PROTELION
GOVERNMENT SOLUTIONS

ArmoredMobile

Comprehensive mobile security

Advantages and Use Cases

Mobile phones have become indispensable tools in every workplace, including the most sensitive environments. However, in government, defense, and corporate settings, standard devices can rapidly become vulnerabilities. Contemporary attacks do not merely target applications or networks — they exploit the phone itself, ranging from software vulnerabilities to physical interference.

That is why Protelion developed ArmoredMobile. It is more than a conventional smartphone — it is a fortified solution engineered for users who cannot tolerate security compromises. Operating on Google Pixel hardware and driven by our proprietary ArmoredOS, it integrates robust encryption, traffic segregation, and rigorous security protocols within a single device. The outcome is a smartphone crafted to safeguard vital communications and information, even in the face of the most sophisticated threats.

- Rock-solid protection of sensitive user data on the system level for the most strict requirements
- ArmoredOS - hardened mobile OS built from scratch leveraging the best of AOSP[1]
- Based on trustworthy Protelion AR VPN technology, securing all data while it is delivered over unprotected networks[2]

ArmoredMobile is a part of a turnkey platform designed for secure multi-service communications and powered by Protelion advanced data protection technology.

1 Google Pixel phones 8 and newer, Google Pixel Tablets are supported
2 Protelion AR VPN infrastructure is required to operate ArmoredMobile

ArmoredMobile Protects Against

1. Malicious Apps

- Built-in kernel-level antivirus
- No Google Mobile Services (GMS)
- No app permissions granted by default
- Only verified and digitally signed apps are allowed
- Kernel-level isolation of microphone, camera, GPS

2. Zero-Day Exploits

- Hardened OS components (malloc, kernel, libc)
- Custom secure browser and office applications
- Regular and timely OS and security updates
- Designed to mitigate threats like NSO's Pegasus, Predator and others

3. Network Traffic Interception

- System-wide Protelion AR VPN protection by design
- Secure communication with Protelion AR Messenger app
- Device lock for particular mobile operators' sims (PLMN ID)
- Using unsecure cellular networks is restricted by default
- No public push notification services are used

4. Mobile Forensics Tools

- Verified Boot with Protelion encryption keys
- Boot loader locked and protected
- No ADB or debug interfaces
- USB port is blocked in rest state
- No diagnostic phone menus

5. Loss and Theft

- AI-based anti-snatch technology
- Protection from brute-force attack on PIN
- Special PIN securely wipes user data
- Remote data wiping and location tracking through MDM

Use Cases

1. Secure Access to Internal Network Resources

- Secure access to internal corporate services such as email, calendar, video conferencing, storage and CI/CD
- All communications secured by Protelion AR VPN
- Data does not leave the corporate network perimeter

2. Restriction of Internet Access

- Only approved websites can be reached through Protelion AR VPN tunnels
- Access to Internet sites may be completely prohibited by administrator

3. Secure Messaging and Calls

- End-to-end encrypted communication through Protelion AR Messenger
- Messaging infrastructure with no push services

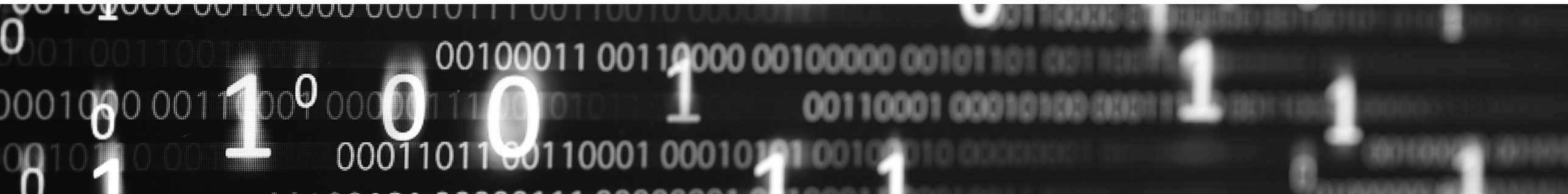
4. Secure External Telephony

- Protected SIP-based calls to cellular and PSTN phones
- Integrated SIP-PBX with Protelion infrastructure

5. Trusted VPN Connectivity

- Protection from ISP-based network interception
- VPN routing limited to approved mobile network operators (MVNOs)
- Intelligent auto-routing to private or public IP addresses of organization

> "ArmoredMobile combines secure hardware, a custom hardened OS, and built-in protections to defend against surveillance, data interception, and advanced mobile threats — all within a strictly controlled environment"

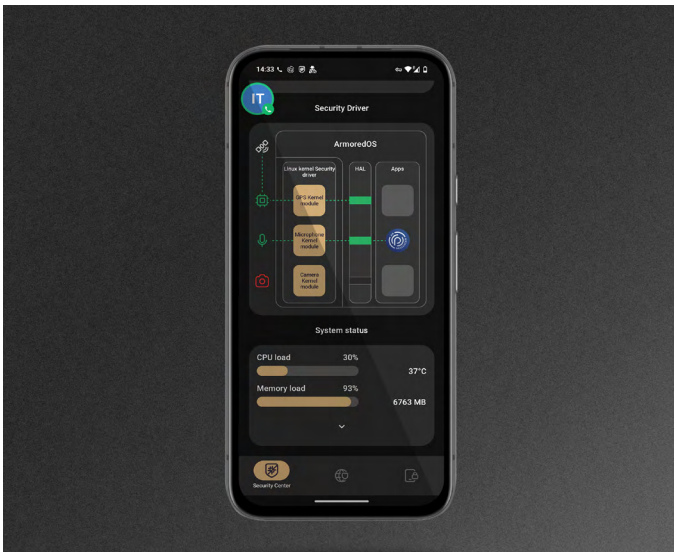


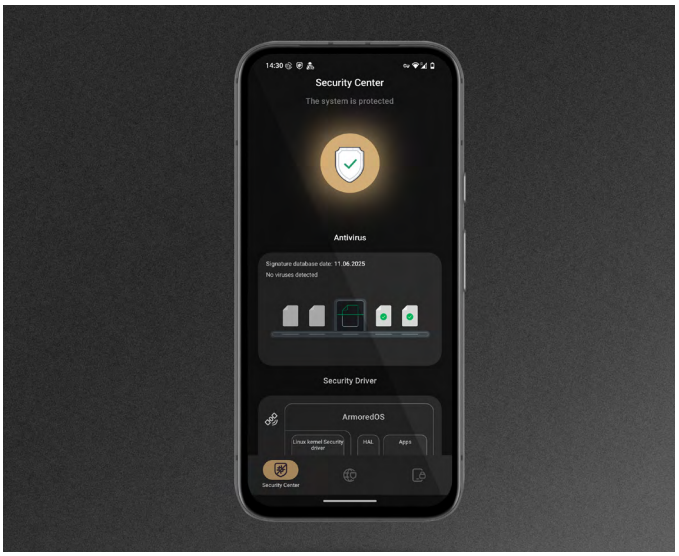
Why ArmoredMobile?

Your mobile device deserves the same protection as your most secure data center.

- Trusted by organizations across the globe
- Designed for defense, intelligence, government, and critical enterprise use
- Developed and supported by Protelion — experts in advanced cybersecurity
- Equipped with built-in, kernel-level antivirus protection
- Includes isolation controls for the microphone, camera, and GPS drivers
- Operates without Google Mobile Services (GMS)
- Comes with applications without tracking libraries

ArmoredMobile: Real security does not compromise.





G.AM.26_v02_LfEng

PROTELION
GOVERNMENT SOLUTIONS

Oberwallstr. 24
D-10117 Berlin,
Germany

+49 30 206 43 66-50

gov@protelion.com

gov.protelion.com