



PROTECTION

WHAT THE RED.ONE VPN DOES

Red.One protects traffic in transit and applies secure DNS filtering whenever the tunnel is active.

FULL-TRAFFIC PROTECTION

Encrypted traffic

Web, app, email, and DNS traffic leaving the device is routed through an encrypted tunnel to the Red.One gateway. This helps prevent local networks, public Wi-Fi providers, and nearby observers from reading or altering it in transit.



ENCRYPTED NAME RESOLUTION

Protected DNS

DNS requests travel through the encrypted connection and a secure filtering layer, reducing local monitoring, manipulation, and common DNS leaks.



SECURITY FILTERING

Threat blocking

Known phishing, malware, command-and-control, and other high-risk domains can be blocked before the device connects.



PRIVACY FILTERING

Ad and tracker reduction

Many advertising, tracking, telemetry, and unnecessary data-collection domains are blocked. Online services generally see the Red.One gateway's public IP instead of the current network's public IP.



EVERYDAY USE

QUICK CONTROL

Turn protection on or off quickly

Open the VPN app and use the switch beside Red.One. On a computer, select Red.One and choose Activate or Deactivate. Confirm the app shows Active before browsing.



AUTOMATIC RECONNECTION

Optional on-demand protection

On Apple devices, enable On-Demand Activation for Wi-Fi, cellular data, or both. On Android, enable Always-on VPN in system VPN settings. The stronger block-without-VPN option stops internet access if the tunnel cannot connect. On Windows, leave Red.One activated for continuous protection.

