Fixmo Sentinel™ is the leading mobile security and device management platform for Government agencies and Enterprises in regulated markets. With Fixmo Sentinel you can manage all mobile devices from a single console while ensuring they start, and remain, in a trusted and compliant state. In addition to managing policy controls and device configurations, it continuously monitors system integrity and software configurations, and helps you act upon risks and potential compliance breaches before they happen.

Fixmo Sentinel has been developed as part of a Co-operative Research and Development Agreement (CRADA) with the U.S. National Security Agency (NSA) and is trusted by Government agencies and private Enterprises around the world to enable secure and compliant mobile computing in the workplace.

Device Integrity and Security
The leading solution for integrity monitoring, tamper detection, root detection and policy verification

Compliance Monitoring and Audit Reporting
Proactive compliance monitoring and reporting based on actual current state of devices and policies

Mobile Device and Application Management
Provisioning and deployment, lifecycle management, whitelist/blacklist monitoring, reporting and more

Adaptive Policy Management
Advanced policy management including location-aware and context-aware IT policies and access controls

Risk And Compliance Alerts

Configure and secure mobile devices
Monitor device, OS and data integrity
Prevent tampering and security breaches
Mitigate the risk of data loss and exploits
Monitor and maintain policy compliance
Produce auditable compliance reports
Support for iOS, Android® and BlackBerry®

Part of the AME 2000 Solution for Secure and Trusted Mobile Computing
Assured Mobile Environment (AME) 2000 from Motorola Solutions provides an end-to-end secure platform for trusted and compliant mobile computing in the workplace. Fixmo Sentinel operates as a core set of services within the AME 2000 solution providing centralized device, policy and user management, application whitelisting and blacklisting, system-level integrity monitoring and tamper detection, auditable compliance reporting and more.
**Device Integrity Monitoring**
Fixmo’s device integrity service continuously monitors the state of mobile devices and OS’s.

- Digital fingerprinting of trusted state configuration
- Detect and prevent changes to OS and policy configs
- OS Rooting and Jailbreak detection
- Compliance monitoring and alerting
- Update IT policies, lock/wipe device or lock/wipe corporate data in response to integrity breach
- Tracking and reporting for auditable compliance

**Compliance & Audit Reporting**
Fixmo Sentinel monitors your compliance posture and enables auditable reporting.

- Compliance monitoring and actionable alerts
- Reporting based on actual current state of devices and OS rather than last known state
- Pre-configured and custom compliance reports
- Centralized compliance reporting across BlackBerry, iOS, and Android
- Solutions for Government, Finance, Healthcare

**Mobile Device and App Management**
Fixmo Sentinel provides comprehensive MDM and mobile application management (MAM).

- Centralized user and device administration
- Software inventory and device tracking
- Application provisioning and whitelist/blacklist
- Remote diagnostics and analysis
- User self-service and integration with ITSM systems

**Adaptive Policy Management**
Fixmo Sentinel centrally manages policy configurations across all mobile devices.

- Device passcode and application control policies
- Restrict camera, Bluetooth, screen capture and more
- Remote lock/wipe/reset with automated rules
- Location- and network-based adaptive policies
- Policy management for Fixmo SafeZone™ container

---

**Ensure your devices start, and remain, in a known trusted state.**

*Detect and prevent security and compliance breaches.*

*Maintain and prove compliance through auditable reporting.*

---

**Exclusive Features for AME 2000**
In addition to the core feature set described above, Fixmo Sentinel has been customized to offer a deeper set of policy control over mobile devices powered by the AME 2000 platform including:

- Disable and manage USB features and functions
- Manage discrete Location/GPS permissions
- Bluetooth Address whitelisting and blacklisting
- Enable or disable SD Card usage

**Defense-Grade Solutions Built on Government Heritage**
Fixmo Sentinel has been developed as part of a Co-operative Research and Development Agreement (CRADA) and Technology Transfer Program (TTP) with the U.S. National Security Agency (NSA). Fixmo Sentinel is included as part of the Security Technical Implementation Guidelines (STIG) for BlackBerry and Android deployments as specified by the U.S. Department of Defense’s Defense Information Systems Agency (DISA).

---

For more information on Fixmo and our Mobile Risk Management Solutions, please contact sales@fixmo.com or visit us at www.fixmo.com

Copyright © 2012 Fixmo Inc. All rights reserved. Fixmo, Fixmo Sentinel, Fixmo SafeZone, Fixmo MRM and the Fixmo logo are trademarks of Fixmo Inc. All other product or company names may be trademarks and/or registered trademarks of their respective owners. Fixmo Inc does not accept liability for any errors or omissions in this document, which may be subject to change without notice. Version 05/2012.