



Cleaning Up The Mess
Time To Redefine 'Disinfection'?

Gergely Erdélyi

Gergely.Erdelyi@F-Secure.com

F-SECURE

The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a large, dark purple inverted triangle with a white outline, and a smaller, light purple inverted triangle nested within it, also with a white outline. The background of the slide is a faint, stylized globe with a grid of latitude and longitude lines, rendered in shades of blue, green, and yellow.

F-SECURE[®]

Introduction

- What is 'disinfection'?
- What is 'removal'?
- Why to disinfect?
- What makes a disinfection complex?

Dis is one half.
Press any key to continue...

The F-Secure logo consists of the text "F-SECURE" in a bold, black, sans-serif font, with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo featuring a large, black-outlined letter 'F' that is partially filled with a purple-to-blue gradient. The logo is set against a circular background with a grid pattern, resembling a globe.

F-SECURE®

One_Half

- One_Half is a polymorphic DOS virus from 1994
- Infects COM, EXE files and MBR
- Contains memory resident stealth routines
- **Encrypts two cylinders of the hard drive everytime the computer starts**
- The encrypted data is decrypted on-the-fly
- Disinfection of One_Half needs a special tool or a full backup of the hard drive

The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside.

Affected system areas today - File System

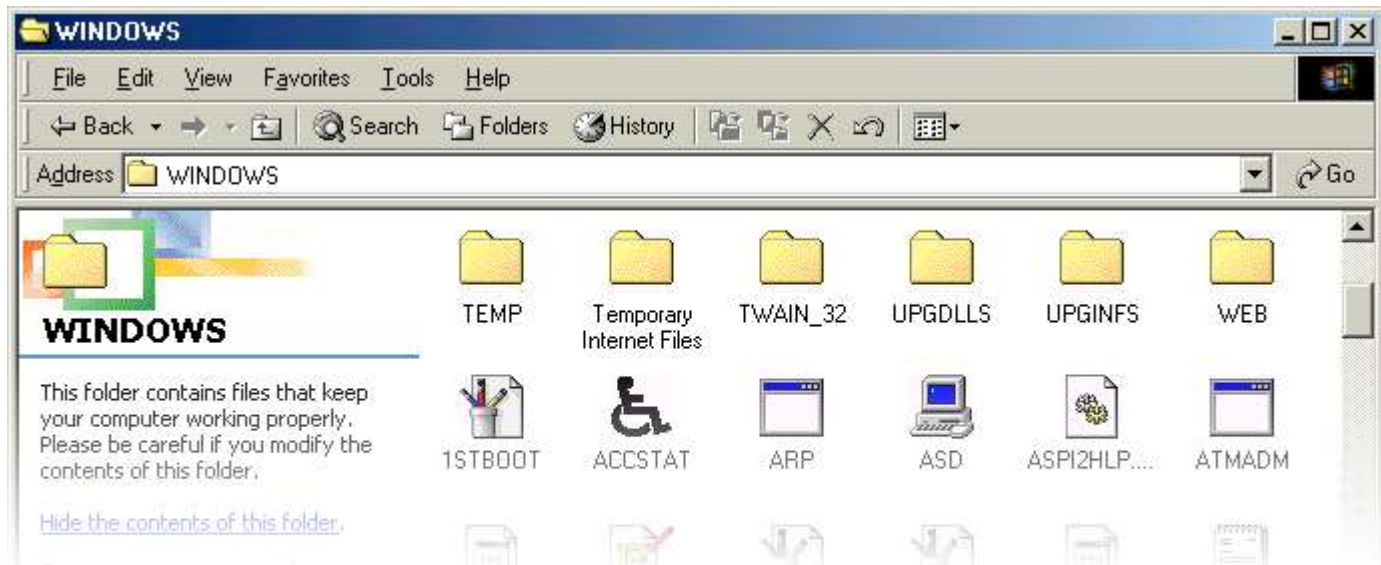
- Infection of program files
- Stand-alone infection
- Companion infection
- Most often affected directories :
 - Windows Directory
 - Windows System Directory
 - Recycle Bin Directory
 - Temp Directory
 - User's StartUp Directory

F-SECURE®



Affected system areas today - File System

- Low level filesystem modifications are rare
- Other features used by viruses: streams
- Example stream name: 'FILENAME.EXT:STR'

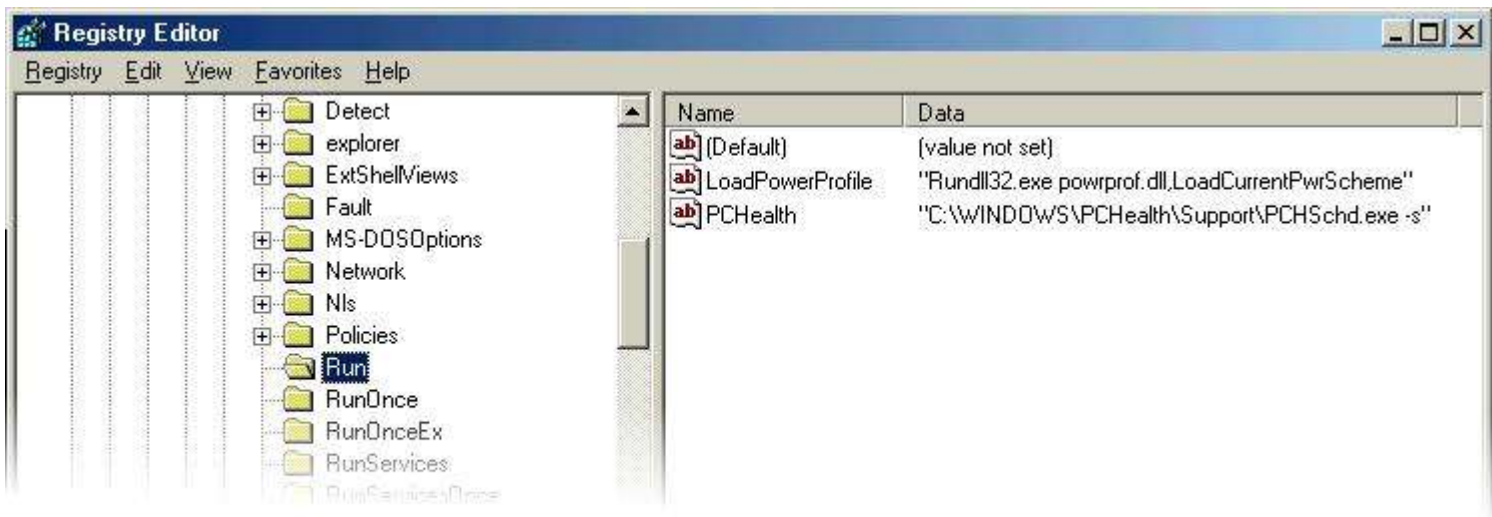


F-SECURE®



Registry

- Registry is used in all modern Windows versions
- Most of the configuration data is stored there
- Modifications to the Registry can seriously affect the system's behavior



The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a large, dark blue triangle pointing downwards, with a smaller, lighter blue triangle nested inside it, and a black outline around the entire shape. The background of the slide is a faint, stylized globe with a grid of latitude and longitude lines, rendered in shades of blue and yellow.

F-SECURE[®]

Repairing the registry

- Registry file format is undocumented
- File-level modification of Registry is risky
- WIN32 API provides full access to the Registry
- Access to certain Registry branches might be tricky

The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside.

Configuration files

- Autoexec.bat
- Config.sys
- Win.ini
- System.ini
- Application specific config files (e.g: mIRC)

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a large, downward-pointing triangle with a smaller, upward-pointing triangle inside it, creating a central square-like shape. The logo is rendered in shades of purple and black.

F-SECURE®

Processes

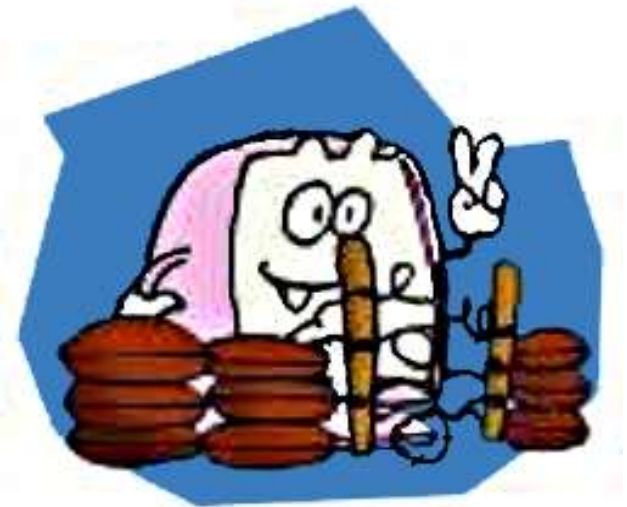
- The “Running malware” problem
- Locked files can not be deleted/modified
- Services are invisible from the standard tools
- Malware can attach itself to other processes
(e.g: Explorer.exe)

F-SECURE®



Security configuration

- File and directory access rights
- Network sharing
- Server settings:
 - Internet Information Server



F-SECURE®



Restoring the security settings

- Sensible default values must be set
- User interaction is needed if it's not possible to set the defaults automatically



F-SECURE®

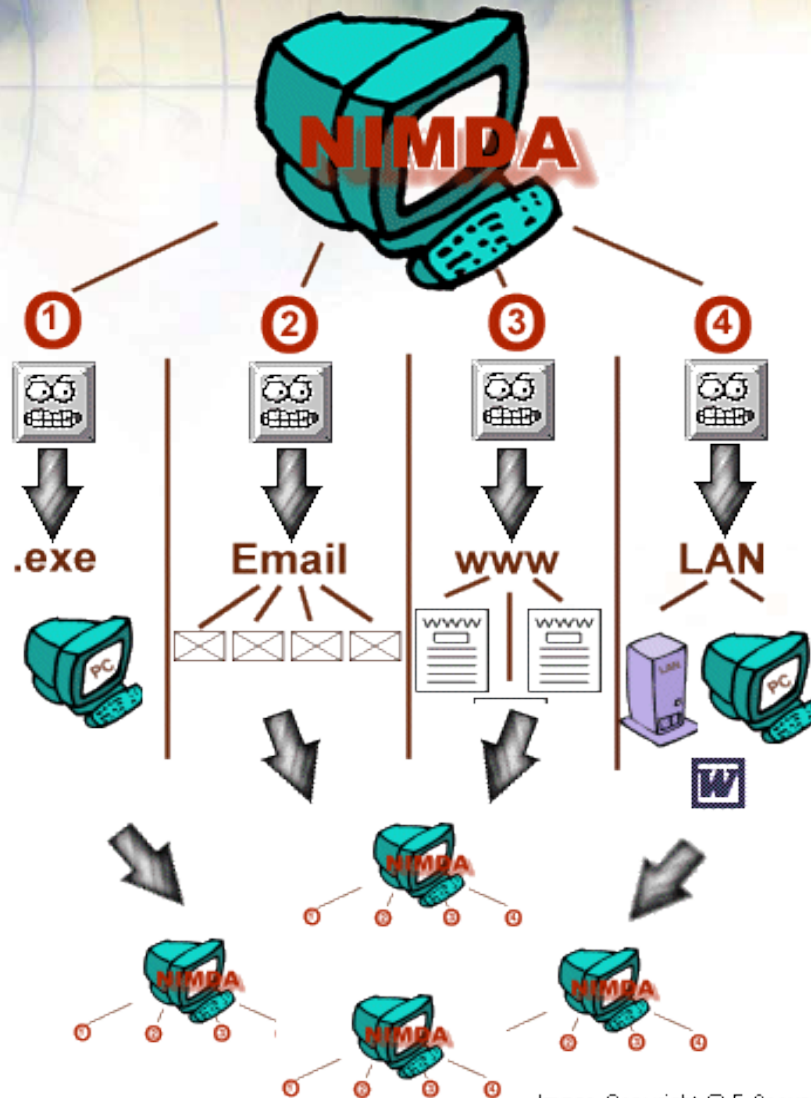


Image Copyright © F-Secure

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside.

Nimda disinfection steps

- Terminate all the worm processes
- Remove Nimda from all the infected files
- Remove all the droppers (.EML, .NWS files)
- Clean up the infected HTML files
- Fix 'shell=' variable in *system.ini*
- Fix registry entries for Windows Explorer:
 - Hidden
 - ShowSuperHidden
 - HideFileExt

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside.

Nimda disinfection steps continued

- Deactivate the guest account
- Remove guest user from the admin group
- Remove all the open shares from the computer
- Restore the overwritten RICHED20.DLL
- Apply the required security patches

F-SECURE®



Cleaning up the mess - Stand-alone tools

- Frequently used solution today
- These tools can target either one or more specific malware
- They are mostly written using low-level languages and tools (C, C++, etc.)



The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside.

Cleaning up the mess - Stand-alone tools

- Small size, easy to distribute through the Internet
- Not only existing customers can use them
- It is hard to maintain the small tools in long term
- Complex functionality might be hard to add

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a large, dark blue triangle pointing downwards, with a smaller, lighter blue triangle inside it, and a black outline.

Cleaning up the mess - Built-in tools

- Built-in to the antivirus product
- Can be distributed through the regular definition database updates
- These tools have access to the complex functionality of the antivirus (e.g: scan engines)
- Built-in tools require the antivirus application
- Viruses that attack the antivirus are hard to remove with built-in tools

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, purple and black shield-like emblem with a white 'F' shape inside.

Built-in tools - Executable code

- Such tool can be DLL or EXE file
- Familiar tools (C, C++) can be used to develop them
- Executable modules written in C, C++ can be fast
- Complex functionality is time consuming to implement with lower-level tools
- A programming error might have serious consequences (e.g.: application crash)

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to the upper right. Below the text is a stylized, purple and black shield-like graphic with a white 'F' shape inside.

Built-in tools - Script based approach

- The special disinfection routines are implemented in some script language
- The runtime for the language is shipped with the antivirus application
- Script languages tend to be more intuitive and less error prone than low-level languages
- Script files are small and easy to distribute
- Hard to update the runtime when needed

The logo for F-SECURE, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric logo consisting of a large, dark blue triangle pointing downwards, with a smaller, lighter blue triangle nested inside it, creating a sense of depth and movement.

F-SECURE®

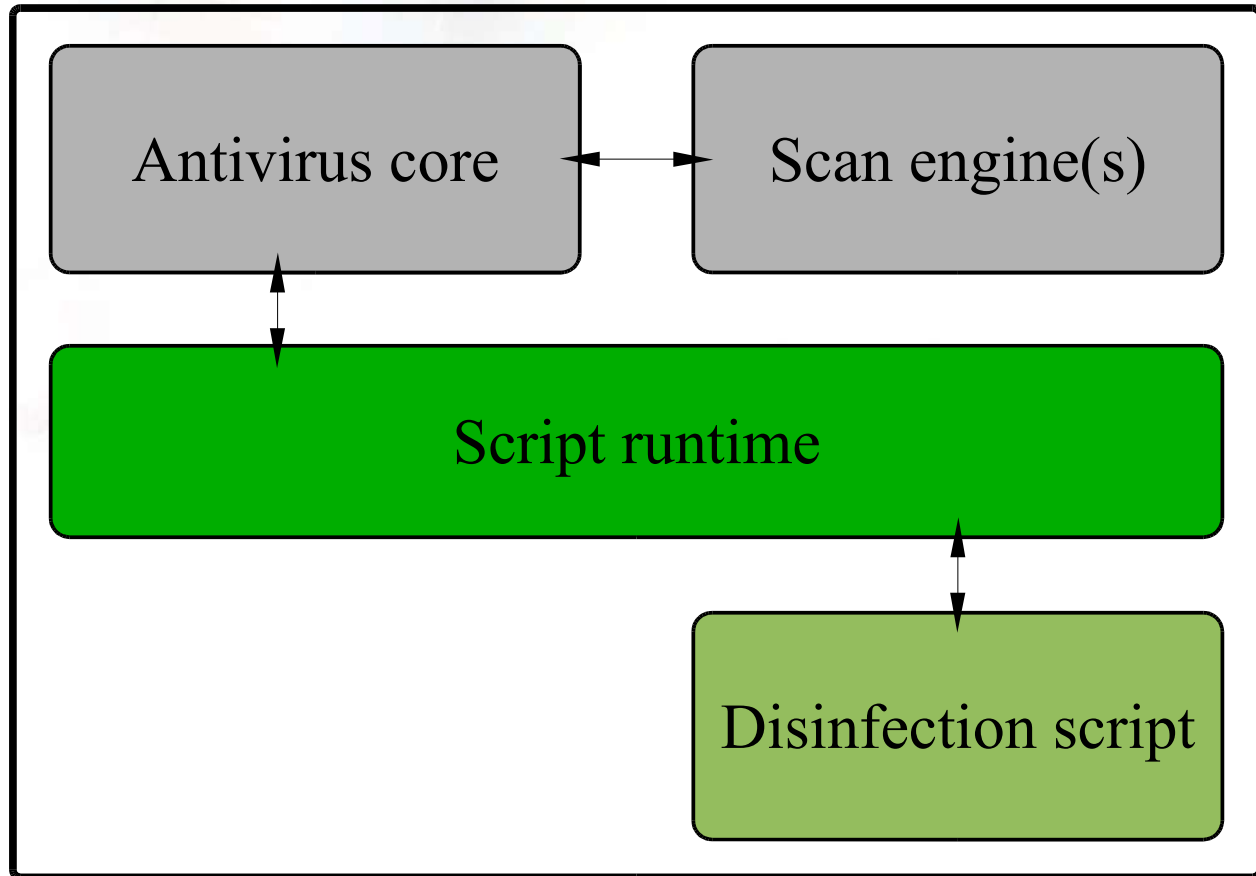
Built-in tools - Hybrid solution

- The script runtime environment is shipped with the antivirus
- The runtime does not need updates frequently
- A small executable extension module provides the needed functionality not supported by the runtime
- The extension module is distributed with the scripts

F-SECURE®



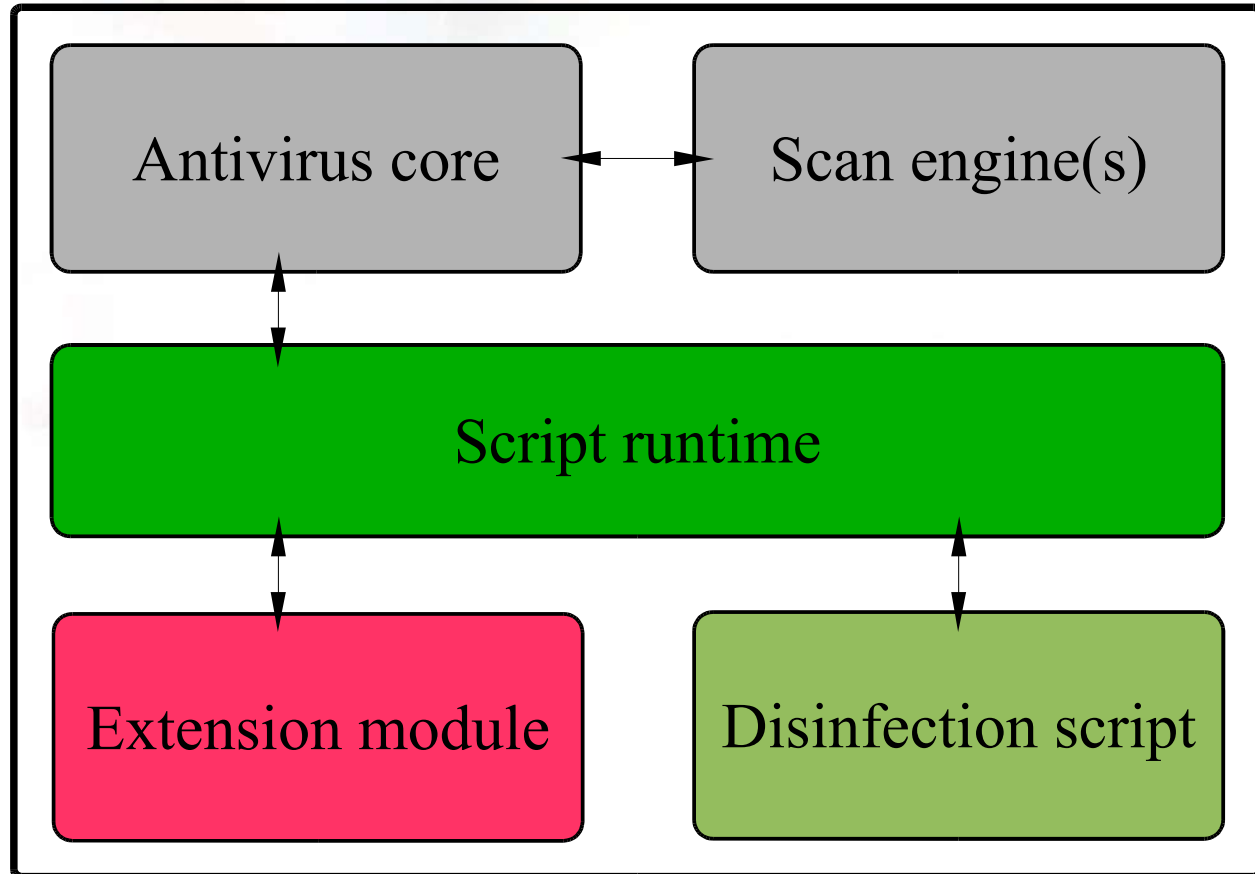
Script solution - Block diagram



F-SECURE®



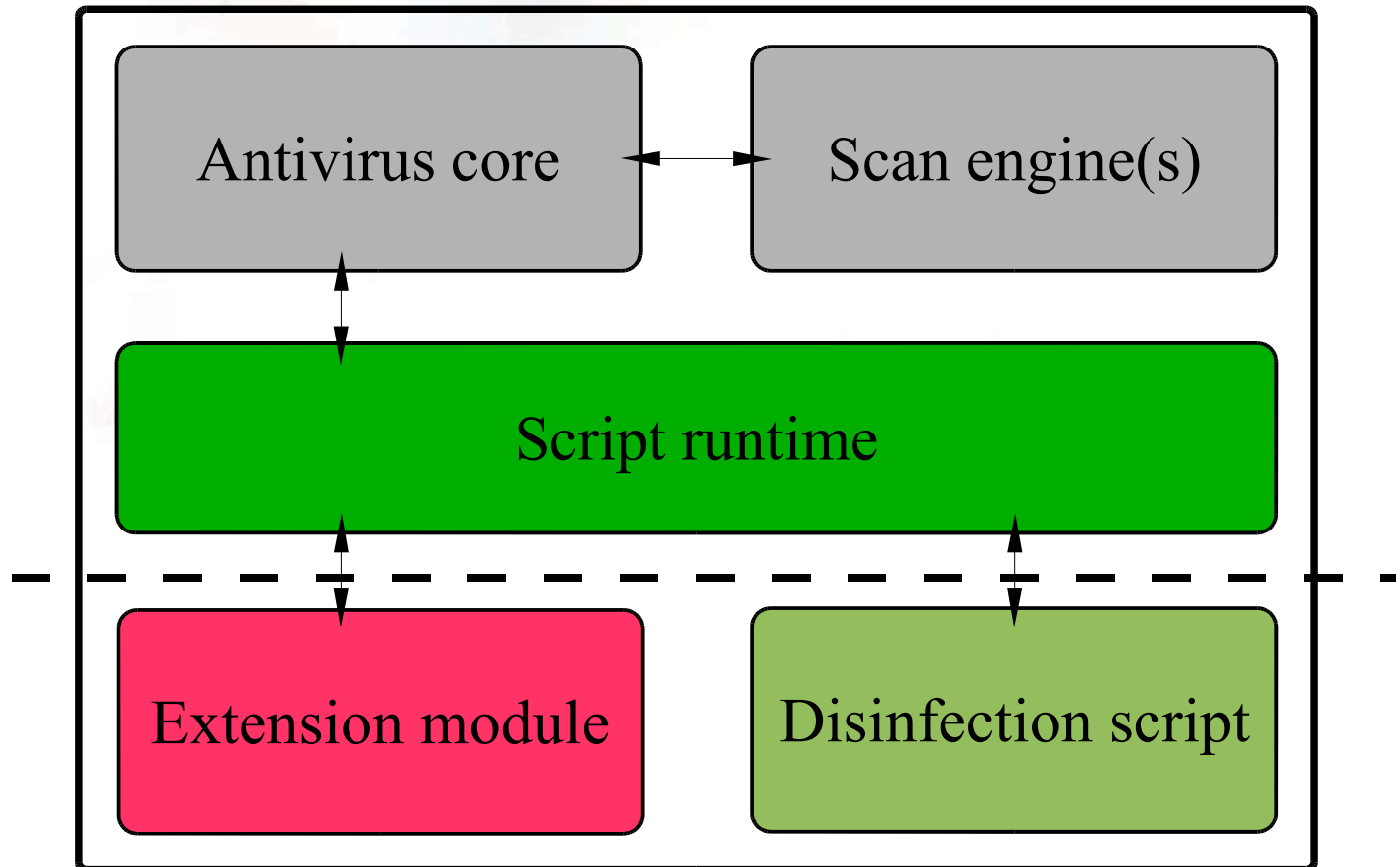
Hybrid solution - Block diagram



F-SECURE®



Hybrid solution - Block diagram



F-SECURE®



Security considerations

- These tools must be tamperproof
- Malicious users might exploit a weakness in the tool to elevate their privileges
- Secure methods, checksums, cryptographic hashes must be used to ensure that the components are intact



F-SECURE®



What do such tools give us?

- Better response time in the case of a virus outbreak
- Reduced support load
- Higher level of customer satisfaction



The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol (®) to its upper right. Below the text is a stylized, geometric shield-like symbol composed of overlapping purple and black shapes.

F-SECURE®



Is it time to redefine 'disinfection'?

F-SECURE[®]



Q & A