**🔐 A. SECURITY MEASURES**

**✅ 1. Code Obfuscation**

* Use tools to **obfuscate your code** and make it unreadable for reverse engineering.
* Applies to: .exe, .dll, .jar, .pyc, etc.
* Tools:
  + **.NET** → Dotfuscator
  + **Java** → ProGuard, DashO
  + **Python** → pyarmor
  + **C/C++** → LLVM Obfuscator

**✅ 2. License Enforcement**

* Use strong **license keys** tied to:
  + Hardware ID (MAC, CPU ID)
  + Time validity (e.g., 1 year)
  + User identity (email/domain)
* Validate license **online** via secure API.

**✅ 3. Anti-Tamper & Anti-Debugging**

* Add runtime checks to detect:
  + Debuggers (like OllyDbg, x64dbg)
  + Modifications to binary
  + File integrity via hash check
* Terminate the app if tampering is detected.

**✅ 4. Server-Side Critical Logic**

* Keep core logic (e.g., pricing, AI models, compliance validation) on a **remote server**.
* Make the thick client just a **front-end** that connects via secure APIs (HTTPS with mTLS).

**✅ 5. Cryptographic Protection**

* Encrypt:
  + Software configuration files
  + Sensitive local storage (SQLite, XML, config files)
* Use **AES-256** and rotate keys periodically.

**✅ 6. Secure Packaging & Installer**

* Digitally sign your installer with a **code-signing certificate** (from DigiCert, Sectigo, etc.).
* Distribute via secure channels only.
* Use installer tools like **Inno Setup, NSIS, or Advanced Installer** with license checks.