Competitive Review 11/8/2010

McAfee Enterprise Mobility Management vs. MobileIron

McAfee Enterprise Mobility Management (EMM®) provides a total solution that secures and manages mobile data, devices, and applications of enterprises; MobileIron does not provide strong security, lacks scalability and redundancy capabilities, and has limited data integration capabilities.

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 security policies while integrating with the enterprise IT infrastructure, including Active Directory/LDAP, VPN, Wi-Fi as well as with existing end-point security infrastructure such as CA/PKI certificates. McAfee EMM is a scalable architecture that can manage tens of thousands of mobile users.

Comparison Criteria: Strong Security Authentication and Policy Compliance

Data Protection and Authentication

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. The 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. 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.

MobileIron: Installs a server appliance in the DMZ zone that is not configured for high-availability and results in a less secure approach since it is a single point of failure.

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. 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 4G. 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.

MobileIron: Requires using multiple proprietary ports that introduce additional security risks.

Data Compliance and Security Policy Management

Security policies and configuration updates are pushed in real-time to the devices 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. 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.

MobileIron: Provides only partial compliance since it does not implement Active Directory groups directly. This results in difficulties implementing group policies.

McAfee EMM Comparison Criteria

- **Strong Security**— Strong Authentication for ActiveSync email without any impact on performance, latency, or battery life impact.
- **Connectivity**— Securely connects to enterprise services: VPN, Wi-Fi, messaging, and LOB applications.
- **Compliance**—Sets policies, ensures policies are persistent, verifies policies for automatic real-time compliance enforcement.
- **Enterprise-Grade Scalability**—Supports scalable server-centric architecture.
- **Enterprise Data Center Integration**—Integrates deeply into existing systems.

McAfee EMM Solution Scalability and Integration

- **Scalability—** The platform is a software overlay that can be virtualized, load -balanced, and is a single pane of transparent visibility and control over all devices in multiple geographies. It is part of the IT data center environment and architected to avoid inefficiencies, poor scalability, and interoperability.
- **Integration—** 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.

Comparison Criteria: Scalability and Integration into Existing Network Infrastructure

Enterprise-Grade Scalability

The McAfee EMM solution integrates into the enterprise's existing environment and scales to tens of thousands of devices, while managing these devices from a single Web console. EMM supports SQL clustering, leverages existing data-center virtualization, and utilizes load balancing and DB replication to provide high-availability and business continuity across multiple geographic areas. Each EMM proxy supports 2000 devices and can be load-balanced for high concentrations of users by using a group of proxies. It enables redundancy since each proxy server can take the load from another if it is unavailable.

MobileIron: Does not scale to a large number of users and is more suitable for mid-size enterprises. It can only support 500 devices per appliance, has no load balancing capability, does not provide highly-availability, and does not have any built-in redundancy.

Enterprise Data Center Integration

The McAfee EMM solution allows connecting mobile devices to enterprise applications via an organization's current infrastructure such as ActiveSync. It bridges mobile users, applications, and devices to the data services that these entities need to access. EMM integrates into enterprise data center, including CA/PKI that delivers certificates from the enterprise CA to each iPhone for VPN and WiFi access.

MobileIron: Provides only partial data integration with Active Directory or Wi-Fi, resulting in mobile device functioning outside of the enterprise network and security architecture.

McAfee vs. MobileIron Security and Management Features Comparison

Capability Comparison	Description	McAfee	MobileIron
Authentication	Device single sign-on. Strong authentication.	yes	partial
Encryption	SSL Connections. Encrypted connectivity.	yes	partial
Real-time Compliance	Applications compliance. Messaging compliance.	yes	partial
Enterprise-Grade Scalability	Scalability to 10,000+ seat devices. Redundancy and geographic resiliency. Disaster Recovery options.	yes	no
Enterprise Data Center Integration	Existing network and services infrastructure: Active Directory, VPN, Wi-Fi, native e-mail. Existing end-point security infrastructure. Whole device and applications.	yes	partial

McAfee EMM Comparison Conclusion

- EMM allows attaching devices such as iPhones to the rest of the McAfee security portfolio.
- Even though MobileIron provides device-side APIs, it lacks a solid solution for the core problem of securing and managing enterprise data, devices, and applications.

Summary and Key Differences

Only McAfee EMM provisions SSL client certificates to iPhones by pushing e-mail with strong authentication with no performance or battery impact. EMM offers the only solution that automatically detects changes to Smartphone configuration profiles and other device status by automatically enforcing compliance without any IT administrative involvement. It leverages corporate e-mail (e.g., Exchange or Lotus Notes, Active Directory, and LDAP), is standards-based, and integrates with ePO. EMM is capable of scaling up to 10,000 or more devices. While appearing to be rich in features, MobileIron positions itself in the "Do it all" market segment. In contrast,, McAFee provides the the most secure solution specifically for managing mobile devices and enterprise applications.