SafeCase™ FAQs

What is SafeCase?

The first of its kind, Privoro SafeCase is a smartphone-coupled secondary compute device (or ExoComputer) enabling unique data protections and high-security services that would be impossible to deliver within the smartphone ecosystem. SafeCase's integrated anti-surveillance features provide unprecedented defense against illicit camera and microphone usage while allowing full use of most smartphone features.

What is a "smartphone-coupled ExoComputer"?

At a basic level, a smartphone-coupled ExoComputer is a compute device wrapped around a smartphone, providing trusted services independent of the associated device. This two-system approach enables organizations to leverage the commercial mobile device for mainstream applications like email and internet access while offloading critical services and protections like sensor control, digital key storage and identity to the secondary compute device, with its own stand-alone hardware root of trust. The secondary device brings its own processing, storage, communication and sensing capabilities.

Why is SafeCase necessary?

Smartphone architecture is intrinsically vulnerable. However advanced, no software-only mobile security solution can overcome the limitations of that architecture. Motivated attackers can take control of a smartphone and siphon away data, including the audio and visual information in the vicinity of the device. Given the security risks of relying on untrusted, commercial smartphones, SafeCase has been designed to work with but remain functionally independent of a user's mobile device.

PRIVORO®

SafeCase FAQs

What makes SafeCase more secure than a commercial smartphone?

Commercial smartphones support millions of third-party apps, which run on the same application processor or system on a chip as security-critical code and the device's operating system (OS). Depending on the vendor, these processors also store cryptographic keys or are tightly connected to coprocessors that do the same. The openness of these platforms — which is needed to enable users to both conduct business and play games on the same processor — has repeatedly been shown to allow application, OS, and chip-based vulnerabilities to be exploited, leaking sensitive data. By comparison, the high-security architecture of 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 attacks. The SafeCase architecture is also designed to mitigate direct memory access and other attacks from connected devices and processors/components.

Does the SafeCase device protect my smartphone from malware attacks?

SafeCase operates independently of the smartphone and does not defend against malware. SafeCase mitigates the capture of audio and video in the vicinity of the protected smartphone from being swept up by unauthorized third parties – even if it has been compromised.

What smartphones have compatible SafeCase models?

SafeCase is currently available for the iPhone 7, 8, and SE. Coming in Q2 of 2022, SafeCase will be available for iPhone 12 and Galaxy S21.

While using SafeCase can I access the functions of my smartphone?

Most phone functions are still available while using SafeCase, including texting, app usage, email, web browsing, etc. Functions that require the use of cameras and microphones require the disablement of SafeCase audio and camera protections.

Does SafeCase have its own power source?

Yes. SafeCase has an independent battery that is designed to last up to 18-20 hours on a single charge, depending on the model.

To protect your smartphone against attacks via RF signals (wireless attacks), see Privoro Vault™.

PRIVORO®