



Secure Spaces

Empower federal workers through trusted mobility

Increase federal workforce productivity and access to key resources by allowing protected mobile devices into secure workplaces.

Samsung's Galaxy S Series and Hardware Device Manager (HDM) partnered with Privoro's SafeCase uses hardware-to-hardware integration to control and block the phone's radio and sensor peripherals—preventing cyber attacks at the hardware level.

Create a foundation for trusted mobility with enhanced security protections that improve situational awareness and speed decision-making.

Key features



Protected mobile devices
secured at the hardware level, independent from OS



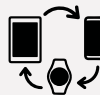
Samsung Knox security
and hardware device management can disable all RF radios



Prevent eavesdropping
by physically blocking cameras and microphones



Allow mobile device access
with data from emails, texts, and documents



Samsung DeX compatibility
for streamlined computing from phone to desktop monitor



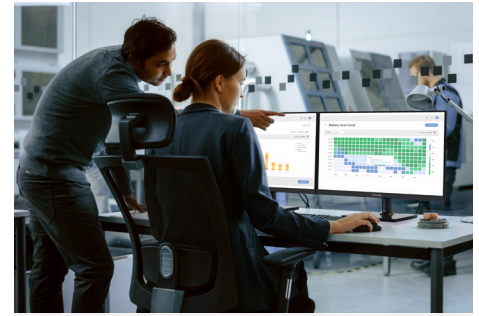
Intelligence

Secure your agency's most sensitive data at the hardware level. Protect top-secret intelligence from cyber attacks by disabling all RF radios, cameras, and microphones.



Defense

From the battlefield to the secure ops center, ensure your mobile devices are protected. SafeCase's Visual indicators confirm the solution is active, so your data is protected no matter your location.



Research

Maintain security in labs and research facilities. Make the next scientific breakthrough with secure access to the data you need on your mobile device.

Partners:



For complete product information and accessories, visit samsung.com/government insights.samsung.com

Product support: 1-866-SAM4BIZ | Follow us:  youtube.com/samsungbizusa  [@SamsungBizUSA](https://twitter.com/SamsungBizUSA)

SAMSUNG