COMMUNITAKE

CommuniTake Technologies IntactPhone

Comparison Chart

Intact Mobile Security

The Intact Mobile Security Platform from CommuniTake, delivers a game-changing unified platform for mobile security and productivity.

IntactPhone™
Specially manufactured fully trusted devices with built-in security - both standard and rugged

IntactOS
Purpose-built private by design and security-rich OS with no Google services

IntactCC
Fused central governance with unique security measures to control, track, monitor and alert against cyber threats

IntactDialog
Encrypted voice and messaging on any Android™ or iOS device

IntactApps
Diverse powerful suite of security tools built into the device, designed for better security from the start

IntactCare
Remote control technology and self-troubleshooting app enable a productivity-first approach

	CommuniTake	GSMK	Sikur	Blackberry	Kaymera	Atos	Secure Group	Samsung	Silent Circle	Bittium
Company	CommuniTake	GSMK	Sikur	Blackberry	Kaymera	Atos	Secure Group	Samsung	Silent Circle	Bittium
Product name	IntactPhone	Cryptophone	Granite Phone	Motion	Kaymera	Hoox	Secure Phone	KNOX	BlackPhone	Tough Mobile
Device Model	Proprietary	Samsung S5	Proprietary	Motion	Google Pixel	K3; K30	HTC M8; Nexus5	Various	BlackPhone 2	Proprietary
PROTECTION - DEVICE										
Trusted hardware	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓
Secure bootloader	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data self-destruct on unauthorized boot access	✓	✗	✗	✗	✓	✗	✓	✓	✗	✓
Trusted official drivers	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓
Enhanced storage protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PROTECTION – OPERATING SYSTEM										
Custom-built OS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Internal integrity verification	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Stand-alone enforcement operation	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Obfuscation layer on top of resource APIs	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
PROTECTION - COMMUNICATIONS										
Encrypted voice calls	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Midway encrypted midway calls	✓	✗	✗	✓	✓	✗	✓	✗	✓	✗
Anonymous phonebook	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗
Anti-eavesdropping restrictions (mic; con calls)	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗
Encrypted messages	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Encrypted in-message attachments	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
Hashing in-message links	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Controlling in-message content sharing	✓	✗	✗	✓	✓	✓	✓	✗	✓	✗
Encrypted emails	✗	✗	✓	✓	✗	✗	✓	✗	✗	✓

	CommuniTake	GSMK	Sikur	Blackberry	Kaymera	Atos	Secure Group	Samsung	Silent Circle	Bittium
Company	CommuniTake	GSMK	Sikur	Blackberry	Kaymera	Atos	Secure Group	Samsung	Silent Circle	Bittium
Product name	IntactPhone	Cryptophone	Granite Phone	Motion	Kaymera	Hoox	Secure Phone	KNOX	BlackPhone	Tough Mobile
Device Model	Proprietary	Samsung S5	Proprietary	Motion	Google Pixel	K3; K30	HTC M8; Nexus5	Various	BlackPhone 2	Proprietary
PROTECTION - APPLICATIONS										
Internal app store	✓	✗	✗	✓	✓	✓	✓	✗	✗	✓
Apps risk scoring	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗
No Google Play store	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗
Proprietary apps permissions management	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓
Built-in malware protection	✓	✗	✗	✓	✗	✗	✓	✗	✗	✗
Apps' anomalies scanning	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓
Blocking apps' access to malicious sites	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗
THREATS PREVENTION										
IMSI Catcher detection	✓	✓	✗	✗	✓	✗	✓	✗	✗	✗
Man-in-the-Middle attacks detection	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓
Blocking forensic equipment action	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗
Complete Google services replacement	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗
Fused controls in the OS eliminating careless use	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗
Panic button blocking access to device data	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓
Targeting obfuscation via persistent VPN	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓
Utilizing only complete known code	✓	✗	✗	✓	✗	✗	✗	✓	✓	✓
PERFORMANCE ASSURANCE										
Built-in complete remote control technology	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Self-troubleshooting app	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Security assurance app	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗

	CommuniTake	GSMK	Sikur	Blackberry	Kaymera	Atos	Secure Group	Samsung	Silent Circle	Bittium
Company	CommuniTake	GSMK	Sikur	Blackberry	Kaymera	Atos	Secure Group	Samsung	Silent Circle	Bittium
Product name	IntactPhone	Cryptophone	Granite Phone	Motion	Kaymera	Hoox	Secure Phone	KNOX	BlackPhone	Tough Mobile
Device Model	Proprietary	Samsung S5	Proprietary	Motion	Google Pixel	K3; K30	HTC M8; Nexus5	Various	BlackPhone 2	Proprietary
CENTRAL CONTROLS										
Policies: password; backup; use restrictions	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓
Granular apps management	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓
Kiosk mode and location/time based policies	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗
Browsing control	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗
Files container	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
Usage monitoring and statistics	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Policies enforcement and alerts management	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗
Remote device recovery (lock; locate; wipe)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
UNIQUE FEATURES										
Built-in push-to-talk communication	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Self-destruct messages	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗
Any device enterprise mobility management	✓	✗	✗	✓	✗	✗	✗	✓	✓	✗
Stand-alone secure communications	✓	✗	✗	✓	✓	✗	✓	✗	✓	✗
Communications archiving	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓
DEPLOYMENT										
Purpose-built devices (rugged etc.)	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
Locked-down virtual private enterprise network	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓
Supporting both BYOD and COPE devices	✓	✗	✗	✓	✓	✗	✗	✓	✓	✗
Supporting both Android & iOS devices (app)	✓	✗	✓	✓	✓	✗	✗	✓	✓	✗
On-premises and cloud delivery methods	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

The Importance of A Trusted Operating System

Bootloader

The bootloader is a proprietary closed source code received from the chipset manufacturer.

Without an official source code, a solution provider is forced to hack the mobile device and the bootloader in order to load its operating system.

This means that this bootloader is actually open or hackable and the provider has no way to eliminate this security breach.

Drivers, proprietary binaries, code changes and configurations

Without the official source code and the configurations from the manufacturer, a solution provider is required to hack and to reverse-engineer the drivers, proprietary binaries, code changes and configurations from an off-the-shelf device.

In addition, the solution provider has no way to know whether he is devising it correctly and remaining true to the original code.

(Analogy: it is like constructing a car by other car parts).

No Google Services: CommuniTake has replaced all Google services. This provides:*

1. Inability for Google to track the device location.
2. Inability for Google to access on-device information.
3. Protecting against Google Play store hazards of installing malicious apps and apps with risky permissions.
4. Defending against Google Play network traffic and its meta data which can be used to gather information about the device via man-in-the-middle techniques.

Conclusions:

1. Transformed commercial devices will always consist 3rd party code and cannot be regarded as secure.
2. Converting a commercial device to a secured device introduces a significant security breach.
3. Providers who are disconnected from the manufacturers, have no way to receive security or bug fixes.
4. Hacking and loading a proprietary OS on a commercial device voids the original warranty.

* CommuniTake does enable a hybrid solution in special cases for prospects that wish to have Google services with no Google Play store.

Why IntactPhone

HOLISTIC APPROACH

Holistic, multilayer approach: fully trusted device & OS, encrypted communications, fused governance, threat detection, security-enhanced utilities, productivity tool-set.

SECURE TRUSTED FRAMEWORKS

Purpose-built frameworks, based on official full OS code received from the manufacturer, for preventing threats and minimizing the attack surface:

- Trusted Kernel, drivers and bootloader;
- No Google services; Global secured app store;
- Internal resources APIs layer; Proprietary push notifications.

This method assures that the OS enhancements are clear, certain, valid and lasting.

EAVESDROPPING PROTECTION

In-depth eavesdropping protection via encrypted communications and internal ROM based resources control.

THREAT DETECTION

Advanced behavior analysis for detecting anomalies across connectivity and apps.

BUILT-IN CONTROLS & PRODUCTIVITY

Fused defense controls with complete remote control & self-troubleshooting app.

LOCKED-DOWN NETWORK

Private enterprise network (on premises deployment).

DIVERSE DEVICES

Standard, custom-built, and rugged devices.

FLEXIBLE DELIVERY METHODS

COPE & BYOD; Android & iOS; app level and hardware level; cloud & on premises deployment.