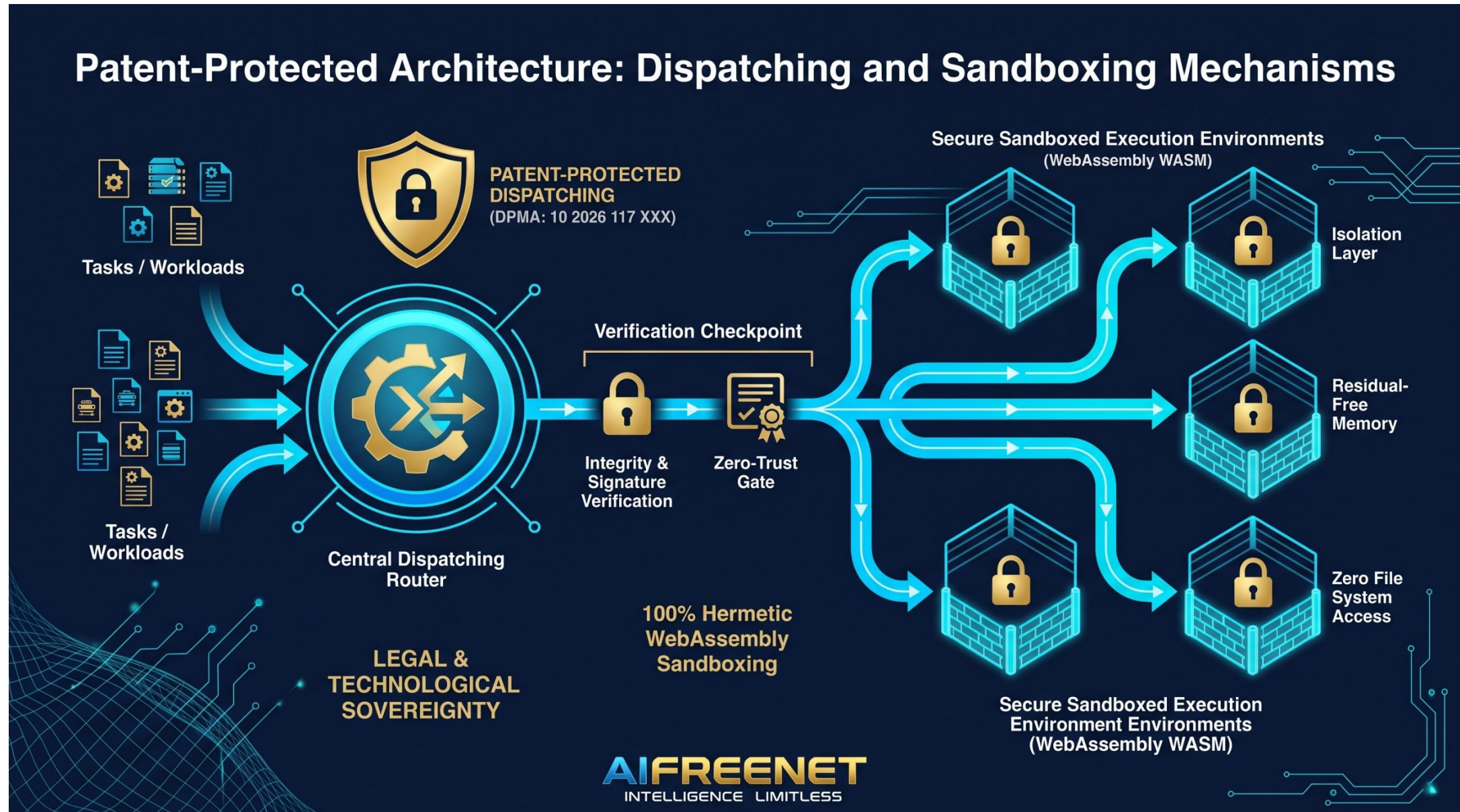


AIFREENET CORE SICHERHEITSARCHITEKTUR



10-Schichten-Sicherheitsarchitektur für Dezentrales KI-Computing

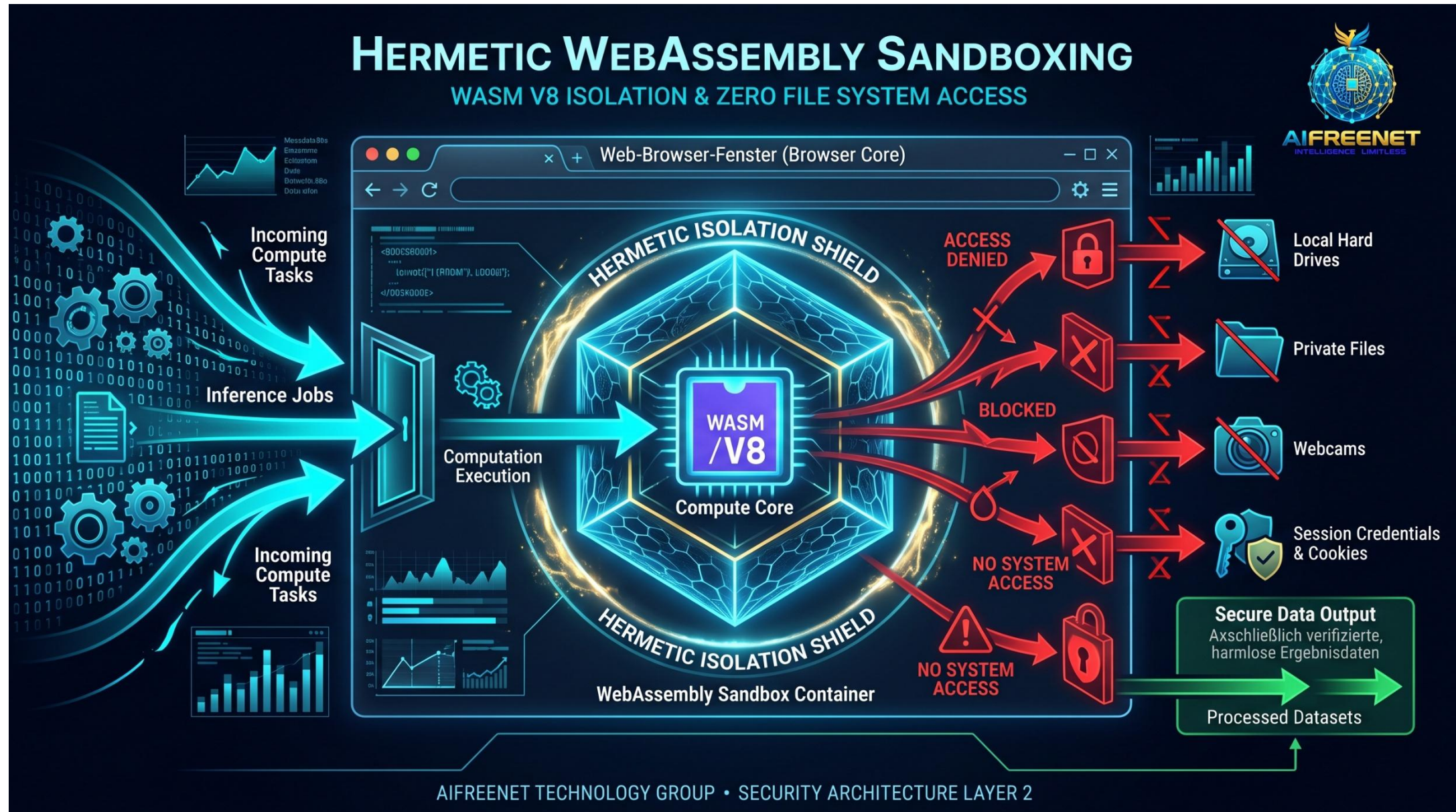
1. Patentierte Dispatching- & Sandboxing-Mechanismen (DPMA / PCT) für technologische Souveränität ohne Abhängigkeiten von Drittanbieter-Code.



- Zentraler Dispatcher: Verteilt KI-Berechnungen über einen zertifizierten Zuweisungs-Router.
- Isolierte Ausführungsschichten: Aufgaben werden durch feste Checkpoints geschleust, um fremde Code-Injektionen auszuschließen.

2. Hermetic WebAssembly Sandboxing

V8- und WebAssembly-Isolation: Absoluter Schutz vor Dateisystemzugriffen.

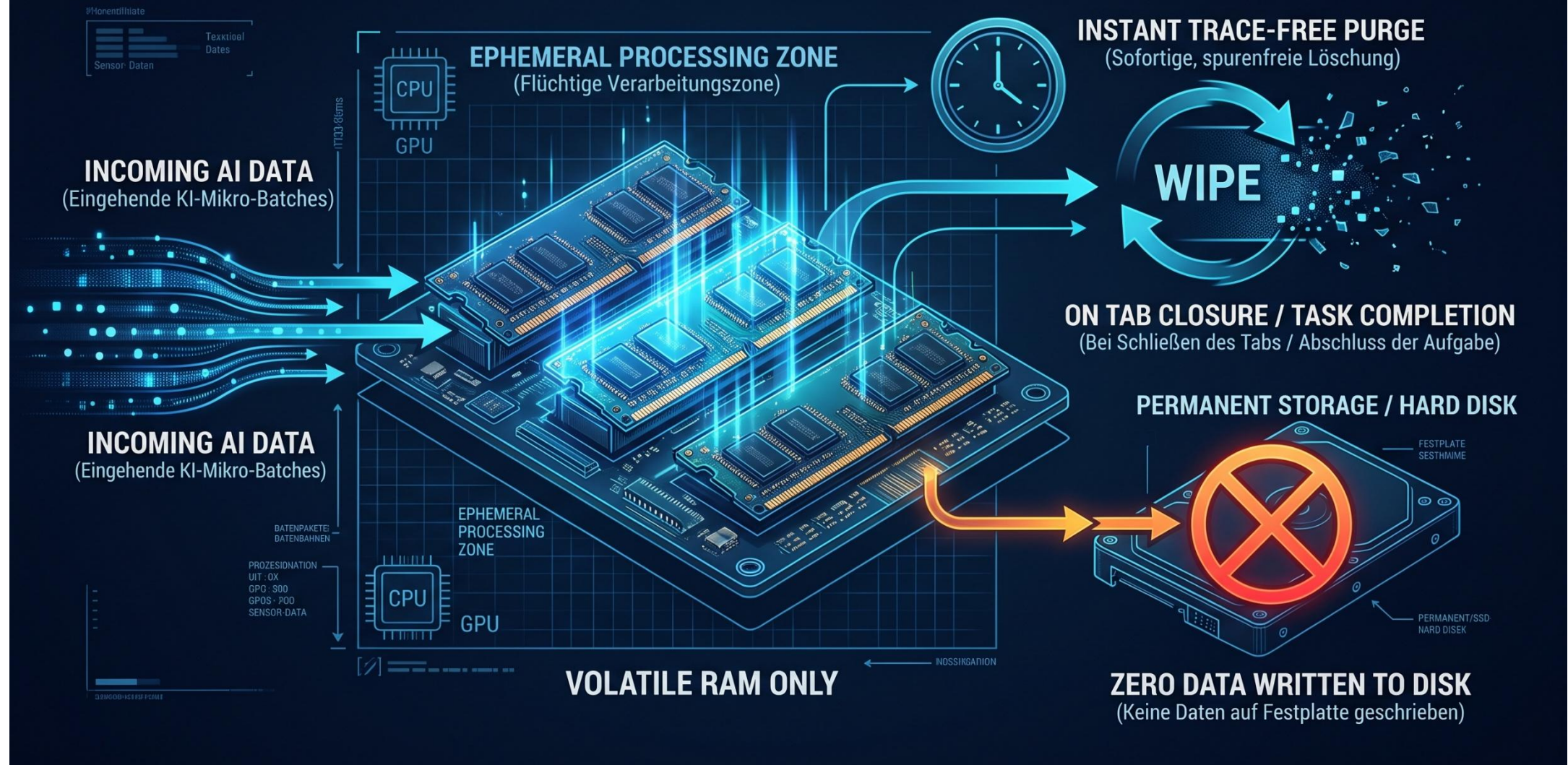


- Hermetische Hülle: Der Browser Core führt Inferenzaufgaben ausschließlich in einem versiegelten WebAssembly-Container aus.
- Zugriffsbarrieren: Feste Sperrungen verhindern jeglichen Zugriff auf Festplatte, Fotos, Passwörter, Webcams oder Browser-Cookies.

3. Zero Local Data Storage (RAM Only)

Flüchtiger Arbeitsspeicher ohne persistente Rückstände auf den Rechnern der Knotenbetreiber.

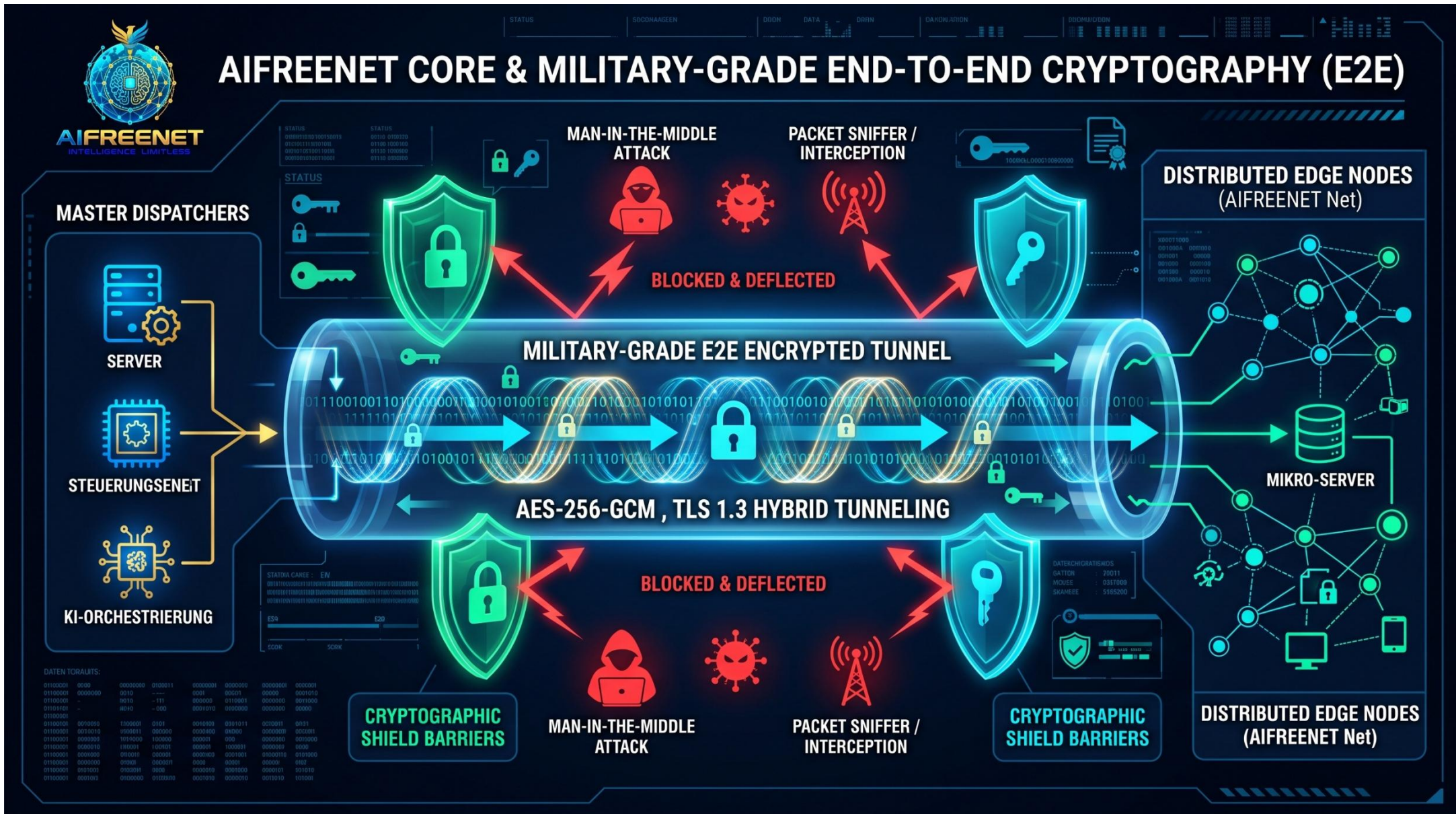
ZERO LOCAL DATA STORAGE (RAM ONLY ARCHITECTURE)



- Reine RAM-Verarbeitung: Berechnungs-Batches verbleiben zu 100 % im flüchtigen Arbeitsspeicher.
- Trace-Free Purge: Sobald ein Tab geschlossen oder die Aufgabe abgeschlossen wird, löscht sich der Speicherbereich vollständig und rückstandsfrei.

4. Military-Grade E2E Cryptography

Ende-zu-Ende-Verschlüsselung (AES-256-GCM & TLS 1.3 Hybrid-Tunneling).



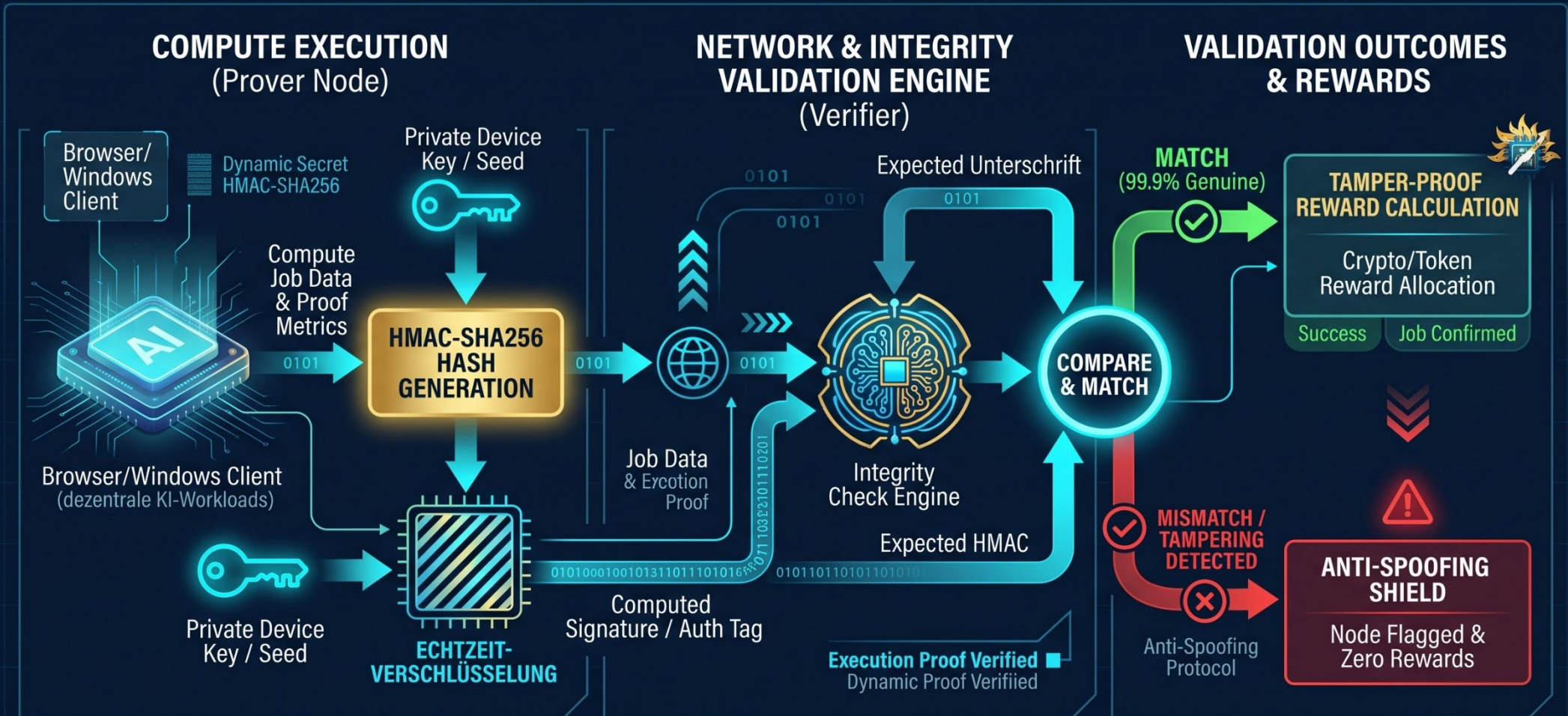
- Geschützter Transport-Tunnel: Sämtliche Datenströme zwischen Dispatcher und Edge-Nodes sind kryptografisch abgesichert.
- Man-in-the-Middle-Schutz: Abfangen oder Manipulieren von Datenpaketen (selbst in ungesicherten WLAN-Netzen) ist mathematisch ausgeschlossen.

5. HMAC-SHA256 Integrity Verification

Proof-of-Compute & Anti-Spoofing: Manipulationssichere Ergebnisvalidierung.

TECHNICAL ARCHITECTURE: HMAC-SHA256 INTEGRITY VERIFICATION

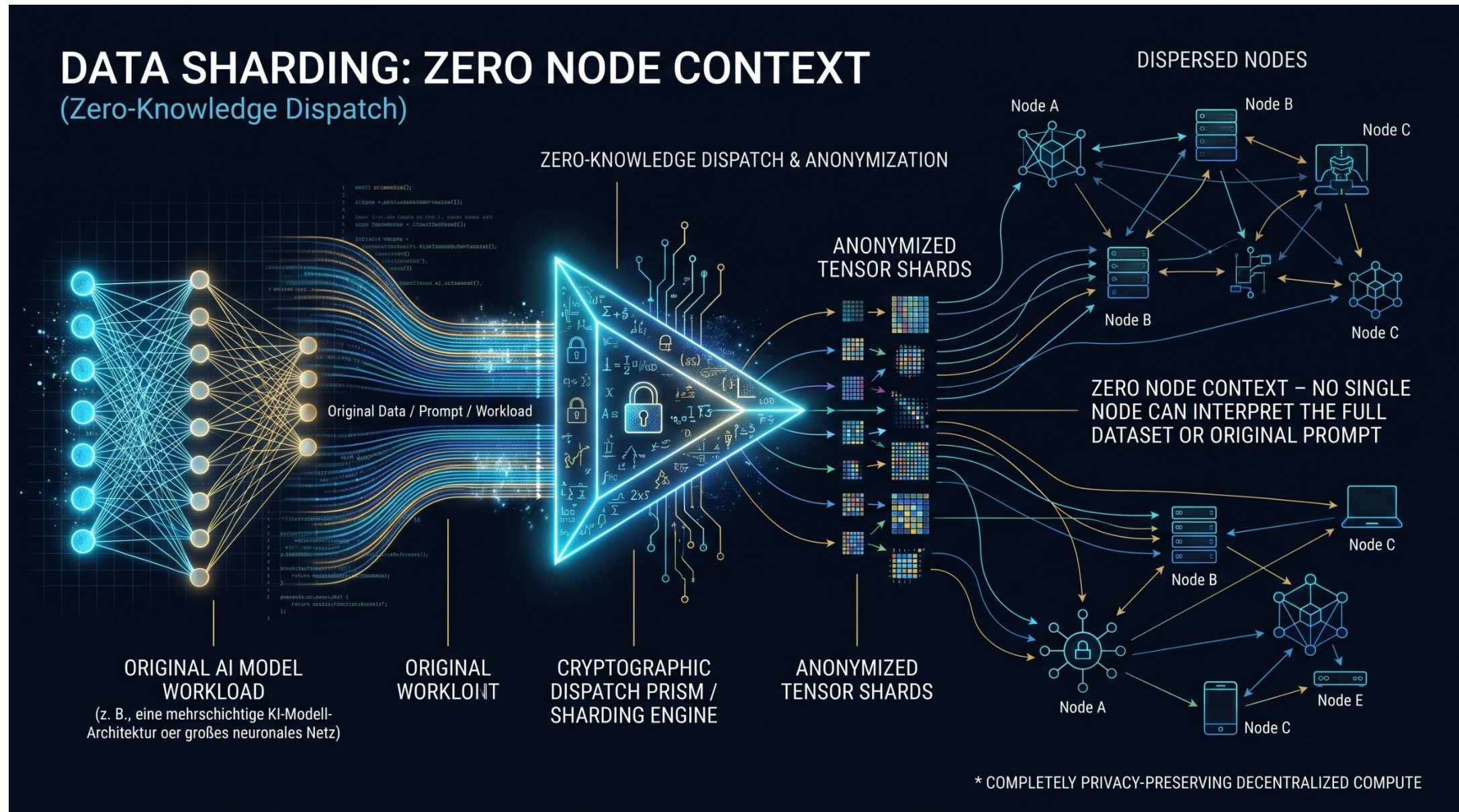
Proof of Compute & Anti-Spoofing Validation



- Kryptografischer Herzschlag: Jede ausgeführte Rechenoperation erzeugt einen unveränderlichen Hash-Fingerabdruck.
- Manipulationssichere Vergütung: Belohnungen und E-Wallet-Gutschriften werden nur bei gültigem Beweis der echten physischen Rechenausführung freigegeben.

6. Data Sharding: Zero Node Context

Zero-Knowledge Dispatch: Kein Rechner kennt den Gesamtkontext der Daten.



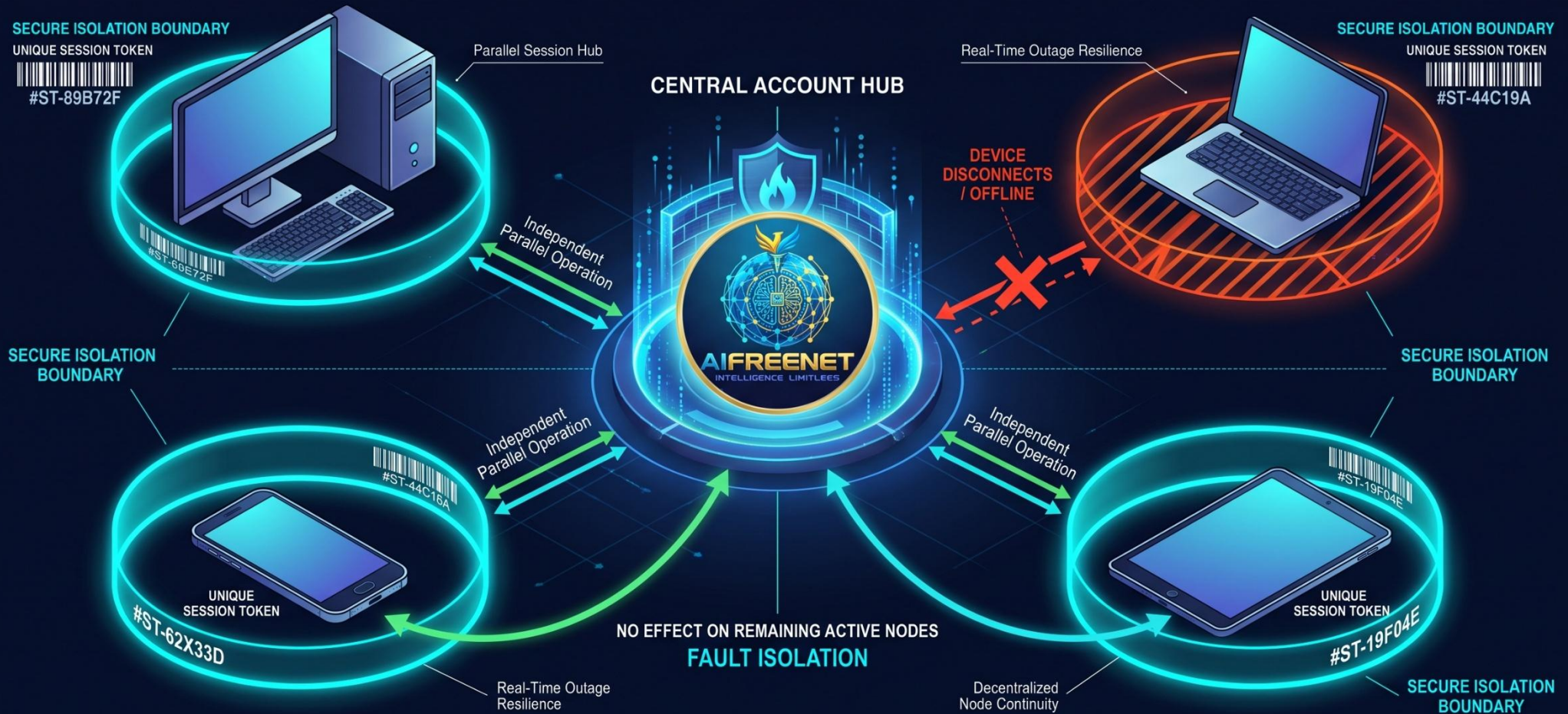
- Tensor-Fragmentierung: Sensible Workloads von Unternehmenskunden werden in isolierte mathematische Bruchstücke zerlegt.
- Keine interpretierbaren Daten: Kein einzelner Knoten erhält vollständige Prompts oder lesbare Datensätze – vollständiger Datenschutz für Kunden und Betreiber.

7. Secure Multi-Device Orchestration

Parallele Nutzung mehrerer Endgeräte ohne Überschneidungsrisiken.

SECURE MULTI-DEVICE ORCHESTRATION

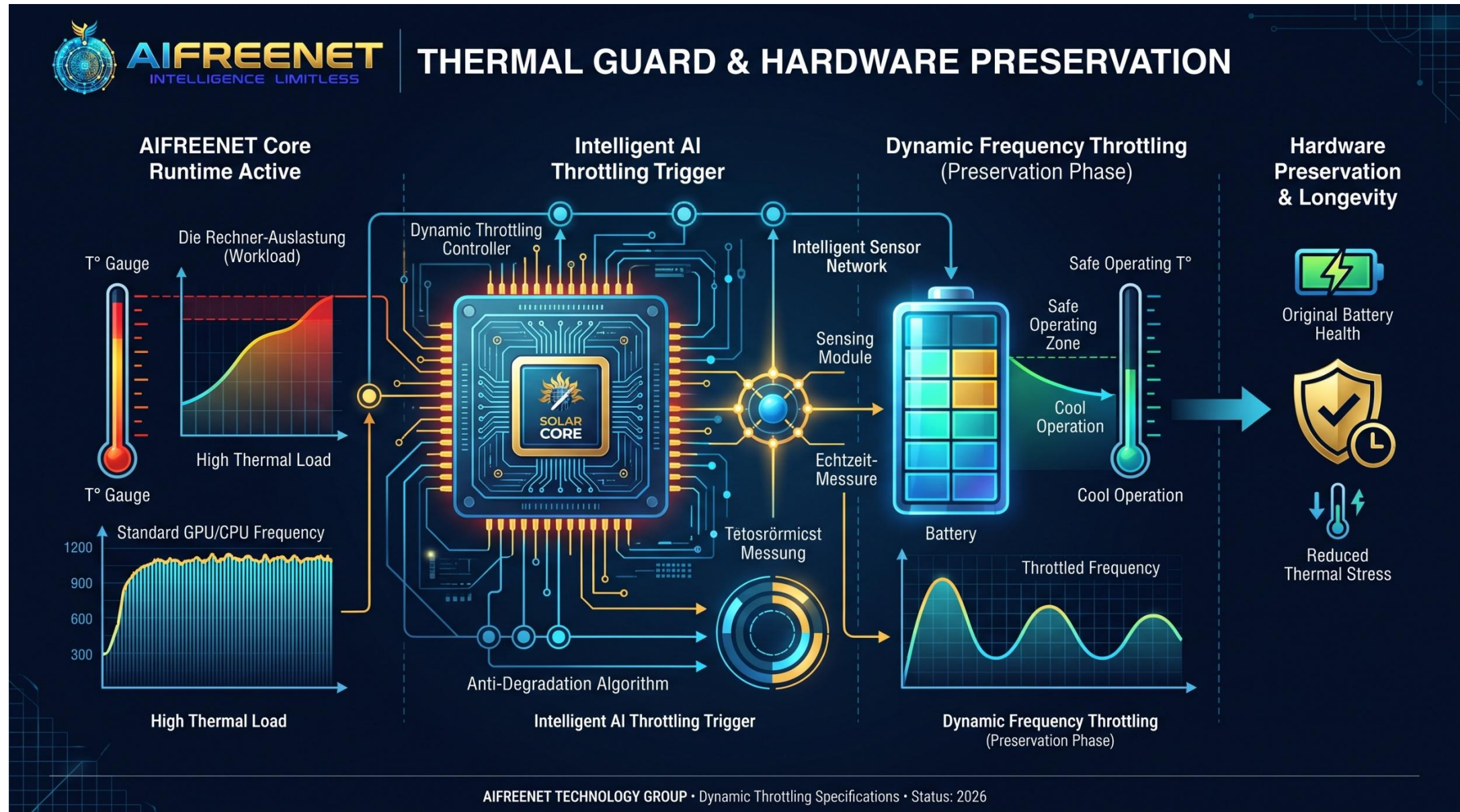
AIFREENET CORE: Secure Session Multi-Device Connection Flow



- Eindeutige Session-Tokens: Smartphones, PCs und Tablets laufen unter einem Benutzerkonto in getrennten Sitzungen.
- Fehlerisolierung: Die Trennung oder der Ausfall eines Geräts beeinträchtigt die übrigen aktiven Nodes im Cluster zu keinem Zeitpunkt.

8. Thermal Guard & Hardware Preservation

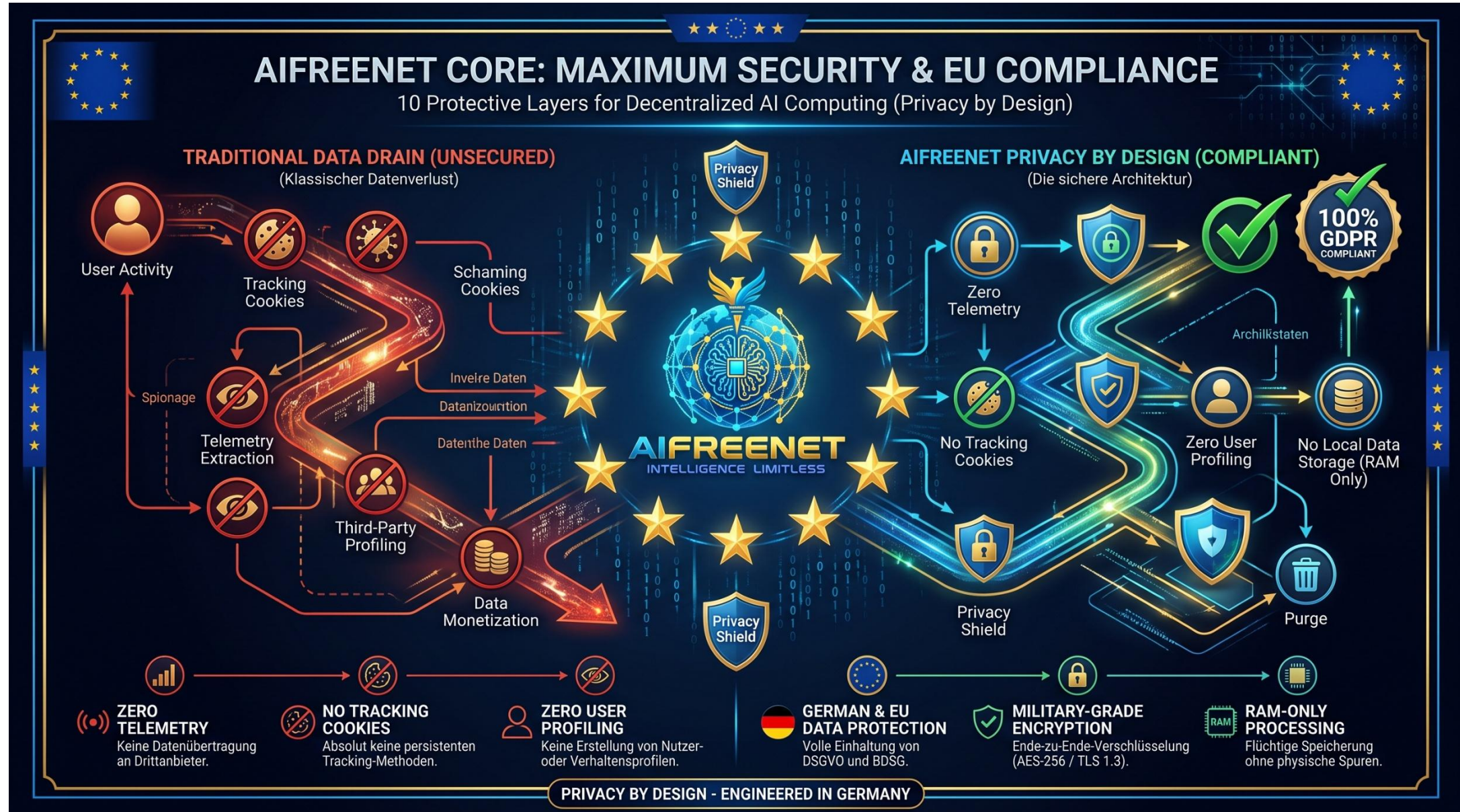
Intelligenter Hardware-Schutz & dynamische Leistungs-drosselung.



- Kein Krypto-Mining-Verschleiß: Das System überwacht Akku-, Chip- und Gehäusetemperaturen kontinuierlich.
- Dynamische Taktung: Bei hoher Last oder niedriger Akkukapazität drosselt der Core automatisch herunter, um die Lebensdauer der Hardware zu sichern.

9. 100% GDPR & EU Regulatory Compliance

Privacy by Design nach deutschem und europäischem Datenschutzstandard.



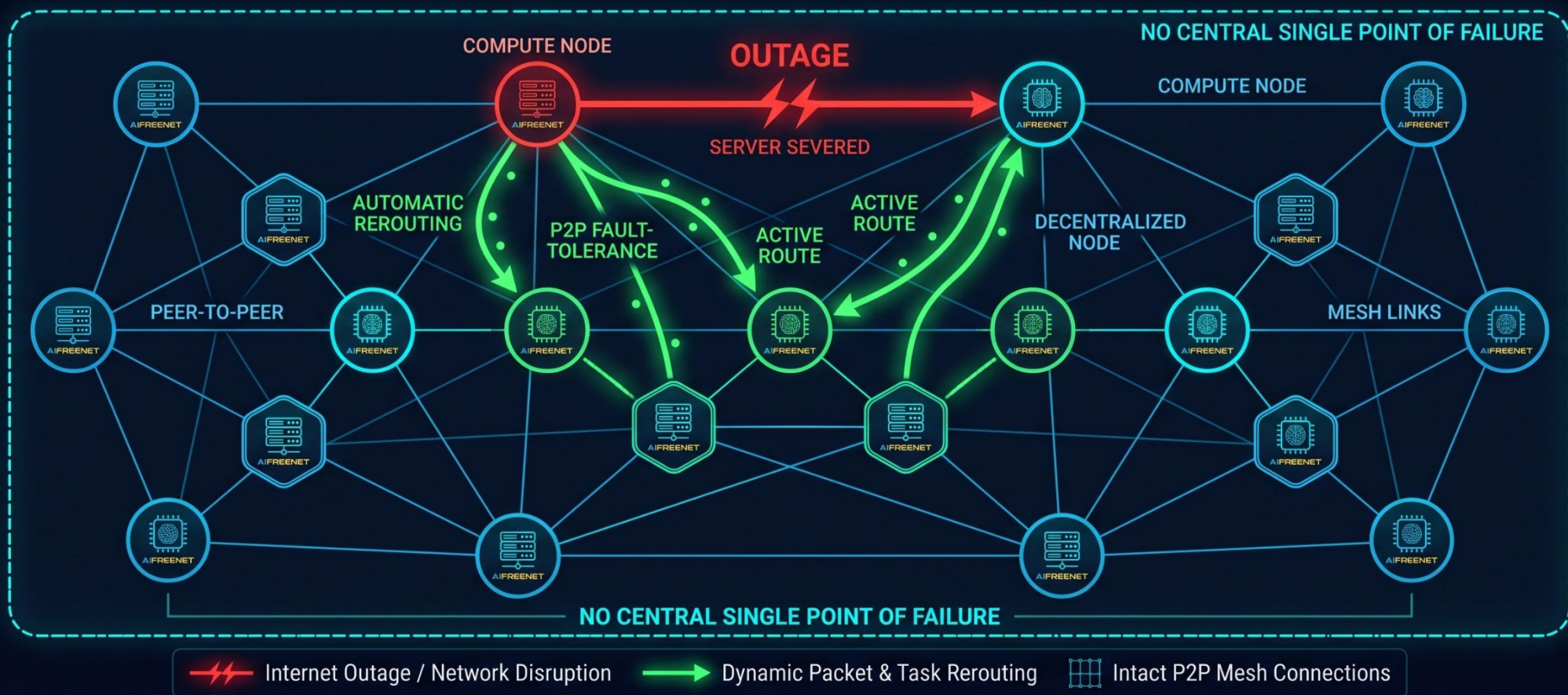
- Keine Nutzer-Profilierung: Es werden weder Verhaltensmuster analysiert noch Werbe-Tracker eingesetzt.
- Rechtssicherheit: Vollständige Konformität für Privatanutzer, gewerbliche Partner, Stadtwerke und Kommunen.

10. Decentralized Mesh: Outage Resilience

Ausfallsicheres Peer-to-Peer-Netzwerk ohne Single Point of Failure.

DECENTRALIZED MESH: OUTAGE RESILIENCE

P2P FAULT-TOLERANCE & DYNAMIC REROUTING



10. Decentralized Mesh: Outage Resilience

P2P FAULT-TOLERANCE • HIGH-AVAILABILITY CLUSTER

Every node is a peer. If a route fails, the mesh instantly dynamically reroutes tasks. Ongoing operation is guaranteed.

AIFREENET
INTELLIGENCE LIMITLESS

- Dynamisches Rerouting: Fällt ein übergeordneter Knoten oder eine regionale Internetverbindung aus, leitet das Mesh-Netzwerk Datenpakete sofort über alternative Knoten um.
- Kontinuierlicher Betrieb: Das verteilte Netzwerk bleibt auch bei lokalen Leitungsstörungen voll arbeitsfähig.