Security and Service, Not Spying

Mobile devices in the workplace are here to stay. From smartphones to tablets, this convenient technology brings added freedom and benefits to employees, but also creates a high security risk for businesses. More often than not, a tool like mobile device management (MDM) is utilized to protect confidential data, but there is a common misnomer that MDM can be used for spying purposes. This is simply not the case.

MDM protects confidential information from thieves and hackers. Whether your company embraces a Bring Your Own Device (BYOD) model or provides mobile devices to employees, it is absolutely critical to safeguard the company's IT infrastructure against security breaches and protect the confidential information that can be accessed if a mobile device is lost or stolen. Our MDM software is designed only to service and secure the mobile devices – no spying, period.

MDM Services Provided	MDM Myths Debunked
Configure access to a corporate Exchange email or a personal IMAP/POP email account	We cannot view, track, capture or store emails or other messages sent from configured accounts
Configures VPN network and Wi-Fi settings	We cannot view or monitor websites visited or other online activity
Enables corporate directory search for a contact or email address when composing emails	We cannot view or access contact information stored on the mobile device
Sets passcode requirements, including passcode length, character requirements and maximum passcode age	We are only able to perform a reset in the event a user forgets their passcode; the passcode cannot be viewed by technicians
Specifies the number of times a passcode can be entered incorrectly before all data on the device is erased	We are only able perform a remote wipe in the event someone other than the user attempts to access the device; we cannot see who is trying to gain access
Geographical location lookup	We will attempt to pinpoint the physical location of a mobile device on a geographical map only when a device is reported lost or stolen by the device owner
Performs a complete wipe in the event of a lost or stolen mobile device	We will only perform this action when a loss or theft is reported by the owner of the device
Selective wipe of mobile devices (available only on Apple iOS® devices)	We will remove any policies and configurations that were deployed to the device when it was under management in the event an employee leaves the company, leaving personal information intact
When company policy requires, the MDM software can restrict access to app stores, explicit media, use of the web browser and websites such as YouTube, the ability to screen capture, the use of voice dialing or voice assistants, and the use of the camera	We will only activate these restrictions when company policy dictates or when regulatory requirements exist

The goal of our MDM solution is only to secure and protect the sensitive company information stored on employee-owned and corporate mobile devices, as well as maintain the overall integrity of the company's IT system by putting the necessary policies and configurations in place to prevent or eliminate security breaches. Your employees have nothing to fear when installing MDM software on their mobile devices and are welcome to contact us if they would like any additional information about the services provided or the capabilities of the software.

Bardissi Enterprises, LLC
1250 Bethlehem Pike, S247
Hatfield, PA 19440
2158532266
www.bardissi.net