Mission-Focused Secure Personal Mobility

Mobile phones were developed for consumers, not government. Agencies requiring a higher level of security and privacy turn to altOS to secure mobile devices.

Benefits

100% management and control of your mobile devices

Prevent data leakage from untrusted applications and services

Verifiable control over access to device interfaces and location

Effective against insider mobility threats, travel threats, data leaks, supply chain and other targeted attacks

The altOS Platform

Mobility powers extraordinary capabilities, but also introduces significant new operational risks. As an alternative to consumer-centric smartphones, CIS Secure's altOS platform provides a comprehensive security capability that is missing from consumer mobile operating systems. Custom-built for government, altOS is designed to provide complete control of the user's device, applications and overall experience. The altOS platform is based on our security-enhanced Android operating system, designed to run on approved smartphone hardware to provide optimal protection for mission-critical operations. altOS is a complete solution that includes a management server and an over-the-air update server designed to deliver the policy-based control required by government users.

Operating System

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

Management Server

Application, network and security management including control and monitoring services

OTA Update Server

Distribution of updates and security patches to mobile phones over-the-air or via direct connect

Professional Services

Custom software development for advanced use cases and unique governmnet requirements

sales@cissecure.com

703-996-0500

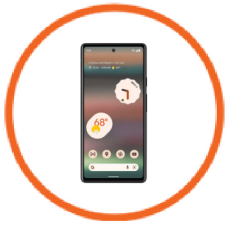
Mission-Focused Secure Personal Mobility

Device Flexibility

CIS Secure's altOS device operating system is device agnostic and can run on a wide variety of mobile device. With the ability to run on any Android based device, altOS allows Agencies and organizations to secure the right device, in the right situation in support of the mission.

Nokia XR21

Getac ZX10 Tablet



Google Pixels

Use Cases

Containers - Deploy multiple secure containers to the same phone, with each container operating as an isolated Android profile, while quickly switching between them with a fingerprint, PIN or passcode. Each container follows unique policy rules defined by the administrator, and each can be managed as a separate device by your preferred mobile device management system. Carry a single phone that allows for personal use as well as strictly controlled government use.

Secure Mode - Strike a balance between security and usability with policy-controlled setting that locks down all radios, cameras, and microphones in the device – preventing their use anywhere near or inside designated facilities. Rather than excluding smartphones from the facility, a device in Secure Mode can be allowed into designated buildings where it can connect to the internal wired network and still function as a useful computing device.

Data Exhaust - Government employees on critical missions must maintain complete control over network usage, location services, modems, and sensors. Unfortunately, most user actions such as turning off Wi-Fi don't actually eliminate the electronic trail left behind by consumer mobile phones. But when altOS turns something off, it's not a mere request to the device OS, which might choose to switch it on. With altOS, "Off Means Off."

Advanced Protection - Ensure protection for users and devices from the most complex types of tracking and attacks. With advanced features like policy-controlled DNS filtering, and cellular network identity (IMEI/IMSI) management and rotation, the altOS platform delivers a robust feature portfolio for protection against nation-state attacks.

CIS Secure Computing, Inc
21050 Ashburn Crossing Drive, Suite 145
Ashburn, VA 20147
(703) 996-0500
www.cissecure.com