Integration
developer news

Architecting the
Intelligent Enterprise

Expert Voices

Cathy Lippert
Director of Product Management
Oracle SOA Governance

ORACLE

ORACLE®

Policing the Cloud

Cathy Lippert, Director Product Management SOA Governance

Top of Mind for Cloud / Inter-Enterprise
Oracle SOA Governance Customer Advisory Board 2010-11 Survey

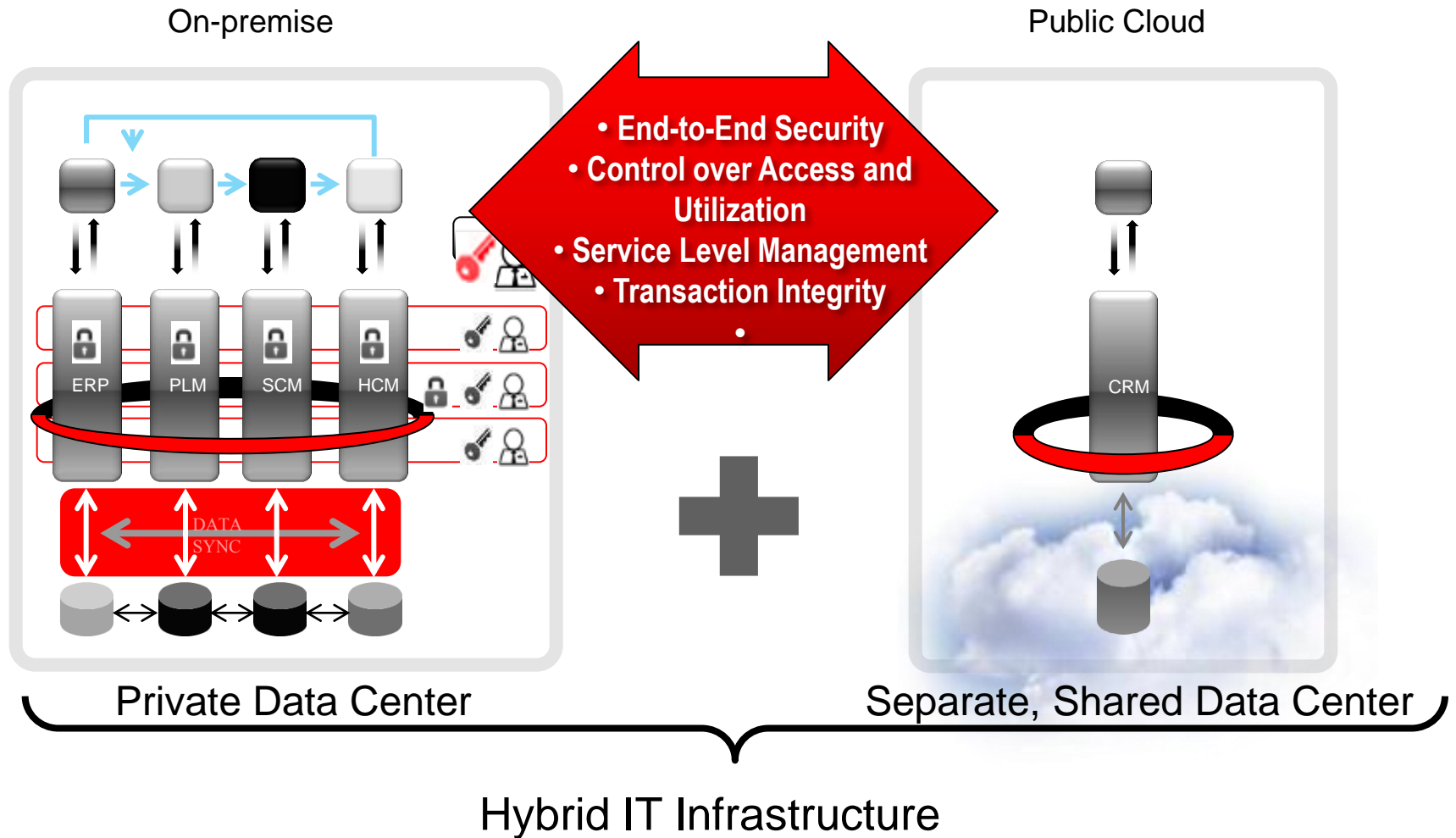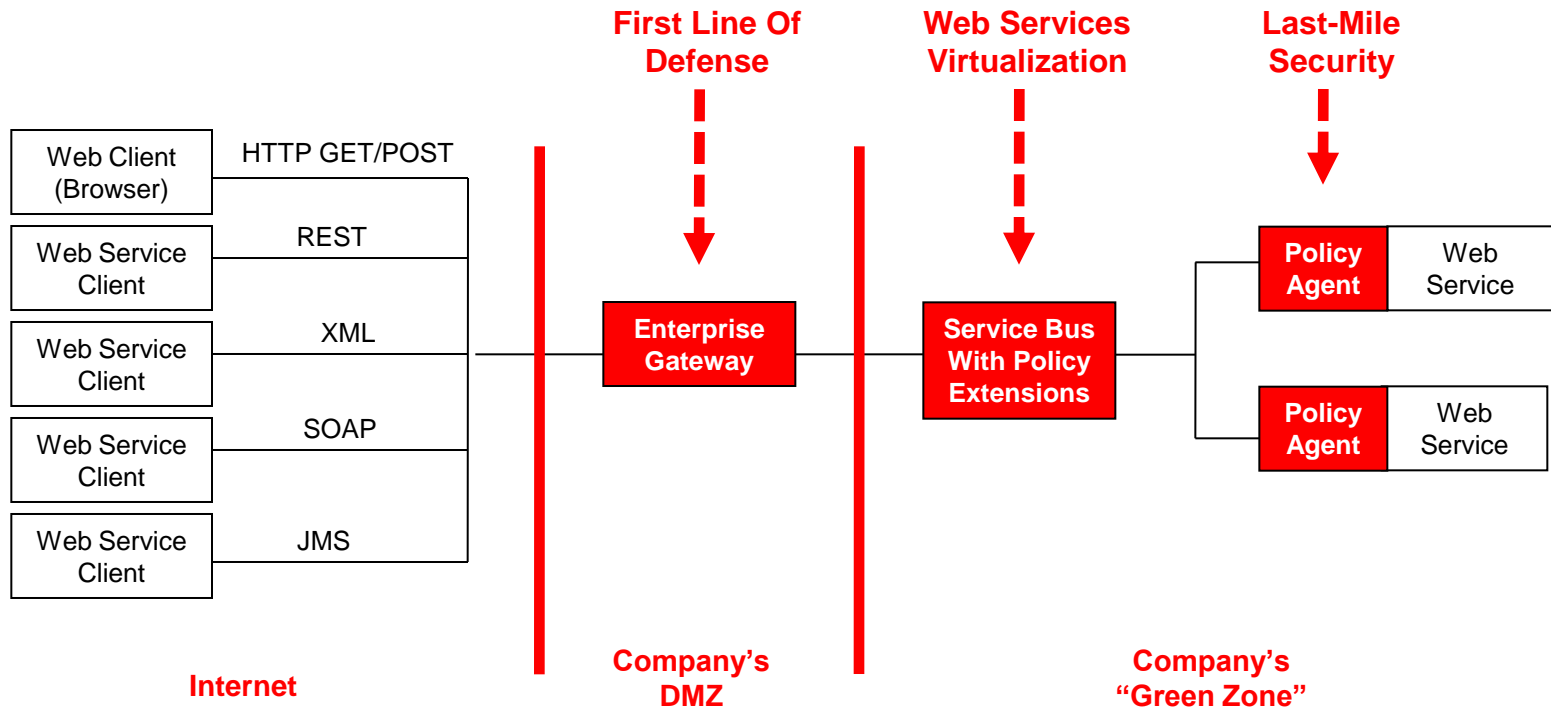| Please characterize your interest in Governance for cloud or B2B computing	
Managing the integrity of transactions across organizational boundaries	83%
Meeting service levels for clients	81%
Managing security across organizational boundaries	81%
Controlling access to and utilization of external resources	83%

ORACLE®

Common Hybrid Infrastructure
Blend of Private and Shared, Public Data Centers

On-premise

Public Cloud

- **End-to-End Security**
- **Control over Access and Utilization**
- **Service Level Management**
- **Transaction Integrity**
-

ERP   PLM   SCM   HCM

DATA SYNC

CRM

Private Data Center

Separate, Shared Data Center

Hybrid IT Infrastructure

ORACLE®

End-to-End Security

First Line Of Defense

Web Services Virtualization

Last-Mile Security

Web Client (Browser)	HTTP GET/POST
Web Service Client	REST
Web Service Client	XML
Web Service Client	SOAP
Web Service Client	JMS

Enterprise Gateway

Service Bus With Policy Extensions

| **Policy Agent** | Web Service |
| **Policy Agent** | Web Service |

Internet

Company's DMZ

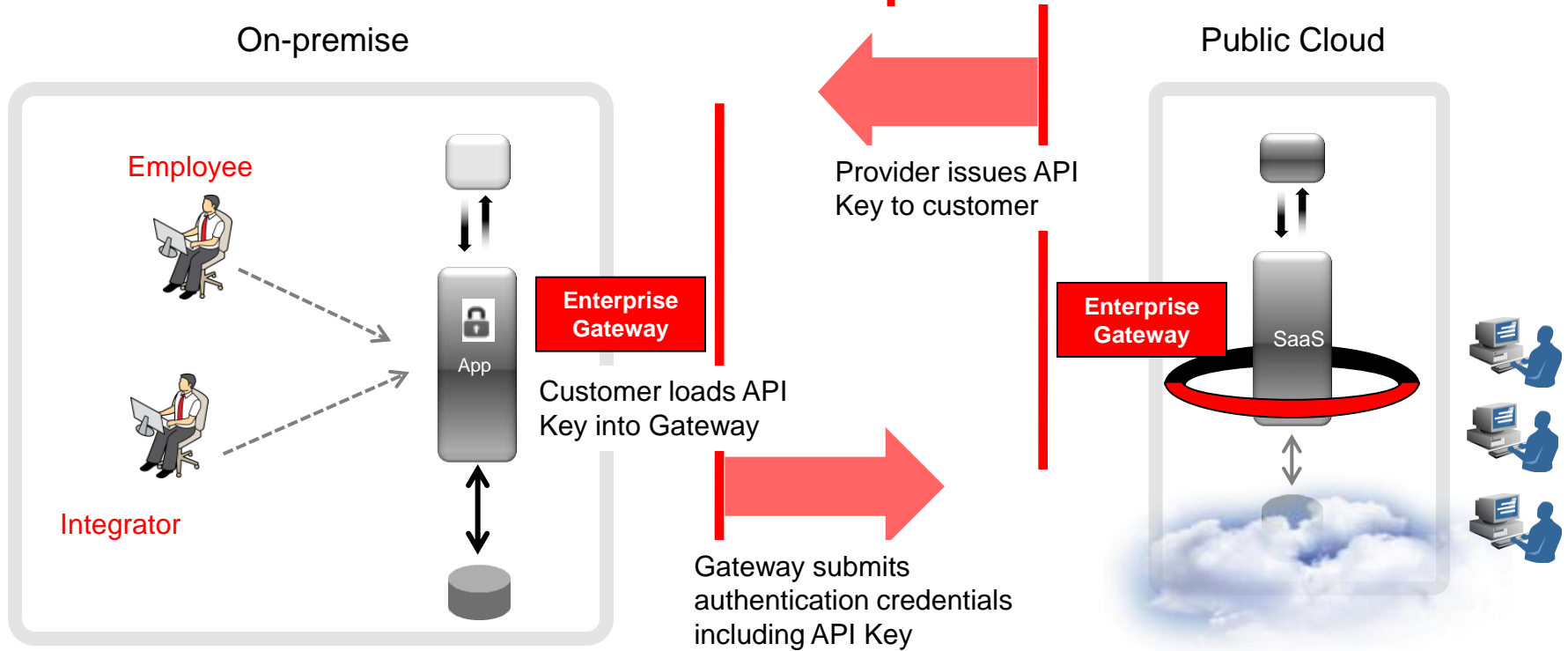**Company's "Green Zone"**

ORACLE®

5

First Line of Defense
XML Firewalling Against Attacks

- XML content attacks
  - Checking for XML well-formedness; XML document size; XPath and XQuery injection; SQL injection; XML encapsulation; XML viruses
  - Scanning outgoing messages for sensitive content based on metadata or regular expression patterns
  - Detecting XML bombs and XML clogging
  - Scanning WSDL files

- XML schema and DTD attacks
  - Checking for schema and DTD validation
- Cryptographic attacks
  - Public Keys
  - Replay
- SOAP attacks
  - SOAP operation filtering
  - Checking for rogue SOAP attachments (e.g., viruses)
- Communication attacks
  - HTTP header and query string analysis
  - IP address filtering
  - Traffic throttling

ORACLE

End-to-End Security
Authentication Across Enterprise Boundaries

On-premise

Public Cloud

Employee

Integrator

Enterprise Gateway

App

Provider issues API Key to customer

Enterprise Gateway

SaaS

Customer loads API Key into Gateway

Gateway submits authentication credentials including API Key

Customers use Cloud services
- Gateway applies outbound security required to access services
- If request must be signed, Gateway does the signing

Providers offer Cloud services
- Gateway provides inbound security for provider's services
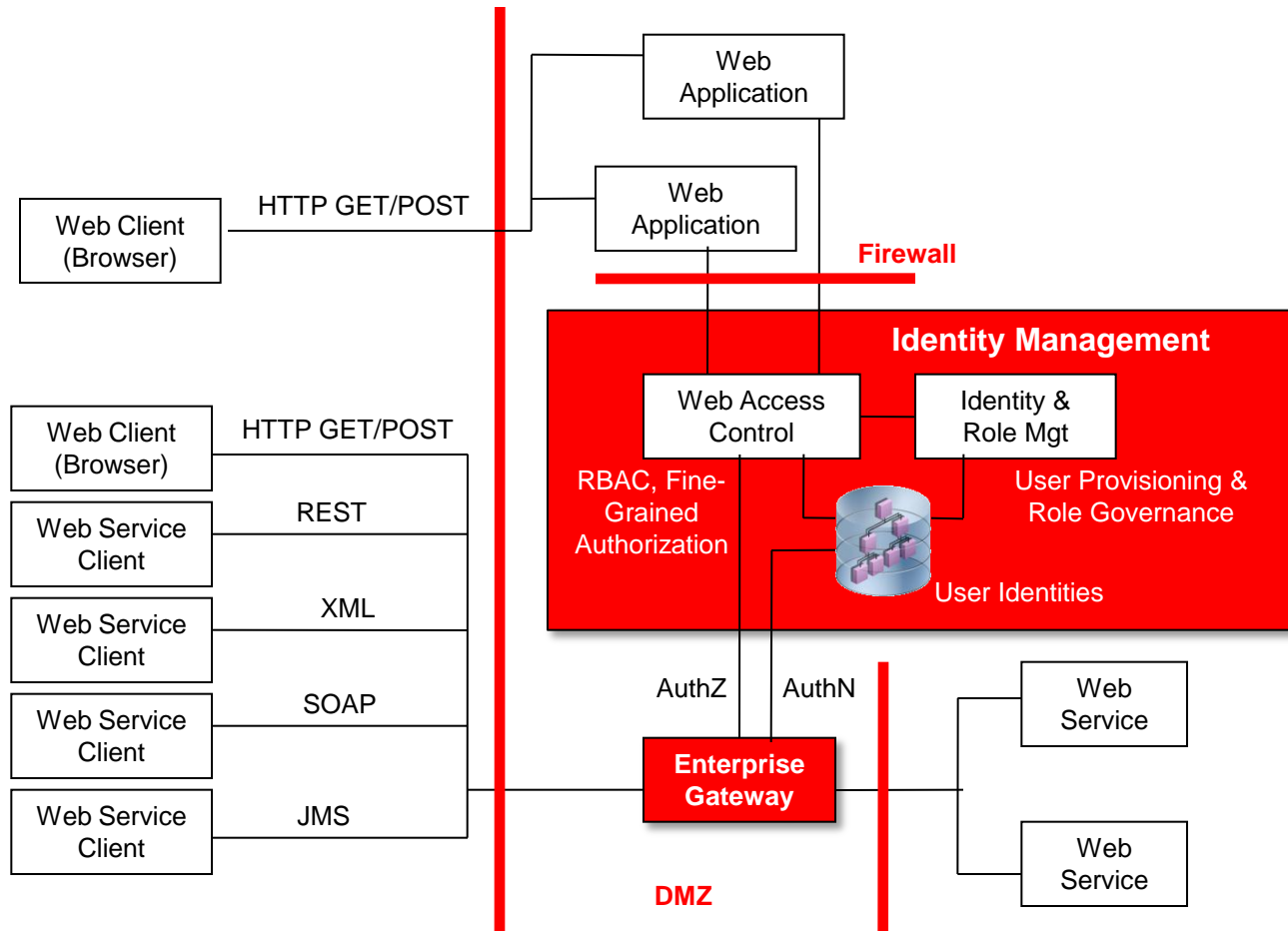
ORACLE®

Access to Cloud Services
Enterprise Gateway Connectors

- Configure Enterprise Gateway to connect to Cloud services
  - Salesforce.com using a combination of a password and pre-shared key for authentication
  - Amazon Web Services doing HMAC signature over the request
  - Providers like Terremark using the vCloud API (through HTTP Authentication)
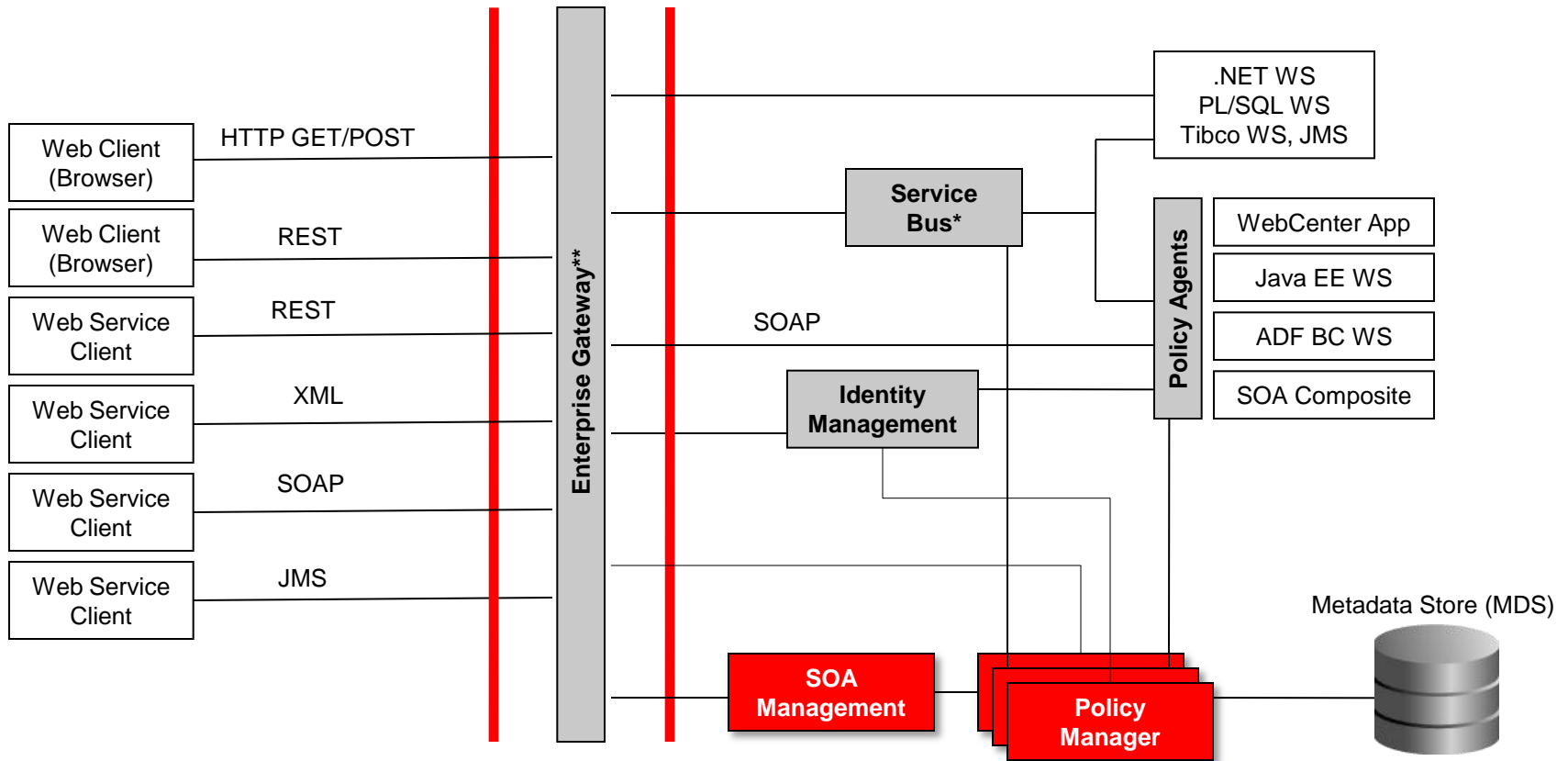
End-to-End Security
Identity Management and Propagation

Web Application

Web Client (Browser) — HTTP GET/POST — Web Application

Firewall

Identity Management

Web Access Control

Identity & Role Mgt

RBAC, Fine-Grained Authorization

User Provisioning & Role Governance

User Identities

Web Client (Browser) — HTTP GET/POST

Web Service Client — REST

Web Service Client — XML

Web Service Client — SOAP

Web Service Client — JMS

AuthZ   AuthN

Enterprise Gateway

Web Service

Web Service

DMZ

Control Access and Utilization
Apply Policy for Security & Service Levels

Web Client (Browser) — HTTP GET/POST
Web Client (Browser) — REST
Web Service Client — REST
Web Service Client — XML
Web Service Client — SOAP
Web Service Client — JMS

Enterprise Gateway**

Service Bus*

SOAP

Identity Management

.NET WS
PL/SQL WS
Tibco WS, JMS

Policy Agents

WebCenter App
Java EE WS
ADF BC WS
SOA Composite

SOA Management

Policy Manager

Metadata Store (MDS)

Unified policy model from the request to endpoint

* Service Bus can be used with or without Policy Manager integration
** Enterprise Gateway may optionally use same policies as Service Bus and Policy Agents

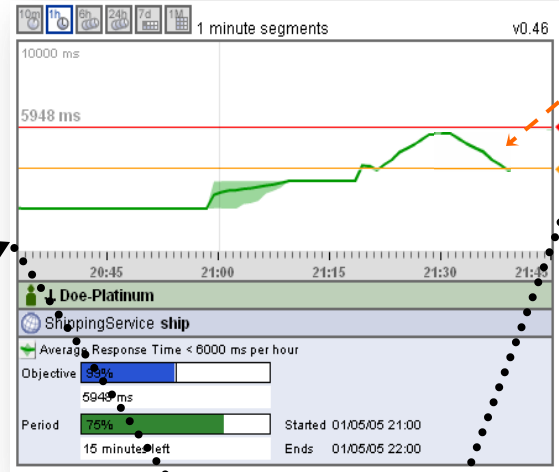**ORACLE**

10

Meet Service Levels
Client-Based SLA Alarms

(1) **Service Level Agreement**

Service Level Objective (SLO)
For Platinum customers:
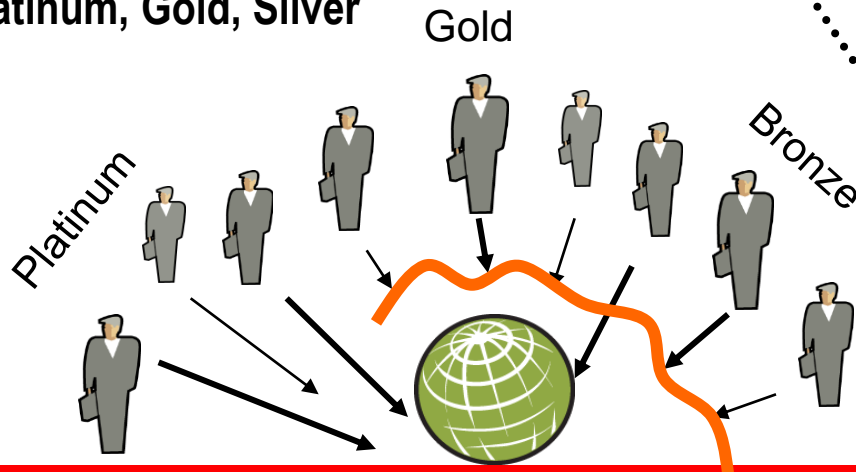- Ave. Response time per hour < 6 sec
  - Warning threshold <= 4 sec
    - Action: alerts

(2) **Usage tracked and segmented – e.g. by Platinum, Gold, Silver**

Gold

Bronze

Platinum

(3) **Performance against objectives**

10000 ms
5948 ms
1 minute segments   v0.46
20:45   21:00   21:15   21:30   21:4
Doe-Platinum
ShippingService ship
Average Response Time < 6000 ms per hour
Objective   5948 ms
Period   75%   Started 01/05/05 21:00
15 minutes left   Ends   01/05/05 22:00

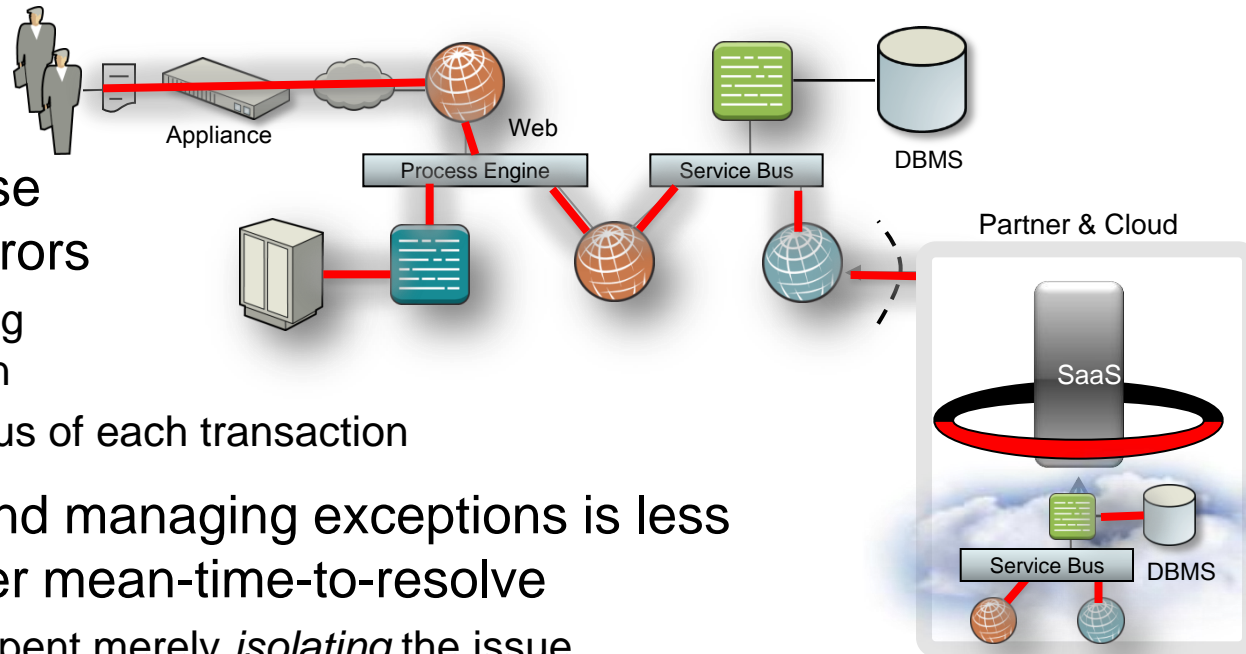**(5)** **Stabilized response times for Platinum customers**

(4) **Automatically triggers alerts _before_ compliance failure for Platinum customers**

ORACLE

12

Transaction Integrity
Across Enterprise and Cloud

Appliance   Web   DBMS
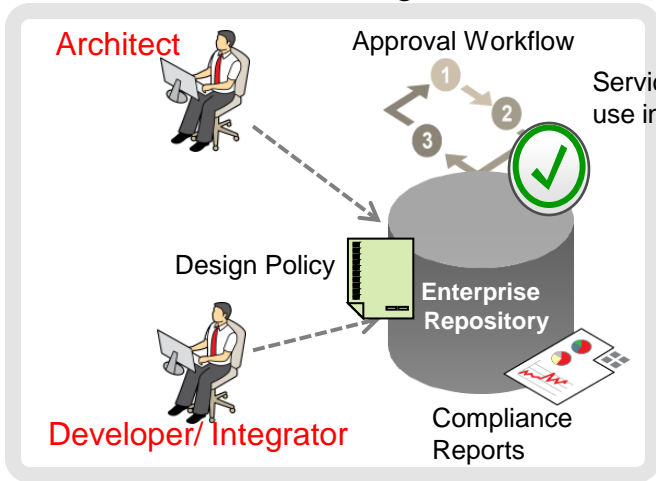
Process Engine   Service Bus

Partner & Cloud

SaaS

Service Bus   DBMS

- Transactions no longer vanish because of delays, failures, errors
  - Monitoring and alerting before users complain
  - Single source for status of each transaction

- Problem diagnosis and managing exceptions is less laborious, with shorter mean-time-to-resolve
  - Averts 80% of effort spent merely *isolating* the issue
  - No longer a manual effort based on log mining
  - Fewer developer resources diverted to IT fire-drills

- Business transaction context (not just system-centric monitoring)
  - Includes critical business context (Customer name, order size, part numbers)
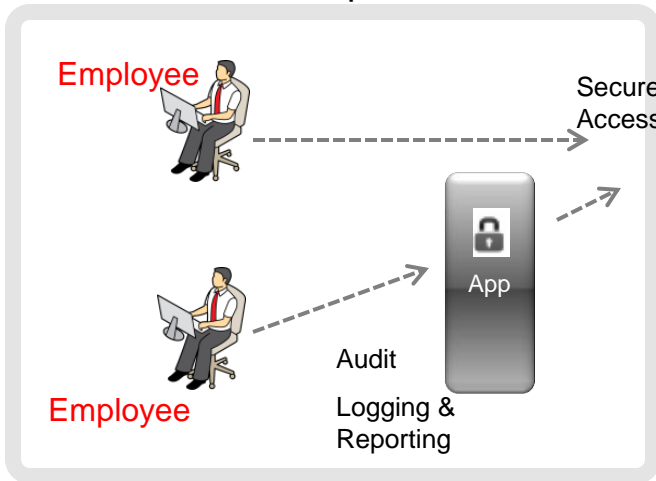 - Captures a range of *business*-oriented errors & faults
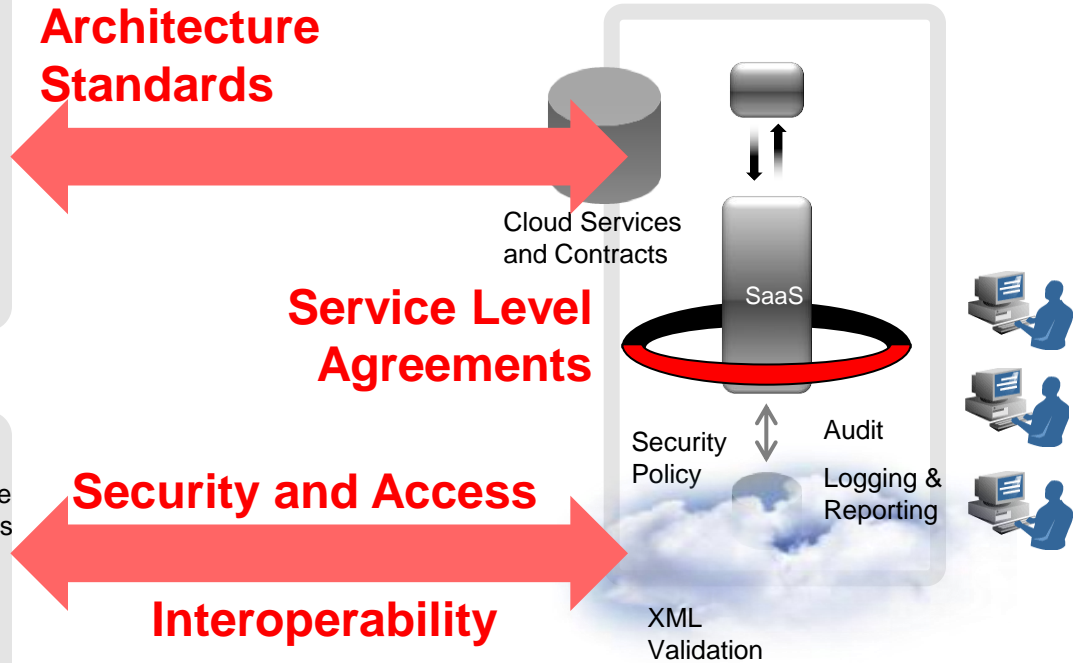
ORACLE

Compliance in the Cloud

On-Premise: Design time

Architect

Approval Workflow

Service approved for use in this Organization

Design Policy

Enterprise Repository

Developer/ Integrator

Compliance Reports

Architecture Standards

Public Cloud

Cloud Services and Contracts

SaaS

Service Level Agreements

Security Policy

Audit

Logging & Reporting

On-Premise: Operations

Employee

Secure Access

App

Audit

Logging & Reporting

Employee

Security and Access

Interoperability

XML Validation

Corporate & Regulatory Compliance

• Payment Card Industry Data Security Standards (PCI DSS)
• Statement on Auditing Standards 70: Service Organizations (SAS 70) per Auditing Standards Board of the AICPA.
• Health Insurance Portability and Accountability Act (HIPAA.)

Governing SOA in the Cloud
Farmers Insurance Group Challenges Similar to Shared Services

Key Capabilities & Requirements		Shared Services	Cloud Computing
Platform Considerations			
Multi-tenant architecture	Infrastructure	Yes	Yes
	Middleware	Yes	Yes
	Services	Yes	Yes
	Processes	No	Yes
Abstracted / virtualized shared platform		Yes	Yes
Self-Service control panel		No	Yes
On-demand scaling		No	Yes
Visibility and Control Considerations			
Security		**Yes**	**Yes**
On-demand provisioning		**No**	**Yes**
IT service catalog		**Yes**	**Yes**
IT service management		**Yes**	**Yes**
Lifecycle Management		**Yes**	**Yes**
Standardization		**Yes**	**Yes**
Governance and Compliance		**Yes**	**Yes**
Business Considerations			
Financial Management	Metering	Yes	Yes
	Billing	Yes	Yes

15

ORACLE®

Oracle Fusion Middleware
For Policing the Cloud

Oracle SOA Governance	
Oracle Enterprise Gateway	XML Gateway for Perimeter Security; Connections to Cloud
Oracle Web Services Manager	Security Policy Management; Policy Agents for Endpoints
Oracle Identity Management	User Provisioning; Authentication; Authorization and Fine-Grained Entitlements; Role Management
Oracle Enterprise Manager	Service Level Management & Diagnostics; Business Transaction Management; Monitoring & Reporting by Client
Oracle Enterprise Repository and Service Registry	Catalog of IT Services and Contracts; Governance Workflow; Reuse Analytics; Design/Architecture Compliance

ORACLE®

Next Steps

1. Explore Oracle's Web Sites

www.oracle.com/soa
http://bit.ly/soagov
http://bit.ly/OEGateway

2. Run Oracle SOA on the Cloud

Amazon EC2:
http://snipurl.com/soa-ec2

3. Attend an Upcoming SOA "Eat & Learn" Event

Oracle Event Site
www.oracle.com/events

4. Oracle SOA Governance Resource Kit – Whitepapers, Datasheets, Demos, etc.

http://bit.ly/soagovkit

5. Join Oracle SOA communities:

twitter.com/OracleSOA

facebook.com/OracleSOA

"Oracle SOA" Group

Blog – blogs.oracle.com/governance

ORACLE