F-Secure Internet Security 2014
Data Transfer Declaration

The product's impact on privacy and bandwidth usage

F-Secure Corporation
April 15th 2014

Table of Contents

Version history

15.4.2014	Document created, MA

Abstract

The security of a computer depends on the whole system, including any software products installed on it. Owners of computer systems should evaluate all installed software components to ensure the security of the system and the privacy of the user. The objective of this declaration is to assist system owners in this work and provide information about how the covered product from F-Secure Corporation affects system security, user privacy and bandwidth consumption. It documents what data the product can transfer from the device to backend systems and how much bandwidth the product consumes.

F-Secure Corporation respects the customers' privacy and this is a top priority in product design and development. The product does not transmit any data identifying the user[1] and minimizes the transfer of technical data. Technical data is only collected to the extent needed to provide the protection service efficiently and to plan future development and maintenance of the product. F-Secure Corporation's backend systems are designed to separate different data streams originating from the client so that security analytics would be separate from the customer relationship management information as much as feasibly.

Subject of the declaration

This declaration describes F-Secure Internet Security 2014 for Windows. The core anti-malware technology is shared among F-Secure Corporation's products for the Windows platform, and this declaration should be fairly accurate for other Windows-products as well, even if some differences may occur.[2]

Disclaimers

- The purpose of this document is to help customers evaluate the product's usage of network services and its impact on privacy and bandwidth consumption. This is not an official legally binding statement behalf F-Secure Corporation. Our official privacy policies can be found at the company website.
- F-Secure Corporation has made its best effort to ensure the accuracy of this document. If you find any deviations between reality and this document, they are unintentional and will be rectified.
- The scope of this document is limited to the described product. Other products, services, management tools and portals provided by F-Secure Corporation collect and transfer other / additional information about the device and/or customer.

Privacy design principles

Customer privacy is a top priority in F-Secure Corporation's product development. The described product has been designed and developed with these principles in mind.

[1] The product transfers information needed to identify the license, and this may be linkable to the customers contact details in F-Secure Corporation's backend systems, depending on the used purchase channel. Information about the user operating the computer is not transferred.
[2] Note that corporate products may redirect part of the communication described here to a management server in the customer's network.

- **Minimize upstream of technical data**. Data about the customer's computer is not transferred and collected unless the data is essential for providing the protection service or for planning and prioritizing development and maintenance work.
- **Do not upstream personal data**. The product is designed to not send any information that can identify the person using the computer.[3]
- **Prevent backend data consolidation**. The product uses three different unique IDs for different connections with the F-Secure backend systems. This prevents F-Secure from consolidating data in the backend by comparing user IDs from different systems.
- **Do not store IP-addresses**. The customer's IP-address is never stored. A city-level geo-mapping may be done and the result stored, if it is beneficial for providing the service.
- **Do not trust the network**. All sensitive network transfers are encrypted using strong crypto. Asymmetric encryption is used for authentication when appropriate.
- **Business model not relying on customer data**. The product's business model is traditional license or subscription sales, not ad-based.
- **Ensure the product's own security**. Great care is taken to harden the product and ensure that it won't contain vulnerabilities. Such vulnerabilities could be exploited by malicious software and violate the customer's security and privacy. The hardening applies to both code developed by F-Secure Corporation and modules licensed from external sources.

Upstream data

Mandatory customer-specific upstream data

This section lists data that can identify the customer. This data is sent automatically and there is no possibility to opt out.

Item	Purpose	Notes
Product license key	To ensure validity of license	F-Secure Corporation may be able to link this information to information identifying the customer, depending on the channel used to purchase the product
Unique computer ID for licensing	To identify different computers linked to the same license	

Mandatory anonymous upstream data

This section lists upstream data that is anonymous, i.e. F-Secure Corporation can't tell which customer the data came from. This data is sent automatically and there is no possibility to opt out.

Item	Purpose	Notes
F-Secure product version	To provide appropriate updates. For statistical purposes.	
Installed update packages	To provide appropriate updates	
Function and settings statistics		Covers only settings and functions in the F-Secure product

[3] Note that the product reveals its license identity to the backend system for license control purposes. This info may be linkable to the customer's name and contact information, depending on the used purchase channel. No information about the person using the computer is sent.

Operating system version, including service pack level	For statistical purposes, to develop the product's feature set and prioritize maintenance	
Operating system language		
Amount of RAM memory		
32 or 64 bit architecture		
Unique computer ID for statistical data	Needed to manage consecutive statistics reports from the same device.	This ID is separate from other unique IDs and can't be linked to them.
Computer name	To enable the user to distinguish between managed computers in remote management consoles	Not used in all installation scenarios
Hashes of executable files	Used by the file reputation service to determine if the file is safe or not	
Unique computer ID for reputation services	To manage repetitive connections from the same computer. To calculate number of users, verify reliability of the upstream data and remove duplicate and bogus data.	Only kept in backend short-term, never stored long-term in reputation databases. This ID is separate from other unique IDs and can't be linked to them.
Reputation service statistical data	To monitor and improve the performance of the reputation service.	Contains data like bytes received and transmitted, number of queries and response latency.
Public IP address	Required by the network	Never stored, but is used for city-level geo lookup in the reputation services. The geo-lookup result is stored in the database.

Optional anonymous upstream data

This section lists data that can be sent upstream automatically depending on the product configuration. The user/customer can prevent this data from being sent by altering settings or disabling product modules. This data is fully anonymous and can't be linked to the customer.

Item	Purpose	Notes
Metadata about executable files	To enable further analysis of unknown suspicious files	This data may be requested by the backend system. Contains file header information like file version, file origin (including download URL), file signature information and other similar data.
Hash of visited URL or URLs embedded in web pages	Used by the URL reputation service to determine if the URL is safe and suitable for minors.	Only if Browsing Protection or Banking Protection is enabled
The actual URL visited and referrers to URLs	To enable further analysis of suspicious URLs	Only if Browsing Protection or Banking Protection is enabled. This data may be requested by the backend system. Any private info, like parameters, are typically

		stripped from the URL.[4] URLs in private networks are never sent.
Crash reports	To assist maintenance work and bug fixing	The product may send crash reports after failures in the product's own modules. These reports do not contain any memory dumps that could contain user data.
Search parameters	To improve privacy by providing an alternative search provider	Only sent if the F-Secure Search provider is activated. Search parameters are revealed to F-Secure but never stored. The query contains no info about the user or customer. The parameters are passed on to Google, but the service ensures privacy by filtering out cookies.
Hashes of data in mail messages	To provide spam protection	The spam scanning engine may send hashes of selected message properties from both the header and content of received mail messages.
Malware scanning statistics	Used to analyze and develop the malware scanning system	Statistical data of the usage of the product and status information like number of scanned files, number of found infections, average scan times of the files, list of hashes of the files that are slow to scan etc.

Manually sent anonymous upstream data

This section lists items that the user can select to send case by case. Every transfer is separately approved by the user. This data is anonymous and can't be linked to the customer.

Item	Purpose	Notes
Unknown suspicious executable files	To enable analysis of suspected malware detected with heuristic methods	Only if the user selects to submit the file. This option is offered by the suspicious file warning dialog.

Data normalization

Some technical data that is needed by F-Secure Corporation's backend may contain user data. All such data is passed through a normalization process on the client before it is sent. There are two types of normalization.

[4] The product may in some cases send URL parameters on request from the backend if it is suspected that malware distribution depends on the used parameters.

File path normalization

Paths to user folders may contain the user's name. These paths are normalized by substituting parts of the path with system variable names. This both improves privacy and makes analysis easier.

Example: "C:\users\john\test.exe" -> "%user%\test.exe"

URL normalization

Parameters are stripped from URLs before sending them. The backend system may however request the URL with parameters if there is reason to believe that malware distribution depends on the used parameters.

Bandwidth usage

This section lists the bandwidth usage of the different services. The Typical-value describes a normal situation where the computer is used in a typical manner. The Peak-values describe conditions with higher bandwidth usage that can occur fairly frequently. These figures are not theoretical maximum values, the transferred data amount may exceed these figures in extreme situations.

Large product updates typically occur 1 – 2 times per year. Smaller patches and module updates occur more frequently, but are insignificant compared to the total bandwidth usage.

Definition database updates occur constantly when the computer is on. The number and size of the definition update packages vary depending on the malware situation. Having computers turned off for longer periods will cause a load peak when the computer is turned on and needs to catch up.

The bandwidth used by reputation services is hard to estimate as it is driven by user activity. The figures below try to provide a typical range for light to heavy use. Your actual figures may be outside of this range. Especially use of web pages with embedded content (such as ads) will raise this load. This is caused by the fact that URL reputation is volatile and can't be cached for long periods. Reputation service data is sent encrypted and caching proxies can't be used to reduce the load.

Transfer type	Typical downstream	Typical upstream	Peak downstream	Peak upstream
Product or module version upgrades	0 MB / week	Insignificant	80 MB / week	Insignificant
Definition database updates	7 MB / week	Insignificant	15 MB / week	Insignificant
Reputation services	1 MB / week	0,7 MB / week	3 MB / week	2 MB / week