

Privacy Tools

By [Sven Taylor](#) [Comments](#)



With both governments and corporate entities trampling over the privacy rights of people throughout much of the world, choosing the right privacy tools is now more important than ever.

Why should you be using privacy tools in the digital age?

Let us answer this question by examining a few trends:

1. **Global surveillance** - [mass surveillance technology](#) continues to strengthen and expand around the world - particularly in the United States, United Kingdom, [Australia](#), and other Western countries. (See also the [Five Eyes, Nine Eyes & 14 Eyes](#) surveillance alliances.) This trend continues on, regardless of which political party is in office.
2. **ISP Spying** - Internet providers often record connection times, metadata, and DNS requests, which gives them every website you visit (unless you're using a good VPN). In many countries, this is not only legal, but required. See for example in the United Kingdom (with the [Investigatory Powers Act](#)), United States ([Senate Joint Resolution 34](#)), and now also in Australia ([mandatory data retention](#)). A VPN is now essential protection against your internet provider if you want to retain a basic level of online privacy.
3. **Censorship** - The internet is also becoming less free due to censorship efforts and content blocking. Whether it is China, Germany, or the United Kingdom, authorities are working hard to censor content online. This is particularly the [case in Europe](#). The UK is [now considering](#) 15 year jail sentences for people who view "offensive" websites.
4. **Malicious ads & tracking** - Websites are increasingly hosting invasive advertisements that also function as tracking. Pop-ups and dangerous "click-bait" ads can also deliver malware and take your device over for ransom ([ransomware](#)). Malicious ads, which are delivered through third party ad networks, can even be hosted on [major websites](#).

While the trends are alarming, there are relatively simple solutions to restore both your privacy and security.

But before we begin, one key consideration is your **threat model**. How much privacy and security do you need given your unique situation and the adversaries you may face?

Many people, such as every day internet surfers, are seeking protection against advanced tracking online through advertising networks as well as a higher level of online anonymity and security. Others, such as investigative journalists working with sensitive information, would likely opt for an even higher level of protection.

Here are some privacy and security tools to get you started.

Privacy Tools

Secure and privacy-friendly browser

Everyone needs to be using a secure and privacy-friendly browser for three important reasons:

- Browsers have a large attack surface and can be compromised in many ways.
- By default, most browser will contain lots of private information, including your browsing history, usernames, passwords, and autofill information, such as your name, address, etc.
- Browsers can reveal lots of identifying information about your location, system settings, hardware, and much more, which can be used to identify you through [browser fingerprinting](#).

Secure Browsers: Here are some great options from the [best secure browser](#) guide:

Privacy Tools

- [Firefox](#) - Firefox is a great browser for both privacy and security. It is highly customizable to give you the level of security and privacy you desire, while also being compatible with many browser extensions.
- [Waterfox](#) - Waterfox is a fork of Firefox, with telemetry and other items stripped out to give users more privacy. It is based on Firefox 56 with ESR patches.
- [Brave](#) - Brave is a chromium-based browser that is very privacy-focused right out of the box, unlike Firefox, which requires some customization. By default, it will block ads and trackers, and it's also customizable, fast, and has built-in protection against browser fingerprinting.
- [Pale Moon](#) - Like Waterfox, Pale Moon is also a fork of Firefox, but an older version (based on Firefox 38 ESR).
- [Tor browser](#) - The Tor browser is hardened version of Firefox that also utilizes the Tor network by default (but this can be disabled). It should be noted that Tor was created by the US military and continues to be funded by the US government today. (See the in-depth [Tor](#) guide for more details.)

There are a few other browsers that may be popular, but they are not good choices for privacy reasons. [Google Chrome](#), for example, offers security, but it is extremely invasive and collects all kinds of private data, which Google uses for targeted ads. Similarly, [Opera](#) browser also has a troubling privacy policy, which explains their data collection and data sharing practices.

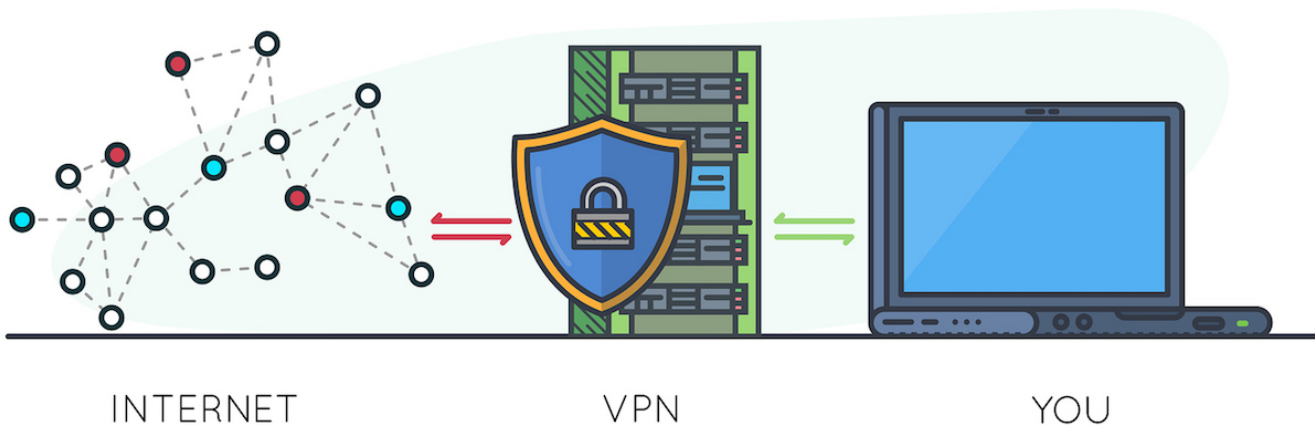
Browser add-ons worth considering - As discussed in the [Firefox privacy](#) guide, here are a few good browser add-ons that may be worth considering:

- **uBlock Origin** - A powerful blocker for advertisements and tracking.
- **HTTPS Everywhere** - This forces an HTTPS connection with the sites you visit.
- **Decentraleyes** - Protects against third-party tracking via content delivery networks (CDNs).
- **Cookie AutoDelete** - Deletes those unwanted tracking cookies.
- **Privacy Badger** - Another add-on from the Electronic Frontier Foundation, Privacy Badger blocks spying ads and trackers.
- **uMatrix** - While this may be overkill for many users, this powerful add-on gives you control over requests that may be tracking you on various websites.
- **NoScript** - This is a script blocker that allows you to control which scripts run on the sites you visit.

Worth mentioning: Don't use a browser-based password manager, which will store your usernames and passwords in plaintext, thereby leaving them vulnerable to exploitation (discussed more below).

Virtual Private Network (VPN)

Using a good [VPN](#) (virtual private network) is one of the simplest and most effective ways to protect your privacy, secure your devices, and also access blocked/censored content online. While VPNs are gaining popularity, there are a number of problematic [free VPN](#) apps that collect user data, as well as [VPN scams](#) and various marketing gimmicks.



VPNs can range in price from \$2.99 per month ([NordVPN](#)) all the way up to \$6.67 per month ([ExpressVPN](#)), and in some cases even more, such as with Perfect Privacy. When you purchase a VPN subscription you will be able to use the VPN on various operating systems and devices, from computers and tablets to phones and routers.

Below are some of the latest recommendations from the [best VPN service](#) report, based on extensive testing and research:



\$6.67
(49% discount)
(30 day refund)

Review
([ExpressVPN](#))

[Visit Site >>](#)
expressvpn.com



€8.95
(7 day refund)

Review
([Perfect Privacy](#))

[Visit Site >>](#)
perfect-privacy.com



\$2.99
(75% discount)
(30 day refund)

Review
([NordVPN](#))

[Visit Site >>](#)
nordvpn.com



\$4.92
(7 day refund)

Review
([VPNArea](#))

[Visit Site >>](#)
vpnarea.com



\$4.80
(7 day refund)

Review
([VPN.ac](#))

[Visit Site >>](#)
vpn.ac

Keep in mind, the “best VPN” will likely vary for each person depending on your own unique needs and circumstances.

Advertisement, tracking, and malware blocker

A good ad blocker is essential for privacy and security reasons. From a privacy perspective, it’s important to block ads because they also function as tracking by recording your online activity to create an intimate user profile, which is used for targeted ads. Ads are also risky from a security perspective because they are often malicious and can infect your device when a web page loads - no clicks required.

Effectively blocking all ads is the only way to go. Here are a few different options from the [ad blocker](#) guide:

1. **Browser ad blocker extensions** - Browser-based ad blocker extensions, such as **uBlock Origin** are quite popular, but they also come with some tradeoffs. Online ads may still be using up resources and tracking you, even if the ads are not being displayed. Choose your ad blocker carefully - some ad blockers, such as Ghostery and Adblock Plus will collect user data for profit and/or show you “approved” ads.
2. **Ad blocker apps** - A dedicated app will most likely do a very good job blocking ads on your device. One popular and well-regarded option is **AdGuard**.
3. **VPN ad blocker** - Another option is to use a VPN that offers an ad blocking feature (VPN ad blocker). I tested various options for the [VPN ad blocker](#) guide and found Perfect Privacy to perform the best.
4. **eBlocker** - [eBlocker](#) is a small plug-and-play device that hooks up to your router and blocks all ads on the network level. It did well in testing for the [eBlocker review](#), but it is rather expensive.

5. **Ad blocking on a router** - Ad blocking on a router can be accomplished various ways - from using ad blocking DNS to loading custom filter lists onto your router.
6. **Pi-hole** - [Pi-hole](#) is a network-wide ad blocker that functions as a DNS server and can be deployed in various ways. It is most often used on a Raspberry Pi, connected to your home router (but there are many other different setup options).

The best ad blocking setup will depend on your situation and needs. If you have numerous devices you use at home, setting up a network-wide ad blocker would be a good solution for blanket protection. uBlock Origin remains a popular option for browser-based ad blockers. I find Perfect Privacy's [TrackStop](#) filters to also work well.

Password manager

The topic of passwords is actually quite large, encompassing password strength, password management, and password storage. In this section we'll focus on password management and storage. Many people store passwords in the web browser, but this is risky because your passwords could be hacked by third parties, since they are stored in cleartext. Instead, you would be better off using a dedicated password manager.

Best password managers:

- **KeePass** - [KeePass](#) is a free, open source password manager that stores all passwords locally, which are secured with a master key or key file. I like KeePass because it can still be used with different browsers through official [extensions or plugins](#), and it works well with Firefox (see [Kee](#)).
 - **LessPass** - [LessPass](#) is also a free and open source password manager that generates unique and secure passwords for you. LessPass can be used through browser extensions, see [their site](#) for more details.
 - **Bitwarden** - [Bitwarden](#) is another great open source password manager that is secure and easy to use. Bitwarden supports all major operating systems and browsers.
-

Secure messaging apps

Secure messaging apps are a great alternative to email, which has numerous inherent flaws and vulnerabilities. The secure messaging apps below utilize very strong encryption standards and work well for teams or individual use on various operating systems and devices.

Messaging Service
Jurisdiction
Price
Operating System
Open source?
Website



Keybase

United States
Free
Windows; Linux; Mac OS; iOS; Android
Yes
[Keybase.io](#)



United States
Free
Android; iOS; Windows; Linux; Mac OS
Yes
[Signal.org](#)

Threema.

Switzerland
\$2.99
Android; iOS
Partially
[Threema.ch](#)



Switzerland
Free
Windows; Linux; Mac OS; Android; iOS
Yes
[Wire.com](#)

Private search engine

Privacy Tools

The big search engines (Google, Yahoo, Bing) record and track your searches, which helps them to build a user profile for their advertising partners. Consider these alternatives instead:

1. [Searx](#) - A very privacy-friendly and versatile metasearch engine.
2. [Owant](#) - A private search engine based in France.
3. [DuckDuckGo](#) - This is a great privacy-friendly Google alternative that doesn't utilize tracking or targeted ads. They also have a zero-sharing policy with other features, but they do record search terms.
4. [StartPage](#) - StartPage gives you Google search results, but without the tracking.
5. [Metager](#) - A private search engine based in Germany.

Private Email

Insecure email providers like Gmail, Yahoo, and iCloud are all bad options when it comes to privacy and security. You regularly read about these providers and their users getting hacked, giving third parties access to emails, and/or cooperating with surveillance authorities ([PRISM program](#)). Here are some alternative secure email providers:

Email Service

Storage

Price/mo.

Website



20 GB+
€1.00 (Free to 1 GB)
Visit Site >>



Up to 20 GB
€2.50 (Free to 500 MB)
Visit Site >>



Up to 20 GB
€1.00
Visit Site >>



Up to 20 GB
\$5.00
Visit Site >>



Up to 25 GB

\$1.66

[Visit Site >>](#)



50 GB+

€1.00

[Visit Site >>](#)



4 GB+

\$4.00

(Free 1 week trial)

[Visit Site >>](#)



2 GB+

€4.41

[Visit Site >>](#)



Up to 20 GB

€4.00

(Free to 500 MB)

[Visit Site >>](#)



Up to 100 GB

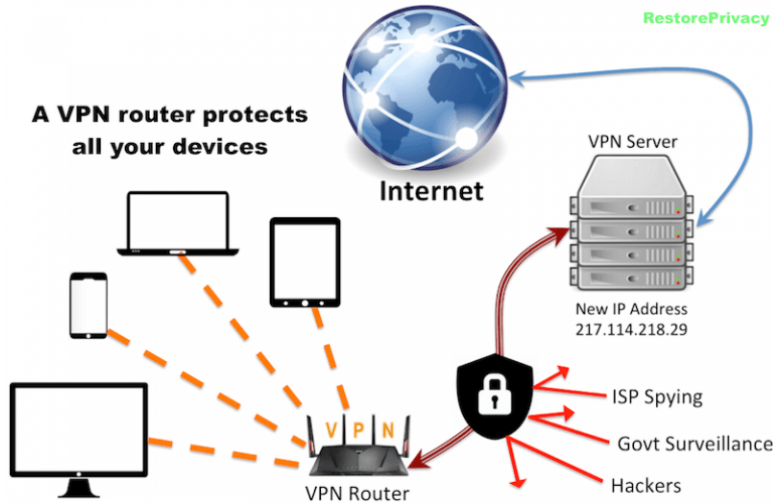
\$1.95

[Visit Site >>](#)

Secure/encrypted router (with a VPN)

If you're looking for a relatively simple way to secure your entire home network and all devices, a VPN on a router is an excellent option. A good VPN router will:

- extend the benefits of a VPN to all your devices without installing software
- protect you against mass surveillance and internet service provider (ISP) spying
- secure your home network against attacks, hacking, and spying
- unlock the entire internet, allowing you to get around geographic restrictions, blocks, and censorship



The only brand that currently offers a large selection VPN-enabled routers is **Asus**. The default Asus firmware, which is called ASUSWRT, supports OpenVPN, PPTP, and L2TP, right out of the box (no flashing required).

When choosing a router, the biggest consideration is **processing power (CPU)**. Running a VPN on a router is a very CPU-intensive task requiring the router to process lots of encrypted data. For these reasons, it's typically good to go with a router that's at least 800 Mhz or more.

For an in-depth overview of all the different VPN router options, see this [VPN router guide](#).

I have also put together three different setup guides using the AsusWRT firmware with different VPN providers:

- [VPN Router Setup - Simple Guide](#) (with [VPN.ac](#))
- [Ad Blocker on a Router with a VPN](#) (with [Perfect Privacy](#))
- [VPN on a Router - Step by Step](#) (with [VyprVPN](#))

Firewall and Network Monitor

Using a third-party firewall and network monitor is a good way to see what connections are being made by various apps in the background on your operating system. These apps can affect your privacy when they "phone home" to send third parties various data from your operating system. With Windows and Mac OS, for example, there are many applications that are connecting to various servers and sending data.

Here are a few good options worth considering:

Little Snitch - Similar to GlassWire, Little Snitch also gives you the ability to monitor all connections going through your Firewall. Little Snitch is only available for **Mac OS**, but it provides many different features and blocking options. It also has a feature to show you the geographic location different apps are connecting to. Check out [Little Snitch here](#).

GlassWire - GlassWire describes itself as a "network monitor & security tool with a built in firewall." GlassWire offers a [free Android app](#) and a paid **Windows** app. The GlassWire Android app is purely a network monitor with no blocking features. However, the Windows app offers more features and full blocking capability.

Operating system



Consider using the free and open source [Linux](#) operating system. There are many different versions of the Linux operating system designed for different types of users:

- If you want the look and feel of Mac OS or Windows, check out [Elementary OS](#).
- [Ubuntu](#) and [Mint](#) are two other popular options.

[Tails](#) is another privacy-focused operating system that can be run live on a USB drive, CD, or SD card.

Problems with Windows and Mac OS

Windows - The latest version of Windows (Windows 10) is a platform built for total surveillance - giving corporations and governments complete access to everything you do on your machine. The basic problem is that the operating system is entirely built on data collection.

Mac OS - While Apple may be slightly better in terms of privacy, it too has many problems. Just like Microsoft, Apple has configured its operating systems to collect vast amounts of your private data, whether it is browsing history through Safari, connection data, location services, and more.

Antivirus software

While not necessarily a “privacy” tool, using good antivirus software is a necessary and critical step. After all, privacy is meaningless without security. The problem, however, is that many antivirus solutions abuse your privacy and may come with some invasive and “unwanted” additions.

Just like with sketchy free VPN services, free antivirus software is also problematic. In testing eight popular free antivirus suites, [Emsisoft discovered](#) that seven of them were bundled with PUPs (potentially unwanted programs), which can be harmful and very annoying. **Tip: avoid free antivirus software!**

Another major issue is privacy. Many popular antivirus suites utilize invasive data collection, to include browsing history, “suspicious” files, metadata, and more. Carefully read through the privacy policy of your antivirus before installing.

Although Restore Privacy does not devote much attention to antivirus software, one solution that offers the highest levels security ([excellent ratings](#)) while also respecting user privacy is [Emsisoft](#).

See also the [antivirus privacy](#) guide.

Restore your privacy

That’s all for now, although this guide will continue to be updated with more privacy tools and information.

Comments?

If you have any feedback, tips, or suggestions based on privacy and security tools you are using, feel free to drop a comment below!

1. John May 6, 2019

Hi Sven,
will you make a guide for android users?

[Reply](#)



- o Sven Taylor May 6, 2019

Hi John, I made a basic [Android privacy](#) guide a while back, but it is a bit outdated. I don’t spend too much time on Android, aside from occasionally testing Android VPN apps, but I’ll keep your feedback in mind for either updating that guide or coming out with something better.

[Reply](#)



2. Irtshy April 24, 2019

Hello all.

I have a recommendation in the category “password managers”:

Password manager is more and more a must have, even more if you use 2FA’s in everyday life.

So, I work mainly with 1password and enpass. Enpass is a good alternative to 1password.

Very important for me is the security, like “AES-256 Encryption” and “data are stored locally by default” (lesspass is only a online based password manager, I think). Bitwarden has some negative critics, because, there are lines in the code, who allows reload JavaScript from third party sources. In addition to this, in the app for iOS and Android are tracker included (Google Analytics, Google Firebase Analytics, HockeyApp).

An another recommendation in the category “Advertisement, tracking, and malware blocker” is:

For the firefox user, Ghostery should be mentioned here as a very good add-on.

Thanks.

[Reply](#)




- o Sven Taylor April 24, 2019

Hello, yes, a very in-depth password manager guide is upcoming (sometime in the next month or so). This page will get updated as well. Thanks for your feedback.

[Reply](#)

Privacy Tools

3.  Myname April 23, 2019

I have a question about Telegram message app. Is it still safe? I've researched a lot but haven't found a decent answer

[Reply](#)

o  John May 12, 2019

No, there is a reason why it is not included in the recommendations.

Messaging is not encrypted by default and even when enabling it, it is not end-to-end encrypted, allowing traffic to be intercepted at the server.

I would suggest using Signal, which is similar to WhatsApp (owned by Facebook), with the added privacy.

[Reply](#)

4.  Flako April 19, 2019

Love your site/ blog!! Incredibly useful info here.

What about Whonix?

Any thoughts about the Whonix OS?

Vm inside a VM.....


F

[Reply](#)

o  Sven Taylor April 20, 2019

Yep, Whonix is a Debian Linux bistro that's a good option for privacy and security.

[Reply](#)

5.  justyou April 7, 2019

Hi Sven, which operating system do you recommend of these? Mint, Elementary, or Zorin OS?

[Reply](#)

o  Sven Taylor April 8, 2019

There are many factors to consider and nobody agrees lol. I'd opt for Mint, but that's just me.

[Reply](#)

6.  Vector April 6, 2019

<https://puri.sm/posts/purism-becomes-pia-first-oem-partner/>

It seems that PIA is the new OEM partner of Purism and will be fully integrated in future Librem 5 phone. Sven, do you think that it is an advantage?

[Reply](#)

o  Sven Taylor April 6, 2019

Hi Vector, I saw that. Well, they are both in the privacy business, but I'm not a fan of bundling unnecessary software on devices. I'm testing out PIA for a new review right now and I have to say it has certainly improved in the past year.

[Reply](#)

7.  Miguel April 5, 2019


Hello all. I would like to purchase a laptop that still has Windows 7. This is obviously for reasons of privacy. However with support and updates ended for this OS is it still possible to set it up and still have safety and good performance? Thanks

[Reply](#)

o  Sven Taylor April 5, 2019

If Windows 7 is no longer supported, and you need Windows, you could get a Linux laptop and run Windows inside VirtualBox.

[Reply](#)

■  Hard Sell April 6, 2019

Whatever happened to the 'UnaPhone Zenith' that Tutanota back in 2016-04-29 was thrilled enough to partner with?

<https://tutanota.com/blog/posts/una-phone-zenith-crowdfunding/>

-

How IT can spy on your iPhone or Android smartphone

<https://www.computerworld.com/article/3259868/how-it-can-spy-on-your-smartphone.html>

.

You Are the Product:

In an Internet world dominated by Facebook and Google, most people understand the phrase "If you aren't paying for it, you are the product." What people don't understand is that this concept has also landed on the shores of the privacy industry. History has proven that as any industry becomes "hot," marketers will inevitably enter it. Companies that have demonstrated little regard for privacy are now using misleading marketing messages to tout their free privacy services, all the while supporting themselves through advertising and selling user data. This leads to important questions, such as why did Facebook pay \$120 million to buy a free VPN app? Why did a popular free browser proxy turn its free users into a botnet for hire? And, what's next?

<https://www.goldenfrog.com/blog/price-of-free-in-online-privacy-industry>

[Reply](#)



o Hard Sell April 5, 2019

Hi Miguel,

I'd say no to your security questions of Win 7. M\$ not supporting patches any longer is like being dropped into a pit of lions or vipers.

- If you persist, try looking for just the Win 7 OS and add it to a partition on the laptop. (Duel boot w/ perhaps Win 10).

Being on the latest hardware will always be a performance driver.

Ebay has listings yet for Win7.

Win 7 wikipedia page mentions paid support for Windows 7 Professional and Enterprise for three years after the end of extended support.

See: Support lifecycle > https://en.wikipedia.org/wiki/Windows_7

Here's an article mentioning more on end-of-life -

<https://www.extremetech.com/computing/276582-microsoft-relents-confirms-extended-support-option-for-windows-7>

-

If your not wanting go with Sven's mention of Linux w/ Win 7.

Go with Win 10 and use some/all of these-

Edited Host file with every URL you can find calling out Windows telemetry. Still everything is doing telemetry today, drivers too.

.

Sphinx Win10FC = firewall that blocks everything by default, uses its own rules, it doesn't set any in the Windows firewall, you can switch the WINDOWS Built-in Firewall ON or OFF at your option due to the completeness of Sphinx Win10FC products independence.

- Free version has limits, as it can not manage system applications (located in c:\windows*).

- Note: originally called the Windows Vista Firewall Control it updates to the latest name of Windows OS to sound current.

*From your computers stand point the Sphinx Win10 Firewall Control stops all the telemetry leaving your device.

<https://www.sphinx-soft.com/Vista/>

.

The Windows OS has plenty of it's own telemetry going on, so the Blackbird (free-donation) program (no installation) takes care of this and runs on all recent desktop editions (Home, Pro, etc.) and to the versions of Windows (Vista, 7, 8, 8.1, 10).

<https://www.getblackbird.net/>

-

Not knowing how you'll go with an OS - anything Windows Updates are covered on this site (ex: safe, not, security only, risks, etc...) from the menu on the lower right.

<https://www.askwoody.com/>

Hope this is helpful :)

[Reply](#)



8. Ghis March 25, 2019

So, I should not trust a free AV, but trust a password-manager like the ones you mentioned above.... (??)

Anyone willing to put some light on this?

[Reply](#)



o Sven Taylor March 25, 2019

Recommended password managers = open source

Antivirus = closed source (and much more potential for invasive/malicious activity going on behind the scenes)

[Reply](#)



o Hard Sell March 26, 2019

Hi Ghis,

You can see it this way -

Addon password managers = specific data stored securely in a vault area on your device accessible by a master password you've given.

*Browsers should never be used for saving login credentials...

**Local device storage is better than cloud storage that has the benefit to sync to your other devices - - but clouds are a bigger risk target to hacks, as not only yours but everybody's data stored there.

Where as -

A / V security products have access to the whole device and it's access to all sections data because it runs at a high system level privileges.

Think 'administer' versus 'user' privileges...

You can restrict it's access by excluding drives, folders, files but unless that's done it reach is the greatest of anything you'll install to a device.

* It may even access the installed files of the 'password manager' but as I understand can not reach the vault area because your master password locks it out.

** So if you'd consider both like dogs, a lap hound compared to a guard dog. Which bite impacts greater harm and who's poop is more substantial...

Both you invite into a device but a wise choice of understanding and a research of the TOS and Privacy Policy, along of users experiences documented should weed out bad actors.

Hope my off the wall rendition - helps :)

[Reply](#)



9. Ronald Bedford March 25, 2019

What about AppMoat by Seventh Knight?

<https://www.seventhknight.com/appmoat.html>

<https://www.seventhknight.com/eula.html>

<https://www.seventhknight.com/privacy.html>

[Reply](#)



o Hard Sell March 26, 2019

What about it - this an advertisement?

Since you can't buy it yet - it's to new to be trusted, no user reviews!

Why mention it then ???

Very Quick look seams similar in functions like VoodooShield.

[Reply](#)



10. Kevin Johnston March 25, 2019

What about Firefox Focus aka "Firefox Klar" ?

<https://support.mozilla.org/en-US/kb/focus>

<https://blog.mozilla.org/blog/2016/11/17/introducing-firefox-focus-a-free-fast-and-easy-to-use-private-browser-for-ios/>

Mainly on android and ios. Doesnt have as many downloads as the main firefox though.

It'd be cool to take a look at this browser and see if its worth all the hype or if its just another free tracking scheme like Opera.

Can it be configured just like normal firefox in your guides?

[Reply](#)



o Sven Taylor March 25, 2019

Hi Kevin, yes, that is a great solution for mobile devices (Android and iOS).

[Reply](#)



11. Grover March 2, 2019

You have great confidence in Emsisoft antivirus. I have used Emsisoft antivirus in the past. It was fair in performance and it was not difficult to find better. At that point, I came to the conclusion that Emsisoft is itself, a virus. Have you tried to get that POS out of your computer? It invades everywhere and regenerates crap you remove. For months, elements keep cropping up everywhere. Emsisoft is a malignant hemorrhoid in a computer system.

[Reply](#)



o Hard Sell March 2, 2019

Grover is it your cold and need to get your temperature going to warm up something. Without any facts and links in support of your proof, your just spouting useless and false tales around about your own opinions that are groundless and useless to anybody else otherwise... Lets be fair by proving some proof for everyone :)

-

As I see it, there is no best Antivirus marketed today and I'm a little put off by the AV industry as my research into it leads me to hope for better of them in 2019 onward. <https://restoreprivacy.com/antivirus-privacy/>

- But, at lest Emsisoft makes the point to tell people about their security and privacy practices. As Emsisoft is pushing the knowledge out about how both benefits you and other helpful articles in their Blog posts. <https://blog.emsisoft.com/en/>

-

Besides an A/V's roll covering the whole system - this leads to infringing on users' privacy. As they then can be a backdoor to devices of your personal data, documents, and files. As far to going in intercepting the web traffic run on it. You can't block them by a firewall as need for verifying file maliciousness and updating itself exists.

- As A/V's run it's access with high system level privileges, then for an whoever entity that leverages them - they have to comply with the laws of the countries in which they are established.

- Not only do A/V security software's reduce the HTTPS connections security, but also introduce vulnerabilities such as in a failure to validate sites certificates properly. https://zakird.com/papers/https_interception.pdf

-

So Emsisoft gets mentioned here, not as perfect but, as a conscientious antivirus provider who respects their users private data, and to only using it when absolutely necessary, while other A/V's are much less scrupulous in the very same roll.

@ Sorry but it almost sounds like your torrenting or download pirated stuff that puts your infections there or it respawn from. With an

A/V software turned off - is in NoWay going to protect the system it's installed on. Excluding hacks, cracks with it = same...

<https://blog.emsisoft.com/en/category/protection-guides/>

Please don't torment yourself without supplying the facts/links in making such further accusations about any A/V - friend :)

[Reply](#)

12.  Hard Sell February 24, 2019

ON A WINDOWS BOX ? Give this a thought...

Should a local or a Microsoft account in Windows 8 and/or 10, be used?

-

What is a local offline account in Windows ?

A local account is a 'username and password' combination that you have likely used to log into any of the legacy Windows operating systems of the past - that is before 8 and 10 came to be.

It grants you access to the system's resources and allows you to customize it of your settings and preferences. As a local user account in Windows 8, 10, it will allow you to install the traditional desktop apps, personalize your settings and use the operating system the old fashioned way (desktop) or limited somewhat in the Metro UI.

{Please offer knowledge on Metro, I've stripped most of it out long ago.}

Of course, in using a local offline account it must be created for a single system each time, so if you have any multiple of systems/devices, you will need to use a different local account for each of them.

-

What is a Microsoft account?

Starting with Windows 8, Microsoft has tried to push users to sign into Windows with a Microsoft linked account. Some features of Windows 8 and Windows 10 require access to the Microsoft cloud, and you therefore have to authenticate the device with a Microsoft account.

[-For a complete list, just type "sync" in the Start menu or Start screen.]

A Microsoft account is the rebranding of any in the previous accounts for Microsoft products. If you have ever used services like Hotmail, Outlook.com, Skype, or devices like Xbox game consoles or Windows smartphones, then you are sure to have a Microsoft account already.

- By rebranding and combining all these different accounts, Microsoft allows for a complete integration of all their services into a single online account. This means that you can use it to get access to everything connected to the Microsoft ecosystem. It means M\$ knows a lot about U.

-

The main difference - mostly it's about trusting your privacy with M\$.

The big difference from a local accounts stance, is that you use an email address instead of a username (in local account) to log into the operating system. So you must use either a Microsoft indentured email address (hotmail.com, live.com or outlook.com), or Gmail, and even your ISP specific email address to create your Microsoft account. This type of sign-in as the cloud process is meant that you cannot remove your system account password protection.

You can only change it.

- Also, signing in with Microsoft account allows you to configure a two-step verification system of your identity each time you sign in. This requires you to enter a security code each time you sign into a device that is not on your trusted list.

- Is this not as bad as using Google products for most everything as well ?

<https://restoreprivacy.com/google-alternatives/>

-

Some Pro's and Con's

This is all on top of Windows known Telemetry in it's OS systems.


- You'll likely have access to the Windows Store but, if you use Windows 8, 10 Home, you cannot download and install apps without a Microsoft account supplied. Windows 8, 10 Pro, Enterprise or Education, you can download and install apps from the Windows Store, but only if they're free. You must sign in using a Microsoft account so that their paid licenses are associated with you.

- A local offline account in Windows, pertaining to your system settings will not be synchronized across any of the computers and devices you may also have.

- Ensure signing up/in Windows by creating a local account - simply disconnect your computer from the Internet when you install Windows 8, 10 it's that easy to see a different menu.

- A downside of this Windows account feature is that whenever you log on to your Windows computer, you'll also sign in to the Microsoft's cloud. *This means that Redmond knows when you sign in, and from where. NOT everyone feels comfortable with this power given to M\$ by itself.

[Reply](#)

13.  dwg February 23, 2019

Boa tarde Sven gostaria de usar o Starpage mais possui problema com imagens sexy poderia me ajudar com indicação de um filtro para imagens ou até total remoção de imagens do Star page .

Good afternoon Sven would like to use the most possible Starpage with sexy images could help me with the indication of a filter for images or even the total removal of images from the Star page.

[Reply](#)



o Hard Sell February 24, 2019

Hi dwg,

Try looking here for what your wanting to do or settings changed.

<https://support.startpage.com/index.php?Knowledgebase/Article/View/192/5/what-is-your-family-filter-and-how-does-it-work>


or

<https://support.startpage.com/index.php?Knowledgebase/Article/View/1162/19/the-family-filter-is-blockingreturning-too-much-content-how-do-i-turn-it-off-or-tighten-it>

or

<https://support.startpage.com/index.php?Knowledgebase/Article/View/1237/19/video-results>

[Reply](#)

14.  Paul January 30, 2019

Great site Sven! Regarding another privacy site, privacytools.io, that site is contradictory. It says that "You need your browser to look as common as everyone else. Disabling JavaScript, using Linux, or even the TBB, will make your browser stick out from the masses." And yet it advertises the like of NoScript and Linux systems. Does the person running it not know that making all the changes to Firefox's about:config as shown, and installing the advertised browser extensions, will make a person's browser stand out more?

[Reply](#)

o  Sven Taylor January 30, 2019


Hi Paul, yes, that is the tricky issue with [browser fingerprinting](#), it is a catch-22.

[Reply](#)

o  Hard Sell February 1, 2019

Hi Paul,
It's comments like yours I keep hoping to see show up here as more people find the site. I try to offer insights that I understand as well. Good points you've brought up - Sir :)

[Reply](#)

15.  Vector January 25, 2019

Hi Sven,
I currently use VoodooShield (VS) and it seems to me that the privacy terms related to product are not abusive - at least it looks like VS just collects very minimal information that is not aimed for re/selling.
<https://voodoooshield.com/>
<https://voodoooshield.com/Privacy.aspx>
<https://voodoooshield.com/Terms.aspx>
VoodooShield is a kind of security software that complements the AV programs and it simply locks the system (something like a NoScript for Windows system) by preventing any process to run outside those who has been white-listed. It is not open source but it seems to me like a good option for security reason which impacts to certain extend the privacy. I was wondering have you ever tried VoodooShield and would you please share your opinion? In this regard, do you know any website similar to the one of <https://thatoneprivacysite.net/> where the terms and conditions related to AV products have been analyzed? I am thinking that probably after the Kaspersky public issues maybe someone has publish some interesting article about the privacy aspects of the AV products. Thanks.

[Reply](#)

o  Hard Sell January 29, 2019


Hi Vector,
I've tried VoodooShield for a short time and couldn't get the knack of my system running it. That was back some years ago... You can see some favorable users opinions here about two years ago and beyond that - <https://malwaretips.com/threads/voodoooshield-have-you-tried-it-would-you-recommended-it.61800/page-4>
Then an extensive users talk and time coverage of it here - <https://www.wilderssecurity.com/threads/voodoooshield.313706/>
-
I use to used KIS by Kaspersky back 3 years ago till VPN.ac said not too as they said it'll cause me problems with their clients. Same troubles I suppose happened with AdGuard, as it ran into priority problems with the order of some kind of KIS driver calls made in my system - in about the same time frame of events before loosing KIS.
Then I caught word that the US defense departments dropped it from their 'to use list' of software's as it's founders were suspected of KBG ties as reviled - all before the last presidential election scandal's broke.
I completely moved over to Emsisoft Internet Security that's gone now. It has since merged with Emsisoft Anti-Malware.
<https://blog.emsisoft.com/en/28245/merging-emsisoft-internet-security-with-emsisoft-anti-malware/>
-

AV products have been analyzed? About your metadata privacy you mean? Good point, what else has free run to every nook and cranny of your system. Even to whats known of VirusTotal, as I use it as a second opinion or first understanding to a lot of things. There are others in this lineup of file uploads in online checking services, even the online scanners of the most popular anti-virus/malware vendor's to run scans and check out your PC for free. What else do they find out about you?

-
Only one study I know of was done in 2014 by AV-Comparatives, for Data Transmission in Internet Security Products.
http://www.av-comparatives.org/wp-content/uploads/2016/12/avc_datasending_2014_en.pdf
Emsisoft Blog had a post JUNE 26, 2015 covering Antivirus software: protecting your files at the price of your privacy.
<https://blog.emsisoft.com/en/17153/antivirus-software-protecting-your-files-at-the-price-of-your-privacy/>
AV Comparatives did not include questions about data retention which is unfortunate. Some companies may use the transmitted data only to determine the correct course of action, while others may save it for a period of time or maybe even forever.
It has been suggested that users only download and install products of reputable companies, and that they read the End User Agreements before they do.

-
Despite claim's they anonymize any user's data that's collected. If they anonymize your data, don't you think they are able to un - or de-anonymize this same data just as easily on their end?
- Then when you do install something run the terms through the below program-
EULalyzer Personal / Free for personal & educational use - <https://www.brightfort.com/eulalyzer.html>
Would be nice if thatoneprivacysite would branch out and cover the A/V likes there too...
Thanks :)

[Reply](#)

16.  Mark January 4, 2019

Disposable email addresses providers like Burner Mail and Blur are also privacy tools.

[Reply](#)

o  Sven Taylor January 4, 2019

Good point Mark, I'll consider that for the next update.

[Reply](#)

o  Hard Sell January 5, 2019

33MAIL is another one I can say works very well.

[Create a new e-mail address whenever you need one. Maintain complete control over active addresses. Forwards all mail to your existing e-mail address. You can even reply anonymously to emails forwarded by 33Mail. Never receive unwanted e-mail again!]

[Reply](#)

o  Hard Sell January 6, 2019

Hi Sven and Mark,

@Sven I don't know if disposable email address are really a privacy tool, when Private Email >Best Secure Email Providers list on your site already, offers Aliases - through their services. Although most of the encrypted mail services offered there, you can't easily delete an alias but only disable it from being active.

-

@Mark did you know Abine Blur recently compromised it users. I don't believe this was out of wilful miss-conduct but more to a problem of gross negligence.

<https://www.abine.com/blog/2018/blur-security-update/>


-

Even my own mention of 33MAIL deserves scrutiny, as I don't see a Privacy Policy offered on it's site but only a TOS, and usually one or the other gives an indication to their actual address of location and/or jurisdiction.

And a whois look up doesn't offer much to their location - <https://www1.domain.com/whois/whois.bml>

- FYI, the US may be headed to a recession as the trade wars and now General Motors layoffs lay the indications of more to come.

[Reply](#)

17.  Vector January 4, 2019

What is your opinion on Riot? It is based on the Matrix protocol.

<https://about.riot.im/>

How do you like the open-source XMPP clients like Gajim? Particularly Gajim may use the OMEMO protocol.


<https://gajim.org/>

[Reply](#)

o  Sven Taylor January 4, 2019

Hi Vector, I like Riot quite a bit. I haven't looked into Gajim much yet.

[Reply](#)


■  Vector January 5, 2019

Unfortunately, Gajim is not multi-platform messenger (no iOS, no Android support).

I am not sure what's happened with Jitsi and particularly with the support of OMEMO protocol. They implement the OTR protocol but I am not sure whether it is not a bit obsolete.

<https://jitsi.org>

[Reply](#)

18.  Hard Sell January 1, 2019

The most widely used privacy tool anyone has is setting right behind their eyes. Called common sense or that gut feeling, trust your instincts that your brain gives to you.

-One practice I find helpful is to limit the installed programs to what I need and use, uninstalling those that have had little use to me in 6 months of the year.

-

How many people actually read a 'EULA' license agreement of the software they install?

Or for that matter of a Website's Privacy Policy to make sense of the nonsensical?

Don't just write off the 'EULA' license agreements and Privacy Policies as too long and verbose to read...

And other similar documents, including language that deals with:

Advertising - Tracking - Data Collection - Privacy Related Concerns
Installation of Third-Party / Additional Software
Inclusion of External Agreements By Reference
Potentially Suspicious Clauses

-
You know in today's world that it's important to know things like-

1. If the software you're about to install, displays pop-up ads, transmits personally identifiable information, uses unique identifiers to track you, or much more.
2. Of a website's privacy policy for potentially interesting words and phrases, then what role Third-Party External Agreements play.

-
Know What You're Getting Into - Pop it into EULalyzer .

This one's free as you do some work for the results.

<http://www.brightfort.com/eulalyzer.html#Overview>

-
EULalyzer Pro for powerful and instant analysis using EULA-Watch, supports automatic license agreement detection and scanning for most major software installers.

<http://www.brightfort.com/eulalyzerpro.html#EULAWatch>

Note: This program does not provide legal advice.

You should always consult a lawyer for advice on legal issues.

<http://www.brightfort.com/privacypolicy.html>

[Reply](#)



19. Hard Sell December 31, 2018

The Good Trustworthy Antivirus programs should be in the Ranks above.

To thwart off malicious and unwanted software, and to reliably prevent phishing- and ransomware-attacks.

STAY away from the Free versions and you really don't need their Internet Suites that some offer in all the bundled sub products.

I like to call these Jack of all Master of none...

-
Privacy - (taken from #5) <https://blog.emsisoft.com/en/29702/choosing-antivirus-software-2018/>

Some are extensively collecting data about your computer usage to improve their products. While simple product usage telemetry is usually anonymized, some products may also upload suspicious files from your computer to the vendor's scanning cloud. You need to be able to fully trust that the vendor will handle your files responsibly, ethically and securely. After all, a private document could be part of such an upload, too.

-
Free Versions - "Has the antivirus industry gone mad?"

https://blog.emsisoft.com/en/11550/has-the-antivirus-industry-gone-mad/?ref=offer000012&utm_source=newsletter&utm_medium=newsletter&utm_content=mainnews&utm_campaign=offer000012

Fact: 7 out of 8 tested free antivirus suites bundle with PUPs

Comodo AV Free: changes home page and search engine provider to Yahoo during the installation process, unless the user unchecks the box.

-
Avast Free: offers Dropbox during installation by default, unless you uncheck the box.

-
Panda AV free: installs Panda Security toolbar, yahoo search takeover and MyStart (powered by Yahoo) home page takeover.

-
AdAware free: installs WebCompanion by default unless user unchecks the box. Also installs Bing Homepage takeover and Bing search takeover by default, unless opted out.

-
Avira free: offers Dropbox after installation. Takes over search with Avira Safe Search, which is a white-labeled version of the Ask toolbar. Avira does disclose that it partners with Ask.

-
ZoneAlarm free AV + Firewall: with Custom Install: ZoneAlarm homepage and search takeover. This is a rebranded Ask toolbar, which is not mentioned on ZoneAlarm's website.

-
AVG free: installs Web Tuneup, including AVG SafeGuard. Sets AVG Secure Search as homepage, new tab page and defaults search engine. Toolbar is Ask powered, although this is not explicitly stated. Also offers AVG Rewards, which displays popup advertisements with coupons and deals.

-
When the product is free the real product is YOU

[Reply](#)



o Sven Taylor December 31, 2018

Excellent points, Hard Sell, thank you. I'm going to update this guide with that information. Emsisoft is a solid choice and is one of the few AV's that give you both security and privacy.

[Reply](#)



■ Hard Sell January 1, 2019

I agree about Emsisoft's security and privacy practices, and then their always trying to get the word out about both. Here's some interesting facts you may find helpful to reference of anti-virus companies.

<https://www.ivpn.net/blog/are-anti-malware-products-uploading-your-private-data>

-
<https://sanfrancisco.cbslocal.com/2017/03/08/wikileaks-cia-documents-antivirus-software-reviews/>

-
<https://blog.emsisoft.com/en/17153/antivirus-software-protecting-your-files-at-the-price-of-your-privacy/>

[Reply](#)



20. Hard Sell December 31, 2018

Hello all

If - one key consideration is your digital threat model.

I'd definitely set the privacy bar HIGH there - as with all the Corporate, Government, and Web advertising entities collecting your data massively like never before.

A picture develops from all your collected data that can be like looking at a cross-cut of an adult tree growth rings, they'll see an extended picture of your online life with all the collected data - just think of a two year period online what could be learnt of ourselves.

-

Did you know some advertisers attach the MAC address of a users devices to their demographic profiles so they can be retargeted even if the user clears their cookies and browsing history.

Clearing cookies doesn't help you with web bugs and respawning cookies by the way.

-

If that old saying - Fruit doesn't fall far from the tree - think about your offspring and relatives having similar likes as yourself, that your online habits and interests could most likely & will affect them.

How I try to guard my privacy and remember once it's captured by one entity it can be shared, hacked in to, or go into a data base to live on for a very long time.

-

I'm running a 8.1 x64 Windows rig with IE 11 / Slimjet browsers, SSD and 16GB Ram. No Pen or Touch for display, no camera.

I've cleaned out most of the Metro crud for mostly a desktop experience as of the older Windows OS's.

StartPage = my homepage and search engine.

Emsisoft = my main anti-malware.

Malwarebytes = 2nd line layer for malware defense.

RoboForm = (locally) not cloud, password manager for website logins with a strong password generator (usually at 20+ characters).

Maxa Cookie Manager = DATED / but still works covering many browsers - cleans cache, history, timed auto cookie deletion, w/ cookie evaluation - white/black lists, last update was 12 February 2014.

Adguard = ad blocker w/ personal privacy modules and stealth settings, really a lot more it has to offer than blocking ads.

VPN.ac = hides real IP - server side DNS, never surf without it.

VPNCheck Pro = DATED / DNS leak fix, changes your MAC address automatically but also your Hostname and Computer name, this also applies for all the Computer ID sniffer algorithms on networks.

Shadow Defender = runs your system in a virtual environment with no change to your real environment.

AOMEI Backupper Pro = is a complete yet simple backup software for Windows PCs and laptops, supports system/disk/files/partition backup & restore, file sync, and system clone as well as provides scheduling backup, merge images, dynamic volumes backup, UEFI boot, and GPT disk backup.

Sphinx Win10FC = firewall that blocks everything by default, uses its own rules, it doesn't set any in the Windows firewall, you can switch the WINDOWS Built-in Firewall ON or OFF at your option due to the completeness of Sphinx Win10FC product independence - free version has limits as can not manage system applications (located in c:\windows*).

Note: originally called Windows Vista Firewall Control it updates to the name of current OS to sound current.

The most understandable detailed review I've seen here-

<https://msfn.org/board/topic/174417-sphinx-windows-er-10-firewall-control/?tab=comments#comment-1107771>

-

Most of the above have free versions but, all these I use are paid for except the web browsers - search engine.

Although free has more of a consequence to an individuals privacy, there is really no guarantee that a paid product by way of your paying for it, offers you any more of a guarantee that of your data won't be collected and then sold on to others. From your computers stand point the Sphinx Win10 Firewall Control stops all the telemetry.

The Windows OS has plenty of it's own telemetry going on, so the Blackbird (free-donation) program (no installation) takes care of this and runs on all recent desktop editions (Home, Pro, etc.) and the in versions of Windows (Vista, 7, 8, 8.1, 10).

<https://www.getblackbird.net/>

-

I also run two system cleaners-

R-Wipe & Clean = automatically at browser close for browser / user set tasks, and at system shut down for full computer task list.

PrivaZer = automatic and manually at browser close for internet traces, and once weekly on the c:\drive.

HOPE this helps some people to know what steps I feel necessary in todays era of the internet.

[Reply](#)



o Hard Sell January 1, 2019

I said 'The most understandable detailed review I've seen' about 'Sphinx - Win10FC' was with that above link, I forgot about this more detailed one.

Allowing network access to only trusted programs is a fundamental step in increasing your security and privacy. Windows 10 Firewall Control is a simple free/paid third party program to control and monitor the network activity of applications. It prevents undesired information leaks for incoming and outgoing connections for applications running locally or remotely on Windows.

-

Windows 10 Firewall Control puts you in control of all network communications your PC has. It can prevent applications from "phoning home", sending "telemetry", showing advertisements, checking for updates without your permission and so on. It's very useful to detect and stop zero-day malware by blocking its network activity. By adopting a block-everything-by-default approach and allowing access to only whitelisted apps, Windows 10 Firewall Control gives you full control over network communication.

-

The application is very compact, has a small installer and low memory footprint. It's compatible with Windows 7, 8, 8.1 and 10. The installer includes both 32-bit / 64-bit versions and automatically installs the appropriate version. Both IPv4 and IPv6 protocols are fully supported.

What's special about Windows 10 Firewall Control is that it blocks connections by default, automatically detects when a program on your computer is trying to connect and shows a clear notification prompt asking your permission to allow or disallow it. Although the built-in Windows firewall includes a prompt for inbound connections, Windows 10 Firewall Control goes one step further and shows you prompts for outbound notifications too. The ease and transparency in setting up it's firewall permissions for desktop and Store apps is what sets this program apart.

Privacy Tools

-

You can set the desired network permissions for any program easily with a single click. The most safe and reasonable permissions are advised automatically. A rich set of predefined permissions is available, you can choose and apply the chosen permission anytime. It has an optional balloon notification that instantly pops up and includes detailed activity of each app and a description of why the app was blocked or allowed.

Both, already established and potential app connections are listed. In the paid versions, a predefined set of permissions (security zones) can be set for each program and activity type. A zone can be applied to any application with a single click. You can customize a predefined zone or create a new one that fits your needs precisely.

-

Many other features are included and the application is continuously being improved for many years. For instance, there is a way to automatically configure hardware routers/firewalls, create a safe virtual sub-network inside a single local network and control network permissions remotely. The application's features are configurable such as disabling popup for new detected program trying to connect, suppress the log balloon, change the sound used for the prompt, import/export settings, password protect the settings panel and others. Windows 10 Firewall Control runs from the notification area (system tray) and also has taskbar integration.

-

The program has a simpler, free version but the advanced features are available in paid versions. All versions and editions are available in English, German and French. Very careful and personal support is available for free. You can compare the features available in the free version and the paid versions here: <http://sphinx-soft.com/Vista/order.html>