

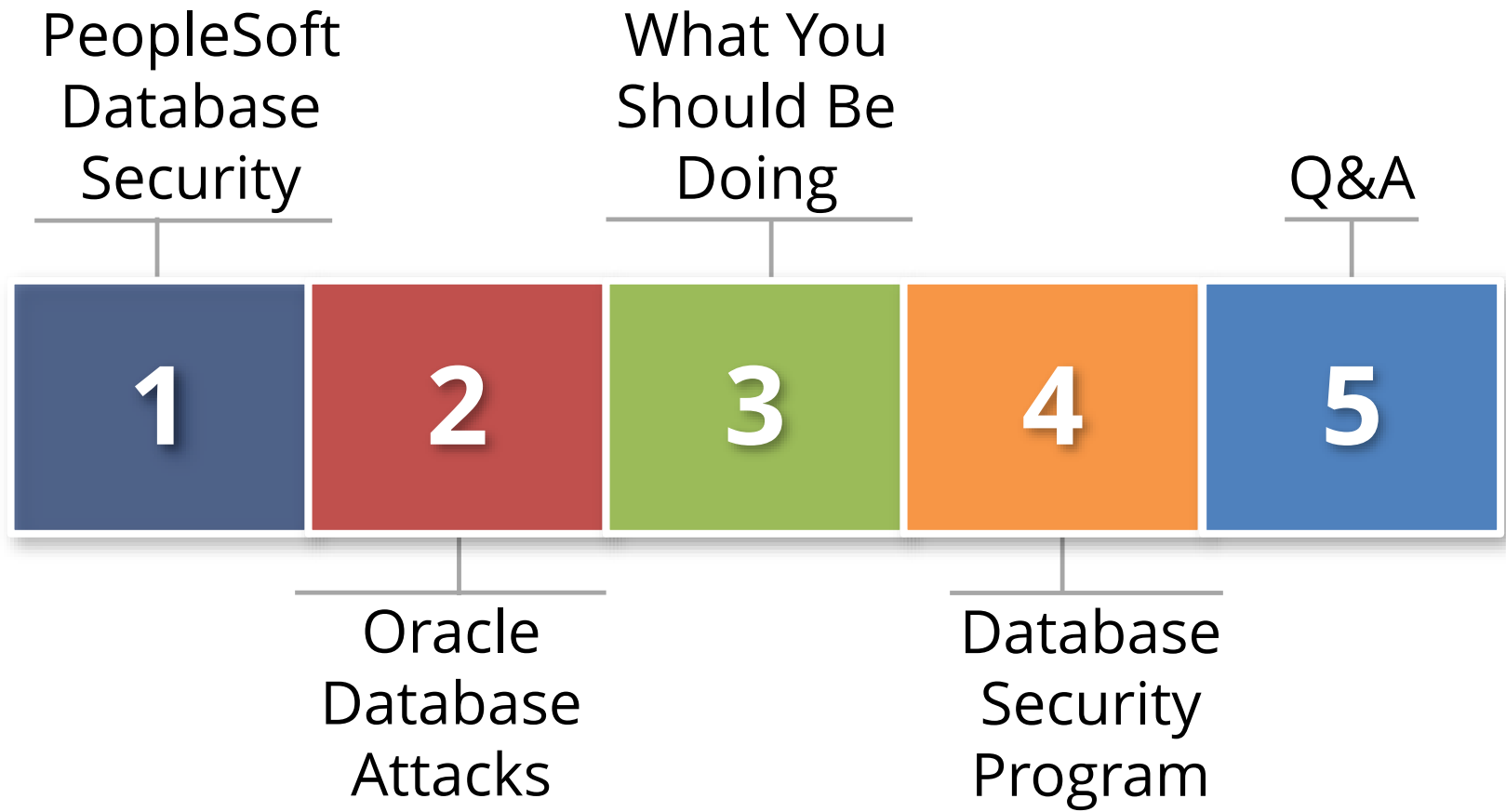
# PeopleSoft Database Security

**May 12, 2016**

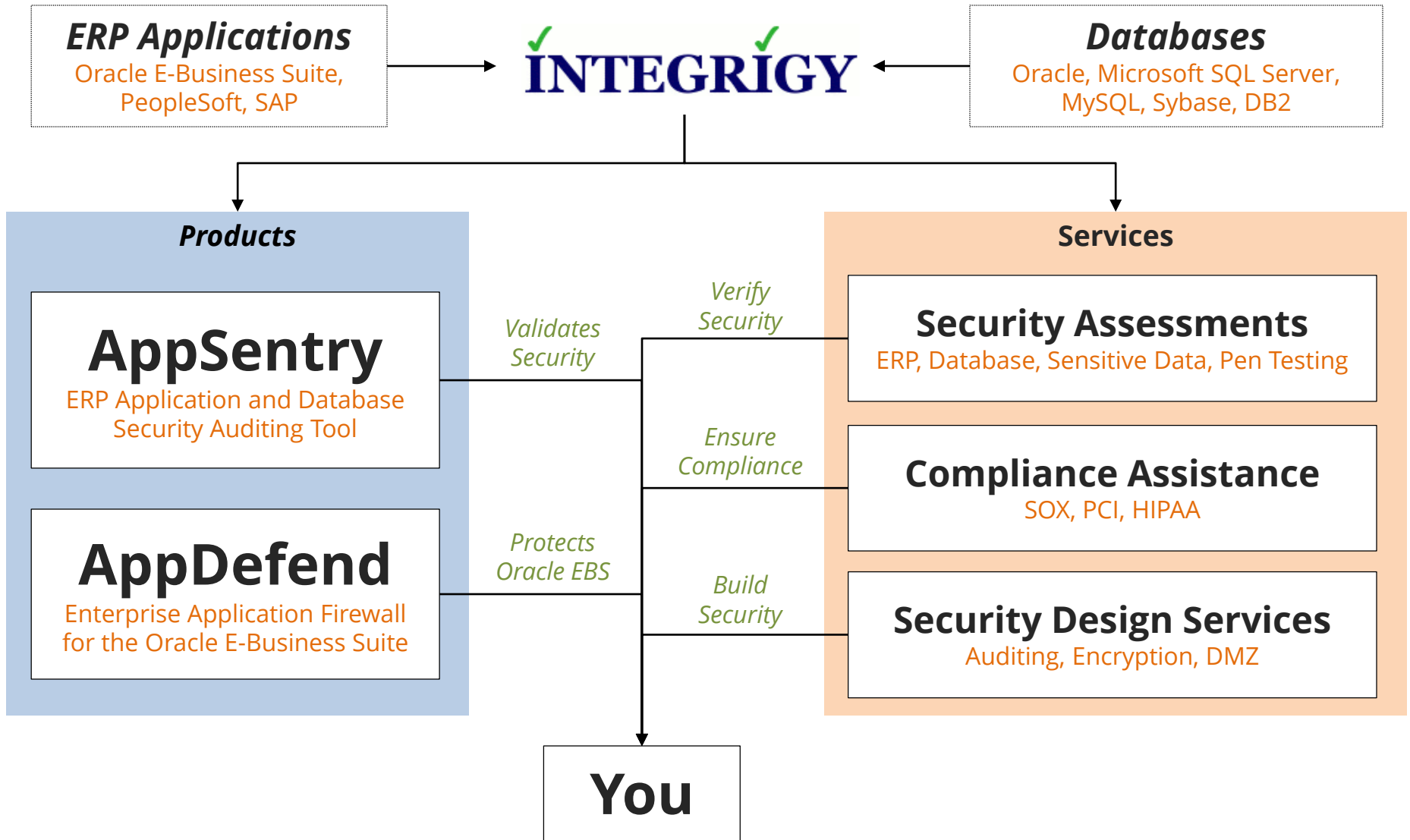
Michael Miller  
Chief Security Officer  
Integrigy Corporation

Phil Reimann  
Director of Business Development  
Integrigy Corporation

# Agenda



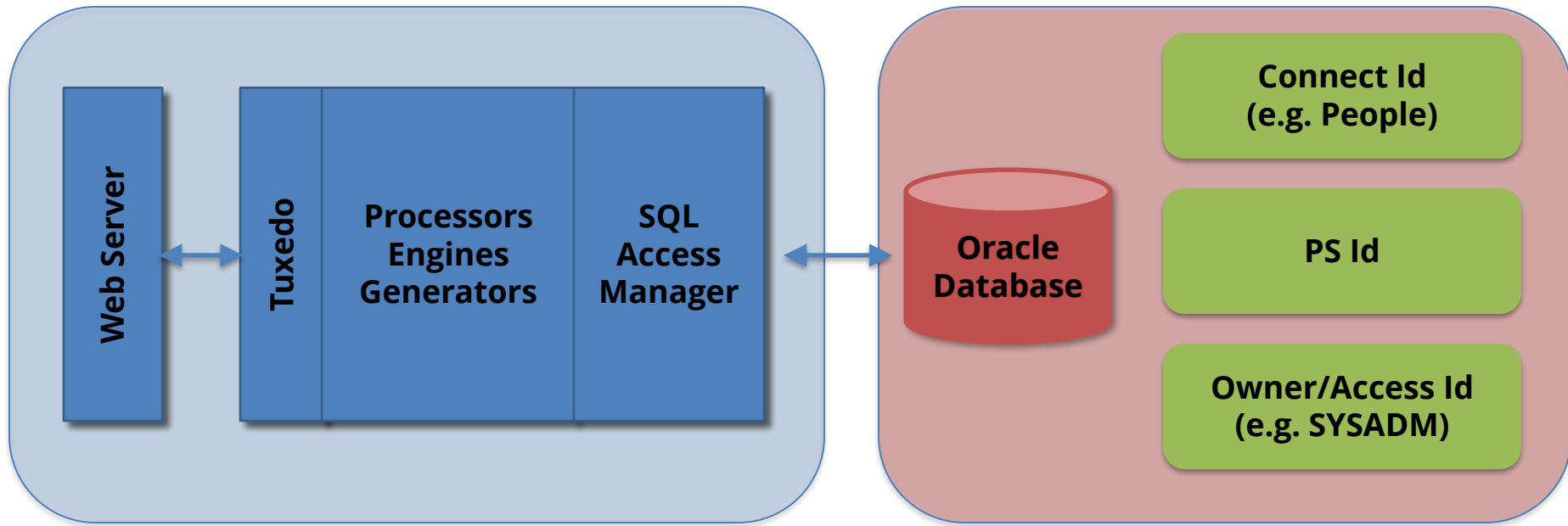
# About Integrigy



# Agenda



# PeopleSoft Oracle Database Usage

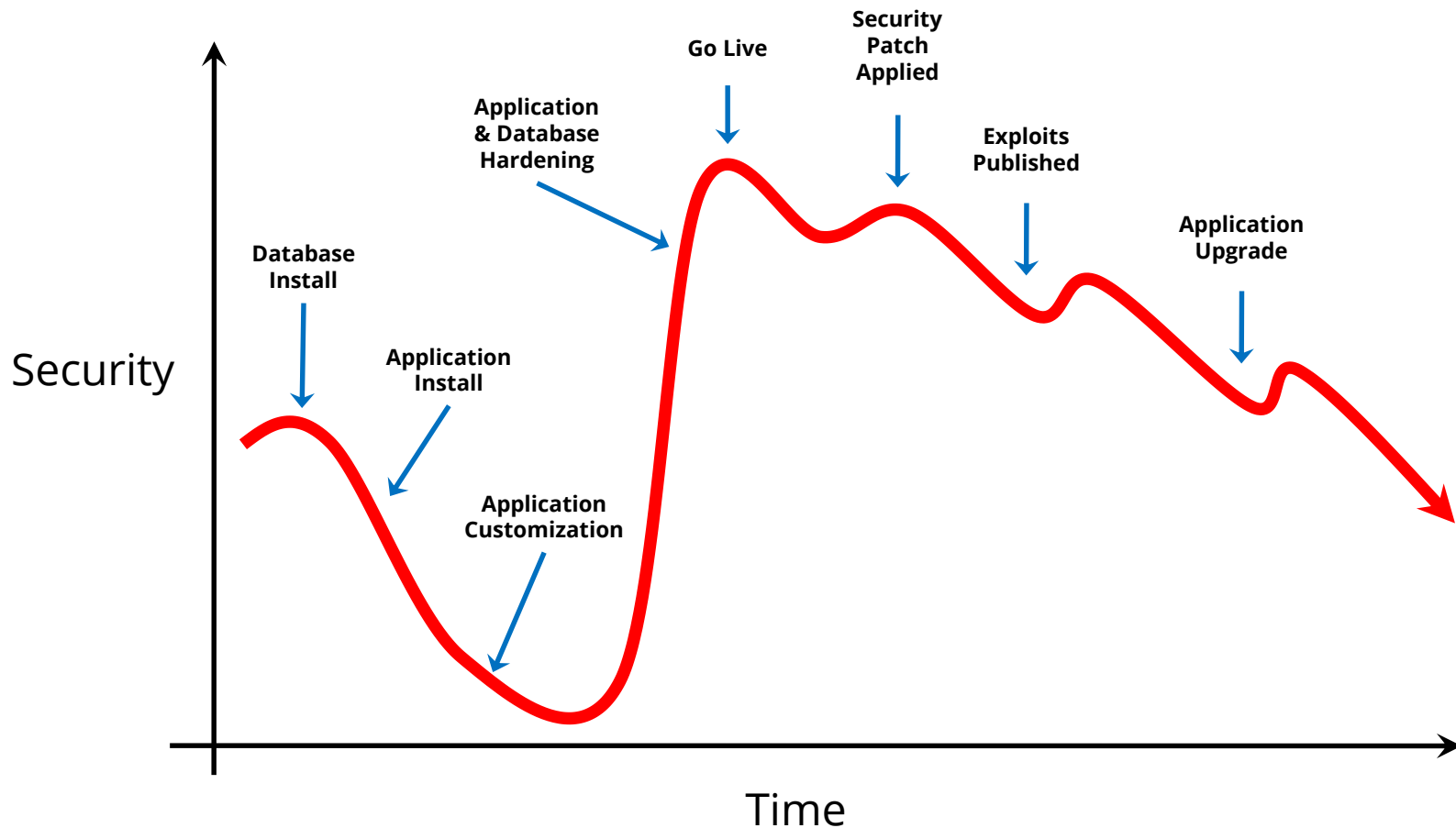


**Today's focus**

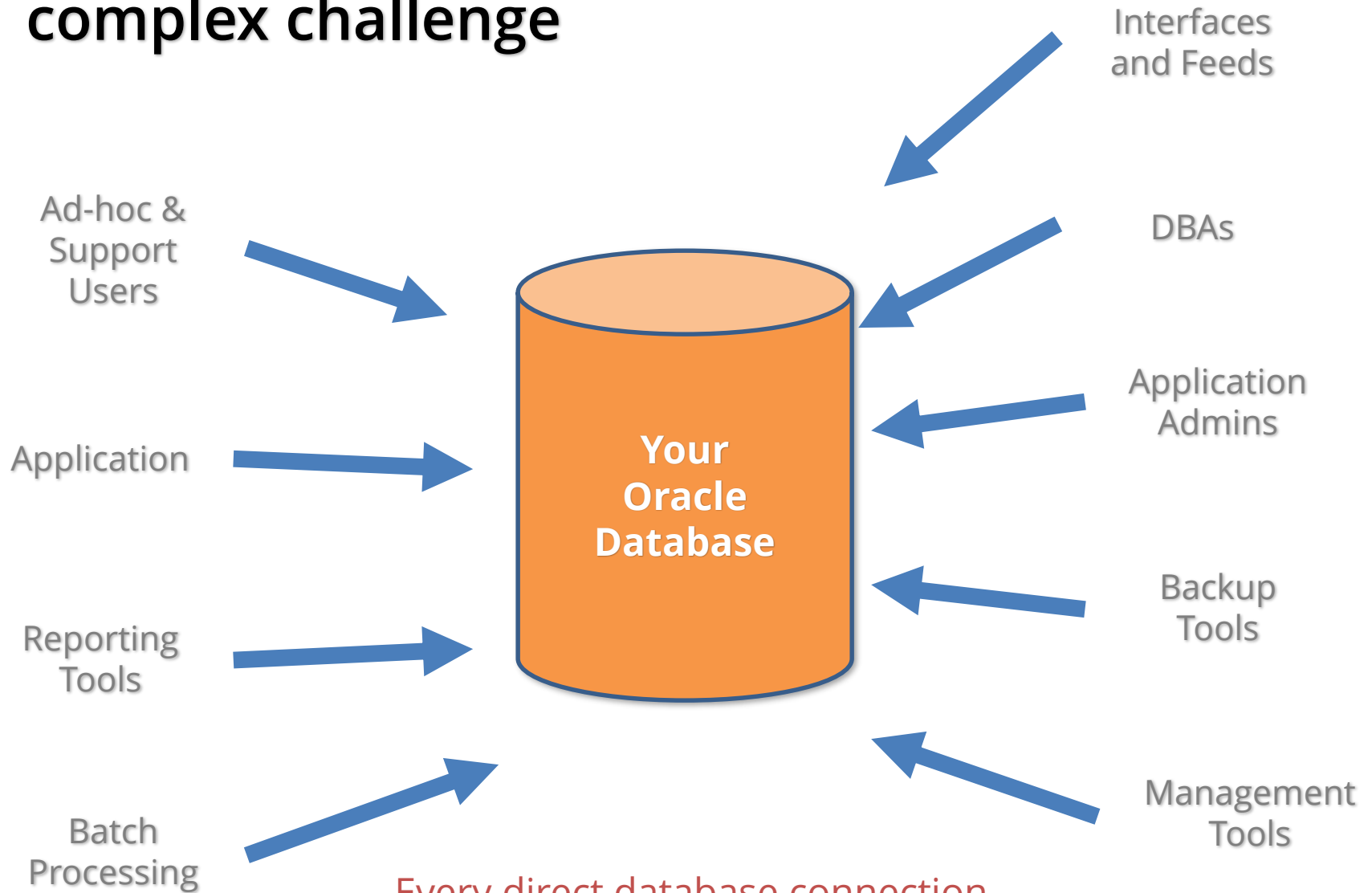
Does PeopleSoft protect and secure the database? **No**

# Database Security Decay

**Database security decays over time due to complexity, usage, application changes, upgrades, published security exploits, etc.**

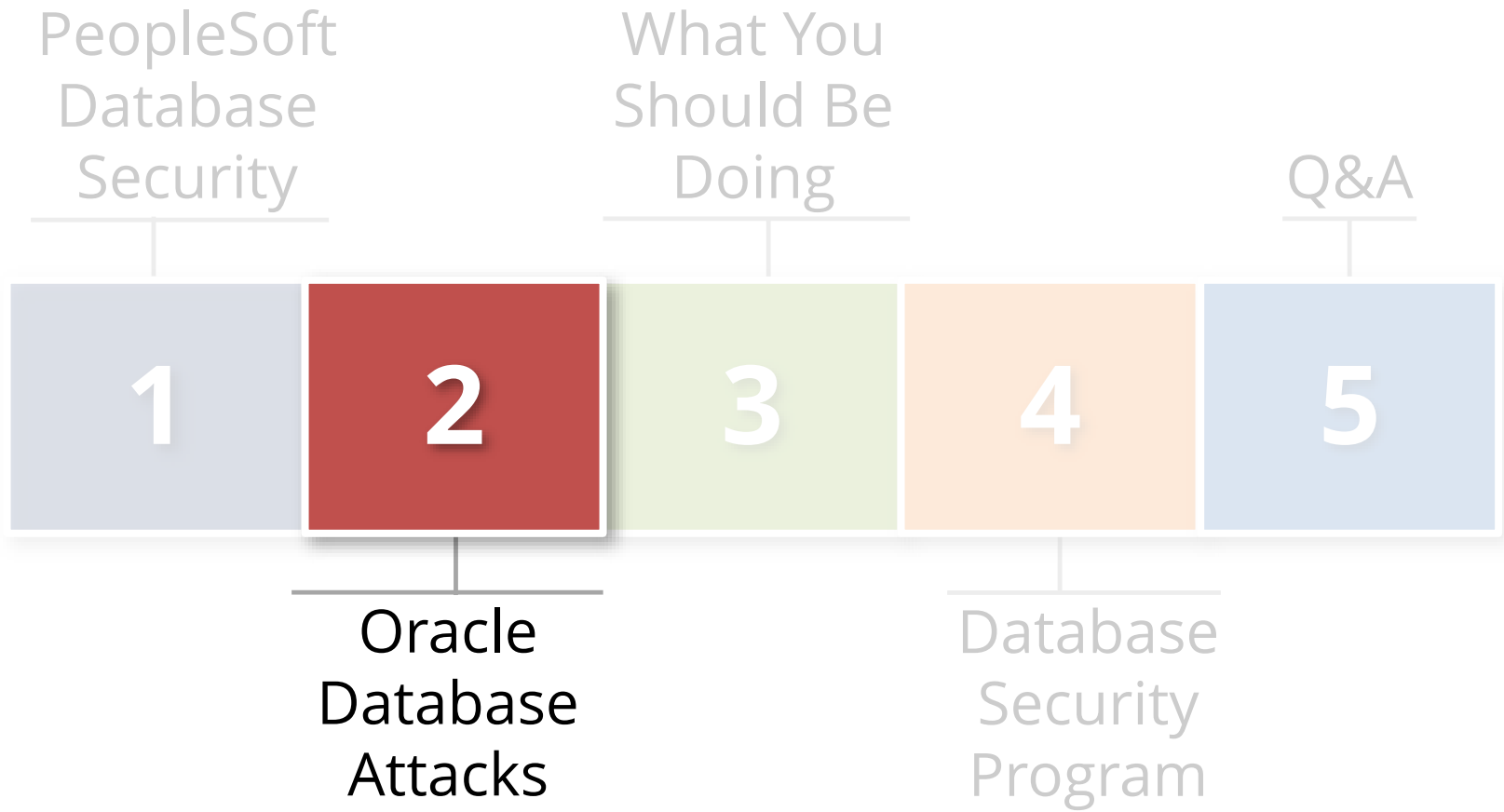


# Database Security is a complex challenge



Every direct database connection  
is a security risk

# Agenda





# Targeted Database Attacks

**Advanced Persistent Threat (APT)**

**Organized Crime**

**State Sponsored**

**Anonymous, LulzSec, Legion of Doom, ...**

# What is your data worth?\*

<b>\$1 – \$5</b>	<ul style="list-style-type: none"><li>▪ First and last name</li><li>▪ Social Security number</li></ul>	<b>Tax information (e.g., 1099)</b>
<b>\$20 – \$40</b>	<ul style="list-style-type: none"><li>▪ First and last name</li><li>▪ Social Security number</li><li>▪ Current address</li><li>▪ Date of birth</li></ul>	<b>Health care Human Resources</b>
<b>\$30 – \$100</b>	<ul style="list-style-type: none"><li>▪ First and last name</li><li>▪ Social Security number</li><li>▪ Current address</li><li>▪ Date of birth</li><li>▪ Bank account number or credit card number</li><li>▪ Salary</li></ul>	<b>Payroll</b>

\*Assuming financial and not political and/or hacktivist motivation

# Oracle Database Attack Tools

- **Used for both white-hat (good) and black-hat (evil)**
  - Mature, powerful and freely downloadable tools
  - Do not require expert Oracle knowledge
  - Most exploits seek to gain full control over database
  - Come with user guides and examples
  - Tools: Metasploit and Oracle Attack Tool
- **Older and unpatched versions of Oracle are much more vulnerable**
  - All databases with default and weak passwords are at risk

# Asset and Data Discovery Techniques

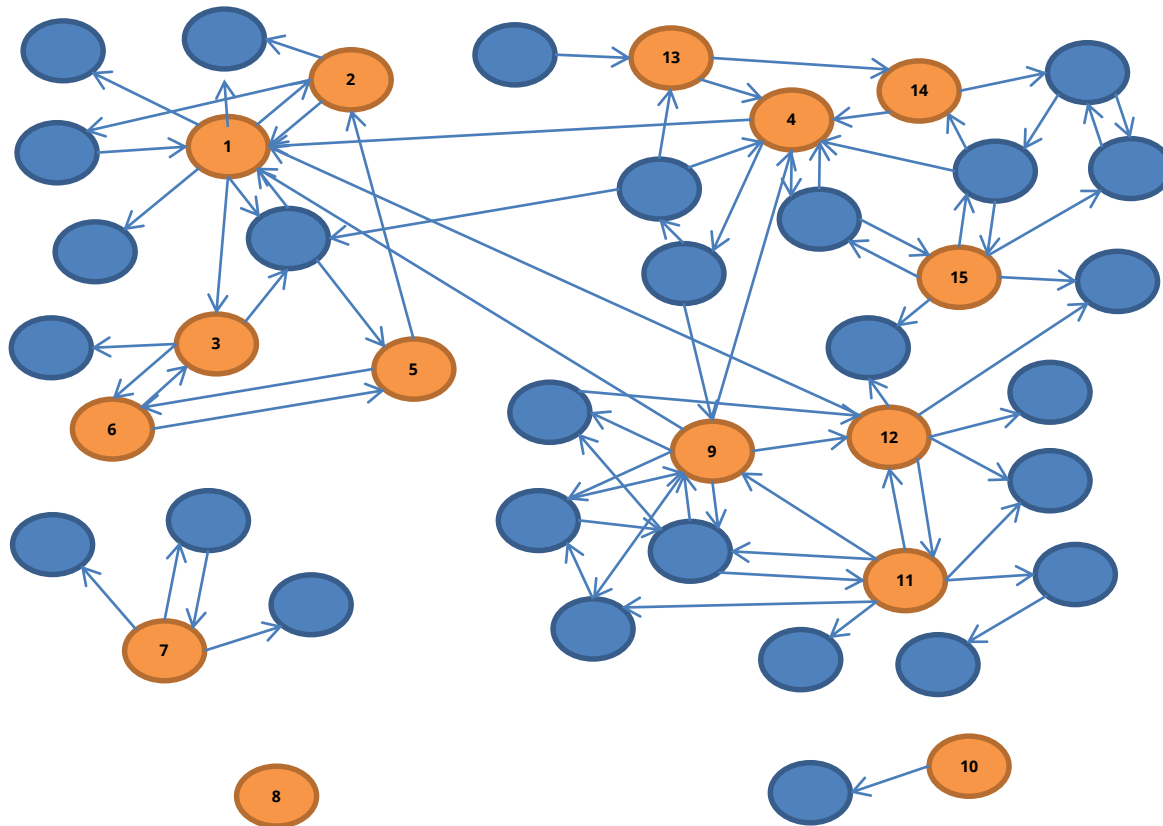
<b>Passive</b>	<ul style="list-style-type: none"><li>▪ Search internal knowledge repositories for architecture diagrams, design documents, code repositories, etc.</li><li>▪ Find TNSNAMES.ORA files</li></ul>
<b>Active</b>	<ul style="list-style-type: none"><li>▪ Compromise DBA credentials through phishing or social engineering attacks</li><li>▪ Install malware on DBA machines and steal credentials, such as saved in SQL Developer</li><li>▪ Use Nmap to scan internal network for Oracle Databases on default port 1521 – very noisy</li></ul>

# Default Oracle Password Statistics

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
<b>DBSNMP</b>	<b>DBSNMP</b>	<b>99%</b>	<b>52%</b>
<b>OUTLN</b>	<b>OUTLN</b>	<b>98%</b>	<b>43%</b>
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
<b>CTXSYS</b>	<b>CTXSYS</b>	<b>54%</b>	<b>32%</b>

\* Sample of 120 production databases

# Database Link Case Study



## Overview

- Organization with about 150 production Oracle Databases
- Integrity assessed 15 key SOX and PCI compliance Oracle databases
- Reviewed database links for connectivity and appropriateness

## Conclusion

Database links are widely used in most organizations

# TNS Poisoning Attack – Man-in-Middle

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
<b>CVE-2012-1675</b>	<b>Listener</b>	<b>Oracle Net</b>	<b>None</b>	<b>Yes</b>

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
<b>7.5</b>	<b>Network</b>	<b>Low</b>	<b>None</b>	<b>Partial+</b>	<b>Partial+</b>	<b>Partial</b>	<b>ALL VERSIONS</b>

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c and 11.2.0.4 protected by default, but vulnerable when Valid Node Checking Registration (VNCR) is disabled.

# TNS Poisoning Mitigation

<b><i>Database Version</i></b>	<b><i>SSL Encrypt with Cert</i></b>	<b><i>COST</i></b> <i>class of secure transport</i>	<b><i>VNCR</i></b> <i>Valid node checking registration</i>
<b><i>References</i></b>	See ASO	1453883.1 1340831.1 (RAC)	1600630.1
<b>8.1.7.x – 10.2.0.3</b>	✓		
<b>10.2.0.3 – 10.2.0.5</b>	✓	✓	
<b>11.1.0.x</b>	✓	✓	
<b>11.2.0.1 – 11.2.0.3</b>	✓	✓	
<b>11.2.0.4*</b>	✓	✓	✓ (Enabled by default)
<b>12.1.0.x*</b>	✓	✓	✓ (Enabled by default)

\* 11.2.0.4 and 12c does not allow remote registration by default.



# Agenda



# Traditional Database Security Approaches

**Database security checklists** are used to secure databases one at a time.

- **Excellent baseline and starting point**
  - Example: US DoD DISA STIG <http://iase.disa.mil/stigs/app-security/database/Pages/index.aspx>
- **Often in conflict with application configuration**
- **Too many exceptions required to handle application limitations**
- **Security decay requires constant or periodic assessments**

# Supported Database Versions and CPUs

		PeopleTools					
		8.55	8.54	8.53	8.52	8.51	8.5
Database	12.1.0.2	✓	✓	✓	✓		
	12.1.0.1 (7/2016)		✓	✓	✓		
	11.2.0.4 (10/2020)	✓	✓	✓	✓	✓	✓
	11.2.0.3			✓	✓	✓	✓
	11.2.0.2					✓	✓
	11.1.0.7			✓	✓	✓	✓
	10.2.0.5			✓	✓	✓	✓

Do you need to apply both application and database CPUs? **Yes**

Is database security more than just applying CPUs? **Yes**

# Integrigy #1 Security Recommendation

- **Limit direct database access whenever possible**
  - Much harder to hack database if attacker can not connect
- **Use firewalls in front of data center, network ACLs, TNS invited nodes, Oracle Connection Manager, Oracle Database Firewall, etc.**
  - DBAs should use bastion hosts to manage databases

# Database Security Preventative Controls

- **Apply Oracle Critical Patch Updates on a regular basis on all databases**
  - Reduce risk of compromise and escalation of privileges
- **October 2014 PeopleTools CPU must be applied**
  - Connect ID used to authenticate users has access to the table PSACCESSPRFL
  - Script to decrypt to Access ID password freely available on Internet
  - CPU changes encryption: 8.52.24, 8.53.17, 8.54.04

# PeopleSoft Database Security Specific Controls

- **Secure PeopleSoft database passwords**
  - Secure key accounts: Connect Id, Access Id, IB and PS
  - Change regularly and no defaults e.g. PEOPLE/PEOP1e
  - Password should never equal username or be shared
- **Default tablespace should never be 'SYSTEM'**
  - Never for Connect ID
  - Only SYS and SYSTEM should use the SYSTEM tablespace
- **Encrypt SYSADM password**
  - Use psadmin utility to encrypt passwords in config files
- **Ensure EnableDBMonitoring is ALWAYS enabled**
  - Enabled by Default (psappssrv.cfg)
  - Populates client\_info with user, IP address and program name

# PeopleSoft Database Security Specific Controls

- **One PeopleSoft database per Oracle RDBMS instance**
  - Production must be exclusive
  - No demo databases for production
- **User tablespaces should never use PSDEFAULT**
  - Reserve for application use only
- **Do not use SYSADM for day-to-day support**
  - Use named accounts
- **Check for Public grants**
  - Any connection to the database has 'PUBLIC'

# PeopleSoft – Application

- **Application Accounts**

- Standard accounts and default passwords
- Password policies

- **Application authorization**

- Guest account menus and roles
- Administrator and webprofile roles
- Sensitive roles and menus
- PeopleTools

- **Application auditing**



# PeopleSoft - Additional

- **WebLogic**
  - Passwords
  - Security baseline
  - Console security and whitelisting
- **Security settings**
  - Web portal
  - Jolt
  - Tuxedo
  - Integration Broker
- **PSKEY password and template file encryption**

# Create Fewer Insiders With Password Controls

- 1 Don't share passwords between production and non-production**
- 2 Rotate passwords regularly**
- 3 Use a password safe**
- 4 Don't forget about Oracle database default accounts**

# Constantly Check for Weak and Default Passwords

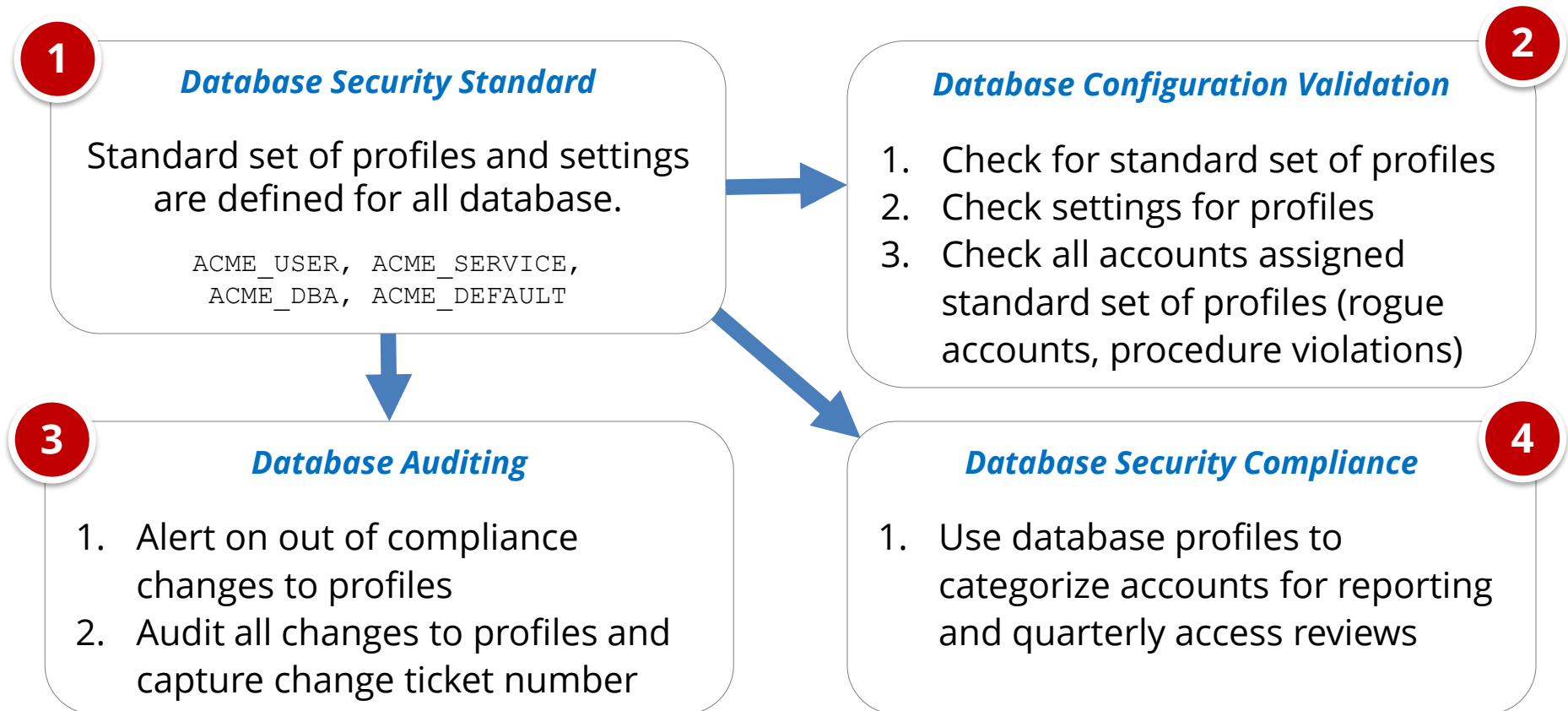
- **Use Oracle's DBA\_USERS\_WITH\_DEFPWD**
  - Limited set of accounts
  - Single password for each account
- **Command line tools (orabf, etc.)**
  - Difficult to run – command line only
- **AppSentry**
  - Checks all database accounts
  - Uses passwords lists - > 1 million passwords
  - Allows custom passwords

# Use Database Profiles to Manage Passwords by Risk

Profile Name	Accounts
<b>DEFAULT</b>	None
<b>&lt;your org&gt;_PROFILE</b>	All named accounts
<b>DB_PROFILE</b>	All standard Oracle Database accounts and all non-interactive application accounts (e.g. SYS, SYSTEM, DBSNMP, CTXSYS, etc.)
<b>APP_PROFILE</b>	All interactive application databases including web application and interface accounts (e.g. PS owner, access and PS IDs)

Resource Name	Current Default	Suggested Default	<your org>_PROFILE	DB_PROFILE	APP_PROFILE
FAILED_LOGIN_ATTEMPTS	UNLIMITED	10	5	10	UNLIMITED
PASSWORD_GRACE_TIME (Days)	UNLIMITED	7	10	10	UNLIMITED
PASSWORD_LIFE_TIME (Days)	UNLIMITED	180	90	365	UNLIMITED
PASSWORD_LOCK_TIME (Days)	UNLIMITED	1	DEFAULT	DEFAULT	DEFAULT
PASSWORD_REUSE_MAX (Passwords)	UNLIMITED	UNLIMITED	DEFAULT	DEFAULT	DEFAULT
PASSWORD_REUSE_TIME (Days)	UNLIMITED	UNLIMITED	DEFAULT	DEFAULT	DEFAULT
PASSWORD_VERIFY_FUNCTION	NULL		XORG_VERIFY_FUNC	XORG_VERIFY_FUNC	XORG_VERIFY_FUNC
Database Accounts	None	None	All individual accounts	All standard Oracle DB accounts	All interactive application accounts

# Operational Controls Around Oracle Password Profiles

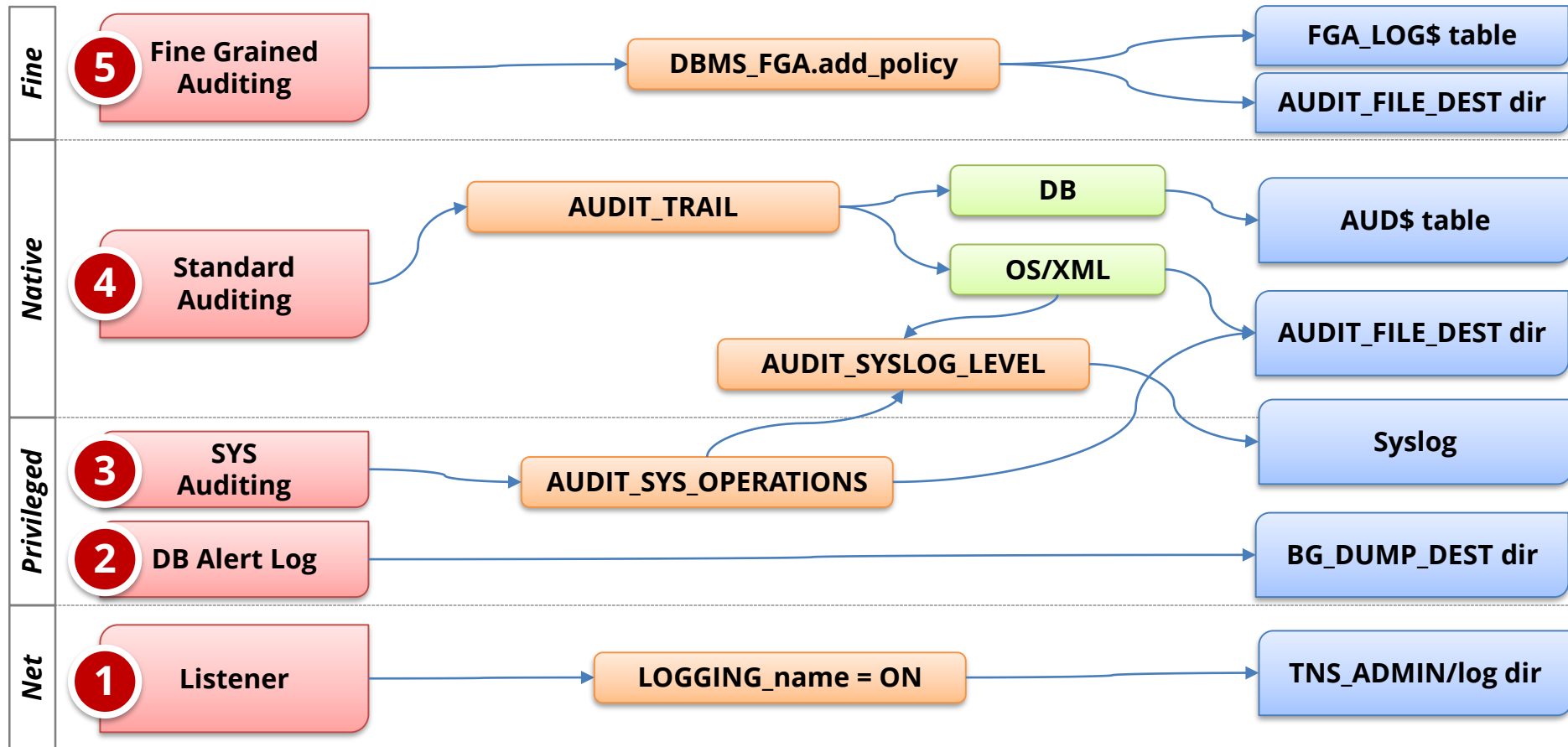


# Generate and Use Database Audit Data

Database auditing in most organizations done simply for a **compliance checkbox**.

- **Auditing poorly defined**
- **No review of audit data**
- **No mapping of business requirements to auditing, alerts, or reports**
- **Zero value to the organization**

# Native Oracle Database Auditing



Type of auditing and logging

Audit and logging parameters

Location of audit data

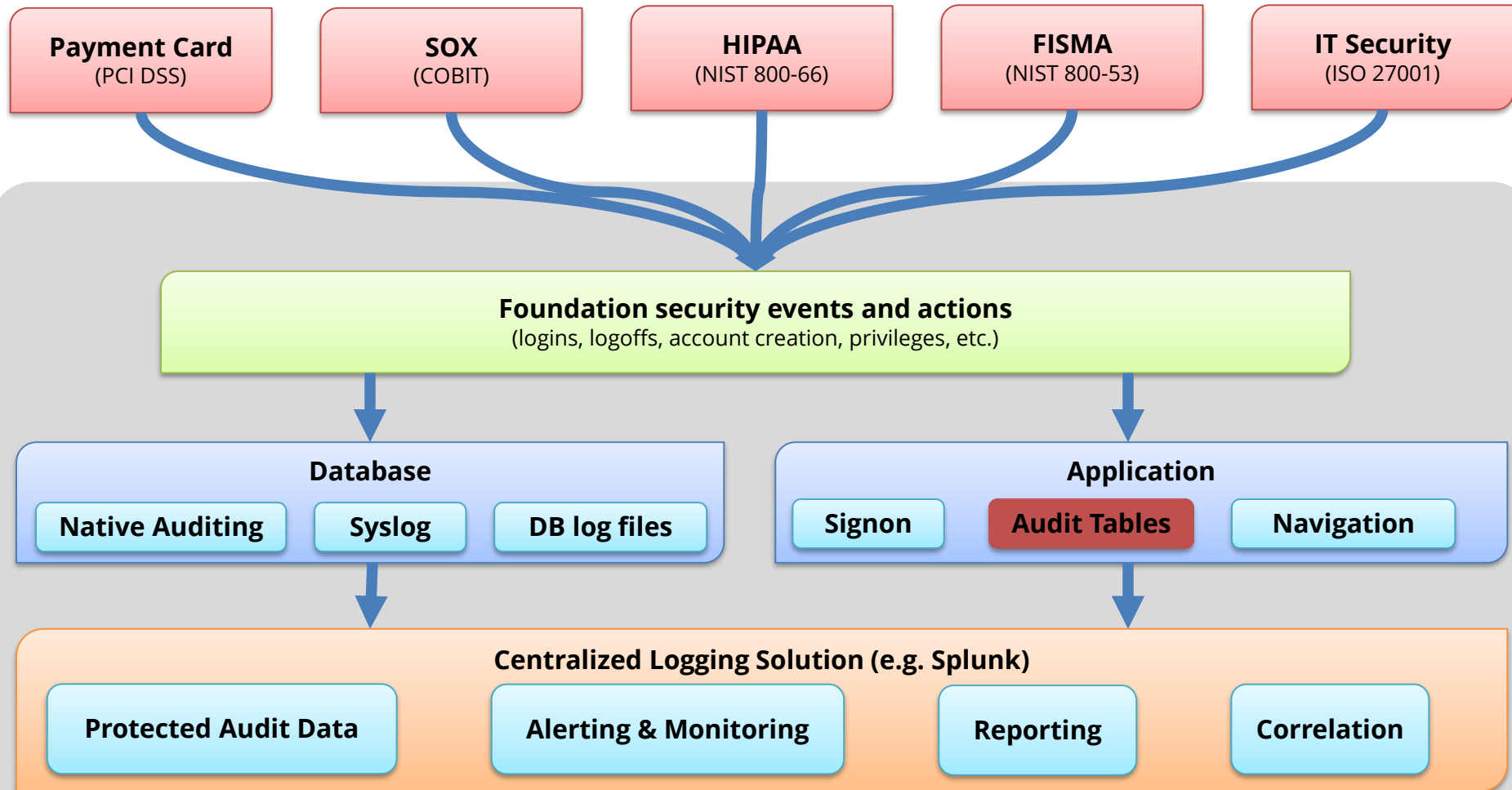
# Database Auditing and Monitoring

## **Intelligent and business-focused auditing and monitoring**

- **Transform audit data into actionable information**
- **Use auditing as mitigating control when necessary**
- **Auditing is in harmony with database security program to proactively identify non-compliance**
- **Solve compliance and security challenges – change ticket tracking and workflow**



# Integrity Framework for Database Auditing



*Integrity Framework for Auditing and Logging*

<http://www.integrity.com/security-resources/integrity-guide-database-auditing-and-logging>

# Foundation Security Events and Actions

The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

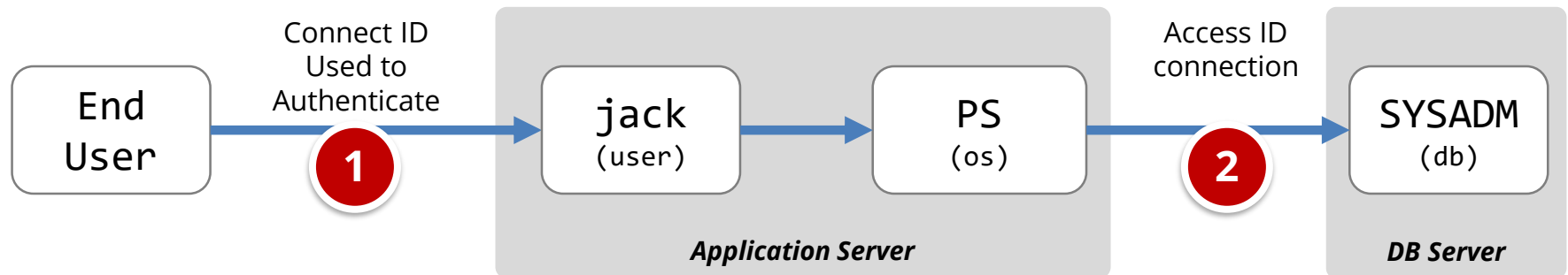
<b><i>E1 - Login</i></b>	<b><i>E8 - Modify role</i></b>
<b><i>E2 - Logoff</i></b>	<b><i>E9 - Grant/revoke user privileges</i></b>
<b><i>E3 - Unsuccessful login</i></b>	<b><i>E10 - Grant/revoke role privileges</i></b>
<b><i>E4 - Modify auth mechanisms</i></b>	<b><i>E11 - Privileged commands</i></b>
<b><i>E5 - Create user account</i></b>	<b><i>E12 - Modify audit and logging</i></b>
<b><i>E6 - Modify user account</i></b>	<b><i>E13 - Create, Modify or Delete object</i></b>
<b><i>E7 - Create role</i></b>	<b><i>E14 - Modify configuration settings</i></b>

# Foundation Security Events Mapping

<b>Security Events and Actions</b>	<b>PCI DSS 10.2</b>	<b>SOX (COBIT)</b>	<b>HIPAA (NIST 800-66)</b>	<b>IT Security (ISO 27001)</b>	<b>FISMA (NIST 800-53)</b>
E1 - Login	10.2.5	A12.3	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	DS5.5	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - Modify authentication mechanisms	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E5 – Create user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E6 - Modify user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E7 - Create role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E8 - Modify role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E9 - Grant/revoke user privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E10 - Grant/revoke role privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E11 - Privileged commands	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E12 - Modify audit and logging	10.2.6	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-9
E13 - Objects Create/Modify/Delete	10.2.7	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-14
E14 - Modify configuration settings	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2

# Application End User Tracking – **Solution**

**EnableDBMonitoring** allows database auditing to capture web application end-users and correlate the application end-user to SQL statements.

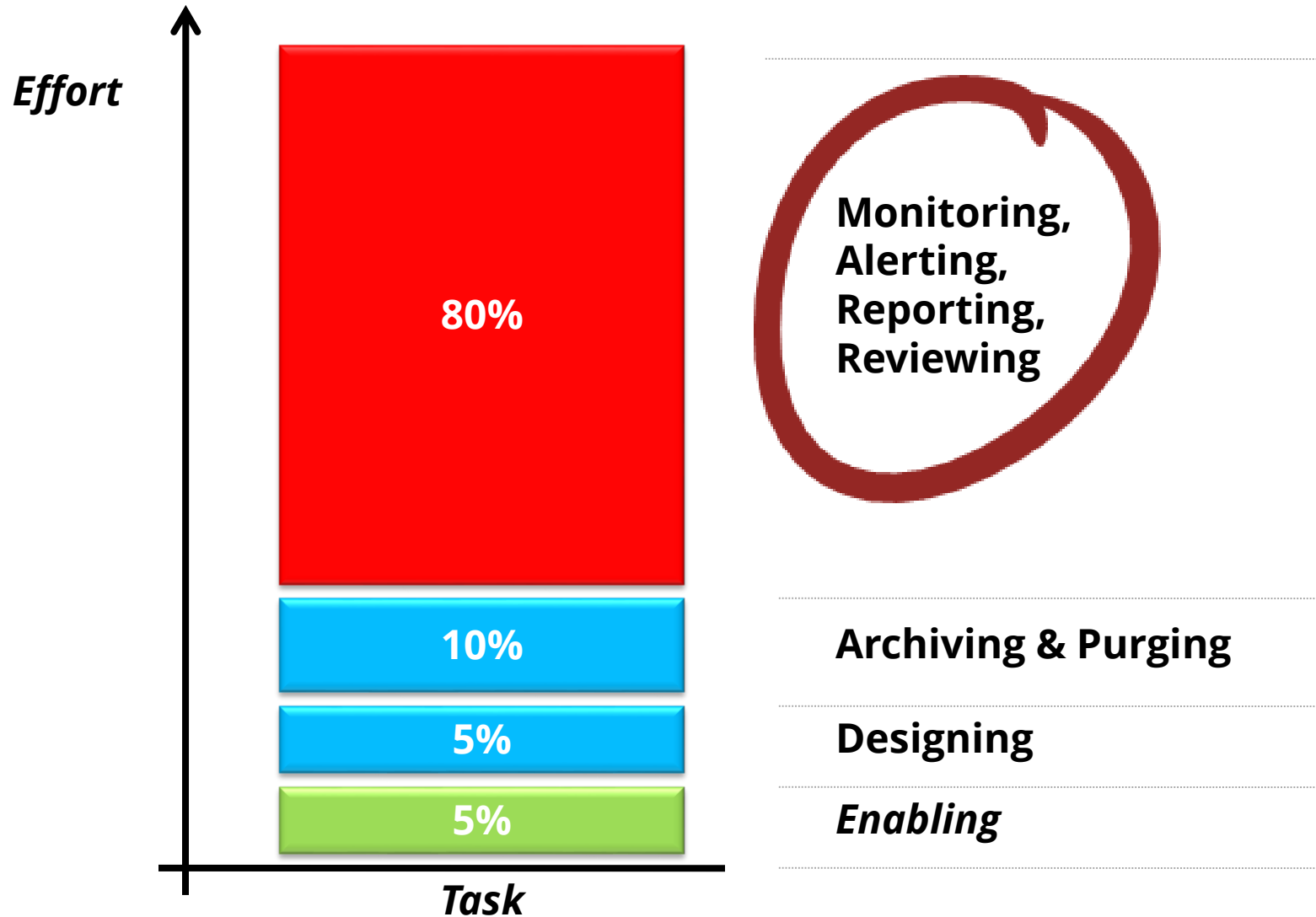


## Use CLIENT\_INFO for DAM solutions (e.g. Splunk)

DB User	OS User	Client IP	Program	SQL	Application User
SYSADM	PS	192.168.1.11	PSAPPSRV.exe	select * from ps_person	jack

```
select sid,serial#,username, program, module, client_info from v$session
```

# Database Auditing Effort by Task



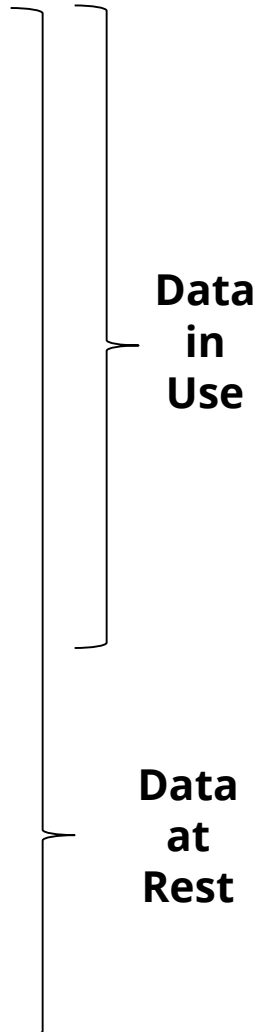
# Encryption Options

- **Storage (Data at rest)**
  - **Disk, storage, media level encryption**
  - Encryption of data at rest such as when stored in files or on media
- **Access (Data in use)\***
  - **Application or database level encryption**
  - Encryption of data with access permitted only to a subset of users in order to enforce segregation of duties
- **Network (Data in motion)**
  - **Encryption of data when transferred between two systems**
  - SQL\*Net encryption (database)

# Misconceptions about Database Storage Encryption

- **Not an access control tool**
  - Encryption does not solve access control problems
  - Data is encrypted the same regardless of user
  - Coarse-grained file access control only
- **No malicious employee protection**
  - Encryption does not protect against malicious privileged employees and contractors
  - DBAs have full access
- **Key management determines success**
  - Access to Oracle wallets (TDE) controls everything
  - You and only you can should control the keys
- **More is not better**
  - Performance cost of encryption
  - Cannot encrypt everything

# Storage/Access Oracle Encryption Solutions

<b>Application</b> (access ~ role)	<ul style="list-style-type: none"><li>▪ <b>PeopleCode Encryption</b></li><li>▪ Database Encryption API (DBMS_CRYPTO/Voltage)</li></ul>	 <b>Data in Use</b>
<b>Database</b> (access ~ db account)	<ul style="list-style-type: none"><li>▪ <b>View/Trigger Encryption</b></li></ul>	
<b>Disk/Storage</b> (access = database)	<ul style="list-style-type: none"><li>▪ <b>Transparent Data Encryption (TDE)</b></li><li>▪ Third-party Solutions (e.g., Vormetric)</li><li>▪ Disk/SAN Vendor Encryption Solutions</li><li>▪ Backup Encryption (e.g., RMAN)</li></ul>	<b>Data at Rest</b>



# PeopleTools Application Encryption

- **Encrypt, decrypt, sign, and verify fields in a database or external files**
  - Obtain library (e.g. PGP). Open source OpenSSL provided.
  - Develop API glue code to library (if not OpenSSL or PGP)
  - Write PeopleCode to invoke
- **Note full table encryption (PTENCRYPTPET/PTDECRYPTPET) “ is not intended for widespread usage”**
  - Used to encrypt encryption keys (DOC ID 1382024.1)
- **PeopleTools Application Designer option for field “column” level encryption with Oracle TDE**
  - Will cover later

[http://docs.oracle.com/cd/E66686\\_01/pt855pbr0/eng/pt/tsec/concept\\_UnderstandingPeopleSoftEncryptionTechnology-c07784.html](http://docs.oracle.com/cd/E66686_01/pt855pbr0/eng/pt/tsec/concept_UnderstandingPeopleSoftEncryptionTechnology-c07784.html)

# What is Oracle TDE?

- **Transparent database encryption**
  - Requires no application code or database structure changes to implement
  - Only major change to database function is the Oracle Wallet must be opened during database startup
  - Add-on feature licensed with Advanced Security Option
- **Column or Full Tablespace**
- **Column encryption restrictions (not Tablespace)**
  - Cannot be a foreign key or used in database constraint
  - Only simple data types like number, varchar, date, ...
  - Less than 3,932 bytes in length

# What does TDE do and not do?

- **TDE only encrypts “data at rest”**
- **TDE protects data if following is stolen or lost -**
  - disk drive
  - database file
  - backup tape of the database files
- **An authenticated database user sees no change**
- **Does TDE meet legal requirements for encryption?**
  - California SB1386, Payment Card Industry Data Security
  - Ask your legal department

# PeopleSoft Oracle TDE Support

- **Supports both Column and Tablespace Encryption**

- Column 'field' encryption supported from Application Designer (e.g. Social Security Number field is tagged for encryption)
- No changes required for Tablespace encryption

- **Certifications**

- PeopleTools release 8.46 and higher on Oracle 10gR2 and higher can use TDE column encryption
- PeopleTools release 8.48 and higher on Oracle 11g and higher can use TDE tablespace encryption

- **More information:**

<http://www.oracle.com/technetwork/database/security/rp-tse-ptools-8-134112.pdf>

# Consider Using Oracle Database Vault

- **Enhanced data protection**
  - Prevent ad-hoc access to sensitive data by privileged users
  - Define and enforce trusted paths & operational controls
  - Segregation of duties between DBA and security administrator
- **Layer on top of existing database**
  - No effect on direct object privileges or PUBLIC object privileges
- **Rule driven**
  - Control individual SQL commands, privileges
  - Control by IP address, time, etc.
- **Includes audit reporting**
  - Privilege analysis and success/failure
- **Add-on option, licensed separately**
  - PeopleTools 8.46 and higher
  - Out-of-box realms for PeopleSoft

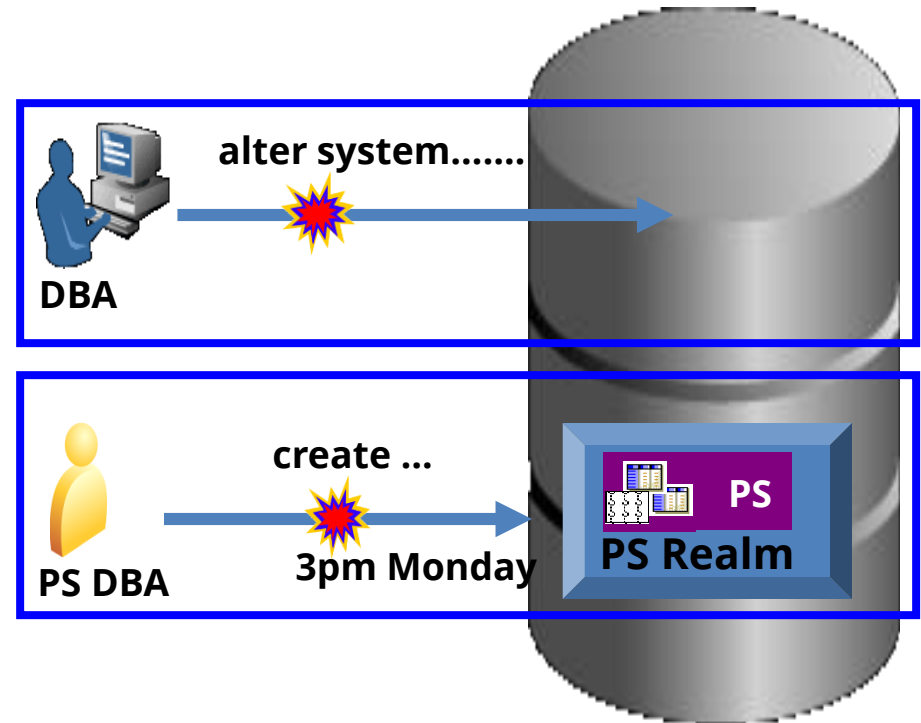
# Oracle Database Vault

- Database DBA attempts remote *"alter system"*

Rule based on IP Address blocks action

- PeopleSoft DBA performs unauthorized actions during production

Rule based on Date and Time blocks action



Factors and Command Rules provide flexible and adaptable security controls

# Database Vault Support for PeopleSoft

- **Database realm for PeopleSoft**
  - Default realm protects all PeopleSoft data against unauthorized access by privileged users and DBAs
- **New PSFTDBA account created for DBAs**
  - Blinds DBAs to PS data while allowing day-to-day support
  - Access Id used only by application
  - Recommend auditing usage of Access Id, SYSTEM, SYSDBA
- **Filters for direct database access using Connect command rules**
  - Pre-defined list of processes: middle tier, PeopleTools, Cobol
  - Recommend extending to specify IP address or hostname

*Value proportionately diluted by who has what password*

# Database Vault Protection Matrix (Default)

Database Vault	Access Id (SYSADM)	DBA (PSFTDBA)	SYSTEM	SYSDBA	O/S Root
PeopleSoft Realm	Owner		When/How?	When/How?	No protection
Select Command Rules		No select* (default)	When/How?	When/How?	No protection
Connect Command Rules	PS Access Rule Set		When/How?	When/How?	No protection
Drop Tablespace Command Rule	Disabled Rule Set	Disabled Rule Set	When/How?	When/How?	No protection

\* Can still issue all other DML e.g. UPDATE



# Use Command Rules to limit Direct Database Access<sup>1</sup>

	IP Address	Program <sup>1</sup>	OS User <sup>2</sup>
<b>o1 - SYS</b>	database server	unlimited	oracle
<b>o2 - SYSTEM</b>	PS server	unlimited	oracle/ps
<b>o3 - Management</b>	OEM server	unlimited	oracle
<b>o4 - Backup</b>	backup server	unlimited	oracle
<b>a1 - Interactive</b>	PS server	unlimited	oracle/ps
<b>a2 - Data Owner</b>	PS server	unlimited	oracle/ps
<b>a3 - Interface</b>	per interface	per interface	per interface
<b>u1 - DBA</b>	PS server & jump	unlimited	unlimited
<b>u2 - Client/Server</b>	none	none	none
<b>u3 - Ad-hoc</b>	unlimited	approved list	unlimited

<sup>1</sup>Could you attempt the same with VPD and logon triggers?

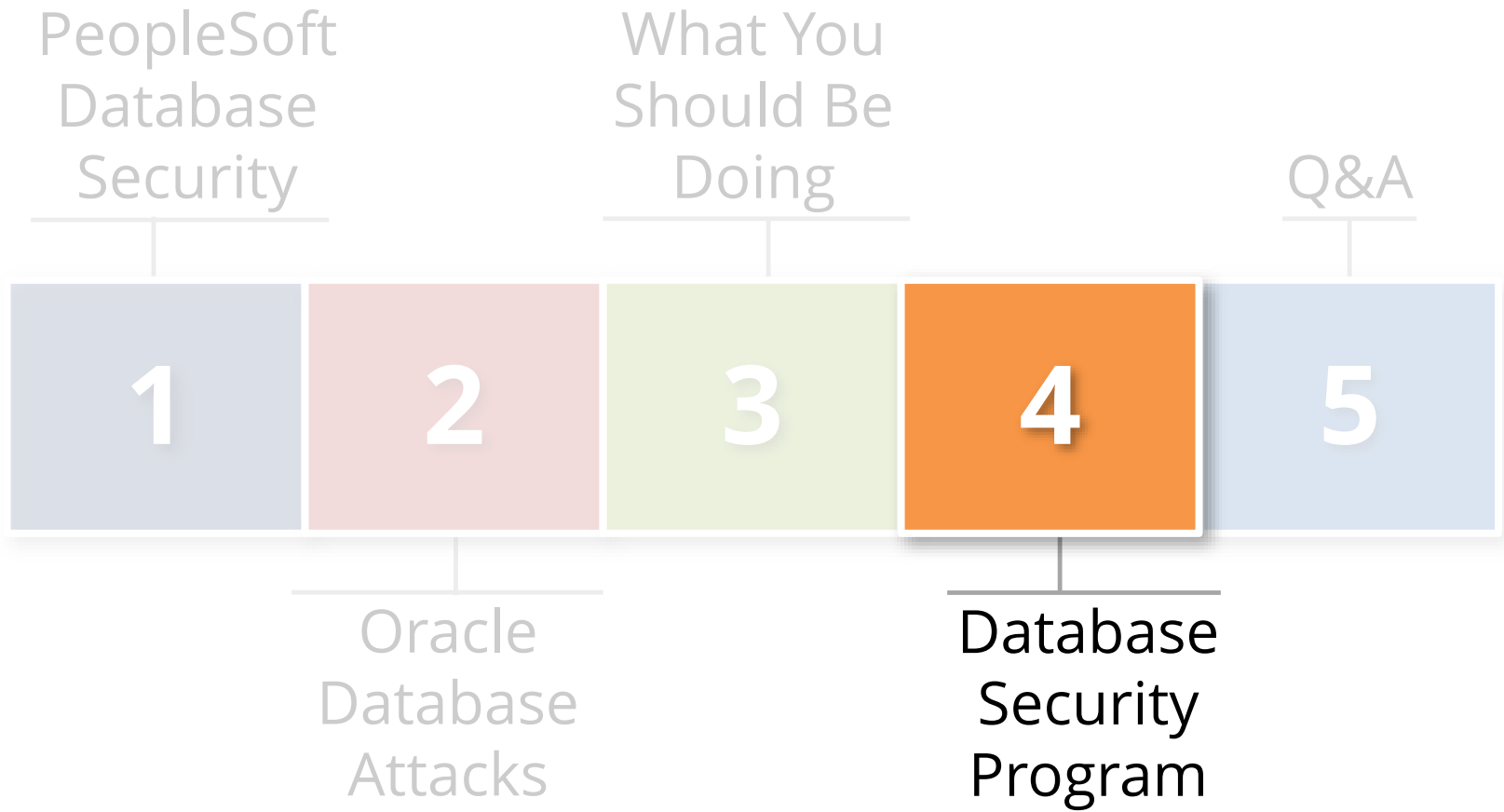
<sup>2</sup>Program and OS user may be spoofed by the client and are not fully reliable.

# Data Protection vs. Threats (Sample)

Data Access Method and Threats	Oracle Options						
	1 App Encrypt	2 Trigger View	3 Oracle TDE	4a FGAC	4b Internal Audit	4c External Audit	3 + 4 TDE + Auditing
1. Application access by end-users (role/RBAC)	E	E		C	A	A	A
2. Application access by application administrators	E+	E-		C	A	A	A
3. Database access by DBA	E	E		C	A+	A	A
4. Database access by application DBA (SYSTEM, SYSADM)	E+	E+			A+	A+	A+
5. Database access by other database accounts	E	E		C	A	A	A
6. Operating system access to database data files	E	E	E				E
7. On-line or off-line access to database backups	E	E	E				E
8. Exploitation of applications security vulnerabilities	E-	E-		C+	A+	A+	A+
9. Exploitation of Oracle Database security vulnerabilities	E+	E+		C+	A+	A+	A+
10. Exploitation of operating system security vulnerabilities	E	E	E				E

**E** = Encrypted, **C** = Access Controlled, **A** = Access Audited, **+** = Mostly **-** = Partially

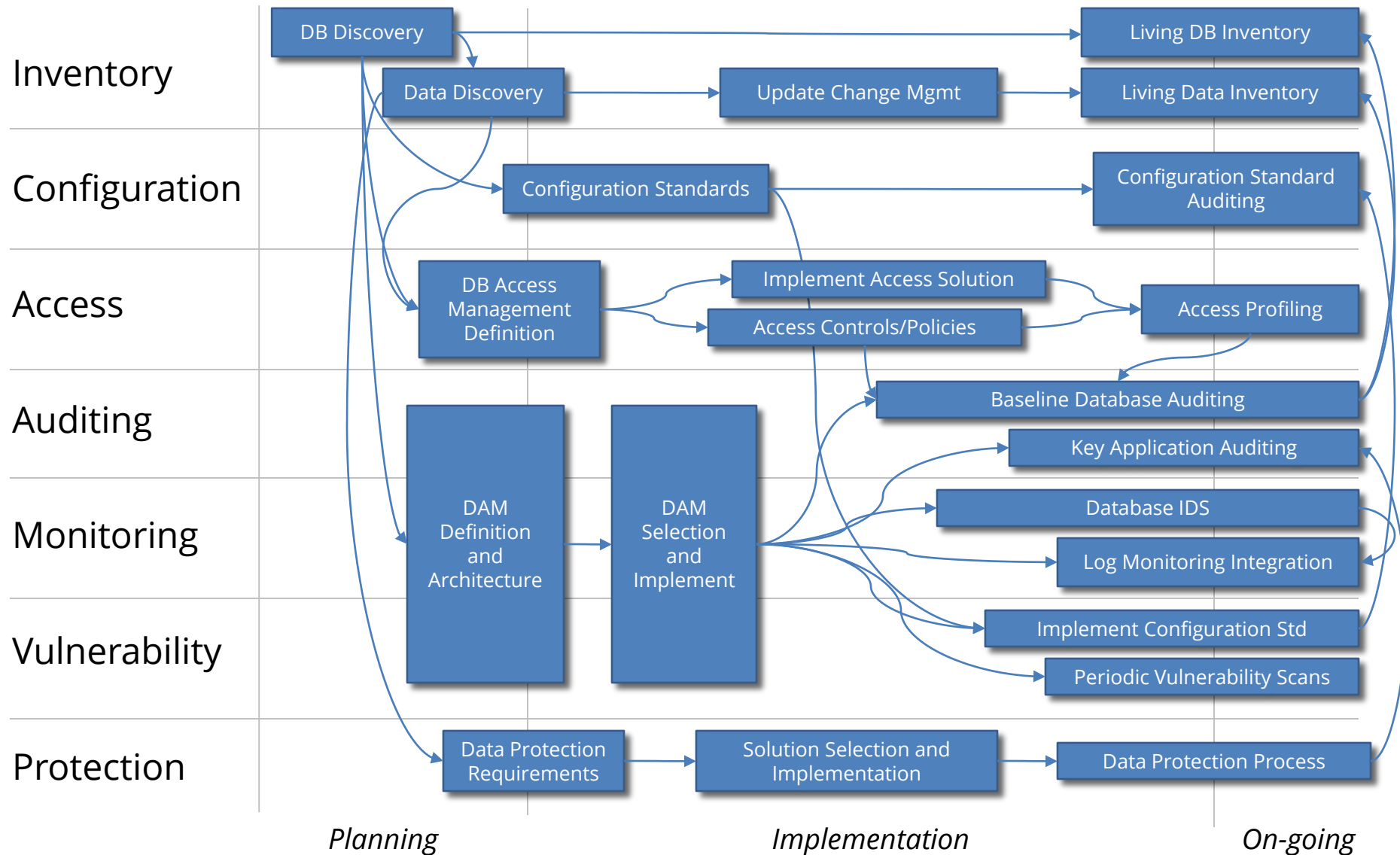
# Agenda



# Database Security Program Components

<b>Inventory</b>	<ul style="list-style-type: none"><li>▪ An inventory of all databases and sensitive data locations</li><li>▪ Methods and processes to maintain the inventories</li></ul>
<b>Configuration</b>	<ul style="list-style-type: none"><li>▪ A measureable database security standard and baseline</li><li>▪ Periodic validation with compliance to the standard</li></ul>
<b>Access</b>	<ul style="list-style-type: none"><li>▪ Database access management policies, procedures, and tools</li><li>▪ Database access profiling and monitoring</li></ul>
<b>Auditing</b>	<ul style="list-style-type: none"><li>▪ Database auditing requirements, processes, and definitions</li><li>▪ Centralized auditing retention and reporting solution</li></ul>
<b>Monitoring</b>	<ul style="list-style-type: none"><li>▪ Database real-time security monitoring and intrusion detection</li><li>▪ Database monitoring definition and tools</li></ul>
<b>Vulnerability</b>	<ul style="list-style-type: none"><li>▪ Vulnerability assessment and management for databases</li><li>▪ Vulnerability remediation strategy and processes</li></ul>
<b>Protection</b>	<ul style="list-style-type: none"><li>▪ Sensitive data protection strategy – encryption, data masking, redaction, scrambling</li><li>▪ Data protection policies, procedures, and tools</li></ul>

# Program Implementation



# Database Security Program Silos

Processes should be unified, but standards and procedures need to be vendor specific.

## Unified Database Security Processes

**Oracle  
Standards &  
Procedures**

**SQL Server  
Standards &  
Procedures**

**DB2  
Standards &  
Procedures**

**Big Data/  
NoSQL  
Standards &  
Procedures**

# DB Security Standards - Structure

## Security Baseline – All Databases

Security  
IT General Controls  
Basic Change Management

**Oracle  
Standard**

**SQL Server  
Standard**

**DB2  
Standard**

**Big Data/  
NoSQL  
Standard**

**SOX**  
Financial Data  
External Audits

**PCI**  
Credit Cards  
QSA Audits

**HIPAA**  
Health Data

**Additional  
compliance and  
security requirements**

# Agenda





# Contact Information

web: **[www.integrigy.com](http://www.integrigy.com)**

e-mail: **[info@integrigy.com](mailto:info@integrigy.com)**

blog: **[integrigy.com/oracle-security-blog](http://integrigy.com/oracle-security-blog)**