



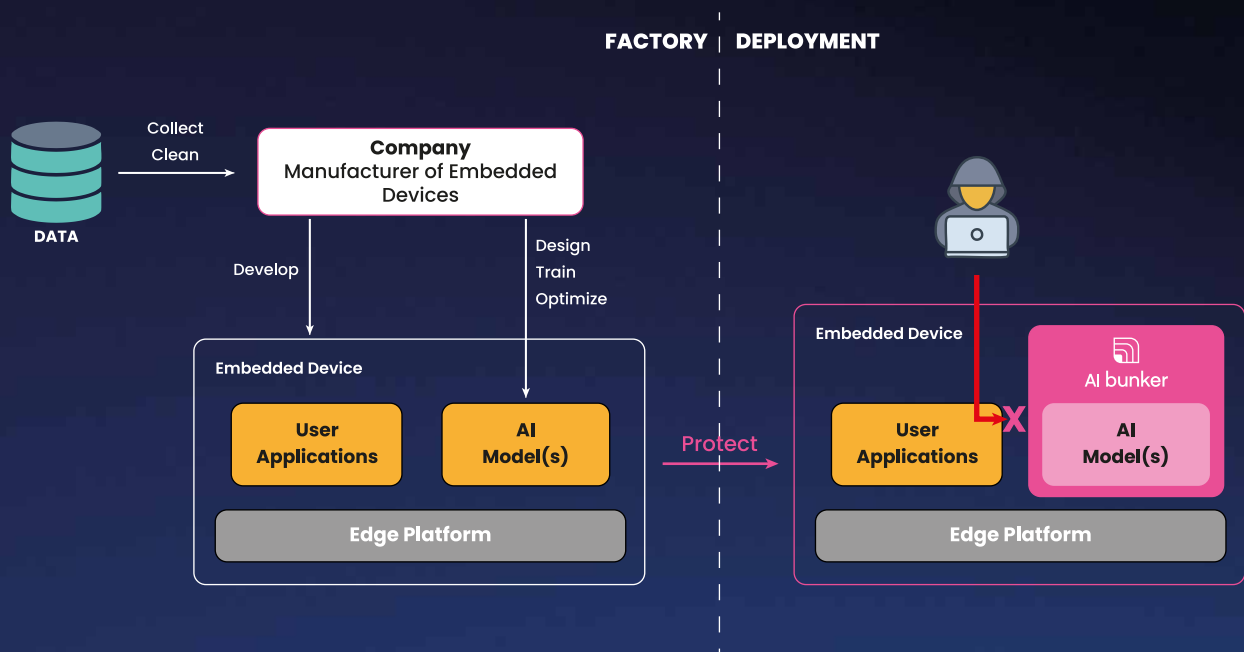
AI bunker

Protect Your AI Models At The Edge

PROTECTION FROM THEFT
AND UNAUTHORIZED ACCESS

SEAMLESS MODEL INVOCATION
WITH STANDARD AI WORKFLOWS

REAL-TIME INFERENCE
PERFORMANCE



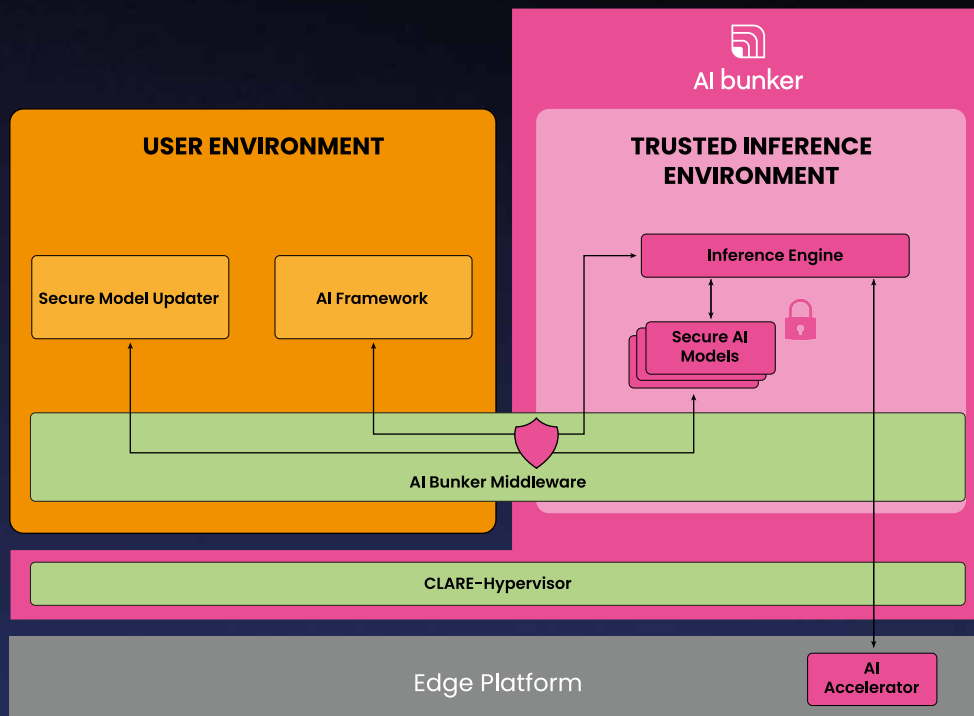
AI Bunker empowers embedded device manufacturers to:

- Safeguard **proprietary AI models** from theft, reverse engineering, and unauthorized access
- Ensure **seamless model invocation** with standard AI workflows, reducing development and deployment complexity
- Deliver **real-time inference performance** for secure AI use cases on embedded devices
- Provide **secure model storage** in isolated partitions
- Implement **advanced security protocols** and **AI model updates**
- Support **tamper detection**



AI bunker

Protect Your AI Models At The Edge



- A strongly isolated **Trusted Inference Environment (TIE)** for storing and executing encrypted AI models at runtime
- A customized version of **CLARE-Hypervisor**, an Accelerat's proprietary next-generation hypervisor conceived with cutting-edge safety and security features that implements strong isolation and security run-time monitoring
- Pre-installed and pre-configured **security hardening mechanisms** at both Hypervisor and TIE levels
- **AI Bunker Middleware**, which:
 - Abstracts **secure AI model inference invocation** in the TIE via a standard API compatible with popular AI frameworks
 - Enables secure **AI model updates** within the TIE