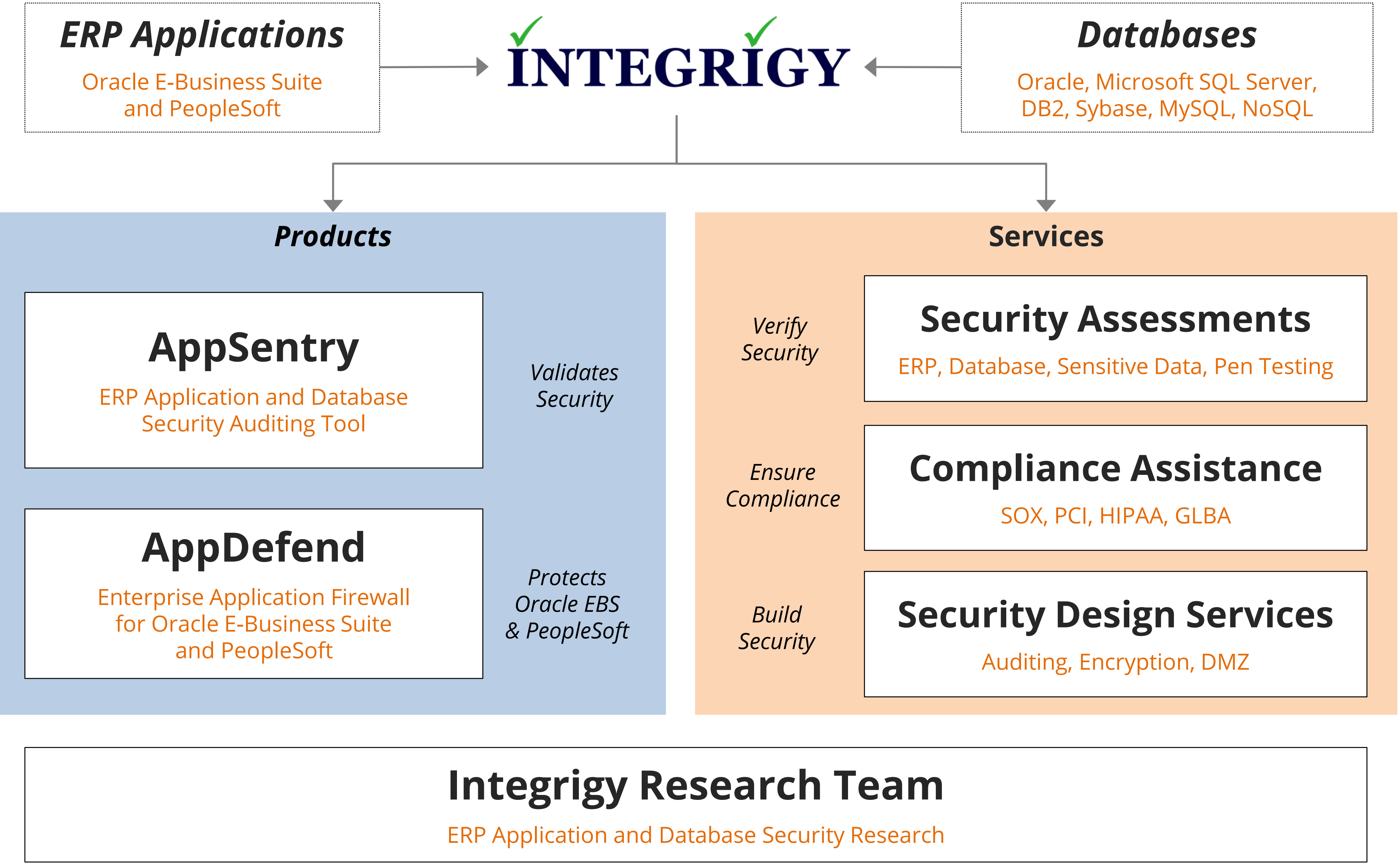
Security Considerations When Running Oracle E-Business Suite in the Cloud

February 20, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



ERP Applications

Oracle E-Business Suite and PeopleSoft

INTEGRIGY

Databases

Oracle, Microsoft SQL Server, DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database Security Auditing Tool

Validates Security

AppDefend

Enterprise Application Firewall for Oracle E-Business Suite and PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

Agenda

1 Cloud and Oracle E-Business Suite

2 Oracle E-Business Suite in the Cloud

3 Recommendations and Approaches

4 Database Security Features

5 Q & A

Agenda

1 Cloud and Oracle E-Business Suite

2 Oracle E-Business Suite in the Cloud

3 Recommendations and Approaches

4 Database Security Features

5 Q & A

Why is the Cloud Inevitable?

- **Increasing feasibility of what is possible**
  - Cloud evolved from outsourcing and hosting
  - Fundamentally outsourcing moving up the stack
  - More multi-tenancy and lawyers, but very concept of what and where a server is changing
  - Is running a data center a competitive advantage for your organization?

- **Commoditization**
  - Paint-power-pipe (data center)
  - Baumol’s cost disease - rise of salaries in jobs that have experienced no increase of labor productivity

Does the Cloud Change Oracle E-Business Suite Security?

Not the what and why,

maybe the how

Data Ownership Does NOT Change

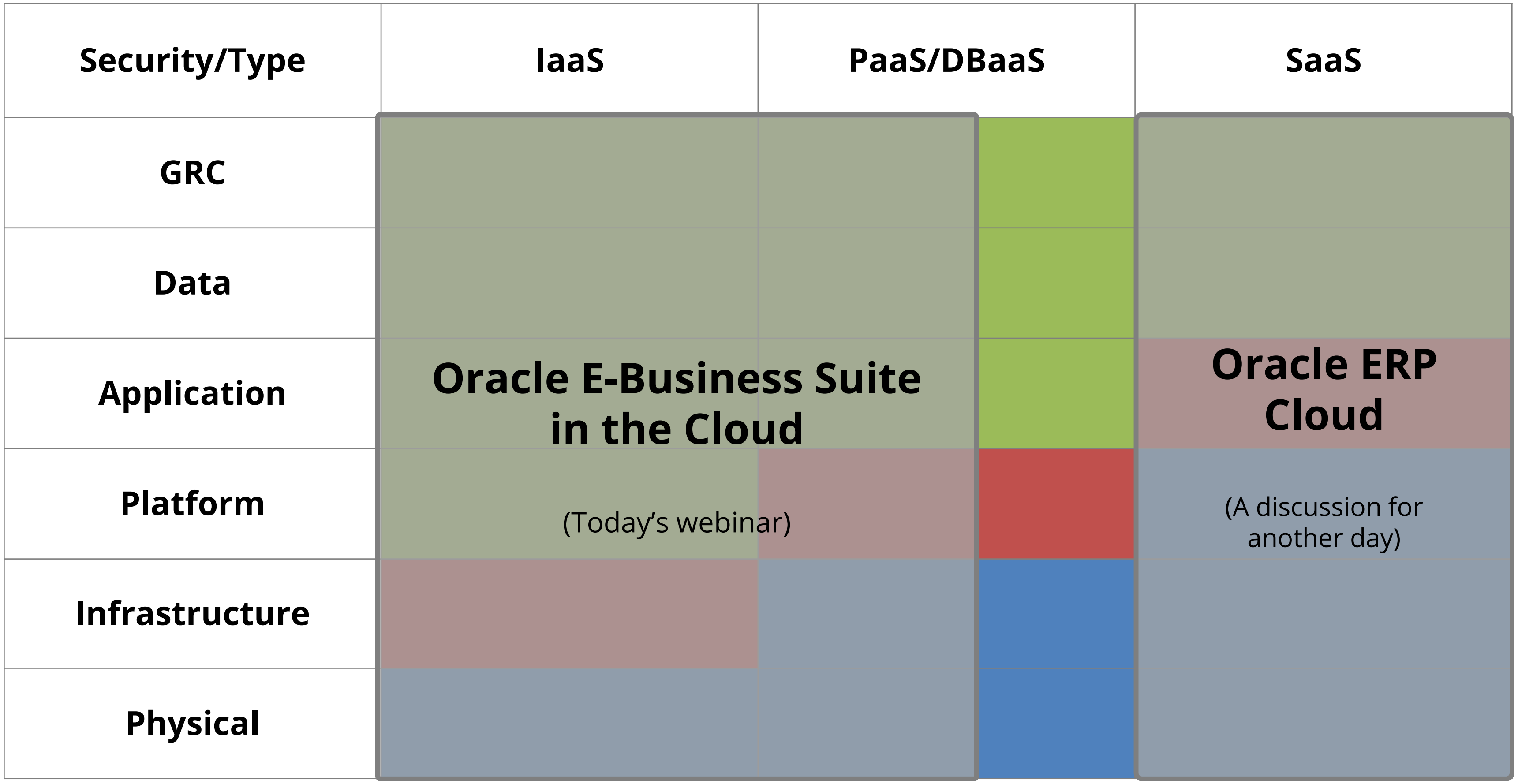
- **You own your data**
  - You are responsible regardless of where it is stored
- **Legal and compliance mandates should flow out and down to your vendor(s)**
  - “Onward transfer” is your responsibility
  - This includes your cloud provider
- **Cloud extends only what should already be in place to protect YOUR data**
  - Security needs to be scaled up
  - Clouds create more insiders

Security Responsibility by Cloud Type

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

Organization = **Green** Shared = **Red** Cloud Provider = **Blue**

Security Responsibility by Cloud Type



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

Oracle E-Business Suite in the Cloud

(Today's webinar)

Oracle ERP Cloud

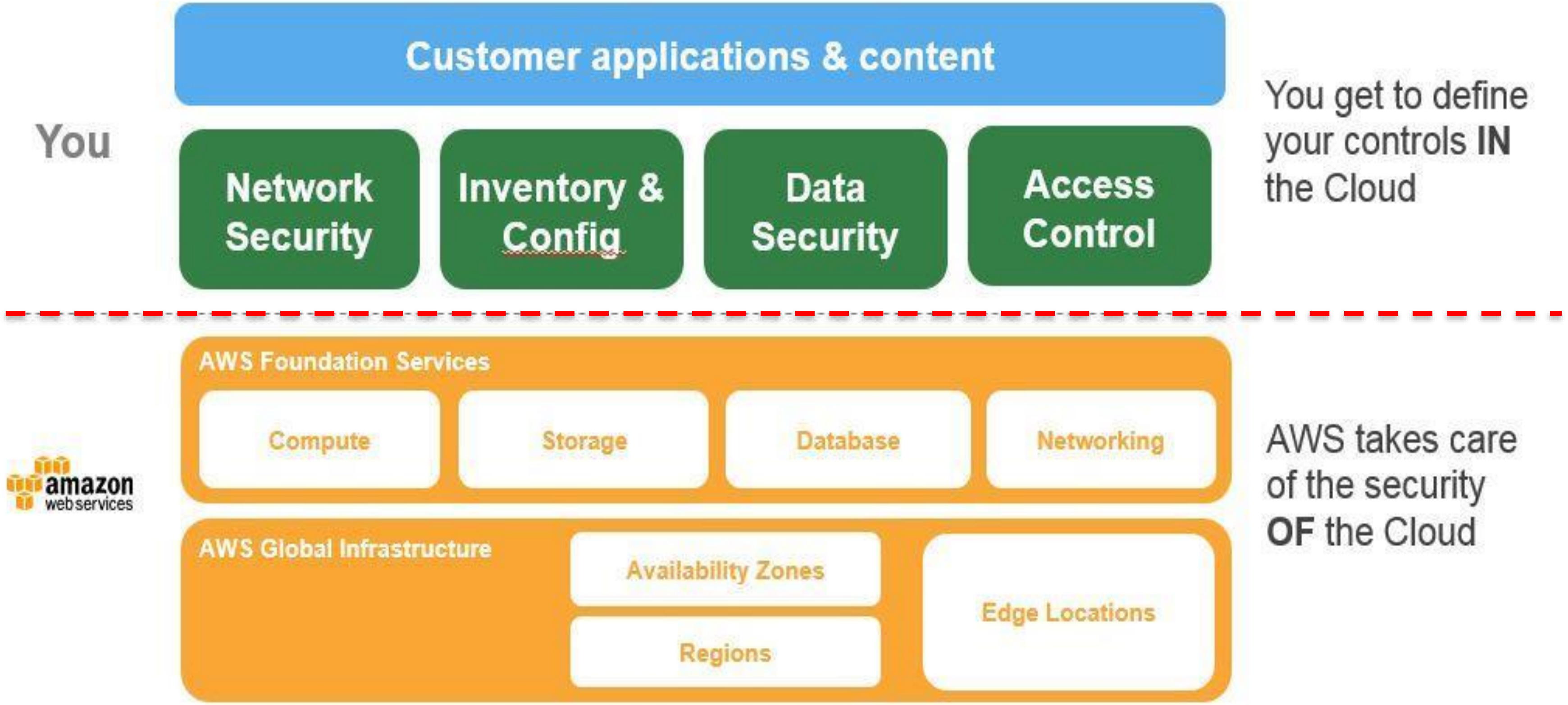
(A discussion for another day)

Organization = **Green** Shared = **Red** Cloud Provider = **Blue**

Oracle E-Business Suite Cloud Vendors

	Oracle EBS Cloud Hosting	**Oracle EBS Managed Services**
Oracle – Oracle Cloud Infrastructure (OCI)	✓	OMCS ACS
Amazon Web Services (AWS) (no RDS)	✓	
Data Intensity	✓	✓
Rackspace	✓	✓
Syntax	✓	✓
Velocity	✓	✓

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”
  - Cloud Controls Matrix (CCM)
  - Security Trust and Assurance Registry (STAR)
  - Consensus Assessments Initiative Questionnaire (CAIQ)
  - https://cloudsecurityalliance.org
- **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 mitigated accepted, avoided, or transferred**
  - Do so wisely
- **Before signing contract**
  - Require SOC 1 annually
  - Push for SOC 2 & CSA CCM controls
  - Read SOC carefully BEFORE signing and assuming nothing
  - Vet provider's supply chain for insiders (additional SOC reports)
- **After signing contract**
  - Hold Provider fully accountable

Agenda

1 Cloud and Oracle E-Business Suite

2 **Oracle E-Business Suite in the Cloud**

3 Recommendations and Approaches

4 Database Security Features

5 Q & A

Oracle E-Business Suite in the Oracle Cloud References

- Getting Started with Oracle E-Business Suite on Oracle Cloud (Doc ID 2066260.1)
- Getting Started with Oracle E-Business Suite on Oracle Cloud Infrastructure (Doc ID 2517025.1)
- Obtaining Support for Oracle Applications on Oracle Cloud - Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) (Doc ID 2181340.2)
- Oracle E-Business Suite on Oracle Cloud Frequently Asked Questions https://docs.oracle.com/cd/E72030_01/infoportal/ebscfaq.html

Oracle OCI Database Cloud Options for Oracle EBS

- **Application tiers always run on Compute Cloud Service**
- **Database tier may run one of the following –**
  - Compute Cloud Service – same as on-premise
  - 1-Node VM DB System (Single Instance)
    - Enterprise Edition
    - Enterprise Edition High Performance
    - Enterprise Edition Extreme Performance
  - 2-Node VM DB System (Oracle RAC)
    - Enterprise Edition Extreme Performance
  - Exadata DB System

Database Cloud Service (Virtual Machine)	▪ SSH and SQL*Net access ▪ Security features based on product
Database Exadata Cloud Service	▪ SSH and SQL*Net access ▪ Enterprise edition plus all options

Oracle Database Cloud Service – Security Options

		Oracle Database Cloud Service	
	Compute Cloud	Enterprise	High Performance Extreme Performance Exadata
Enterprise Edition[1]	**BYOL** Based on your current license	✓	✓
Transparent Data Encryption		✓	✓
Data Masking and Subsetting		✓	✓
Oracle Database Vault			✓
Oracle Advanced Security – Data Redaction			✓
Oracle Label Security			✓

[1] Database Enterprise Edition includes Real Application Security, Virtual Private Database (VPD), and Fine-Grained Auditing (FGA)

Agenda

1 Cloud and Oracle E-Business Suite

2 Oracle E-Business Suite in the Cloud

3 Recommendations and Approaches

4 Database Security Features

5 Q & A

Oracle EBS Security in the Cloud – Issues

- **Complete application and database control equals complete responsibility, same as before**
  - Same access as on-premise to oracle, applmgr, SYS, SYSTEM, SYSADMIN, etc.
  - Slightly less access and control at the operating system
- **Marginal to material security impacts**
  - Insecurities about the Cloud
  - Excessive concerns by auditors (and others)
  - Insufficient auditor capacity and expertise
  - Increased number of insiders
  - Indeterminate technical complexities and expertise
  - Ineptitude due to junior DBAs or no DBAs

Professional Management Still Needed

- **Infrastructure, architecture, Oracle EBS, and databases still need professional management**
  - Applications and databases are critical assets that need to be under your change control
  - Provisioning processes and gatekeepers needed
  - Technical decisions still need to be made

High-level/Architect DBA expertise required for Cloud oversight

Restrict Access to Database and Console

- **Secure Provider's management console**
  - Separate admin accounts for production and test/development
  - 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)
- **Network**
  - Oracle – Security IP lists & Rules
  - AWS – security Groups (IP ACLs) & subnets
  - Bastion host/jump box for admins and DBAs

Database Security Patches (Critical Patch Updates)

Oracle	▪ For Database Cloud Service – - CPU patches available quickly - Approved patches can be applied through the Service Console or dbaascli-dbpatchm ▪ For Compute Cloud Service – - Same as on-premise
AWS	▪ Same as on-premise

Continuously Audit to Verify Trust

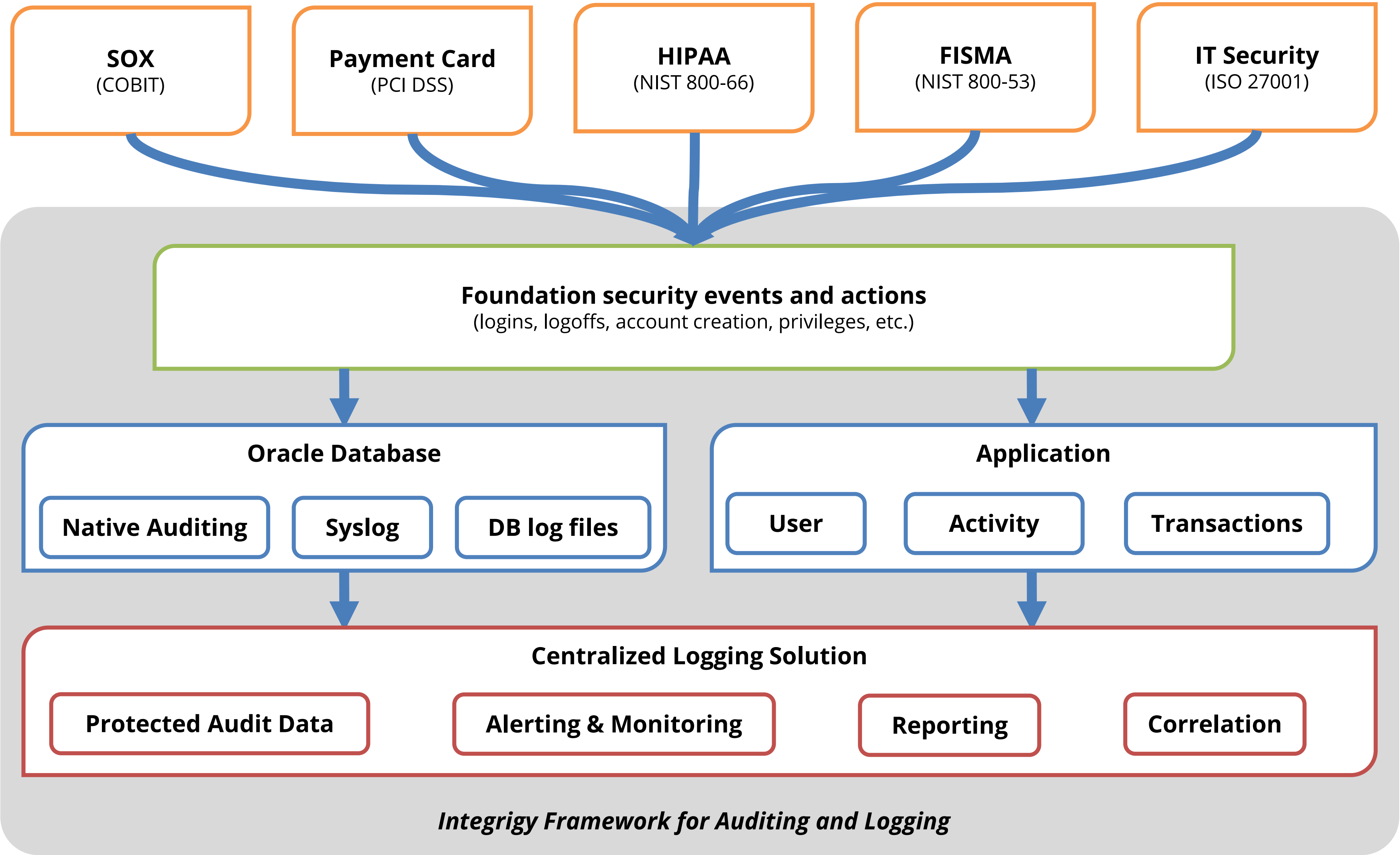
- **Risks to Oracle EBS in the Cloud**
  - What level of service is vendor providing? Managed Services?
  - How do guard against authorized changes and access?
  - How to identify poor or risky behaviors?
  - How to meet compliance requirements (SOX, HIPAA, PCI)?
- **All research says to use policy of 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 E-Business logging and auditing**

  https://www.integrigy.com/security-resources/guide-auditing-oracle-applications

Log and Audit File Retention

Oracle OCI	**Oracle Database Service** ▪ Alert log, database audit files, listener log files retained by default for 14 days ▪ Edit `/var/opt/oracle/cleandb/cleandblogs.cfg` to change retention periods

Integrigy Framework for Auditing and Logging



Integrigy Framework for Auditing and Logging

Foundation Security Events Mapping

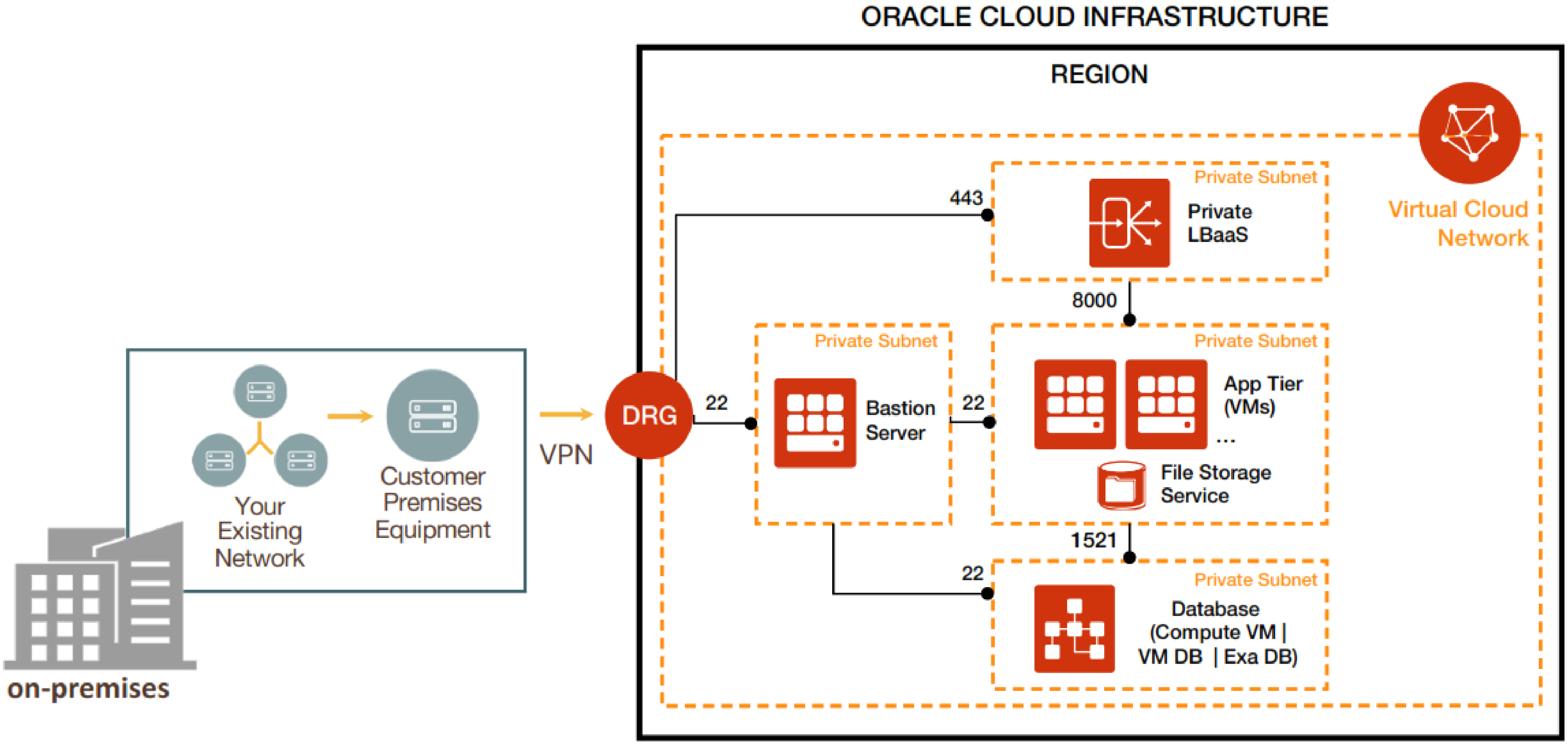
Security Events and Actions	PCI DSS 10.2	SOX (COBIT)	HIPAA (NIST 800-66)	IT Security (ISO 27001)	FISMA (NIST 800-53)
E1 - Login	10.2.5	A12.3	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	DS5.5	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - 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

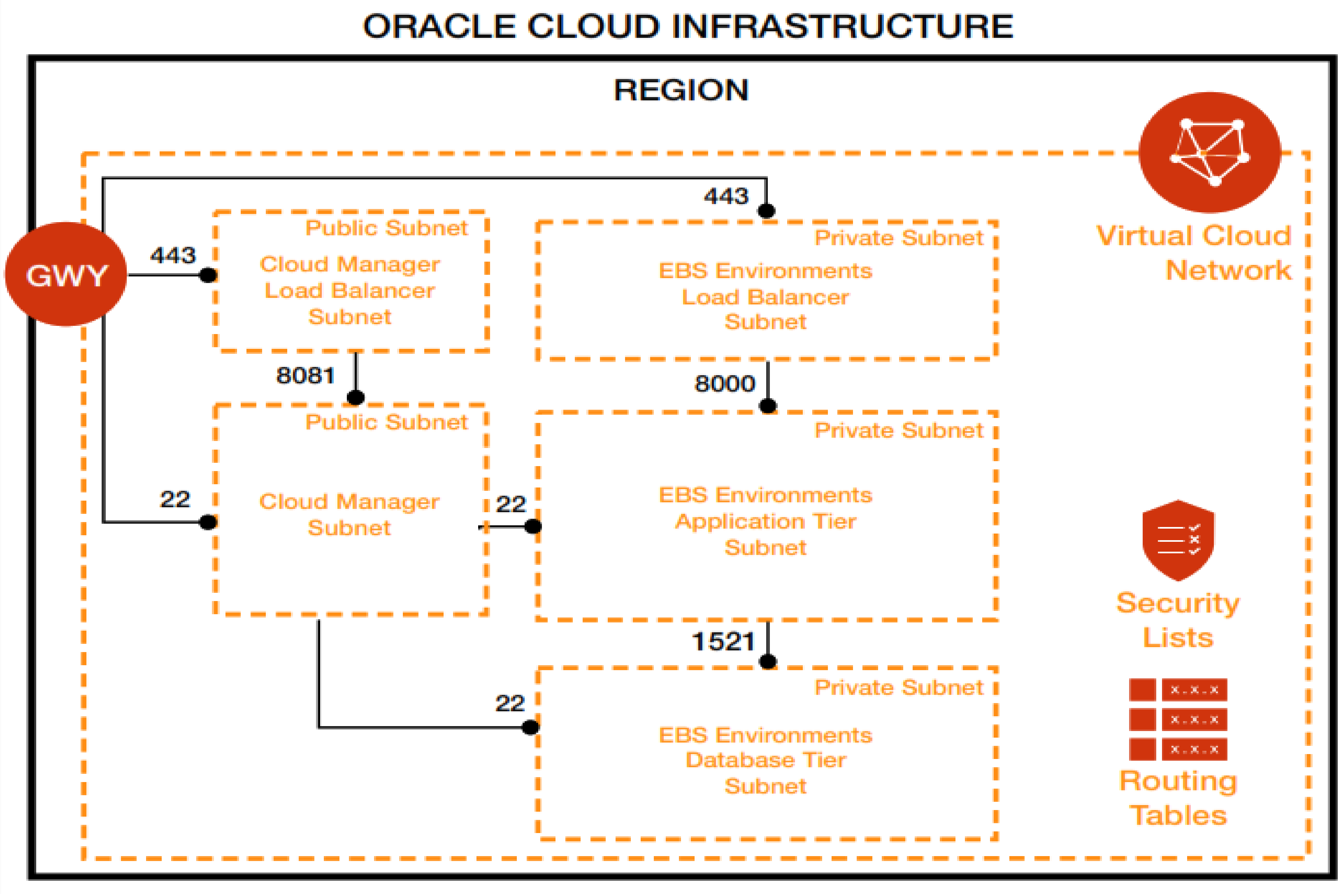
- **Based on database security research**
  - Designed as part of a holistic database security program
  - Enforces configuration and access management best practices
  - Compliance matrix mapping – SOX, PCI etc.
  - Specific high-risk events, sensitive packages, alerts, error codes and usage patterns
  - 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

OCI Network Security

- Virtual Cloud Network (VCN) and subnets
- Security lists and route tables
- Internet gateway and dynamic routing gateway

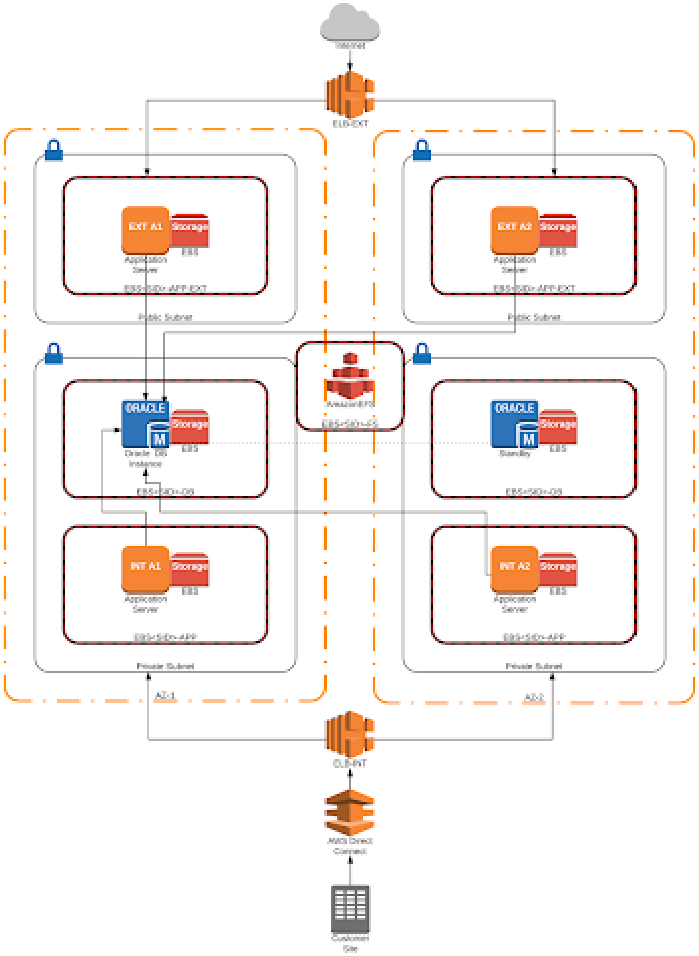


OCI Network Security Sample



AWS Cloud Network Security

- Regions / Availability Zones
  - Subnets
  - Network interfaces
  - Route tables
- Security
  - Network ACLs
  - Security Groups
  - Internet Gateway
- Virtual Private Gateway
  - IPSec VPN tunnel with your on-premise network



Cloud Network Security

- **Use bastion hosts to connect to servers**
  - Prevent direct access from internal network
  - Bastion host is in the public subnet but requires ACL to allow access only from on-premise network
  - Open ports to allow access to servers as required
  - All OS level access should be through bastion host

- **Use load balancers for all application server traffic**
  - Use even if only one application server
  - Use for all SSL/TLS termination
  - Acts as a reverse proxy
  - Do not need to configure SSL/TLS on application servers
  - Oracle EBS SSL stack is dated and requires periodic patching
  - AWS – use Global Accelerator for improved International network performance

Agenda

1 Cloud and Oracle E-Business Suite

2 Oracle E-Business Suite in the Cloud

3 Recommendations and Approaches

4 **Database Security Features**

5 Q & A

Oracle Database Cloud Service – Security Options

		Oracle Database Cloud Service	
	Compute Cloud	Enterprise	High Performance Extreme Performance Exadata
Enterprise Edition[1]	BYOL Based on your current license	✓	✓
Transparent Data Encryption		✓	✓
Data Masking and Subsetting		✓	✓
Oracle Database Vault			✓
Oracle Advanced Security – Data Redaction			✓
Oracle Label Security			✓

[1] Database Enterprise Edition includes Real Application Security, Virtual Private Database (VPD), and Fine-Grained Auditing (FGA)

Cloud Encryption Options

- **Network (Data in motion)**
  - Encryption of data when transferred between two systems
  - SQL*Net encryption (database)
- **Storage (Data at rest)**
  - Disk, storage, media level encryption
  - Encryption of data at rest such as when stored in files or on media
  - Oracle TDE (database)
- **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
  - Not provided by cloud providers

SQL*Net Encryption

Oracle OCI	▪ For Database Cloud Service, SQL*Net encryption enabled by default
	▪ For Compute Cloud Service, SQL*Net encryption may be default of Requested and should be set to Required –
	`SQLNET.ENCRYPTION_SERVER = required`
	`SQLNET.CRYPTO_CHECKSUM_SERVER = required`

AWS	▪ SQL*Net encryption may be default of Requested and should be set to Required –
	`SQLNET.ENCRYPTION_SERVER = required`
	`SQLNET.CRYPTO_CHECKSUM_SERVER = required`

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 Consumer Privacy Act (CCPA), Payment Card Industry Data Security (PCI-DSS)
  - Ask your legal department

Oracle Transparent Data Encryption

Oracle OCI	▪ Oracle TDE included with Database Cloud Service, not when running Compute Cloud Service ▪ For Database Cloud Service – - Oracle TDE enabled by default - Oracle Wallet set to auto-open - Allows access and control of the Oracle Wallet - Customer responsible for rotating TDE master key - TDE master keys may be stored in Oracle Key Vault ($) - **Lift and Shift databases may not be encrypted during migration – may have to be encrypted after migration**
AWS	▪ Oracle TDE is an option and must be enabled ▪ Requires an Oracle TDE license ▪ AWS manages the Oracle wallet and TDE master key ▪ No capability to rotate the TDE master key

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
- **Oracle OCI = Included with High/Extreme Performance**
- **AWS = Must purchase license and implement**

Use Command Rules to limit Direct Access

	IP Address	Program[1]	OS User[1]
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] Program and OS user may be spoofed by the client and are not fully reliable.

Agenda

1 Cloud and Database Security

2 Databases at Oracle and Amazon

3 Recommendations and Approaches

4 Database Security Features

5 Q & A

Integrigy Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

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

youtube – **youtube.com/integrigy**