

Afaria Antivirus & Firewall Manager

PRODUCT DATASHEET

ANTI VIRUS KEY FEATURES

- Full protection from the latest mobile threats, via automatic virus definition updates
- The only mobile Antivirus solution employing advanced heuristic detection
- Real-time Monitor scans any file received via SMS, MMS, Bluetooth, WiFi, infrared, or desktop sync

FIREWALL KEY FEATURES

- Inbound and outbound traffic monitoring
- Network-level IP based packet filtering
- Filtering based on a customizable White list and Black list

CALL FILTERING KEY FEATURES

- “Black list” filtering of mobile spam and unwanted calls
- Option to block calls, messages or both
- Available for Windows Mobile and Symbian

With advances in wireless technology, smart phones and PDAs have evolved into many organizations mobile computing device of choice. These devices are now able to operate on multiple networks (i.e. cellular carrier network to a WiFi hotspot) and communicate with other devices via peer to peer communication, such as Bluetooth. The proliferation and convergence of technologies, such as business process automation, mobile application deployment, mobile commerce, mobile banking, and push email have generated widespread adoption of smart phones and PDAs across virtually all industries. As a result, threats to mobile operating systems are on the increase.

Mobile threats have escalated from simply a lost or stolen device scenario to more sophisticated, invisible attacks designed to either cause irreparable harm to your mobile device or intercept sensitive company data.

IDENTITY/INFORMATION THEFT

Mobile devices have become the place where corporate data resides when it is beyond the firewall, and as such, sensitive information is present on a variety of devices. This especially true in a field service environment where a field worker is providing service at customer locations making customer account information is vulnerable. Malware can secretly access information on the device and steal critical information such as a name, address, phone numbers, credit card number and banking information. Losing this information due to identity theft can have serious consequences for an organization, including but not limited to fines.

UNAUTHORIZED DEVICE USAGE

An infected device can trigger unauthorized application behavior in which a connection from the mobile device to the enterprise back-end can be triggered unknown to the end user or IT, and insert malware into the corporate network, which could cause anything from unwanted, erratic network behavior to the erasure of valuable data.

ANTIVIRUS PROTECTION

Afaria Antivirus secures mobile devices by scanning for malicious content on-demand and on-access. The on-access feature is continuously monitoring the device and scans all data received by the device. Once harmful content is detected, it alerts the user and offers the option to delete the data or save it. The user may also initiate a scan, using the on-demand feature.

Administrators can control the delivery of updates through administrative policies. Virus definition files are easily, securely and efficiently downloaded over-the-air to protect the enterprises mobile devices from the latest threats. And all activity is logged in the application's log files, recording the date and time of any scan performed, along with any virus activity detected and resolved during a scan, thus providing comprehensive compliance reporting tools.

SNOOPWARE

Snoopware is a subset of mobile malware that is capable of stealthily and remotely monitoring activities on mobile devices. These snooping activities include voice calls, messages, e-mails, and remote activation of functions such as a microphone.

FIREWALL

Afaria Antivirus & Firewall protects users from current and future threats by providing filtering and blocking of TCP/IP traffic. Afaria offers a bi-directional port and IP-based packet filtering option, protecting the mobile device from accessing harmful or questionable content and preventing malicious content from being transferred to the device.

The firewall monitors cellular data connections, WIFI, and all TCP/IP traffic, blocking and allowing incoming and outgoing data packets. The firewall can also be configured to block/accept traffic from a specific IP address or a range of IP addresses, providing control over all data traffic on all devices. For security audit purposes, the firewall has an activity log that keeps track of any changes to the firewall security level and information about any packets that are filtered.

Firewall Features Include:

- Inbound and outbound traffic monitoring
- Network-level packet filtering
- Full control of the alerts and logging functions
- User-friendly Interface
- Filtering based on a customizable White list and Black list

SMS CALL FILTERING

SMS Call Filtering is the premier message and call manager for mobile devices. Enhanced call and message filtering allow users to prevent interruptions and disturbances. With the capability of customizing the contacts into groups of black listed (blocked) numbers, Administrators can choose to block calls and messages from those numbers.

Solution Elements Include:

- Automated call & message filtering
- Creation of blacklists to provide customized call and message filtering
- Import feature, to blacklist numbers from the device's existing list of contacts
- Spam folder to detain unwanted messages
- Tracking logs for all blocked calls and messages