

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



**APPLICATION
SECURITY, INC.**

www.AppSecInc.com

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



**APPLICATION
SECURITY, INC.**

www.AppSecInc.com

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)



APPLICATION
SECURITY, INC.

www.AppSecInc.com

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



**APPLICATION
SECURITY, INC.**

www.AppSecInc.com

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

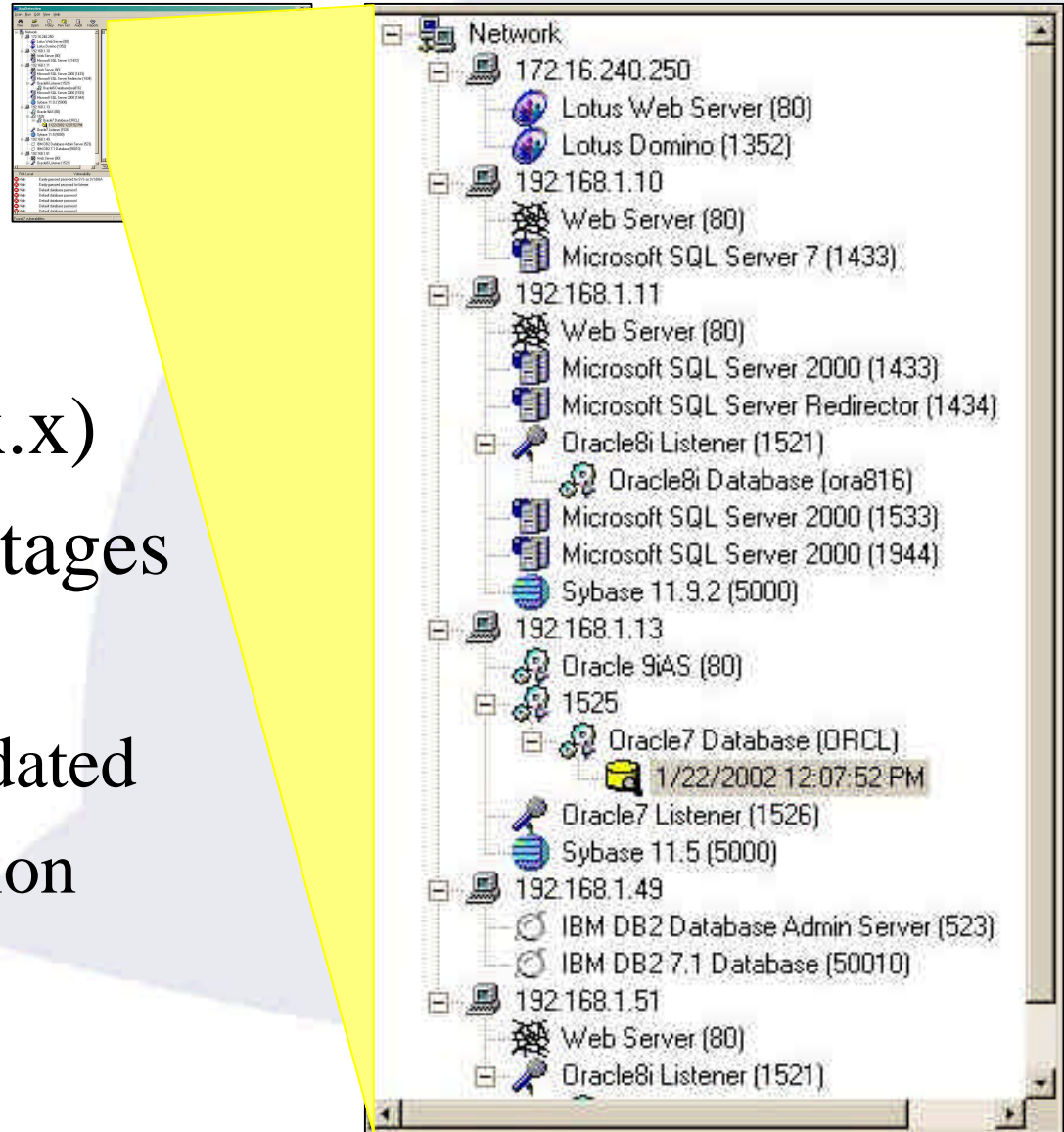


APPLICATION
SECURITY, INC.

www.AppSecInc.com

1. Discovery and Inventory

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



APPLICATION
SECURITY, INC.

www.AppSecInc.com

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

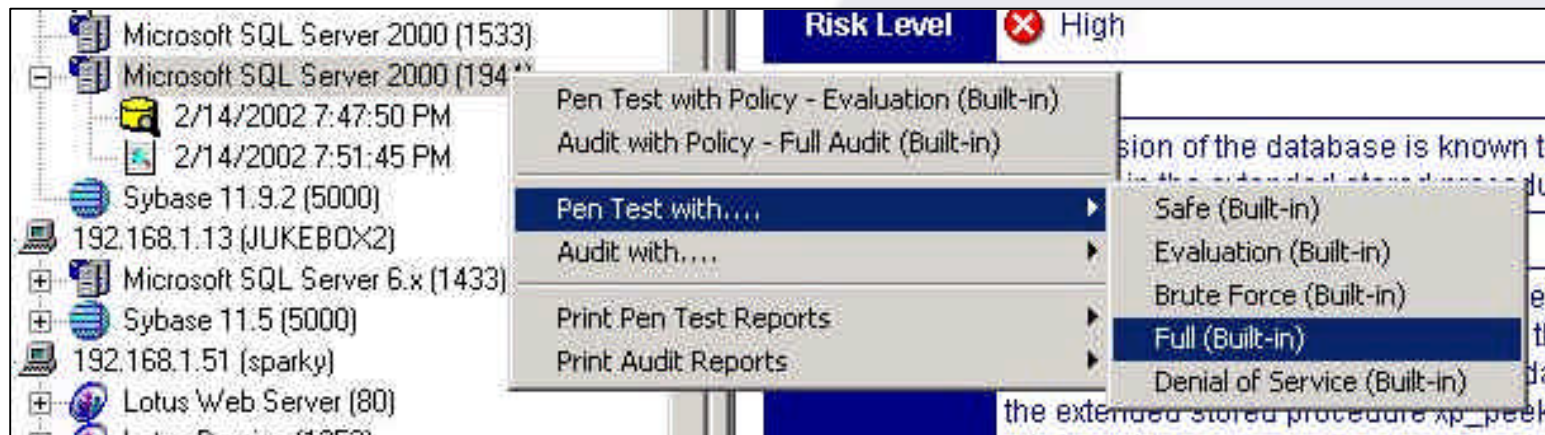


APPLICATION
SECURITY, INC.

www.AppSecInc.com

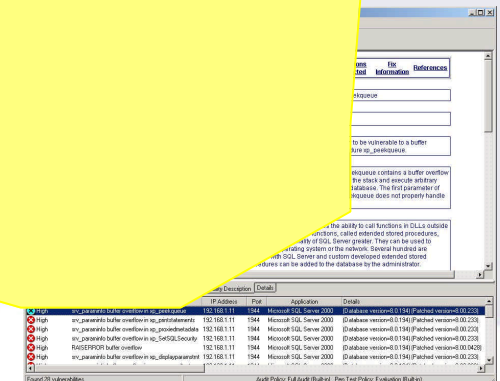
2. Penetration Testing

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



APPLICATION
SECURITY, INC.

www.AppSecInc.com



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.



**APPLICATION
SECURITY, INC.**

www.AppSecInc.com

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

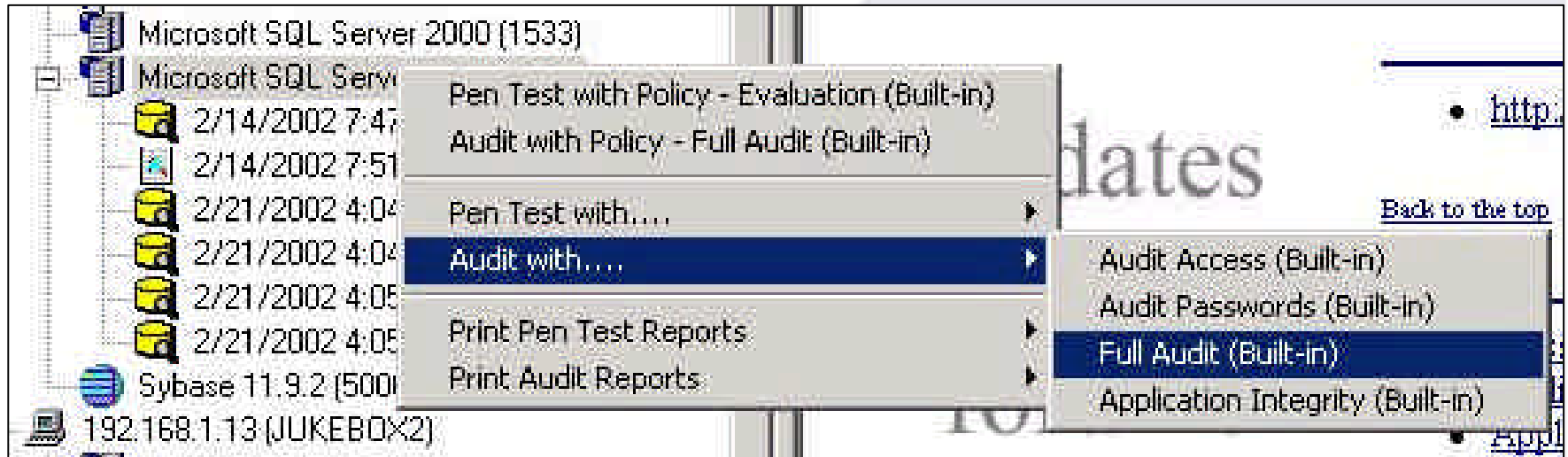


APPLICATION
SECURITY, INC.

www.AppSecInc.com

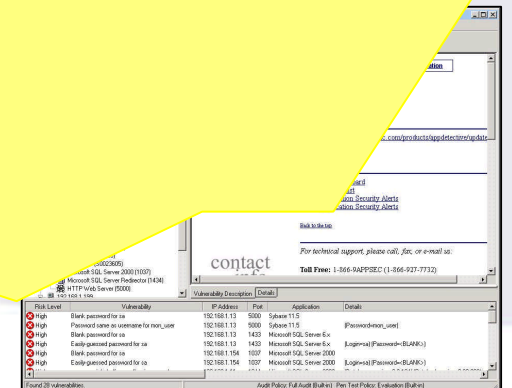
3. Security Auditing

- 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



APPLICATION
SECURITY, INC.

www.AppSecInc.com

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

Vulnerability Summary

APPLICATION SECURITY, INC.

Date of scan: 1/25/2002 12:08:53 PM
 Range scanned: 192.168.1.1-192.168.1.254(80,1352,1433,1521-1530)

A security review has been run on a number of applications on your network. This review consisted of probing the application and comparing the results to a knowledge base of application security vulnerabilities.

This report displays a summary list of all vulnerabilities found include a summary analysis of the problem. To review a more detailed list of vulnerabilities and a comprehensive description of each vulnerability found, you can view the Vulnerability Details report.

Vulnerabilities by Risk Level

| Risk Level | Count |
|---------------|-------|
| High | 76 |
| Informational | 10 |
| Medium | 14 |
| Low | 0 |
| Critical | 0 |

Vulnerabilities by IP Address

| IP Address Range | Count |
|------------------|-------|
| 192.168.1.10 | 1 |
| 192.168.1.11 | 1 |
| 192.168.1.12 | 1 |
| 192.168.1.13 | 1 |
| 192.168.1.14 | 1 |
| 192.168.1.15 | 1 |
| 192.168.1.16 | 1 |
| 192.168.1.17 | 1 |
| 192.168.1.18 | 1 |
| 192.168.1.19 | 1 |
| 192.168.1.20 | 1 |
| 192.168.1.21 | 1 |
| 192.168.1.22 | 1 |
| 192.168.1.23 | 1 |
| 192.168.1.24 | 1 |
| 192.168.1.25 | 1 |
| 192.168.1.26 | 1 |
| 192.168.1.27 | 1 |
| 192.168.1.28 | 1 |
| 192.168.1.29 | 1 |
| 192.168.1.30 | 1 |
| 192.168.1.31 | 1 |
| 192.168.1.32 | 1 |
| 192.168.1.33 | 1 |
| 192.168.1.34 | 1 |
| 192.168.1.35 | 1 |
| 192.168.1.36 | 1 |
| 192.168.1.37 | 1 |
| 192.168.1.38 | 1 |
| 192.168.1.39 | 1 |
| 192.168.1.40 | 1 |
| 192.168.1.41 | 1 |
| 192.168.1.42 | 1 |
| 192.168.1.43 | 1 |
| 192.168.1.44 | 1 |
| 192.168.1.45 | 1 |
| 192.168.1.46 | 1 |
| 192.168.1.47 | 1 |
| 192.168.1.48 | 1 |
| 192.168.1.49 | 1 |
| 192.168.1.50 | 1 |
| 192.168.1.51 | 1 |
| 192.168.1.52 | 1 |
| 192.168.1.53 | 1 |
| 192.168.1.54 | 1 |
| 192.168.1.55 | 1 |
| 192.168.1.56 | 1 |
| 192.168.1.57 | 1 |
| 192.168.1.58 | 1 |
| 192.168.1.59 | 1 |
| 192.168.1.60 | 1 |
| 192.168.1.61 | 1 |
| 192.168.1.62 | 1 |
| 192.168.1.63 | 1 |
| 192.168.1.64 | 1 |
| 192.168.1.65 | 1 |
| 192.168.1.66 | 1 |
| 192.168.1.67 | 1 |
| 192.168.1.68 | 1 |
| 192.168.1.69 | 1 |
| 192.168.1.70 | 1 |
| 192.168.1.71 | 1 |
| 192.168.1.72 | 1 |
| 192.168.1.73 | 1 |
| 192.168.1.74 | 1 |
| 192.168.1.75 | 1 |
| 192.168.1.76 | 1 |
| 192.168.1.77 | 1 |
| 192.168.1.78 | 1 |
| 192.168.1.79 | 1 |
| 192.168.1.80 | 1 |

Company Name: Sample Company Page 1 of 5 Print Date: 1/26/2002

Application Inventory

APPLICATION SECURITY, INC.

Scan Date: 1/25/2002 12:08:53 PM
 Scan Range: 192.168.1.1-192.168.1.254(80,1352,1433,1521-1530)

Your network was inventoried for enterprise applications such as database, groupware, ERP, and Web servers. This inventory was conducted by scanning a range of IP addresses and investigating the responsive ports for the existence of applications. Utilizing a proprietary recognition system, the application type, version, and components of the discovered applications are identified.

An application inventory differs in many ways from a typical scan run by other security tools. Typical network scans are effective at finding IP addresses and collecting a list of port that are responsive, but do not recognize the applications running on the ports. An application inventory, as performed by AppDetective, looks for specific applications and detects those applications even if they are listening on non-default ports. An application inventory also takes a scan to the next phase by performing an in-depth discovery of details about the application a network scan can not determine.

After the inventory, the next step is to perform a penetration test against each application. A pen test is an external evaluation of the security as a hacker would view the application. After the pen test, the next step would be to run a security audit of the application. A security audit is a test run internally on an application. A security audit provides the most detailed view of your system as seen from a non-privileged internal user as well as administrators.

Database, or External Procedure Server - Database applications from Oracle Corporation. The database is the system which stores the data. The External Procedure Server is a program which allows functions external to the database to be run from within the database.

Microsoft SQL Server 2000 - An enterprise groupware application that provides email, message boards, workflow, and other features.

Microsoft SQL Server 7.0 - An application which listens for and responds to HTTP requests.

Microsoft SQL Server 6.5 - A database application from Microsoft.

Microsoft SQL Server 6.0 - A database application from Microsoft.

Microsoft SQL Server 5.5 - A database application from Microsoft.

Microsoft SQL Server 5.0 - A database application from Microsoft.

Microsoft SQL Server 4.2 - A database application from Microsoft.

Microsoft SQL Server 4.0 - A database application from Microsoft.

Microsoft SQL Server 3.5 - A database application from Microsoft.

Microsoft SQL Server 3.0 - A database application from Microsoft.

Microsoft SQL Server 2.0 - A database application from Microsoft.

Microsoft SQL Server 1.0 - A database application from Microsoft.

Microsoft SQL Server 0.0 - A database application from Microsoft.

Applications By Type

Sample Company Page 1 of 3 Print Date: 1/26/2002 12:05:18PM

Check Status

APPLICATION SECURITY, INC.

Date of scan: 1/25/2002 12:08:53 PM
 Range scanned: 192.168.1.1-192.168.1.254(80,1352,1433,1521-1530)

A number of penetration tests and audits were performed on the application in your network. Below is a list of checks that were executed along with an indication of whether any violations of the check were found. Also listed is the start and end time of when the check ran.

If at least one vulnerability was found for a check, the 'Status' field will read 'Violation Found'. For checks in which no vulnerabilities were found, the 'Status' field will read 'No Violation Found'. If a check failed for any reason, the 'Status' field will read 'Failed' and a short description of what caused the check to fail will be displayed. If the 'Status' field has a value of 'Working', then the check is still running. If a check was not able to be performed for any reason, the 'Status' field contains a value of 'Skipped' and a status message should be provided containing details about why the check was skipped.

The Check Status report can be used to review which checks were run as well as which checks may have failed.

Check Status Summary

| Status | Count |
|--------------------|-------|
| No Violation Found | 20 |
| Violation Found | 76 |

Legend: No Violation Found (Blue), Violation Found (Red)

Legend: No Violation Found (Green), Violation Found (Red), Skipped (Yellow), Failed (Purple), Running (Blue)

Check Name: Blank password for sa

| IP Address | Port | Application | Status | Time Run |
|--------------|------|------------------------|--------------------|-------------------------|
| 192.168.1.87 | 1433 | Sybase 11.3.2 | Violation Found | 2:15:57 PM - 2:15:59 PM |
| 192.168.1.11 | 1433 | Microsoft SQL Server 7 | No Violation Found | 1:08:51 PM - 1:08:52 PM |
| 192.168.1.13 | 1433 | Microsoft SQL Server 7 | Violation Found | 1:09:01 PM - 1:09:01 PM |

Check Name: Default database password

| IP Address | Port | Application | Status | Time Run |
|---------------|------|--------------------------|--------------------|-------------------------|
| 192.168.1.222 | 1521 | Oracle®i Database(9i) | Violation Found | 1:58:21 PM - 1:59:02 PM |
| 192.168.1.18 | 1521 | Oracle®i Database(9iCL) | Violation Found | 1:13:28 PM - 1:13:35 PM |
| 192.168.1.199 | 1521 | Oracle®i Database(9iSRV) | No Violation Found | 1:14:20 PM - 1:14:20 PM |

Check Name: Easily guessed probe password

| IP Address | Port | Application | Status | Time Run |
|------------|------|-------------|--------|----------|
|------------|------|-------------|--------|----------|

Company Name: Sample Company Page 1 of 4 Print Date: 1/26/2002 6:14:34PM

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**



**APPLICATION
SECURITY, INC.**

www.AppSecInc.com

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.**



**APPLICATION
SECURITY, INC.**

www.AppSecInc.com

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)



APPLICATION
SECURITY, INC.

www.AppSecInc.com

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

- A. Assess Risk
- 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>



APPLICATION
SECURITY, INC.

www.AppSecInc.com

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



**APPLICATION
SECURITY, INC.**

www.AppSecInc.com

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