CYERA

From blind spots to continuous control: How a fast-growing Fintech company rebuilt data-security visibility in less than 30 days

A high-velocity fintech, processing billions in payments and subject to a plethora of new state privacy statutes, operates entirely in the cloud. A lean security team supports hundreds of micro-services in AWS and GCP, thousands of S3 buckets, petabyte-scale Splunk logs, and more than 100 SaaS applications.

The CISO leading the program has spent two decades at global brands (Walmart, eBay, Palo Alto Networks, Twitter, Rubrik) and knew first-hand that **data ambiguity is the root of most modern security failures.**

Challenges the team Faced:

Zero authoritative inventory.
Each new service, SaaS integration or analytics pipeline created a fresh data store, but no central record of *what* was inside.

Manual, error-prone discovery.
Ad-hoc scans and developer surveys took weeks and still missed hidden copies, especially in third-party tools.

Escalating regulatory pressure.
Privacy and Legal needed defensible evidence that sensitive data was located, classified, and protected.

Evaluating Solutions

The team evaluated traditional DLP and DSPM add-ons but ruled them out: regex-heavy tuning, limited SaaS reach, and deployment times measured in quarters. Cyera stood out because it delivered:

The Journey Deploying Cyera

1. Stakeholder alignment

Security, Privacy, and Legal jointly approved the read-only access model—no production downtime, no code changes.

2. Connection & first scan

Within two hours, Cyera ingested CSP IAM roles, SaaS OAuth tokens, and log-source metadata.

3. Early “aha” moments (week 1)

Detected raw customer addresses inside Splunk debug logs generated by a mis-configured micro-service.

Flagged credit-card numbers stored in a collaboration tool’s attachment history, violating PCI segmentation rules

4. Process integration (weeks 2-4)

Findings auto-ticketed to Jira; developers pushed fixes that masked or purged the offending data

Continuous scanning confirmed remediation and prevented regressions.

Total time from first connector to actionable insights: **<30 days.**

FinTech Company’s Results

- **Access to a complete data map:**
  Unknown stores dropped and every bucket, database and SaaS repository now catalogued.
- **Faster classification:**
  What once took days per store now finishes in minutes, enabling weekly risk reviews instead of quarterly.
- **Incident prevention:**
  3x as many potential sensitive-log exposures caught *before* they left production.
- **Cross-functional cohesion:**
  Shared dashboards that gave Privacy and Legal the same evidence as Security

“Cyera gave us the map, the context, and the automation to fix issues before they turned into incidents, without adding headcount.”

— Chief Information Security Officer, Fintech customer

Cyera turned months of blind-spot hunting into minutes of continuous assurance, demonstrating that modern DSPM is no longer optional for cloud-first, regulation-bound enterprises.