



Secure Mobility for High-Threat Environments

CIS Secure delivers a secure mobility platform designed to protect sensitive government information while safeguarding the privacy and security of the workforce. The altOS platform integrates a hardened mobile operating system, a dedicated management server, and supported devices into a controlled mobile environment.

The platform is engineered to prevent tracking and data exhaust while maintaining compatibility with existing applications, enterprise tools, networks, and cloud infrastructure. This ensures organizations can adopt secure mobility without disrupting current operations.

altOS is purpose-built as an alternative to consumer-centric smartphones. It enables government organizations to maintain full control over user permissions, device behavior, and the overall mobile experience. This level of control is essential for operations conducted in high-threat environments.

At the same time, altOS leverages the broader mobile ecosystem. Customers benefit from ongoing advancements in networks, hardware, operating system updates, applications, enterprise mobility tools, and security technologies without compromising control or security.

The altOS logo, featuring the word 'altOS' in a white, lowercase, sans-serif font. The 'O' is stylized with a white outline and a dark fill, and the 'S' is also in a white, lowercase, sans-serif font. The logo is positioned in the bottom right corner of the image, overlaid on a stack of smartphones.

altOS

Effective Against

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

Operational Advantages

altOS ensures that control resides with the organization, not the device.

- Full management and control across all devices
- Prevention of data leakage from untrusted applications and services
- Verifiable control over access to device interfaces and location

How It Works

altOS is a security-enhanced Android operating system designed to run on modern commercial smartphone hardware. It is delivered as a complete solution that includes a centralized management server and a private over-the-air update capability.

This architecture provides administrators with authoritative control over devices, containers, and policies. It also ensures that updates and security patches are delivered in a secure and timely manner.

Platform Components



Operating System

Android based on AOSP with integrated security enhancements, system services, containerization, and embedded management



Management Server

Centralized control for applications, networks, security policies, monitoring, and administration



OTA Update Server

Secure distribution of updates and patches to mobile devices



Services

Custom development aligned to mission-specific government requirements

Solutions and Capabilities



Secure Mode

Dynamically control device capabilities for use in secure or restricted environments



Secure Containers

Support multiple isolated profiles on a single device, including personal, enterprise, and mission environments with varying security levels



Sensitive Site and Mission Support

Disable modems, cameras, microphones, and location tracking as required



Covert and Overseas Usage

Enable specialized networking, anti-forensics capabilities, hidden containers, and duress features



Extensive Partner Ecosystem

Integrate with secure communications platforms, private cellular solutions, and other mission technologies



Device Management

Centralized administration with rapid QR-based provisioning and streamlined policy enforcement



Secure Supply Chain

Mitigate supply chain risk through customer-controlled builds and update processes



Provisioning

Enable secure onboarding through QR-based enrollment and centralized policy control

Mission Impact

altOS enables secure mobility in environments where threats are persistent and consequences are significant. It provides the control, security, and operational flexibility required to deploy mobile capabilities with confidence while maintaining mission integrity.

About CIS Secure

CIS Secure is a trusted provider of mission-ready communications, technology, and operational services supporting national security missions worldwide. With a workforce composed largely of veterans and cleared professionals, CIS Secure brings decades of operational experience, deep technical expertise, and an unwavering commitment to customer missions.

Our teams operate across enterprise, tactical, and edge environments, delivering solutions that enable secure collaboration, resilient communications, and decision advantage in the most demanding conditions.



cissecure.com
1.703.996.0500

21050 Ashburn Crossing Drive, Suite 145
Ashburn, VA 20147