SafeCase™ Cheat Sheet

What is the SafeCase?

The Privoro SafeCase is a first-of-its-kind ExoComputer for mobile devices, enabling unique data protections and high-security services that would be impossible to deliver on the smartphone itself.

What is an ExoComputer?

At a basic level, an ExoComputer is a secondary computing device providing trusted services independently of the associated mobile device. This two-system approach enables organizations to leverage the commercial mobile device for mainstream applications like email and web browsing while offloading critical services and protections like sensor control, digital key storage and identity to the ExoComputer. The ExoComputer brings its own processing, storage, communication and sensing capabilities, tied together in a specialized, high-security architecture designed to deliver high-trust features, not to support millions of potential apps.

Why is the SafeCase necessary?

Unfortunately, even the most advanced mobile security solutions on the market, whether integrated into the operating system or available as third-party apps, can’t overcome the limitations of the smartphone’s vulnerable architecture. Motivated attackers can take control of a smartphone and then siphon away data, including the audio and visual information in the vicinity of the device. Given the security risks of relying on an untrusted, commercial smartphone – even the most locked-down hardware within it – the SafeCase has been designed to work with, but be functionally independent of, a user’s smartphone.

PRIVORO®

SafeCase Cheat Sheet

What makes the SafeCase more secure than a commercial smartphone?

Commercial smartphones support any of millions of third-party apps, which run on the same application processor or system on a chip (SoC) where security-critical code and the device's operating system (OS) run. Depending on the vendor, these processors also store cryptographic keys or are tightly connected to coprocessors that do so. The openness of these platforms — which is needed to enable users to both conduct business and play games on the same processor — has been repeatedly demonstrated to allow application, OS and chip-based vulnerabilities to be exploited, leaking sensitive data. By comparison, the high-security architecture of the SafeCase, anchored on an independent hardware root of trust, limits interaction to only approved, vetted and signed software, in effect eliminating third-party code, preventing core system software from being exploited and mitigating the use of current and future chip-based vulnerabilities. The SafeCase architecture is also designed to mitigate direct memory access and other attacks from connected devices and processors/components.

Is the SafeCase compatible with every smartphone model?

The SafeCase is currently only compatible with the iPhone 7/8. Future editions of the SafeCase will be compatible with additional iPhone and Android models. The core electronics and firmware of the SafeCase have been designed to be directly transferrable to future editions, with changes required only to the plastics to accommodate the smartphone's shape and camera/microphone locations.

How does the SafeCase integrate into an organization's infrastructure?

The SafeCase includes its own secure, cloud-based management infrastructure. From the Privoro Portal, an administrator can create custom policies around SafeCase usage, monitor SafeCase activity, push out SafeCase firmware updates and perform other management tasks. Privoro's policy engine monitoring and reporting can be integrated with an organization's existing unified endpoint management (UEM) or mobile device management (MDM) solution, enabling administrators to take policy enforcement actions directly on the user's mobile device.

What does the SafeCase not do?

The SafeCase does not currently do any of the following:

- Stop the smartphone from being hacked
- Protect against attacks via RF signals
- Make encrypted phone calls
- Charge the smartphone

SafeCase Cheat Sheet

UNDERSTANDING SAFECASE'S MOBILE HARDENING FEATURE

What is the mobile hardening feature?

Mobile hardening leverages anti-surveillance features built into the SafeCase to mitigate the risks of mobile eavesdropping and spying. Physical protections prevent audio and visual data in the vicinity of the phone from being swept up by third parties who have hijacked the mobile device's cameras and microphones. Optional policy enforcement features prevent illicit camera/microphone access from occurring within locations of concern.

How does mobile hardening work?

The SafeCase uses a proprietary audio masking technique that floods each of the smartphone's microphones with randomized noise specific to that microphone. This technique ensures that a captured conversation's content (the words spoken) and the context (accents, tones, number of participants, etc.) are unidentifiable with even the most sensitive audio forensic equipment. In addition, a physical barrier prevents image capture by blocking each of the smartphone's cameras.

Can users control the mobile hardening protections?

Users may disengage mobile hardening protections by either raising the hood of the SafeCase (to use the smartphone's cameras and microphones) or by pressing and holding the front button (to use just the microphones) when needing to make phone calls, capture audio/images or make requests to the phone's virtual assistant.

How does policy enforcement work?

Through the Privoro Portal, administrators can create policies prohibiting camera/microphone usage within geofenced locations or in designated circumstances and then monitor policy violations based on SafeCase activity. Optional MDM integration enables automatic policy enforcement directly on users' smartphones, providing the ability to lock devices or delete certain apps.

Does the user maintain full use of their smartphone when mobile hardening protections are engaged?

Most phone functions – like email, text messaging, internet browsing and app usage – are available with the protections engaged. To access the phone's microphones or cameras, protections must be disengaged.

How does the user know that mobile hardening protections are working?

The easiest way for the user to verify that both audio and video protections are working is to record a short video while the hood is both raised and lowered. When the recording is played back, the portion captured when the hood was lowered should include a black image output and scrambled audio. The Privoro app also provides a visual indication that audio protections are working as intended for the various smartphone microphones.

PRIVORO®