SOLUTION BRIEF

altOS Overview

Mobile Sovereignty in Contested Environments: A Secure Architecture for Government Operations

Version 12

February 2026

Contents

Terms and acronyms

Term	Meaning
AOSP	**Android Open-Source Project** – an open-source project, led by Google, who develops and licenses the reference implementation of the Android operating system. AOSP may also refer to the open-source version of the Android operating system, default apps, and build tools and scripts that the AOSP licenses under the Apache open-source license.
Autonomous system	The big networks that make up the Internet. An autonomous system (AS) is a large network or group of networks that has a unified routing policy. Typically, each AS is operating by a single organization, such as an ISP, a technology company, or a government agency,
DNS	**Domain Name System** – the Internet Domain Name System, which is used by devices and hosts to obtain public IP addresses corresponding to domains.
AWS-GC	**AWS GovCloud** – the AWS cloud computing service for sensitive US government applications and data. AWS-GC is exclusively for US government agencies, contractors, and other organizations operating under US regulations, including FedRAMP, ITAR, and DoD SRG.
HTTPS	Hypertext Transfer Protocol Secure – the secure version of HTTP which uses the TLS protocol to encrypt data transmitted between a client and a server and enables the client to authenticate the server via public key cryptography.
Keycloak	An open-source identity and access management product. Keycloak supports protocols, such as OIDC and SAM. Keycloak can integrate with other OIDC servers to support Single Sign-On (SSO) by acting as either an Identity Provider (IdP) or Service Provider (SP).
MTD	**Moving Target Defense** – a proactive defense mechanism that dynamically changes an attack surface, making it more difficult for threat actors to identify and/or target.
OIDC	**OpenID Connect** – an identity authentication protocol built on top of the OAuth 2.0 framework. It allows applications to verify a user's identity. OIDC also provides a secure, interoperable way to implement Single Sign-On (SSO) to multiple servers.
OSINT	**Open-Source Intelligence** – the collection and analysis of data from open sources to produce actionable intelligence.
Reverse Proxy	A reverse proxy is a server that sits in front of one or more web servers and forwards client (e.g. web browser) requests to those web servers. Reverse proxies are typically implemented to help increase security, performance, and reliability.
RTB	**Real-Time Bidding** – RTB auctions are automated ad auctions run by ad exchange companies, such as Google. When a user is viewing a web page or using a mobile app, these companies receive and broadcast data about users, such as geo-location, to RTB auctions around the world for the purpose of generating advertising revenue. .
SOC	**System on a Chip –** a single, integrated circuit that contains the CPU, GPU, modem and memory in modern smartphones. Qualcomm is the largest supplier of smartphone SOCs in the world but other suppliers include Google, Samsung, Huawei (based in China), and MediaTek (based in Taiwan). SOC

	suppliers also provide reference software implementations of firmware (e.g. the device bootloader) that are compatible with their chips and are fundamental to the overall device security.
TLS	**Transport Layer Security** – a cryptographic protocol that provides secure communications over a network. TLS is widely used for email, instant messaging, and web browsing (HTTPS).

Introduction

This whitepaper provides an overview of altOS, a mobile cybersecurity platform developed by CIS Secure to address the security and operational requirements of government mobile users operating in high-threat environments.

High threat environments differ from typical mobile use environments because the users, their mobile devices, and the proprietary servers their devices connect to[1] may be subject to attack by nation-state ("Tier 1"), cartel, or terrorist ("Tier 2") threat actors. These attacks include highly targeted cyber attacks – such as spyware, network intrusion, and other malware, directed at specific individuals, groups of users, devices, or government systems as opposed to cyber attacks by hacktivists or lower-level ("Opportunistic") threat actors that are opportunistic and indiscriminately target devices and servers. These attacks may also include attacks on users – blackmail, coercion, bribery or even kinetic attacks.

In addition to being targeted by Tier 1 and Tier 2 threat actors, altOS users have operational and regulatory requirements that are not addressed by the consumer/enterprise mobile eco-system. These are reflected in the altOS use cases portrayed in figure 1. For example, to enable mobile device use in secure facilities, our customers require the ability to disable sensors and modems on mobile devices with a high assurance level, to prevent the exfiltration of sensitive or classified data. They also require geo-fencing to prevent circumvention of dark mode in the secure facility.

Figure 1. altOS use cases

- Secure communications in the field
- International travel
- Smartphones in secure facilities
- Active OSINT

- Evidence collection
- ISR
- Retransmission device
- Nonattributable use
- Covert use

[1] For example, device management, mobile enterprise app distribution, messaging or tactical awareness servers.

Beyond the altOS threat model and supported use cases, the altOS platform is unique in providing:

- **End-to-end management** – the mobile device software (a customized version of the Android operating system) is managed via a dedicated altOS management server (not a third-party MDM server). This provides the ability to rapidly develop and deploy new features controlled by administrators (CIS Secure can implement compatible capabilities and controls on the device and server rather than relying on a third party to support them),
- **Minimal reliance on users** – security capabilities are managed end-to-end from a central management server, ensuring that controls are configured and governed by qualified administrators rather than individual users (through device-level settings). This aligns with a core platform principle: reducing the burden on users to understand and implement safeguards against sophisticated security threats,
- **Customer control and privacy** – the platform software, comprising a mobile operating system, proxy servers, and a Backend server, can be hosted or deployed by our customers without any reliance or connectivity to CIS Secure (e.g. a device registration server, license server, or OTA update server) to protect customer privacy and provide customer control over their "mobile eco-system",
- **Intuitive user interface** – the user interface is almost identical to the consumer Android user interface to minimize the user learning curve and deliver a modern smartphone user experience consistent with user expectations,
- **Digital anonymity** – Ubiquitous Technical Surveillance (UTS) is the threat of large-scale surveillance and profiling of government employees and network assets made possible by the aggregation and retention of online/protocol and commercial telemetry, and analytics, including AI. UTS is an asymmetric threat because it enables threat actors to deduce identities, relationships, locations/events, and patterns of life at scale at very low cost using easily accessible data, including OSINT. The altOS platform implements countermeasures to preserve the digital anonymity of altOS-enable devices, altOS servers, and ultimately altOS users to mitigate this asymmetric threat, and
- **Supply chain threat mitigation** – supply chain attacks are a concern for customers exposed operating in a high threat environment and CIS Secure works diligently to mitigate these threats. This includes implementing a secure source code repository and development processes for altOS software, eliminating pre-installed apps in device system images, supporting devices that use ARM or Google SOCs and device firmware, and seeking and supporting devices developed and manufactured in allied nations.

A complete solution

altOS is a complete mobile solution providing the security and controls that intelligence, defense, and civilian government agencies need to address the unique threats and operational requirements they face.

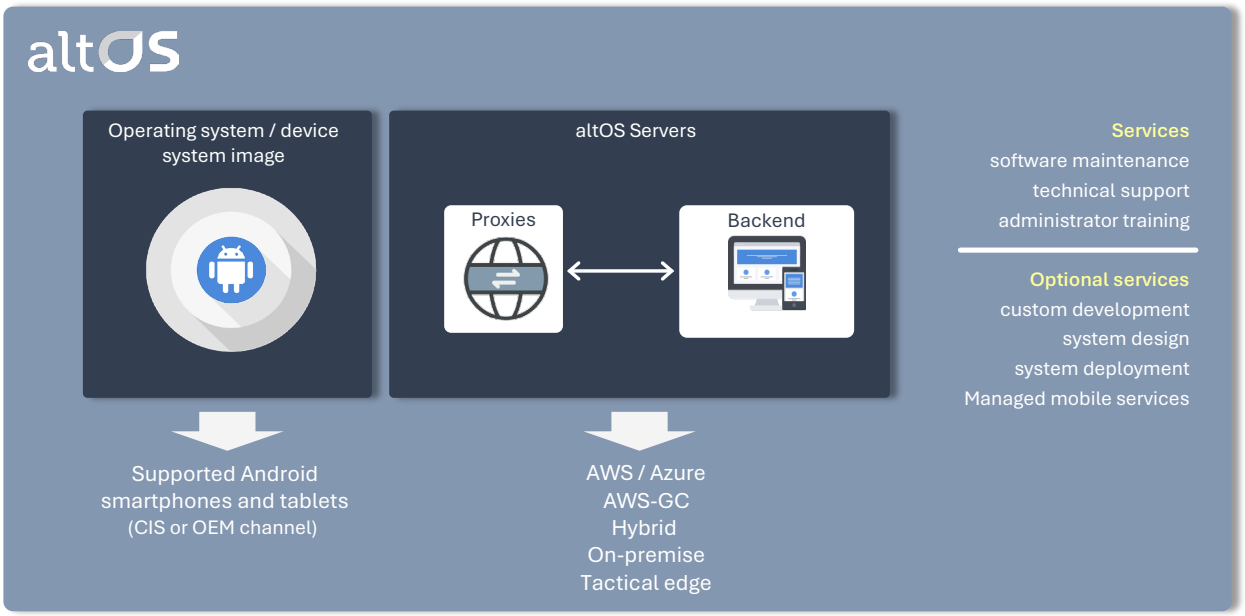
The components of the platform, as well as the deployment platforms and services provided by CIS Secure are shown in Figure 2. The software components of the platform are licensed by CIS Secure, under device software licenses that include software maintenance (bug fixes and updates), technical support, and training.

The altOS operating system is supported on select Android smartphones and tablets that may be sourced from CIS Secure or from device OEM channels. The availability of the devices from CIS Secure or the device OEM channels depends on the business arrangement between CIS Secure and the OEM and certain technical aspects – the ability to unlock and lock the device bootloader.

The altOS servers can be deployed on cloud computing platforms, including AWS, Azure, and AWS-GC. They can also be deployed in a customer data center or in a hybrid configuration (e.g. with the Proxy servers deployed in the public cloud and the Backend server deployed in a customer data center.

CIS Secure also offers customers the following services: customer feature development, system design, system installation, and managed mobile services where the platform is deployed, maintained and operated by CIS Secure staff.

Figure 2. altOS solutions



System

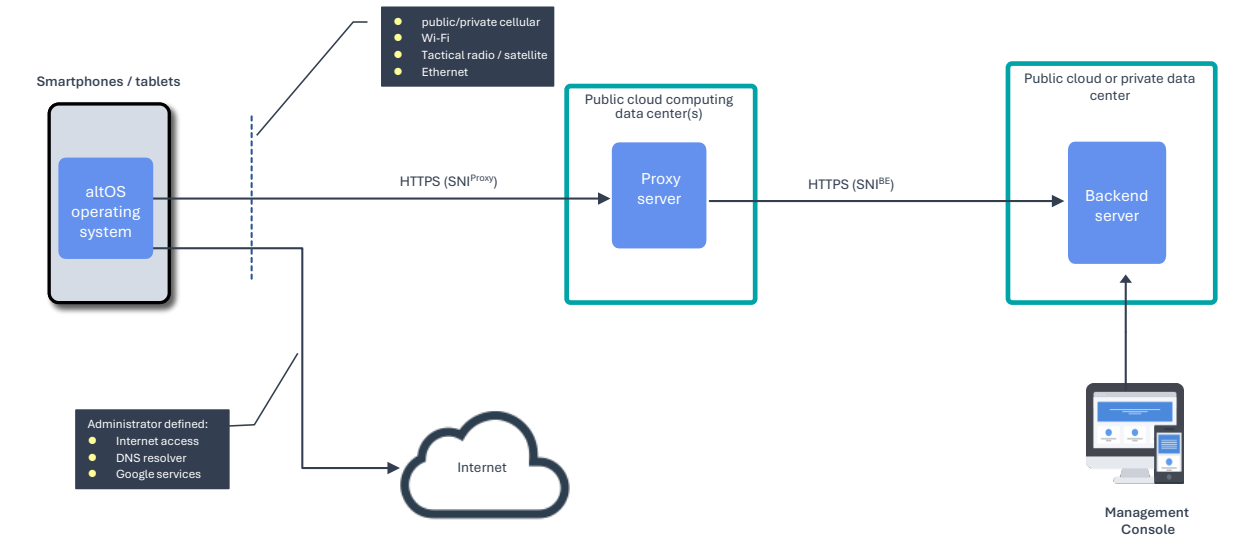
Figure 2 provides a system diagram for the altOS platform as it would typically be deployed. Devices connect to the Backend server via Proxy servers that are typically deployed in the public cloud computing data centers.

The primary software components of the system are:

- **altOS operating system** – the operating system is derived from AOSP software. This open-source software is modified, compiled, tested, and supported by CIS Secure and replaces the consumer version of the Android OS on supported third-party Android smartphones and tablets. The operating system is signed by CIS Secure, and the integrity is verified during the device boot process against a CIS Secure public key cert installed on the device,
- **Proxy servers** – the Proxy servers act as reverse proxies relaying HTTPS traffic from devices to the Backend server. Multiple Proxies can be associated with the Backend server and they can individually be added or deleted at any time by an administrator. Proxy servers: (1) isolate the Backend from the Internet, (2) enable us to obfuscate device traffic to the Backend server, (3) enable a moving target defense (MTD), and (4) isolate (e.g. prevent an adversary from associating) different groups of devices from one another, and
- **Backend server** – this is comprised of several services and micro-services that support: device management, cloud messaging, device and administrator logging, device provisioning, device certificate generation, and device OTA (Over-the-Air) updates. Devices are enrolled with the Backend server via invitations (typically QR codes) that can be user-locked and distributed out-of-band to users.

Devices connect to the Proxy server assigned in administrator controlled “Proxy Profiles” that can be customized for every device or group of devices managed by an administrator. Device connections to

Figure 3. System diagram



Proxy servers can be via public or private cellular, Wi-Fi, tactical radio, satellite, or Ethernet (via a USB to Ethernet adapter) and the connection interval can be customized by the administrator to be persistent (an open web socket), intermittent, or user initiated.

Connectivity to the Internet is optional as is connectivity to public services such as DNS – these are controlled by the adminstrator and can be changed dynamically for devices in the field. Additionally, the platform does not require connectivity to third-party services, such as the Google app store or Google maps, although these may be enabled to support different use cases.

Administrators access the Backend server via a web-based management console to:

(1) configure the system (e.g. Proxy servers or storage for policies and private apps),

(2) add or delete administrators and manage administrator privileges,

(3) perform device configuration and management functions, and

(4) manage device OTA updates.

Administrator authentication uses Keycloak and 2FA is supported, as well as single sign-on (SSO) to third-party servers that support OIDC.

Containers

A unique capability of the altOS platform is the ability to support and manage multiple containers while supporting intuitive and secure user access to those containers.

Figure 3 shows a device configured with three containers. Each device can support multiple containers where each container is a separate Android user space and has different apps, encrypted file systems, app sources, contacts, accounts, phone profiles, security policies, wallpapers, etc. Containers can be provisioned during device enrollment with the Backend server, or they can be pushed to devices by administrators after enrollment.

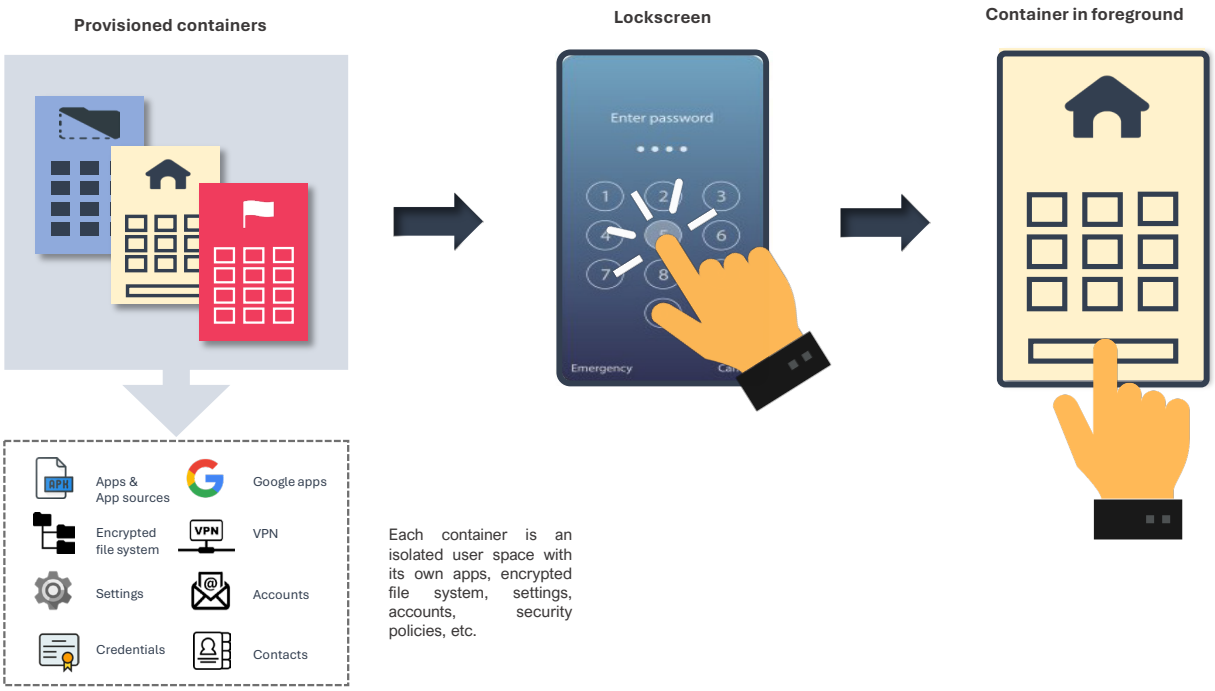
Users unlock and access containers by entering the PIN, password, or fingerprint associated with the container as shown in Figure 3. Once the correct PIN, password, or fingerprint is entered, the container is moved to “foreground” on the device display screen, meaning the user can interact with the container and apps in the container via the device display.

Containers can be in one of three states, depending on the actions the user takes concerning unlocking and accessing different containers, and subject to administrator policy settings. These states are:

- **Locked** – the container file system is encrypted and inaccessible. Apps are inactive (unless they have been written specifically to use Device Encrypted memory) and the user has entered the password or PIN for the primary container.
- **Unlocked in foreground** – the user has entered the corresponding credential, the container (wallpaper, apps, notifications) is visible, and the user can interact with the container and objects in it via the device touchscreen. Additionally, the container file system is unlocked and apps can access sensors, and RF modems as allowed by the device and container policy settings, and
- **Unlocked in background** – the user has entered the container access credential and then switched containers to bring another container to the foreground. In this state, access to system services may be limited by the operating system (e.g., location data) or by some administrator settings (e.g., exclusive network access will prevent containers in the background from accessing the network if applied to the foreground container).

While containers may be provisioned for personal use (usually the primary container), the administrator has the ability to control, update, and delete all containers on the device and retains control of critical policy settings. For example, the administrator may grant access to Google Play in a personal container but can define an app blacklist that is applied at the device level. This could be used, for example, to blacklist an app that is found to be harmful (note that a blacklisted app and any associated user data will also be removed from the phone if it was installed prior to being blacklisted).

Figure 4. altOS container concepts

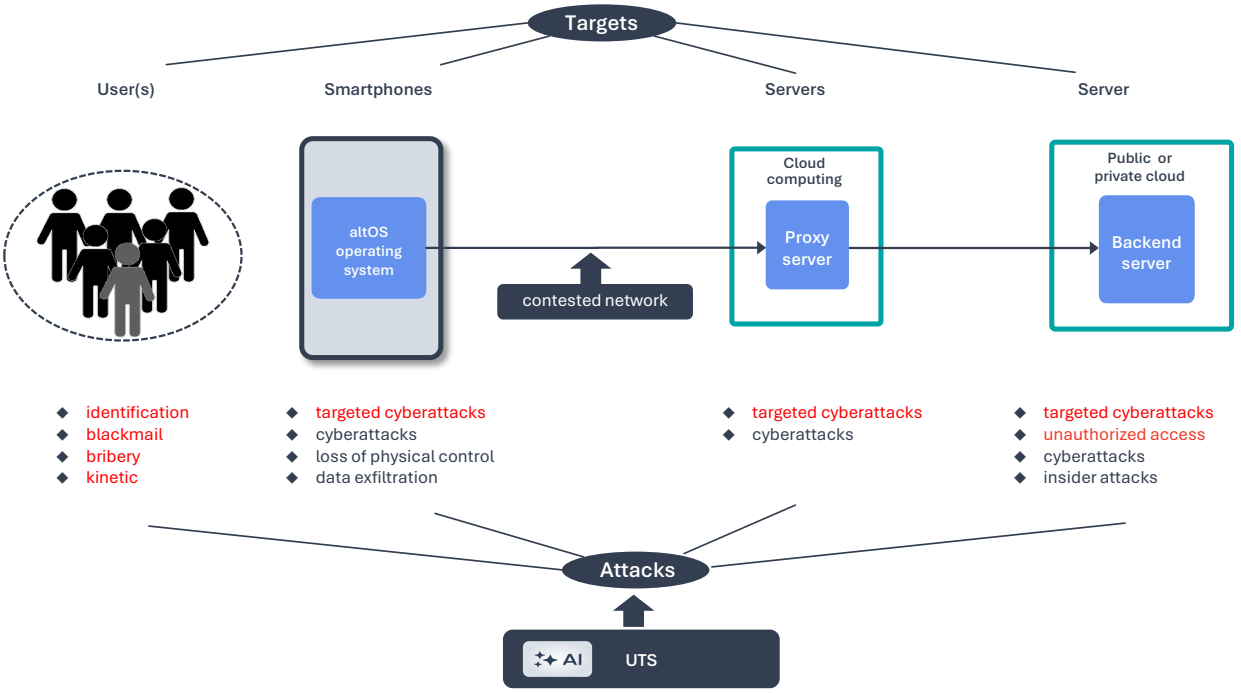


Threat model

The objective of a threat model is to identify potential threats, the objectives of threat actors, and defenses against the anticipated attacks. This section discusses the altOS threat model and some of the assumptions that are unique to it.

Mobile device threat models generally contemplate lost or stolen devices and opportunistic cyber attacks – ransomware, malware, phishing attacks – by low-level threat actors with limited resources. The objective of these types of cyber attacks may be profit, reputational damage, bragging rights, or ideology.

Figure 5. Threat model



The altOS threat model is illustrated in Figure 5. The targets include altOS-enabled devices, altOS servers, and device users. The threat model makes the following assumptions:

- **Contested network** – device connect to Proxy servers over contested networks[2]. In the extreme case, a tier 1 threat actor is assumed to have the capabilities of a sophisticated national censor (e.g. the ability to monitor, filter or inject traffic, and monitor, block, or inject responses to DNS queries responses) across several Autonomous Systems. These capabilities may be used to identify and profile altOS servers and devices connecting to those servers and make associations between those devices and their users (e.g. the users of devices connecting to a common private server are all government employees and share a common mission).
- **UTS** – tier 1 and tier 2 threat actors actively use UTS to identify and profile government mobile devices and other internet-connected assets on a large scale. By aggregating and analyzing this data, they can infer identities, relationships, locations, and behavioral patterns. This intelligence

[2] The connection from the Proxies to the Backend are TLS encrypted, at a minimum, but the Backend server should not be publicly routable – e.g. it has only a private IP address or a public IP address that accepts traffic from Proxy and administrator IP addresses.

enables targeted cyber operations against altOS devices and servers, and also facilitates real-world targeting of device users and missions,

- **Device inspection/analysis** – a user may have to relinquish physical control of his mobile device temporarily (e.g. to enter a building or attend a meeting) or may be forced to surrender a device to an official for cursory inspection (e.g., at a border crossing). In the later case, inspection of the unlocked device may reveal sensitive apps and data on the device. This, in turn, may lead to further questions of the user's intentions, role, or activities, and/or forensic extraction of data from a device, and
- **Other threats** – in addition to the targeted cyber attacks by sophisticated threat actors, altOS-enabled devices and altOS servers are exposed to regular cyber attacks by lower-level threat actors. For example, an altOS device user may still receive phishing and ransomware attacks on their devices. While these are not the worst case, the threat model must still take these into account.

The altOS platform provides multiple layers of defenses with "outer layer" defense to prevent or mitigate UTS directed at altOS enabled devices and the altOS servers and "inner layers" of defense to prevent or mitigate the cyberattack. These include defenses to prevent RTB data exhaust from devices, and specific server deployment guidelines and scripts to minimize OSINT that normally results form deploying and having devices connect to an internet-connected host (e.g. DNS data, CT Logs, Zone files)

For a more detailed discussion of the altOS threat model and defensive capabilities, please see the ***altOS Threat Model*** whitepaper which is available from CIS Secure on request.

Summary

altOS is a platform purpose-built for government mobile users operating in high-threat, high-consequence environments where conventional enterprise and consumer mobility solutions are insufficient. Unlike consumer-based mobile devices and enterprise platforms that primarily address opportunistic threats and device loss, altOS is engineered around a threat model that assumes sophisticated Tier 1 and Tier 2 adversaries, contested networks, large-scale surveillance, and the potential for both cyber and real-world targeting of device users.

The platform delivers a tightly integrated, end-to-end solution spanning a hardened mobile operating system, Proxy infrastructure, and a dedicated Backend server, under unified administrative control. This architecture enables rapid capability development, minimizes dependence on third-party services, and minimizes reliance on end-users to make complex security decisions.

By combining layered cyber defenses, moving target techniques, digital anonymity countermeasures, and supply chain risk mitigation, altOS addresses both outer-layer surveillance threats (including UTS and OSINT exploitation) and inner-layer device and server compromise attempts.

Equally important, altOS balances security with operational usability. Its intuitive Android-based interface, flexible deployment models (cloud, hybrid, or on-premises), containerized user environments, and administrator-defined policy controls support diverse mission requirements without compromising assurance. The result is a sovereign, privacy-preserving mobile ecosystem that government customers can host, manage, and evolve independently.

In environments where mobile devices represent both a mission enabler and a high-value attack surface, altOS provides a comprehensive, defensible, and controllable platform aligned to the realities of modern state-level threat actors and regulatory demands.