

THE FORGE ADVANTAGE

Capabilities no other platform delivers.

CAPABILITY	FORGE	OTHERS
Shadow AI / Rogue LLM Detection	✓	partial
Local LLM Detection UNIQUE	✓	✗
Agent-to-Agent Communication Visibility UNIQUE	✓	✗
Full Trace DAG with 800ms Replay	✓	partial
Host-Level Probes (Process / Network / File / MCP)	✓	partial
MCP Server Governance	✓	partial
Human-in-the-Loop Approval Workflows UNIQUE	✓	✗
AI Firewall & Real-time Intervention	✓	partial
Cost Attribution & Token Budget Enforcement	✓	partial
Quality SLA Enforcement	✓	partial
13 Compliance Frameworks UNIQUE	✓	✗
11 SIEM Platform Integrations	✓	partial
66 REST API Endpoints — Full Programmability	✓	✗

30 MINUTE DEPLOYMENT

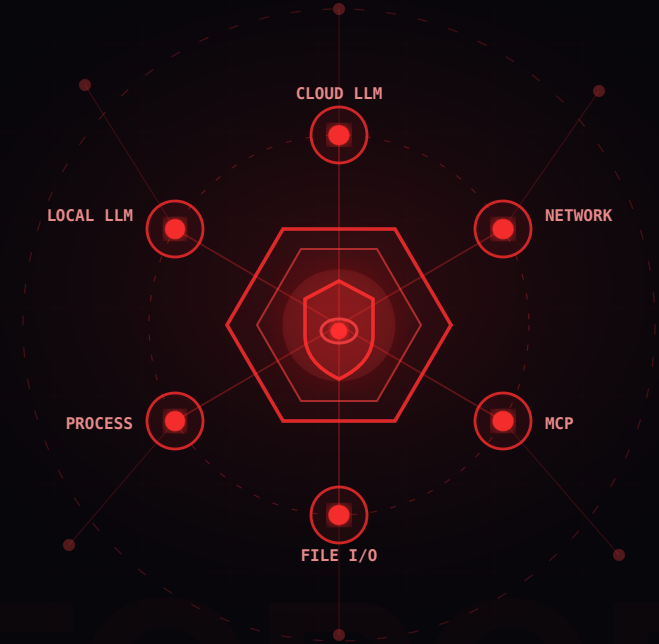
Agent-less · API-first · Works alongside existing infrastructure

CONTACT US

[privify.io](#)

enterprise@privify.io

[privify.io/forge/demo](#)



FORGE

FEDERATED OVERSIGHT & RISK GOVERNANCE ENGINE

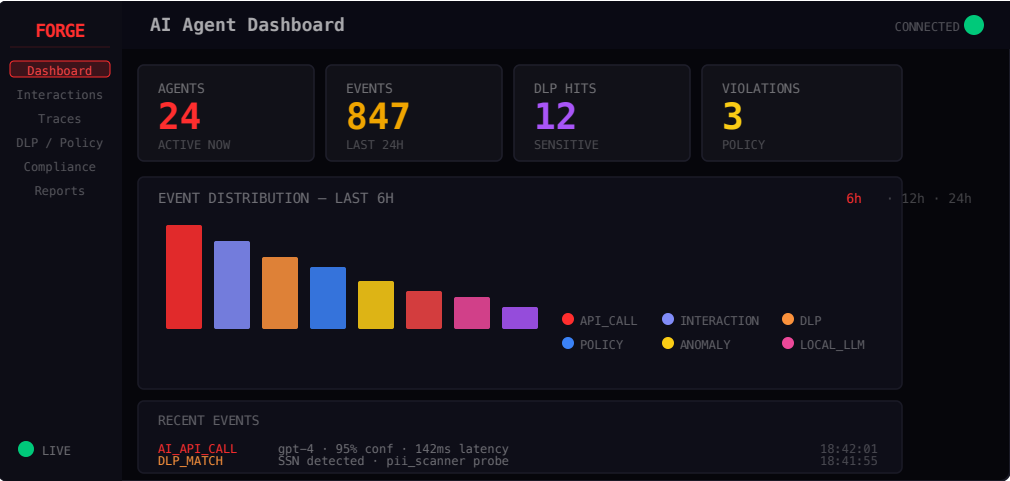
Every AI agent.
Every interaction.
Governed.

The only platform that combines Shadow AI discovery, real-time behavioral observability, and policy-driven governance — purpose-built for enterprise AI deployments.

DISCOVER Shadow AI · Probes	OBSERVE Traces · Analytics	GOVERN Policy · Compliance
---------------------------------------	--------------------------------------	--------------------------------------

 **privify**
privify.io
▶ See demo online

LIVE DASHBOARD PREVIEW



- DISCOVER
- Find every AI in your environment
- Shadow AI & Rogue LLM

Detect unauthorized AI usage via network intercept, process monitoring, and AI library fingerprinting
- Local LLM Detection

Identify Ollama, LM Studio, and private model instances running on-device — invisible to API-only tools
- MCP Server Enumeration

Auto-discover Model Context Protocol servers and map tool capabilities exposed to AI agents
- Agent Process Mapping

Map every AI framework (LangChain, AutoGen, CrewAI) and build a living inventory of your AI fleet

- OBSERVE
- 360° visibility into every agent
- Real-time Event Streaming

Live WebSocket feed of all 17 event types including API calls, DLP hits, and policy violations with sub-second latency
- Trace DAG with Replay

Reconstruct full agent call chains as directed acyclic graphs. Replay any session at 800ms cadence for forensic analysis
- Agent-to-Agent Visibility

The only platform tracking communication between orchestrator and subagents — critical for multi-agent AI systems
- Cost & Quality Analytics

Per-agent token spend, latency histograms, quality scoring, and SLA tracking across all AI providers

GOVERN

Enforce policy. Control risk. Prove compliance.

Policy Engine

Keyword, regex, semantic, and context-aware rules. Configurable actions: alert, block, redact, or route for human approval.

DLP Scanning

12 data patterns: PII, SSN, credit cards, API keys, PHI, financial data. Scans every prompt and response in real time.

AI Firewall

10 threat signatures covering jailbreaks, prompt injection, loop detection, and data exfiltration attempts.

Human-in-the-Loop

Intercept high-risk actions for human approval before execution. Full approval audit trail with timestamps.

Cost Governance

Per-agent and per-team token budgets. Real-time spend tracking and automatic cap enforcement across providers.

SIEM Integration

11 platforms supported: Splunk, Elastic, Datadog, IBM QRadar, Microsoft Sentinel, and more — native and webhook.

REGULATORY COMPLIANCE IS NO LONGER OPTIONAL

The EU AI Act (enforcement from Aug 2025), India's DPDP rules, Singapore's PDPA, and Canada's PIPEDA all impose obligations on AI system operators. FORGE provides automated evidence collection, audit trails, and compliance scoring — reducing audit preparation from weeks to minutes.

13 Compliance Frameworks

Automated evidence collection & control scoring

100% automated

SECURITY

SOC 2HIPAAPCI-DSS

PRIVACY

GDPRCCPA DPDP PDPA PIPEDA

AI REGULATION

EU AI ActDSA CA SB53 NIST AI RMF ISO 42001