

Brent Rockwood

Principal / Staff Software Engineer · AI Systems, Security & Systems Architect

Johns Creek, GA · +1 404-960-2864 · brent@brentrockwood.com

- <https://www.linkedin.com/in/brentrockwood/>
- <https://github.com/brentrockwood>
- <https://rockwoodlab.com>

SUMMARY

Principal / Staff Software Engineer with **30+ years of experience** building and operating software platforms, security systems, data-processing workflows, and operational tooling across **finance, cybersecurity, identity governance, and SaaS**.

Recent work centers on **AI systems and Linux-native infrastructure**: local and cloud model workflows, agent systems, retrieval and evaluation pipelines, and human-in-the-loop automation. Builds practical systems that combine deterministic software, data platforms, and AI models for reliable technical and operational decision-making.

Deep expertise in **Linux, TypeScript, security architecture, and large-scale distributed systems**. Brings hands-on systems experience—from application and data pipelines through containers, local inference, and production operations—and a long record of turning ambiguous requirements into maintainable working systems.

CORE SKILLS

AI Systems, Agents & Evaluation

Agent Workflows, Human-in-the-Loop Systems, RAG, Vector Databases, Knowledge Retrieval Systems, Model Evaluation Frameworks, Prompt & Context Engineering, Multi-Model Orchestration, Local LLM Infrastructure, Operational Automation

Linux, Infrastructure & Operations

Linux systems engineering, Docker, Devpods, local inference environments, infrastructure automation, AWS (Elastic Beanstalk, EC2, S3, RDS), CI/CD, Nginx

Languages & Runtimes

TypeScript, JavaScript, Node.js, Python, Go, Rust, C#, C++, SQL

Backend, Data & APIs

PostgreSQL, MS SQL Server, MySQL, SQLite, Qdrant, MongoDB, Redis, REST, GraphQL

Frontend

React, Redux, Tailwind, AngularJS (legacy)

AI Security & Systems

LLM and agent security, prompt injection, instruction hierarchies, AI control and monitoring, guardrails, model extraction, data poisoning, adversarial ML, ML threat modeling

Security & Architecture

RBAC, IAM Integrations, Data Governance, Compliance Reporting, Identity Lifecycle Management, Enterprise Security Architecture, Windows Kernel Development (historical)

PROFESSIONAL EXPERIENCE

Rockwood Lab — *Principal Engineer / Founder (AI Systems & Software Architecture)*

May 2024 – Present

- Founded and operate Rockwood Lab, an independent engineering practice focused on applied R&D, AI systems engineering, systems architecture, and full-stack delivery.
- Design and implement AI systems that combine local and cloud-hosted models, deterministic automation, retrieval, and human-in-the-loop workflows.
- Build and operate **Linux-based AI environments**, including containerized inference systems, developer tooling, local-model orchestration, and infrastructure automation.
- Develop agent-oriented systems for operational automation, documentation generation, infrastructure support, and software-development workflows.
- Develop vector-database-backed knowledge systems enabling semantic retrieval across technical documentation, runbooks, and project artifacts.
- Design evaluation and experimentation frameworks for comparing models, prompts, workflows, and autonomous behaviors.
- Port and adapt open-source AI systems—including Karpathy’s Autoresearch and NVIDIA OpenShell/NemoClaw—to local infrastructure environments.
- Develop multi-model orchestration tooling that coordinates frontier and local models in shared, repeatable workflows.
- Lead contract engagements delivering production React/TypeScript applications, including billing and payment-system integrations.
- Serve as technical lead and architect, owning requirements, system design, implementation, and delivery end-to-end.

Selected AI Systems & Infrastructure Projects

- **Autoresearch Strix Halo Port** — Ported and optimized Karpathy’s Autoresearch framework for AMD Strix Halo local infrastructure, enabling autonomous research workflows on local hardware.
- **OpenShell / NemoClaw Local-LLM Enablement** — Implemented Ollama provider support and contributed infrastructure for local and remote model orchestration within agent-driven development workflows.
- **Trio Multi-Model Collaboration Tool** — Built a command-line workflow coordinating frontier and local models for comparative analysis and collaborative problem solving.
- **Operational Knowledge & RAG Systems** — Designed vector-database-backed knowledge-retrieval systems integrating infrastructure documentation, runbooks, and operational procedures to support AI-assisted troubleshooting and decision-making.

Tech: TypeScript, JavaScript, Node.js, Go, Rust, Python, React, GraphQL, SQL, Docker, Linux, Qdrant, AI Tooling, Infrastructure Automation

Wells Fargo — *Vice President, Lead Information Security Engineer*

May 2019 – May 2024

- Architected and owned a suite of internal security platforms used to ingest, normalize, and visualize enterprise-wide cybersecurity and compliance metrics.

- Designed and operated event-driven platforms supporting enterprise security decision-making, regulatory reporting, and executive visibility across large-scale distributed environments.
- Built workflow automation and data-processing systems responsible for ingesting, normalizing, and correlating information from multiple enterprise sources.
- Designed event-driven data pipelines in Node.js and TypeScript feeding GraphQL APIs consumed by executive dashboards and federal oversight teams.
- Implemented delta-sync, partial-query caching, and resolver optimization, significantly reducing latency and payload size under load.
- Led cross-team design reviews to harden authentication, RBAC, and service-to-service API security.
- Systems supported CISO-level reporting and ongoing regulatory scrutiny at enterprise scale.

Tech: Node.js, TypeScript, React, Redux, GraphQL, MS SQL Server, Jenkins, Nginx

TEKsystems — *Senior Software Engineer*

2017 – 2019

- Delivered full-stack features for Fortune 50 retail and financial clients supporting high-throughput transactional workflows.
- Optimized GraphQL resolvers and query batching strategies.
- Refactored legacy Redux middleware into typed, normalized slices, improving maintainability and developer velocity.
- Built centralized logging and diagnostics pipelines.

Tech: Node.js, TypeScript, React, Redux, GraphQL, MS SQL, Elasticsearch

Soltech — *Senior Backend Developer / Technical Lead*

2016 – 2017

- Led backend development for automotive logistics and airline service platforms.
- Designed and deployed stateless microservices on AWS Elastic Beanstalk.
- Implemented PostgreSQL transaction strategies and connection pooling to reduce deadlocks under concurrency.
- Managed a small engineering team and reported directly to executive leadership.

Tech: Node.js, TypeScript, PostgreSQL, Docker, AWS

Independent Consultant

2001 – 2016

Selected engagements:

- **Identity Governance & IAM Integrations — Cenovus Energy, State of Colorado**
Built bidirectional identity lifecycle connectors integrating Quest One Identity Manager, Google Workspace, and enterprise service desks.
- **Enterprise AngularJS Component Library — Liberty Mutual**
Developed reusable UI components interfacing with large Java-based REST backends.

- **Municipal Election Reporting Platform — City of Halifax** Designed real-time vote aggregation system with fault-tolerant mobile ingestion.
- **Bitcoin Mining Marketplace — GAW Miners** Built Node.js backend services supporting cloud-based mining rentals and marketplace operations.

Quest Software / Dell Software — *Senior Software Engineer*

2004 – 2012

- Co-developed multiple commercial identity and governance products including Quest One Identity Manager (Data Governance Edition), Quest Group Policy Manager, and Quest Archive Manager.
- Implemented backend services and a Windows kernel minifilter driver to audit and intercept filesystem access.
- Reverse engineered Microsoft Group Policy internals and implemented XML-based comparison and reporting systems.
- Managed regression testing, installer packaging, and enterprise deployment tooling.
- Worked as a member of an Agile/Scrum software development team.

Tech: C#, C++, Windows Kernel APIs, NTFS, ADSI, MS SQL Server

Earlier Career

Software Engineer / Systems Analyst — Mount Sinai School of Medicine (1997–1999)

Developed NIH-compliant clinical trial software and supported neurology research systems.

Hardware & Software Generalist — Rockwood Electronics (1990–1997)

Built custom PCs, performed forensic troubleshooting, and developed Access/VBA automation systems.

PROFESSIONAL DEVELOPMENT

AI Security Bootcamp (AISB) — Las Vegas

Completed August 2026

Completed an intensive, hands-on AI security curriculum covering LLM and agent security, prompt injection and instruction hierarchies, AI control and monitoring, guardrails and jailbreaking, model extraction, data poisoning, adversarial ML, AI infrastructure security, and ML threat modeling. Completed hands-on security exercises and practical work involving coding-agent attack and defense scenarios, model-level attacks and mitigations, and infrastructure threat analysis.

EDUCATION

Bachelor of Computer Science Technical University of Nova Scotia

Completed two years of the program.