LAYERED PROTECTION

Integrated network and mobile defense

A bespoke encrypted tunnel and policy-driven DNS layer work together to protect traffic, reduce network visibility, and block risky destinations before a connection is completed.

Encrypted transport
Protects traffic on untrusted networks and presents a protected exit address to internet services.

Secure DNS
Applies threat intelligence, phishing and malware blocking, deceptive-domain defense, and configurable policies.

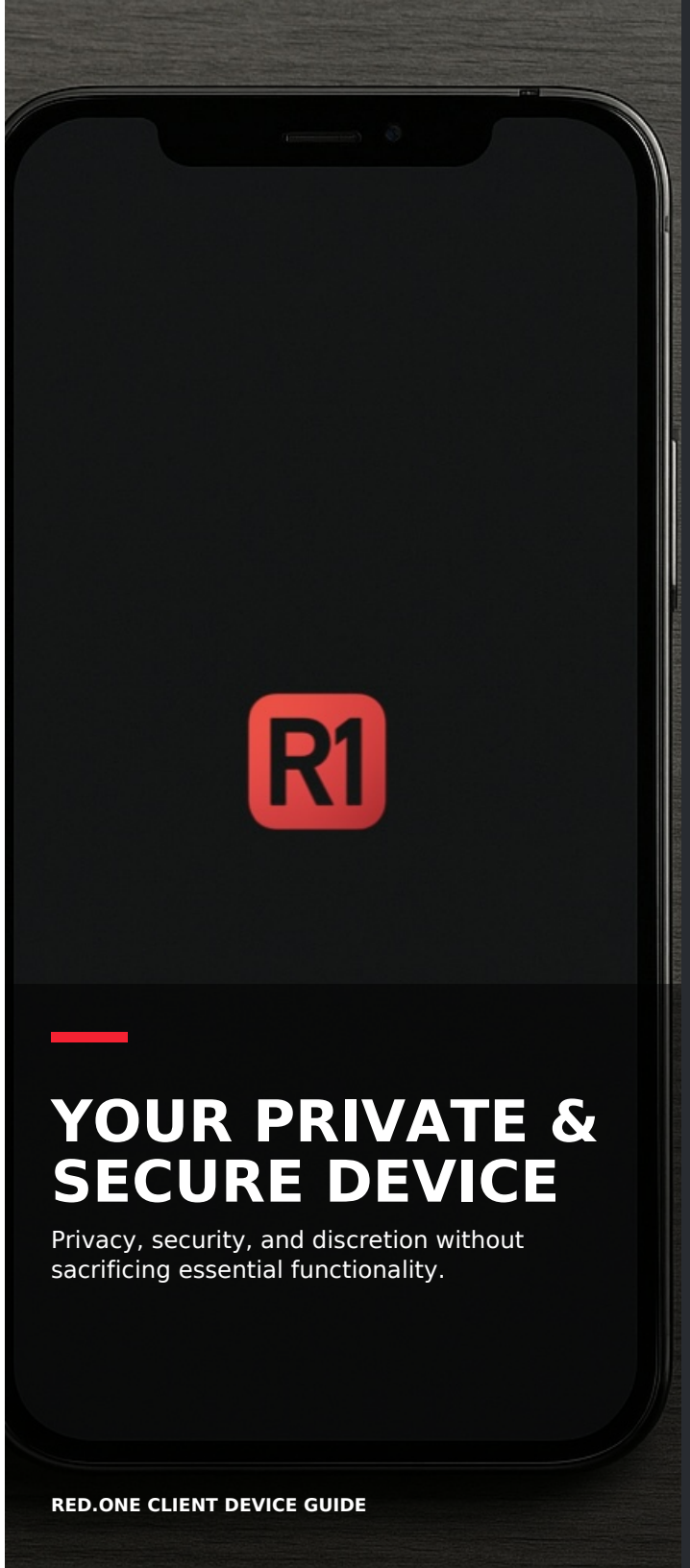
Mobile threat defense
Monitors apps, files, networks, operating-system risks, phishing, unsafe Wi-Fi, and device integrity.

10-SECOND CHECK

- VPN / encrypted tunnel and secure DNS are active.
- No unexpected alerts, prompts, apps, or profile changes.
- Wi-Fi, Bluetooth, location, and scanning are off unless needed.

red-one.info

Red.One solutions reduce exposure and attribution risk; they do not guarantee anonymity or protection from every technical, legal, or operational threat.



YOUR PRIVATE & SECURE DEVICE

Privacy, security, and discretion without sacrificing essential functionality.

RED.ONE CLIENT DEVICE GUIDE

WHY RED.ONE

Built for elevated privacy and security concerns

Red.One provides privacy-focused devices, connectivity, applications, and operational solutions for executives, high-profile individuals, protective teams, travelers, and others with elevated risk.

- Hardened Apple and Android devices
- Privacy-focused mobile, eSIM, and hotspot service
- Encrypted communications, VPN, and secure DNS
- Privacy, navigation, safety, and operational apps
- Turnkey provisioning for individuals and teams

CORE OBJECTIVE
Reduce unnecessary tracking, attribution, telemetry, and digital exposure while preserving the functionality the user needs.

CUSTOMIZED SETTINGS

Configured to collect less, reveal less, and expose less

Exact settings vary by platform, mission, and client requirements. Typical provisioning includes:

- Separate accounts configured to minimize attribution to the end user.
- No personal identifiers used for service, payment, recovery, contacts, or cloud profiles unless authorized.
- Strong access controls: passcode, short auto-lock, hidden notification previews, and restricted lock-screen access.
- Minimum permissions for location, microphone, camera, photos, contacts, and nearby devices.
- Reduced telemetry: advertising personalization, analytics, diagnostic sharing, and unnecessary background activity minimized.
- Protected networking: persistent encrypted tunnel, secure DNS, no automatic Wi-Fi joining, and private addressing where supported.
- Managed security: approved updates, remote management, threat defense, backup, lock, and wipe according to policy.

Hardened does not mean invulnerable. Unsafe account choices, repeated co-location, personal-network use, oversharing, or unapproved apps can defeat a secure configuration.

STRATEGIC APP SUITE

Approved capabilities for privacy, work, travel, and safety

PRIVACY & SECURITY
Encrypted VPN, private and custom DNS, private browser, app privacy analysis, cellular security monitoring, and remote security camera.

COMMUNICATION
End-to-end encrypted messaging and calls, encrypted email, group communications, and push-to-talk.

PRODUCTIVITY
Secure storage, calendar, password manager, MFA, remote desktop, encrypted notes, cloud tools, and a privacy-focused AI assistant.

NAVIGATION & TRAVEL
Primary and offline navigation, temporary or group location sharing, ride-hailing, weather radar, and translation.

HEALTH & SAFETY
Emergency-room locator and offline first-aid guidance.

TSCM SCREENING
Bluetooth tracker detection, Bluetooth device scanning, and Wi-Fi environment analysis.

Account separation
All accounts created for the device are configured to minimize attribution to the end user.

Some applications require proprietary mobile frameworks or associated push-notification infrastructure.

OPERATIONAL SEPARATION

Keep the device unassociated with your personal identity

PRIVACY IS OPERATIONAL.
Your habits determine whether the device remains separate from your personal digital identity.

1 Do not sign in to personal accounts or use personal phone numbers, emails, payment cards, addresses, or trusted devices for recovery.

2 Do not import personal contacts, photos, calendars, passwords, browser history, backups, or SIM profiles.

3 Do not connect to home Wi-Fi, personal hotspots, vehicle systems, wearables, printers, earbuds, or personally associated devices unless approved.

4 Avoid routine co-carry. Repeated operation beside your primary phone can create a behavioral association.

5 Use approved apps only. Grant minimum permissions and disable Wi-Fi, Bluetooth, location, and scanning when unnecessary.

6 Keep the purpose narrow. Do not gradually convert the Red.One device into a second personal phone.

IF SOMETHING DOES NOT LOOK RIGHT
Stop the affected activity, leave untrusted networks, preserve alert details, and report the event. Do not factory-reset, delete evidence, or install unapproved tools unless directed.