

### Lock & Wipe, Encryption and VPN *powered by Mossec*



**The iMDM Advantage** - Mobile subscribers, particularly enterprises, are increasingly thinking about security - and with good reason. As the capabilities and capacities of smartphones increase, the amount of data on those devices increases as well. While this provides opportunities for greater mobile productivity, it also creates challenges. What happens if a handset is lost or stolen? How do you keep data secure on the device? How do you ensure that your mobile workforce has the access they want with the security that the organization needs?

Through our partnership with Mossec, a leader in mobile device security, InnoPath extends MDM with Lock and Wipe, Encryption and VPNs for Open OS devices in support of enterprise deployments. InnoPath's iMDM Server provides a framework which can be used to manage these capabilities over the entire fleet of handsets in an organization, securing data on mobile devices while also ensuring access and maintaining productivity. Note that InnoPath also supports Lock & Wipe for RTOS devices as part of its iMDM Client Suite.

**Lock & Wipe** - Lost or stolen handsets can be locked and if needed, even wiped remotely. It is possible to lock a handset such that a password or PIN is required to unlock, and a set number of attempts to input the PIN can be specified. It is also possible for an operator customer care organization or a corporate helpdesk to lock the handset in such a way that it can only be unlocked by customer care or IT.

**Encryption** - Leaving data on mobile devices in an unencrypted state is tantamount to giving that data away. The media provides numerous examples of unencrypted data being compromised because it was on a laptop that was lost or stolen. With the capabilities of smartphones approaching those of laptops, it is increasingly likely that the loss of a physical handset could result in a similar compromise of sensitive data. Encryption of the data on the handset, while not unbreakable, can certainly help keep information out of the hands of all but the most skilled cryptologists.

**VPN** - VPNs, Virtual Private Networks, provide both connectivity and security for devices operating over public networks. With the increased use of both public and private internet access over WiFi and similar IP-based networks, the risks associated with unencrypted data traffic increase. Indeed, traffic going over WiFi and the Internet is subject to being sniffed by a variety of means, which can expose data left in plain text. VPNs, while providing access to enterprise resources, also ensure that traffic is encrypted end-to-end, limiting the risks of interception.

**About Mossec** - Mossec was launched by recognized experts in the Spanish security market, with a strong track record in security software for the Spanish government. The company develops a complete set of security applications for mobile devices. It is supported by Venture Capital & public government funding, contributing with credibility and financial stability. For more on Mossec, please see the Mossec website.



**Contact** - For more information, please call +1 408.962.9200 or email us at [websales@innopath.com](mailto:websales@innopath.com).