Redwoods Research

Founded in 2020, Redwoods Research builds and operates confidential-compute Super Intelligence (SI)/AI systems and network collection infrastructure — for environments where the data is the mission. Our team, co-founders of the communities behind The Tor Project, DarkOwl, and the first large-scale domain intelligence platforms, spans three decades across industry and government.

We design and build the systems that collect the intelligence, and the confidential-compute SI/AI that turns it into decisions — end to end, blind to everyone but you.

NAICS 541511, 541512, 541519, 518210

Record of Delivery

Redwoods has built, deployed, and trained customer teams to maintain fully encrypted, near-terabit collection networks for US IC, DoD, FVEY and allied services, and Interpol — petabytes per day, on COTS hardware, in data centers across 31 countries.

Selected work:

- **SHARKSEER** (NSA / DISA)
- **MEMEX, SAFER** Warfighter (DARPA) — both through Phase 3 to commercialization
- **The Tor Project** — the anonymous, multilayer encrypted overlay network; a global proxy network for exfiltration from targeted countries (PoC)
- **Interpol** (human trafficking/child exploitation) — a gateway for member states to share terabytes of open-case data, CSAM segregated from operational traffic; a near-real-time darknet index (text, context, multimedia) with an agency-only tier for sensitive content
- **Army CID / Navy CIS** — technical advisory and investigator training: darknet traffic, markets, cryptocurrency, undercover work; a low-cost dedicated workstation for safe darknet operation
- **CRISP** (DOE) — piloted actionable cyber threat information sharing protecting the US grid
- **Lineage** — Co-founder, The Tor Project; co-founder, DarkOwl (adversary emulation, darknet search); C-suite, TechTarget and Farsight Security (now DomainTools), domain and security analytics; head of engineering, Norse Federal.

We are proud members of the Fort Meade Alliance, INSA, AFCEA, and TUG.

www.redwoodsresearch.com | +1 415-316-9794 | sales@redwoodsresearch.com

#DUNS Number 11-933-9939 SAM.gov Unique Entity ID: RSCXUUNXND28 SAM.gov CAGE/NCAGE: 0YGF1 #CAL E-Procure Bidder/Supplier ID: BID0118873

Confidential SI/AI

Confidential SI/AI is an end-to-end encrypted inference platform for OSINT and signals intelligence. It trusts nothing — not the model, not the user, not the build. Public, open-weight, or customer-developed models, of any size, run read-only inside a TEE; every instance is isolated behind post-quantum public-key cryptography (PQC); every release ships as a reproducible Rust binary with minimal dependencies.

- **Encrypted at rest, in transit, and in processing.** Your queries are encrypted with your public key and decrypted only inside the TEE — outside the OS. We never see your data. Zero-Trust Principles provide constant attestation.
- **You hold the key.** Only you hold the private key. We store only the public key.
- **Post-Quantum Cryptography.** We use X-Wing (ML-KEM-768 + X25519 hybrid) and HKDF-SHA256 + AES-256-GCM post-quantum cryptographic algorithms.
- **Your terms, your schedule.** We build to your spec, price, and service level. Host it in your data center or subscribe to our service.
- **You own what you buy.** Full support, training, and he ability to keep it running — unlike proprietary stacks, which lock you in. Optional same-developer support over end-to-end encrypted chat, voice, or video.

Network Collection & Intelligence

We build collection architectures that scale to your mission — from the edge to the data center — on COTS hardware.

Collection

- Open-source collection and normalization up to 400 Gbps, with near real-time triage.
- Capture and analysis of encrypted communications.
- Analysis of darknet-market tradecraft.
- OSINT collection on COTS hardware and open-source tooling.
- Active and passive signal interception, with noise reduction.
- Compartmentalized, low-attribution-risk collection infrastructure.

Integration & Intelligence

- We fuse collection feeds into queryable, operational intelligence on event-driven data pipelines and data lakes — Elasticsearch, Apache Cassandra, Hadoop — or with Apache Drill querying Parquet and HDF5 directly.
- Adversary emulation and offensive and defensive cyber operations, keeping collection ahead of counter-collection.
- High-throughput, fully encrypted networks, demonstrated at near-terabit scale on COTS hardware, cross-country and customer-hosted.
- OPSEC and second-order risk engineering — host licensing, mosaic exposure, chain of custody — built into every design.

Internet collection. Network collection.
We build both — quietly, to your mission.

Redwoods Research