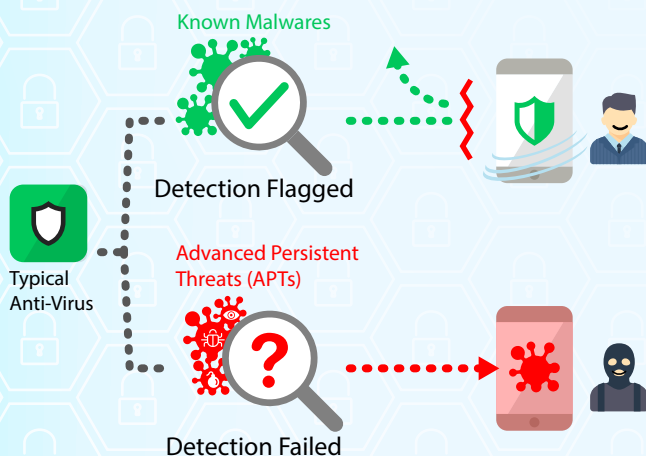# ST Protect

An Innovative AI Software Against Cyber Attack

Mobile devices enhance your operation efficiency and productivity by mobilising your everyday work. Mobility gives you convenience to access company data wherever you are and whenever you need it. Under the trend of mobilisation, a robust security solution is pivotal to protect your IT infrastructure and your business.

Solution Description

To mitigate cyber attacks, ST Protect monitors and detects the threats and unusual behaviors of the mobile devices, the applications, as well as the network. Empowered by A.I. and Machine Learning behavioral technology, it comprehensively protects the iOS and Android devices against the advanced mobile threats by integrating offline and real time detection in a multi-layers approach.

How Secure is your Mobile Device ?

Typical Anti-Virus:
- Known Malwares — Detection Flagged
- Advanced Persistent Threats (APTs) — Detection Failed

ST Protect:
- Known Malwares — Detection Flagged
- Advanced Persistent Threats (APTs) — Detection Flagged

Advanced Persistent Threats (APTs)

- Able to pass through basic virus scans undetected by hiding in seemingly harmless apps
- Release malware once the app is launched
- Access other apps in your device, including email, online payment or social media apps

Sensitive information such as user credentials and financial data will be stolen

ST Protect is a suite of enterprise security products that delivers continuous, real-time and end-to-end threat protection to device, network and application with better user experience.

Flexibility on Enterprise Mobility Solution Integration
(Enterprise version only)

- Integrate with Enterprise Mobility Solution to restrict secure container access, or make real-time, risk-based policy adjustments on compromised devices
- Enjoy the flexibility on whether integrating the security policy with the Enterprise Mobility Solution, without occupying EMM profile in your iOS device

Advanced End-to-End Threat Prevention

- Analyse device, application and network level attacks through A.I. & Machine Learning behavioral engine Identify known & unknown threats and Zero Day attack by on device behavior analysis
- Monitor device behavior continuously in an offline, online and real-time mode
- Optimise battery life with minimal device impact
- Protect user privacy: No DPI, Custom Privacy Configuration
- Prevent from the attack to MMS, NFC, Bluetooth and file

Real-time WiFi Network Detection

- Prevent WiFi Man-in-the-Middle (MitM) attack by detecting malicious network behavior and conditions in both incoming and outgoing traffic
- Disable suspicious networks automatically to keep devices and your data safe

Easy-to-use with Simple Procedures

- Offer better user experience with simple user interface
- Display the analysis of all apps including the information of the mobile devices, the applications and the network
- Require No IT Support

Flexible Solution at Affordable Cost

- No restriction on ISP (Enterprise version only)
- On-demand license scale up
- No Upfront CAPEX investment. One monthly fee.

Contact us

For more information, please contact your Account Manager

☎ 2281 8818
✉ business_markets@smartone.com
www.smartone.com

SmarTone SOLUTIONS