COMPLEAR

SOVEREIGN DEFENCE INTELLIGENCE INFRASTRUCTURE

One integrated infrastructure.

Full-spectrum sovereign security.

Complear OS delivers a unified on-premises platform where AI continuously detects vulnerabilities, correlates threats across all endpoints, enforces attested encryption, and ensures information governance across all connected systems — operating entirely within the defended perimeter. No cloud dependency. No foreign data exposure. No fragmented point solutions.

CORE CAPABILITIES

01 LIVE SECURITY OPERATIONS CENTRE

Real-time SOC dashboard aggregating telemetry from every deployed edge agent across all facilities. Live alert counters by severity, network traffic visualisation, endpoint inventory, patch compliance — complete situational awareness from a single command view.

02 NEURAL NETWORK THREAT INTELLIGENCE

AI-powered neural network continuously learns attack patterns, behavioural anomalies, and zero-day signatures across all managed endpoints simultaneously.

Full MITRE ATT&CK coverage across 14 tactics and 150+ threat actor groups — from APT1 to nation-state actors — with real-time technique mapping and proactive threat hunting.

03 VULNERABILITY & MALWARE DETECTION

Continuous CVE scanning across 3,000+ vulnerabilities with severity classification. Cross-agent malware correlation identifies campaigns targeting multiple endpoints in parallel. Behavioural indicator analysis, YARA scanning, rootcheck detection, and file integrity monitoring — with full forensic drill-down and 30-minute event granularity.

04 ATTESTED ENCRYPTION

End-to-end AES-256 encrypted communications between server and all edge agents. Hardware-attested integrity verification at every node — from endpoint to command layer. Post-quantum cryptographic readiness at architecture level.

05 AUTOMATED COMPLIANCE

Continuous monitoring against NATO INFOSEC, NIS2, ISO/IEC 27001, HIPAA, GDPR, NIST 800-53, and PCI DSS. Audit-ready compliance dashboards at all times — no manual data collection. Executive-ready reports generated on demand for regulators, partners, and boards.

06 INFORMATION GOVERNANCE

Centralised data lifecycle management enforced by policy engine. Classification, access control, and retention applied across all connected systems. Full audit trail export with DQL search across all agent events — complete forensic reconstruction of any incident.

07 ACTIVE RESPONSE ORCHESTRATION

Automated countermeasures pushed from the command centre to any edge agent in real time — block IPs, kill processes, isolate machines, patch vulnerabilities. Edge agents can also act autonomously on local conditions without requiring live server connectivity. Self-healing security loop.

✓ **HUMAN-IN-THE-LOOP BY DESIGN** **EU AI Act Article 14 · NATO AI Principles of Responsibility**

All critical decisions require human authorisation. Accountability is enforced at platform level — not added as policy. Fully aligned with EU AI Act Article 14 (High-Risk AI Systems) and the NATO AI Principles of Responsibility.

INFRASTRUCTURE COVERAGE *Multi-site · Multi-OS · On-premises*

ENDPOINT COVERAGE

Windows Server 2016–2022 · Windows 10/11 · Ubuntu · RHEL · Debian · CentOS · macOS · QNX RTOS medical devices (MRI controllers, infusion pumps, patient monitors)

DEPLOYMENT MODEL

Fully on-premises within the defended perimeter. Private cloud or hybrid deployment supported. Multi-facility, multi-site architecture — all facilities managed from a single command centre with zero external data dependencies.

COMMUNICATIONS

AES-256 encrypted TCP between command server and all edge agents. Zero-trust architecture. Edge agents auto-enrol using deterministic SHA-256 agent IDs derived from hostname and MAC address — no manual registration.

ALIGNED STANDARDS *among others*

NATO INFOSEC Policy · EU AI Act — Art. 14 · NIS2 Directive · ISO/IEC 27001 · NIST 800-53 · NIST CSF 2.0 · CNSA 2.0 · NATO Data Sovereignty Policy · HIPAA · GDPR · PCI DSS · MITRE ATT&CK · EDF / EDOCC

WHY COMPLEAR FOR SOVEREIGN DEFENCE SYSTEMS

Unlike fragmented point solutions, Complear OS integrates all security functions into a single on-premises stack.

External data dependencies are eliminated. Attack surface is reduced. Technological sovereignty is real, not nominal. The AI operates entirely within the defended perimeter — with no cloud dependency and no foreign data exposure. Every capability, from live threat detection and MITRE ATT&CK mapping to compliance reporting and autonomous response, runs inside the secured perimeter without a single external call.

FROM HEALTHCARE TO DEFENCE — THE SAME DNA

Four years of excellence in regulated healthcare environments. Before expanding into defence, Complear built its foundation in one of the most demanding regulated sectors: healthcare. The same rigour, compliance frameworks, and AI governance principles that protected patient data and medical devices now power sovereign defence infrastructure.

Medical devices and defence systems share a common challenge: **critical compliance in high-stakes, regulated environments.** Complear's proven methodology, frameworks, and AI governance infrastructure translate directly into sovereign defence applications.

CEO'S IP POSITION — 7 PATENTS PENDING

Complear's CEO holds **7 patents pending** across two domains: compliance lifecycle infrastructure and post-quantum cryptography. A defensible, hardware-anchored position with cross-sector application across Defence, MedTech, Autonomous Systems, Aerospace, and Advanced Manufacturing.

Compliance Lifecycle — 4 patents: Regulatory Compiler · Kinetic Envelope · Liability Tokeniser · Compliance Orchestration Platform

POST-QUANTUM CRYPTOGRAPHY — 3 PATENTS

ASSESS — PQC-1

CVLAS

Cryptographic Vulnerability Lifecycle Assessment

Dynamic probabilistic timelines for when current cryptography becomes unsafe. Risk-based migration planning — not binary exposure alerts. Enables proactive action before vulnerabilities are exploited.

COMPLY — PQC-2

TCVS

Temporal Consent Verification System

Links consent validity to cryptographic lifetimes. Automated key destruction with forensic proof — data governance obligations survive cryptographic transitions intact.

MIGRATE — PQC-3

PQCMOP

PQC Migration Orchestration Platform

AI-driven orchestration migrating thousands of cryptographic deployments at scale. OBIL layer carries Standard Essential Patent potential within emerging quantum security standardisation frameworks.

PEER-REVIEWED RESEARCH Multiple published papers in post-quantum cryptography by the CEO, providing independent scientific validation of the underlying science beyond patent filings.

CNSA 2.0 Aligned · SEP Potential — OBIL Layer · Hardware-Anchored Claims · NATO INFOSEC Compatible · Full Assess → Comply → Migrate Coverage

CLIENT REFERENCES — HEALTHCARE SECTOR

Anonymised for security purposes · Identification available under NDA

A

IT & HEALTH — PORTUGAL

Major Portuguese IT & Health Group

Full MDR/IVDR compliance mapping for software medical devices. Ongoing regulatory monitoring and audit support across the complete post-market lifecycle.

B

TELECOM & HEALTH — MULTINATIONAL

Multinational Telecom & Health Services

EU AI Act compliance framework implementation. Data governance and information security alignment across health data platforms at multinational scale.

C

MEDICAL DEVICES — EUROPE

European Medical Device Manufacturer

End-to-end regulatory pathway: CE marking through post-market surveillance. ISO 13485 and IEC 62304 compliance automation.

CURRENT DEFENCE PIPELINE

▸ **Portuguese Armed Forces** [ACTIVE PILOT] — Information security compliance across security information management, supply chain integrity, and NATO-aligned regulatory certification pathways.

- **NATO Security Authorisation** [IN PROGRESS] — Certification process covering engineering compliance and information security requirements for global supply chains.
- **European Defence Fund (EDF)** [ACTIVE] — Engagement across EDOCC and CYBER-QSTN calls, positioning Complear as a key enabler of European technological sovereignty in defence.

SECTOR LEADERSHIP

A team that has operated inside the systems it now secures. Senior expertise across law, defence, military intelligence, EU institutional governance, and post-quantum science.

OUR CHIEF EXECUTIVE OFFICER & FOUNDER

Corporate CEO, technology entrepreneur, EU Institutions leader, and Complear's CEO. Maria brings a rare convergence of business discipline, hands-on tech company scaling, EU institutional reach, and original post-quantum cryptography science. She founded and scaled XPAND to multinational level before founding Complear, and as Chairwoman of the EU's Joint AI Undertaking operates at the intersection of the technological, regulatory, and political domains that define sovereign defence compliance. Maria was responsible at the EIT for the AI Act review team.

BACKGROUND & COMMERCIAL

- **Business Studies (Oxford & Stanford)** · Degree, MBA, Executive Studies and PhD (pending)
- **XPAND** — *Group CEO — Scaled multinational visualisation technology group*
- **N2 Groups** — *Board Member — HPC Companies*

EU INSTITUTIONAL ROLES

- **European Innovation Council (EIC)** — *Jury Member*
- **EIT — European Institute of Innovation & Technology** — *European Head of Digital Innovation*
- **European Digital SME Alliance** — *Chairwoman — Joint AI Undertaking & AI Steering Committee*

OUR HEAD OF DEFENCE, DATA PRIVACY & CYBERSECURITY

The direct operational bridge between military requirements and Complear's technological capabilities. Serafim brings first-hand knowledge of military legal frameworks, intelligence operations, and security governance — having served inside the Portuguese Army's Land Forces Command and Military Security & Intelligence Centre. His dual background in law and military service positions him to translate sovereign defence requirements into precise technical specifications.

LEGAL & MILITARY FORMATION

- **Law Degree (LLB)**
- **Army Officer Training**
- **Master's in Strategic Studies** — *University College Cork, Ireland*
- **Master's in Law and Technology** — *Tilburg University, Netherlands*

OPERATIONAL SERVICE

- **Junior Officer & Legal Adviser** — *Portuguese Army, Land Forces Command*
- **Analyst** — *Military Security & Intelligence Centre*
- **Protection & Security Officer EMEA & AME** — *Multinational security firm*

ADVANCED QUALIFICATIONS

- **Auditor** — *National Defence Institute*
- **Postgraduate** — *International Relations & Diplomacy*
- **Advanced Specialisation** — *Forensic Sciences & Criminal Investigation*