

TELARCH COGNITIVE INFRASTRUCTURE

High-Assurance Cognitive Architecture · Deterministic Agent Infrastructure

Knapsack Context Budgeting · Cryptographic Vault Leases · Tamper-Evident Ledger

Document: Technical Evaluation Brief (TCI-2026-B)
Architecture: Telarch Triad (Harpe + Kibisis + Argus)
Licensing: MIT License © 2026 Perseus Computing LLC
Distribution: Public Technical Release · October 2026

Architectural Divergence & Industry Landscape: Enterprise agentic AI is currently bottlenecked by heuristic memory wrappers (Mem0, Letta/MemGPT, Zep, LangMem) engineered for informal conversational chat rather than regulated multi-agent deployments. In production environments, these legacy architectures exhibit three fatal structural failure modes: (1) **Unbounded Context Inflation** via unbudgeted vector top-K injection and recursive LLM self-edits, inflating prompt costs and collapsing reasoning windows; (2) **Mutable Plaintext Storage & Ghost Leaks** where soft-delete flags leave residual vector embeddings across search shards (Carrier Leakage) with no distributed concurrency fencing; and (3) **Zero Cryptographic Provenance**, failing federal compliance mandates (NIST SP 800-53 AU-2/3, CMMC Level 2). The **Telarch Suite (TCI)** solves these systemic liabilities through an air-gapped, mathematically bounded architecture.

Operational Delivery Model: 100% sovereign, local-first execution with zero external cloud dependencies or telemetry reachback. Engineered and maintained by Perseus Computing LLC under the MIT License.

1. THE TELARCH ARCHITECTURAL TRIAD (HARPE, KIBISIS, ARGUS)

Subsystem	Technical Architecture & Core Invariants	Operational Guarantees & Impact
Harpe Engine Context Knapsack	Deterministic Context Knapsack: Enforces strict token ceilings prior to model invocation using priority shingle pruning and dynamic headroom reservation. Resolves dynamic context at microsecond bounds (1.72 μs p50).	87.2% to 99.0% token reduction across benchmark suites; eliminates context poisoning and stabilizes inference latency to microsecond bounds.
Kibisis Vault Storage & Leases	Encrypted Vault & Concurrency Leases: AES-256-GCM memory store paired with atomic monotonic fencing-token leases and Suite D cryptographic tombstones. Coordinates multi-agent swarm state with zero distributed lock manager.	Zero ghost leaks; raw content is purged synchronously from tables and FTS5 indexes while durable SHA-256 digest prevents adversarial re-ingestion.
Argus Ledger Audit & Provenance	Tamper-Evident POSIX Ledger: Local POSIX-locked append-only JSONL ledgers with continuous SHA-256 parent-hash chaining, recording every prompt, decision branch, tool call, and state transition.	NIST SP 800-53 AU-2/3 & CMMC L2 compliance. Sub-millisecond tamper detection (46 μs); non-repudiable post-incident forensic replay.

2. EMPIRICAL BENCHMARKS & VERIFIED PERFORMANCE METRICS

87.2% – 99.0% Prompt Token Reduction Context-Bench (2,590 vs 20,186 tokens); LongMemEval-S (1,179 vs 123,770 tokens/inst)	97.0% Recall@5 Accuracy LongMemEval-S benchmark with 0.9085 Mean Reciprocal Rank across 500 instances	0.0% Sequence Inversions Deterministic RECON temporal ordering vs 15–25% in legacy vector wrappers	0 Ghost Leaks Cryptographic Tombstones 100% SHA-256 anti-resurrection rejection; synchronous FTS5 index purging
---	---	--	---

3. SYSTEM CAPABILITY & ARCHITECTURAL COMPARISON MATRIX

Capability Dimension	Mem0	Letta (MemGPT)	Zep	LangMem	Telarch Suite (TCI)
Architecture	Vector wrapper	LLM OS / Core Mem	Graph/Temporal DB	Client vector helper	Modular Triad (Budget+Vault+Ledger)
Deployment	Cloud API / Qdrant	Self-hosted / Cloud	Proprietary server	Local Python helper	100% Sovereign / Zero Cloud Dep
Context Ceiling	None (Top-K dump)	Soft LLM window	Heuristic prune	Token window slice	Strict Knapsack Ceiling (TokenBudget)
Token Efficiency	0% (Bloats prompt)	Negative (Tool calls)	Moderate (~30–50%)	Basic slice truncation	87.2% to 99.0% Measured Reduction
Storage Security	Plaintext / SaaS DB	Plaintext SQLite/PG	Plaintext Postgres	Plaintext memory/disk	AES-256-GCM Envelope Encryption
Erasure Integrity	Soft delete (Leaks)	Soft delete (Leaks)	Soft delete / Prune	Soft delete (Leaks)	Cryptographic Tombstone (Zero Leak)
Anti-Resurrection	None (Can re-add)	None	None	None	Durable SHA-256 Digest Rejection
Swarm Concurrency	None (Race hazard)	Process locks	Server transactions	None	Monotonic Lease Fencing (Race Free)
Audit Non-Repudiation	Ephemeral logs	Console logging	Activity logs	LangSmith SaaS	Tamper-Evident SHA-256 Chaining
Federal Compliance	Fails NIST / CMMC	Fails NIST / CMMC	Fails NIST / CMMC	Fails NIST / CMMC	NIST SP 800-53 AU-2/3 & CMMC L2

Institutional Assurance & Verification Standing: Stage 0 deterministic gauntlet, Stage 1 subsystem pressure tests, and Stage 2 LongMemEval integration verified 100% PASS with zero failures across Linux, macOS, and Windows. Available as modular native crates or self-contained binary execution with zero cloud reachback.

Corporate Entity: Perseus Computing LLC (Austin, TX) · Licensing: MIT License · Repository: github.com/Perseus-Computing-LLC · Inquiries: contact@perseuscomputing.com