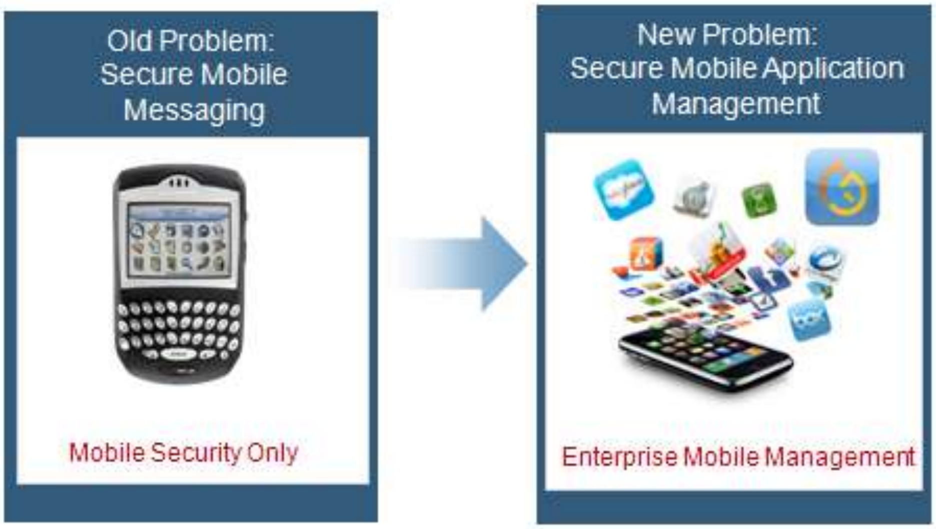
McAfee Enterprise Mobility Management vs. Good Mobile Enterprise

McAfee Enterprise Mobility Management (EMM®) provides a total solution that secures and manages mobile data, devices, and applications of enterprises whereas Good Mobile Enterprise and Good Mobile Government merely offer security by securing mobile messaging.

As the world's largest dedicated security company, McAfee enhances its mobile phone security portfolio with data and device protection for today's most popular Smartphones. Award-winning McAfee® Enterprise Mobility Management solution enables enterprise mobile security to configure mobile devices in accordance with company security policies, while automating the configuration and connectivity of WiFi, VPN, and native e-mail synchronization. McAfee EMM is a scalable architecture that can manage thousands of mobile users.

Problem: Old Secure Mobile Messaging needs New Secure Mobile Application Management.

Mobility has moved beyond e-mail. Today, an assortment of applications that solve real business Mobile Application Management challenges are either commercially available or available as development tools to allow organizations to build custom, enterprise-specific applications. Only after an IT organization has fully digested the scope of mobilizing business applications and laid the foundational requirements—security, connectivity, provisioning, integration, and scalability—will they be able to deliver tangible business value, increase top-line growth, and improve operational efficiencies. Organizations intent on mobilizing their workforce rely on the McAfee EMM solution to provide the protection and flexibility to manage their data, devices, and applications.



Solution: McAfee EMM provides a Secure Mobile Application Management

The business driver in the old paradigm was mobile e-mail and the problem that needed to be solved was secure mobile messaging. This paradigm, however, required little to no enterprise data center integration and relied on front-end messaging solutions that could create a narrow silo outside the enterprise network, security architecture and provision e-mail.

McAfee EMM Comparison Criteria

- **Strong Security**—Pushes e-mail with strong authentication for iOS platform without any performance or battery impact.
- **Provisioning**—Provisions all devices and applications and not just e-mail.
- **Compliance**—Sets policies, ensures policies are persistent, verifies policies for automatic real-time compliance enforcement.
- **Enterprise Data Center Integration**—Integrates deeply into existing systems.
- **Connectivity**— Securely connects to enterprise services: VPN, Wi-Fi, messaging and LOB applications.
- **Scalability**—Supports enterprise-grade solution scalable server-centric architecture.

Although McAfee makes all reasonable efforts to maintain the accuracy of the contents of this document, it relies on third parties for much of the information provided and does not accept any liability for information that is found to be incomplete, inaccurate or out of date. The information contained in this document is only for general information, and is not intended to provide any advice, make any offer or in any other way result in the creation of a legally enforceable relationship between McAfee and yourself. You should place no reliance on such information for investment purposes or otherwise, and McAfee excludes all liability for loss or damage, whether financial or otherwise (to the fullest extent permitted by law) ensuing from your use of this information.

The new paradigm, however, is driven by the need to deliver secure mobile applications and prevent data loss with device loss. To accomplish this, the MacAfee EMM solution provides deep and broad integration with the enterprise IT infrastructure. This includes integration with Active Directory/LDAP, VPN, Wi-Fi, as well as existing end-point security infrastructure such as CA/PKI certificates.

Strong Security for Mobile Devices

The McAfee EMM solution protects all enterprise data on supported mobile end-points, including business application data, user credentials, shared credentials, e-mail, and personal information management. EMM architecture leverages native security—PIN/password, encryption, local and remote wipe, as well as management features that are built into enterprise-class mobile devices. By properly configuring mobile devices connected to existing IT infrastructure, EMM enables data services be delivered to mobile end-points while maximizing the infrastructure investment that offers the best possible experience to end-users. This architecture provides IT seamless security controls to end-users that do not negatively affect device performance or battery life. Good Mobile provides security only for e-mail applications. It does not offer two-factor authentication; instead it authenticates through a proprietary mechanism vs. a standard-based certificate.

Whole Device and Applications Provisioning

EMM's self-service provisioning sets security policies, configures network connectivity, and automatically personalizes devices for users by configuring e-mail, Wi-Fi, and VPN.. Users can provision their own mobile devices and perform basic functions, troubleshoot some device issues on their own without having to rely on Helpdesk personnel for assistance. Other device and application provisioning provided include application updates for a fully configured end-point. Good Mobile provisions only Good mobile e-mail. It neither supports HTML e-mail nor preserves the user experience of the device.

Automatic Real-time Policy Compliance

Security policies and configuration updates are pushed in real-time to the device over-the-air including selective and remote wipe if the device is lost or stolen. Devices are automatically checked prior to network access to ensure that only authorized, managed, and secured devices access enterprise applications and services. The EMM solution integrates seamlessly with an enterprise's Active Directory infrastructure to perform user management, group-based policies, device activation, and administrative role-based access control to the management console. EMM enforces compliance to ensure that all devices connecting to a corporate network are compliant with the company's security policies. Reporting and auditing capabilities are also provided. Good Mobile provides only partial compliance. With Good, pushing policies to groups requires that multiple systems be managed which makes it cumbersome.

Active Directory Data Center Integration

The McAfee EMM solution mobilizes the enterprise application architecture by connecting mobile devices to enterprise applications via an organization's current infrastructure—Sync, WiFi, VPN, and PKI. It bridges mobile users, applications, and devices to the data services that these entities need to access. The platform is a software overlay that is part of the IT datacenter environment and architected to avoid inefficiencies, poor scalability, and interoperability. Good Mobile does not integrate with AD, VPN, Wi-Fi, or PKI; Rather it provides a light front-end messaging solution by creating a narrow silo outside of the enterprise network and security architecture.

Encrypted Connectivity

McAfee EMM servers use encrypted SSL (HTTPS) connections to ensure all data transmitted between mobile devices and servers are encrypted. iPhones that do not have native encryption can be blocked from accessing the network.

Although McAfee makes all reasonable efforts to maintain the accuracy of the contents of this document, it relies on third parties for much of the information provided and does not accept any liability for information that is found to be incomplete, inaccurate or out of date. The information contained in this document is only for general information, and is not intended to provide any advice, make any offer or in any other way result in the creation of a legally enforceable relationship between McAfee and yourself. You should place no reliance on such information for investment purposes or otherwise, and McAfee excludes all liability for loss or damage, whether financial or otherwise (to the fullest extent permitted by law) ensuing from your use of this information.

Current generation mobile devices are powerful productivity tools because they provide an array of connectivity options. Devices can access data over carrier networks via WiFi, 2G, 3G, and now 4G. In addition, enterprise-class devices provide powerful VPN capabilities which, when combined with wireless connectivity, provide secure remote access to enterprise data. These EMM's networking capabilities enable a new world of transaction-oriented applications in addition to the important and well-supported enterprise e-mail application. They automate the configuration of secure WiFi, VPN, and native e-mail synchronization, enabling users to connect to the services needed while maintaining the level of data protection the organization requires. While Good uses secure transport layers, it transports the data through a network operation center (NOC) that is a single point of failure.

Scalability

The McAfee EMM solution allows mobility to be scaled to thousands of mobile users for multiple business applications, over a geographically dispersed data network. It integrates into the enterprise's existing environment and scales to tens of thousands of devices, while managing these devices from a single web console. The EMM solution leverages existing data-center virtualization, load balancing, and DB replication to provide high-availability and business continuity across multiple geographies. Good Mobile and EMM are both enterprise-grade, offering scalability capabilities such as virtualization on VMware, disaster recovery options, and load balancing. However, Good has some performance issues which impact its scalability.

McAfee vs. Good Security and Management Features Comparison

Capability Comparison	Description	McAfee	Good Mobile
Native Device User Interface	Support for html mail. E-mail configuration and management, using native e-mail Inbox.	yes	no
Application Management	Enterprise OTA App push, configuration and management.	yes	no
Real-time Compliance Authentication	Device single sign-on. Strong authentication. Applications compliance messaging compliance.	yes	partial
Data Center Integration	Existing network and services infrastructure s: Active Directory, VPN, Wi-Fi, native e-mail. Existing end-point security infrastructure	yes	no
Provisioning	Whole device and applications. Network facilities. Security tools.	yes	only e-mail
Enterprise-grade	Scalability to 10,000+ seats. Redundancy and geographic resiliency. Disaster recovery options.	yes	yes

Summary and Key Differences

EMM is a broad mobility management solution that is focused on management functions. This requires that EMM be a piece of security infrastructure.

Only McAfee EMM provisions SSL client certificates to iPhones by pushing e-mail with strong authentication with no performance or battery impact. EMM also offers the only solution that automatically detects changes to Smartphone configuration profiles and other device status, automatically enforcing compliance without any IT administrative involvement. McAfee leverages corporate e-mail (e.g., Exchange or Lotus Notes, Active Directory & LDAP), is standards-based and will integrate with ePO.

Good Mobile is focused on the narrow application of e-mail using a dedicated device. Moreover, it uses sandboxes that are slow, drain device batteries, are expensive to purchase, and depend on an inherently flawed architecture that will require replacement as enterprise applications accelerate.

Although McAfee makes all reasonable efforts to maintain the accuracy of the contents of this document, it relies on third parties for much of the information provided and does not accept any liability for information that is found to be incomplete, inaccurate or out of date. The information contained in this document is only for general information, and is not intended to provide any advice, make any offer or in any other way result in the creation of a legally enforceable relationship between McAfee and yourself. You should place no reliance on such information for investment purposes or otherwise, and McAfee excludes all liability for loss or damage, whether financial or otherwise (to the fullest extent permitted by law) ensuing from your use of this information.