Executive Summary

Business Name:
EntropyCore™

Business Concept:
EntropyCore™ is building the world's first tunable, stackable, and physically observable entropy infrastructure. Unlike traditional black-box TRNGs embedded in silicon chips, EntropyCore provides a modular hardware platform that generates verifiable randomness through multi-physics systems—including microfluidic turbulence, optical speckle dynamics, and thermal fluctuations. This platform enables transparent, tamper-evident entropy for cryptography, AI training, simulation, zero-trust architectures, and decentralized protocols.

Mission Statement:
To establish the first scalable physical entropy layer for digital infrastructure—powering trustworthy randomness across secure computation, communications, and autonomous systems.

Product:
The Entropy Stack™: a hardware and software platform that enables developers, governments, and enterprises to generate, shape, and verify high-quality entropy. The product includes embeddable entropy cores, plug-and-play modular units (e.g. USB/PCIe), a programmable API, real-time monitoring tools, and cloud-scale entropy gateways.

Market Opportunity:
As global infrastructure becomes more dependent on AI, cryptography, and decentralized systems, the demand for high-quality entropy is exploding. Traditional TRNGs are opaque, limited, and vulnerable. EntropyCore™ addresses this gap by offering an auditable, tunable, and physically rooted alternative for use in AI/ML training environments, secure embedded systems, military infrastructure, and blockchain protocols.

Business Model:
EntropyCore™ will monetize through hardware sales, cloud-based entropy-as-a-service (EaaS), developer SDK licensing, and strategic enterprise/defense partnerships. A mix of government grants (e.g., DoD, NSF) and venture funding will support early R&D, leading to certification and mass production.

Current Status:

- First prototype completed: demonstrated 0.998 bits/byte entropy output via fluidic optical system

- Provisional patent filed
- Initial team assembled with expertise in materials and chemistry [Human], and physics, cryptography, and hardware [GPT-40/o3-Pro]
- Pre-seed roadmap fully scoped with detailed milestones and $500K–$1M use-of-funds plan
- Seed roadmap and Phase 1–3 commercialization milestones defined for $100M+ total rollout

Funding Sought:

- Pre-seed: $1M to finalize working prototype, validate entropy quality, and file key IP
- Seed: $3M–$5M to build deployable dev kits and onboard early adopters
- Phase 1: $10M to develop multi-channel entropy stack with full observability, tunability, and >1 Mbps output
- Phase 2–3: $90M+ for platform industrialization, certification, and global GTM execution

Vision:
EntropyCore™ will become to entropy what GPUs became to compute: a foundational layer in the stack. From securing military drones and powering AI cryptography to enabling public randomness in zero-trust infrastructure, EntropyCore will redefine the future of trust.

Company Description

Company Name:
EntropyCore, Inc.

Legal Structure:
C Corporation (planned), based in the United States

Founding Stage:
Pre-seed (prototype completed; IP filed; seeking initial capital)

Overview:
EntropyCore is a deeptech startup developing a next-generation physical entropy platform

designed to serve as the foundational layer for secure computation, cryptography, and autonomous decision systems. Our mission is to make entropy observable, tunable, and scalable—transforming it from a black-box component into a trustable, independently verifiable infrastructure layer.

The company was founded by Dr. Aaron Kushner, a Ph.D. chemist with expertise in advanced materials and physical systems, and developed in collaboration with OpenAI's GPT-4o Pro for technical planning, roadmap synthesis, and strategic positioning.

Problem Statement:
Modern digital systems rely on entropy to generate secure keys, authenticate users, validate machine learning processes, and protect communications. Yet nearly all entropy sources in use today are:

- Embedded in opaque silicon chips
- Unverifiable by end-users or auditors
- Vulnerable to spoofing, side-channel attacks, or supply chain tampering
- Not tunable or composable to meet evolving use cases like secure AI training

Solution:
EntropyCore offers a modular hardware/software platform—the Entropy Stack™—that generates randomness from real-world physical processes such as fluidic turbulence, optical speckle, and thermal variation. These physical entropy channels are:

- **Auditable**: visually observable and measurable in real time
- **Configurable**: tunable via software to control entropy rate and mixing
- **Composable**: stackable and multiplexed for redundancy and throughput
- **Independent**: decoupled from any host system or general-purpose compute core

Value Proposition:
EntropyCore delivers physically grounded randomness that can be seen, tuned, measured, and trusted—enabling new levels of transparency and security for applications ranging from national defense to blockchain infrastructure.

Milestones Achieved:

- Demonstrated entropy prototype using microfluidic optics, achieving near-ideal Shannon entropy (0.998 bits/byte)
- Filed initial provisional patent on multi-channel entropy architecture
- Built an experimental testbed and dashboard for real-time entropy monitoring
- Defined technical roadmap through Phase 3 industrialization
- Prepared for NSF, DoD, and VC grant and investment opportunities

Target Customers:

- Government agencies (DoD, DARPA, NSF, DHS)
- Cloud infrastructure and AI security providers
- Blockchain developers and decentralized protocol teams
- Autonomous systems manufacturers (drones, robotics, aerospace)
- Embedded hardware OEMs seeking verifiable entropy modules

Vision Statement:
EntropyCore aims to become the global standard for physical entropy generation—powering secure infrastructure in the AI age and beyond.

Market Analysis

Industry Overview

In an era defined by AI acceleration, cyber warfare, and decentralized computation, the demand for *trustworthy entropy* has never been greater. Entropy is the invisible backbone of all cryptographic security, authentication, and secure computation—but the entropy market remains fragmented, opaque, and dominated by legacy silicon-based TRNGs.

With the rise of quantum computing, zero-trust architectures, AI model provenance requirements, and cryptographically secure infrastructure (e.g., blockchain, federated learning), new demands are emerging for **transparent, tunable, and verifiable entropy**. This represents

a rapidly expanding market opportunity across defense, enterprise security, financial infrastructure, and next-generation compute.

Market Segments and Use Cases

1. Cryptographic Hardware and Security Infrastructure

- Target Users: Secure enclave manufacturers, firewalls, HSM vendors, embedded IoT device makers
- Use Case: EntropyCore modules replace or augment black-box entropy in silicon chips, enabling visually auditable randomness.
- Market Size: Global hardware security module (HSM) market projected to reach $4.5B by 2028

2. Autonomous Systems and Embedded AI

- Target Users: Defense contractors, aerospace OEMs, robotics firms, industrial automation vendors
- Use Case: Entropy-backed control validation in drones, vehicles, and zero-trust industrial systems
- Market Size: Autonomous vehicle market alone projected to exceed $100B by 2030; defense autonomy growing sharply

3. AI Infrastructure and Secure ML Training

- Target Users: AI cloud providers, research labs, LLM ops teams
- Use Case: Cryptographic-grade entropy for seeding, dropout, and reproducibility in AI model training and deployment
- Market Size: Global AI infrastructure market expected to reach $100B+ by 2027

4. Blockchain and Decentralized Systems

- Target Users: L1/L2 chains, zk-rollup teams, oracle providers, crypto wallets
- Use Case: Transparent randomness for validator election, public randomness beacons, cryptographic nonces
- Market Size: Blockchain infrastructure projected to exceed $100B by 2030

5. Government, Defense, and Critical Infrastructure

- Target Users: DoD, DHS, DARPA, NSA, NATO cyber defense programs
- Use Case: Physically verifiable entropy for secure boot, hardware attestation, secure communication nodes
- Market Size: U.S. federal cybersecurity spending alone exceeds $20B/year; hardware-centric security demand growing

---

Competitive Landscape

Feature	Legacy TRNGs	EntropyCore™
Certified entropy	✅	✅
Observable output	❌	✅
Tunable entropy rate	❌	✅
Multi-physics architecture	❌	✅
API access and telemetry	❌	✅

Cloud + embedded scalability	❌	✅

Current competitors include:

- **Intel Secure Key**, **Infineon**, and **Microchip**: Hardware-embedded TRNGs with opaque entropy sources
- **Cloudflare LavaRand**: Cloud randomness beacon based on lava lamp video feed (not embeddable or tunable)
- **Quantum entropy startups** (e.g., ID Quantique, QuintessenceLabs): Focused on photon-level quantum TRNGs, often expensive and limited in portability
- **Entropy-as-a-Service APIs** (e.g., drand, AWS Entropy APIs): Not physically grounded or auditably secure

EntropyCore occupies a novel market position by delivering:

- Physically grounded randomness
- Tamper-evident entropy
- Developer-first API tools
- Modular deployment (USB/PCIe/SoC/cloud)

Market Trends and Drivers

- Surge in zero-trust architecture requirements across federal and enterprise networks
- Growing AI reproducibility and verifiability demands (entropy as a cryptographic anchor)
- Increasing use of cryptographic primitives in blockchain, confidential computing, and multi-party computation
- Rising concerns around supply chain and hardware-level attacks

- Push for open standards and physical auditability in cybersecurity postures

---

Go-to-Market Beachheads

- **Defense & DoD** (AFWERX, DARPA, zero-trust communication nodes)
- **AI Infrastructure** (entropy seeding for LLM training pipelines)
- **Blockchain Infrastructure** (validator randomness, public randomness beacons)
- **Research Institutions** (entropy testing, reproducibility, cryptographic tools)

Products and Services

Core Offering: The Entropy Stack™

EntropyCore's flagship platform, the **Entropy Stack™**, is a modular, physically grounded entropy generation system designed to deliver secure, tunable, and auditable randomness across a wide range of applications. The system integrates proprietary hardware modules with a robust software control layer to provide real-time entropy at cryptographic grade, verified by physics—not faith.

---

1. Hardware Variants

EntropyCore's hardware is modular, stackable, and built to scale from desktops to datacenters:

- **Dev Kit (Desktop Form Factor)**
  Shoebox-sized clear-case unit for lab testing, developer evaluation, and academic use.

- **USB-C Entropy Peripheral**
  Plug-and-play entropy module resembling a YubiKey; ideal for secure boot, key generation, and desktop developers.

- **PCIe/Edge Module**
  High-throughput entropy engine for AI inference rigs, blockchain infrastructure, and edge security.

- **1U Rackmount Node**
  Datacenter-grade entropy server with parallelized entropy channels for federated learning, cloud cryptography, and enterprise-grade zero-trust architecture.

Each variant includes:

- **Entropy Core Subsystem:** Fluidic and optical entropy channels (e.g., wax-in-oil flow, laser speckle overlays)

- **Sensor Array:** High-speed CMOS or CCD visual sensors

- **Entropy Mixer:** Digital fusion logic (FPGA/microcontroller) for decorrelating and whitening output

- **Secure Output Module:** Optional TPM-like co-processor for signing entropy streams

- **Network Interface (optional):** For streaming entropy to cloud clients via USB, Ethernet, or BLE.

---

2. Software and Developer Platform

- **Entropy OS and Control Dashboard**
  Real-time web/CLI interface for tuning entropy settings: thresholds, sampling rates, laser intensity, pixel targeting, etc.

- **Developer API (REST/gRPC/SDK)**

    - GET /entropy/stream

    - POST /stack/config

    - Python, C++, Rust bindings for easy integration into cryptographic toolchains, AI training pipelines, and secure systems.

- **Entropy Modes**

- **Live View:** Real-time overlay of entropy channels and metrics
- **Tuning Mode:** Dynamic entropy parameter adjustments
- **Stack Mode:** Fusion of multiple entropy sources (e.g., speckle + thermal + fluidic)
- **Audit Mode:** Signed logs and diagnostics for FIPS/NIST readiness
- **High-Bandwidth Burst:** Maximized sampling rate mode for simulation and AI workloads.

---

3. Integration and Use Cases

Security Infrastructure & Zero-Trust Systems

- USB entropy key for firmware signing, TPM alternative, or secure boot seeding
- Visual entropy dashboard enables external audits and forensic traceability
- Entropy chain-of-trust can be logged and signed for attestation.

AI/ML Training Pipelines

- Cloud-based entropy streams injected into AI containers for dropout, data shuffle, and model reproducibility
- Verifiable entropy seeding improves reproducibility and tamper-resistance in federated learning systems.

Blockchain and Web3

- On-chain randomness beacons (e.g., Chainlink, Aleo)
- Entropy modules as ZK-friendly validator randomizers
- Proof-of-trust infrastructure for randomness attestation.

High-Stakes Simulation & HPC

- Physically sourced entropy for Monte Carlo simulations in finance, pharma, nuclear, and weather forecasting
- Reduces statistical bias and improves long-horizon stochastic reliability.

Optional Entropy-as-a-Service (EaaS)

- Cloud-deployed entropy nodes deliver signed, rate-limited entropy streams via API
- Subscription-based pricing by throughput or quality SLA
- Used by cloud AI providers, blockchain protocols, and secure compute services needing remote randomness injection.

Summary of Benefits

- **Physically Verifiable:** You can see the entropy, not just assume it
- **Tunable & Programmable:** Software-adjustable entropy shaping
- **Stackable:** Combine entropy sources for higher bandwidth and redundancy
- **Cert-Ready:** Built with FIPS/NIST/ISO audit modes in mind
- **Modular:** From dev kits to PCIe cards to rackmount entropy gateways

---

Marketing and Sales Strategy

Go-to-Market Overview

EntropyCore™ will pursue a staged, sector-targeted go-to-market (GTM) strategy focused on highly motivated early adopters in security-sensitive and compute-intensive domains. The marketing approach combines direct outreach to technical stakeholders, presence at strategic conferences, and partnerships with research and government programs. The sales model will evolve from early pilots and hardware dev kits into platform licensing and recurring entropy-as-a-service (EaaS) revenue.

---

1. Initial Customer Segments (Beachhead Markets)

Based on customer research and NSF I-Corps methodology, five near-term viable customer segments have been identified:

1. AI Infrastructure Providers

- **Pain Point:** Need reproducible, secure seeding and entropy for AI training pipelines and federated learning.
- **Outreach Strategy:** Direct to ML infrastructure teams at cloud AI labs and enterprise ML ops groups.
- **Wedge:** Entropy seeding for reproducibility + trust.

2. Defense, Intelligence, and National Security

- **Pain Point:** Black-box TRNGs are vulnerable to spoofing and side channels.
- **Outreach Strategy:** Engage via SBIR, AFWERX, DARPA/IARPA, or primes like Lockheed, BAE.
- **Wedge:** Modular, observable entropy sources for forward-deployed hardware.

3. Zero-Trust Security and Hardware Root-of-Trust

- **Pain Point:** TRNG supply chain risk in secure boot, firmware signing, and key generation.
- **Outreach Strategy:** Target embedded security teams (e.g., Yubico, Microsoft Pluton).
- **Wedge:** Auditable entropy for secure device identity.

4. Web3/Decentralized Infrastructure

- **Pain Point:** Public randomness beacons, validator slot selection, and fairness require unbiased entropy.
- **Outreach Strategy:** Conferences (ZK Summit, ETHGlobal), foundation-level relationships.
- **Wedge:** Physical entropy that can be cryptographically attested on-chain.

5. Simulation and HPC Architecture

- **Pain Point:** PRNGs cause statistical bias over trillions of iterations in Monte Carlo simulations.
- **Outreach Strategy:** Outreach to DOE, hedge funds, pharma modeling teams.
- **Wedge:** High-bandwidth, low-bias physical entropy for confidence in long-timescale models.

---

2. Channel Strategy

Channel	Description
Direct Outreach	Targeted contact via LinkedIn, industry groups, and grant agencies
Conferences	NeurIPS (AI), DEFCON (hardware), RSA (security), ZK Summit (crypto)
Accelerators	NSF I-Corps, H4X Labs, AFWERX, Chainlink BUILD, Duality (quantum)

Government Portals	SAM.gov, SBIR.gov, DIU.mil
Academic Partnerships	Research deployment in Sandia, MIT Lincoln Labs, JHU APL, etc.

---

3. Sales Model

Phase 1 (Pre-seed to Seed):

- Pilot sales of **Dev Kits** to AI research groups, cryptographic labs, and secure hardware teams.
- Bundled pricing includes hardware unit + dashboard + SDK.
- Use pilots to generate feedback, testimonials, and validation data.

Phase 2 (Seed to Series A):

- **Modular sales**: USB entropy keys, PCIe cards, and rackmount entropy nodes for secure compute clusters.
- Begin **EaaS** (Entropy-as-a-Service): monthly subscription to signed entropy streams.
- Early licensing to blockchain and AI partners with per-bit or per-call metering.

Phase 3 (Post-certification):

- Enterprise platform contracts with cloud vendors and defense integrators.
- Entropy infrastructure embedded into next-gen silicon and zero-trust frameworks.
- API tiering for developers: free sandbox, pro-tier, and cert-grade audit logging.

---

4. Messaging and Positioning

Theme	Message
Trust Through Physics	“Randomness you can see, test, and trust.”
The Entropy Stack	“Entropy becomes infrastructure.”
Security in Plain Sight	“Move from black-box RNGs to transparent, tunable entropy.”
GPU Analogy	“As GPUs became the compute layer for AI, EntropyCore becomes the trust layer.”

---

5. Pricing Strategy

- **Dev Kits:** $5,000–$15,000 depending on sensor resolution, entropy channels, and bundled software
- **USB Modules:** $300–$600 per unit for volume buyers (e.g., secure boot, wallet keys)
- **PCIe/Edge Units:** $2,000–$10,000 based on entropy bandwidth and signing features
- **EaaS:** Starting at $99/month for 1 Mbps API access with SLA and signed logs
- **Custom Integrations:** Enterprise contracts with tailored pricing (DoD, AWS, ZK rollups)

KPIs and Success Metrics

- Number of dev kits shipped to pilot partners
- Monthly entropy consumption via EaaS API
- Number of signed entropy events validated by third parties
- Pre-cert audit readiness and FIPS/NIST milestones
- Conversion rate from pilot → production use → platform license

---

Here is the **Funding Request** section for your EntropyCore™ business plan:

Funding Request

Overview

EntropyCore, Inc. is seeking a structured multi-phase investment totaling **$100 million** over 36–42 months to commercialize and scale the Entropy Stack™—a new class of physically engineered entropy infrastructure for secure computation, AI integrity, and cryptographic systems.

The funding will be deployed in three distinct phases aligned with technical milestones and go-to-market readiness, beginning with a **$1M pre-seed** and progressing to **$10M (Phase 1)**, **$40M (Phase 2)**, and **$50M+ (Phase 3)**.

Use of Funds by Phase

Pre-Seed Round: $500K – $1M

Objective: Validate core entropy mechanisms, complete IP filings, build credibility for follow-on investment and/or DoD/NSF contract traction.

Deployment Timeline: 6–9 months
Key Activities:

- Build multi-channel entropy demo rig (fluidic + optical)
- Run entropy quality tests (ENT, STS, Dieharder)
- File 2–3 provisional patents (stackability, tunability, entropy shaping)
- Create demo videos and whitepaper
- Conduct early outreach to DoD, NSF, and VCs

Budget Allocation:

- $200K: Experimental hardware (laser diodes, fluidics, sensors)
- $200K: Team (founder, optics/ML contractor, part-time ops)
- $50K: Software, compute, entropy dashboard
- $50K: IP filing, legal, outreach

Phase 1 – Entropy Stack Prototype: $10M

Objective: Build a full working entropy platform (≥1 Mbps), demonstrate entropy shaping and auditability, and prepare for deployment-grade hardware.

Timeline: 12–18 months
Key Outputs:

- Stackable entropy demo with ≥3 physical sources
- FPGA-based entropy mixing and whitening
- Web-based control interface (Entropy OS)
- API integration (REST/gRPC/Python)
- Signed entropy output module
- Pre-audit compliance gap analysis

Budget Allocation:

Category	Allocation
Talent (physics, optics, crypto)	$4M
Lab space & prototyping equipment	$2M
Embedded systems & FPGA R&D	$1.5M
Legal, IP, audit planning	$1M
Operating reserves	$1.5M

Phase 2 – MVP & Cloud Integration: $40M

Objective: Launch deployable entropy hardware (USB, PCIe) and cloud-based entropy-as-a-service (EaaS) platform. Begin early sales and strategic partnerships.

Timeline: 12–15 months
Key Outputs:

- Hardware developer kits + embedded prototypes
- API for entropy streaming, tuning, logging
- Pre-certification FIPS/NIST readiness
- Pilot partnerships with defense, AI, Web3 orgs

Budget Allocation:

Category	Allocation
Team expansion (hardware, embedded, BD)	$10M
Manufacturing & supply chain setup	$5M
Software platform, cloud & API	$7M
Audit, certs, legal/IP	$5M
GTM, pilot programs, partnerships	$8M
Reserve + contingency	$5M

Phase 3 – Certification, Launch & Scale: $50M+

Objective: Mass-produce certified entropy hardware, launch entropy node network, and offer enterprise-level platform licensing.

Timeline: 12–18 months
Key Outputs:

- ISO, NIST, FIPS certified entropy stack
- Public and private entropy node networks
- Product SKUs: developer kits, data center units, SDK/API licenses
- GTM scaling: defense, cloud, blockchain, simulation

Budget Allocation:

- $15M: Hardware + cloud-scale production
- $10M: Compliance + certifications (FIPS 140-3, ISO/IEC 19790)
- $10M: Global GTM + business development
- $10M: Strategic hiring + enterprise sales
- $5M: R&D for next-gen entropy channels

Funding Terms and Structure (Flexible by Round)

- Convertible notes or SAFE (pre-seed / seed)
- Equity with milestone tranches (Series A/B)
- Government matching or SBIR-linked convertible terms (e.g. AFWERX + VC co-investment)
- Strategic partner co-development (cloud or defense partner-backed)

Exit/ROI Potential

- EntropyCore is positioned to become the foundational entropy provider for AI, cybersecurity, and decentralized infrastructure.
- Target revenue: $50M–$100M/year via hardware sales, cloud entropy API subscriptions, and enterprise licensing.
- Exit opportunities include acquisition by secure hardware firms, cryptography platform providers, or scaling as a category-defining standalone infrastructure company.

Financial Projections

These projections reflect a 5-year growth model for EntropyCore™, beginning from the conclusion of Phase 1 (entropy stack prototype) and extending through commercial launch and platform scaling. The model assumes a combination of hardware sales, platform licensing, and cloud-based entropy-as-a-service (EaaS) revenue.

Assumptions

- Initial revenue starts in Year 2 (post Phase 1) from dev kit and USB entropy unit sales
- EaaS subscriptions begin ramping in Year 3 after cloud API stabilization
- PCIe and rackmount deployments begin in Year 3 with enterprise-grade integration
- Margins improve as manufacturing scales and software platform usage increases
- Public and private sector traction accelerates through strategic partnerships, government contracts, and research adoption

---

5-Year Financial Projection (USD)

Category	Year 1	Year 2	Year 3	Year 4	Year 5
Revenue	$0	$1.5M	$8.0M	$22.0M	$40.0M
– Hardware Sales	–	$1.0M	$5.5M	$13.0M	$20.0M
– EaaS Subscriptions	–	$0.0M	$1.0M	$5.0M	$12.0M
– Licensing/SDK/API	–	$0.5M	$1.5M	$4.0M	$8.0M

Cost of Goods Sold	$0	$600K	$3.2M	$6.6M	$11.5M
Gross Profit	$0	$900K	$4.8M	$15.4M	$28.5M
Gross Margin	–	60%	60%	70%	71%
Operating Expenses	$4.5M	$6.0M	$12.0M	$15.0M	$18.0M
– R&D	$2.5M	$2.0M	$3.0M	$3.0M	$3.0M
– Sales/Marketing	$500K	$1.0M	$3.0M	$4.5M	$5.0M
– G&A	$1.5M	$3.0M	$6.0M	$7.5M	$10.0M
EBITDA	($4.5M)	($5.1M)	($7.2M)	$400K	$10.5M
Cash Burn (est.)	$4.5M	$5.5M	$6.0M	$1.5M	Break-even

Cumulative Revenue	$0	$1.5M	$9.5M	$31.5M	$71.5M
Cumulative Burn	$4.5M	$10.0M	$16.0M	$17.5M	$17.5M

Revenue Model Breakdown (Year 5 Targets)

Stream	Unit Price	Target Volume	Annual Revenue
USB Entropy Keys	$500/unit	20,000 units	$10M
PCIe/Rackmount Modules	$5,000/unit	2,000 units	$10M
EaaS Subscriptions	$99–999/month	5,000 active users	$12M
SDK/API Licensing	Custom	30 enterprise clients	$8M

Scalability Outlook

- EntropyCore's hybrid model (hardware + API) allows for exponential margin expansion as EaaS adoption grows.
- Post-certification, recurring revenue from long-term SaaS/API contracts with defense and blockchain partners is expected to dominate.

- Physical entropy modules open the door for long-tail licensing into consumer-grade security, IoT, and mobile compute.

Long-Term Exit Potential

- $100M+ ARR within 6–8 years across hardware, cloud entropy, and secure compute integrations.

- Strategic acquisition targets include: NVIDIA (AI hardware), Intel (TRNG/IP), Palantir (DoD), AWS (cloud trust), or hardware security firms like Yubico, Ledger, or Qualcomm.
