Product Requirements Document for a Firewall Solution for Smartphones



Gallneukirchnerstrasse 17a

A - 4040 Linz

Autor:

Dr. Michael Nadehrirn  
Dipl.Ing. Christian Bernthaler

im Auftrag von

**Green Danube Cloud**

Linz, June 9, 2014

Inhaltsverzeichnis

[2 Changelog 3](#_Toc394904981)

# Changelog

|  |  |  |  |
| --- | --- | --- | --- |
| Ref. | Date | Comment | Editor |
| 1.00 | 30th May 2014 | First Draft (German) | Michael Naderhirn |
| 1.01 | 04.08.14 | Feature Classification and Description | Christian Bernthaler |
|  |  |  |  |

# Purpose and Scope

Over the last couple of years smartphones started to play a constant increasing important role in digital communication.

The scope of the project is to develop a security solution for businesses which safely integrates mobile devices into the IT infrastructure of a company. It is the goal to make privately owned mobile devices of employees available for the use during their daily work without actually putting the IT infrastructure to a thread. The advantage for the employee is that he/she can use this private owned devices without changing it every day while the advantage for a business is that they don’t have to maintain a mobile device for every employee which is very expensive. Instead the IT of the business can focus on the maintenance and the development of the business related apps and their secure integration into the IT infrastructure. The solution should be very economic but still maintain certain high level of safety.

From a technical point of view the following features are commercial available today for the two main operating systems Android and iOS.

## Android

Most evaluated Android apps provide features beyond a simple Virus Scanner. They compete within the following categories: Antivirus, Firewall, Privacy, Backup, Antitheft and System-tweaks.

### Antivirus

Within the Antivirus category a scanner feature is provided by all Apps, which will scan your phone for Viruses and Malware. The algorithm as well as the signature database is executed and stored on the phone by the majority of Apps. However, the App from Sophos Ltd. does the processing in the cloud which obviously will produce network traffic. As far as described by the developer most of the scanner will check for virus and malware infections. Some companies choose to offer a malware scan as an optional premium feature, while others are very unspecific about what they scan for. While technically any virus is malware, news reports about viruses resulted into marketing Applications as Antivirus rather than Antimalware. In regard of the capability of these scanners, it all comes down to marketing which (falsely) splits the applications in Antivirus and Malware. While the underlying database with signatures is different the functionality is the same for both. Some apps allow the user to select the files, folders (incl. external SD cards), apps, etc. to be scanned. A scan scheduling feature is provided by some apps to allow the phone to execute the scanner automatically at the user defined date and time, which might also be sold as a premium feature by some Apps.

### Firewall

This feature category is divided into the classical firewall (blocking IPs and services) and what is referred to as “Web Shield” by most of the apps (blocking websites). Classical Firewall implementations does exist only in a minority of Apps, due to implementation restriction (as described in the “Technical” section). On the other hand all seem to provide the ability to filter websites.

### Privacy

Very few of the tested apps provide specialized scanners (sometimes as separate app) for facebook, twitter, or other social apps which will alert the user of insecure settings. The crucial features within the category are App-Permissions, Parental-Control (App Lock) and Spam Block. App Permission are presented to the user filtered by a scanner or as a classified list. Some offer to block permissions if root access is available. Parental-Control will block the execution of apps by asking for an unlock pattern or key. The spam blocking feature checks incoming phone calls and SMS and blocks them.

### Backup

While most apps provide the ability to store contacts, only a few also backup sms, call histories, file (pictures, documents,…). Application Backup is mostly available as a premium service (probably due to the traffic volume required).

### Anti-Theft

The features within this category try to offer security in case the device gets lost or is stolen. Most of the features can be triggered by SMS commands or using the developers web-service. Depending on the country (not allowed in Germany and Austria) the App will take a picture of anyone who enters the wrong unlock code more than three times. In case one has misplaced the phone, another feature will play a siren sound to locate it this way. However, the most advertised feature is locating via geo location (GPS, Network…). More advanced features, not provided by all apps include, remote controlling the security app itself, taking pictures, sending messages and initiate callbacks. One app even offers a geo fencing feature, where the geo location is used to block apps, content, or send automated alerts (calls, SMS, E-Mail) to user-defined contacts.

### System Tweaks

The simplest of these features display statistics, like network data usage, battery consumption and memory allocation. More advanced features allow to automatically stop running application or free memory by scanning for unused files.

## iOS

Compared to Android, very little Apps exist that handle security related Tasks. Those that does exist can be placed in the same categories as Android, but competition is very category specific.

### Antivirus

Unlike Android there are only a few Apps that advertise the use an antivirus scanner. Most of these scanners work in regard to known vulnerabilities, watch for unknown processes and malware or conduct cloud-based scans of cloud-stored files. Scan scheduling or other features available under Android are missing entirely.

### Firewall

Like with the Antivirus category, classical firewalls do not exist for iOS. There are a variety of Apps providing web traffic filtering, link on Android.

### Privacy

These kind of features are also missing from security apps, but are available separately for all kind of social media. Some apps offer Parental-Control settings as premium feature.

### Anti-Theft

Like the other categories, this functionality is provided by separate Apps which were not part of this analysis.

### Backup and System-Tweaks

Backup is limited to contacts and photos, and also system tweaks could only be found in one of the test apps.

# Stakeholder Identification

Direct involved:

* GDC stuff
* NM Robotic

Indirect involved:

* Business development of product like ITACH

# Market Assessment and Target Demographics

In the following a market assessment is performed. Potential competitors are analyzed in terms of company, products, functionality and IP rights. To give a consecutive overview of the functionality a comparison table finalizes the market assessment.

## Companies, Products and IP Protection

The company is analyzed in terms of company history, product range and business model. To find any IP protection rights a patent recherché is performed on <http://worldwide.espacenet.com/advancedSearch?locale=en_EP>.

### Avira

#### Company

Is a German based company.

#### Products

They offer a range of free and commercial security products. Their free security products are available for the following OS:

* Win
* MAC
* Android
* iOS

The commercial products are only available Windows platforms (that’s where the make money). They offer a desktop pilot solution where you can manage all your personal devices where Avira is installed.

#### IP Protection

There where three patents found, where one is considered to be relevant.

### AVG Antivirus

#### Company

AVG is Dutch based company

#### Products

AVG’s detection technology is based on several layers (<http://www.avg.com/de-de/avg-software-technology#mainFaqDiv-3382054907185018189-0>) which are:

* Signature based (detects known viruses)
* Polymorph based (detects anomalies)
* Heutristic based (analyzes the behavior of software in order to detect unknown viruses)
* Behavior based (patented technology – see IP protection)

AVG offers a range of products for mobile devices and tablets. For mobile devices and tablets the main product is an anti-virus scanner (free and commercial) for Android which can be used to check the system offline. For Windows, Android and iOS they offer different free and commercial products with functionality of synchronization, safe browser, and family safety.

#### IP Protection

AVG maintains several patents, but only one can be considered as kind of relevant.

### AVAST Security

#### Company

Is a Czech based company and was founded in 1988. It is strongly backed by venture capital

#### Products

For private users AVAST offers a free and a commercial product. The free product contains an offline virus scanner, a webshield for infected homepages (how does it work?), and a firewall functionality which is only working on rooted mobile phones. The commercial product contains functionality for remote access and control. As far as possible to see, only Android OS is supported.

#### IP Protection

No patents were found.

### Malware Bytes

#### Company

Is a US based company and was founded in 2004. It is strongly backed by venture capital

#### Products

Malwarebytes offers solution for private users under the brand name Norton. For business solutions

#### IP Protection

No patents were found.

### Symantec - Norton

#### Company

Is a US based company and was founded in 1982. Symantec is listed on the stock exchange.

#### Products

Malwarebytes offers solution for private users under the brand name Norton. For business solutions Symantec offers a product called BYOD (Bring Your Own Device).

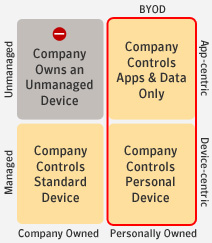


Figure Sketch of the BYOD product

The basis for BYOD is the categorization of mobile device according it user (company or personally owned) and how it is managed (unmanaged or managed) (see Figure 1). The most expensive solution is the lower left one (Company controls standard device) while the most economic one is the right upper solution (Company controls apps & data only).

In order for a business to implement a mobile device strategy four areas are identified:

* User- and app-access
* Security for apps and data
* Device management
* Device security
* Safe data access

Each of this areas comes with its on technological solution (product – basically a combination of the single product solution of the competition) and must guarantee that everything the private traffic is clearly and safe separated from the business traffic. Their product range can be seen at <http://www.symantec.com/de/de/products-solutions/solutions/detail.jsp?parent=mobile&child=5_pillars_mobile>.

#### IP Protection

A patent search with the keywords “Symantec” & “mobile” resulted to 38 hits, where the most relevant (24) are examined where 8 can be considered of importance.

### McAfee

#### Company

Is a US based company and was founded in 2004. In 2011 it became a subsidiary of Intel.

#### Products

McAfee offers a mobile security solution for Android OS and iOS. There is a free and commercial version where the commercial is ad-free and with support. Additionally they offer products for identity management and data access. All products are market as standalone solutions.

#### IP Protection

McAfee owns several patents and some of them can be considered as critical.

### KaperskyLab

#### Company

Is a Russian based company and was founded in 1997.

#### Products

Offers a product range which very similar to the Norton products. The BYOD product uses containers which can be encrypted in order to run company specific apps. An interesting feature is the real time protection against malware (see <http://www.kaspersky.com/products/business/security-applications/mobile-device-management> - see Anti Malware protection)

#### IP Protection

No relevant patents were found.

### TrustGo Inc

#### Company

Is a US based company.

#### Products

Offers only an app with a very unique feature that it scans traffic going to the web browser.

#### IP Protection

Holds one relevant patent.

### Note:

Even the patent and IP research was done carefully there is no guarantee of its total coverage. The search should be understood as a technical overview.

Only the most relevant companies were examined.

## Comparison Table for Functionality



Figure Feature table Antivirus Solutions (to see details look at according Excel sheet in the project folder)



Figure 3 BYOD and MDM Players



Figure 4 Feature table BYOD Solutions (to see details look at according Excel sheet in the project folder)

## Patent Table



Figure 5 Patent Table

## Conclusion

Looking over the whole product floor today shows a few interesting points:

* No “real-time” protection available on mobile devices, mostly offline protection
* Most companies focus on private users.
* Larger companies (Norton, Kapersky) offer a mobile concept for commercial users.
* No mentioning of multipathing protection
* iOS does not play a big role, most of the products are for Android based mobile devices.

# Product Overview and Use Cases

# Requirements

## Functional Requirements

**Personally owned Device in an Enterprise Infrastructure**

The “Bring your own device” strategy, which is part of Mobile Device Management, is controversial not solely because of its pros and cons but also due to legal (DSG (DACH), GDPR (EU), HIPAA/HITECH (US),..) and privacy aspects, and not suited for all companies.  
However, if a company allows their employees to bring their own devices the question is, what are key issues with regard to security, when do they come into effect? Also, how much control over its own device is the user willing to give to the company?

Security is a vast topic and cannot be addressed by software alone, yet with regard to the matter it can be condensed to information- and data security (which includes threads by malware). These issues start to occur as soon as users start a connection to the enterprise network to access data with their mobile device. What are the dangers? The dangers to security due to such connections are:

* Storage of confidential information on the device which
  + may be accessed by unauthorized entities through theft or loss
  + may be accessed by installed applications which
    - store them in third party storage (like cloud storage). Which may be legitimate but against company policy.
    - silently sends this data to third parties (without user knowledge)
  + sending or forwarding of data to external persons through unsecure data connections like UMTS which may be intercepted or would otherwise be blocked by the cooperate firewall
  + is (un-)consciously retained by the user after quitting the company
* Creating of a connection to the enterprise network which may be exploited by third parties via Malware on the mobile device

**User Requirements**

A user may want to / have to store certain company data on the device in order to work with them. This kind of data includes, but is not limited to:

* E-Mail and Attachments
* Presentations
* Notes
* Documents (Doc, PDF,…)
* Pictures and other Media
* Customer Information (Phonenumbers, E-Mail, Notes,…)
* Calendar Entries

In addition the user may want

* the embed the Company’s Calendar with their personal calendar entries, which are only stored on the phone and synced by another account (like google,…)
* Share Company Data with authorized personal (Who decides who is authorized to receive data? How to monitor that data is exchanged?)
* Access Intranet Websites from foreign (to the company) networks (Knowledgebase, CRM, …)
* Use Mobile Business Apps (Powerpoint, Word, CRM,…) maybe provided by the company
* Store Pictures or other Media on Company Servers for Documentation or other purposes
* Use Remote Locations and MDM solutions of Google or other Providers
* Allow Company to Locate Mobile if Lost (Optional)
* Use Private Apps without restrictions (Social, Games,…)
* Use internet and other phone services without restriction
* Modify and Root/Jailbreak Device as required

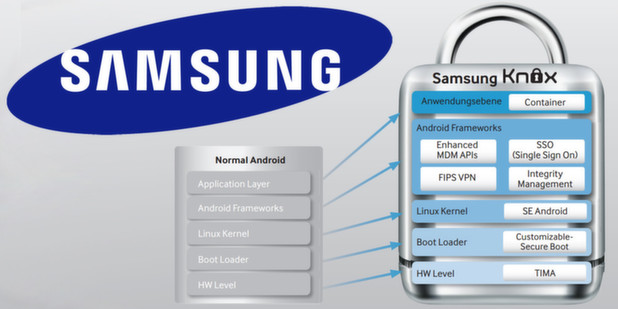
**Company Requirements**

Without any administrative solution the company can only trust in the user to properly (in the interest of the company) handle this data. From an administrative standpoint requirements are:

* remove all enterprise related data from user devices when necessary (device is lost, user leaves company,…)
* initiate wipe of company data via sms
* control which applications a user can run on the device when on company property
* detect malware that make it possible to hijack the phone and grand access to the stored data to unauthorized third party
* block, remove or warn the user about unsafe apps (determined by company administration)
* provide an app store to the user with selected save or self-developed apps and block other app stores.
* Mobile Device Management Solution which integrates with existing solutions
* Locate Mobile Device when lost
* Enforce password policies
* Encrypt company data stored on the phone

**Solutions**

Besides the available solutions presented in Figure 4, introducing to their Products in 2013 introduces a low-level solution to enterprise security and personal privacy just like Blackberry Balance. As displayed in the picture below, The Concept basically is to provide an Operating System with altered security policies inside a password protected, encrypted container which can easily be switched to and which completely separates enterprise data, apps, policies and device settings from those that are privately used.



Clearly, the possibility of this kind of virtualization of the operating system remains a sole prerogative of device Manufacturers as the integration of such a system without rooting and modifying the operating system is simply impossible.

**Concept**

Like competitors listed in Figure 4 shows, at least parts of the above solution can be implemented within the limitations of the API. Even with user owned devices and BYOD in mind, certain features might also be of interest with regard to corporate owned personally enabled (COPE) which is the opposite strategy to BYOD. The following compilation will try to establish a base set of features independent of any Mobile Operating Systems. They will have to be reviewed for each targeted Operating-System.

BYOD strategy features

* Application to start with system optional
* Application to start only though password, fingerprint, …
* Security Measure definable by Administrator through policy
* When uninstalled by the user all company data shall be removed with it
* Provide an app store for company owned, developed apps (controllable by the admin)
* Installed apps through that store (enterprise definied apps) shall be uninstalled upon uninstall of main app (unless the app was obtained by the user through the playstore)
* Optionally block Google, Samsung, and other app stores if the device is company owned
* Prevent execution of apps based on location (user acceptance?)
* Data is to be stored inside a password encrypted folder (referred to as container)
* E-Mails are kept on the server (IMAP, Exchange…)
* E-Mail Attachments are only downloaded on request of the user and only to the container
* SMS from company registered contact should also be redirected to storage inside the container
* Company Contacts are
  + Either provided by a browseable contact list implemented inside this main app
  + Is added to the mobile device by adding a sync-able account which deleted all contacts when the account is removed (encryption cannot be guaranteed if required)
* Access to Data is regulated to

Additional COPE strategy features

* Block Google, Samsung, and other app stores if the device is company owned
* Install app as System app to survive Factory reset (requires temporary root or custom rom)
* Remote lock and factory reset phone (SMS and web).



## Usability Requrements

## Technical Requirements

e.g. security, network, platform, integration, client

## Environmental Requirements

## Support Requirements

## Interaction Requirements

e.g. how the product should work with other systems

# Assumptions

# Constraints

# Workflow Plan

High level workflow plans, timelines and milestones (more detail is defined through a [project plan](http://en.wikipedia.org/wiki/Project_plan))

# Evaluation Plan and Performance Metrics