

COST OF NO ONGOING OPS

STATIC EVALS DECAY · CONTINUOUS THREAT LANDSCAPE

STATIC EVAL HARNESS
DECAY

90 days

One-time eval harness (M12) **decays in 90 days**. OWASP LLM Top 10 v2 evolves quarterly · jailbreak corpora publish bypasses weekly · MITRE ATLAS v5.4 added 11 agent-specific TTPs in March 2026 that static suites miss.

PRODUCTION AGENT
BREACH COST

\$4.88M

Average breach cost (IBM 2025). Autonomous agents with **unbounded tool authority + external access + PHI/NPI scope** are the highest-risk class. M16 monthly red-team battery + quarterly deep-scenario detects pre-breach.

SAAS PLATFORM LOCK-IN
TAX

\$30K-\$400K
per year

Annual recurring SaaS fees (Lakera + HiddenLayer + Protect AI + CalypsoAI) on **3-year contracts** with platform lock-in. M16 native-Foundry service = no lock-in · customer owns custom evaluators.

DIRECTOR FIDUCIARY
LIABILITY

Personal \$

In re Boeing + Marchand v. Barnhill: directors **personally liable** for failure to monitor mission-critical AI risk. SEC Item 106 + Item 1.05 public-issuer disclosure. M16 Enterprise quarterly Board pack = **direct fiduciary cover**.

12-MONTH RETAINER VALUE

M12 · SETUP

2-4 wks · \$25K-\$75K one-time

Eval harness built · Sentinel + Defender configured

→

M16 · OPERATE

12-mo min · \$180K-\$660K annual

Weekly + Monthly + Quarterly cadence · 24x7 named (Enterprise)

6 OPERA

HANDOFF

✓

Weekly + Monthly + Quarterly Cadence

Weekly CI/CD regression + drift detection · Monthly OWASP LLM Top 10 v2 + MITRE ATLAS v5.4 · Quarterly deep-scenario red-team · Continuous Sentinel correlation.

✓

Anthropic MCP Security Working Group Intelligence

Kriv is CPN participant — direct early access to Feb 2026 draft hardening guidance + Q2 2026 quarterly updates. Pre-emptive vs reactive.

✓

Named US-Based Engineers (Enterprise)

2 named US-based engineers cleared for HIPAA BAA + SR 26-2 scope · Dedicated Microsoft Teams channel · P1 1hr response SLA · Not offshore SOC.

✓

Quarterly Board Quality + Risk Pack (Enterprise)

Caremark + SEC Item 106 + Item 1.05 framing · NIST AI RMF Measure/Manage evidence · ISO 42001 AIMS surveillance audit evidence · D&O renewal posture.

M16 RETAINER VS SAAS PLATFORM 3-YEAR COST

PLAN	KRIV M16 12-MO ACV	SAAS PLATFORM 3-YEAR COST
FOUNDATION \$15K/mo · 3 agents	\$180,000	\$90K – \$450K (Lakera / Langfuse 3-yr)
STANDARD RECOMMENDED \$32K/mo · 5 agents	\$384,000	\$150K – \$750K (HiddenLayer / Protect AI 3-yr)
ENTERPRISE \$55K/mo · 10 agents	\$660,000	\$250K – \$1.2M+ (CalypsoAI / Fiddler 3-yr)

Kriv = SERVICE (Foundry-native · no lock-in · customer owns evaluators) · SaaS = PLATFORM (lock-in · recurring · platform-specific)

► Ready to operate agent eval + red-team monthly?

info@kriv.ai · Microsoft Marketplace · kriv.ai