Quarkslab

AI PROTECTION

Shield

AI SECURITY

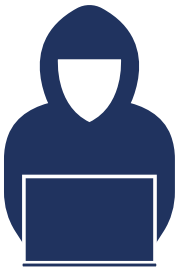
PROTECT YOUR AI MODELS: SAFEGUARD TRUST AND INNOVATION

As AI becomes integral to your business, safeguarding your models from **reverse engineering, unauthorized access, and tampering** is essential for maintaining trust, growth, and sustainability.

- **Prevent unauthorized and malicious exploitation**
- **Protect your investments and sensitive data**

Secure the core of AI innovations: Model, Data, & Code

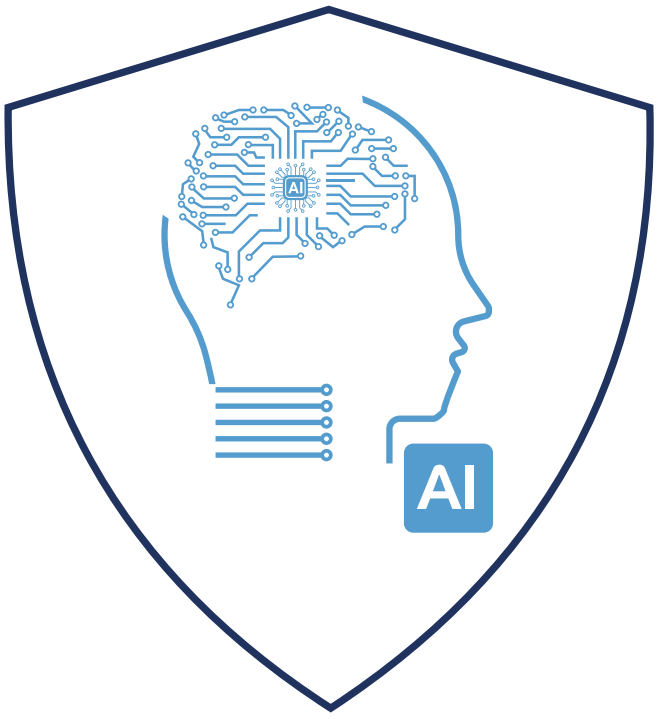
KEY RISKS



Reverse engineering, replication, manipulation

Theft & extraction of AI model

Data manipulation leading to distorted outcomes



QShield

AI SECURITY

PROTECT AGAINST STATIC AND DYNAMIC ATTACKS WITH QSHIELD APP PROTECTION

Protect your AI Assets

- **Advanced Code Obfuscation to Shield the AI Engine:** Use sophisticated techniques to hide the AI engine's source code, making it difficult for attackers to understand or tamper with the proprietary algorithms and logic.
- **Robust Encryption to Protect Trained Models:** Implement strong cryptographic methods to secure the data of trained AI models, preventing unauthorized access and extraction of valuable insights.
- **Runtime Application Self-Protection (RASP):** Integrate security measures within the application to detect and respond to tampering or misuse in real-time, ensuring the application remains secure and functions correctly.

Platforms

- iOS, MacOS
- Android
- Linux
- Windows
- Baremetal

Preserve value

- **Make it harder for attackers to interpret & misuse your technology**
- **Preserve your strategic & commercial value**
- **Maintain integrity, ensure reliable & secure operations**

Quarkslab

QShield

AI SECURITY

QShield App Protection Obfuscation Passes: C, C++, Objective C, Java, Kotlin, Swift

Comprehensive Protection

- **Control Flow Protection:** Safeguards the control flow graph, making it harder to decipher
- **Data Protection:** Protects constants and arrays
- **Call Graph Protection:** Protects the function call graph
- **Operations Protection:** Protects the operations in functions

Customizable Obfuscation

- Customize protection levels and performance impact.
- Apply obfuscations probabilistically or systematically.
- Combine passes to create unique schemes for different codes or versions.
- Generate countless unique obfuscation schemes to boost security.

Runtime App Self Protection (RASP): Android, iOS, Linux & MacOS

RASP protects the app against its environment and adjusts its behavior accordingly. QShield injects checks at compile time to detect alterations by attackers, safeguarding against dynamic attacks.

- **Anti-native code lifting:** guarantees that attackers cannot execute the native libraries of an Android app outside the original application
- **Bind APIs:** protects shared libraries from being replaced and encodes them
- **Breakpoint Detection and anti-debugging**
- **Code Integrity Checks**
- **Date dependency**: limits code usage after a certain period
- **Anti Root/Jailbreak:** blocks code execution on rooted/jailbroken devices
- **Anti Virtual Machines:** prevents code execution in virtualized environments
- **Custom checks:** enables developers to define and perform runtime checks on specific conditions, signatures, files, and portions of their applications against modifications

WHY CHOOSE US?

- Code & data obfuscation & RASP to protect against static and dynamic analysis
- Adaptive protection for constrained environments and high-performance algorithms
- Easy integration within days
- Suitable for initial design and connected devices
- Over 30 obfuscation passes
- Support for multiple environments and OS
- Low-code approach

QUARKSLAB AS YOUR LONG-TERM TRUSTED SECURITY PARTNER

We are a team of highly skilled engineers who possess extensive knowledge in compilation infrastructure, program analysis, software engineering, and cryptography. Our team includes reverse engineers, vulnerability researchers, and security engineers.

Our product evolves through an iterative process of attack and defense,

resulting in constant improvement over time. This unique approach is why our customers invest in us as their long-term security partner.

Learn more and check our latest resources

Whitepapers: **https://quarkslab.com/resources/**
On demand webinar: **https://quarkslab.com/webinars/**

Quarkslab

Contact and follow us