



ENTERPRISE AI OPERATIONS BRIEF

See, control, and prove how AI operates across your business

Shield360 connects AI activity, agents, endpoints, tools, data access, policy decisions, evidence, and cost in one enterprise operating layer.

Built for the leaders responsible for AI adoption, security, compliance, engineering, and financial accountability.

Discover

AI systems and shadow usage

Govern

access, policy, and sensitive data

Evidence

activity, decisions, and cost



What AI is operating? **INVENTORY**

What can it access? **CONTROL**

What did it cost? **ATTRIBUTE**

What can we prove? **EVIDENCE**

AI ADOPTION IS OUTRUNNING OVERSIGHT

The enterprise cannot govern what it cannot see or explain

AI now spans employee subscriptions, APIs, internal applications, coding assistants, autonomous agents, external tools, and company data. Each surface creates a different record of activity.

1

Visibility is fragmented

Finance sees invoices.
Security sees endpoints.
Engineering sees traces.
Procurement sees contracts. No single view explains the whole picture.

2

Agents expand access

Agents can call tools, retrieve documents, use credentials, retain memory, and take actions across systems designed for human users.

3

Evidence arrives late

Teams reconstruct incidents, audits, and budget questions from provider logs, screenshots, invoices, and disconnected controls.

The operational question

Can your organization identify an AI system's owner, explain its last consequential action, show what data and tools it used, attribute its cost, identify which policy applied, and intervene when necessary?

Applications

Model calls, prompts, retrieval, latency, tokens, errors, and cost.

Agents

Steps, tools, memory, documents, secrets, grants, and outcomes.

Endpoints

Coding agents, desktop AI tools, machine context, and usage signals.

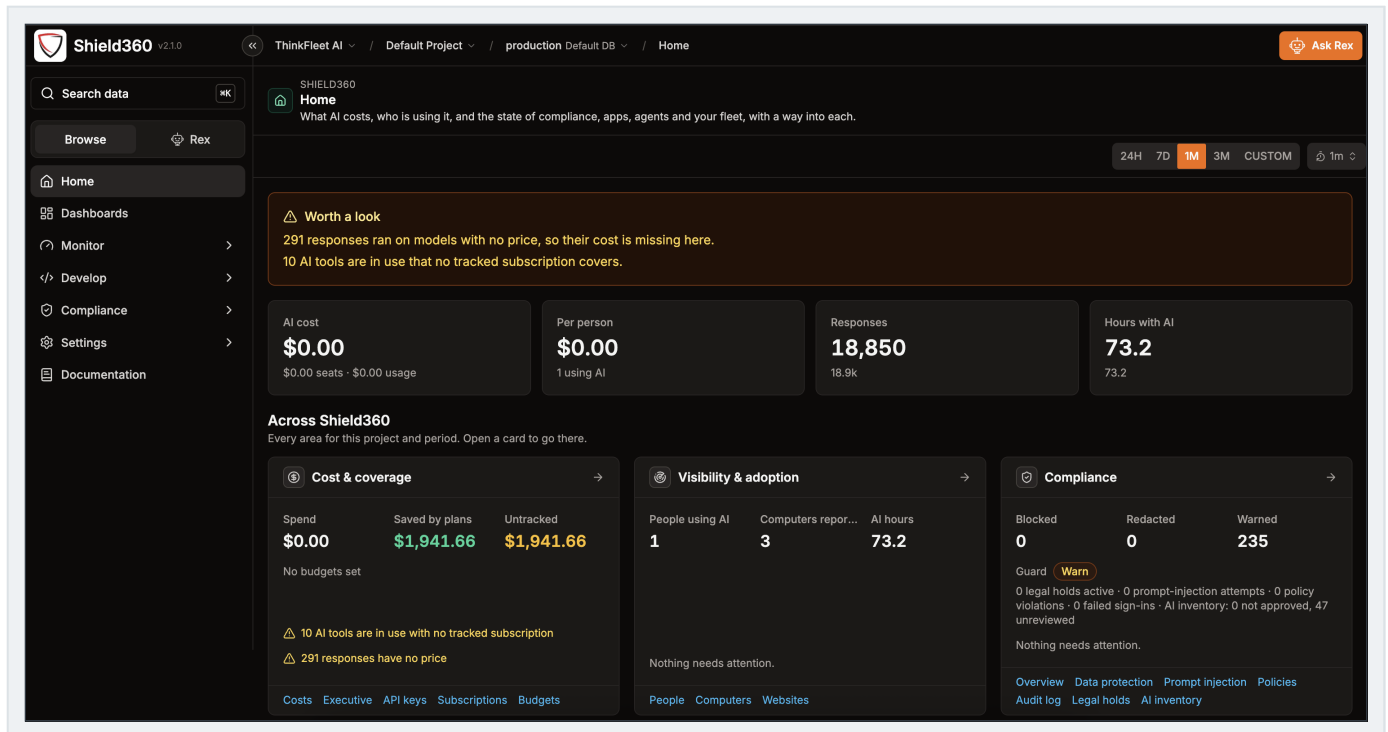
Leadership

Inventory, ownership, policy, risk, evidence, and financial decisions.

ONE OPERATING PICTURE

Bring AI activity, governance, and economics into the same view

Shield360 connects AI adoption and cost with application, agent, endpoint, policy, compliance, and audit context. Teams work from shared evidence instead of reconciling separate reports.



AI inventory

Systems, vendors, models, agents, owners, and approval state.

Cost visibility

Subscriptions, API usage, estimates, and billing variance.

Operational controls

Policies, grants, access, secrets, and sensitive data.

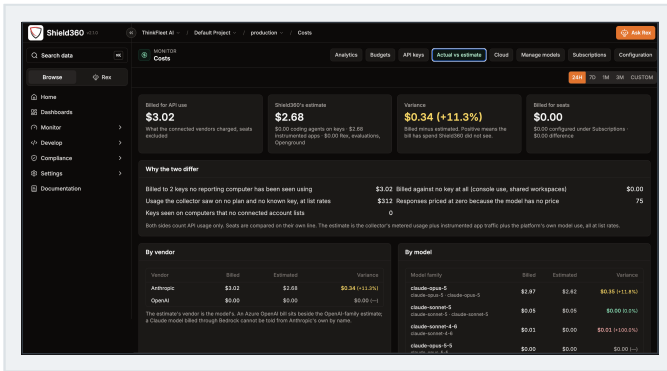
Reviewable evidence

Traces, audit activity, decisions, findings, and holds.

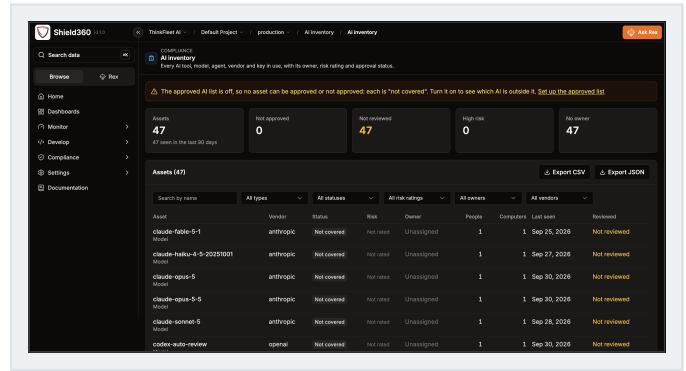
Shield360 test environment. Figures shown are demonstration data.

START WITH QUESTIONS LEADERS ALREADY ASK

Know what AI is in use, who owns it, and what it costs



Compare connected billing with telemetry-based estimates to expose coverage gaps and unexplained variance.



Organize models, tools, agents, vendors, credentials, owners, computers, and approval state.

Subscriptions

Review seats, coverage, underuse, and usage reported without a tracked plan.

API usage

Connect model activity, tokens, pricing, projects, and applications.

Shadow AI

Surface tools and usage that security or procurement may not yet know about.

Ownership

Tie activity to people, projects, applications, machines, models, and vendors.

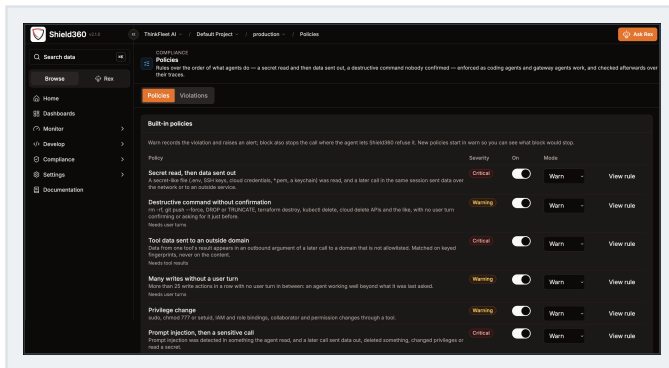
Business value

Create a defensible AI inventory, investigate cost variance, and prioritize governance based on observed activity rather than survey responses alone.

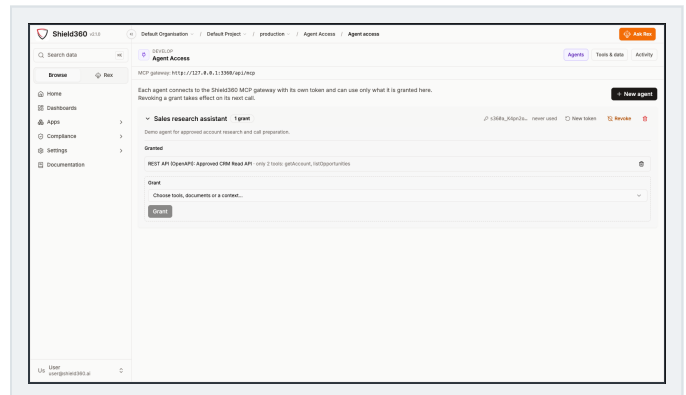
MOVE FROM OWNERSHIP TO OPERATIONAL CONTROL

Govern what agents can reach and preserve what they did

An agent owner needs more than a name in a registry. Shield360 connects identity, scope, tools, documents, credentials, policy, memory, sensitive data, cost, and evidence around the agent's work.



Apply policies to AI traffic and agent workflows with reviewable decisions.



Scope which tools and resources an agent can use through explicit grants.

Controlled tools

Wrap REST APIs from OpenAPI descriptions, MCP servers, and company document sources as governed tools.

Protected credentials

Keep credentials in Shield360 and fetch secrets from supported external vault providers only when needed.

Governed context

Provide live, redacted, permissioned document access without copying or indexing source content.

Every tool call can be checked and recorded. Tokens and grants define access while policies evaluate the traffic around agent actions.

MAKE GOVERNANCE REVIEWABLE

Build evidence while AI operates, not after the investigation begins

Shield360 brings policy outcomes, sensitive-data findings, audit activity, trace context, and legal holds into a shared review path.

Trace evidence

Inspect execution hierarchy, tokens, cost, tool use, errors, wrong turns, and injection signals.

Audit activity

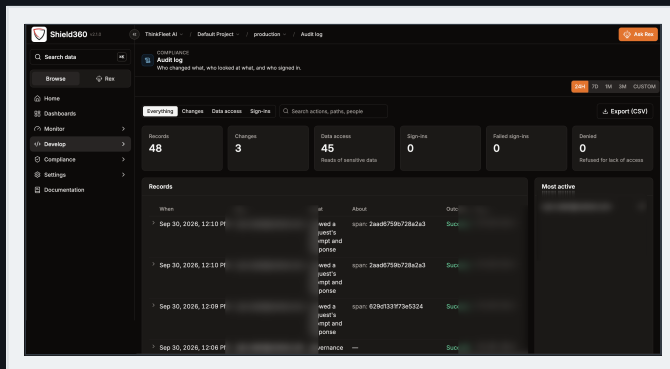
Record administrative changes and reads of protected resources for investigation and review.

Sensitive-data handling

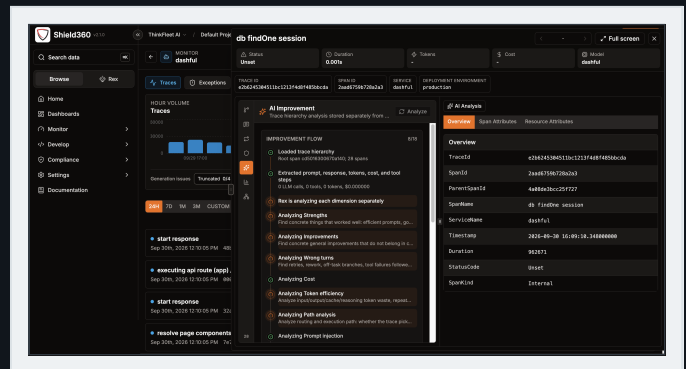
Find and redact sensitive values before they reach models or agents while retaining useful finding metadata.

Legal holds

Preserve relevant evidence for defined matters without relying on scattered screenshots and exports.



Audit activity supports a review path for protected resources and administrative actions.



Trace analysis connects technical execution with financial and governance context.

MEET THE ENTERPRISE WHERE IT OPERATES

Connect existing AI workflows without replacing the observability stack

Shield360 uses OpenTelemetry-compatible collection paths and supports cloud or self-hosted deployment models for different enterprise requirements.

Collect

Receive application, agent, model, tool, endpoint, and billing signals.

Normalize

Connect identity, organization, project, vendor, model, owner, and cost context.

Evaluate

Apply signed, versioned policy bundles across server, collector, and SDK paths.

Review

Present shared evidence to engineering, security, compliance, finance, and leadership.

Integration-friendly

- OpenTelemetry and OTLP collection paths
- Application and agent instrumentation
- Endpoint visibility for supported developer workflows
- Connected billing and subscription records

Enterprise deployment choices

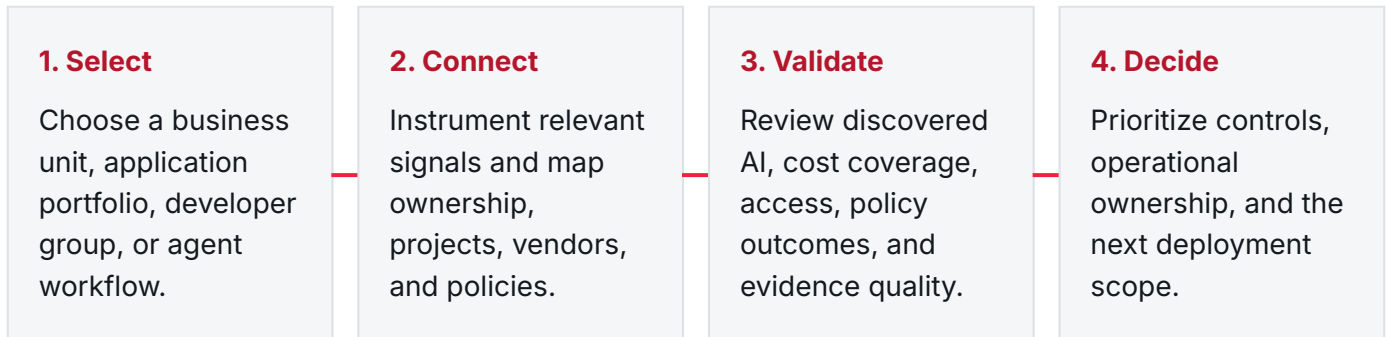
- Cloud or self-hosted deployment
- Organization and project hierarchy
- Role-based access and audit controls
- Privacy-aware evidence handling

Designed to complement existing systems

Shield360 gives enterprise teams a common operating layer for AI-specific context while preserving existing observability, security, identity, and secret-management investments.

START WITH A BOUNDED BUSINESS QUESTION

Prove value on a defined scope, then expand from shared evidence



Common evaluation questions

STAKEHOLDER	QUESTION SHIELD360 HELPS ANSWER	EVIDENCE TO REVIEW
CIO / CTO	Where is AI operating, who owns it, and which areas require intervention?	Inventory, ownership, adoption, projects, applications, and agents.
CISO	What can agents access, which policies apply, and where is sensitive data exposed?	Grants, tools, credentials, policy outcomes, and redacted findings.
Finance / FinOps	What are we paying, what activity explains it, and where are coverage gaps?	Subscriptions, invoices, model-priced telemetry, attribution, and variance.
Compliance	Can we reconstruct activity and preserve evidence for review?	Traces, audit events, policy decisions, legal holds, and findings.
AI platform	Can developers build agents with governed prompts, tools, memory, secrets, and context?	Prompt Hub, Memory, MCP gateway, Vault, Contexts, Scanner, and Rule Engine.

A practical first conversation

Bring one AI system, agent workflow, developer group, or cost question. We will map the available signals, responsible stakeholders, and evidence needed to define a useful evaluation.

Make AI visible enough to manage and controlled enough to trust

Shield360 gives enterprise teams a shared way to discover AI, understand cost, govern agents, protect data, apply policy, and preserve evidence across the AI lifecycle.

Discover	Inventory applications, agents, tools, models, vendors, endpoints, owners, and approval state.
Understand	Connect subscriptions, API usage, tokens, projects, and observed activity to cost.
Control	Govern tool access, credentials, documents, memory, sensitive data, and AI traffic.
Prove	Retain trace context, policy decisions, audit activity, findings, and legal holds for review.



ryan@thinkfleet.ai · [linkedin.com/in/ryanrader](https://www.linkedin.com/in/ryanrader)
shield360.ai · Enterprise AI operations