VitaShield

Vitashield

Vitashield is a UK-based deep-tech security platform addressing the growing risk of autonomous execution in modern systems. The company builds security infrastructure for smart contracts and blockchain applications that control financial value, and AI agents that can execute tools and access sensitive systems in regulated environments.

Company Purpose and Business Activities

Vitashield develops and commercialises security software that enables organisations to verify, control, and evidence the safe operation of autonomous code and autonomous agents.

Core activities include:

- Building a cloud-based security platform (web dashboard + API) for continuous smart contract verification and governance risk reporting.
- Developing a runtime access control, policy enforcement, and sandboxing layer for AI agents interacting with tools, APIs, internal data, and operational systems.
- Providing compliance-oriented outputs (audit trails, structured reports, risk summaries) suitable for internal governance and external stakeholder assurance.
- Offering customer onboarding and configuration support as optional professional services (not core revenue).

PROBLEM DEFINITION

Why This Matters in the UK/EU

Smart contracts and on-chain financial infrastructure

Smart contracts increasingly underpin financial functionality (payments, tokenised assets, stablecoin rails, lending logic). However, security controls are often limited to point-in-time audits and ad hoc internal review.

Ongoing risk drivers include:

- Upgradeable contract patterns (proxies) where implementation can change.
- Governance parameter changes that can alter risk exposure.
- Admin privilege structures that create centralisation and key-compromise risk.
- Integration risk with external protocols and dependencies.

AI agents in regulated operations

Enterprises and fintechs are deploying LLM-based agents to automate workflows (customer operations, compliance checks, data retrieval, incident response, and internal tooling). Many deployments lack a robust runtime permission system, leading to:

Many deployments lack a robust runtime permission system, leading to:

- Unauthorised actions or tool misuse,
- Data exposure and access escalation,
- Limited auditability for governance and regulatory review,
- Operational risk when “autonomous” actions cannot be reliably constrained.

Market Research Summary

The FCA Cryptoasset Regime (October 2027)

The UK is building its most comprehensive crypto regulatory framework, creating non-discretionary demand for security tooling:

- The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (SI 2026/102) was made on 4 February 2026 and comes into force on 25 October 2027 (legislation.gov.uk; Lewis Silkin; Global Regulation Tomorrow).
- The regime brings stablecoin issuance, custody, trading platforms, dealing, arranging, and staking under full FCA authorisation (FCA; Latham & Watkins;
- Skadden).
- The FCA application window for new cryptoasset permissions opens from 30 September 2026 to 28 February 2027, meaning hundreds of firms will need to demonstrate regulatory readiness starting in Q4 2026 (FCA; Lewis Silkin).
- The FCA's consultation papers (CP25/14, CP25/40–42) explicitly require that stablecoin codes be "robust" and that firms address crypto-specific risks, including "private key security and validator risks; code vulnerabilities; and decentralised network disruptions" (FCA CP25/14; Hogan Lovells; Ashurst).
- Operational resilience requirements (SYSC 15A) will be applied to all cryptoasset firms at bank-equivalent standards (FCA CP25/25; DLA Piper).
-
- The FCA estimates average implementation costs of approximately £100,000 per firm plus £30,000 annually for operational resilience compliance (FCA CP25/25).
- Inside information rules explicitly list "code vulnerabilities known to developers" As a category, making code security a legal compliance matter is not optional (DLA Piper; Skadden; FCA CP25/41).

Bank of England Systemic Stablecoin Regime

- The Bank of England published its systemic stablecoin consultation in November 2025, requiring backing of at least 40% in unremunerated BoE deposits and proposing individual holding limits of £20,000 (Bank of England; Morrison Foerster; Mayer Brown; Norton Rose Fulbright).
- The BoE acknowledges stablecoins could become "critical to UK retail payments within months of launch" (Bank of England consultation paper).

UK Government's Stated Crypto Hub Ambition

- The government has explicitly stated its ambition for the UK to become "a global hub for cryptoasset technology and investment" (HM Treasury/ Chancellor).
- The FCA launched a regulatory sandbox for stablecoin testing in January 2026 (FCA Press Release, November 2025).
- An Imperial College London report warned the UK risks "digital dollarization" without GBP stablecoins and noted the UK accounts for 3.5% of global GDP but only 11% of the fintech sector and 40% of global FX turnover. (Imperial College London)

CUSTOMER PROFILE

Ideal Customer Profile and Segmentation

Primary ICP (Years 1–3): UK/EU Fintech + Blockchain Infrastructure

Primary target customers:

- UK/EU-based fintech startups and blockchain infrastructure firms
- Seed to Series A (raised ~£500k–£5M)
- 4–15 engineers, limited dedicated security headcount
- Building on-chain financial primitives (stablecoin rails, tokenised assets, lending, custody-related smart contract logic)
- Have completed at least one audit or are preparing for an audit
- Face investor/compliance scrutiny and need evidence of ongoing risk management

Buying triggers:

- After completing an audit (need continuity),- Pre-launch with real capital exposure,
- Before next funding round / due diligence,
- After sector incidents that increase risk awareness.

Secondary ICP (Years 3+): Regulated AI adopters

Secondary customers include regulated firms deploying AI agents with tool access (fintech, compliance-heavy SaaS, financial operations). This segment becomes a stronger revenue driver once agent runtime enforcement is mature and budgets are clearer.

Competitive Landscape and Differentiation

Competitive categories:

1) One-off auditors (services): high quality, expensive, not continuous.
2) Developer static tools: free/low cost, technical outputs, not governance-ready.
3) Monitoring/automation platforms: strong operational tooling, not structured assurance.

Vitashield’s differentiation (why customers choose it):

- Assurance continuity between audits” rather than replacing audits.
- Governance-level outputs: admin surface maps, upgrade exposure summaries, centralisation risk descriptors.
- Compliance-oriented reporting suitable for investors, partners, and regulated stakeholders.
- Integration into CI/CD to reduce marginal effort and improve repeatability.

Year 1

Year 1: validation and credibility

Primary goals:

• 5–10 developer teams actively testing the product,

• 2–3 design partners providing structured feedback,

• Publish authority content (exploit breakdowns, governance risk explainers),

• Produce 2–3 credible case studies.

Year 2

Channel strategy

1) Direct founder outreach (CTOs/Founders) aligned with trigger events.
2) VC portfolio partnerships (discounted programme for portfolio companies).
3) Ecosystem partnerships (auditors, dev shops, and infrastructure providers as referral sources).4) Content credibility (technical write-ups) supporting inbound interest.

Year 2: 3–5 paying customers

Primary goals:

• Convert 3–5 customers to Growth/Assured tiers,

• Target customers with audit history and upcoming upgrades,

• Use warm intros via VCs, accelerators, and fintech networks,

• Maintain founder-led sales to reduce cash CAC while refining messaging.

Capital efficient growth

Lean cost base (founder-led sales; small engineering team).

Indicative operating costs:

Break-even is realistically expected in Year **4–5** without external acceleration, which is consistent with deep-tech infrastructure businesses

Capital efficient growth

EIC Accelerator Grant Strategy
(Supported by)

- Target: **$350k-$2.1M**
- R&D Acceleration
- Compliance Readiness
- Enterprise Grade Scaling
- Reduced Early Dilution
- Faster Market Entry

Current Runway (supported by)

- Founders Savings
- Friends & Family Commitment
- MVP Development & Validation Pilots

Platform Pricing

Starter Tier

£3,000 per annum

For early-stage DeFi teams and blockchain developers deploying first smart contracts.

- Continuous static analysis
- Basic vulnerability scanning
- Structured risk reporting
- Up to 3 contracts
- Across 2 blockchain networks

Growth Tier Most Popular

£6,000 Most Popular

For scaling protocols with expanding contract portfolios.

- Multi-contract monitoring
- Governance modelling
- Advanced compliance reporting
- Priority support
- Up to 10 contracts

Enterprise Tier

£12,000 per annum

For stablecoin issuers and regulated digital asset projects with higher exposure

- Unlimited contract coverage
- Real-time monitoring
- Custom compliance workflows
- Dedicated support with SLA

Vitashield

Vitashield is a deep-tech security platform designed to support safe and compliant deployment of autonomous systems in finance and regulated environments. The company's staged approach—validation first, focused commercial wedge second, and scalable infrastructure expansion third—aligns with UK Innovator Founder endorsement requirements for innovation, viability, and scalability.

Email: @gmail.com