3 Tools You Need to Remove Windows 11 Tracking

Don't completely trust the default settings when it comes to privacy. Windows 11 is no exception, as it often oversteps its bounds when it comes to data collection.

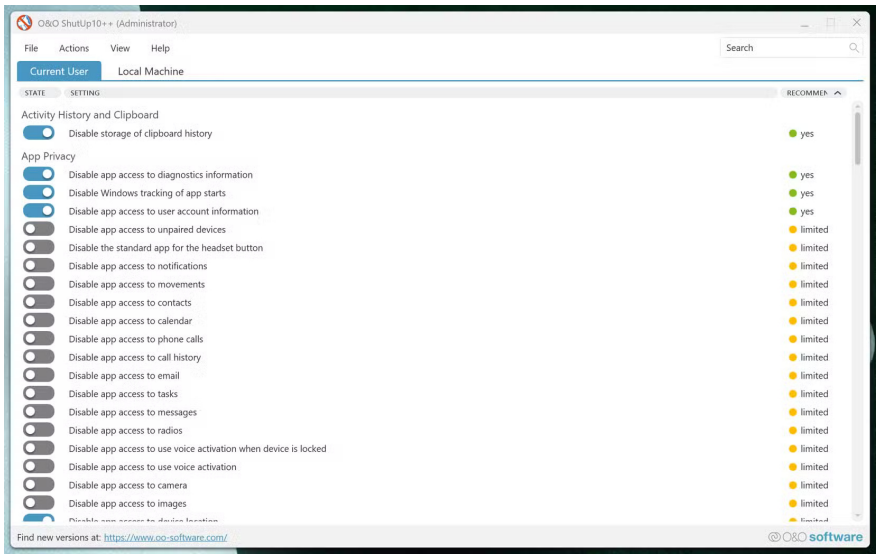
Don't completely trust the default settings when it comes to privacy. Windows 11 is no exception, as it often oversteps its bounds when it comes to data collection. However, these specific tools can effectively limit Windows telemetry without disrupting functionality.

3. O&O ShutUp10++

Turn off hidden Telemetry settings

You won't just find Windows privacy options on the surface. There's also telemetry at the registry level that runs in the background. O&O ShutUp10++ will expose the registry settings that Windows hides.

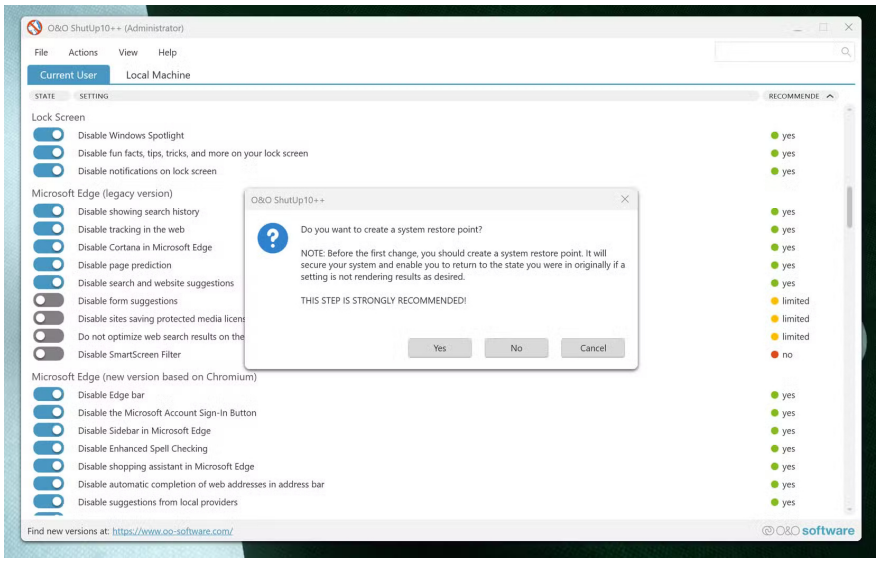
It is a portable application that provides access to over 100 privacy control options and categorizes them as **Recommended** , **Limited** or **No** based on potential impact on the system.



The interface shows the extent to which Windows monitors user activity. You'll see this in the **App Privacy** settings , which include collecting diagnostic data and sharing account information, suggesting that Windows 11 won't respect your privacy by default. Each setting includes basic explanations, although some are still technical.

Follow these steps to use O&O ShutUp10++ safely:

1. Run the downloaded executable file with admin rights.
2. Select the **Current User** or **Local Machine** scope .
3. Accept the system restore point prompt (recommended for safety reasons).



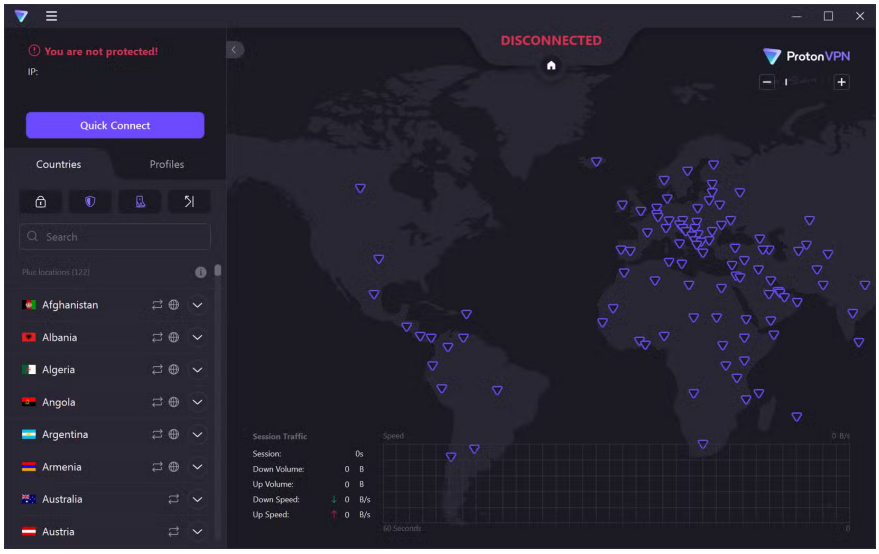
2. Use a VPN

Hide your location from Microsoft services

We can disable location services in O&O ShutUp10++, but sometimes that is not the best option, as other services benefit from this feature. Microsoft services collect that location data through IP geolocation. Every time you check for Windows Update, sync OneDrive, and connect to the Microsoft Store, your approximate location is revealed to their servers.

To avoid this, you should use a VPN. This doesn't prevent Windows telemetry from being collected, but it does mask your real IP address by routing your traffic through remote servers. This creates a geographic disconnect between your actual location and what Microsoft's telemetry system records.

Your free VPN will only cover basic security needs, although paid services often offer better server infrastructure and connection speeds. The important thing to consider is not the cost, but the provider's data handling policies and technical implementation.

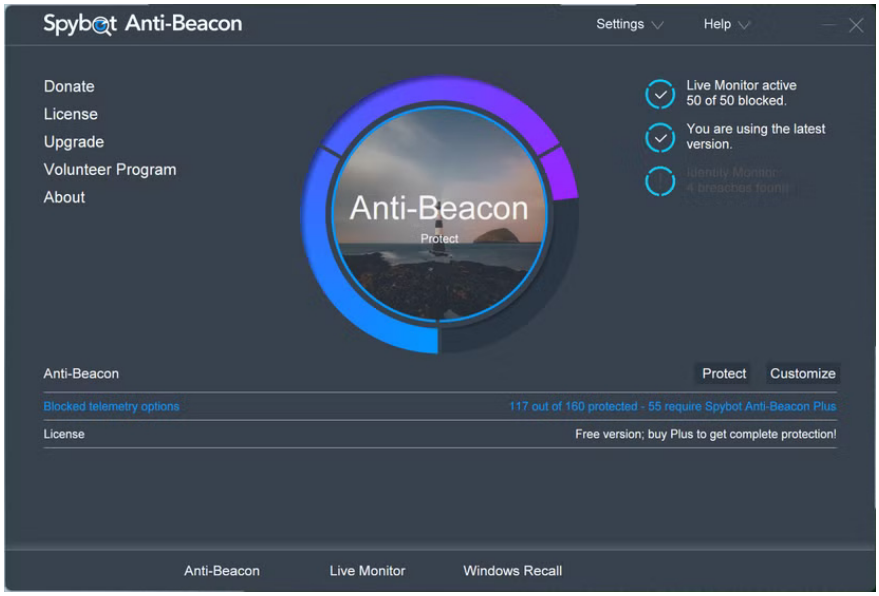


1. Spybot Anti-Beacon

Block Telemetry hosts

This tool blocks telemetry at the network level by preventing Windows from contacting specific Microsoft data collection servers. The tool modifies the system's hosts file to redirect telemetry requests to local server addresses.

When Windows tries to send diagnostic data to **telemetry.microsoft.com** or similar endpoints, those requests are blocked before they leave your computer. This creates a more comprehensive barrier than just tweaking the registry.

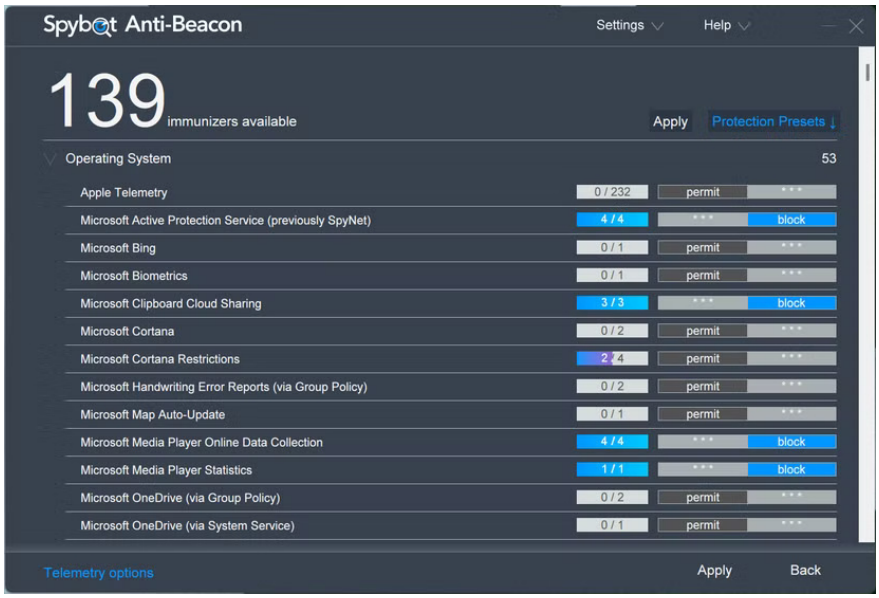


Spybot Anti-Beacon targets over 100 known Microsoft telemetry hosts. The blocking is transparent; Windows continues to attempt to send data, but the connection fails. It blocks telemetry transmissions without disrupting

core system functionality, such as updates or activation.

Follow these steps to configure Spybot Anti-Beacon:

1. Run the installer with admin rights.
2. After installation, review the list of hosts you want to block in the main interface.
3. Click **Apply** to enable telemetry blocking.
4. Restart the system to ensure the changes in the hosts file take effect.



You finished reading the article "**3 Tools You Need to Remove Windows 11 Tracking**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.