Independent Tests of
Anti-Virus Software

Summary Report 2024

Awards, winners, comments

TEST PERIOD: 2024

LAST REVISION: 19TH DECEMBER 2024

WWW.AV-COMPARATIVES.ORG

Contents

INTRODUCTION	3
MANAGEMENT SUMMARY	5
ANNUAL AWARDS	9
PRICING	17
TRIAL VERSION AVAILABILITY	19
HELP AND SUPPORT FOR TECHNICAL ISSUES	20
USER-EXPERIENCE REVIEWS	22
AVAST FREE ANTIVIRUS	25
AVG INTERNET SECURITY	29
AVIRA FREE SECURITY	32
BITDEFENDER TOTAL SECURITY	35
ESET HOME SECURITY ESSENTIAL	38
F-SECURE INTERNET SECURITY	42
G DATA TOTAL SECURITY	45
KASPERSKY STANDARD	48
MCAFEE TOTAL PROTECTION	51
MICROSOFT DEFENDER ANTIVIRUS	54
NORTON ANTIVIRUS PLUS	56
PANDA FREE ANTIVIRUS	59
QUICK HEAL INTERNET SECURITY	62
TOTALAV ANTIVIRUS PRO	65
TOTAL DEFENSE ESSENTIAL ANTI-VIRUS	68
TREND MICRO INTERNET SECURITY	71
FEATURE LIST	74
COPYRIGHT AND DISCLAIMER	75

Introduction

About AV-Comparatives

We are an independent test lab, providing rigorous testing of security software products. We were founded in 2004 and are based in Innsbruck, Austria.

AV-Comparatives is an **ISO 9001:2015** certified organisation. We received the TÜV Austria certificate for our management system for the scope: "Independent Tests of Anti-Virus Software".

http://www.av-comparatives.org/iso-certification/

AV-Comparatives is the first **certified EICAR Trusted IT-Security Lab** http://www.av-comparatives.org/eicar-trusted-lab/

At the end of every year, AV-Comparatives releases a Summary Report to comment on the various consumer anti-virus products tested over the course of the year, and to highlight the high-scoring products of the different tests that took place over the twelve months. Please bear in mind that this report considers all the Consumer Main-Test Series of 2024, i.e. not just the latest ones. Comments and conclusions are based on the results shown in the various comparative test reports, as well as from observations made during the tests (https://www.av-comparatives.org/consumer/test-methods/).

Tested Vendors

The following vendors' products were included in AV-Comparatives' Public Consumer Main-Test Series of 2024 and had the effectiveness of their products independently evaluated. We are happy that this year's tests helped several vendors to find critical and other bugs in their software, and that this has contributed to improving the products.

Management Summary

Tests

In 2024, AV-Comparatives subjected 16 consumer security products for Windows to rigorous investigation. All the programs were tested for their ability to protect against real-world Internet threats, identify thousands of recent malicious programs, defend against advanced targeted attacks, and provide protection without slowing down the PC.

Results and Awards

Whilst all of the programs in our test reached an acceptable level overall, some programs outperformed others. For details, please see "Overview of levels reached during 2024". In order to recognise those products that achieve outstanding scores in our tests, we have given a number of end-of-year awards that highlight the best results in each test, and overall. The Product of the Year, Outstanding Product and Top-Rated Awards are based on overall performance in the Public Consumer Main-Test Series; there are also Gold, Silver, and Bronze awards for each individual test type. Please see the Award Winners section for more details of the awards. The 2024 **Product of the Year Award** goes to **ESET. Avast**, **AVG, Bitdefender,** and **Kaspersky** win the **Top-Rated Award**.

Overview of Tested Products

Here we provide a summary for each of the programs tested, with a note of each one's successes during the year. Although the user interface does not affect any awards, we have noted some of the best UI features as well.

Avast takes a **Top-Rated Product Award** in 2024, after reaching Advanced+ level in six out of seven tests and Advanced for the remaining test. It also receives the **Gold Award** for the **Real-World Protection Test** and **Bronze Awards** for the **Malware Protection Test** and **Advanced Threat Protection Test**. It features a very clean and intuitive user interface, allowing you to manage multiple malware detections through a single informative alert box. Additionally, it provides a good range of scan options, including on-access protection that scans for malware while copying files.

AVG receives a **Top-Rated Product Award** for 2024, having reached Advanced+ level in six out of seven tests, and Advanced in the remaining test. It also wins the **Gold Award** for the **Real-World Protection Test** and a **Bronze Award** for the **Advanced Threat Protection Test**. It has a very clean and touch-friendly user interface, allowing you to manage multiple malware detections via a single informative alert box. In addition, it offers a solid range of scan options, including on-access protection that scans for malware while copying files.

Avira takes a **Gold Award** for the **Real-World Protection Test** this year. It also received three Advanced+ and three Advanced Awards in the 2024 tests. The program offers a simple, easy-to-navigate user interface, that can be switched between light and dark modes, and displays sensible, persistent alerts.

Bitdefender takes a **Top-Rated Product Award** in 2024, after receiving six Advanced+ and one Advanced Awards in seven tests. It took the **Gold Award** for the **Malware Protection Test**, **Silver Awards** for the **Real-World Protection Test** and **Advanced Threat Protection Test**, and a **Bronze Award** for **Low False Positives**. Its well-designed user interface includes a customisable home page and various scan options. The program combines multiple malware detections into a single alert and provides additional details to assist with threat analysis.

ESET is AV-Comparatives' **Product of the Year** for 2024, having received the highest Advanced+ Award in all seven tests this year. It also takes the **Gold Award** for the **Advanced Threat Protection Test**, a **Silver Award** for **Low False Positives**, and **Bronze Awards** for the **Real-World Protection Test** and **Performance Test**. Reviewers were impressed by the clean, intuitive user interface designed for non-expert users, as well as extensive customization and scan options available for power users.

F-Secure was successful this year, reaching Advanced level in three out of six tests. Testers noted the simple and easy-to-navigate interface, helpful feature explanations, and built-in offline help functionality.

G Data took three Advanced+ and four Advanced Awards in the 2024 tests. It also receives a **Silver Award** for the **Malware Protection Test**. Reviewers highlighted the interface's easy navigation, detailed status display, and excellent access control.

Kaspersky receives a **Top-Rated Product Award** in 2024, having taken Advanced+ level in six out of seven tests, and Advanced for the remaining test. It additionally receives a **Gold Award** for **Low False Positives**, and **Silver Awards** for the **Performance Test** and **Advanced Threat Protection Test**. The program's modern, tiled interface makes all essential features easily accessible, and advanced users will find a wide range of configuration options.

McAfee takes **Gold Awards** for the **Real-World Protection Test** and **Performance Test** this year. It also received four Advanced+ and two Advanced Awards in the 2024 tests. It features a modern and touch-friendly user interface that makes essential functions easily accessible, with clear and persistent malware alerts.

Microsoft received five Advanced Awards in this year's tests. The product is integrated into Windows and provides all essential antivirus features through a simple, unobtrusive interface.

Norton received one Advanced+ and three Advanced Awards in this year's tests. The program features a modern interface with essential features easily accessible. Its on-access protection scans files when they are copied to the disk and malware alerts are clear and persistent.

Panda received two Advanced+ and one Advanced Awards in this year's tests. Reviewers noted its simple user interface and small, integrated security blog, allowing you to read the latest IT-security news from Panda. Although it is a free product, upselling is very subtle and unobtrusive.

Quick Heal got one Advanced+ and one Advanced Award in the 2024 tests. The program interface is simple to navigate and displays a security/privacy score, along with articles from the Quick Heal blog. It offers various scan options and parental control features.

TotalAV got five Advanced Awards in the 2024 tests. The user interface is highly intuitive, with program features easily accessible. Malware alerts are clear and informative, allowing you to manage multiple detections from a single dialog box.

Total Defense took two Advanced+ and one Advanced Awards in this year's tests. It stands out for its simple and accessible user interface, offering a wide range of scan customization options, strong access controls, and the ability to manage all devices linked to the same user account.

Trend Micro received two Advanced Awards in this year's tests. The program is easy to install and features a simple user interface that provides quick access to key functions while also offering advanced options. Reviewers appreciated its persistent malware and status alerts, as well as the helpful online manual.

Applicability of results to Windows 11

We used the current released build of Windows 10 for the Consumer Main Series Tests, as well as for the User-Experience Reviews, in 2024. As of December 2024, statistics show that the majority of Windows users are still running Windows 10. We also note that Windows 10 is compatible with the great majority of PC hardware in current use. However, Windows 11 is gaining in popularity, and is now usually provided with new consumer PCs. Windows 11 is fully supported by all the vendors participating in this year's tests. Considering the similarities between Windows 10 and Windows 11 in terms of core system operations and security architecture, the conclusions derived from our assessments for Windows 10 can confidently be extended to Windows 11. The fundamental principles governing the effectiveness of anti-virus software against diverse threats are equally applicable to these two Windows versions, ensuring the relevance of our test results to both operating systems. In 2025, we will use Windows 11.

Advice on Choosing Computer Security Software

There is no such thing as the perfect security program, or the best one for all needs and every user. Being recognized as "Product of the Year" does not mean that a program is the "best" in all cases and for everyone: it only means that its overall performance in our tests throughout the year was consistent and unbeaten. Before selecting a security product, please visit the vendor's website and evaluate their software by downloading a trial version. Our awards are based on test results only and do not consider other important factors (such as available interface languages, price, and support options), which you should evaluate for yourself.

Overview of levels reached during 2024

AV-Comparatives provides a wide range of tests and reviews in comprehensive reports (https://www.av-comparatives.org/consumer/test-methods/). Annual awards for 2024 are based on the Public Consumer Main-Test Series: **Real-World Protection Test**, **Performance Test**, **Malware Protection Test, False-Alarm Test** and the **Advanced Threat Protection Test**.

All the programs tested are from reputable and reliable manufacturers. Please note that even the STANDARD level/award requires a program to reach a good standard, although it indicates areas which need further improvement compared to other products. ADVANCED indicates that a product has areas which may need some improvement, but is already very competent. Below is an overview of awards reached by the various anti-virus products in AV-Comparatives' Consumer Main-Test Series of 2024.

	Malware Protection	Performance	Real-World Protection	ATP	Malware Protection	Performance	Real-World Protection
	March 2024	April 2024	February-May 2024	Autumn 2024	September 2024	October 2024	July-October 2024
ESET	***	***	***	***	***	***	***
Bitdefender	***	***	***	***	***	**	***
Kaspersky	***	***	***	***	***	***	**
Avast	***	***	***	**	***	***	***
AVG	***	***	***	**	***	***	***
G Data	***	**	***	**	***	**	**
McAfee	**	***	***	*	**	***	***
Avira	**	***	***		**	**	***
Microsoft	**	**	**		**	**	*
Total Defense	**	*	***		***	*	*
Total AV	**	**	*		**	**	**
Norton	*	**	**		*	***	**
F-Secure	*	**	**		**	*	*
Panda		***	**			***	
Trend Micro		**	*			**	
Quick Heal		***				**	

Key: * = Standard, ** = Advanced, *** = Advanced+

Annual Awards

Awards for individual tests

For each of the test types[1] in the Public Consumer Main-Test Series (Real-World Protection, Malware Protection, Advanced Threat Protection, Performance and False Positives), we give **Gold**, **Silver** and **Bronze** awards, for the first, second and third highest-scoring products, respectively.

Awards for combined scores of all tests

As in previous years, in 2024 we are giving our **Product of the Year Award** to the product with the highest overall scores across all the tests in the Public Consumer Main-Test Series. This depends on the number of Advanced+ awards received in all the tests. As the overall scores are considered, a product can receive the Product of the Year award without necessarily reaching the highest score in any individual test. A product cannot win the Product of the Year Award in two consecutive years if in the second year there is another product (or other products) with the same highest award levels.

We sometimes have a situation where two products reach exactly the same highest award levels. We think it is fair to highlight the fact that more than one product has reached an excellent level, and so in such cases we give the Product of the Year Award to the product that didn't get it most recently. The other product with the same highest award levels will receive the **Outstanding Product Award**. It even happens that three or more products reach the same highest award levels. In this situation, the product with the highest individual scores wins Product of the Year, while the others receive the Outstanding Product Award. In cases of uncertainty, the final allocation of the 'Product of the Year' and 'Outstanding Product' awards will be decided by the tester, considering principally the precise results of the individual tests.

As in previous years, we will also be giving **Top-Rated Product Award** to a select group of tested products which reached a very high standard in the Public Consumer Main-Test Series. We have used the results over the year to designate products as "Top-Rated". Results from all the tests are assigned points as follows: Tested = 0, Standard = 5, Advanced = 10, Advanced+ = 15. Products with 90 points or more are given the **Top-Rated award**.

To get the **Approved Windows Security Product Award**, at least 35 points must be reached.

[1] For some test types, there may be two actual tests conducted in a year; the awards are based on the combined score of both tests.

Approved Security Product Award

The vast majority of products from the 16 vendors tested have earned the prestigious AV-Comparatives 2024 Approved Windows Security Product certification, underscoring their commitment to excellence in security solutions. These are listed below:

Avast, AVG, Avira, Bitdefender, ESET, F-Secure, G DATA CyberDefense, kaspersky, McAfee, Microsoft, norton, panda a WatchGuard brand, TOTAL AV, total defense

Product of the Year 2024

AV-Comparatives' 2024 Product of the Year Award goes to:

ESET

Top-Rated Products 2024

AV-Comparatives' Top-Rated Awards for 2024 goes to:

Avast, AVG, Bitdefender, Kaspersky

Please see our summary and awards pages – links below:
https://www.av-comparatives.org/test-results/
https://www.av-comparatives.org/awards/

Real-World Protection Test winners

Security products include various different features to protect systems against malware. Such protection features are taken into account in the Real-World Protection Test, which tests products under realistic Internet usage conditions. Products must provide a high level of protection without producing too many false alarms, and without requiring the user to make a decision as to whether something is harmful or not.

The programs with the best overall results over the course of the year were from: **Avast, AVG, Avira, Bitdefender, ESET,** and **McAfee**.

AWARDS

Avast, AVG,

Avira, McAfee

Bitdefender

ESET

For details and full results of the 2024 Real-World Protection tests, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/real-world-protection-tests/

Malware Protection winners

The Malware Protection Test evaluates an AV product's ability to protect against malware coming from removable devices or network shares. Products must provide a high level of protection without producing too many false alarms. In the Malware Protection Test, all samples not detected on-demand or on-access are executed.

Bitdefender, G Data and **Avast** scored well in both tests.

AWARDS

Bitdefender

G Data

Avast

For details and full results of the 2024 Malware Protection tests, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/malware-protection-tests/

False Positives winners

False positives can cause as much trouble as a real infection. Due to this, it is important that anti-virus products undergo stringent quality assurance testing before release to the public, in order to avoid false positives. AV-Comparatives carry out extensive false-alarm testing as part of the Malware Protection Tests. Additionally, also false alarms from the Real-World Protection Test are counted for this category.

The products with the lowest rates of false positives during 2024 were **Kaspersky** (5), **ESET** (15) and **Bitdefender** (20). These figures represent the SUM of the false positives from all False Alarm Tests.

AWARDS

Kaspersky

ESET

Bitdefender

False Alarm Testing is included in each Protection Test.

For additional details about False Positives in the Malware Protection Test, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/false-alarm-tests/

Overall Performance (Low System-Impact) winners

Security products must remain turned on under all circumstances, while users are performing their usual computing tasks. Some products may have a higher impact than others on system performance while performing some tasks.

McAfee, Kaspersky and **ESET** demonstrated a lower impact on system performance than other products.

AWARDS

McAfee

Kaspersky

ESET

For details and full results of the 2024 Performance Tests, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/performance-tests/

Advanced Threat Protection (Enhanced Real-World Test) winners

This tests a program's ability to protect against advanced targeted and fileless attacks.

ESET blocked 14 targeted attacks (out of 15), while **Bitdefender** and **Kaspersky** blocked 13 attacks, and **Avast** and **AVG** blocked 12 attacks.

AWARDS

ESET

Bitdefender, Kaspersky

Avast, AVG

For details and full results of the 2024 Advanced Threat Protection Test, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/advanced-threat-protection-tests/

Pricing

AV-Comparatives' awards and rankings are based entirely on products' technical capabilities, not on any other factors such as costs. However, the price of a security product is obviously a factor that users consider. We have listed here some considerations that readers may like to take into account when choosing their security software.

We would not recommend choosing a security product based on price alone. We suggest that you look at protection, performance and ease of use first, and consider the price last.

It is clear that some free programs' protection and performance are on a par with paid-for programs, and are easy to use. One of the main disadvantages to free programs can be limited technical support, however. Additional features may also be lacking or limited. Finally, some free programs make extensive advertising for their paid-for counterparts, which many users may find irritating.

It is possible to buy security programs from third-party vendors (e.g. online or in electronics stores) more cheaply than the vendor's list price. We would advise users to check that they are buying the latest version of the product, or that the product purchased can be upgraded to the latest version without additional cost.

When purchasing a product from the vendor's own website, there are two factors that users might like to consider. The first concerns multi-platform licences. Many vendors now offer a licence for e.g. 5 devices, which you can use for Windows, macOS or Android devices, or a mix. In some cases, the price may vary depending on which section of the website you buy from. For example, a multi-platform licence bought from the "Products for Mac" page may be a different price from an (effectively identical) product bought from the "Products for Windows" page.

The second point to consider is auto-renewal. Some vendors offer or automatically apply auto-renewal of the subscription when you buy from their website. Unless you cancel this, you will be charged again at the end of the initial licence period, and the subscription will be extended accordingly. Clearly this is to the advantage of the vendor, as it makes it easy for them to keep you as a customer. If you buy an AV product from the vendor's own website, we suggest that you check the auto-renewal situation first. Some vendors do not have auto-renewal at all. Others let you opt in by putting a tick in a checkbox, while others have auto-renewal activated by default, but let you opt out easily by removing the tick from the checkbox. In some cases, auto-renewal is automatically applied, and cannot be deactivated at the time of purchase; you have to message the vendor afterwards to cancel it. This gives the vendor the opportunity to try to keep you as a customer, by offering various incentives. Most vendors offer the first year at about half the price of what they charge for subsequent years with auto-renewal.

Before agreeing to purchase a product with auto-renewal, we suggest that you find out what the renewal price will be when your subscription expires. In some cases, this may be very much higher than the initial purchase price. However, it might also be cheaper. It is also possible that if you opt out of auto-renewal at the time of purchase, the price shown in the basket will increase. Although also our Security Survey[2] indicates that most users are not happy with mandatory auto-renewal, more and more vendors are nowadays imposing mandatory auto-renewals.

[2] https://www.av-comparatives.org/surveys/it-security-survey-2021/

In the table below we have listed the (rounded) current discount price, full list price and auto-renewal prices (where applicable), including sales tax, for the paid products in the 2024 Main-Test Series.

Product	Devices	Discounted[3] price first year (in EUR incl. VAT)	Full List Price (in EUR incl. VAT)	Auto-renewal price (in EUR incl. VAT)	Auto-renewal ON by Default
AVG Internet Security	1	44 €	73 €	73€	Yes (mandatory)
Bitdefender Total Security	**5**	40 €	95 €	95€	Yes (mandatory)
ESET HOME Security Essential	1	n/a	40 €	40 €	Yes (optional)
F-Secure Internet Security	1	n/a	50 €	50 €	Yes (mandatory)
G Data Total Security	1	n/a	50 €	50 €	Yes (optional)
K7 Total Security	1	17 €	26 €	n/a	No
Kaspersky Standard	1	25 €	35 €	35 €	Yes (mandatory)
McAfee Total Protection	1	30 €	87 €	87 €	Yes (mandatory)
Norton AntiVirus Plus	1	15 €	35 €	35 €	Yes (mandatory)
Quick Heal Internet Security	1	22 €	54 €	n/a	No
TotalAV Antivirus Pro	**5**	29 €	99 €	99 €	Yes (mandatory)
Total Defense Essential Antivirus	**3**	38 €	57 €	57 €	Yes (mandatory)
Trend Micro Internet Security	1	20 €	50 €	50 €	Yes (optional)

Key: Ratio of rounded autorenewal price to rounded discounted first-year price is (green) no more than twice; (yellow) more than twice but no more than three times; (red) more than three times.

Where "Auto-renewal on by default" is shown as "optional", it means that auto-renewal is activated by default, but can be deactivated at the time of purchase, e.g. by removing a tick/checkmark in the relevant box. Where it is shown as "mandatory", you cannot deactivate it at the time of purchase, but have to cancel it afterwards. Each vendor has its own procedure for deactivating auto-renewal, so we suggest that readers find out about this in good time before the renewal date. It might be that e.g. uninstalling the product from the computer makes cancelling auto-renew more difficult.

The aim of this table is to get an overview about each product's full list price with both its discounted price for the first year and its renewal price for the second year of the subscription. We advise readers NOT to use the data here to compare prices between products. Some products provide just malware protection, whilst others include e.g. parental controls as well, so it would not be a fair comparison. Our 2024 Consumer Main-Test Series tested free products by Avast, Avira, Microsoft and Panda. These products are not shown in the table, as pricing does not apply to them. For three of the products shown in the table, the lowest-price subscription allows you to install the product on more than one device. If you only want to protect one device with these products, you will still have to pay the price shown here. We have given the prices shown on the respective vendor's website at the time of writing (December 2024), applicable to users in Austria. In 2021, the UK's consumer watchdog published guidelines for AV vendors on acceptable practice for auto-renewal. For further details, please see our blogpost[4]. In 2022, similar guidelines were released in Germany[5].

Although the majority of vendors make auto-renewal mandatory, we should point that most commendably, ESET, G Data, K7, Quick Heal and Trend Micro do not impose auto-renewal on users.

[3] It is possible that some vendors may offer additional discounts at specific times or under specific circumstances.

[4] https://www.av-comparatives.org/av-comparatives-welcome-uk-guidelines-on-auto-renewal-by-antivirus-vendors/ and https://www.ecommerce-verbindungsstelle.de/einkaufen-im-internet/online-vertraege-und-abos-kuendigen.html

Trial version availability

The landscape of accessing antivirus trial versions has significantly transformed, departing from its former simplicity of anonymous usage for a set duration. Previously, users could freely download trial versions without the need to disclose payment details or personal information. However, today[5], accessing these trials frequently involves sharing sensitive payment information, such as credit card data, potentially leading to automatic charges once the trial concludes. Furthermore, vendors commonly request personal details like email addresses and phone numbers, which might expose users to subsequent promotional emails or unwanted solicitations aimed at pushing product purchases. This evolution in trial procedures not only complicates the initial user experience but also raises concerns about privacy and unwarranted marketing intrusions.

Product	Requires Payment Information	Requires Account Registration
Avast Free Antivirus	**No**	No
AVG Internet Security	**No**	No
Avira Free Antivirus	**No**	No
Bitdefender Total Security	**No**	Yes
ESET HOME Security Essential	**No**	Yes
F-Secure Internet Security	**No**	Yes
G Data Total Security	**No**	Yes
Kaspersky Standard	**YES**	Yes
McAfee Total Protection	**YES**	Yes
Microsoft Defender Antivirus	**No**	No
Norton Antivirus Plus	**YES**	Yes
Panda Free Antivirus	**No**	No
Quick Heal Internet Security	**No**	Yes
TotalAV Antivirus Pro	**YES**	Yes
Total Defense Essential Antivirus	**No**	Yes
Trend Micro Internet Security	**No**	No

Requires Payment Information: This may include details such as credit/debit card information or PayPal account. Users may face automatic charges after the trial period if the otherwise-applicable subscription is not cancelled.

Requires Account Registration: This may involve providing or creating an account with personal details like name, email, password, mobile phone number, and country. Users might receive promotional emails or calls to encourage product adoption. For trial purposes, users could try to use pseudonyms and disposable/fake email addresses to maintain privacy.

Whether users have to provide payment or account information might vary from country to country (e.g. McAfee).

The four free products in the table above do not require personal information in order to get the product. It is commendable that AVG and Trend Micro do not require any information to use the trial.

[5] As of December 2nd, 2024. We searched for trials on the main product pages of the international/global and various localized websites.

Help and support for technical issues

One reason for purchasing an AV product, as opposed to using a free one, is that help and extended support options for technical issues are included in the licence fee. Effective support from the vendor can be hugely valuable in solving any sort of technical issue with the product. Whilst you might not need it that often, when you do need it, it's really good to have it. If you are using a product, and the vendor does not provide effective support when you need it, you might want to consider using a different product instead.

For clarity, we would define the difference between "help" and "support" as follows. By "help" we mean manuals, online help pages, FAQs and chat bots, where you can access previously-prepared answers and instructions. By "support" we mean communication with a member of the vendor's staff (via email, chat, phone), where you can ask for assistance with your specific problem. User forums may or may not fall into the category of vendor support. In some cases, you may get a reply from an official representative of the vendor, whereas with others you can only ask other users.

Before buying a security solution, you might like to investigate the help and support options provided by the vendor. Here we have noted some things to consider if you do this.

A downloadable user manual is helpful, as it can be used offline. So, if you were having problems accessing the Internet, you could check the manual to see if the product's network protection features might be having any effect on this, and reconfigure them if necessary.

Some vendors offer a free malware-removal service with their products. This is likely to be cheaper than going to a computer repair shop. Vendors may also offer a "malware-removal guarantee", whereby if your computer is infected and the vendor cannot remove the malware, you get back the money you paid for the product.

We note that some help and support options require you to log in to the vendor's online account before you can use them. In such cases, you might not be able to see what options are available until you actually purchase the product. Some vendors make it quite difficult to find contact options for e.g. phone support; you may have to click your way through a number of other pages to find them. You might also find that a vendor additionally offers a premium support service, but if you have purchased the product, you should be entitled to support as part of the licence fee.

Many vendors have different websites for different countries. In some cases, you may have to contact the support service in the country whose website you purchased the product from. Help and support options available for a product may vary from country to country. You should also consider that for telephone support, you may have to call a number in another country, which could mean higher telephone charges. Also, you might not get support in your native language, and you might have to call at an inconvenient time for you, if the vendor only provides support e.g. during their own office hours.

Sorry, AV-Comparatives does not provide technical support for any product. However, if you need assistance with your AV product, we have listed below some of the English-language help and support options for the products in our Consumer Main-Test Series. You can click on the links to go directly to the relevant pages of the respective products' websites.

Product	Online Help	Support Forum	Contact Support
Avast Free Antivirus	Online Help	Avast Forum	n/a
AVG Internet Security	Online Help	AVG Forum	Contact
Avira Free Antivirus	Online Help	Avira Forum	Contact
Bitdefender Total Security	Online Help	Bitdefender Forum	Contact
ESET HOME Security Essential	Online Help	ESET Forum	Contact
F-Secure Internet Security	Online Help	F-Secure Forum	Contact
G Data Total Security	Online Help	n/a	Contact
Kaspersky Standard	Online Help	Kaspersky Forum	Contact
McAfee Total Protection	Online Help	McAfee Forum	Contact
Microsoft Defender Antivirus	Online Help	Microsoft Forum	n/a
Norton Antivirus Plus	Online Help	Norton Forum	Contact
Panda Free Antivirus	Online Help	Panda Forum	n/a
Quick Heal Internet Security	Online Help	n/a	Contact
TotalAV Antivirus Pro	Online Help	n/a	Contact
Total Defense Essential Antivirus	Online Help	n/a	Contact
Trend Micro Internet Security	Online Help	Trend Micro Forum	Contact

User-Experience Reviews

Review Format

The aim of the user-experience review is to give readers an idea of what each tested product is like to use in everyday situations. For each of the tested products, we have looked at the following points (where applicable).

About the program

To start off by stating whether the program is free or paid. We do not list individual protection components (e.g., signatures, heuristics, behavioural protection), for the following reasons. Our protection tests verify how well each program protects the system, regardless of which components are involved. It is not the number of features that is important, but how effectively they work. Also, different vendors may use different names for individual functions or combine multiple types of functionalities under one name, making comparisons misleading. For readers' convenience, we mention any non-malware-related features, such as parental controls or spam filtering, but do not evaluate their functionality, except for a replacement firewall (see below).

Summary

We provide a concise product summary by focusing on the program's usability and emphasising key features and observations covered in the following sections.

Setup

We note any options available during setup, including any decisions users need to make and other points of interest, such as introductory wizards that explain the program's features. We suggest offering a simple installation option for non-expert users, with clear and straightforward explanations for any decisions they may need to make at any stage.

System Tray icon

We state what functionality is available through the program's System Tray icon menu, which can provide quick access to commonly used features like scans and updates. A System Tray icon is a standard and very useful feature of modern consumer security programs, indicating. that the program is running. However, we note that by default, Windows 10 hides third-party System Tray icons, meaning many non-expert users may not notice the icon for a non-Microsoft AV app.

Security status alert

Here, we disable the program's real-time protection, and check to see what alerts are shown in the program window or elsewhere. We also look for a quick and easy mean of reactivating the protection. An effective status display in the main program window, which shows a clear warning if protection is disabled, is a very standard feature, as is a "Fix-All" button/link with which the user can easily re-enable protection if it is not active. We regard both of these as very important, especially for non-expert users. We suggest that additional pop-up alerts, which the user would see even if the program window was not open, are a desirable bonus.

Malware detection alert

We check what sort of alert each program shows when malware is encountered. To do this, we try to copy some malware samples from a network share to the Windows Desktop of our test PC. If the AV product does not detect the copied malware, we then execute one of the samples (by this stage at the latest, all the tested programs will detect the malware samples used).

At whichever point the malware is detected, we look to see what sort of alert is shown, if the user has to take any action, and how long the alert is shown for. If the message box provides a link to more details, we click on this to see what information is provided. We also note whether multiple alerts are shown when multiple malicious files are detected at the same time.

We regard it as ideal if the malware is deleted or quarantined automatically, without the user having to make a decision on what to do with it. We would definitely recommend that any alert box should NOT include an option to instantly whitelist the file (i.e. allow it to be executed there and then). A much safer option is to quarantine the file, after which power users could go into the program's settings to whitelist and restore it if they wanted.

We suggest that persistent alerts, which are displayed until the user closes them, are ideal, as they ensure the user has time to read them. If a separate alert box is shown for every malicious file discovered, it can be a nuisance to have to close them all when multiple detections are made at once. We would say that a single alert box that lets you browse through detections, but can be closed with a single click, is optimal.

Scan options

Here, we review the different types of on-demand scans offered by the program, including how to access and configure them. We also look at how to set scan exclusions, schedule scans, and the available options for PUA detection.

Quarantine

We examine the program's quarantine function, focusing on the information it provides about the detection location, detection date/time, and the malware itself. We also check what options for processing quarantined items, such as delete or restore, are available.

Logs

Here, we note what information is provided in the program's log function.

Help

In this section, we take a quick look at the help features directly accessible within the program. Some vendors will have additional online resources, such as manuals and FAQ pages, that can be typically found on their respective websites.

Advertising

In this section, we evaluate how the program handles advertisements. This includes whether the software promotes its own products, offers additional services, or displays third-party ads. We also note the intrusiveness of these ads and how they are presented to the user.

Access control

For users who do not share their computer with anyone, this section is not relevant. However, if you share a computer, e.g. with your family at home, or colleagues in a small business, you might want to read it. Here we check, if it is possible to prevent other users of the computer from disabling the security program's protection features or uninstall it altogether. There are two ways of doing this. Firstly, access can be limited using Windows User Accounts: users with Administrator Accounts can change settings and thus disable protection, whereas those with Standard User Accounts can't.

Alternatively, a program can provide password protection, so that any user – regardless of account type – must enter a password to change settings. Some programs provide both methods, which we regard as ideal. When testing access control, we try to find all possible means of disabling protection, to ensure that any restrictions apply to all of them.

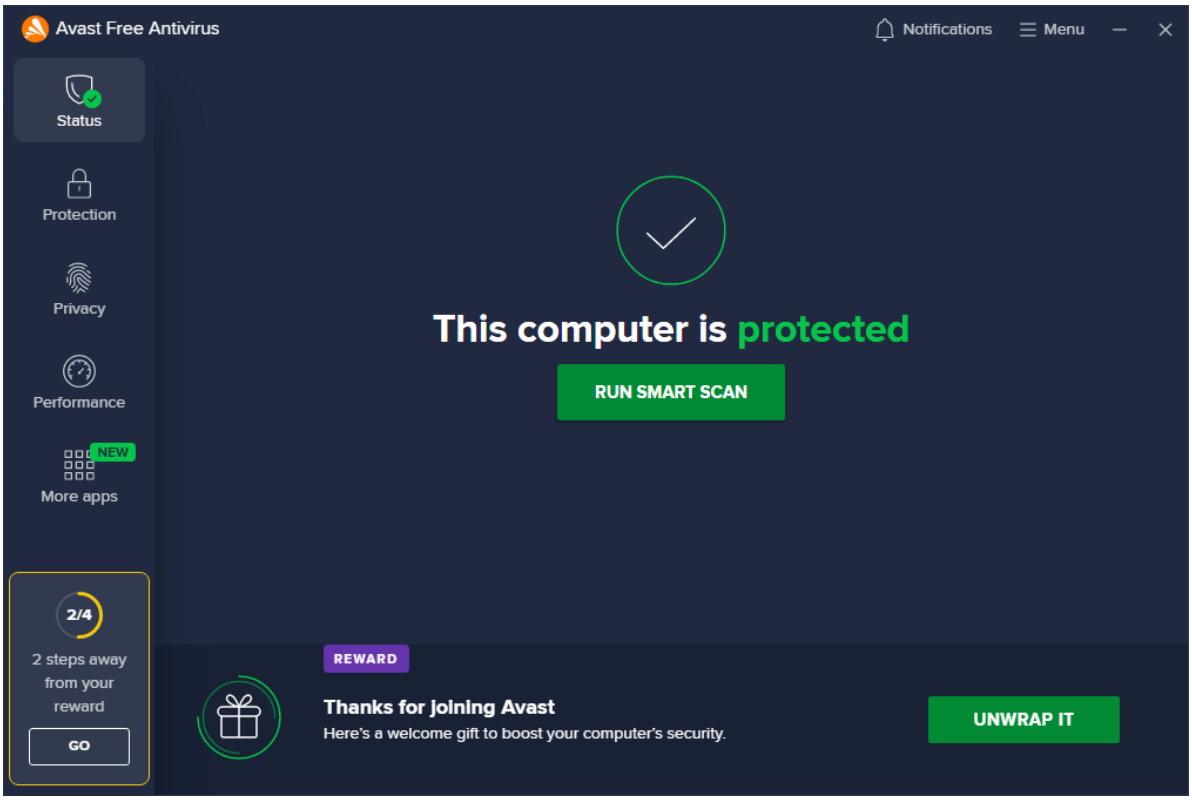
Other points of interest

Here we note anything we observe or find out about a product that we think is relevant. This may include privacy-related items, descriptions of the product on the vendor's website, unusual places to find features, customisation options, prompts to install additional features, upselling, bugs, explanations of functions, and out-of-the-ordinary features and notifications.

Support for Windows 11

All the tests in the 2024 Consumer Main-Test Series were performed using Windows 10. However, all tested/reviewed products are fully compatible/supported with Windows 11. In 2025, we will use Windows 11.

Avast Free Antivirus



About the program

Avast Free Antivirus is a free security program. In addition to anti-malware features, it includes a manual software-updater, a ransomware shield, and a feature that alerts you if the password for a specified online account is leaked online. You can find out more about Avast Free Antivirus on the vendor's website: https://www.avast.com/free-antivirus-download

Summary

The interface of Avast Free Antivirus is clean, touch-friendly, and easy to navigate. We liked the informative malware detection alerts, which let you manage multiple detections from a single alert box and persist until closed by the user. There is a good range of scan options, and on-access protection means that files are scanned for malware if you try to copy them to your PC.

Setup

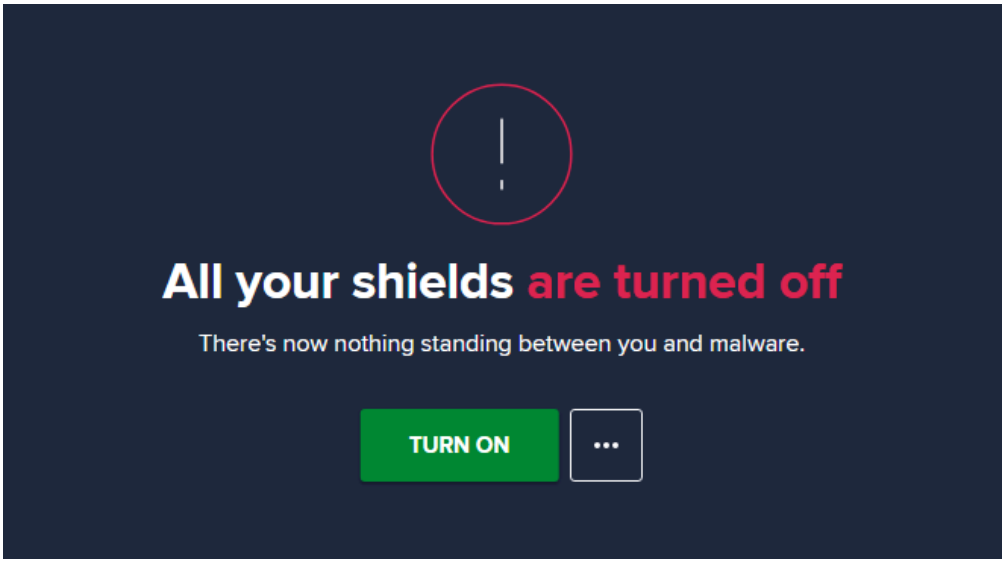
The setup wizard offers to install the *Avast Secure Browser* and set it as the default browser. However, you can easily opt out by removing the corresponding tick (checkmark). We chose not to install the Avast browser for our functionality test. After clicking *Install*, Avast Free Antivirus installs in the background. Power users can customize the installation by selecting which individual components should be installed. We used the default configuration for our functionality test. After completing setup, we were presented with an option to upgrade to the paid version, followed by a prompt to run a first scan.

System Tray icon

From the System Tray menu, you can open the program window, disable protection for a specified time, enable *Silent Mode*, open quarantine, run *Bank Mode*, update the program and/or definitions, and view program and registration information.

Security status alert

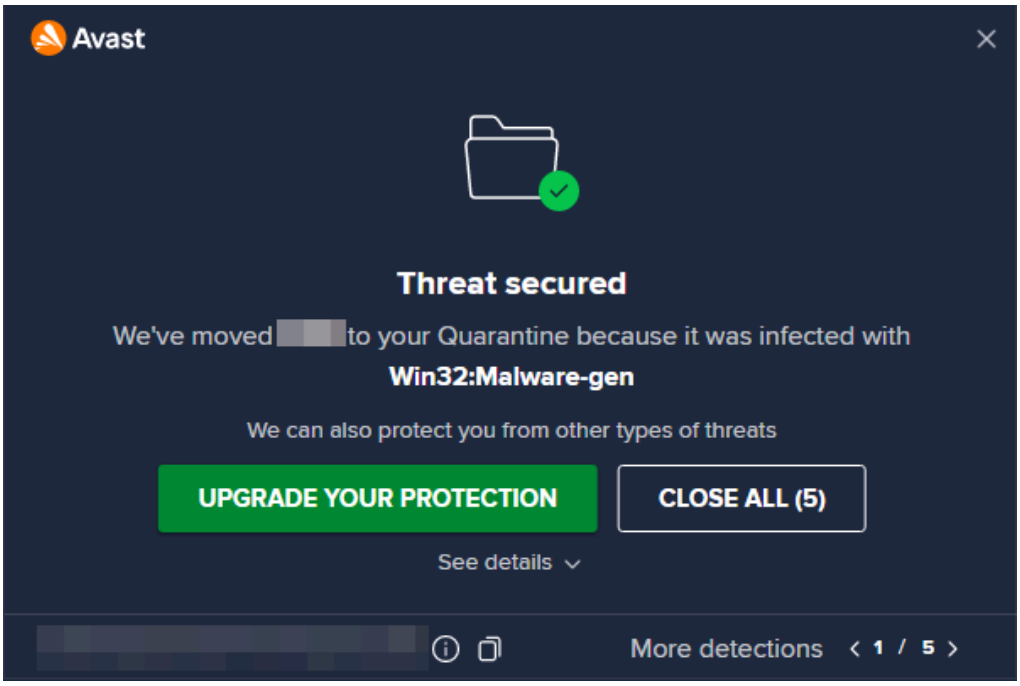
When we disabled real-time protection in the program's settings, we were prompted to confirm this action and choose how long to disable protection. We appreciated that protection was automatically turned on afterwards. An alert was shown on the program's home page (screenshot below). We were able to reactivate the protection easily by clicking *Turn On*.



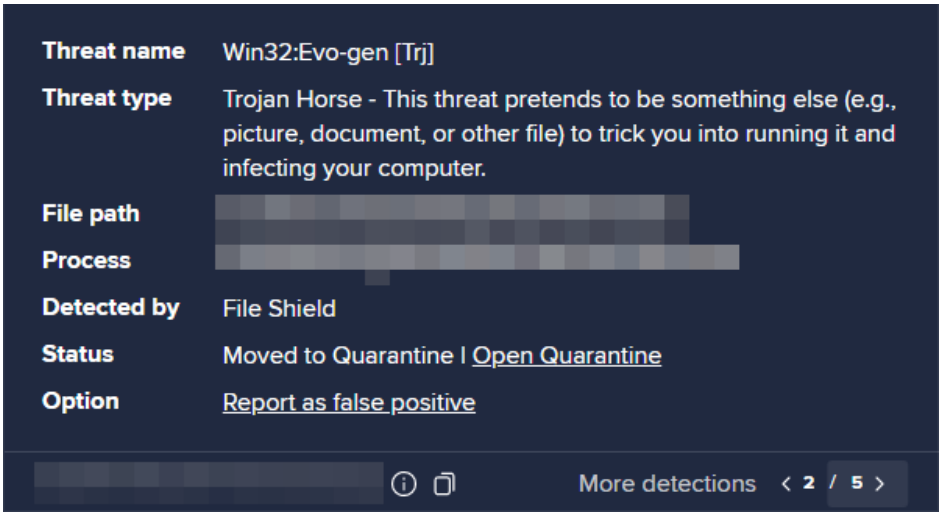
Clicking the three-dot button gives you the option to select *Ignore*. We do not recommend using this option, as it permanently deactivates the security status alert.

Malware detection alert

When a malicious file was detected in our functionality check, Avast displayed the alert shown below. We did not need to take any action. This alert window persisted until we closed it.



Clicking on *See details* displayed additional information about the threat, including a brief and simple definition of the threat type:



Whenever multiple malicious files were detected simultaneously, Avast showed a single alert. From there, we could browse through the various threats, view details, and close all alerts with a single click.

Scan options

The *Smart Scan* button on the home page checks for security vulnerabilities in the OS settings, runs a quick malware scan, and checks for so-called advanced issues. However, a premium license is required to resolve the advanced issues, and Avast prompts you to purchase a license every time when you attempt to resolve these. The *Protection\Virus Scans* page offers *Full, Targeted, Boot-Time,* and *Custom* scan options. A *Custom* scan can be scheduled on a daily, weekly or monthly basis. You can also scan a local drive, folder or file, or a network share, by using Windows Explorer's right-click menu.

Under *Menu\Settings\Protection\Virus Scans*, you can change the default action to be taken when malware is discovered, and whether to scan for potentially unwanted applications. PUA detection is enabled by default for on-demand scans and real-time protection. Scan exceptions can be configured on the *General* tab of the settings dialog.

Quarantine

Avast's quarantine feature can be accessed from the *Protection* tab. Here you can view a list of all quarantined files along with the threat name and date when it was found. You can select individual files, or all of them, and take one of the following actions: *Delete, Restore, Restore and add exception, Extract, Send for analysis*. The *Extract* function lets you restore the file to a custom location.

Logs

A log of completed scans can be found by clicking *Protection/Virus Scans/Scan History*. This shows the date of each scan, along with the detection name, file name/path, and action taken for each detection.

Help

The help feature can be accessed by clicking *Menu\Help\Help*. This opens the support page of the vendor's website, which lists common tasks such as installation, scanning, making exclusions, and uninstallation. For each task, simple step-by-step instructions along with multiple screenshots are provided.

Access control

Standard Windows User accounts have full access to the program's settings by default, and so can disable protection features. However, they cannot uninstall the program. If you share your computer, you might like to use the Password feature (under *Menu\Settings\General|Password)*. There are two options for doing this. The *Require password only to access settings* option locks the settings dialog. However, it is still possible to disable protection using the System Tray menu. The second option, *Require password to open Avast and access settings*, makes it impossible to access settings or disable protection by any means. However, it also locks any form of access to the main program window and the functionality of the System Tray menu. The only thing a user can do then is to run a right-click scan from Windows Explorer, though it will not be possible to see the scan results or take any action when malware is found.

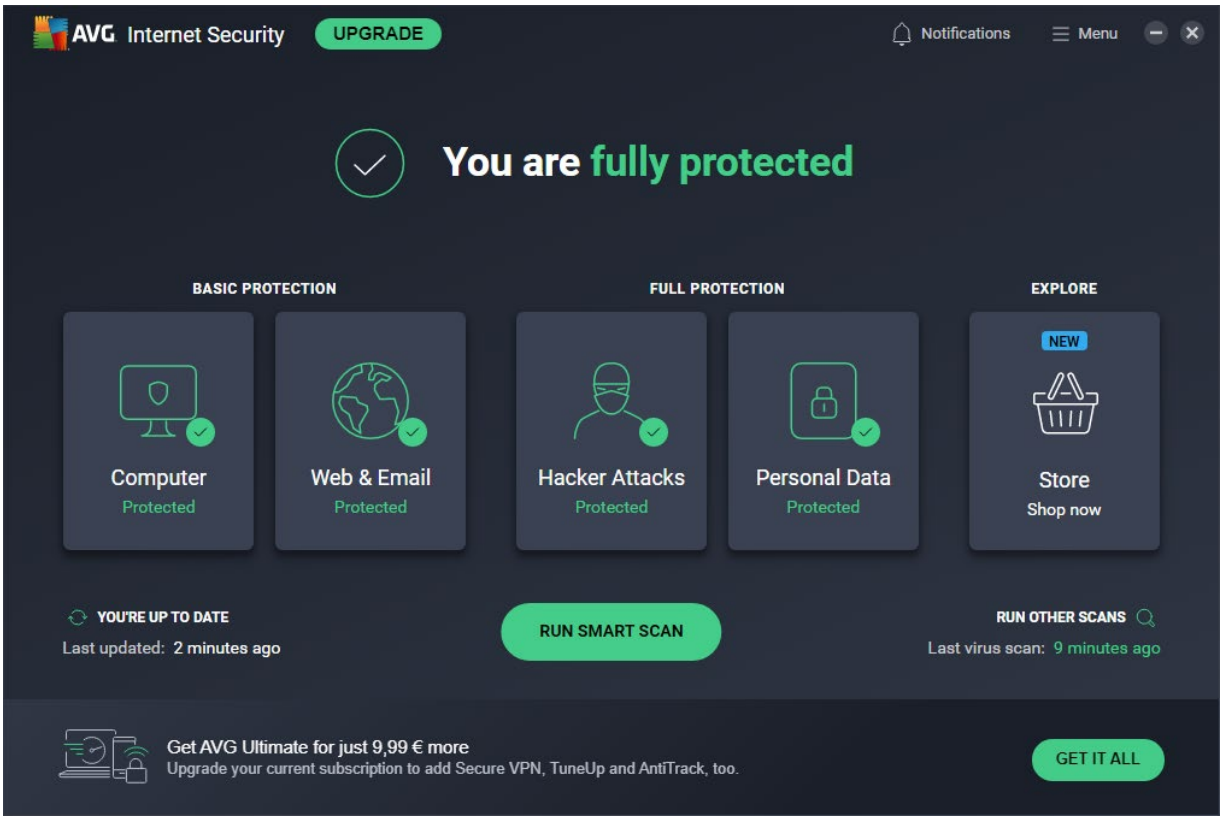
Advertising

The user interface of Avast Free Antivirus actively promotes the paid-for Premium Security product and other security products in various ways. Some people may find this a considerable irritation. In any event, we would suggest that users obtain independent advice on what other types of security/performance-related programs are appropriate to their needs before buying any additional products.

Other points of interest

- The *Rescue Disk* feature can be found on the *Protection\Virus Scans* page. This allows you to make a bootable CD/DVD/flash drive that you can use to scan and remove malware from an infected PC.
- While Avast Free Antivirus is a free product, we found the frequent prompts to fix issues that required a paid license to be quite intrusive.
- By default, Avast collects user data via 3rd-party analysis services. However, they inform us that this is only used in-house for e.g. product improvement purposes.

AVG Internet Security



About the program

AVG Internet Security is a paid-for security program. It offers anti-malware features, as well as a ransomware shield, and a secure delete function. You can find out more about the program on the vendor's website: https://www.avg.com/en-eu/internet-security#pc

Summary

AVG Internet Security features a modern and touch-friendly interface, which is straightforward to use. We liked the informative malware detection alerts, which let you manage multiple detections from a single alert window and persist until closed by the user. There is a good range of scan options, and on-access protection means that files are scanned for malware if you try to copy them to your PC.

Setup

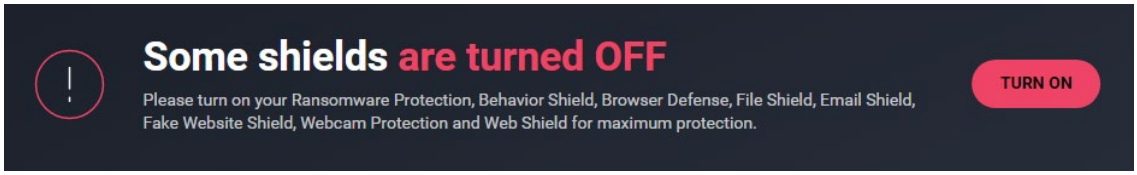
The setup wizard offers to install the *AVG Secure Browser* and set it as the default browser. However, you can easily opt out by removing the relevant ticks (checkmarks) on the first page of the setup wizard. We chose not to install the AVG browser for our functionality test. The setup wizard also lets you select the interface language, after which you can simply click *Install*. Power users customize the installation by selecting which individual components should be installed. We used the default configuration for our functionality test. After completing the setup, we were prompted to activate and register the product by signing in to the AVG account. We were also presented with an option to upgrade and renew the subscription, followed by a prompt to run a first scan.

System Tray icon

Hovering over the System Tray icon displays the protection status. Right clicking the icon lets you open the program, scan the computer, and disable protection.

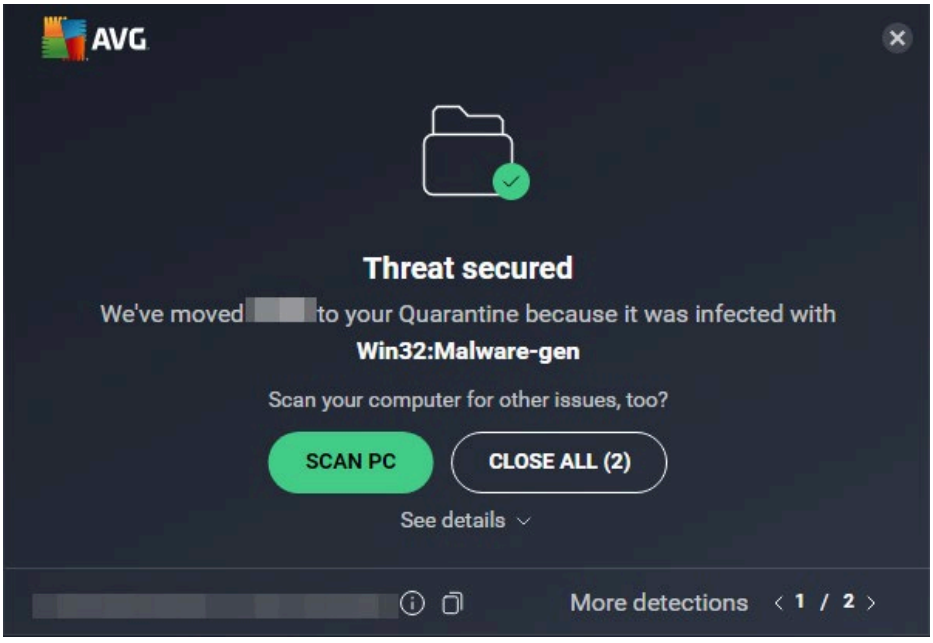
Security status alert

When we disabled protection features, we were prompted to confirm this action and to choose how long to disable protection. We appreciated that protection was automatically turned on afterwards. Additionally, an alert was shown on the status page (screenshot below) and *Computer* tile of the main program window. We were able to reactivate the protection easily by clicking *Turn on*.

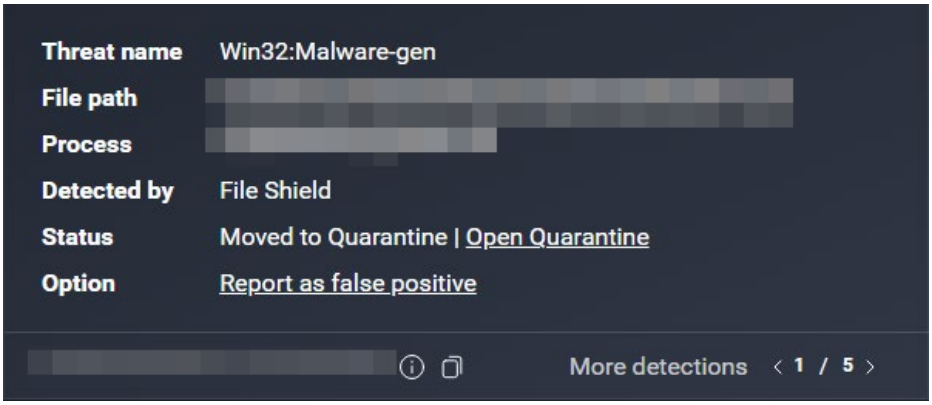


Malware detection alert

When a malicious file was detected in our functionality check, AVG blocked it and displayed the alert shown below. We did not need to take any action. The alert persisted until we closed it.



Clicking on *See details* displayed additional information about the threat:



Whenever multiple malicious files were detected simultaneously, AVG showed a single alert. From there, we could browse through the various threats, view details, and close all alerts with a single click.

Scan options

The *Smart Scan* button on the home page checks for security vulnerabilities in the OS settings, runs a quick malware scan, and checks for so-called advanced as well as performance issues. However, AVG prompts you to purchase the necessary AVG TuneUp subscription to resolve performance issues. Other scans can be run by clicking on *RUN OTHER SCANS* next to the *Run Smart Scan* button which offers options for a *Deep, File or Folder, Boot-Time, USB/DVD,* or *Performance* scan. *Scheduled* scans can be scheduled on a daily, weekly, or monthly basis. You can also scan a local drive, folder or file, or a network share, by using Windows Explorer's right-click menu.

Under *Menu**Settings**Basic protection**Detections*, you can change the default action to be taken when malware is discovered, and whether to scan for potentially unwanted applications. PUA detection is enabled by default for on-demand scans and real-time protection. Scan exceptions can be configured on the *General* tab of the settings dialog.

Quarantine

AVG's quarantine page can be accessed from the *Tools* section of the *Menu* but you have to scroll down to find it. It shows the file names and detection names of quarantined items, along with their location and date/time of detection. You can select individual files, or all of them, and take one of the following actions: *Delete, Restore, Restore and add exception, Extract, Send for analysis*. The *Extract* function lets you restore the file to a custom location.

Logs

Separate log files are created for each component of AVG Internet Security. The logs are stored under C:\ProgramData\AVG\Antivirus\report. Report generation can be toggled at the bottom of *Menu**Settings**Basic protection**Detections*.

Help

The help feature can be accessed by clicking *Menu**Help*. This opens the product's support page on the vendor's website. Here frequently asked questions, such as installation, uninstallation, scanning, and operating the quarantine function, are answered. Each topic provides simple, step-by-step instructions, along with well-illustrated screenshots.

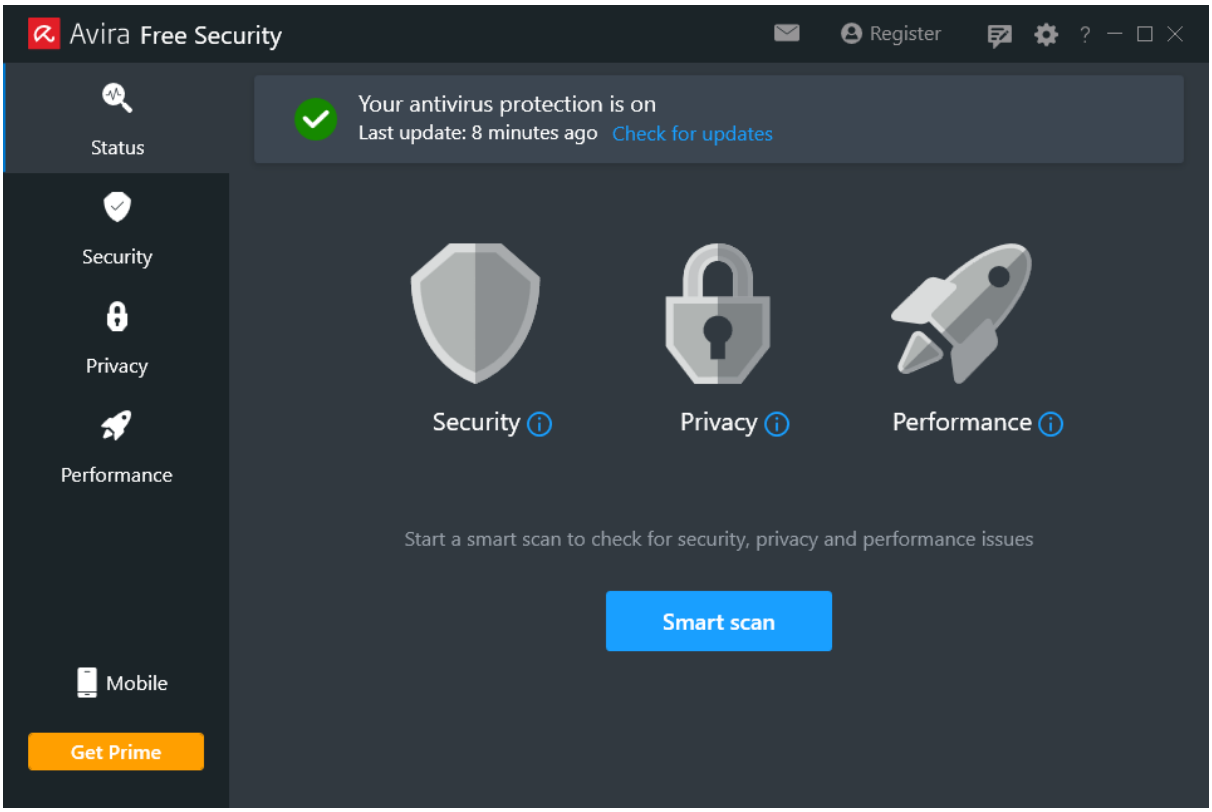
Access control

By default, Standard Windows User accounts can change settings and disable protection features, but not uninstall the program. If you share your computer, you might like to use the *Password* feature under *Settings**General*. If you choose the *Require password to open AVG and access settings* option, nobody will be able change any settings or disable protection without knowing the password. The program window will be completely inaccessible, and the only action unauthorised users can perform is a right-click scan from Windows Explorer. However, it will not be possible to view the scan results. The *Require password only to access settings* option locks the settings dialog, but all users can still disable protection from the System Tray menu, or the *Computer* tile on the home page.

Other points of interest

- Despite being a paid product, AVG Internet Security frequently prompts you to upgrade the license.
- AVG Internet Security includes a *Fake Website Shield* which warns you about fake websites.

Avira Free Security



About the program

Avira Free Security is the free version of Avira's paid-for security program Avira Prime. It includes an antivirus component, a VPN (limited to 500 MB/month), Password Manager, and Update scanner. You can find out more about Avira Free Security on the vendor's website: https://www.avira.com/en/free-antivirus-windows

Summary

Installing Avira Free Security is very straightforward, and the program's simple interface is easy to navigate, offering the choice between light and dark modes. Safe default settings and sensible alerts are provided.

Setup

To set up Avira Free Security, download and launch the installer from the vendor's website. The setup wizard requires only one click to complete. Once finished, the installer prompts you to run a *Smart Scan*.

System Tray icon

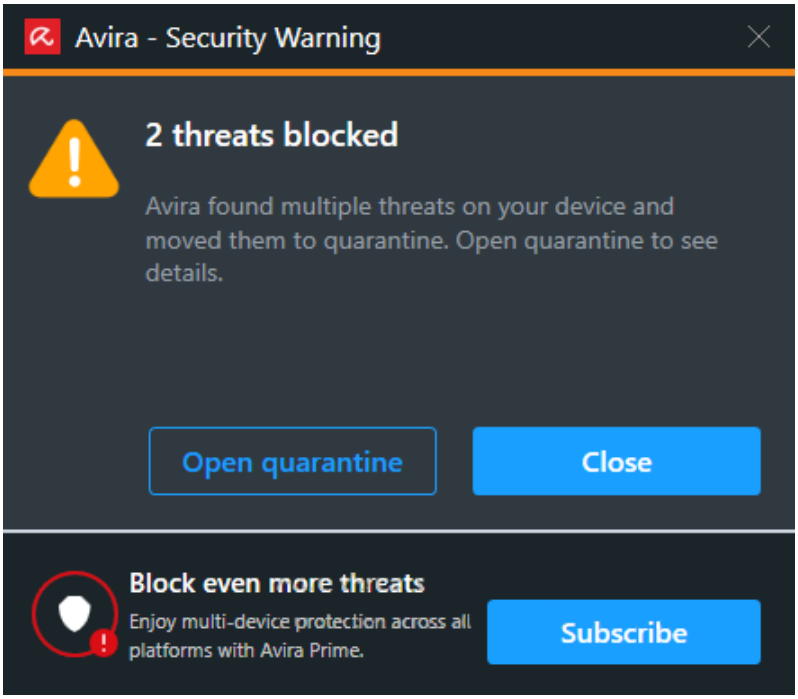
The System Tray icon menu lets you open the program window, run scans and updates, enable/disable real-time protection, and activate the VPN.

Security status alert

When we disabled real-time protection in the program's *Security* tab, an alert was shown on the program's home page. We were able to reactivate the protection easily by clicking *Turn on*.

Malware detection alert

When a malicious files were detected in our functionality check, Avira displayed a single message box, shown below. We did not need to take any action. The alert persisted until we closed it.



Clicking on *Open quarantine*, opened the *Security\Quarantine* page in Avira's main program window.

Scan options

You can run a *Smart Scan* by clicking the button on the program's home page. This scan takes about a minute and checks for privacy and performance issues, viruses, outdated apps, and network threats. Under *Security\Virus Scans,* you can choose between quick and full scans, both of which can be scheduled. There is also an option to create custom scans. You can additionally scan a local drive, folder or file, by using Windows Explorer's right-click menu. Under *Settings\Security\Virus scans,* you can define, which file types and archives should be scanned, and set scan exclusions. Similar extensive options for real-time and web protection are also available under *Protection options*.

Quarantine

The Quarantine can be accessed from the *Security* page. It displays the threat name, file name and path, as well as the date and time of detection. Quarantined files can be selected individually or all together to restore or delete them.

Logs

You can view a record of all scans performed in the past 24 hours under *Security\Virus scans*.

Help

Clicking *Help* under the *?* menu opens Avira's online manuals page. It contains searchable FAQs grouped by different categories, offering simple text instructions along with screenshots and videos for the features of Avira Prime. The support can also be contacted from the *?* menu.

Access control

Standard Windows User accounts cannot disable protection features, change settings, or uninstall the program, which is ideal in our opinion.

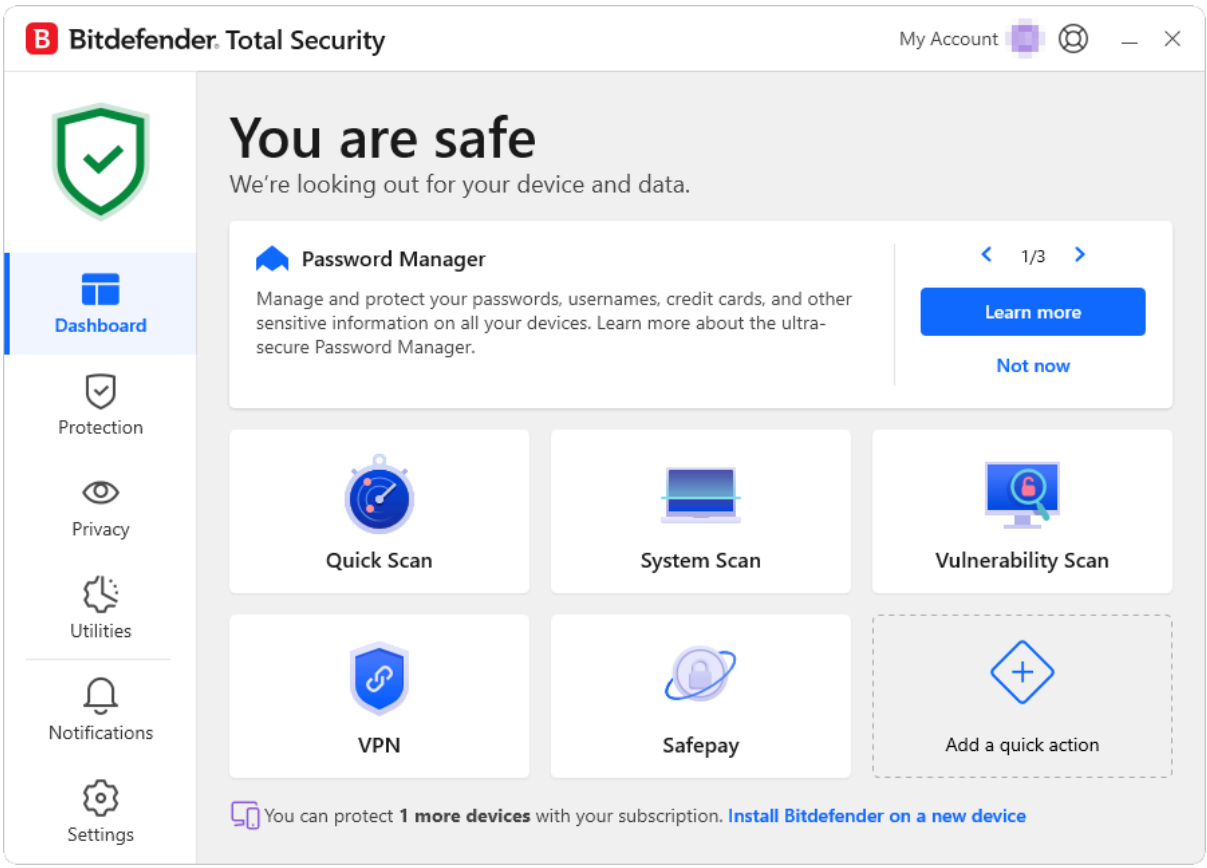
Advertising

The user interface of Avira Free Security actively promotes the paid-for product and other related security products in various ways. Some people may find this a considerable irritation. In any event, we would suggest that users obtain independent advice on what other types of security/performance-related programs are appropriate to their needs before buying any additional products.

Other points of interest:

- The included VPN is limited to 500 MB/month. This might be ok for occasional use but not for continues usage since a single software update can quickly use this up.
- Avira Free Security offers a light and dark mode for its program interface, which can be toggled in the settings under *General\Language & Appearance*.

Bitdefender Total Security



About the program

Bitdefender Total Security is a paid-for security program. In addition to anti-malware features, it includes a replacement firewall, vulnerability scanner, antispam, ransomware remediation, parental controls, file shredder (secure deletion), and a limited VPN. You can find out more about the program on the vendor's website: https://www.bitdefender.com/en-us/consumer/total-security

Summary

Bitdefender Total Security is straightforward to install, easy to navigate, and provides good scan options. We liked the option to customise the six tiles on the home page. However, ads for special offers are displayed which we believe should not be present in a paid product.

Setup

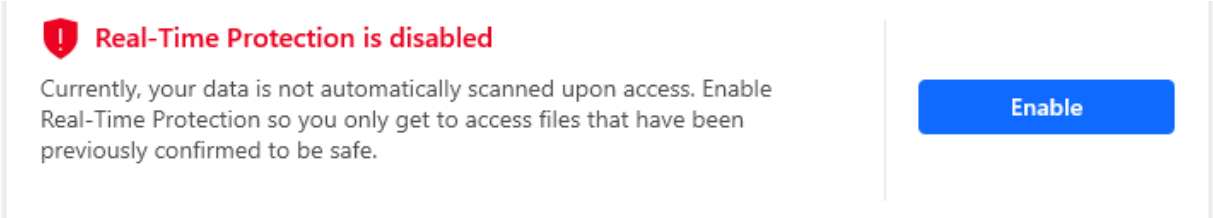
The installation is very straightforward by downloading and open the installer from Bitdefender Central. During setup, you must accept the Subscription Agreement and have the option of sending product reports. At the end, an optional "Device Assessment" is suggested. When launching Bitdefender Internet Security for the first time, a brief but skippable tour of the product's main features is displayed.

System Tray icon

The System Tray icon menu lets you open the program window, see program information, run updates, and show/hide the security widget.

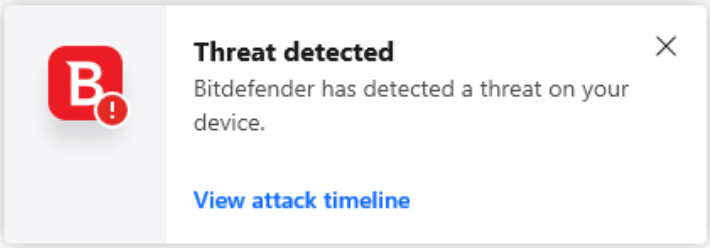
Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). We were able to reactivate the protection easily by clicking *Enable*.

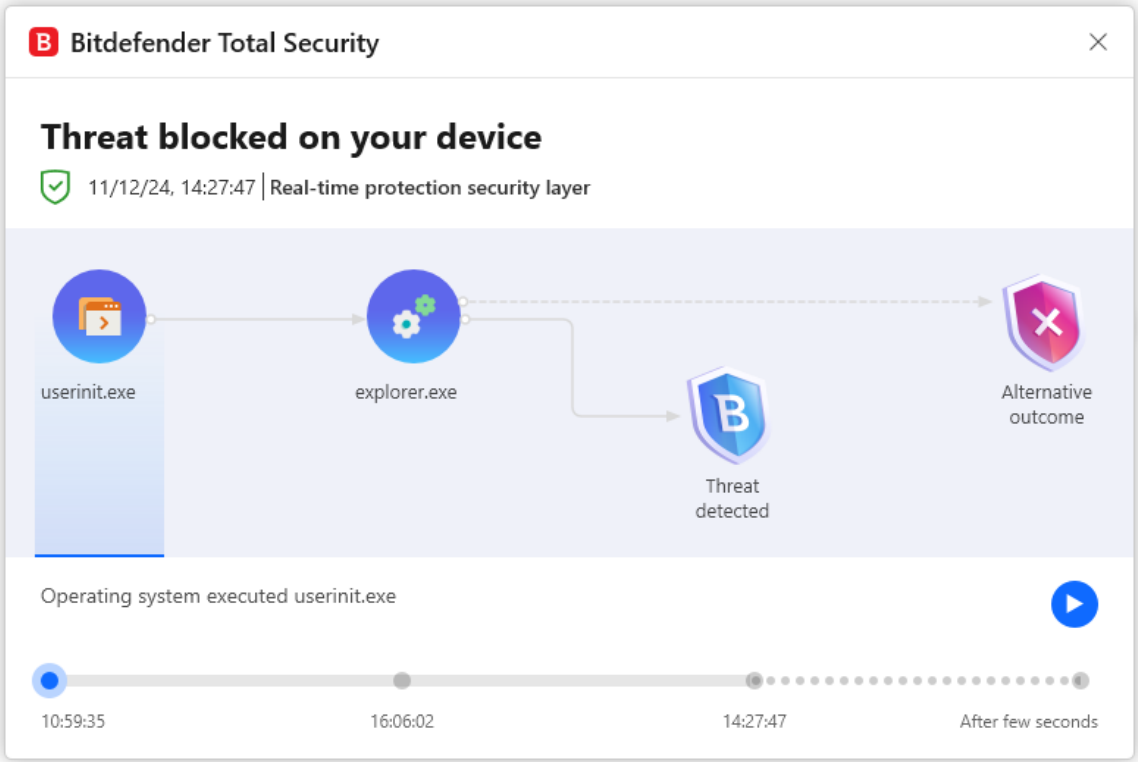


Malware detection alert

After detecting malicious files, Bitdefender displayed the alert shown below. We did not need to take any action. The alert persisted until we closed it.



When we clicked *View attack timeline,* the following window opened, showing a timeline of the Windows processes involved in the detection. This valuable tool could help advanced users investigate behaviours and actions of malicious programs.



When multiple malicious files were detected simultaneously, only one alert was shown.

Scan options

The *Dashboard* page lets you run a *Quick Scan*, *System* Scan, and a *Vulnerability Scan*. Under *Protection\Antivirus\Scans,* you can also set up a *Custom Scan*. This scan can be scheduled and offers various customization options, including whether to scan for potentially unwanted applications, the scan location, memory scanning, whether only new and modified files should be scanned, and more. Scan exceptions can be configured on the *Settings* tab of the *Antivirus* page, where you can also access the quarantine and set up (automatic) scanning of USB drives, optical media, and network drives. Additionally, you can scan a local drive, folder or file, or a network share, by using Windows Explorer's right-click menu.

Quarantine

The *Quarantine* page can be found under *Protection\Antivirus\Settings*, although we feel this is not the most intuitive location and could be made easier to find. It displays the file name and path, detection name, and time/date each item was quarantined. Items can be selected individually or all at once, and then be deleted or restored.

Logs

Logs can be found on the *Notifications* page, displaying all events that occurred. Clicking on individual notifications provides more details. For scan notifications, you can view the full log with details about the type of scan and the scan options.

Help

Clicking the lifebelt icon in the top right-hand corner of the window opens the help centre where you can find links to the *User Guide*, *Support Center*, and *Bitdefender Community*. The *User Guide* is a very comprehensive manual of almost 300 pages, covering all aspects of installing, configuring and using the program. There is a glossary of relevant technical terms and contact details for Bitdefender's support services. The *Support Center* is an online, searchable FAQ page that includes detailed instructions, illustrated with screenshots and video tutorials.

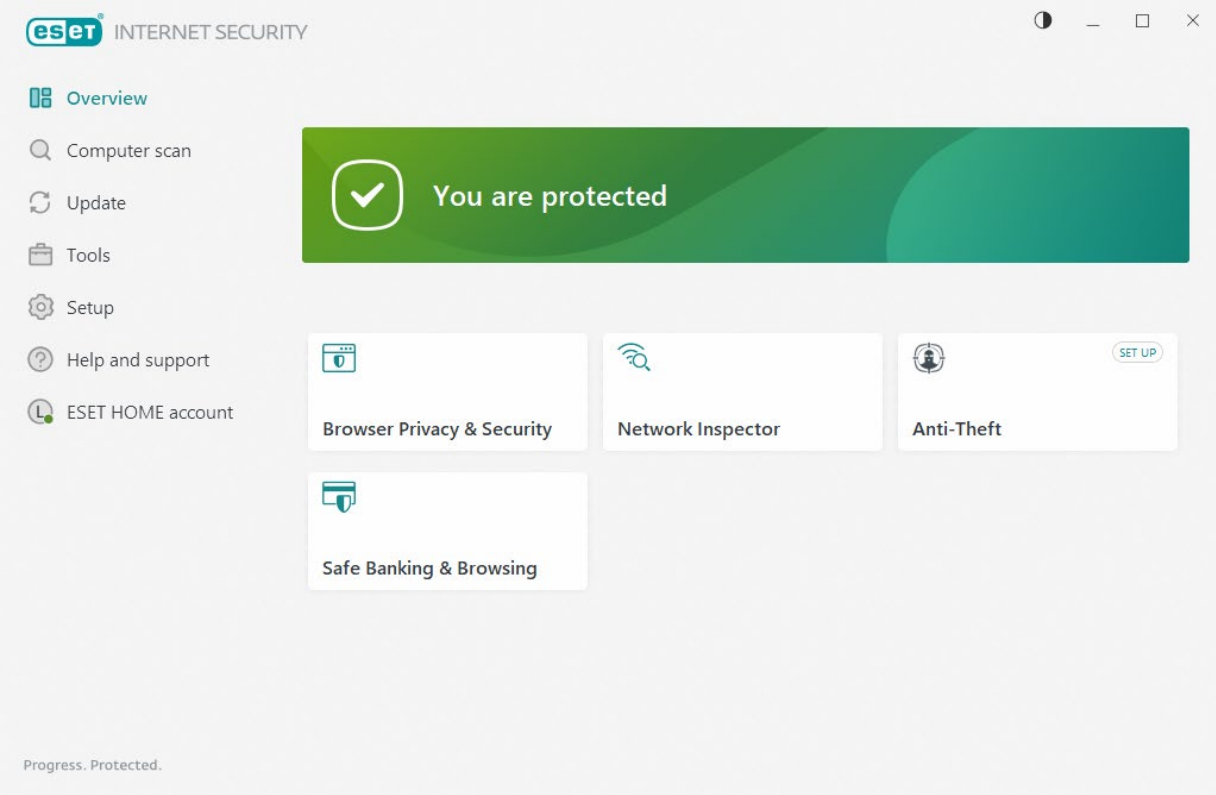
Access control

Standard Windows users cannot disable protection features or uninstall the program, which is ideal in our opinion. You can also password-protect the settings, preventing other users from disabling protection without entering the password.

Other points of interest:

- You can customise which tiles are shown on the *Dashboard* (home page).
- The tool Bitdefender File Shredder, included in the program, claims to permanently delete files without leaving a trace on the hard drive.

ESET HOME Security Essential



About the program

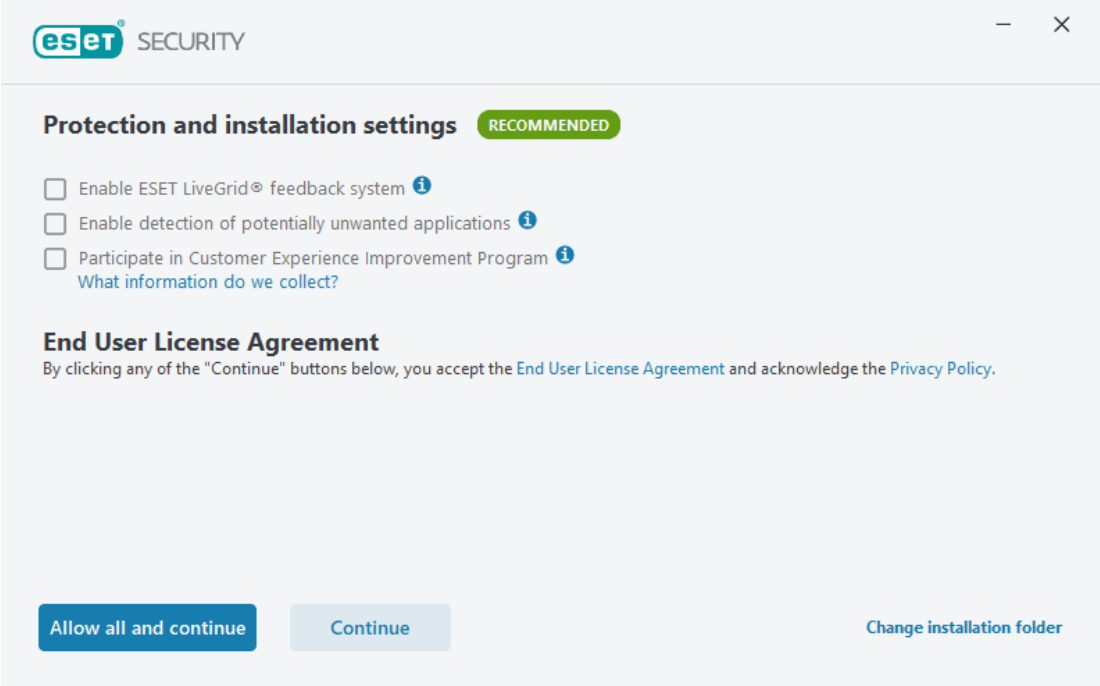
ESET HOME Security Essential is a paid-for security program. In addition to anti-malware features, it includes several other features, such as the ESET Firewall, Network Inspector, Anti-Theft, Safe Browsing, and Banking & Payment Protection. You can find out more on the vendor's website: https://www.eset.com/int/home/protection-plans/

Summary

ESET HOME Security Essential is a well-designed and easy-to-use security product. It provides safe default settings and a clean, intuitive interface for non-expert users, with essential features easily accessible. The settings dialog has plenty of advanced options for power users, while the help features and access-control options are excellent.

Setup

After downloading the personalized installer from the ESET HOME portal, the first page of the installation wizard lets you choose the interface language and provides helpful links to installation instructions and the user guide. In the next step, you can enable *LiveGrid* (data sharing), PUA detection, and the *Customer Experience Improvement Program*. Here, the button layout can be confusing: the dark blue *Allow all and continue* button suggests it must be selected. However, you can also click *Continue* instead, which will only accept the license agreement and proceed with the installation. You can also change the installation folder at this point.



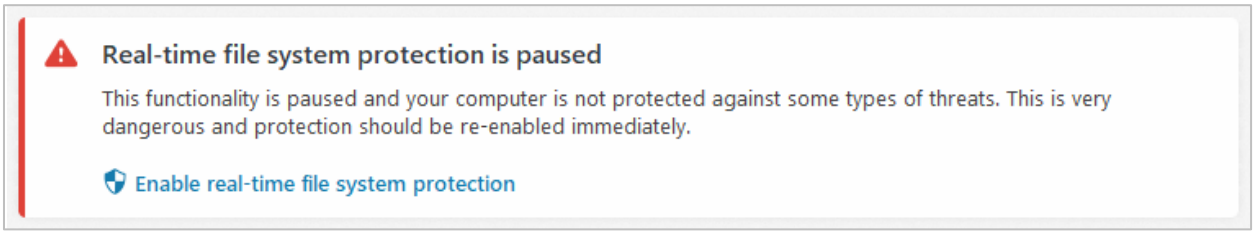
Next, you can set a device name to easily recognize it in ESET HOME. After that, you are logged in and you can review the activation details before the program is installed. Upon first launch, ESET HOME Security Essential provides a brief product and starts an initial scan of the computer. Depending on the device's specifications, this may take some time but can be stopped. Next, the computer must be connected to an ESET HOME online management account. The browser extension *ESET Browser Privacy & Security* is automatically installed as well.

System Tray icon

The System Tray icon menu lets you view the protection status, pause protection and firewall, block all network traffic, open settings, view log files, open the program window, view program information, and check for updates.

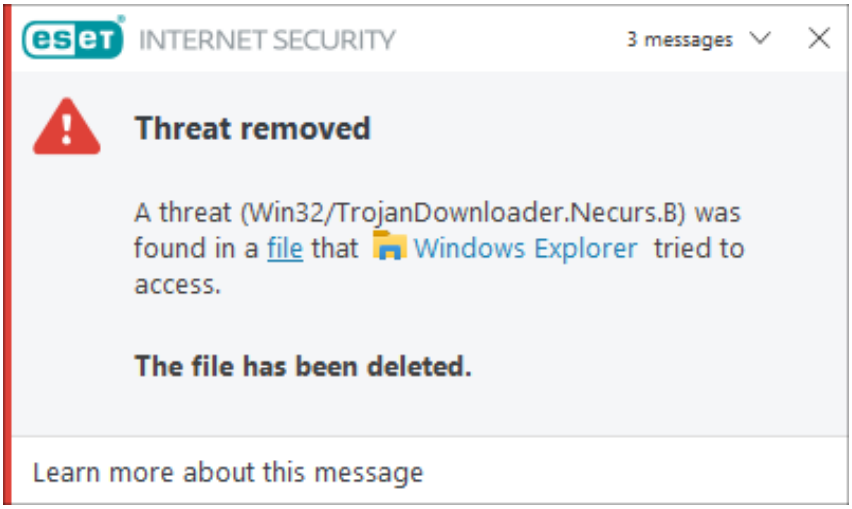
Security status alert

When we disabled real-time protection, an alert was shown on the home page (screenshot below) along with a Windows notification. We were able to reactivate the protection easily by clicking *Enable real-time file system protection*.



Malware detection alert

When a malicious file was detected in our functionality check, ESET displayed the alert shown below. We did not need to take any action. The alert was closed after 10 seconds.



When multiple malicious files were detected simultaneously, ESET displayed a single alert. This enables you to view threats one by one using the *X* button or close all messages at once using the drop-down menu in the top right-hand corner.

Scan options

The *Computer scan* page lets you start a full system scan, drag and drop files for scanning, or start an advanced scan. The later allows you to create a custom scan, scan removable media scan, or repeat the last scan. The custom scan provides very granular options, including scanning operating memory, boot sectors/UEFI, WMI database, and registry. You can also scan files and folders via Windows File Explorer's right-click menu. Scanning for potentially unwanted (e.g., browser toolbars, trackware), potentially unsafe (e.g., hacker tools), and suspicious applications (e.g., those using typical malware obfuscation packing) can be enabled in *Setup|Advanced Setup|Protections*. Scan exceptions can be configured under *Advanced Setup\Detection engine\Exclusions*.

Quarantine

The *Quarantine* page can be found under the *Tools* menu. For each detection, the date and time of detection, file name and path, file size, detection name, number of occurrences, the name of the active user, and the SHA-1 file hash are shown. Multiple quarantined files can only be selected by using keyboard shortcuts, which may not be intuitive to casual users. Similarly, there is no direct way to empty the quarantine as selected files can only be deleted and restored from quarantine by right-clicking.

Logs

The *Logs* page is also available under the *Tools* menu. It lists records of detections, events (such as updates), and scan results, along with events related to other program features, such as anti-spam and parental control.

Help

The *Help and support* page shows information about the license and the installed product and includes links to *Help page, Knowledgebase*, and *Technical Support*. Clicking *Help page* opens an online manual, where you can browse and search for different topics. In addition, a question mark icon displayed on most pages of the program interface directly links to the relevant online help page, eliminating the need to search manually for specific topics. Each help page consists of detailed explanations, instructions, and annotated screenshots.

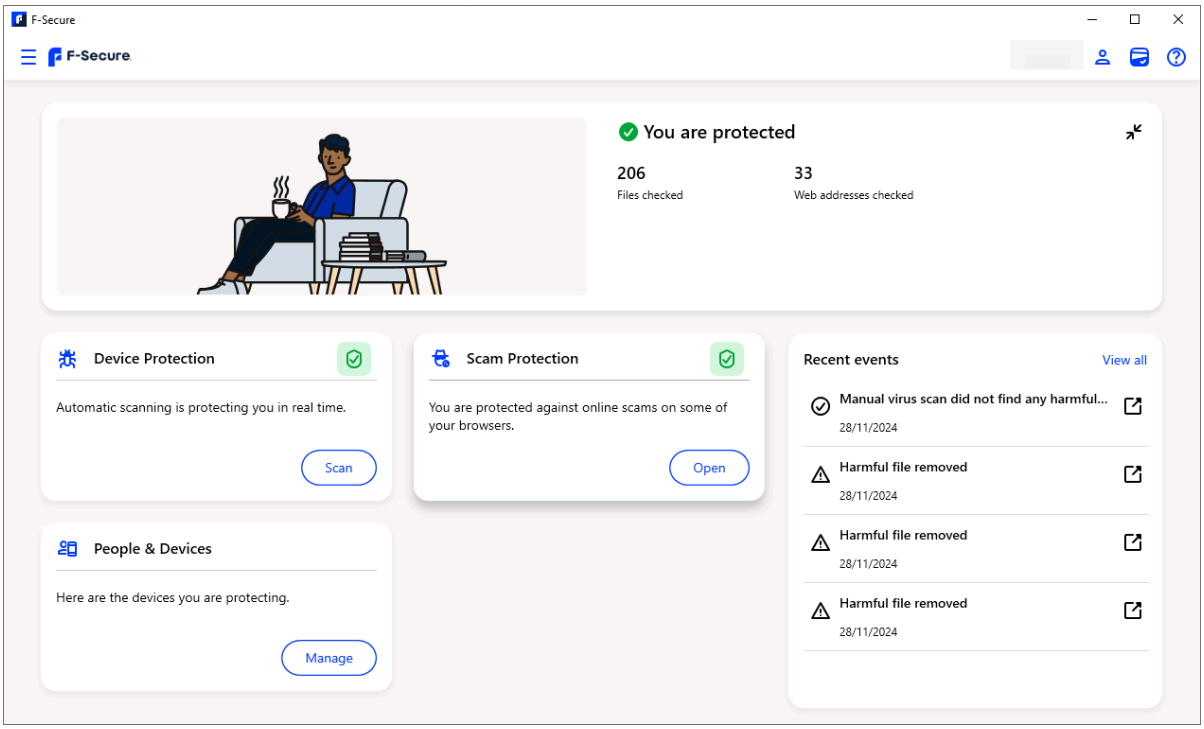
Access control

Standard Windows User accounts cannot disable protection features or uninstall the program, which is ideal in our opinion. Additionally, you can password-protect the settings (*Setup\Advanced setup\User interface\Access setup*), allowing all users (including administrators) to use all program features while preventing them from changing settings or disabling protection.

Other points of interest

- The advanced setup includes a search bar which you can use to quickly find settings you want to change.
- Under *Tools\More tools*, ESET provides several system utilities for advanced users, such as *Running processes*, *Security report*, *Network connections*, and *System cleaner,* which could be useful for investigating suspicious behaviour on your system.

F-Secure Internet Security



About the program

F-Secure Internet Security is a paid-for security program with a sleek and visually pleasing design, which gives you quick access to all the features. It includes anti-malware and secure browsing features. There are browser extensions for browsing and banking protection available, as well as an ad blocker (which were not part of the functionality check). You can find out more about the program on the vendor's website: https://www.f-secure.com/en/internet-security

Summary

Installing F-Secure Internet Security is very straightforward, and the program's simple interface is easy to navigate and offers helpful explanations of all features.

Setup

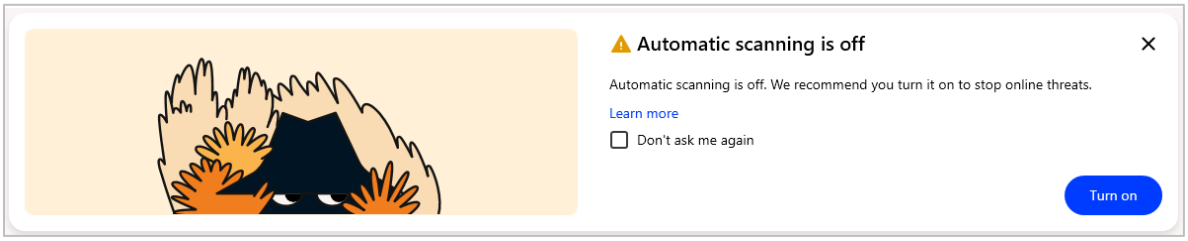
When downloading the installer, you have to select whether you are installing the program on your own device, you child's device, or the device of someone else (for this review we selected *My Device*). The installer allows you to choose the language for the installer, and you can opt-in sending usage data. There are no further steps necessary and F-Secure launches automatically when the installation is finished. At this point, you can again select who you want to set up the program for.

System Tray icon

The system tray icon can be used to open the program, check for updates, open the settings, and view recent events and program information.

Security status alert

When we disabled protection features in the settings, an alert was shown on the home page (screenshot below) along with a Windows pop-up alert. We were able to reactivate all protection easily by clicking *Turn on*.



Malware detection alert

When we opened a folder containing malicious files in our functionality check, F-Secure immediately quarantined all files and displayed the alert shown below. We did not need to take any action. The alert disappeared after 5 seconds.

When multiple malicious files were detected simultaneously, F-Secure displayed an alert for each of them. Clicking on the alert opened the event history.

Scan options

Clicking the *Scan* button on the home page runs a quick scan of the file system. By opening *Device Protection**Virus Scan* you can also run a full computer scan. Under *Settings**Scanning settings*, you can set up scheduled scans.

Quarantine

The quarantine is found under the *Device Protection* section of the settings; administrator privileges are needed to open this window. Here, you can view quarantined, blocked, excluded, and protected (from ransomware) files, folders and programs. The quarantine shows the date and time of detection, the file name, and the infection name. Clicking on the latter opens a threat description on F-Secure's website. Clicking on an item reveals the original file path, and allows you to set an exception, delete the file permanently, or report it as a false positive. Multiple quarantined files can only be selected by using keyboard shortcuts, which may not be intuitive to casual users.

Logs

Recent events are displayed on the program's home page, and respectively in the sections *Device Protection* and *Scam Protection*. Here, you can click on *View all* to show all applicable events that have taken place. Administrator rights are needed to clear or show all events.

Help

Clicking the ? button on the home page allows you to open the product help; unlike most other products reviewed, the help feature is built into the program and therefore available offline. Clicking the *?* symbol elsewhere in the app opens the help page specific to the feature currently viewed. The help pages are mostly text-based, supplemented with occasional images of certain buttons.

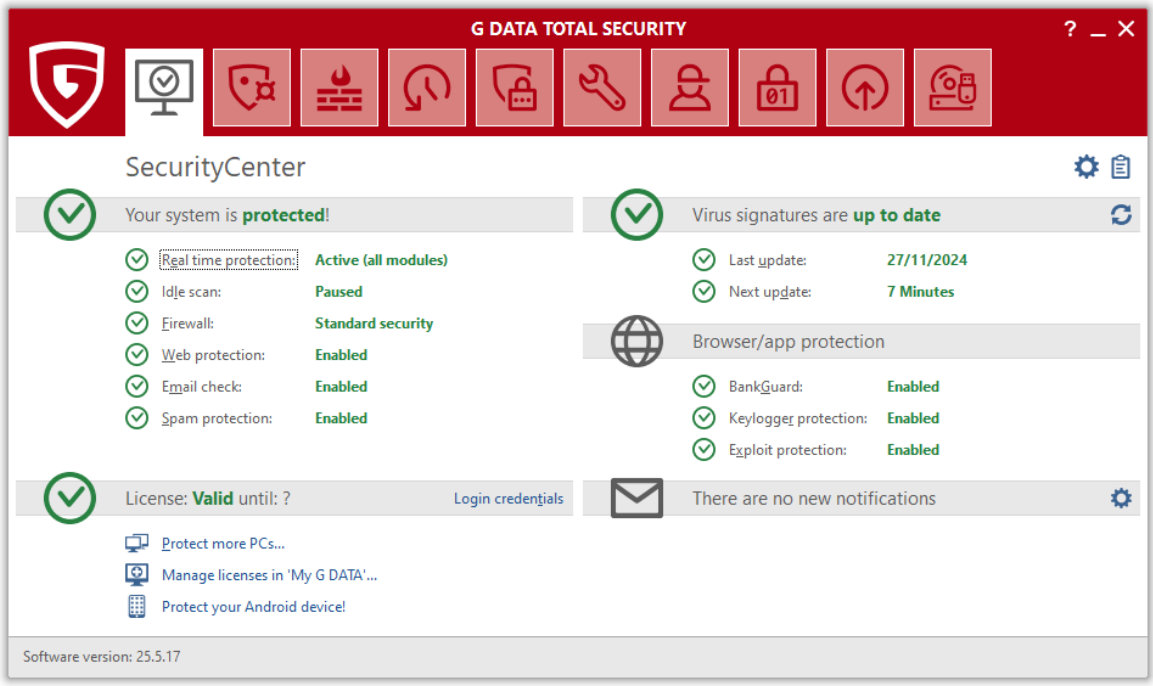
Access control

Standard Windows User accounts cannot disable protection features or uninstall the program, which is ideal in our opinion. Additionally, editing most settings requires you to open the configuration page with administrator privileges. This extra step might be frustrating when frequently changing settings, but also prevents accidental changes.

Other points of interest

- When opening a feature for the first time, you are shown a brief description of what it does.
- If you have a license for multiple users and devices, you can see the protection status of the other users in the *People & Devices* section.

G Data Total Security



About the program

In addition to anti-malware features, G Data Total Security includes anti-spam and anti-phishing components, a replacement firewall, backup function, encryption manager, password manager, device control, performance tuner, and parental controls. You can find out more about the program on the vendor's website: https://www.gdatasoftware.com/total-security

Summary

The interface of G Data Total Security is easy to navigate by a single row of tiles. Users can choose between a default or customised installation, with the latter allowing selection of individual components to install. The status display provides detailed information about each protection component, and access control is excellent.

Setup

The setup wizard starts by prompting you to select the interface language. Users can then choose between *Standard* or *User-Defined Installation, w*ith the latter allowing the selection of optional components, such as anti-spam and parental controls, and the option to change the installation folder. For our functionality test, we used *Standard Installation*. Upon completion, you can activate the full license using a registration key or login credentials, or opt for the 30-day trial. A system restart is required to finalize the installation.

System Tray icon

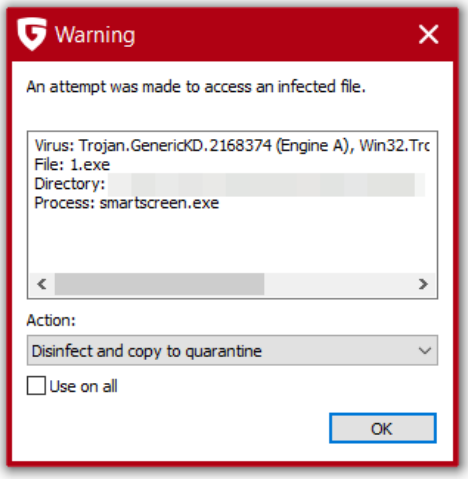
The System Tray icon menu lets you open the program window, disable malware, the G Data firewall, and *Autopilot*, as well as run updates and view protection statistics.

Security status alert

When we disabled real-time protection in the program's settings, G Data displayed an alert in the program window (screenshot below). We were able to reactivate protection by clicking *Real time protection\Enable virus monitor*.

Malware detection alert

When a malicious file was detected in our functionality check, G Data displayed the alert shown below. With a click on *OK*, the malware was disinfected and quarantined. Other actions to take are *Block file access*, *Move to Quarantine*, and *Delete*. The alert turned slightly transparent after a few second but persisted until we closed it.



When multiple malicious files were detected simultaneously, G Data displayed a separate alert for each one. However, selecting the *Use on all* checkbox allowed the same action to be applied to all malware detections without showing further alerts.

Scan options

The *Virus protection* page (second icon from left on the top toolbar) provides different scan options: *Check computer (all local drives); Scheduled virus checks; Check memory and Autostart; Check directories and files; Check removeable media; Check for rootkits*. You can also scan a local drive, folder or file, or network share, using Windows File Explorer's right-click menu. Scan options in the *Anti-Virus* section of the *Settings* dialog let you choose the used protection components (all are on by default). You can also decide whether to detect potentially unwanted programs (on by default). Exceptions for both real-time protection and on-demand scans can be set here too.

Quarantine

The quarantine function can be opened from the *Anti-Virus* page which shows the date and time of detection, threat name, file name, and file path. You can disinfect, delete, or restore individual files or use standard Windows keyboard shortcuts to select multiple items, which may not be intuitive to casual users.

Logs

Logs can be opened from the clipboard icon in the top right-hand corner of the window. You can view details of scans, detections and signature updates. Clicking on an item reveals a details pane below with applicable information about the event in question, such as program and signature versions, protection components used, and areas scanned. You can view all logs or filter them by *Updates, Real-Time Protection, Virus Scans,* or *Web & Mail*.

Help

G Data 's online help pages can be opened by clicking the question-mark icon in the top right-hand corner of the window or pressing F1. This opens the online documentation for the G Data Security Center which lists several categories, such as *Overarching Features, Real-time protection, Idle scan*, or *Firewall* among others. For each item, there is a very detailed page of instructions and explanations, illustrated with screenshots.

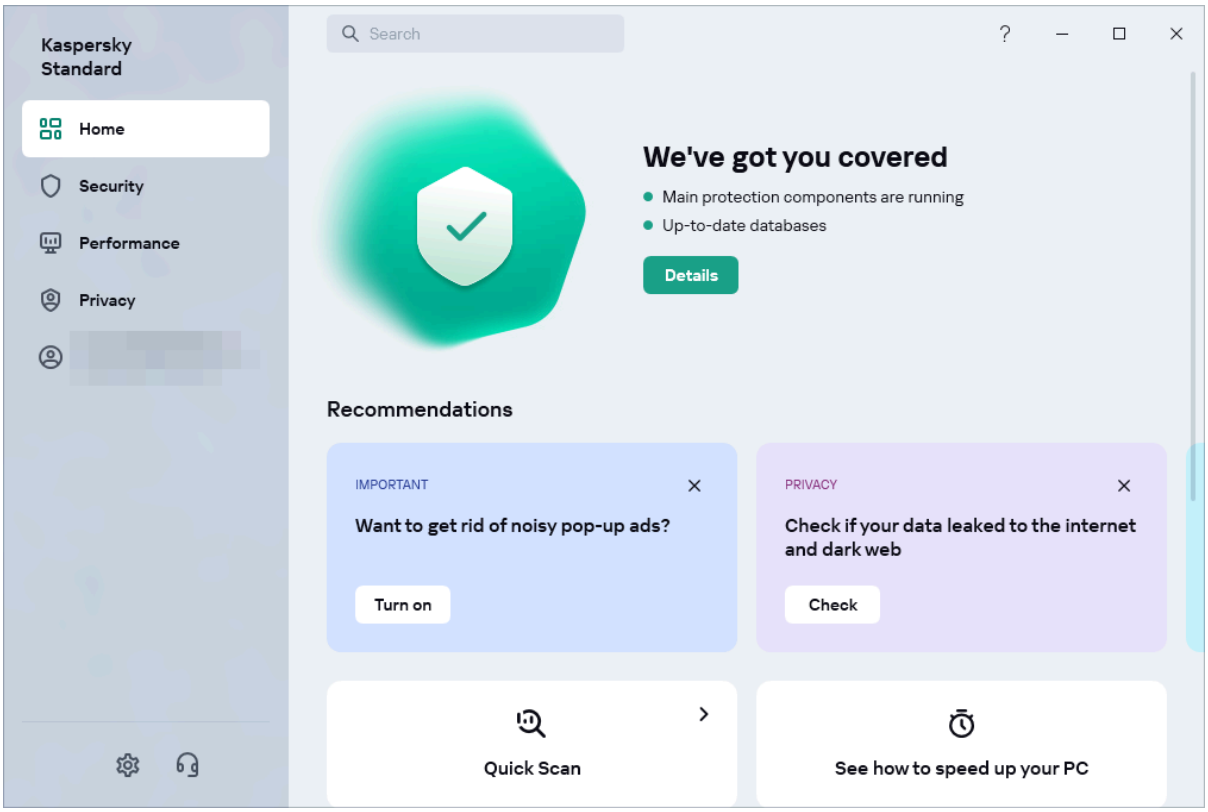
Access control

Standard Windows User accounts cannot disable protection features or uninstall the program, which we regard as ideal. You can also password protect the settings to prevent any other users changing them.

Other points of interest

- After installation, we were prompted to install the G Data browser extension for Google Chrome.
- On the *Virus protection* page, under *Boot medium*, you can create a bootable CD/DVD/USB drive to scan a PC without starting the operating system.

Kaspersky Standard



About the program

Kaspersky Standard is a paid-for security program that includes various anti-malware functions as well as other features, such as vulnerability scanner, software updater, ransomware protection, added protection for banking and financial websites, webcam protection, and browser privacy. You can find out more about the product on the vendor's website: https://kaspersky.com/standard

Summary

The installation of Kaspersky Standard is straightforward, using safe default options. The program's modern, tiled interface makes all essential features easily accessible from the home page. Advanced users will find a wide range of configuration options under the settings.

Setup

The entire setup process is very smooth and intuitive. At the beginning, new program features introduced in the latest version are shown by clicking on *About this version*. During installation, you can opt out of data processing for marketing purposes and the *Kaspersky Security Network* (both of which are on by default). Upon completion, you must accept the EULA and activate your subscription. You are then prompted to run a scan in the background and introduced to the program features. The program also prompts you to turn on the Kaspersky browser extension for Google Chrome.

System Tray icon

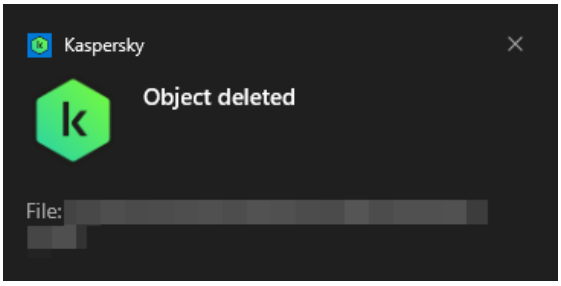
The System Tray icon menu lets you open the program, pause/resume protection, open settings, turn on *Do not Disturb Mode* and *Gaming Mode*, view the support page and program information, or exit the program.

Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below) along with a Windows pop-up alert. We were able to reactivate the protection easily by clicking *Details* and *Turn on*.

Malware detection alert

When a malicious file was detected in our functionality check, Kaspersky displayed the message shown below. We did not need to take any action. The alert closed after 5 seconds.



Clicking on the alert opened the logs page with additional information about the detection. When multiple malicious files were detected simultaneously, Kaspersky displayed one alert for each detection.

Scan options

Clicking the arrow on the *Quick Scan* tile on the program's home page or on *Security\Choose scan* opens the *Scan* page. From there, you can run a *Quick Scan*, *Full* Scan, *Selective Scan*, *Removable Drive Scan*, or *Application Vulnerability Scan*. All these scan options can be scheduled by clicking the cogwheel icon next to the scan. A local drive, folder or file, or a network share can be scanned from Windows Explorer's right-click menu. Exclusions can be managed by going to *Settings\Security Settings* and *Exclusions and actions on object detection* at the very bottom of the page. You can specify which protection components, such as e.g. real-time protection or on-demand scans, the exclusion should be applied to. The detection of *Adware* and *Auto-dialers* is activated by default and cannot be disabled. The option to detect other PUA (*Unwanted App Installation Blocker*) is switched on in the Privacy section.

Quarantine

The quarantine feature can be found by opening *Security\Quarantine*. It shows the file name and path, detection name, date/time of detection, and the action taken. You can select individual files or all at once. Files can be deleted or restored, and you can open the folder where the file was detected.

Logs

The log function is available at *Security\Reports*. A wide variety of reports is provided, including individual reports for different protection components, such as *File Anti-Virus, Web Anti-Virus*, and *Firewall,* and additional features, such as *Anti-Spam* and *Software Updater*. The reports can be filtered by time and importance.

Help

The ? symbol in the top right-hand corner of the window opens Kaspersky's online manual for the current program page. Straightforward and text-only instructions of each feature are provided. You can easily navigate to other topics using the menu on the left-hand side.

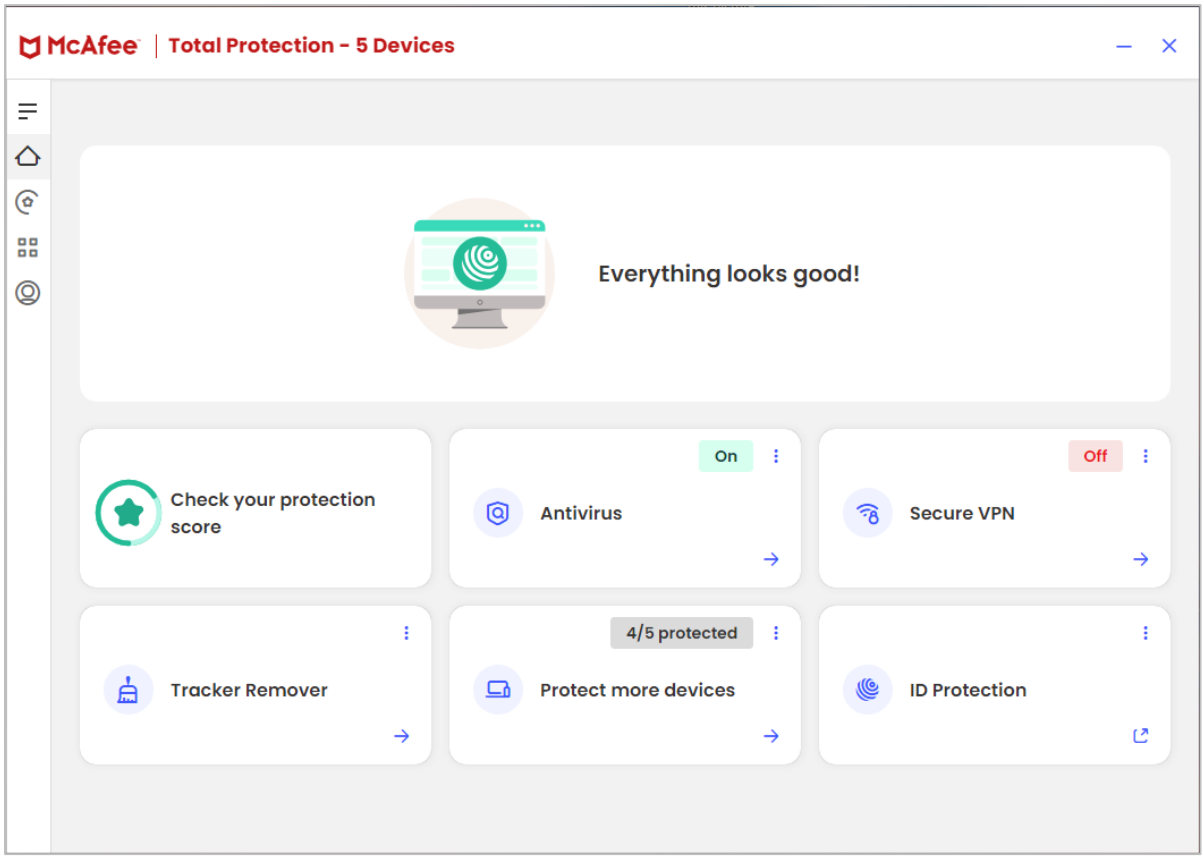
Access control

Standard Windows User accounts have full control of the program's settings and can disable protection features. However, only users with administrator accounts can uninstall the program. You can password protect the program which allows you to create users with different access levels for the settings.

Other points of interest

- The search bar at the top of the program window can be used to find features and settings.
- The Security\Weak Settings Scan can search for settings that might put your device at risk.
- There are several options available to improve system performance in the *Performance* section. They were not part of our functionality check.

McAfee Total Protection



About the program

McAfee Total Protection is a paid-for security program. In addition to anti-malware features, it offers a VPN, password manager, replacement firewall, tracker remover, and secure file-deletion feature. You can find out more about McAfee Total Protection on the vendor's website: https://www.mcafee.com/en-us/antivirus/mcafee-total-protection.html

Summary

McAfee Total Protection is very simple to install, and has a modern, touch-friendly interface. All essential functions can be accessed via tiles on the home screen, and the malware alerts are clear and persistent.

Setup

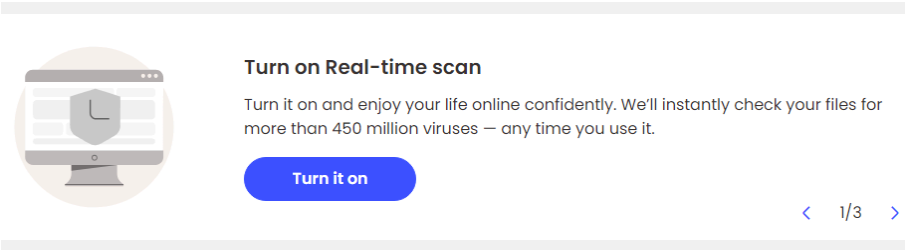
The program is very straightforward to install – simply click *Install* and you are done. The program window opens automatically after installation finishes.

System Tray icon

The System Tray icon menu lets you open the program window, check for updates, run scans, access settings, turn on the VPN, view subscription information and your account, and open the help page.

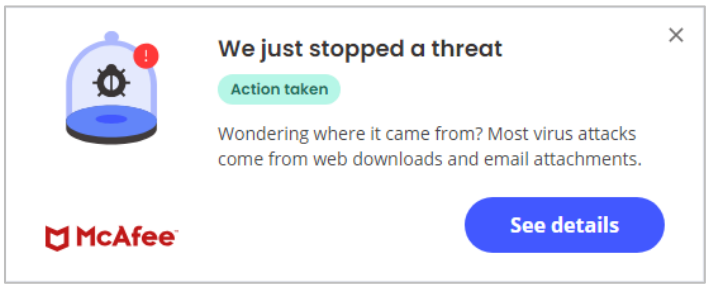
Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below) and a pop-up notification appeared, which persisted until we closed it. We were able to reactivate the protection easily by clicking *Turn it on*.



Malware detection alert

When we tried to open a malicious file in our functionality check, McAfee blocked the threat and displayed the alert shown below. We did not need to take any action, and the alert persisted until we closed it.



Clicking *See details* displays the file name, file path, detection name, and action taken (*Quarantined*).

Scan options

A quick scan can be initiated by clicking the *Antivirus* tile on the home page. You can run a full scan under *Scan Types* and configure scheduled scans. You can also scan a local drive, folder or file, or a network share, from Windows Explorer's right-click menu. *Real-Time Scanning* under *My Protection* (menu item with four squares on the left-hand side of the program window) lets you exclude individual files from being scanned. We could not find any settings regarding PUA detection.

Quarantine

The quarantine can be found under *My Protection\Quarantined items*. It shows the file name, threat name, date/time of detection, and status. Clicking on an item displays the original file path. You can restore or delete individual items, or all items at once using the *Select all* button.

Logs

The log feature is available under *My Protection\Security Report*, providing a record of activities such as threats resolved, files scanned, and items quarantined. The results can be filtered by the last week, month, or year.

Help

The help features can be accessed by clicking the *Account* icon (last item in the menu on the left-hand side of the program window). The *Help* and *Support Website* links redirect to the same contact page, which could make finding instructions difficult, especially for novice users.

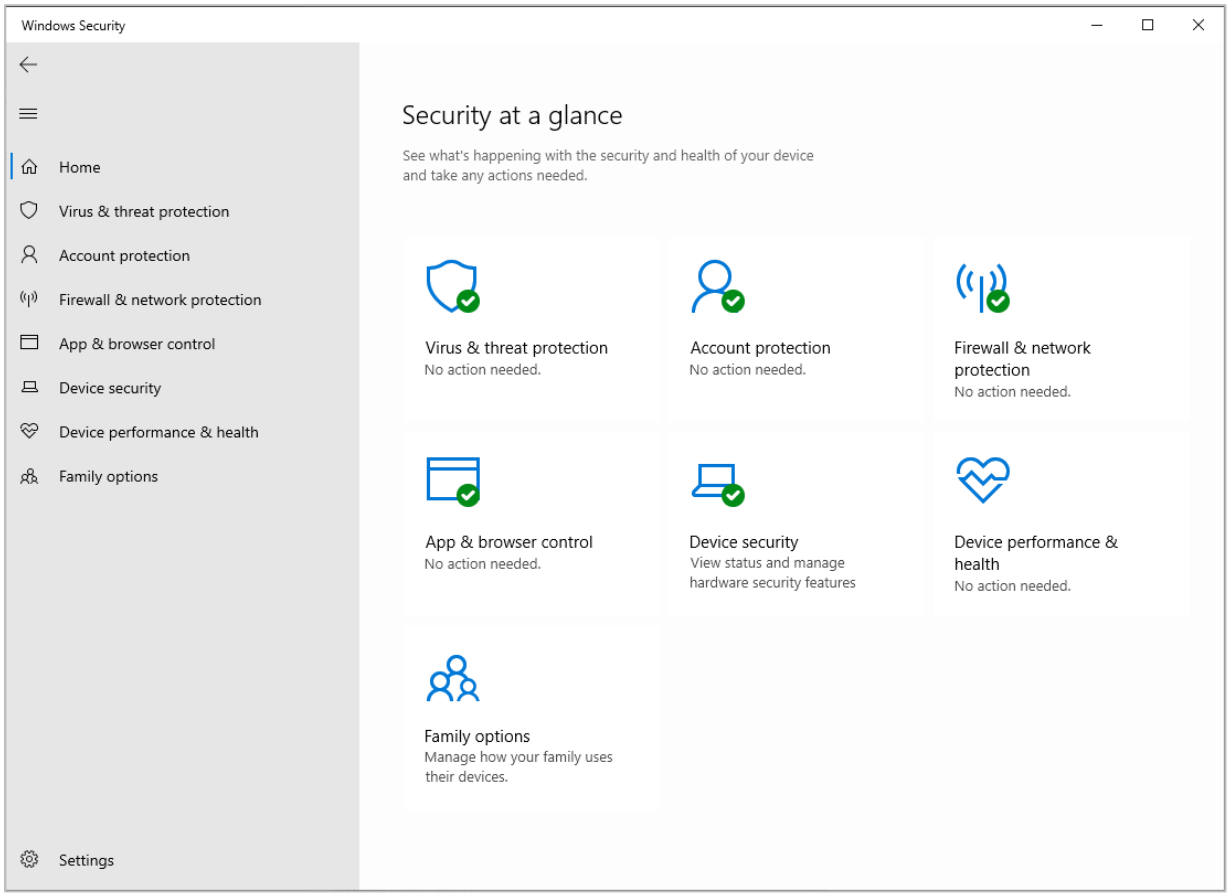
Access control

Standard Windows User accounts cannot disable protection features (switches are deactivated) or uninstall the program, which we regard as ideal.

Other points of interest

- There is a VPN included, offering a wide selection of countries.
- The included file shredder, which can be accessed from Windows Explorer's right-click menu, claims to permanently delete files without leaving a trace on the hard drive.

Microsoft Defender Antivirus



About the program

Microsoft Defender Antivirus is a free security program, included with Windows 10 (and Windows 11). You can find out more about the program on the Microsoft website: https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963

Summary

Microsoft Defender Antivirus includes all the essential features of an antivirus program in a clean, touch-friendly interface. The program is simple to use and comes pre-installed with Windows.

Setup

Setup is not required as the program is built into Windows.

System Tray icon

The System Tray icon menu lets you run a quick scan, check for updates, view notification options, and open the Windows Security dashboard.

Malware detection alert

When a malicious file was detected in our functionality check, Microsoft Defender Antivirus displayed the alert shown below. We did not need to take any action, and the alert closed after a few seconds.

Clicking on *Get details* opened the *Virus & threat protection* page of Windows Security. When multiple malicious files were detected simultaneously, an individual alert was shown for each detection.

Scan options

Opening *Virus & threat protection* allows you to run a quick scan. By clicking on *Scan options*, you can start a quick scan, full scan, custom scan (choose files or folders to scan), or *Microsoft Defender Offline scan*. The later involves restarting the device and claims to remove difficult-to-remove malware. Local drives, folders, files, or networks shares can be scanned by using Windows Explorer's right-click menu. Exclusions can be managed under *Virus & threat protection\Manage Settings*. PUA detection is activated by default and can be configured under *App & browser control\Reputation-based protection settings*.

Quarantine

To see the quarantined items, you must open *Virus and threat protection\Protection history* and then filter for *Quarantined items*. Items are listed with date and time of detection, and severity. Clicking an item reveals more details, including the file path, file name, a brief description of the threat, and the action taken. Files in quarantine can only be individually restored or removed. Clicking *Learn more* opens the Microsoft Security Intelligence website with additional information about the threat.

Logs

All events are logged and accessible under *Protection history*.

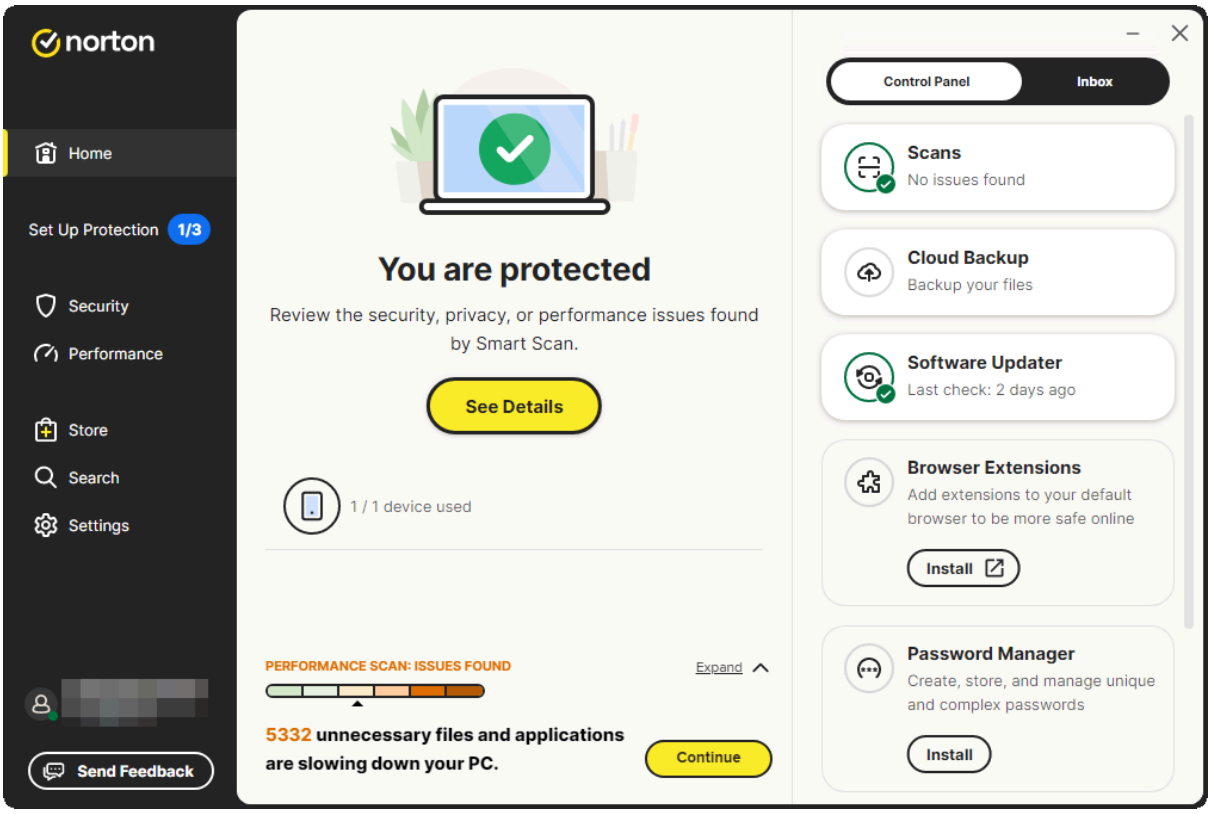
Help

Clicking *Virus & threat protection* page*Get help* opens an automated chat service where you can type in a query and search for assistance. In our functionality check, we found the search results to be less helpful. For example, "Set scan exclusion" first gave information on how to use a scanner with your PC, before linking to the correct page under *More help* which brought up a brief description illustrated with a screenshot.

Access control

Standard Windows User accounts cannot disable protection features, which we regard as ideal.

Norton AntiVirus Plus



About the program

Norton Antivirus Plus is a paid-for security program. In addition to anti-malware features, it includes a cloud backup feature, password manager, software updater, and performance tune-up features. You can find out more about the product on the vendor's website: https://us.norton.com/products/norton-360-antivirus-plus

Summary

Norton AntiVirus Plus is easy to set up and features a modern interface with essential features easily accessible. It provides safe default settings, and on-access protection scans files when you try to copy them to your PC.

Setup

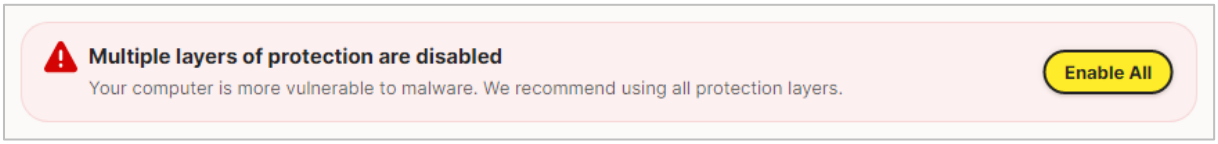
You can download the installer after logging into your Norton online account. During setup, you can choose to opt into Norton's data-sharing scheme. After installation , we needed to sign in again to activate the product. Once activated, you can set up Cloud Backup and Password Manager.

System Tray icon

The System Tray menu lets you open the program, run scans and updates, access support, enable silent mode, disable antivirus and firewall features, open settings, and view logs.

Security status alert

When we disabled protection features in the program's settings, an alert was shown on the settings page (screenshot below), and a pop-up appeared in the bottom right-hand corner of the screen. We could reactivate protection easily by clicking *Enable All*.



Malware detection alert

When a malicious file was detected in our functionality check, Norton displayed the alert shown below. We did not need to take any action, and the alert persisted until we closed it. When multiple threats were detected, only a single alert was shown. As seen, Norton has undergone changes in Q4 2024, now utilizing the Avast engine. This shift is also reflected in the updated user interface, which closely resembles that of Avast.

Scan options

Clicking the *Scans* tile on the *Security* page opens the *Scans* page, where you can run smart, quick, full, targeted, and startup scans. Custom scans can be configured under the corresponding tab. Local drives, folders or files, and network shares can be scanned using Windows Explorer's right-click menu, which also allows you to check a file with Norton's reputation service. Exclusions are managed under the *Exclusions* tab of the *Scans* page.

Quarantine

The quarantine can be found under *Security\Quarantine*, where it displays the file name, detected threat, original location, along with date and time of the detection. You can select files individually or all at once and then choose to restore, create an exclusion and restore, extract, or send the file for analysis.

Logs

Logs are listed under *Security\Security History* and can be filtered by severity, type of log entry, and by recent or all detections.

Help

On the S*earch* page, accessible from the ribbon on the left-hand side, you can search for program features and access help and support.

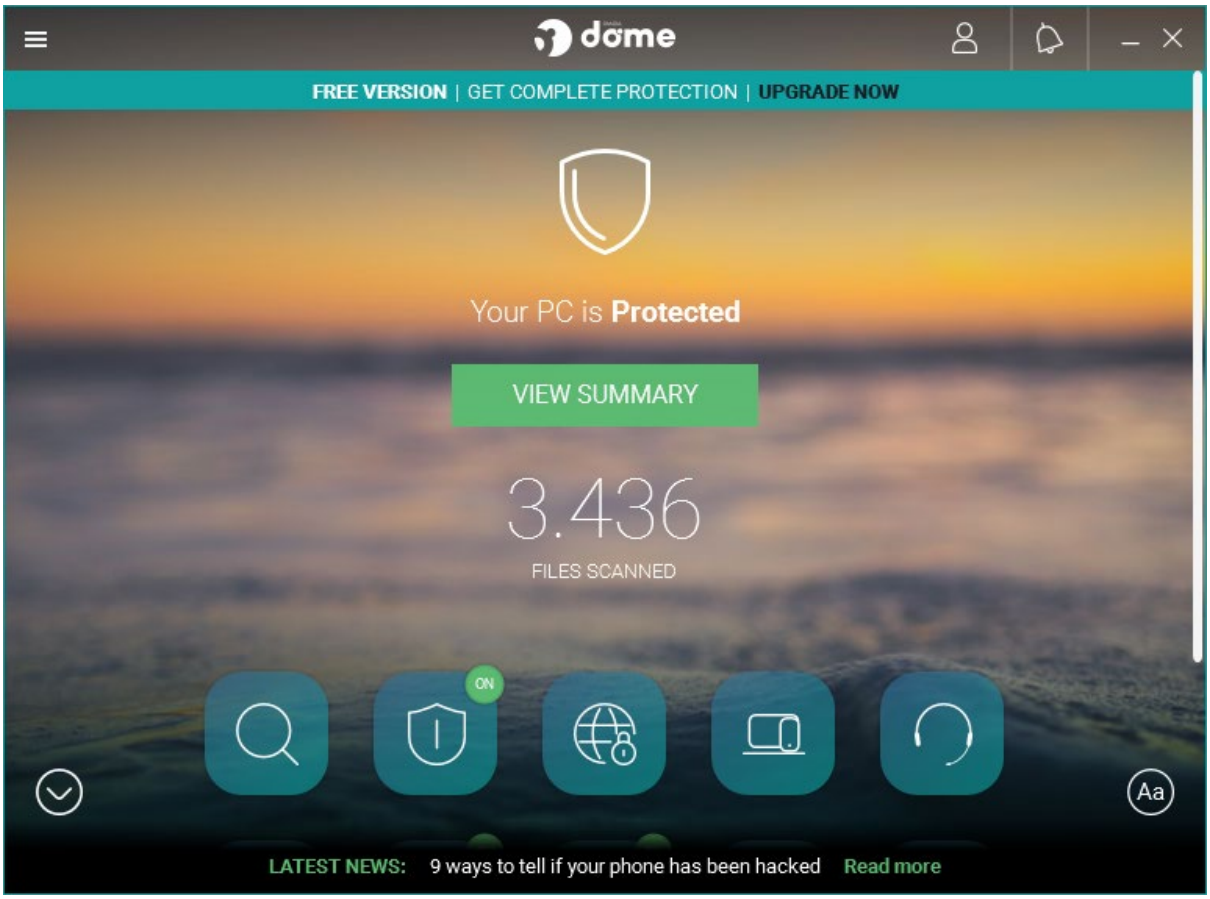
Access control

Standard Windows users cannot disable protection features or uninstall the program, which is ideal in our opinion. When the program is used with a standard user account, protection settings are inaccessible. Additionally, a password protection feature is available, requiring a password to change settings or disable protection.

Other points of interest

- Norton AntiVirus Plus includes 2GB of cloud storage.
- There are performance tools included, such as Software Updates, File Cleanup, Startup Manager, and a defragmentation tool.

Panda Free Antivirus



About the program

Panda Free Antivirus is a free security program. In addition to anti-malware features, it includes a limited VPN. You can find out more about the product on the vendor's website: https://www.pandasecurity.com/en/homeusers/free-antivirus/

Summary

We found Panda Free Antivirus to be very straightforward to install and use. The program interface is simple to navigate, with safe default settings. A free VPN is included, which is limited to 150MB of data per day and automatic server selection.

Setup

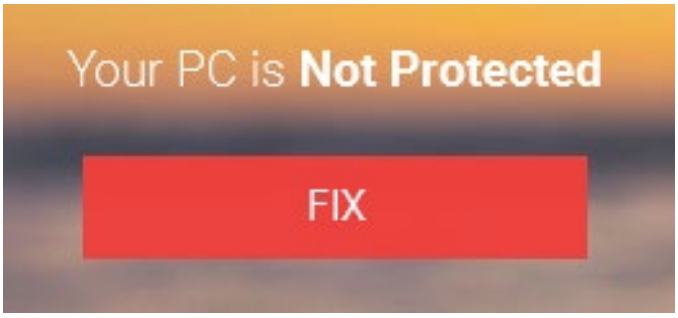
The program installation is straightforward. You can change the installation folder and interface language. Additionally, the Opera browser will be installed by default, but you can easily opt out of this with a single click. In our functionality test, we did not install Opera. After setup is complete, you are prompted to sign in or create a new Panda account. While this step is not mandatory, if you skip it, you will be prompted to sign in every time you open the program.

System Tray icon

The System Tray icon menu lets you open the program window, enable gaming/multimedia mode, reach help and support services, disable/enable protection, and connect to the Panda VPN.

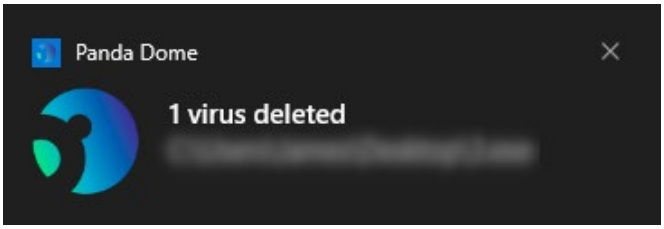
Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). After clicking *Fix* and then *Enable*, protection was turned on again.



Malware detection alert

When a malicious file was detected in our functionality check, Panda displayed the alert below. We did not have to take any action, and the alert disappeared after a few seconds.



Clicking on the alert opened the *Event report* (logs) page, showing detection name, file name and path, date and time of detection, and action taken (deleted). When multiple malicious files were detected simultaneously, individual notifications for each detection were displayed.

Scan options

Clicking the *Scan* button (magnifying-glass symbol) in the program windows lets you run *Critical areas*, *Full, or Custom* scans. On the *Antivirus* page, you can schedule scans, view the last scan, and access the quarantine. You can scan a local drive, folder or file using Windows Explorer's right-click menu. To set exclusions and configure PUA detection (enabled by default), open *Settings\Antivirus* from the *Antivirus* page.

Quarantine

The quarantine can be found on the *Antivirus* page. It displays the detection name (along with the action taken), file name and path, and date and time of detection. You can recover or delete quarantined items one by one or empty the quarantine by clicking on the trash-can icon.

Logs

You can find the log feature on the *Antivirus* page, by clicking *View report*. It displays the same information as the quarantine page, along with the status (e.g. "Deleted" or "Finished").

Help

The help feature is located in the "hamburger" menu in the top left-hand corner of the program window which opens the product's online manual. The Support page can be accessed by clicking the support button on the program's home page.

Access control

Standard Windows User accounts can disable protection features but cannot uninstall the program. You can password-protect the program to prevent access to the Panda console, though it will still be possible to run scans from Windows Explorer's right-click menu and view scan results.

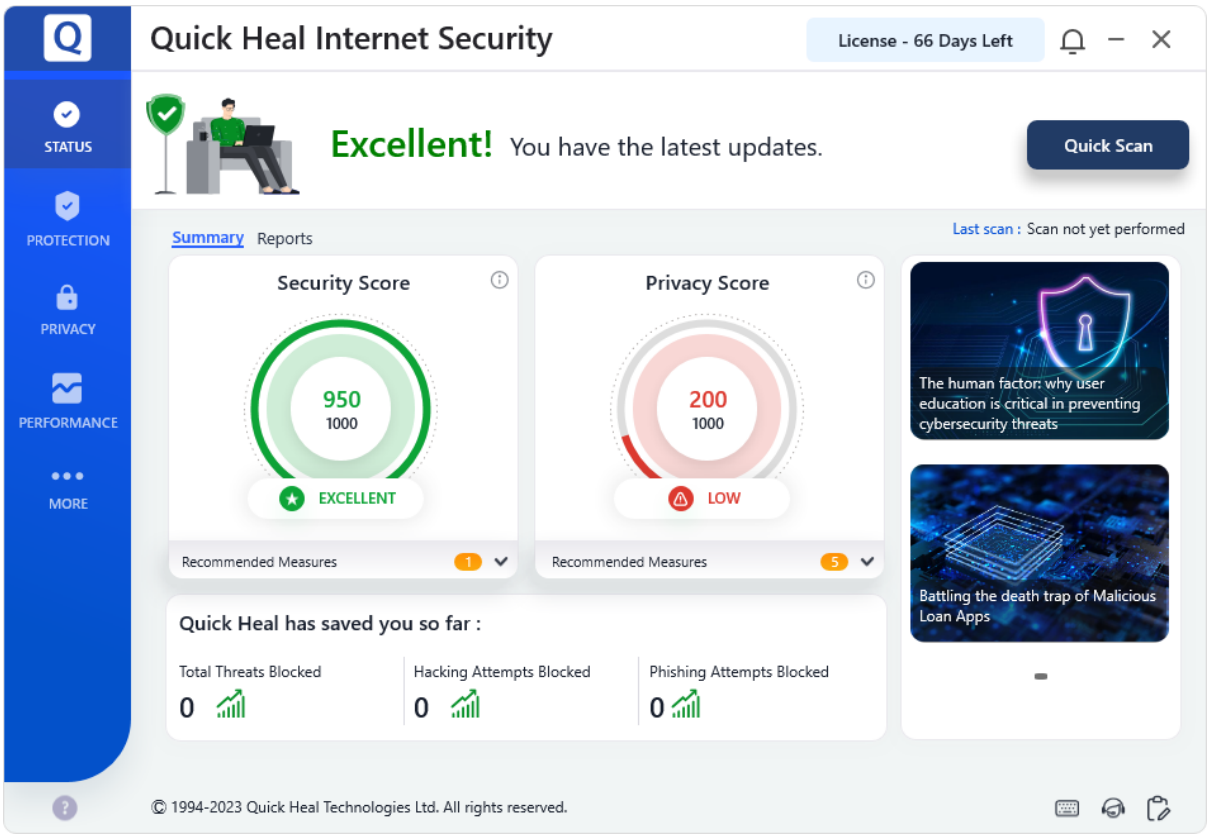
Advertising

Although Panda Free Antivirus promotes other paid Panda products, it does so in a very subtle, non-intrusive manner, using a thin strip along the top of the program window.

Other points of interest

- The setup wizard states that free support is included for "any PC or Internet related problems". Telephone numbers for the UK, USA, and Canada are provided (in the English version of the program), and Panda told us that the calls are free of charge.
- A strip at the bottom of the program window displays headlines of various IT-security-related articles from Panda's media center.

Quick Heal Internet Security



About the program

Quick Heal Internet Security is a paid-for security program. It includes anti-malware features as well as phishing and spam protection. You can find out more about the product on the vendor's website: https://www.quickheal.com/quick-heal-internet-security

Summary

Quick Heal Internet Security is easy to install and use. The program interface is simple to navigate, with safe settings provided by default. The program window displays a security score, privacy score, and articles from the Quick Heal blog.

Setup

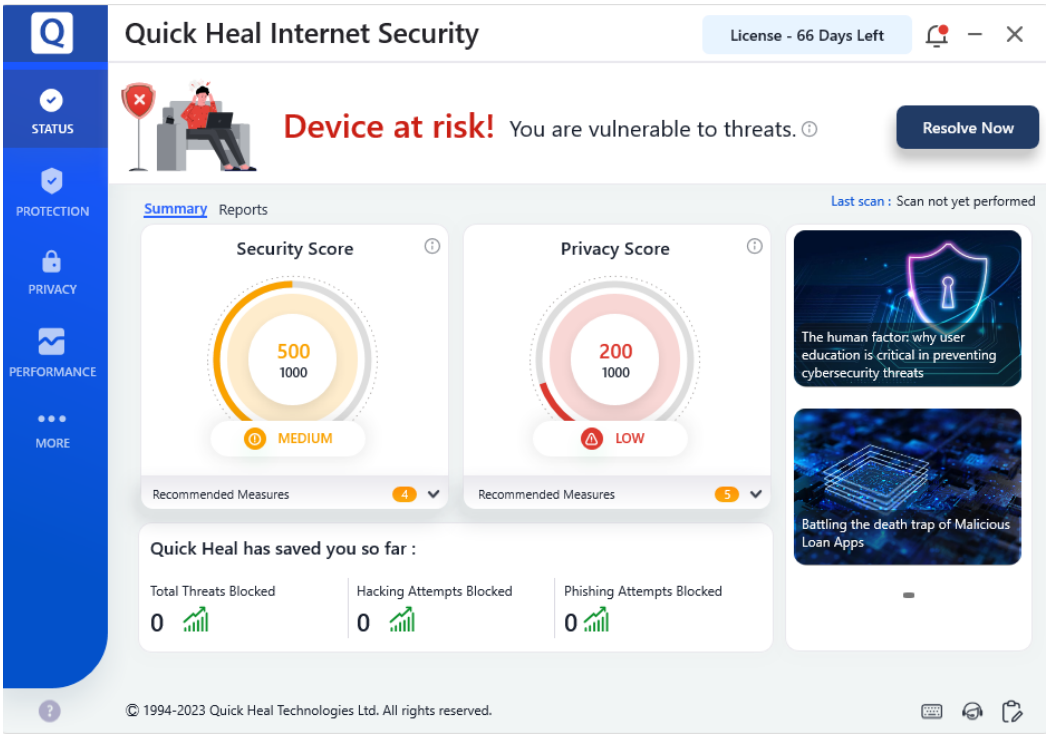
The program installation is simple and straightforward by choosing the language for the installer, accepting Terms and Conditions, and selecting the installation location. Once installation completes, you must either activate the product or continue with the free trial.

System Tray icon

The System Tray icon menu lets you open the program window as well as launch Safe Banking and Secure Browse. You can also contact the support, update the databases, and open the virtual keyboard.

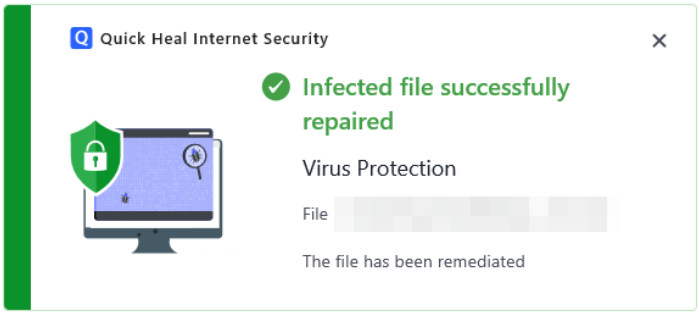
Security status alert

When we disabled virus protection in the program's settings, an alert was shown on the home page (screenshot below). After clicking *Resolve Now,* protection was turned on again.



Malware detection alert

When a malicious file was detected in our functionality check, Quick Heal displayed the alert below. We did not have to take any action, and the alert disappeared after a few seconds.



Scan options

All available scan options can be accessed by clicking *All Scans* on the *Protection* page. This includes *Quick, Full Device, Memory, Vulnerability, AntiMalware, Custom* and *Boot Time Scan*. Clicking on *Custom Scan*, lets you scan individual folders and files. Schedule scans of certain folders can also be configured. You can scan a local drive, folder or file using Windows Explorer's right-click menu. Exclusions and other scan settings can be managed by clicking the cog icon on the *All Scans* page.

Quarantine

The quarantine is available on the *All Scans\Setting* page. You can set the number of days after which quarantined files are deleted. Clicking *View Files* shows the file name and path, status, quarantine date, and whether it has been submitted for analysis. You can restore or delete quarantined items individually or submit them for analysis. Files can also be manually added to the quarantine.

Logs

You can find the log feature on the home page by clicking *Reports,* Displaying screen time, the number of blocked websites, and blocked threats.

Help

The help feature is located under *MORE\Support* offering the following customer support options: live chat, FAQ and How-to videos, phone support, and the option to raise a ticket.

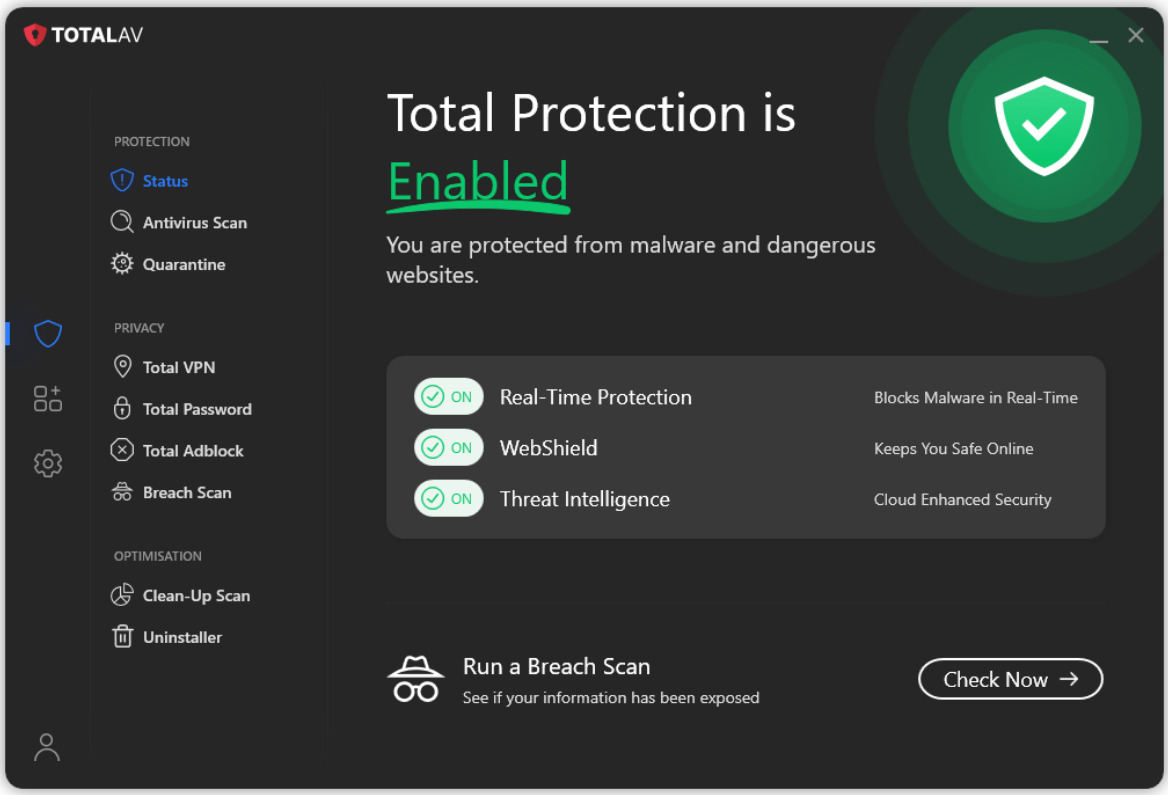
Access control

Standard Windows user accounts can view the program status, support page, and perform scans from the Window Explorer's right-click menu. You can also protect program settings using a password.

Other points of interest

- Quick Heal Internet Security also includes parental control features.
- You can only select individual file in the quarantine, which makes situations with many quarantined files quite tedious.

TotalAV Antivirus Pro



About the program

TotalAV Antivirus Pro is a paid-for security program. In addition to anti-malware features, it includes phishing protection and a system performance tuner. You can find out more about TotalAV Antivirus Pro on the vendor's website: https://www.totalav.com/product/antivirus-pro

Summary

We found TotalAV Antivirus Pro to be very simple to install and use. The program's features are easily accessible in a single menu panel, and default settings and alerts are sensible. The program also includes an adblocker, although we did not test this.

Setup

The program installation is quick and simple by running the installer and clicking *Install*. After installation, TotalAV opens automatically and downloads definition updates.

System Tray icon

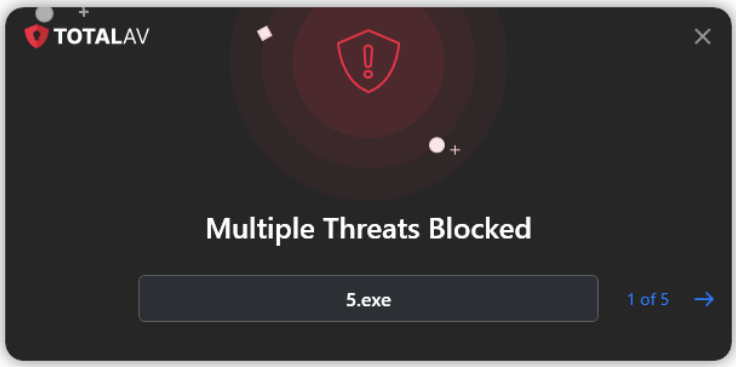
The System Tray icon menu lets you open the program window, quarantine, settings, check for updates, and view information about the program and definitions versions.

Security status alert

When we disabled real-time protection in the advanced settings, an alert was shown on the home page (screenshot below), along with a pop-up notification. Clicking *Enable Total Protection* or the toggle switches reactivated protection.

Malware detection alert

When a malicious file was detected in our functionality check, TotalAV displayed the alert shown below. We did not need to take any action. The alert was displayed over all other windows and persisted until we closed it. When multiple threats were detected simultaneously, only a single alert was shown.



Scan options

The scan options can be accessed by clicking on *Antivirus Scan* under *Protection* in the menu on the left-hand side of the program window. From there, you can run a quick and full system scan as well as configure custom and scheduled scans. You can also scan a local drive, folder or file using the right-click menu in Windows File Explorer. Exclusions can be set up by adding them to the allow list in the settings. In the program's advanced settings, you can change a number of options, such as whether to scan removeable drives, type and time of scheduled scans, and action to be taken when malware is discovered. TotalAV informed us that PUA detection is enabled by default and individual apps can be excluded if necessary.

Quarantine

The quarantine is available from the home section (shield icon on the left-hand side) and *Protection\Quarantine*. It displays the file name, threat name, the quarantine date, and original file location. You can select individual or multiple items and delete or restore them.

Logs

While you can view the day when threats were encountered in *Quarantine*, there is no separate logs feature available.

Help

The help feature is located in the *Support Centre* under the *My Account* section (figure icon at the bottom-left). This opens the *Help Center* page on Total AV's website, which offers tiles for different categories and products. You can find topics related to the antivirus program, namely *Setup*, *Configuration and Setting*, *Issues and Malware*, *VPN,* and *Total Password*, under *Technical Support*. Each topic includes clear explanations and instructions, with ample annotated screenshots and videos. However, some support pages where not yet complete at the time of testing.

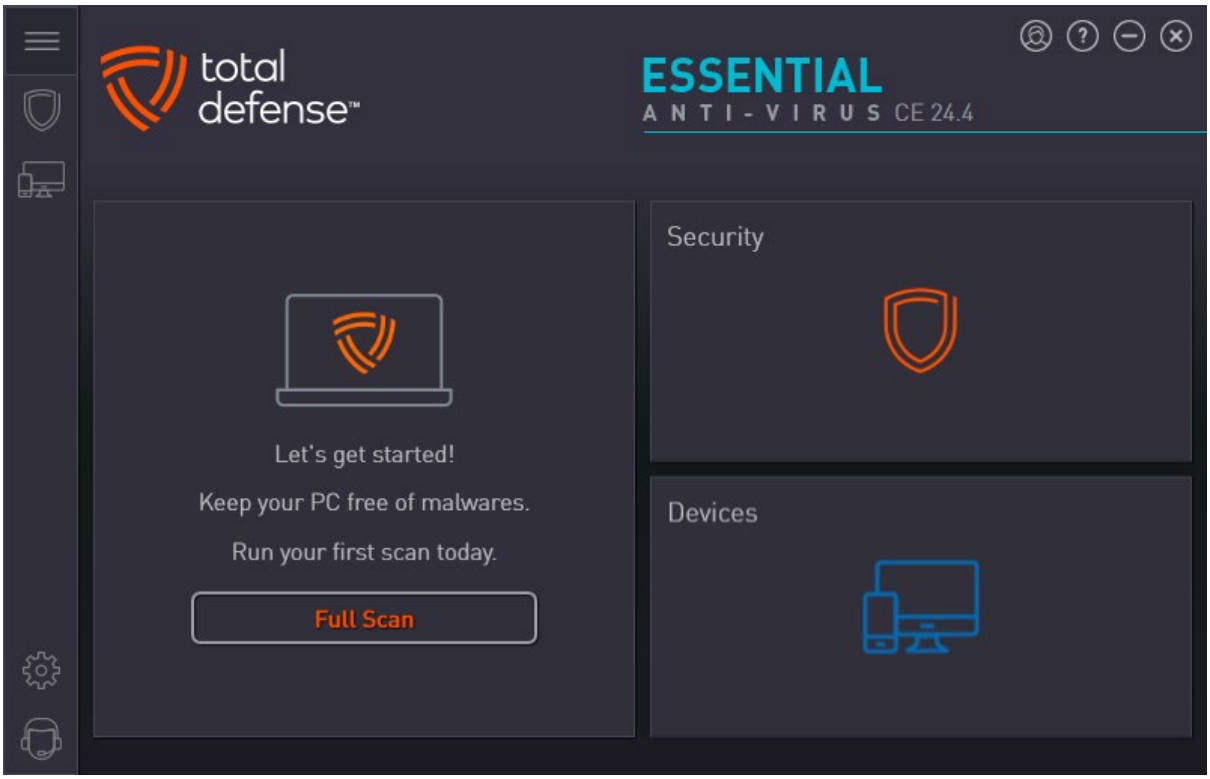
Access control

Standard Windows user accounts cannot disable protection features or uninstall the program. They can however change other settings.

Other points of interest

- TotalAV Total Protection includes a *Breach Scan*, which checks if a provided email address is included in any data breach and your personal data has been exposed, as well as an ad blocker and cloud storage (limited to 2GB).
- A VPN, unlimited cloud storage, and password manager are available as add-ons for an additional charge.

Total Defense Essential Anti-Virus



About the program

Total Defense Essential Anti-Virus is a paid-for security program that provides malware and phishing protection. Its Privacy Protection feature monitors which apps use the camera and microphone. You can find out more about the product on the vendor's website: https://www.totaldefense.com/shop/anti-virus

Summary

Total Defense Essential Anti-Virus is easy to install and features a simple, user-friendly program interface that makes important functions readily accessible. The help articles are clear, well-illustrated, and easy to follow.

Setup

The installer allows you to select the interface language and customize the installation folder under *Custom Install*. The installation process is fast and requires no further user intervention. Once installed, the program automatically checks the product status, updates malware signatures, and runs a performance optimization scan which takes only a few minutes.

System Tray icon

The System Tray icon menu lets you open the main program window, check for updates, run a quick scan, and pause real-time protection.

Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). Clicking *Fix all* turned on real-time protection again.

Malware detection alert

When a malicious file was detected in our functionality check, Total Defense displayed the alert shown below. We did not need to take any action, and the alert closed after a few seconds. Clicking *Details* opened the corresponding entry on the program's log page.

When multiple malicious files were detected simultaneously, one alert for each detection was displayed.

Scan options

You can initiate a full scan directly from the *Home* page. The *Security* tab offers additional scan options, including quick, system, full, and custom scan. The *Suspend Scans* button temporarily deactivates real-time protection for a specified duration. You can scan a local drive, folder or file, or a network share using Windows Explorer's right-click menu. Under *Security\Settings\Scanner*, the *Scan Options* slider allows you to adjust the protection level to *Low, Recommended* (default), *High*, or *Custom*. Total Defense told us that PUA detection is enabled by default. Selecting *Custom* lets you fine-tune settings, such as scanning network, archive, and hidden files, and determining whether suspicious files should be treated as infected.

Quarantine

The quarantine can be found under the corresponding tab (shield icon with a lock) on the *Security* page. It shows the date and time of a detection, along with the file name. Clicking on an item reveals further details, such as threat name, threat type, and action taken. You can select individual files or all at once to restore or delete them.

Logs

The *Reports* tab on the *Security* page provides a detailed list of detected threats, including the detection date, time, and type of scan that identified them. You can also view a summary that categorises and counts the blocked threat types.

Help

Clicking the ? icon in the top right-hand corner of the program window opens the *About* page. From there, selecting *Support Info* and then *Online Support* directs you to the vendor's support page. A searchable FAQ can be found under *Product Support*. Each article provides clear, step-by-step instructions accompanied by annotated screenshots.

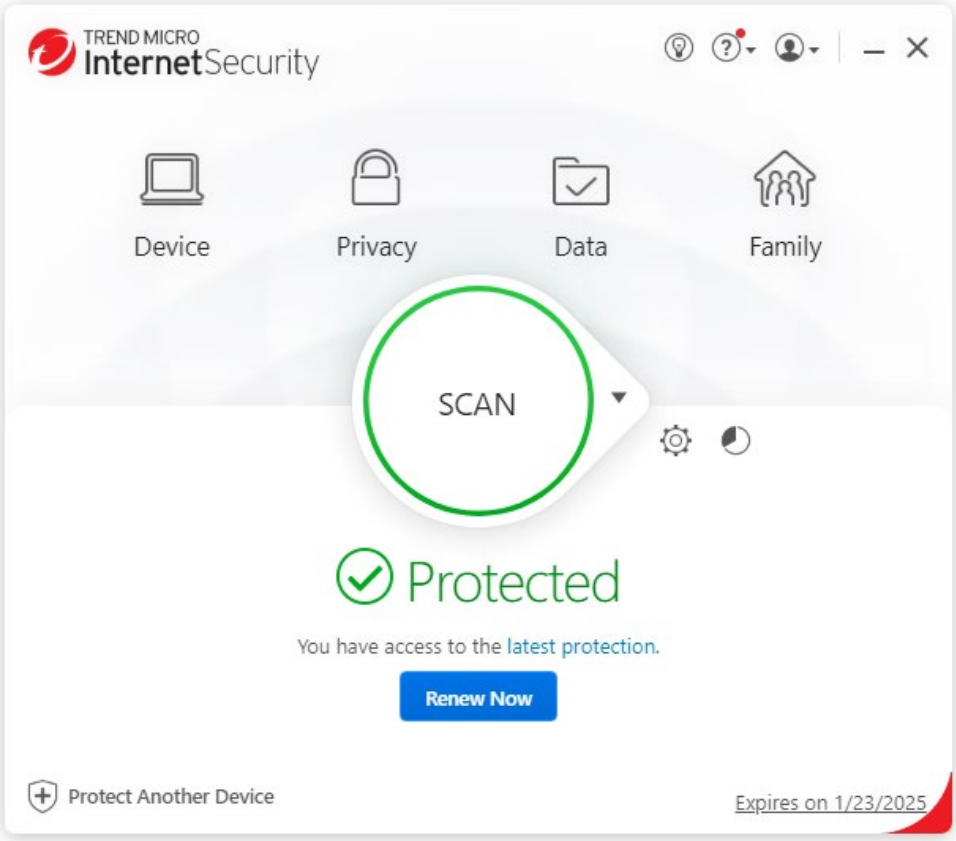
Access control

Under *Settings\Console*, you can prevent other users from disabling protection or modifying security settings. By enabling the *Restrict access to antimalware configuration* option, users will be required to enter the Total Defense account password to change AV settings. The *Restrict access to devices configuration* option allows you to control access to the *Devices* page.

Other points of interest:

- You can also use Windows Explorer's right-click menu to exclude a drive, folder or file from scans.
- The *Devices* page shows all devices associated with your account. For each device, you can view details such as device type (e.g., PC), installed product (e.g., AntiVirus), security status, the dates of the last update and scan, and the number of threats resolved. You can also rename a device, change its user avatar, and delete the device to free up its license.

Trend Micro Internet Security



About the program

Trend Micro Internet Security is a paid-for security program. In addition to anti-malware features, it includes a ransomware shield, parental controls, secure erase feature, and a secure browser mode for financial transactions. You can find out more about the product on the vendor's website: https://www.trendmicro.com/en_us/forHome/products/internet-security.html

Summary

The program is easy to install, and the simple user interface makes important features easy to find. It comes with safe default settings, and we liked the persistent malware and status alerts. The online manual is clear and simple to follow.

Setup

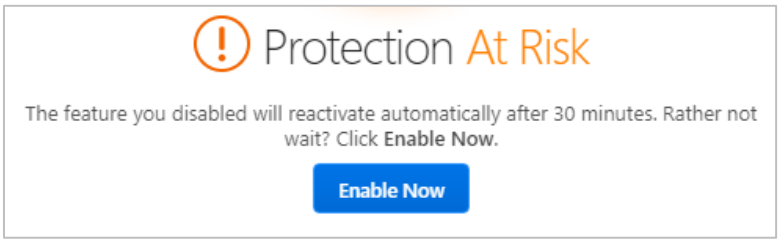
After launching the installer, you must accept the license agreement, privacy policy, and data collection notice. You can also choose to make notifications more relevant. After setup, you set the device name, and the product will be activated. You will then be prompted to configure the ransomware shield, which by default covers Windows' Documents, OneDrive, and Pictures folders. Additional folders can be added as needed.

System Tray icon

The System Tray icon menu lets you open the main window, run a scan, check for updates, disable/enable protection, start mute mode, check your Trend Micro account and subscription, run a troubleshooting tool, and quit the program.

Security status alert

When we disabled protection in the program's settings, an alert was shown on the home page (screenshot below) and an additional, persisted pop-up alert above the System Tray icon. We were able to reactivate the protection easily by clicking *Enable Now*.



Malware detection alert

When a malicious file was detected in our functionality check, Trend Micro displayed the alert shown below. We did not need to take any action, and the alert persisted until we closed it.

Clicking *More details* opens the program's scan log page, displaying date and time of the detection, file name and path, detection name, and action taken. When multiple malicious files were detected simultaneously, only one alert box was shown.

Scan options

The *Scan* button in the main program window starts a quick scan. Clicking the small down arrow next to the *Scan* button reveals additional scan options, including full and custom scans. Scans can be scheduled through the program's settings. By default, a smart schedule is used which runs appropriate scans based on computer usage. Alternatively, scans can be scheduled at specific times. You can also run scans from Windows Explorer's right-click menu. PUA detection is enabled by default and can be configured under *Settings\Scan Preferences*. The *Settings\Exception Lists* page allows you to customize scan exclusions.

Quarantine

The quarantine is part of the *Security Report*, which can be opened by clicking the pie-chart symbol next to the *Settings* icon. The page displays a summary of detected threats, grouped by type (e.g., ransomware, web threats, computer threats). Clicking *See more details* opens a log of individual security-related events for each threat. Selecting *Viruses* from the drop-down menu, shows a list of malware detections, including the detection date and time, file name, file path, threat name, and action taken. Clicking on an entry opens a panel with further information. If malware was quarantined (Trend Micro labels these files as "removed"), the details pane will show a *Restore* button. However, we suggest that this process could be simplified to make it more user-friendly for non-expert users.

Logs

There is no separate logs feature, as quarantine and logs are combined on the *Security Report* page.

Help

Clicking the *?* menu and selecting *Product Support* opens the program's online manual, providing an overview of the program's main functions. Clicking the *?* on other program pages directs you to the corresponding help page. Each help article consists of clear explanations and instructions, with some articles featuring well-illustrated screenshots.

Access control

Standard Windows user accounts can disable protection features but cannot uninstall the program. Under *Other Settings\Password*, you can configure a password to prevent other users from changing the program settings. This setup asks for a password hint and an email address for password recovery. Trend Micro Internet Security also mandates a password to disable protection via the System Tray icon menu, although this is not required through the program's settings.

Other points of interest:

- At the end of the setup wizard, an overview of the program's features is shown, along with an option to *Explore More Features*. This prompts a few questions about your computer usage to suggest relevant features and provide additional information. You can also access this feature later by clicking on the lightbulb icon at the top of the program window.
- Trend Micro Internet Security includes a parental control feature (this was not part of our functionality test).

Featurelist Windows (as of December 2024)	FREE	COMMERCIAL	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	COMMERCIAL	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL
Product name	Avast Free Antivirus	AVG Internet Security	Avira Free Security	Bitdefender Total Security	ESET Home Security Essential	F-Secure Internet Security	G Data Total Security	Kaspersky Standard	McAfee Total Protection	Microsoft Defender Antivirus	Norton Antivirus Plus	Panda Free Antivirus	Quick Heal Internet Security	TotalAV Antivirus Pro	Total Defense Essential Anti-Virus	Trend Micro Internet Security
Supported Program languages	All	English, Czech, Danish, German, Spanish, French, Hungarian, Indonesian, Italian, Japanese, Korean, Malaysian, Dutch, Norwegian, Polish, Portuguese, Russian, Slovak, Serbian, Turkish, Chinese	English, German, Italian, French, Spanish, Portugese, Russian, Dutch, Turkish, Japanese, Chinese, Indonesian	English, French, German, Dutch, Spanish, Italian, Romanian, Portuguese, Polish, Greek, Vietnamese, Turkish, Korean , Czech, Japanese, Hungarian, Thai	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Kazakh, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian Latin, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukrainian, Vietnamese, Indonesian, Catalan	English, Bulgarian, Chinese, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish, Vietnamese	English, German, French, Italian, Spanish, Portuguese, Dutch, Polish	English, Arabic, French, Bulgarian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, German, Greek, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lituanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Chinese, Spanish, Swedish, Thai, Turkish, Ukrainian, Vietnamese	English, Chinese, Danish, Dutch, Finnish, French, German, Greek, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish	English, French, Dutch, Portuguese, Czech, Danish, German, Spanish, Italian, Norwegian, Polish, Russian, Finnish, Swedish, Turkish, Chinese, Japanese, Korean, Arabic, Hebrew	English, French, German, Japanese, Spanish, Italian, Dutch, Swedish, Finnish, Norwegian, Danish, Portuguese, Czech, Polish, Hungarian, Romanian, Slovak, Russian, Greek, Turkish, Chinese, Korean, Arabic, Hebrew	English, Bulgarian, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Italian, Norwegian, Polish, Portuguese, Russian, Chinese, Slovak, Slovenian, Spanish, Swedish, Turkish	English, Arabic, Chinese, French, German, Italian, Japanse, Korean, Polish, Spanish	English, Czech, Danish, Dutch, French, German, Italian, Norwegian, Polish, Portuguese, Spanish, Swedish, Turkish	English, Spanish	English, German, French, Italian, Spanish, Portuguese, Japanese, Chinese, Russian, Dutch, Danish, Norwegian, Swedish, Indonesian, Korean, Thai, Turkish, Vietnamese
Third-party scan engine included	proprietary	Avast	proprietary	proprietary	proprietary	Avira	Bitdefender	proprietary	proprietary	proprietary	Avast	proprietary	proprietary	Avira	Bitdefender	proprietary
Protection																
Scans file on execution	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Scans files on demand	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
On-access file scan after Internet download (by DEFAULT)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
On-access file scan while copying/moving files (by DEFAULT)	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●
Prevents access to phishing and other malicious websites	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●
Alerts when visiting a Fake Shop Scam Sites (>60% Yes, >30% limited)	●	●	limited		limited	●			●		●			limited		limited
Detects also threats for e.g. Android, Mac, Linux	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Detection of potentially unwanted applications (PUA) turned ON by DEFAULT	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
Is the online malware detection the same as offline				●	●		●						●		●	
Additional features (selection chosen by AV-Comparatives)																
Multi-device protection / Multi-platform licensing	●	●	●	●	●	●	●	●	●	●				●	●	●
Firewall	●	●	●	●	●		●	●	●	●	●		●			
WiFi protection / Home Network Protection	●	●	●	●	●				●				●	●		●
Browser cleanup / Privacy cleaner / File Eraser	●	●	●	●	●		●	●	●	●				●		●
Rescue disk	●	●	●	●	●		●	●		●	●	●				●
Scans HTTPS traffic	●	●	●	●	●	●	●	●			●		●		●	●
Secure Browser / banking protection / Private Browsing	●	●	●	●	●	●	●	●		●	●		●			●
Device Access Control / USB Protection	●	●	●	●	●		●	●		●		●	●		●	
Software Updater / Vulnerable-Software Reporter	●	●	●	●				●	●	●			●		●	
Parental Control				●	●	●	●		●	●			●			●
Webcam / Audio Protection	●	●		●	●			●			●				●	
Anti-Spam				●	●		●			●			●			●
Password Manager			●	●			●		●		●					
Data-Breach checker	●	●	●						●					●		
VPN (unlimited)			●	●					●							
Ad-Blocker / Anti-Tracker			●	●				●								
Secure Keyboard / Virtual Keyboard				●				●		●			●			
Application Manager								●		●				●		
Malware Removal support guarantee (money-back)									●		●				●	
Backup							●		●		●		●			
Folder Shield / Data Locker	●	●					●			●						●
Are ARM processors supported on non-Apple ARM (Microsoft ARM64) devices?	●	●	●	●	●				●	●	●					●
Support options (may vary depending on location and language)																
Online Help	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Support Forum	●	●	●	●	●	●		●	●	●	●	●	●			●
Phone Support		●	●	●	●	●	●	●	●		●		●	●	●	●
Email Support		●	●	●	●		●	●					●	●	●	●
Downloadable User Manual (PDF)				●		●				●	●					●
Supported languages (of support)	English, French, Czech, German, Italian, Spanish, Russian, Dutch, Japanese, Portuguese, Polish	English, German, Czech, French, Italian, Spanish, Portuguese, Dutch, Japanese, Polish	English,German, French, Italian, Portuguese, Spanish	English, French, German, Romanian, Portuguese, Italian, Spanish	All	English, Bulgarian, Chinese, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish, Vietnamese	English, German, French, Italian, Spanish, Portuguese, Dutch, Polish	English, Cantonese, Chinese, French, German, Greek, Hindi, Italian, Japanese, Polish, Portuguese, Romanian, Russian, Spanish, Turkish.	English, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukrainian	English, Chinese, German, French, Portuguese, Spanish, Turkish, Polish, Danish, Dutch, Finnish, Greek, Italian, Norwegian, Romanian, Russian, Swedish, Slovenian, Hungarian	English, Spanish	English, Hindi, Japanese, Indian regional languages	English, Czech, Dutch, Danish, French, German, Italian, Norwegian, Polish, Portuguese, Spanish, Swedish, Turkish	English	English, Japanese, Chinese

Copyright and Disclaimer

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

AV-Comparatives
(January 2025)