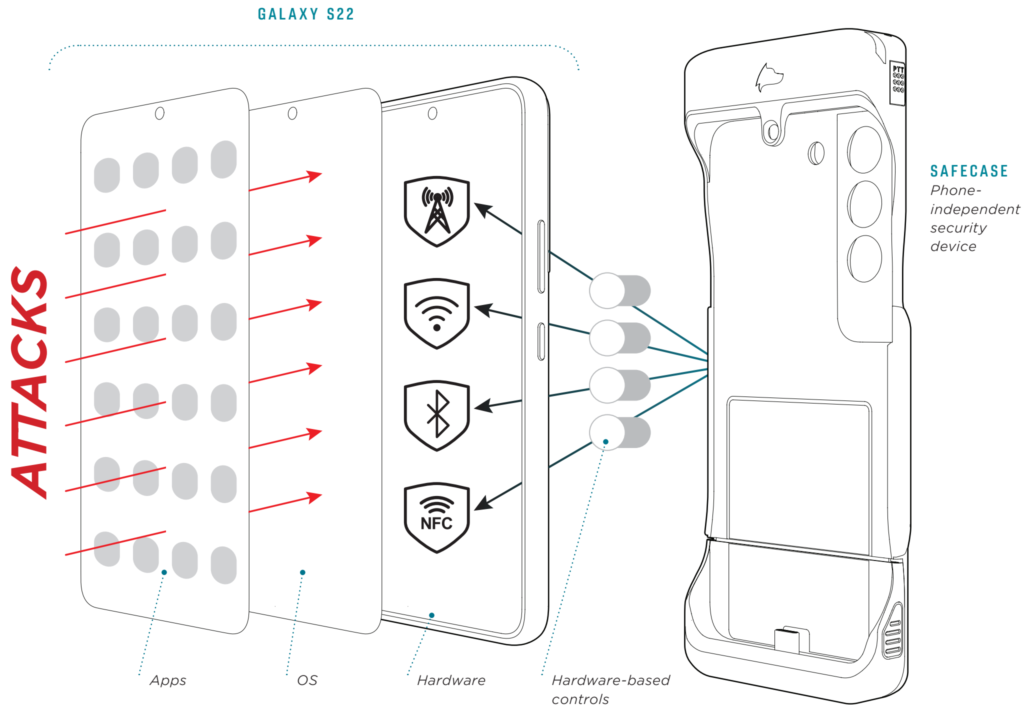
Transform smartphones from security outcasts into building blocks for secure computing.

Introducing the marriage of two independent, hardware-based fail-safes.

The combination of a Samsung Galaxy phone and a Privoro SafeCase security device means that even in the event of an advanced mobile attack, an organization's most important secrets are kept safe. Security-conscious organizations within the Federal government can stop neglecting employees' mobile devices and instead lean on them as the basis for a powerful new model for computing.



SAMSUNG | PRIVORO®

CURRENT STATE

Acceptance of mobile risks

Whether government-furnished or personally owned, mobile devices are typically excluded from sensitive areas and missions and largely ignored the rest of the time.

- Encourages risk-taking from personnel needing to use their phones to get their jobs done or keep in touch with family and friends
- Spyware can typically gather intel through hijacked cameras, microphones and cellular radio and potentially capture passwords for accessing enterprise systems

Desk-centric work model

In an enterprise setting, phones are typically restricted from secure spaces and are kept in lockboxes throughout the day.

- Inability to respond to messages on the go
- Overreliance on pen and paper in meetings
- Challenges around recruiting, retention and morale

Multiple endpoints per user

The IT team must provision and monitor a variety of endpoints – desktops, laptops, tablets and smartphones – for multiple domains and classification levels.

- Complex IT environment
- High capital expenditures
- Maintenance of legacy wired infrastructure

FUTURE STATE

24/7 OPSEC

The combined Samsung-Privoro solution leans on defense-grade security from Knox and independent, hardware-based protections from SafeCase to keep information safe around the clock.

- On device, Knox Vault prevents the leakage of passwords, cryptographic keys and other critical information
- Off device, SafeCase prevents audio/video surveillance via audio masking and camera blocking
- A hardware-to-hardware integration between SafeCase and Galaxy prevents exfiltration over cellular radio

Seamlessly working from anywhere

Whether on campus or off site, users have continuous access to communications, file repositories and shared calendars.

- Increased productivity through improved situational awareness and faster decision-making
- Easier to recruit, retain and engage mobile natives and those accustomed to working and living with phones
- Redundant monitoring on and off device for compliance with smartphone policies

Single endpoint per user

IT only needs to manage SafeCase-Galaxy pairs and on-site wireless equipment, with DeX enabling full desktop capability and Knox supporting multiple classification levels.

- Smaller attack surface
- Lower chances of misconfiguration errors
- Reduced capital expenditures
- Sets the stage for future wireless initiatives

SafeCase trials are underway across the Federal government.

Let's create a custom game plan for driving your organization forward.

Learn more **privoro.com**
Initiate a trial **sales@privoro.com**

GALAXY S22®
AVAILABLE NOW