DefenceOS

The sovereign software stack for European defence manufacturing

THE PROBLEM

Fragmented, non-sovereign defence manufacturing infrastructure

Operational challenges

- Fragmented systems across multi-tier supply chains, with limited cross-organisation visibility.
- Complex defence export and compliance regimes (ML categories, national controls, ITAR/EAR[1]) managed with manual, error-prone workflows.
- Limited end-to-end traceability of components, sub-systems and materials.
- Data silos preventing real-time collaboration between primes, Tier-1/2/3 suppliers and logistics partners.

Strategic imperatives

- Sovereign handling of defence-industrial data within EU jurisdictions.
- Continuous audit readiness and regulatory compliance.
- Secure collaboration between prime contractors, suppliers and logistics operators.
- Supply-chain resilience under geopolitical stress and export-control constraints.

[1] Applies to dual-use and US-origin components.

WHY NOW?

Policy and security tailwinds

01

EU strategic autonomy

EDF and EDA drive cross-border defence industrial cooperation and capability development across Member States.

02

Defence industrial modernisation

EDF, NSPA and NATO DIANA programmes prioritise dual-use technologies and supply-chain digitalisation, creating funding and pilot channels.

03

Sovereign cloud requirements

NIS2, GDPR and data-sovereignty mandates require defence-industrial software hosted within EU jurisdictions and outside non-EU CLOUD Act reach.

04

Supply-chain resilience

Geopolitical uncertainty reinforces the need for transparent, traceable and coordinated cross-border supply chains.

SOLUTION OVERVIEW

DefenceOS Platform

Integrated platform for multi-tier supply-chain visibility, export-control compliance and secure collaboration across the European defence manufacturing ecosystem.

Production & compliance

1. Real-time visibility on manufacturing operations
2. Automated documentation and audit trails for export-control and quality

Supply-chain coordination

1. Multi-tier supply-chain visibility into orders, suppliers and bottlenecks.
2. Logistics orchestration across borders and facilities.

Quality & traceability

1. Component-level traceability aligned with defence standards.
2. Rapid root-cause analysis for defects and non-conformances.

Cross-border operations

1. Secure multi-site and international collaboration under EU data-sovereignty constraints.
2. Configurable jurisdictional controls for cross-border programmes.

AI enablement[2]

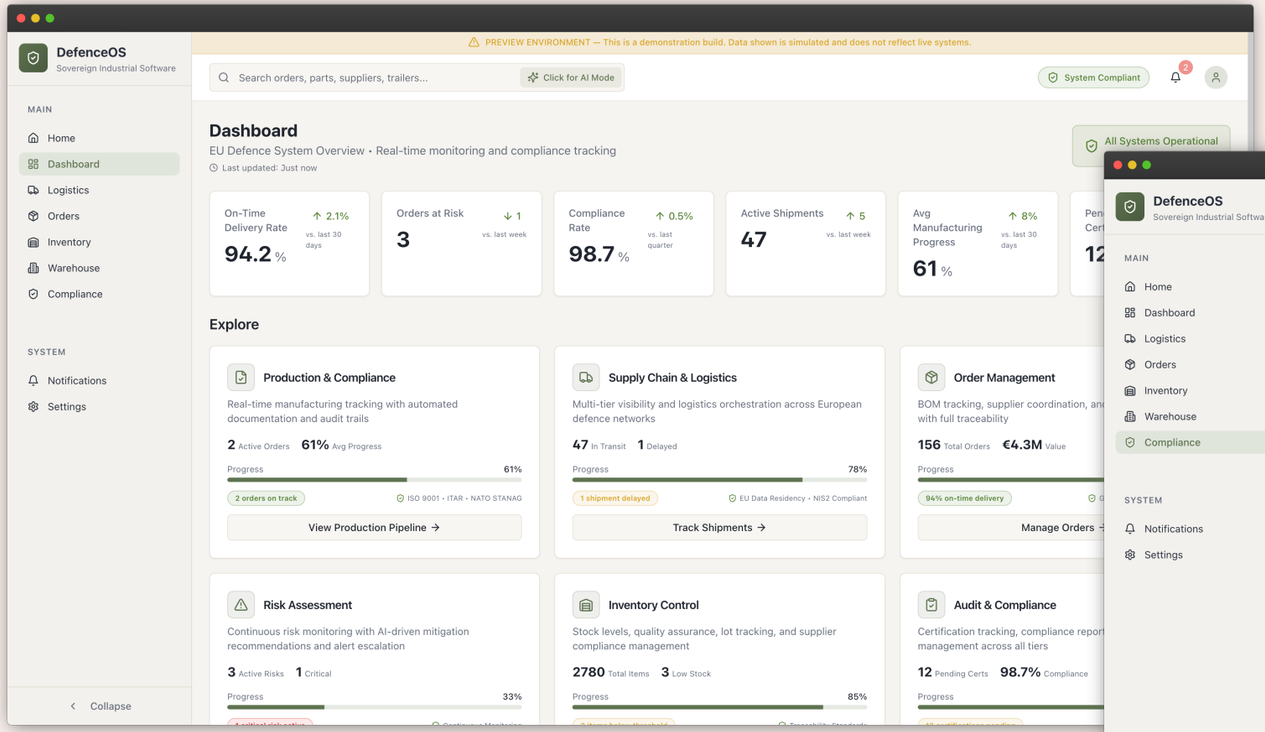
1. Document intelligence for export control and compliance documentation
2. Automated classification of components, materials and suppliers
3. Traceability analytics across multi tier supply chains
4. Manufacturing anomaly detection and risk alerts
5. AI generated compliance reports and audit preparation

[2] AI features provide assistive analytics and workflow automation only. The platform does not perform operational control of military systems. All AI functions are assistive; final decisions remain human-controlled.

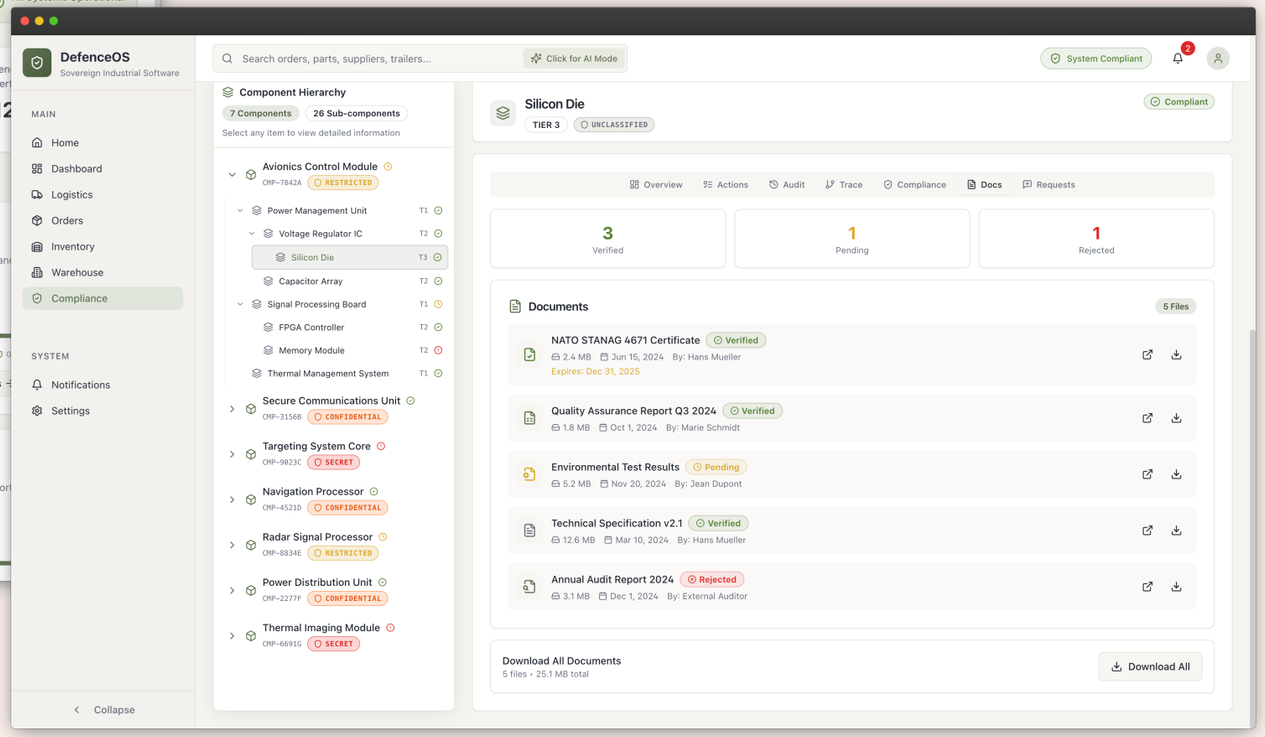
PRODUCT & UI

What DefenceOS looks like

Integrated platform for multi-tier supply-chain visibility, export-control compliance and secure collaboration across the European defence manufacturing ecosystem.



(DefenceOS Dashboard)



(DefenceOS Compliance Center)

MARKET POSITION

European defence transformation

€381B+

projected EU-27 defence spending in 2025, up 80% since 2021

~€800B

upto defence investment mobilisation targeted by 2030 under EU Readiness / ReArm Europe plans

>9%

annual growth across EU defence budgets since 2021, driven by re-armament and capability gaps

Defence spending growth

European defence budgets are increasing as Member States respond to security threats and commit to higher spending targets, creating momentum for industrial modernisation.

Digital infrastructure gap

Thousands of European defence manufacturers still rely on legacy ERP/MES systems that are expensive, inflexible and often hosted outside EU jurisdiction.

Sovereignty requirements

European defence policy increasingly emphasises strategic autonomy and supply-chain resilience, extending beyond components and hardware to the digital infrastructure that manages them.

Sources: EDA, European Parliament, Public EU defence readiness communications

ARCHITECTURE

DefenceOS Architecture – Sovereign, modular platform stack

From applications down to sovereign deployment, designed for secure integration into EU defence ecosystems

Applications & interfaces

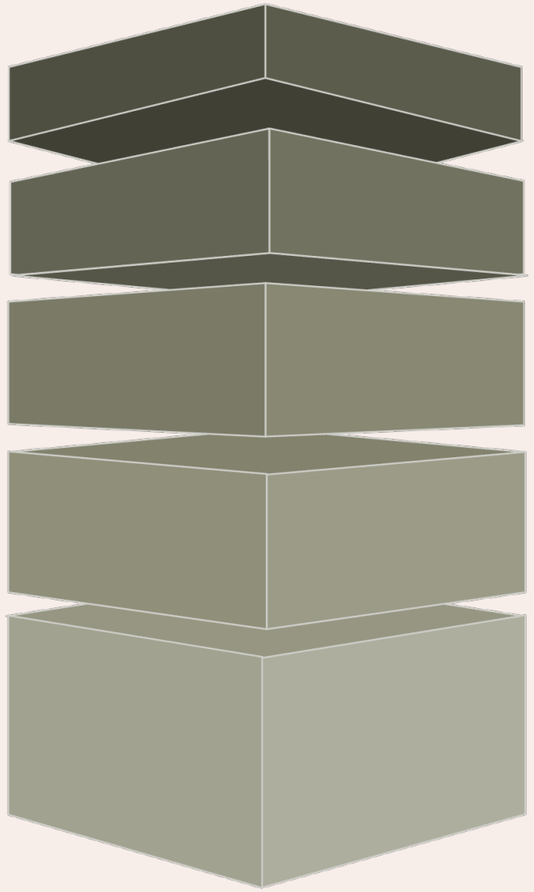
Web and desktop UIs, supplier and partner portals.
Integration endpoints (REST APIs), ERP / MES / PLM plug-ins.
Reporting and dashboards.

Core data & knowledge

Master data models (BOM, orders, parts, suppliers).
Traceability and provenance graph.
Compliance schemas, document metadata and audit trails.
Telemetry and time-series data.

Deployment & sovereignty

EU sovereign cloud.
On-premises deployments. Isolated / restricted networks and air-gapped environments.
EU data-residency controls and jurisdiction control.
Encryption at rest and in transit



Operational domains

Production & compliance.
Supply-chain & logistics.
Quality & traceability.
Document & audit management.

Platform services

Data ingestion and integration.
Workflow orchestration.
Identity & access control (RBAC / zero-trust).
Audit logging and telemetry.
API gateway and interoperability.
AI / analytics (assistive, human-in-the-loop).
Secure data storage.

DESIGN

Sovereignty, Interoperability and Security by Design

Built to align with EU data-sovereignty, industrial standards and defence-grade security expectations from day one

01

Data sovereignty

1. EU-located hosting infrastructure
2. No exposure to non-EU CLOUD Act jurisdictions
3. Compliance with GDPR and NIS2
4. Member State data-residency options

02

Interoperability

1. NATO STANAG consideration in design
2. Alignment with industrial data-exchange standards
3. Integration with MES, PLM and ERP systems

03

Security posture

1. Zero-trust security architecture
2. Encryption at rest and in transit
3. Granular RBAC and audit logging

TRACTION

Where we stand today

From concept to architecture to product preview within weeks, moving at startup speed with enterprise-grade rigour.

Architecture and Compliance Framework defined

Core software engineering architecture and compliance framework in place, laying the foundation for a compliant, modular and sovereign platform

Team expanding

Beyond engineering with our first compliance hire, bringing banking, Amazon regulatory and MBA experience to build defence-grade governance from day one.

Early product preview

Interactive product preview available for stakeholder feedback, demonstrating our platform direction and validating core workflows before MVP development.

ECOSYSTEM

Target customers and initial beachhead

We focus on industrial users in Germany and Benelux; Ministries of Defence and EU institutions act as ecosystem stakeholders and sponsors.

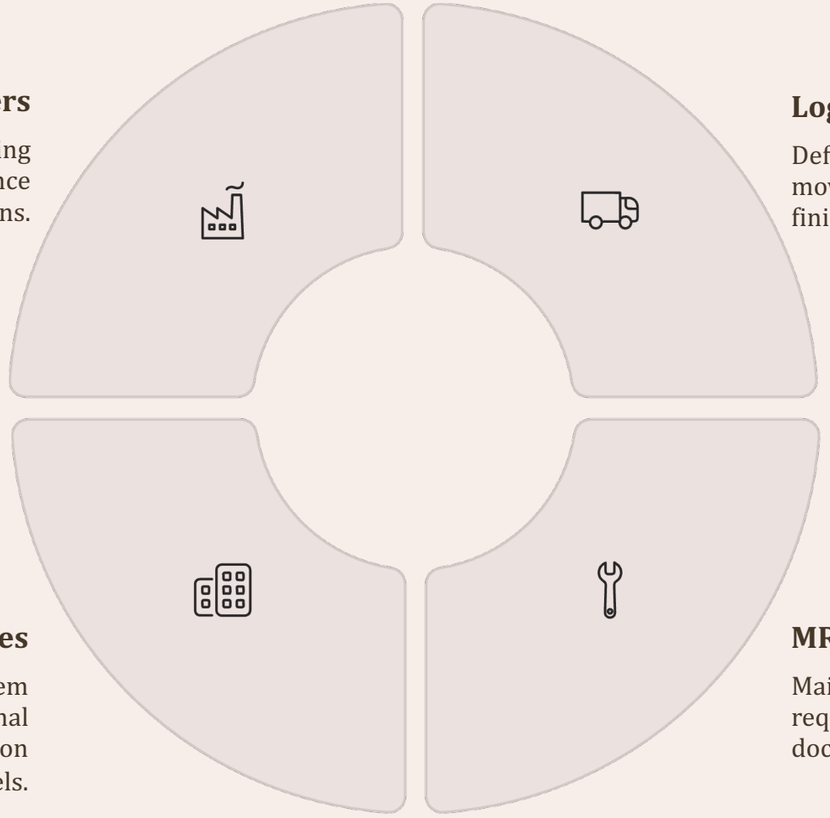
Beachhead segment: Tier-2/3 defence manufacturers in Germany and Benelux producing dual-use and ITAR/EAR components.

Buyer personas: Head of Operations, Plant Manager, Quality & Compliance, CTO.

Pain today: Spreadsheet-driven compliance, limited traceability, non-sovereign ERP/MES.

Defence Manufacturers

Tier 1, 2, and 3 suppliers requiring production tracking and compliance management across complex supply chains.



Logistics Operators

Defence logistics providers coordinating movement of materials, components, and finished goods across borders.

Defence Ministries

Ministries of Defence as ecosystem stakeholders; NSPA, EDA, EDF and national defence innovation agencies as innovation and funding channels.

MRO & Industrial Suppliers

Maintenance, repair, and overhaul facilities requiring traceability and quality documentation for defence assets.

MARKET POSITION

Positioning vs alternatives

DefenceOS complements and, where necessary, replaces legacy systems that were not built for EU-sovereign, multi-tier defence supply chains.

	Legacy ERP / MES	US Defence Cloud Tools	DefenceOS
EU Data Sovereignty	Often non EU hosting and limited control over CLOUD Act exposure	Frequently subject to US CLOUD Act	EU first hosting architecture, designed to avoid non EU CLOUD Act exposure, with Member State data residency options
Multi Tier Traceability	Site centric systems with limited cross supplier visibility	Often programme specific and difficult for SMEs	Purpose built for multi tier supplier networks and cross programme visibility
Export Control Workflows	Manual, spreadsheet driven, or bolt on compliance tools	Primarily focused on US regulations	Native workflows for EU, national, and ITAR/EAR export control compliance
Deployment in Air Gapped Environments	Possible but heavy and costly to operate	Typically cloud first	Designed from day one for cloud, on prem, and air gapped deployments

BUSINESS

Deployment & Business Model

EU sovereign cloud

Hosted on EU-based infrastructure meeting defence data-sovereignty requirements with multi-tenant isolation and Member State data-residency options.

On-premises installation

Private deployment within customer infrastructure for organisations with air-gapped or specific security mandates.

Isolated networks

Deployment pathways for isolated networks and air-gap-compatible environments, with controlled update and support models.

Business Model

Enterprise SaaS subscriptions or perpetual licences with maintenance.
Support packages and professional services available for implementation and integration.

IMPLEMENTATION

Execution Plan and Roadmap

01

NOW - Validation & seed funding

1. Raise €2M seed to accelerate engineering, compliance and go-to-market.
4. Structured problem and market validation with defence industry stakeholders across Germany, Benlux
5. Internal compliance and security framework development.
6. Company incorporation and set-up in the EU (Luxembourg).

02

Phase I - MVP & first design partners

1. MVP development: production tracking, compliance management and core workflows.
2. Onboard 2–3 design partners from defence manufacturing for co-development.
3. Begin certification pathway assessment (e.g. ISO 27001, EU/NATO ecosystem).

03

Phase II - Controlled pilots

1. Deploy with design partners in controlled pilot environments.
2. Iterate based on real-world feedback and measured impact.
3. Compliance validation with regulatory advisors.
4. Grow engineering team for platform hardening.

04

Phase III - Early traction

1. Convert pilot-validated SME partners into first paid engagements.
2. Apply to EU defence innovation and funding programmes (EDF, EDIP and national channels).
3. Build pipeline through defence industry events and ecosystem engagement.

DREAMERS

Founding Team

We have spent the last decade building mission-critical systems; DefenceOS focuses this experience on European defence sovereignty

Kalpesh Singh

Senior software engineer with 10+ years building advanced frontend and user-centric systems. Experienced in leading engineering teams across international environments, with exposure to tech ecosystems. Focused on user experience, secure interfaces, and operational tooling for mission-critical defence applications.

Subhasish Das

Senior software engineer specializing in distributed systems and high-reliability backend architecture. Experienced in designing and scaling infrastructure for mission-critical services, bringing expertise in resilient systems, data pipelines, and security-focused backend engineering for enterprise and defence-grade software platforms.

ASK & USE OF FUNDS

Our raise and use of funds

The Round

Raising: €2M seed equity round

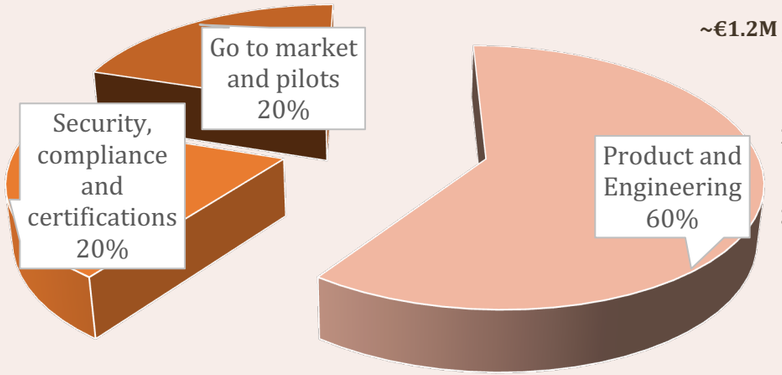
Geography focus: Germany and Benelux defence-industrial SMEs and their ecosystems.

Runway: ~18 months

Use of funds

~€0.4M

1. Secure and run 2-3 pilots with Tier-2/3 manufacturers
2. Participate in EU and national defence innovation programmes to leverage non-dilutive capital.
3. Build a small commercial team (founder-led sales plus first GTM hire) and invest in industry events and cluster engagement.



~€1.2M

1. Complete MVP focused on production tracking, export-control compliance and multi-tier traceability.
2. Build integrations with common ERP/MES systems used by German and Benelux SMEs.
3. Harden platform for cloud, on-prem and air-gapped deployments.

~€0.4M

1. Implement security controls and monitoring aligned with ISO 27001 and defence-sector expectations.
2. Progress along national and EU defence accreditation pathways
3. Establish secure operations and support processes for sovereign deployments.

TOGETHER

Partner With Us

We are building DefenceOS to become the sovereign software stack for European defence manufacturing. We are seeking strategic partners, investors and industry collaborators who share our commitment to sovereign, compliant infrastructure for European defence.

INVESTORS

Looking for seed partners with deeptech and defence experience

OEMs & PRIMES

Seeking integration and pilot partners for cross-supplier programmes

SUPPLIERS

Looking for Tier-1/2/3 manufacturers willing to co-design workflows and pilots

ADVISORS

Defence, export-control and security accreditation expertise

Website | defenceos.eu

Subhasish Das, Co-founder | subhasish@defenceos.eu
Kalpesh Singh, Co-founder | kalpesh@defenceos.eu