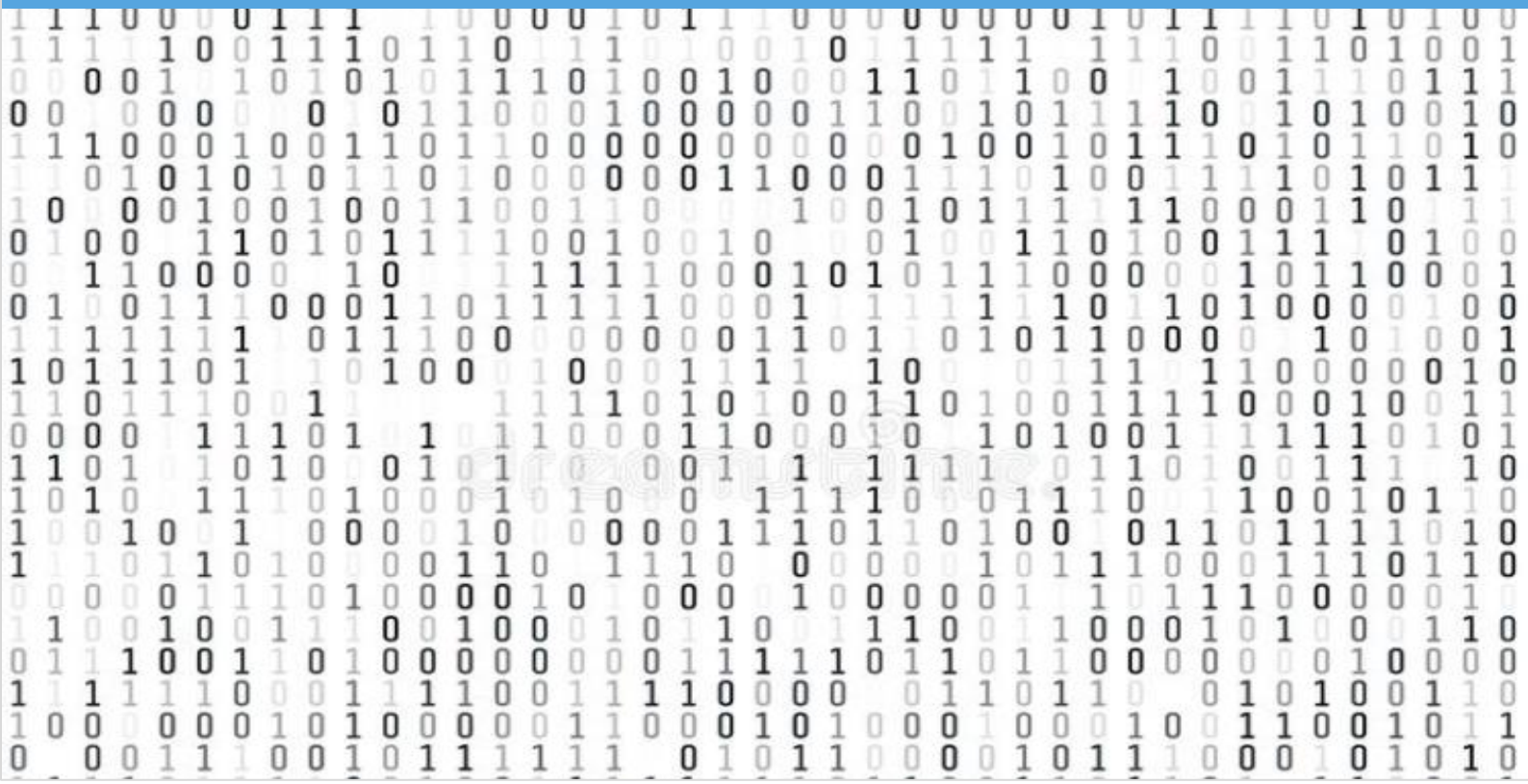
TMG

FortOne
White Paper



TMG Solutions Ltd.

Overview

The following white paper is for security professionals, organizations' administrators and professional end users who are in charge of mobile cyber security. The white paper explains the challenges which FortOne is designed to confront, the system structure and capabilities, and the different modules.

In recent years, the primary cyber-attack interface has changed. According to cyber analytics, end-points in general and especially smartphones are currently the most common cyber-attack interfaces. In the days before the business mobile phones, attackers addressed the organization back-bone, going through the organization's firewalls and other network appliances and applications in order to collect data or for any other malicious reasons. But as the business world changed to smartphones, so did the cyber-attack interface change to target mobile phones.

Mobile phones are popular cyber-attack targets for the following reasons:

- Most of the mobile phones includes private data and applications which coexist alongside organizational and any other sensitive data on the device. The end-user's primary use of the mobile phone is private, and private applications will get higher attention from the user, increasing the interface's vulnerability to attack.
- Mobile phones can create a tunnel or a gateway to the organization's data center, thereby increasing the level of damage created by the attack
- End users carry the mobile phone everywhere and all the time, including 'out of the office' meetings and 'off schedule' tasks
- Since mobile phones are always connected to a variety of network interfaces it is easier to trace and attack them
- Some organizations are using BYOD which make the device defiance more complicated and problematic
- Mobile phone allows an easier more specific attack when the attackers are after one employee or team

Cyber-attacks vary in type and can include a number of different options. Examples of the most frequently used attack options are:

- Voice recording (calls and eavesdropping)
- On device data collection
- Network data collection
- Location spoofing (trace)
- Identity theft
- And more…

Some attacks may include more than one option.

It is important to be aware and to take into account that along with the direct and immediate impact of the attack, usually easily traceable, some attacks can create long lasting untraceable damage like a continuing data leakage,

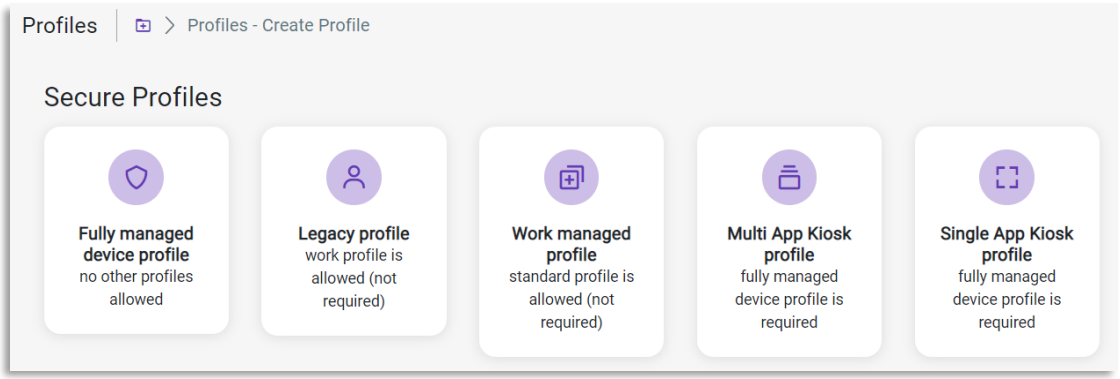
a backdoor to the organization's resources or nesting on the device for a later, trigger-based, attack.

Attack technologies are rapidly developing, constantly becoming more advanced and sophisticated. At the same time more and more sensitive data is getting used on mobile devices. It is an ever-growing challenge to create security solutions that will give overall protection for both data and device.

FortOne

FortOne is an on-premises/on-device solution designed to secure Samsung devices on the highest level. FortOne includes a combination of different static and dynamic procedures which are seamlessly connected to provide a complete end-to-end security solution, and at the same time provide the best possible user experience.

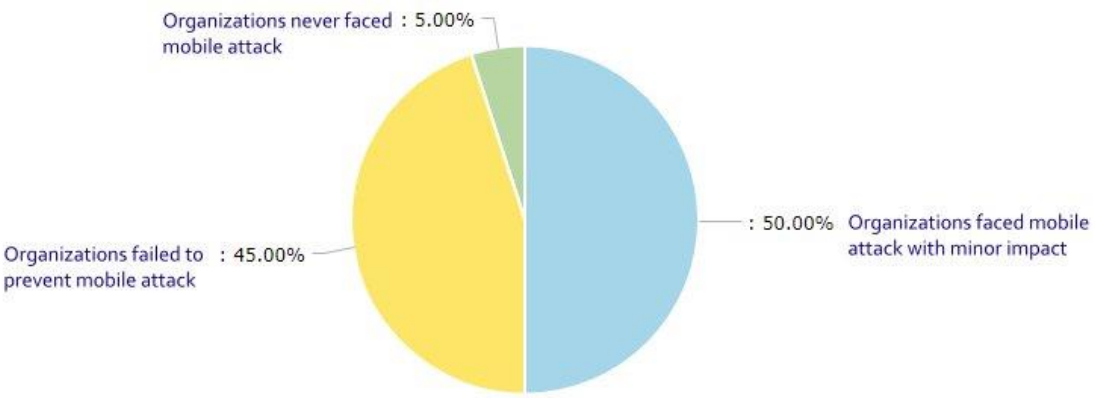
FortOne is a unique propriety technology. It is based on years of hands-on mobile cyber security experience, of confronting attacks from lowest to highest risk levels, and providing protection for endpoints and data in the enterprise and security worlds. The experience gained in these years, combined with up-to-date field knowledge of end-user experience, helped us design a holistic protection doctrine for our engineers and analysts.



FortOne's design approach is based on a core structure of different mechanisms including AI and machine learning procedures. In order to eliminate attacks on endpoint interfaces FortOne maps the devices' interfaces and establishes defense mechanisms for each of them. Usually, several different mechanisms will be established for each interface, using static, dynamic and behavioral related mechanisms.

FortOne uses real-time data to erect the most effective defense mechanisms on the go and everywhere. It requires no other interface or mechanism to supply overall protection. Data is collected and securely sent

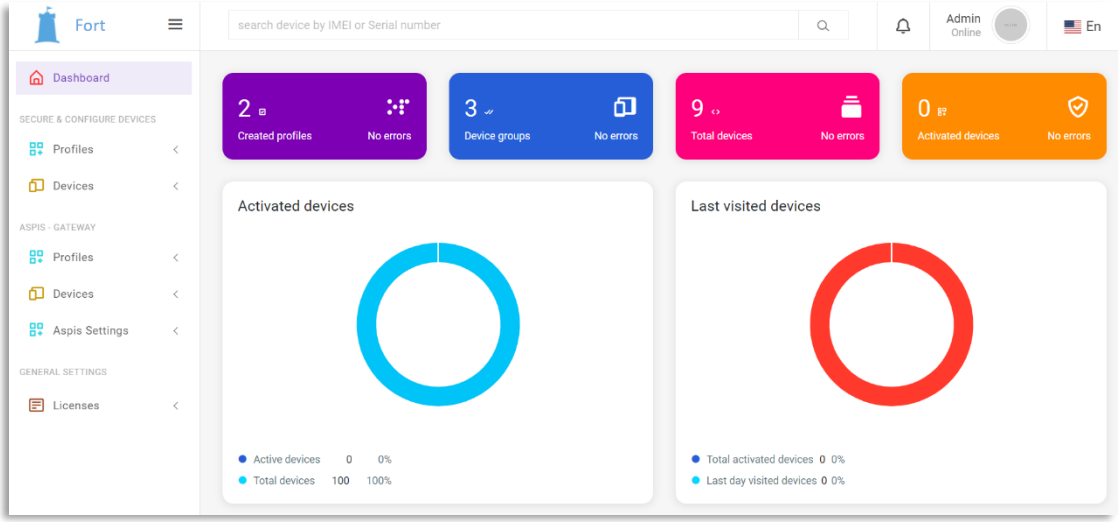
back to its unique server at the organization, for further analysis and archiving (optional).
This state-of-the-art technology utilizes hardware components of all device vendors (Google and Samsung) along with newly designed components and methods, creating a strong synergy between FortOne's components which results in a holistic defense solution for both data and device.



Any attempt to affect any of the device's OS load steps will trigger immediately the following processes:

- Set the warranty bit to 0X1 (hardware-based implementation with no undo option)
- Erase the unique, hardware based, encryption key
- Permanently block the access to any confidential/sensitive data on the device. The same block will take place in any attempt to remove one of the hardware sensitive chips (memory related).

The combination of hardware and software defense procedures creates a completely secure device with a number of defense levels to allow the best UI and UX along with the highest level of security.



With our **unique** capabilities FortOne users and organizations can completely rely on end-user device security system.

Based on our up-to-date, hands-on knowledge of end-user experience, FortOne architecture is designed with the user in mind, making it very user friendly and keeping the devices' original UI and UX.

FortOne's design includes a core module and a tailor-made modular configuration capability (optional) in order to create the best solutions for our customers. The customized configuration option of FortOne includes UI and UX options such as auto define communications profiles, boot animations, auto define backgrounds, auto define contacts, auto documents download, auto applications installation, re-assign physical device buttons, auto define APN/VPN profiles and much more.

An important part of the holistic defense solution offered by FortOne, is the FortOne Server. Though FortOne is an independent on-device system, the unique design enables secure data streaming from the device to the server for AI analysis to detect possible attacks as well as further analysis and archiving (optional).
The FortOne Server regularly collects information from devices, analyzing the collected data and triggering actions according to the analyzed data output. The collected data includes devices' core events output, network events, resources used by on-device apps and by the device OS.
The server deploys several different analysis engines in order to find any abnormal behaviors and network requests, restrictions requests, components usage (allowed or disallowed) and more. Based on the analyzed data the system can then trigger an action on the device according to the organization's configuration and the risk level to the device or to the on-device data. This automatic action can include a variety of procedures (from sending alerts to the device's user/administrator, through locking the device and up to deleting all device data).

FortOne Server regularly collects information regarding the device behavior, actions and events

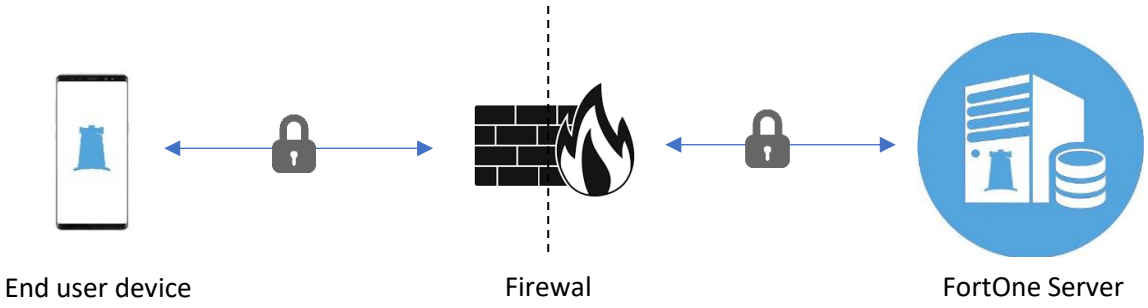
↓

Running analysis engines over the collected data using AI methods and procedures

↓

Triggering actions on devices when required, according to the organization's FortOne policies

The FortOne Server is a stand-alone, on-premise server which can be located on the Organization's premises. Devices communication with the server is secured and encrypted and will never include personal user data (IM chats, email, pictures, videos and etc.).



About TMG Solutions

TMG Solutions was founded in 2008 by an elite team experienced in all aspects of mobile enterprise: development, cyber security, system integration, device and data management, technical support and professional services for enterprise mobile systems and mobile operating systems.

Among TMG Solutions' products you will find a variety of security products, control & monitoring products, mobile device application development, server-side development, tailor-made applications for cross-market businesses and a wide range of unique technological projects related to the mobile cyber security and mobile enterprise worlds.

Our customer list includes large enterprises from all sectors, major banks and financial institutions, mobile carriers, telecommunication companies, government ministries and entities, commercial enterprises, defense related enterprises and many others. We are the prime supplier of mobile security services for all sensitive data – from national security to financial data – in Israel.

TMG Solutions is the Israeli government's sole provider for mobile security solutions, and has been for the past 7 years. We provide all government ministries complete solutions from devices and mobile applications to related servers.

TMG Solutions Ltd.
9 Mota Gur
Petach Tiqwa, Israel
e: fortOne@tmg.co.il
w: www.tmg.co.il