VIASAT MOBILE DYNAMIC DEFENSE

Security that goes deeper, so missions can go further

Capability snapshot: Hardware Device Manager (HDM)

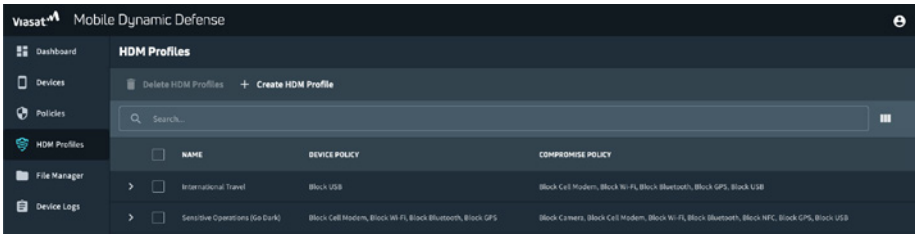
Viasat Mobile Dynamic Defense (MDD) combined with Samsung Knox Hardware Device Manager (HDM) delivers a defense-in-depth, high-assurance security model engineered for sensitive environments.

Secure edge devices

By combining MDD's offline-capable policy engine with HDM's below-OS enforcement and tamper-resistant persistence, organizations achieve a capability that most competitors lack: unified software + hardware control.

› Android OS provides rich policy control but can be targeted at the OS/app layer.

› HDM (hardware) enforces device states below the OS — persistent across resets and resilient to compromise.



Secure your operating system

With a growing risk of zero-click exploits, un-patched vulnerabilities, and malware leveraging CVEs to gain OS-level control, MDD minimizes the attack surface by remotely validating that HDM hardware policies (for example, Bluetooth-off or camera-off states) are enforced.

Key Benefits

LOST DEVICES ARE SECURED

› MDD + HDM reduces the risk of data extraction by tools that rely on a subverted OS and/or USB port access.

› Exploitable interfaces are hardware-disabled before the OS boots.

PREVENT ZERO-DAY, REMOTE EXPLOITS

› Uses cryptographic attestation, rather than trusting Android to self-report compliance — provable, not assumed.

› Ensures MDD can detect policy drift and alert operators.

Global headquarters
6155 El Camino Real, Carlsbad, CA 92009-1699, USA

Inside Sales
TEL 888 842 7281 (US Toll Free) EMAIL insidesales@viasat.com WEB vsat.co/mdd
+1 760 476 4755

11557606432-2026-003