INTEGRIGY

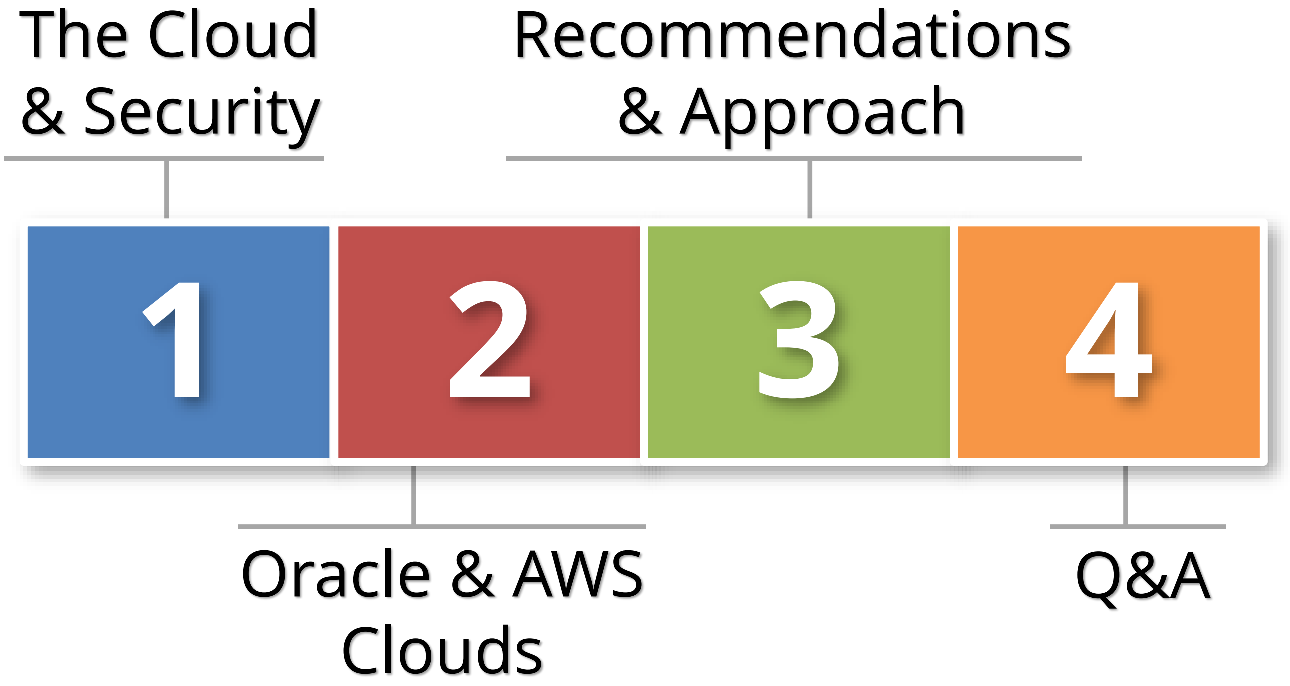
Oracle Database Security
in the Cloud

February 25, 2016

Michael Miller
Chief Security Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



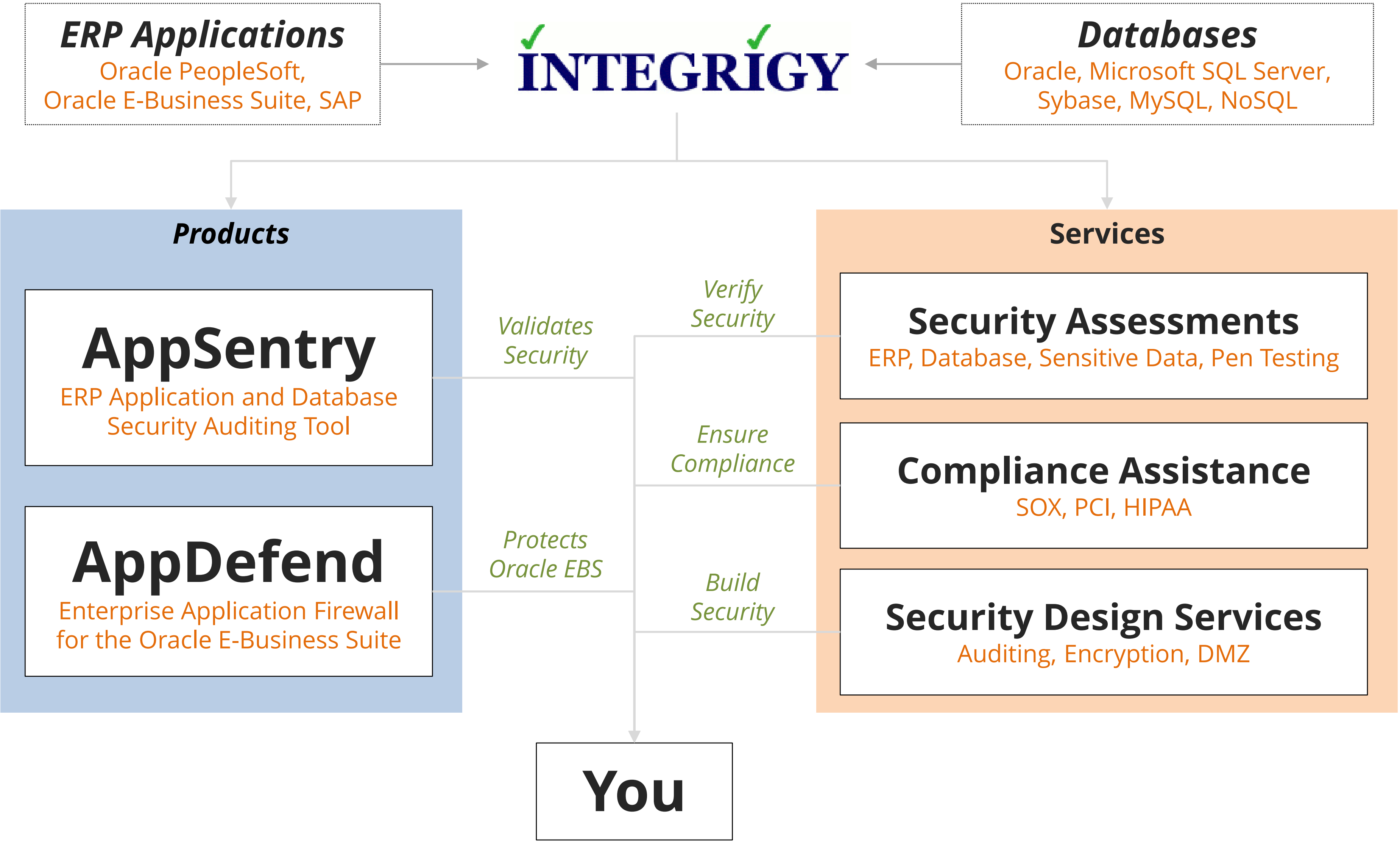
1 The Cloud & Security

2 Oracle & AWS Clouds

3 Recommendations & Approach

4 Q&A

About Integrigy



ERP Applications
Oracle PeopleSoft,
Oracle E-Business Suite, SAP

INTEGRIGY

Databases
Oracle, Microsoft SQL Server,
Sybase, MySQL, NoSQL

Products

AppSentry
ERP Application and Database Security Auditing Tool

Validates Security

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Protects Oracle EBS

Services

Verify Security

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

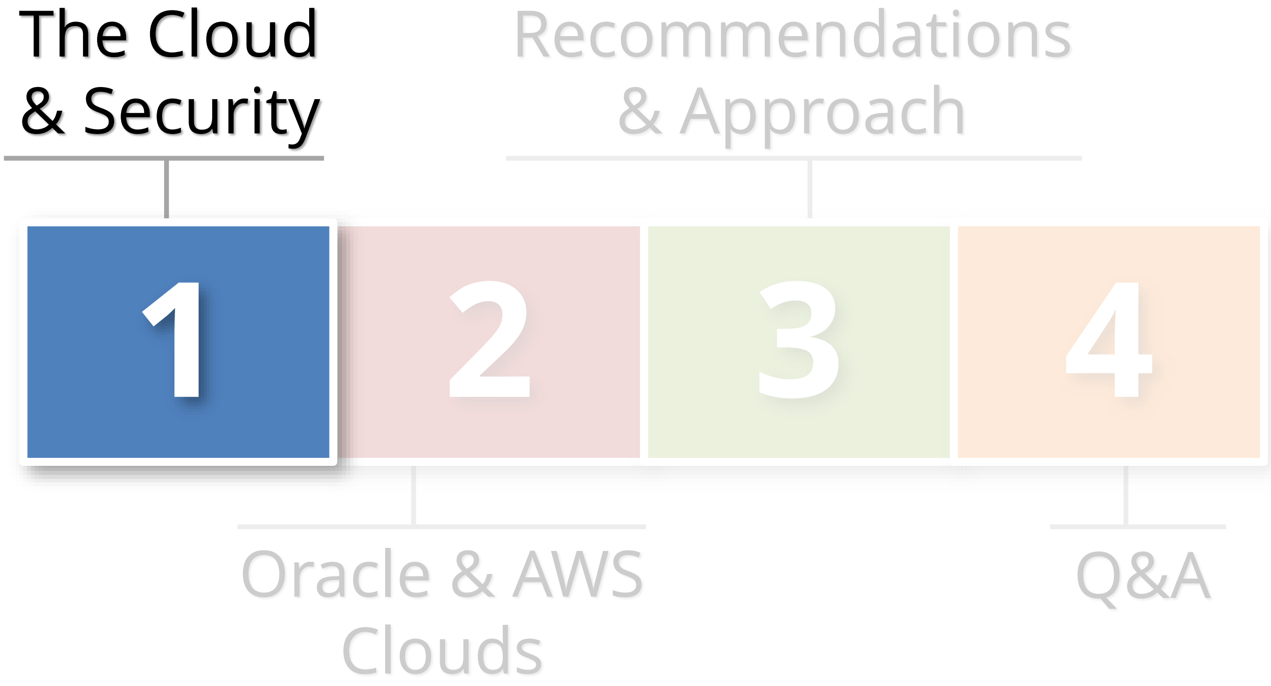
Compliance Assistance
SOX, PCI, HIPAA

Build Security

Security Design Services
Auditing, Encryption, DMZ

You

Agenda



1 The Cloud & Security

2 Oracle & AWS Clouds

3 Recommendations & Approach

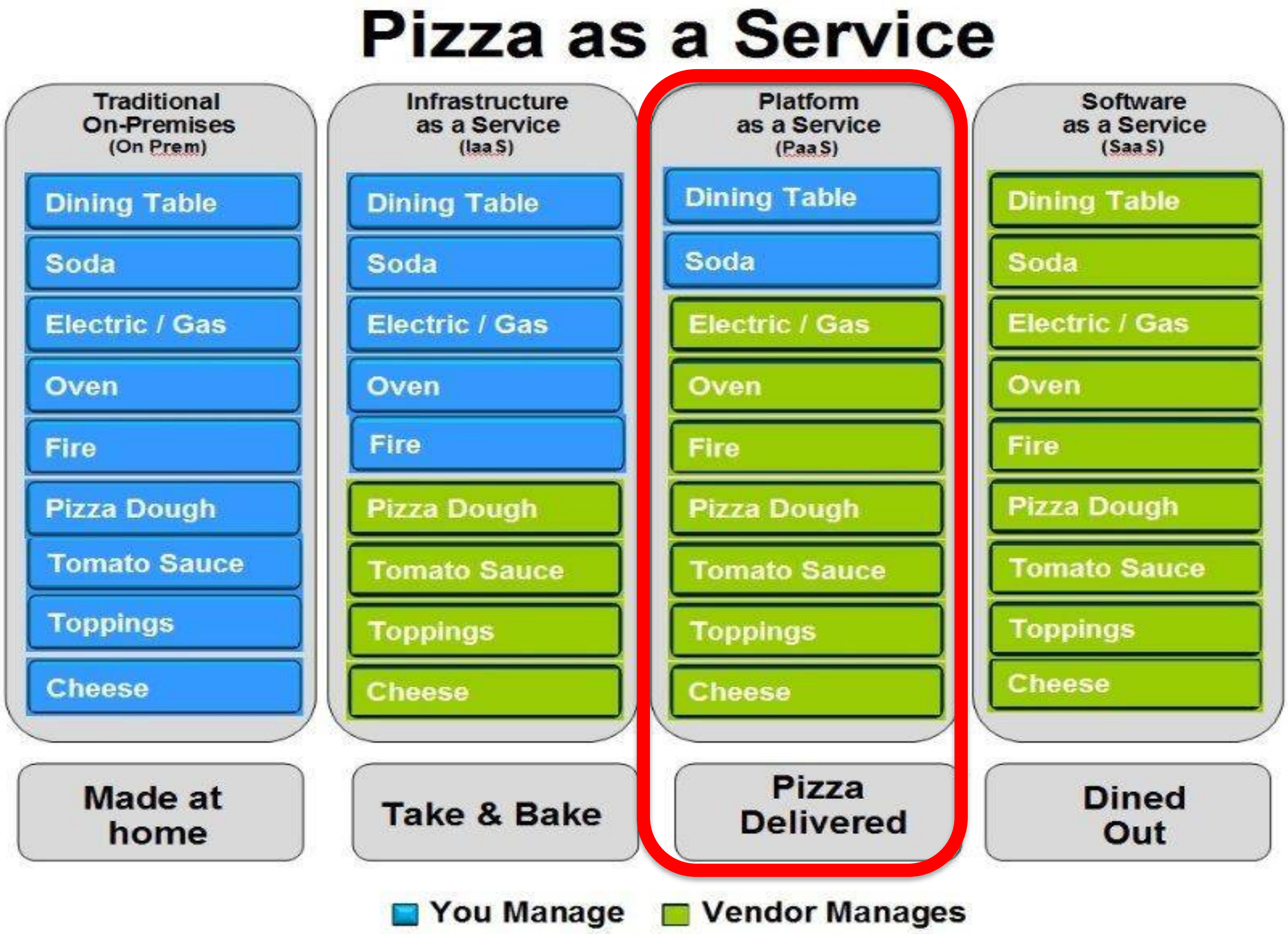
4 Q&A

Why is the Cloud Inevitable?

- **Increasing feasibility of what is possible**
  - Cloud evolved from, but is not a variation of hosting
  - More multi-tenancy and lawyers, but very concept of what & where a server is changing
- **Commoditization**
  - Paint-power-pipe (data center)
  - Baumol’s cost disease
- **The World is flat**
  - Demographic trends

On-premise private data centers
will become increasingly rare

Clouds Defined As Pizza



Pizza as a Service

Traditional On-Premises (On Prem)	Infrastructure as a Service (Iaa S)	Platform as a Service (Paa S)	Software as a Service (Saa S)
🟦 Dining Table	🟦 Dining Table	🟦 Dining Table	🟩 Dining Table
🟦 Soda	🟦 Soda	🟦 Soda	🟩 Soda
🟦 Electric / Gas	🟦 Electric / Gas	🟩 Electric / Gas	🟩 Electric / Gas
🟦 Oven	🟦 Oven	🟩 Oven	🟩 Oven
🟦 Fire	🟦 Fire	🟩 Fire	🟩 Fire
🟦 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough
🟦 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce
🟦 Toppings	🟩 Toppings	🟩 Toppings	🟩 Toppings
🟦 Cheese	🟩 Cheese	🟩 Cheese	🟩 Cheese
Made at home	Take & Bake	Pizza Delivered	Dined Out

🟦 You Manage 🟩 Vendor Manages

Does the Cloud Change Security?

No

Data Ownership Does NOT Change

- **You own your data**
  - You are responsible regardless of where it is stored

- **Legal and compliance mandates flow out and down to your vendor(s)**
  - “Onward transfer” is your responsibility
  - This includes your cloud provider

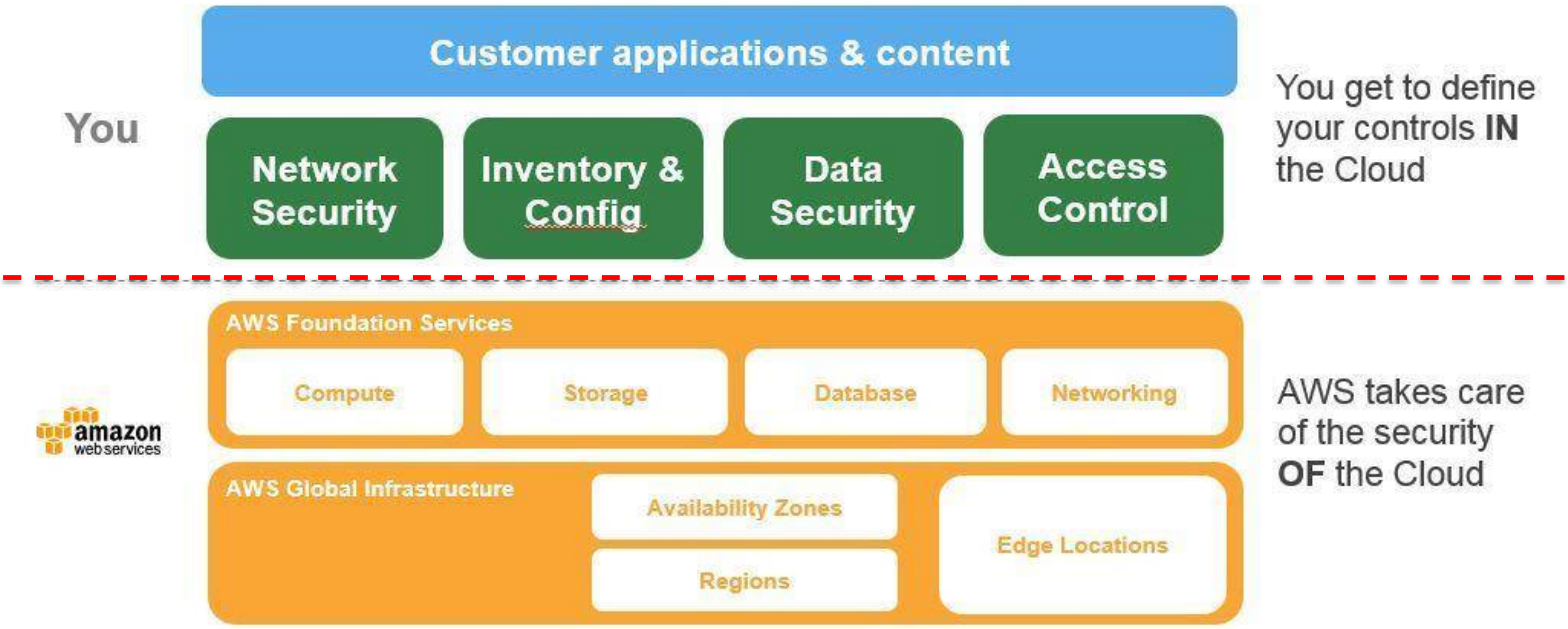
- **Cloud extends only what should already be in place to protect YOUR data**
  - Security needs to be scaled up
  - Clouds create more insiders

Security Responsibility by Cloud Type

Security/Type	IaaS	PaaS/DaaS	SaaS
GRC	🟩	🟩	🟩
Data	🟩	🟩	🟩
Application	🟩	🟩	🟥
Platform	🟩	🟥	🟦
Infrastructure	🟥	🟦	🟦
Physical	🟦	🟦	🟦

Client = Green   Shared = Red   Cloud Provider = Blue

Amazon AWS Shared Security



You get to define your controls **IN** the Cloud

AWS takes care of the security **OF** the Cloud

“Customers are responsible for the Confidentiality, Integrity and Availability of their data”

Cloud Security Alliance (CSA)

- **Mission statement**

  "To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing"

  - Site: https://cloudsecurityalliance.org
  - Cloud Controls Matrix (CCM)
  - Security Trust and Assurance Registry (STAR)
  - Consensus Assessments Initiative Questionnaire (CAIQ)

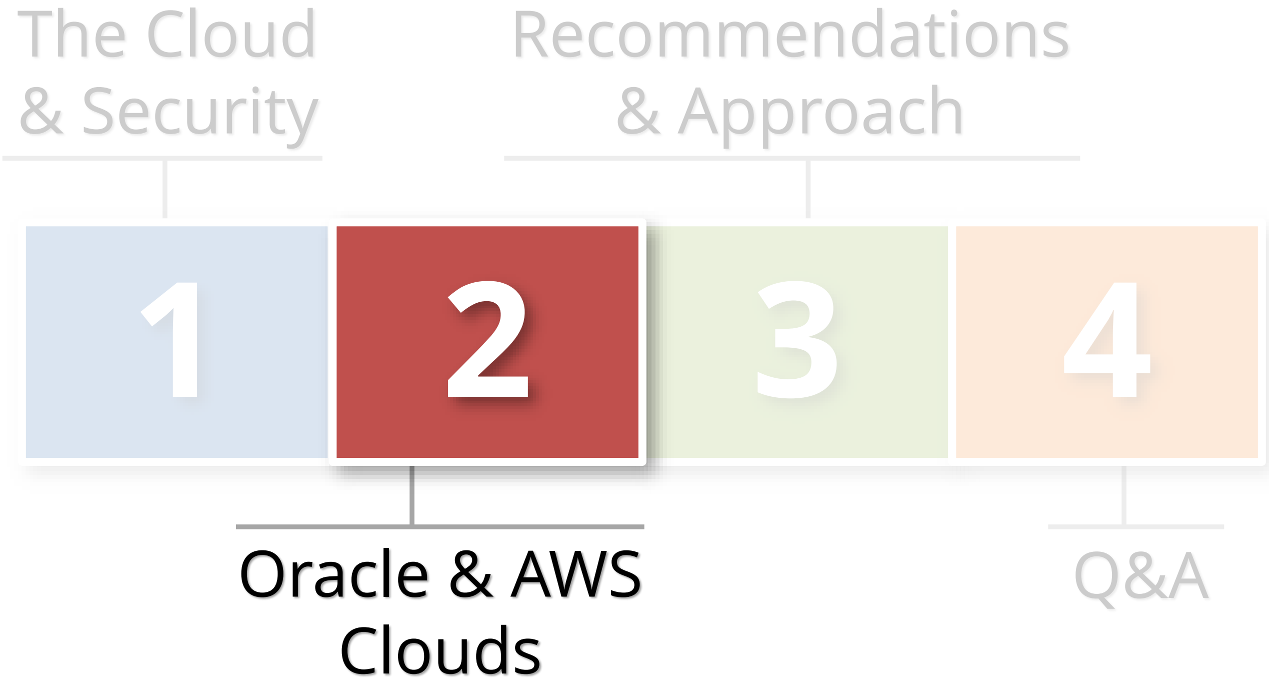
- **Recommendations**
  - Use CSA certified Provider – Security Trust and Assurance Registry (STAR)
  - Map your Provider's controls to CCM

#1 Recommendation: Its All In The Contract

- **Risk can be accepted, avoided or transferred**
  - Do so wisely
- **Before signing contract**
  - Vet Provider's supply chain for insiders
  - Require SOC 1 annually for the FULL year
  - Read SOC carefully BEFORE signing and assuming nothing
  - Stipulate and/or negotiate changes to SOC
  - Retain consulting services to evaluate the SOC
  - Vet Provider's supply chain (additional SOC reports)
  - Vet reputation of advisory firm producing the SOC
  - Push for SOC2 & CSA CCM controls
- **After signing contract**
  - Hold Provider fully accountable

SANITARY INSPECTION GRADE
A
NYC
SANITARY INSPECTION GRADE
B
NYC
SANITARY INSPECTION GRADE
C
NYC

Agenda



The Cloud & Security

Recommendations & Approach

1

2

3

4

Oracle & AWS Clouds

Q&A

Oracle Public Cloud

Service	Ideal Customer Need
Compute	Cloud environment with complete control to install and setup any Oracle software. Bring Your Own License.
Database Schema Service/Multitenant/ Cloud Service	Single Schema. No SQL*Net, only REST access. TDE used to encrypt. Auditing and DV not possible. Use for APEX non-prod?
Virtual Image	Complete control over environment. DB software staged, you install & patch database. Backup services provided.
Database as a Service (DBaaS)	Same as virtual image. Database is pre-installed per your specification.
DBaaS-Managed	Future direction

Available from https://cloud.oracle.com/database

Oracle DBaaS & Virtual Image

- **Full control over environment**
  - Full administrative root OS and SYSDBA access
- **Dedicated virtual machine**
  - License included with monthly or hourly billing
  - Pre-installed 11g or 12c or you can install
- **Storage managed by Oracle**
  - Automatic backup & point-in-time recovery
  - TDE possible (not default & no HSM support)
- **Access**
  - Public IP address created, SSH to VM
  - SQL * Net with through open ports or SSH tunnel
  - ASO network encryption enabled (REQUIRED) by default

Do Not Confuse DBaaS with Cloud Security

- **‘Oracle Cloud Security Services’ is a Managed Services offering**
  - Tools and services
  - Compatible with DBaaS? Ask Oracle Sales.

- **More information:** http://www.oracle.com/us/industries/financial-services/sb-managed-cloud-security-services-2538956.pdf

Amazon Oracle Database Services

- **Relational Database Service (RDS)**
  - Pre-configured, Amazon managed Oracle database
  - No SSH. SYS and SYSTEM locked and cannot be used
  - AWS Volume Encrypt or Oracle ASO (TDE) BYOL option
  - Patching (CPU included) per AWS's schedule
  - Standard Auditing supported (not FGA)
  - Database Vault not supported
  - Bring your own or rent-by-hour license options
- **Elastic Compute Cloud (EC2)**
  - Self-managed Oracle database, full control over environment (SYS, SYSTEM, Oracle/SSH)
  - Virtual Private Cloud (VPC) – isolated network space
  - AWS Volume Encrypt or Oracle ASO (TDE) (either Amazon managed wallets or HSM option with Amazon's CloudHSM)
  - Bring your own license

Agenda

1. The Cloud & Security
2. Oracle & AWS Clouds
3. Recommendations & Approach
4. Q&A

Database Security in the Cloud - Issues

- **Complete control equals complete responsibility, same as before**
  - AWS RDS
  - AWS EC2 & Oracle DBaaS
- **Marginal to material security impacts**
  - Insecurities about the Cloud
  - Inordinate concerns by auditors (and others)
  - Invitingness of overall target profile of Provider
  - Increased number of insiders
  - Introspection, isolation and image provenance failures
  - Insufficient auditor capacity and expertise
  - Indeterminate technical complexities and expertise
  - Ineptitude due to junior DBAs or no DBAs

Database Security in the Cloud - Solutions

Feasible recommendations to likely database security issues when moving **whole data centers** to the Cloud - not one (1) database

- **Professional management still needed**
  - Provisioning & oversight processes
  - Baseline configuration
  - Automate baseline audits
- **Restrict access**
  - Management console
  - Network & Database Listener
- **Audit and monitor**
  - Trust-but-verify & continuous auditing
  - Implement a DAM
- **Protect data**
  - Encryption
  - Database Vault

The Cloud requires a higher level proof of being in control

Professional Management Still Needed

- **Data center and databases still need professional management**
  - Databases are critical assets that need to be under <u>your</u> change control
  - Provisioning processes and gatekeepers needed
  - Technical decisions still need to be made
  - AWS RDS security patches <u>NOT</u> applied quarterly
  - Use Oracle OEM if possible
- **Guard against rogue databases**
  - How would you know? NMAP?

High-level/Architect DBA expertise required for Cloud oversight

Restrict Access to Database

- **Secure Provider's management console**
  - AWS: Multi-factor authentication (Key Fob or Display Card)
  - AWS: Don't use root (Console account) for day-to-day, create super admins using Identity Access Management (IAS)
  - Separate admin accounts for prod, test and dev
- **Network**
  - AWS: security Groups (IP ACLs) & subnets
  - Oracle DBaaS*: Security IP lists & Rules
  - Bastion host/jump box for admins and DBAs
- **Database**
  - Database ACLs and services
  - Valid Node Checking/ VNCR
  - Network encryption is free, use it

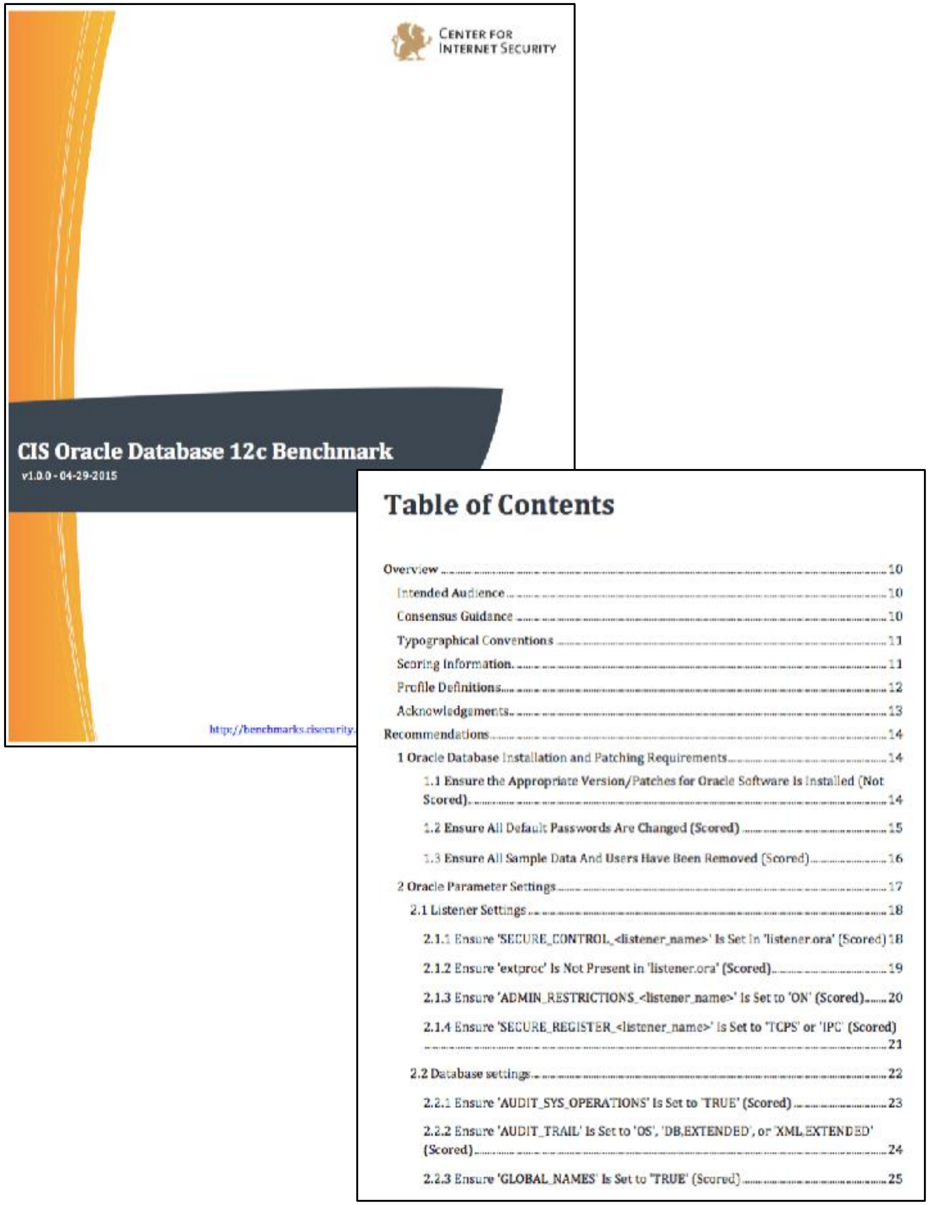
    ```
    SQLNET.ENCRYPTION_SERVER = REQUIRED
    ```
  - Implement Oracle Database Vault and/or Database Firewall

*Oracle will be shortly announcing new network options

Prove Governance by Using Baselines

- **Use security best practice baseline configurations specific to Oracle RDBMS**
  - CIS Oracle 12c https://benchmarks.cisecurity.org/downloads/show-single/?file=oracle12c.100
  - US DoD DISA STIG http://iase.disa.mil/stigs/app-security/database/Pages/index.aspx
- **Sanity check Provider's baseline and guard against configuration drift**
  - Hundreds of thoroughly researched controls
  - Must edit, CIS or DISA STIG as-is will BREAK things
  - Must prove on-going adherence, not just one-time project
  - Use to calm and objectively communicate with auditors

CIS and DISA STIG Oracle Baselines



Center for Internet Security

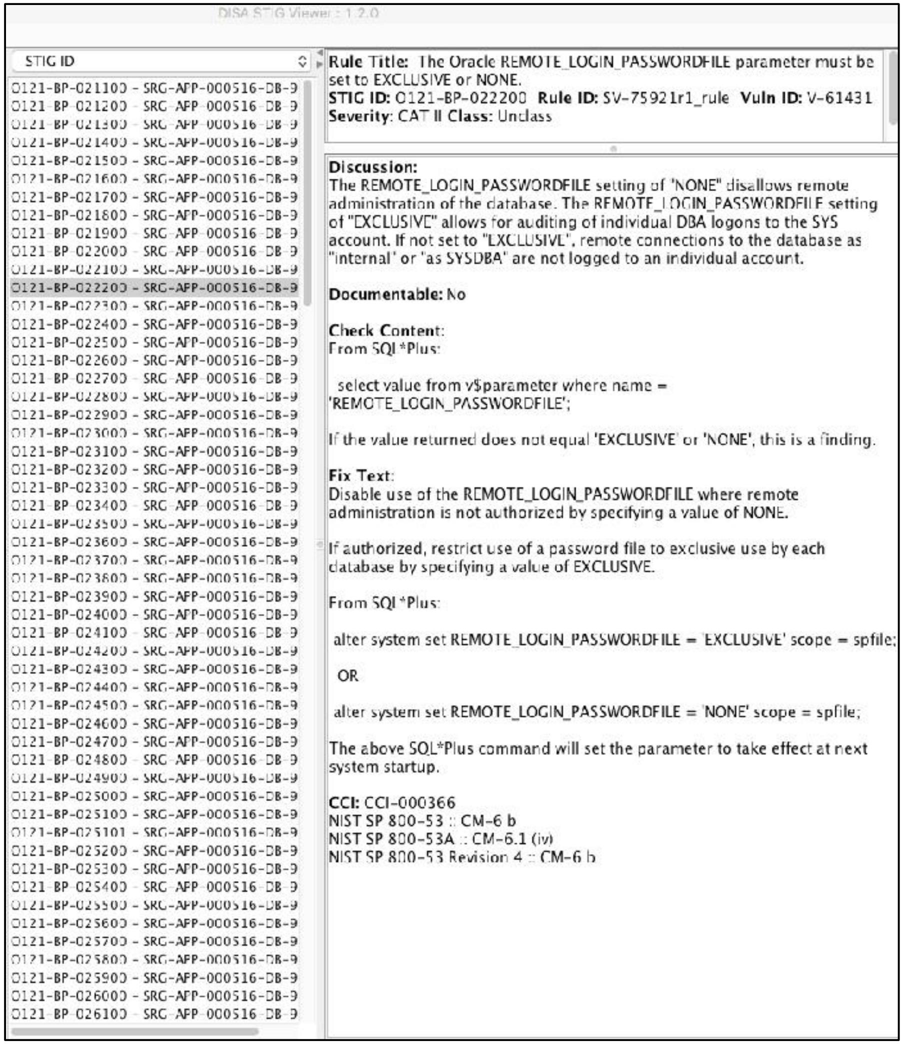
CIS Oracle Database 12c Benchmark

v1.0.0 - 04-29-2015

http://benchmarks.cisecurity.

Table of Contents

Overview 10
Intended Audience 10
Consensus Guidance 10
Typographical Conventions 11
Scoring Information. 11
Profile Definitions 12
Acknowledgements. 13
Recommendations 14
1 Oracle Database Installation and Patching Requirements 14
1.1 Ensure the Appropriate Version/Patches for Oracle Software Is Installed (Not Scored). 14
1.2 Ensure All Default Passwords Are Changed (Scored) 15
1.3 Ensure All Sample Data And Users Have Been Removed (Scored) 16
2 Oracle Parameter Settings 17
2.1 Listener Settings 18
2.1.1 Ensure 'SECURE_CONTROL_<listener_name>' Is Set In 'listener.ora' (Scored) 18
2.1.2 Ensure 'extproc' Is Not Present in 'listener.ora' (Scored) 19
2.1.3 Ensure 'ADMIN_RESTRICTIONS_<listener_name>' Is Set to 'ON' (Scored) 20
2.1.4 Ensure 'SECURE_REGISTER_<listener_name>' Is Set to 'TCPS' or 'IPC' (Scored) 21
2.2 Database settings 22
2.2.1 Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE' (Scored) 23
2.2.2 Ensure 'AUDIT_TRAIL' Is Set to 'OS', 'DB,EXTENDED', or 'XML,EXTENDED' (Scored) 24
2.2.3 Ensure 'GLOBAL_NAMES' Is Set to 'TRUE' (Scored) 25



```
O121-BP-021100 - SRG-APP-000516-DB-9
O121-BP-021200 - SRG-APP-000516-DB-9
O121-BP-021300 - SRG-APP-000516-DB-9
O121-BP-021400 - SRG-APP-000516-DB-9
O121-BP-021500 - SRG-APP-000516-DB-9
O121-BP-021600 - SRG-APP-000516-DB-9
O121-BP-021700 - SRG-APP-000516-DB-9
O121-BP-021800 - SRG-APP-000516-DB-9
O121-BP-021900 - SRG-APP-000516-DB-9
O121-BP-022000 - SRG-APP-000516-DB-9
O121-BP-022100 - SRG-APP-000516-DB-9
O121-BP-022200 - SRG-APP-000516-DB-9
O121-BP-022300 - SRG-APP-000516-DB-9
O121-BP-022400 - SRG-APP-000516-DB-9
O121-BP-022500 - SRG-APP-000516-DB-9
O121-BP-022600 - SRG-APP-000516-DB-9
O121-BP-022700 - SRG-APP-000516-DB-9
O121-BP-022800 - SRG-APP-000516-DB-9
O121-BP-022900 - SRG-APP-000516-DB-9
O121-BP-023000 - SRG-APP-000516-DB-9
O121-BP-023100 - SRG-APP-000516-DB-9
O121-BP-023200 - SRG-APP-000516-DB-9
O121-BP-023300 - SRG-APP-000516-DB-9
O121-BP-023400 - SRG-APP-000516-DB-9
O121-BP-023500 - SRG-APP-000516-DB-9
O121-BP-023600 - SRG-APP-000516-DB-9
O121-BP-023700 - SRG-APP-000516-DB-9
O121-BP-023800 - SRG-APP-000516-DB-9
O121-BP-023900 - SRG-APP-000516-DB-9
O121-BP-024000 - SRG-APP-000516-DB-9
O121-BP-024100 - SRG-APP-000516-DB-9
O121-BP-024200 - SRG-APP-000516-DB-9
O121-BP-024300 - SRG-APP-000516-DB-9
O121-BP-024400 - SRG-APP-000516-DB-9
O121-BP-024500 - SRG-APP-000516-DB-9
O121-BP-024600 - SRG-APP-000516-DB-9
O121-BP-024700 - SRG-APP-000516-DB-9
O121-BP-024800 - SRG-APP-000516-DB-9
O121-BP-024900 - SRG-APP-000516-DB-9
O121-BP-025000 - SRG-APP-000516-DB-9
O121-BP-025100 - SRG-APP-000516-DB-9
O121-BP-025101 - SRG-APP-000516-DB-9
O121-BP-025200 - SRG-APP-000516-DB-9
O121-BP-025300 - SRG-APP-000516-DB-9
O121-BP-025400 - SRG-APP-000516-DB-9
O121-BP-025500 - SRG-APP-000516-DB-9
O121-BP-025600 - SRG-APP-000516-DB-9
O121-BP-025700 - SRG-APP-000516-DB-9
O121-BP-025800 - SRG-APP-000516-DB-9
O121-BP-025900 - SRG-APP-000516-DB-9
O121-BP-026000 - SRG-APP-000516-DB-9
O121-BP-026100 - SRG-APP-000516-DB-9
```

Rule Title: The Oracle REMOTE_LOGIN_PASSWORDFILE parameter must be set to EXCLUSIVE or NONE.
STIG ID: O121-BP-022200 **Rule ID:** SV-75921r1_rule **Vuln ID:** V-61431
Severity: CAT II **Class:** Unclass

Discussion:
The REMOTE_LOGIN_PASSWORDFILE setting of "NONE" disallows remote administration of the database. The REMOTE_LOGIN_PASSWORDFILE setting of "EXCLUSIVE" allows for auditing of individual DBA logons to the SYS account. If not set to "EXCLUSIVE", remote connections to the database as "internal" or "as SYSDBA" are not logged to an individual account.

Documentable: No

Check Content:
From SQL*Plus:

```
  select value from v$parameter where name =
'REMOTE_LOGIN_PASSWORDFILE';
```

If the value returned does not equal 'EXCLUSIVE' or 'NONE', this is a finding.

Fix Text:
Disable use of the REMOTE_LOGIN_PASSWORDFILE where remote administration is not authorized by specifying a value of NONE.

If authorized, restrict use of a password file to exclusive use by each database by specifying a value of EXCLUSIVE.

From SQL*Plus:

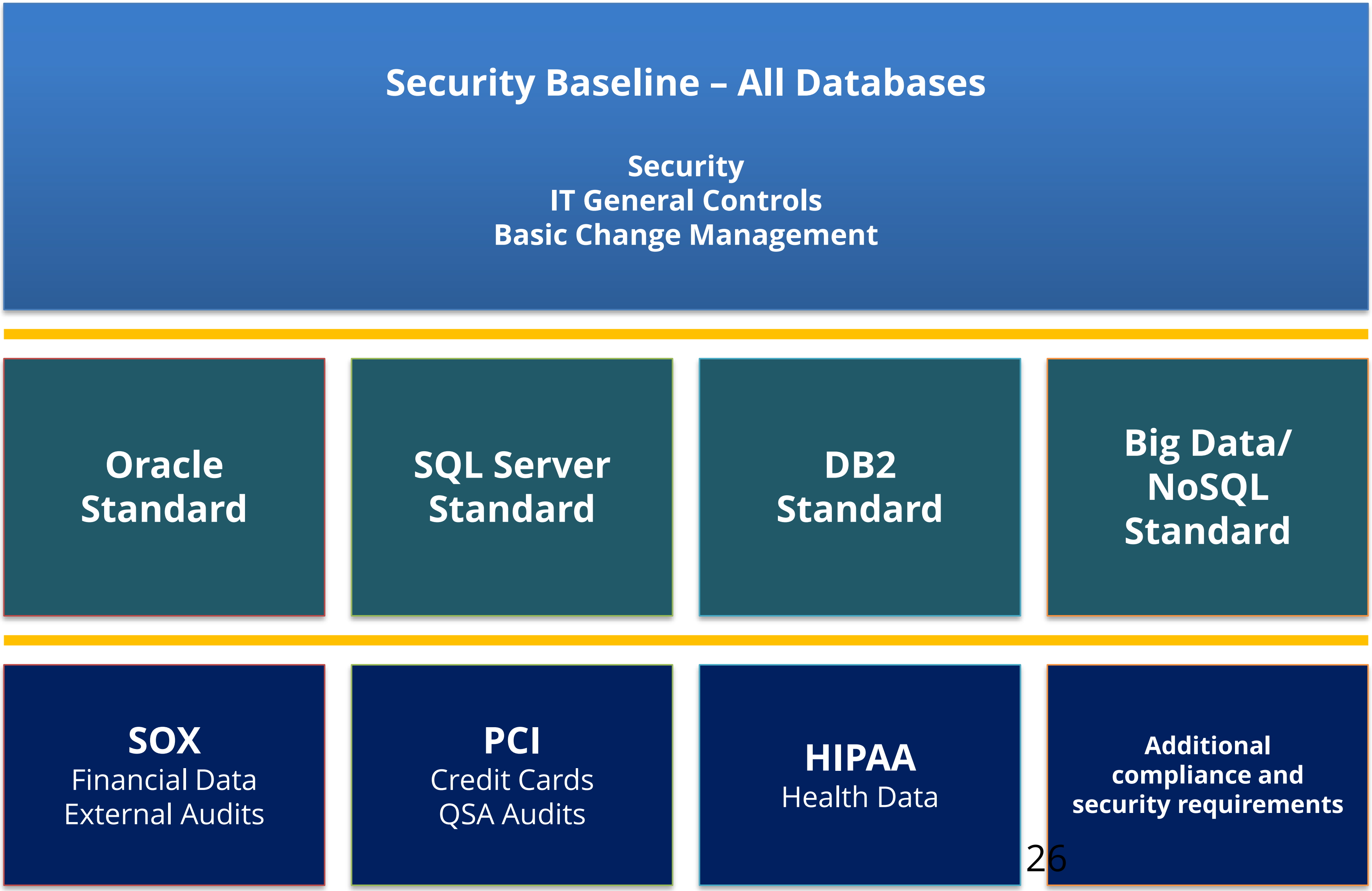
```
 alter system set REMOTE_LOGIN_PASSWORDFILE = 'EXCLUSIVE' scope = spfile;

  OR

 alter system set REMOTE_LOGIN_PASSWORDFILE = 'NONE' scope = spfile;
```

The above SQL*Plus command will set the parameter to take effect at next system startup.

CCI: CCI-000366
NIST SP 800-53 :: CM-6 b
NIST SP 800-53A :: CM-6.1 (iv)
NIST SP 800-53 Revision 4 :: CM-6 b

Baseline = Consistency

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

Automate Baseline Reporting

- **Manual auditing does not work**
  - Very time consuming to check everything – hundreds of items to check and analyze, inclusive of passwords
  - Auditor’s knowledge must be extensive and broad
  - Technical and functional auditing skills required
  - Difficult and expensive to conduct a 2 week annual audit per database
  - New exploits and vulnerabilities are discovered frequently
- **Few tools exist to automate audit process**
  - Multiple tools required to automate entire process
  - Tools are usually a conglomeration of SQL and shell scripts
  - Difficult to keep accurate inventory of new security issues
- **Examples**
  - Oracle Enterprise Manager (with additionally licensed lifecycle mgmt. pack)
  - Integrigy AppSentry

Integrigy AppSentry

AppSentry is a **security scanner** designed and optimized for Oracle DBAs and auditors to provide attestation. Is an ideal Cloud provider governance tool.

- **Security scanner**
  1,000+ in-depth security audits and controls, 3rd party integration, automatic updates, no agents, network and operating system included

- **Database Security**
  Accounts, patches, permissions (e.g. APPS, PS, Connect ID, APPLSYSPUB), listener, links, auditing, exploits

- **Oracle EBS & PeopleSoft Security**
  Apache, SSL, accounts, auditing, patches, privileges, auditing and security settings

- **Security Reports**
  Findings, recommendations, exportable, compliance mappings (PCI, HIPAA, SOX…)

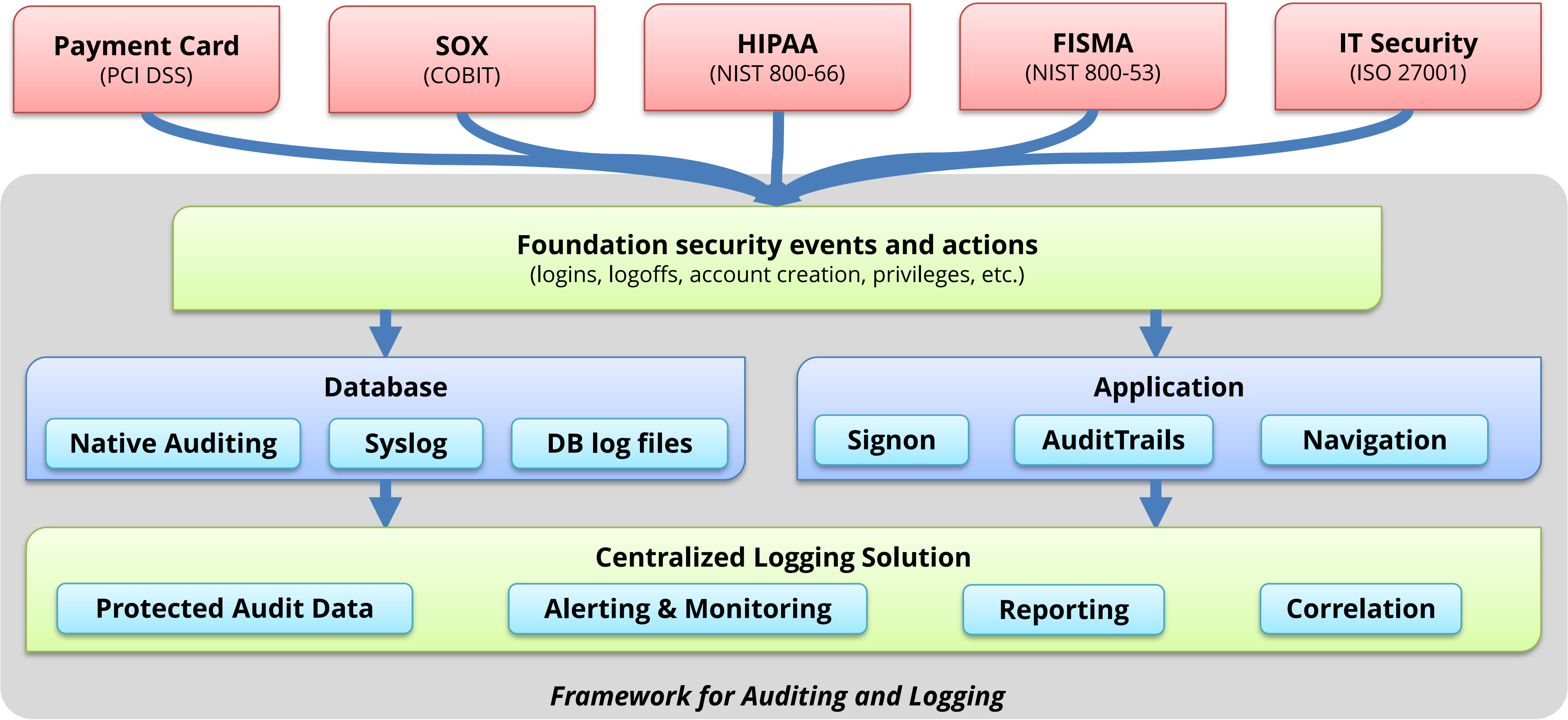
Continuously Audit to Verify Trust

- **Risks to databases in the Cloud**
  - How do guard against authorized changes and access
  - How to identify poor or risky behaviors
  - How to meet compliance requirements (SOX, HIPAA, PCI)

- **All research says to use policy of Trust-but-Verify for continuous auditing**
  - Implement log and audit framework for whole tech stack
  - Regular assessments (e.g. Integrigy to professionally review)

- **Integrigy Framework for Oracle database logging and auditing**
  - Free 27 page whitepaper
  - http://www.integrigy.com/security-resources/guide-auditing-oracle-applications

Integrigy Framework for Auditing and Logging



Payment Card (PCI DSS)

SOX (COBIT)

HIPAA (NIST 800-66)

FISMA (NIST 800-53)

IT Security (ISO 27001)

Foundation security events and actions
(logins, logoffs, account creation, privileges, etc.)

Database

- Native Auditing
- Syslog
- DB log files

Application

- Signon
- AuditTrails
- Navigation

Centralized Logging Solution

- Protected Audit Data
- Alerting & Monitoring
- Reporting
- Correlation

Framework for Auditing and Logging

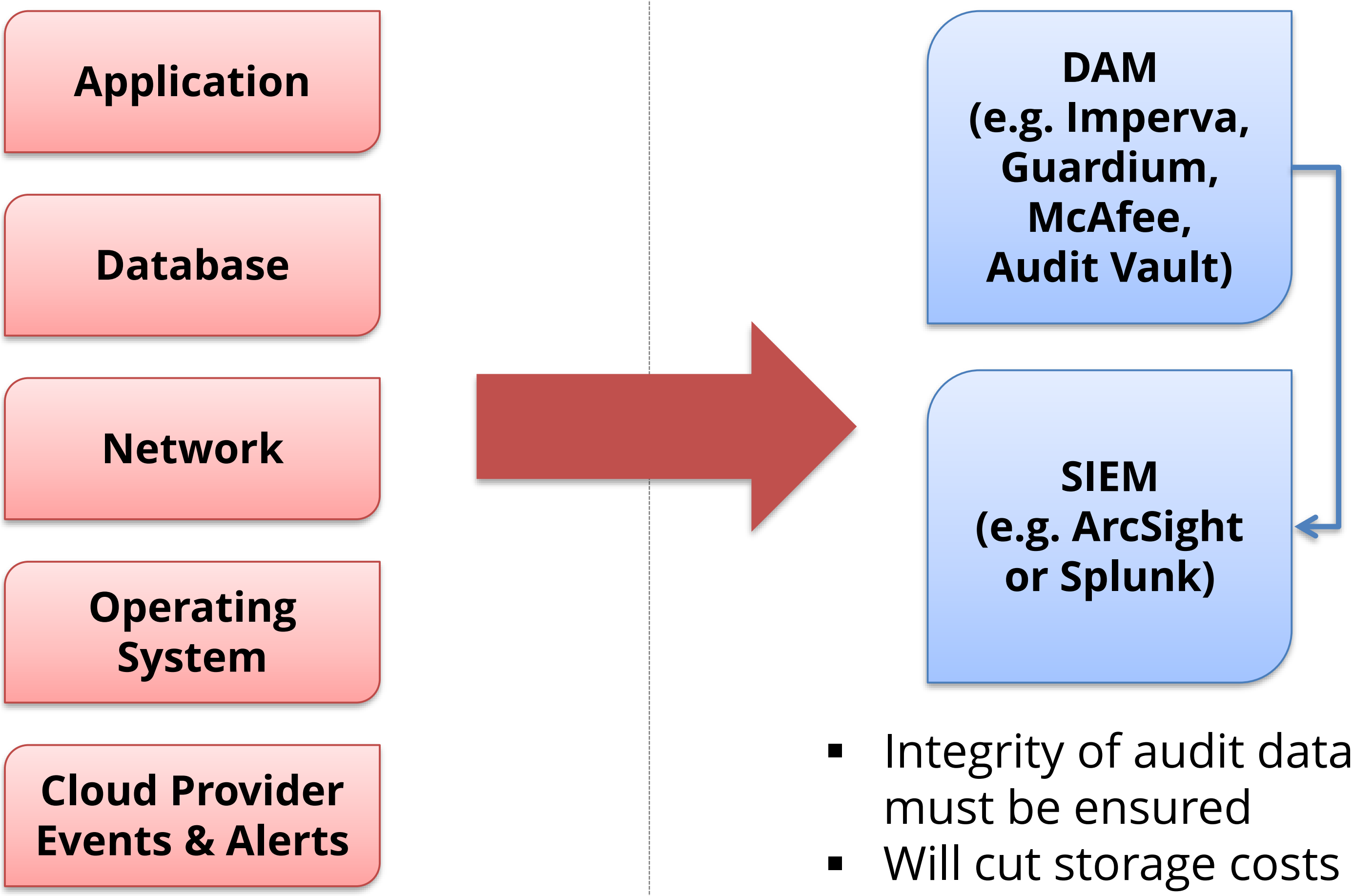
Foundation Security Events Mapping

Security Events and Actions	PCI DSS 10.2	SOX (COBIT)	HIPAA (NIST 800-66)	IT Security (ISO 27001)	FISMA (NIST 800-53)
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

Benefits of the Log and Audit Framework

- **Based on database security research**
  - Designed as part of a holistic database security program
  - Enforces configuration and access management best practices
  - Compliance matrix mapping: SOX, PCI etc.
  - Specific high-risk events, sensitive packages, alerts, error codes and usage patterns
  - Machine learning should only augment basic auditing
- **Designed for use with a SIEM for decision making**
  - Integrate database events with infrastructure and applications
  - Correlate with AWS CloudWatch, CloudTrail and Config
- **Roadmap for future**
  - Will help get started or improve existing DAM implementation
  - Three levels of maturity

Safeguard Your Audit Data



Application

Database

Network

Operating System

Cloud Provider Events & Alerts

DAM (e.g. Imperva, Guardium, McAfee, Audit Vault)

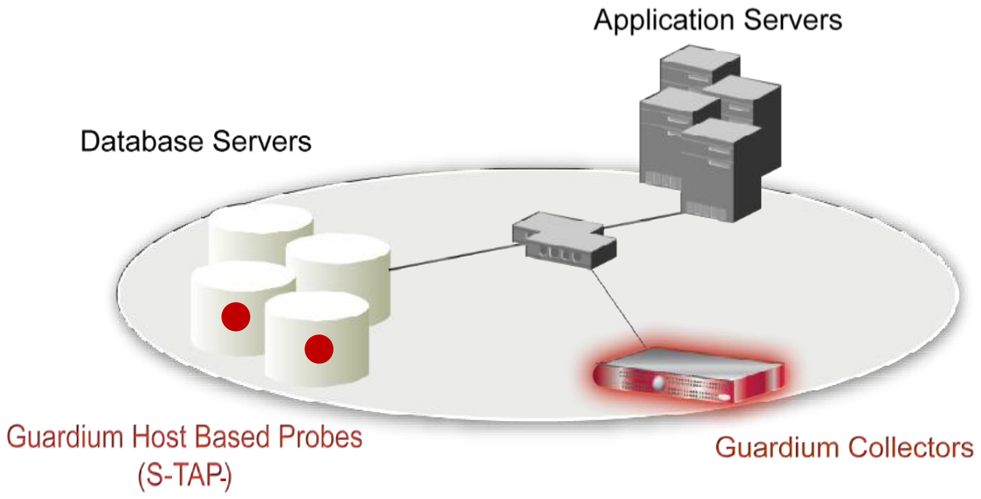
SIEM (e.g. ArcSight or Splunk)

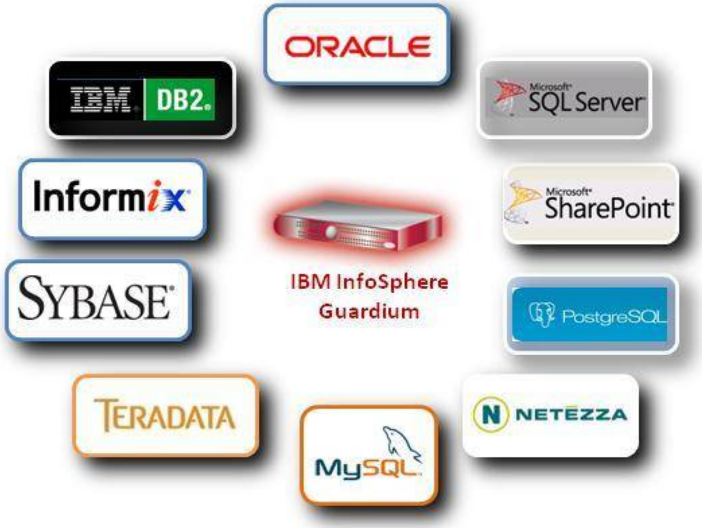
- Integrity of audit data must be ensured
- Will cut storage costs

Cloud Provider

On-premise or 3rd party

DAMs Provide Non-Invasive, Real-Time Database Security



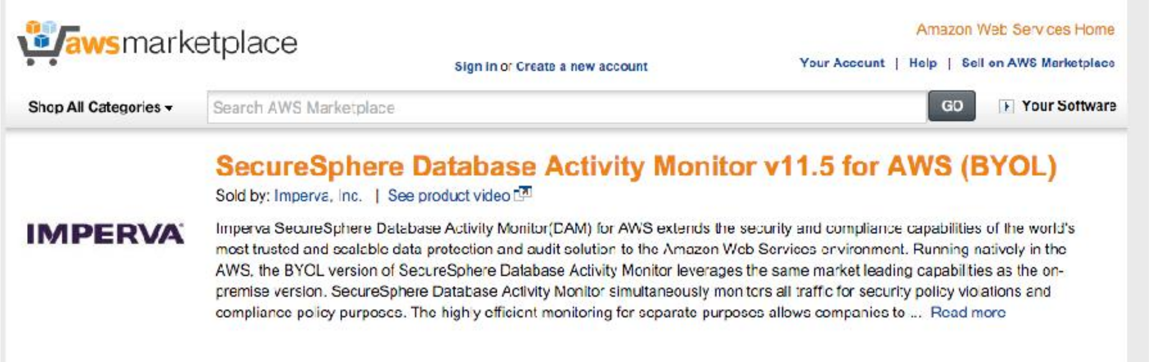


- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS audit logs
- Minimal performance impact (2-3%)
- No DBMS or application changes

- Supports Separation of Duties
- Activity logs can’t be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

Key DAM Vendors

- **Oracle**
  - Audit Vault and Database Firewall (AVDF) (formerly Secerno)
- **IBM**
  - IBM Security Guardium
- **McAfee**
  - Data Center Security for Databases (formerly Sentrigo)
- **Imperva**
  - SecureSphere for Databases



SecureSphere Database Activity Monitor v11.5 for AWS (BYOL)

Sold by: Imperva, Inc. | See product video

Imperva SecureSphere Database Activity Monitor(DAM) for AWS extends the security and compliance capabilities of the world's most trusted and scalable data protection and audit solution to the Amazon Web Services environment. Running natively in the AWS, the BYOL version of SecureSphere Database Activity Monitor leverages the same market leading capabilities as the on-premise version. SecureSphere Database Activity Monitor simultaneously monitors all traffic for security policy violations and compliance policy purposes. The highly efficient monitoring for separate purposes allows companies to ... Read more

Cloud 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 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**
  - To encrypt for security, you hold the keys
  - To encrypt for compliance the Provider holds the keys

What does Oracle TDE do and not do?

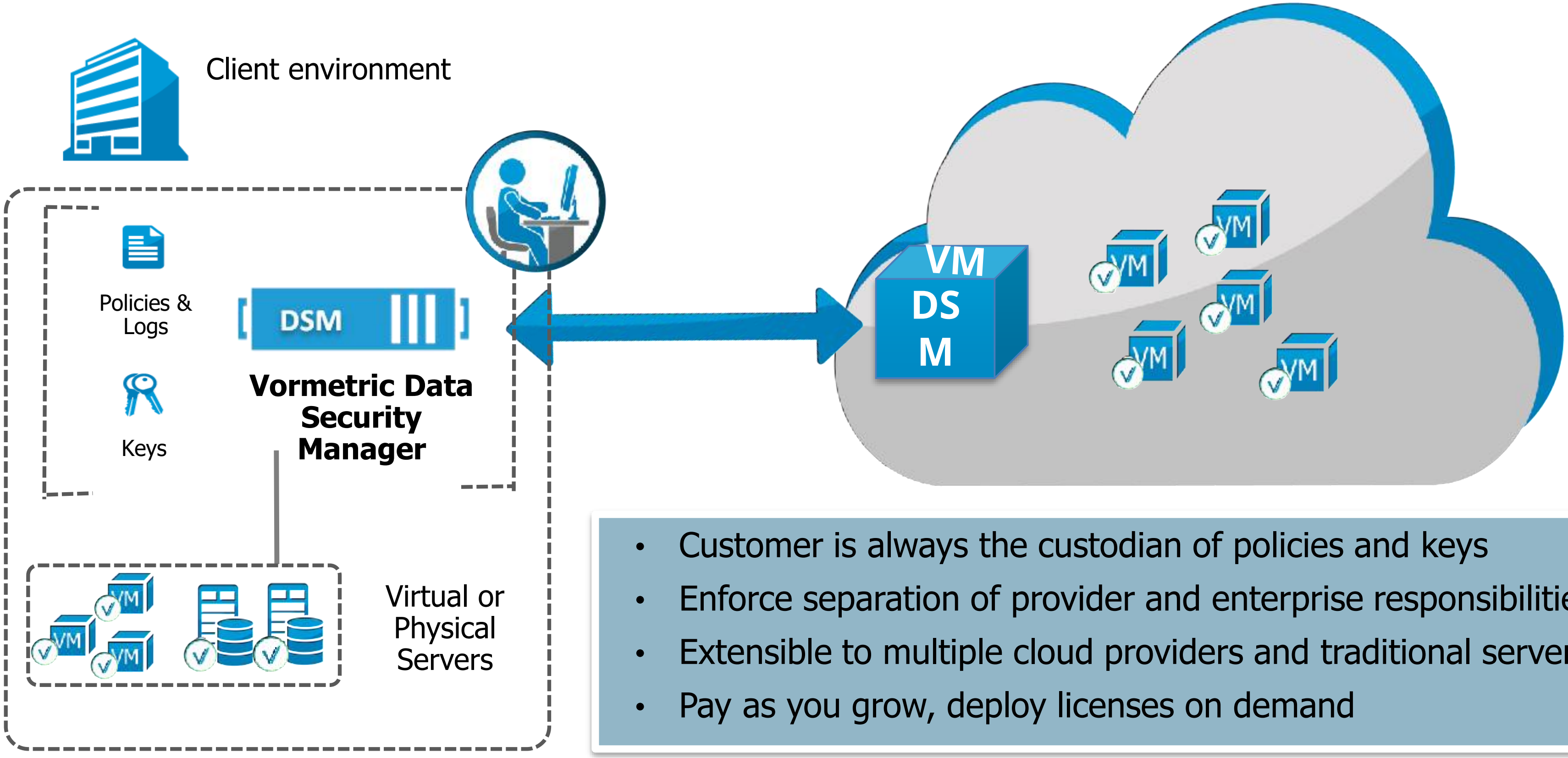
- **TDE only encrypts “data at rest”**
- **TDE protects data if following is stolen or lost -**
  - disk drive
  - database file
  - backup tape of the database files
- **An authenticated database user sees no change**
  - Query results will be decrypted and shown in clear text
- **Does TDE meet legal requirements for encryption?**
  - Access to Oracle wallets (TDE) controls everything
  - California SB1386, Payment Card Industry Data Security
  - Ask your legal department

Encrypt Cloud Databases using HSMs

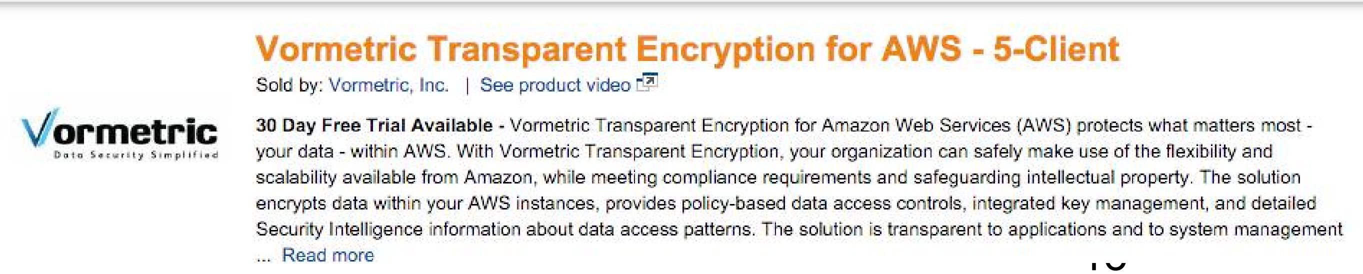
- **Hardware Security Module (HSM)s are physical devices**
  - Secure storage for encryption keys
  - Secure computational space (memory) for encryption and decryption
- **Oracle TDE fully certified to use HSMs**
  - More secure alternative to the Oracle wallet
  - Several third party vendors
    - Vormetric, SafeNet (as Oracle Compute Node)
    - AWS CloudHSM
- **Use HSMs for databases in the Cloud**
  - Design new applications to use

Control your data. Control your keys!

HSM for the Cloud or at Customer



- Customer is always the custodian of policies and keys
- Enforce separation of provider and enterprise responsibilities
- Extensible to multiple cloud providers and traditional servers
- Pay as you grow, deploy licenses on demand



Vormetric Transparent Encryption for AWS - 5-Client

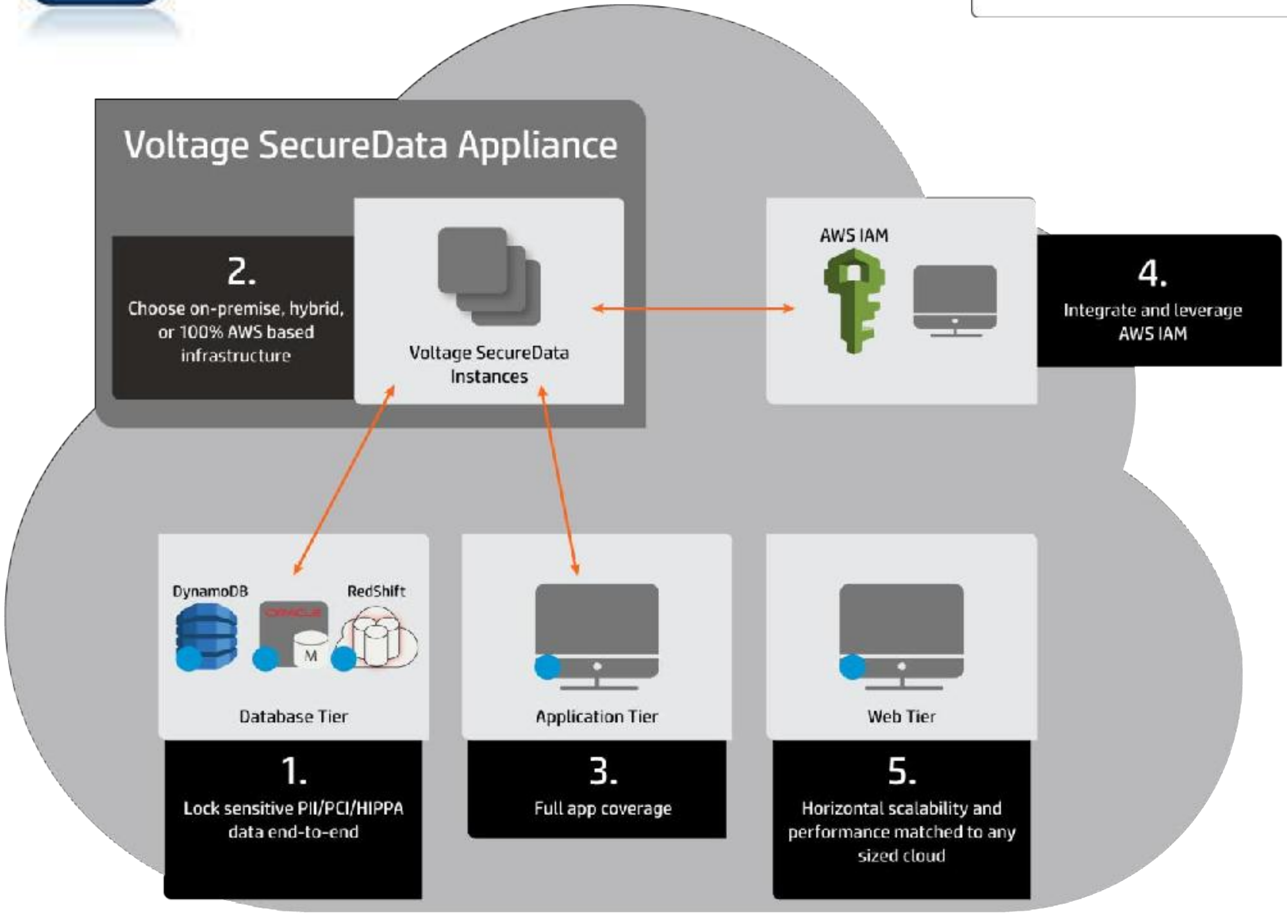
Sold by: Vormetric, Inc. | See product video

30 Day Free Trial Available - Vormetric Transparent Encryption for Amazon Web Services (AWS) protects what matters most - your data - within AWS. With Vormetric Transparent Encryption, your organization can safely make use of the flexibility and scalability available from Amazon, while meeting compliance requirements and safeguarding intellectual property. The solution encrypts data within your AWS instances, provides policy-based data access controls, integrated key management, and detailed Security Intelligence information about data access patterns. The solution is transparent to applications and to system management ... Read more

Tokenization Alternative to Encryption

amazon web services | Partner Network

TECHNOLOGY PARTNER



Voltage SecureData Appliance

2. Choose on-premise, hybrid, or 100% AWS based infrastructure

Voltage SecureData Instances

AWS IAM

4. Integrate and leverage AWS IAM

DynamoDB

RedShift

Database Tier

Application Tier

Web Tier

1. Lock sensitive PII/PCI/HIPPA data end-to-end

3. Full app coverage

5. Horizontal scalability and performance matched to any sized cloud

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**
  - Not compatible with AWS Oracle RDS

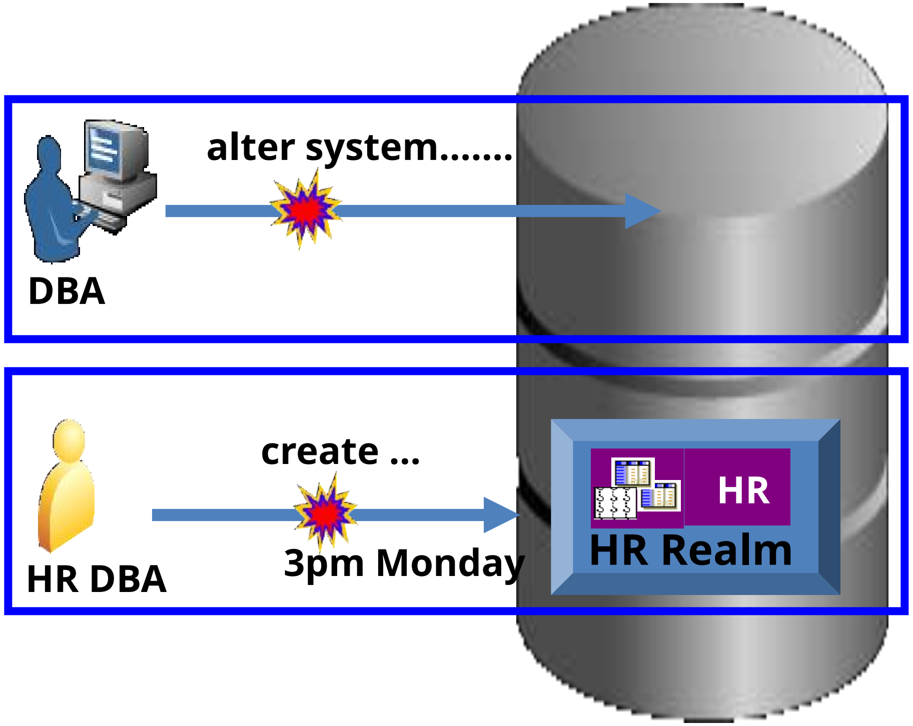
Oracle Database Vault
Rules & Multi-factor Authorization

- **Database DBA attempts remote “*alter system*”**

  Rule based on IP Address blocks action

- **HR DBA performs unauthorized actions during production**

  Rule based on Date and Time blocks action



Factors and Command Rules provide flexible and adaptable security controls

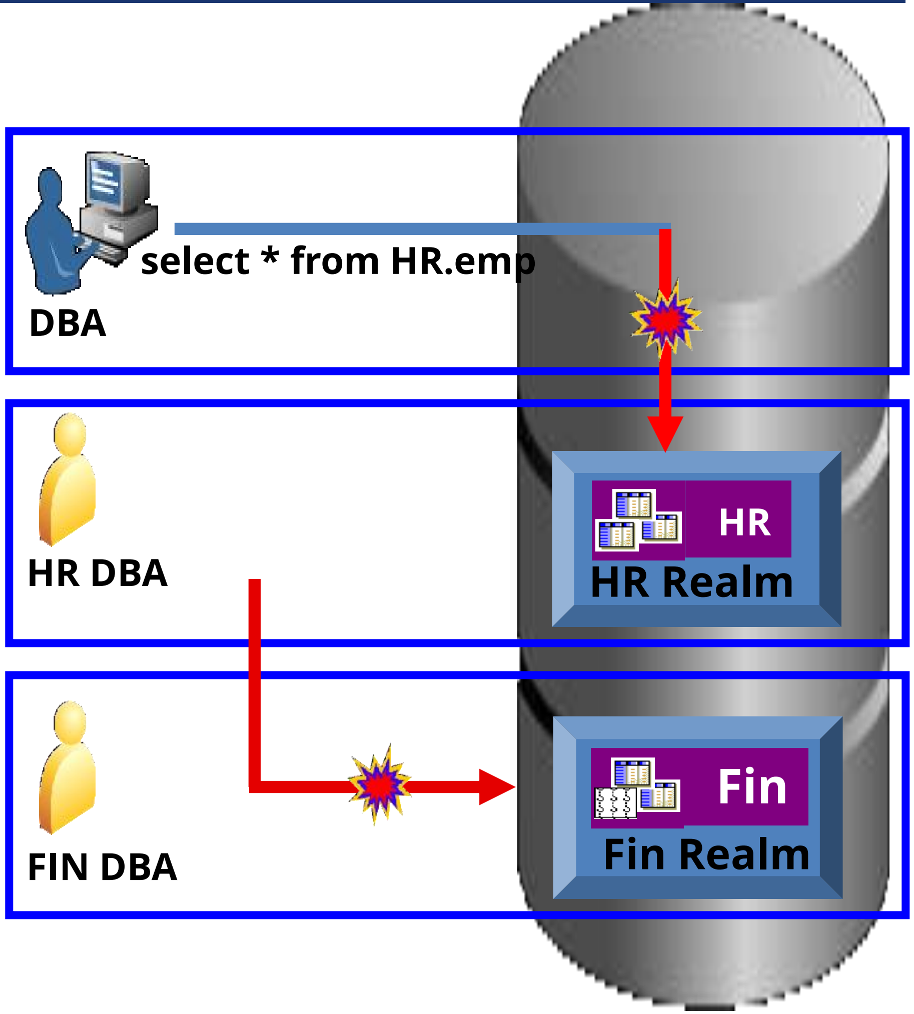
Oracle Database Vault Realms

- **Database DBA views HR data**

  Compliance and protection from insiders

- **HR DBA views Fin. data**

  Eliminates security risks from server consolidation



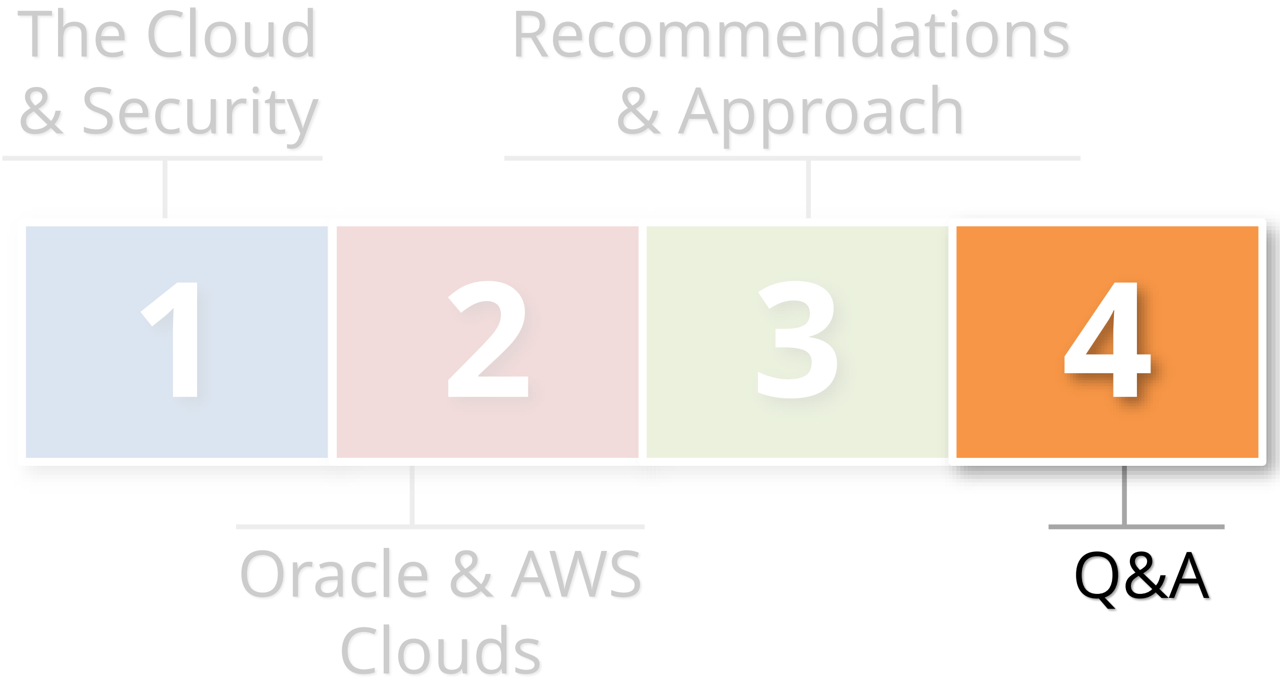
Realms can be easily applied to existing applications with minimal performance impact

Use Command Rules to limit Direct Access[1]

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

[1] Could you attempt the same with VPD and logon triggers?
[2] Program and OS user may be spoofed by the client and are not fully reliable.

Agenda



1 The Cloud & Security

2 Oracle & AWS Clouds

3 Recommendations & Approach

4 Q&A

Contact Information

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

twitter: **@integrigy**

youtube: **youtube.com/integrigy**