IBM Connect 2015

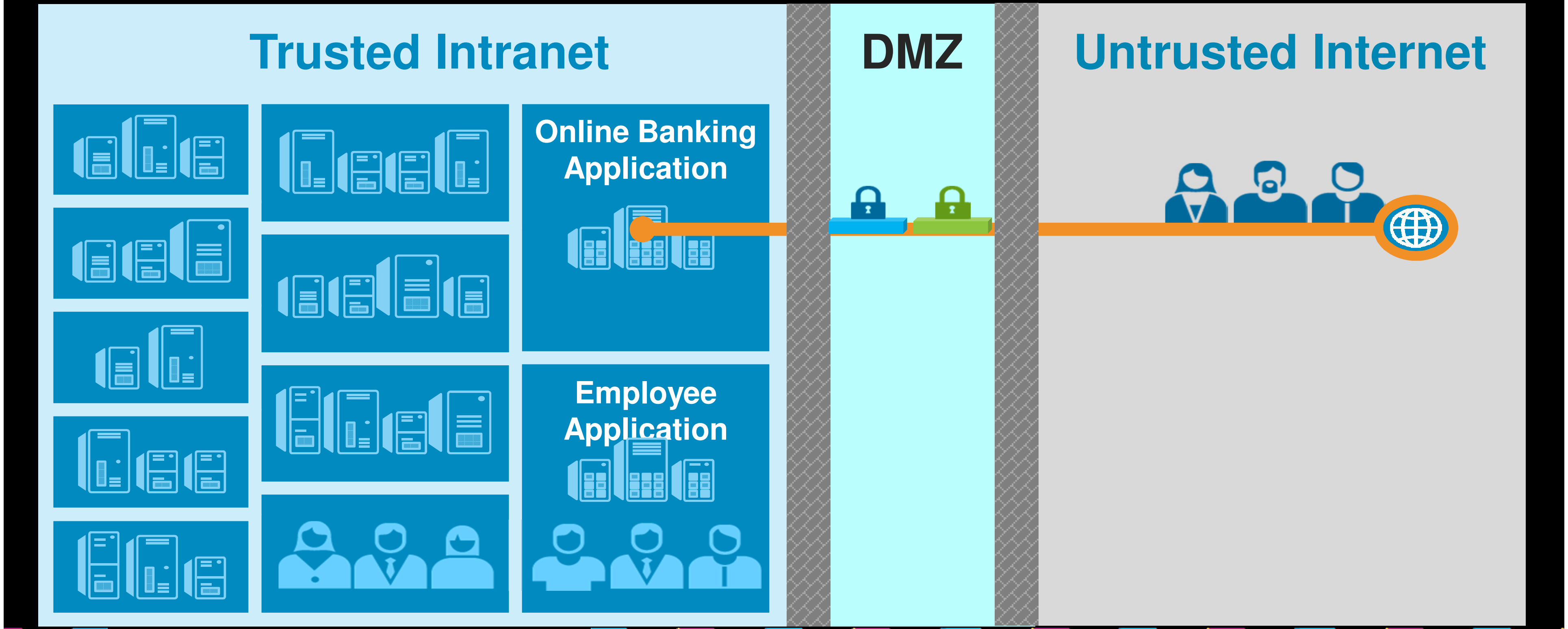
Innovate. Understand. Engage.

Is Your Data Safe in the Cloud?

Mike Murphy, CISSP

Worldwide Data Governance Solution Architect

Traditional IT infrastructures
IT security is obtained through the Demilitarized Zone (DMZ)



Trusted Intranet

DMZ

Untrusted Internet

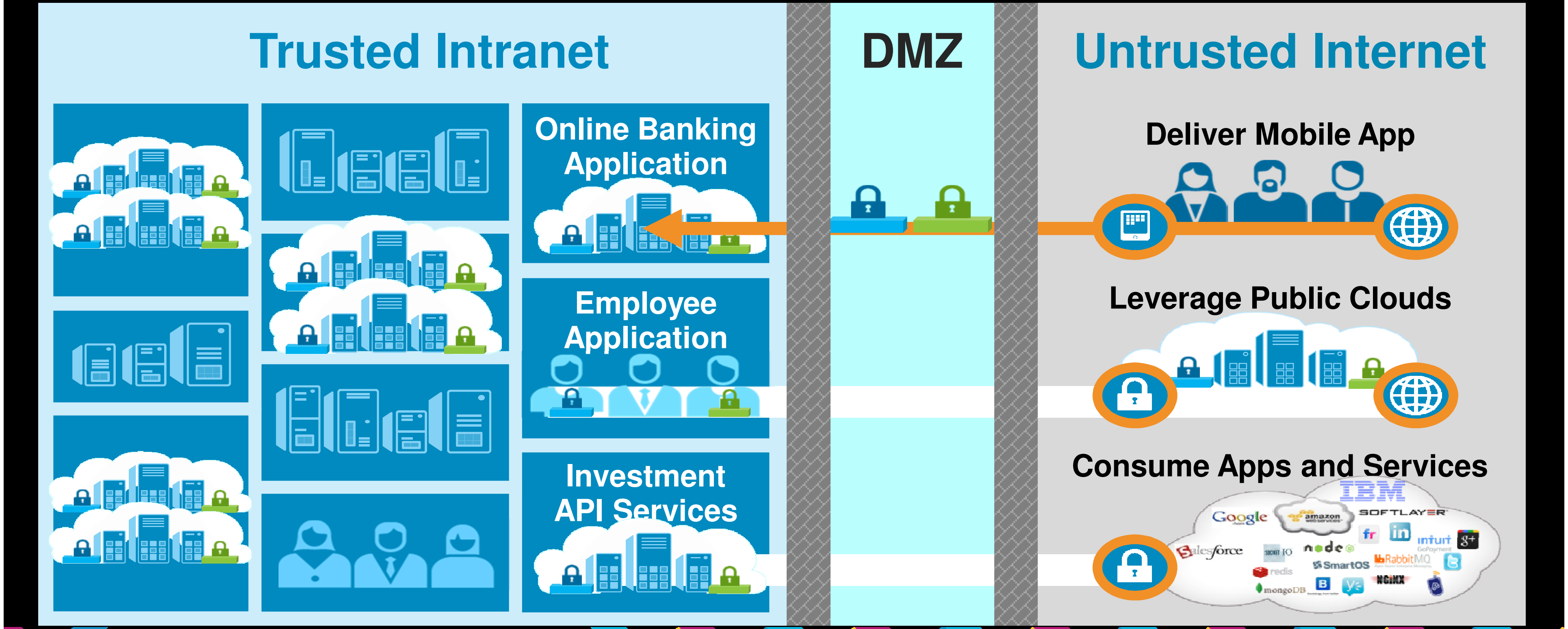
Online Banking Application

Employee Application

IBM Connect 2015

Innovate. Understand. Engage.

Cloud IT infrastructure
Enterprise security is obtained through “application zones”



Trusted Intranet

DMZ

Untrusted Internet

Online Banking Application

Employee Application

Investment API Services

Deliver Mobile App

Leverage Public Clouds

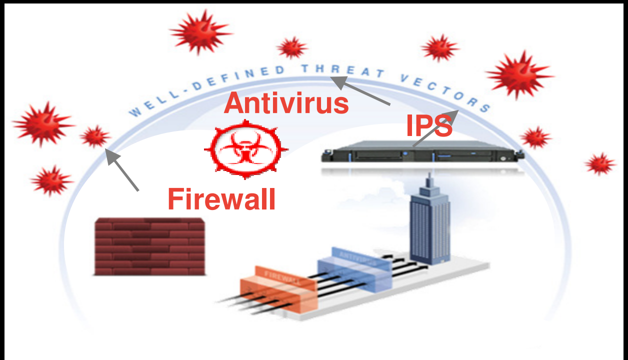
Consume Apps and Services

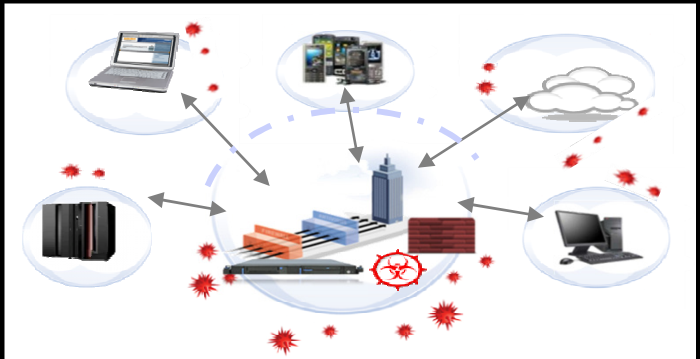
The new era of computing has arrived

Data explosion	Consumerization of IT	Everything is everywhere	Attack sophistication

Extending the Perimeter Shifts Protection Focus to Data

Moving from traditional perimeter-based security… → …to logical "perimeter" approach to security - focusing on the data and where it resides

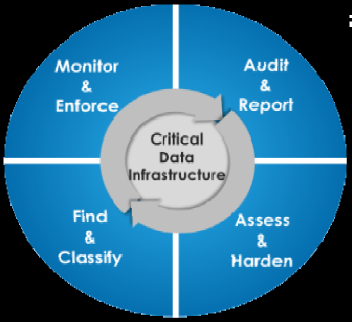




Cloud, Mobile and Data momentum is breaking down the traditional perimeter and forcing us to look at security differently……. Focus needs to shift from the perimeter to the data that needs to be protected

Data Security Vision

- Protect data in any form, anywhere, from internal or external threats
- Streamline regulation compliance process
- Reduce operational costs around data protection



Data Classification

- **Type of data**
- PCI data
- SOX data
- Video
- Document
- Proprietary Data

Data Repository

- **Repository**
- Databases
- DW/Hadoop
- Hadoop
- No-SQL
- File Shares

- **Location**
- On premise
- Private cloud
- Public cloud
- Managed

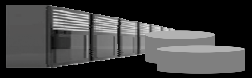
Data Consumers

- **Consumer**
- Customers (anyone)
- Outsourced (3rd party)
- Employees (internal)
- Role-based (trusted)

- **Channel**
- Hosted applications
- Cloud applications
- Mobile

Data Discovery

Data at Rest



Stored

(Databases, File Servers, Big Data, Data Warehouses, Application Servers, Cloud/Virtual ..)

- Encryption
- Tokenisation
- Redaction
- Masking
- Storage

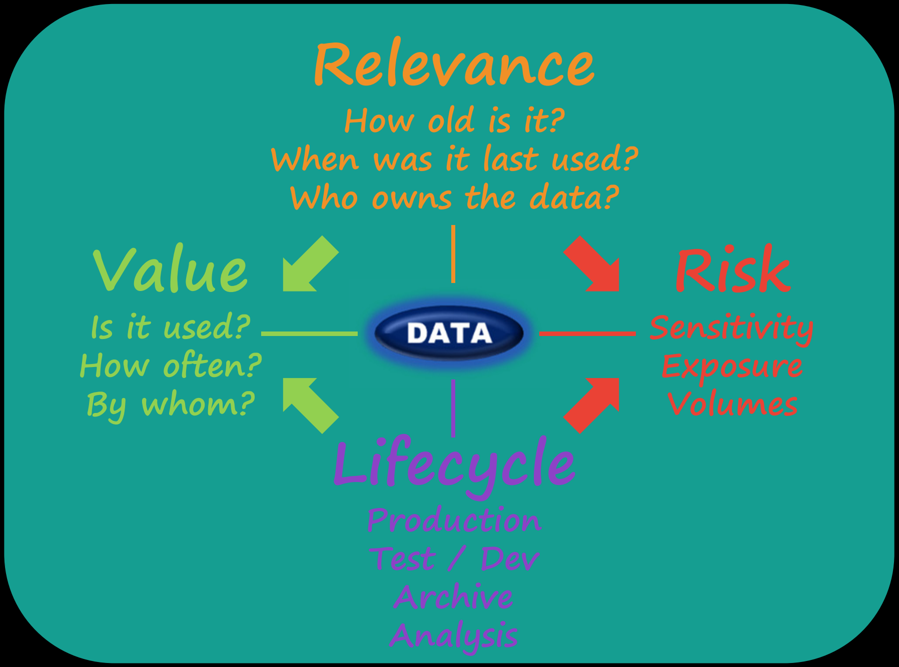
Data in Motion

Over Network

(SQL, HTTP, SSH, FTP, email,. …)

- Activity Monitoring
- Real-time Alerting
- Dynamic Masking
- Blocking
- Activity Reporting

Our Philosophy:
You need to understand the data in order to protect it



Relevance

How old is it?
When was it last used?
Who owns the data?

Value

Is it used?
How often?
By whom?

DATA

Risk

Sensitivity
Exposure
Volumes

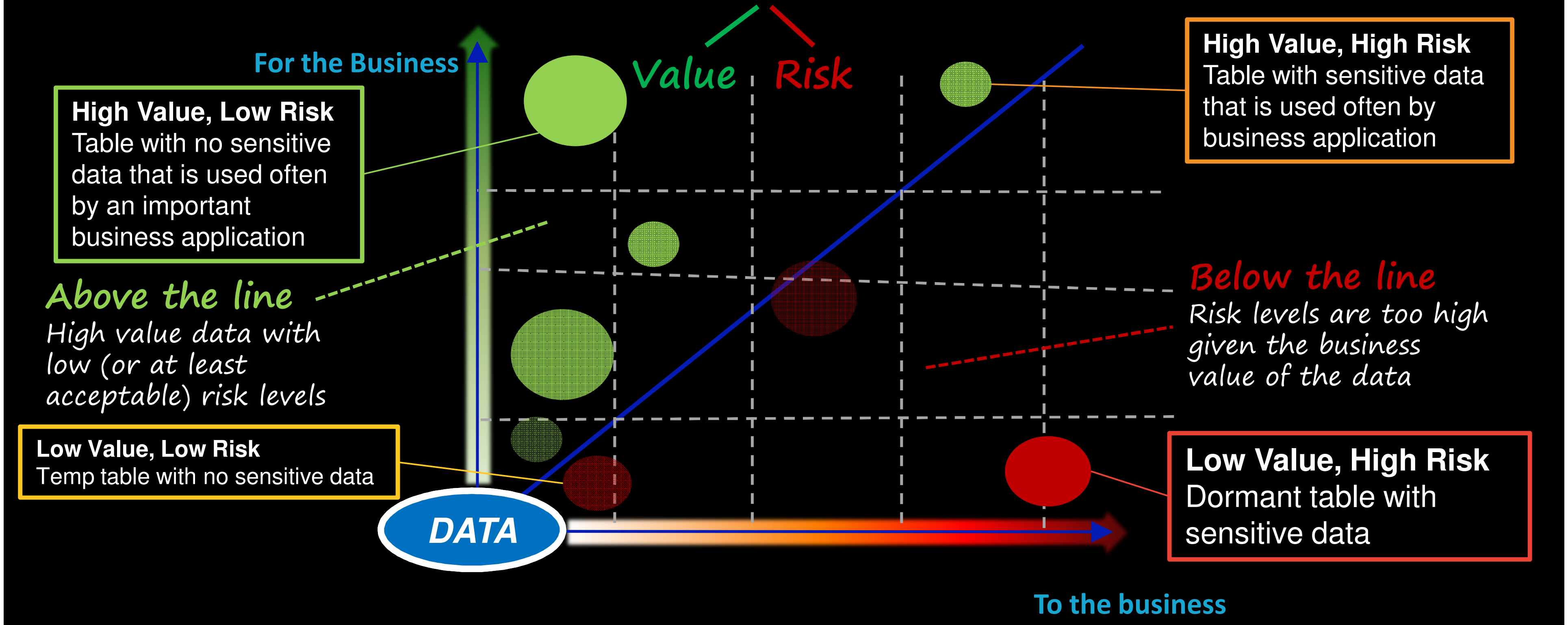
Lifecycle

Production
Test / Dev
Archive
Analysis

IBM Connect 2015

Innovate. Understand. Engage.

Data Security Fundamentals



High Value, Low Risk
Table with no sensitive data that is used often by an important business application

Above the line
High value data with low (or at least acceptable) risk levels

Low Value, Low Risk
Temp table with no sensitive data

High Value, High Risk
Table with sensitive data that is used often by business application

Below the line
Risk levels are too high given the business value of the data

Low Value, High Risk
Dormant table with sensitive data

IBM Connect 2015
Innovate. Understand. Engage.

Key challenges to protecting data in virtualised and cloud environments

Compliance

Limited time, lots of regulation, growing costs of compliance

Audits require monitoring and reporting on database activities

Access

Ability to know who’s accessing your data when, how and why

Complex role based data access requirements

Productivity

Manual approaches lead to higher risk and inefficiency

Centralised security management required for maximum efficiency

Vulnerability

Complex database vulnerabilities

New sources of threats: outsourcing, web applications, stolen credentials

Streamline compliance in virtualised and cloud environments

Receive alerts of suspicious activity

- Audit all database activities
  - User activity
  - Object creation
  - Database configuration
  - Entitlements
- Enforce separation of duties
- Trace users between applications, databases
- Automate compliance with sign-off and escalation procedures
- Integrate with enterprise security systems (SIEM)

Data access is both an external and internal issue

Prevent "power users" from abusing their access to sensitive data (separation of duties)

- DBA and power users

Prevent authorised users from misusing sensitive data

- For example, third-party or off-shore developers

Prevent intrusion and theft of data

- For example, someone walking off with a back-up tape
- Hacker
- Block suspicious network traffic

IBM Connect 2015

Innovate. Understand. Engage.

IBM InfoSphere Guardium provides real-time data activity monitoring for security & compliance

✓ Activity Monitoring

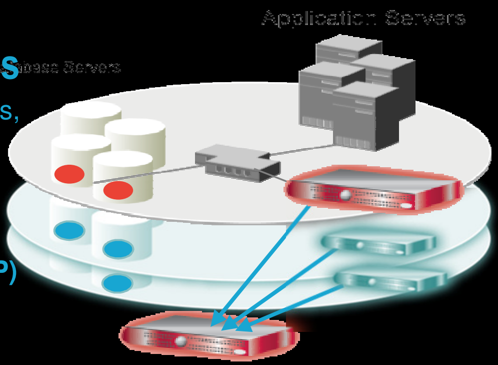
Continuous, policy-based, real-time monitoring of all data traffic activities, including actions by privileged users

✓ Blocking & Masking

Data protection compliance automation

✓ Vulnerability Assessment

Database infrastructure scanning for missing patches, mis-configured privileges and other vulnerabilities



Data Repositories

(databases, warehouses, file shares, Big Data)

Host-based Probes (S-TAP)

Collector Appliance

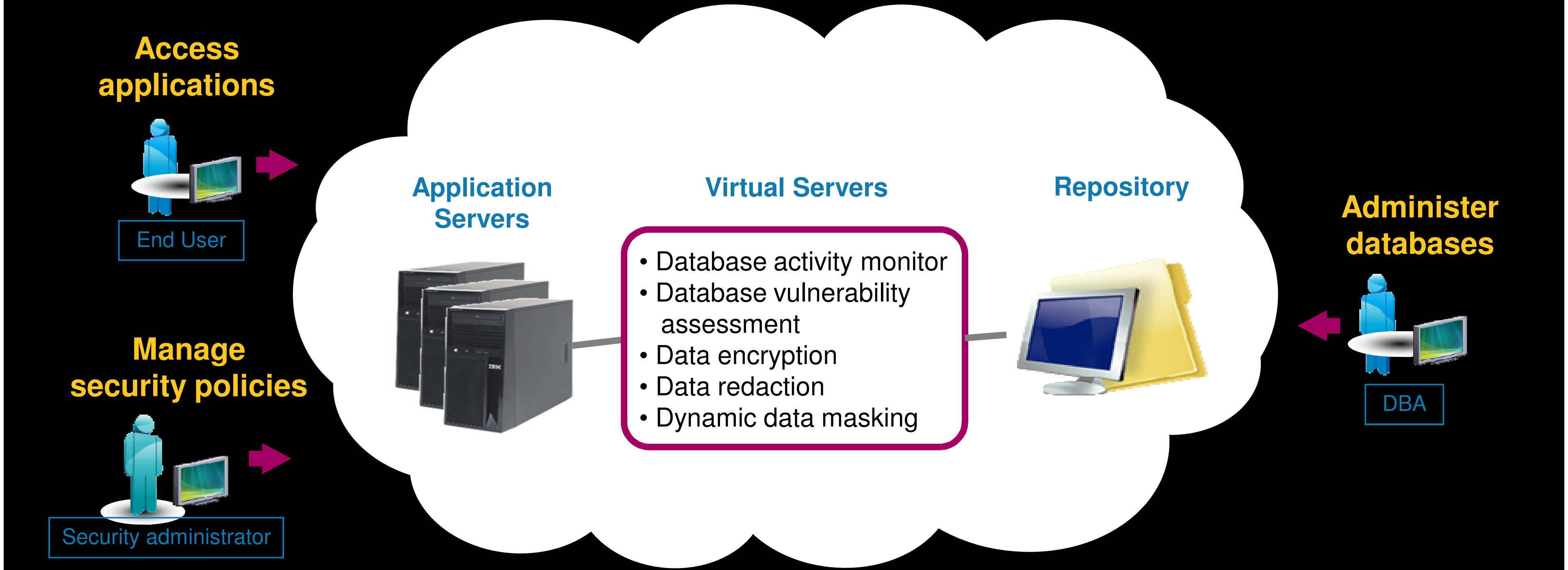
Central Manager Appliance

Key Characteristics

- Single Integrated Appliance
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- SOD enforcement for DBA access
- Auto discover sensitive resources and data
- Detect or block unauthorized & suspicious activity
- Granular, real-time policies
  - *Who, what, when, how*
- 100% visibility including local DBA access
- Minimal performance impact
- Does not rely on resident logs that can easily be erased by attackers, rogue insiders
- No environment changes
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

InfoSphere Guardium database security

Comprehensive data protection for virtual and cloud infrastructures



Access applications

End User

Manage security policies

Security administrator

Application Servers

Virtual Servers

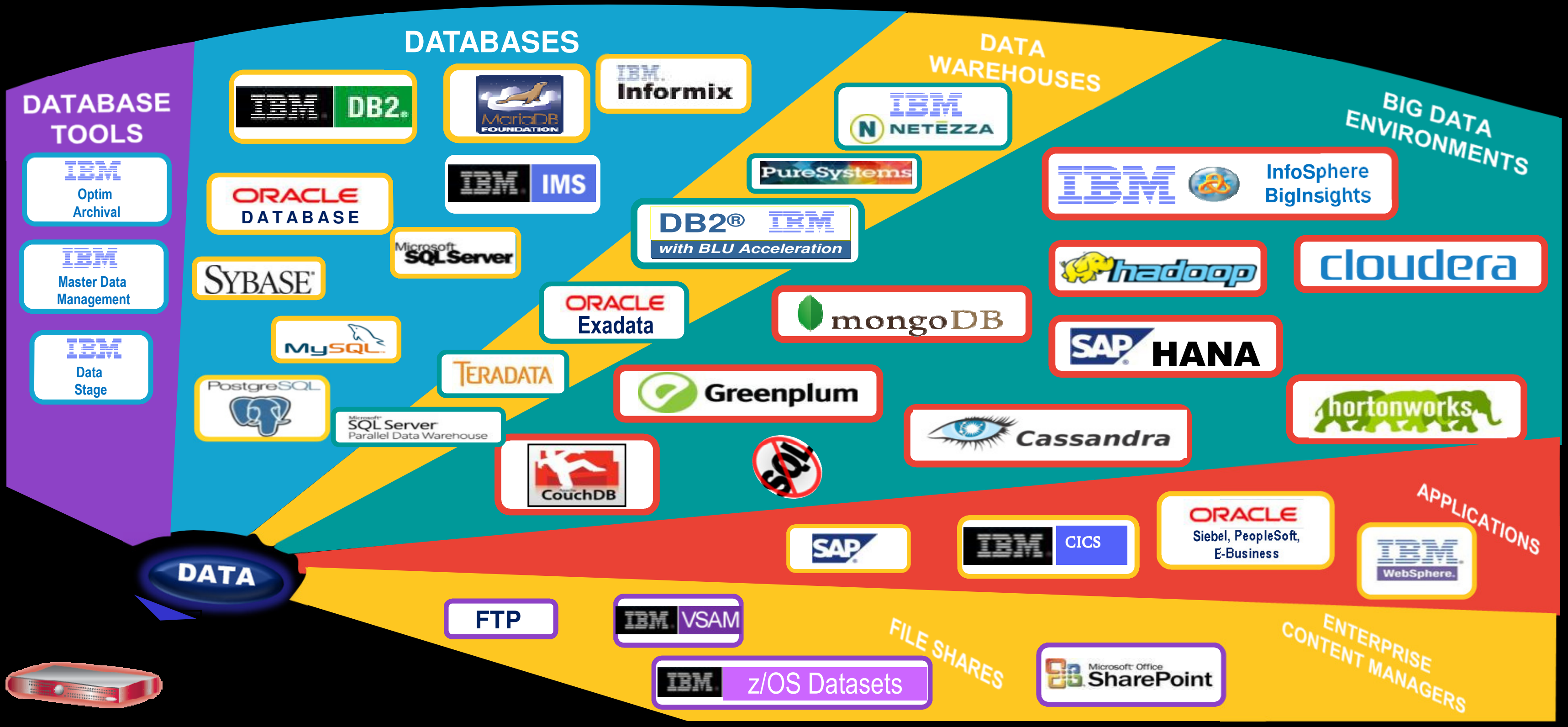
- Database activity monitor
- Database vulnerability assessment
- Data encryption
- Data redaction
- Dynamic data masking

Repository

Administer databases

DBA

How is Guardium Different? Covers all your Data Sources.



DATABASE TOOLS

- IBM Optim Archival
- IBM Master Data Management
- IBM Data Stage

DATABASES

- IBM DB2
- MariaDB Foundation
- IBM Informix
- ORACLE DATABASE
- IBM IMS
- Microsoft SQL Server
- SYBASE
- MySQL
- PostgreSQL
- Microsoft SQL Server Parallel Data Warehouse
- TERADATA
- CouchDB

DATA WAREHOUSES

- IBM NETEZZA
- PureSystems
- DB2® IBM with BLU Acceleration
- ORACLE Exadata

BIG DATA ENVIRONMENTS

- IBM InfoSphere BigInsights
- hadoop
- cloudera
- mongoDB
- SAP HANA
- Greenplum
- hortonworks
- Cassandra
- NoSQL

APPLICATIONS

- SAP
- IBM CICS
- ORACLE Siebel, PeopleSoft, E-Business
- IBM WebSphere

DATA

FILE SHARES

- FTP
- IBM VSAM
- IBM z/OS Datasets

ENTERPRISE CONTENT MANAGERS

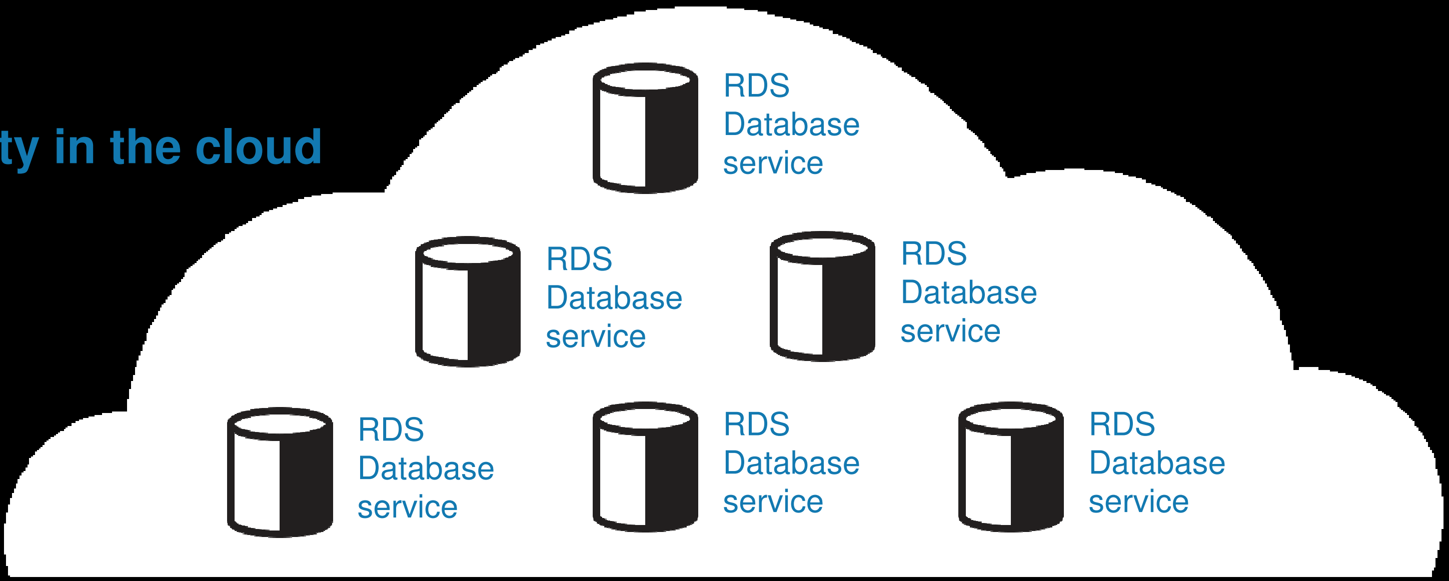
- Microsoft Office SharePoint

IBM Connect 2015

Innovate. Understand. Engage.

Security Challenges For Databases In The Cloud

Security in the cloud



RDS Database service

RDS Database service

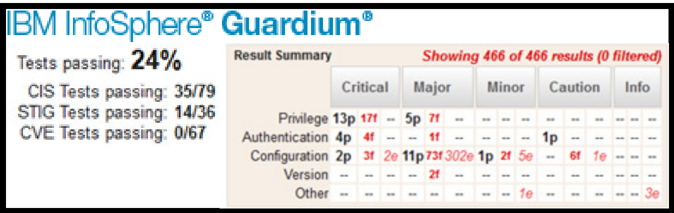
RDS Database service

RDS Database service

RDS Database service

RDS Database service

- How many databases do I have?
- Is the database secure?



IBM InfoSphere® Guardium®

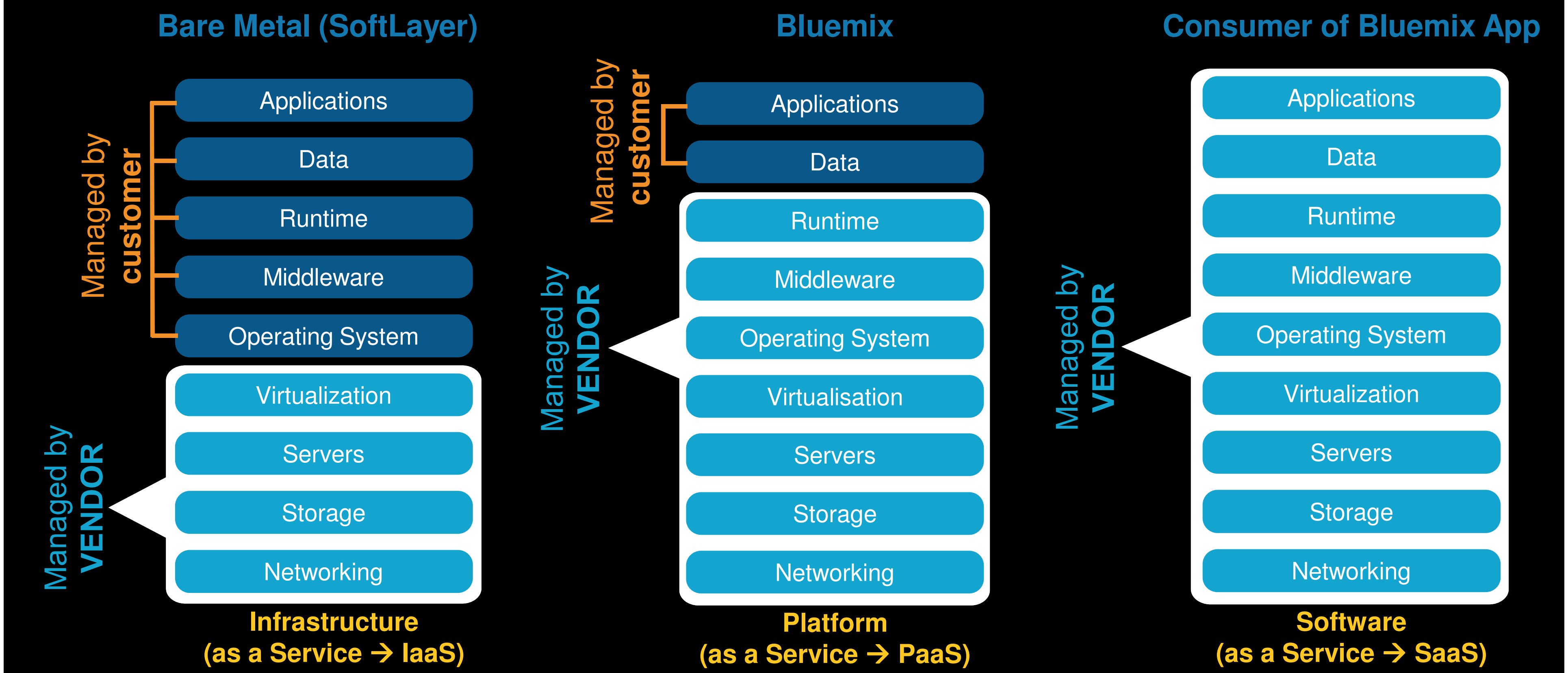
Tests passing: **24%**

CIS Tests passing: 35/79
STIG Tests passing: 14/36
CVE Tests passing: 0/67

Result Summary *Showing 466 of 466 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	13p	17f	--	5p	7f	--	--	--	--	--	--	--	--	--	--
Authentication	4p	4f	--	--	1f	--	--	--	--	1p	--	--	--	--	--
Configuration	2p	3f	2e	11p	73f	302e	1p	2f	5e	--	6f	1e	--	--	--
Version	--	--	--	--	2f	--	--	--	--	--	--	--	--	--	--
Other	--	--	--	--	--	--	--	--	1e	--	--	--	--	--	3e

Cloud terminology



Bare Metal (SoftLayer)

Managed by **customer**
- Applications
- Data
- Runtime
- Middleware
- Operating System

Managed by **VENDOR**
- Virtualization
- Servers
- Storage
- Networking

Infrastructure
(as a Service → IaaS)

Bluemix

Managed by **customer**
- Applications
- Data

Managed by **VENDOR**
- Runtime
- Middleware
- Operating System
- Virtualisation
- Servers
- Storage
- Networking

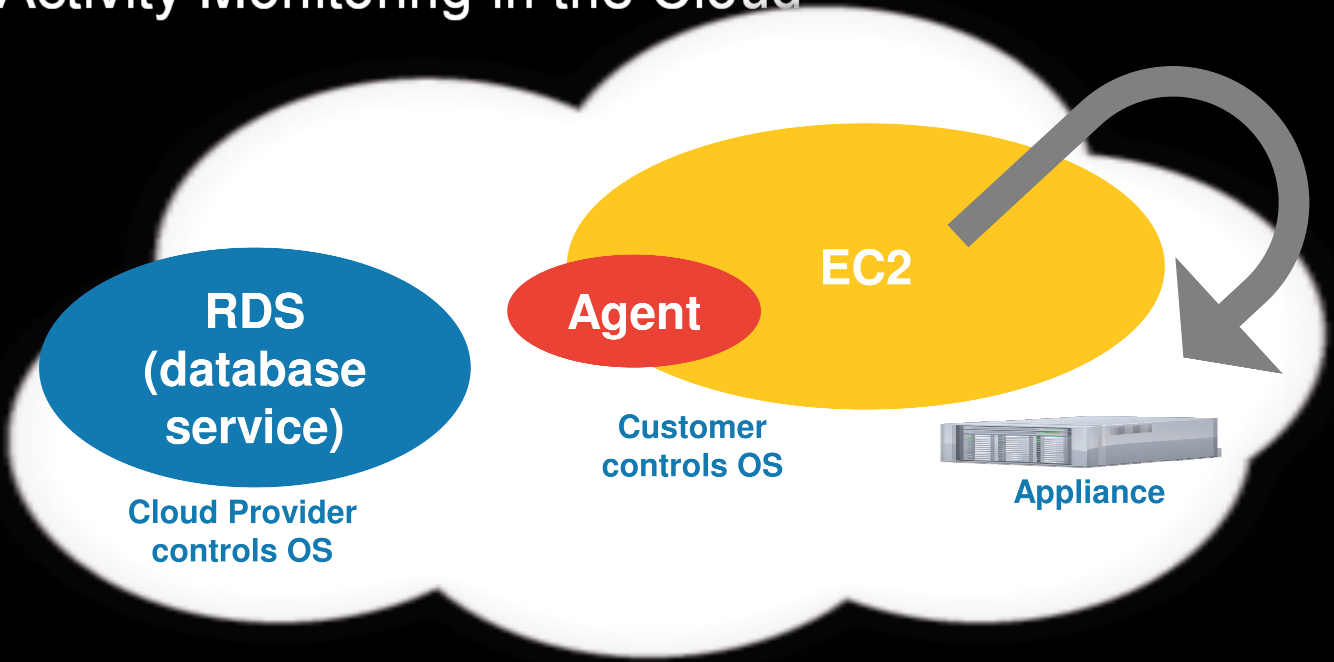
Platform
(as a Service → PaaS)

Consumer of Bluemix App

Managed by **VENDOR**
- Applications
- Data
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

Software
(as a Service → SaaS)

Security Challenges for Database Activity Monitoring in the Cloud



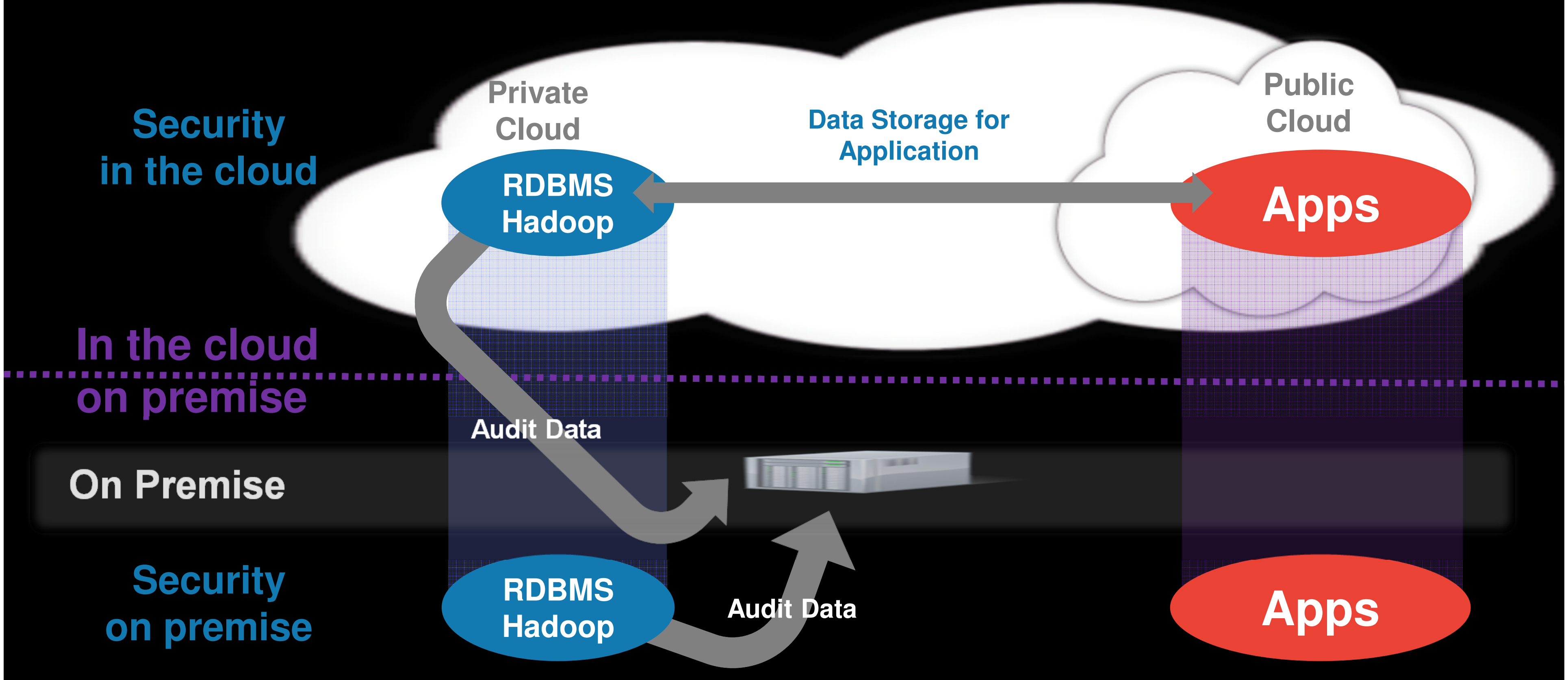
Security in the cloud

- How do you monitor “privileged users” in the cloud?
- Where do you put the appliance in the cloud? Or on premise?

IBM Connect 2015

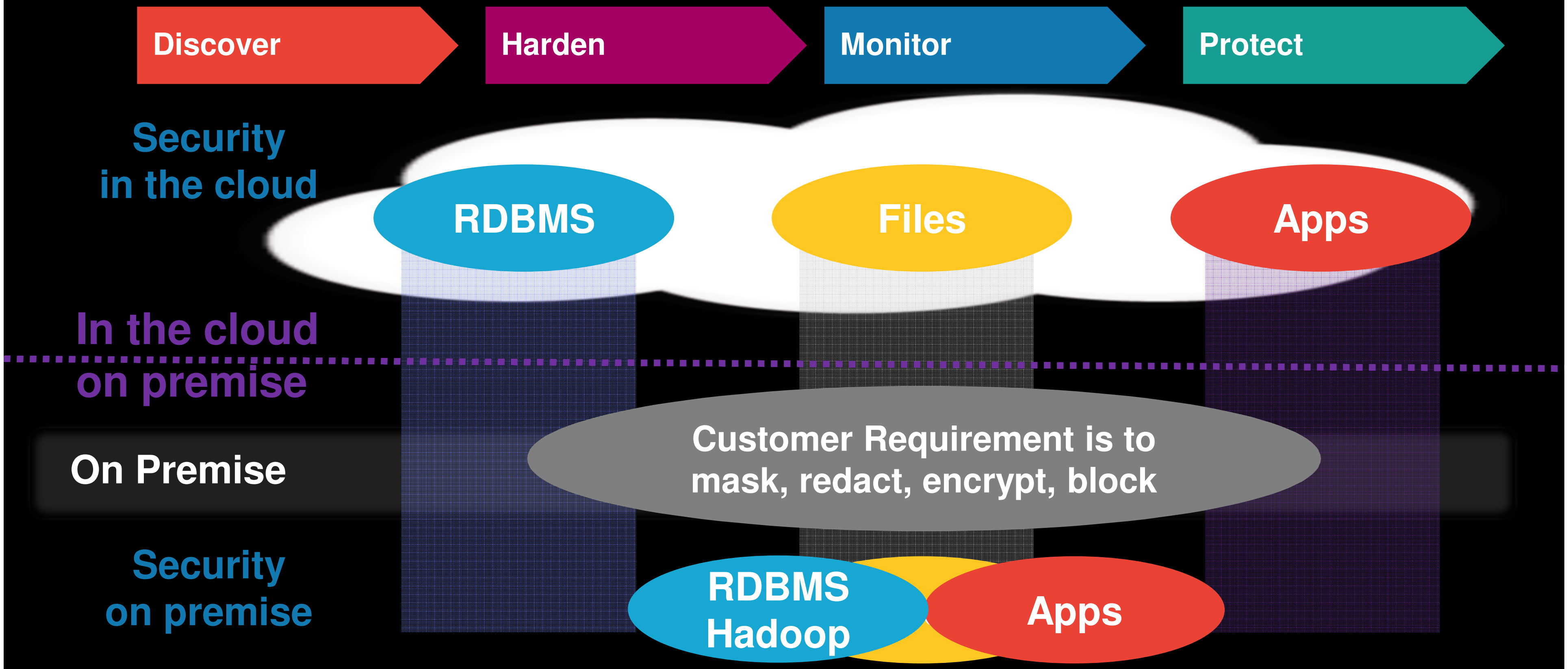
Innovate. Understand. Engage.

Security Challenges For Databases In The Cloud



IBM Connect 2015

Innovate. Understand. Engage.



Discover

Harden

Monitor

Protect

Security
in the cloud

RDBMS

Files

Apps

In the cloud

on premise

On Premise

Customer Requirement is to
mask, redact, encrypt, block

Security
on premise

RDBMS
Hadoop

Apps

Can data security policies be easily, consistently and automatically enforced?

Big Data

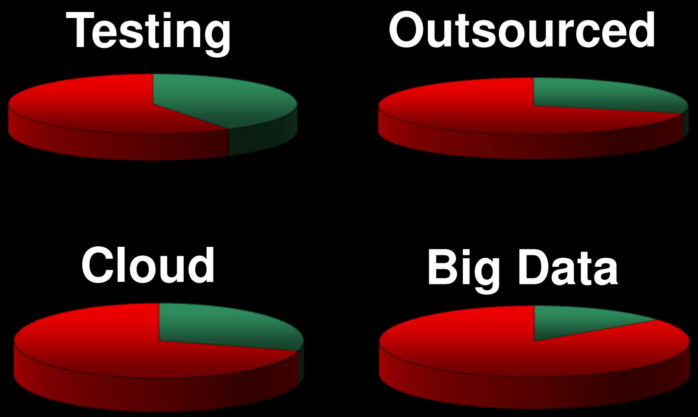
Cloud

Mobile

Can data security policies be easily, consistently and automatically enforced?

2/3rds of organisations feel they can enforce policies in production environments

However there is a struggle to manage policies in newer platforms



IBM Connect 2015
Innovate. Understand. Engage.

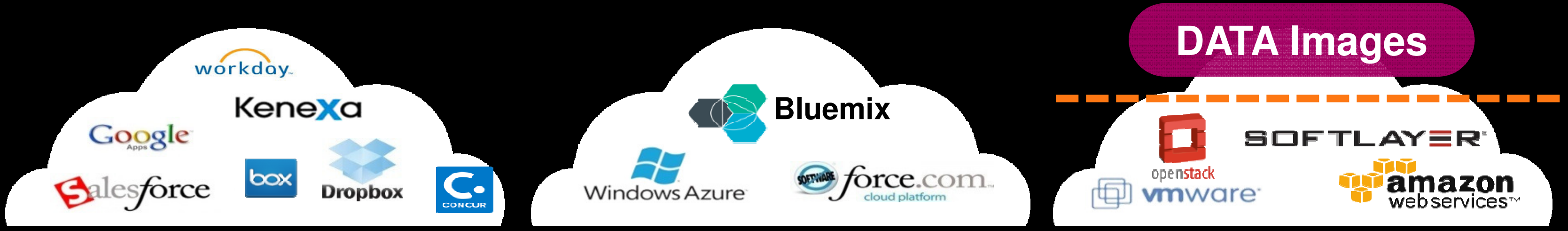
Cloud Deployment Models

IBM

SaaS
Business Applications

PaaS
Data Platforms

IaaS
Infrastructure and workloads



Make sure you cover the basics when working in the cloud.
These 4 elements are key to good security…

Discover → **Harden** → **Monitor** → **Protect**

Who owns this responsibility?

Data Security is a board room discussion

CEO

Loss of market share & reputation

Legal exposure

CFO/COO

Audit failure

Fines & criminal charges

Financial loss

CIO

Loss of data confidentiality, integrity &/or availability

CHRO

Violation of employee privacy

CMO

Loss of customer trust

Loss of brand reputation

Increasingly, companies are appointing CROs and CISOs with a direct line to the Audit Committee

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

Chosen by leading organisations worldwide to secure their most critical data

8 of the top 10 global banks
Protecting access to Billions of dollars in financial assets

2 of the top 3 global retailers
Safeguarding the integrity of 2.5 billion credit card or personal information transactions per year

7 of the top 8 global insurers
Protecting more than 100,000 databases with personal and private information

Protecting over 7 million credit card transactions per year

4 of the top 5 global managed healthcare providers
Protecting access to 136 million patients private information

Top government agencies
Safeguarding the integrity of the world's government information and defense

9 of the top 10 telcos worldwide
Maintaining the privacy of over 1,100,000,000 subscribers

The Compliance Mandate – What must you monitor?

Audit Requirements	PCI DSS	COBIT (SOX)	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)	✓		✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)		✓	✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

DDL = Data Definition Language (aka schema changes)
DML = Data Manipulation Language (data value changes)
DCL = Data Control Language

How Guardium Addresses APRA PPG 234

APRA PPG 234 Guideline	InfoSphere Guardium Solution Description and Notes
20 - For the purposes of managing IT risk, a regulated institution would typically classify IT assets based on business criticality and sensitivity. Institutions may seek to leverage the existing business impact analysis process to achieve this. The institution's IT asset classification method and granularity would normally be determined by the requirements of the business.	Guardium database discovery and data classification discover and classify sensitive data. The discovery process can be configured to probe specified network segments on a scheduled or on-demand. Once instances of interest are identified, the content is examined to identify and classify sensitive data.
26 - APRA envisages that a regulated institution would adopt a set of high-level IT security principles in order to establish a sound foundation for the IT security risk management framework. Common IT security principles include: **(a)** defence-in-depth and diversity of controls, where multiple layers and types of controls are used to address risks in different ways. Therefore, should one control layer be compromised, other control(s) limit the impact on a regulated institution;	Guardium provides defense of database assets. IBM helps thousands of clients address the challenges of securing their people, data, applications and infrastructure. The IBM Security Framework provides a more integrated, intelligent approach to security. The application of security intelligence and analytics along with external threat intelligence, helps organizations to detect, analyze and remediate threats that point products will always miss.
(b) denial of all features, permissions, functions and protocols unless required to conduct business operations. This reduces the number of attack approaches that may be used to compromise IT assets;	Guardium Data-Level Access Control simplifies enterprise security with a single set of granular policies for enforcing separation of duties spanning multiple DBMS platforms—without disrupting application access or changing database configurations. It's the only cross-DBMS technology that blocks privileged users—such as DBAs, developers, outsourced personnel and other superusers—from viewing or changing sensitive data.
(c) timely detection and reporting of IT security breaches. This minimises the time in which a compromise of an IT asset can impact on a regulated institution;	Guardium provides rapid, policy-based detection of anomalous activities that violate corporate policies; real-time responses, such as alerts; auditable workflow to ensure appropriate resolution of exceptions; and automated reporting capabilities, which simplify validation of compliance for mandates, such as SOX, PCI DSS and data privacy regulations.
(d) appropriately controlled error handling. Errors should not allow unauthorised access to IT assets or other IT security compromises;	Guardium discovers vulnerabilities by observing all database transactions in real time, such as an excessive number of database errors (indicating a possible SQL Injection attack), usage of shared administration accounts and service IDs or usage of default vendor accounts.
(e) distrust of unfamiliar IT assets, including internal and external IT assets. Such assets have an unknown and possibly reduced level of IT security control;	Guardium provides granular, real-time policies to prevent unauthorized or suspicious actions by privileged database accounts and attacks from rogue users or outsiders.
(f) segregation of duties, enforced through appropriate allocation of roles and responsibilities. This reduces the potential for the actions of one person to compromise IT assets;	Guardium Data-Level Access Control can be managed by IT security, compliance or risk teams, because it uses simple English language policies that can be customized through drop-down menus, without requiring knowledge of database commands and structures. In addition, Guardium Data-Level Access Control uses a hardened, Linux based network appliance to manage access policies, preventing privileged users from disabling or modifying policies and further strengthening separation of duties.
(g) a control environment designed to enforce compliance rather than assume staff are fully familiar with IT security policies and procedures.	Guardium offers policy enforcement and fine-grained auditing in a single solution, further reducing cost and complexity.

How Guardium Addresses APRA PPG 234 (Cont.)

APRA PPG 234 Guideline	InfoSphere Guardium Solution Description and Notes
27 - APRA envisages that a regulated institution would adopt a set of high-level IT security principles in order to establish a sound foundation for the IT security risk management framework. Common IT security principles include: **(a)** defence-in-depth and diversity of controls, where multiple layers and types of controls are used to address risks in different ways. Therefore, should one control layer be compromised, other control(s) limit the impact on a regulated institution;	Guardium Policy-based actions can include real-time security alerts (SMTP, SNMP, Syslog); software blocking; full logging; user quarantines; and custom actions such as shutting down VPN ports and coordinating with perimeter IDS/IPS systems. Additionally, Guardium sends alerts and audit reports to IBM Security QRadar and other SIEM solutions, enabling a more insightful cross-IT security intelligence analysis based on in-depth data activity findings.
(e) monitoring and incident management to address the identification and classification of incidents, reporting and escalation guidelines, preservation of evidence and the investigation process;	Guardium provides a business user interface and workflow automation for resolving security incidents, along with a dashboard for tracking key metrics such as the number of open incidents, severity levels and the length of time incidents have been open.
37 - A key requirement for ensuring IT security is an effective process for providing access to IT assets. A regulated institution would normally only authorise access to IT assets where a valid business need exists and only for as long as access is required.	Guardium monitors enterprise data sources in real time including databases, warehouses, file shares and Hadoop based systems to enforce policies and protect sensitive data. It continuously monitors all data access operations in real time, using linguistic analysis to detect unauthorized actions based on detailed contextual information—the "who, what, where, when and how" of each data access. This contextual approach minimizes false positives and negatives while providing a significant level of control, unlike traditional approaches that only look for predefined patterns or signatures only on database traffic or audit logs.
38 - Factors to consider when authorising access to users and IT assets include: business role; physical location; remote access; time; patch and antimalware status; software; operating system; device; and method of connectivity.	The Guardium platform supports granular, deterministic policies to positively identify violations (rather than relying on heuristics). Rules are based on specific session properties, such as client IP address, MAC address, source application, DB user, OS user, Application user, time-of-day, SQL command and table names, which are typically defined by way of pre-defined groups to simplify ongoing management. A broad range of policy actions can be invoked for policy violations, such as real-time alerts (SMTP, SNMP, Syslog, CEF), user quarantine and terminate connection.
39 - The provision of access involves the following process stages: **(a)** identification and authentication: determination of who or what is requesting access and confirmation of the purported identity;	Guardium empowers IT security organizations to rapidly identify fraud and other actions that violate corporate policies, such as unauthorized changes to sensitive data. In addition, Guardium Entitlement Reports provide a simple means of aggregating and understanding database entitlements throughout the organization.
(b) - authorisation: assessment of whether access is allowed to an IT asset by the requestor based on the needs of the business and the level of IT security (trust) required. **Note**: Identification, authentication and access authorisation processes are applicable to both users and IT assets.	Guardium Data Activity Monitor prevents unauthorized or suspicious activities by privileged insiders and potential hackers, and automates governance controls in heterogeneous enterprises.
40 - A regulated institution would normally take appropriate measures to identify and authenticate users or IT assets. The required strength of authentication would normally be commensurate with risk.	Guardium real-time Data Activity Monitoring with application end-user translation creates an audit trail of all database activities including execution of all SQL commands on all database objects; audits all logins/logouts, security exceptions such as login failures and SQL errors and extrusion detection (identifying sensitive data returned by queries); provides 100 percent visibility and granularity into all database, file share, data warehouse, Hadoop and NoSQL transactions across all platforms and protocols - with a secure, tamper-proof audit trail that supports separation of duties.

How Guardium Addresses APRA PPG 234 (Cont.)

APRA PPG 234 Guideline	InfoSphere Guardium Solution Description and Notes
44 - A regulated institution would typically deploy the following controls to limit access to IT assets, based on a risk assessment: **(c)** prohibiting the sharing of accounts and passwords (including generic accounts);	Guardium Data Activity Monitor's "one user, one IP"" report can highlight occurrences of shared or suspicious user accounts so that appropriate actions can be taken.
45 - For accountability purposes, a regulated institution would normally ensure that users and IT assets are uniquely identified and their actions are auditable.	Guardium real-time Data Activity Monitoring with application end-user translation creates an audit trail of all database activities including execution of all SQL commands on all database objects; audits all logins/logouts, security exceptions such as login failures and SQL errors and extrusion detection (identifying sensitive data returned by queries); provides 100 percent visibility and granularity into all database, file share, data warehouse, Hadoop and NoSQL transactions across all platforms and protocols - with a secure, tamper-proof audit trail that supports separation of duties.
46 - 'Data leakage' is defined as the unauthorised removal, copying, distribution, capturing or other types of disclosure of sensitive data/information. Access to data removal methods would normally be subject to risk assessment and only granted where a valid business need exists.	Guardium provides automated, real-time controls (blocking or quarantining users) that prevent privileged users from performing unauthorized actions, such as: executing queries on sensitive tables, changing sensitive data values, adding or deleting critical tables (schema changes) outside change windows and creating new user accounts and modifying privileges.
47 - Controls, commensurate with the sensitivity and criticality of the data/information involved, would normally be implemented where sensitive data/ information is at risk of leakage. Examples of such data leakage methods include the use of: portable computing devices (e.g. laptops, PDAs, mobile phones); portable storage devices (e.g. USB flash drives, portable hard drives, writable disks); electronic transfer mechanisms (e.g. email, instant messaging); and hard copy.	Guardium provides automated, real-time controls (blocking or quarantining users) that prevent privileged users from performing unauthorized actions, such as: executing queries on sensitive tables, changing sensitive data values, adding or deleting critical tables (schema changes) outside change windows and creating new user accounts and modifying privileges.
48 - Common controls for data/information removal methods would normally be commensurate with risk. Users with a greater level of access to sensitive data/information would be subject to an increased level of scrutiny. Such controls could include: **(a)** authorisation, registration and regular review of users and associated transfer mechanisms and devices (including printers);	Guardium provides automated, real-time controls (blocking or quarantining users) that prevent privileged users from performing unauthorized actions, such as: executing queries on sensitive tables, changing sensitive data values, adding or deleting critical tables (schema changes) outside change windows and creating new user accounts and modifying privileges.
(c) appropriate segmentation of data/information based on sensitivity and access needs;	Guardium provides automated, real-time controls (blocking or quarantining users) that prevent privileged users from performing unauthorized actions, such as: executing queries on sensitive tables, changing sensitive data values, adding or deleting critical tables (schema changes) outside change windows and creating new user accounts and modifying privileges.
(d) appropriate blocking, filtering and monitoring of electronic transfer mechanisms and printing;	Guardium provides automated, real-time controls (blocking or quarantining users) that prevent privileged users from performing unauthorized actions, such as: executing queries on sensitive tables, changing sensitive data values, adding or deleting critical tables (schema changes) outside change windows and creating new user accounts and modifying privileges.

How Guardium Addresses APRA PPG 234 (Cont.)

APRA PPG 234 Guideline	InfoSphere Guardium Solution Description and Notes
49 - In APRA's view, wholesale access to sensitive data/information would be highly restricted to reduce the risk exposure to significant data leakage events. Industry experience of actual instances in this area includes the leakage of debit/credit card details and the sale/trade or exploitation of customer identity information.	Guardium provides automated, real-time controls (blocking or quarantining users) that prevent privileged users from performing unauthorized actions, such as: executing queries on sensitive tables, changing sensitive data values, adding or deleting critical tables (schema changes) outside change windows and creating new user accounts and modifying privileges.
50 - In APRA's view, cryptographic techniques would normally be used to control access to sensitive data/information, both in storage and in transit. The strength of the cryptographic techniques deployed would be commensurate with the sensitivity and criticality of the data/information as well as other supplementary or compensating controls. (Refer to Attachment F for further guidance.)	All connections to the Guardium appliance are encrypted, either by TLS/SSL or SSH. Under no circumstances is data available for sniffing, neither as part of a normal user session nor as part of the dialog between the Guardium appliance and its remote agents. Any data exported from the appliance (archives, backup or aggregation) is encrypted using Triple-DES encryption, with three 56-bit keys. These archives can be decrypted only within the Guardium solution and only at the same customer's environment. The connection and communication between a collector and aggregator is encrypted and secured via SCP.
51 - In order to minimise the risk of compromise, an end-to-end approach would normally be adopted, where encryption is applied from the point of entry to final destination.	All connections to the Guardium appliance are encrypted, either by TLS/SSL or SSH. Under no circumstances is data available for sniffing, neither as part of a normal user session nor as part of the dialog between the Guardium appliance and its remote agents.
54 - Acquisition and implementation controls would typically be in place to ensure that the IT security of the technology environment is not compromised by the introduction of new IT assets. Ongoing support and maintenance controls would typically be in place to ensure that IT assets continue to meet business objectives. Examples of controls include: **(a)** change management controls to ensure that the business objectives continue to be met following change (refer to Attachment A for further guidance);	Guardium can simplify and automate the integration of data from external databases or text files. Its powerful capabilities enable a wide variety of functionality, ranging from new applications like automated change-control reconciliation to process and policy improvements that eliminate costly manual efforts.
58 - A regulated institution typically deploys specific technology solutions in key locations to control or monitor the security of various IT assets. Examples include: firewalls; network access control; intrusion detection/prevention devices; anti-malware; encryption and monitoring/log analysis tools. The degree of reliance that is placed on these technology solutions and their criticality and sensitivity necessitate a heightened set of life-cycle controls, including but not limited to: **(a)** guidelines outlining when IT security-specific technology solutions should be used;	Guardium monitors enterprise data sources in real time including databases, warehouses, file shares and Hadoop based systems to enforce policies and protect sensitive data. It continuously monitors all data access operations in real time, using linguistic analysis to detect unauthorized actions based on detailed contextual information—the "who, what, where, when and how" of each data access. This contextual approach minimizes false positives and negatives while providing a significant level of control, unlike traditional approaches that only look for predefined patterns or signatures only on database traffic or audit logs.
62 - New technologies potentially introduce a set of additional risk exposures (both known and unknown). A regulated institution would normally apply appropriate caution when considering the introduction of new technologies.	Guardium Data Privacy for Hadoop de-identifies and monitors sensitive data which resides within big data environments. The solution provides a complete set of Hadoop capabilities to mask or redact data, monitor and audit data activity and maintain common data definitions. InfoSphere Data Privacy for Hadoop protects data and supports compliance initiatives across all variety of Hadoop environments.

How Guardium Addresses APRA PPG 234 (Cont.)

APRA PPG 234 Guideline	InfoSphere Guardium Solution Description and Notes
65 - A regulated institution would normally have monitoring processes in place to identify events and unusual patterns of behaviour that could impact on the security of IT assets. The strength of the monitoring controls would typically be commensurate with the criticality and sensitivity of an IT asset. APRA envisages that alerts would be investigated in a timely manner, with an appropriate response determined.	Guardium monitors enterprise data sources in real time including databases, warehouses, file shares and Hadoop based systems to enforce policies and protect sensitive data. It continuously monitors all data access operations in real time, using linguistic analysis to detect unauthorized actions based on detailed contextual information—the "who, what, where, when and how" of each data access. This contextual approach minimizes false positives and negatives while providing a significant level of control, unlike traditional approaches that only look for predefined patterns or signatures only on database traffic or audit logs.
66 - Common monitoring processes include: **(a)** activity logging including exceptions to approved activity (e.g. device, server and network activity; security sensor alerts);	Guardium provides rapid, policy-based detection of anomalous activities that violate corporate policies; real-time responses, such as alerts; auditable workflow to ensure appropriate resolution of exceptions; and automated reporting capabilities, which simplify validation of compliance for mandates, such as SOX, PCI DSS and data privacy regulations.
(b) environment and customer profiling;	Guardium provides rapid, policy-based detection of anomalous activities that violate corporate policies; real-time responses, such as alerts; auditable workflow to ensure appropriate resolution of exceptions; and automated reporting capabilities, which simplify validation of compliance for mandates, such as SOX, PCI DSS and data privacy regulations.
(c) checks to determine if IT security controls are operating as expected and are being complied with; and	Guardium provides rapid, policy-based detection of anomalous activities that violate corporate policies; real-time responses, such as alerts; auditable workflow to ensure appropriate resolution of exceptions; and automated reporting capabilities, which simplify validation of compliance for mandates, such as SOX, PCI DSS and data privacy regulations.
(d) monitoring staff or third-party access to sensitive data/information to ensure it is for a valid business reason.	Guardium Policy-based actions can include real-time security alerts (SMTP, SNMP, Syslog); software blocking; full logging; user quarantines; and custom actions such as shutting down VPN ports and coordinating with perimeter IDS/IPS systems. Additionally, Guardium sends alerts and audit reports to IBM Security QRadar and other SIEM solutions, enabling a more insightful cross-IT security intelligence analysis based on in-depth data activity findings.
67 - APRA envisages that a regulated institution would establish a clear allocation of responsibility for regular monitoring, with appropriate processes and tools in place to manage the volume of monitoring required, thereby reducing the risk of an incident going undetected.	Guardium real-time Data Activity Monitoring with application end-user translation creates an audit trail of all database activities including execution of all SQL commands on all database objects; audits all logins/logouts, security exceptions such as login failures and SQL errors and extrusion detection (identifying sensitive data returned by queries); provides 100 percent visibility and granularity into all database, file share, data warehouse, Hadoop and NoSQL transactions across all platforms and protocols - with a secure, tamper-proof audit trail that supports separation of duties.
68 - Highly sensitive and/or critical IT assets would typically have logging enabled to record events and monitored at a level commensurate with the level of risk.	Guardium Data-Level Access Control simplifies enterprise security with a single set of granular policies for enforcing separation of duties spanning multiple DBMS platforms—without disrupting application access or changing database configurations. It's the only cross-DBMS technology that blocks privileged users—such as DBAs, developers, outsourced personnel and other superusers—from viewing or changing sensitive data.
69 - Users with elevated access entitlements (e.g. system administrators) would normally be subject to a greater level of monitoring in light of the heightened risks involved.	Guardium provides granular, real-time policies to prevent unauthorized or suspicious actions by privileged database accounts and attacks from rogue users or outsiders.

How Guardium Addresses APRA PPG 234 (Cont.)

APRA PPG 234 Guideline	InfoSphere Guardium Solution Description and Notes
74 - APRA envisages that a regulated institution would ensure audit trails exist for IT assets that: satisfy the institution's business requirements (including regulatory and legal); facilitate independent audit; assist in dispute resolution (including non-repudiation); and assist in the provision of forensic evidence if required. This could include, as applicable: **(a)** the opening, modification or closing of customer accounts;	Guardium creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics; monitors all data transactions to create a continuous, fine-grained audit trail that identifies the "who, what, when, where and how" of each transaction.
(b) any transaction with financial consequences;	Guardium creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics; monitors all data transactions to create a continuous, fine-grained audit trail that identifies the "who, what, when, where and how" of each transaction.
(c) authorisations granted to customers to exceed a pre-approved limit;	Guardium creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics; monitors all data transactions to create a continuous, fine-grained audit trail that identifies the "who, what, when, where and how" of each transaction.
(d) accessing or copying of sensitive data/information; and	Guardium creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics; monitors all data transactions to create a continuous, fine-grained audit trail that identifies the "who, what, when, where and how" of each transaction.
(e) granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets.	Guardium creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics; monitors all data transactions to create a continuous, fine-grained audit trail that identifies the "who, what, when, where and how" of each transaction.
75 - Audit trails would typically be secured to ensure the integrity of the information captured, including the preservation of evidence. Retention of audit trails would normally be in line with business requirements (including regulatory and legal).	Guardium creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics; monitors all data transactions to create a continuous, fine-grained audit trail that identifies the "who, what, when, where and how" of each transaction.
76 - A regulated institution would typically develop a formalised IT security reporting framework that provides operational information and oversight across the various dimensions of the IT security risk management framework. The framework would incorporate clearly defined reporting and escalation thresholds and reflect the various audiences responsible for either acting on or reviewing the reports. Reporting mechanisms would typically ensure appropriate consideration of both risk and control dimensions.	Guardium Built-in compliance workflow (review, escalations, sign-offs) — Supports SOX, PCI, HIPAA and more with pre-defined reports for top regulations. An easy-to-use graphical user interface allows a wide variety of processes to be created to match the unique needs of the tasks and individuals involved. Many different audit tasks are supported, including reviewing the results of automatically generated vulnerability assessments, asset discovery and data classification.
77 - In APRA's view, there would normally be sufficient management reporting to enable effective oversight of the performance of the IT security management function in meeting its stated objectives. Reporting may include: risk profile(s); exposure analysis; progress against strategy; incident analysis; system capacity and performance analysis; recovery status; infrastructure and software analysis; project assessment and analysis; audit findings and ageing reports; and fraud analysis.	Guardium Built-in compliance workflow (review, escalations, sign-offs) — Supports SOX, PCI, HIPAA and more with pre-defined reports for top regulations. An easy-to-use graphical user interface allows a wide variety of processes to be created to match the unique needs of the tasks and individuals involved. Many different audit tasks are supported, including reviewing the results of automatically generated vulnerability assessments, asset discovery and data classification.

Vulnerability Assessment Controls for APRA PPG 234

APRA PPG 234 Guideline	InfoSphere Guardium Solution Description and Notes
19 - The IT security risk management process is a continuous and dynamic process that ensures emerging IT vulnerabilities/threats are identified, assessed and appropriately managed in a timely manner.	Guardium Vulnerability Assessment evaluates the database and operating system configurations and recommends concrete actions to strengthen security and eliminate the enormous risk created by insecure database configurations, missing databases patches, weak passwords and other vulnerabilities. Database protection knowledgebase subscription leverages automatic database vulnerability remediation updates with the latest vulnerability standards.
21 - A regulated institution could find it useful to regularly assess the completeness of its IT security risk management framework by comparison to peers and established control frameworks and standards.	Guardium Vulnerability Assessment hardens databases based on hundreds of comprehensive, preconfigured test. Built-in best practices such as those developed by the Center for Internet Security (CIS) and the Database Security Technical Implementation Guide (STIG) are included, as is support for SCAP. These tests are updated on a monthly or quarterly basis to ensure comparison to the most current industry best practices.
44 - A regulated institution would typically deploy the following controls to limit access to IT assets, based on a risk assessment: **(d)** changing of default passwords and user names;	Guardium Vulnerability Assessment scans database infrastructure for vulnerabilities to identify security risks such as missing patches, weak passwords, misconfigured privileges, and default vendor accounts.
(e) removal of access rights whenever there is a change in role or responsibility, and on cessation of employment. Access rights can then be granted in line with the new role or responsibility, without risk of unnecessary access remaining;	Guardium Vulnerability Assessment provides a simple means of aggregating and understanding entitlement information from your entire database infrastructure. This allows Entitlement information to be collected on a frequent, systematic basis without the use of scarce technical resources, providing timely, accurate information that will enhance your security posture and satisfy the needs of auditors, while reducing operational costs.
(f) processes to notify appropriate personnel of user additions, deletions and role changes;	Guardium Vulnerability Assessment scans database infrastructure for vulnerabilities to identify security risks such as missing patches, weak passwords, misconfigured privileges, and default vendor accounts.
(g) audit logging and monitoring of access to IT assets by all users;	Guardium Vulnerability Assessment provides a variety of predefined reports from different views of entitlement data, enabling organizations to quickly and easily identify security risks, such as inappropriately exposed objects, users with excessive rights and unauthorized administrative actions.
(h) regular reviews of user access by IT asset owners to ensure appropriate access is maintained;	Guardium Vulnerability Assessment scans database infrastructure for vulnerabilities to identify security risks such as missing patches, weak passwords, misconfigured privileges, and default vendor accounts.
54 - Acquisition and implementation controls would typically be in place to ensure that the IT security of the technology environment is not compromised by the introduction of new IT assets. Ongoing support and maintenance controls would typically be in place to ensure that IT assets continue to meet business objectives. Examples of controls include: **(b)** configuration management controls to ensure that the configuration minimises vulnerabilities and is defined, assessed, registered and maintained;	Guardium Vulnerability Assessment evaluates the database and operating system configurations and recommends concrete actions to strengthen security and eliminate the enormous risk created by insecure database configurations, missing databases patches, weak passwords and other vulnerabilities. Database protection knowledgebase subscription leverages automatic database vulnerability remediation updates with the latest vulnerability standards.
(d) patch management controls to manage the assessment and application of patches to software that address known vulnerabilities in a timely manner;	Guardium Vulnerability Assessment evaluates the database and operating system configurations and recommends concrete actions to strengthen security and eliminate the enormous risk created by insecure database configurations, missing databases patches, weak passwords and other vulnerabilities. Database protection knowledgebase subscription leverages automatic database vulnerability remediation updates with the latest vulnerability standards.

IBM Connect 2015

Innovate. Understand. Engage.

#IBMConnect

The Client Journey – Panel Discussion

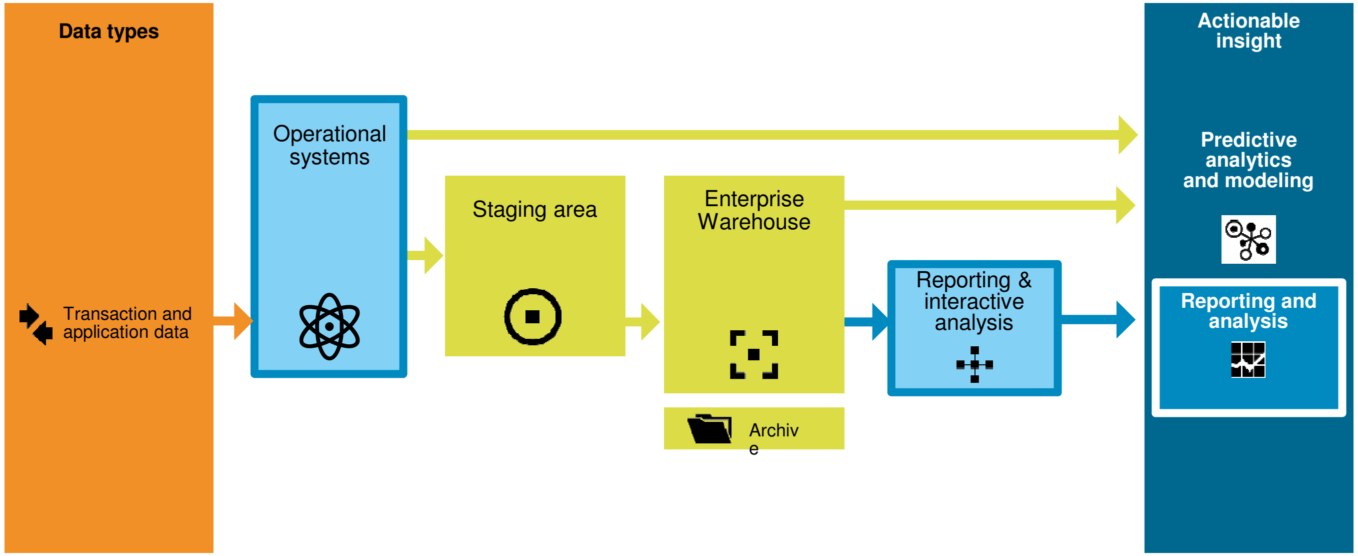
Moderator - Ruth Sun, Director, Client Success – WW Analytics Ecosystem Sales

James Hartwright Data Services Manager, News Corp
Julien Redmond IM/BA Solutions Director, Certus

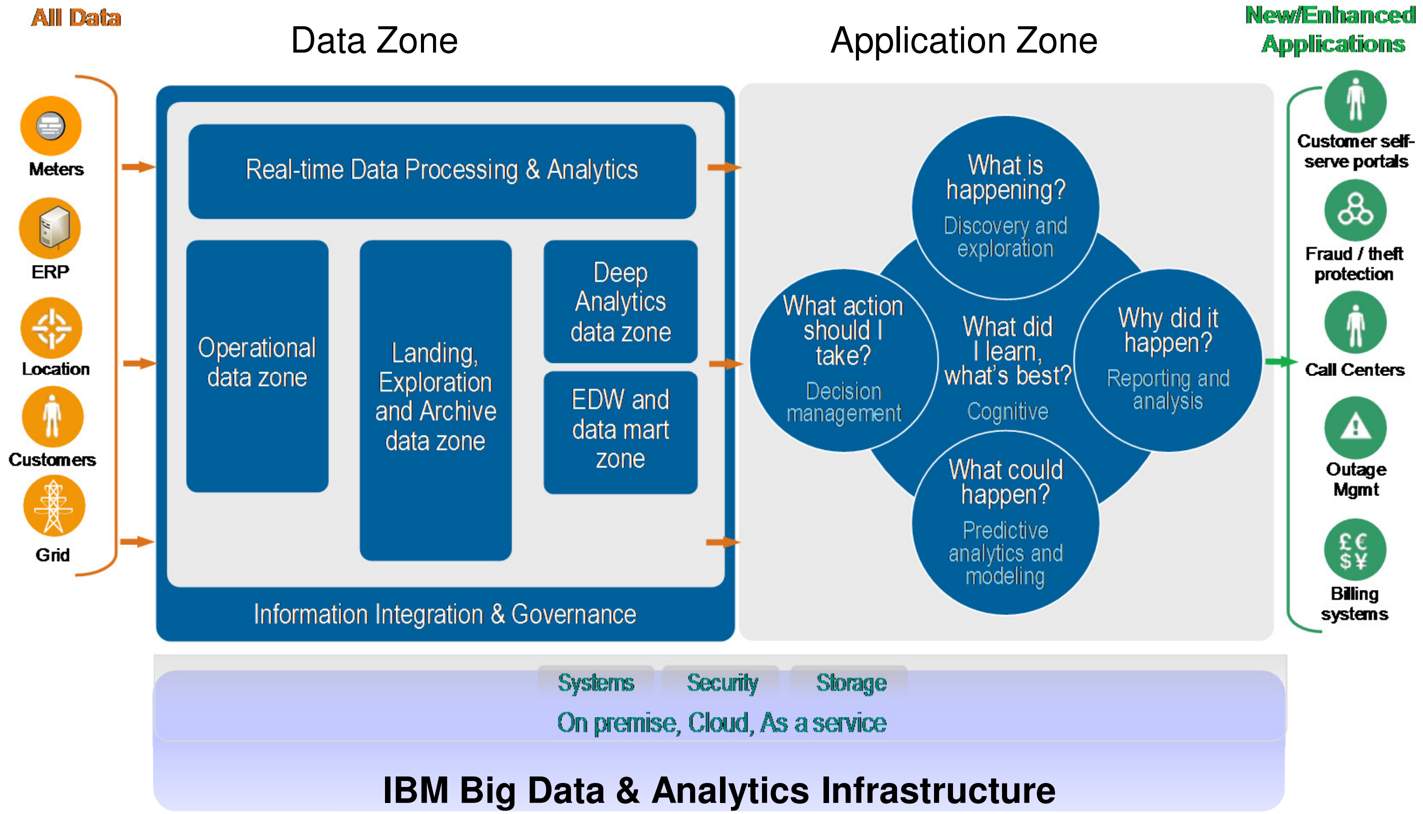
IBM Connect 2015
Innovate. Understand. Engage.

The way it was

The Information Supply Chain – Straight Forward Linear



A new architectural approach for Big Data & Analytics


All Data
Data Zone
Application Zone
New/Enhanced Applications
Meters
ERP
Location
Customers
Grid
Real-time Data Processing & Analytics
Operational data zone
Landing, Exploration and Archive data zone
Deep Analytics data zone
EDW and data mart zone
Information Integration & Governance
What is happening?
Discovery and exploration
What action should I take?
Decision management
What did I learn, what's best?
Cognitive
Why did it happen?
Reporting and analysis
What could happen?
Predictive analytics and modeling
Customer self-serve portals
Fraud / theft protection
Call Centers
Outage Mgmt
£€ $¥
Billing systems
Systems
Security
Storage
On premise, Cloud, As a service
IBM Big Data & Analytics Infrastructure

The Client Journey – Panel Discussion

Moderator - Ruth Sun, Director, Client Success – WW Analytics Ecosystem Sales

James Hartwright Data Services Manager, News Corp
Julien Redmond IM/BA Solutions Director, Certus

IBM Connect 2015
Innovate. Understand. Engage.