

Access Control for the AI Era

CAMARA Zero Trust AI Inference Gate*

Centillion's CAMARA Zero Trust AI Inference Gate adds an independent, operator-originated network evidence layer to enterprise AI. Before inference, CAMARA telecom APIs evaluate SIM-swap, device-swap, roaming, and location signals for the device, surfacing account takeover and credential abuse before a prompt reaches the model.

Running on Intel® Core™ Ultra processors, OpenVINO™ Toolkit optimizes local AI inference for responsive performance at the edge, while a risk-based policy engine determines whether requests are approved, restricted, or denied. The result is secure, auditable AI access without requiring specialized security hardware.



*CAMARA is an open-source Linux Foundation project defining standardized APIs for telecom network capabilities, exposed commercially via GSMA Open Gateway. Individual CAMARA APIs, including Device Location, are subject to operator commercial availability.



Key Intel-Enabled Features



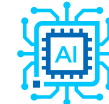
Real-Time Verification



Policy-Based Access



Location Awareness



Local AI Inference

- [Intel® Core™ Ultra processors](#) accelerate local AI inference for responsive, low-latency enterprise AI access.
- [OpenVINO™](#) optimizations enable efficient LLM execution on Intel-based edge systems.
- Intel AI acceleration supports real-time verification and policy decisions before inference.
- Intel® processor-based local inference keeps model execution at the edge, while network evidence supports auditability.

By leveraging Intel® technologies, Centillion's CAMARA Zero Trust AI Inference Gate combines local AI inference with operator-originated network evidence to govern access to sensitive AI applications.

Notices & Disclaimers:

Intel technologies may require enabled hardware, software or service activation. // No product or component can be absolutely secure. // Your costs and results may vary. // Intel Statement on Product Usage: Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's [Global Human Rights Principles](#). Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights. © Intel Corporation, Intel, the Intel logo, Intel Core, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as property of others.

*CAMARA Zero Trust AI Inference Gate by Centillion turns operator-originated network evidence into a **policy and audit layer for enterprise AI.***

Ordering Guidance:

- [Contact Us](#)

Country/Geo: Worldwide

Edge Verticals: Enterprise; Cross-Industry

Edge Use Cases: Zero Trust AI; Account Takeover Prevention; AI Governance & Auditability; Secure AI for Distributed Workforces

Learn more:

- [Centillion AI Website](#)