

AsterionDB + Oracle AI Database

Customer ROI Brief: Reduce cost, risk, and audit friction without leaving Oracle

AsterionDB is positioned as an Oracle-native integration layer that moves unstructured data, business logic, access control, and AI provenance into the Oracle-governed data layer. The result is a simpler operating model: fewer middleware costs, less credential sprawl, stronger audit evidence, and materially lower expected breach and ransomware exposure.

\$850K-\$13.5M modeled 3-year net savings by customer scale	\$629K-\$1.44M modeled annual net savings at medium-enterprise scale	9-11 months modeled break-even window	BYOL lever can reduce incremental Oracle database cost
---	--	---	--

The customer value proposition

Do not add another security tool around Oracle. Use Oracle as the security, governance, audit, and AI control plane - then remove the expensive middleware and file-system exposure that drive cost and risk.

Why Customers Should Care

Standalone Oracle OCI AI is a strong platform, but standard enterprise deployments can still leave expensive gaps: business logic often lives in middleware, unstructured data often lives outside the database, and AI workflows often require separate evidence trails. Those gaps create recurring spend and recurring risk.

Customer issue	Economic consequence	AsterionDB outcome
Middleware carries business logic	Licensing, infrastructure, admin FTEs, security tooling, and patch burden remain embedded in the cost base.	Move logic to Oracle data layer and reduce or eliminate the middleware cost category.
Files sit outside Oracle governance	Object storage, NFS shares, and compute file systems create ransomware targets and separate audit evidence.	Move unstructured assets into Oracle BLOBs under unified Oracle governance.
Multiple credentials and access paths	Credential sprawl increases breach probability and investigation cost.	Use DbTwig Single-Point API to force governed access through a single audited path.
AI decisions need defensible evidence	Audit teams need to know which documents, models, and parameters informed an AI output.	Create traceable AI provenance inside the Oracle boundary.

ROI Snapshot

The source model shows positive 3-year economics across small, medium, and large customer profiles after accounting for Oracle licensing increases, estimated AsterionDB platform cost, and migration investment. Actual results should be validated against the customer's Oracle discounts, BYOL rights, data volume, middleware footprint, and breach assumptions.

Customer profile	Scale assumption	Conservative 3-year net savings	Break-even	Primary economic driver
Small	50 employees / 5 TB	\$850K	~11 months	Middleware savings + reduced breach expected value
Medium	500 employees / 50 TB	\$4.4M	~10 months	\$629K-\$1.44M modeled annual net savings
Large	2,500 employees / 250 TB	\$13.5M	~9 months	Large middleware footprint + elevated ransomware / breach exposure

Where the Money Comes From

Savings lever	What changes	Economic outcome message
Middleware elimination	Business logic moves from middleware into the Oracle data layer.	Recurring licensing, compute, admin, and security tooling costs can be reduced or removed.
Breach and ransomware event reduction	NoFS removes static file-system targets; Single-Point API removes common bypass paths.	Risk exposure is reduced structurally, not simply monitored after the fact.
Audit and compliance simplification	Structured and unstructured data move under one Oracle audit boundary.	Less evidence gathering, fewer disconnected logs, faster compliance response.
Oracle commercial leverage	Spend shifts away from middleware and toward database consolidation.	BYOL and ELA / ULA negotiation can materially improve ROI.
AI cost and provenance control	AI inference and data trace remain inside the Oracle-governed environment.	Reduced external API / storage friction and stronger AI accountability evidence.

Customer Action Plan

The fastest path is not a full enterprise rollout. The right first step is a narrow ROI and architecture validation against one representative workflow or environment.

Step	Action	Customer provides	Output
1	30-minute ROI screen	User count, middleware processors, data volume, environments, Oracle BYOL / ELA / ULA status	Initial savings range and fit assessment
2	Data residency + logic audit	File-system / Object Storage inventory and app access patterns	Map of where cost, risk, and audit friction live today
3	Customer-specific 3-year model	Actual Oracle discounts, support costs, FTE cost, breach assumptions	Validated ROI, break-even, and investment case
4	60-90 day proof-of-value	One representative workflow or program segment	Before/after evidence: access control, audit trail, file-surface reduction, and economics
5	Rollout decision	Security, finance, architecture, and program stakeholder review	Go/no-go recommendation with budget and implementation path

Decision Criteria for a Proof-of-Value

AsterionDB adoption should move forward when the customer can validate at least three of the following economic or operational conditions:

- Meaningful spend on WebLogic, SOA, OIC, API gateways, integration servers, middleware compute, or middleware admin FTEs.
- Sensitive documents, telemetry, packages, images, logs, or operational files stored in Object Storage, NFS, or compute file systems.
- Audit teams need a unified chain of custody across structured and unstructured data.
- The customer has elevated ransomware, breach, or credential-compromise exposure.
- Existing Oracle Database EE / Premier Support / BYOL rights can reduce incremental Oracle database cost.
- AI workflows require defensible provenance that ties outputs back to source data, model version, and execution parameters.

Recommended Next Step

Approve a 30-minute ROI and architecture screen. Bring five inputs: user count, middleware processors, unstructured data volume, number of environments, and Oracle BYOL / ELA / ULA status.

Commercial note

The ROI figures in this customer brief are modeled estimates based on the source white paper. A customer-specific business case should be calibrated with actual Oracle pricing, BYOL eligibility, AsterionDB pricing, implementation scope, FTE costs, breach probability, and data volume before procurement decisions are made.