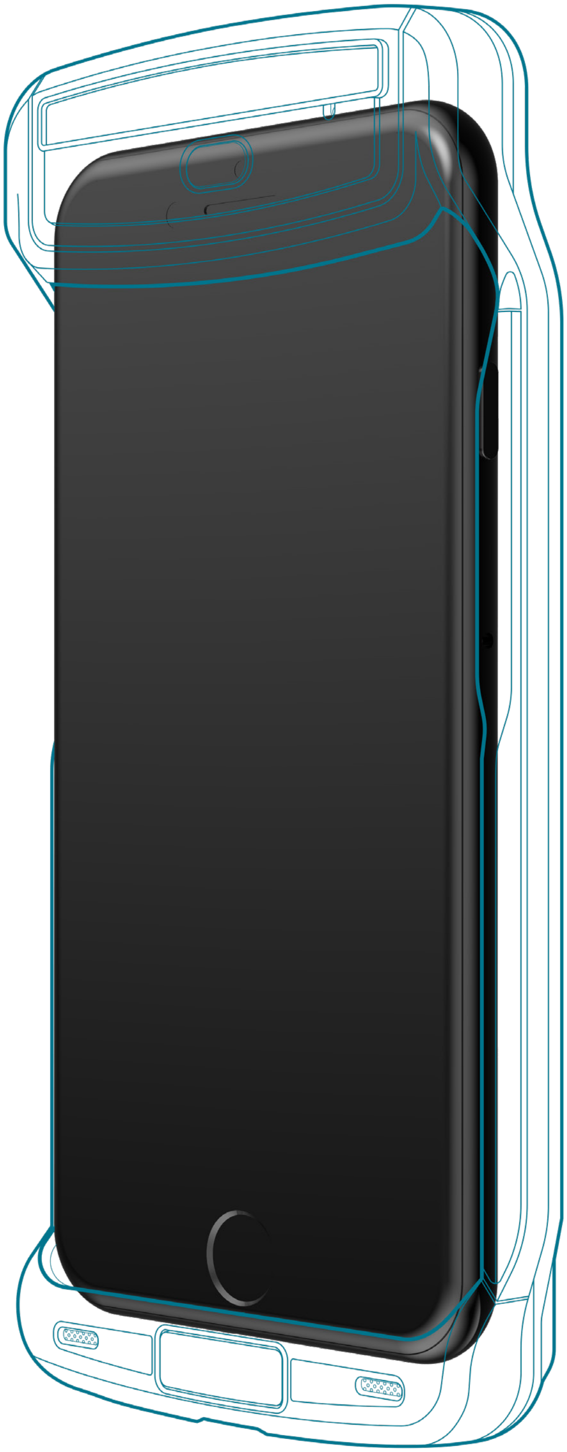
SafeCase™: ExoComputer

Introducing true hardware separation at the mobile edge.

The SafeCase is the first device to bring trusted, external computing to an organization's untrusted, commercial mobile devices.

At a basic level, an ExoComputer is a secondary computing device providing trusted services independently of the protected 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.



PRIVORO®

SafeCase: ExoComputer

Hardware root of trust

A unique key pair is generated, bound and exclusively contained within a single secure chip.

Built and provisioned within a US-based, ITAR-compliant facility utilizing embedded supply-chain protections.

Trusted execution environment

Secure boot, updates, firmware and code signing.

Tamper protection

Physically sealed and tamper-resistant.

Protections against side-channel attacks.

Isolated components

Closed-system architecture.

The SafeCase's processor is used exclusively for running authenticated firmware.

Motion sensors

A nine-axis inertial measurement unit (IMU) – which includes a three-axis gyroscope, accelerometer and magnetometer.

Wireless data technologies

WiFi, Bluetooth and NFC – enable communications with local devices, including the paired smartphone.

Digital signal processor

For audio quality, voice masking and audio path control.

GPS module

Enables location tracking for policy management purposes.

Some questions people ask:

How is an ExoComputer different from a standard mobile device?

Simply put, an ExoComputer is built for security first. Unlike a smartphone or tablet, an ExoComputer operates within a closed, high-security system that extends from the device's hardware to its cloud. And without a screen, cellular modem or commercially available OS, the ExoComputer minimizes opportunities for attack.

Why is an ExoComputer necessary?

Users within organizations dealing with high-value information and assets are relying more and more on their commercial mobile devices to get their jobs done. And yet, at the end of the day these devices are still geared toward consumers. Even with attempts to isolate security-critical functionality at the hardware level within separate execution environments and coprocessors, proximity to third-party code puts an organization's most important data at risk. The specter of chip-based exploits exacerbates this situation.

How does an ExoComputer work?

An ExoComputer conveniently wraps around a mobile device and pairs with it over Bluetooth. However, the ExoComputer doesn't trust the paired device and as such is functionally independent of it – the ExoComputer merely leverages the paired device's capacity for user interface (to keep the user informed) and its data channel (to communicate with the cloud via an encrypted inner tunnel). From the cloud, high-security services provided by the ExoComputer platform can be managed.