Fixmo

Mobile Risk Management

Identifying, mitigating and managing the risks with mobile devices

Why Mobile Risk Management?

Smartphones and tablets have changed the way we work, play, communicate and navigate our way through the physical and virtual worlds. We're now seeing **mass proliferation of connected mobile devices** across consumer, business and government markets. Heterogeneous deployments of BlackBerry®, Android®, iOS, Windows Phone and other mobile platforms are becoming the norm while organizations embrace the **"bring your own device" (BYOD)** trend, allowing personal-liable devices onto the corporate network. Smartphones and tablets are becoming a **hub for business and personal data**, identities, social networking, gaming, commerce and a wide range of apps provided by both commercial software developers and corporate IT departments. And with technologies like Bluetooth and NFC, **machine-to-machine (M2M)** interactivity is on the rise and mobile devices are now exchanging private and personal data with a range of connected devices and will soon become our wallets.

The opportunities associated with mobile devices are significant and the BYOD trend can provide real cost savings. But along with this comes an **unprecedented and complex set of security and compliance risks** that require a thoughtful approach to mobile risk management that goes beyond traditional mobile device management (MDM) practices to help you protect your privacy and mitigate the risks of data loss, security breaches, malicious cyber attacks and non-compliance.

Where did your mobile devices come from, and what exactly are they doing?

A smartphone or a tablet may be purchased by the IT department or by an individual employee, and...

- It could be running one of hundreds of different variations of OS platforms and versions.
- It could be used for personal and business use and will likely have dozens of apps installed over its lifetime.
- It will be used to access and store private corporate documents and emails.
- It likely has a camera and will be used to post content to social networking sites.
- It may get connected to Bluetooth peripherals or be used as a wallet or security access badge thanks to NFC.
- It will roam onto insecure WiFi networks, and may be accidentally forgotten on a restaurant table or left in a cab.
- It may be passed around to friends and family members, including young children, to use or play games on.
- **Its owner may be any one of your employees, including a C-level executive.**

Understanding Your Mobile Risks

Mobile devices can introduce sophisticated and complex risks that go beyond the devices themselves, including risks associated with mobile infrastructure, apps and end-users as well as external and context-specific situational threats:

Infrastructure Risk

Are your mobility servers properly configured and compliant, and have they remained that way?

Device, OS and Application Risk

How can you verify the integrity, authenticity and compliance of each device's OS, modules, policy configurations and installed apps?

User, Loss and Theft Risk

How can you mitigate the risks of intentional and accidental user actions, device loss and data theft?

Situational and Context Risk

What are the risks associated with roaming onto different networks, connecting to peripheral devices or using sensitive apps in high-risk locations or environments?

Fixmo

Mobile Risk Management

MRM: A Comprehensive Approach to Managing Mobile Risk

Mobile Risk Management (MRM) is a comprehensive approach to identifying, mitigating and managing the risks associated with using or deploying mobile devices. MRM solutions help to protect organizations from private data loss and leakage, security breaches, identity theft, fraud and cyber attacks – threats that can expose organizations to a range of potentially costly risks including:

- ✓ **Financial Risks** due to regulatory non-compliance
- ✓ **Reputational Risks** resulting from security breaches and violations
- ✓ **Competitive Risks** associated with Intellectual Property leaks

A New Approach to Confidently Enabling Mobility

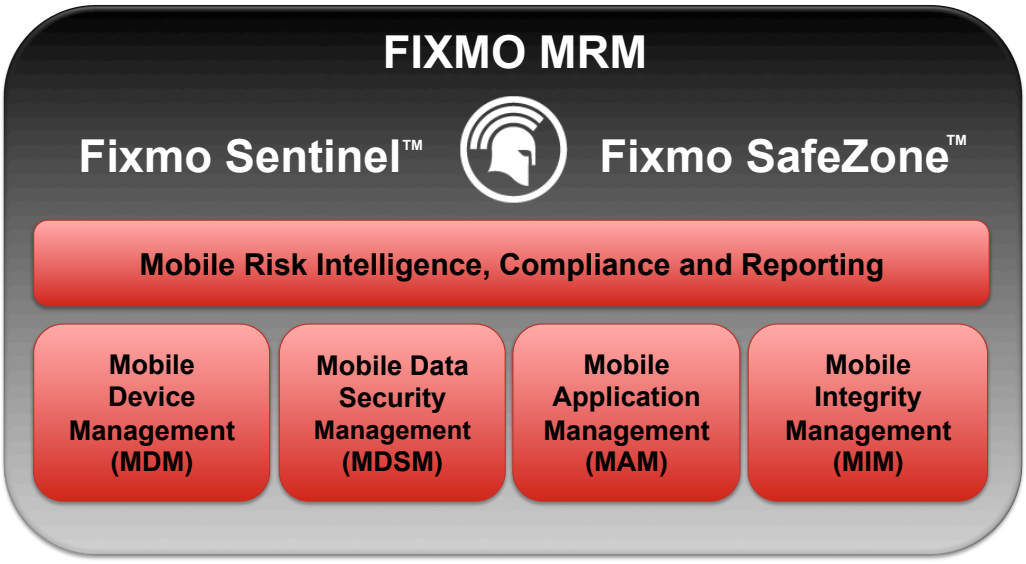
MRM helps organizations go beyond traditional mobile device management (MDM) practices to help them exercise the full potential of mobility while protecting corporate data and ensuring regulatory compliance. Using a **risk mitigation** philosophy, MRM helps organizations embrace a wide range of mobile devices and the BYOD trend by taking a holistic approach to MDM, corporate data security, mobile application management (MAM), device and software integrity verification, remote system monitoring and compliance reporting. MRM gives you the tools you need to ensure mobile devices start, and remain, in a trusted state and that you can prove compliance with internal policies and government regulations.

MRM Highlights

- Ensure mobile infrastructure, devices and apps start and remain in a trusted and compliant state
- Protect devices from data loss; prevent breaches and non-compliance scenarios
- Securely deploy and manage private corporate apps, data and documents
- Mitigate the risks associated with devices operating in a compromised state or within an environment that could expose it to threat
- Address regulatory compliance and reporting requirements

Fixmo's Approach to MRM: Verify, Protect, Comply, Prove.

Fixmo provides MRM solutions for government agencies and enterprises that continuously monitor and **verify** the configuration and integrity of mobile devices and infrastructure, **protect** corporate data from loss or theft and provide powerful risk intelligence, reporting and **compliance** tools to help organizations prevent potential threats, and **prove** regulatory compliance. Fixmo's MRM solutions act as an integrated component of a holistic approach to Managed Mobility, Enterprise Security and IT Compliance and can be deployed as a comprehensive solution set or in a complementary fashion to existing MDM or MAM solutions.



Verify Integrity
Configure
Monitor & Preserve

Protect Data
Contain
Detect & Prevent

Comply
Monitor
Analyze & Alert

Prove It
Reporting
Auditability

For more information on Fixmo, please contact **sales@fixmo.com** or visit us at **www.fixmo.com**.