The Value of IBM's MaaS360 Solution

Executive Summary:

With the number of mobile devices increasing as well as the amount of sensitive corporate data on mobile increasing, customers are looking for a solution to protect against threats like: Data Leak, Mobile Malware, Lost/Stolen, Internal Theft and End User Vulnerabilities/Lack of Compliance.

With hundreds or thousands of mobile endpoints, administrators need a solution to manage their corporate content while protecting end user privacy. Below is an outline of four of the major value adds of MaaS360.

1.) **Industry Analyst** - Every major industry analysts agrees that no enterprise company should go without an EMM solution like IBM MaaS360.

2.) **Mobile Risks and Breaches** - It is well documented that risks associated with mobile device use in the workplace is on the rise. While the majority of media coverage is often focused on Android malware, that is only the tip of the iceberg. Additional risks include iOS Malware, litigation associated with BYOD, encryption and breaches associated with improper employee access

3.) **Help Desk Productivity** – Customers should complete an analysis of service desk calls related to mobile. How many of these calls can be avoided with an EMM solution like IBM MaaS360? How many of these calls can be resolved faster with MaaS360?

4.) **MaaS360 vs. EAS** – Customers current strategy leveraging Microsoft Exchange ActiveSync is not comprehensive enough for today's enterprise mobile environment.

Analyst Opinions

1.) Forrester -Brief: Plan Your Four-Tiered Approach To Enterprise Mobile Security (Attached). MaaS360 provides the tools for all the items highlighted in yellow

2.)Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration (MaaS360 provides items in **BOLD)**

" The best defense is to keep mobile devices fixed in a safe configuration by means of a **mobile device management (MDM) policy**, **supplemented by app shielding** and '**containers**' that protect important data. "

3.) Gartner The Top Eight Best Practices for Starting or Extending a BYO Program (available upon request)

Isolate, Protect and Manage Organization Digital Assets While Respecting User Privacy - (MaaS360 provides items in **BOLD)**
Sample of Recommendations:

- At minimum, **containerize enterprise apps and data on mobile devices, enforcing encryption of enterprise data on user-owned devices**.
- Use **EMM to apply policies to employee BYOD devices**, which facilitate **containerization**, **certificate management** and **secure content access**, in addition to providing **tools to make support easier**.

Mobile Risks and Breaches

ComputerWorld -One-fifth of IT pros say their companies had mobile data breach

- " Nearly one-fourth (24%) of respondents said mobile devices used in their organizations had connected to a malicious Wi-Fi hotspot in the past, while 39% said those devices downloaded malware. The responses included both worker-owned or corporate-owned devices."
- " The survey found that just 34% of respondents wipe sensitive data from employee devices when they leave the company. Whether the device is employee or corporate-owned, unwiped data can be stolen by unauthorized parties, risking a worker's privacy as well as corporate and customer data."
- " Perhaps more troubling was a finding that 37% of organizations were not even sure whether mobile devices had been involved in security breaches in the past."

CU Times -Most Breaches Stem From Employee Mobile Access: Report

- " Two thirds of organizations surveyed for a recent report said they suffered a data breach that resulted from employees using mobile devices to access confidential company information, according to the San Francisco-based security firm Lookout and Traverse City, Mich.-based Ponemon Institute."
- " The companies said an average of 3% of employees' mobile devices are infected with malware at any point in time, which equals more than 1,700 mobile devices in a typical organization that connect to an enterprise network every day."

CBS News -Common software would have unlocked San Bernardino shooter's iPhone

- "If the technology, known as mobile device management, had been installed, San Bernardino officials would have been able to remotely unlock the iPhone for the FBI without the theatrics of a court battle that is now pitting digital privacy rights against national security concerns."

PR Newswire - A Mobile Data Breach Could Cost an Enterprise $26.4 Million

- " Take customer records, one of the most at-risk types of data: on average, IT believes that 19 percent of employees can access customer records via mobile while 43 percent of employees say they have access to that data. With mobile data breaches happening in the majority of enterprises today, this visibility gap introduces unacceptable risk."
- " Fifty-six percent of data accessible on PCs is also accessible on mobile devices. " and " Mobile data access is expected to increase at least 50 percent in the next 2 years."
- " Two thirds (67 percent) of respondents say it was certain or likely that their organization had a data breach as a result of employees using their mobile devices to access the company's sensitive and confidential information."

Labor Dish -What Recent Case Law Can Teach About BYOD Workplaces

- "In Rajaee v. Design Tech Homes, et al., the company remotely wiped the iPhone of a sales rep when he resigned. This deleted all of the data—personal and work-related—and restored it to its factory settings. This ex-employee brought suit under the ECPA (which makes it illegal to intentionally access electronic information without authorization) and CFAA (which, among other things, makes it unlawful to cause $5,000 or more in damage to electronically stored information)."
- "Many companies are **partitioning work-related content from personal content** on their employees' personal devices so when an employer needs to **remotely wipe a lost or stolen device**, it will do so only

the corporate side of the wall." MaaS360 allows customers to selectively wipe corporate data therefore limiting litigation risk of wiping an employee's device

IT Business Edge - Studies Show Rise of the Mobile Malware Threat

- " According to a study conducted by G DATA, a new strain of Android-centric malware is identified every 11 seconds, with approximately 2.3 million new Android malware samples discovered in 2015."
- " iOS-based malware XcodeGhost and FlexiSpy made the top 20 list of malware."
- " This rise in mobile infections comes at a time when infections targeting PCs are dropping. Clearly, cybercriminals have restructured their attacks to target the devices we are using most often. "

MaaS360 for Help Desk Productivity

Simplified Device Configuration – reduces IT effort with users self-registering
–Time to register (minutes per device), number of devices needing registration (per month)
•**Reduced Inventory Management**
–Effort – time to create/validate inventory of mobile devices, inventory management hours per month
•**Application and Content Management IT Staff Savings (ITCR)** – can push or pull data and apps using policies, including whitelisting, blacklisting and requiring apps. Less time for IT to distribute of sensitive data in secure containers.
•**Additional Labor Avoidance** – reduction/elimination of additional resources to manage mobile devices in other geographies, divisions, etc. due to centralized control of enterprise device management
•**Reduced Service Desk Calls** – reduction of help desk calls from users due to **end user self-service portal** with an intuitive interface and simplified app and content management. Service Desk calls minimized using IBM MaaS360 could include the following: password reset, email configuration, WiFi configuration, VPN configuration, locating lost devices, app downloads, malware detection, new device support, etc....

MaaS360 vs. Exchange ActiveSync Only

MaaS360 delivers a complete mobility lifecycle management solution providing support for all mobile OS's
EAS is insufficient to manage devices from deploying to decommissioning
Proof Points for what MaaS360 can & EAS can't do:

- Zero Touch for IT with user configuration of email, Wi-Fi & VPN, etc.
- Complete control of users accessing corporate data (email, calendar, contacts) on mobile devices
- Delivers complete visibility and collection of device data
- Location Services for lost of stolen devices with full wipe capabilities if irretrievable
- Performs a selective wipe of corporate data & preserves personal data for all employee owned devices after dismissal
- Mobile Threat Management- **Detect, analyze and remediate** mobile malware on compromised devices as well as jailbroken or rooted detection
- MaaS360 Mobility Intelligence dashboards & reports for the entire mobile IT environment
- Provides app security, secure email & secure web browser
- Comprehensive data leak prevention/containerization features like disabling copy/paste, forwarding data, uploading to other apps & data backups,
- Provides expense management to help control mobile data costs