

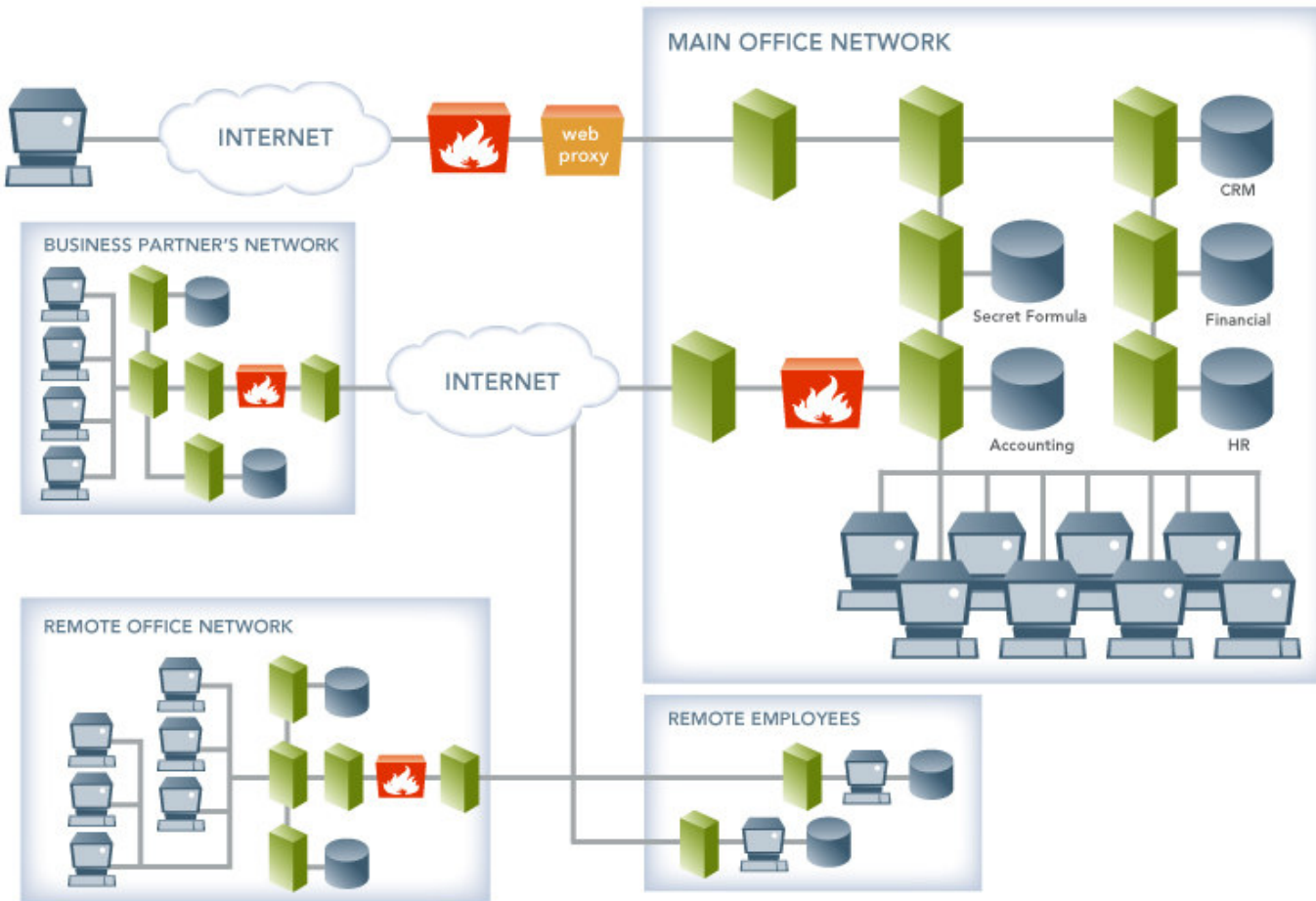
# **Database Attacks, How to protect the corporate assets**

Presented by: James Bleecker

# Agenda

- Introduction
  - Network/Application Landscape
  - Database Vulnerabilities Are The New Front-Lines
- Attacking Where the Data Resides
  - Planning an Attack
  - Attacking Database Vulnerabilities
- How Do You Protect Your Database?
- What is Application Security direction/Vision?

# Typical Network Landscape



# Database Vulnerability Exploitation

A decade ago, attacks were

- Broad based
- Launched by disaffected “Hackers”
- Intended to disrupt, gain respect / notoriety in the community

Now, attacks are

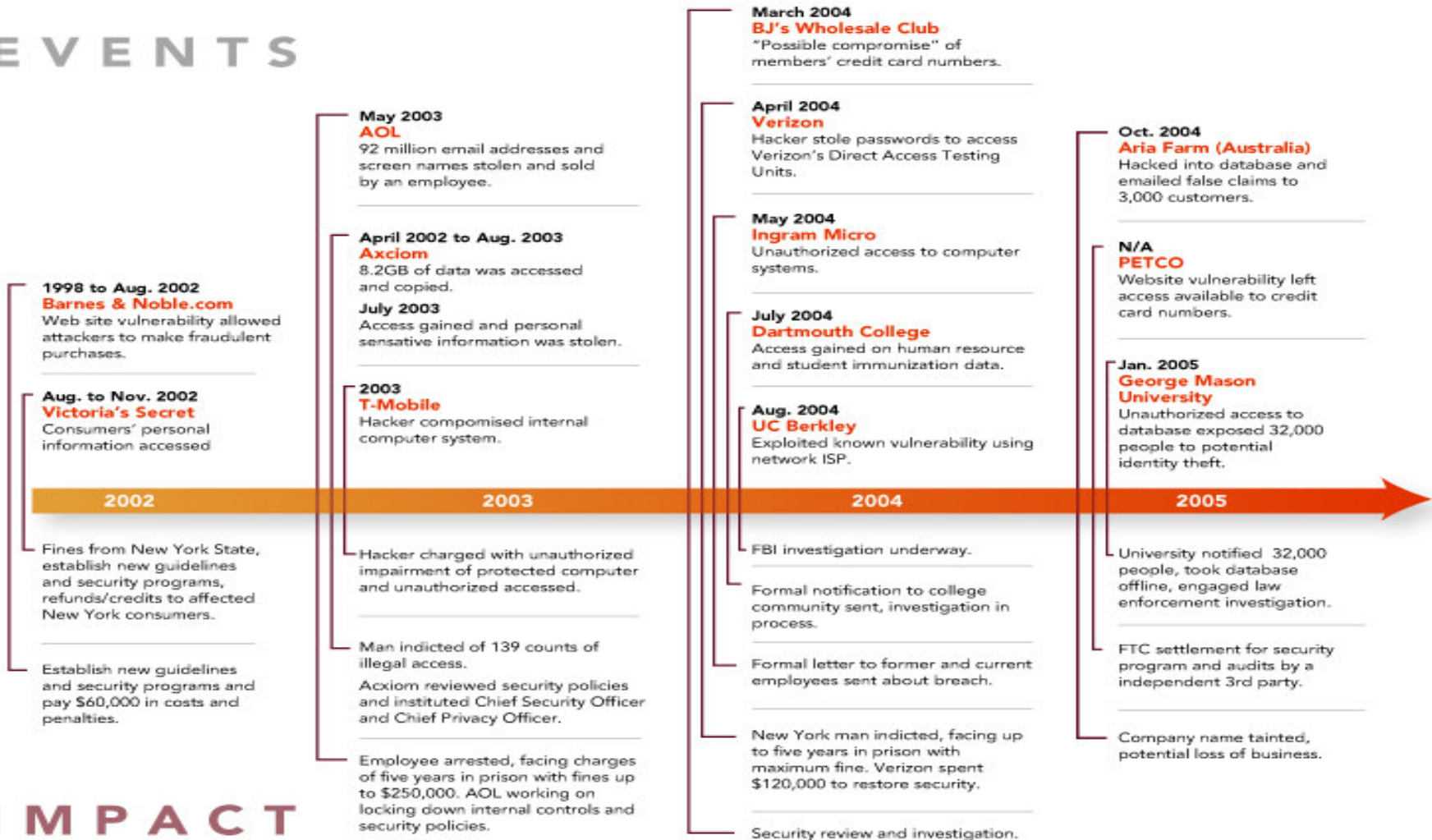
- Targeted against specific resources
- Launched by sophisticated professionals
- Intended to bring monetary gain to the attacker

**Data is a valuable resource in your company**

- Value increases with greater integration and aggregation
- But so does the threat of data theft, modification, or destruction

# Databases Are Under Attack

## EVENTS



## IMPACT

# Top 10 Customer Data Loss Incidents – 2005 to date

Company/Organization	Number of Affected Customers	Date of Initial Disclosure
<a href="#">Citigroup</a>	3,900,000	6-Jun
<a href="#">DSW Shoe Warehouse</a>	1,400,000	8-Mar
<a href="#">Bank of America</a>	1,200,000	25-Feb
<a href="#">Time Warner</a>	600,000	2-May
<a href="#">LexisNexis</a>	310,000	9-Mar
<a href="#">Ameritrade</a>	200,000	19-Apr
<a href="#">Polo Ralph Lauren</a>	180,000	14-Apr
<a href="#">ChoicePoint</a>	145,000	15-Feb
<a href="#">Boston College</a>	120,000	17-Mar
<a href="#">Bank of America &amp; Wachovia</a>	108,888	23-May
<b>Total # of customers affected</b>	<b>8,163,888</b>	
Source: InformationWeek, public disclosures by companies		

# How Do You Secure Apps?

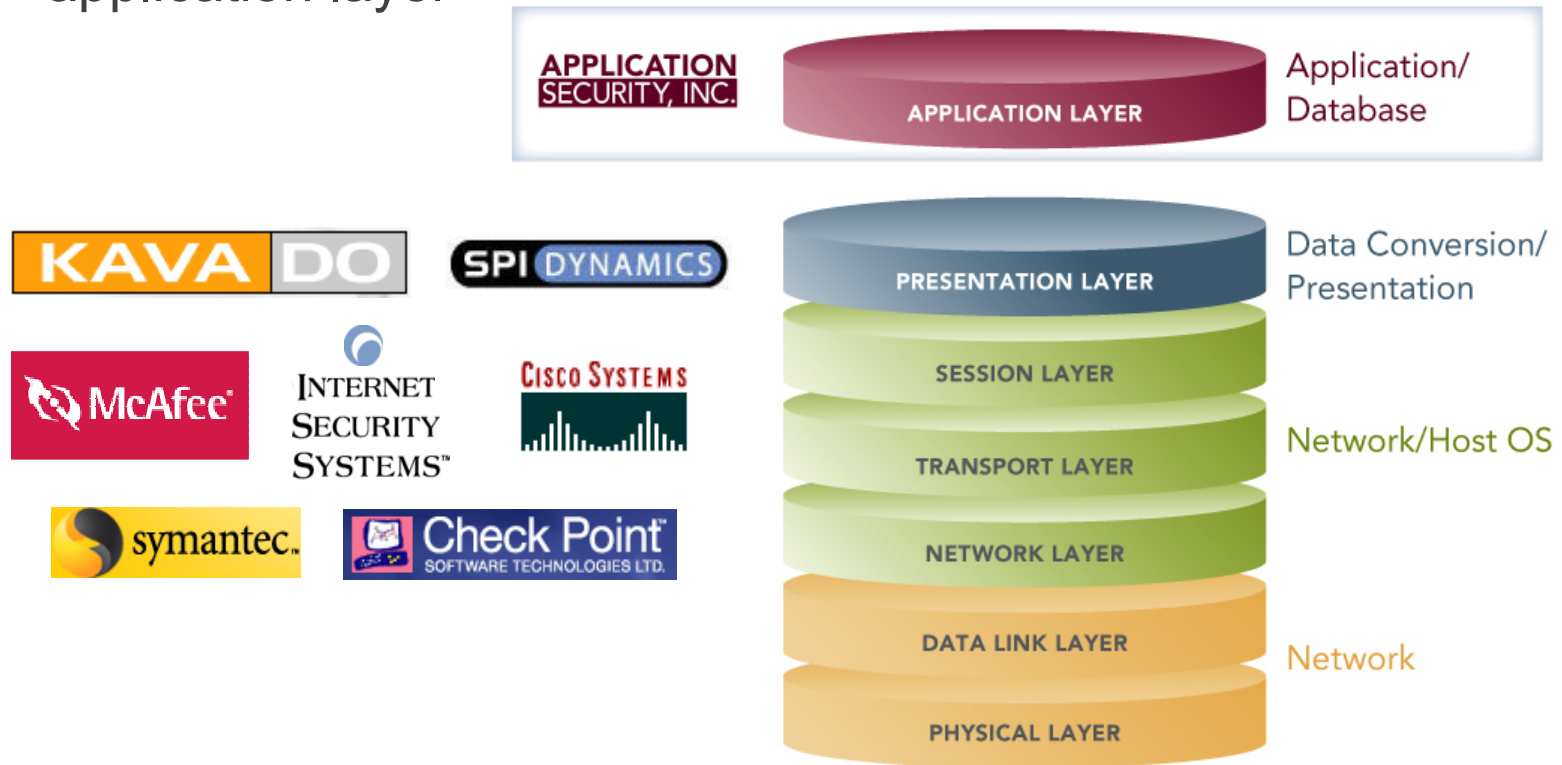
## Key Components of Enterprise Applications



Vulnerabilities exist within each of these components

# Why Database Security?

- Legacy solutions address (pre-attack) security discovery, assessment, and protection in every layer... except in the application layer










# Database Vulnerabilities:

- Default & Weak Passwords
- Denial of Services (DoS) & Buffer Overflows
- Misconfigurations & Resource Privilege Management Issues

# Database Vulnerabilities: Default & Weak Passwords

- Databases have their own user accounts and passwords

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords					

# Database Vulnerabilities

## Default Passwords

- Oracle Defaults (Over 200 of them)
  - User Account: internal / Password: oracle
  - User Account: system / Password: manager
  - User Account: sys / Password: change\_on\_install
  - User Account: dbsnmp / Password: dbsnmp
- IBM DB2 Defaults
  - User Account: db2admin / Password: db2admin
  - User Account: db2as / Password: ibmdb2
  - User Account: dlfm / Password: ibmdb2

# Database Vulnerabilities

## Default Passwords

- MySQL Defaults
  - User Account: root / Password: null
  - User Account: admin / Password: admin
  - User Account: myusername / Password: mypassword
- Sybase Defaults
  - User Account: SA / Password: null
- Microsoft SQL Server Defaults
  - User Account: SA / Password: null

# Database Vulnerabilities

## Weak Passwords

- It is important that you have all of the proper safeguards against password crackers because:
  - Most databases do not have Account Lockout
  - Database Login activity is seldom monitored
  - Scripts and Tools for exploiting weak identification control mechanisms and default passwords are widely available

# Database Vulnerabilities: Denial of Services (DoS) & Buffer Overflows

- Databases have their own DoS's & Buffer Overflows

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓

# Denial of Services

## Databases Have Their Own Class of DoS Attacks

Category of attacks that could result in the database crashing or failing to respond to connect requests or SQL Queries.

### Significant Database Denial of Services:

Oracle8i: NSPTCN data offset DoS

<https://www.appsecinc.com/Policy/PolicyCheck31.html>

Oracle9i: SNMP DoS

<https://www.appsecinc.com/Policy/PolicyCheck45.html>

Microsoft SQL Server: Resolution Service DoS

<https://www.appsecinc.com/Policy/PolicyCheck2066.html>

IBM DB2: Date/Varchar DoS

<https://www.appsecinc.com/Policy/PolicyCheck3014.html>

# Buffer Overflows

## Databases Have Their Own Buffer Overflows

Category of vulnerabilities that could result in an unauthorized user causing the application to perform an action the application was not intended to perform.

Most dangerous are those that allow arbitrary commands to be executed by authenticated users.

- No matter how strongly you've set passwords and other authentication features.

### Significant Database Buffer Overflows:

- Oracle9i: [TZ OFFSET buffer overflow](#)
- Microsoft: [pwdencrypt buffer overflow](#) / [Resolution Stack Overflow](#)
- Sybase: [xp\\_freedll buffer overflow](#)



# Database Vulnerabilities Misconfigurations & Resource Privilege Management Issues

- Misconfigurations can make a database vulnerable

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Resource Privilege Management	✓	✓	✓	✓	✓

# Misconfigurations & Resource Privileges

## Misconfigurations Can Make a Database Vulnerable

### Oracle

- External Procedure Service
- Default HTTP Applications
- Privilege to Execute UTL\_FILE

### Microsoft SQL Server

- Standard SQL Server Authentication Allowed
- Permissions granted on xp\_cmdshell

### Sybase

- Permission granted on xp\_cmdshell

### IBM DB2

- CREATE\_NOT\_FENCED privilege granted
  - This privilege allows logins to create stored procedures

### MySQL

- Permissions on User Table (mysql.user)

# Database Vulnerabilities Wrap-up

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Resource Privilege Management	✓	✓	✓	✓	✓

# Planning an Attack

- Create a Map
  - What does the network look like?
- Reconnoiter
  - Collect information about the layout of the target
  - What looks interesting?
- Probe, Progress, Plot
  - What can we do?
  - Build the springboard for further activity
  - Plan the strike
- Retreat and Re-attack

# How are search engines used for attacks?

- First thing an attacker needs is information
  - Where to attack
  - What a site is vulnerable to
- Search engine is a large repository of information
  - Every web page in your application
  - Every domain on the Internet
- Search engines provide an attacker:
  - Ability to search for attack points on the Internet
  - Ability to search for an attack point in a specific website
  - Ability to look for specific URLs or files
- <http://johnny.ihackstuff.com/index.php?module=prodreviews>

# Example – looking for iSQL\*Plus

- Oracle HTTP Servers
  - Provides a way to run queries on database using an HTTP form
  - Accessed using the URL /isqlplus
  - By default runs on any Oracle HTTP server installed with:
    - Oracle Applications Server
    - Oracle Database Server
- Search can be performed on Google or Yahoo
  - looking for Oracle HTTP servers
  - Using the “allinurl” advanced search feature

# Using Google Advanced Search



**Find results**

with **all** of the words

with the **exact phrase**

with **at least one** of the words

**without** the words

10 results

**Language** Return pages written in

**File Format**  return results of the file format

**Date** Return web pages updated in the

**Numeric Range** Return web pages containing numbers between  and

**Occurrences** Return results where my terms occur

**Domain**  return results from the site or domain

**SafeSearch**  No filtering  Filter using [SafeSearch](#)

[e info](#)

## Froogle Product Search (BETA)

**Products** Find products for sale

To browse for products, start at the [Froogle home page](#)

# Results of Google Advanced Search

[iSQL\\*Plus Release 9.2.0.5.0 Production: Anmelden](#) - [ [Translate this page](#) ]

Anmelden. Benutzername: Kennwort: Connect-String: ueb.

[holle.db.informatik.uni-kassel.de/isqlplus](#) - 3k - [Cached](#) - [Similar pages](#)

[iSQL\\*Plus Release 9.2.0.4.0 Production: Logowanie](#)

Logowanie. Nazwa użytkownika: Hasło: Identyfikator połączenia:

[dmlab.cs.put.poznan.pl/isqlplus](#) - 4k - [Cached](#) - [Similar pages](#)

[iSQL\\*Plus Release 9.2.0.1.0 Production: Anmelden](#) - [ [Translate this page](#) ]

Anmelden. Benutzername: Kennwort: Connect-String:

[lwis02.inf.fh-koeln.de:7778/isqlplus](#) - 3k - [Cached](#) - [Similar pages](#)

[\[doc\] Table des matières](#)

File Format: Microsoft Word 2000 - [View as HTML](#)

... Middle Tier □ Serveur Oracle HTTP. Pour installer **iSQLPlus** : Unzipper la distribution **iSQLPlus** en .zip dans un répertoire temporaire. ...

[www.isnetne.ch/lbd/SGBD/oracle/ documents/isqlplus/Inst\\_isqlplus817.doc](#) - [Similar pages](#)

[iSQL\\*Plus Release 9.2.0.1.0 Production: Login](#)

Login. Username: Password: Connection Identifier: oracle.unc.edu.

[https://oraclient.unc.edu/isqlplus](#) - 3k - [Cached](#) - [Similar pages](#)



Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [Next](#)

allinurl: "/isqlplus"

Search

[Search within results](#) | [Language Tools](#) | [Search Tips](#)



# Yahoo! Advanced Search Works Too.....








Yahoo! My Yahoo! Mail Welcome, **Guest** [Sign In]

Web | Images | Directory | Local **NEW!** | News | Products

**YAHOO!** search "iSQL\*Plus Release" Search

[Shortcuts](#) [Advanced](#)

**Search Results** Results 1 - 10 of about 79 for "**iSQL\*Plus Release**" - 0.23

1. [iSQL\\*Plus Release 9.2.0.1.0 Production: Login](#)   
Help. Login. Username: Password: Connection Identifier:  
[gettysburg.wccnet.edu:7777/isqlplus](#) - 3k - [Cached](#) - [More from this site](#)
2. [iSQL\\*Plus Release 9.0.1](#)   
Script Location: Enter statements:  
[student.cob.ohiou.edu/jb250299/ sqlweb.htm](#) - 20k - [Cached](#) - [More from this site](#)
3. [iSQL\\*Plus Release 9.0.1](#)   
Script Location: Enter statements:  
[student.cob.ohiou.edu/jb250299/ sarasql.htm](#) - 23k - [Cached](#) - [More from this site](#)
4. [iSQL\\*Plus Release 9.2.0.5.0 Production: Login](#)   
Help. Login. Username: Password: Connection Identifier:  
[isqlplus.it.swin.edu.au:7777/ isqlplus](#) - 3k - [Cached](#) - [More from this site](#)
5. [What's New in SQL\\*Plus?](#)   
... Any user customizations can be manually merged into the default **iSQL\*Plus Release 9.2** configuration file ... There are several new parameters for sizing and tuning **iSQL\*Plus Release 9.2** ...  
[cs.utah.edu/classes/cs6530/oracle/... /server.920/a90842/whatsnew.htm](#) - 30k - [Cached](#) - [More from this site](#)
6. [iSQL\\*Plus Release 10.1.0.2](#)   
\* Indicates required field. Username. Password. Connect Identifier. Help. Copyright © 2003, Oracle. All rights reserved.  
[www.onlinecreation.com:5560/ isqlplus](#) - 9k - [Cached](#) - [More from this site](#)
7. [SQL\\*Plus FAQ](#)   
SQL\*Plus and iSQL\*Plus Frequently Asked Questions  
[otn.oracle.com/support/tech/ sql\\_plus/btdocs/runtime.html](#) - 47k - [Cached](#) - [More from this site](#)

# Connect with default username/password

iSQL\*Plus Release 9.2.0.5.0 Production: Login - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address <http://localhost:7778/isqlplus> Go

Google Search Web Search Site Options

ORACLE<sup>®</sup>

iSQL\*Plus

Help

Login

Username:

Password:

Connection Identifier:

Login

# Attacker can execute any query

Work Screen

File or URL:  Browse... Load Script

Enter statements:

```
select * from dba_users
```

Execute Save Script Clear Screen Cancel

USERNAME	USER_ID	PASSWORD	ACCOUNT_STATUS	LOCK_DATE	EXPIRY_DA	DEFAULT_TABLES
SYS	0	9BDBFDA5BC24F760	OPEN			SYSTEM
SYSTEM	5	9BC141C650274F20	OPEN			SYSTEM
OUTLN	11	4A3BA55E08595C81	OPEN			SYSTEM
CTXSYS	33	24ABAB8B06281B4C	OPEN			DRSYS
APPSCHEM	10	5066D314D5421CCC	OPEN			SYSTEM

# Example – SQL Injection in demo applications

- Oracle HTTP Servers
  - Provided default web applications
    - /demo/sql/jdbc/JDBCQuery.jsp
    - /demo/sql/tag/sample2.jsp
- Contains SQL Injection
  - Google search value of “allinurl:JDBCQuery.jsp”

# Vulnerable Oracle HTTP Servers

Yahoo! My Yahoo! Mail Welcome, **Guest** [Sign In]

Search Home Help

**YAHOO!** search






Web | Images | Directory | Local <sup>NEW!</sup> | News | Products

"Please enter a suitable JDBC connection string, before you try

Search

Shortcuts Advanced Search Preferences

**Search Results** Results 1 - 5 of about 499 for **"Please enter a suitable JDBC connection string, before you try the above demo**

1. <http://coreapps2.evosource.net/demo/xml/xmlquery/XMLQuery.jsp>   
**Please enter a suitable JDBC connection string, before you try the above demo**  
[coreapps2.evosource.net/demo/xml/xmlquery/XMLQuery.jsp](http://coreapps2.evosource.net/demo/xml/xmlquery/XMLQuery.jsp) - 608 - [Cached](#) - [More from this site](#)
2. <http://infotrek.er.usgs.gov/demo/sql/sqlj/SQLJIterator.sqljsp>   
**Please enter a suitable JDBC connection string, before you try the above demo.** To use the thin driver insert your host, port and database id.  
[infotrek.er.usgs.gov/demo/sql/sqlj/SQLJIterator.sqljsp](http://infotrek.er.usgs.gov/demo/sql/sqlj/SQLJIterator.sqljsp) - 672 - [Cached](#) - [More from this site](#)
3. <http://ias.itec.suny.edu/demo/sql/tag/sample5.jsp>   
**Please enter a suitable JDBC connection string, before you try the above demo**  
[ias.itec.suny.edu/demo/sql/tag/sample5.jsp](http://ias.itec.suny.edu/demo/sql/tag/sample5.jsp) - 303 - [Cached](#) - [More from this site](#)
4. [OracleJSP](#)   
... **Please enter a suitable JDBC connection string, before you try the above demo ...**  
[rnsdemo.rnsolutions.com/ojspdemos/sql/index.jsp](http://rnsdemo.rnsolutions.com/ojspdemos/sql/index.jsp) - 4k - [Cached](#) - [More from this site](#)
5. [XML and XSL Tag Support](#)   
... <font size=+0> <B>**Please enter a suitable JDBC connection string, before you try the above demo**</B> <pre> To use the ...  
[deakin.edu.au/div\\_its/isg/dba/docs/9iasrel2/web.902/a958883/xmlxsl.htm](http://deakin.edu.au/div_its/isg/dba/docs/9iasrel2/web.902/a958883/xmlxsl.htm) - 43k - [Cached](#) - [More from this site](#)

- My Documents
- My Computer
- My Network Places
- Recycle Bin

Application Security, Inc. - Securing Business by Securing Enterprise Applications

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address <http://localhost:7778/demo/EnterCustomerName.htm> Go

# APPLICATION SECURITY, INC.

# Oracle Example

## Form Posting

---

Name:

---



Application Security, Inc. - Securing Business by Securing Enterprise Applications

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail

Address <http://localhost:7778/demo/WrongWayToSearchCustomer.jsp> Go

# APPLICATION SECURITY, INC.

---

Customer address: EED9B65CCECDB2E9

```
SELECT 'user: ADAMS password is the default (WOOD/72CDEF4A3483F60D)' "default:
SELECT 'user: ADLDEMO password is the default (ADLDEMO/147215F51929A6E8)' "d
SELECT 'user: ADMIN password is the default (JETSPEED/CAC22318F162D597)' "de
SELECT 'user: ADMIN password is the default (WELCOME/B8B15AC9A946886A)' "def:
SELECT 'user: ADMINISTRATOR password is the default (ADMINISTRATOR/1848FOA31:
SELECT 'user: ADMINISTRATOR password is the default (ADMIN/F9ED601D936158BD)
SELECT 'user: ANDY password is the default (SWORDFISH/B8527562E504BC3F)' "de:
SELECT 'user: AP password is the default (AP/EED09A552944B6AD)' "default pas:
SELECT 'user: APPLSYS password is the default (FND/OF886772980B8C79)' "defau
SELECT 'user: APPLYSYSPUB password is the default (PUB/A5E09E84EC486FC9)' "d
```

[http://www.pentest.co.uk/sql/check\\_users.sql](http://www.pentest.co.uk/sql/check_users.sql)

Internet



My Documents



My Computer



My Network Places



Recycle Bin

**The JDBCQuery JSP - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media RSS Mail Print Mailbox Favorites RSS

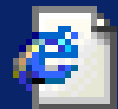
Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

**Enter a search condition:**

Done Internet





# The JDBCQuery JSP

- My Documents
- My Computer
- My Network Places
- Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

Enter a search condition:

Ask Oracle

Done Internet

7778/demo/sql/jdbc/JDBCQuery.jsp

- My Documents
- My Computer
- My Network Places
- Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail Stop

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

**Enter a search condition:**

**sys.database\_name**

Done Internet



My Documents



My Computer



My Network Places



Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%27%27+UNION+SELECT+sys.datab> Go Links

Google Search Web Search Site Options

**Search results for : '1'='2' UNION SELECT sys.database\_name, -500 FROM dual**

- TEST.US.ORACLE.COM earns \$ -500.

---

Enter a search condition:

Done Internet

- My Documents
- My Computer
- My Network Places
- Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Refresh Print Mail Stop

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

**Enter a search condition:**

**sys.login\_user**

Done Internet



My Documents



My Computer



My Network Places



Recycle Bin

**The JDBCQuery JSP - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address [http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%27%27+UNION+SELECT+sys.login\\_](http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%27%27+UNION+SELECT+sys.login_) Go Links

Google Search Web Search Site Options

**Search results for : '1'='2' UNION SELECT sys.login\_user, -500 FROM dual**

- SCOTT earns \$ -500.

---

**Enter a search condition:**

Done Internet

- My Documents
- My Computer
- My Network Places
- Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail Stop

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

**Enter a search condition:**

`'1'='2' UNION SELECT NUMTOYMINTERVAL(1,'AAAAAAAAAABBBBBBBE` Ask Oracle

**NUMTOYMINTERVAL**

Done Internet





http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond='1'='2'+UNION+SELECT+NUMTOY - Microsoft Internet ...

File Edit View Favorites Tools Help

http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond='1'='2'+UNION+SELE

Back Forward Stop Home Search Favorites Media Refresh Print Mail Stop

Address http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%27%27+UNION+SELECT+NUMTOYM Go Links

Google Search Web Search Site Options

## JSP Error

---

**Exception:**

```
java.sql.SQLException: No more data to read from socket
    at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:134)
    at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:179)
    at oracle.jdbc.dbaccess.DBError.check_error(DBError.java:1160)
    at oracle.jdbc.ttc7.MAREngine.unmarshalUB1(MAREngine.java:963)
    at oracle.jdbc.ttc7.MAREngine.unmarshalSB1(MAREngine.java:893)
    at oracle.jdbc.ttc7.Oclose.receive(Oclose.java:101)
    at oracle.jdbc.ttc7.TTC7Protocol.close(TTC7Protocol.java:683)
    at oracle.jdbc.driver.OracleStatement.close(OracleStatement.java:644)
    at _demo._sql._jdbc._JDBCQuery.runQuery(_JDBCQuery.java:54)
    at _demo._sql._jdbc._JDBCQuery._jspService(_JDBCQuery.java:147)
    at oracle.jsp.runtime.HttpJsp.service(HttpJsp.java)
```

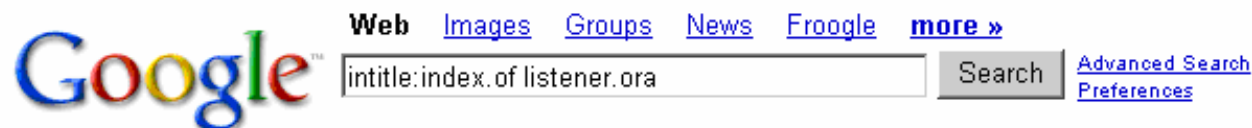
Done Internet

# Example – Directory Indexing

- Common feature
  - Displays list of files in a directory
  - If sensitive files exist in directory, easy to find
  - /demo/sql/tag/sample2.jsp
- Finding directory indexing
  - Google search value of “intitle:Index of”
- Looking for sensitive Oracle files with directory index
  - Listener.ora
  - Tnsnames.ora
  - Sqlnet.log
  - pwdSID.ora



# Directory Indexing in Oracle HTTP Servers



**Web** Results 1 - 6 of about 9 for **intitle:index.of listener.ora** with **Safesearch on**. (0.20 seconds)

Tip: Try [Google Answers](#) for help from expert researchers

## [Index of /afs/sipb/service/oracle/network/admin](#)

**Index of** /afs/sipb/service/oracle/network/admin. Name Last modified Size Description

Parent Directory - **listener.ora** 03-Oct-1999 18:31 632 sqlnet.fdf 03-Oct ...

[stuff.mit.edu/afs/sipb/service/oracle/network/admin/](#) - 2k - [Cached](#) - [Similar pages](#)

## [Index of /afs/sipb/service/oracle/network/admin](#)

**Index of** /afs/sipb/service/oracle/network/admin. Name Last modified Size Description

Parent Directory - tnsnames.ora 23-Apr-2001 00:31 311 **listener.ora** 03-Oct ...

[stuff.mit.edu/afs/sipb/service/oracle/network/admin/?C=S;O=A](#) - 2k - [Cached](#) - [Similar pages](#)

[ [More results from stuff.mit.edu](#) ]

## [Index of /oracle/nt](#)

**Index of** /oracle/nt. ... M bdesetup5.zip 04-Feb-2003 15:01 12.1M installInterfd.zip

30-Jul-2002 14:14 2.8M leadtools13.zip 24-Jan-2003 14:58 4.9M **listener.ora** 17-Apr ...

[www.rola.ch/oracle/nt/](#) - 3k - [Cached](#) - [Similar pages](#)

## [Index of /afs/net/project/afs32/andrew/wsadmin/ini/etc](#)

**Index of** /afs/net/project/afs32/andrew/wsadmin/ini/etc. ... 10 - killgetconsole

15-Jul-1996 15:00 1k killgetconsole.wrapper 15-Jul-1996 14:56 1k **listener.ora** 20- ...

[lost-contact.mit.edu/afs/net/project/afs32/andrew/wsadmin/ini/etc/](#) - 15k - [Supplemental Result](#) - [Cached](#) - [Similar pages](#)

## [Index of /afs/net/project/afs32/andrew/wsadmin/se/etc](#)

**Index of** /afs/net/project/afs32/andrew/wsadmin/se/etc. ... Aug-1996 12:11 1k hp-ux.bigData

08-May-1995 16:01 2.3M inetd.conf 07-Nov-1995 16:37 2k **listener.ora** 29-Feb ...

# How Do You Address These Vulnerabilities?

- Stay Patched
  - Stay on top of all the security alerts and bulletins
- Defense in Depth
- Multiple Levels of Security
  - Regularly perform audits and penetration tests on your database
  - Encryption of data-in-motion / data-at-rest / data-in-use
  - Monitor database activity log files
  - Implement application layer intrusion detection
    - Especially if you can't stay patched!

# How Do You Address These Vulnerabilities?

- “I’m running auditing, vulnerability assessment, and IDS tools for the network/OS. Am I secure?”
  - NO!!!!
- Databases are extremely complex beasts
- Databases store your most valuable assets
- Significantly more effort securing databases is necessary

“If your workstation gets hacked, that’s bad. But if your database gets hacked, you’re out of business.”

<http://www.devx.com/dbzone/Article/11961>

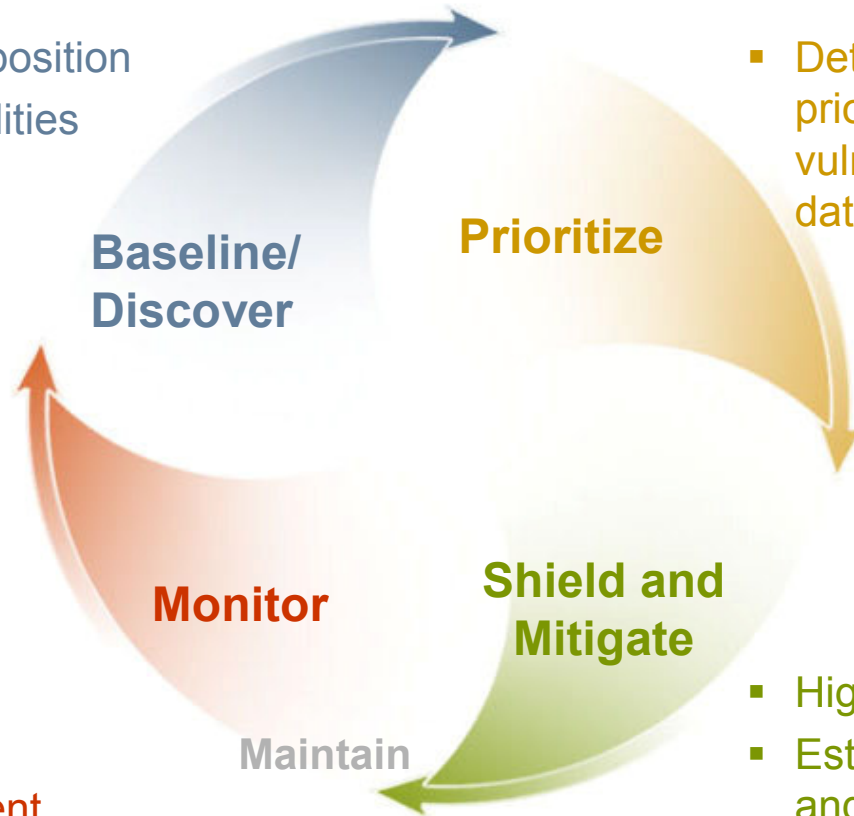
# Database Security Resources

- SQL Server Security
  - [www.SQLSecurity.com](http://www.SQLSecurity.com)
  - [www.microsoft.com/sql/techinfo/administration/2000/security/securingsqlserver.asp](http://www.microsoft.com/sql/techinfo/administration/2000/security/securingsqlserver.asp)
- Oracle Security
  - [www.sans.org/score/checklists/Oracle Database Checklist.doc](http://www.sans.org/score/checklists/Oracle_Database_Checklist.doc)
  - [otn.oracle.com/deploy/security/oracle9i/index.html](http://otn.oracle.com/deploy/security/oracle9i/index.html)
- Database Security alerts
  - [www.appsecinc.com/resources/maillinglist.html](http://www.appsecinc.com/resources/maillinglist.html)
- Database Security Discussion Board
  - [www.appsecinc.com/cgi-bin/ubb/ultimatebb.cgi](http://www.appsecinc.com/cgi-bin/ubb/ultimatebb.cgi)

# How Do You Secure Apps?

## Apply the vulnerability management lifecycle...

- Establish “as is” position
- Identify vulnerabilities
- Develop ideal baseline



- Determine risk and prioritize based on vulnerability data, threat data, asset classification

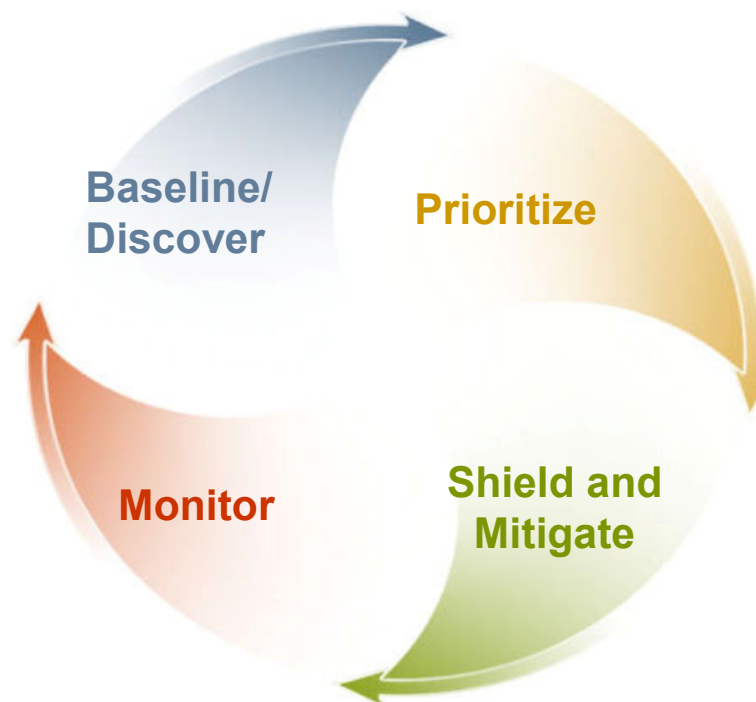
- Baseline compliance
- Vulnerabilities
- Threat environment

- High-priority vulnerabilities
- Establish controls and eliminate root causes

# Proactive Hardening

## Complete Database Vulnerability Assessment

- Database Discovery
- Penetration Testing
- Security Audit
- Reporting
- Remediation: Fix Scripts
- Enterprise-Class Features:
  - Easy to deploy: agent-less architecture, supports distributed engines
  - Easy to use: simple UI, save and edit policies, schedule and distribute tasks across multiple engines, correlate results
  - Easy to update: ASAP updates protect against latest threats
  - Complete: over 1,000 checks & tests across all major platforms



# Real-Time Monitor

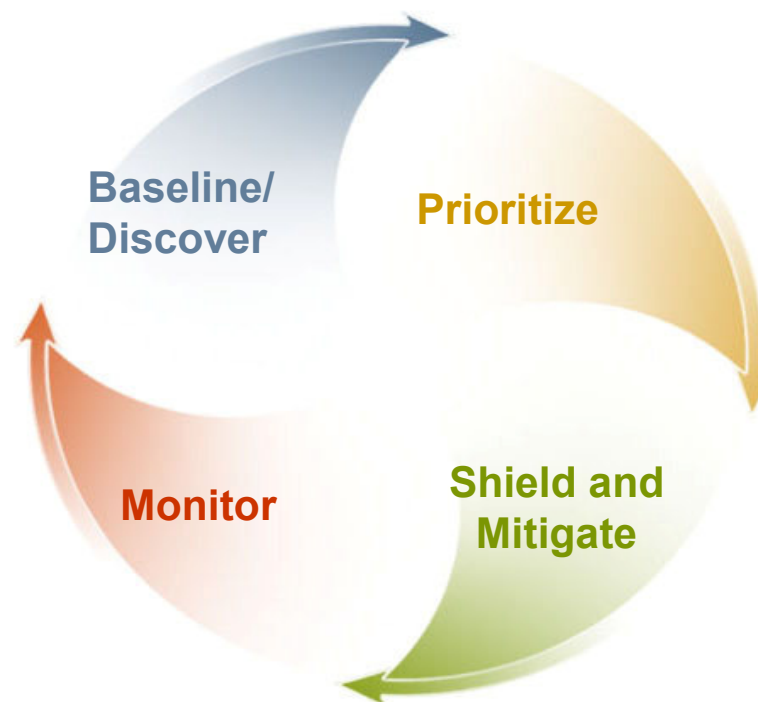
## Security Alerts + Focused, Granular Monitoring

- **Database IDS & Security Audit**

- Complex attacks
- Misuse and malicious behavior
- Without requiring native database auditing

- **Configurable Detection**

- Traditional security events: buffer overflows, password attacks, Web application attacks (SQL injection), privilege escalation
- Audit & System Events: events like SELECT ALL queries, by user, etc.
  - Application layer security demands
  - Contextual security auditing



# Last Line of Defense - Shield

## Usable Crypto for Production Databases

- **Column-level Encryption**
  - Selective protection
- **Built in Key Management**
  - Control Administrator rights
- **Easy to Implement**
  - Clustering / Mirroring
  - Back up / Disaster Recovery
- **Easy to Use**
  - Application Transparency
  - User Invisibility
- **Cryptographically Strong**
  - Broad set of algorithms



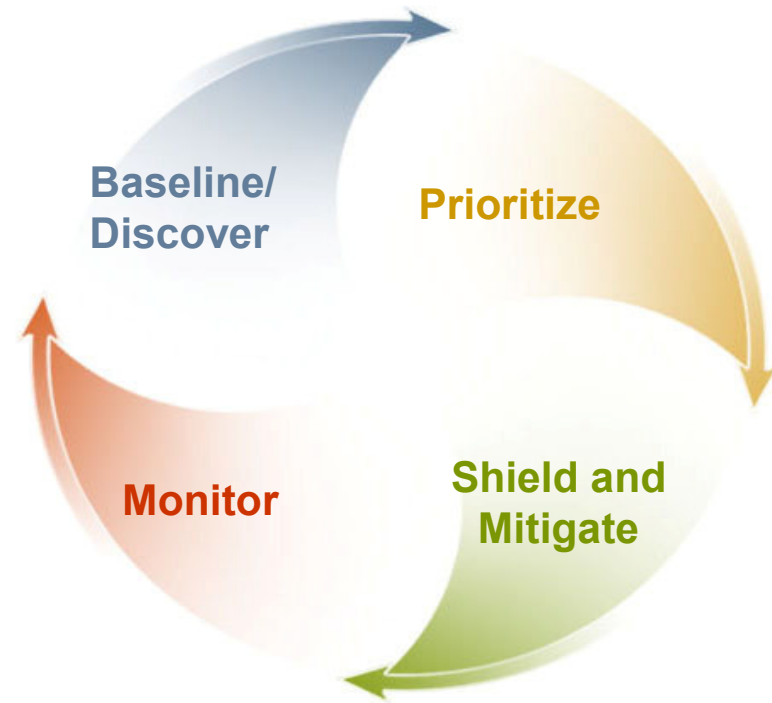


# Application Security Direction

- **Industry direction**
  - **More focused and complex attacks**
  - **Blended attacks**
  - **Increased audit and tracking requirements**
  - **Mixed Database vendors with less resources**

# AppSecInc Direction

- Product working closer to together
- Vulnerability scan feeding IDS monitoring
- Reporting across functions for compliance issues
- Security Change Audit tracking



# Application Security Inc Contacts

- [www.appsecinc.com](http://www.appsecinc.com)
- Chuck Dart, Regional Sales Manager  
[cdart@appsecinc.com](mailto:cdart@appsecinc.com)  
(972) 462 7724
- James Bleecker, Senior Sales Engineer  
[jbleecker@appsecinc.com](mailto:jbleecker@appsecinc.com)  
(949) 597 1326