



BARTHOLOMEW AI (BTP v5.4.16)

The In-Process Runtime Execution Gateway for Autonomous AI Agent Swarms

SLIDE 1 / 8

THE EXECUTIVE THESIS

- **The Fundamental Shift:** AI models have graduated from text chat to autonomous agents with full terminal, database, and API execution authority.
- **The Autonomous Execution Gap:** Giving agents execution privileges introduces catastrophic risks: prompt injection, system wipes (rm -rf), SQL truncation, and secret leakage. Prompt filters and LLM judges cannot stop this without massive latency.
- **The Bartholomew Standard:** Operates directly inside the agent's memory process and cloud edge, enforcing multi-language AST invariants in **under 35 microseconds (< 0.035 ms)** with 100% mathematical determinism.
- **The Financing:** Raising **\$2,000,000 USD** on a **\$15M Valuation Cap Post-Money SAFE** (\$0 prior dilutive equity raised).

KEY VALIDATION SIGNALS AT A GLANCE

- **4,500+ Active Developers:** Organic bottom-up adoption across npm (btp-guard: 1.6k/wk), PyPI (1.8k/mo), and Open VSX (1,026+ installs).
- **50,000x Faster Than LLMs:** Deterministic sub-35us latency eliminates the 2,000ms latency penalty of secondary LLM judges.
- **2,500+ Production Receipts:** Metered tool calls logged in tamper-proof RFC 8785 Ed25519 Merkle ledgers.
- **\$360,000 Active Pipeline:** 12 enterprise design partner discussions (\$30k ASP) across fintech, logistics, and agent platforms.
- **Non-Dilutive Cloud Backing:** Compute and infrastructure jumpstart from **Google Cloud, Microsoft for Startups, and Amazon Web Services.**



WHAT THE INDUSTRY MISSED: THE AUTONOMOUS EXECUTION GAP

SLIDE 2 / 8

Why Perimeter WAFs and LLM-as-a-Judge Fail in Autonomous Agent Deployments

1. The Perimeter WAF Blindspot	2. The LLM-as-a-Judge Fallacy	3. The Missing In-Process Layer
Built for HTTP, Blind to Agents • Traditional firewalls and cloud WAFs guard network boundaries. • Autonomous agents execute commands <i>inside</i> the server (bash subshells, local file I/O, database drivers). • Network perimeters cannot see or block an agent running <code>rm -rf</code> / or dropping internal SQL schemas.	Stochastic, Slow & Expensive • Secondary LLMs (e.g. LlamaGuard) introduce 1,500 to 2,500 ms of latency per tool call, breaking interactive workflows. • Doubles inference token costs on every action. • Fundamentally probabilistic: vulnerable to adversarial prompt jailbreaks, encoding tricks, and hallucinated permissions.	Bartholomew's Deterministic Gate • What was missing: an execution gate running inside the agent process memory. • Evaluates Abstract Syntax Trees (AST) and security invariants in under 35 microseconds (< 0.035 ms). • Zero external network latency, zero token cost, 100% mathematical determinism.



WHY BARTHOLOMEW IS SPECIAL: FOUR CORE INVENTIONS

SLIDE 3 / 8

Deterministic Microsecond Security, In-Flight Masking, and Cryptographic Evidence

1. Sub-35 Microsecond AST Invariant Gating	2. In-Flight Secret Vault Masker
• Compiles and inspects Abstract Syntax Trees across Bash, Python, SQL, JS/TS, Go, and Rust before execution. • Halts catastrophic shell injection, SQL database drops, and infinite spend retry loops in under 35 microseconds. • Runs 100% in-process with zero external API calls, adding no perceptible overhead to agent execution.	• Scans agent prompts, function parameters, and tool arguments in real-time. • Automatically detects and redacts OpenAI keys (sk-*), AWS credentials, GitHub PATs, and SSH keys. • Prevents inadvertent secret exfiltration to external model providers, logs, or vector stores.
3. Ed25519 Cryptographic Attestation	4. Zero-Install Cloud Gateway & M2M Economy
• Issues RFC 8785 canonical JSON receipts signed with Ed25519 digital signatures for every evaluated tool action. • Bundled into local Merkle trees that provide mathematical, non-repudiable audit evidence for SOC 2 Type II & HIPAA. • Allows downstream tools and auditors to independently verify action validity 100% offline.	• Zero-install reverse proxy (gateway.bartholomew.info/v1) for Grok (xAI), Meta AI (Llama), Claude, and Muse. • Programmatic L402 Lightning network settlement (\$0.01/allowed action) for autonomous machine-to-machine swarms. • Machine-readable service discovery via .well-known/btp.json.



TECHNICAL VALIDATION & RIGOR THAT INVESTORS CARE ABOUT

SLIDE 4 / 8

Engineered by Systems Architects, Grounded in Formal Methods, Proven in Production

1. 100% Test Suite Pass Rate (2,920 Tests)	2. Formal Mathematical Foundation (Rice's Theorem)	3. Enterprise Cloud Edge Infrastructure
Production Reliability at Scale • 2,920 automated tests running in continuous CI with 100% pass rate. • Covers polyglot AST syntax engines, multi-tenant isolation, cryptographic verifiers, and adversarial penetration suites. • Validated sub-35 microsecond latency benchmarked under high-concurrency loads.	Proven Theoretical Limits • Grounded in Rice's Theorem: proves that semantic behavior cannot be decided by LLM prompts. • Authored formal research paper establishing the Three-Tier Composition Model for agentic runtime safety. • Formally registered and published on Zenodo with permanent DOI.	Multi-Cloud Deployment & Backing • Non-dilutive grant and compute jumpstart backing from Google Cloud, Microsoft, and Amazon. • Distributed low-latency cloud edge gateways deployed across global regions. • Certified anti-malware and zero-vulnerability clearance across npm and PyPI distributions.



MOMENTUM: WHY TRACTION IS ACCELERATING QUICKER THAN EXPECTED

SLIDE 5 / 8

The Confluence of Bottom-Up Developer Pull and Top-Down Enterprise Mandates

BOTTOM-UP DEVELOPER PULL (PLG)

- **4,500+ Active Developers:** Organic weekly adoption across npm (btp-guard: 1.6k/wk), PyPI (1.8k/mo), and Open VSX (1,026+ installs).
- **35% MoM Growth:** 100% organic growth driven by developer word-of-mouth with \$0 spent on paid marketing.
- **The REAPER Fair Developer Model:** Unrestricted local evaluation makes Bartholomew the zero-friction standard for engineers building agents.
- **Universal Ecosystem Support:** 1-line drop-in integrations published for AutoGen, LangChain, LangGraph, CrewAI, Claude Computer Use, and Cursor IDE.

TOP-DOWN ENTERPRISE MANDATE (SALES)

- **12 Enterprise Design Partners in Pipeline:** Fast-growing AI startups, fintech platforms, and health-tech teams with active agent deployments.
- **\$360,000 Pipeline Value:** Based on our standard \$30,000/year enterprise compliance & SIEM streaming tier.
- **Unblocking the CISO Veto:** Over 80% of enterprise AI agent initiatives are stalled by security teams. Bartholomew provides the deterministic audit controls that turn CISO 'No' into 'Yes'.
- **Regulatory Tailwinds:** EU AI Act, NIST AI RMF, and SEC disclosure rules mandate verifiable, non-repudiable audit trails for autonomous systems.



COMPETITIVE DIFFERENTIATION: AN UNRIVALED MOAT

SLIDE 6 / 8

Why Bartholomew Outclasses LLM Judges, Cloud WAFs, and Container Sandboxes

Capability Dimension	LLM Judges (LlamaGuard)	Cloud WAFs & Proxies	Docker / E2B Sandboxes	Bartholomew Protocol (v5.4)
Decision Latency	1,500 - 2,500 ms (Halts agents)	30 - 100 ms (Network hop)	200 - 500 ms (Cold start)	< 35 us (Sub-0.035 ms)
Execution Seam	External Cloud API	Network Edge Perimeter	Container Hypervisor	In-Process Memory + Edge Proxy
Determinism	Stochastic (Bypassed by jailbreaks)	HTTP status codes only	OS Container Boundary	100% AST Invariant Proof
Token & Cloud Cost	Doubles LLM token bills	Data transfer egress fees	Continuous VM compute cost	\$0 Token Spend (Local CPU)
Secret Masking	No (Exposes raw payload)	Basic TLS termination only	No inspection capability	Real-Time Automatic Token Scrubber
Audit Evidence	Plaintext unstructured logs	Centralized syslog / Splunk	Container exit status codes	Ed25519 Canonical Receipts
Integration Overhead	Complex asynchronous wrapping	DNS & proxy reconfiguration	Container image management	1-Line Decorator (@guard.protect)

TIER 1: DEVELOPER / COMMUNITY	TIER 2: TEAM FLEET	TIER 3: ENTERPRISE CUSTOM
\$0 / Free Forever (REAPER Model) • Unlimited local in-process AST evaluations. • Sub-35us execution safety & secret scrubbing. • Local Ed25519 cryptographic receipts. • Zero hard stops, zero crippleware. • <i>Drives developer lock-in as the default execution gate for all agent frameworks.</i>	\$49 / month (Self-Serve SaaS) • Centralized multi-agent policy dashboard. • Real-time Slack, Discord, and Webhook threat intercept alerts. • 1-Year cloud telemetry and analytics retention. • Up to 10M agent actions evaluated/month. • Multi-agent mesh policy synchronization.	\$24k – \$60k / year (Invoiced ARR) • Continuous SOC 2 Type II & HIPAA compliance auditor evidence packs. • Native SIEM streaming (Datadog Logs v2, Splunk HEC, AWS CloudWatch). • Custom proprietary AST grammar rules. • Dedicated cloud gateway edge nodes & SLA. • 88% – 94% Gross Margins.



THE SEED FINANCING & WHY BARTHOLOMEW IS THE FUTURE

SLIDE 8 / 8

Scaling From Organic Developer Standard to the Enterprise AI Agent Gatekeeper

THE SEED FINANCING ASK	CAPITAL ALLOCATION & THE FUTURE
• Round Size: \$2,000,000 USD • Instrument: Post-Money SAFE (\$15,000,000 Valuation Cap) • Cap Table Health: 100% founder-bootstrapped through v5.4 with \$0 prior institutional dilution. • Non-Dilutive Provenance: Accelerated by non-dilutive grant & compute backing from Google Cloud, Microsoft for Startups, and Amazon Web Services. • 18-Month Target Milestones: Reach \$1.5M ARR, scale to 25,000+ active developers, and close 30+ enterprise logos. • Founder & Contact: Itsub Alemayehu • Founder & Chief Architect Email: itsub@bartholomew.info • Web: https://bartholomew.info	• 60% Low-Latency Systems Engineering (\$1.2M): Hire 3 senior low-latency systems engineers (compiler AST, eBPF kernel tracing, and high-speed cryptography) to expand cross-language runtime gates. • 25% Enterprise Sales & Compliance Certification (\$500k): Complete formal SOC 2 Type II certification, expand HIPAA/GDPR modules, and convert the 12 design partner pilots into multi-year contracts. • 15% Developer Ecosystem Expansion (\$300k): Build native plugins for newly emerging frontier model agent SDKs (Anthropic, OpenAI, Meta, Google, xAI) and sponsor open-source agent hackathons. • The Future: Every computing paradigm shift creates a multi-billion dollar execution gatekeeper (Cisco for networking, Cloudflare for the web, CrowdStrike for endpoints). In the autonomous agent wave, Bartholomew is the execution gatekeeper.