Privacy [OS]



ACTIVE DETECTION. IMMEDIATE DEFENSE.

True security requires admitting that third-party apps introduce risk. That is why Privacy OS pairs an aggressively minimized attack surface with active, continuous defense. We have eliminated major vulnerabilities by removing Bluetooth, location tracking, and GSM telephony, but our core strength is vigilance. Built-in, OS-level threat detection constantly scans for unauthorized packages and tampered binaries. If a vulnerability is ever exploited through an external app, the system immediately catches the anomaly—triggering automated safeguards and instant data-destruction protocols to ensure your information remains permanently out of reach.

SECURITY COMES STANDARD

Active Threat Detection and Response
Continuous automated checks identify unauthorized packages, cloaking apps, root access, and tampered system binaries.

Emergency Reset
Hold the power button to trigger a one-step wipe of all data and settings. No menus, no delays.

Asset Loss Prevention
Factory reset on inactivity ensures all data is automatically destroyed if a device is lost, stolen, or expires.

Location Services Removed
Location and fused location code is fully stripped from the OS, not just disabled.

USB Data Disabled
Charging functionality is maintained while preventing unauthorized data transfers, device enumeration, and physical USB-based attacks.

Overlay and Accessibility Protection
By permanently disabling unauthorized overlays and accessibility services, the OS eliminates common vectors for credential theft, clickjacking, and spyware.

No Google Services or FCM
Replaced with proprietary secure socket tunneling. No data touches any of Google's infrastructure, preventing tracking.

Screen Capture Disabled
Screenshots and screen recording are disabled at both the system and ADB level.

Private Keyboard
Spell-check runs locally. None of your keystrokes, typing history, or suggestions are transmitted to any external server.

Duress Password
A secondary password instantly wipes the device and returns it to the activation screen for fast data control.

GSM Calling, MMS and SMS Removed
Standard telephony features are eliminated, protecting against zero-click baseband attacks and common scam vectors. Data only runs over Wi-Fi or SIM data.

Emergency Alerts Removed
Alert exploits have been used to remotely infect devices. This attack surface has been fully removed.

Bluetooth Removed
Bluetooth is removed at the Hardware Abstraction Layer, eliminating one of the most common vectors for proximity-based attacks.

Automatic Restart (BFU Mode)
The device restarts on a set schedule, clearing residual data and placing the phone into Before First Unlock mode for heightened security.

YOUR TOOLS, YOUR CHOICE

VPN Providers

Proton VPN
Mullvad VPN
Orbot: Tor for Android
IPsec VPN

Encrypted Messaging

Session
SimpleX
Threema
WhatsApp
Telegram
FluffyChat
Molly
Zangi
Silent Circle
Signal
Briar
ChatMail

Custom Built Apps

Camera
Gallery
Contacts
Currency Converter
Calculator
Bricknati

Supported Devices

Pixel 6A, Pixel 7A, Pixel 8A, Pixel 9A