Independent Tests of Anti-Virus Software

Data transmission of consumer security products

TEST PERIOD: AUGUST 2022 – JULY 2023

LAST REVISION: 31ST JULY 2023

IN COOPERATION WITH: PC MAGAZIN, PCGO, CONNECT-LIVING.DE, ET AL.

WWW.AV-COMPARATIVES.ORG

Contents

Management Summary

Many Internet users are concerned about who has access to their personal information and what is done with it. Computer security software has legitimate grounds for sending its makers some information about the system it's running on; in particular, details of malware found on the machine must be sent to the manufacturer to protect the user effectively. However, this does not mean that a program should have carte blanche to send all personal information found on a computer to the manufacturer (other than with the specific knowledge and agreement of the system's owner).

This report analysed the data collection and data sharing practices of 20 market-leading consumer Anti-Virus (AV) products. Each vendor was scored based on their data collection; data sharing; accessibility; control of software and processes; and openness. The scoring system is meant to provide a general overview based on qualitative evaluation and some vendors that failed to respond received lower scores. The report aims to encourage user awareness about data-sharing practices and transparency.

How vendors performed

The scores range from one (lowest) to five (highest). Higher scores indicate better practices. The vendors with the highest scores are **Bitdefender, ESET, F-Secure, G Data, K7, Kaspersky**, and **VIPRE**. Those of these achieved a score of four stars or more. The vendors with the lowest scores are Malwarebytes, TotalAV, Total Defense, Sophos, Norton, and Microsoft. McAfee and Trend Micro received mixed scores.

Data sending can be an important factor when deciding which security solution best matches your needs. This report highlights the importance of user privacy, options for users to consent to the transfer of certain personal data, the trust required between users and vendors as well as the transparency of the vendors.

Introduction

Over the past time, we got a lot of requests to analyse the transparency and data-sending in IT security products. The products and criteria featured in this report was selected in collaboration with magazines, editors, readers and other stakeholders.

In the course of preparing this report, we reached out to various vendors to obtain their insights on their consumer security solutions. While many provided input, it is significant to note that some few vendors opted not to respond or faced challenges in addressing the inquiries posed. This highlights the sensitivity of the topic, given the varied reactions it evoked.

In the past year, there have been a lot of concerns about data security and privacy risks raised in general, but in special against companies in the IT security market. Even the BSI (German Federal Office for Information Security) issued a warning against the use of Kaspersky (which was later revealed that it might have been politically motivated[1]), countries banning the use of TikTok on government devices, or the recent congressional hearing of Shou Chew, the CEO of TikTok[2].

Frequently cited concerns are the potential for an update to suddenly turn an app into a spying tool or that social media algorithms could be hijacked for misinformation or social engineering campaigns. While these scenarios are theoretically possible, it is important to remember that this is possible with software from any company. It is also important to compare the differences in thread scenarios encountered by government employees vs. private individuals. For example, soldiers using fitness trackers might expose military bases, which could be a security risk, but this is not a concern for individuals[3].

There is also a precedent for US government agencies to spy on foreign citizens and to work closely with US-based companies, which must share user data when doing so[4]. Some would even argue that the distrust of Kaspersky is the desired outcome, due to Kaspersky's history of uncovering government malware[5]. With the continued espionage, this raises the question of why the reporting on this topic is so one-sided.

Like any other company, antivirus manufacturers must comply with local and international data protection laws, along with the laws of the country/countries in which they are selling the product. These laws govern data handling and give a legal framework for what companies may do with user data. However, in the end, there is always a degree of trust required when handing over data to a company, as the final discretion is up to the receiver and their data handling policies. Therefore, users should always be wary of what data they provide to companies and what information might be collected from user behaviour or metadata.

[1] https://www.heise.de/news/Interne-Dokumente-BSI-Warnung-vor-Kaspersky-war-stark-politisch-motiviert-7205028.html
[2] https://www.malwarebytes.com/blog/news/2023/04/tiktok-whats-going-on-and-should-i-be-worried
[3] https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/
[4] https://apnews.com/article/how-big-tech-created-data-treasure-trove-for-police-e8a664c7814cc6dd560ba0e0c435bf90
[5] https://www.av-comparatives.org/spotlight-on-security-politics-and-cyber-security-a-troubled-relationship/

Data sending can be an important factor when deciding which security solution best matches your needs. This report highlights the importance of user privacy, options for users to consent to the transfer of certain personal data, the trust required between users and vendors as well as the transparency of the vendors.

Please note, that this report only focuses on consumer software and does not consider any enterprise security solutions, which often have a much deeper access to user behaviour.

The last time we released a report about the data sending behaviour of AV-Vendors was in 2014[6], following the revelations regarding the extent of eavesdropping by the NSA by Edward Snowden. This resulted in users becoming increasingly aware of privacy issues and laws. In addition to this there have been several changes to privacy laws and court cases since then, such GDPR and the Schrems II ruling, which confirmed that data transfers to the US are a violation of European privacy right. There are prepared questionnaires for EU data controllers or processors to send to EU controllers or processors with ties to the US[7] (or by asking EU national data protection authorities https://edpb.europa.eu/about-edpb/about-edpb/members_en). Users can also directly ask companies for their data with prepared forms: https://gdpr.eu/faq/.

How was the data collected?

Each security product was installed on a test machine, whose network traffic was monitored, and a user was simulated. During these actions, Wireshark was used to collect and analyse network traffic, to determine if data was being sent.

It was also looked at the privacy statements and End User License Agreement (EULA) of each tested product (***as of August 2022***). These should state clearly which data may be sent to the respective manufacturer. Attached at the end of this report is a list with all direct links to the vendors.

Finally, each manufacturer was provided with a detailed questionnaire to fill out, requesting details of the data sent by their Internet security product. It was asked how the data is handled, what it is used for and some general questions about their company. Fourteen of the 20 vendors responded to the survey, but unfortunately, six chose not to respond to our inquiries.

Wherever possible, the responses from the vendors were augmented with our own measurements and research, especially in the cases where vendors did not respond at all. In cases where no answer was received to a question and where it was not possible to find any information, the answer was marked as “not disclosed”. We gave priority to our measurements and the End-User License Agreement (EULA) over the vendor responses. We cannot take any responsibility for the correctness of the data provided here.

In case of discrepancies between our own measurements and the answers to the questionnaires, we gave the vendors the opportunity to clarify any misunderstandings or misinterpretations. We understand that too much openness and transparency might be useful for criminals, who could thus find out how to bypass some features of the security products. We thus accept that vendors cannot provide us with any information which could compromise security.

[6] https://www.av-comparatives.org/wp-content/uploads/2016/12/avc_datasending_2014_en.pdf
[7] https://noyb.eu/files/CJEU/EU-EU_form_v3.pdf

Tested Products

In this evaluation popular AV products have been selected: Avast, Avira, Bitdefender, eScan, ESET, F-Secure, G Data, K7, Kaspersky, Malwarebytes, McAfee, Microsoft, Norton, Panda, Sophos, TotalAV, Total Defense, Trend Micro, VIPRE, Webroot.

Scoring

Scores were assigned to each vendor in five different categories, related to data sending. These scores are based on the responses from the vendors and our measurements. The categories we used are Data Collection, Data Sharing, Accessibility, Control of Software & Processes, and Openness. The exact scoring method and weighting of the individual questions was determined in collaboration with journalists and stakeholders. Since some vendors did not respond to our questionnaire, we were forced to rely on various data points, own measurements and information available online. In these cases, the vendors might have received a lower final score.

In the first category, **Data Collection**, vendors are awarded points based on the data they collect. The less data that is collected the better the score. The kind of data collected also affects the score, since some data is required for an antivirus to function. Certain information, such as license information, needs to be transmitted when registering a product. Other data, such as samples of potential malware might help identify new threats. However, vendors might also use their AV product to collect other data, such as browsing behaviour or information about installed programs. This could then be used for targeted advertising.

Next, we scored the respondents based on what they did with the collected data in the **Data Sharing** category. Here vendors received lower scores if they for example used collected data for targeted advertising or shared the data with third parties for other purposes.

For **Accessibility**, we looked at things like the readability of the policies and how easy these are to find. We also scored vendors higher, if they provided a FAQ or a simple language version along with their policies, which explained what data is collected as well as why this is necessary.

Next, we looked at how much of the software is produced in-house or if for example a third-party scan engine is used. We also inquired about the usage of third-party cloud storage for collected data. We present these scores in the category **Control of Software & Processes**.

Finally, we looked at the companies' **Openness**, both in responding to the questionnaire and about their practices in general. Points were awarded based on how many questions the vendor responded to if the company allows independent audits of its software and processes or is open about its processes in general.

Finally, we also assigned bonus points for questions we deemed especially important regarding security and trust in the AV vendor. These questions are marked in bold in the response table.

In each category, we assigned a score between one and five, with five being the best score. The following table shows the scores of each vendor in the five categories, followed by the vendors' final rating.

Vendor	Data Collection	Data Sharing	Accessibility	Control of SW / Processes	Transparency	Score
Avast	1	4	4	5	3	★★★
Avira	3	1	2	5	3	★★★
Bitdefender	2	4	4	5	5	★★★★½
eScan	2	5	2	5	3	★★★
ESET	2	5	4	5	5	★★★★½
F-Secure	4	5	3	3	5	★★★★½
G Data	5	5	3	5	4	★★★★½
K7	5	4	2	5	5	★★★★
Kaspersky	4	4	3	5	5	★★★★½
McAfee	2	0	5	3	5	★★★
Norton	3	1	5	3	2	★★★
Panda	5	1	3	5	3	★★★
VIPRE	5	5	2	5	4	★★★★
Webroot	1	4	4	3	2	★★★
Malwarebytes	0	4	1	3	1	★
Microsoft	4	4	1	3	2	★
Sophos	1	4	1	3	2	★
TotalAV	4	4	0	3	1	★
Total Defense	3	4	0	3	1	★
Trend Micro	3	4	1	3	1	★

Among the Vendors with the highest scores, listed alphabetically, are **Bitdefender, ESET, F-Secure, G Data, K7, Kaspersky,** and **VIPRE**. All of these Vendors achieved a score of four stars or higher. None of the Vendors achieved a perfect score of five stars, as that would require the product to be fully open source and not transmit or barely transmit any data, among other requirements.

Unfortunately, some vendors refused to respond, resulting in lower scores. These vendors are included at the end of the table and marked in light red.

It is important to note that these scores provide a general overview based on qualitative evaluation. Individual users may prioritize different categories differently.

Nowadays, most AV vendors rely on cloud-based systems, and this is not necessarily a negative aspect. In fact, cloud technology can be leveraged to provide better protection and enhance security measures.

Users should choose a product that fits their needs and preferences. If they are comfortable with a higher amount of data being sent by the product, then that is a valid choice. However, if users prioritize transparency and value products that are more open about their data-sharing practices, they have the option to select a more transparent product. Ultimately, the decision lies with the users and their individual preferences.

Vendor Responses

All vendors mentioned in this report were invited in Q3 2022to respond to the findings and answer a questionnaire. There was also the possibility to answer questions with "Not disclosed".

Product Version and License

All manufactures send the product version and license information along with a unique identification number of the machine. Sending the product version is obviously essential if it is to be updated to the latest version, which is of course recommended. Clearly, license information also needs to be transmitted to validate that the user receives the product they are paying for. These are among the examples of information that needs to be transmitted, in order to have a properly functioning antivirus product.

Most vendors also transmit product usage data; this could be very useful for improving the product, and so has a legitimate purpose, but this information can also, for example, be used to gather computer usage information about the user. All products send a unique identification number (UID), which can be used for licensing purposes.

Machine Information

It seems entirely reasonable that antivirus programs should send their manufacturers technical information about the machine they are running on, so that they can e.g., optimise for different operating systems and hardware specifications. Any conflicts with specific Windows updates/service packs and third-party software can be rectified. Sending product versions of third-party programs can be useful to warn of known vulnerabilities or outdated versions, e.g., for antivirus products that include a patch management component, or compatibility issues. The information could also allow vendors to understand the use of exploits by malware authors.

All respondents stated that their programs send operating system versions, which is entirely legitimate. Sending the workgroup name, local IP address and hostname (computer name) might seem to be an invasion of privacy. Many programs do send the local hostname; the most common reason given for this is that it is necessary for license key mapping, although most of the programs that do this also submit a unique identification number as well. In some cases, technical data which would appear to be very useful is not transmitted. For example, most programs do not send the IP address of the DNS server used by the system, even though this could be relevant, as malware can attempt to change a computer's DNS configuration. Information about display resolution, time zone and location can be used to identify individual users even if other personally identifying information is not transmitted, through so-called fingerprinting[8], which is used by many websites to identify users. However, more than half of the vendors transmit this information.

In some cases, our research showed that several AV products were transmitting machine information, despite the vendor stating that this was not the case. One vendor stated that this was due to a component inherited from the enterprise version and that this behaviour had not been noticed until that point. According to this vendor, this issue will be fixed in future versions of the product. This shows the importance of this research in finding such issues, so they can be fixed in future versions and unnecessary data transmission can be avoided.

[8] https://coveryourtracks.eff.org/about

Personal Information

The most personal information in this category might be the Windows username, which in many cases will be the user's full real name. About half of responding vendors stated that their products send the Windows username. Some claim that this is necessary for the parental control feature, and the username is only sent if the parental control feature is activated. However, not all the programs that send the Windows hostname even have a parental control function.

Roughly half the respondents' programs send country, region, and language settings. These could be used for several legitimate purposes, such as license control, providing the correct interface language, and noting the effect of regional settings on malware-hosting websites.

Sending information on URLs visited makes obvious sense if the product has a URL blocker. Sending details of the referrer (linking website) also seems relevant for blocking malware and finding out how users reach malicious pages on the internet. IP addresses of web servers are also obviously important. Some vendors state that they remove any personal information such as email addresses and passwords before sending details of a URL, which strikes us as the right thing to do.

The OS region settings are transmitted by most vendors, this information allows the AV product to, for example, set the correct language in the installer and in communication with the user. The keyboard layout could in theory also be used for this however but seems somewhat redundant and none of the questioned vendors stated that they transmit this information.

Almost all vendors stated that they did not transmit the user's SID or information about other Windows accounts on the computer. In cases where this information is transmitted one of the reasons given was the use of parental controls.

File-related Info

Sending information such as detection names, file hashes, names, paths, and sizes of potentially malicious executable program files is obviously important in counteracting malware, and almost all respondents' programs do this. What is less easy to justify is sending personal data files (e.g., documents) or non-malicious executable program files. We feel that users should be able to decide on a file-by-file basis whether such files are sent, especially since most vendors state that not transmitting suspicious files has no impact on product performance. Most programs allow users to opt out of file-sending either completely or on a case-by-case basis, although a number send files without explicitly asking the user (there may be a warning in the EULA that this will happen).

If malware steals personal data, we do not feel there is justification for the AV program to send the same information to the manufacturer. Some products' EULAs or privacy statements note that the product might transmit such data to the product vendor, though this is for legal reasons, in case the product inadvertently sends personal data along with legitimate information about the malware itself.

General

Sending of personal information/files should be pointed out/requested during setup. It's not reasonable to expect people to read the license agreement in full.

Many products make use of silent detections. This involves sending to the vendor details of files that have triggered a detection, without the user being alerted in any way. This can be done e.g., to check whether the file is genuinely malicious or not and reduce the number of false positives.

Most (but not all) manufacturers answered the question as to the jurisdiction in which collected data is stored. In some cases, this is dependent on the country in which the software is first installed.

We asked whether special updates are delivered to users with specific IDs. This could theoretically allow authorities with a suitable court order to monitor specific individuals e.g., by supplying them with a modified version of the product made for spying or that does not detect the spy software. All updates would however be supplied to all other users, ensuring that their PCs were still fully protected. Most of the vendors responded that they do not do this, although a few did not reply to this question.

All vendors that responded to our data-sending questionnaire provided links to the terms and conditions, EULA, and privacy policies of their respective products.

Transparency

Only a few of the contacted vendors provide a transparency report, which is a concerning trend, as we think users should be provided with easily accessible and understandable information about how their data is used. We have listed these vendors and links to their transparency reports below.

Vendor	Link
Avast	https://www.avast.com/transparency-report
G Data	https://www.gdata.de/business/it-sicherheit-made-in-germany/faq
Kaspersky	https://www.kaspersky.com/transparency-center

Some vendors allow for third-party review of their source code. Considering that a thorough code-review would take a very long time and might not give much real insight especially since any update after this could invalidate the code review. Each update to the product source code (which can take place several times a day) can change product behaviour, so most of the information that could be gained from a code review might not be applicable for long. However, most vendors do regularly have independent audits and certifications of their procedures, with the most common being SOC2 and ISO 27001 certifications.

None of the vendors stated, that they had refused a code review by a national government. However, the reason for this might simply be, that they were never asked. With some vendors telling us as much. Several vendors also reported that they have uncovered state-sponsored cyber-attacks. Such attacks are often politically or ideologically motivated and are often developed by teams of cyber security experts and can therefore be very dangerous and hard to detect. Probably the best-known example of this is Stuxnet, which specifically targeted industrial equipment used by the Iranian nuclear program.

Vendors about vulnerabilities that were uncovered in their products and if these where publicly disclosed. About half of the vendors provided links to reports detailing the vulnerabilities uncovered in their software.

Another trend we noticed, was that US and UK-based vendors are those who tended to not respond to the questionnaire at all.

Company

During our research, we sought to gather general information about the companies of the antivirus vendors we surveyed. Specifically, we inquired about the locations of their development centres. The results indicated that most of these centres are situated in Europe or North America, although some vendors also have development centres in India, Russia, and China. It is worth noting that most of the vendors only have development centres in a single country. In terms of the diversity of their workforce, we found that most companies employ individuals from many different countries.

Data Collection

Many vendors' data centres are located within the EU; however, some also have data centres in the US or India. While GDPR automatically applies to data about EU citizens, regardless of where the data is stored, non-EU residents' data stored within the EU is also protected by GDPR. A few vendors informed us, that the users' location influences where the user's data is stored since this is necessary to comply with GDPR regulations.

About half of the respondents, which answered this question, stated that they use user data for targeted advertising. However, in most cases, users can opt-out of data collection to varying degrees. Many companies use services such as VirusTotal, which could lead to sharing of classified or personal files collected along with or as malware samples. These files would then be available globally to all customers of VirusTotal[9]. Therefore, we asked how vendors would react in this situation almost all of them stated that they would delete the files from their servers and inform the party the file originated from, if possible.

About half of the security vendors share threat intelligence data with other AV vendors, including those located outside of their country's jurisdiction. Sharing threat intelligence with other AV vendors allows vendors to profit from each other's research.

Finally, we also asked if vendors refuse to share data with certain countries, almost all vendors have certain countries with which they do not have any dealings. These are typically countries embargoed by the US, UN, or EU.

[9] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2022/2022-206270-1032.pdf

Third-party Services

This refers to any services included in an AV product which were not developed by the company themselves, we are specifically interested services which collect user data. If such services are included user data might become available to the third party providing the services. A common example for this is user experience tracking services. Slightly less than half of the respondents stated they used third-party services however these respondents refused to provide additional information about which services they use.

We also asked the AV vendors, if they stored any user data in a third-party cloud, which cloud-service providers they used and where these stored user data. Most vendors use third-party cloud providers, with the most common being AWS and data typically being stored in the EU or US. Another common third-party service included with many AV solutions is a VPN product, with some form of VPN being offered by about half of the AV vendors. Most of these VPN services are developed by the companies themselves, however, some also include a third-party VPN or use third-party infrastructure, the most common being Aura. While a VPN can be used to keep your internet information private, the VPN provider can in theory monitor your entire activity online.

There are also a few AV products which use third-party scan engines or signatures for detecting malware, this means the AV vendor did not develop the AV product but instead repackages a third-party product.

Other Questions

Finally, we also asked the AV vendors some other questions about company processes. This includes reporting illegal files, such as child pornography to governments or other investigating bodies like INHOPE, or assisting authorities in investigating cybercrime, which less than half of the respondents have done. Depending on the data collected or accessible by the AV vendor it might be difficult for them to be of any assistance.

Only a few of the vendors provide an SBOM[10] for their products, this would be useful for users since knowing what software is used in the product can help users stay informed, for example when vulnerabilities are discovered in these products.

Lastly, we asked if the company has a secure coding process in place, which is something most vendors do. Vendors also told us that the data gathered and transmitted by each product does not go to a single collection centre; rather, specific elements are transmitted separately to different isolated endpoints, without any connection between them. Thus e.g., license-management data is sent separately from product-usage statistics. They say that as there is no connection between these systems, the data collected by one cannot be linked with the data collected by another. Consequently, the privacy of the users should be safeguarded.

[10] Software bill of materials, a list of all the software components used in the product.

Bug Bounties

We also asked vendors if their companies have bug-bounty programs. Such programs allow users to submit vulnerabilities discovered in a security product and be rewarded for their work. This can incentivize reporting vulnerabilities instead of exploiting them for nefarious purposes.

About half of the vendors offer such programs, we have gathered links to these in the table below:

Vendor	Link
Avast	https://www.avast.com/coordinated-vulnerability-disclosure
Avira	https://www.avira.com/en/report-a-security-vulnerability
Bitdefender	https://www.bitdefender.com/site/view/bug-bounty.html
ESET	https://hacktrophy.com/en/
F-Secure	https://www.f-secure.com/en/home/support/vulnerability-reward-program
G Data	https://www.gdata.de/sicherheitsluecke-melden
Kaspersky	https://support.kaspersky.com/general/vulnerability.aspx?el=12429
Norton	https://www.nortonlifelock.com/us/en/contact-us/report-a-security-vulnerability/
VIPRE	https://hackerone.com/ziff-davis?type=team

It seems that the following vendors do not have a bug bounty program: eScan, K7, Malwarebytes, McAfee, Microsoft, Panda, Sophos, TotalAV, Total Defense and Trend Micro.

Data as of August 2022	Czech Republic **Avast**	Germany **Avira**	Romania **Bitdefender**	India **eScan**	Slovakia **ESET**	Finland **F-Secure**	Germany **G Data**	India **K7**	Russia **Kaspersky**	USA **Malwarebytes**	USA **McAfee**	USA **Microsoft**	USA **Norton**	Spain **Panda**	UK **Sophos**	UK **TotalAV**	USA **Total Defense**	USA **Trend Micro**	USA **VIPRE**	USA **Webroot**
Product information																				
Is the product version and license infromation transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is a unique identification number for the machine transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are statistics for product usage transmitted?	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Machine information																				
Is the version of the operating system transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is the computer name (hostname) transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	not disclosed	Yes	Yes	No	Yes
Is the Windows Workgroup name transmitted?	No	No	No	Yes	No	No	No	No	No	not disclosed	No	not disclosed	Yes	No	not disclosed	not disclosed	not disclosed	not disclosed	No	Yes
Is information about installed third-party applications (e.g. version numbers) transmitted?	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes
Is information about other installed AVs transmitted?	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	not disclosed	Yes	Yes	Yes	not disclosed	not disclosed	not disclosed	No	Yes
Is information about the hardware (e.g. CPU, RAM) transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes
Is the BIOS version transmitted?	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	No	Yes	not disclosed	not disclosed	Yes	not disclosed	No	No
Is information about running processes transmitted?	Yes	No	Yes	Yes	No	Yes	No	No	Yes	Yes	No	Yes	Yes	No	not disclosed	not disclosed	not disclosed	Yes	No	Yes
Is the internal IP address transmitted?	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	not disclosed	Yes	Yes	No	Yes
Is the external IP address transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	not disclosed	Yes	Yes	Yes	not disclosed	not disclosed	Yes	No	Yes
Is the MAC address transmitted?	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	not disclosed	Yes	Yes	not disclosed	not disclosed	Yes	not disclosed	No	Yes
Is/are the IP address(es) of the DNS Server(s) transmitted?	Yes	No	No	No	Yes	No	No	No	No	not disclosed	No	not disclosed	No	No	Yes	not disclosed	not disclosed	not disclosed	No	Yes
Is the Network name transmitted?	Yes	Yes	Yes	No	Yes	No	No	No	Yes	Yes	No	Yes	No	No	not disclosed	not disclosed	not disclosed	not disclosed	No	Yes
Are error-logs or operating system event logs transmitted?	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes
Is the time of the last boot and/or login transmitted?	No	No	No	Yes	No	Yes	No	No	No	not disclosed	Yes	not disclosed	Yes	No	not disclosed	not disclosed	not disclosed	not disclosed	No	No
Is the display resolution transmitted?	Yes	Yes	No	No	Yes	No	No	No	No	not disclosed	Yes	not disclosed	Yes	Yes	Yes	Yes	Yes	not disclosed	Yes	No
Is location information (e.g. coordinates, city, country, etc.) transmitted?	Yes	Yes	No	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	not disclosed	Yes	No	Yes
Is the timezone transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	not disclosed	Yes	not disclosed	Yes	Yes	Yes	not disclosed	not disclosed	not disclosed	No	No
Personal information																				
Are visited URLs (malicious and non-malicious URLs) transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Is the referer (previous page with link to malware-hosting site) transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	not disclosed	No	No	not disclosed	Yes	Yes	not disclosed	Yes	Yes
Are IP addresses of visited webservers transmitted?	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	not disclosed	No	No	not disclosed	Yes	not disclosed	not disclosed	No	Yes
Is the content of cookies transmitted?	No	No	No	No	No	No	No	No	Yes	not disclosed	No	not disclosed	No	No	not disclosed	not disclosed	not disclosed	not disclosed	No	No
Are the OS country/region settings transmitted?	Yes	Yes	No	No	Yes	No	Yes	No	No	Yes	Yes	not disclosed	Yes	Yes	Yes	Yes	not disclosed	not disclosed	No	No
Is the keyboard layout of the operating system transmitted?	No	No	No	No	No	No	No	No	No	not disclosed	No	not disclosed	No	No	not disclosed	not disclosed	not disclosed	not disclosed	No	No
Is the Windows username transmitted?	No	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	not disclosed	Yes	No	Yes	not disclosed	not disclosed	Yes	Yes	Yes
Is the current Windows user's SID transmitted?	No	No	Yes	No	No	No	No	No	No	not disclosed	No	not disclosed	Yes	Yes	not disclosed	not disclosed	not disclosed	not disclosed	No	No
Is information about other Windows accounts on the computer transmitted?	No	No	Yes	Yes	No	No	No	No	No	not disclosed	No	not disclosed	No	No	not disclosed	not disclosed	not disclosed	not disclosed	No	No
File-related information (clean and malicious)																				
Are hashes of files and/or parts of files transmitted?	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	not disclosed	Yes	Yes	Yes	not disclosed	not disclosed	Yes	No	Yes
Are malware detection names transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	not disclosed	Yes	No	Yes	not disclosed	Yes	Yes	Yes	Yes
Is the file name and path transmitted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	not disclosed	Yes	Yes	Yes	Yes
↳ If "suspicious" files are transmitted: Are executable files transmitted?	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	not disclosed	not disclosed	Yes	No	Yes
↳ If "suspicious" files are transmitted: Are non-executable files (e.g. documents) transmitted?	Yes	No	No	No	Yes	Yes	No	No	Yes	not disclosed	No	not disclosed	No	No	Yes	not disclosed	not disclosed	Yes	No	Yes
Can user opt out of sending files?	Yes	No	No	N/A	Yes	Yes	Yes	N/A	Yes	not disclosed	Yes	not disclosed	Yes	No	not disclosed	not disclosed	not disclosed	not disclosed	N/A	Yes
Does opting out of data collection have any direct technical impact on the product (e.g. reduced protection)?	No	N/A	N/A	No	No	Yes	Yes	No	No	not disclosed	Yes	not disclosed	No	N/A	not disclosed	not disclosed	not disclosed	not disclosed	N/A	Yes
When potential malware collects and sends user data, is a sample of the collected data transmitted?	No	No	No	Yes	Yes	No	No	No	Yes	not disclosed	No	Yes	No	No	Yes	not disclosed	not disclosed	Yes	No	Yes
General																				
Do you make use of silent detections (e.g. for FP mitigation of new algorithms)?	Yes	not disclosed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	not disclosed	Yes	Yes	not disclosed	not disclosed	not disclosed	not disclosed	No	Yes
Are special updates delivered to users with specific IDs? We do NOT mean staged rollouts of regular updates e.g. by region.	No	not disclosed	No	Yes	No	No	No	No	No	not disclosed	Yes	Yes	No	No	not disclosed	not disclosed	not disclosed	not disclosed	No	No
In which jurisdiction(s) is the data stored (e.g. EU, USA)? Please list all.	EU, US	EU, US	EU	not disclosed	EU, US	not disclosed	EU	USA, India	EU, Canada, US, Russia	not disclosed	USA, India	not disclosed	EU, US	EU	not disclosed	not disclosed	not disclosed	not disclosed	EU, US	not disclosed
Do you provide an SBOM for its products?	not disclosed	No	Yes	No	No	Yes	Yes	No	Yes	not disclosed	No	not disclosed	not disclosed	Yes	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed
Do you operate a bug-bounty program?	Yes	Yes	Yes	not disclosed	Yes	Yes	Yes	No	Yes	not disclosed	No	not disclosed	Yes	No	not disclosed	not disclosed	not disclosed	not disclosed	Yes	not disclosed
Do you run secure coding processes in your company?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	not disclosed	Yes	not disclosed	Yes	No	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed
Transparency																				
Do you provide a transparency report?	Yes	No	No	No	No	No	Yes	No	Yes	not disclosed	No	not disclosed	No	No	not disclosed	not disclosed	not disclosed	not disclosed	No	No
Do you allow independent code reviews (secure access to your source code for enterprises and/or governments)?	not disclosed	Yes	No	No	No	No	No	No	Yes	not disclosed	No	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	No	not disclosed
↳ If yes, do code reviews cover the whole product (including engine and databases), or are there limitations?	not disclosed	not disclosed	N/A	N/A	N/A	N/A	N/A	N/A	Yes	not disclosed	N/A	not disclosed	N/A	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	N/A	not disclosed
↳ If yes, can reviewers reproduce the final build from the reviewed sources, to verify that the reviewed code is the same as that in public builds:	not disclosed	not disclosed	N/A	N/A	N/A	N/A	N/A	N/A	Yes	not disclosed	N/A	not disclosed	N/A	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	N/A	not disclosed
Have any independent audits/certifications of your procedures and secure development been done in the last 5 years?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	not disclosed	not disclosed	not disclosed	Yes	Yes	not disclosed	not disclosed	not disclosed	not disclosed	No	not disclosed
Have you uncovered any so-called state-sponsored cyberattacks in the last 5 years?	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	not disclosed	Yes	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	No	not disclosed
Has your company ever reported illegal files (e.g. child pornography) to authorities or other appropriate bodies (e.g. INHOPE)?	Yes	No	Yes	not disclosed	No	No	Yes	not disclosed	Yes	not disclosed	No	not disclosed	not disclosed	Yes	not disclosed	not disclosed	not disclosed	not disclosed	No	not disclosed
Has your company ever assisted authorities with investigation into cybercrime?	Yes	No	Yes	not disclosed	Yes	Yes	Yes	not disclosed	Yes	not disclosed	Yes	not disclosed	not disclosed	Yes	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed	not disclosed
Data collection, storage and sharing																				
Is there a correlation between the user location and the location of your own datacentre(s), e.g. to follow GDPR requirements?	Yes	No	No	No	No	No	No	No	Yes	not disclosed	Yes	not disclosed	No	No	not disclosed	not disclosed	not disclosed	not disclosed	Yes	not disclosed
Do you use any of the collected data for targeted advertisements, etc.?	Yes	Yes	No	No	No	No	No	Yes	Yes	not disclosed	No	not disclosed	Yes	Yes	not disclosed	not disclosed	not disclosed	not disclosed	No	not disclosed
Can users opt out from this data collection/selling?	Any/All data	Only other data	N/A	N/A	N/A	N/A	N/A	No	Any/All data	not disclosed	N/A	not disclosed	No	Only other data	not disclosed	not disclosed	not disclosed	not disclosed	N/A	not disclosed
If you come across classified documents (e.g. through analysis by your cloud services, or via 3rd-party sample-sharing services such as VirusTotal																				
↳ Will the document be erased from your systems?	Yes	Yes	Yes	not disclosed	No	Yes	Yes	Yes	Yes	not disclosed	Yes	not disclosed	not disclosed	Yes	not disclosed	not disclosed	not disclosed	not disclosed	Yes	not disclosed
↳ Will you inform the party it originated from?	No	Yes	Yes	not disclosed	Yes	Yes	Yes	Yes	No	not disclosed	Yes	not disclosed	not disclosed	No	not disclosed	not disclosed	not disclosed	not disclosed	No	not disclosed
Third-party services																				
Does any of your consumer products use any (your own or third-party) services that collect information (e.g. user-experience tracking)?	Yes	Yes	Yes	No	No	No	No	No	Yes	not disclosed	Yes	not disclosed	Yes	Yes	not disclosed	not disclosed	not disclosed	not disclosed	No	not disclosed
↳ If yes, can the user opt out?	Yes	No	Yes	N/A	Yes	N/A	No	N/A	Yes	not disclosed	No	not disclosed	Yes	N/A	not disclosed	not disclosed	not disclosed	not disclosed	N/A	not disclosed
Is any of the data that you collect from users' devices stored in a third-party cloud?	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	not disclosed	Yes	not disclosed	Yes	Yes	not disclosed	not disclosed	not disclosed	not disclosed	No	not disclosed

Why are people often especially sceptical towards security vendors?

Mikko Hyppönen, the Chief Research Officer of F-Secure cancelled his scheduled participation in the 2014 RSA Security Conference, in protest at collaboration by security company RSA with the United States NSA in the form of weakening security in its encryption systems. He stated that "*RSA is hardly the only vendor facing scrutiny. He said that the trustworthiness of U.S.-based security and technology companies is quickly eroding, pointing to a letter recently sent to 20 of the world's largest antivirus companies by Bits of Freedom, a Netherlands-based organization focused on digital rights. In that letter, the group asked whether the vendors had whitelisted government-authored malware. Most of those companies gave a prompt response in the negative, but U.S-based AV giants McAfee Inc. and Symantec Corp. never replied*".[11]

It is possible that intelligence/law-enforcement agencies in some countries prohibit vendors (security or otherwise) from revealing any co-operation with them[12].

Some people may ask why malware such as Stuxnet and R2D2 remained undetected for many years.

In the past, there have been cases of security vendors removing (or not creating) detection for commercial spyware/keyloggers, due to issues of commercial law. Thus, it is not far-fetched to assume that the same would be done for the software of law-enforcement agencies if instructed to do so.

Security vendors have an important duty to protect users' privacy. Equally, users must be able to trust the security products they use. Equally, users need to trust the security products they use, as it would otherwise be better not to go onto the Internet at all. However, with the frequent reports about data leaks, possible state-sponsored attacks and other dangers to be encountered on the Internet, this relationship is becoming more and more strained. https://www.av-comparatives.org/spotlight-on-security-politics-and-cyber-security-a-troubled-relationship/

[11] https://www.lastwatchdog.com/f-secures-mikko-hypponen-boycotted-rsa-2014/
[12] https://en.wikipedia.org/wiki/National_security_letter

Considerations for Users

It is important for users to inform themselves what information the software and hardware can collect, what data the vendor states they collect and for what purpose. Next consider if collecting and using this data is justified for the specific product. Ideally the information about what data is collected and for what purpose should be provided by the vendor in an easily accessible form, such as a FAQ written in understandable language, in addition to a privacy policy which goes into more detail. In fact, an easily readable privacy policy is a requirement under GDPR[13].

As with all software it is important to only purchase from a reputable manufacturer. Especially since AV products are potentially able to collect a lot of personal data that could be misused by an unscrupulous vendor. Therefore, it is also important to stay up to date on acquisitions of antivirus vendors since these could potentially lead to a change in the privacy policy or even the product ceasing to exist. You can read more about the potential consequences of take overs in the IT-security industry in the blog post on this topic[14]. Users should also avoid being lured into using free products that require submitting personal data (data mining is a business model too, as well as the inclusion of third-party tools which collect information on their own).

While AV vendors having offices all over the world might confuse or even discourage users, this is the case for most larger companies in our globalized world.

When choosing an AV product check if it is possible to choose which data the program is allowed to collect and share. Also consider that some data might inadvertently contain personal identifying information, such as file paths which include your username or information about hardware configuration which can in some cases also uniquely identify a PC through so called “fingerprinting”[15].

Warning issued by governments or notices prohibiting the use of certain apps on government issued devices might seem damning at first glance. However, in such cases, it is important to see these in context. Governments are typically at much higher risk of espionage or data theft, especially from other state actors. For individual users, it is far less likely to be targeted in such a way. Additionally, such warnings are often politically motivated as well[16].

Once you have selected anti-virus products that meet your security requirements, you may consider extra features, such as web-based management consoles/online accounts, parental control, lost devices, included VPN or even just the look and feel of a product.

[13] https://readable.com/blog/make-your-privacy-notices-readable-it-s-the-law/
[14] https://www.av-comparatives.org/av-comparatives-explains-the-implications-of-takeovers-in-the-it-security-industry/#more-35543
[15] https://coveryourtracks.eff.org/about
[16] https://www.heise.de/news/Interne-Dokumente-BSI-Warnung-vor-Kaspersky-war-stark-politisch-motiviert-7205028.html

Considerations for Vendors

The growing interest in cybercrime from private users, should at best be answered in a well maintained and updated FAQ. Firstly, this should clarify the definitions and help to understand the security offered by an anti-virus product. The FAQ should also explain what data the product collects and for what purpose. A section featuring general security best practices can also be very useful for users, as it can encourage users to take initiative in protecting their own data and safe behaviour on the Internet. All of this should be presented in an easily readable and searchable form, as well as being presented prominently on the vendors website and in the product.

In addition to a FAQ, it would be good to see vendors provide regular transparency reports. These should include information about the companies' data handling practices, changes in the privacy policy, information about security threats in the product and how these where addressed.

Besides providing the above-mentioned information, it is just as important for vendors to employ safe coding practices and to use secure deployment methods for updates to their products. These updates should also be delivered on a regular basis and address new threats uncovered.

Users should be asked each time before a file is sent to the vendor unless they have explicitly opted out of this by choosing either "always send" or "never send". Users should be able to specify in detail what information is being sent, as well as where it is being sent and how long it will be stored.

The path to files in a user profile can and should be sent as *%userprofile%* to avoid providing the user's name. It should be possible to genuinely opt out of data sending without losing or compromising protection or usability. Security products should not include third-party toolbars or other add-ons that collect data separately from the AV vendor.

Policies and EULAs

Product	Terms and Conditions/EULA/Privacy Policy
Avast	https://www.avast.com/legal https://www.avast.com/privacy-policy https://www.avast.com/products-policy#pc https://www.avast.com/eula#pc
Avira	https://www.avira.com/en/privacy-policy/homepage https://www.avira.com/en/privacy-policy/general-processing https://www.avira.com/en/privacy-policy/product https://www.avira.com/en/legal-terms
Bitdefender	https://www.bitdefender.com/legal/ https://www.bitdefender.com/site/view/legal-privacy-policy-for-home-users-solutions.html https://www.bitdefender.com/site/view/subscription-agreement-and-terms-of-services-for-home-user-solutions.html
eScan	https://escanav.com/en/about-us/privacy-policy.asp https://escanav.com/en/escan-software-agreement/end-user-license-agreement.asp
ESET	https://www.eset.com/us/policy-hub/legal-information/ https://www.eset.com/us/policy-hub/privacy/ https://help.eset.com/eula/
F-Secure	https://www.f-secure.com/en/legal/privacy/statement https://www.f-secure.com/en/legal/terms
G Data	https://www.gdatasoftware.com/privacy https://www.gdatasoftware.com/eula
Kaspersky	https://www.kaspersky.com/products-and-services-privacy-policy https://www.kaspersky.com/end-user-license-agreement
K7 Computing	https://www.k7computing.com/in/privacy-policy https://www.k7computing.com/in/terms-conditions https://www.k7computing.com/in/eula
Malwarebytes	https://www.malwarebytes.com/legal/privacy-policy https://www.malwarebytes.com/legal https://www.malwarebytes.com/eula
McAfee	https://www.mcafee.com/en-us/consumer-support/policy/legal.html
Microsoft	https://privacy.microsoft.com/en-us/privacystatement https://www.microsoft.com/en-us/servicesagreement/
Norton	https://www.nortonlifelock.com/privacy/ https://www.nortonlifelock.com/us/en/privacy/product-privacy-notices/ https://www.nortonlifelock.com/us/en/legal/
Panda	https://www.pandasecurity.com/en/homeusers/media/legal-notice/#e10 https://www.watchguard.com/wgrd-trust-center/privacy-policy https://go.pandasecurity.com/eula/
Sophos	https://www.sophos.com/en-us/legal/sophos-group-privacy-notice https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use
TotalAV	www.totalav.com/privacy www.totalav.com/terms
Total Defense	https://www.totaldefense.com/privacy/ https://www.totaldefense.com/eula/
Trend Micro	https://www.trendmicro.com/en_us/about/trust-center/privacy.html https://www.trendmicro.com/en_us/about/trust-center/privacy/notice.html
VIPRE	https://vipre.com/privacy-policy/ https://vipre.com/eula/
Webroot	https://www.opentext.com/about/privacy https://eula.webrootanywhere.com/

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(July 2023)