SECURITY & TRUST

Vidcomply Security & Architecture Overview

A customer-neutral summary of how Vidcomply protects media assets, personal data, processing environments, and compliance outputs.

01

Buyer-owned source

Source media can remain in customer-controlled storage; Vidcomply receives only required permissions.

02

Isolated workloads

Dedicated processing resources, separate queues, least-privilege IAM, and network controls.

03

Agreed region

Deployment location is agreed for residency, security, and latency requirements.

04

No model training

Customer content is processed only for the contracted service and is not used to improve models.

05

Auditable activity

Outputs, processing records, and relevant audit logs can be provided under the agreed access model.

06

Controlled retention

Temporary processing files follow contract-defined lifecycle, return, and deletion procedures.

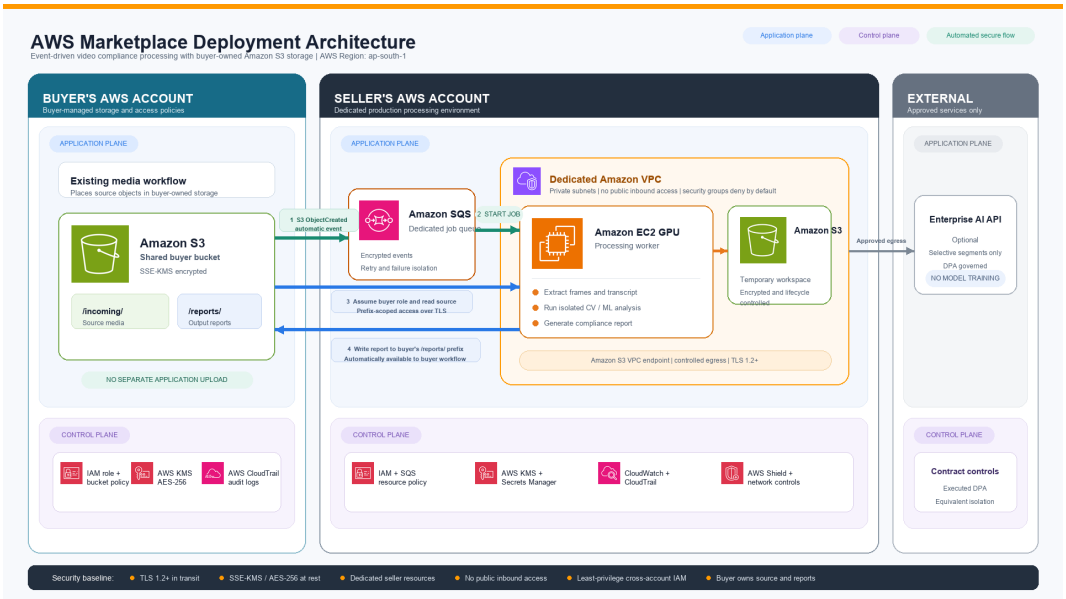
PUBLIC SUMMARY

This document describes Vidcomply's standard control approach. Customer-specific architecture, service providers, regions, and contractual commitments are defined in the applicable Order Form, DPA, and Security Schedule.

01 / REFERENCE ARCHITECTURE

AWS Marketplace deployment pattern

Vidcomply is available through AWS Marketplace. The primary enterprise pattern keeps source media in buyer-controlled Amazon S3 storage, grants only the minimum cross-account permissions required, runs dedicated seller-side processing, and writes reports back to the buyer's designated location.



Reference architecture shown for illustration. The deployment region, customer storage model, enabled services, and integration boundaries are agreed during onboarding.

CUSTOMER CONTROL

Buyer-owned source storage | Dedicated processing | Agreed data residency | Auditable access | No model training | Contractual deletion

Core flow

- A customer-owned storage event initiates a controlled processing job.
- Least-privilege IAM access is scoped to agreed source and report locations.
- Processing runs inside an isolated Amazon VPC with restricted ingress and controlled egress.
- Optional enterprise AI services receive only approved data segments where required.

02 / SECURITY CONTROLS

Six customer security promises

Source control	Media can remain in buyer-owned storage. Vidcomply receives only the minimum permissions required to process the asset and return results.
Workload isolation	Dedicated processing resources and separate queues are protected with least-privilege IAM and network controls. Dedicated-account deployment is available where required.
Region choice	Deployment region is agreed before onboarding based on data-residency, security, and latency requirements.
No AI training	Customer content is processed solely for the contracted service and is subject to equivalent no-training controls at approved AI subprocessors.
Auditability	Processing, infrastructure, and access activity are logged. Relevant outputs, processing records, and audit logs can be provided under the agreed access model.
Retention control	Temporary files are lifecycle-controlled. Retention, return, and deletion procedures are agreed contractually.

Shared responsibility

AWS and approved service providers protect their underlying services under their own assurance programmes. Vidcomply configures and operates the application controls. Customers control their users, source-content permissions, approved workflows, and contractual deployment choices.

Customers are not granted broad administrative access to Vidcomply's shared AWS account. Read-only infrastructure visibility or dedicated-account deployment can be provided where required and agreed.

03 / GOVERNANCE & ASSURANCE

Evidence, ownership, and due diligence

Customer content governance

- The customer retains ownership of its source content and Vidcomply-generated outputs.
- Processing is limited to providing the contracted compliance service.
- Data residency, retention, deletion, and transfer safeguards are recorded contractually.
- Subprocessors are disclosed and bound by relevant confidentiality and data-protection terms.

AWS assurance

Vidcomply completed a review in the AWS Well-Architected Tool on 5 June 2026 against the AWS Well-Architected Framework version dated 25 February 2025. All questions were answered across the four assessed pillars: Operational Excellence, Security, Reliability, and Performance Efficiency. The report recorded no high-risk improvement items and identified medium-risk opportunities tracked through an improvement plan. Cost Optimization and Sustainability were not assessed in that review.

The review is an architecture-assessment and improvement exercise; it is not an AWS certification. The full report and detailed customer architecture are available to qualified security teams during due diligence, subject to confidentiality controls.

Available diligence material

- Sample Data Processing Agreement and current subprocessor overview.
- Detailed AWS Well-Architected Tool report under NDA.
- Customer-specific deployment architecture and security schedule.
- Security questionnaires and additional evidence on request.

SECURITY CONTACT

support@vidcomply.ai

Report security concerns or request enterprise due-diligence material.