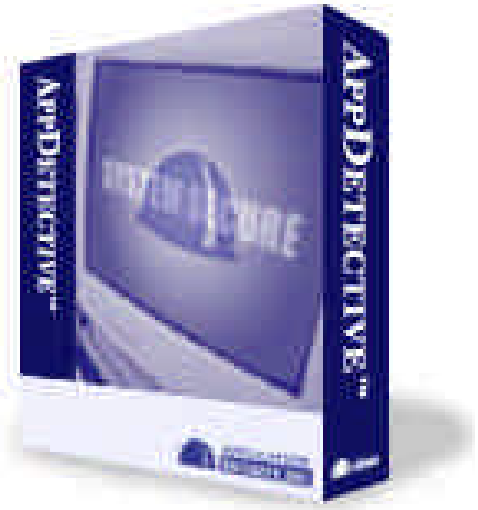


AppDetective

for Microsoft SQL Server

Product Briefing

APPLICATION SECURITY, INC.

www.AppSecInc.com

AppDetective™ Briefing Agenda

- **There is a problem…**
  - Database Security Problems
    - In General
    - Industry Requirements and Regulations
- **There is a solution…**
  - AppDetective™ Capabilities
    - Key Technology Feature Differentiation
    - Who Benefits? How? Why?
  - Requirement and Regulation Compliance
    - Financial Services, Health Care, and E-Commerce
- **There is a way… and a plan…**
  - What's included?
  - Our Organization, Current Position and Future Plans

Database Security Problems

- Inability to Effectively Inventory and Identify Databases
- Database Vulnerabilities and Threats are Easily Exploitable and are Growing Every Day
- Database Vulnerabilities and Threats Endanger Trusted Systems
  - Host Operating Systems
  - Network Operating Systems
  - Web Servers/Applications

Database Security Problems

- Database security problems directly affect how organizations are able to fulfill industry requirements such as the following:
  - VISA CISP (Cardholder Information Security Program)
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability Accountability Act (HIPAA)

Existing Security Solution Shortcomings

- Security Management / Policy Compliance
  - Agent Based
  - Mainly Configuration Settings Management and Policy Compliance Solutions
- Vulnerability Assessment
  - Many Solutions Do Not Check the Database Security Subsystem Level
  - Require Administrative-Level Privileges
  - Require Lengthy Connection Configuration Procedures
- Latest Versions and Vulnerabilities
  - Organizations aren't necessarily dedicated to security vulnerabilities and threats on this level

AppDetective™ is the Answer

- AppDetective™ for Microsoft SQL Server Empowers Organizations with the Following Capabilities:
  1. Database Discovery and Identification
  2. Penetration Testing
  3. Security Audit
  4. Reporting Facilities
  5. Complimentary and Compatible
  6. Extensive and Updated Library of Vulnerabilities and Misconfigurations

APPLICATION SECURITY, INC.

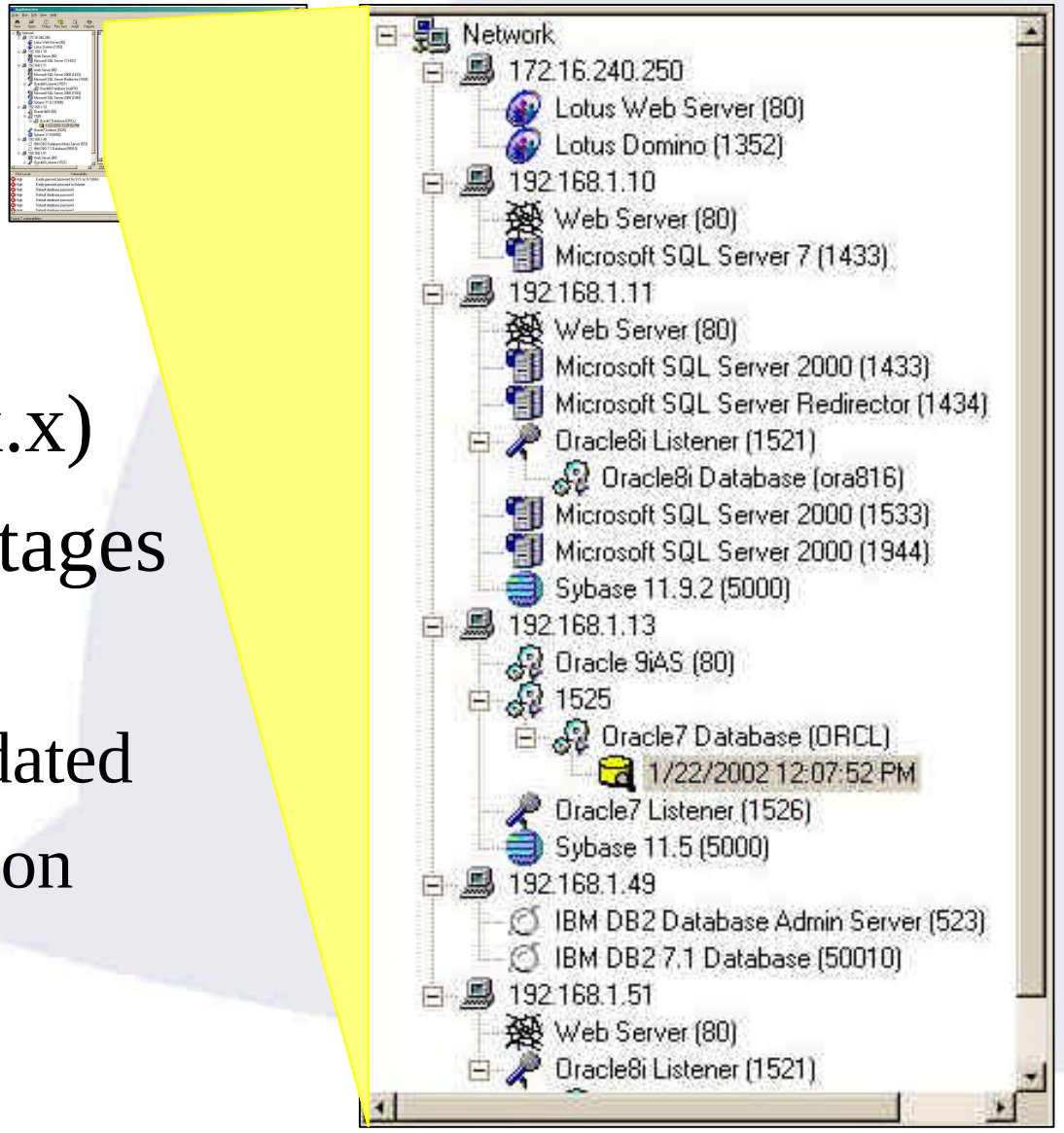
www.AppSecInc.com

AppDetective™ is the Answer

- AppDetective™ for Microsoft SQL Server Empowers the Following Individuals:
  - Security Practitioners
  - Internal Auditors
  - General System Administrators
  - Database Administrators

1. Discovery and Inventory

- Scanning
  - IP Number
  - Port Number
  - Version (x.x.x.x)
- Scanning Advantages
  - Accurate
  - Continually Updated
  - NMAP Integration

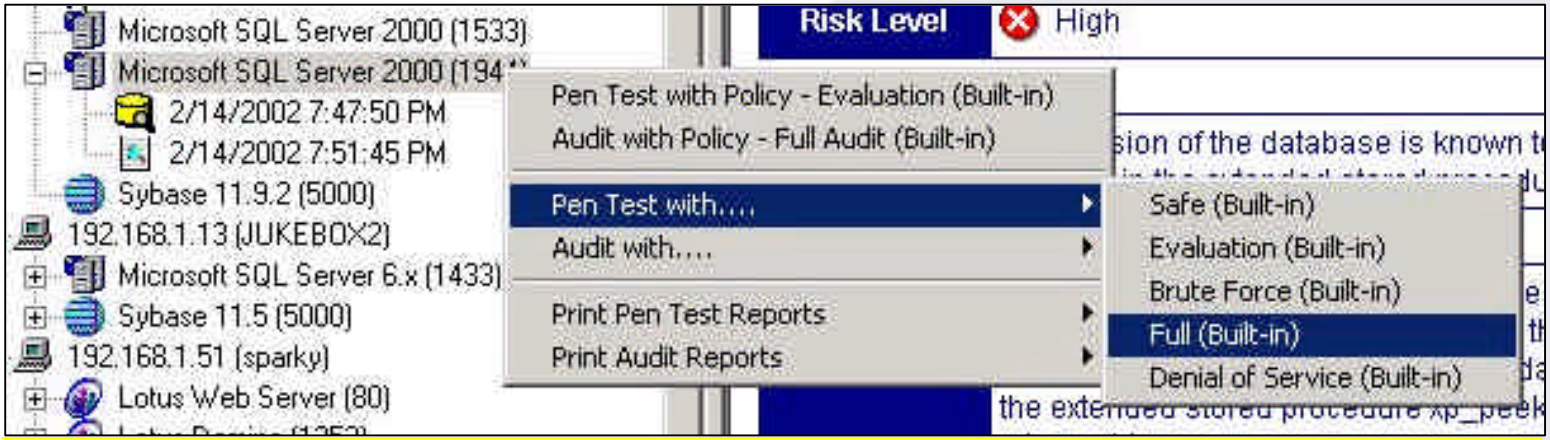


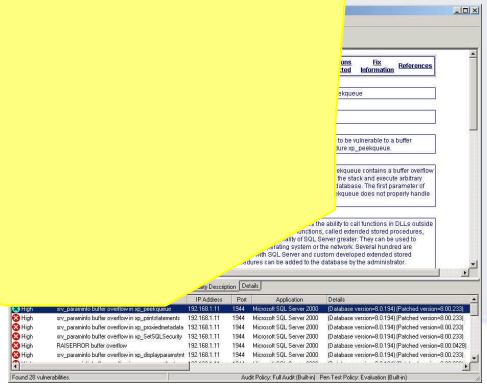
2. Penetration Testing

- Pen Test™
  - True “Zero Knowledge” and non-intrusive penetration techniques are utilized – as simple as:
    1. Discover the database through a Scan
    2. Right-clicking on the selected database
    3. Selecting “Pen Test” from the provided menu
  - All checks are performed externally without elevated privileges
  - Target database is not affected

2. Penetration Testing

- Pen Test™
  - True “Zero Knowledge” and non-intrusive penetration techniques are utilized





2. Penetration Testing

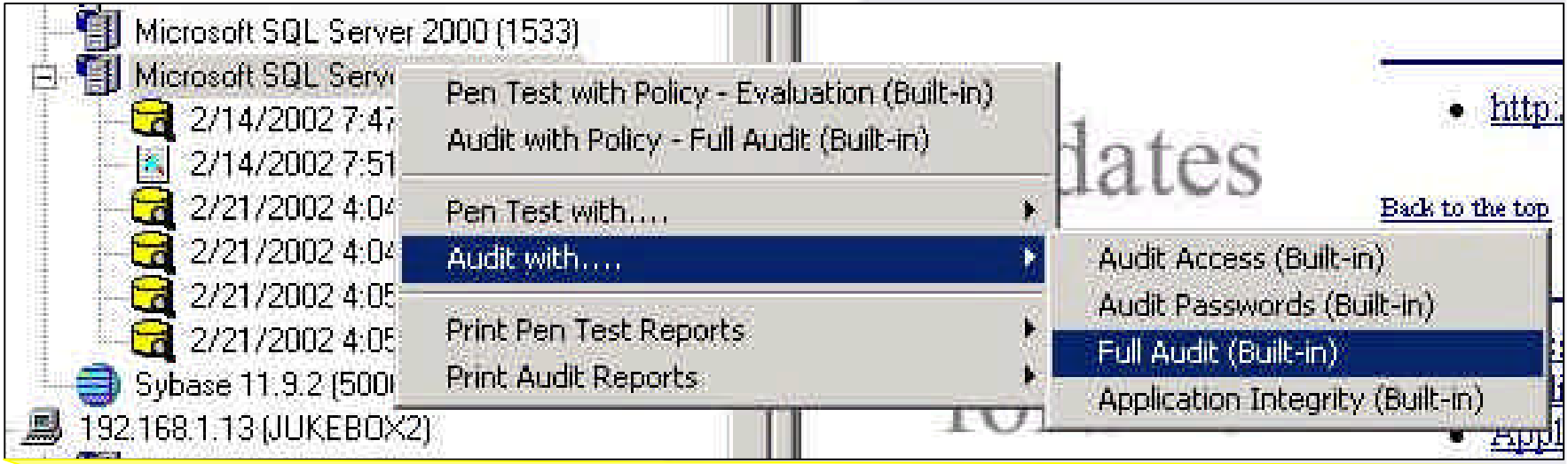
- **Pen Test™ Categories**
  - Denial of Services (DoS) Attacks
    - Examples: Malformed RPC request DoS, Malformed TDSpacket header, etc.
  - Misconfigurations
    - Examples: SQL Server Authentication
  - Password Attacks
    - Examples: Blank, Default, and Easily Guessed Passwords
  - Vulnerabilities
    - Examples:Clear text passwords, Escalated privileged in heterogeneous joins, buffer overflows, etc.

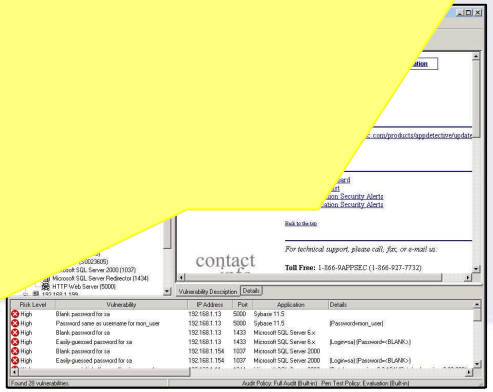
3. Security Auditing

- Security Audit Advantages
  - Provides an “Inside-out” approach to auditing the security of your database
  - Examine how an unauthorized user can obtain elevated privileges or circumvent security controls from the inside
  - Automatic configuration upon discovery

3. Security Auditing

- Security Audit





APPLICATION SECURITY, INC.

www.AppSecInc.com

3. Security Auditing

- **Security Audit Categories**
  - Access Control
    - Examples: Temporary stored procedures bypass permissions
  - Identification/Password Control
    - Examples: Clear-Text, Default, and Easily Guessed Passwords
  - Application Integrity
    - Examples: Denial of Service Checks, Buffer Overflows, Configuration Settings

4. Reporting Facilities

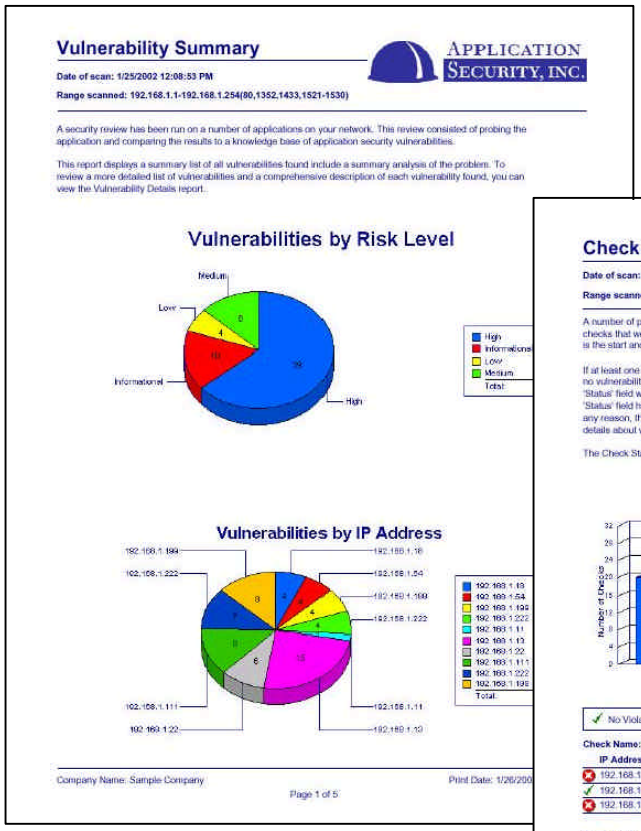
- **Report Generation Facilities**
  - Policy Reports
  - Summary Reports of the Tests Performed
  - Detailed Reports of the Tests Performed
  - High-Level Overview and Detailed Overview of Found Vulnerabilities
  - Recommendations and Fix Information
- Report Generation Advantages
  - Report on Servers Across Your Network

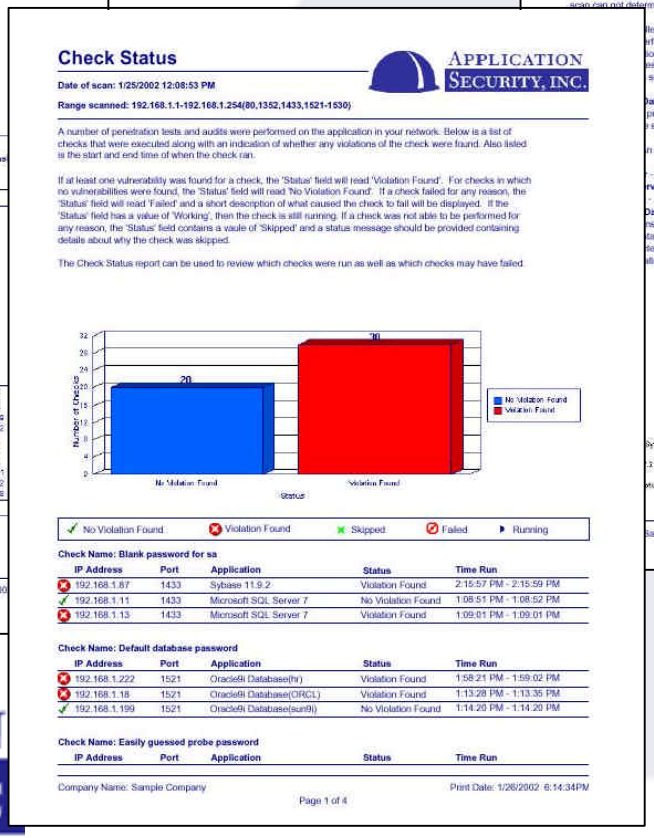
APPLICATION SECURITY, INC.

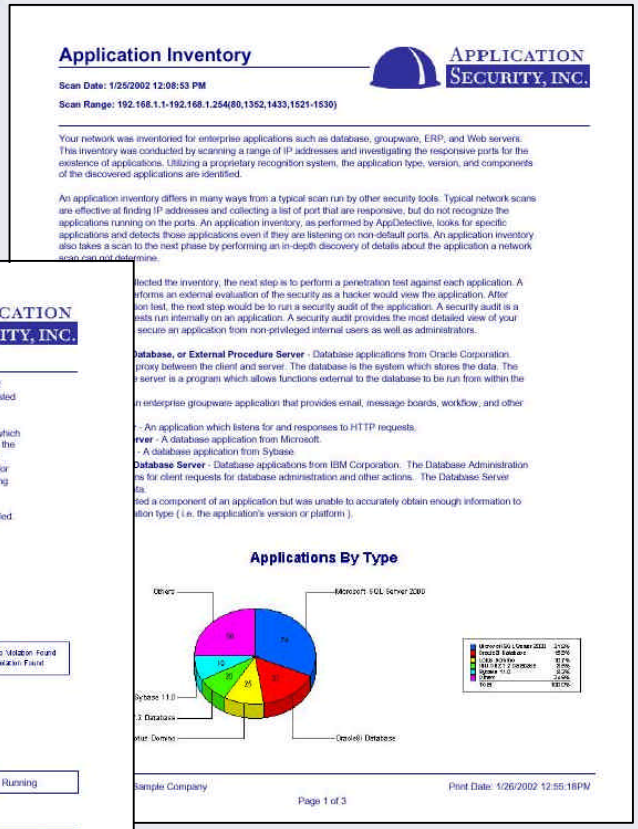
www.AppSecInc.com

4. Reporting Facilities

- **Reporting Examples**







APPLICATION SECURITY, INC

www.AppSecInc.com

5. Complimentary and Compatible

- **AppDetective essentially picks up where all of the following leave off:**
  - **Network and Host Operating System Scanners**
  - **Port Scanners**
  - **Other “Database” Scanners**

6. Vulnerabilities and Misconfigurations

- **Databases**
  - Oracle, Microsoft SQL Server, IBM DB2, Sybase, and MySQL
- **Groupware**
  - Lotus Notes/Domino and Microsoft Exchange
- **ERP**
  - SAP R/3, PeopleSoft, CRM
- **Key Industry Advantage**
  - **Application Security, Inc. concentrates its entire R&D to the security, protection, and defense of applications.**

AppDetective™ Fulfilling Requirements

- AppDetective™ capabilities provide organizations with a way to fulfill industry requirements in the following:
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability Accountability Act (HIPAA)
  - VISA CISP (Cardholder Information Security Program)

AppDetective™ and the GLBA

- Gramm-Leach-Bliley Act (GLBA)
- TITLE V – PRIVACY
  - SEC. 501 PROTECTION OF NONPUBLIC PERSONAL INFORMATION
  - SEC. 505 (b) ENFORCEMENT OF SECTION 501.
- Interagency and NCUA Standards for Safeguarding Objectives and Guidelines

APPLICATION SECURITY, INC.

www.AppSecInc.com

AppDetective™ and the GLBA

AppDetective™ Capabilities

- Inventory and Identification
- Penetration Testing
- Security Audit
- Reporting Facilities
- Extensive and Updated Library of Application Vulnerabilities and Misconfigurations

Interagency and the NCUA Guidelines

B. Assess Risk

C. Manage and Control Risk

D. Oversee Service Provider Agreements

E. Adjust the Program

F. Report to the Board

APPLICATION SECURITY, INC.

www.AppSecInc.com

AppDetective™ and HIPAA

AppDetective™ Capabilities

- Inventory and Identification
- Penetration Testing
- Security Audit
- Reporting Facilities
- Extensive and Updated Library of Application Vulnerabilities and Misconfigurations

Administrative Procedures

- Certification
- Contingency Plan
- Information Access Control
- Internal Audit
- Personnel Security
- Security Configuration Management
- Security Incident Procedures
- Security Management Process
- Termination Procedures
- Training

APPLICATION SECURITY, INC.

www.AppSecInc.com

AppDetective™ and HIPAA

AppDetective™ Capabilities

- Inventory and Identification
- Penetration Testing
- Security Audit
- Reporting Facilities
- Extensive and Updated Library of Application Vulnerabilities and Misconfigurations

Technical Security Services

- Access Control
- Audit Controls
- Authorization Controls
- Data Authentication
- Entity Authentication

APPLICATION SECURITY, INC.

www.AppSecInc.com

AppDetective™ and Visa CISP

AppDetective™ Capabilities

- Inventory and Identification
- Penetration Testing
- Security Audit
- Reporting Facilities
- Extensive and Updated Library of Application Vulnerabilities and Misconfigurations

Visa CISP Requirements

1. Install and maintain a working firewall to protect data accessible via the Internet
2. Keep security patches up to date
6. Restrict access to data by business need-to-know.
7. Assign a unique ID to each person with computer access to data.
8. Do not use vendor-supplied defaults for system passwords and other security parameters
9. Track all user access to data by unique ID
10. Regularly test security systems and processes
11. Administrative Data Security

APPLICATION SECURITY, INC.

www.AppSecInc.com

Availability

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

AppDetective™ Future Plans

- Expanded Database and Groupware Platforms
  - Oracle
    - http://www.appsecinc.com/products/appdetective/oracle/
  - Lotus Domino
    - http://www.appsecinc.com/products/appdetective/domino/
  - Sybase
    - http://www.appsecinc.com/products/appdetective/sybase/
  - IBM DB2
    - http://www.appsecinc.com/products/appdetective/db2
  - MySQL
  - Microsoft Exchange

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 Application Security, Inc. (ASI) is Heading
  - Develop security solutions providing "protection where it counts"

APPLICATION SECURITY, INC.

www.AppSecInc.com

Proposed Product Family Suite

- Database Encryption
  - DbEncrypt™
    - Oracle | SQL Server
- Pen Test / Vulnerability Assessment
  - AppDetective™
    - Lotus Domino | Microsoft SQL Server | Sybase | Microsoft Exchange | IBM DB2/UDB | MySQL
- Intrusion Detection
  - AppRadar™ (Coming Soon)

APPLICATION SECURITY, INC.

www.AppSecInc.com

Wrapping Up…

- **There is a problem…**
  - Database Security Problems
    - In General
    - Industry Requirements and Regulations
- **There is a solution…**
  - AppDetective™ Capabilities
    - Key Technology Feature Differentiation
    - Who Benefits? How? Why?
  - Requirement and Regulation Compliance
    - Financial Services, Health Care, and E-Commerce
- **There is a way… and a plan…**
  - What's included?
  - Our Organization, Current Position and Future Plans

APPLICATION SECURITY, INC.

www.AppSecInc.com