

altOS

Developed to meet the special security requirements of governments



MISSION-FOCUSED SECURE MOBILITY

CIS Mobile protects sensitive government information in addition to workers' privacy and security, delivering a secure mobility platform, management server, and devices. altOS prevents tracking and data exhaust, but retains compatibility with existing apps, enterprise tools, networks, and cloud infrastructure.

As an alternative to consumer-centric smartphones, the altOS platform is designed for the government to have complete control in all aspects of the user's permissions and overall experience.

Our platform benefits from the huge investment that the mobile industry has already made, which allows our customers to stay current with innovation in networks, hardware, OS version updates, apps, mobile enterprise management, and security tools.

EFFECTIVE AGAINST

- Insider mobility threats
- Travel threats
- Data leaks
- Supply chain attacks
- Targeted attacks

ADVANTAGES

altOS **enables the government to control the device**, and not the other way around.

⚙️ 100% management and control of your devices

🔗 Prevent data leakage from untrusted apps and services

📍 Verifiable control over access to device interfaces and location



OPERATING SYSTEM

Android (AOSP) + security enhancements, system services, containers & embedded management

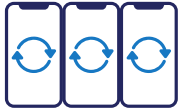


MANAGEMENT SERVER

Application, network, and security management, control and monitoring



OTA UPDATE SERVER



Distribution of updates and security patches to the mobile phones



SERVICES

Custom development for unique government requirements

HOW IT WORKS

The altOS platform is a security-enhanced Android operating system, designed to run on the latest off-the-shelf smartphone hardware. altOS is a complete solution that includes a management server that gives the government complete control over devices, containers and policies and includes a private over-the-air update server.

SOLUTIONS AND CAPABILITIES

- ✓ **Secure Mode:** Dynamically control device capabilities – particularly useful when devices are brought into secure or covert sites.
- ✓ **Multiple Containers:** Allow a single device to have multiple profiles, including personal, enterprise, and mission containers with support for multiple levels of security.
- ✓ **Sensitive Site and Mission Support:** Options to disable modems, cameras, microphones, and location tracking.
- ✓ **Covert and Overseas Usage:** Includes networking, anti-forensics, hidden containers, special duress and other capabilities.
- ✓ **Extensive Partner Ecosystem:** Wide-ranging support for partner add-ons such as secure communication suites, private cellular, etc.