TECHNICAL CAPABILITY STATEMENT

DEMONIC BINARY

Mobile · Backend · Security Engineering

California-based
Remote and onsite by agreement
demonicbinary.com
sales@demonicbinary.com

Find the failure. Fix the system. Verify the result.

Demonic Binary works with product and engineering teams on difficult problems across native mobile applications, APIs, identity systems and production infrastructure. We separate diagnosis, agreed code-level implementation and verification so each engagement has clear boundaries.

Native mobile engineering

Swift, Kotlin, iOS and Android architecture; authentication flows; device trust, offline recovery, releases and lifecycle defects.

Backend & API systems

Service integration, API authorization, multi-tenant boundaries, system reliability, testing and operational troubleshooting.

Security and adversarial review

Authorized security testing, threat modeling, protocol analysis, trust-boundary assessment and prioritized technical remediation.

Release & platform hardening

CI/CD integrity, rollback design, observability, incident follow-up and validation against agreed acceptance criteria.

AI and agent integrations

Tool permission boundaries, service integrations, workflow testing, evaluation and human oversight for applied AI systems.

Engineering ownership

Defined technical investigation, production-safe changes when approved, regression tests, evidence handoff and optional follow-on support.

Typical engagement sequence

01 Diagnose: establish symptoms, authorize access and identify evidence. **02 Fix:** implement an independently approved scope. **03 Verify:** test the failure, regressions and operational handoff.
A diagnostic can stand alone; implementation and continuing support are separately contracted.

Inspectable engineering evidence

- First-party Cloudflare Worker routing incident and tested fix.
- Internal simulated SiteGuard monitoring and API authorization labs.
- Published mobile/backend engineering overviews and security research.

Labs and samples are labeled; they are not represented as approved named-customer results.

Engagement and procurement boundaries

- Written scope, permitted environments and accountable client owner.
- Deliverables, access restrictions, change control and acceptance tests.
- NDA, SOW, data protection and vendor documentation as applicable.

Insurance, certifications, legal entity details and third-party customer references require document-level verification; none are asserted here.