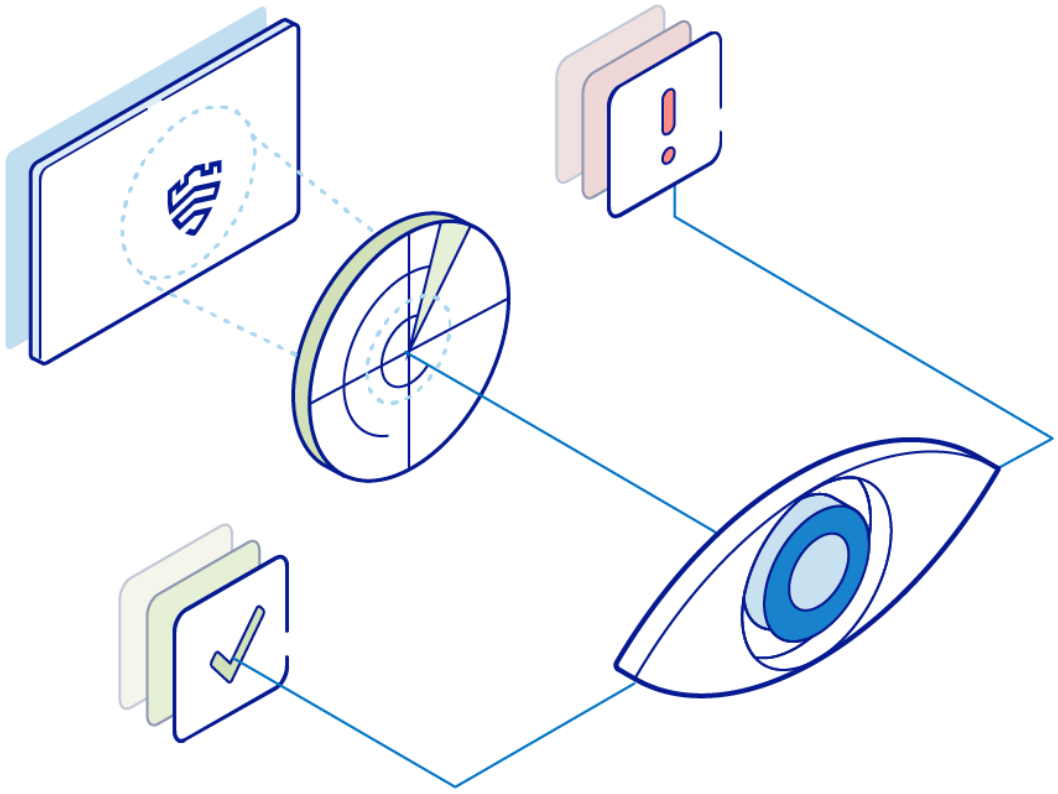
Mobile Threat Defense | Knox Partner Program

Archived: 2026-04-06 02:58:55 UTC

Remediate threats using our powerful Knox SDK to deliver the next generation of AI-powered security. Mobile Threat Defense (MTD) solutions can use machine learning to continually analyze mobile forensics and understand patterns of bad behavior.

Once you detect these threats, Samsung Knox empowers you to remediate through access to comprehensive management and security features.

Detect threats with Knox



Gain exclusive, secure, and privacy-compliant access to hundreds of **data points** with the Samsung Knox SDK.

App & process data

> Details about which apps are running, their current state, how long they've been running, and what device resources they're using.

Network data

Information about the data being sent from the device, the network conditions, connection quality, and routing tables.

Kernel data

How the device kernel and memory are being used: apps running in privileged mode, whether memory is being used normally.

File system data

The mounted file systems, usage type, and read/write permissions granted.

Remediate with Knox

Use cases

Threat	Scenario	Android Enterprise*	Knox Differentiation
Data leakage	Employee uses an unauthorized device app to store confidential files in the cloud, or a personal email app to send files, or device clipboard to copy private data to another app.	• Prevent users from installing certain apps or using app stores to download personal apps • Uninstall, update, disable, or blacklist apps • Wipe app data • Encrypt data while it is at rest on the device • Encrypt data while it is in transit, using VPN	• Restrict network domains that can be accessed • Advanced app management • Force an app to stop • Prevent clipboard access • DualDAR (Data-At-Rest) encryption of data • Advanced VPN features
Social engineering	Email or text asks user to click a link, which goes to fake banking website that gets user’s banking credentials.	• Hardware-based authentication used as a physical security key for two-factor authentication	• Restrict network domains that can be accessed

Threat	Scenario	Android Enterprise*	Knox Differentiation
Physical device breach + poor password management	Employee loses mobile device, which contains private customer data.	• Enforce authentication • Lock a device, block access to sensitive data, wipe all device data	• Force two-factor authentication or enterprise AD credentials • Integrate Samsung Pass or FIDO biometric authentication • Secure the certificates used to authenticate users • Keep a device locked even after a user authenticates successfully. • Remotely capture device screen activity, control device actions

*Android Open Source Project (AOSP) without Knox Platform for Enterprise

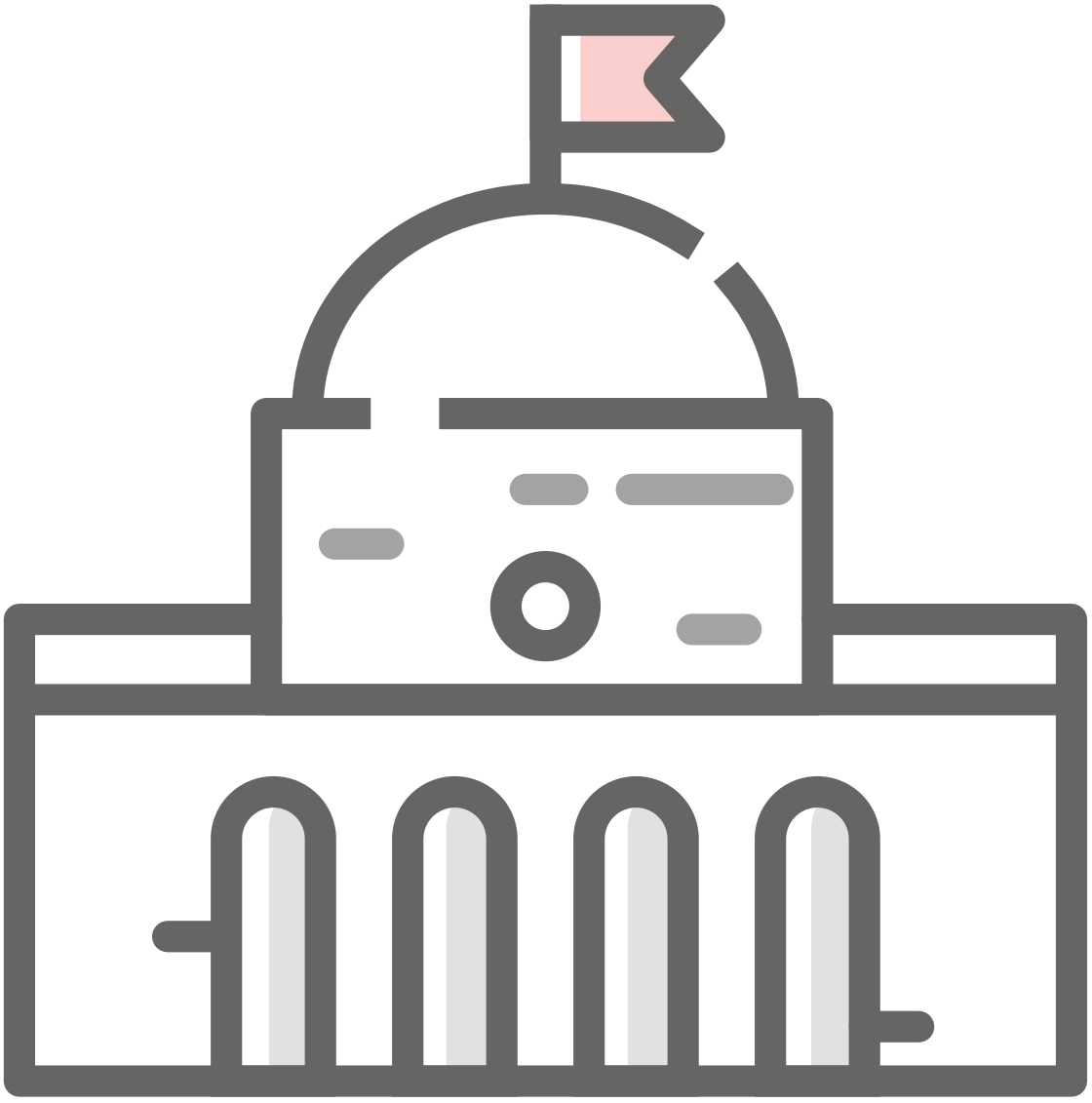
Find new business by integrating Knox features

Join the Knox Partner Program to enter our markets, meet systems integrators in our program, and identify potential customers.

Government/public service

Guarding critical infrastructure as well as personally identifiable info has never been more challenging with the continuing evolution of cyber espionage and malware. MTD is ideally positioned to innovate the future security of our mobile infrastructure.

Government/public service

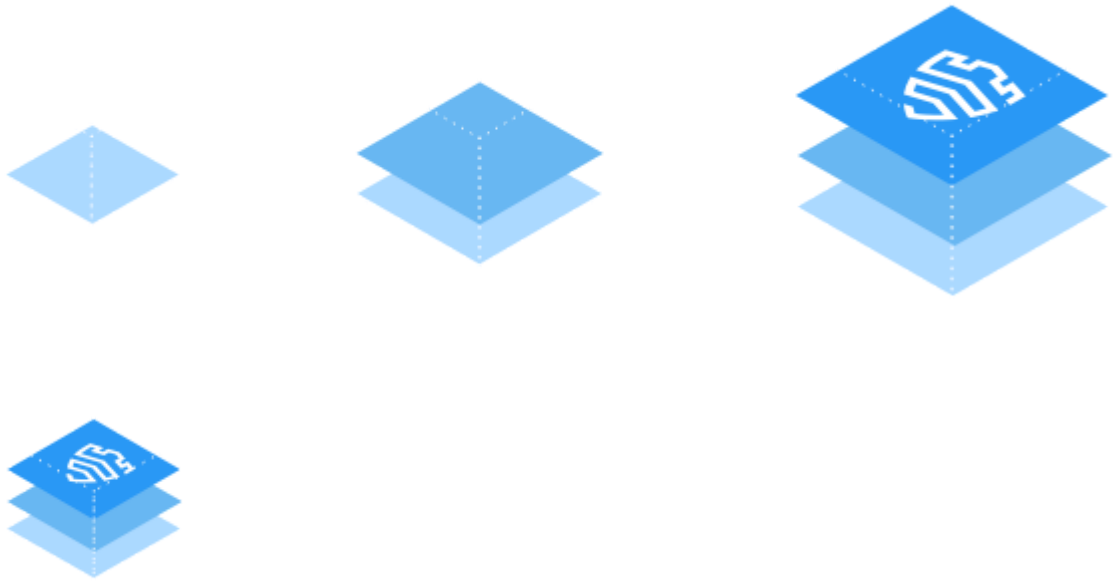


Guarding critical infrastructure as well as personally identifiable info has never been more challenging with the continuing evolution of cyber espionage and malware. MTD is ideally positioned to innovate the future security of our mobile infrastructure.

Get started

To add Knox features to your MTD solution, contact us to connect with your mobility experts.

Contact us



Source: https://partner.samsungknox.com/mtd