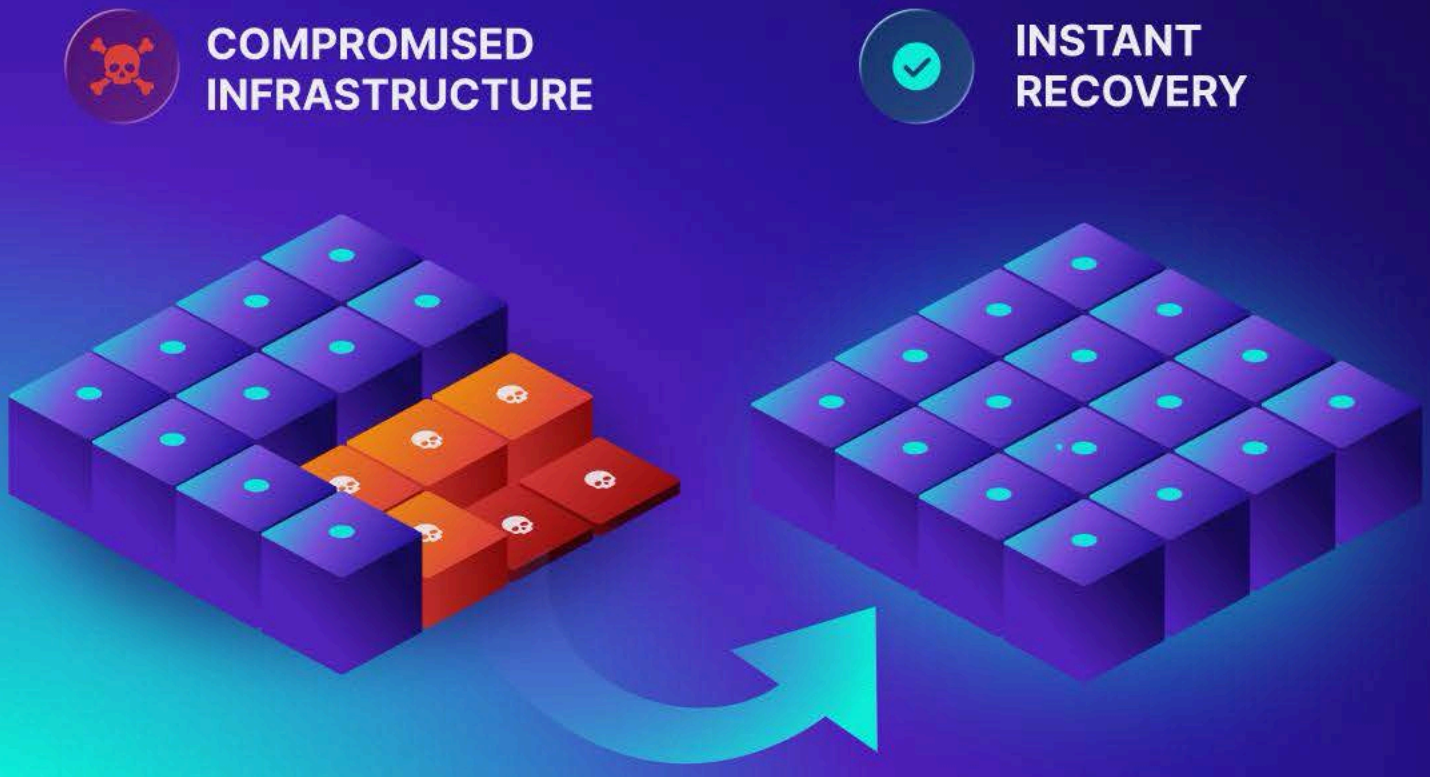
Firefly

firefly.ai

The Buyer's Guide to Cyber Resilience for Cloud Applications

Why Data Backup Alone Can't Save Your Business
(And What Comes Next)



Firefly

The Buyers's Guide To Cyber Resilience For Cloud Applications

Why Data Backup Alone Can't Save Your Business (And What Comes Next)

Table of Contents

Executive Summary

In March 2026, a cyberattack shut down Stryker's global operations. It wasn't until nearly a month later that the company confirmed in an SEC filing that it was fully operational again. This followed an AWS outage in late 2025 (among others) that had already taken down 1,000+ companies for 15 hours. And that was not because data was lost, but because the infrastructure collapsed, and no one had a plan for that.

Now add AI agents into the mix, and the blast radius gets bigger. Agents that provision, modify, and delete infrastructure autonomously can take down in seconds what used to take a human hours to break.

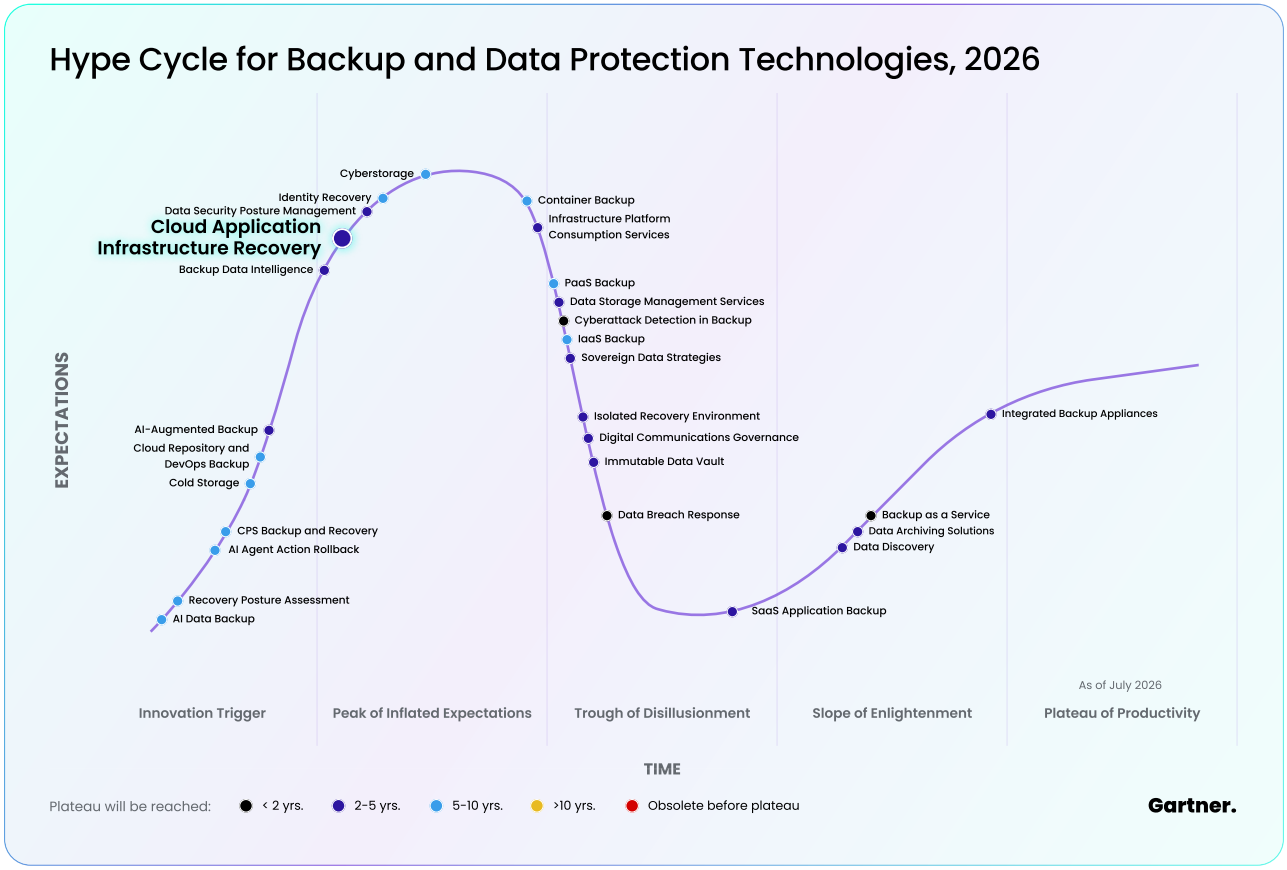
This is the backup industry's most disheartening secret: they protect your databases, but not the VPCs, IAM roles, load balancers, and dozens of additional resources from the configuration layer that make your applications run. When your infrastructure isn't available, there's no business continuity.

For years, the industry assumes that Disaster Recovery & Business Continuity is the same as backing up data. Modern cyber attacks, increases in cloud outage frequency, and the risk of AI Agents deleting and/or changing infrastructure makes it clear that backups alone aren't sufficient anymore

Resilience is not about backups; it's about bringing your business applications back, quickly. This buyer's guide explains what that looks like, and how leading organizations are getting there.

Why Traditional Backup Failed Cloud

Gartner's 2026 research on CAIRS, Cloud Application Infrastructure Recovery, shattered a comfortable illusion: that traditional data protection tools work in modern cloud environments. The reality is harder: cloud and third-party backup tools typically protect *only* the underlying data of an application, but not all dependent cloud services.



This insight from Gartner shouldn't come as a surprise, then.

> **"Gartner predicts that by 2030, 35% of organizations will utilize CAIRS solutions to complement infrastructure as code (IaC) disaster recovery orchestration, up from less than 5% in 2026: [a 10x jump].** (Top Trends in Backup and Data Protection for 2026, Michael Hoeck, March 12, 2026)
>
> - Gartner

Modern applications are complex ecosystems of resources like auto-scaling groups, security policies, load balancers, and dozens of interconnected services. They all appear and disappear based on demand. When disaster strikes, a clean database backup is useless if the infrastructure that runs the application no longer exists. Over time, more business logic has shifted away from VMs running custom code and into managed infrastructure. This shift is even sharper in AI applications: instead of executing your own code, the app calls out to something like AWS Bedrock or Google Vertex AI, and the infrastructure becomes the business logic, not just the thing that hosts it.

Multi-cloud adoption has compounded the problem. Gartner identified the core issue:

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

Using 3rd party tools on top of a multi-cloud estate - like Cloudflare for CDN, Datadog for Observability, and Okta for Identity - creates an even larger hole in many teams' Business Continuity and Cyber Recovery strategies.

Businesses spend millions recovering databases while ignoring the infrastructure required to run applications, only to discover the gap when it is too late. The question isn't "Do we have backups?", rather it is "Can we recover?". These are not the same.

Why Prevention Fails in the AI Era, and Why Cyber Resilience Is a Must

For two decades, security strategy has aimed at one goal: stopping the attack before it lands. AI has made that goal unattainable, and the industry has largely conceded the point: measuring security success by breach prevention no longer reflects reality, because prevention at scale is no longer achievable.

The reason is structural. Prevention was always an unfair fight, as the attacker needs one working path, and the defender has to secure every one. AI widens that gap, letting attackers map, exploit, and hunt at a scale and speed no defensive team can match. Worse, it runs on a clock defenders can't keep: when an attack executes at machine speed, a defense waiting for a human to review and approve is simply too slow.

Security leaders have drawn the conclusion. Board-level investment is shifting from prevention alone toward response and recovery, driven by an "assume breach" mindset that treats a serious incident as a matter of when, not if. That shift has a name: cyber resilience, which NIST defines as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, attacks, or compromises.

Prevention lowers the odds of an incident; resilience determines its cost. Because the modern business runs on cloud infrastructure, not just the data inside it, resilience comes down to one capability: rebuilding that infrastructure quickly, reliably, and on demand. That is the premise for everything that follows.

The Hidden Crisis in Disaster Recovery

Recent high-profile failures (Think Microsoft Azure automation failures, Google Cloud deleting UniSuper's entire account, GitHub breaking critical workflows, an AI coding agent wiping **PocketOS's production database and its backups in under 10 seconds, Amazon's Kiro agent triggering a 13-hour AWS outage, a wiper attack disrupting Stryker's global operations,** and the latest AWS outage) all reveal the same problem: organizations cannot reliably recover complex cloud infrastructure when it matters most.

Crisis 1

IaC Adoption and Coverage ≠ Recovery Readiness

Enterprises now run on multi-cloud by default, and that default has a cost: fragmented environments, inconsistent controls, and infrastructure sprawl no single team fully understands. Most companies have adopted Infrastructure-as-Code to manage it, but few have the resources to use it as a real recovery tool. That gap between "we have IaC" and "we can actually rebuild from it" is the difference between a bad day and losing a business capability overnight.

Crisis 2

The Recovery Time Disconnect

There is a significant gap between what teams expect recovery to take and what it actually requires. Manual, undocumented rebuilds routinely stretch into weeks: one Accenture client faced a 26-day recovery timeline before automating the process, eventually cutting it to 16 hours. That's a 38x gap between where most teams start and where they need to be. The prerequisite: a trusted, executable blueprint of every asset, stored outside the blast radius. Infrastructure-as-Code is that blueprint.

Crisis 3

Ransomware Targets Infrastructure, Not Just Data

Modern ransomware attacks infrastructure directly. Effective response requires re-instantiating clean environments quickly, reliably, and securely. Traditional backup approaches, which are designed for data restoration, are completely inadequate for rebuilding entire infrastructures from scratch under time pressure.

Infrastructure Recovery: Beyond Data

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 Infrastructure Recovery

Comprehensive discovery maps dependencies between services, applications, and data across multi-cloud environments, including continuous visibility into infrastructure relationships, real-time configuration drift tracking, and external dependencies traditional backup ignores.

Infrastructure codification converts live infrastructure into executable IaC rather than backing up ephemeral resources, generating clean, deployable code while maintaining version control across multiple IaC frameworks.

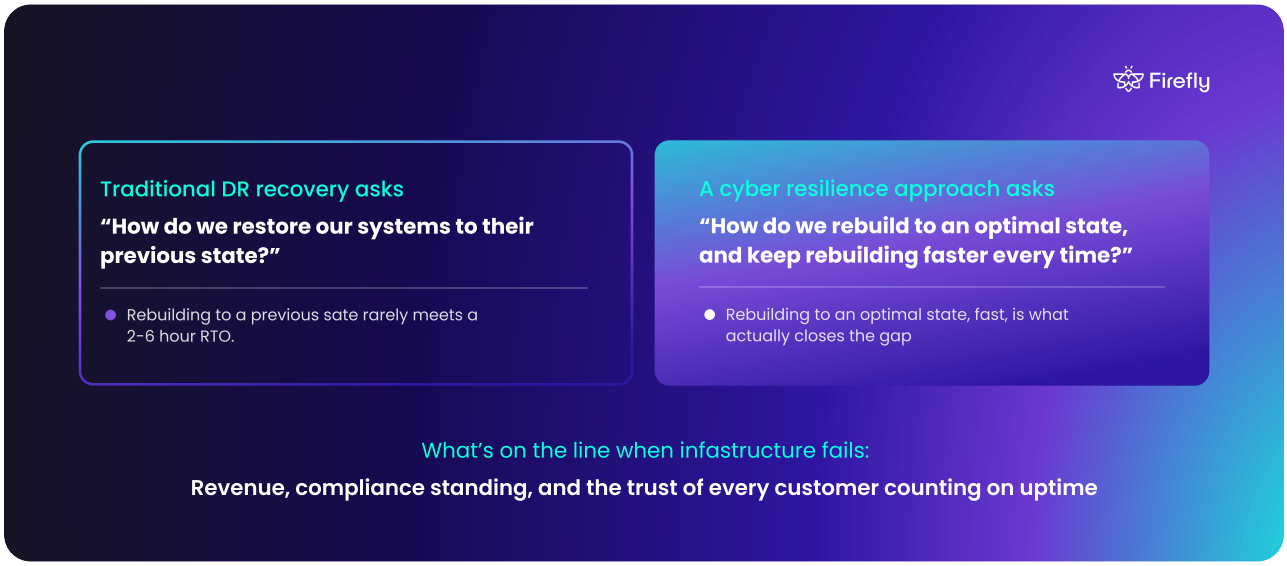
Automated recovery enables rapid rebuild through push-button deployment, cross-cloud recovery support, CI/CD integration, and comprehensive rollback verification.

Governance and compliance ensures recovery meets enterprise requirements through consistent policy enforcement, audit trails, and support for regulatory standards increasingly focused on infrastructure resilience.

What To Look For When You Buy

Cloud and cyber resilience treat disaster recovery as a software engineering problem, not a backup-and-restore task. That shift, from restoring data to rebuilding infrastructure, represents the most significant evolution in how infrastructure recovery purchases are evaluated. DR-as-Code is how that shift gets implemented in practice.

1. **Revenue Protection and Business Continuity:** Cloud infrastructure failures eliminate entire business capabilities instantly, halting revenue streams. Years of infrastructure configuration can disappear when traditional backup lacks the scope to protect it.
2. **Regulatory and Compliance Requirements:** Auditors now scrutinize cloud deployments for disaster recovery capabilities. DORA, NIST, SOX, GDPR, and evolving industry standards increasingly require proof of infrastructure resilience that traditional backup cannot address.
3. **Industry Requirements:** Most enterprises commit to 2-6 hour RTOs to customers and partners. Rebuilding to a "previous state" rarely gets there in time. Rebuilding to an optimal state, fast, is what actually closes the gap.
4. **The Cost of Inaction:** Recovery times measured in weeks threaten customer relationships and competitive position. Clean data backups mean nothing without the ability to rebuild the infrastructure that runs the application.



Implementation Framework: Strengthen. Recover. Prove.

Phase 1: Strengthen. Make the environment recoverable before anything fails

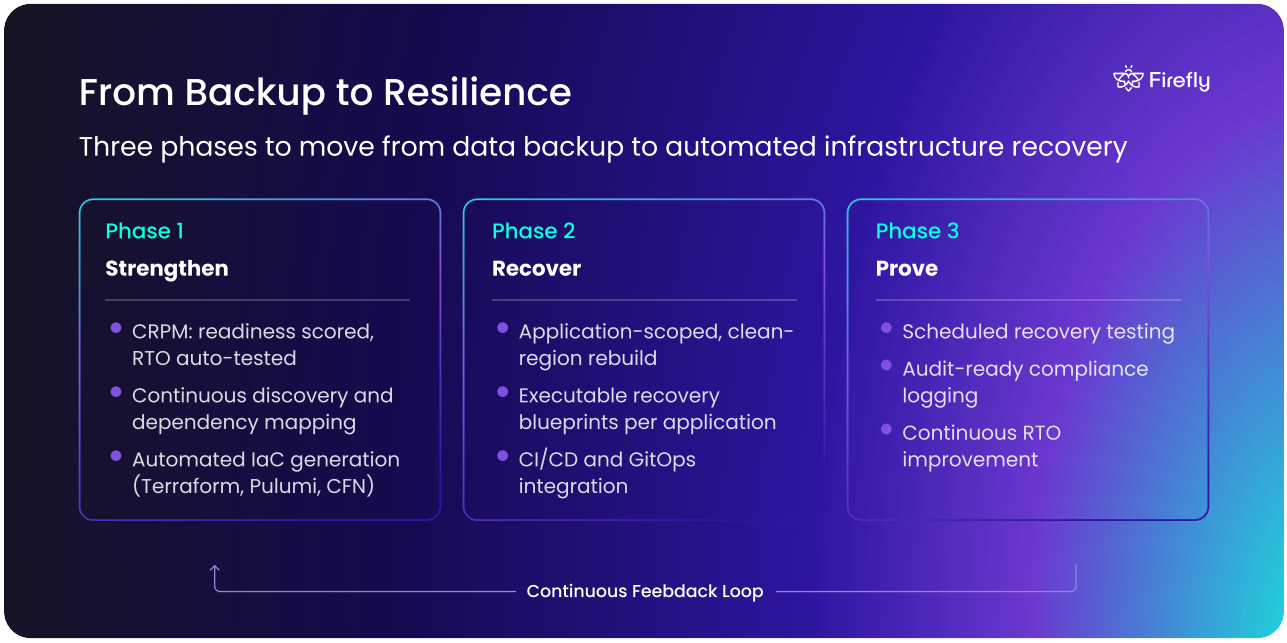
- **Cloud Resilience Posture Management (CRPM)** scores every asset on restore readiness and auto-tests RTO before an incident, so RTO becomes a number you can commit to.
- **Comprehensive Discovery and Dependency Mapping** continuously discovers every resource across your clouds and maps the relationships between them, so you know exactly what a rebuild has to bring back.
- **Automated Code Generation** converts existing infrastructure into deployable IaC in Terraform, Pulumi, CloudFormation and other frameworks.
- **Drift and Policy Remediation** detects where live infrastructure has diverged from its code and closes the gap, and fixes policy violations before they spread, so a rebuild reproduces a compliant environment.

Phase 2: Recover. Rebuild complete environments in minutes, not weeks

- **Application Blueprints** are scoped from a single resource: Firefly follows the dependency map to define the application boundary and snapshots everything inside it as deployable IaC.
- **Clean-Environment Rebuild** deploys that IaC into an isolated region or account the attacker can't reach, and any earlier snapshot can be selected to roll back to a pre-breach state, with snapshots immutable so ransomware can't encrypt them.
- **Pipeline Integration** runs recovery through your existing CI/CD pipelines and GitOps processes, so development teams recover their own applications using tools and approvals already in place.
- **RTO Under One Hour** with no manual runbooks, so recovery is measured in minutes rather than in lost business days.

Phase 3: Prove. Turn recovery readiness into evidence

- **Scheduled Recovery Testing** restores into a test environment on a schedule and validates the result providing evidence for leadership.
- **Audit-Ready Logging** records every change, recovery action and test, so evidence for DORA, NIS2, SOC 2, ISO 27001, HIPAA, PCI-DSS, NIST, SOX and GDPR is ready the moment an auditor asks.
- **Continuous Improvement** feeds each test and incident back into recovery readiness, reducing RTO over time.



The Future of Cyber Resilience

Cloud and Cyber resilience are no longer a backup problem. They are an infrastructure problem, and solving it requires treating recovery with the same rigor, automation, and continuous improvement applied to the rest of the software development lifecycle.

The organizations that get there first will share a few things in common: they treat infrastructure as software, recovery as deployment, and every incident as an opportunity to strengthen their systems. Those still relying on traditional backup will find the gap widening: in recovery time, compliance posture, and resilience against the threat types that are already here.

Firefly is built for this shift. Recognized by Gartner in the Cloud Application Infrastructure Recovery category, Firefly rebuilds complete environments from Infrastructure-as-Code into a clean, isolated region the attacker can't reach, with rollback to any pre-breach state in under an hour. Firefly strengthens that readiness before an attack and proves it afterward, with recovery validated continuously rather than assumed.

Ready To Make Your Cloud Resilient?

Schedule a 30 Minute call with Firefly

Book Demo