Mobile Dynamic Defense
Mobile Device Cybersecurity

- Defense in Depth security for smartphones and tablets on the battlefield
- Policy and device integrity in both connected and disconnected modes
- DISA STIG and IA RMF Compliant
- ATO to operate on US Government Networks

SECURELY DEPLOY SMARTPHONES AND TABLETS ON THE BATTLEFIELD

The utility of commercial mobile devices on the battlespace is undeniable, but how to protect the sensitive information stored and accessed on those devices has been the challenge. The Mobile Dynamic Defense (MDD) software addresses mobile device management IA security requirements (e.g. DISA STIG) for tactical deployment. What makes it highly-valuable at the tactical edge is its ability to provide the necessary policy enforcement and in-mission configuration flexibility without a connection to a remote management system. This security is achieved through self-attestation, event logging, and automated threat response. Built-in robust root detection and system image validation ensures the device is truly protected from malicious cyber or physical activity. Additionally, warfighters have the flexibility to remotely or locally (without live network access) provision and configure devices.

MOBILE DYNAMIC DEFENSE AT-A-GLANCE

Features

- Defense in Depth security software for COTS Android devices
- Locally configure and provision devices as the mission changes
- Policy and device integrity maintained even when disconnected from remote management system
- DISA STIG and IA RMF Compliant
- ATO to Operate on US Government Networks
- Mobile security solution for TACLAN FCD-W Platform

Viasat Mobile Dynamic Defense

CAPABILITIES

MOBILE DEVICE MANAGEMENT

- Application management (install, whitelist, blacklist, mandatory)
- Configure application store access
- Detect and prevent silent installs and side-loading
- User certificates installation
- Device encryption enforcement (internal and external storage)
- Significant amount of security and policy settings
- Control device connections (Wi-Fi, Bluetooth, Cellular, USB)
- Device firewall administration
- Wi-Fi access management
- Tiered access control levels (user, operator, administrator)
- Device password policy administration
- Authorized reconfiguration of device security and policy
- Over-the-air update administration
- Audit logging (policy changes, logins, applications)
- Rapidly and securely change policy setting without physical cabling

THREAT DETECTION

- Previously rooted device
- Device root attempts
- Unauthorized system and policy modification
- Unauthorized application install/uninstall (whitelist, blacklist, unknown sources, removal of mandatory apps)

AUTOMATED RESPONSE

- Lock, reboot, or wipe device
- Block installation of blacklisted or unknown source applications
- Disable network access
- Notification of events on devices

CONNECTED

Remotely configure and provision through a secured connection; Operations Center receives device security status.

DISCONNECTED

Locally provision and configure as the mission changes.

CONTACT

SALES
TEL 888 842 7281 (US Toll Free) **EMAIL** dynamicdefense@viasat.com **WEB** www.viasat.com/mobile-enterprise-security