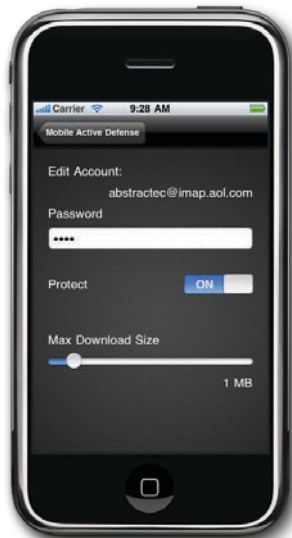


The 'Last Mile' is all too often a congested and troublesome bottleneck for mobile communications. It's no wonder that it has become such a sore point for many carriers, businesses, and subscribers. Here are some facts we know:

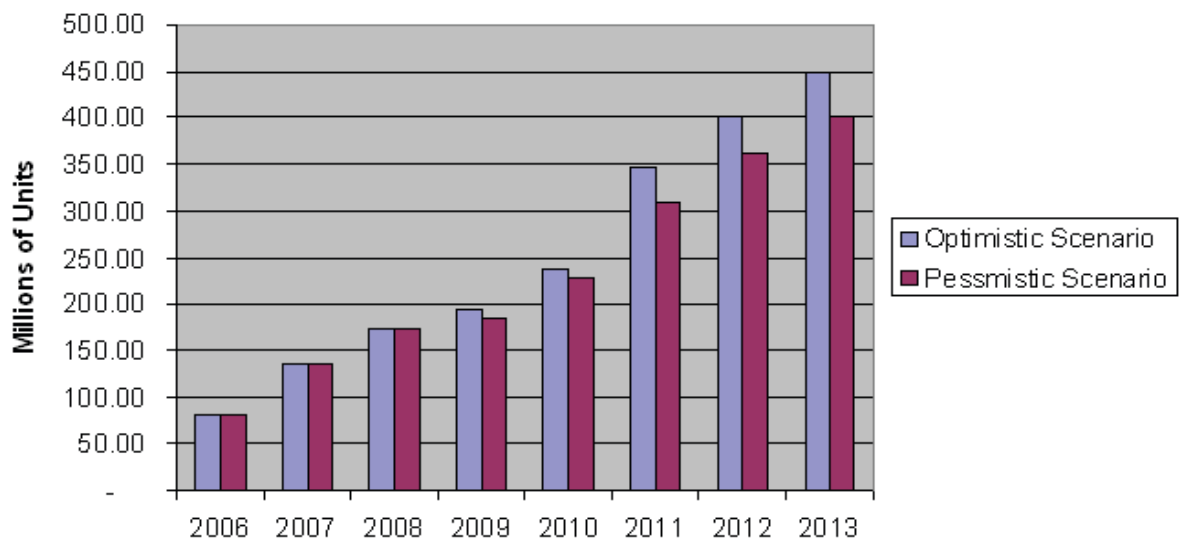
- 74 Trillion pieces of junk email (2009)
- 81-97% of email is spam, ads or malware
- 4.6 Billion mobile devices 2009
- By the end of 2009, 600 million of the world's 4.6 Billion mobile subscribers connected to the Internet used broadband technology.
- Mobile phones will overtake PCs as the dominant web access device worldwide by 2013
- 1.82 Billion smart phones and 1.72 Billion laptops by 2013
- Largely non-technical users and an inherently insecure infrastructure.

Currently the Last Mile is filled with vast amounts of spam, phishing, viruses, adware, malicious software and other uninvited or undesired content. Delivering this vast amount of junk email to the mobile endpoint creates problems for everyone in the communications chain.

- Overloading the Last Mile creates a poor user experience, bad carrier image, dropped calls, and gives subscribers a reason to switch carriers.
- Non-technical users must learn how to protect themselves.
- Smart phones do not lend themselves to security as we have practiced it for 30+ years.
- Delivering 81-97% junk email in the Last Mile is tremendously expensive for the carrier.



iSuppli Figure: Global Smart Phone Unit Shipment Forecast (Millions of Units)



With Mobile Active Defense (M.A.D.) Carrier Edition, problems disappear:

- The carrier reclaims significant amounts of bandwidth in the Last Mile. Our current analysis shows that we filter an additional 40-43% of the email from ever touching the Last Mile or the subscriber's device.
- The carrier does not need to become involved in the security process. M.A.D. Carrier Edition is automatic and transparent to the carrier and the subscriber.
- The subscriber's inbox no longer receives phishing attacks, spam, viruses or hostile software – automatically with no active involvement.
- Large attachments can be filtered before ever reaching the mobile endpoint.

Typical security methods are inadequate and ineffective in the smart phone and mobile environment:

- They require users to have technical skills and become actively involved in the security process.
- They require the smart phone to host software applications to perform the filtering and the 'heavy lifting'.
- They do not alleviate any load on the Last Mile.
- They use up even more bandwidth on the Last Mile, compounding the problem.



Key features of Mobile Active Defense Carrier Edition

- Keeps the unwanted traffic off the Last Mile - saving money and increasing the number of users that can be supported.
- Filters emails for viruses, malware, and spam.
- Prevents phishing attacks by removing them before they reach your users.
- Deletes messages that are too large before being downloaded drastically lowering bandwidth usage.
- Does NOT slow down the smart phone.
- Works with existing smart phone email applications.
- Mobile Active Defense gets updated over 100 times a day to keep you safe from the newest threats.
- Automatically imports all of existing email server configuration information from the phone with no need to retype complicated server information.
- Supports POP3 and IMAP email accounts.
- No limit to the number of email accounts that can be protected.
- Works with all leading online email services including Gmail, Yahoo, and AOL.
- Exchange support coming in 2010.
- Requires no technical background to install and configure. Grandma can do it!

M.A.D. Mobile Enterprise Compliance & Security (MECS) Server

The MECS Server offers your customers *best-in-class* smart phone security, privacy and compliance:

- Expand traditional IT networks to your mobile offerings
- Generate additional revenues through enhanced services to your customers:
- Single policy driven compliance and management tool that puts all non-BlackBerry mobile devices under one administrative control.
- Does not require any change to existing IT infrastructure and can be implemented in hours using the customer's existing security policy.
- Allows enterprise to safely expand its mobile infrastructure in hours – not months. Simple and rapid deployment.
- Maintains compliance.
- Some customers call Mobile Active Defense, “BES for the iPhone, only simpler.”
- Operates hosted in your carrier cloud, ideal for SMEs, or non-hosted in the customer's cloud, which larger customers are currently doing with BlackBerry BES.
- Managed or unmanaged administrative services.

Subscribers and Mobile Active Defense (M.A.D.)

Mobile Active Defense combines the best of Enterprise grade spam, phishing, malware and virus protection without running software on the smart phone.

- Subscribers' emails are screened before they ever reach the expensive Last Mile.
- This lowers cost by allowing carriers to support more subscribers while delivering only the pure email that users want.
- Mobile Active Defense functions with existing smart phone email applications to make user support simple.
- We perform over 100 updates every day without any intervention from the user or the need to download anything to their phone. This ensures that they always have the latest protection available against the newest threats and that the latest scams are caught before being sent to the phone.
- Mobile Active Defense can be up and running for your users in less than 5 minutes time. Simply preinstall the Mobile Active Defense Controller Application to that smart phone before it is sent to the user. The user can also download and install the software if prior installation is not possible. The user runs the application.
- The application will import all of the user's existing email configurations so that they do not have to retype technical server information. Then, they simply tell Mobile Active Defense which of their email accounts they want to protect. We do the rest.

M.A.D. uses Zero Footprint Security

- Does not slow down the smartphone.
- Does not use valuable memory.
- Does not use storage space other than the small app and help videos.
- Does not use any CPU resources.
- Does not use costly bandwidth to keep your smartphone current with the latest security updates.

For full details on the M.A.D. MECS Server, contact M.A.D. Partners at: 1.877.halo.mad (425 6623) and visit www.MobileActiveDefense.Com

A small configuration app is installed on each smartphone in the Enterprise. The M.A.D. client employs Zero Footprint Security for these platforms.

- iPhone/iTouch/iPad (OS3, iOS4)
- Windows Mobile
- Android
- Nokia Symbian



Copyright 2010, M.A.D. Partners, LLC. All rights reserved. Mobile Active Defense and M.A.D. logos and trademarks are property of M.A.D. Partners, LLC. Other product names and trademarks, may be trademarks of their respective owners. M.A.D. Partners, LLC does not accept any liability for errors or omissions in these specifications, which may be subject to change without notice.