

MDM is not Security

“Disruption” at the Mobile Security Pavilion and Theater - RSA 2012

Atlanta, GA Feb. 14th, 2012 - Many enterprises in the private and government sectors, initially under the belief that MDM alone would solve their mobile enterprise security needs, have discovered the painful truth: MDM is not security.

They are now experiencing the cost and pain of dismantling their previous MDM products in favor of truly secure and comprehensive mobile MDSM (Mobile Device Security Management) suites.

At the annual RSA Conference held in San Francisco from Feb. 27th – March 1st 2012, watch for the “**disrupters**”; security technologies that are ahead of the curve, providing leading edge solutions to problems and issues many companies have not anticipated, realized or experienced yet.

But that’s what Security Disrupters do. Think ahead; plan ahead – far ahead of mainstream companies such as an incredible demonstration to be put on by Mobile Active Defense (SC Magazines’ 2011 Innovator of the Year in Mobile Device Protection) and AirPatrol (2011 InformationWeek Magazine’s Top 10 Mobile Security Vendors to Watch). For the first time in a public forum – mobile policy enforcement (firewall and filtering rules, for example) is so incredibly granular, that iPads and iPhones will automatically have their policies change as attendees move throughout the booth from one policy zone to another.

AirPatrol calls this Cognitive Mobile Security and MAD (Mobile Active Defense) calls it Geo-Location Based Policy Enforcement. In short, the demonstration shows the capabilities of a mobile device to morph and adhere to changing security policies based on the physical location of the device.

Whichever term you prefer, the two company’s integrated technologies is a game-changer for companies who really care about securing their mobile enterprise – and have, like so many others, realized or discovered the hard way, MDM is not security.

Healthcare cares because doctors and nurses need different policies on their mobile devices to comply with HIPAA and other regulatory guidelines. Same thing for the financial sector. The government and military care because there may be several sets of policy guidelines to be applied throughout the Pentagon and another set while traveling. Military personnel in various areas of their commands must restrict data access due to



security (red zone vs. green zone) – and now their policies can be applied to any of their mobile devices.

This functionality is a breakthrough for every industry and is a Disrupter for companies who are battling with BYOD issues.

The Mobile Security Pavilion & Theater (Booth 2247) will host the strongest set of mobile security tools and techniques available from real security companies offering real mobile security solutions for the enterprise.

Throughout each day, the Mobile Security Pavilion & Theater will present non-stop relevant, non-product presentations covering the mobile security issues every enterprise cares about.

- Hardware-Based Mobile Secure Voice for Blackberry, iOS and Android
- Total Mobile Enterprise Security & Compliance
- Secure (not MDM) BYOD Solutions
- Mobile Security Awareness Training for the Enterprise
- Mobile Enterprise MSSP and SIEM
- Mobile Malware Detection
- Mobile Firewall, Content Filtering & Email Security
- Granular Location-Based and Context-Aware Mobile Policy Enforcement
- Mobile Crypto and IPsec VPN (not just SSL)
- Mobile App Protection
- Hostile Threat Remediation

For more information on the scheduled events, presentations or demo's contact:

jbaumann@mobileactivedefense.com

About MAD: M.A.D. provides the MECS Solution globally to Enterprises and Government Agencies to secure smartphones and tablet devices to the utmost and stringent security and compliance standards available in the industry today. The award winning MECS Server Solution is the flagship product made by M.A.D., The Smartphone Security Company.
<http://www.mobileactivedefense.com>