

# AppDetective for IBM DB2

---

Product Briefing



APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://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, Pharmaceutical, 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](http://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](http://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)
  - American Express Data Security Standard
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability Accountability Act (HIPAA)



APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://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](http://www.AppSecInc.com)

# AppDetective™ is the Answer

- AppDetective™ for IBM DB2 Empowers Organizations with the Following Capabilities:
  1. Database Discovery and Identification
  2. Penetration Testing (Outside-In Tests)
  3. Security Audit (Inside-Out Tests)
  4. Reporting Facilities
  5. Complimentary and Compatible
  6. Extensive and Updated Library of Vulnerabilities and Misconfigurations



APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://www.AppSecInc.com)

# AppDetective™ is the Answer

- AppDetective™ for IBM DB2 Empowers the Following Individuals:
  - Security Practitioners
  - Internal Auditors
  - General System Administrators
  - Database Administrators

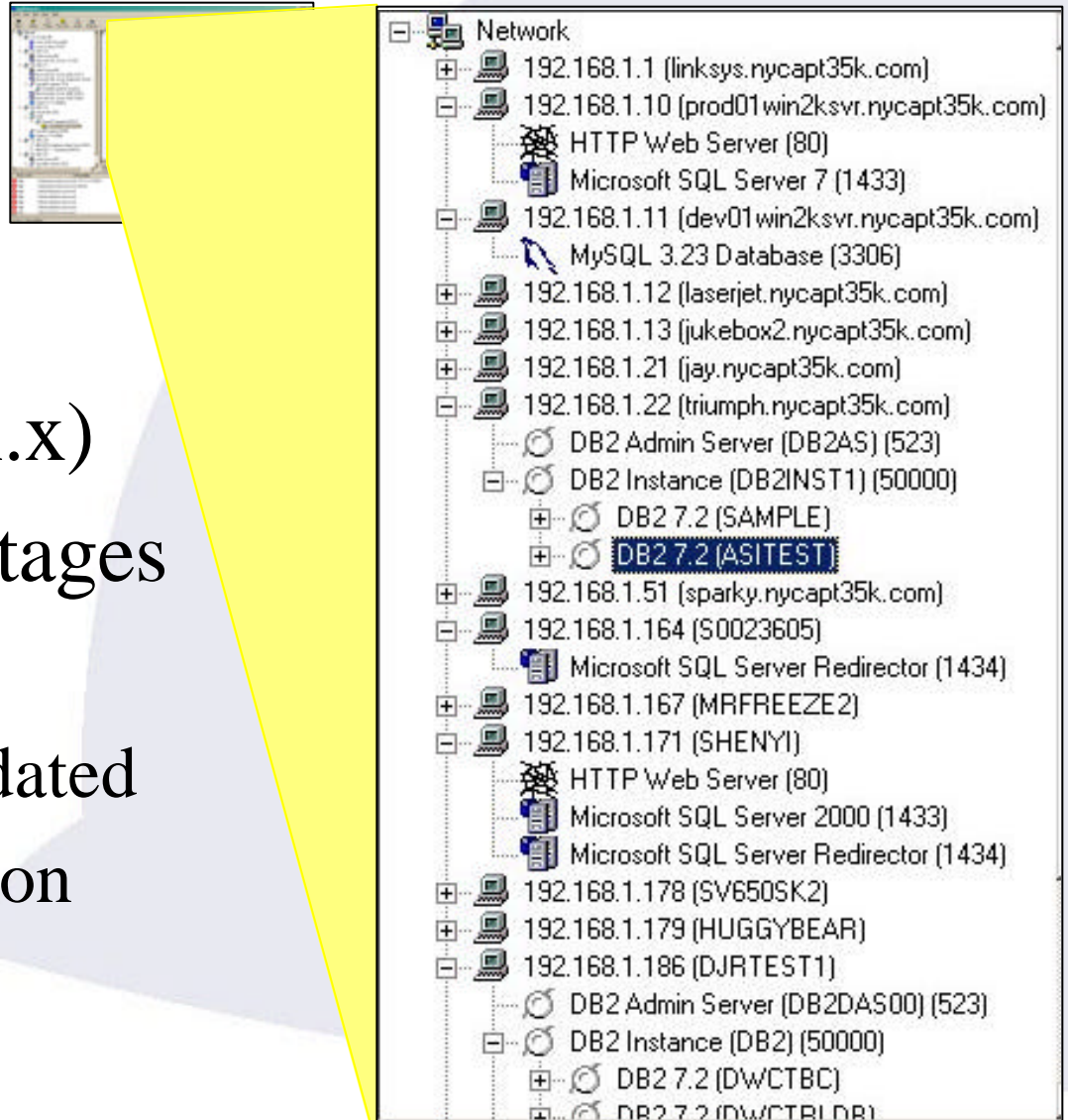


APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://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](http://www.AppSecInc.com)



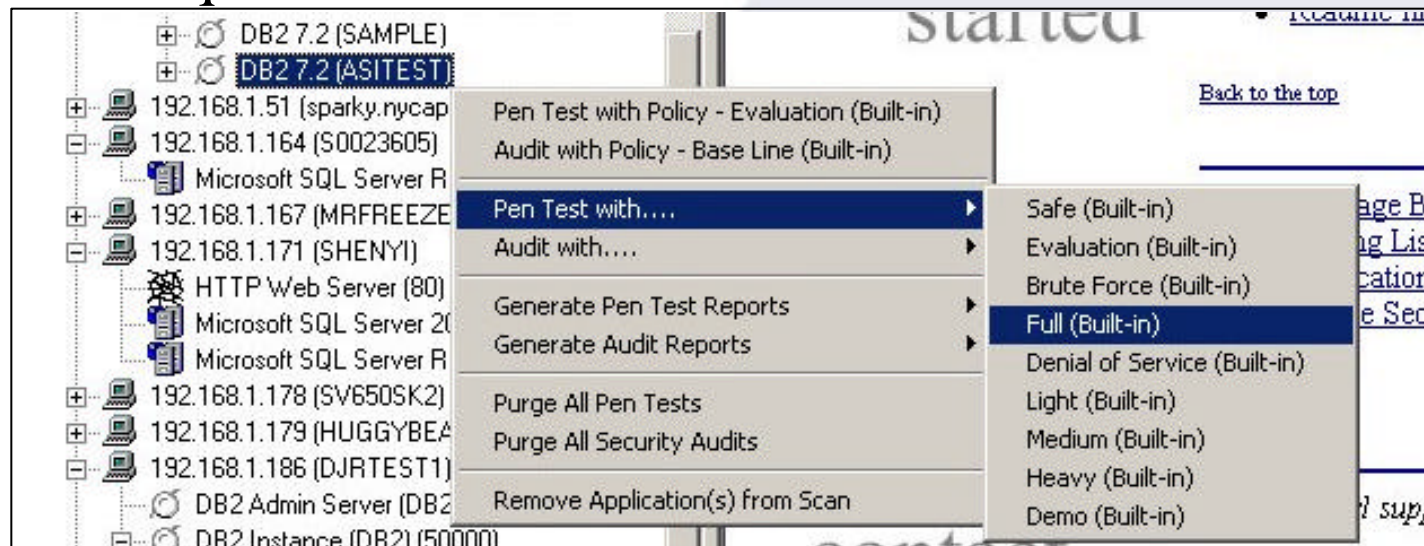
## 2. Penetration Testing

- **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



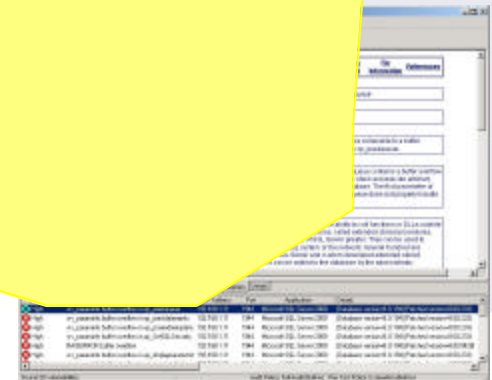
## 2. Penetration Testing

- **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
  - Examples: Control Center Buffer Overflow
- Miconfigurations
  - Examples: CLIENT authentication, DCS Authentication; Server Authentication
- Password Attacks
  - Examples: Blank, Default, and Easily Guessed Passwords
- Vulnerabilities
  - Examples: Control Center Buffer Overload; db2ckpw Buffer Overflow



**APPLICATION  
SECURITY, INC.**

[www.AppSecInc.com](http://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

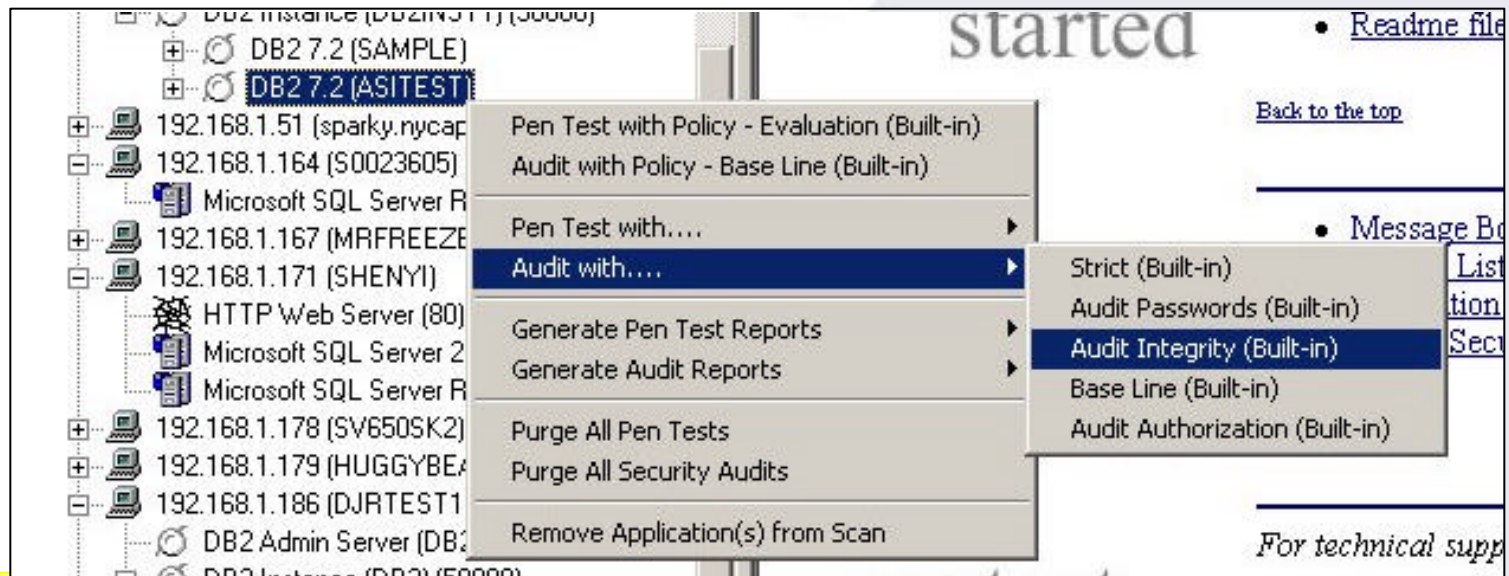


APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://www.AppSecInc.com)

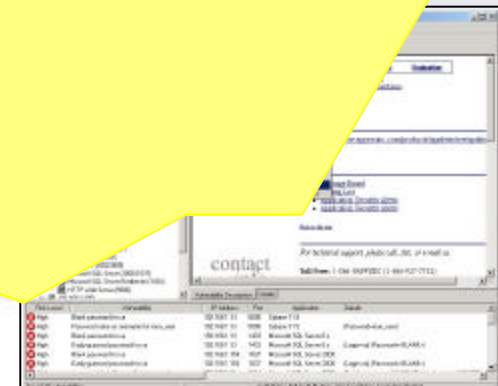
# 3. Security Auditing

- Security Audit



**APPLICATION  
SECURITY, INC.**

www.AppSecInc.com



# 3. Security Auditing

- **Security Audit Categories**

- Access Control

- Examples: CREATE\_NOT\_FENCED privilege granted; Permissions granted to PUBLIC; Permissions on system catalog

- Application Integrity

- Examples: Password.Attack; Unfenced Package; db2ckpwd buffer overflow

- Identification/Password Control

- Examples: Dormant Accounts; CLIENT AUTHENTICATION; SERVER Authentication

- OS Integrity



**APPLICATION  
SECURITY, INC.**

[www.AppSecInc.com](http://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](http://www.AppSecInc.com)

# 4. Reporting Facilities

## • Reporting Examples

### Vulnerability Summary

APPLICATION SECURITY, INC.

Date of scan: 12/28/2012 12:00:00 PM  
 Range scanned: 192.168.1.1-192.168.1.254(96,1342,1432,1433,1521-1536)

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 and also a summary analysis of the results. To review a more detailed list of vulnerabilities and a more extensive description of each vulnerability found, you can view the Vulnerability Details report.

#### Vulnerabilities by Risk Level

Risk Level	Count
High	10
Informational	30
Low	40
Stopped	10
Failed	10

#### Vulnerabilities by IP Address

IP Address Range	Count
192.168.1.1-192.168.1.10	10
192.168.1.11-192.168.1.20	10
192.168.1.21-192.168.1.30	10
192.168.1.31-192.168.1.40	10
192.168.1.41-192.168.1.50	10
192.168.1.51-192.168.1.60	10
192.168.1.61-192.168.1.70	10
192.168.1.71-192.168.1.80	10
192.168.1.81-192.168.1.90	10
192.168.1.91-192.168.1.100	10
192.168.1.101-192.168.1.110	10
192.168.1.111-192.168.1.120	10
192.168.1.121-192.168.1.130	10
192.168.1.131-192.168.1.140	10
192.168.1.141-192.168.1.150	10
192.168.1.151-192.168.1.160	10
192.168.1.161-192.168.1.170	10
192.168.1.171-192.168.1.180	10
192.168.1.181-192.168.1.190	10
192.168.1.191-192.168.1.200	10
192.168.1.201-192.168.1.210	10
192.168.1.211-192.168.1.220	10
192.168.1.221-192.168.1.230	10
192.168.1.231-192.168.1.240	10
192.168.1.241-192.168.1.250	10
192.168.1.251-192.168.1.254	10

Company Name: Sample Company Page 1 of 3 Print Date: 12/28/2012

### Application Inventory

APPLICATION SECURITY, INC.

Scan Date: 12/28/2012 12:00:00 PM  
 Scan Range: 192.168.1.1-192.168.1.254(96,1342,1432,1433,1521-1536)

Your network was inventoried for enterprise applications such as databases, groupware, ERP, and Web servers. This inventory was conducted by scanning a range of IP addresses and bringing along the response 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 focused on 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 step to the next phase by performing an in-depth discovery of details about the application a network administrator desires.

Checked the inventory, the next step is to perform a penetration test against each application. A primary an external evaluation of the security as a hacker would view the application. After the test, the next step would be to run a security audit of the application. A security audit is a wide scan necessary on an application. A security audit provides the most detailed view of your product an application from non-privileged internal users as well as other entities.

**Database or External Procedure Server** - Database applications from Oracle Corporation, entry between the client and a server. The database is the system which stores the data. The server is a program which allows functions external to the database to be run from within the enterprise (program application that provides external message handling, workflow, and other...)

**Web Server** - An application which listens for and responds to HTTP requests.

**Web** - A database application from Microsoft.

**Database Server** - Database applications from IBM Corporation. The Database Access interface for client requests for database administration and other actions. The Database Server interface is a component of an application but was unable to accurately obtain enough information to identify (i.e. the application's version or platform).

#### Applications By Type

Application Type	Count
Microsoft SQL Server 2008	30
Microsoft SQL Server 2005	20
Microsoft SQL Server 2000	10
Microsoft SQL Server 2003	10
Microsoft SQL Server 2004	10
Microsoft SQL Server 2006	10
Microsoft SQL Server 2007	10

Company Name: Sample Company Page 1 of 3 Print Date: 12/28/2012 12:00:00 PM

### Check Status

APPLICATION SECURITY, INC.

Date of scan: 12/28/2012 12:00:00 PM  
 Range scanned: 192.168.1.1-192.168.1.254(96,1342,1432,1433,1521-1536)

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 is listed '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 'Skipped', then the check is still running. If a check was not able to be performed for any reason, the 'Status' field reads as a value of 'Stopped' and a status message should be provided containing details about why the check was stopped.

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	20

Check Name	IP Address	Port	Application	Status	Time Run
Check Name: Blank password for sa	192.168.1.87	1433	Microsoft SQL Server T	Violation Found	2/15/27 PM - 2/15/27 PM
Check Name: Default database password	192.168.1.11	1433	Microsoft SQL Server T	No Violation Found	1/26/21 PM - 1/26/21 PM
Check Name: Empty password probe password	192.168.1.15	1433	Microsoft SQL Server T	Violation Found	1/26/21 PM - 1/26/21 PM
Check Name: Default database password	192.168.1.203	1521	CheckDB Database(DBC)	Violation Found	1/26/21 PM - 1/26/21 PM
Check Name: Default database password	192.168.1.16	1521	CheckDB Database(DBC)	Violation Found	1/13/20 PM - 1/13/20 PM
Check Name: Default database password	192.168.1.160	1521	CheckDB Database(DBC)	No Violation Found	1/14/20 PM - 1/14/20 PM

Company Name: Sample Company Page 1 of 4 Print Date: 12/28/2012 12:00:00 PM



## 5. Complimentary and Compatible

- **AppDetective essentially picks up where all of the following leave off:**
  - **Port Scanners**
    - **NOS / OS Oriented and Can't Discover Applications and Databases**
  - **Network and Host Operating System Scanners**
    - **Able to Assess Only NOS and OS's**
  - **Web Application Scanners**
    - **Able to only scan for vulnerabilities relevant to the components within a web application infrastructure**
  - **Other "Database" Scanners**
    - **Able to only perform inside out audits and are out of date**



**APPLICATION  
SECURITY, INC.**

[www.AppSecInc.com](http://www.AppSecInc.com)

# 6. Vulnerabilities and Misconfigurations

- **Key Industry Advantage**
  - **Application Security, Inc. R&D concentrates on the security, protection, and defense of applications.**
    - **S.H.A.T.T.E.R.**
      - **Research and Development Team**
    - **Application Security Alerts**
      - <http://www.appsecinc.com/resources/alerts/>
    - **Application Vulnerability Checks**
      - <http://www.appsecinc.com/asap/checks/>
    - **ASAP Updates**
      - <http://www.appsecinc.com/asap/>
      - **Average of 3 Updates Per Month**



**APPLICATION  
SECURITY, INC.**

[www.AppSecInc.com](http://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)
  - American Express Data Security Standard



APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://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](http://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](http://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](http://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](http://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](http://www.AppSecInc.com)



# AppDetective™ and Amex Data Security

## AppDetective™ Capabilities

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

## American Express Data Security Standard

- Employee Access / Passwords
- Systems
  - Routinely test internal security systems and processes.
- Audits
  - Be prepared to provide audit reports to American Express or allow American Express audits.



**APPLICATION  
SECURITY, INC.**

[www.AppSecInc.com](http://www.AppSecInc.com)

# Availability

---

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



APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://www.AppSecInc.com)

# AppDetective™ Future Plans

---

- Expanded Database and Groupware Platforms
  - MySQL
  - Microsoft Exchange
  - OracleiAS
  - IBM WebSphere



APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://www.AppSecInc.com)

# Who is Application Security, Inc.

- Unique Position and Background
  - SHATTER™ focuses on database, groupware, web, application server, and ERP applications
    - Database Encryption
    - Penetration Testing/Vulnerability Assessment
    - Intrusion Detection
- Application Security, Inc. (ASI) Mission
  - Develop security solutions providing “protection where it counts”



APPLICATION  
SECURITY, INC.

[www.AppSecInc.com](http://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](http://www.AppSecInc.com)