

Whitepaper:

F-Prot Antivirus SDK

Technology Licensing

Table of Contents

Executive Summary	3
1 Introduction	4
2 F-PROT Antivirus SDK	5
2.1 Components of the F-PROT Antivirus SDK Package	6
3 Award-winning F-PROT Antivirus Scanning Engine	6
3.1 Key Features Of The F-PROT Antivirus Scanning Engine	7
3.2 F-PROt Antivirus Scanning Engine Supported Object Formats	7
3.3 Supported Platforms	7
4 Partnering with FRISK Software	8
Company Background	9

Executive Summary

Add virus detection to your application on any platform, Windows, Solaris, AIX, Linux, BSD and Mac OS X. F-PROT works with any kind of application on most platforms. The award-winning F-PROT Antivirus Scanning Engine protects against viruses, worms, Trojans and other malware. Advanced heuristics detect new and unknown threats and offer the strongest possible defense for desktops and servers.

The F-PROT Antivirus SDK is a professional antivirus software development package that allows the addition of antivirus functionality to nearly any type of application running under Windows, Solaris, AIX, Linux, BSD and Mac OS X on various types of hardware; from an office PC to a multi-processor server.

F-PROT Antivirus SDK includes the F-PROT Antivirus Scanning Engine and F-PROT Antivirus Definition Handler libraries (dynamic or static), detailed technical documentation, program samples and tools to help software developers integrate F-PROT Antivirus into their work. The F-PROT Antivirus Updater protocol documentation is also included as part of the SDK.

For further information on licensing F-PROT Antivirus technology or evaluation of the SDK, complete the application at www.f-prot.com/partners or contact us at oem-info@f-prot.com.

Contact Information

FRISK Software International

Mailing Address:

Thverholt 18

IS-105 Reykjavík

Iceland

Tel: +354-540-7400

Fax: +354-540-7401

www.f-prot.com

oem-info@f-prot.com

1 Introduction

Computer viruses are spreading through the internet at an unprecedented rate, leading to the worldwide antivirus market totaling around US\$ 8.2 billion (USD) in 2006, a 13 percent increase from 2005 revenue.¹

"The motive and intention of virus writers have changed," said Brian Burke,² research manager, Security Products, IDC.

"In the past, worms and viruses were typically created to destroy data by amateurs seeking notoriety. Today, more sophisticated attackers, often organized crime, are increasingly using worms and viruses to obtain credit card numbers, bank account information, and other personal information to perpetrate identity theft. IDC believes this profit-driven motivation will cause the number of attacks to increase in sophistication, frequency, and severity.

As antivirus technologies continue to improve, virus writers have become more inventive in the ways they combat security solutions. The overwhelming majority of new malicious programs use a range of methods to pack their code. This makes it more difficult for virus analysts to analyze these files. Increasingly, encryption is being used to hinder analysis, as is garbage code."

There is an enormous demand for virus protection and IT security solutions. Trying to meet this demand can be costly and time-consuming. FRISK Software offers a simple and cost-effective approach by means of delivering superior antivirus functionality into their products.

F-PROT Antivirus technology has been proven reliable and efficient by thousands of companies around the world who have successfully employed it, as well as by certificates and technology awards. At present, the F-PROT Antivirus Scanning Engine detects well over a eight hundred thousand³ viruses, worms, Trojan horses and other malware.

This document provides an overview of F-PROT Antivirus SDK technology licensing, the benefits of the solution and of partnering with FRISK Software.

1 Gartner, Inc.

2 Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc. Source: IDC study, published 27 Sep 2005

3 September 2007

2 F-PROT Antivirus SDK

The F-PROT Antivirus SDK provides software developers and service providers with the ability to design and implement antivirus solutions in nearly any type of application running under Windows, Solaris, AIX, Linux, BSD and Mac OS X on various types of hardware; from a 32 bit to 64 bit operating systems. F-PROT Antivirus SDK is also fully re-entrant in preparation for the age of multi-threading and parallel programming.

The F-PROT Antivirus SDK has three major parts:

- **F-PROT Antivirus Scanning Engine (FPAVENG)** is the core that provides extensive scanning and disinfection capabilities and consists of a number of mini-engines that handle different types of objects (Win32, OLE, Scripts, LE, NE, PE, ELF and more) making the scanning engine itself highly flexible. The scanning engine provides signature-based malware detection, heuristics detection, emulation and more.

The FPAVENG interacts with the vendor's application using either dynamic or static libraries.

- **F-PROT Antivirus Definition Handler (FPAVDEF)** provides access to the virus definition file, called *antivir.def*, which contains the binary patterns of malware definitions and disinfection information.

The vendor's application interacts with the definition handler to load the *antivir.def* and then passes the handle to the scanning engine when it scans a file. The scanning engine will then use the handle from the definition handler to access its information.

The FPAVDEF allows the differential updates of the *antivir.def* to decrease traffic load on the download servers.

- **F-PROT Antivirus Updater protocol.** The SDK includes a description of a protocol rather than a software API. This Updater protocol provides the necessary information to implement communication between the *F-PROT DirectUpdates Servers* and the download of the *antivir.def*. Simple examples are included in the documentation.

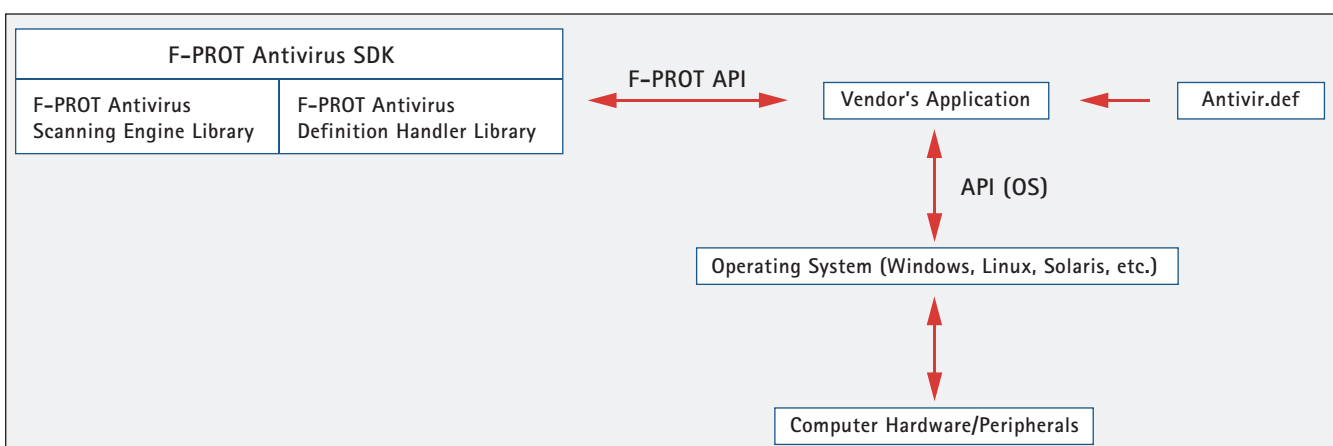


Figure 1: Graphical representation of the F-PROT Antivirus SDK.

2.1 Components of the F-PROT Antivirus SDK

The F-PROT Antivirus SDK development includes:

- **A set of C libraries** (static or dynamic): F-PROT Antivirus Scanning Engine (FPAVENG) and F-PROT Antivirus Definition Handler (FPAVDEF).
- **In-depth technical documentation** of the provided structures, function prototypes and constants.
- **The programmer's guide**, which contains detailed information for programmers on how to write an application using the F-PROT Antivirus SDK.
- A number of **sample programs in C**.
- Fully featured **F-PROT Antivirus Command-Line Scanner** for testing purposes including the complete, commented source code.
- **F-PROT Antivirus Updater protocol** is also included with the SDK. The Updater itself is rather the description of a protocol than an API provided by the SDK.

A more detailed technical document is accessible on the company website and the API documentation is available upon request. For further information on licensing F-PROT Antivirus technology or evaluation of the SDK, complete the application at www.f-prot.com/partners or contact us at oem-info@f-prot.com.

3 F-PROT Antivirus Scanning Engine

The heart of F-PROT is the F-PROT Antivirus Scanning Engine. The renowned scanning engine, originally developed in 1989, was one of the first fully functional, effective antivirus solutions invented. In 1991 the engine featured the world's first heuristic behavior scanner – a standard in the industry today. The scanning engine has delivered the most innovative antivirus technology available at each time, protecting thousands of servers and end-user workstations against viruses, worms, Trojan horses and other malware.

The reliability and effectiveness of the technology is made possible by its signature-based malware detection, heuristic rules and emulation algorithms and up-to-date virus signature files. Updates are released on a regular basis; often released several times a day during times of crisis. The scanning engine has undergone extensive redevelopment to deliver an even more robust and powerful antivirus technology and to cope with a rapidly escalating malware climate.

In independent comparative testing (VB100) carried out over the past years by Virus Bulletin, the antivirus industry's most respected journal, the F-PROT Antivirus Scanning Engine has repeatedly demonstrated a 100% detection rate of the magazine's collection of all "In the Wild" viruses as well as generating zero false positives. For further information on the F-PROT Antivirus certificates and technology awards, see <http://www.f-prot.com/company/>.

3.1 Key Features of the F-PROT Antivirus Scanning Engine

- Advanced heuristic technology defends against new and unknown threats
- Low resource consumption and small memory footprint
- Disinfection of malware
- High detection rates and low false positive rates
- Excellent scanning speed
- Scans an extensive array of formats
- Customizable scanning level and heuristic level
- Broad range of supported platforms including 32 & 64 bit

3.2 F-PROT Antivirus Scanning Engine Supported Object Formats

The F-PROT Antivirus Scanning Engine scans into archives through multiple layers of varying compression types. It processes the supported formats with detailed algorithms. Below is a partial list of widely used object formats that are currently supported by the scanning engine:

Archive Formats:⁴ ZIP, ARJ, CAB, RAR, TAR, GZ, ACE, BZ2, HQX and more.

Mail Formats:⁵ TNEF, MIME, BASE64 and more.

Executable Formats: COM, EXE, BOOT, MBR, SYS, WIN_PE32, WIN_NE16, OS/2_LX, OS/2_LE, ELF, WinCE, Win64, SIS and more.

Documents and Images Formats: CHM, WPD, OLE, WORD2, HLP, WKS, RTF, TEXT, JPG, WORD6, EMF, UNICODE, UNICODEB, PNG, XML, WMF and more.

All Other Formats: MACBIN, MACRSRC, MACHYPER, MACPEF, LINEAR, UNICODE4, UNICODE4B, 8BY2, 8BY3, EBCDIC, RIFF, AIF, REG, XOR, DOOM, APP, DUMP and more.

The list is continuously updated to add new or dangerous formats and extensions. All other currently unsupported file and media formats can be scanned as plain binary files in order to find known and unknown viruses.

3.3 Supported Platforms

All supported platforms have the same F-PROT Antivirus Scanning Engine inside.

- NetBSD on x86, 32 bit
- FreeBSD on x86, 32 bit
- OpenBSD on x86, 32 bit
- Mac OS X on PPC, 32 bit
- Linux on PPC, 32 & 64 bit
- Linux on MIPS, 32 bit
- Solaris on SPARC, 32 bit
- Solaris on x86, 32 & 64 bit
- AIX on PPC, 32 & 64 bit
- Windows on x86, 32 & 64 bit
- Linux on x86, 32 & 64 bit

4,5 Infection is prevented but disinfection is not currently supported.

Contact us for other available platforms at oem-info@f-prot.com.

4 Partnering with FRISK Software

Antivirus solutions grow more and more sophisticated in response to an explosion in online threats and the escalating complexity of current malware. The sheer magnitude of dealing with the intricacies of viruses, trojans and other malware make it difficult for vendors to add antivirus scanning in new or existing solutions, or to offer their own antivirus software.

In order to offer a solution that is state-of-the-art, reliable and of high quality, as well as cost effective, you should integrate antivirus software that has proven capabilities and is driven by some of the foremost experts in the field.

FRISK Software offers a software development kit (SDK) with unusually extensive platform support, virus detection coverage, heuristics technology and ease of integration.

Key benefits of choosing F-PROT Antivirus SDK:

- Award-winning F-PROT Antivirus Scanning Engine
- Faster Time-to-Market
- Simplifies the development process of designing and implementing an antivirus solution
- Increases the competitive edge of your solution.
- Provides customers with unmatched security against new attacks, based on proven technology and security expertise.
- Speedy and effective virus outbreak response
- Differential virus definition file updates
- Tested, multi-product support
- Excellent technical support from our expert development team.

In this paper, we have outlined what F-PROT Antivirus SDK offers and why it makes a smart choice for gateway vendors. Even with some of the most specialized solutions, the F-PROT Antivirus SDK has the flexibility to deal with scenarios and product designs where many other virus scanning engines fail.

The F-PROT Antivirus SDK is licensed with competitive pricing and on terms, flexible enough to suit the varied needs of modern day software companies and solution providers.

For further information on F-PROT Antivirus technology licensing, contact us at oem-info@f-prot.com.

Company Background

FRISK Software International is one of the world's leading companies in antivirus research and product development. For 18 years, FRISK Software has achieved success by delivering the most innovative antivirus technology available. Today, thousands of servers as well as end-user workstations rely on the company in the fight against viruses, worms, Trojan horses and other malware.

FRISK Software offers a full collection of antivirus solutions and an extensive array of platforms on various types of hardware, protecting computer networks of all sizes. As a result, FRISK Software provides its customers, from OEM partners to business and home users, with comprehensive computer security solutions to suit.

FRISK Software is largely privately owned, with some employee shareholders. FRISK Software is headquartered in Reykjavik, Iceland and has a regional office in the United States and developers in other countries as well as a partner network around the globe.

The FRISK name and logo, the F-PROT name and logo and their respective symbols are trademarks of FRISK Software. Other company and product names may be registered trademarks of their respective owners. Copyright © 2008 FRISK Software International. WP-SDK-230408