Mobile Security Solutions & Architecture Design

Overview

Mobile Security Solutions & Architecture Design facilitates the expansion of an organization's mobile / Bring Your Own Device (BYOD) goals by planning, designing and constructing a secure conduit to enhance current business objectives and to expedite new ones. Our security engineers are very well-versed in a variety of security technologies: Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Data Loss Prevention (M-DLP), Mobile Data Management, Mobile Payments, and more. Our specialists work towards increasing business performance and reducing risk to create a secure foundation for mobile business.

Benefits

Emagined Security can help you design and implement a mobile security solution so you are assured the highest level of protection for your corporate and personal mobile assets. Emagined Security is a one-stop shop in offering a complete security architecture solution from design to implementation.

Emagined Security can help you address security risks such as the following:

- Secure Rapid Development
  - Explosion of new technologies that increase the "connectivity" are on the rise
  - Mobility vendors (e.g., MDM) ability to adapt to changing technologies & Applications
  - Adoption programs can't assess every device / application being released in the wild

- Device / Network Security
  - Ensuring security of multiple device types and operating systems is an growing issue
    - — Authentication
    - — Encryption
    - — Patching
    - — Malware
    - — Vulnerability Management
    - — Guest Access
    - — Etc.

- Enterprise Data Management
  - Sensitive data is located personal devices and are being removed from the corporate environment
    - — Data Protection
    - — Legal Hold
    - — Data Backup & Retrieval
    - — Data Removal

- Data Segregation
  - Both personal and corporate sensitive data is located personal devices
    - — Segmented Data Ownership
    - — Segmented Data Access
    - — Legal & Compliance Responsibilities

- Data Loss Protection
  - Protection of data is difficult when the device is no longer onsite or under the corporate protection
    - — Data Forwarding
    - — Corporate Responsibility for Personally Identifiable Information (PII)

Once we have gathered the relevant information, Emagined Security will provide you with a detailed report outlining the requirements for building a secure mobile solution. Once we determine the proper design to fit your needs, we will assemble a team of experts to design, implement, and test security solutions for your networks and systems.

Description of Service

The following table presents Emagined Security's eight-phase methodology for Mobile Security Solutions & Architecture Design development:

Phase	Description
1	Requirements gathering / discovery
2	Requirement analysis
3	Solution recommendation
4	Solution development and lab testing
5	Information technology design & documentation
6	Implementation and rollout
7	Vulnerability testing
8	Training

Details of the first three phases are as follows:

Phase 1 - Requirements Gathering / Discovery

Requirements are gathered and reviewed using any combination of the following methods:

- Review existing documentation
- Listen to presentations by the project initiators
- Lead discussions by asking relevant questions about the intended uses of the tool

Participants for these meetings are generally approximately 10-12 individuals representing the following functions:

- Business and system owners – representatives from business units with anticipated uses for the tool
- Corporate information security management
- Administrators of systems that the tool will need to interface with
- Risk management personnel, as appropriate
- Other associated personnel

The identified requirements are then grouped into categories such as the following:

- General
- Technical Requirements

- Technical Architecture
- Support Services
- Financial Analysis

Following this categorization, the requirements are assigned weightings based upon importance. Importance weightings are based on the following levels of importance and each level is assigned a point value.

Importance	Point Value
Mandatory	5
Important	4
Desired	3
Nice to have	2
Optional	1

Depending on the number of mandatory requirements, products may not satisfy all mandatory requirements: the competing products are therefore scored based on their ability to meet the most number of mandatory requirements.

Phase 2 – Product / Solution Identification

Products are identified that appear to meet the requirements. Depending on the number of products in the space, a shortlist is created usually based on analyst reports (e.g., it may be decided that only products rated as "Positive" or better in the latest Gartner MarketScope or Magic Quadrant). The products are chosen specifically taking into account the needs in the following areas:

- Hardware - based on internally supported systems
- Software compatibility - with identified products
- Availability of service - redundancy
- Class of products - meets requirements
- Automation - ability to automate processes

Phase 3 - Solution Recommendations

During this task, the identified requirements and the results of the requirements analysis are evaluated to determine the appropriate recommendations. The potential solutions are assessed while taking into consideration the requirements and their importance. This is performed in the following steps:

- Step 1 – Solution Mapping to Mandatory Requirements
- Step 2 – Solution Elimination Based on Mandatory Requirements
- Step 3 – Residual Solution Mapping to the Remainder of Identified Requirement
- Step 4 – Solution Score Calculations Using Importance Weighting
- Step 5 – Solution Recommendations and Write-up

Step 1 – Solution Mapping to Mandatory Requirements

Each solution provider is asked to respond to a questionnaire comprising the mandatory requirements from the overall list of requirements and to identify what functionality was available out-of-the-box and what would require customization (e.g., setting up an ODBC connection and mapping fields, using a Web services API, or even importing from Excel) by answering "Yes" or "No" for each requirement.

Step 2 – Solution Elimination Based on Mandatory Requirements

The solution providers are shortlisted based on their responses to the mandatory requirements questionnaire by totaling the number of "Yes" responses. The resulting scores are evaluated and the top three or four solution providers are selected to continue in the process.

Step 3 – Residual Solution Mapping to the Remainder of Identified Requirement

Each shortlist solution providers is asked to respond to a questionnaire containing all of the requirements and to identify what functionality was available out-of-the-box and what would require customization (e.g., setting up an ODBC connection and mapping fields, using a Web services API, or even importing from Excel) by answering "Yes" or "No" for each requirement. They are also asked to provide cost estimates projected out over three years including:

- License Fees
- Hardware Fees (estimate of equipment required to support the needed infrastructure)
- Yearly Software Maintenance Fee

- Installation Fees (to make operational)
- Ongoing Configuration Fees (to configure operations)

Step 4 – Solution Score Calculations Using Importance Weighting

The responses to the questionnaires are scored based on the "Yes" responses and the weighting of the required. The detailed responses are tabulated by category and total and the solution providers are ranked on score. In addition to this scoring model, the solution providers are ranked based on the cost estimates provided for the high-level scope scenario.

Step 5 – Solution Recommendations and Write-up

Based on the analysis of the residual requirements and the cost estimates provided by the solution provider, a final ranking is prepared based on the combination of ability of each solution to meet the requirements balanced by the costs.