QShield

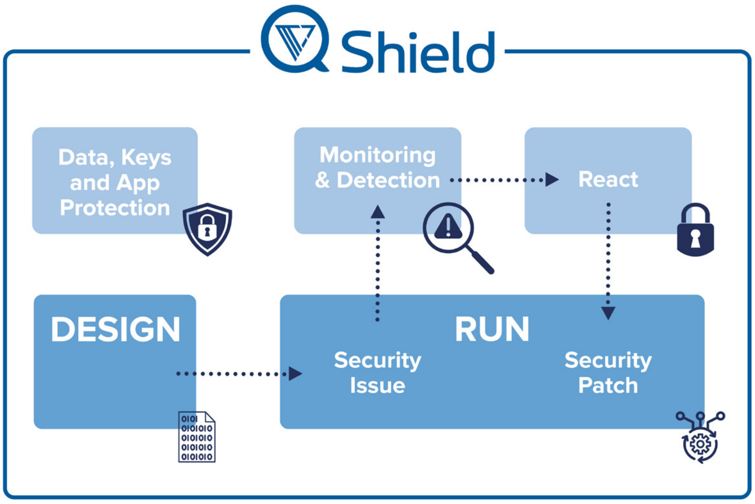
DEVICE & APPLICATION SECURITY

Secure connected devices and apps against data, code, and IP extraction or alteration from design to deployment

The rise of **connected devices** across industries (manufacturing, automotive, energy, utilities, retail, etc.) with the increased reliance on software, has made devices and their **applications** an attractive target for cyber attackers. **Application and service providers risk a negative impact on their business-** loss of revenues, negative brand image, loss of trust from customers and increased competition, as a result of several security challenges today:

- Extraction/**tampering of sensitive algorithms and unprotected data** risks **intellectual property** theft, counterfeiting, damaging, ransomware, service disruption, abuse, or usurpation
- The lack of **real-time visibility on vulnerabilities** on the field makes it challenging to detect attacks/issues and adapt security levels
- **Misconfigurations** due to **shared TLS certificates** for instance or unprotected configuration files can lead to device damages, recall, fake devices and failure to comply with **regulations**.

*According to a Gartner® report *, "AMTD is an evolution of MTD, which is based on the basic premise that, 'a moving target is harder to attack than a stationary one.' It involves the use of strategies for orchestrating movement or changes in various IT environment components and layers, across the attack surface, to increase uncertainty and complexity within a target system."*



- Applies to all devices (including memory and CPU constrained environments)
- Fast integration (few days only)
- No device remanufacturing required
- Complies with latest regulations (EU CRA, ETSI, AFNOR, NIST, SESIP, ISO)
- NIST verified white-box cryptography accelerates FIPS certification

ST life.augmented Authorized Partner

Part of ST Partner Program for data and IP protection.

MENDER

Integrated with Mender's device management solution.

QShield's MTD technology enables service providers to adapt the security strategy for their fleet, in real time, without having to recall devices or recode an application.

Build your defense against fraud, theft, damage and unlawful reproduction of apps and devices

App Protection

Code & data protection, dynamic protections and integrity checks thanks to obfuscation & RASP

Keys Protection

Cryptographic keys protection against extraction thanks to white-box cryptography

EMVCo EVALUATED

Data Protection

Safely store sensitive/ value-added data using software and/ or hardware security components.

Environment Checks

Monitor device fleet sanity and detect tampering in real time. Adapt security policies thanks to Moving Target Defense.

* Gartner, Emerging Tech: Security - The Future of Cyber Is Automated Moving Target Defense, 28 February 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved

Contact and follow us ✉ 🌐 in

Quarkslab