Independent Tests of
Anti-Virus Software

Summary Report 2020

Awards, winners, comments

TEST PERIOD:	2020
LANGUAGE:	ENGLISH
LAST REVISION:	15TH JANUARY 2021

WWW.AV-COMPARATIVES.ORG

Content

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-Series Tests of 2020, 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 2020 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.

avast | AVG | Avira | Bitdefender

eset | F-Secure | G DATA | K7 COMPUTING

kaspersky | McAfee | Microsoft | Norton LifeLock

panda a WatchGuard brand | TOTAL AV | total defense | TREND MICRO Securing Your Journey to the Cloud

VIPRE

Approved Security Product Award

The tested products of all the 17 vendors above are AV-Comparatives 2020 Approved Windows Security Products.

AV comparatives
APPROVED
Security Product
2020

Management Summary

Tests

In 2020, AV-Comparatives subjected 17 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 2020". 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 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 2020 Product of the Year Award goes to Kaspersky; Bitdefender and ESET receive Outstanding Product Awards; the Top Rated Product Awards go to Avast and AVG.

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 is a **Top-Rated Product** in 2020. It received an Advanced+ Award in four of this year's tests, and Advanced in the other three. It also takes a joint **Silver Award** for **Real-World Protection** and a joint **Bronze Award** for **Advanced Threat Protection**. It has a very clean, modern interface, and the setup wizard offers ideal options for both expert and non-expert users.

AVG receives a **Top-Rated Product** award this year. In four of this year's tests it took an Advanced+ Award, along with Advanced in the other three. It also received a joint **Silver Award** for **Real-World Protection**, and a joint **Bronze Award** for **Advanced Threat Protection**. It has a touch-friendly interface and good setup options.

Avira took three Advanced+ and three Advanced Awards in this year's tests. It features a modern, touch-friendly interface.

Bitdefender wins an **Outstanding Product Award**, having reached Advanced+ in all seven tests in 2020. It additionally receives joint **Silver Awards** for **Malware Protection** and **Advanced Threat Protection**, and the **Bronze Award** for **False Positives**. Its well-designed user interface includes a customisable home page, and real-time protection is highly sensitive.

ESET gets an **Outstanding Product Award** for 2020, as it reached Advanced+ level in all 7 tests this year. It also receives the **Gold Award** for **False Positives**, and joint **Silver Awards** for **Malware Protection** and **Advanced Threat Protection**. Reviewers were impressed with the clear and simple layout of the GUI, and ease of use.

F-Secure took three Advanced+ and three Advanced Awards this year. It features an easy-to-use, simply laid-out interface.

G Data takes this year's **Gold Award** for **Malware Protection**. It also received 4 Advanced+ and 1 Advanced Award in the 2020 tests. Reviewers noted its especially detailed status display and excellent access control.

K7 takes this year's **Gold Award** for **Performance**. It also got two Advanced+ and three Advanced Awards in the 2020 tests. Reviewers liked its simple design and impressive scanning speed.

Kaspersky is AV-Comparatives' **Product of the Year** for 2020, having got Advanced+ Awards in all 7 of the year's tests. In addition, it receives **Gold Awards** for **Real-World Protection** and **Advanced Threat Protection**, the **Silver Award** for **False Positives**, and **Bronze Awards** for **Malware Protection** and **Performance**. It has an easy-to-use tiled interface, and a wide range of configuration options.

McAfee received three Advanced+ and two Advanced Awards in the year's tests, along with a **Silver Award** for **Performance**. Its user interface is clean, modern and touch friendly. The program's status alerts are exemplary.

Microsoft took the **Bronze Award** for **Real-World Protection** this year. It also received two Advanced+ Awards and one Advanced Award in the year's tests. The product is integrated into Windows 10, and has a simple, unobtrusive interface.

NortonLifeLock's product took six Advanced Awards in this year's tests. It has a well-designed overall user experience, with detailed malware information accessible from alerts.

Panda received two Advanced+ and three Advanced Awards in this year's tests. Reviewers noted its security-blog feature, which lets you read articles on various IT-security related topics.

Total AV got one Advanced+ and four Advanced Awards in the 2020 tests. It features a very simple, easy-to-navigate program window.

Total Defense took one Advanced+ and four Advanced Awards this year. Its user interface stands out for its simplicity.

Trend Micro received one Advanced+ and two Advanced Awards in this year's tests. The user interface presents a simple overview, but allows easy access to advanced options. Its persistent malware and status alerts stand out.

Vipre took four Advanced+ and two Advanced Awards in this year's tests. It has a very clean design and good online help feature, which you can search directly from the program.

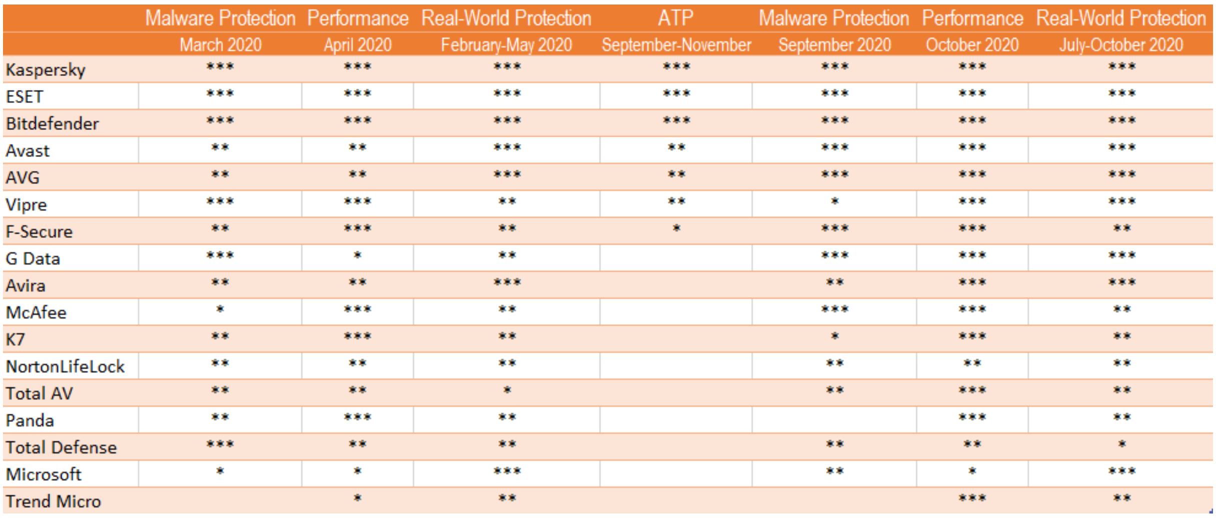
Advice on Choosing Computer Security Software

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 2020

AV-Comparatives provides a wide range of tests and reviews in comprehensive reports (https://www.av-comparatives.org/consumer/test-methods/). Annual awards for 2020 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 2020.



	Malware Protection	Performance	Real-World Protection	ATP	Malware Protection	Performance	Real-World Protection
	March 2020	April 2020	February-May 2020	September-November	September 2020	October 2020	July-October 2020
Kaspersky	***	***	***	***	***	***	***
ESET	***	***	***	***	***	***	***
Bitdefender	***	***	***	***	***	***	***
Avast	**	**	***	**	***	***	***
AVG	**	**	***	**	***	***	***
Vipre	***	***	**	**	*	***	***
F-Secure	**	***	**	*	***	***	**
G Data	***	*	**		***	***	***
Avira	**	**	***		**	***	***
McAfee	*	***	**		***	***	**
K7	**	***	**		*	***	**
NortonLifeLock	**	**	**		**	**	**
Total AV	**	**	*		**	***	**
Panda	**	***	**			***	**
Total Defense	***	**	**		**	**	*
Microsoft	*	*	***		**	*	***
Trend Micro		*	**			***	**

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 all combined scores of all tests

As in previous years, in 2020 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 2 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 (as is the case this year). In this situation, the product with the highest individual scores wins Product of the Year, while the others receive the Outstanding Product Award.

As in previous years, we will also be giving **Top Rated Awards** to a select group of tested products which reached a very high standard in the Public Consumer Main Series tests. 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** (see page 4), 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.

Product of the Year 2020

AV-Comparatives' 2020 Product of the Year Award goes to:

Kaspersky

Outstanding Products 2020

AV-Comparatives' 2020 Outstanding Product Awards go to (in alphabetical order):

Bitdefender, ESET

Top-Rated Products 2020

AV-Comparatives' Top-Rated Awards for 2020 go to (in alphabetical order):

Avast, AVG

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: **Kaspersky, Avast, AVG** and **Microsoft**.

AWARDS

Kaspersky

Avast, AVG

Microsoft

For details and full results of the 2020 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.

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

AWARDS

G Data

Bitdefender, ESET

Kaspersky

For details and full results of the 2020 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-positive 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 2020 were **ESET** (5), **Kaspersky** (15) and **Bitdefender** (19). These figures represent the SUM of the false positives from all FP Tests.

AWARDS

ESET

Kaspersky

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:

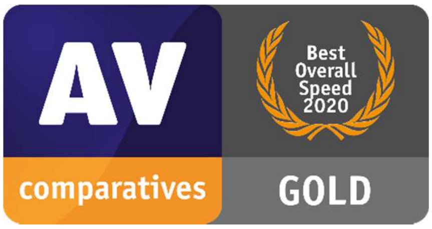
https://www.av-comparatives.org/consumer/testmethod/false-alarm-tests/

Overall Performance (Low System-Impact) winners

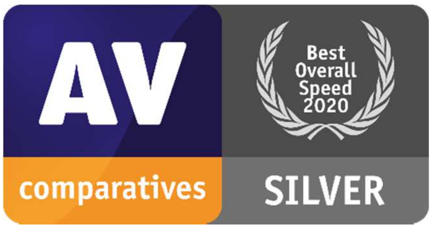
Security products must remain turned on under all circumstances, while users are performing their usual computing tasks. Some products may have a higher impact than others on system performance while performing some tasks.

K7, McAfee and **Kaspersky** demonstrated a lower impact on system performance than other products.

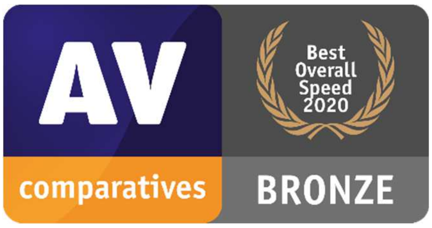
AWARDS



K7



McAfee



Kaspersky

For details and full results of the 2020 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.

Kaspersky blocked 14 targeted attacks (out of 15), **Bitdefender** and **ESET** blocked 13 attacks, **Avast** and **AVG** blocked 11 attacks.

AWARDS

AV
comparatives
ATP
2020
GOLD

Kaspersky

AV
comparatives
ATP
2020
SILVER

Bitdefender, ESET

AV
comparatives
ATP
2020
BRONZE

Avast, AVG

For details and full results of the 2020 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 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.

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. Our 2020 Security Survey indicates that about 9 out of 10 users are not happy with mandatory auto-renewal.

In the table below we have listed the (rounded) current discount price, full list price and auto-renewal prices (where applicable) for the paid products in the 2020 Main Test Series.

Product	Devices	Discounted[2] 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
Avira Antivirus Pro	1	35 €	47 €	47 €*	Yes (mandatory)
Bitdefender Internet Security	1	27 €	50 €	50 €*	Yes (optional)
ESET Internet Security	1	n/a	35 €	n/a	No
F-Secure SAFE	1	30 €	50 €	50 €	Yes (optional)
G Data Internet Security	1	n/a	40 €	28 €	Yes (optional)
K7 Total Security	1	20 €	34 €	n/a	No
Kaspersky Internet Security	1	28 €	40 €	40 €*	Yes (optional)
McAfee Total Security	1	30 €	70 €	70 €	Yes (mandatory)
NortonLifeLock Norton 360	1	30 €	75 €	75 €	Yes (mandatory)
Total AV Antivirus Pro	**3**	35 €	120 €	120 €	Yes (mandatory)
Total Defense Essential Antivirus	**3**	25 €	40 €	40 €*	Yes (mandatory)
Trend Micro Internet Security	1	25 €	50 €	50 €*	Yes (mandatory)
Vipre Advanced Security	1	22 €	50 €	50 €	Yes (mandatory)

Key: Ratio of rounded full list price/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.

**We presume that the auto-renewal price will be the same as the full list price. However, either the information on the vendor's website was unclear, or it stated that the vendor had the right to change the price on auto-renewal.*

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 compare 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 2020 Consumer Main Test Series tested free products by Avast, AVG, Microsoft and Panda. These products are not shown in the table, as pricing does not apply to them. For two of the products shown in the table, the lowest-price subscription allows you to install the product on three devices. If you only want to protect one device with these products, you will still have to pay the price shown here.

The terms "full list price" and "discounted price" could potentially be used by vendors in a misleading way. Some countries, such as the UK and Germany, have laws stating that a vendor can only use terms like "special offer" if the lower price is offered for a shorter period than the full list price. Readers might like to check the applicable law in the country from which they are purchasing the product. We have given the prices shown on the respective vendor's website at the time of writing (December 2020), applicable to users in Austria. We have not investigated if or for how long the full list prices stated on the vendors' websites have been offered. Thus we cannot say if they are in accordance with the applicable law in the country of purchase.

We should point out some good practices by some vendors. G Data is actually cheaper in the second year, and along with Bitdefender, ESET, F-Secure, K7 and Kaspersky does not impose auto-renewal on users.

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

User Experience Review

Review Format

For each of the tested products, we have looked at the following points (where applicable).

About the program

To start off with, we state whether the program is free or has to be paid for. We don't 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, whereby it is not important which component(s) are involved. It is not the number of features that is important, but how effectively they work. Also, different vendors may have different names for individual functions, or combine multiple types of functionality under one name. This could make it misleading to compare products using the vendors' component names. For readers' convenience, we do note any non-malware-related features, such as parental controls or spam filtering. With the exception of a replacement firewall (see below), we do not check the functionality of these additional features.

Setup

We note any options available, whether you have to make any decisions, and any other points of interest, such as introductory wizards that explain the program's features. We suggest that there should be a simple installation option for non-expert users. If at any stage the user has to make a decision in order to proceed, the options should be explained simply and clearly.

System Tray icon

Here we state what functionality is available from the program's System Tray icon. This can be a convenient way of accessing commonly-used functions, such as scans and updates. A System Tray icon is a standard feature for modern security programs for consumers. We regard it as a very useful means of showing that the program is running.

Security alerts

First, we disable the program's real-time protection, and check to see what alerts are shown. We also look for a quick and easy means of reactivating the protection. An effective status display, 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. We regard both of these as important for non-expert users. Additional pop-up alerts, which the user would see even if the program window were not open, are a desirable bonus. Next, we check how each program reacts when malware is encountered. We start off by downloading the EICAR test file (a harmless text file that antivirus products are programmed to detect for test purposes). We look to see what sort of alert is shown, if there are any options provided for dealing with the malware, if any information about the malware is given, and how long the alert is displayed. For non-expert users at least, we feel it is appropriate for a security program to show an alert when malware is detected, so that the user understands why the file in question cannot be downloaded/accessed. Also for non-expert users, 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.

The next step is to connect a USB flash drive to the review system, containing a few very prevalent and well-known malware samples. We note if any action is taken automatically by the security program, or if it prompts to scan the drive. If a scan is offered, we decline it, and open the drive in Windows Explorer. If the malware is not detected at this point, we attempt to copy the files on the drive to the Windows Desktop. If this is successful, we then execute them. We note at which stage the malware is detected, what sort of alert is shown, and if any action needs to be taken by the user.

All the programs in our Consumer Main-Test Series detect malware on execution, which is enough to keep the system free of infection. However, many users may expect their security program to detect malware on access, i.e. when the drive or folder containing it is opened in Windows Explorer, or at the latest when it is moved or copied. This would prevent them inadvertently passing on malicious files to somebody else on an external drive. We note that programs without on-access scanning may have a performance advantage as a result.

Scan options

Here we look at the different types of on-demand scan provided by each program, how to access and configure them, set scan exclusions, schedule scans, and what options are provided for PUA detection. We also look at how the results are displayed at the end of an on-demand scan, and whether the user needs to make any decisions. If multiple malicious files are found in a scan, it should be easy to carry out a safe action on all of them at once, rather than having to select an action for each one individually.

Quarantine

In the program's quarantine function, we look to see what information it provides about the detection location/time and the malware itself, and what options are available for processing it, e.g. delete, restore or submit to vendor for analysis.

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. We look to see if it possible to prevent other users of the computer from disabling the security program's protection features, or uninstalling 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 – can only change settings by entering a password. 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.

Help

In this section, we take a quick look at whatever help features can be directly accessed from the program itself. Some vendors will have additional online resources, such as manuals and FAQ pages, that can be found by visiting their respective websites.

Logs

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

Firewall

Some of the products in this year's tests have a replacement firewall. That is to say, they include their own firewall, which is used in place of Windows Firewall. For these products, we perform a very simple functionality test, to check that basic functions of their replacement firewalls work as expected. In essence, this just verifies that network discovery and file sharing are allowed on private networks, but blocked on public ones.

For this test, we use a laptop PC, running Windows 10 Professional, with a wireless network adapter. We share the Documents folder, with read and write permissions for "Everyone", and enable Remote Desktop access. In Windows Firewall/Advanced Sharing Settings, we turn on network discovery, file sharing, and Remote Desktop access for Private networks, but turn them all off for Public networks. We then verify that network access is working as expected in both Private and Public networks. It is initially connected to a wireless network that is defined as Private in Windows network status settings. We then install the security product with default settings, and reboot the computer. If during installation the third-party firewall in the security product were to prompt us to define the current network as public or private, we would designate it as private at that point. After the reboot, we check to see if we can still ping the PC, open and edit a document in its shared folder, and gain Remote Desktop access. We would expect the third-party firewall to allow all these types of access.

We then connect the laptop to a new, unknown wireless network, which we define as Public in Windows' network status prompt. If the third-party firewall were to display its own network-status prompt, we would also choose the public/untrusted option here. Next, we attempt to ping the test laptop (IPv4 and IPv6) from another computer on the same network, access its file share, and log in with Remote Desktop. We would expect the third-party firewall to block all these forms of access, as Windows Firewall would do.

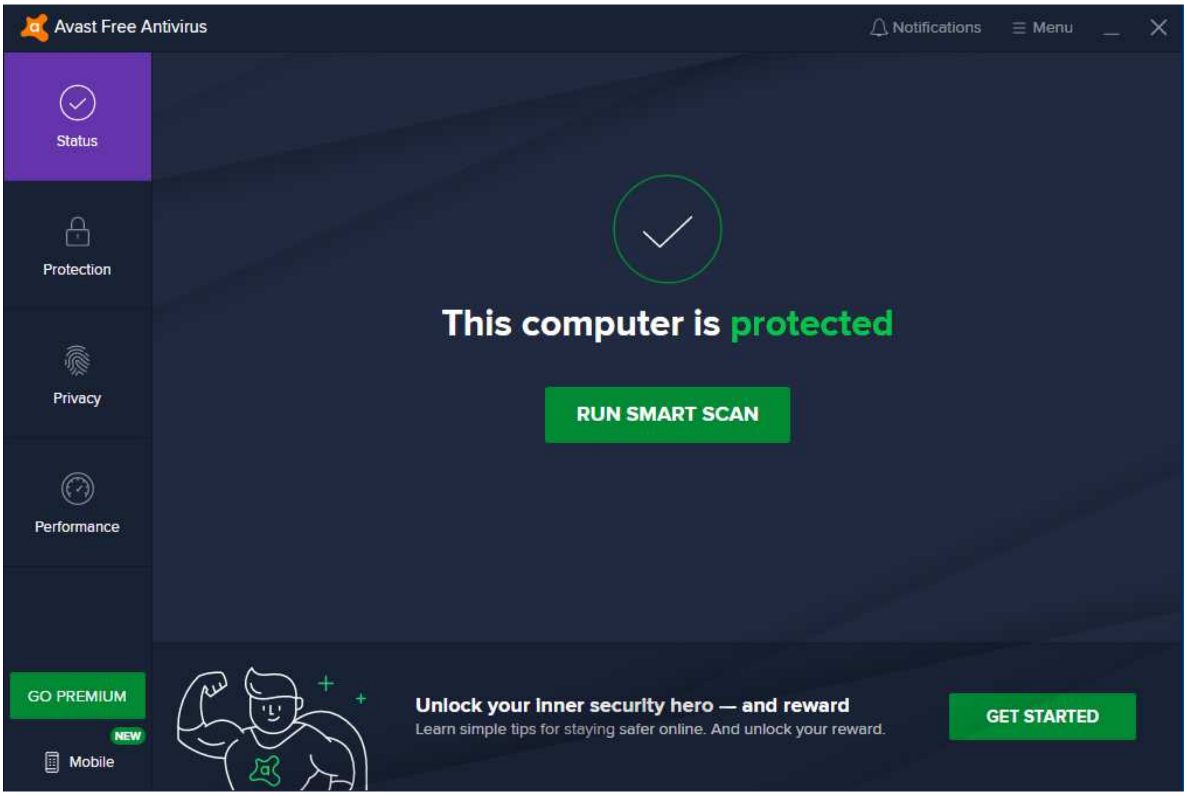
We also check what happens if the network status is changed from Private to Public in Windows network settings, i.e. if the third-party firewall in the tested product picks up the new status automatically, or displays its own prompt at that point.

In our opinion, a third-party firewall in a security program should either adopt Windows' network status settings automatically, or achieve the same result by means of displaying its own prompts. This allows laptop users to share files when at home, but keep intruders out when using public networks. We recognise that some users may like to use Windows Firewall – which is a known standard – rather than the third-party firewall in their security product. For such users, it is ideal if the security product's own firewall can be cleanly disabled (i.e. permanently disabled, without security alerts being constantly shown), and Windows Firewall can be activated instead. We check to see if this is possible.

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.

Avast Free Antivirus



This computer is protected

Unlock your inner security hero — and reward

Learn simple tips for staying safer online. And unlock your reward.

About the program

Avast Free Antivirus is, as its name suggests, a free security program. In addition to anti-malware features, it includes a manual software update feature and network-security scanner. You can find out more about Avast Free Antivirus on the vendor's website: https://www.avast.com/free-antivirus-download. Avast tell us that they have recently improved the accessibility features, and the product is WCAG 2.0 AA compliant. You can find out more about this standard here: https://www.w3.org/WAI/WCAG2AA-Conformance

Summary

The interface of Avast Free Antivirus is clean and modern, and makes most important features easy to find. Malware alerts and default actions on detection are good. By and large, it is very easy to navigate and use. The setup wizard provides the choice of a default, one-click installation, or a fully customisable install for power users, which we liked. The program actively promotes other Avast products, some of which have to be paid for. We would suggest that users obtain independent advice on what other types of security/performance-related products are appropriate to their needs before buying any additional products.

Setup

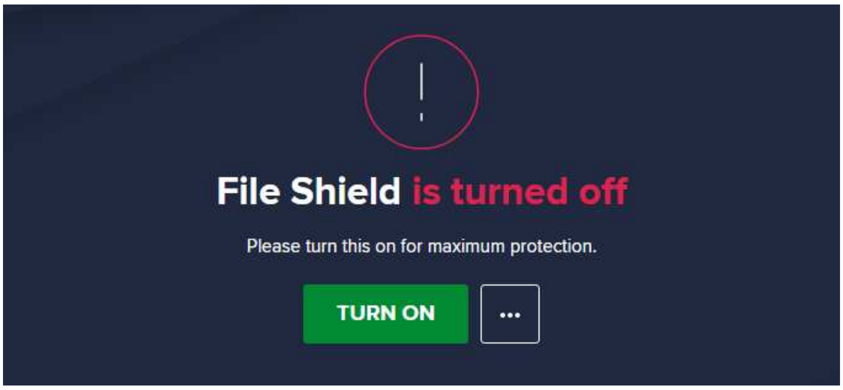
The default installation of Avast Free Antivirus includes the *Avast Secure Browser*, and sets this as the default browser. You can easily opt out of this by removing the relevant ticks (checkmarks) on the first page of the setup wizard. We chose not to install the Avast browser for our functionality test. Setup lets you change the interface language, after which you can simply click *Install*. For power users, a custom installation is provided. With this option, you can select individual components to be installed, and change the installation folder. We used the default configuration (all components except *Passwords* are installed). The wizard prompted us to run a *Smart Scan* when setup completed.

System Tray icon

The System Tray menu lets you open the program window, disable protection for a specified time, use "Silent Mode", open quarantine, update the program and/or definitions, and see program and registration information.

Security alerts

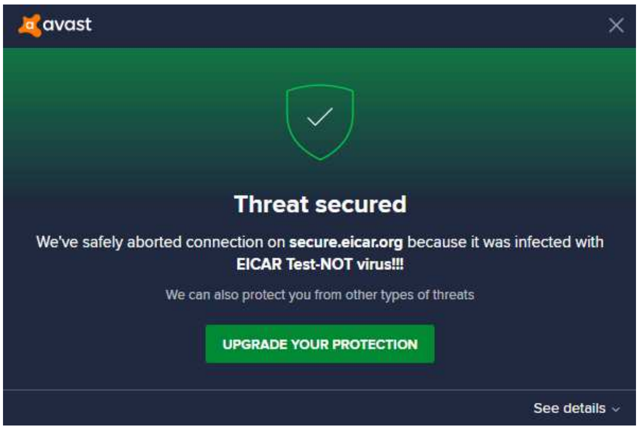
When we disabled real-time protection in the program's settings, an alert was shown on the program's home page (screenshot below). We were able to reactivate the protection easily by clicking *Turn On*.



File Shield is turned off

Please turn this on for maximum protection.

We note that if you click the three dots button, you will get the option *Ignore*. We do not recommend using this, as it permanently disables the warning message normally shown when protection is disabled. When we tried to download the EICAR test file, Avast blocked it and displayed the alert shown below. We did not need to take any action. The alert persisted until we closed it.



Threat secured

We've safely aborted connection on **secure.eicar.org** because it was infected with **EICAR Test-NOT virus!!!**

We can also protect you from other types of threats

When we connected a USB drive containing some malware to the system, Avast offered to scan the drive. This prompt can be disabled directly form the alert box. We chose not to run a scan, but instead opened the USB drive in Windows File Explorer. Avast did not initially take any action. However, as soon as we copied the malicious files to the Windows desktop, Avast detected and quarantined the copied files. An alert similar to the one above was shown, and a warning sound was played. If multiple malicious files are found at the same time, separate alerts are shown one after the other. You have to close each of these individually. Clicking on *See details* opens a panel at the bottom of the alert box, showing additional information. For e.g. the WannaCry worm, we could see the threat name, file name and path, the process that encountered the malware, and the Avast protection component that detected it. When we ran an on-demand scan of malware samples on a USB drive, Avast presented us with a list of threats found. From this, we were able to select all threats with one click, and deal with them by clicking *Resolve All*.

Scan options

The *Smart Scan* button on the home page runs a very quick malware scan, and checks for outdated apps and browser threats. It also displays "Advanced issues", which is a means of promoting features only found in Avast Premium Security. The *Protection\Virus Scans* page additionally provides the options *Full\Targeted\Boot-Time\Custom* scans. A *Custom* scan can be scheduled. You can also scan a drive, folder or file 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, but disabled for real-time protection. Scan exceptions can be configured on the *General* tab of the settings dialog.

Quarantine

Avast's quarantine feature is called *Virus Chest*. Here you can see 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*. It appears that the *Extract* function lets you restore the file to a custom location. We could not find any further information about the malware on the quarantine page.

Logs

A basic log of scans completed 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.

Help

The help feature can be accessed by clicking *Menu\Help\Help*. This displays a series of frequently asked questions, such as "How do I scan my PC for potential threats?" and "How do I resolve my protection status?", grouped together into categories. A simple text-only answer is provided for each question.

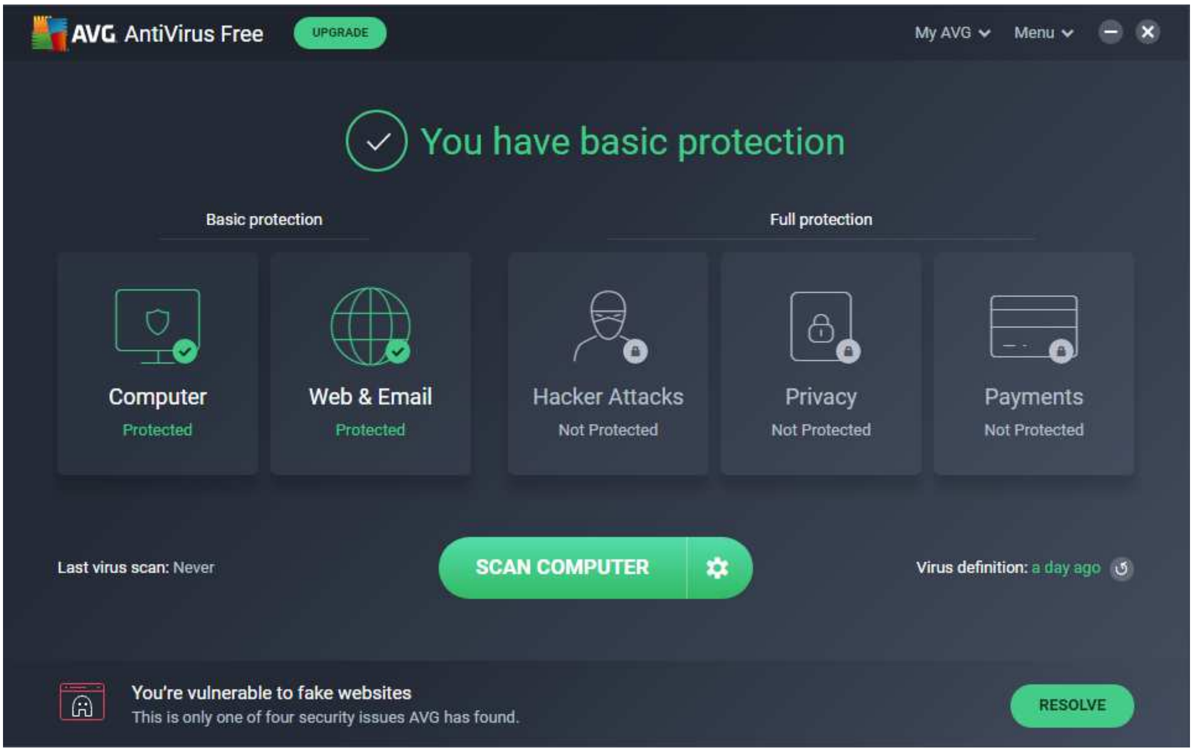
Access control

Standard Windows users have full access to the program's settings by default, and so can disable protection features. However, they cannot uninstall the program. It is possible to password protect the program under *Menu\Settings\Password*, and 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 on malware found.

Other points of interest

- When we first opened a web browser after installing Avast Free Antivirus, the Avast Online Security page on the Chrome Web Store was displayed.
- The *Rescue Disk* feature can be found on the *Protection\Virus Scans* page.
- 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 AntiVirus Free



About the program

AVG AntiVirus Free is a free security program, as its name suggests. In addition to anti-malware features, it includes *Data shredder,* a secure delete function. You can find out more about the program on the vendor's website: https://www.avg.com/en-eu/free-antivirus-download

Summary

The interface of AVG AntiVirus Free is straightforward to use, and makes most important features easy to find. Malware alerts and default actions on detection are good. By and large, it is very easy to navigate and use. The setup wizard provides the choice of a default, one-click installation, or a fully customisable install for power users, which we liked. The program advertises other, paid-for AVG products on its home page and in the default scan. We would suggest that users obtain independent advice on what other types of security/performance-related products are appropriate to their needs before buying any additional products.

Setup

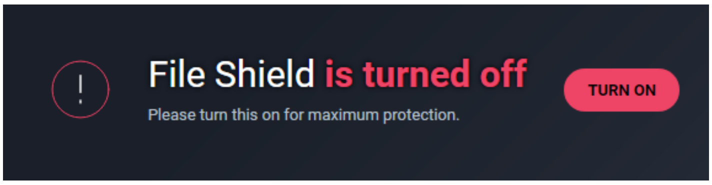
The default installation of AVG AntiVirus Free includes the *AVG Secure Browser*, and sets this as the default browser. You can easily opt out of this by removing the relevant ticks (checkmarks) on the first page of the setup wizard. We chose not to install the AVG browser for our functionality test. Setup lets you change the interface language, after which you can simply click *Install*. For power users, a custom installation is provided. With this option, you can select individual components to be installed, and change the installation folder. We used the default configuration (all components selected) here. The wizard prompted us to run a scan when setup completed. At the end of this, the user is prompted to run a *Smart Scan* once a month. When we first opened our default browser after installing AVG Free, we were prompted to install the AVG Online Security add-on from the Chrome Web Store.

System Tray icon

The System Tray icon menu lets you open the program, scan the computer, and disable protection.

Security alerts

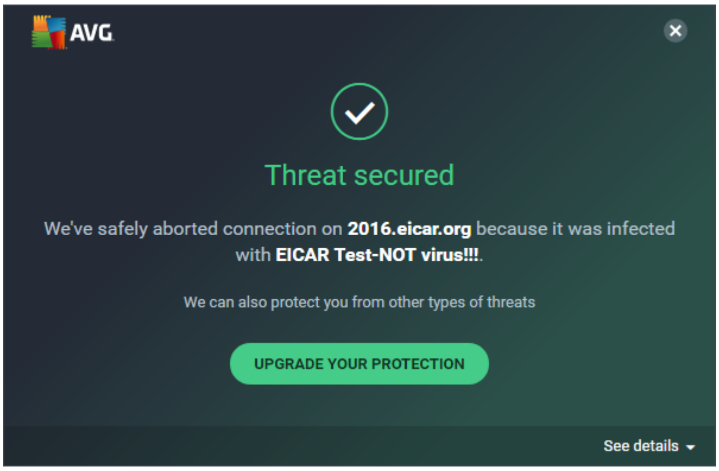
When we disabled real-time protection in the program's settings, an alert was shown on the status area (screenshot below) and *Computer* tile of the main program window. We were able to reactivate the protection easily by clicking *Turn on*.



File Shield is turned off

Please turn this on for maximum protection.

When we tried to download the EICAR test file, AVG blocked it and displayed the alert shown below. We did not need to take any action. The alert persisted until we closed it.



Threat secured

We've safely aborted connection on **2016.eicar.org** because it was infected with **EICAR Test-NOT virus!!!**.

We can also protect you from other types of threats

When we connected a USB drive containing some malware to the system, AVG offered to scan the drive. We chose not to run a scan, but instead opened the USB drive in Windows File Explorer. AVG did not initially take any action. However, when we copied the malicious files to the Windows Desktop, AVG immediately detected and quarantined them. An alert like the one above was shown. Clicking *See Details* opened a drop-down panel showing the threat name, file name and path, Windows process that encountered the malware, detection component, action taken, and an option to report the file as a false positive. An individual alert box was shown was shown for each malware item detected, and each had to be closed individually. When we ran an on-demand scan of malware samples on a USB drive, AVG presented us with a list of the items detected, and noted that they had all been quarantined. We then just had to click *Done* to close the scan results window.

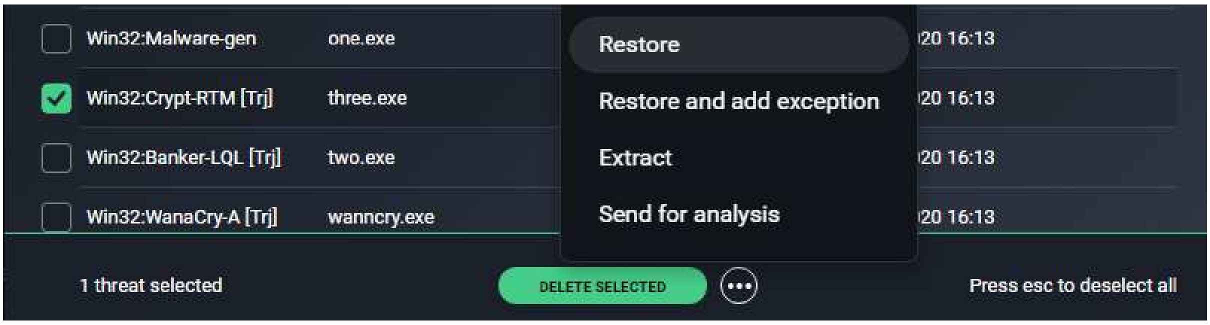
Scan options

The *Run Smart Scan* button on the home page runs a very quick malware scan, and checks for browser threats. It also displays "Advanced issues", which is a means of promoting features only found in AVG Internet Security. When the scan is finished, the program will prompt you to schedule a monthly scan. If you click the three dots icon next to the *Run Smart Scan* button, a menu with scan options opens. This additionally lets you run a *Deep Scan* (full scan), USB/DVD scan, file or folder scan, or boot-time scan. You can also set up a scheduled scan from here. It is also possible to scan a drive, folder or file using Windows Explorer's right-click menu.

Under *Menu\Settings\General\Exceptions* you can configure scan exceptions. *Basic Protection\Detections* lets you change the real-time protection's default detection behaviour (automatic) and PUA detection (ignore). Under *Basic Protection\Scans* you can configure the same options for on-demand scans. Here, the default behaviour is to detect PUAs. If malware is detected in an on-demand scan, the default behaviour is *Fix automatically*.

Quarantine

The quarantine page can be found in the *Tools* section of the *Menu*. This is shown below, along with available options for quarantined items.



☐	Win32:Malware-gen	one.exe	20 16:13
☑	Win32:Crypt-RTM [Trj]	three.exe	20 16:13
☐	Win32:Banker-LQL [Trj]	two.exe	20 16:13
☐	Win32:WanaCry-A [Trj]	wanncry.exe	20 16:13

1 threat selected

Press esc to deselect all

Logs

AVG AntiVirus FREE doesn't have separate log feature in. However, the date and time of malware detections can be seen in the *Quarantine* window.

Help

The help feature can be accessed by clicking *Menu\Help*. This displays a series of frequently asked questions, such as "How do I scan my PC for potential threats?" and "How do I resolve a red protection status?", grouped together into categories. A simple text-only answer is provided for each question.

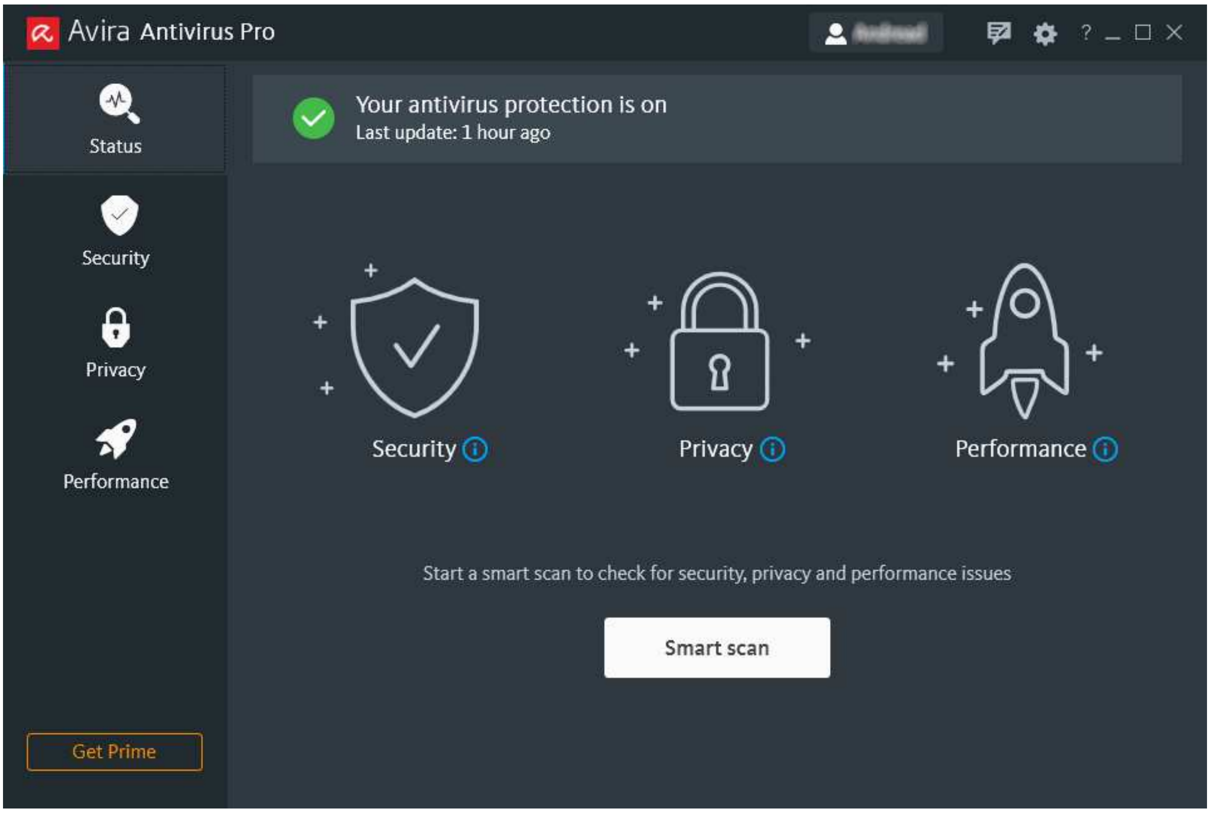
Access control

By default, Standard Windows Users are able to 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. It will not be possible to see the results, however. The *Require password only to access settings* option locks the settings dialog, but unauthorised users can still disable protection from the System Tray menu, or the *Computer* tile on the home page.

Other points of interest

- The update function is found under *Menu/Settings/General/Update*.
- By default, AVG 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.

Avira Antivirus Pro



Your antivirus protection is on
Last update: 1 hour ago

Start a smart scan to check for security, privacy and performance issues

About the program

Avira Antivirus Pro is a paid-for security program that includes anti-malware features and a VPN with data/location limitations. There is no free trial as such. However, Avira Free Antivirus has an identical interface, so you could use this to see what the program looks like. You can find out more about Avira Antivirus Pro on the vendor's website: https://www.avira.com/en/antivirus-pro

Summary

Installation of Avira Antivirus Pro is extremely simple, and the program's most essential features are easy to find. Safe default settings and sensible alerts are provided. Access control options are outstanding. Most of the program has a very modern, clean and touch-friendly interface. Aside from the display language, all options are found in an older, more mouse-oriented dialog. Avira Antivirus Pro promotes the company's *Prime* service.

Setup

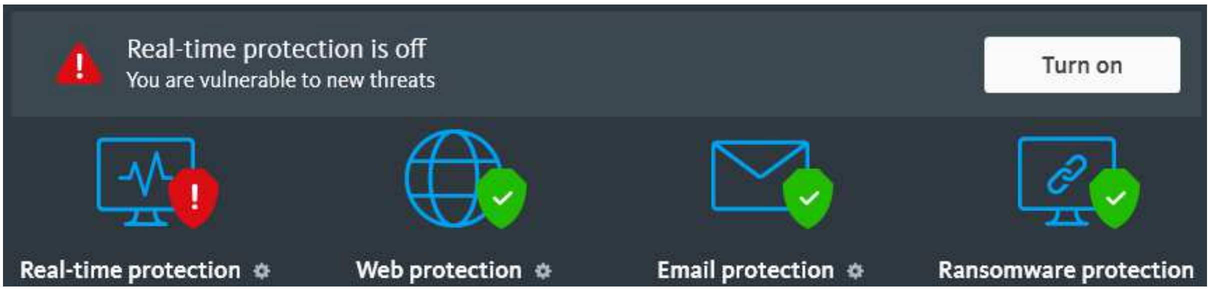
To install Avira Antivirus Pro, log in to your Avira online account and go to *Devices\Protect more devices\Windows* to download the installer. You can email a link to yourself from here. Just one click is required to install the program, and the installer window explains the program's features while it is being set up.

System Tray icon

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

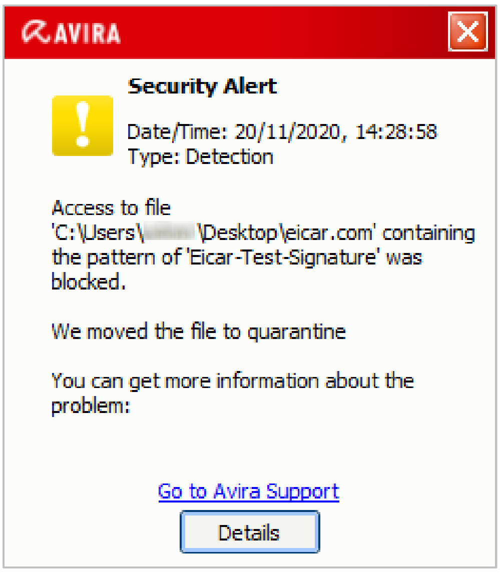
Security alerts

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



Real-time protection is off
You are vulnerable to new threats

When we downloaded the EICAR test file, Avira detected and quarantined the downloaded file. We did not need to take any action. The alert shown below was displayed, and persisted until we closed it. An audible alert was also played.



Security Alert

Date/Time: 20/11/2020, 14:28:58
Type: Detection

Access to file 'C:\Users\[redacted]\Desktop\eicar.com' containing the pattern of 'Eicar-Test-Signature' was blocked.

We moved the file to quarantine

You can get more information about the problem:

When we connected a USB drive containing some malware to our test system and opened it in Windows File Explorer, Avira immediately detected and quarantined the malicious files. An alert like the one above was shown, and the audio alert was also played. Clicking *Details* displayed the malware on the program's quarantine page.

When we ran an on-demand scan of malware samples on a USB drive, Avira presented us with a list of the items found, with a suggested action (*Clean up*) for each one. We just had to click *Apply now* to deal with all of them. We note that it is possible to change the suggested action for any threat by right-clicking its entry.

Scan options

You can run a *Smart Scan* from the button of the same name on the program's home page. This takes about a minute, and is supposed to check for security, privacy and performance issues. It serves to advertise Avira Prime, by showing additional actions that could be taken with this service.

Under *Security\Virus Scans* you can choose from quick, full and custom/scheduled scans. You can also scan a drive, folder or file by using Windows Explorer's right-click menu.

Scan options can be set by going to *Security\Protection options*, and clicking the cogwheel icon to the right of *Real-time protection*. This opens a dialog box in an older interface design, from which you can configure all protection options, including on-demand scans, password protection, and network protection. There are detailed choices for types of threat to be detected, including PUAs (detection is enabled by default), and the action to take when a threat is detected.

Quarantine

This displays the threat name, file name and path, plus date and time of detection. You can select individual quarantined files, or all together, and rescan, restore or delete them. No additional information about the malware samples is provided.

Logs

We could not find a log feature as such in Avira Antivirus Pro. The *Quarantine* page shows the date and time of malware detections.

Help

Clicking *Help* in the *?* menu opens Avira's online manuals page. Under *Windows* you will find a searchable FAQ feature. Simple text instructions and explanations are provided for each topic.

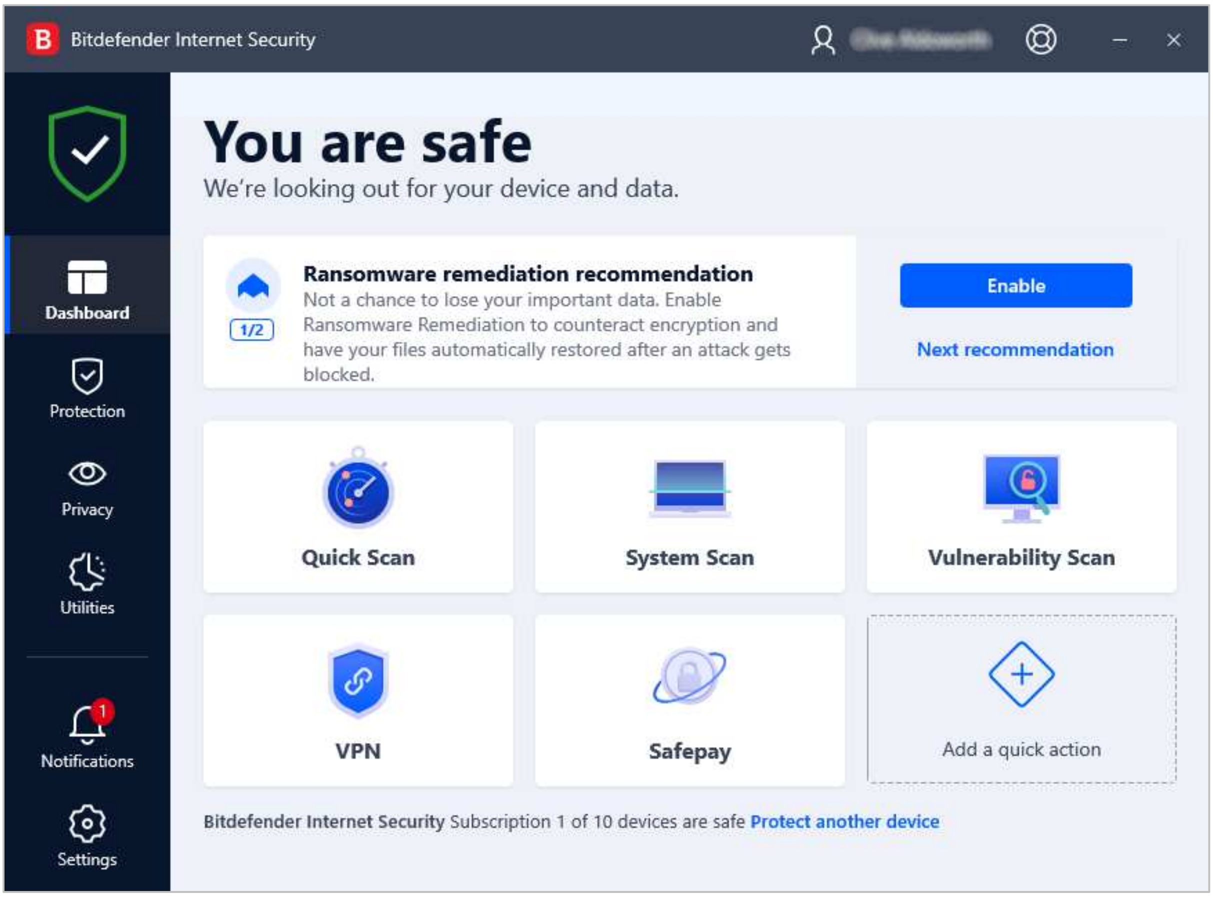
Access control

Standard Windows users cannot disable protection features, or uninstall the program. This is as it should be. There is also a password protection feature, which lets you specify in detail which actions are password protected. This can prevent other users disabling protection or uninstalling the program, amongst other things.

Other points of interest:

- The *Firewall* feature on the *Security* page provides controls for the Windows firewall. Avira does not provide its own firewall.
- Subscription information can be found by clicking the *?* menu, then *About, Manage my licences*. This opens the subscriptions page of your online Avira account.
- When we opened our default browser after installation, we were prompted to enable the *Avira Safe Shopping* add-on for Chrome.

Bitdefender Internet Security



You are safe

We're looking out for your device and data.

Ransomware remediation recommendation
Not a chance to lose your important data. Enable Ransomware Remediation to counteract encryption and have your files automatically restored after an attack gets blocked.

Bitdefender Internet Security Subscription 1 of 10 devices are safe Protect another device

About the program

Bitdefender Internet Security is a paid-for security program. In addition to anti-malware features, it includes a replacement firewall, vulnerability scanner, antispam, ransomware remediation, Wi-Fi security advisor, 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/solutions/internet-security.html

Summary

Bitdefender Internet Security is very straightforward to install and navigate, with almost all important functions easy to find. We liked the ability to customise the tiles on the home page. Malware on a USB drive is automatically detected in an instant, and access-control options are optimal. Default options are very safe for non-expert users. A double warning is shown if you try to access a risky website. However, we feel that co-ordination of the Bitdefender Firewall with Windows's security settings could be improved.

Setup

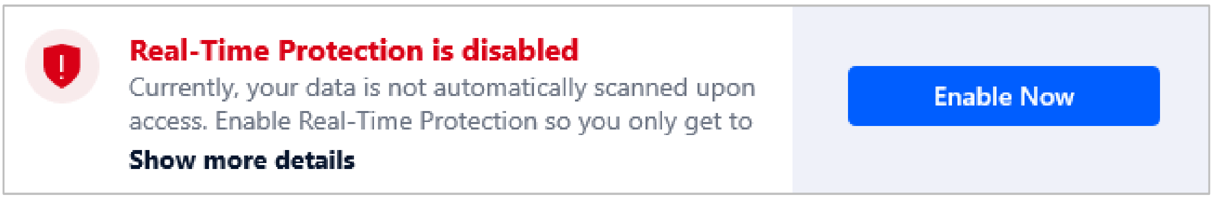
The setup wizard lets you choose the interface language, and opt out of sending product reports. Otherwise there are no decisions to make, and installation completes very quickly. An optional "Device Assessment" is suggested at the end of the setup process; this took 2 minutes in our functionality check. You have to create a Bitdefender account, or log in with an existing one. You can then enter a licence key, or opt to use the 30-day free trial.

System Tray icon

The System Tray icon menu lets you open the program window, run updates, and see program information.

Security alerts

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 Now*.

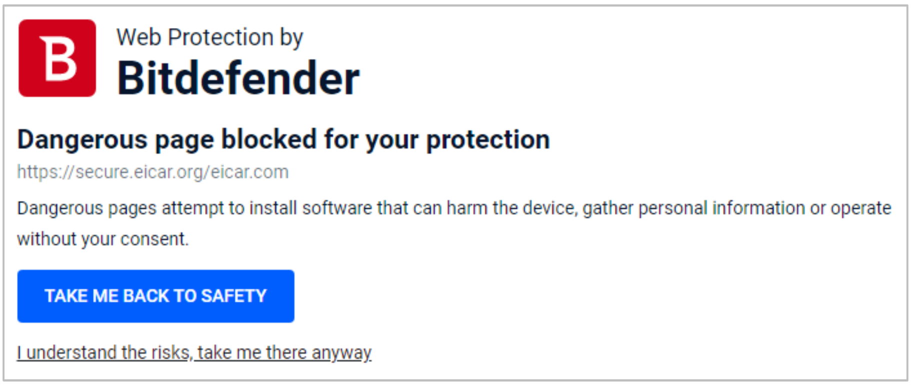


Real-Time Protection is disabled

Currently, your data is not automatically scanned upon access. Enable Real-Time Protection so you only get to

Show more details

When we tried to download the EICAR test file, Bitdefender initially showed a warning in the browser:



Web Protection by

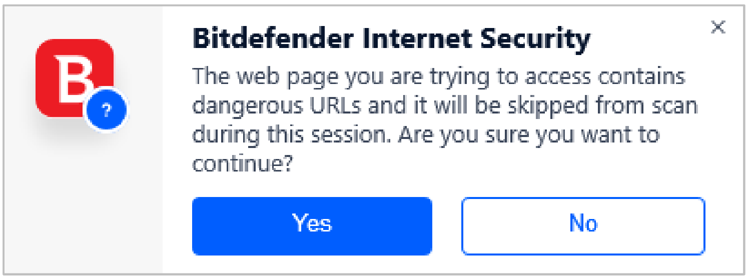
Bitdefender

Dangerous page blocked for your protection

https://secure.eicar.org/eicar.com

Dangerous pages attempt to install software that can harm the device, gather personal information or operate without your consent.

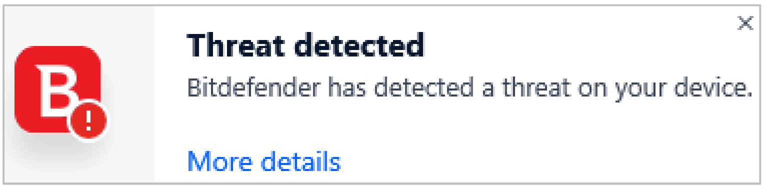
We persisted, by clicking *I understand the risks, take me there anyway*. Bitdefender then showed us a second alert:



Bitdefender Internet Security

The web page you are trying to access contains dangerous URLs and it will be skipped from scan during this session. Are you sure you want to continue?

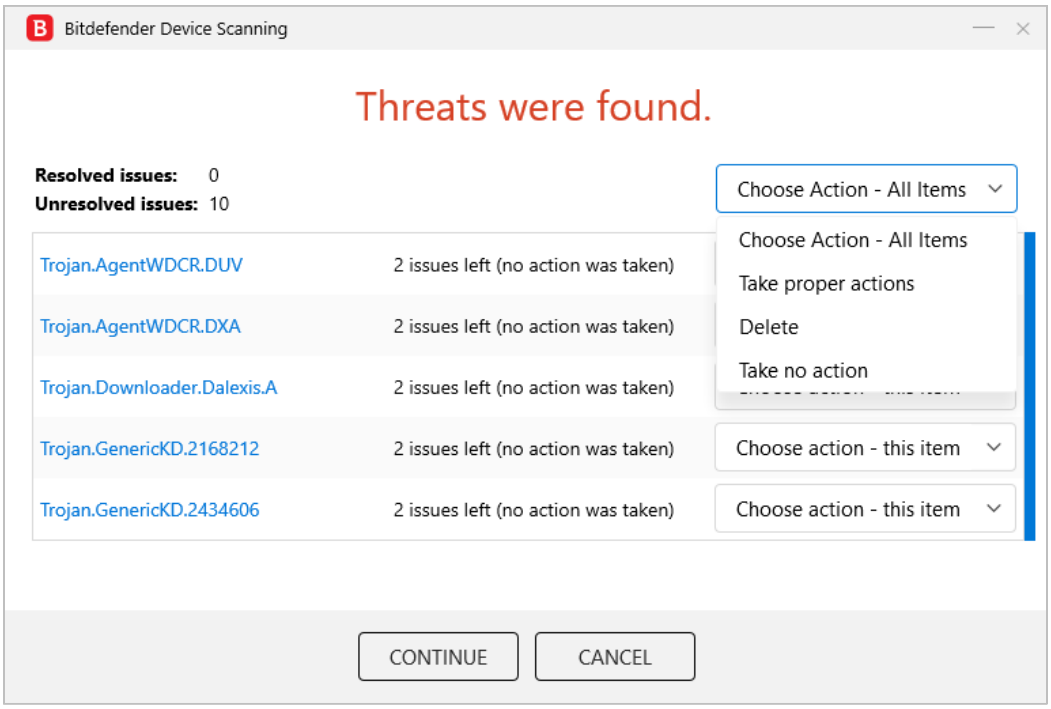
Again we persisted, by clicking *Yes*. Bitdefender then immediately detected and deleted the EICAR test file, and showed the alert below. We did not need to take any action. The notification closed by itself., and the alert closed after 30 seconds.



Threat detected

Bitdefender has detected a threat on your device.

When we connected a USB drive containing some malware to the system, Bitdefender offered to scan the drive. However, before we had had time to react to this, the program displayed a detection window, listing all the malicious files (shown below). We just had to select an action to take for all items (we chose *Take proper actions*) and click *Continue*. Bitdefender then quarantined the malware and ran a quick scan. We can only describe this proactive detection of malware on a USB device as exemplary.



Bitdefender Device Scanning

Threats were found.

Resolved issues: 0
Unresolved issues: 10

Trojan.AgentWDCR.DUV	2 issues left (no action was taken)
Trojan.AgentWDCR.DXA	2 issues left (no action was taken)
Trojan.Downloader.Dalexis.A	2 issues left (no action was taken)
Trojan.GenericKD.2168212	2 issues left (no action was taken)
Trojan.GenericKD.2434606	2 issues left (no action was taken)

Choose Action - All Items
Choose Action - All Items
Take proper actions
Delete
Take no action
Choose action - this item
Choose action - this item
CONTINUE
CANCEL

We found that even when we chose *Take no action* in the detection window, Bitdefender’s real-time protection still prevented the malware being copied or executed.

Scan options

The *Dashboard* page lets you run a *Quick Scan* or *System Scan*. Under *Protection\Antivirus\Scans* you can set up a *Custom Scan,* which can be scheduled. You are also provided with a wide range of options, including whether to scan for potentially unwanted applications, whether to scan the memory, and if only new and modified files should be scanned. On the *Settings* tab of the *Antivirus* page, you can create scan exceptions, open the quarantine, and configure (automatic) scanning of USB drives, optical media, and network drives.

Quarantine

The *Quarantine* page (found under *Protection*) shows the file name and path, detection name, and time/date that each item was quarantined. From here, you can select one or multiple items, and delete or restore them. The dialog box notes that restoring a file automatically excludes it from future scanning.

Logs

At the end of a scan, it is possible to see a log of that scan. Other than this, we could not find a log feature in the program.

Help

The lifebelt icon in the top right-hand corner of the window has links to the *User's Guide* and *Support Center*. The *User's Guide* is a very comprehensive manual of over 200 pages. It covers all aspects of installing, configuring and using the program. It includes a glossary of relevant technical terms, and contact details for Bitdefender's support services. The *Support Center* is a searchable FAQ. There are detailed instructions and explanations, very well illustrated with screen videos.

Access control

Standard Windows users cannot disable protection features, or uninstall the program. This is as it should be. You can also password protect the settings, meaning that no other users can disable protection without entering the password.

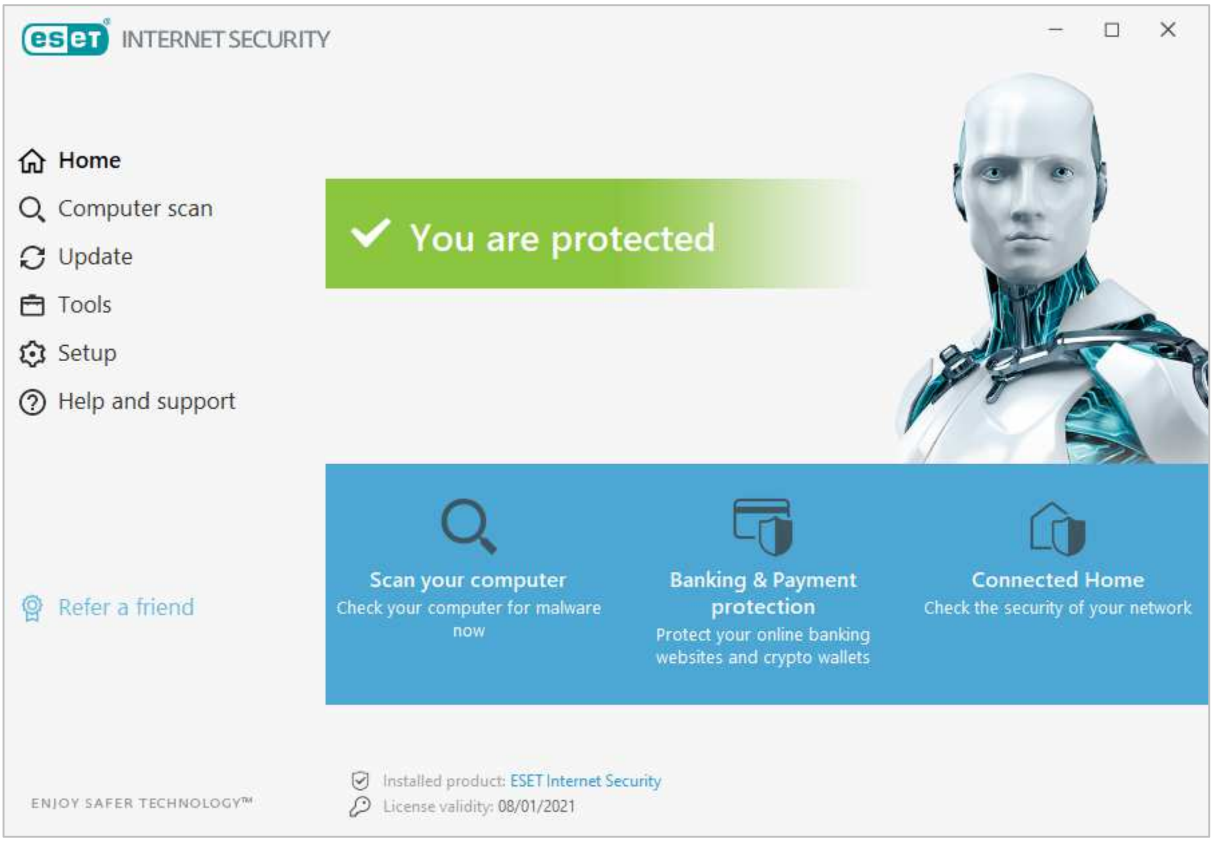
Bitdefender Firewall

In our functionality test, we found that the firewall in Bitdefender Internet Security does not co-ordinate perfectly with Windows security settings. If you join a new wireless network and designate this as public, the Bitdefender firewall will adopt this setting. However, if you then change the network type to private in Windows network settings, the Bitdefender firewall will not change, but will continue to see it as a public network. We feel this could be problematic if a user accidentally designated a wireless network in e.g. a coffee shop as public; trying to rectify the mistake by changing the network type to public in Windows settings would not have any effect. The user would need to go into the settings of the Bitdefender firewall and change the network type there. If you prefer to use Windows Firewall, you can cleanly disable the Bitdefender Firewall in the program's settings. This will activate the Windows Firewall.

Other points of interest:

- The update function can be found in the System Tray menu
- Subscription information can be found on the *My Account* page (user menu)
- The tiles shown on the *Dashboard* (home page) can be customised
- In the course of our functionality test, we were prompted to set up *Ransomware Remediation*
- When we first opened our default browser after installing Bitdefender, we were prompted to enable the *Bitdefender Wallet* extension for Chrome

ESET Internet Security



eset INTERNET SECURITY
Home
Computer scan
Update
Tools
Setup
Help and support
Refer a friend
ENJOY SAFER TECHNOLOGY™
✓ You are protected
Scan your computer
Check your computer for malware now
Banking & Payment protection
Protect your online banking websites and crypto wallets
Connected Home
Check the security of your network
Installed product: ESET Internet Security
License validity: 08/01/2021

About the program

ESET Internet Security is a paid-for security program. In addition to anti-malware features, it includes the ESET Firewall, Connected Home Monitor, Anti-Theft, Anti-Spam, Anti-Phishing, and Banking & Payment Protection. You can find out more about the program on the vendor's website: https://www.eset.com/int/home/internet-security/

Summary

We found ESET Internet Security to be very well designed and easy to use. Non-expert users are provided with safe default settings and a clean, easy-to-navigate interface. All the essential features are very easily accessed. The settings dialog – which has a useful search function – has plenty of advanced options for power users. Real-time file-system protection is very sensitive and reacts very quickly when needed. Help features are excellent.

Setup

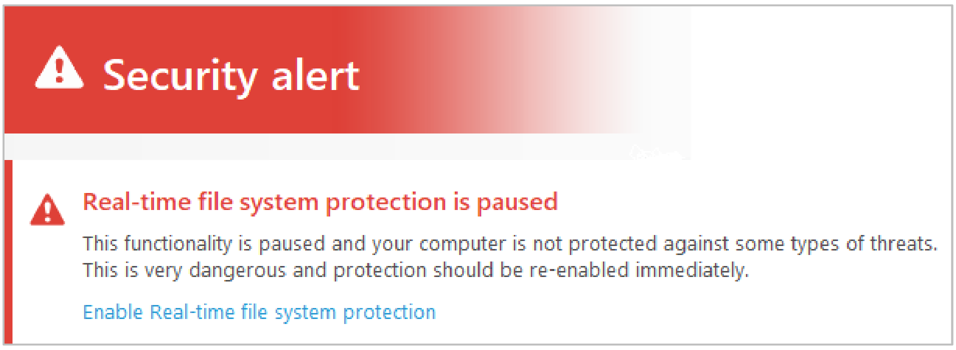
You can download the program from its page on the vendor's website. The installer lets you enter a licence key if you have one, or opt for a 30-day free trial. Setup is straightforward, and starts by letting you choose the interface language. You have to provide an email address, and decide whether to enable LiveGrid (data sharing), PUA detection, and the Customer Experience Improvement Program. However, the wizard provides an explanation of what each of these things does. At the end, you are prompted to set up Anti-Theft and Parental Control, though these are optional. An initial scan is run after installation.

System Tray icon

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

Security alerts

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



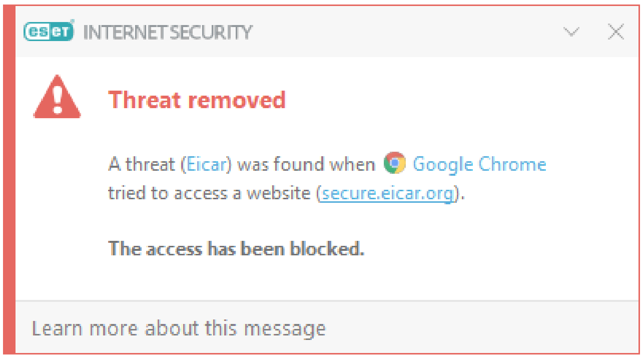
Security alert

Real-time file system protection is paused

This functionality is paused and your computer is not protected against some types of threats. This is very dangerous and protection should be re-enabled immediately.

Enable Real-time file system protection

When we tried to download the EICAR test file, ESET blocked it and displayed the alert shown below. We did not need to take any action, and the alert closed after 10 seconds. We note that this interval can be changed in the settings.



Threat removed

A threat (Eicar) was found when Google Chrome tried to access a website (secure.eicar.org).

The access has been blocked.

Learn more about this message

When we connected a USB drive containing some malware to the system, ESET offered to scan the drive. It's possible to change the default action here to *Automatic device scan* or *Do not scan*, using the program's settings. We chose not to run a scan, but instead opened the USB drive in Windows File Explorer. ESET's immediately detected and quarantined the malware. An alert like the one above was shown.

If multiple malicious files are found at the same time, ESET displays separate alerts for each one, shown one after the other. You can dismiss all the alerts at once from the menu in the top right-hand corner of the message box.

Clicking on the threat name in an alert box opens the relevant page of ESET's threat encyclopaedia in a browser window. For e.g. the WannaCry worm, ESET provides a very detailed information page about the threat. This includes a general description, information about files, folders, file extensions and registry entries created or modifies, plus screenshots of the malware's GUI and messages displayed.

When we ran an on-demand scan of malware samples on a USB drive, ESET displayed the number of detected threats, and noted that these had all been cleaned, in the program window. By clicking on Show Log, we were able to see the file names, paths and detection names, along with other scan details such as date and time.

Scan options

The default scan, accessible from the home page, is a "Smart Scan". The scope of this can be configured in the settings. The scan page, opened by clicking the *Computer scan* menu, has a number of options. You can run a complete system scan, removable media scan, or custom scan. The latter provides very granular options, including operating memory, boot sectors/UEFI, WMI database and registry. There is also an option to repeat the last scan. You can scan a file, folder or drive by dragging it to the *Computer scan* page, or using Windows File Explorer's right-click menu. Malware found in an on-demand scan is automatically quarantined. Under *Advanced Setup\Detection Engine\Real-Time & Machine Learning Protection*, you can choose whether to detect potentially unwanted applications, potentially unsafe applications (e.g. hacker tools), and suspicious applications (e.g. those using typical malware obfuscation packing). Scan exceptions can be set in the *Exclusions* section. *Real-time file system protection* lets you choose to detect malware on file open, creation, execution or removable media access (all on by default). Overall, ESET provides a very wide range of scanning and other options, letting users fine-tune the program to their requirements.

Quarantine

The *Quarantine* page can be found under the *Tools* menu\More tools. It shows the date and time of detection, file name and path, file size, detection name, number of occurrences, and name of the user that was active at the time. To delete a quarantined file, you have to right-click it and then click *Delete from Quarantine*. There is a *Restore* button, and also a *Move to quarantine* button. The latter allows you to browse the file system for any suspicious files that have not been detected yet. Once they are in quarantine, you can submit them for analysis, or delete them, using the right-click menu.

Logs

The *Logs* page is under the *Tools* menu\More tools. It provides records of detections, events (such as updates), and scan results, along with events relating to the program's other features, such as anti-spam and parental control.

Help

The *Help and support* page includes links to *Open help* and *Search ESET Knowledgebase*. The former opens an online manual, with topics such as *System requirements, Installation* and *Beginner's guide* in a menu column on the left-hand side of the page. Each page opens detailed explanations and instructions, very clearly laid out, and well illustrated with annotated screenshots. The *Knowledgebase* lets you search for specific queries, such as exclusions.

Access control

Standard Windows users cannot disable protection features, or uninstall the program. This is as it should be, in our opinion. Additionally, you can password protect the settings (*Setup\Advanced setup\User interface\Access setup*). If this is set up, any other users can operate all the features of the program, but not disable protection in any way.

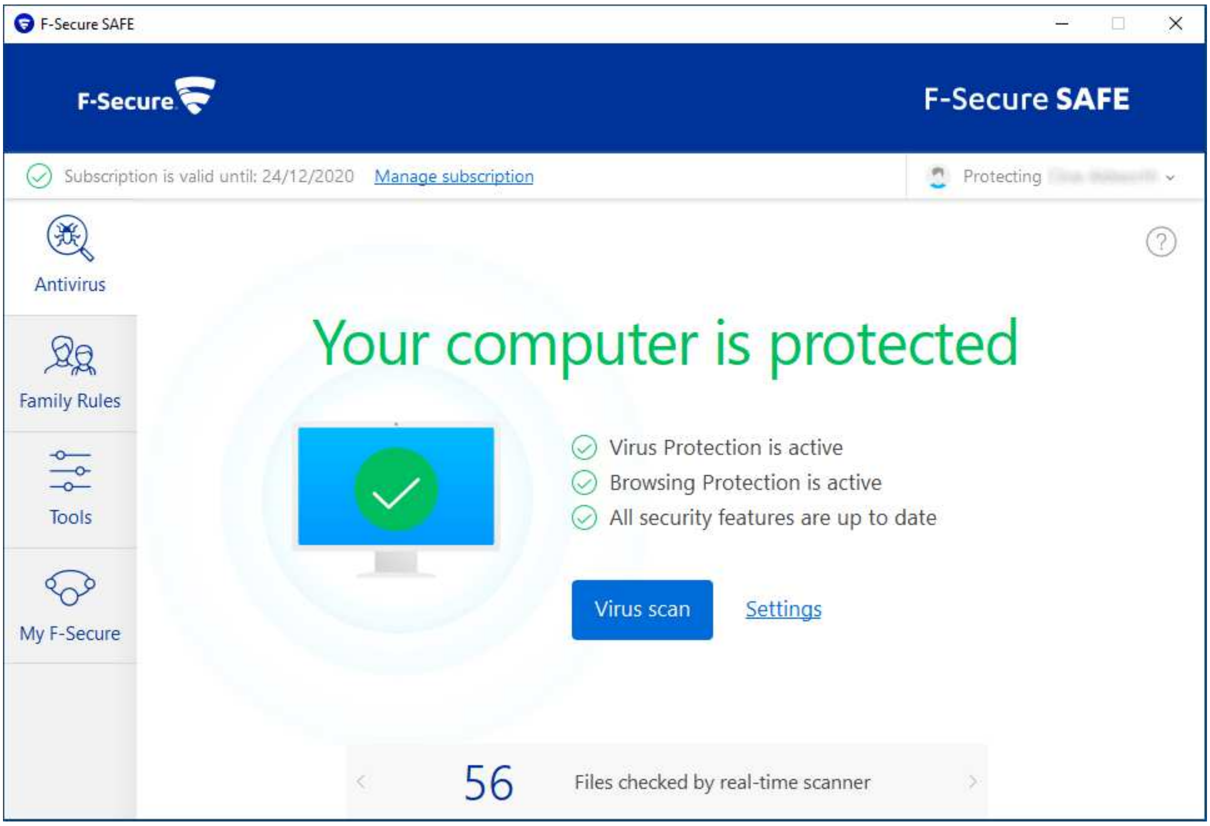
ESET Firewall

In our functionality test, the firewall in ESET Internet Security behaved exactly as expected. It co-ordinated perfectly with Windows' own network-type settings. It allowed network access such as file sharing in a network we had designated as private, but blocked it in a network we had defined as public. This is exactly as it should be, we feel. Should you nonetheless prefer to use Windows Firewall, you can cleanly disable the ESET Firewall in the program's settings. This will activate the Windows Firewall.

Other points of interest

Under *Tools\More tools*, ESET provides a number of useful system utilities. *Running processes* lists currently active processes with a reputation score, relative number of users, time of discovery, and software manufacturer. *Network connections* shows you which programs have made network connections, and the IP address of the remote computer, along with transfer speeds and amount of data sent/received. You can use *Watch activity* to view dynamic graphs of file system activity and network activity. All of these utilities could be useful for investigating suspicious behaviour on your system.

F-Secure SAFE



Subscription is valid until: 24/12/2020

Protecting [redacted]

Your computer is protected

Virus Protection is active

Browsing Protection is active

All security features are up to date

56 Files checked by real-time scanner

About the program

F-Secure SAFE is a paid-for security program. In addition to anti-malware features, it includes parental controls. You can find out more about the program on the vendor's website: https://www.f-secure.com/en/home/products/safe

Summary

We found F-Secure SAFE to be straightforward to install and use. The program window is quite simple and clean, with a number of features found in the *Tools* menu and *Settings* dialog. Real-time protection is sensitive, and alerts are kept simple. One suggestion for improvement would be to show the "Fix-all" button when any protection features are disabled.

Setup

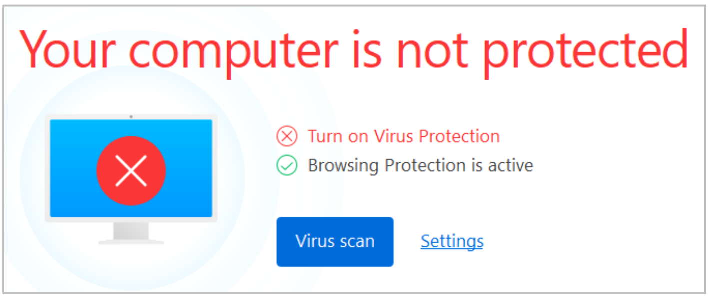
First of all, you have to create an F-Secure account and log in to it on the vendor's website. To download the installer, you have to specify if you want to install SAFE on your own computer, your child's computer, or another device. This allows for the parental control feature in the program.
Once you have downloaded and run the installer, you have the options of changing the language and sending anonymous user data. A single click then starts installation, and in less than a minute the program is up and running. A Chrome extension has to be approved.

System Tray icon

The System Tray menu lets you access your online account, check for updates, view messages and events, open settings, use gaming mode and see program information.

Security alerts

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). No "Fix-All" button was provided, so to reactivate protection, we had to go into the program's settings and find the relevant switch. We note that when we disabled all protection components (*Tools\Turn of all security features*), a very obvious *Turn on* button appeared on the home page, allowing us to restore complete protection with a single click. If any or all protection components are disabled individually from the *Settings*, the *Turn on* button is not shown. The rationale behind this escapes us.

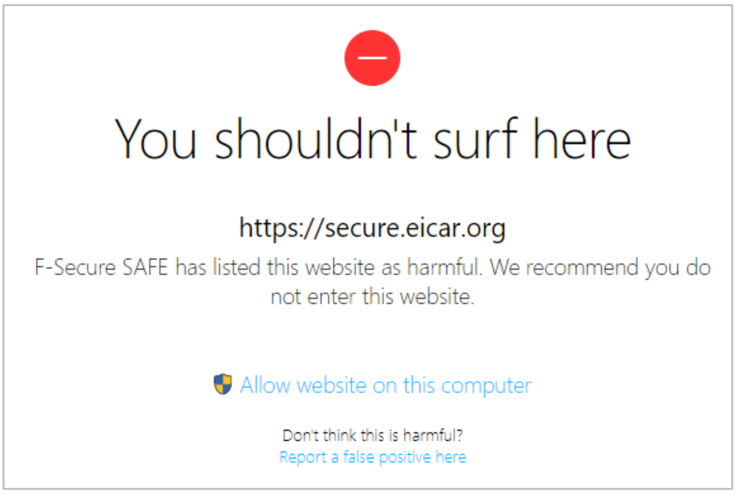


Your computer is not protected

Turn on Virus Protection

Browsing Protection is active

When we tried to download the EICAR test file, F-Secure initially showed a warning in the browser:



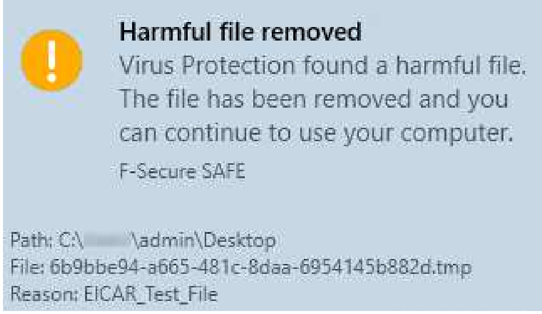
You shouldn't surf here

https://secure.eicar.org

F-Secure SAFE has listed this website as harmful. We recommend you do not enter this website.

Don't think this is harmful?
Report a false positive here

We persisted, by clicking *Allow website on this computer*. After we had confirmed a Windows User Account Control prompt initiated by F-Secure, we were able to download the file. However, as soon as the download was complete, F-Secure detected and quarantined the file. The alert below was shown. We did not need to take any action, and the alert closed after about 10 seconds.



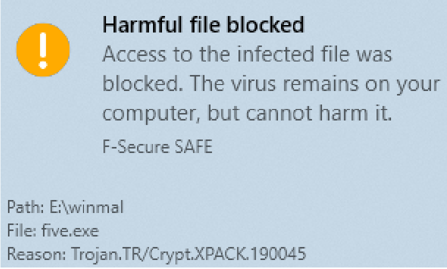
Harmful file removed

Virus Protection found a harmful file. The file has been removed and you can continue to use your computer.

F-Secure SAFE

Path: C:\[redacted]\admin\Desktop
File: 6b9bbe94-a665-481c-8daa-6954145b882d.tmp
Reason: EICAR_Test_File

When we connected a USB drive containing some malware to the system, F-Secure prompted us to scan the drive. The prompt can be disabled in the settings if you prefer. We chose not to run a scan, but instead opened the drive in Windows File Explorer. F-Secure immediately displayed the alert below:



Harmful file blocked
Access to the infected file was blocked. The virus remains on your computer, but cannot harm it.
F-Secure SAFE

Path: E:\winmal
File: five.exe
Reason: Trojan.TR/Crypt.XPACK.190045

Whilst F-Secure did not delete the files from the flash drive, we were unable to execute or copy any of them. When we ran an on-demand scan of malware samples on a USB drive, F-Secure presented us with a list of the items found, with both file and detection names. The default action to be taken for each one (*Clean Up*) was shown, and could be changed. We just had to click *Handle all* to deal with all of the items at once.

Scan options

The *Virus Scan* button on the program's home page runs a quick scan. You can run a full scan by going to *Virus scan options* in the *Tools* menu. A scheduled scan can be set up under *Settings\Scanning settings\Scheduled scanning*. You can also scan a drive, folder or file using the right-click menu in Windows Explorer. Exclusions can be set under *Tools\App and file control\Excluded*. There is no means of configuring PUA detection.

Quarantine

You can open the *Quarantine* function from the main page of the *Settings* dialog. It shows the date and time of detection, plus file name and detection name. From here, you can allow or delete individual quarantined files. You can click on the detection name of any file to see a description of it in F-Secure's online malware encyclopaedia. For the samples used in our functionality test, only generic descriptions were provided.

Logs

The log feature is found by clicking the *Tools* menu, then *Recent events*. It shows various system events, including installation, changes in protection status, and detections.

Help

You can open the help feature by clicking the question-mark symbol in the top right-hand corner of the main window. A local help file opens, with a list of topics in a left-hand menu column. These explain the essential functions of the program and how to use them, using simple text instructions.

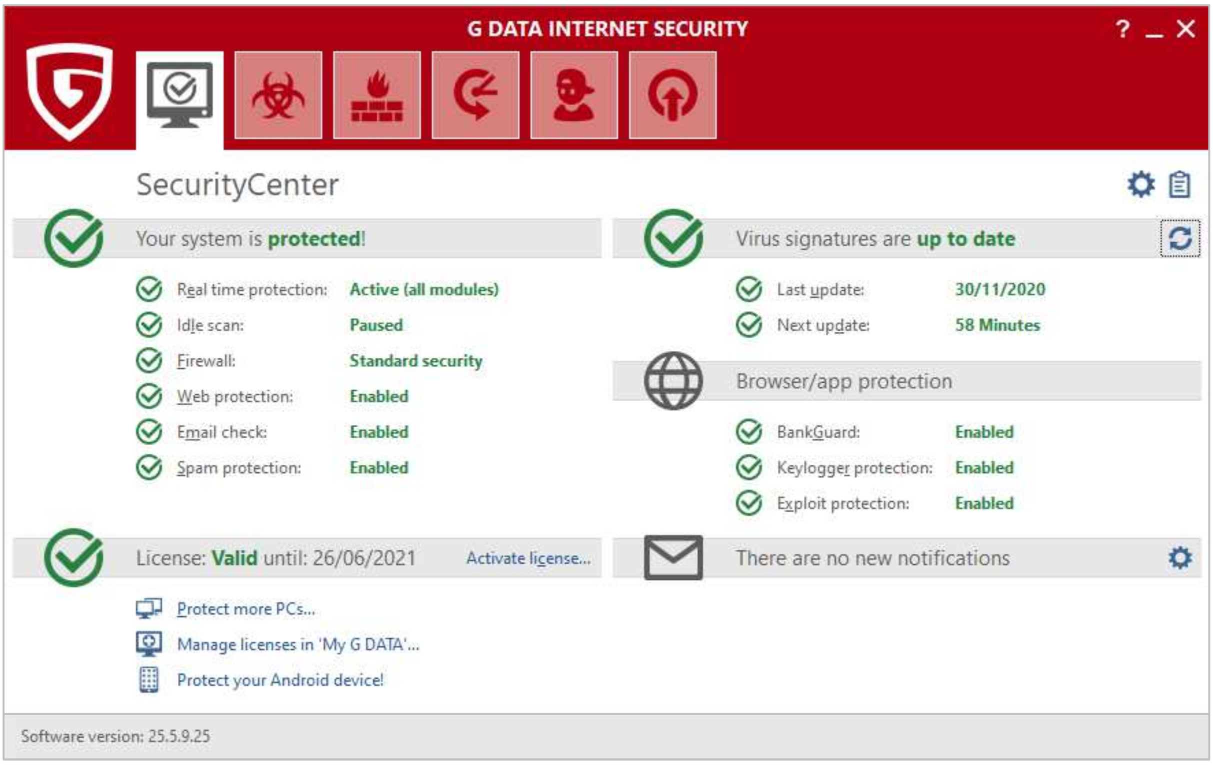
Access control

Standard Windows users cannot disable protection features, or uninstall the program. This is as it should be, in our opinion. We could not find a password-protection feature in the program.

Other points of interest:

- When you first log in to a Standard Windows User Account, F-Secure prompts you to set up parental controls.
- Updates and subscription information can be found under *Settings\Updates* and *Settings\Support* respectively.

G Data Internet Security



SecurityCenter

Your system is **protected!**

Real time protection: Active (all modules)
Idle scan: Paused
Firewall: Standard security
Web protection: Enabled
Email check: Enabled
Spam protection: Enabled

Virus signatures are **up to date**

Last update: 30/11/2020
Next update: 58 Minutes

Browser/app protection

BankGuard: Enabled
Keylogger protection: Enabled
Exploit protection: Enabled

License: **Valid** until: 26/06/2021 Activate license...

There are no new notifications

Protect more PCs...
Manage licenses in 'My G DATA'...
Protect your Android device!

Software version: 25.5.9.25

About the program

G Data Internet Security is a paid-for security program. In addition to anti-malware features, it includes a replacement firewall, backup function, and parental controls. You can find out more about the program on the vendor's website: https://www.gdatasoftware.com/internet-security

Summary

We found G Data Internet Security to be largely very straightforward to install and use. The status display provides details of individual protection components, and access control is excellent. We do however have some concerns that the G Data Firewall might leave users unknowingly unprotected in public Wi-Fi networks.

Setup

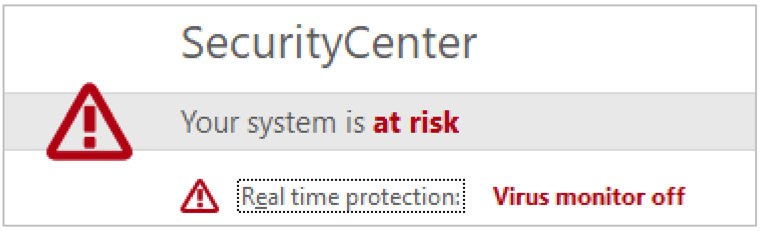
The setup wizard starts by asking you which interface language you would like to choose. There is then a choice of *Standard* or *User-Defined Installation*. The latter lets you choose which optional components, such as anti-spam and parental controls, to install. You can also change the installation folder. At the end of the wizard, you can enter a license key, or opt for the 30-day trial. You need to restart your computer to finish the installation.

System Tray icon

The System Tray icon menu lets you open the program window, disable malware protection, disable the G Data firewall, disable *Autopilot*, and see protection statistics.

Security alerts

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

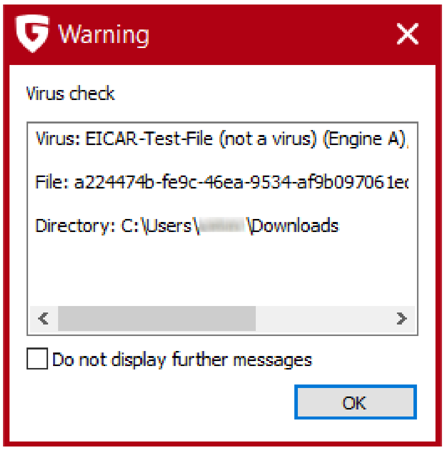


SecurityCenter

Your system is **at risk**

Real time protection: **Virus monitor off**

When we tried to download the EICAR test file, G Data deleted the file, and showed the alert below. We did not need to take any action. The alert persisted until we closed it.



Warning

Virus check

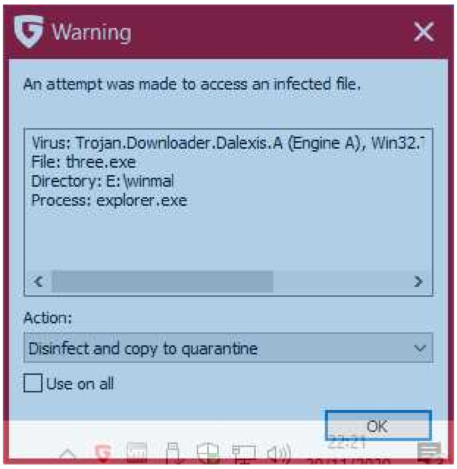
Virus: EICAR-Test-File (not a virus) (Engine A),

File: a224474b-fe9c-46ea-9534-af9b097061e

Directory: C:\Users\ \Downloads

□ Do not display further messages

When we connected a USB drive containing some malware to the system, G Data offered to scan the drive. This prompt can be disabled directly from the dialog box, if you so choose. We declined to run a scan, but instead opened the drive in Windows File Explorer. G Data immediately detected the malicious files, and displayed the dialog box shown below. We took the default action for all detected threats, whereby the files were moved to quarantine.



Warning

An attempt was made to access an infected file.

Virus: Trojan.Downloader.Dalexis.A (Engine A), Win32.
File: three.exe
Directory: E:\winmal
Process: explorer.exe

Action: Disinfect and copy to quarantine

□ Use on all

When we ran an on-demand scan of malware samples on a USB drive, G Data presented us with a list of items found. The default action to be taken (this can be changed for individual files) was *Disinfect and copy to quarantine*. We just had to click *Execute actions* to deal with all of the samples at once.

Scan options

The *Virus protection* page (second icon from left on the top toolbar) provides a number of different scan options. These are: *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 drive, folder or file using Windows File Explorer's right-click menu. Scan options let you choose which protection components should be used (all are on by default). You can also choose whether to detect potentially unwanted programs (on by default). Exceptions for both real-time protection and on-demand scans can be set in the *Anti-Virus* section of the *Settings* dialog.

Quarantine

The quarantine function can be opened from the *Anti-Virus* page. It shows the date and time of detection, threat name, file name and path. You can disinfect, delete or restore items one at a time.

Logs

Logs can be opened from the clipboard icon in the top right-hand corner of the window. You can see detections and signature updates. Clicking on any item displays a details pane below with more information, such as program and signature versions, protection components used, and areas scanned.

Help

The question-mark icon in the top right-hand corner of the window opens G Data 's online help pages. These take the form of a searchable manual, with items listed in categories such as *First Steps*, *Virus Protection* and *Settings*. For each item, there is a very detailed page of instructions and explanations, very well illustrated with screenshots.

Access control

Standard Windows users cannot disable protection features. You can also password protect the settings, to prevent any other users changing them.

G Data Firewall

In our functionality test, G Data Firewall did not co-ordinate with Windows' network settings at all. Nor did it display any prompts of its own regarding network type. We feel that this could lead to users unknowingly being exposed to threats on public Wi-Fi networks.

We installed the program on a system with the currently connected network defined as public, on which ping, file-sharing and RDP access were blocked by Windows. After installing G Data Internet Security and rebooting the system, we found that all three forms of access were allowed on this network. When we connected to a new wireless network, and defined this as public in the Windows prompt, G Data again allowed ping, file-sharing and Remote Desktop access, even though these had been blocked in Windows settings. When we changed the current network type from *Trusted* (the default for all networks) to *Untrusted* in G Data 's settings (under *Firewall\Networks\Show networks*), we found that ping and Remote Desktop access were immediately blocked. However, we were still able to access the file share, and add, edit or delete documents in it. It was not until we rebooted the computer that access to the file share was blocked.

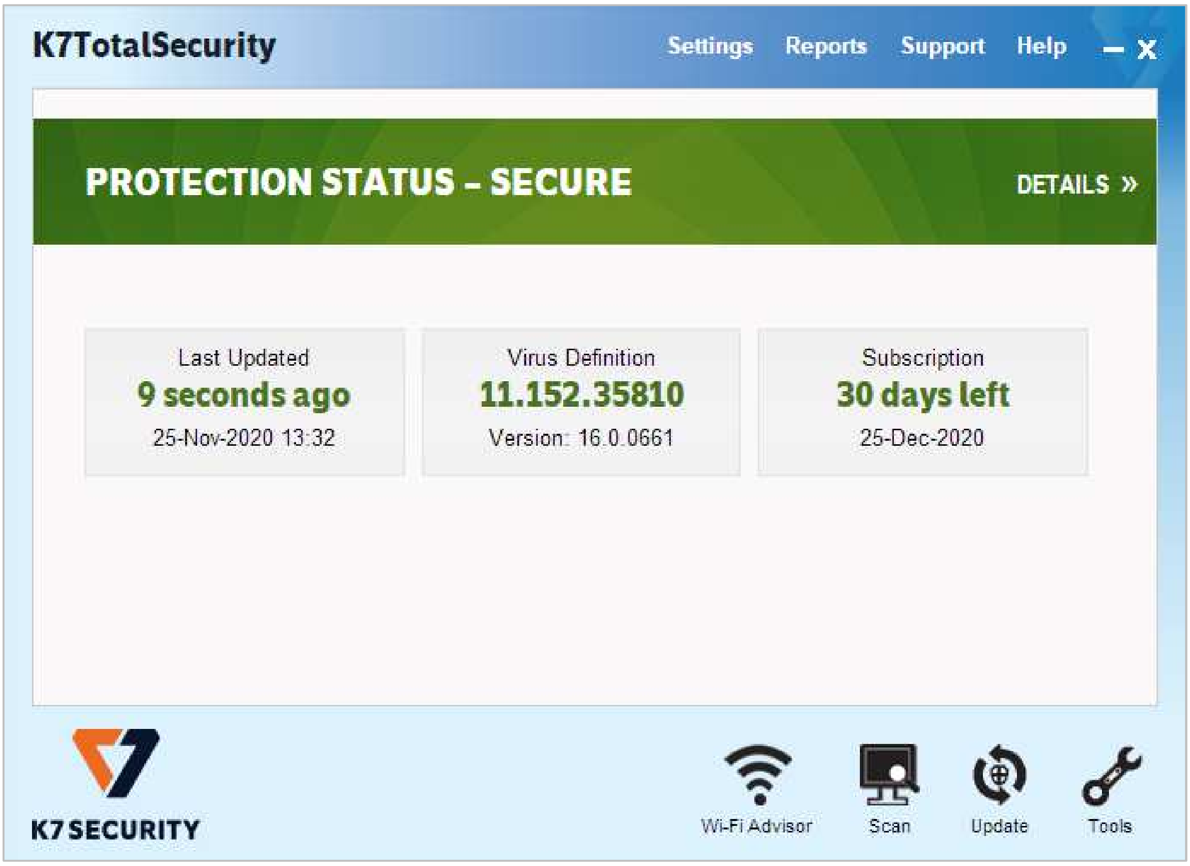
Our advice to users of G Data Internet Security would be to check in the program's own network settings that the current network is configured appropriately. If it is necessary to change the network type here, they should then reboot the computer.

We could not find a means of disabling the G Data firewall and using Windows Firewall instead. However, the *User-Defined Installation* will allow you to deselect installation of the G Data Firewall, in which case the Windows Firewall will remain active.

Other points of interest

- After installation, we were prompted to install the G Data add-on for Google Chrome.
- A G Data prompt asked whether updates should be installed using the current network connection. We assume that this is to let users avoid updating when using metered connections.

K7 Total Security



PROTECTION STATUS – SECURE

Last Updated
9 seconds ago
25-Nov-2020 13:32

Virus Definition
11.152.35810
Version: 16.0.0661

Subscription
30 days left
25-Dec-2020

About the program

K7 Total Security is a paid-for security program. In addition to anti-malware features, it includes a basic parental control feature, with a blacklist/whitelist web filter and Internet time restrictions. There is also an anti-spam feature, a replacement firewall, tune-up function, and secure delete feature. You can find out more about the product on the vendor's website: https://k7computing.com/us/home-users/total-security

Summary

We found K7 Total Security to be very simple to install, and straightforward to use. The most important everyday functions can easily be accessed from the home page. Real-time protection is very sensitive, and the default actions for connecting external drives and malware detection are ideal. Access control is very good. There is a minor non-security issue with the K7 Firewall, which blocks write access to file shares.

Setup

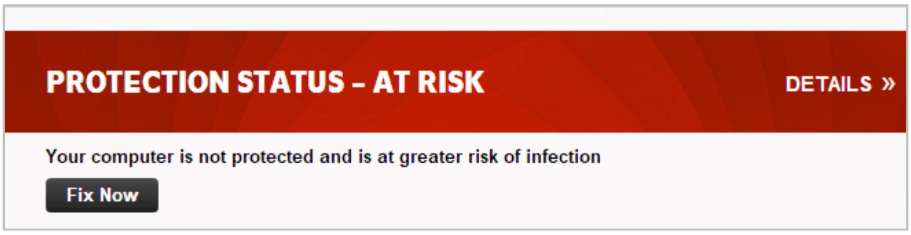
Installation is extremely quick and simple. Having started the installer file, you just need to click *Install*, and less than a minute later the program is up and running. At the end of the wizard, you have to supply an email address, and enter a licence key or opt for the 30-day trial.

System Tray icon

The System Tray menu lets you open the program, run scans and updates, disable protection, stop network traffic, enable gaming mode, see product information, and access help features.

Security alerts

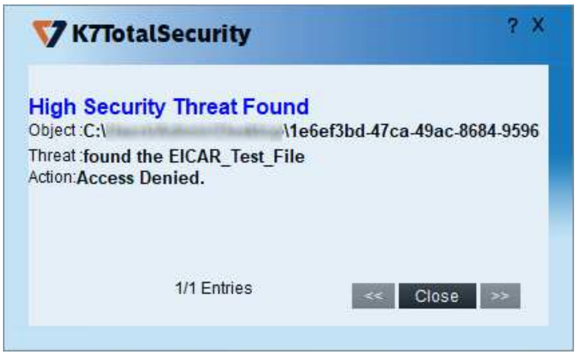
When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). We were able to reactivate the protection easily by clicking *Fix Now*.



PROTECTION STATUS – AT RISK

Your computer is not protected and is at greater risk of infection

When we tried to download the EICAR test file, K7 blocked it and displayed the alert shown below. We did not need to take any action, and the alert closed after a few seconds.



K7TotalSecurity

High Security Threat Found

Object :C:\[redacted]\1e6ef3bd-47ca-49ac-8684-9596

Threat :found the EICAR_Test_File

Action:Access Denied.

1/1 Entries

When we connected a USB drive containing some malware to the system, K7 offered to scan the drive. This prompt can be disabled directly from the dialog box if you wish. We chose not to run a scan, but instead opened the USB drive in Windows File Explorer. K7 immediately detected and quarantined the malicious files, and alerts like the one above were shown (one for each sample). When we ran an on-demand scan of malware samples on a USB drive, K7 displayed a list of the threats that had been found, with file name/path and detection name. It informed us that they had all been removed, and so no further action was necessary.

Scan options

The *Scan* button at the bottom of the program window lets you run quick, complete, custom, rootkit and scheduled scans. You can also scan a drive, folder or file using Windows Explorer's right-click menu. Under *Settings\Antivirus and Antispyware*, you can choose whether to scan for PUA (on by default), and set scan exclusions. It's also possible to change the default action on detection from here.

Quarantine

The quarantine feature is found under *Reports\Quarantine Manager*. From here, you can delete or restore detected malware items. The page shows date and time of detection, file name and path, malware type, and file hash.

Logs

You can find the logs feature under *Reports\Security History*. The *Virus Found Events* page shows the date and time of detections, current user at the time, application involved, file name and path, malware type, and action taken.

Help

If you click on *Help* in the top right-hand corner of the window, a local help file opens. This lists a variety of topics, covering the configuration and use of the product. Simple, clear instructions are provided for each topic, illustrated with screenshots where appropriate.

Access control

Standard Windows users are not able to disable protection features, or uninstall the program. This is as it should be, in our opinion. You can also set password protection, so that all users must enter a password to disable protection by any means.

K7 Firewall

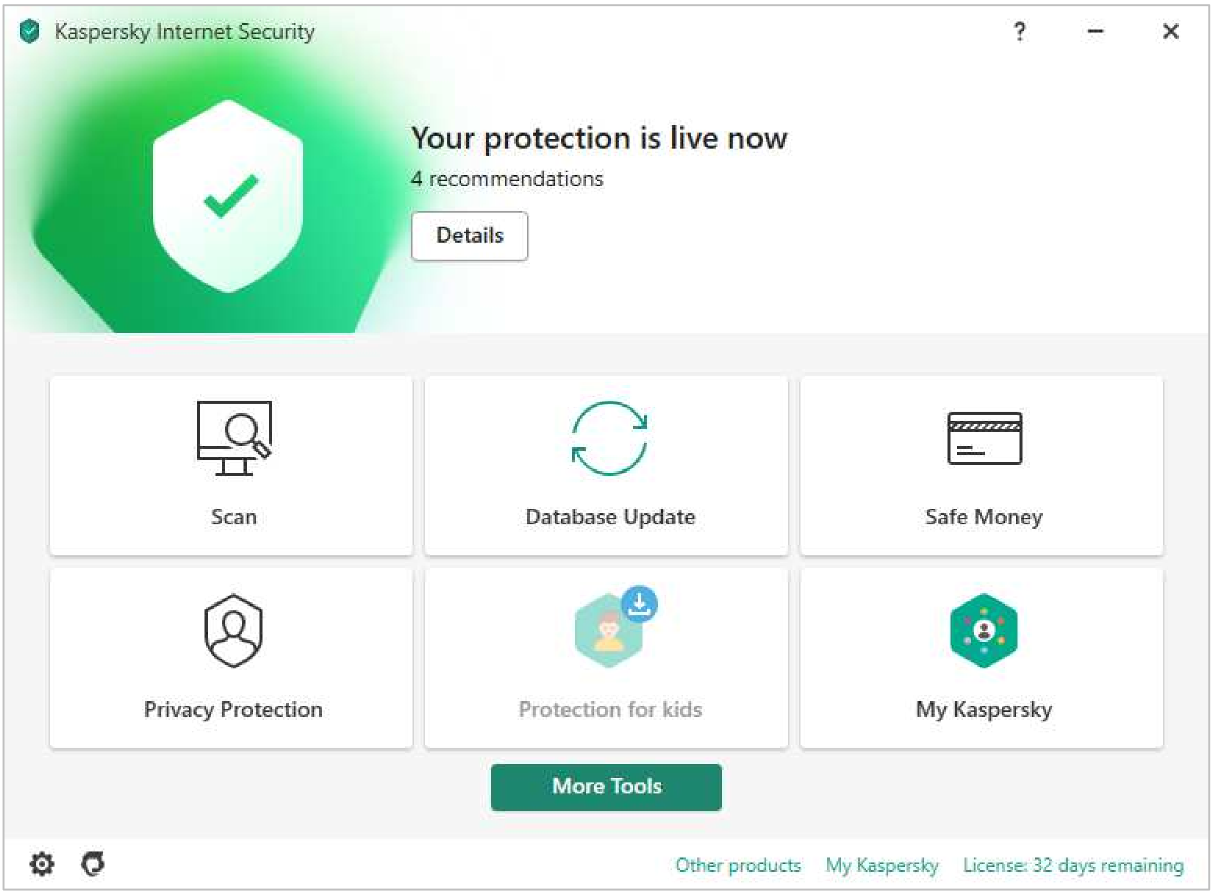
In our functionality test, the firewall in K7 Total Security co-ordinated very well with Windows' own network-type settings. It allowed network access such as (read-only) file sharing in a network we had designated as private, but blocked it in a network we had defined as public. This is exactly as it should be, we feel. We did however find that the minor problem reported last year, namely that write access to file shares is blocked, still exists. This does not affect security.

Other points of interest

While testing K7 Total Security, we found a serious bug, relating to network security, which applied to its enterprise product as well. We immediately reported this to K7, who have now fixed the problem in all its products[3]. We recommend users of K7 to ensure that their products are up to date.

[3] https://support.k7computing.com/index.php?/solutions/view-article/Advisory-issued-on-23rd-October-2020

Kaspersky Internet Security



Your protection is live now

4 recommendations

About the program

Kaspersky Internet Security is a paid-for security program. In addition to anti-malware functions, it includes ransomware protection, set of privacy protection functionalities including banking protection, webcam protection, a VPN (with server/data limitations) and browser privacy features. You can find out more about the product on the vendor's website: https://www.kaspersky.com/internet-security

Summary

Installation is straightforward, with safe default options. Kaspersky's modern, tiled interface makes all essential features easily accessible from the program's home page. The program deals with malware detection automatically, without requiring any user decisions. Advanced users will find a wide range of configuration options in the settings. The program promotes Kaspersky Safe Kids, which is a freemium parental control product. We feel that co-ordination of the Kaspersky Firewall with Windows's security settings could be improved.

Setup

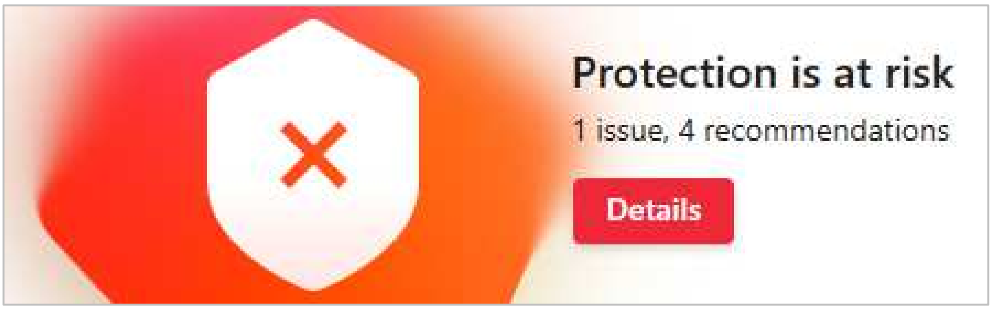
Having accepted the License/Privacy agreement, and decided whether to join the optional Kaspersky Security Network and allow use of your data for marketing purposes, you come to the install page. Here you can opt out of installing Kaspersky Password Manager (on by default). Then you just have to click *Install* to start setup. At the end of the wizard, four options are presented (all selected by default). These are: *Turn on protection against ads to install only desired software and block additional installations; Delete malicious tools, adware, auto-dialers and suspicious packages; Detect other software that can be used by criminals to damage your computer or personal data; Take a tour through the application features*. The introductory tour introduces the banking protection, webcam protection, browser privacy, and parental control features. You can then enter a licence key, or opt to use the 30-day trial. When the program window first opens, it encourages you to create/log in to a *My Kaspersky* online account. However, you can just click *Skip* if you don't want to do this.

System Tray icon

The System Tray icon menu lets you open the program window, pause protection, open settings, view the program's support page, see program information, and shut the program down.

Security alerts

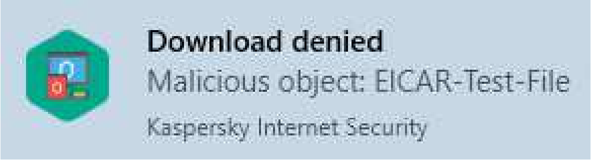
When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below), and as a Windows pop-up alert. We were able to reactivate the protection easily by clicking *Details*, then *Enable*.



Protection is at risk

1 issue, 4 recommendations

When we tried to download the EICAR test file, Kaspersky blocked the download, and displays an alert page in the browser. This included a link to the Kaspersky online threat encyclopaedia. A Windows pop-up alert was also displayed (shown below). We did not have to take any action, and the alert closes after a few seconds.



Download denied

Malicious object: EICAR-Test-File

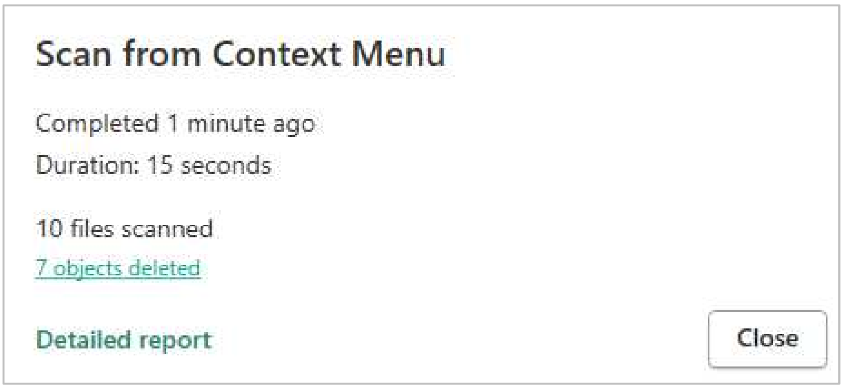
Kaspersky Internet Security

When we connected a USB drive containing some malware to the system, Kaspersky automatically scanned the root directory of the device. As our malware samples were contained within a folder on the drive, the automatic scan did not detect them. However, as soon as we opened this folder in Windows Explorer, Kaspersky immediately detected and quarantined the malicious files. Alerts were shown (one for each sample), similar to the one above. We note that the default removeable drive scan can be set to scan the entire drive, rather than just the root folder. We suggest that this might be a good idea.

Scan options

The *Scan* button on the program's home page opens the *Scan* page. This provides a choice of full, quick, custom, removable media and vulnerability scans. You can also scan a drive, folder or file from Windows Explorer's right-click menu. Scan exclusions are available in the program's settings (cogwheel icon in the bottom left-hand corner of the window), under *Threats and Exclusions*. You can specify which protection components – e.g. real-time protection, on-demand scans – the exclusion should be applied to. PUA detection is also found on the *Threats and Exclusions* page.

When we ran an on-demand scan of malware samples on a USB drive, Kaspersky Internet Security quarantined the items and displayed the following dialog box:



Scan from Context Menu

Completed 1 minute ago

Duration: 15 seconds

10 files scanned

7 objects deleted

Quarantine

The quarantine feature can be found by clicking *More Tools* on the program's home page. It shows the file name and path, detection name and date/time of detection, along with action taken, for every item. From here, you can select files individually and delete or restore them.

Logs

The log function can be opened by clicking the *More Tools\Reports*. A wide variety of reports is provided, including individual reports for the different protection components, such as *File Anti-Virus, Web Anti-Virus* and *Firewall*. There are also reports for additional features, such as *Anti-Spam* and *Software Updater*.

Help

The question-mark symbol in the top right-hand corner of the window opens Kaspersky's online manual for the program. Straightforward text-only instructions for each feature are provided. A left-hand menu column lets you navigate easily to other topics.

Access control

Standard Windows users have full control of the program's settings, and can disable protection features. However, only administrator accounts can uninstall the program. You can password protect the program. All users then have to enter the password to access settings or disable protection by any means.

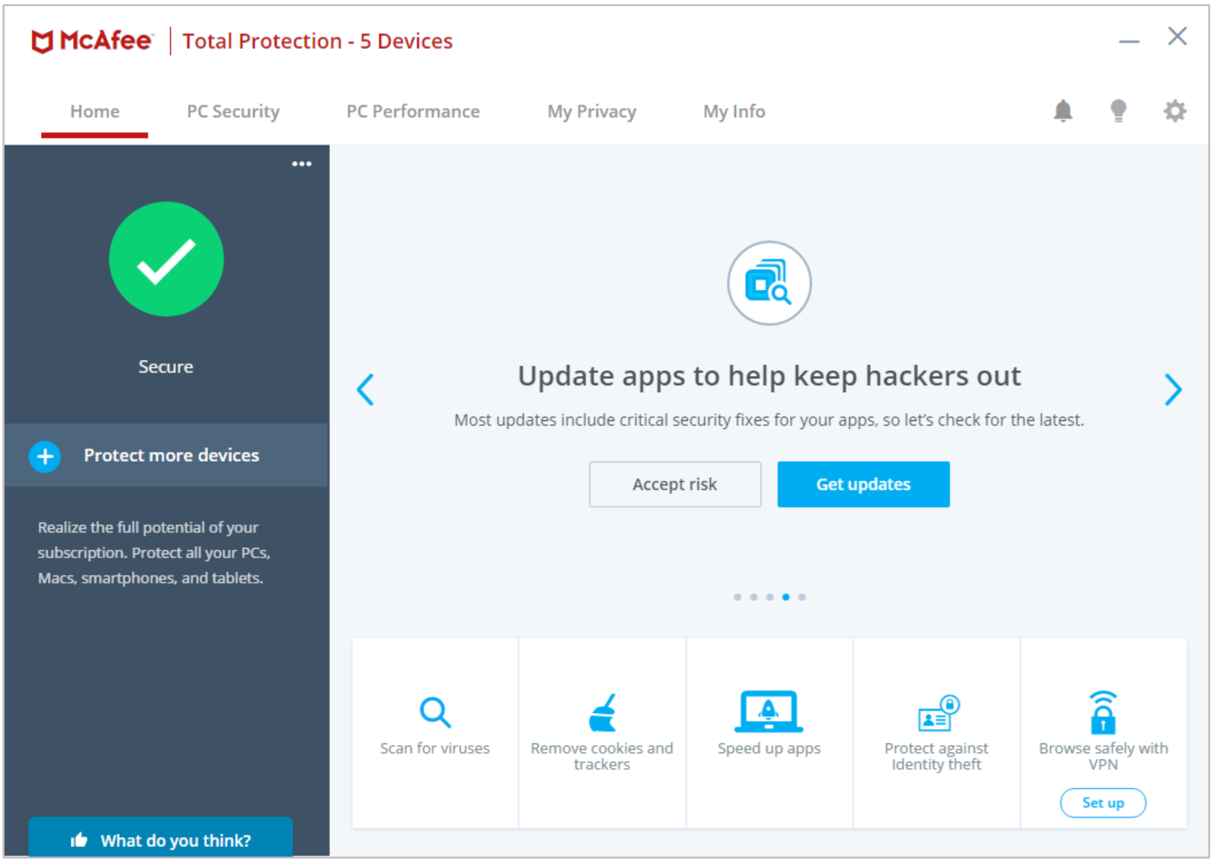
Firewall

In our functionality test, the firewall in Kaspersky Internet Security partially co-ordinated with Windows Security settings. When we connected to a new wireless network, and designated this as public in the Windows file-sharing prompt, Kaspersky also registered this as a public network, and blocked ping and file-sharing access. However, we note that by default, the Kaspersky Firewall allows Remote Desktop access in public networks, regardless of the Windows settings. Kaspersky tell us that this is in response to user feedback. They also say there is a feature in the product that prevents hackers from cracking RDP credentials by brute force. We found that when we changed the status of a network from Private to Public (or vice-versa) in Windows' settings, the Kaspersky Firewall did not register the change until after we had rebooted the computer. We found that restarting the product, or reconnecting to the network, has the same effect. A user who accidentally clicked "Yes" in the Windows file-sharing prompt, and then immediately corrected the mistake by changing the network type to Public, would thus need to take one of these actions to be fully protected. We note that it is possible to cleanly disable the Kaspersky Firewall and use the Windows Firewall instead.

Other points of interest:

- The program's home page displays a *Protection for kids* tile, which is shown in faded colours with a download symbol. If you click on this, an information page informs you that this is an additional download, and that a separate licence is needed to use all the features of Kaspersky Safe Kids. Kaspersky Safe Kids is a separate Kaspersky application that uses a freemium model.
- The setup wizard of Kaspersky Internet Security places a shortcut for Kaspersky Password Manager on the Windows Desktop. This is also a separate Kaspersky freemium application.
- During our test, Kaspersky Internet Security displayed an alert to say that a newer version of a third-party program had been found, and prompted us to install this.
- A prompt was displayed that encouraged us to install a Kaspersky add-on for the Google Chrome browser.

McAfee Total Protection


McAfee
Total Protection - 5 Devices
Home
PC Security
PC Performance
My Privacy
My Info
Secure
Protect more devices
Realize the full potential of your subscription. Protect all your PCs, Macs, smartphones, and tablets.
What do you think?
Update apps to help keep hackers out
Most updates include critical security fixes for your apps, so let's check for the latest.
Accept risk
Get updates
Scan for viruses
Remove cookies and trackers
Speed up apps
Protect against Identity theft
Browse safely with VPN
Set up

About the program

McAfee Total Protection is a paid-for security program. In addition to anti-malware features, it includes a software updater for commonly used apps, replacement firewall, performance booster, cookie and tracker remover, and anti-spam feature. You can find out more about the product on the vendor's website: https://www.mcafee.com/en-us/index.html

Summary

McAfee Total Protection is very simple to install, and has a modern, touch-friendly interface. This makes it very straightforward to find essential functions. The innovative program home page shows various security-related suggestions, and malware alerts are clear and persistent. We note that malware is only detected on execution, and there appears to be no means of enabling on-access detection.

Setup

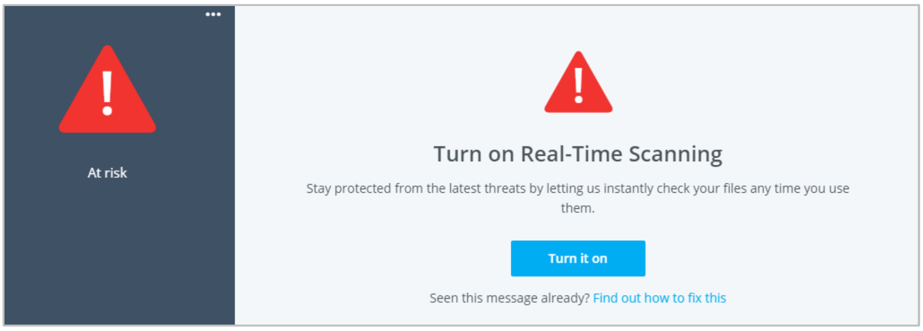
Installation could not be simpler. You only have to click *Install*, and that's it. When the program first runs, you need to sign in with a McAfee account, or create a new one.

System Tray icon

The System Tray icon menu lets you open the program window, check for updates, run scans, open settings, and open the help page.

Security alerts

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 *Turn it on*. The three-dots symbol in the top right-hand corner of the grey panel displays a list of all protection components and their status.

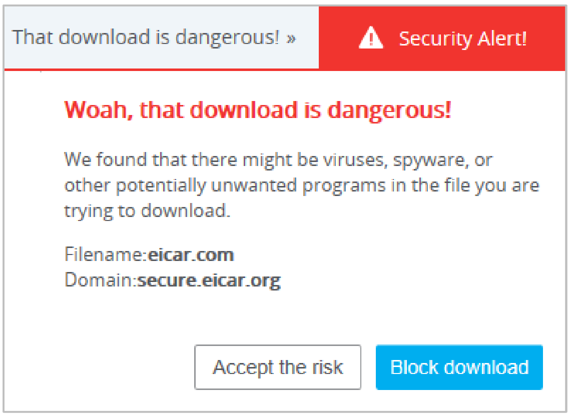


Turn on Real-Time Scanning

Stay protected from the latest threats by letting us instantly check your files any time you use them.

Seen this message already? Find out how to fix this

When we downloaded the EICAR test file, McAfee showed an alert in the browser window. Clicking *Block download* deleted the file, while clicking *Accept the risk* left it in place. In the latter case, we found that trying to execute the file caused it to be detected and deleted by McAfee's real-time protection.

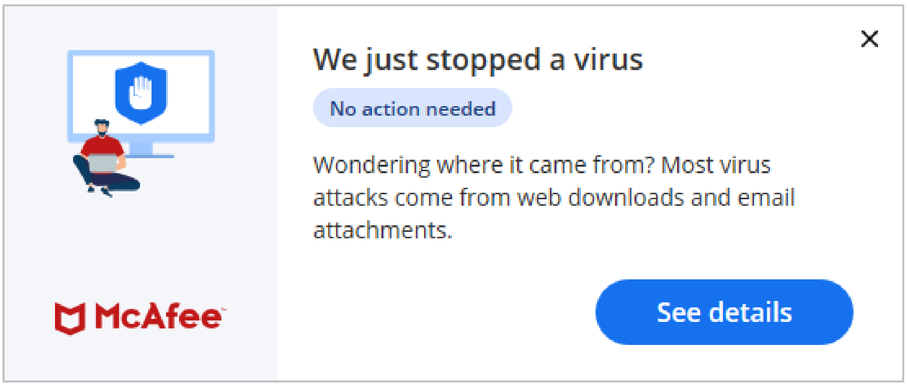


Woah, that download is dangerous!

We found that there might be viruses, spyware, or other potentially unwanted programs in the file you are trying to download.

Filename:**eicar.com**
Domain:**secure.eicar.org**

When we connected a USB drive containing some malware to the system, McAfee offered to scan the drive. The prompt can be disabled directly from the message box, if you so choose. We declined to scan the drive, but instead opened the drive in Windows File Explorer. McAfee did not take any action. We were able to copy the malware from the external drive to the Windows Desktop without it being detected. However, when we executed the samples, McAfee immediately detected and quarantined them. The alert below was shown. We did not need to take any action. The alert persisted until we closed it. By clicking on *See details* we were able to see the detection name, plus file name and path.


We just stopped a virus

Wondering where it came from? Most virus attacks come from web downloads and email attachments.

When we ran an on-demand scan of malware samples on a USB drive, McAfee displayed a list of the detected items, showing file name and path. We were able to see the threat name of an item by clicking on its entry. The accompanying message was "We scanned and you're good", so we just had to click *Close*.

Scan options

The *Scan for viruses* button on the home page lets you run a quick or full scan. There are also instructions for using the right-click context-menu scan with Windows File Explorer. You can schedule a scan from the *Settings* menu (cogwheel icon in the top right-hand corner of the window), *Scheduled scan*. Under *Settings\Real-Time Scanning*, you can exclude specific files from real-time protection. We could not find any means of excluding an entire folder, configuring exclusions for on-demand scans, or configuring PUA detection.

Quarantine

This is found under *Settings\Quarantined items*. It shows the file name and path, threat name, and date/time of detection. You can restore or delete individual items, or all items together.

Logs

The log feature is found under *Settings\Security History*. You can see blocked incoming network connections, scan results, and blocked threats. For the latter, the threat name, plus date and time of detection, are shown.

Help

The help features are found on the *My info* tab, under *Get help and support*. The *Help* link opens an online manual for the product. This provides brief, text-only explanations of the program's features. There is a search box at the top of the page. The *McAfee Support Website* link opens the McAfee knowledge base, which covers all McAfee consumer products. The search function finds answers relating to all of these, so some sifting through search results may be necessary to find relevant answers. Simple text-only explanations are provided.

Access control

Standard Windows users cannot disable protection features (the switches are deactivated), or uninstall the program. This is as it should be, in our opinion. We could not find a means of password protecting the settings.

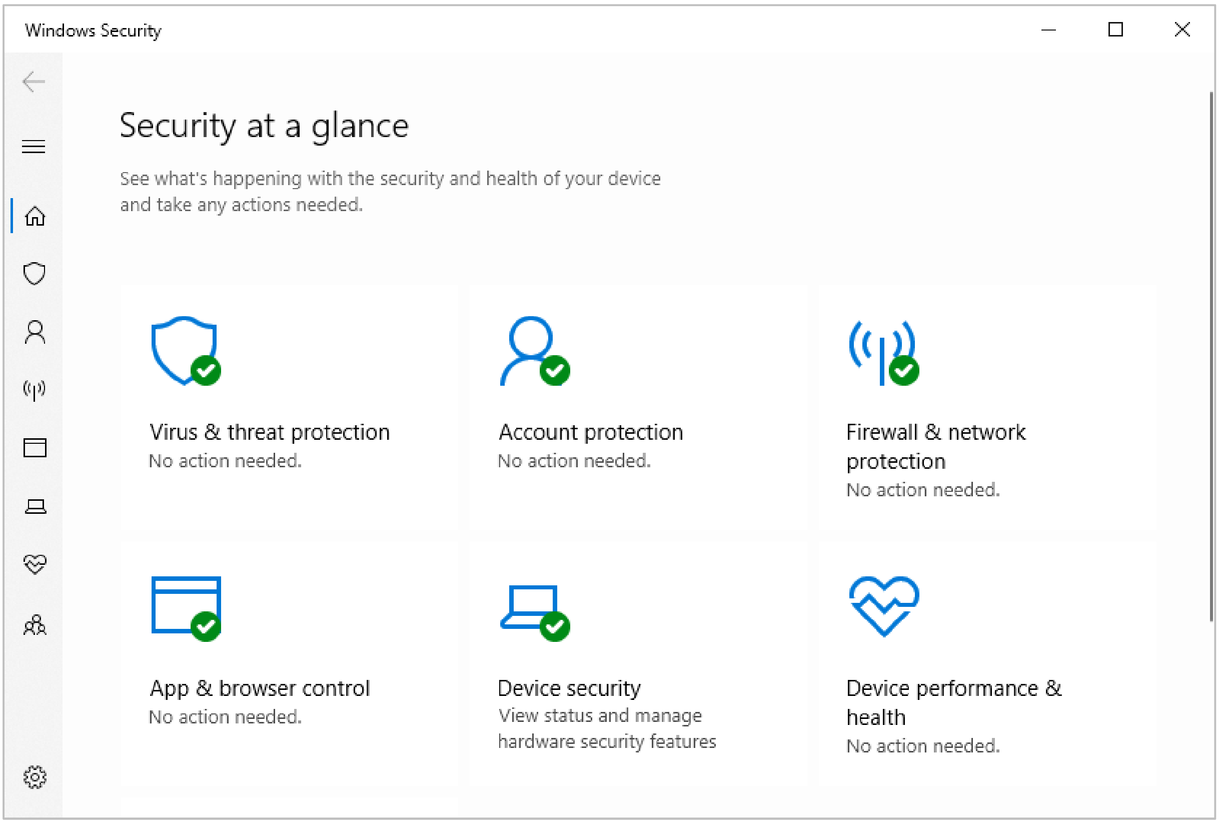
Firewall

In our functionality test, the McAfee Firewall co-ordinated perfectly with Windows' security settings. When we designated a network as private in Windows Settings, the McAfee Firewall allowed ping, Remote Desktop and file-sharing access. When we changed the network status to public in Windows Settings, McAfee blocked all these forms of access.

Other points of interest:

- The main status display panel of the program window shows a variety of reports and prompts regarding different features of the program.
- The update function can be found in the System Tray menu.

Microsoft Defender Antivirus



Windows Security

Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features

Device performance & health
No action needed.

About the program

Microsoft Defender Antivirus is a free security program that is included with Windows 10. Similar protection features are built into Windows 8.1, albeit with a different interface. You can find out more about the program on the Microsoft website: https://www.microsoft.com/en-ie/windows/comprehensive-security

Summary

Microsoft Defender Antivirus includes all the essential features of an antivirus program in a clean, touch-friendly interface. Safe default options are provided for non-expert users. In the scan results dialog, and the quarantine page, you can only take action on malware items individually. A "select all" button would be helpful in dealing with multiple malware detections. We also found a small issue with scans of a USB device only detecting a small proportion of the malicious files on it.

Setup

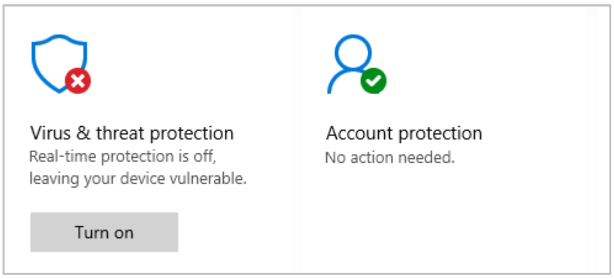
No setup is required, as the program is built into Windows.

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 window.

Security alerts

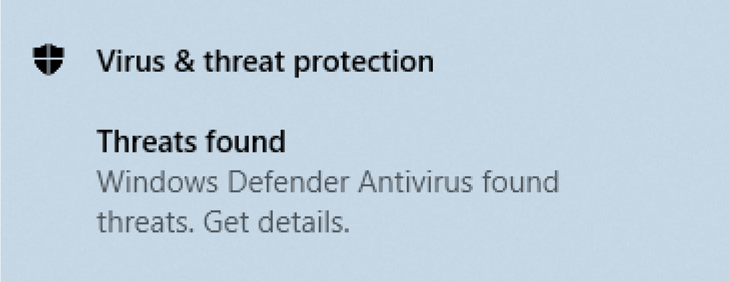
When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). We were able to reactivate the protection easily by clicking *Turn on*.



Virus & threat protection
Real-time protection is off, leaving your device vulnerable.

Account protection
No action needed.

When we downloaded the EICAR test file, Microsoft Defender Antivirus detected and deleted the file. The alert below was shown. 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.



Virus & threat protection

Threats found
Windows Defender Antivirus found threats. Get details.

When we connected a USB drive containing some malware to the system, Microsoft Defender Antivirus did not take any immediate action. However, as soon as we opened the drive in Windows File Explorer, Defender detected and quarantined the malware. An alert similar to the one above was displayed.

Scan options

If you click on *Virus and threat protection\Scan options*, you can run a quick, full or custom scan. You can also run a *Windows Defender Offline Scan*, to deal with hard-to-remove malware. The program informs you that this will restart the device and take about 15 minutes. Exclusions can be set under *Virus and threat protection settings*. We could not find any means of configuring PUA detection.

If malware is detected in an on-demand scan, the *Scan options* page is displayed. This lists the malware found, and displays the *Start actions* button, which by default removes the malware. You can change the action for any individual threat by clicking on it; this provides the additional options *Quarantine* or *Allow on device*. If you choose the latter option, it will be possible to execute the malware.

In our functionality test, we found that if we scanned a USB drive containing six malware samples, Microsoft Defender Antivirus would initially detect one or two of these. The detected sample(s) would be shown on the *Scan Options* page, and could be removed as described above. The other four or five samples could still be seen on the drive in Windows File Explorer. All the samples used in this case would be detected by Microsoft Defender in other circumstances, e.g. on file copy.

Quarantine

The quarantine function is found under *Virus and threat protection\Protection history*. It lists detected items by date and time detected. By clicking on any item, you can see more details of the threat, and restore it if you want. Clicking on *Learn more* opens Microsoft's online threat encyclopaedia, with details of that threat.

Logs

The log feature is effectively combined with quarantine under *Protection history*.

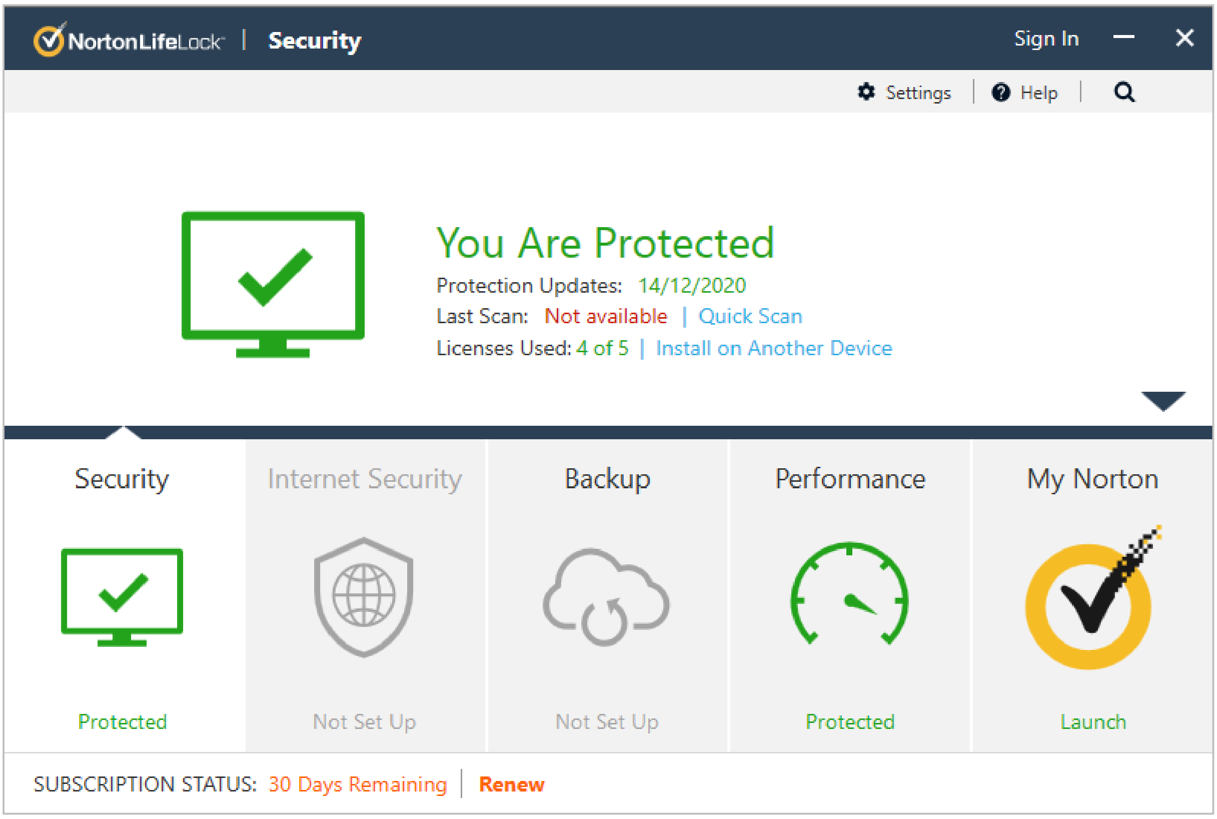
Help

Clicking *Get help* on the *Virus and threat protection* page opens the Microsoft Virtual Agent, which is an automated chat service. You can type in a query, and search. Depending on the question you asked, an answer may appear in the chat window, or a link to an online article may be shown. Our query "Set scan exclusions" brought up three irrelevant answers, plus the option "None of the above". When we clicked on the latter, it correctly suggested "Add an exclusion to Windows Security". Simple and clear instructions, well illustrated with icons and a screenshot, were then provided.

Access control

Standard Windows users cannot disable protection features or restore items from quarantine, which is as it should be, in our opinion.

NortonLifeLock Norton 360 Deluxe



You Are Protected

Protection Updates: 14/12/2020

Last Scan: Not available | Quick Scan

Licenses Used: 4 of 5 | Install on Another Device

SUBSCRIPTION STATUS: 30 Days Remaining

About the program

Norton 360 is a paid-for security program. In addition to anti-malware features, it includes a replacement firewall, backup feature, anti-spam and performance tune-up features. There is no free trial. You can find out more about the product on the vendor's website: https://us.norton.com/products/norton-360-deluxe

Summary

Norton 360 is very simple to set up, and has a very modern, touch-friendly interface. Essential features are easy to find, and safe default settings are provided. Access control is excellent. However, we feel that co-ordination between Windows network settings and the Norton 360 Firewall could be improved.

Setup

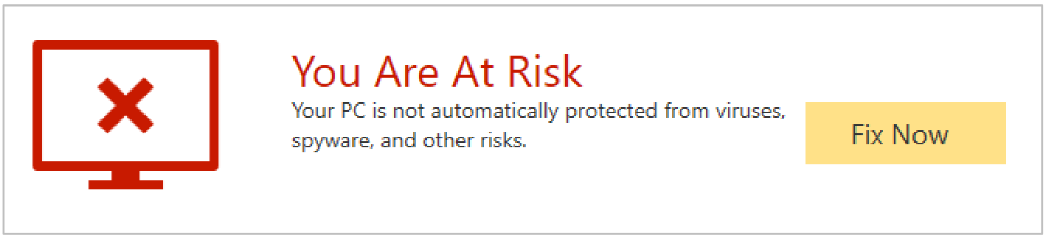
You can opt in to Norton's data sharing scheme, and change the installation folder if you want. Otherwise you only need to click on *Install*.

System Tray icon

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

Security alerts

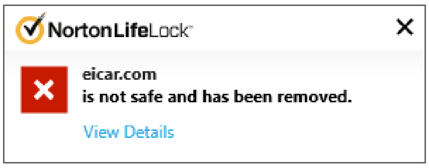
When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). We were able to reactivate the protection easily by clicking *Fix Now*.



You Are At Risk

Your PC is not automatically protected from viruses, spyware, and other risks.

When we downloaded the EICAR test file, Norton 360 deleted it and displayed the alert shown below. We did not need to take any action, and the alert closed after 30 seconds. Clicking *Details* opened the program's *File Insight* page, showing the file name and path.



eicar.com
is not safe and has been removed.

When we connected a USB drive containing some malware to the system, Norton 360 did not initially take any action. However, as soon as we opened the drive in Windows Explorer, Norton 360's real-time protection detected the malware and quarantined it. An alert similar to the one above was shown. We were then prompted to restart the computer.

Scan options

The *Scans* button on the *Security* page lets you run quick, full and custom scans, whereby a custom scan can be scheduled. You can also scan a drive, folder or file using Windows Explorer's right-click menu. Under *Settings\Antivirus\Scans and Risks* you can set exclusions and specify treatment of *Low Risks*, which we assume means PUAs. If malware is detected in an on-demand scan, the scan results page is shown. This shows the threat name, risk level and status/action taken. You do not need to do anything.

Quarantine

This is found under *Security\History*. *Resolved Security Risks* shows you risk level, detection name, plus date and time of detection. Any individual file can be restored, restored and excluded, or submitted to the vendor for analysis.

Logs

This is combined with the quarantine function.

Help

Clicking *Help* in the top right-hand corner of the window displays a number of help options, including *Product Manual*. This opens a very comprehensive .PDF manual of over 80 pages. It covers all aspects of installing, configuring and using the program, explained with simple text instructions.

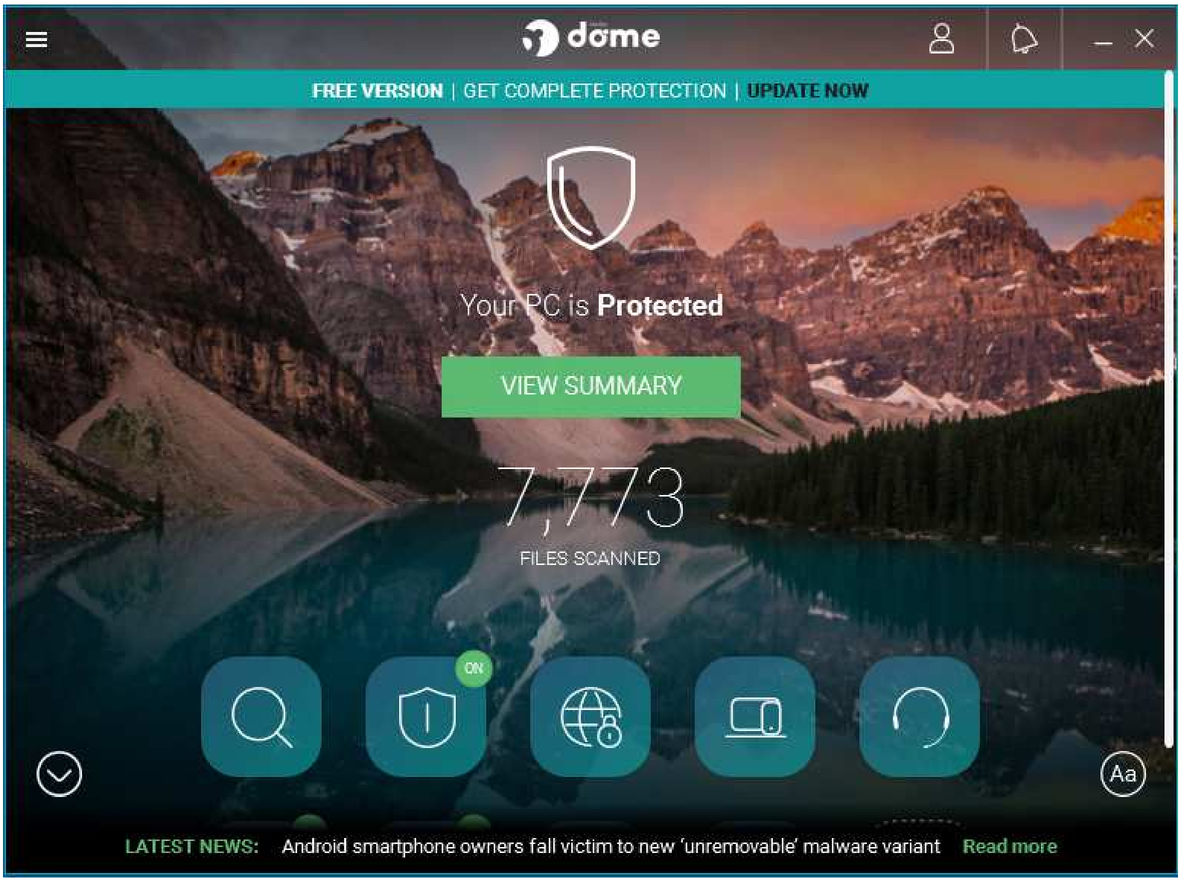
Access control

Standard Windows users cannot disable protection features, or uninstall the program. This is as it should be. Protection settings are greyed out when the program is used by a non-administrator account. There is also a password protection feature. This makes it impossible for other users to change settings or disable protection without knowing the password.

Firewall

In our functionality test, the Norton 360 Firewall co-ordinated partially with Windows network settings. When connected to a network we had previously defined as public, Norton adopted the Windows settings and blocked file-sharing, Remote Desktop and ping access. When connected to a network that we had previously designated as private in Windows Settings, the Norton Firewall allowed ping, file sharing and Remote Desktop access, as it should. However, when we changed the network status to public in Windows network settings, Norton continued to allow ping requests with IPv6, and file-sharing access (although it blocked ping requests with IPv4, and Remote Desktop access). After rebooting the PC, we found that Remote Desktop access was also blocked, although ping requests with IPv6 were still allowed. We would advise Norton users to reboot their PCs after changing Windows network type from private to public. It is not possible to use Windows Firewall with Norton Security, as Norton locks the Windows Firewall settings.

Panda Free Antivirus



dome
FREE VERSION | GET COMPLETE PROTECTION | UPDATE NOW
Your PC is Protected
VIEW SUMMARY
7,773
FILES SCANNED
ON
Aa
LATEST NEWS: Android smartphone owners fall victim to new 'unremovable' malware variant Read more

About the program

Panda Free Antivirus is, as its name suggests, 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/solutions/free-antivirus/

Summary

We found Panda Free Antivirus to be very straightforward to install and use. The program interface is simple to navigate, and safe default options are provided. Although Panda Free Antivirus promotes other, paid-for Panda products, this is done in a very subtle, non-intrusive way, by means of a thin strip along the top of the window.

Setup

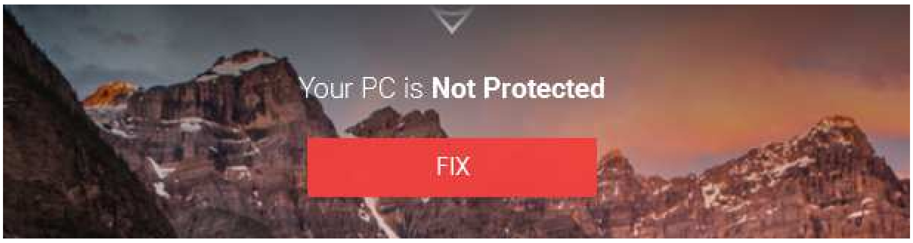
Installation is very straightforward. You can change the installation folder and interface language. By default, the Opera browser is installed. We chose not to install this for our functionality test. When setup is complete, a page of the Panda website opens, showing the additional features available in Panda paid-for products. You are prompted to sign in with a Panda account, or create a new one.

System Tray icon

The System Tray icon menu lets you open the program window, enable gaming mode, reach help and support services, disable/enable protection, and use Panda's VPN feature (which has limitations on servers and data).

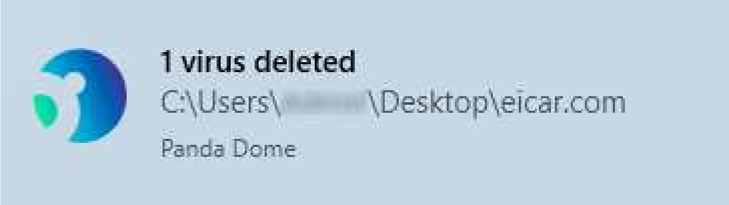
Security alerts

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 *Fix*, and then *Enable*.



Your PC is **Not Protected**

When we downloaded the EICAR test file, Panda detected and quarantined it. The alert below was shown. We did not have to take any action, and the alert closed after a few seconds.



1 virus deleted

C:\Users\[redacted]\Desktop\eicar.com

Panda Dome

When we connected a USB drive containing some malware to the system, Panda offered to scan the drive. This prompt can be disabled directly from the alert dialog box, if you want. We chose not to scan the drive, but instead opened it in Windows File Explorer. Panda did not initially take any action. However, when we tried to copy the malicious files to the Windows Desktop, Panda immediately detected and quarantined the copied files. An alert like the one above was shown.

When we ran an on-demand scan of malware samples on a USB drive, Panda displayed the number of files scanned and detected. By clicking on *Show details*, we could see the file name and path, plus detection time and action taken, for the detected files. We did not have to take any action.

Scan options

The *Scan* button on the home page (magnifying-glass symbol) lets you run *Full, Custom* and *Critical areas* scans. The *Antivirus* page enables you to set a scheduled scan. You can scan a drive, folder or file using Windows Explorer's right-click menu. Under *Settings\Antivirus*, you can set exclusions and choose whether to detect PUAs (on by default).

Quarantine

This feature is found on the *Antivirus* page. It shows you the detection name, file name and path, plus date and time of detection. You can recover or delete quarantined items one by one. No further information is provided about the threats detected.

Logs

You can find the log feature on the *Antivirus* page, by clicking *View report*. It shows the same information as the quarantine page, plus the action taken (e.g. "Deleted").

Help

The help feature is located in the "hamburger" menu in the top left-hand corner of the window. Clicking on this opens an online manual for the product. A menu column on the left-hand side of the page shows various topics. Selecting one of these displays simple, text-only answers in the main pane.

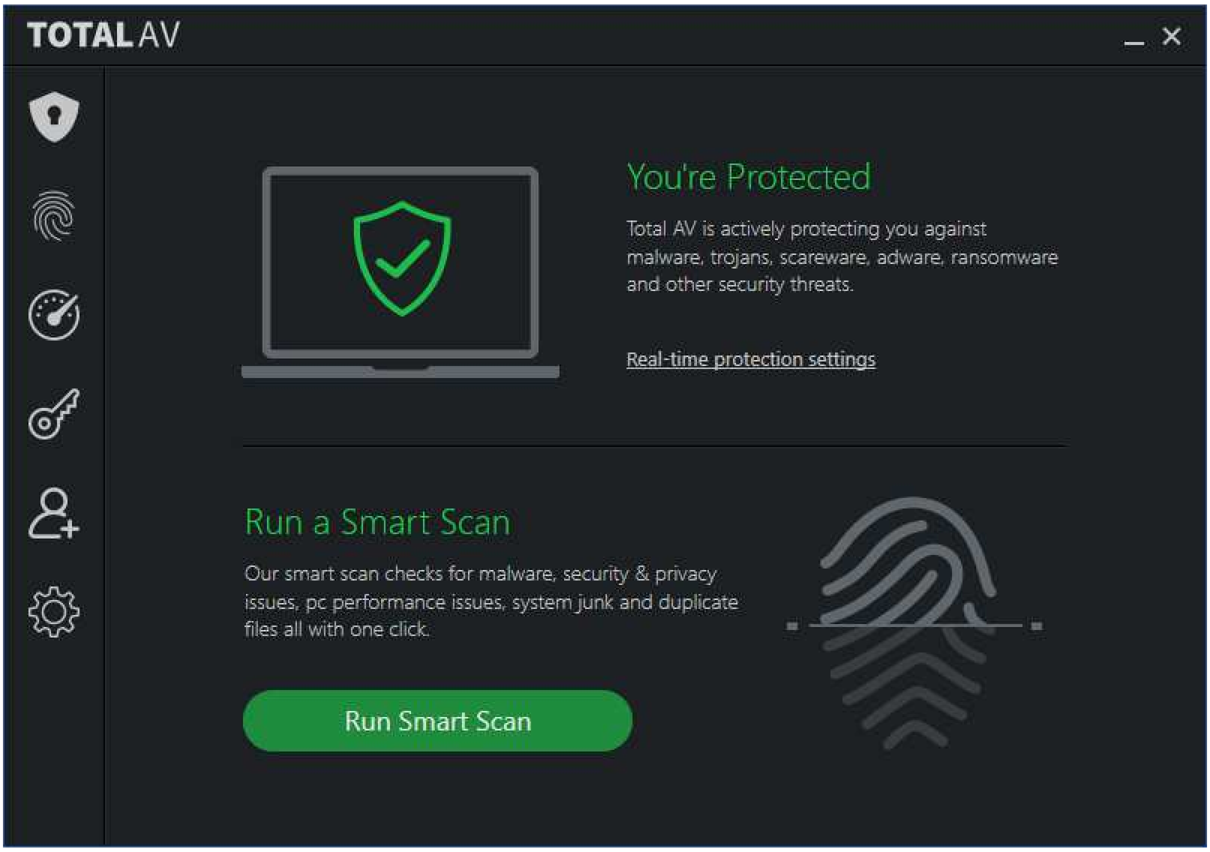
Access control

Standard Windows users can disable protection features, but not uninstall the program. You can however password protect the program. In this case, access to the main program window will be blocked unless the password is entered. However, it will still be possible to run scans from Windows File Explorer's right-click menu, and see the results of this.

Other points of interest

- The download link for Panda Free Antivirus on the Panda website redirects to cnet.com.
- The setup wizard states that free support is included for "any PC or Internet related problems". UK, USA and Canadian telephone numbers are provided (in the English version of the program); Panda tell us that the calls are free of charge.
- The "Aa" symbol in the bottom right-hand corner of the window lets you show or hide the names of the symbols on the home page.
- The program's settings are found in the "hamburger" menu in the top left-had corner of the program window.
- A strip along the bottom of the windows displays headlines from Panda's Media Center. You can click on this to read the full story, and others. There are articles on various IT-security related topics.

Total AV Antivirus Pro



TOTAL AV
You're Protected
Total AV is actively protecting you against malware, trojans, scareware, adware, ransomware and other security threats.
Real-time protection settings
Run a Smart Scan
Our smart scan checks for malware, security & privacy issues, pc performance issues, system junk and duplicate files all with one click.
Run Smart Scan

About the program

Total AV Antivirus Pro is a paid-for security program. In addition to anti-malware features, it includes a system performance tuner.

Summary

We found Total AV Antivirus Pro to be very simple to install and use. The program's features are easily found in a single menu panel, and default settings and alerts are sensible. In our functionality test, the product behaved mostly as expected, with one exception, which we think should be fixed. When we scanned a USB drive containing malware samples using Windows File Explorer's right-click menu, Total AV failed to detect any of the malicious files. In order to detect malware on an external drive, you have to open the drive in File Explorer and scan the files and folders within it.

Setup

Installation is extremely quick and simple. You just need to run the installer, click *Install*, and less than a minute later it's done. You have to log in to your Total AV account when the program first starts.

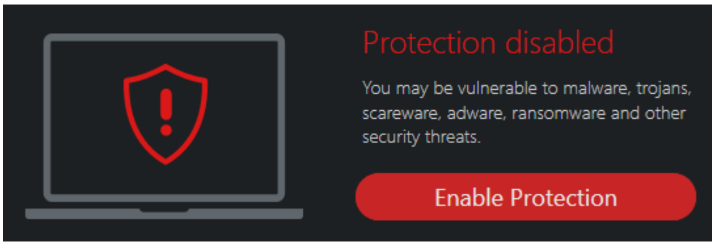
You can install the "Total AV Safe Site" add-on – which is actually an ad blocker - for Chrome, Firefox or Edge by clicking *Internet Security* (fingerprint icon), *Ad Block Pro*. We note that the product's URL blocker is called *WebShield*.

System Tray icon

This lets you open the program window, open the settings dialog box, check for updates, and see program and definitions version information.

Security alerts

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 Protection*.

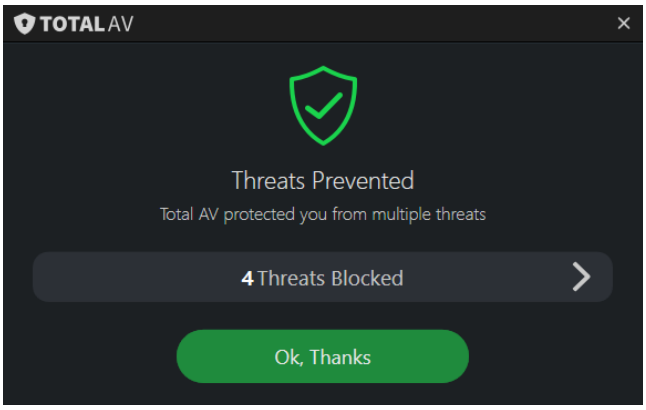


Protection disabled

You may be vulnerable to malware, trojans, scareware, adware, ransomware and other security threats.

When we downloaded the EICAR test file, Total AV detected the condensed file and quarantined it. An alert like the one below was shown.

When we connected a USB drive containing some malware to the system and opened it in Windows File Explorer, Total AV immediately detected and quarantined the malware. The alert below was shown; this persisted until we closed it. By clicking on *4 Threats Blocked*, we were able to see the file and detection names of the malware samples.



Threats Prevented

Total AV protected you from multiple threats

Scan options

You can run a *Smart Scan* from the button of the same name on the home page. The description states that this also checks for performance and privacy issues, and removes duplicate files. More scan options can be found by clicking the shield icon in the top left-hand corner, and then *Malware scan*. There is a choice of *Quick Scan, System Scan,* and *Custom Scan*. You can also scan a drive, folder or file using the right-click menu in Windows File Explorer.

In the program's 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.

We ran an on-demand scan of malware samples on a USB drive, by means of a custom scan run from the program window. The malicious files were detected and displayed as a list in the program window. All we had to do was to click *Quarantine All* to deal with them.

When we scanned the USB stick by right clicking the drive in Windows Explorer, none of the malware samples was detected. When we selected all folders and files manually, and scanned from the right-click menu, all the samples were detected and quarantined. We note that if you do the latter, TotalAV's real-time protection will also take action against the malware. Nonetheless, users who run a right-click scan of an entire drive will believe that all the files on the drive are safe, when they are not. We feel this is an issue that TotalAV should fix.

Quarantine

The quarantine function is opened by clicking the shield icon, then *Quarantine*. For each item, it displays the file name, threat name and date/time the threat was encountered, in chronological order. You can select individual or multiple items using checkboxes, and delete or restore these.

Logs

There is no separate logs feature, though you can see the day and time threats were encountered in *Quarantine*.

Help

The help feature is accessible from the *General* tab of the *Settings* page. We feel this is a far-from-obvious place to put the help feature. Clicking *Visit the help center* opens the support page of the vendor's website. This provides options for contacting support, and about a dozen FAQs. Of these, most are not about technical support, e.g. "How many awards do you have?" and "Do you offer Internet Security?". However, the article on real-time protection provided a comprehensive explanation, well illustrated with screenshots.

Access control

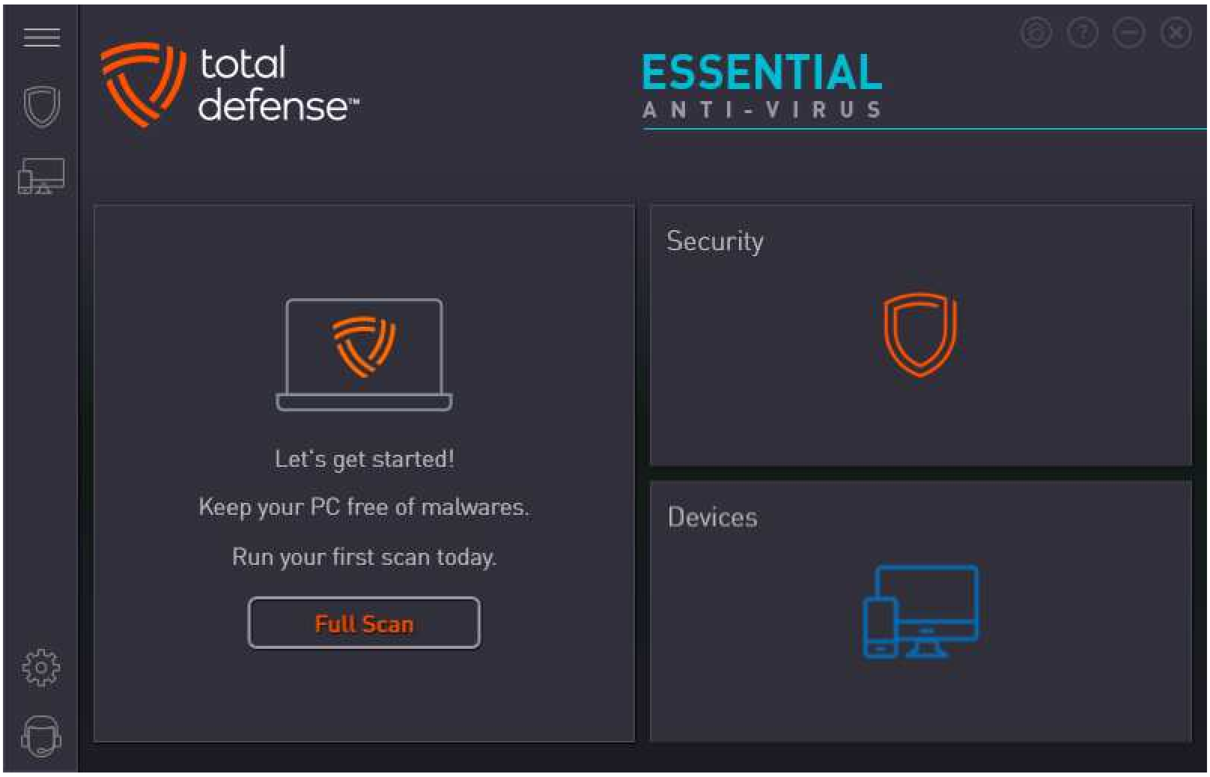
Standard Windows users cannot disable protection features, or uninstall the program. This is as it should be, in our opinion.

Other points of interest

We feel that some descriptions on the TotalAV website are unclear. For example, the landing page of www.totalav.com displays a prominent button marked "Free Antivirus Software". This leads to a page where a 30-day trial of the full product can be downloaded. We do not think this is clear, as a time-limited trial is not the same thing as a free product.

We note that if you wish to cancel your TotalAV subscription, TotalAV advises you to contact their support service before uninstalling the product. They also ask customers to contact them regarding any questions about autorenewal charges.

Total Defense Essential Anti-Virus



Let's get started!

Keep your PC free of malwares.

Run your first scan today.

About the program

Total Defense Essential Anti-Virus is a paid-for security program, which offers phishing protection in addition to anti-malware features. 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 presents a very simple program interface that makes status and scan functions easy to find. Automatic scanning of external drives makes sure these are clear of malware. Help articles are clear and well illustrated. The use of symbols rather than text for menu items means that it may take a little bit of exploring to find the more advanced functions. However, everything is neatly laid out, and we soon managed to find our way around the program. One suggestion for improvement would be to provide password protection for the settings.

Setup

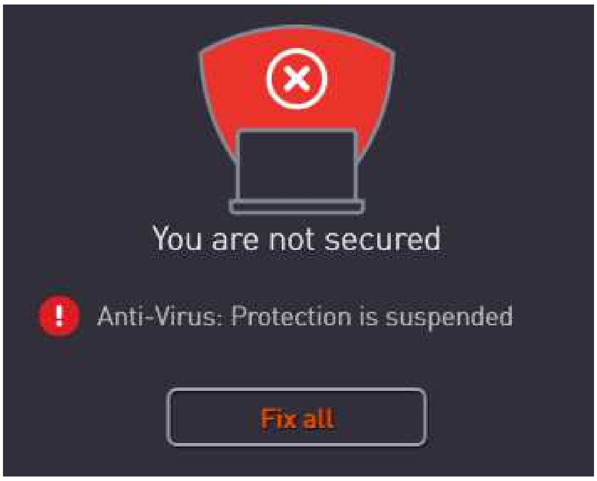
There is a custom installation option, which just lets you change the installation folder. Other than this, there are no options or decisions to make. Setup completes very quickly once you click *Install*. An update runs when you first open the program window.

System Tray icon

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

Security alerts

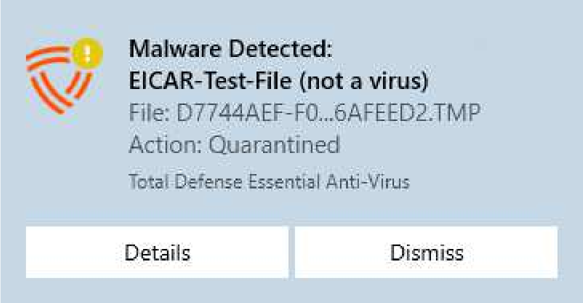
When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). We were able to reactivate the protection easily by clicking *Fix all*.



You are not secured

Anti-Virus: Protection is suspended

When we tried to download the EICAR test file, Total Defense blocked the download and displayed an alert in the browser window. We persisted, by clicking *Advanced Settings\Proceed to Website [Not Recommended]*. This downloaded the file, but it was immediately detected and deleted by Total Defense. The alert below was shown for a few seconds. We did not need to take any action, although clicking *Details* opened the program's log page, which showed the threat name, threat level, and action taken.



Malware Detected:
EICAR-Test-File (not a virus)
File: D7744AEF-F0...6AFEED2.TMP
Action: Quarantined
Total Defense Essential Anti-Virus

When we connected a USB drive containing some malware to the system, Total Defense immediately scanned the drive automatically, and notifies us that it was doing so. When the scan completed a few seconds later, an alert like the one above was shown. Clicking on *Details* opened the program's quarantine page, showing the threat names, file names, and threat level of the detected files.

Scan options

Scans can be run by clicking the *Security* tile and going to the *Overview* page. There is a choice of quick, full, or custom scans. The *Suspend Scans* button on the same page temporarily deactivates real-time protection for a specified number of minutes. You can scan a drive, folder or file using Windows Explorer's right-click menu.

On the *Security* page/*Settings* tab you can set the scan security level to *Low, Recommended* (default), *High* or *Custom*. The latter lets you decide whether to scan network, archive and hidden files, and whether suspicious files should be treated as infected. Exclusions can be set on the tab of the same name. We could not find a way of configuring PUA detection as such. However, Total Defense tell us that the default setting for the application control feature (*Recommended*) enables PUA detection.

Quarantine

This feature is found on the *Security* page, *Quarantine* tab. It shows the date and time of detections, file name, threat severity, threat name, and threat type – although the Trojans used in our functionality test were all listed as “virus”. You can restore or delete quarantined items from here. We could not find any further information about the detected malware.

Logs

The *Reports* tab of the *Security* page displays a list of threats found, along with the detection date/time, and scan type that detected them. This can be displayed as a summary, showing how many of each threat type has been blocked.

Help

Clicking the question-mark icon in the top right-hand corner of the window opens the *About* page. Here you can click *Support Info/Online Support*. This opens the support page of the vendor’s website. If you click *Product Support*, a searchable FAQs page opens. Each article provides simple, step-by-step instructions for the task in question, generously illustrated with annotated screenshots.

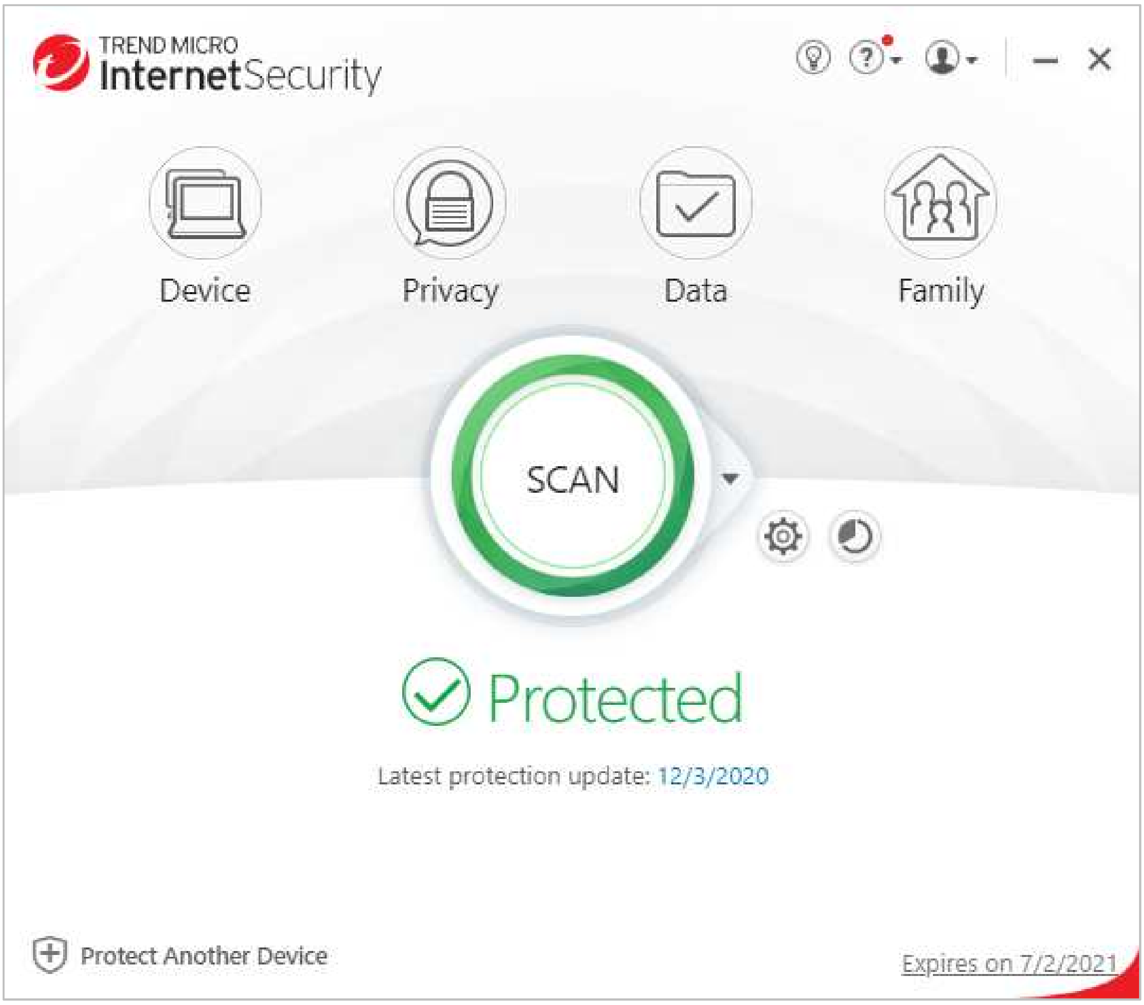
Access control

Standard Windows users are able to disable all protection features, and we could not find a means of password-protecting the settings to prevent this. An administrator account is needed to uninstall the program, however.

Other points of interest:

- The status display prompts you to run a full scan if you haven’t done this recently.
- The cogwheel icon in the vertical menu bar handles updates, notifications and proxy settings; scan settings are found on the *Security* page.
- The *Devices* page shows all the devices you have installed. Actions you can perform on these are limited to changing the device name, and the avatar representing the user. More usefully, the *Add* Device function allows you to send an email to a colleague, friend or family member, with a link to the appropriate installer for their device.
- To find subscription information, log in to your Total Defense online account.

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 ransomware protection, 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 very easy to install, and most important features are easy to find. Safe default settings are provided. We liked the persistent malware and status alerts, and the online manual is simple and clear.

Setup

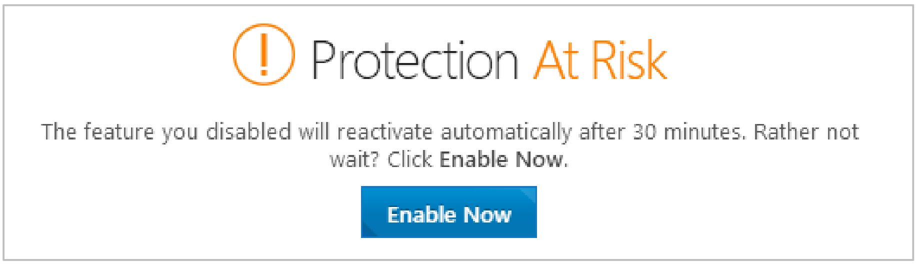
The free trial can be downloaded by clicking *Downloads/Free* Tools on the Trend Micro home page. The setup wizard asks you to enter a licence key or opt for the free trial. Other than this, there are no decisions to make. At the end of the wizard, you are invited to set up the ransomware shield. By default, this covers Windows' Documents, OneDrive and Pictures folders, but you can add further folders if you want.

System Tray icon

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

Security alerts

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 Now*.

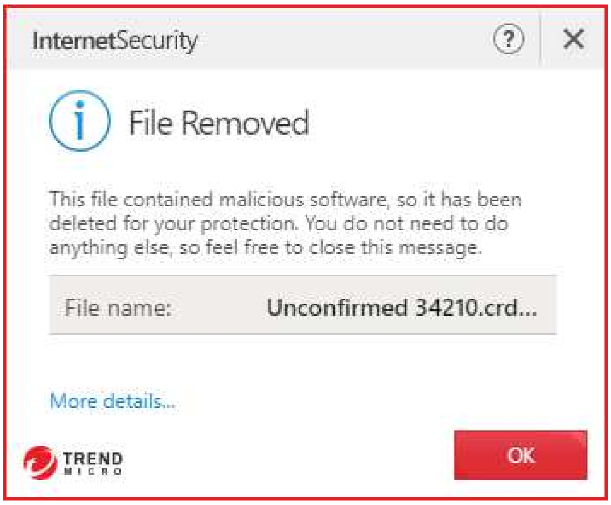


Protection At Risk

The feature you disabled will reactivate automatically after 30 minutes. Rather not wait? Click Enable Now.

An additional pop-up alert was shown above the System Tray. This persisted until we closed it.

When we tried to download the EICAR test file, Trend Micro blocked it and displayed the alert shown below. We did not need to take any action. The alert persisted until we closed it.



InternetSecurity

File Removed

This file contained malicious software, so it has been deleted for your protection. You do not need to do anything else, so feel free to close this message.

File name: Unconfirmed 34210.crd...

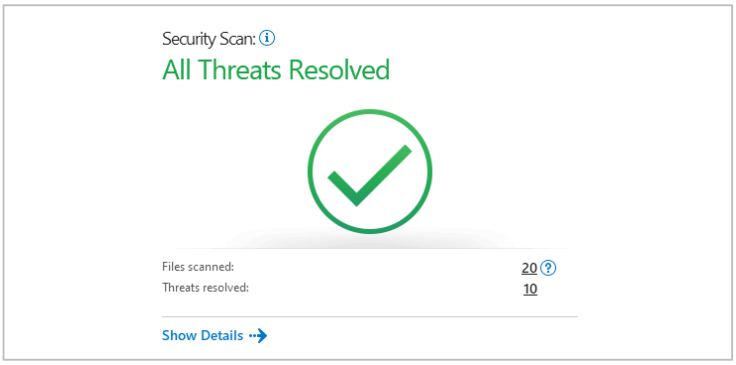
When we connected a USB drive containing some malware to the system, Trend Micro did not initially take any action. However, as soon as we opened the drive in Windows File Explorer, Trend Micro detected and quarantined the malicious files. An alert similar to the one above was shown. Clicking *More details* opened the program's scan log page, showing date and time of detection, file name and path, detection name and action taken, for each item.

Quarantine

The pie-chart symbol to the right of the settings icon opens the *Security Report* page, which shows a summary of threats found. These are divided into different categories, including *Viruses* (which in fact includes many Trojans), *Spyware* and *Ransomware*. If you click *See more details* and select a category, you can see a log of detections in that class. Logs show the date and time of detection, file name and path, threat name, and action taken. Clicking on an individual item displays a details panel, which includes a *Restore* button.

Scan options

The *Scan* button in the main program window runs a quick scan by default. If you click the small down arrow symbol to its right, the choice of quick, full or custom scans is shown. The program's settings dialog lets you schedule scans. You can also scan a drive, folder or file from Windows Explorer's right-click menu. Under *Settings\Scan Preferences*, you can configure detection of PUAs (enabled by default). The *Exception Lists* page of the settings dialog lets you set scan exclusions. If malware is detected in an on-demand scan, the scan results page is shown. If you click *Show Details*, the malware file names and paths are displayed, along with the action taken.



Security Scan: ⓘ

All Threats Resolved

Files scanned: 20 ?

Threats resolved: 10

Logs

Logs are combined with the quarantine feature.

Help

Clicking the *?* menu, *Product Support* opens the program's online manual. The first page has an overview of the program's main functions. There are simple explanations and instructions, well illustrated with screenshots.

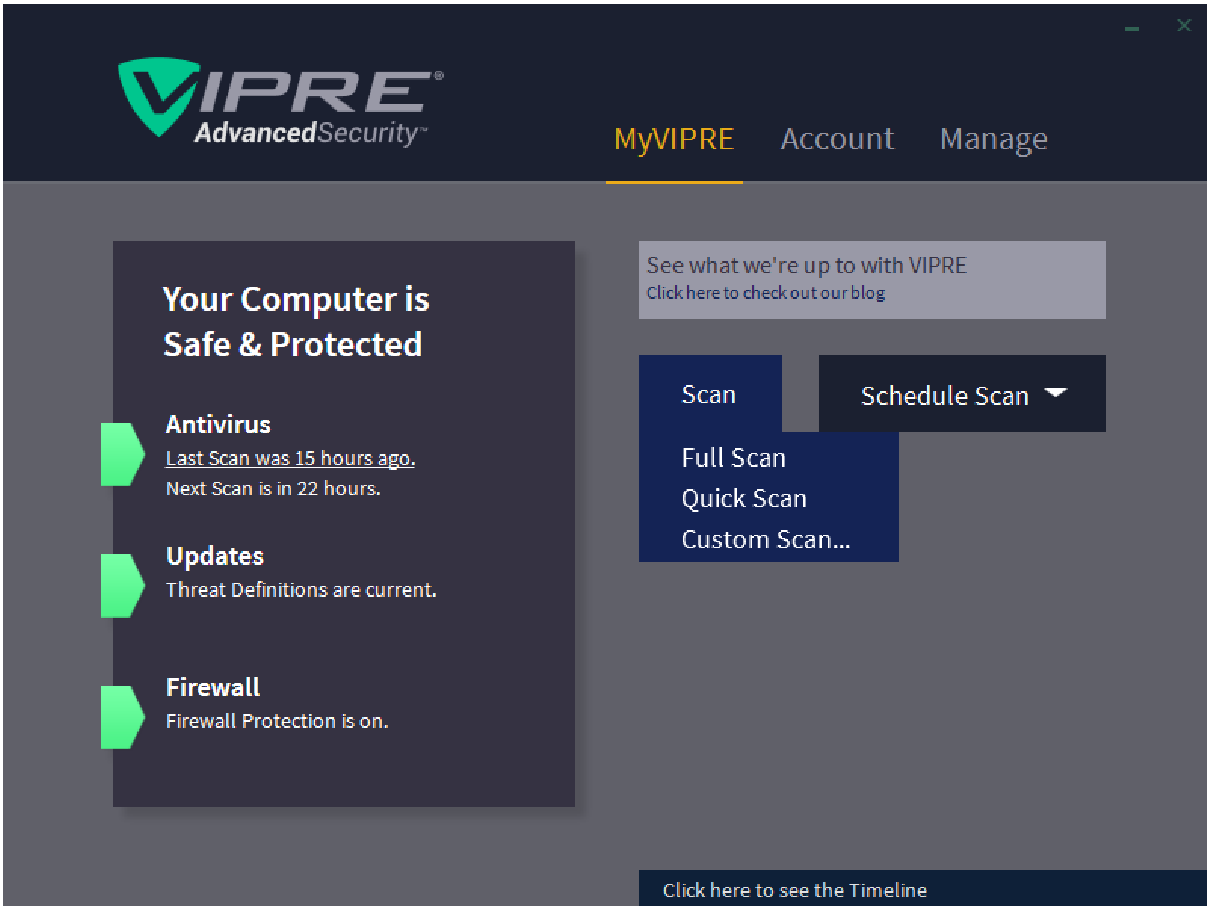
Access control

Standard Windows users can disable protection features, but not uninstall the program. Under *Other Settings\Password*, you can password protect the program to prevent other users changing the settings. You need to enter an email address when doing this, so that you can reset the password if you forget it.

Other points of interest:

- A desktop shortcut to *Trend Micro Pay Guard* is created. This opens the default browser in a secure mode for financial transactions.
- A free trial of Trend Micro's Password Manager is offered on the *Data* page.
- The update function is found in the System Tray menu.

VIPRE Advanced Security



Your Computer is Safe & Protected

Antivirus
Last Scan was 15 hours ago.
Next Scan is in 22 hours.

Updates
Threat Definitions are current.

Firewall
Firewall Protection is on.

See what we're up to with VIPRE
Click here to check out our blog

Click here to see the Timeline

About the program

VIPRE Advanced Security is a paid-for security program. In addition to anti-malware features, it includes a replacement firewall. You can find out more about the product on the vendor's website: https://www.vipre.com/products/vipre-advanced-security/

Summary

VIPRE Advanced Security is very simple to install, and has a very modern, touch-friendly interface. Real-time protection is very sensitive, and default settings provide safe options for non-expert users. We liked the online help feature and the ability to search it directly from the program. The ability to set scanning exclusions using Windows File Explorer's right-click menu is also very convenient. We do however have some concerns that the VIPRE firewall might leave users unknowingly unprotected in public Wi-Fi networks.

Setup

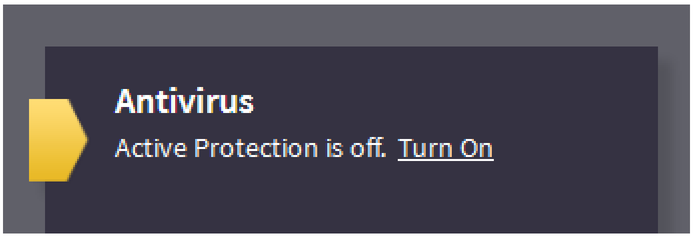
You can change the installation folder if you want. Otherwise installation completes very simply with a single click.

System Tray icon

The System Tray icon menu lets you open the program window, check for updates, shut the program down, enable/disable protection components, and run scans.

Security alerts

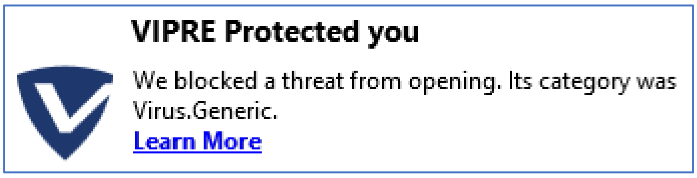
When we disabled real-time protection in the program's settings a (rather subtle) alert was shown in the main program window. We were able to reactivate the protection easily by clicking *Turn On*.



Antivirus

Active Protection is off. Turn On

When we downloaded the EICAR test file, VIPRE deleted the file silently, i.e. without showing an alert. When we connected a USB drive containing some malware to the system, VIPRE offered to scan the drive. You can disable this prompt in the program's settings if you want. We chose not to scan the drive, but instead opened it in Windows File Explorer. VIPRE immediately detected and quarantined the malicious files. The alert below was shown. We did not need to take any action, and the alert closed after 30 seconds.



VIPRE Protected you

We blocked a threat from opening. Its category was Virus.Generic.

Learn More

Clicking *Learn More* opened a page on VIPRE's website, which provided a generic description of computer viruses. When we ran an on-demand scan of malware samples on a USB drive from the Explorer right-click menu, the VIPRE program window opened and showed the scan progress. When the scan was complete, a summary of files scanned and cleaned was shown. No further action was necessary. We found that if we accepted the prompt to scan the USB drive when it was inserted, the scan ran and removed the malware, but the program window did not open, and no indication of scan progress or completion was shown.

Scan options

If you mouse over the *Scan* button on the homepage, a dropdown menu appears, with the options of full, quick and custom scans. The *Schedule Scan* button to its right lets you do precisely that. You can scan a drive, folder or file using Windows Explorer's right-click menu. Very conveniently, the same menu also lets you exclude a drive/folder/file from VIPRE scans. You can reverse this by right-clicking again and clicking *Remove from VIPRE exclusion*. Exclusions can also be set under *Manage\Antivirus*. You can set detection of PUAs here too (on by default), under *Include Low-Risk Programs*.

Quarantine

The quarantine function is found under *Manage\Antivirus*. It shows the name, threat level and type of the detected threats, number of traces (e.g. files or registry entries) for each one, and allows you to delete, restore, or always allow the selected items.

Logs

These are found under *Manage\Antivirus\Antivirus History*. There are separate logs for on-demand scans, real-time protection, blocked websites, and *Edge Protection*. The latter is intended to block the download of online threats, “in most web browsers” (not just Microsoft Edge). The scan log shows the date, time, duration and type of scan, along with the number of files detected and cleaned. The *i* icon opens a panel showing threat name, level and type, number of traces, and action taken.

Help

The help features are found on the *Account* page. *VIPRE Help* opens a Windows Help window, which lists various topics. Simple text instructions are provided for each topic. You can also type a search term into the program’s search box, which will search the online FAQs/forum questions and open the results in a browser window. These include all products made by VIPRE, including beta versions, so you may have to browse through a number of irrelevant results before finding the applicable answer.

Access control

Standard Windows users can disable protection features, but not uninstall the program. We could not find a means of password protecting the settings.

Firewall

In our functionality test, the VIPRE Firewall did not co-ordinate perfectly with Windows security settings. We found that during installation, VIPRE adopts the network type (public or private) currently set in Windows. However, if you later change the network type in Windows settings, this does not change it for the VIPRE firewall. We also found that when connecting to a new network, VIPRE did not co-ordinate with the network type set at the Windows prompt. VIPRE does not show any prompts of its own when you either connect to a new network, or change the type of an existing network.

When either joining a new network, or changing the network type for an existing network, we would recommend users go into the settings of the VIPRE firewall, check whether it is appropriately configured for the current network, and change the network type if necessary.

We also found that in a private network (set to *Trusted* in the settings of VIPRE Firewall, and *Private* in Windows settings), VIPRE blocked IPv6 Ping requests and Remote Desktop connections to our test PC. We tried to enable Remote Desktop access in the settings of the VIPRE Firewall, but without success.

It is possible to disable the VIPRE Firewall completely in the program’s settings, which immediately activates Windows Firewall. A (subtle) warning will be shown on the home page of VIPRE Advanced Security if you do this.

Other points of interest

If you don’t like the default dark mode of the interface, you can easily change it to another colour scheme under *Account*. There are 7 different colour schemes to choose from.

Featurelist Windows (as of December 2020)	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	COMMERCIAL	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL
Product name	Avast Free Antivirus	AVG AntiVirus Free	Avira Antivirus Pro	Bitdefender Internet Security	ESET Internet Security	F-Secure SAFE	G Data Internet Security	K7 Total Security	Kaspersky Internet Security	McAfee Total Security	Microsoft Defender	Norton 360 Deluxe	Panda Free Antivirus	Total AV Antivirus Pro	Total Defense Essential Anti-Virus	Trend Micro Internet Security	VIPRE Advanced 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, Polish, Indonesian	English, French, German, Dutch, Spanish, Italian, Romanian, Portuguese, Polish, Greek, Vietnamese, Turkish, Korean , Czech, Japanese, Hungarian, Thai	English, Arabic, Bulgarian, Czech, Danish, German, Greek, Spanish, Estonian, Finnish, French, Hebrew, Croatian, Hungarian, Chinese, Italian, Japanese, Kazakh, Korean, Lithuanian, Dutch, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Serbian, Swedish, Thai, Turkish, Ukrainian, Vietnamese	English, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish, Vietnamese	English, German, French, Italian, Spanish, Portuguese, Dutch, Polish	English	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, Danish, Dutch, French, German, Italian, Norwegian, Polish, Portuguese, Spanish, Swedish, Turkish	English	English, German, French, Italian, Spanish, Portuguese, Japanese, Chinese, Russian, Polish, Dutch, Danish, Norwegian, Swedish, Indonesian, Korean, Thai, Turkish, Vietnamese	English
Third-party scan engine included	proprietary	Avast	proprietary	proprietary	proprietary	Avira	Bitdefender, Cyren	proprietary	proprietary	proprietary	proprietary	proprietary	proprietary	Avira	Bitdefender	proprietary	Bitdefender
Protection																	
Scans file on execution	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Scans files on demand	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
On-access file scan while copying/moving files (by DEFAULT)	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●
On-access file scan after Internet download (by DEFAULT)	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●
Prevents access to phishing and other malicious websites	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Has capabilities to clean-up an infected system	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●
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																	
Rescue disk	●		●	●	●		●		●	●	●	●	●			●	
Firewall			●	●	●		●	●	●	●	●	●					●
Parental Control				●	●	●	●	●	●	●	●	●				●	
Anti-Spam				●	●		●	●	●	●	●	●				●	●
Software Updater	●		limited	●	●				●	●	●				●		●
Password Manager	●		●	●													
Webcam Protection				●	●			●	●								
Multi-device protection / Multi-platform licensing			●	●	●	●	●		●	●	●	●		●	●	●	●
Secure Browser / banking protection	●		●	●	●	●	●		●			●	●			●	
Browser cleanup / Privacy cleaner / File Eraser	●	●	●	●	●		●	●	●	●	●			●		●	●
WiFi protection / Home Network Protection	●	●		●	●				●	●		●		●		●	
Scans HTTPS traffic	●	●		●	●		●		●			●	●		●	●	
VPN			limited	limited					limited				limited				
Other features				Microphone Monitor	Script-Based Attack Protection, Ransomware Shield, UEFI Scanner, WMI Scanner		Cloud Backup	Data Locker, Vulnerability scanner	Application Control, Private Browsing, Anti-banner, Browser Configuration, Secure Keyboard, On-Screen keyboard	Biometric Password (Truekey), Backup, Malware Removal support guarantee (money-back)	Several of the above features are part of the Microsoft operating system (e.g. Firewall, Software Updater, SmartScreen, Parental Control, Edge, etc.)	Identity Safe password/data protection; Management portal	Cybersecurity-News			Folder Shield	Social Watch, Malware Removal support guarantee (money-back)
Support																	
Online Help	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Support forum	●	●	●	●	●	●		●	●	●	●	●	●			●	●
Phone Support			●	●	●	●	●	●	●	●	●	●			●	●	●
Email support			●	●	●	●	●	●	●	●				●	●	●	●
User manual			●	●	●				●	●	●	●		●	●	●	●
Online Chat				●	●	●		●	●	●	●	●			●	●	●
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, Portuguese, Spanish, Italian, Dutch, German, Romanian, Japanese, Swedish, Norwegian	All	English, Danish, Dutch, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Swedish	English, German, French, Italian, Spanish, Portuguese, Dutch, Polish	English	English, Russian, Spanish, Portuguese, German, Dutch, French, Italian, Greek, Polish, Turkish, Chinese, Hindi, Japanese, Korean	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, Dutch, Danish, French, German, Italian, Norwegian, Polish, Portuguese, Spanish, Swedish	English	English, Japanese, Chinese	English

Copyright and Disclaimer

This publication is Copyright © 2021 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(January 2021)