VIDCOMPLY AI

DOCUMENT TITLE: VidComply Platform Security & Architecture Overview

PREPARED FOR: Prospective Clients

PREPARED BY: Agentic Vision Ltd (trading as VidComply)

DATE: September 2026

1. EXECUTIVE SUMMARY

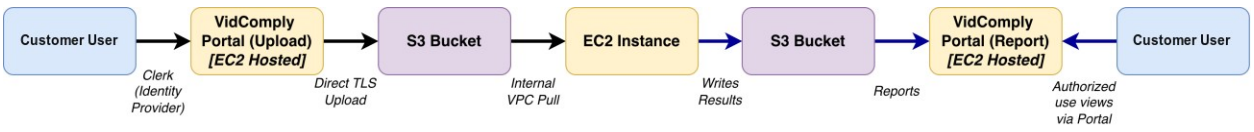
VidComply provides an enterprise-grade AI compliance platform for broadcast and in-flight entertainment media. Our security posture is built on strict data isolation: client content is processed within a dedicated AWS environment with no cross-tenant resource sharing.

- Dedicated infrastructure silo compute and storage provisioned exclusively for clients.
- No AI model training on client content, explicitly prohibited by contract and architecture.
- Enterprise-grade subprocessors only, all governed by the executed DPA.

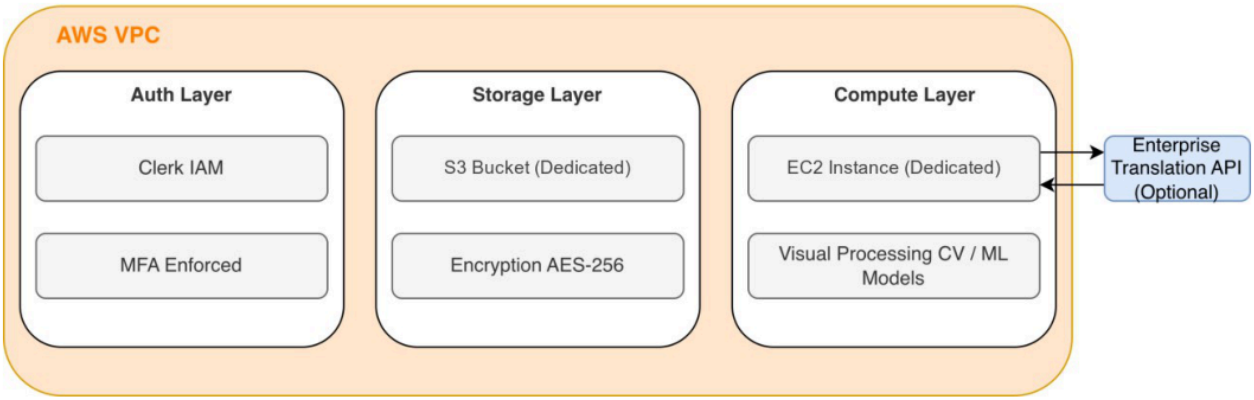
2. ARCHITECTURE OVERVIEW

Client workflows operate in a dedicated AWS silo hosted in the customer-agreed AWS region.

Data flow follows an Ingestion → Isolated Processing → Delivery pipeline.



AWS Infrastructure - Customer-Dedicated Silo (Customer-Agreed AWS Region)



- **Authentication:** User access is managed via Clerk IAM with MFA enforced.
- **Ingestion:** Files are securely uploaded via TLS directly into a dedicated, client-only AWS S3 bucket.
- **Processing:** Compute tasks are executed locally on a dedicated EC2 GPU instance.
- **Delivery:** Compliance reports and processed assets are securely returned to the isolated S3 bucket for client retrieval.

3. NETWORK & INFRASTRUCTURE SECURITY

- **Network Isolation:** Dedicated AWS VPC; all compute and storage are logically separated from other tenants.
- **Firewall:** AWS Security Groups are utilized; inbound traffic is blocked by default, and only internal API calls are permitted.
- **Admin Access:** Restricted SSH via secure VPN; MFA is enforced on all administrative accounts.
- **DDoS Protection:** AWS Shield network and transport layer protection is included by default.

4. DATA SECURITY & ENCRYPTION

- **Data at Rest:** All S3 assets and compliance reports are encrypted at rest using AES-256.
- **Data in Transit:** All connections between users, the portal, and AWS infrastructure utilize TLS 1.2+.
- **Key Management:** Encryption keys are managed and rotated via AWS Key Management Service (AWS KMS).

- Data Residency: Dedicated infrastructure is hosted in the customer-agreed AWS region. The agreed region is recorded in the applicable Order Form or Security Schedule.

5. AI PROCESSING & SUBPROCESSORS

Core compliance processing is executed locally on a dedicated EC2 GPU instance within the VPC. For specific advanced tasks (such as translation, transcription, or selective metadata analysis), isolated data segments may be routed to enterprise-grade external APIs. All subprocessors are governed exclusively by the executed Data Processing Agreement (DPA).

- **AWS:** Primary hosting, storage & compute (SOC 2 Type II, ISO 27001).
- **Clerk:** Identity & authentication (SOC 2 Type II).
- **Enterprise AI API (e.g., OpenAI Ent.):** Advanced NLP tasks via API (SOC 2 Type II).
- AI model training is strictly prohibited by contract.
- Note: The specific enterprise API provider may change. Any replacement will meet equivalent security and data isolation standards as outlined in the DPA.

6. ACCESS CONTROL, LOGGING & INCIDENT RESPONSE

- **RBAC:** AWS production access is limited to authorised core engineering personnel only.
- **MFA:** Strictly enforced for all administrative and infrastructure access.
- **Logging:** All system access, API calls, and infrastructure changes are logged via AWS CloudTrail and CloudWatch; logs are tamper-protected.
- **Incident Response:** In the event of a confirmed breach involving client personal data, VidComply will notify clients within 72 hours per the DPA.

7. VULNERABILITY MANAGEMENT & SECURE DEVELOPMENT

- Automated SAST and dependency scanning (Dependabot/Snyk) is utilized within the CI/CD pipeline.
- Routine patching of EC2 instances and underlying OS for critical vulnerabilities.
- All engineering workstations are encrypted, MFA-protected, and endpoint-secured.
-

8. DISASTER RECOVERY & DATA RETENTION

- Automated encrypted snapshots of system configurations and processing state are maintained for rapid recovery.
- All client-owned video assets are securely deleted from primary storage within 30 days of contract termination or upon request.
- Clients retain full ownership of all uploaded content and compliance reports at all times.

9. COMPLIANCE & CERTIFICATION SUMMARY

Framework	Coverage	Status
AWS SOC 2 Type II	Cloud infrastructure (AWS)	Active (AWS Artifact)
AWS ISO 27001	Cloud infrastructure (AWS)	Active (AWS Artifact)
Clerk SOC 2 Type II	Identity & authentication	Active (Clerk Trust Center)
OpenAI Ent. SOC 2 II	Enterprise API processing	Active (OpenAI Trust Portal)
GDPR / UK GDPR	Personal data processing	Governed by executed DPA

This document is a public, customer-neutral overview of Vidcomply's platform security and architecture.

Customer-specific commitments are defined in the applicable Order Form, DPA, and Security Schedule.