Securing Market-Sensitive Media Assets with GenAI-powered CloudPosture

Customer Case Study

April 2026

Executive Summary

LAMDA Development S.A. — listed on the Athens Exchange and recognised by TIME magazine as one of the world's 100 most influential companies — is Greece's leading real estate developer and the force behind **The Ellinikon, Europe's largest urban regeneration project ($8 billion, 6.2 million m²)**.

LAMDA Development built a **Media Management Portal on AWS** — designed and implemented by LCM Go Cloud — to centralise tens of thousands of videos and media assets for The Ellinikon project. The portal handles market-sensitive pre-release content whose unauthorised disclosure could affect the company's share price.

With no structured security assessment, no forensic visibility into media asset access, and growing GDPR and corporate governance obligations, LAMDA Development engaged **LCM Go Cloud** to assess and harden the portal's security posture using CloudPosture — a GenAI-powered CSPM platform.

Within approximately 10 weeks, LCM Go Cloud deployed an enhanced AWS security baseline, **performed a 644-check assessment across 7 compliance standards, achieved Grade B or above across all frameworks**, and established continuous monitoring — delivering the first auditable security report to the company's audit committee.

About Lamda Development

Greece's leading real estate developer, behind Europe's largest urban regeneration project

Industry

Real Estate Development & Investment

Market

Athens Exchange (ATHEX: LAMDA)

The Ellinikon

$8B project, 6.2M m², Athenian Riviera

Portfolio

4 shopping centres, 3 marinas, offices, residences

Recognition

TIME 100 Most Influential Companies (2024)

Regulation

GDPR, Athens Exchange governance, HCMC

The Business Challenges

Protecting market-sensitive content for a publicly listed company on the Athens Exchange

No Security Assessment

No structured methodology for evaluating the portal's security posture. Misconfigurations, unencrypted volumes, and overly permissive IAM policies accumulated over two years of portal development.

Zero Forensic Visibility

No audit trail for media asset access. If a pre-release Ellinikon rendering was leaked, there was no way to trace who downloaded the file, when, or from where.

GDPR & Governance Obligations

As a publicly listed company, LAMDA Development must demonstrate cybersecurity due diligence to its audit committee, the Athens Exchange, and the Hellenic Capital Market Commission.

Share Price Exposure

Unauthorised disclosure of embargoed investor materials or pre-release content could directly affect the share price of a company that has raised €1.35B through capital markets since 2014.

The Solution

A three-layer approach: AWS Security Baseline + CloudPosture CSPM + Media Asset Protection

Layer 1 — AWS Security Baseline

- CloudTrail — KMS encrypted, S3 data events, Insights, CloudWatch Logs
- AWS Config — continuous recording since April 2023
- GuardDuty — 1-hour finding frequency, all protection features
- Security Hub — FSBP v1.0.0 & CIS v3.0.0
- Inspector v2 — 4 scan types for vulnerabilities
- IAM hardening — MFA, least privilege, credential hygiene
- Codified in CloudFormation for audit committee

Layer 2 — CloudPosture Platform

- 644 security checks via 19 specialised agents
- 7 compliance standards: GDPR, ISO 27001, SOC 2, CIS v3/v5, NIST 800-53, FSBP
- 22 cost optimisation agents
- GenAI remediation (CLI, Terraform, CFN)
- Toxic combination detection with AI
- 7 AWS services unified in one dashboard
- Weekly automated scans with trend tracking

Layer 3 — Media Asset Protection

- Network micro-segmentation: web, app, and data tiers separated
- S3 bucket policies with role-based access per team function
- SSE-KMS encryption at rest for all media assets
- CloudTrail S3 data events: every file access recorded with identity & IP
- GuardDuty anomaly detection on S3 access patterns
- Defence-in-depth: preventive, detective, and forensic controls

Key Capabilities Deployed

Multi-Standard Compliance

644 checks mapped to 7 standards: CIS v3/v5, NIST 800-53, ISO 27001, GDPR, FSBP, SOC 2

GenAI-Powered Remediation

Amazon Bedrock generates executable fix plans in CLI, Terraform, or CloudFormation format

Toxic Combination Detection

Deterministic detection of high-risk misconfigurations with AI explanation of risk chains

7 AWS Services Unified

GuardDuty, Inspector, Shield, Macie, Detective, CloudTrail, Health — one dashboard

Finding Lifecycle Management

Suppress, acknowledge, track, resolve, or risk-accept with audit trail and time-bound expiry

Continuous Monitoring

Weekly scans, compliance drift detection, critical finding alerts, score trending for audit committee

Solution Architecture

LAMDA Development AWS Account (eu-central-1)

Media Management Portal

- CloudFront + Shield
- EC2 (WordPress)
- RDS MySQL
- S3 Media Buckets (50+ TB video assets)
- WorkSpaces + AD

AWS Security Services Baseline (CFN)

- **CloudTrail** KMS + S3 data events + Insights
- **AWS Config** Continuous recording (2+ yrs)
- **GuardDuty** 1-hour freq, all features
- **Security Hub** FSBP + CIS v3.0
- **Inspector v2** 4 scan types
- **KMS + IAM** Customer key + least privilege

Security Telemetry → CloudTrail events · Config changes · GuardDuty threats · Inspector vulns → Security Hub

Forensic Audit & Detection Pipeline

Real-time: CloudWatch metric filters (seconds) · Near-real-time: GuardDuty hourly findings · Periodic: CloudPosture weekly scans

Every S3 media asset access recorded: caller identity · source IP · timestamp · IAM role

GDPR — EU Data Residency (Frankfurt)

Read-Only IAM Creds

LCM Go Cloud Account (eu-central-1)

CloudPosture CSPM Platform

19 Security Agents · 644 checks

7 Standards · 16,400+ mappings

22 Cost Agents

Toxic Combination Detection

Finding Lifecycle Management

Service Sync & Dashboard

GuardDuty · Inspector · Shield · Macie
Detective · CloudTrail · AWS Health

Amazon Bedrock — GenAI Engine (Claude)

AI Remediation · Executive Summary · Toxic Combo AI

Deliverables: Compliance Report · Remediation Plan · CFN Template · Dashboard

LCM GO CLOUD · aws PARTNER Advanced Tier Services

APPLIED GenAI

Governance Transformation

From zero visibility to board-level security governance in 10 weeks

Before

- ✗ No structured security assessment of the portal's AWS environment
- ✗ Zero forensic visibility — no audit trail for media asset access
- ✗ CloudTrail captured bucket-level events only, no object-level access
- ✗ GuardDuty on default 6-hour finding frequency
- ✗ No compliance scores, no reports, no audit committee visibility
- ✗ Ad-hoc security reviews — security was an invisible IT function
- ✗ Overly permissive IAM policies accumulated over 2 years

After

- ✓ Grade B or above across all 7 compliance standards, FSBP at Grade A
- ✓ 100% forensic visibility — every S3 object access logged with identity & IP
- ✓ KMS-encrypted CloudTrail with S3 data events, Insights, CloudWatch Logs
- ✓ GuardDuty at 1-hour frequency — 83% faster threat detection
- ✓ Quarterly audit committee reports with AI Executive Summary
- ✓ Security became a visible corporate governance activity with board accountability
- ✓ IAM least-privilege enforced per team function (press, IR, marketing, agencies)

Outcomes & Results

B+
Compliance Grade Achieved
across 7 standards

644
Security Checks Automated
19 agents, weekly scans

100%
Forensic Visibility on Media Assets
every S3 object tracked

- ✓ All CRITICAL and HIGH severity findings resolved across the environment
- ✓ First auditable multi-framework compliance report delivered to the audit committee
- ✓ Quarterly security governance cadence established with AI Executive Summary
- ✓ All foundational AWS security services enabled, hardened, and codified in CloudFormation
- ✓ Three-layer detection pipeline: real-time (seconds), near-real-time (1 hour), periodic (weekly)
- ✓ Complete forensic capability to investigate any suspected media asset leak
- ✓ Security transformed from invisible IT function to visible board-level governance

Delivery Timeline

From discovery scan to continuous monitoring in approximately 10 weeks

W1–W2

Discovery & Baseline Scan

Free Discovery Scan, full 644-check assessment, 7-standard compliance scoring, initial audit gap identification

W2–W4

Security Services Deployment

CloudFormation baseline, enhanced CloudTrail with KMS + S3 data events, GuardDuty, Inspector, Config

W4–W8

Remediation & Hardening

AI-guided remediation of CRITICAL/HIGH findings, IAM hardening, S3 encryption, micro-segmentation

W8–W10

Validation & Monitor Setup

Post-remediation scan, score verification, audit committee report delivery, weekly monitoring activated

Built on a Proven DR Foundation

LCM Go Cloud built the platform AND secured it — end-to-end ownership, one partner

Media Management Platform (existing)

- 50+ TB video files stored in Amazon S3
- AWS Elemental MediaConvert for video processing
- WordPress on EC2 with RDS MySQL backend
- Amazon CloudFront for secure, low-latency delivery
- Amazon WorkSpaces for remote video access
- 55 TB migrated via AWS Snowball in 2 weeks
- Microservices architecture for extensibility
- AI-ready for Amazon Rekognition integration

CloudPosture Security Layer (new)

- 644-check security assessment across 7 standards
- Enhanced CloudTrail: KMS + S3 data events + Insights
- GuardDuty at 1-hour frequency for rapid detection
- Multi-framework compliance scoring (A–F grades)
- GenAI-powered remediation roadmap
- Quarterly audit committee security reports
- Continuous weekly monitoring & drift detection
- Media asset forensic traceability

What Makes This Engagement Unique

TIME 100 Company

One of TIME magazine's 100 most influential companies — any security incident has amplified visibility and reputational impact

Share Price at Stake

Pre-release content for a €1.35B capital markets company — forensic audit trail protects against market-sensitive leaks

Complete Forensic Visibility

Every download of every rendering, every video, every press asset — recorded with caller identity, source IP, and timestamp

End-to-End Ownership

LCM Go Cloud built the Media Management Platform AND secured it — one partner, one SLA, full-stack accountability

Board-Level Governance

First-ever audit committee security report with AI-generated executive summary — quarterly governance cadence established

7-Standard Compliance

GDPR, ISO 27001, SOC 2, CIS v3/v5, NIST 800-53, FSBP — the most comprehensive multi-framework assessment in portfolio

About LCM Go Cloud

Advanced AWS Consulting Partner

Based in Athens, Greece with offices in Cyprus. LCM Go Cloud specialises in Cloud Resilience and GenAI solutions for enterprise clients, with deep expertise in AWS infrastructure, disaster recovery, and AI/ML workloads.

- 8+ active AWS certifications at Professional and Specialty levels
- GenAI solutions delivered across distribution, retail, manufacturing, legal, education, financial services
- CloudPosture is part of the Applied GenAI portfolio — combining cloud security expertise with Bedrock-powered AI
- Production-grade AI on AWS solving measurable business problems for mid-market enterprises
- Full-stack ownership: infrastructure, AI agents, user interface — one partner, one SLA

Let's Talk!

Discover how CloudPosture can secure and optimise your AWS environment.

www.lcmgocloud.com

Costas Kappos
Managing Partner
LCM Go Cloud
T: +306974899318
costas@lcmgocloud.com

Leonidas Tosidis
Managing Partner
LCM Go Cloud
T: +306978890922
leonidas@lcmgocloud.com

Yiannis Nikolarakis
Director Solutions Architect
LCM Go Cloud
T: +306932400019
yiannis@lcmgocloud.com