INTEGRIGY

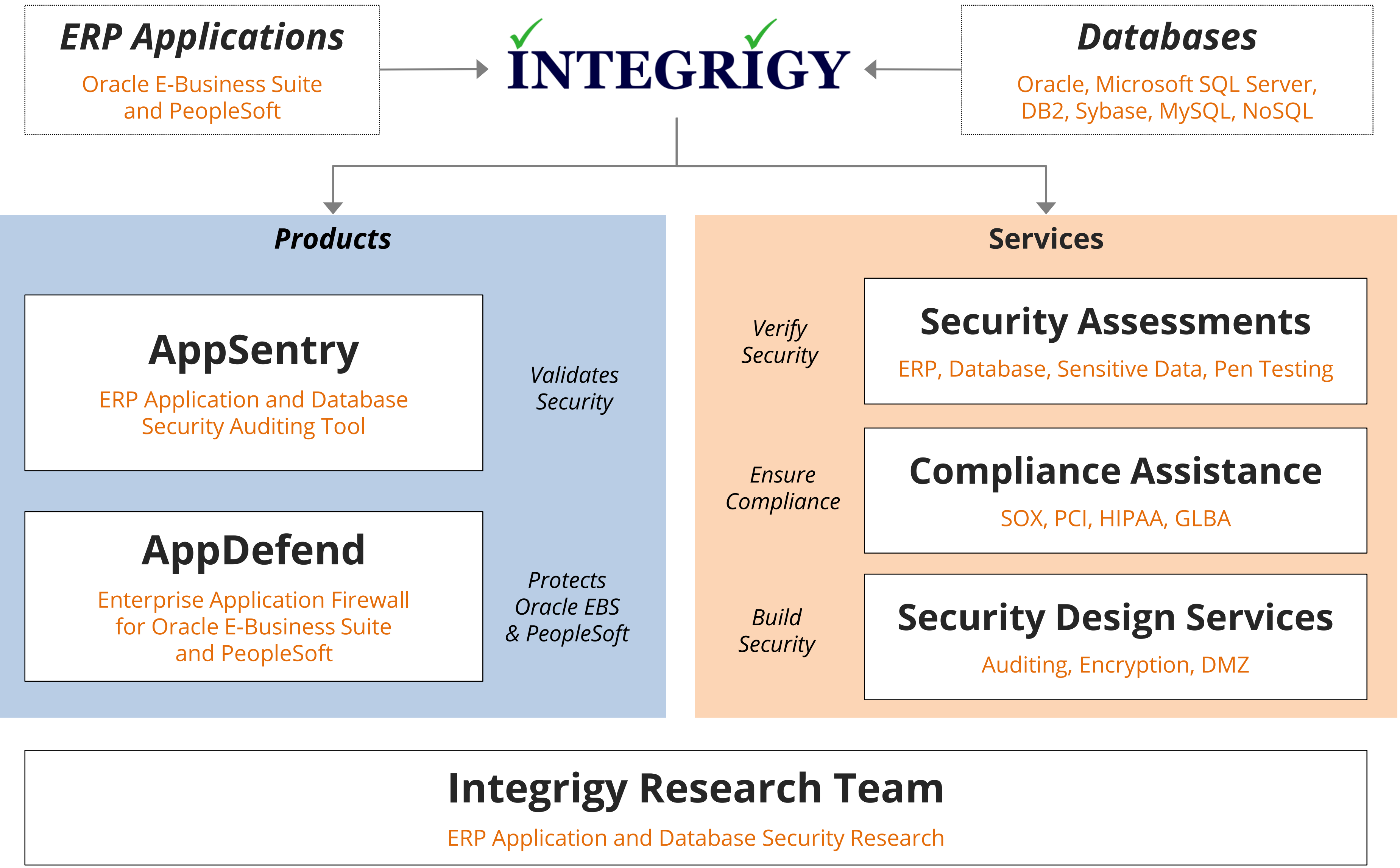
Change Your Thinking About Security with Oracle Database in the Cloud

January 22, 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 Database Security

2 Databases at Oracle and Amazon

3 Recommendations and Approaches

4 Database Security Features

5 Q & A

Agenda

1 Cloud and Database Security

2 Databases at Oracle and Amazon

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 Database Security?

Not the what and why,

maybe the how

Data Ownership Does NOT Change

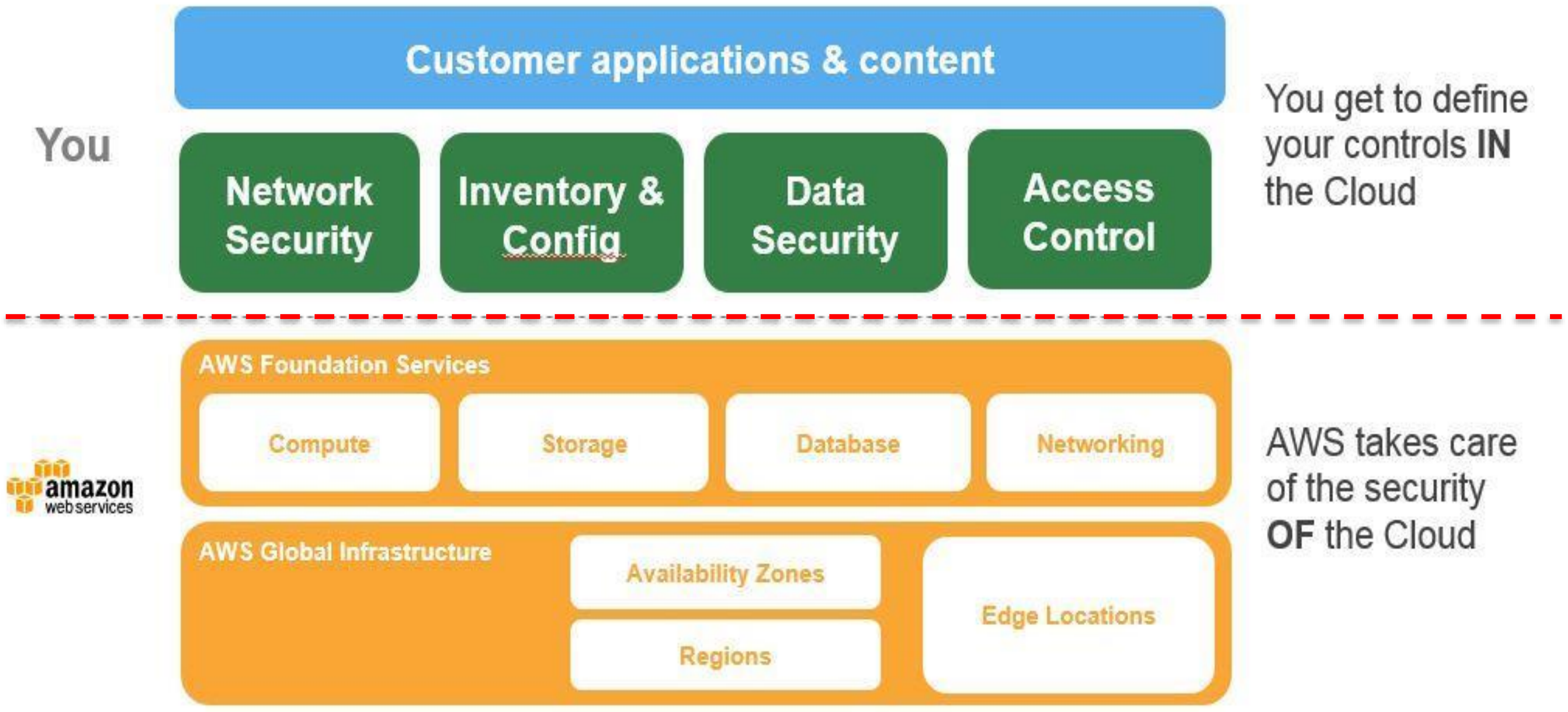
- **You own your data**
  - You are responsible regardless of where it is stored
- **Legal and compliance mandates should flow out and down to your vendor(s)**
  - “Onward transfer” is your responsibility
  - This includes your cloud provider
- **Cloud extends only what should already be in place to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

Amazon AWS Shared Security



You

Customer applications & content

Network Security

Inventory & Config

Data Security

Access Control

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

amazon web services

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

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 Database Security

2 **Databases at Oracle and Amazon**

3 Recommendations and Approaches

4 Database Security Features

5 Q & A

Oracle Database Cloud Offerings – User-managed

Database Cloud Service (Virtual Machine)	▪ SSH and SQL*Net access ▪ Security features based on product
Database Cloud Service (Bare Metal)	▪ SSH and SQL*Net access ▪ Security features based on product
Exadata Express Service	▪ SQL*Net, REST, and SODA access ▪ Pluggable database ▪ Enterprise edition plus options
Database Exadata Cloud Service	▪ SSH, SQL*Net, REST, and SODA access ▪ Enterprise edition plus all options
Database Schema Service	▪ APEX and REST access only

Oracle Database Service – Security Options

	Standard	Enterprise	High/Extreme Performance
Standard Edition 2	✓		
Enterprise Edition		✓	✓
Transparent Data Encryption	✓	✓	✓
Data Masking and Subsetting		✓	✓
Oracle Database Vault			✓
Oracle Advanced Security – Data Redaction			✓
Oracle Label Security			✓

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

Amazon Terminology

AWS	▪ Amazon Web Services
EC2	▪ IaaS ▪ Amazon Elastic Compute Cloud ▪ Virtualized hardware
RDS	▪ DBaaS ▪ Relational Database Service ▪ Supports Amazon Aurora, PostgreSQL, MySQL, MariaDB, **Oracle**, and Microsoft SQL Server

Amazon Oracle Database Cloud Offerings

EC2 (IaaS)	▪ Pure virtualized hardware ▪ Almost the same as running Oracle on-premise
RDS (DBaaS)	▪ SQL*Net access – no SYSDBA ▪ SYS and SYSTEM locked and cannot be used

RDS Supported

- Transparent Data Encryption (Add-on)
- Data Redaction (Add-on)
- SQL*Net Encryption
- Virtual Private Database (EE)
- Fine-Grained Auditing (EE)
- Unified Auditing Mixed Mode (12.2+)

RDS NOT Supported

- Database Vault
- Unified Auditing (12.1)
- Unified Auditing Pure Mode

Amazon Relational Database Service (RDS)

- **Master DBA account used rather than SYS/SYSTEM**
- **DBA account does not have the following privileges**
  - alter database
  - alter system
  - create any directory
  - drop any directory
  - grant any privilege
  - grant any role

Agenda

1 Cloud and Database Security

2 Databases at Oracle and Amazon

3 **Recommendations and Approaches**

4 Database Security Features

5 Q & A

Database Security in the Cloud – Issues

- **Complete database control equals complete responsibility, same as before**
  - Oracle Database Cloud Service
  - Oracle Autonomous Cloud Service = shared database control
  - AWS EC2
  - AWS RDS = shared database control
- **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, and databases still need professional management**
  - Databases are critical assets that need to be under your change control
  - Provisioning processes and gatekeepers needed
  - Technical decisions still need to be made
  - Security patches NOT automatically applied quarterly
  - Use Oracle OEM if possible

High-level/Architect DBA expertise required for Cloud oversight

Restrict Access to Database

- **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

Restrict Access to Database

- **Cloud ACLs and services**
  - Can be fully managed within the cloud tools
- **Oracle Database Valid Node Checking**
  - Simple lists of IP addresses
- **Oracle Connection Manager**
  - Can be deployed on same sever
  - Most flexible rules to restrict access
- **Oracle Database Vault**
  - Connection rules
  - Database add-on – included with Oracle High/Extreme Performance
- **Database Firewall**

Database Security Patches (Critical Patch Updates)

Oracle	▪ CPU patches available quickly ▪ Approved patches can be applied through the Service Console or dbaascli-dbpatchm
AWS RDS	▪ Patch Set Updates (PSU) available for currently supported versions (11.2.0.4 and 12.1.0.2) with other AWS determined patches ▪ RU and RUR available for currently supported versions (19c, 18c, 12.2) with other AWS determined patches ▪ No one-off patches – only PSUs ▪ Delay from release to RDS availability

Prove Governance by Using Baselines

- **Use security best practice baseline configurations specific to Oracle RDBMS**
  - CIS Oracle 11.2, 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 customize CIS or DISA STIG as default will break applications
  - Must prove on-going adherence, not just one-time project
  - Use to calm and objectively communicate with auditors

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 add-on Lifecycle Management Pack)
  - Integrigy AppSentry

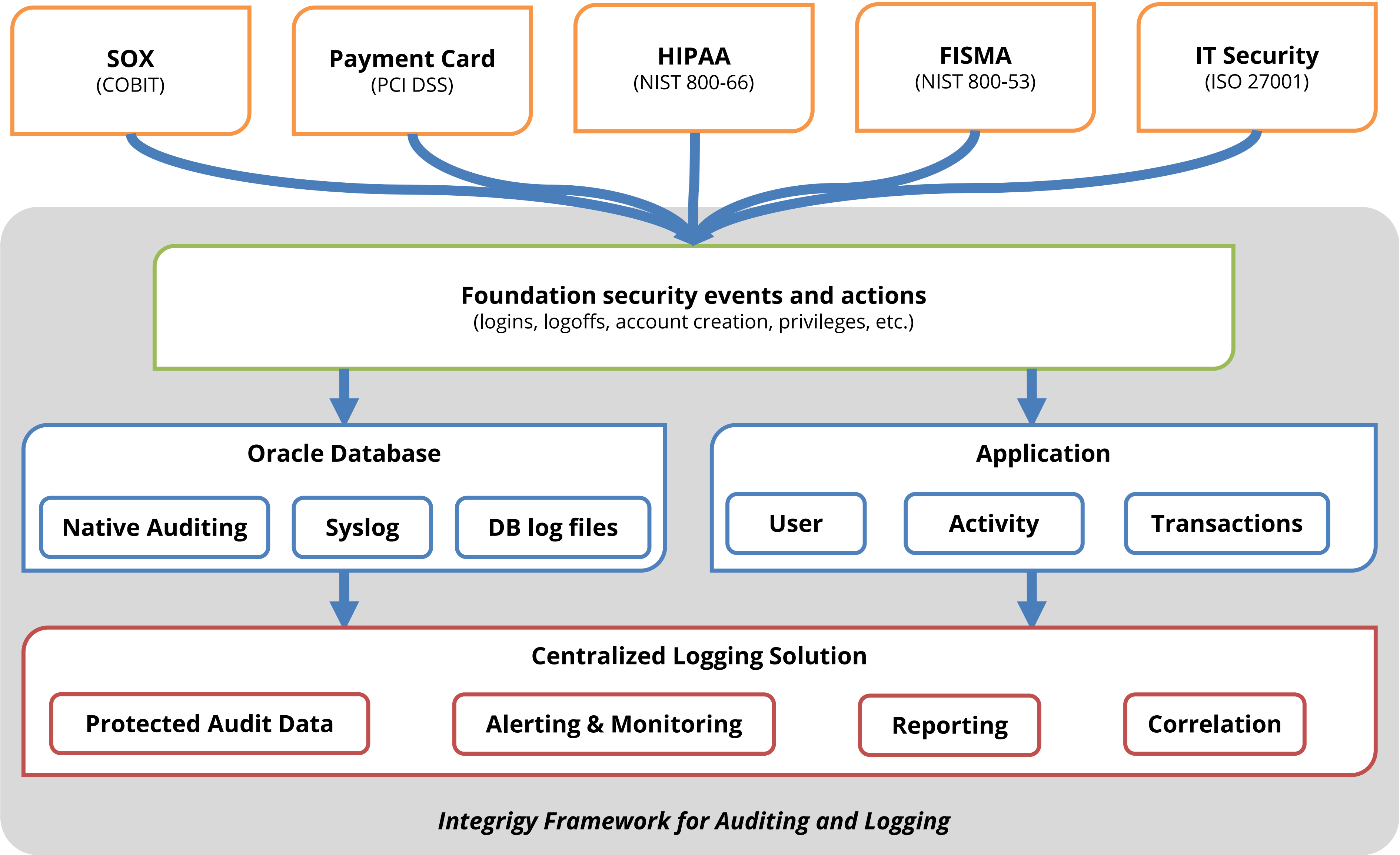
Continuously Audit to Verify Trust

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

Log and Audit File Retention

Oracle	▪ 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
AWS RDS	▪ Alert log, database audit files, listener log files retained by default for at least 7 days and may be removed ▪ Must download files to long-term retention ▪ No access to SYS.FGA_LOG$

Integrigy Framework for Auditing and Logging



SOX
(COBIT)

Payment Card
(PCI DSS)

HIPAA
(NIST 800-66)

FISMA
(NIST 800-53)

IT Security
(ISO 27001)

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

Oracle Database

- Native Auditing
- Syslog
- DB log files

Application

- User
- Activity
- Transactions

Centralized Logging Solution

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

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

Agenda

1 Cloud and Database Security

2 Databases at Oracle and Amazon

3 Recommendations and Approaches

4 **Database Security Features**

5 Q & A

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	▪ SQL*Net encryption enabled by default
	`SQLNET.ENCRYPTION_SERVER = required`
	`SQLNET.CRYPTO_CHECKSUM_SERVER = required`

AWS RDS	▪ SQL*Net encryption is not required by default
	`SQLNET.ENCRYPTION_SERVER = requested`
	`SQLNET.CRYPTO_CHECKSUM_SERVER = requested`
	▪ Referred to as Oracle Native Network Encryption (NNE)
	▪ Set to “required” by creating a new or modifying an existing Option Group

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	▪ Oracle TDE included with all cloud databases ▪ 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 ($) ▪ **Migrated databases are NOT encrypted during migration – must be encrypted after migration**
AWS RDS	▪ 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
- **Included with Oracle High/Extreme Performance**
- **Not available with AWS Oracle RDS**

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**