

Four pillars of security. One data owner.

This brief answers the four questions every technology officer puts to a vendor: **where the data resides, who can reach it, what is recorded, and who owns it.** Written for review by technical and compliance staff; terms are defined where first used.

SECURE BY DESIGN



01

Access

Identity-bound, least privilege



02

Encryption

At rest, in transit, keys held apart



03

Audit

Journalled requests, evidence provenance



04

Validation

Continuous, gated in the pipeline

YOUR AGENCY'S CASE DATA: OWNED BY THE AGENCY, ALWAYS

01

Identity-bound access control on every surface

Every surface sits behind authentication: the web application, service interfaces, and administrative tooling. Authorization is role-based at the account level, with least privilege by default and separation of duties between investigator, supervisor, and administrator roles. Single sign-on (SAML/OIDC) with multi-factor authentication federates to your existing identity provider.

02

Encryption at rest and in transit, with separated key custody

Case data is encrypted at rest (AES-256) and in transit (TLS 1.2+). Keys are held in a hardware-backed key management service, isolated from the data plane: AWS KMS in the cloud, your equivalent on-premises. Each key carries its own access policy, scheduled rotation, and an independent usage log.

03

Complete audit trail across sources and actions

Every authenticated request is journaled: identity, timestamp, session, and the objects touched. Evidence carries provenance from the point of ingestion: source attestation, content hash, and trusted timestamp. Every processing step is written to an append-only, tamper-evident log, and your administrators read the audit surface in-product at any time.

04

Continuous security validation

Security policy is expressed as automated controls, validated on every build and deployment: static analysis, dependency and container scanning, infrastructure-as-code policy checks, and secrets detection gate the pipeline; a failing control blocks release. Runtime configuration is evaluated continuously against the same baseline. Our control baseline meets CJIS Security Policy requirements and is extended by our SOC 2 implementation pipeline. **We welcome peer review and independent audit.**

The audit surface, in the product

Every authenticated request is recorded: who, when, which session, and what was touched.

Administrators inspect accounts, sessions, and activity at any time.

Every authenticated request is recorded: who, when, which session, and what was touched. Sessions reconstructed sign-ins — start time, access method, and time used.

ACCOUNT	TYPE	LAST SEEN	SESSIONS	REQUESTS	CASES OPENED	ACTIVITY (14D)
Administrator	ADMINISTRATOR	Aug 15, 09:13 AM	15	176736	9	
sg.kester	BASIC	Aug 14, 09:46 PM	7	57	3	
avallath	ADMINISTRATOR	Aug 9, 08:27 PM	1	0	0	

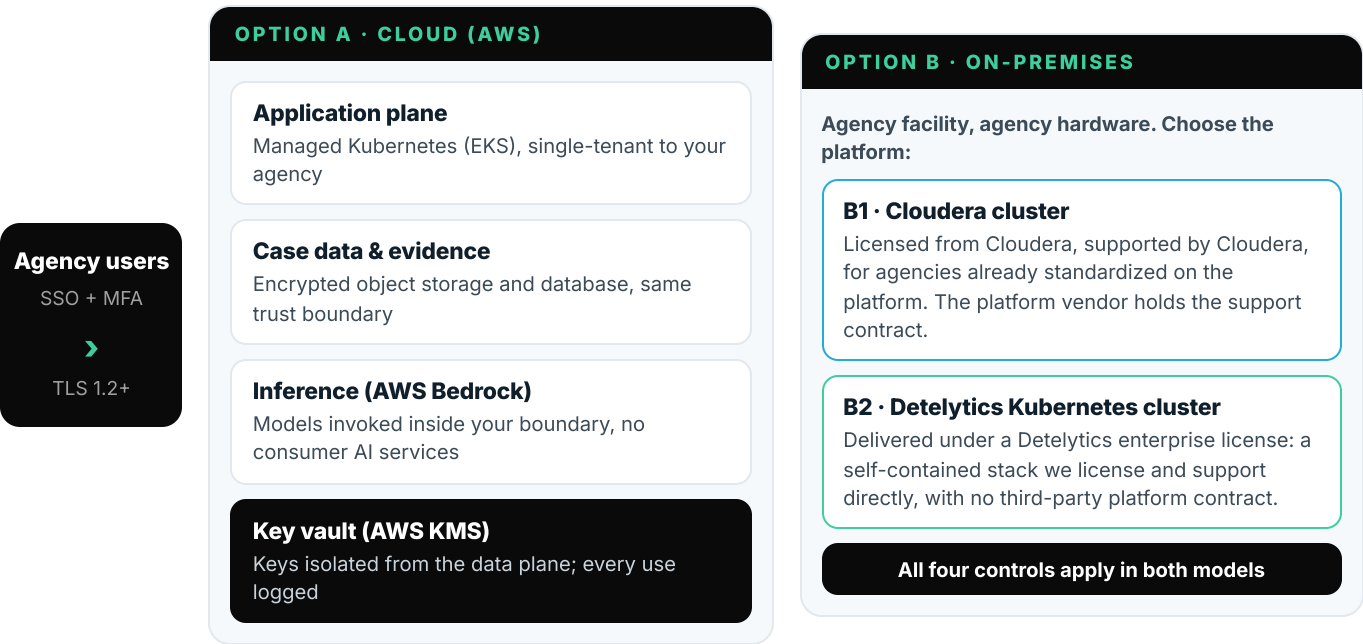
Click to view the filter sidebar

Data ownership

One answer, without qualification: **the agency owns its data: the evidence, the case files, and every artifact DeedEye derives from them.** Detelytics operates the software; the agency holds the record.

- › **Portable on demand.** Export the full case and its evidence at any time, in open formats.
- › **Single-tenant isolation.** A dedicated cluster per agency, not a shared database behind a filter.
- › **Excluded from model training.** Agency data trains nothing and is never pooled across tenants.
- › **Destroyed on instruction.** On request or at contract end, data is destroyed and the destruction evidenced.

Deployment models: two options



The four questions, answered side by side

QUESTION	CLOUD (AWS)	ON-PREMISES (CLOUDERA OR DETELYTICS)
Where is it stored?	A single-tenant cluster in the AWS region you designate. Encrypted at rest.	Your facility, your hardware. Encrypted at rest. No data egress from your network.
How is it accessed?	Authenticated accounts only, federated via SSO with MFA, authorized by role under least privilege. Transport encrypted end to end. Keys held in a separate vault: AWS KMS in cloud, the agency's key service on-premises.	
What is audited?	Every authenticated request: identity, timestamp, session, and objects touched, plus evidence provenance at ingestion and every processing step. Administrators inspect the audit surface directly, in-product.	
Who owns and maintains it?	You own the data. Detelytics maintains the application and cluster under contract.	You own the data and the infrastructure. Platform support from Cloudera (B1) or Detelytics (B2); the application is maintained by Detelytics in both.

OUR DEED TO YOU

Guardrails first

This is the deed we authored into the system as foundational design, enforced as **operational constitution** at every juncture. **Detection, inference, prediction: each carries the weight of our Deed to you.**

Five invariants enforced in code, a grade on every sentence, and provenance on every finding, so an investigator can always ask *where did this come from* and get an answer.

Enforced invariants

ID	RULE	WHAT IT PREVENTS
INV-1	Verified anchors	No finding without a re-verifiable citation to source: nothing unattributable reaches a case file.
INV-3	No identity	Structural presence only. Never face recognition, person identification, or a judgment about truthfulness.
INV-9	Open world	"None found" only under proven full coverage: silence is never reported as absence.
INV-11	No naked numbers	No confidence score crosses the display boundary. No false precision driving a decision.
INV-13	Delta scaled	Incremental processing per arrival, not full rebuild, so findings stay current at case scale.

Citations annotated by evidentiary tier

T1 Established
The vehicle was recovered on 3 May.
 Multiple independent sources in the file support this. Carries no mark: it is the baseline.

T2 Sourced
The witness places him at the depot.
 One source states it. Attributed, not established.

T3 Analysis
The timings suggest a second trip.
 An inference from cited evidence, not a documented fact. Shows its premises and counter-evidence.

T4 Absence
No custody record covers 4–6 May.
 The file does not contain this. A known gap, stated rather than skipped.

Guidance and enablement we provide

- **Role-based operator training.** Investigators, supervisors, and administrators are trained on what the system may assert, how to verify an anchor, and how to document a promotion decision.
- **Supervised onboarding and ingestion.** Our team runs your first case end to end with you, including scanning and loading legacy case files.
- **Written model-use guidance.** A policy-ready document covering appropriate use, limitations, and disclosure, drafted to be attached to agency policy or a prosecutor's discovery packet.
- **Defined escalation path.** A documented route for reporting suspected model error, plus an audit view contrasting AI-proposed against human-promoted findings.

Bring us your policies. We add them to the guardrails.

Every AI policy here can be customized for your agency. Send us your security questionnaire and we complete it directly.

sales@detelytics.com

deedeye.com · Available through Carahsoft