ORACLE®

Privacy and Security – Optimization not Balance

Joseph Alhadeff, VP Global Public Policy, Chief Privacy Strategist, Oracle

Vancouver October, 2013

The Opportunity: 1+1= 3 …
The new math is not a zero sum game

- Security and Privacy need to be considered together as mutually reinforcing and can be optimized together.
- Security and privacy regulation is overlapping in jurisdiction and impact
- Security and privacy professionals don't always know how to interact or speak the same language
- New compliance solution for each problem makes no sense – 70-80% common solution
- Visible at C-level

The Organizational Challenge

- Information is the Digital Currency of the Global Economy and Life blood of Every Organization

- Global Information Flows Create Complex Web of Interrelations
  - Global operations require data flows across borders – ***define your business need!***
  - May include layers of subsidiaries vendors, contractors and agents bound by various types or levels of contract
  - Across various media, devices, systems and technologies subject to different rules and reporting chains
  - **Laws and Regulations Must be Respected *and Bridged* to Enable Flow of Information**
- **Challenge**: Assure consistent policies on Privacy and Security and contractual responsibility across networks of entities that may be Involved in information flows

What is your privacy/security foundation?

- The Ecosystem that is the context of the new normal means we need to understand how information is:
  - Managed
  - Shared
  - Overseen, and
  - Secured
- Across the lifecycle of the information
- With up-to-date people, processes policies and technology

Security and Privacy – Relationship

- You can't have privacy without security
- Tensions between security and privacy may exist in policy choices NOT technology
  - Employee monitoring example
- Both need to be risk-based and context aware
- Both share variable criteria based on the nature, use, and importance of the information
- Both are related to the information lifecycle and must interrelate appropriately

Privacy and Security Concepts*

Least Privilege. The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Need-To-Know. A method of isolating information resources based on a user's need to have access to that resource in order to perform his/her job but no more. The terms "need-to-know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

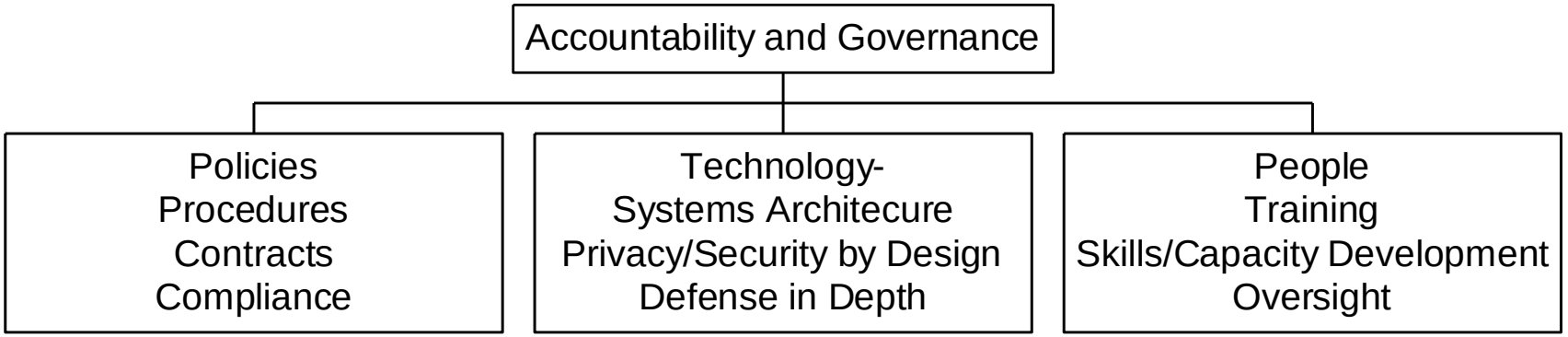
Excerpted from**: Privacy and Security by Design: An Enterprise Approach**, Sept 2013 - http://www.privacybydesign.ca/index.php/privacy-security-design-enterprise-architecture-approach/

Privacy and Security Concepts, Cont'd*

Mandatory Access Control. A means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals and need-to-know) of subjects to access information of such sensitivity.

Segregation of Duties. Separating certain areas of responsibility and duties in an effort to reduce fraud and unintentional mistakes. For example, an employee who accepts cash payments should not also be responsible for making bank deposits and reconciling bank statements.

The Organizational Governance Model



Privacy and Security within the Organization

- Understanding:
  - What information you have
  - Where it is
  - How it was generated
  - Why it is retained
  - Who should have access
  - For how long
- Compliance with:
  - Regulation
  - Internal Process
  - Rules and workflows
- At the
  - Company
  - LOB, and/or
  - Department level

Risk Management Factors

- Nature of the Information
- Nature of the Business
- Size and Type of Infrastructure
- External exposure/remote access
- Level of control over the design, development, configuration and operation of ICT-related components
- Staff expertise/resources
- Legal/regulatory security obligations/requirements and benchmarks of compliance - gap analysis

Privacy and Security: Collaboration not competition…

- Policies, Practices and Technology
- Contracts…
- Compliance Team
- Communications and Training
- Enforcement/Oversight
- Incidence Response/Debrief
- Review, revise, refresh

Compliance Methodology

- Outline the needs
- Identify and assemble the team
- Identify / classify the information
- Map the information and flows
- Broad understanding of the technology possibilities
- Develop polices, practices and procedures
- Identify needed controls and possible control points
- Optimize the processes
- Implement the technology
- Test, review revise

Program Controls: Privacy and Security Policies

Privacy Policies

- Collection, use and disclosure of personal information, which include requirements for consent and notification
- Access to and correction of personal information
- Retention and disposal of personal information

Security Policies

- Risk assessment, management, remediation
- Administrative, physical and technological security controls
- Role-based access and adaptive access controls
- Fine Grained Audit Controls
- Breach Response/Incident management protocols

Training on all policies

Lifecycle Issues: Assessment and Revision

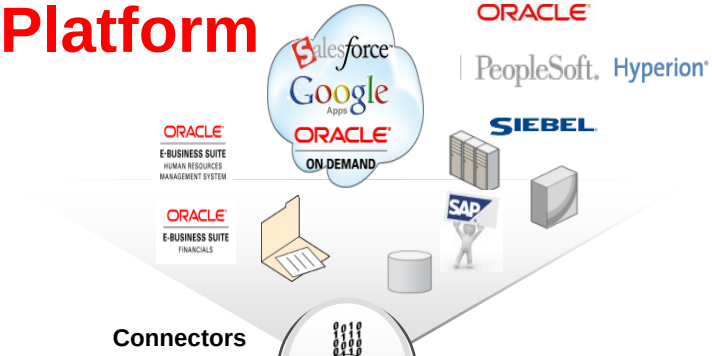
- Develop an oversight and review plan
- Update personal information inventory
- Revise policies, as appropriate
- Treat risk assessment tools as evergreen
- Modify training and education
- Adapt breach and incident response protocols
- Fine-tune service provider management
- Improve external communication

The Access Control Question

- Security question: How do I keep the bad guys out?
- Privacy Question: How Can I make sure that only the ***RIGHT*** good guys get in?
- Tools that accomplish both:
  - Appropriate role definition and privilege management
  - Row level and role-based access controls,
  - Fine grain audit,
  - VPD and Label security

Oracle Identity Governance

Governance Platform



Connectors

Provision | **De-Provision**

Grant User Access | **Monitor User Access**

Access Request

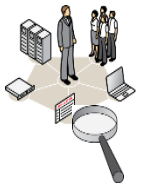
Privileged Account Request

Role Lifecycle Management

Check-in/ Checkout

Identity Certifications

IT Audit Monitoring



Rogue Detection & Reconciliation

Reporting & Privileged Access Monitoring

Roles
Entitlements
Accounts
Glossaries

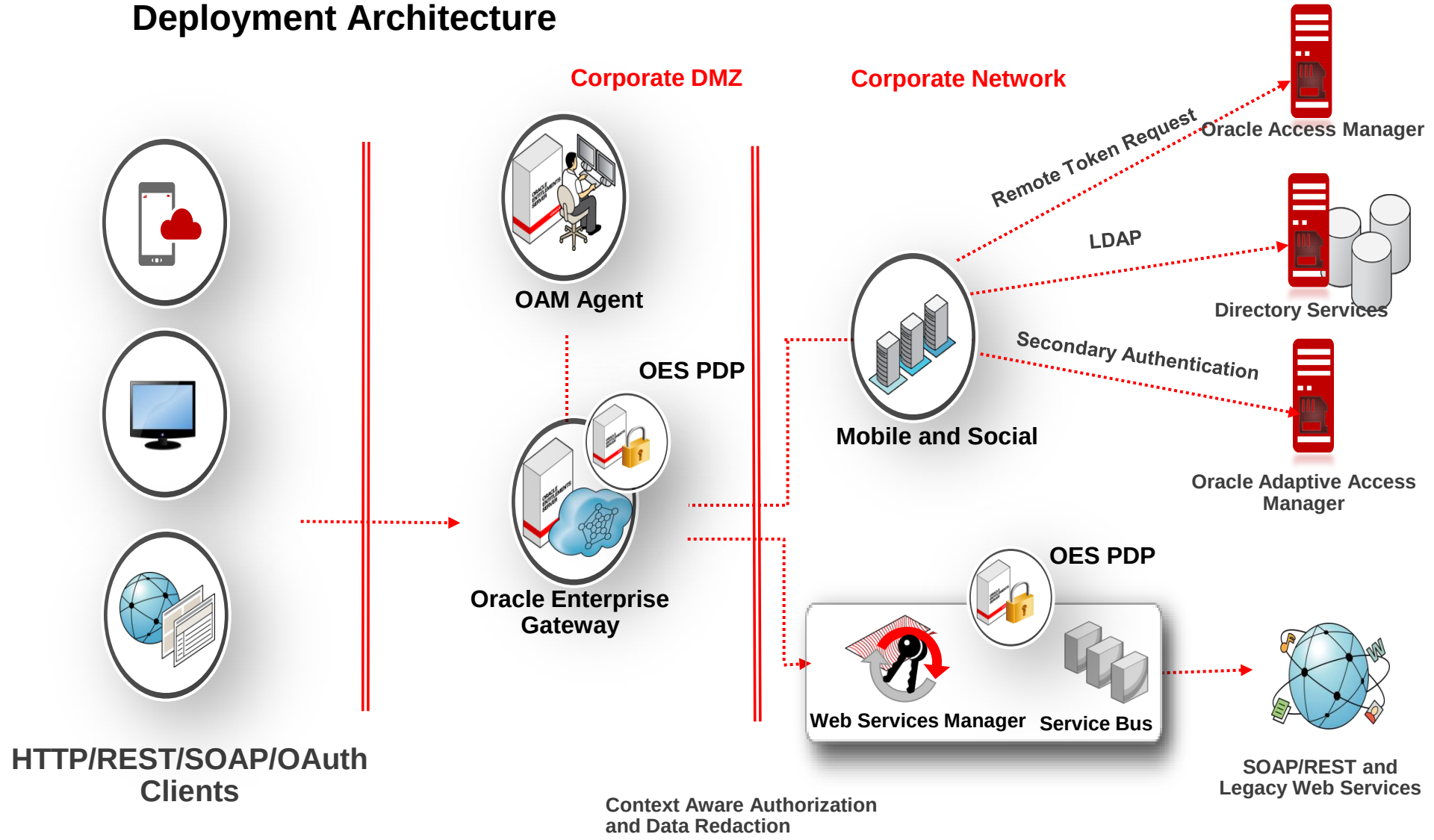
Access Catalog

Ownership, Risk & Audit Objectives

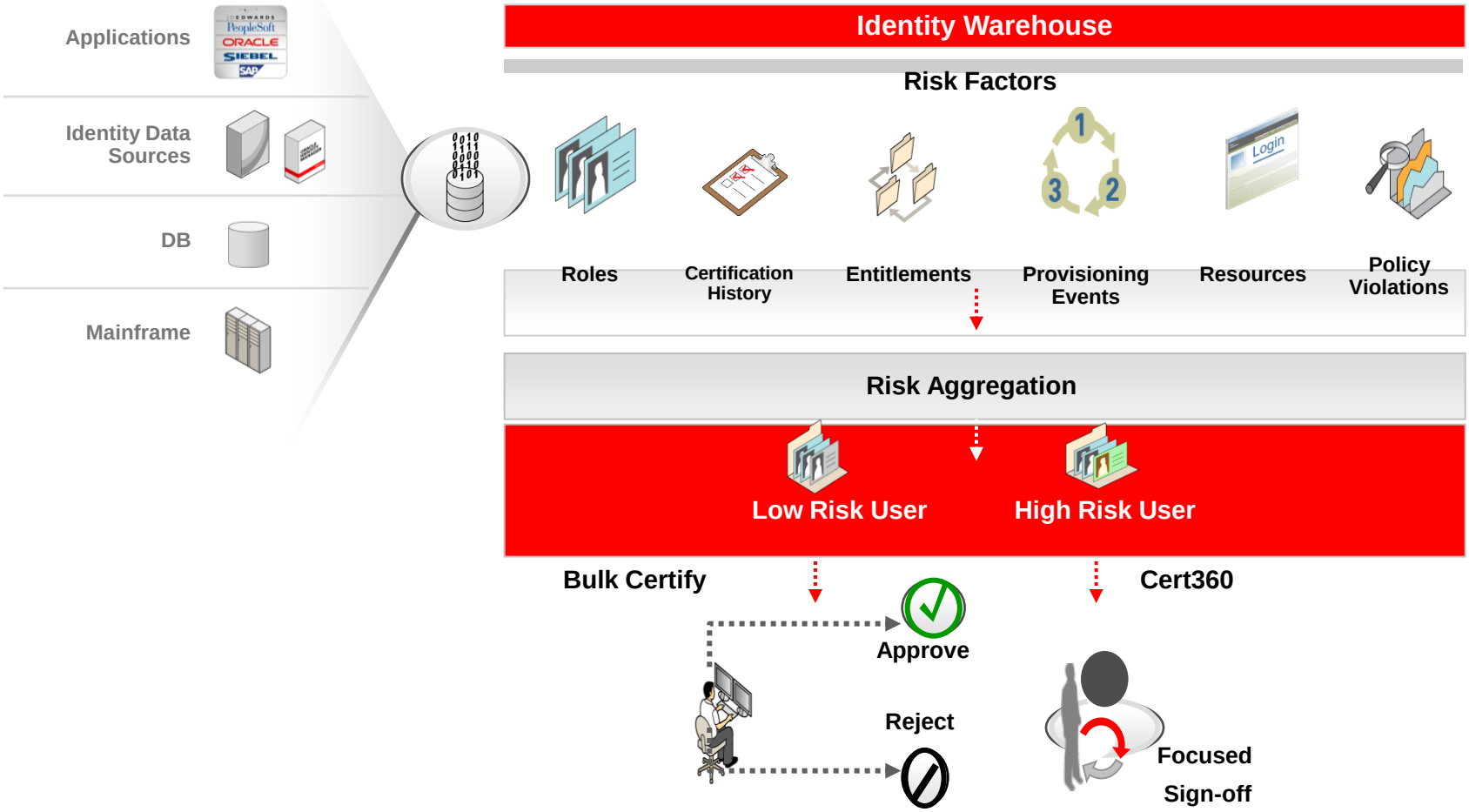
Catalog Management

Oracle Mobile & Social Access Management

Deployment Architecture



Risk Based Certification



ORACLE DATABASE SECURITY

Maximum Security or Critical Data Infrastructure

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption & Redaction	Auditing	Privilege Analysis
Data Masking	Activity Monitoring	Sensitive Data Discovery
Privileged User Controls	Database Firewall	Configuration Management
ORACLE 	ORACLE 	ORACLE 

Privacy Questions for Security

Security Factors

- Where is it stored?
- How is it stored?
- What are the policies
- Who needs access?
- Least privileged access
- Audit
- Incident response
- Prevention/ investigation of breaches

Gating Factors

- How well do job functions and privileges align with need to know controls
- What monitoring is required to assure these controls?
- Change management controls
- Evaluation, reevaluation and lessons learned
- Testing and Training

Privacy Concepts/Security Tools

Privacy Concepts

Limit Uses of PII

Choice/Consent

Integrity

Security

Access and Correction

Accountability

Security Tools

Meta data and permissions

Role based access controls

Application based controls

Recovery to previous state

Defense in depth

Data Masking

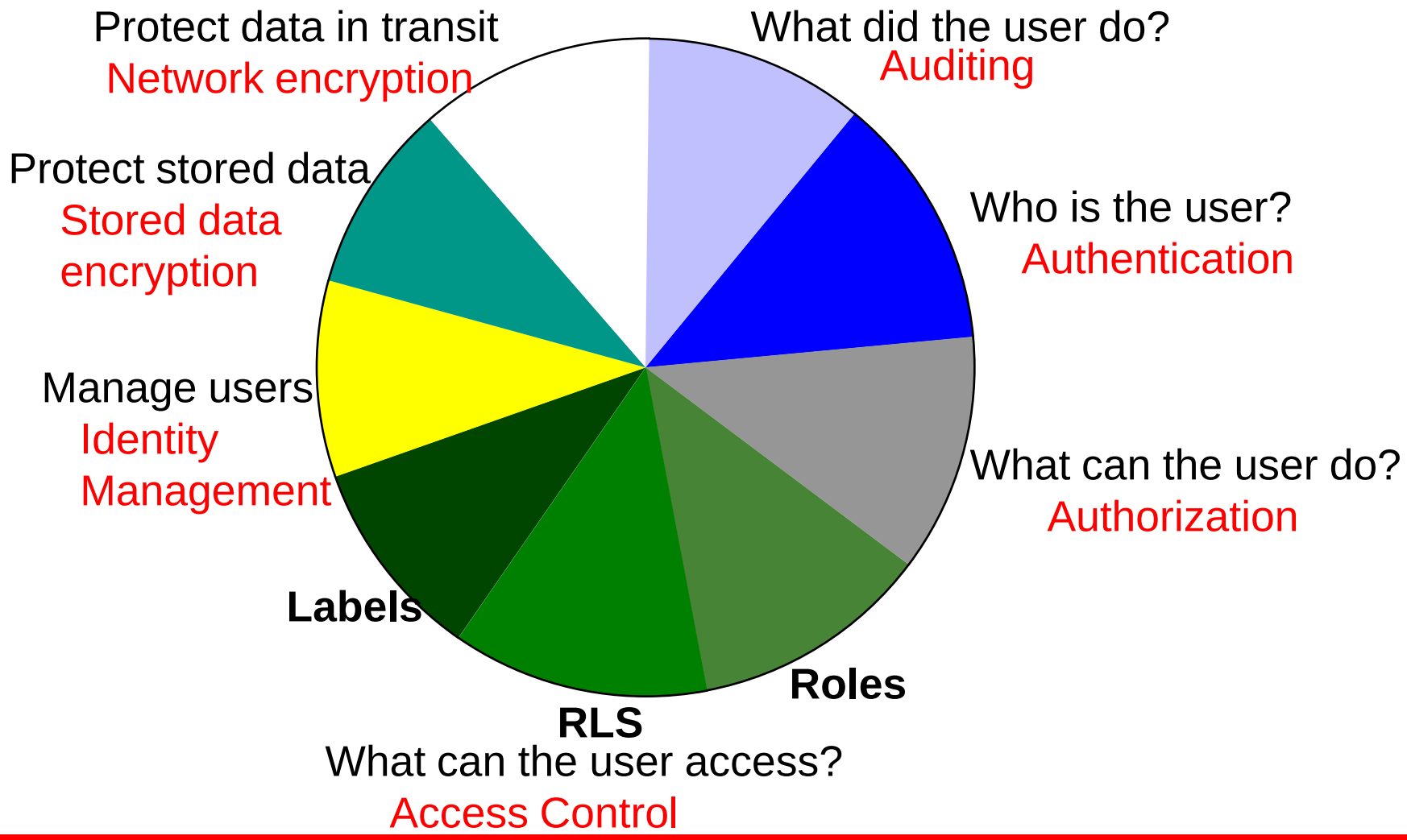
Label Security, VPD

Encryption

Security alerts

Audit controls

Privacy Application Technology



Privacy Supported in Security and Technology

- Authentication: Who is the end user, who are the users accessing the system on the inside
  - Identity Management
- Authorization: What rights to authenticated users have?
  - Tied to HR system allows for updated management upon change of roles
- Access control: Based on user identity and rights, what content can user access
- Audit: Has user behavior contravened policy
  - Selective audit, fine grain audit, investigatory functions
- Encryption: stored and in transit

Collaboration and Cooperation Take-Away Concepts

- ***Responsible*** Information Sharing is essential
- Privacy and security are essential elements of trust and governance.
- Security and privacy need to be discussed in the context of organization and user needs
- These are ecosystem, not just system issues, which include: value chains, logistics, procurement, audit, sourcing, cloud …

- Make compliance requirements and tools part of your review and audit process – develop value propositions for compliance beyond compliance

Analytics is part of the solution... time permitting…

Security is a Barrier for Adoption of IoT

"The horizontal evolution of M2M will require full end-to-end security. Significant efforts need to be invested into M2M application security in order for the M2M market to fully evolve. Whether this is through open source initiatives or standards development, the demand for increased M2M application security will have to be answered, and sooner rather than later."

ABI Research, M2M Dream Challenged by Alarming Security Concerns, Feb 2013

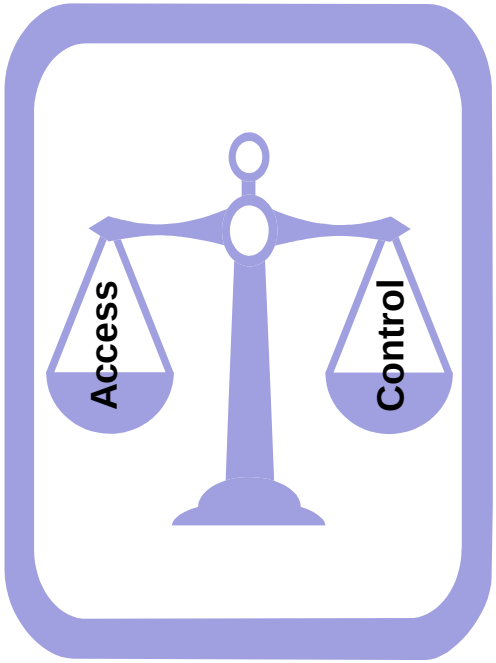
40% Of embedded systems and applications developers have not proactively addressed security in existing development projects

30% Median CAGR growth (2011-2014) in shipments of security solutions for industrial automation, medical devices, consumer electronics, automotive and retail

Source: VDC Research
Strategic Insights 2012: Embedded Software & Tools Market, Security Development & Runtime Solutions

Challenges in IoT Security

- Typical challenges for IoT service providers
  - What protection measures are possible as thousands of intelligent things cooperate with other real and virtual entities in random and unpredictable ways?
  - How do you ensure security given IoT's highly distributed nature and use of fragile technologies, such as limited-function embedded devices?
  - How do you leverage investments in existing internet security technologies for the highly fragmented IoT networks?
  - How can you define and enable trust in a dynamic IoT network with weak trust links between network nodes?



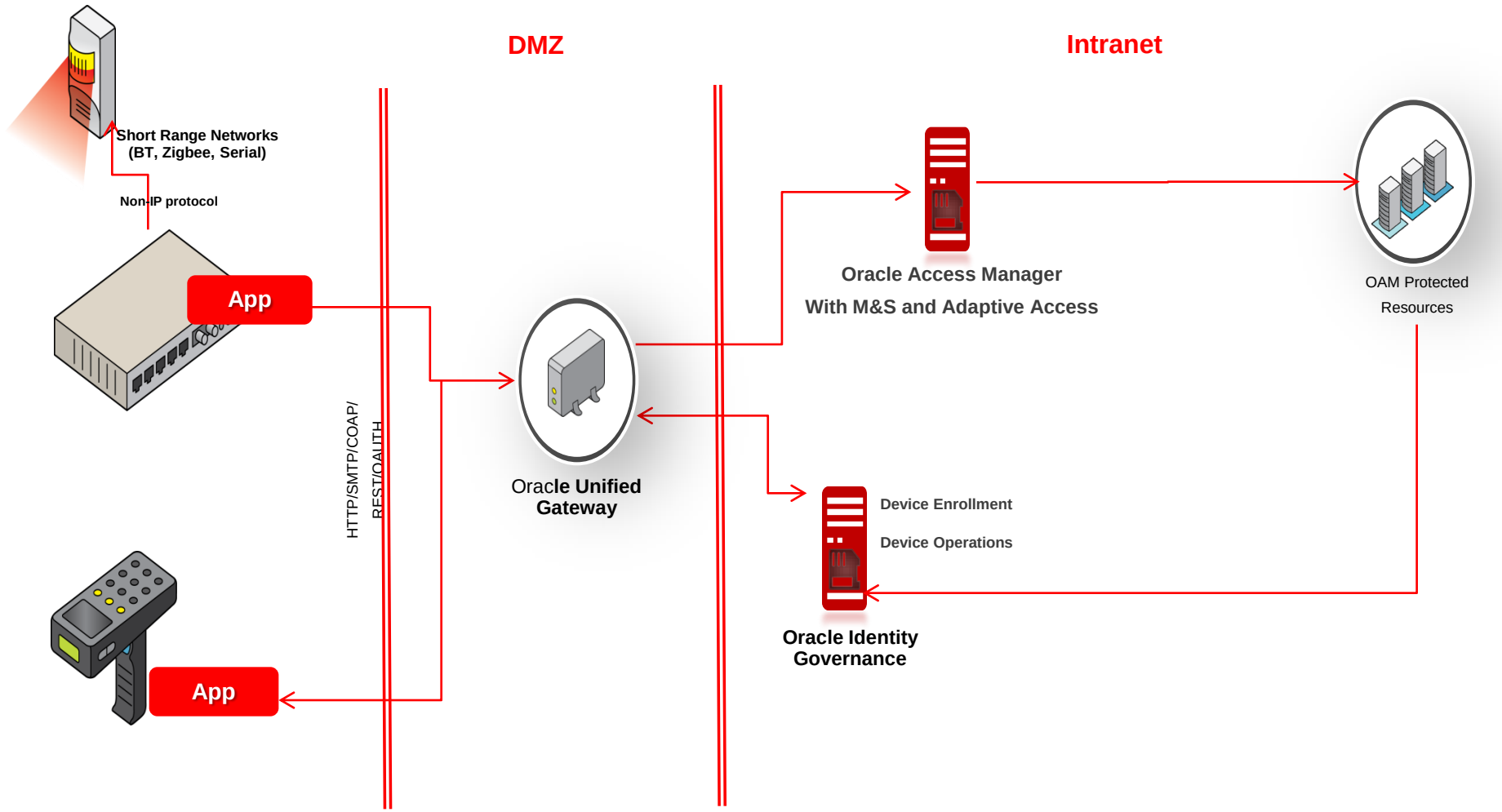
Key IoT Security Requirements

- **Onboarding & Enrollment**
- **Authentication & Authorization**
- **Device Metadata & Control**
- **Policy & Key Management**
- **Application Management & Provisioning**

- Mutual authentication between devices and server
- Confidentiality of data transfer over multi-protocol networks
- Device data management
- Governance of trust relationships in IoT networks
- Device applications provisioning & management

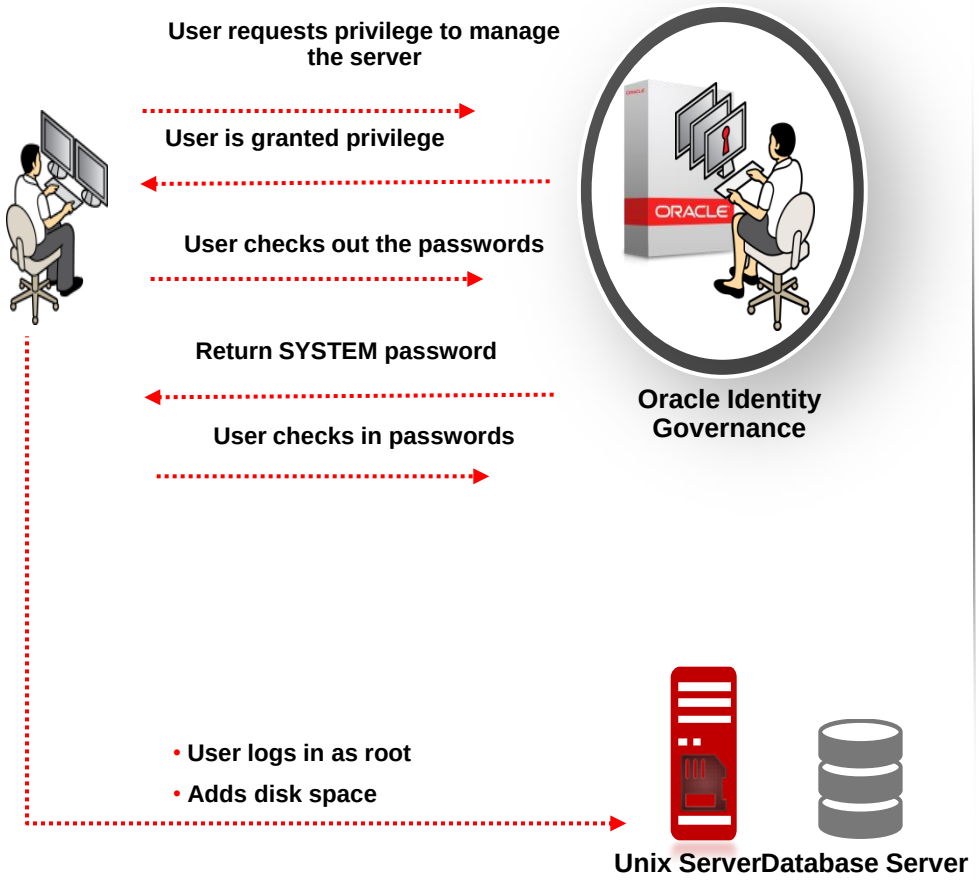
Oracle IoT Security Solution

Overview



Identity Governance

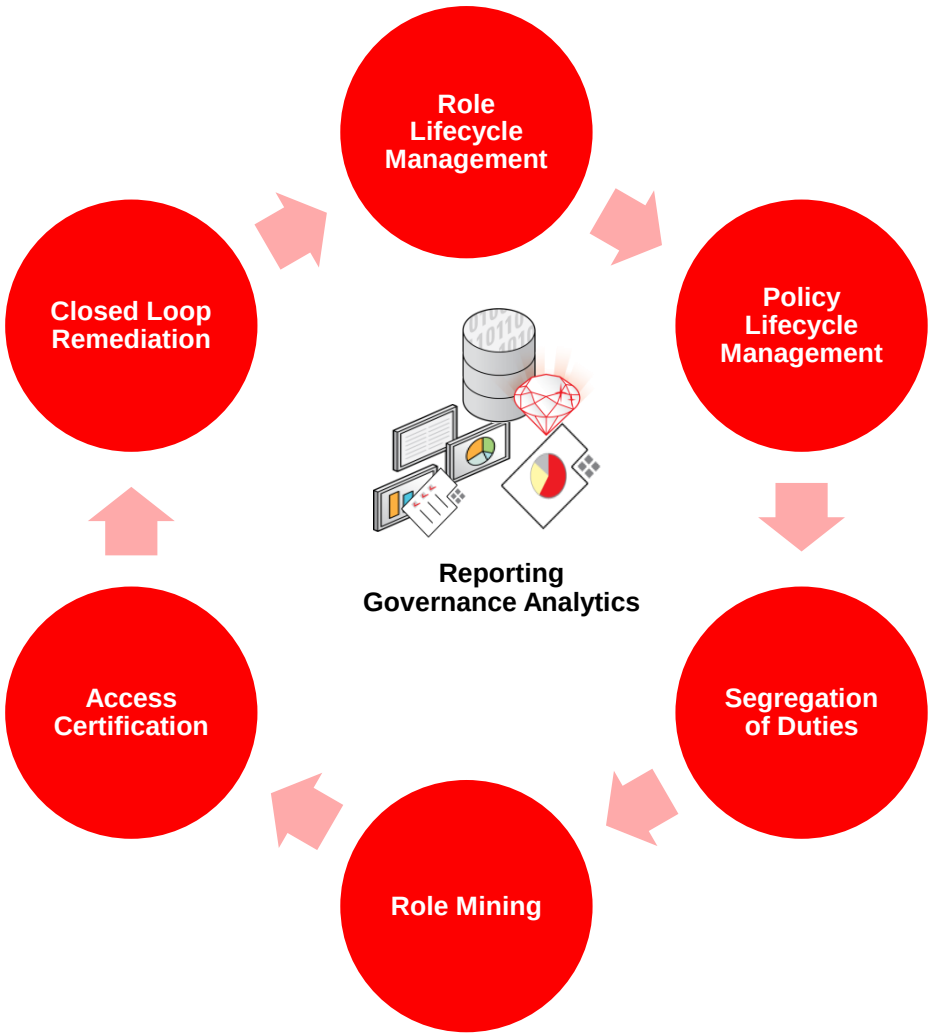
Manage Regular and Privileged Access



- Manage access to applications using Access Request
- Use break glass workflows to get emergency access
- Leverage common Connectors to manage privileged accounts and credentials
- Leverage Access Certification to ensure Compliance

Identity Governance

Continuous Compliance



- Manage the lifecycle of Roles and Policies
- Carry out Role Mining to discover roles
- Prevent violations using Segregation of Duties
- Implement Access Certification
- Address violations using Closed-loop Remediation