F-Secure Mobile Security

for S60

User's Guide

"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

This product may be covered by one or more F-Secure patents, including the following:

GB2353372 GB2366691 GB2366692 GB2366693 GB2367933 GB2368233 GB2374260

Copyright © 2004-2009 F-Secure Corporation. All rights reserved. 12000066-9L08

Contents

About This Guide 1

How This Guide Is Organized 2

Conventions Used in F-Secure Guides 3

Symbols 3

Chapter 1 Introduction 5

1.1 F-Secure Mobile Security 6

1.2 Key features 7

Chapter 2 Installation 8

2.1 System requirements 9

2.2 Getting the product running on your device 9

2.2.1 Installation 9

2.2.2 Activating the product after the installation 11

2.3 Transferring the subscription to a new device 12

2.4 Uninstalling 12

Chapter 3 Using F-Secure Mobile Security 13

3.1 Opening and closing the application 14

3.2 Scanning for viruses 15

3.2.1 Selecting the virus protection mode 15

3.2.2 Processing infected files 17

3.3 Using firewall 18

3.3.1 Selecting the protection level 18
3.4 Protecting confidential information 19
3.4.1 Using the device lock 19
3.4.2 Using the remote Anti-theft 20
3.4.3 Using the SMS alert 21
3.4.4 Locating the lost device 21
3.5 Protecting web browsing 22
3.5.1 Using Browsing protection 22
3.6 Keeping the application up-to-date 24
3.6.1 Selecting the update mode 24
3.6.2 Application updates 25
3.7 Purchasing subscription service time 26
3.8 Troubleshooting 28

Technical Support **25**

Overview 26
Virus descriptions on the web 26
Electronic mail support 26

About F-Secure Corporation

About This Guide

How This Guide Is Organized..... 2
Conventions Used in F-Secure Guides 3

How This Guide Is Organized

F-Secure Mobile Security User's Guide is divided into the following chapters:

Chapter 1. *Introduction*. Provides general information about F-Secure Mobile Security.

Chapter 2. *Installation.* Gives instructions on installing and activating F-Secure Mobile Security.

Chapter 3. *Using F-Secure Mobile Security*. Describes the F-Secure Mobile Security user interface.

Technical Support. Provides the contact information for assistance.

About F-Secure Corporation. Describes the company background and products.

Conventions Used in F-Secure Guides

This section describes the symbols, fonts, and terminology used in this manual.

Symbols

WARNING: The warning symbol indicates a situation with a risk of irreversible destruction to data.

IMPORTANT: *An exclamation mark provides important information that you need to consider.*

REFERENCE - A book refers you to related information on the topic available in another document.

NOTE - A note provides additional information that you should consider.

TIP - A tip provides information that can help you perform a task more quickly or easily.

⇒ An arrow indicates a one-step procedure.

Fonts

Arial bold (blue) is used to refer to menu names and commands, to buttons and other items in a dialog box.

Arial Italics (blue) is used to refer to other chapters in the manual, book titles, and titles of other manuals.

Arial Italics (black) is used for file and folder names, for figure and table captions, and for directory tree names.

Arial underlined (blue) is used for user interface links.

PDF Document

This manual is provided in PDF (Portable Document Format). The PDF document can be used for online viewing and printing using Adobe® Acrobat® Reader. When printing the manual, please print the entire manual, including the copyright and disclaimer statements.

For More Information

Visit F-Secure at http://www.f-secure.com for documentation, training courses, downloads, and service and support contacts.

In our constant attempts to improve our documentation, we would welcome your feedback. If you have any questions, comments, or suggestions about this or any other F-Secure document, please contact us at documentation@f-secure.com.

1 INTRODUCTION

F-Secure Mobile Security 6
Key features 7

1.1 F-Secure Mobile Security

F-Secure Mobile Security is a software product that protects data stored in your S60 device against malicious code attacks and monitors incoming and outgoing connections and protects the device from network intrusion attempts.

F-Secure Mobile Security scans all files for viruses automatically when they are saved, copied, downloaded, synchronized or otherwise modified. All infected files are immediately quarantined to protect all other data on the device. The automatic scanning happens transparently on the background.

To work effectively, antivirus software requires an always up-to-date virus definition database. F-Secure Mobile Security retrieves the latest virus definition databases automatically.

1.2 Key features

F-Secure Mobile Security offers the following key features.

Transparent operation The application runs in the background while you use your device.

Extensive scanning The application automatically scans all files when they are accessed. You can also manually scan your device for viruses whenever you want.

Automatic updates The application automatically downloads regular updates to keep the virus definition database up-to-date.

Firewall The application protects you from potential network harm by blocking information that does not meet the set security criteria.

Anti-theft The application protects your confidential infromation by locking the device automatically when the SIM card is changed. You can also send a message to your mobile device to locate it or remotely wipe the data stored on it if it is stolen.

Browsing protection The application protects you from web sites that may steal your personal information, including credit card numbers, user account information, and passwords.

2 INSTALLATION

System requirements..... 9
Getting the product running on your device..... 9
Uninstalling..... 12

2.1 System requirements

To use F-Secure Mobile Security, your device must meet the following requirements:

Platform:	Nokia S60 (3rd or 5th edition) devices. See http://mobile.f-secure.com/devices/ for a full list of supported devices.
Internet connection:	You must have an Internet connection from your device to activate the application.

To test your Internet access point, browse with your device browser to https://msp.f-secure.com/web-test/

If you can access the page, your Internet access point is suitable for activation and updates.

2.2 Getting the product running on your device

Getting your F-Secure Mobile Security running on your device is a two-step process:

1. Install F-Secure Mobile Security. See "*Installation*", *9*.
2. Activate your subscription. See "*Activating the product after the installation*", *11*.

2.2.1 Installation

Select one of the following ways to install F-Secure Mobile Security on your device:

- Install the application directly on the device, or
- Download the installation file to your computer and install the product via Nokia PC Suite.

Installation on the device

1. Download the installation file to your computer and move it to the device or download the installation directly to your device.
2. If you downloaded the installation file directly, the installation starts automatically. Otherwise, find and open the installation file that you moved to the device.
3. When the installation is ready, restart your device if the installation asks you to do so.
4. After the installation, you need to activate the product. The product does not protect your device if you have not activated it.

Installation using your computer

To install F-Secure Mobile Security on your device using a computer, you must have the .sis installation file and Nokia PC Suite installed on your computer.

1. Connect your device to your computer.
2. Double-click the installation file to start the installation.
3. When the installation is ready, restart your device if the installation asks you to do so.
4. After the installation, you need to activate the product. The product does not protect your device if you have not activated it.

2.2.2 Activating the product after the installation

You need to activate the product after you have installed it.

You can activate the product with your subscription code or you can activate Anti-theft only. Activating the product with only the Anti-theft feature active does not require a subscription code, but other features are not available until you upgrade the product.

The activating the product with the subscription code allows you to download the latest updates from the update service.

To start the activation:

1. Open the application. The Welcome screen is displayed.
2. Press **Continue**.
3. Select the activation type:
   - To activate the product with only the Anti-theft feature active, select **Anti-theft only** as the activation type and press **Continue**.
   - If you already have a subscription code, select **Subscription code** as the activation type and press **Continue**. Then enter your subscription code and press **OK**.

     You can purchase a subscription code from the F-Secure estore; http://www.f-secure.com/estore.

4. The activation requires a connection to the update service. Press **Yes** to connect to the update service.The application connects to the update service and activates the product.

   If you used your subscription code to activate the product, the application downloads the latest virus definition database during the first update. For more information, see “*Keeping the application up-to-date*”, *24*.
5. After the product has downloaded all the necessary updates, the application is complete. Press **Continue** to finish the activation.

After you have finished the activation, scan your device for viruses to make sure your device is clean. For instructions, see "*Manual scanning*", *16*. The default firewall level after the installation and activation is *Normal*.

You should scan your device whenever the application asks you to do so.

2.3 Transferring the subscription to a new device

You can transfer your subscription to a new device a maximum of four times. The procedure is the same as for normal installation and activation. For instructions, see "*Getting the product running on your device*", *9*.

2.4 Uninstalling

IMPORTANT: *Scan you device, and remove all quarantined and infected files before you uninstall F-Secure Mobile Security.*

To uninstall the application:

1. Open the application.
2. Select **Options > Exit** shut down the application.
3. Open **Application Manager** on your device.
4. Scroll to F-Secure Mobile Security.
5. Select **Options > Remove**.
6. Press **Yes** to confirm the uninstallation.

3 Using F-Secure Mobile Security

Opening and closing the application 14
Scanning for viruses 15
Using firewall 18
Protecting confidential information 19
Protecting web browsing 22
Keeping the application up-to-date 24
Purchasing subscription service time 26
Troubleshooting 28

3.1 Opening and closing the application

After you have activated F-Secure Mobile Security, it starts up automatically every time you turn on your device. If you have selected the manual scanning mode, you need to start the application manually:

1. Press the **Menu** key and browse to the icon.
2. Select **Options > Open**.

When the real-time scanning mode is enabled, F-Secure Mobile Security runs on the background automatically. For more information, see "Real-time scanning", 15.

Closing the user interface

Press the **Hide** soft key to hide the user interface. When the user interface is hidden, the application keeps running on the background, scanning your files for viruses automatically when they are accessed if the real-time scanning mode is enabled, and the firewall protects the system.

To shut down F-Secure Mobile Security completely, select **Options > Exit**.

***IMPORTANT:** If you shut down the application, infected files are no longer quarantined and the system is not protected against viruses. Shutting down the application disables the firewall.*

3.2 Scanning for viruses

The application scans all accessed and modified data on your device automatically for malicious content when the real-time scanning is enabled. If you do not want to use the real-time scanning, you can manually scan all the data for viruses whenever you want.

3.2.1 Selecting the virus protection mode

1. Browse to **Settings** and press the selection key.
2. Select **Virus protection** from the settings selection list.
3. Select either the real-time or the manual **Virus protection** mode.
   - *Real-time* - F-Secure Mobile Security runs on the background and scan files when they are accessed or modified. For more information, see "*Real-time scanning*", *15*.
   - *Manual* - F-Secure Mobile Security scans files only when you run the virus scan yourself. For more information, see "*Manual scanning*", *16*.
4. Press **Back**.

Real-time scanning

The real-time scan scans files for malicious content automatically when they are accessed or modified and when they are copied to the device.

Virus alerts

When F-Secure Mobile Security detects a virus during a real-time scan, the virus is quarantined and added to the Infections list immediately.

F-Secure Mobile Security alerts you about viruses detected during the real-time scan. You can press **Yes** to view details about the infected file. For more information, see "*Processing infected files*", *17*.

Manual scanning

To scan all files on your device and the inserted memory card, follow these instructions:

1. Browse to **Virus protection** and press the selection key.
2. Select **Scan now**.
3. After the virus scan is finished, the application displays the following information:

Infected	The number of infections found. For more information about removing infected files, see *”Processing infected files”, 17*
Not Scanned	The number of the files that were not scanned during the scan. A file cannot be scanned if another program has locked it or if the file is corrupted.
Scanned	The number of the files that were scanned.

4. Press **Back** to exit the scan. All infected files are quarantined and cannot be accessed when F-Secure Mobile Security is running in the background.

3.2.2 Processing infected files

When F-Secure Mobile Security finds a virus in a file, you can remove the infected file completely or lock it up so that the infected file cannot be accessed.

To process infected files, follow these instructions:

1. Browse to **Virus protection** and press the selection key.
2. Select **Infected files**.
3. In the Infections view, scroll to the infected file you want to process.
4. Press the selection key.
5. Choose one of the following actions:
   - **Delete** - delete the infected file. This is the recommended option. The file will be removed completely from your device.
   - **Quarantine** - quarantine the infected file. A quarantined file is locked and cannot harm your device when F-Secure Mobile Security is on.
   - **Release** - release the quarantined file. If you release a file, it will not be locked any more. You access it at your own risk.

Press **Details** to view more details about the selected file. The Infection details view displays the path and file name of the infected file, and the name of the virus that has infected the file.

You can find in-depth virus descriptions in the F-Secure web site: http://www.f-secure.com/virus-info/.

3.3 Using firewall

The firewall in F-Secure Mobile Security works quietly in the background. It monitors incoming and outgoing Internet and network information, and protects you from intrusion attempts.

By default, the firewall protection level is set to *Normal*. This level gives you good protection and does not affect using the most common applications.

3.3.1 Selecting the protection level

To select the security level:

1. Browse to **Settings** and press the selection key.
2. Select **Firewall** from the settings selection list.
3. Select the desired firewall level.

The firewall has the following protection levels:

Level	Description	Protection
Deny All	Stops all network traffic. You cannot use your e-mail, MMS or web services.	Total protection
High	Allows most commonly used applications.	High protection
Normal	Allows all outgoing connections. Recommended level.	Good protection
Allow All	Allows all network traffic. Does not stop any incoming or outgoing connections.	No protection
Custom	Allows network traffic based on your custom rules.	Customized rule set

*To edit the custom rule set, select **Options > Edit custom rules** when the **Custom** security level is selected.*

3.4 Protecting confidential information

With Anti-theft, you can make sure that your device or data stored on it is not misused if your device is stolen.

Anti-theft can automatically alert you and lock your device when the SIM card in the device is changed, and you can lock or wipe the device remotely with an SMS text message.

3.4.1 Using the device lock

Anti-theft can automatically lock your device when the SIM card in the device is changed. The locked device can be unlocked only with your lock code.

To set up the device lock:

1. Browse to **Settings** and press the selection key.
2. Select **Anti-theft** in the settings selection list.
3. Enter a **Lock code**. The lock code needs to be at least 5 characters long. Store it in a safe place.

   Your lock code protects the Anti-theft settings. You have to enter your current lock code before you can change any Anti-theft settings.

4. If you want to lock your device when a SIM card changes, select **Yes** on **Lock when SIM changed**.

   When someone inserts a new SIM card into the device and the SIM change lock is turned on, the device asks for the lock code before it can be used.

Unlocking the locked device

To unlock the locked device, enter your lock code.

3.4.2 Using the remote Anti-theft

When the remote Anti-theft is turned on, you can send an SMS that contains your lock or wipe code to your device to lock it or to wipe all information in it.

The locked device can be unlocked only with your lock code. If you wipe the device, the application deletes all the information stored in the device memory.

As memory cards can be easily removed, store your confidential information in the device memory that you can lock and wipe with Anti-theft.

To set up remote Anti-theft:

1. Browse to **Settings** and press the selection key.
2. Select **Anti-theft** in the settings selection list.
3. If you want to be able to lock your device remotely, follow these instructions:
   a. Enter a **Lock code** if you have not created it yet.
   b. Turn on **Remote lock**.
4. If you want to be able to wipe your device remotely, follow these instructions:
   a. Enter a **Wipe code**. The wipe code needs to be at least 8 characters long. Store it in a safe place.
   b. Turn on **Remote wipe**.

To lock or wipe your device remotely:

- To lock the device, send the following SMS message to your device:

  #LOCK#<lock code> (For example: #LOCK#abcd1234)

  Locked device can be unlocked only with the system lock password.
- To wipe the device, send the following SMS message to your device:

  #WIPE#<wipe code> (For example: #WIPE#abcd1234)

  When the device is wiped, all data stored on it is removed.

3.4.3 Using the SMS alert

You can set Anti-theft to send you an SMS text message when somebody changes the SIM card in your device.

To use the SMS alert, turn on the **SMS alert when SIM changed** setting and specify the phone number where the SMS text message should be sent when the SIM card in the device is changed.

3.4.4 Locating the lost device

You can send an SMS text message to your lost device to locate it. the **Remote lock** setting has to be turned on if you want to be able to locate your device.

To locate your device, send the following SMS text message to your device:

#LOCATE#<lock code> (For example: #LOCATE#abcd1234)

Anti-theft replies with an SMS text message with the latest location of the device.

3.5 Protecting web browsing

Browsing protection protects you from web sites that may steal your personal information, including credit card numbers, user account information, and passwords.

Browsing protection checks web sites that you browse with the default browser of your device. If you use any third-party browser, Browsing protection does not protect your web browsing.

Turn off the web browser and clear its cache before you start using the browsing protection.

3.5.1 Using Browsing protection

To turn on Browsing protection:

1. Browse to **Settings** and press the selection key.
2. Select **Browsing protection** in the settings selection list.
3. Turn on **Browsing protection**.
4. In **Network to use**, select whether you want to use Browsing protection all the time or only when you are browsing the web on your own operator's network:
   - Select **My operator only** to use Browsing protection only when you are using your own operator's network.
   - Select the **All operators** setting to keep the protection turned on when you are travelling and outside of your own operator's network.

When you try to enter to a web site that contains harmful content, Browsing protection notifies you and blocks the access to the harmful site. Select **Go back** to return to the page where you left.

If you want to enter the site even though Browsing protection blocked it, follow the I want to enter this web site anyway link in the block page.

Privacy mode

Browsing protection can send information of web sites that contain harmful content to the analysis automatically to maintain the quality of service. You can choose which information you want to submit to the analysis.

Privacy statement

Submitting information does not compromise your privacy.

Even though the submitted information may be considered personal under some jurisdictions, your privacy is protected during the process. We transfer the information securely, remove any unnecessary personal information, and process the information anonymously in an aggregate format. In this way, the information cannot be connected to you in any way. No user account information, no IP address information, or no license information is included in the information you submit. We protect your privacy further by using encryption when transferring the information.

The submitted information is used for improving the protection capabilities of our services and products.

To change the privacy mode:

1. Browse to **Settings** and press the selection key.
2. Select **Other settings** in the settings selection list.
3. In Privacy mode, select
   - Select **Statistics only** to submit only browsing protection statistics and the server connection information.
   - Select **Allow all** to submit statistics and information on web sites that have not been analysed or contained harmful content.

*For the best quality of service, we recommend that you keep the privacy mode as **Allow all**.*

3.6 Keeping the application up-to-date

F-Secure Mobile Security includes an automatic update service, which means that the virus definition database in the application is updated regularly. Only an up-to-date virus definition database protects your device against the latest viruses.

The application requires an active Internet connection for the updates. When a connection to the Internet is available, the application checks when the virus definition database was last updated and downloads new updates if necessary.

You can freely update F-Secure Mobile Security as long as you have an active subscription. To keep your device continuously protected, purchase additional service time well before the expiration date.

3.6.1 Selecting the update mode

Automatic updates are in use after you have activated the product. If you disable automatic updates or do not use real-time scanning mode, you need to update the application manually.

To change the update mode, follow these instructions:

1. Browse to **Settings** and press the selection key.
2. Select **Virus protection** from the settings selection list.
3. Select **Enabled** and press **Ok**.
4. Select one of the following **Automatic updates** mode.
   - *Always* - the application downloads regular updates from the update server automatically to keep the virus definition database up-to-date. (recommended)
   - *In home network* – the application downloads updates from the update server automatically when you are using your own operator's network.
   - *Never* – the virus definitions are not updated automatically. We do not recommend that you disable automatic updates.

Manual updates

To update the application manually, follow these instructions:

1. Browse to **Virus protection** and press the selection key.
2. Select **Update now**.
3. The application requires a network connection. Select **Yes** when the connection the update server is needed.
4. Select the Internet access point to connect to the update server. The application downloads the latest virus definition database and takes it into use immediately.

   For more information, see the User Guide of your device.

5. When the update is complete, press **Yes** to scan your device for viruses. For more information on scanning, see “*Manual scanning*”, *16.*

3.6.2 Application updates

When a new F-Secure Mobile Security version is available, a message asks you to download it. The application restarts automatically when the update is completed.

If the virus definition database update requires a software update to work properly, the upgrade is downloaded automatically.

Upgrading the application manually

If you want to upgrade F-Secure Mobile Security, install the new version. For instructions, see “*Getting the product running on your device*”, *9*.

If you have F-Secure Anti-Virus installed on your device and you want to upgrade it to F-Secure Mobile Security, follow these instructions:

1. Write down your current key code. You need it to activate the new version.
2. Uninstall the installed version.

3. Download the new version.
4. Install F-Secure Mobile Security. For more information, see "*Getting the product running on your device*", *9*.
5. Activate the new version with your key code. For instructions, see "*Activating the product after the installation*", *11*.

3.7 Purchasing subscription service time

To keep your device continuously protected, you should purchase additional service time well before the expiration date. The additional service time purchased is either added to the time remaining in your previous order or to your free evaluation period.

F-Secure Mobile Security supports several purchase methods depending on the distribution channel. Most common purchase methods are:

- The operator-specific continuous service subscription
- F-Secure eStore
- Your local reseller
- Openbit SMS payment

If you wish to purchase F-Secure Mobile Security after using the trial version, use the subscription code provided in the *About* view. If you received a new subscription code when you purchased service time or a new license, use it to activate the software. For more information, follow the instructions in the purchase menu.

Using PC

To purchase more service subscription time through your PC browser, follow these instructions:

1. Open http://www.f-secure.com/estore/avmobile.shtml in the web browser with your computer.
2. Enter your subscription code in the *Subscription Code* field to identify your subscription.

F-Secure eStore accepts the most commonly used credit cards and wire/bank transfers.

3. Follow the instructions on the screen.

Using SMS

To purchase more subscription service time by sending an SMS (only if enabled by your operator), follow these instructions:

1. Browse to **Buy** and press the selection key.

   The *Select method* screen is displayed.
2. Select the **Phone bill** payment method.
3. When prompted to accept payment, press **OK** to complete your subscription service time purchase.
4. In the response SMS, you receive a confirmation of your purchase and a code for activating the service.

Buying with credit card

To purchase more subscription service time using the application, follow these instructions:

1. Browse to **Buy** and press the selection key.

   The *Select method* screen is displayed.
2. Select **Buy with credit card**. the length of your new subscription and the billing method.

   If you have a license already, you can activate the service with your license code.
3. The application open the link to the F-Secure eStore. Follow the on-screen instructions to finish the purchase.

3.8 Troubleshooting

The main view of the user interface displays the security overview and the current status.

If the status displays that your device is not protected, follow these instructions:

1. Browse to **Security overview** and press the selection key.
2. Select the item with either red or yellow status icon and press the selection key to solve the issue.

For more troubleshooting instructions and answers to frequently asked questions, see http://mobile.f-secure.com/FAQ/faqs60.html.

Technical Support

Overview..... 26
Virus descriptions on the web..... 26
Electronic mail support 26

Overview

F-Secure Technical Support is available by e-mail and from our Web site. You can access our Web site from within F-Secure Mobile Security or from your Web browser.

For Technical Support of all F-Secure products, go to F-Secure Support Center at: http://support.f-secure.com/enu/home/.

Virus descriptions on the web

F-Secure Corporation maintains a comprehensive collection of virus-related information on its Web site. To view the Virus Information Database, connect to: http://www.F-Secure.com/virus-info/.

Electronic mail support

If you have questions about F-Secure Mobile Security not covered in the manual or online services at http://www.F-Secure.com/, you can contact your local F-Secure distributor or F-Secure Corporation directly.

For technical assistance, please contact your local F-Secure Business Partner. Send your e-mail to: Anti-Virus-<country>@F-Secure.com

Example: Anti-Virus-Norway@F-Secure.com

If there is no authorized F-Secure Mobile Security Business Partner in your country, you can request basic technical assistance from: Anti-Virus-Support@F-Secure.com

When contacting support, prepare and include the following information in your support request:

- Name and version number of your F-Secure software program (including the build number, if available).
- Name and version number of your operating system (including the build number).
- A detailed description of the problem, including any error messages displayed by the program, and any other details, which could help us duplicate the problem.

When contacting F-Secure support by telephone, please do the following so that we may help you more effectively and save time:

- have your device at hand, so you can follow instructions given by the support technician, or be prepared to write down instructions.
- Have your device turned on and (if possible) in the state it was in when the problem occurred.

About F-Secure Corporation

F-Secure Corporation protects consumers and businesses against computer viruses and other online threats from the Internet and mobile networks. We want to be the most reliable provider of internet security services in the market. One way to demonstrate this is the speed of our response.

F-Secure's award-winning solutions for real-time virus protection are available as a service subscription through more than 170 Internet service providers and mobile operator partners around the world, making F-Secure the global leader in the market of internet and computer security. The solutions are also available as licensed products through thousands of resellers globally.

F-Secure aspires to be the most reliable mobile and computer security provider, helping make computer and smartphone users' networked lives safe and easy. This is substantiated by the company's independently proven ability to respond faster to new threats than its main competitors. Founded in 1988 and headquartered in Finland, F-Secure has been listed on the OMX Nordic Exchange Helsinki since 1999. The company has consistently been one of the fastest growing publicly listed companies in the industry.

The latest news on real-time virus threat scenarios is available at the http://www.f-secure.com/weblog/