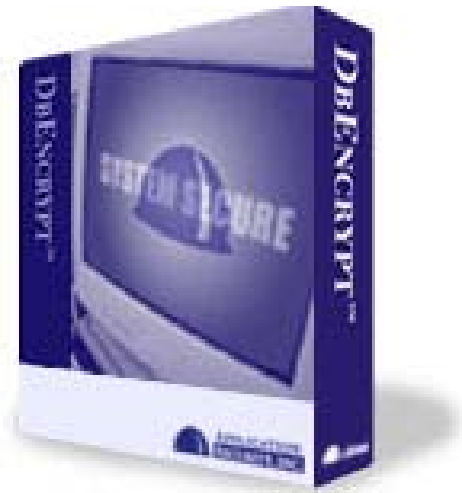

DbEncrypt &

Application Security, Inc.

Product and Company Briefing

APPLICATION SECURITY, INC.

www.AppSecInc.com

Agenda

- **There is a problem…**
  - Main Problem
  - Existing Solution Shortcomings
  - More Granular Industry Problems
- **There is a solution…**
  - ASI's DbEncrypt
  - Who Benefits? How? Why?
  - Key Technology Differentiation
- **There is a way… and a plan…**
  - What's included?
  - Our Organization, Current Position and Future Plans

Main Problem

- The prevention of unwanted users or personnel from viewing data ("data-at-rest")
  - Outside Intrusions
  - Internal Personnel
  - Administrative Personnel
    - Database Administrators
    - System Administrators
    - General Administrators

Existing Solutions

- Security and Data Protection Solutions
  - Existing security solutions do not address this "main problem"
    - Vulnerability Assessment, IDS, Firewalls, Single Sign-On
  - Backup Solutions
    - Provides protection for "off-line" data
- Existing Encryption Solutions
  - Existing Data Encryption ("data-in-transit")
    - SSL, PKI, etc.

Database Security

- Non-existent controls and mechanisms
  - Nothing preventing unwanted personnel or even the DBA from seeing data
- Traditional Database Security Concepts Do Not Apply in Today's World
  - Access Control and Permissions
- Database Vendor Encryption Solutions
  - Oracle's DBMS_OBFUSCATION_TOOLKIT

More Granular Industry Problems

- **Service Provider** & **E-Business** in General (ASPs, ISPs, MSPs, and Internal / External Systems)
  - Providing the data security guarantee
  - Overcoming customer and partner fears
  - Establishing accountability for data security

More Granular Industry Problems

- Regulatory Requirements
  - VISA CISP
    - Requirement #3: Encrypt Stored Data
      - Minimum account information to be encrypted is the Visa account number and expiration date
  - Gramm-Leach-Bliley Act
    - Interagency Guidelines (Manage & Control Risks)
      - Encryption of electronic customer information in transit or in storage
    - TITLE V – PRIVACY
      - Subtitle A – SEC. 501 PROTECTION OF NONPUBLIC PERSONAL INFORMATION

DbEncrypt is the answer

- **Main Problem**:
  - The prevention of unwanted users or personnel from viewing data ("data-at-rest")
- **Answer**:
  - A flexible infrastructure designed to encrypt data stored in the tables of a database.

DbEncrypt Key Features

1. Database Column and Row-Level Encryption
2. Access to world-class security resources that facilitate effective data protection
3. Controls and mechanisms providing authentication, encryption, and data integrity

APPLICATION SECURITY, INC.

www.AppSecInc.com

Purpose Behind DbEncrypt

- DbEncrypt can be utilized in two ways:
  1. Turnkey solution to automatically / transparently encrypt data in columns and rows
  2. As a low-level API providing cryptographic algorithms for PL/SQL developers

1. Turnkey solution…

- **Who benefits?:**

  Database Administrators (DBAs) and Developers that **do not want to bother with the details** – transparent encryption functionality

- **How do they benefit?:**

  Point-and-click on columns and tables to…

  - Encrypt Data
  - Create triggers and views to transparently encrypt/decrypt data
  - Manage the encryption keys

APPLICATION SECURITY, INC.

www.AppSecInc.com

2. Low-Level API…

- **Who benefits?:**

  Database Administrators and Developers that wish to **build their own encryption systems** utilizing the API features

- **How do they benefit?:**
  - PL/SQL Programmers to use encryption as they see fit
  - Provides developers with the ability to write proprietary encryption systems

DbEncrypt Technology

- Shared library
  - DbEncrypt.dll (Windows)
  - Libdbencr.so (UNIX)

DbEncrypt Technology

- Encryption Algorithms
  - Complete list at: http://www.appsecinc.com/products/dbencrypt/algorithms.html
  - 25 of the strongest and most widely analyzed algorithms
    - RSA
    - DES
    - AES
    - RC4
    - MD5
    - SHA-1
    - Blowfish
    - Twofish

DbEncrypt's Position in the Market

- Complementary to Existing Solutions
- Competitive and Differentiation Features
  - Built-In Database Features
    - DBMS_OBFUSCATION_TOOLKIT (Oracle)

DbEncrypt's Position in the Market

DbEncrypt™	DBMS_OBUSCATION_TOOLKIT
25 Algorithms Including Public Key and Symmetrical Key Algorithms, Hashing Functions, Stream Cipher, and Block Cipher	DES and MD5
Variable Length Keys for Customization of Strength and Speed	56, 112, and 168 bit restrictions
GUI that provides you the ability to create working code examples	Undocumented and Poorly Implemented
Granular encryption functionality providing a choice of block modes, initialization vectors, and key lengths	CBC Mode
Encryption of NUMBER, VARCHAR, CHAR, and LOB data types	Encryption of VARCHAR data types
Strong Random Number Generator	No method to generate random numbers

Availability and Price

- Evaluation Copies Available for Download:
  - http://www.appsecinc.com/downloads/
- Updates are easily downloadable from:
  - http://www.appsecinc.com/downloads/

APPLICATION SECURITY, INC.

www.AppSecInc.com

DbEncrypt Future Plans

- Expanded Database Platforms
  - Microsoft SQL Server
  - IBM DB2/UDB
- Features within the Next Version of DbEncrypt
  - Increased integration with the current DBMS_OBFUSCATION_TOOLKIT
  - Increased number of algorithms
  - Fine-grained functionality
    - i.e. allowing the user to set initialization vectors
  - Java version of the library

Who is Application Security, Inc.

- Unique Position and Background
  - SHATTER focuses on database, groupware, web, and ERP applications
    - Encryption
    - Penetration Testing/Vulnerability Assessment
    - Intrusion Detection
- Where ASI is Heading

APPLICATION SECURITY, INC.

www.AppSecInc.com

Proposed Product Family Suite

- Database Encryption
  - DbEncrypt for Oracle
  - DbEncrypt for Microsoft SQL Server
- Pen Test / Vulnerability Assessment
  - AppDetective for Oracle
  - AppDetective for Microsoft SQL Server
  - AppDetective for Lotus Notes/Domino
  - AppDetective for Microsoft Exchange
- Intrusion Detection
  - AppRadar

Wrapping Up…

- **The problem…**
  - Main Problem
  - Existing Solution Shortcomings
  - More Granular Industry Problems
- **The solution…**
  - ASI's DbEncrypt
  - Who Benefits? How? Why?
  - Key Technology Differentiation
- **The way… and the plan…**
  - What's included?
  - Our Organization, Current Position and Future Plans