resume

russell sherman

CTO and co-founder. Applied AI, security, and platform engineering.

Boulder, Colorado · russ.sherman@gmail.com · neverenough.info

Updated Aug 7, 2026

Summary

Engineering leader working where applied AI meets security. Co-founded VISO TRUST in 2020, built the original product from concept to launch, and grew it past $7M ARR and 50 people before its acquisition by Protecht in April 2026 — continuing as CTO through the integration. Before that, led security engineering teams at ASAPP, Varo Money, Lending Club, and Dell SecureWorks. Current work is agentic systems in production: RAG and embeddings pipelines, multi-provider model routing, and eval harnesses running against real enterprise workloads.

Experience

CTO and Co-Founder — VISO TRUST

January 2020 — Present · San Francisco

- Co-founded a SaaS and AI startup that raised over 25 million dollars, developed the original product from concept to launch, and grew annual recurring revenue to more than 7 million dollars.
- Built and managed engineering teams across LLM development and SaaS delivery, scaling the organization from early founding engineers to a team of more than 50 people.
- Worked closely with product and go-to-market leadership to define the roadmap, shape market positioning, support major enterprise deals, and establish the company’s operating model.
- Architected a polyglot platform spanning a Java 21 / Spring Boot backend with GraphQL and REST APIs over PostgreSQL, an Angular signals-era frontend, and a Python FastAPI AI service, delivered on AWS ECS through GitHub Actions CI/CD.
- Built the applied-LLM layer behind the product: RAG and embeddings pipelines, document parsing and chunking, vector search over OpenSearch and pgvector, and multi-provider model routing across Bedrock, Anthropic, and OpenAI.
- Shipped agentic workflows in production for control validation, questionnaire answering, artifact ingestion and reprocessing, subservicer detection, and risk advisory generation, backed by a pytest eval harness, prompt optimization, and LLM tracing in Arize Phoenix.

- Established engineering practice across the organization: OAuth2/OIDC and multi-tenant isolation, OpenTelemetry observability, feature-flagged continuous delivery, supply-chain controls including SBOM generation and dependency pinning, and a structured multi-agent AI-assisted development workflow with human approval gates.
- Led the company through its acquisition by Protecht, an Australian-based global GRC provider and PSG Equity portfolio company, in April 2026; continuing as CTO to integrate VISO TRUST's agentic AI capabilities into the combined platform.

Manager, Security Engineering — ASAPP
January 2018 — January 2020 · New York City

- Led a software engineering team that built the services and integrations needed to connect off-the-shelf detection and response tools into the company's security ecosystem.
- Designed and maintained detection pipelines that combined vendor tools with custom code for data ingestion, signal enrichment, correlation, and alert routing at scale.
- Managed incident response workflows by improving automation, reducing manual steps through custom integrations, and coordinating with engineering teams to deliver durable fixes.

Principal Security Engineer — Varo Money
January 2018 — November 2018 · San Francisco

- Ensured security program visibility and prioritization by serving as a member of the Compliance and Operational Risk Management Team, Risk Leadership Team, and IT Steering Committee.
- Performed information security risk assessment and established the security engineering roadmap based on compliance maturity and risk, allowing for OCC preliminary federal bank charter application approval.
- Developed AWS security architecture strategy using Terraform, enforcing service IAM role-based authentication, web application protection, data encryption, and centralized logging and monitoring.
- Developed a user IAM strategy and implemented it with SSO (Okta) with centralized identity via Active Directory, thereby enforcing role-based authorization and multi-factor authentication for both corporate VPN and SaaS platforms.

Senior Manager, Security Engineering — Lending Club
September 2014 — December 2017 · San Francisco

- Led a team of 5 security engineers, significantly increased efficiency by implementing an agile-inspired system and a standardized security event response framework, and mentored software engineering effort to build various in-house security systems and management tools.

- Developed automation utilities and web applications to inventory and schedule dynamic application security tests, report and alert on publicly available threat surface by correlating network and application infrastructure information, dynamically manage syslog forwarding infrastructure, and mint and deploy key material for certificate-based authentication and communication encryption.

Senior Network Security Analyst — Dell SecureWorks

November 2013 – September 2014 · Atlanta

- Performed real-time analysis and correlation of logs from a multitude of client network and application security devices to determine whether said logs constitute security incidents.
- Configured and maintained network intrusion detection devices and other proprietary or open source security appliances to secure client networks.

Technical Application Analyst — ADP

March 2010 – November 2013 · Chicago

- Served as project manager on product enhancements and system implementations for over 10 enterprise clients.
- Troubleshot, deployed, and secured IP time clock terminals using network expertise and familiarity with the hosted product infrastructure.

Technical skills

- **Languages** — Java, TypeScript, Python, JavaScript, Go, SQL, Ruby, Bash, HCL
- **Backend** — Java 21, Spring Boot 3 (MVC, WebFlux, GraphQL, Security, Data JPA, Batch, Session, Quartz, Actuator), Hibernate 7 + Envers, Blaze Persistence entity views, MapStruct, Gradle multi-project builds; Python 3.13, FastAPI, Uvicorn, Pydantic v2, SQLAlchemy/Alembic, uv
- **APIs and data** — GraphQL schema design and resolver implementation, Apollo, Strawberry; REST/OpenAPI; PostgreSQL, Liquibase migrations, query-performance and N+1 avoidance via projections, Redis, pgvector, OpenSearch
- **AI/ML engineering** — Spring AI, AWS Bedrock, Anthropic, OpenAI, Ollama, Vertex, LiteLLM; Agno agent framework, AG-UI, Model Context Protocol (MCP), CopilotKit; RAG pipelines, embeddings and vector stores, Docling parsing/chunking, tree-sitter; Arize Phoenix tracing and evals, GEPA prompt optimization, pytest-based eval harnesses and model benchmarking; OpenInference instrumentation
- **Frontend** — Angular 21 (standalone components, signal APIs, OnPush, native control flow), NgRx Signal Store, Apollo Client with GraphQL subscriptions, Angular Material + CDK, Tailwind CSS v4, TypeScript 5.9 strict, Chart.js, vis-network, Quill, Bun
- **Cloud and infrastructure** — AWS (ECS/ECR, S3, SQS, Lambda, Secrets Manager, Bedrock, OpenSearch, Comprehend, Marketplace metering, Encryption SDK), Terraform, Docker/docker-compose, Jib, LocalStack, GitHub Actions CI/CD

- **Observability** — OpenTelemetry (SDK, OTLP, Java agent) to Honeycomb, Micrometer/Prometheus, New Relic, structured JSON logging
- **Security and identity** — OAuth2/OIDC, Okta, Keycloak, JWT, role-based authorization, multi-tenant data isolation, field-level encryption, SBOM generation and supply-chain hygiene, ArchUnit architecture tests
- **Testing** — JUnit 5, Mockito, Spring Boot Test, Awaitility, MockWebServer; Jest; Playwright E2E; pytest
- **Integrations and tooling** — Workato connectors (Ruby SDK) for BitSight, Recorded Future, SecurityScorecard, Vanta, Workday; LaunchDarkly, Postmark, Slack API, Metabase, LogRocket, Apache POI, PDFBox