



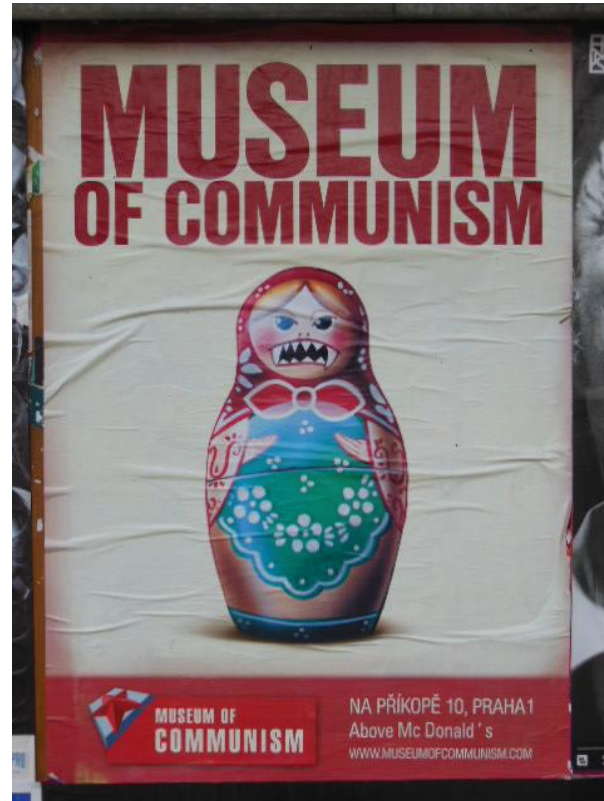
ORACLE®

Security – It's an ecosystem thing...

Joseph Alhadeff

Vice President Global Public Policy, Chief Privacy Strategist

The Security challenge in the before time....



Today's Threat Environment...



67%

Records breached from servers



76%

Breached using weak or stolen credentials



69%

Discovered by an external party

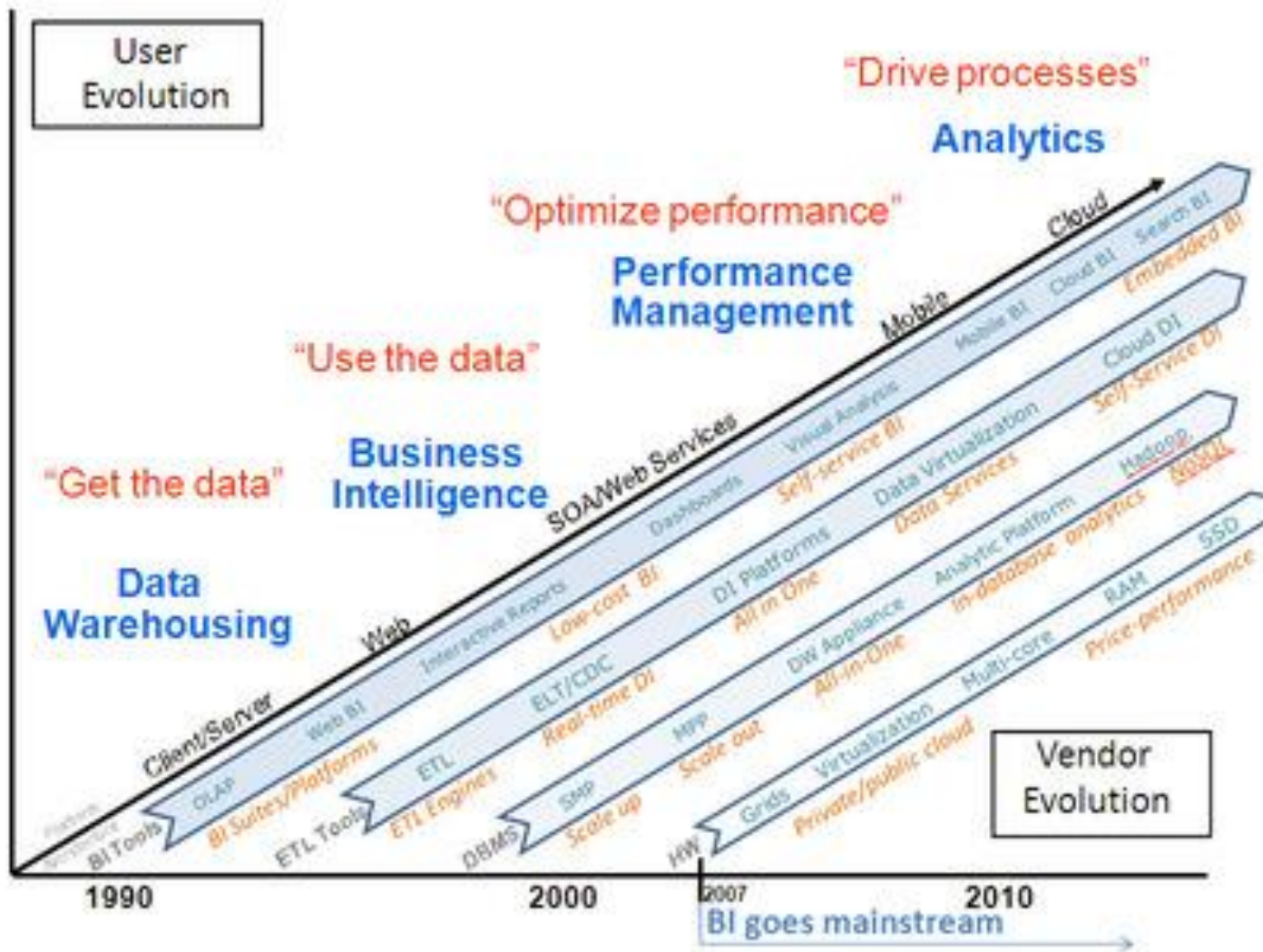


97%

Preventable with basic controls



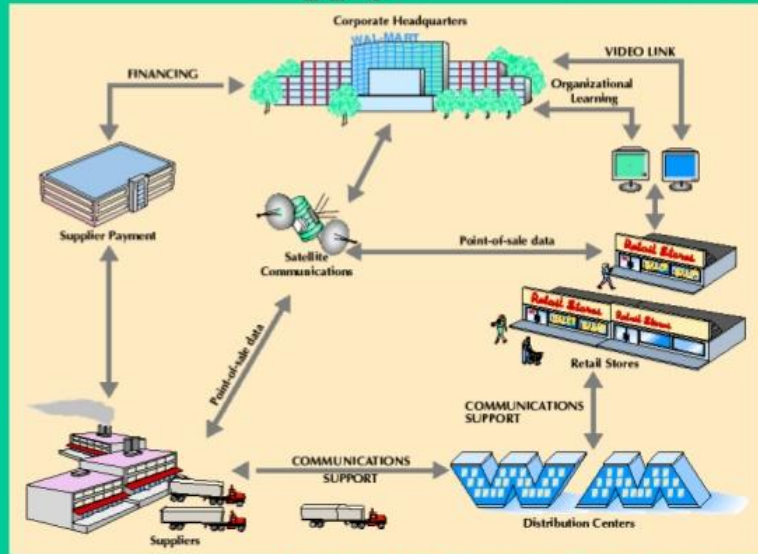
The Continuum Evolves



<http://www.b-eye-network.com/blogs/eckerson/archives/appliances/>

A Corporate Footprint...

Wal-Mart Supply Chain



Source: Adapted from Garrison Wieland for "Wal-Mart's Supply Chain," *Harvard Business Review* 70(2; March-April 1992), pp. 60-71.

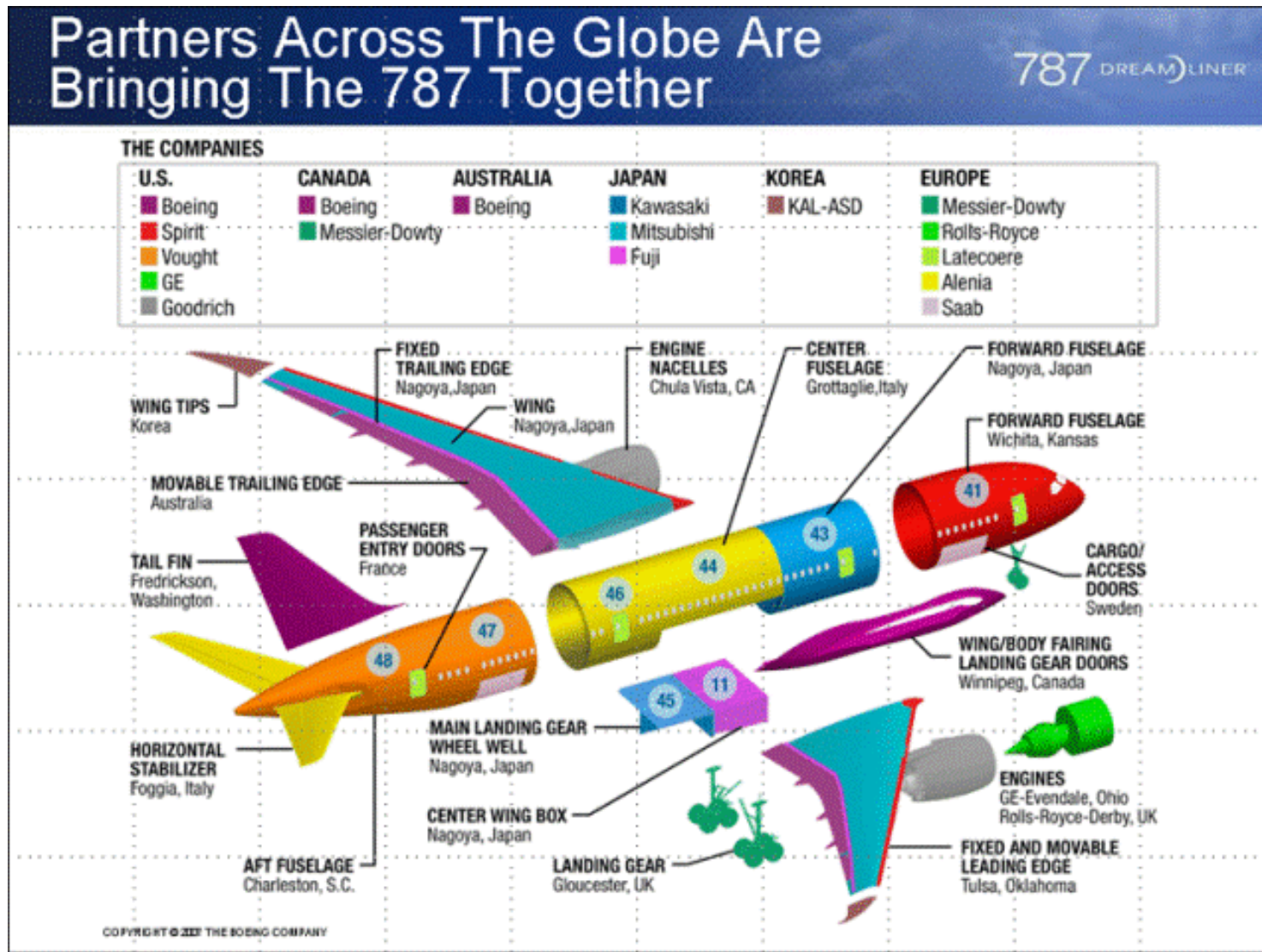
VALUE CHAIN ANALYSIS OF WAL-MART

Support activities	Firm infrastructure					M A R G I N
	Human recourse management					
	Technology development					
	Procurement					
Primary Activities	Inbound Logistics	Operations	Outbound Logistics	Marketing and sales	Service	

“People think we got big by putting stores in small towns. Really we got big by replacing inventory with Information” ... Sam Walton

<http://www.slideshare.net/monicamishra10/walmart-value-chainanalysis>

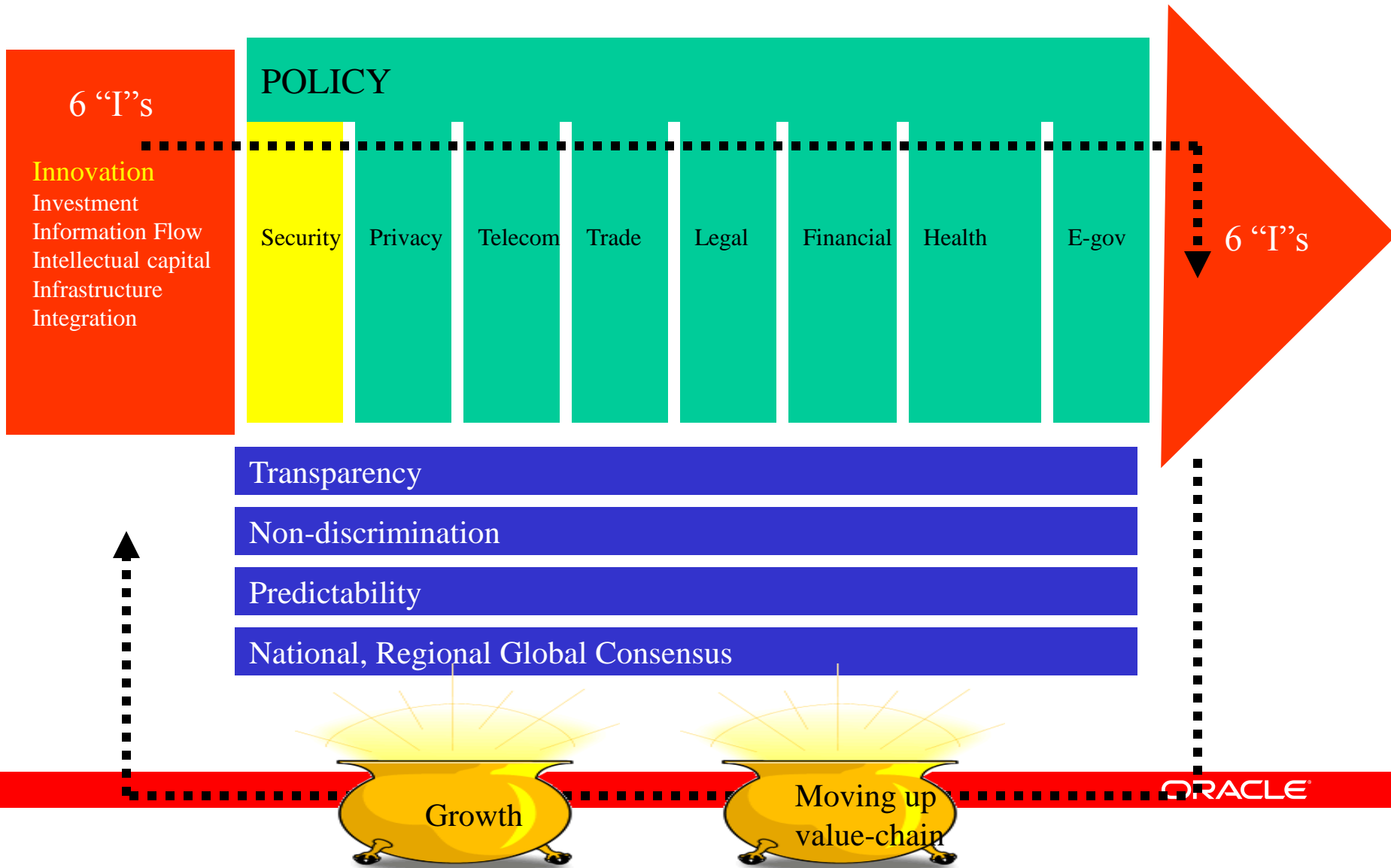
A Global Endeavor... and data flows



Security as an ecosystem concept

- You must consider security in your organization in terms of policies, practices, operational procedures and compliance obligations.
- These policies however are not limited to security
 - Privacy
 - HR
 - Change management
 - Business continuity...
- You then need to consider similar factors across your upstream and downstream chain of organizations and assure that, at least, minimums are met – these will be ecosystem base conditions...

Consider Security in the Broader Regulatory Context



First, know your own system... some highlights...

- Identify business goals and objectives
- Understand and optimize processes and workflows for the applicable operational and technological environment
- Generally understand the nature of the data and the resulting risk both to the enterprise *and the end user/data subject* of a compromise of the data
- Associate roles and privileges to those persons who will access data and assure that they are trained and accurately maintain roles and privileges as they change and apply appropriate separation of duties...
- Identify risks/threats, determine acceptable risk and mitigate risk to acceptable levels
- Security lifecycle management, training, incidence response, business continuity...

HIPAA Security...

Security Standards: Matrix

Standards Sections Implementation Specifications (R)

=Required, (A) =Addressable

Administrative Safeguards

Security Management Process	164.308(a)(1)
Risk Analysis (R)	
Risk Management (R)	
Sanction Policy (R)	
Information System Activity Review (R)	
Assigned Security Responsibility	164.308(a)(2)
(R)	
Workforce Security	164.308(a)(3)
Authorization and/or	
Supervision (A)	
Workforce Clearance Procedure	
Termination Procedures (A)	
Information Access Management	164.308(a)(4)
Isolating Health care	
Clearinghouse Function (R)	
Access Authorization (A)	
Access Establishment and Modification (A)	
Security Awareness and Training	164.308(a)(5)
Security Reminders (A)	
Protection from Malicious Software (A)	
Log-in Monitoring (A)	
Password Management (A)	
Security Incident Procedures	164.308(a)(6)
Response and Reporting	
(R)	
Contingency Plan	164.308(a)(7)

Data Backup Plan (R)

Disaster Recovery Plan (R)

Emergency Mode Operation Plan (R)

Testing and Revision Procedure (A)

Applications and Data Criticality Analysis (A)

Evaluation 164.308(a)(8) (R)

Business Associate Contracts and Other
Arrangement.

164.308(b)(1) Written Contract or Other Arrangement (R)

Physical Safeguards

Facility Access Controls 164.310(a)(1) Contingency

Operations (A)

Facility Security Plan (A)

Access Control and Validation Procedures (A)

Maintenance Records (A)

Workstation Use 164.310(b) (R)

Workstation Security 164.310(c) (R)

Device and Media Controls 164.310(d)(1) Disposal (R)

Media Re-use (R)

Accountability (A)

Data Backup and Storage (A)

Technical Safeguards (see § 164.312)

Access Control 164.312(a)(1) Unique User

Identification (R)

Emergency Access Procedure (R)

Automatic Logoff (A)

Encryption and Decryption (A)

Audit Controls 164.312(b) (R)

Integrity 164.312(c)(1) Mechanism to

Authenticate Electronic Protected Health Information (A)

Person or Entity Authentication 164.312(d) (R)

Transmission Security 164.312(e)(1) Integrity

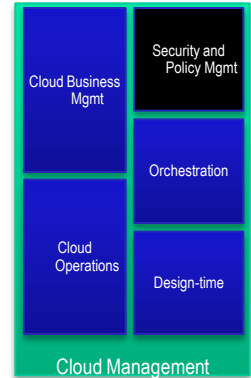
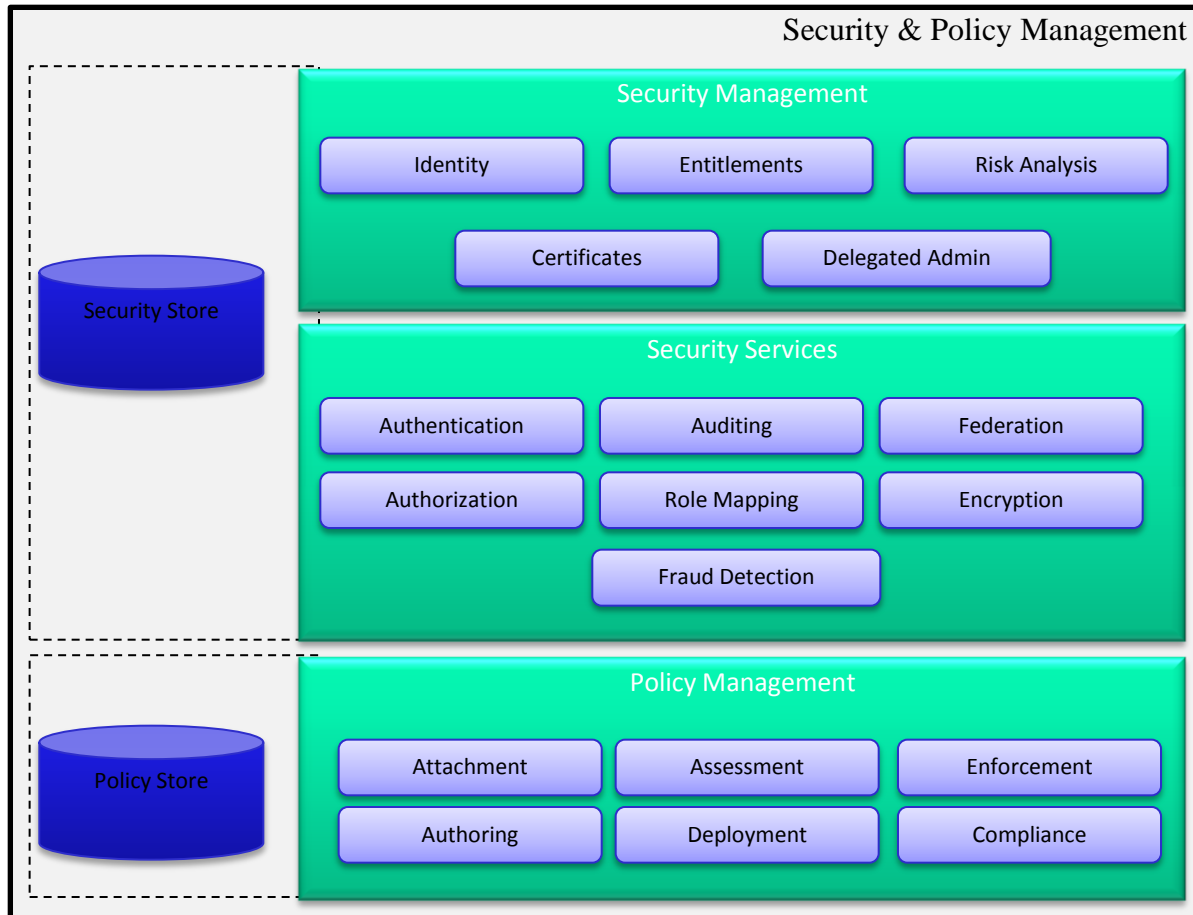
Controls (A)

Encryption (A)

Source:

<http://www.cms.hhs.gov/securitystandard/downloads/securityfinalrule.pdf>

Security and Policy Management



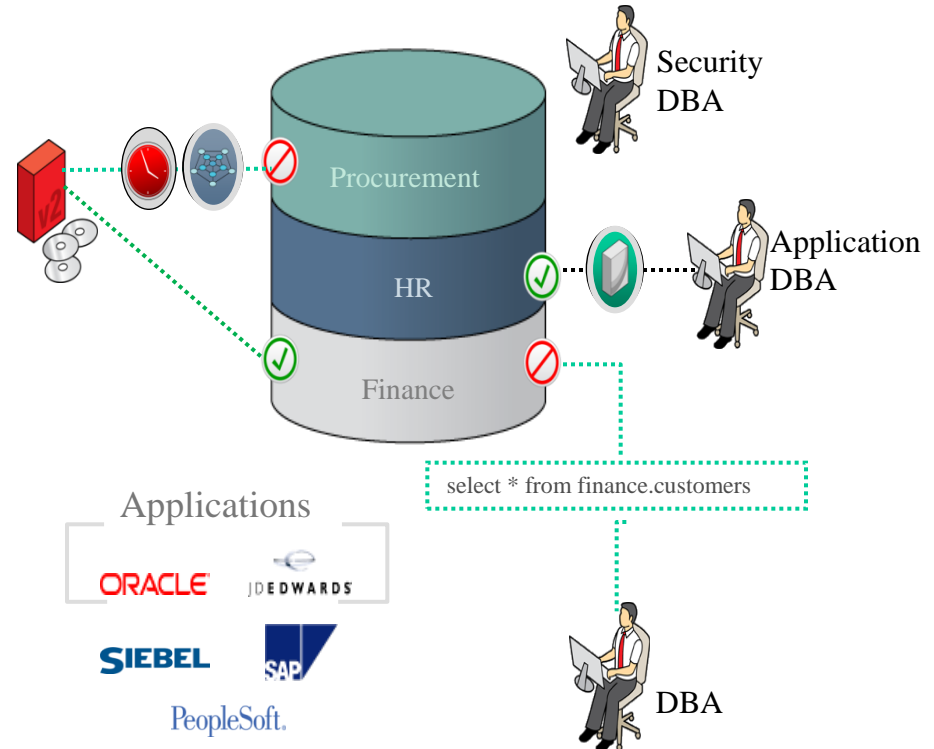
Defense-in-Depth for Maximum Security

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

Privileged User Controls

Oracle Database Vault

- Limit DBA access to application data
- Multi-factor SQL command rules
- Realms create protective zones
- Enforce enterprise data governance, least privilege, segregation of duties
- Out of the box application policies



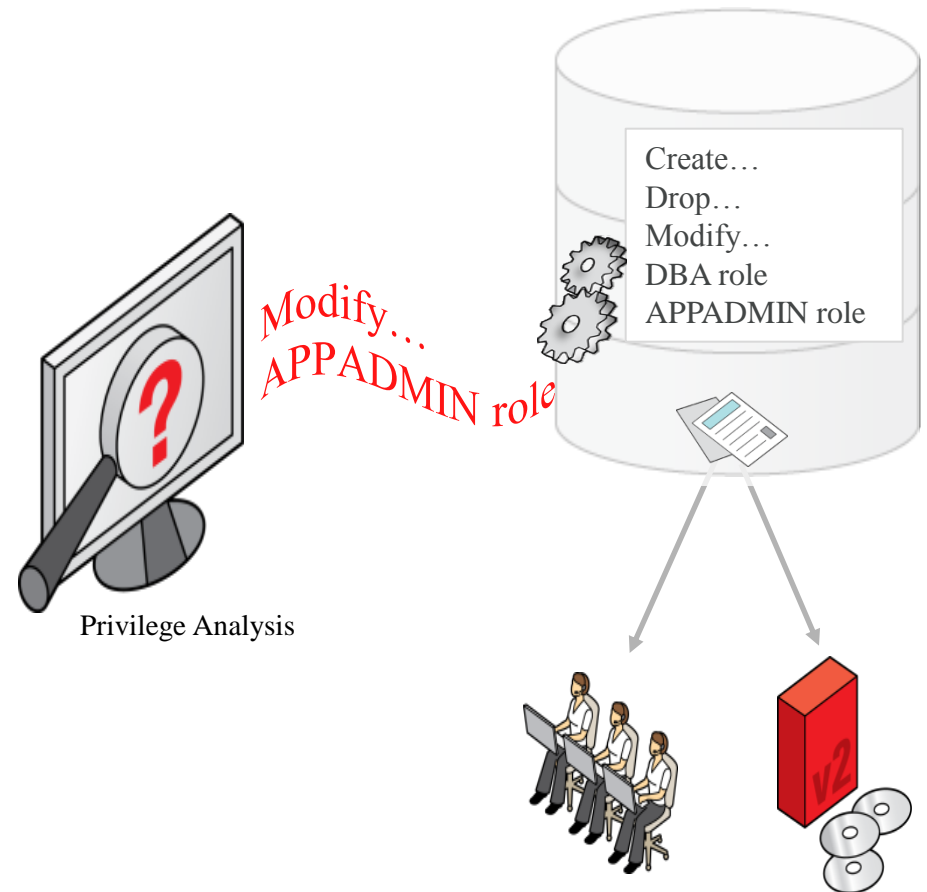
Technology and Security – not a zero sum game



Discover Use of Privileges and Roles

Oracle Database Vault

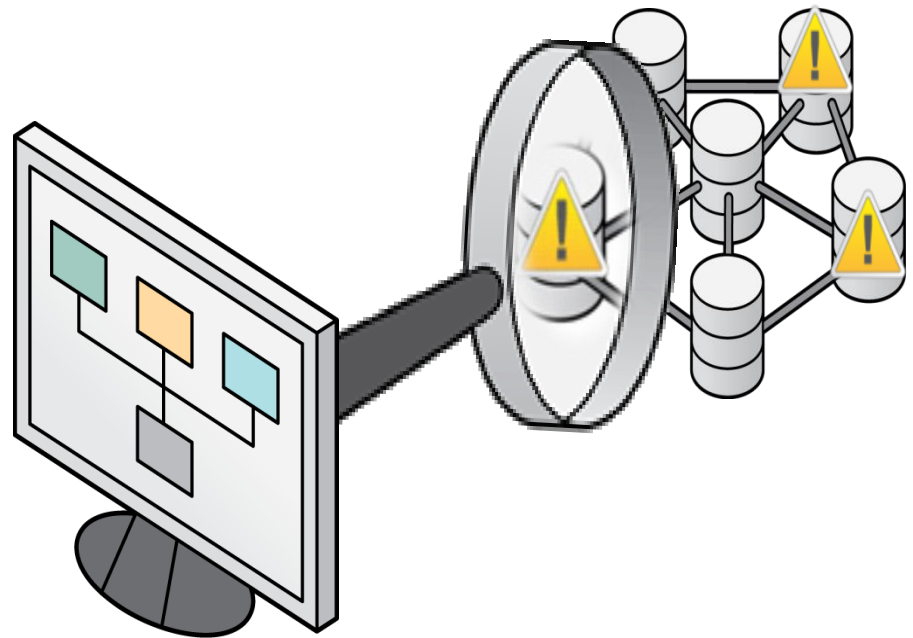
- Turn on privilege capture mode
- Report on actual privileges and roles used in the database
- Helps revoke unnecessary privileges
- Enforce least privilege and reduce risks
- Increase security without disruption



Discover Sensitive Data and Databases

Oracle Enterprise Manager 12c

- Scan Oracle for sensitive data
- Built-in, extensible data definitions
- Discover application data models
- Protect sensitive data appropriately: encrypt, redact, mask, audit...



Making Data and Big Data Safer for Developers



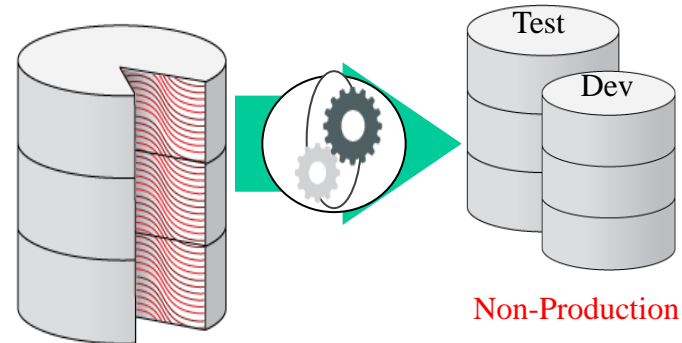
Masking Data for Non-Production Use

Oracle Data Masking

- Replace sensitive application data
- Referential integrity detected/preserved
- Extensible template library and formats
- Application templates available
- Support for masking data in non-Oracle databases

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000

Production



LAST_NAME	SSN	SALARY
ANSKEKSL	323—23-1111	60,000
BKJHHEIEDK	252-34-1345	40,000

Building the team...



Understand who you need to do what...

- There is no single person with enough information to do this. This is a team sport – across roles and departments...
 - Recall while we may be centralizing information, computing resources are being democratized with cloud and other easy to use services.
 - The need to reach beyond the IT team as they are not the only system owners and administrators.
- Do you need external help to map data flows and help configure systems?

Get Help...

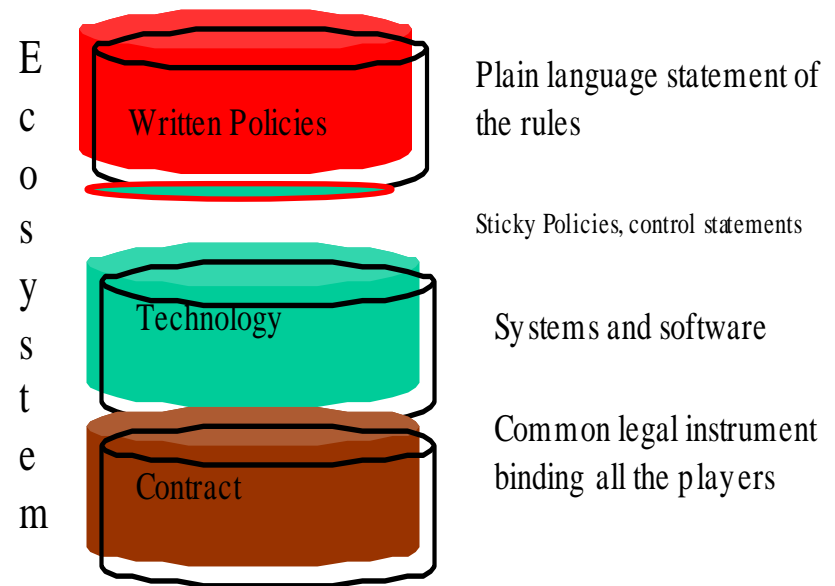
- There are consultants and integrators that have useful skills and experience to assist you role definition, process mapping and technology configuration



The new end-to-end..

- The TAS³ Parable...
- How far does your system reach?
- How far does your responsibility extend?
- What can you control/What can you influence
- How?

TAS³ Governance Architecture










Security knock, knock game...



- Who/what are you?
- How do I know?
- What assurance do I have
- What do you want to do?
- What are you allowed to do
- How is that monitored?
- Now think of it across an ecosystem –
 - Federation...

The Identity Management Problem

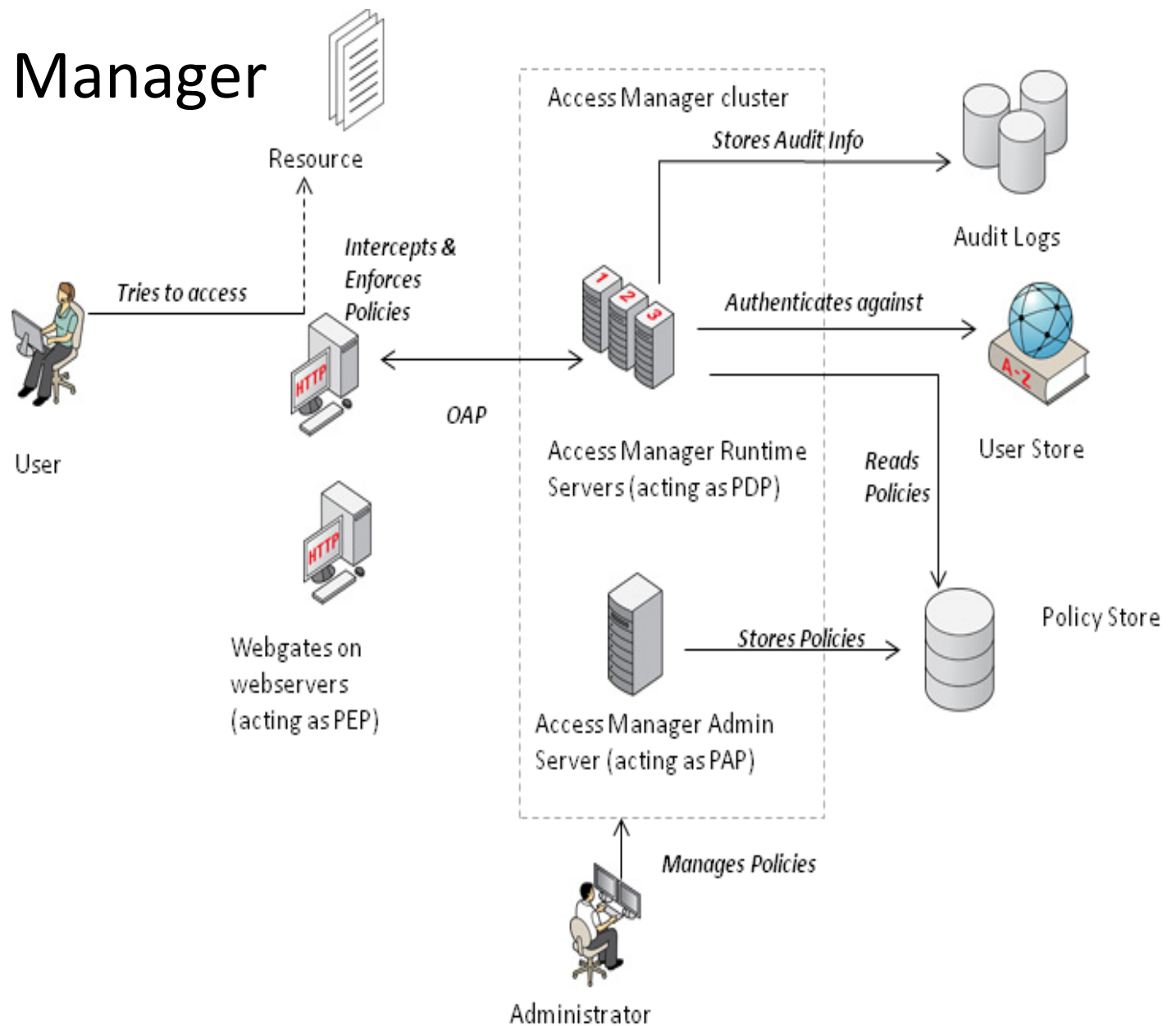
GOER	SFS	PR_DB	OFT LDAP	App A	App B
					
Jberry	Bbanks	A49320	Cooperl	Frenetc	Sequensh
Esiegel	Lsully	A39943	Tinleyj	Smileys	Welchj
Jrowland	Lbitmore	A49454	Harrisd	Entrald	Pettyr
Mfriedel	Ltimble	A93934	patelr	Novacho	Robertsj
Sbenson	Abosyle	A39485	Rowlandr	Alvarag	Julianr
Thanks	Bcoldwel	A49382	Bensons	Narlersh	Nantpre
Jwayne	Dparis	A48382	Quinleys	Woodst	Enaget
Tcarrol	Clriot	A49382	Harminb	Nicklausj	Jhancock
Sharris	Etear	A39485	Travolta	Hoganb	Johnh
Bwhite	Smackay	A29483	Francek	Palmera	Hanwayv
Ddailey	Mturner	A49583	Lipperd	Dimarcoc	Composi
Eheiden	Mmclain	A49382	Skatee	Perryk	Initialy
Lball	Mcpasch	A49302	Marinoe	Beards	rpatel
Hwiggins	Jpasch	A42845	Flamingo	cw33	Stickler
Cjohnson	rakeshp	A20184	Russiak	Fusar	Bourne
r_patel	Tdean	A49284	Crowd	RP738	Fusar
Mthomas	Jtorville	A49248	Patel-A1	Margaglio	Margoliao
Browland	Cdean	A50824	Daoudc	Lithowan	Navka
Mprehn	Nreagan	A42948	Louf	Vanagas	Koskoma
	Rnixon	A49274	Peizerat	Lightes	Hackinsa



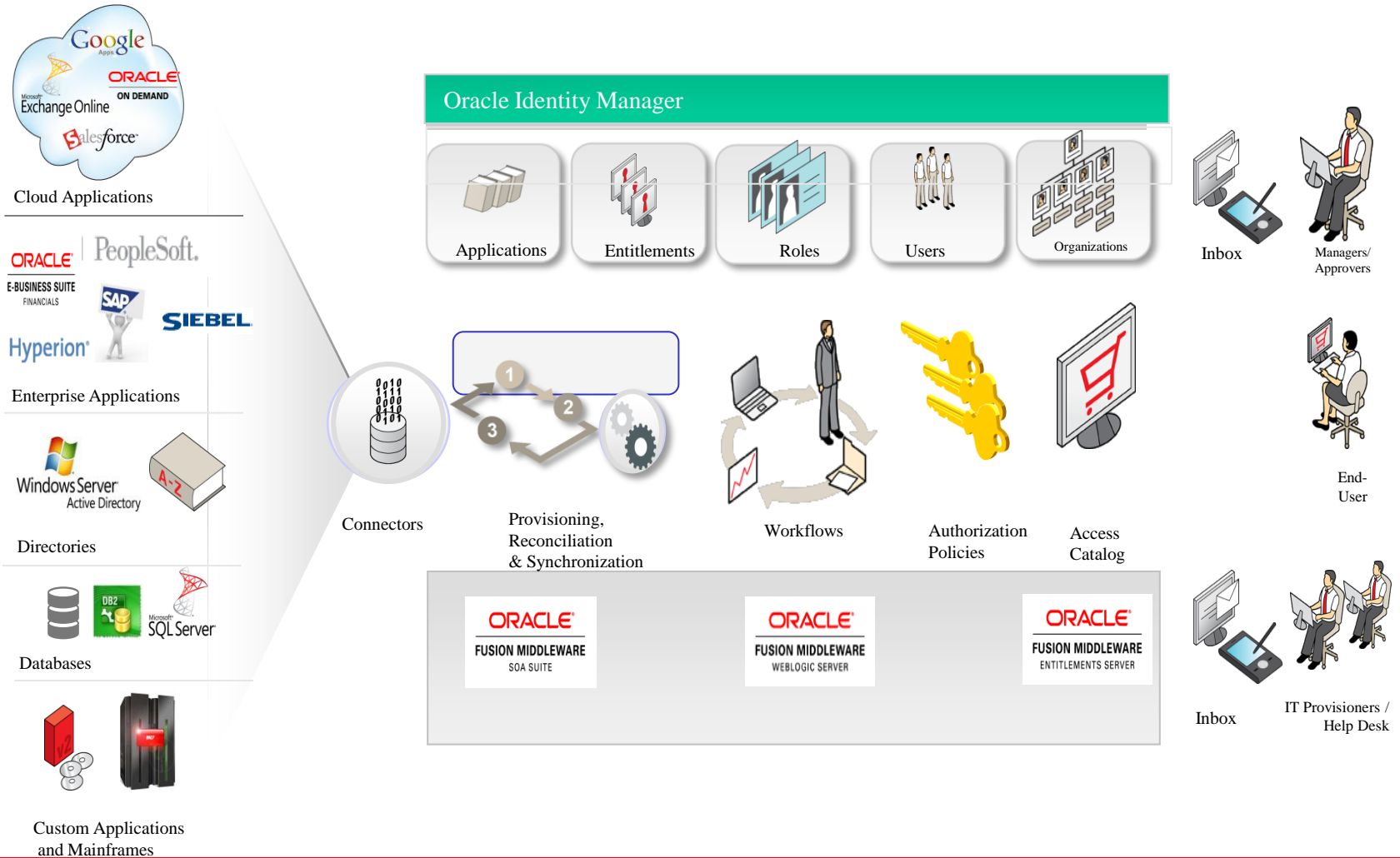
Rakesh Patel

- agency1- r_patel
- agency2 - rakeshp
- agency3 - A449382
- acgency4 - patelr
- Application A - RP738
- Application B - rpatel

Access Manager



Identity Manager



Oracle Entitlements Server

Fine grained authorization for Web Applications & Portals

The screenshot displays the Oracle Entitlements Server web interface. The top navigation bar includes links for Home, Navigator, Recent Items, Favorites, Tags, and Watchlist. The main content area is divided into several sections:

- Watchlist:** Contains sections for Notifications (Management Approvals, Requiring Action), Goals (Employee Goals, Organization Goals), Expenses (Requesting Information, Rejected, Drafts Pending Submission), and Awaiting Completion (My Benefits, My Profile).
- Worklist: Notifications and Approvals:** A table listing various requests and approvals. The table has columns for Priority, Title, Status, Assigned, Assignee, Type, From, and Sent. The data includes requests for Terry Green, Samuel Nielsen, Mindy Crawford, Joe Smith, and others.
- Person Gallery:** A section for finding people, showing a search bar and a list of people in the organization. The list includes Anna Pascal, Pat Mike, Jason Blake, and Stella Harris, each with a profile card showing their name, title, and contact information.
- Activity Stream:** A section showing recent activity, including updates to profiles, connections, and photos.

Control Access to

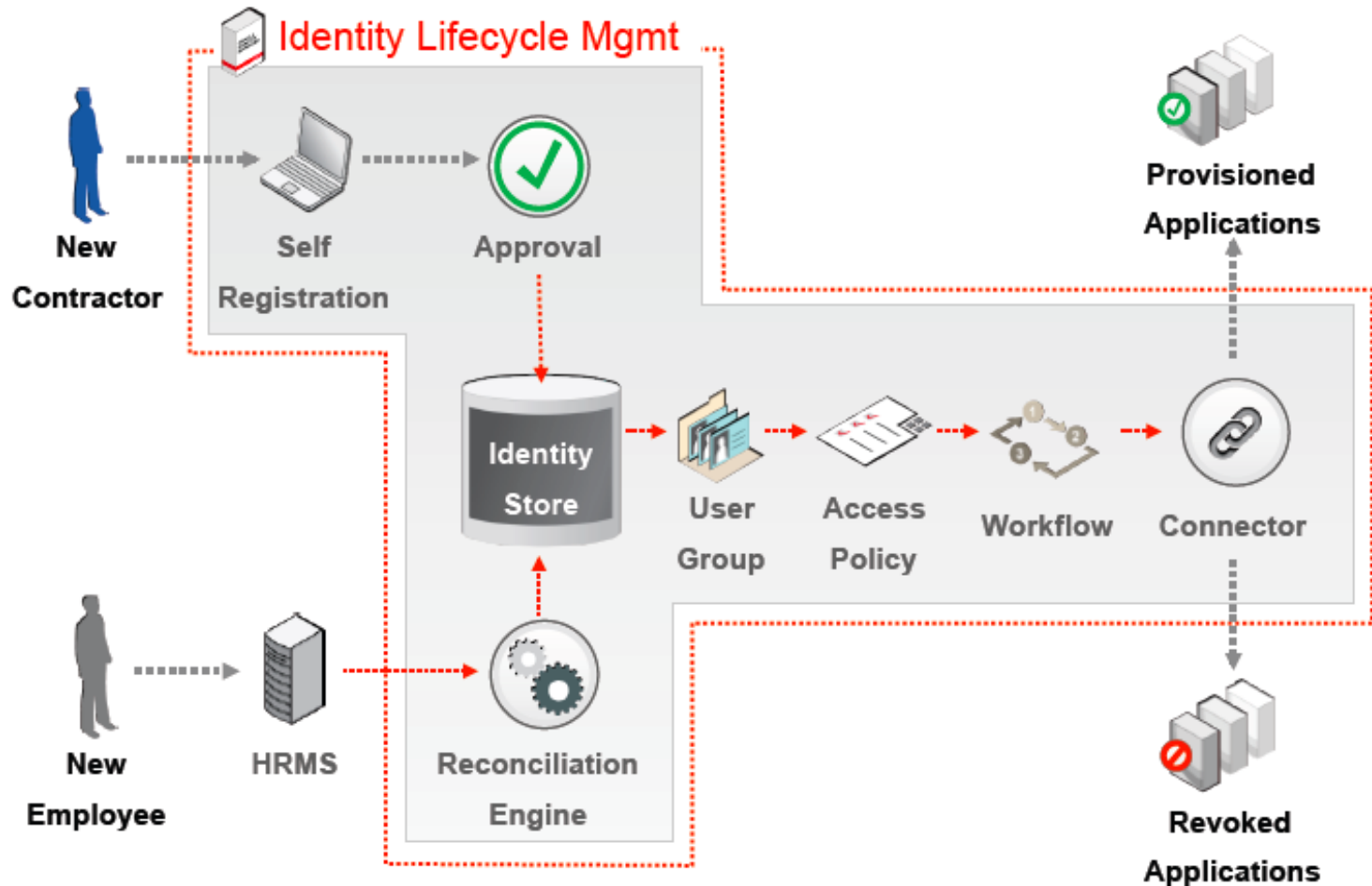
- Pages
- Tabs
- Portlets / Regions
- Tables
- Text Fields
- Buttons
- Tree Nodes
- Graphics / Charts
- Dropdowns / List Items / List of Values
- What data do you get to see (documents, in tables, charts etc)
- Data Masking
- Operations on Data (hire, promote, approve, reject)
- Backend Data & Web Service operations
- Personalization / Customization
- and more...

Change management...Where's the focus?



- How many times have you heard of an employee being paid after termination?
- How often do online credentials survive termination?
- A solution that pairs the two?...

Provisioning and Identity Administration



Keeping a watchful eye...

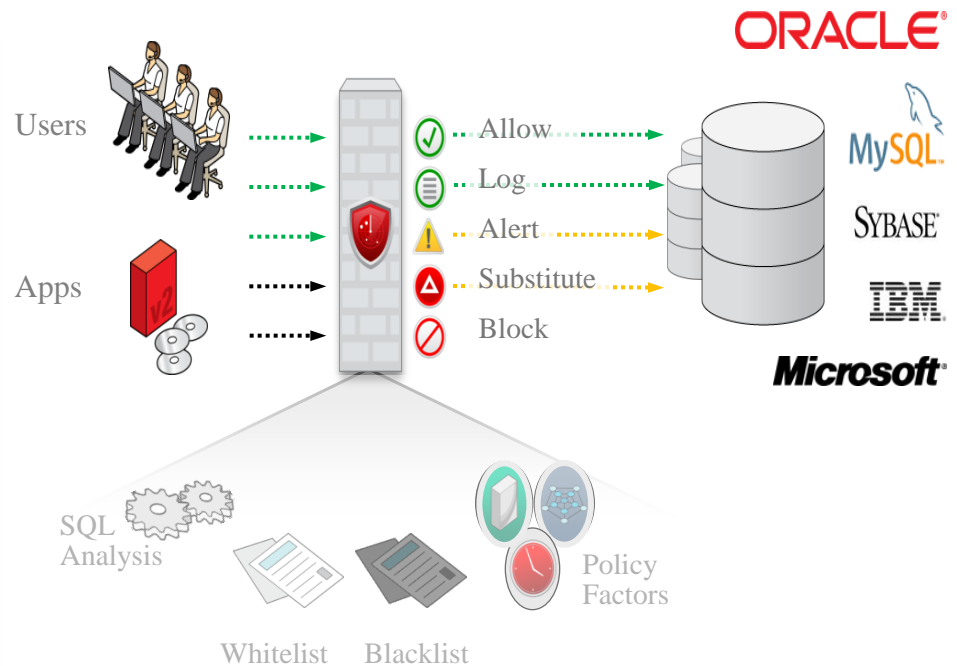


Database Activity Monitoring and Firewall

Detective Control for Databases

Oracle Audit Vault and Database Firewall

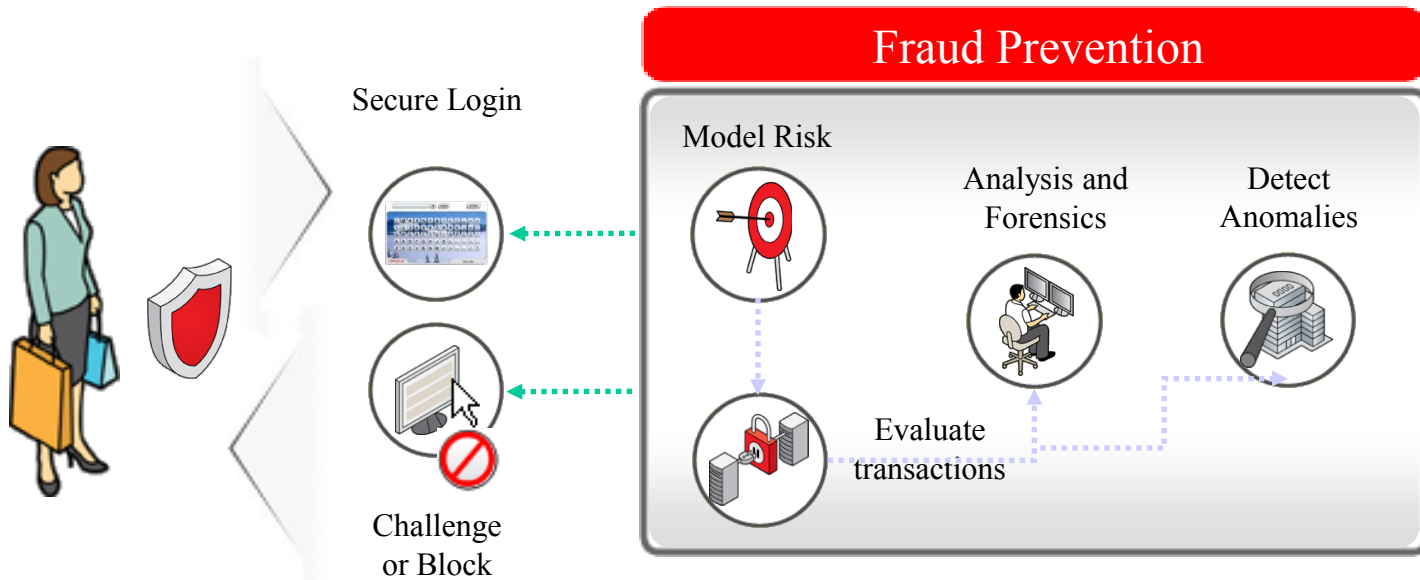
- Monitors network traffic, detect and block unauthorized activity
- Highly accurate SQL grammar analysis
- Can detect/stop SQL injection attacks
- Whitelist approach to enforce activity
- Blacklists for managing high risk activity
- Scalable secure software appliance



Risk Awareness in Context/Prevention



Risk-Aware Security



- Username and password are correct but **is this really Mary?**
- Is Mary doing **anything suspicious?**
- Can Mary answer a **challenge** if the **risk is high** enough?

Real-Time Identity Theft + Fraud Prevention



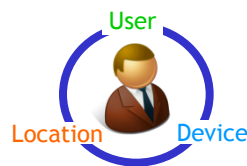
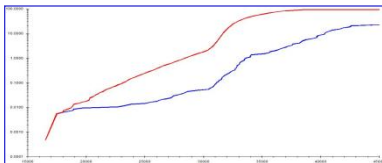
Users



Merchants



Admins



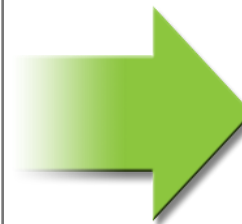
Adaptive Access Control

What A User Knows (Pin, Password, Challenge Questions)

What A User Has (Device Fingerprinting)

What a User Does (Behavior Pattern + Profiling)

Where a User Is (Geo-Location)



Portals

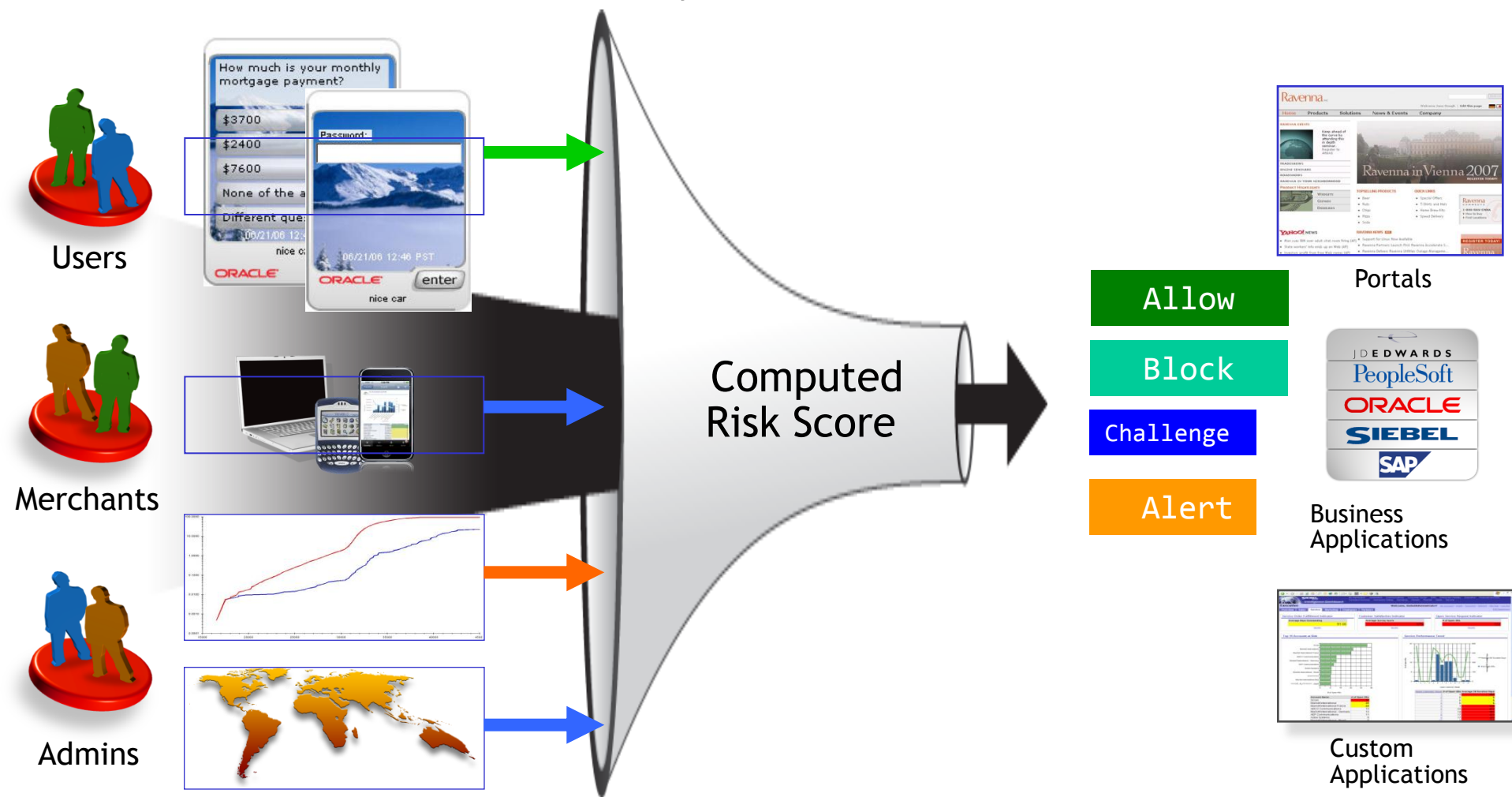


Business Applications



Custom Applications


Real-Time Identity Theft + Fraud Prevention



Fraud Investigation Tools

- Role based access
- Utility Panel
 - Filters – quick search
 - Notes – open case
- Search Transactions
- Compare Transactions

ORACLE® Oracle Adaptive Access Manager

Preferences Help Sign Out 
Signed in as invest1

Fraud

Case 402 Transaction Ret... Filtered Transa... Compare Transac...

Compare Transactions [Link to Case](#)

The table below compares transaction data values from the transaction type Retail Ecommerce.

Show Transactions | All | [Add to Group](#) | ☐ Highlight matching | [Previous](#) | [Next](#) | [Detach](#)

Transaction Data	Retail Ecommerce_403	Retail Ecommerce_404	Retail Ecommerce_405
Transaction Item	Table	lab coats	TV
Transaction Amount	50.0	42.0	975.0
Transaction Count	1.0	20.0	1.0
Credit Card			
Credit Card Number	987654322	987654322	987654322
Expiry Date	12/14	12/14	12/14
Customer			
First Name	Demo	Demo	Demo
Last Name	User001	User001	User001
Shipping Address			
Street Address Line1	123 Fake st	123 Fake st	33 Fraud Ave
City	Santa Clara	Santa Clara	Crime City
State	CA	CA	VZ
Country	USA	USA	China
Zip	97543	97543	123456

Filters: 3

Filter Type	Value
<input type="checkbox"/> Device ID	103
<input type="checkbox"/> IP Address	25.68.75.255
<input checked="" type="checkbox"/> Credit Card.Credit Ca	987654322

Time Range: Any

[Find](#) [Clear](#)

Matching Items Found
5 Sessions , 5 Transactions

Notes: Case_402 [Close](#)

4/4/2012 9:50 AM By invest1:
Filter Items: [Device ID: 103, Credit Card.Credit Card Number: 987654322]
notes

4/4/2012 9:41 AM By invest1:
notes

[Save](#) [Insert Filters](#)

Government Challenges

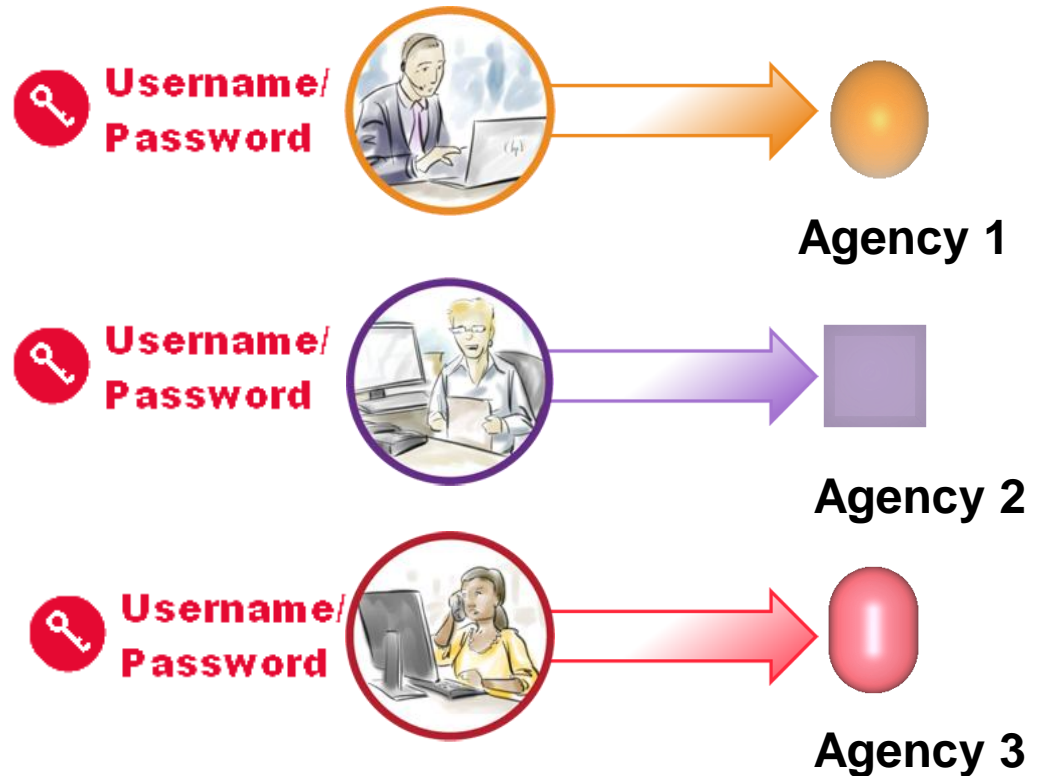


Current Situation

The Citizen View



- Multiple logins
- Duplication of data
- Lack of government coordination.



Identity, Credentials and Access Management Model

