Alessandro Faustini

IBM dissipa la nebbia sul cloud computing

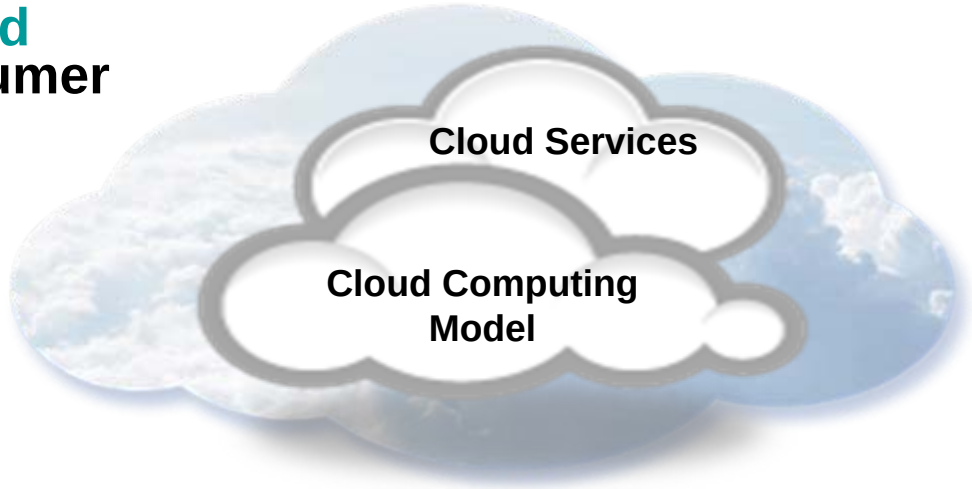
Nuovi modelli tecnologici per la sicurezza IT

Security Day 2010

- Security: Grand Challenge for the Adoption of Cloud Computing
- Cloud Security = SOA Security + Secure Virtualized Runtime
- Access Entitlement request in the new delivery model

Cloud: Consumption & Delivery Models Optimized by Workload

"Cloud" is a new consumption and delivery model inspired by consumer Internet services.



Cloud enables:

- Self-service
- Sourcing options
- Economies-of-scale

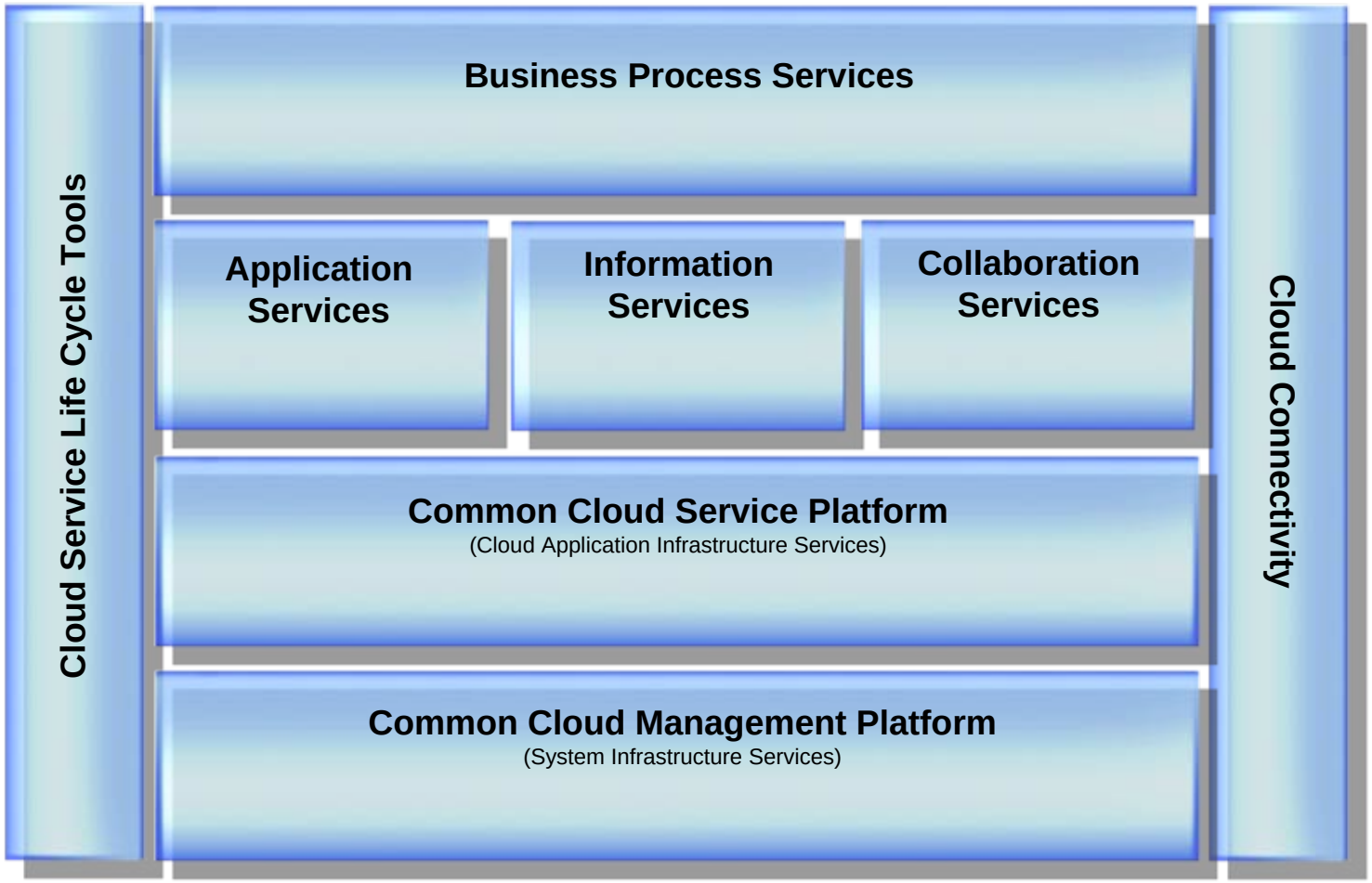
"Cloud" represents:

- The Industrialization of Delivery for IT supported Services

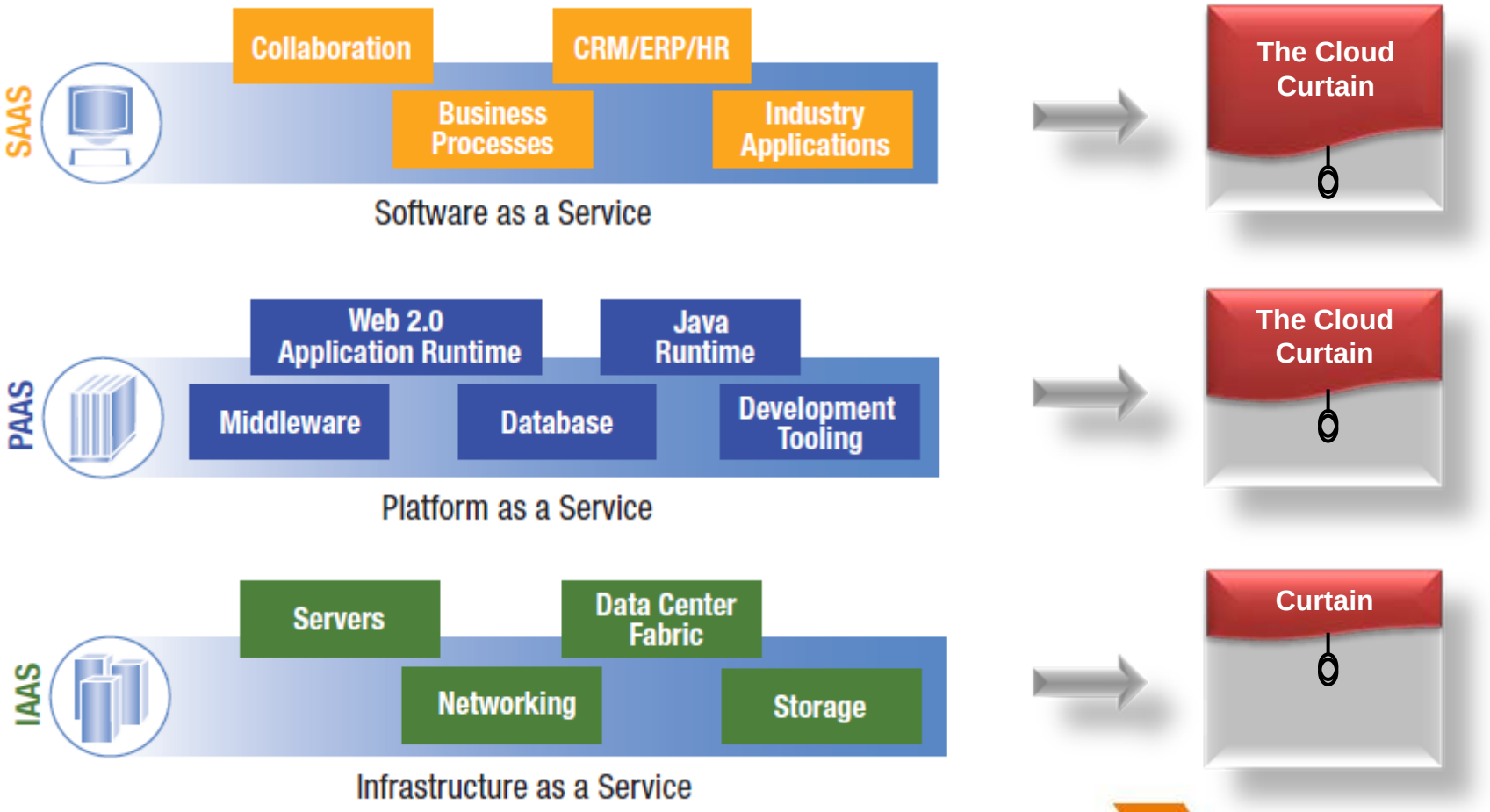
Multiple Types of Clouds will co-exist:

- Private, Public and Hybrid
- Workload and / or Programming Model Specific

Cloud Platforms and Services



Cloud Model Applies at all Levels of the IT Stack – Resulting in Different Security Requirements, Different Responsibilities



Traditional Computing = Physical Separation

Virtualization = Shared Building

Cloud Computing = Shared public infrastructure

What is Cloud Security?

Confidentiality, integrity, availability of business-critical IT assets Stored or processed on a cloud computing platform

There is nothing new under the sun
but there are lots of old things we don't know.
Ambrose Bierce, The Devil's Dictionary

Cloud Security = SOA Security + Secure Virtualized Runtime

Service Oriented Architecture

- *Application / Software as a Service*
- *Platform as a Service*
- *Infrastructure as a Service*
- *Identity & Security as a Service*

- Secure integration with existing enterprise security infrastructure
- Federated identity / identity as a service
- Authorization, entitlements
- Log, audit and compliance reporting
- Intrusion prevention

Secure Runtime for Virtual Images and Virtual Storage

- *Business Support Services*
- *Operational Support Services*
- *Virtualized Resources*
- *System Resources*
- *Physical System / Environment*

- Process isolation, data segregation
- Control of privileged user access
- Provisioning w/ security and location constraints
- Image provenance, image & VM integrity
- Multi-tenant security services (identity, compliance reporting, etc.)
- Multi-tenant intrusion prevention
- Consistency top-to-bottom

Policy aligns individual areas of expertise with common business objectives

Who cares about security policies?

- Corporate Office: They capture policy as business statements.
  - –e.g. Restrict access to customer PII data

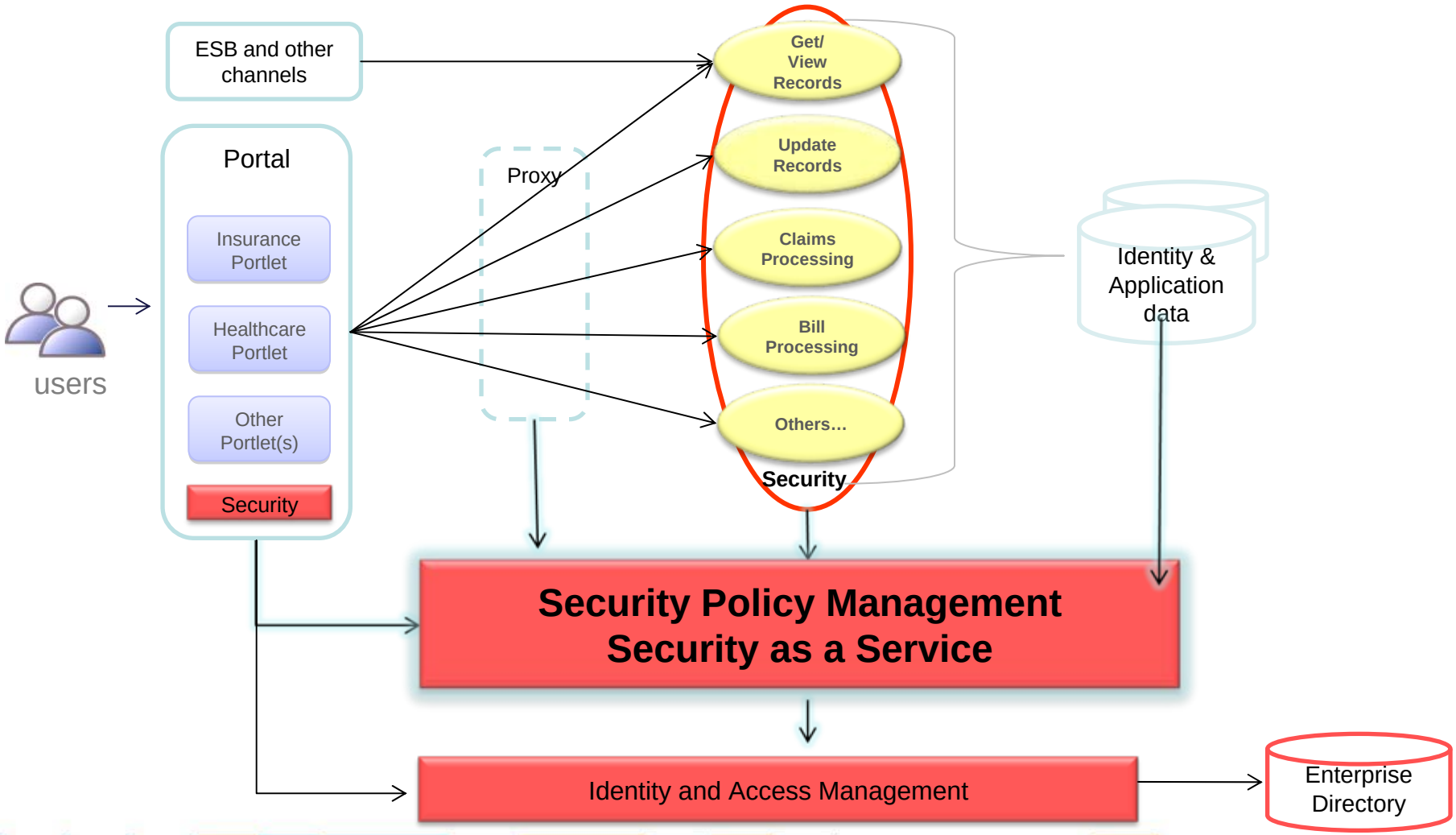
- Application owners: They capture policy as entitlements
  - –e.g. Developers building application logic based on entitlements

- IT/Security Operations: They capture policy as configurations settings
  - –Administrators needing to enforce operational policies, such as a WS-Security policy

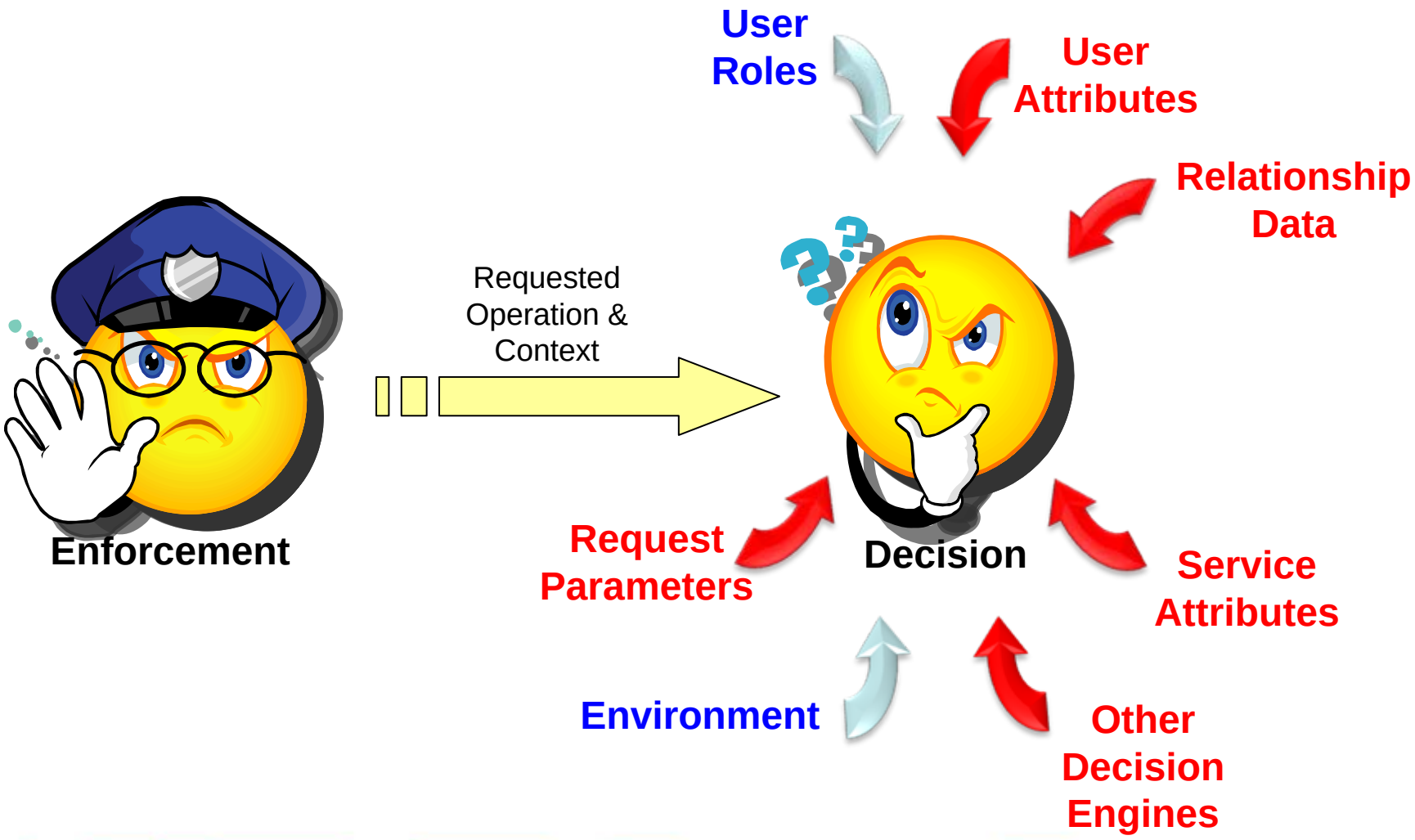
What kinds of policies affect a service oriented environment?

- Described in terms of “domains” helps focus and tie policies back to the business objectives and people who care about them
- Examples include:
  - Message Protection Policies:
    Messages need to ensure integrity and confidentiality
  - Authorization Policies:
    Who can access what? When and under what conditions?

Evolution of Policy Management



Role-Based Access Control is Not Sufficient

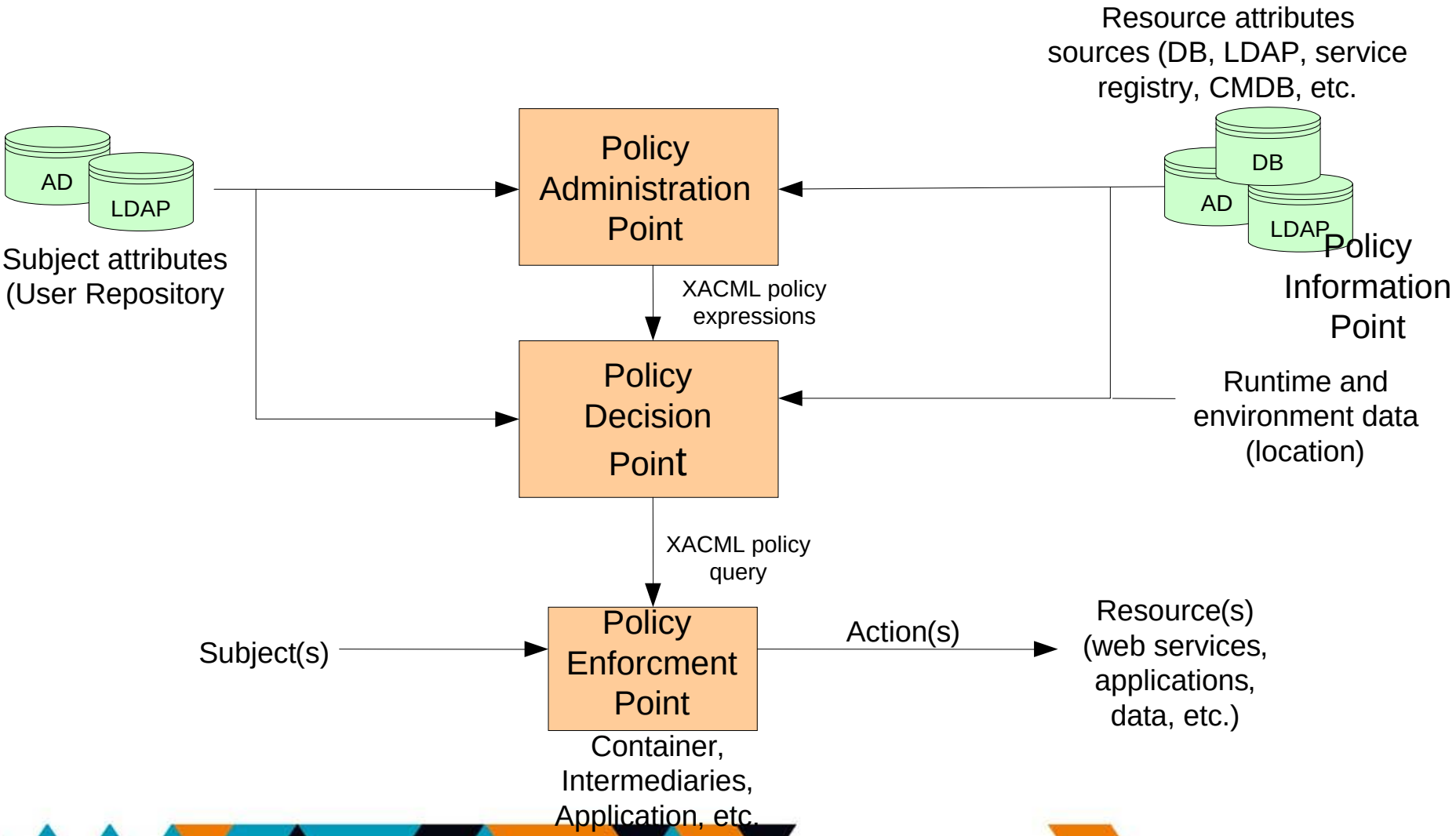


Example – Approval for a Funds transfer

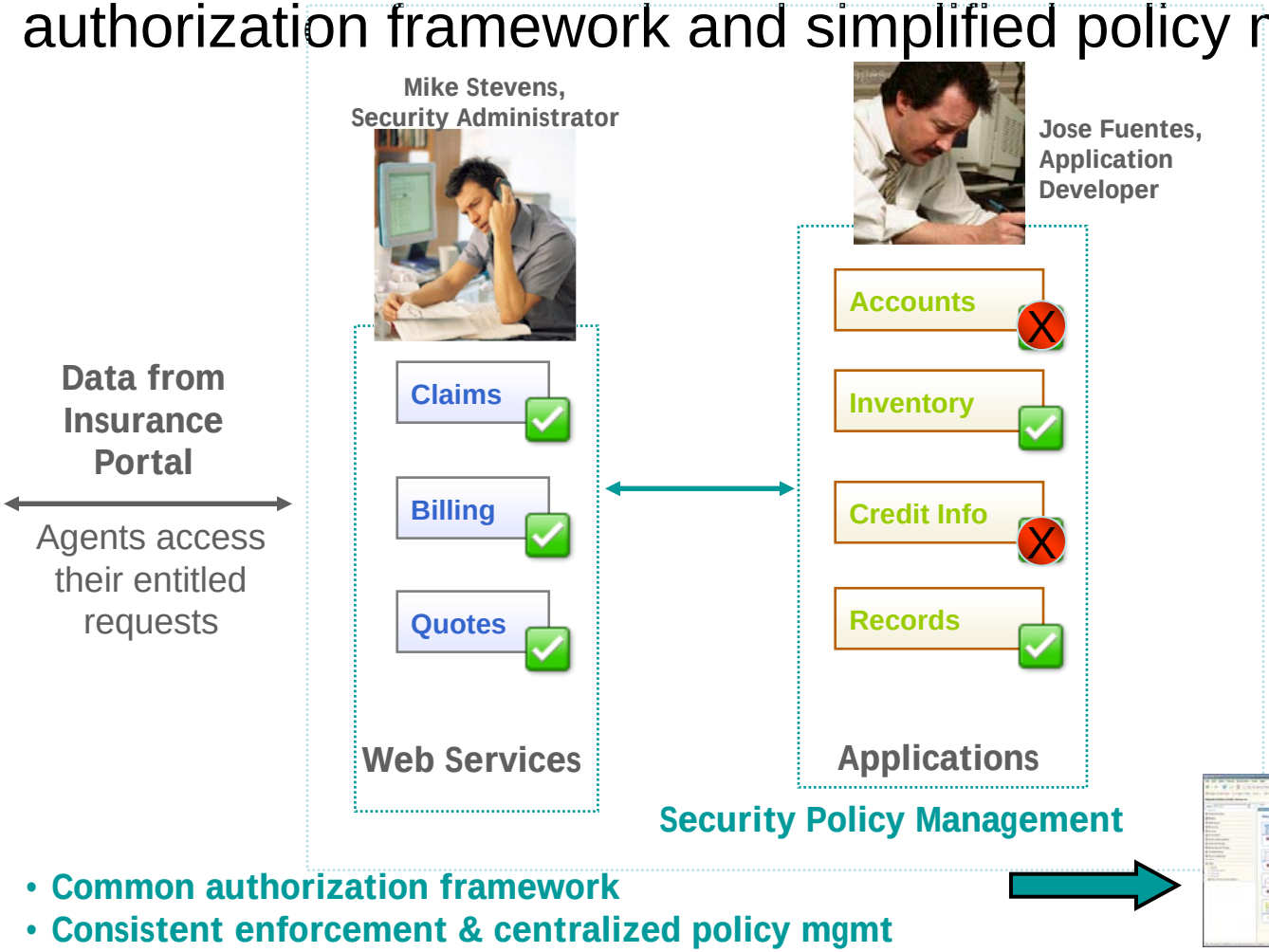
Example: Policy to approve a funds transfer:

- **Role**
  - The user must be in the `tfr_approver` role
- **Service attribute**
  - The transfer amount must be less than the maximum transfer limit for the type of transfer
- **User attribute**
  - The transfer amount must be less than the maximum transfer limit for the user
- **Relationship**
  - The user must have been assigned responsibility for the source account.
- **Environment**
  - The transfer must be made during business hours and from the corporate network
- **Request/Session Context**
  - The user must have authenticated using 2-factor authentication
- **Other Decision Engines**
  - The transaction must pass the criteria checked by the Fraud Detection system

Ability to deliver end-to-end authorization



Tivoli Security Policy Manager offers a common authorization framework and simplified policy management



Mike authors policies for who can access what records and accounts;

Jose externalizes access control decisions from his application and uses an authorization service

Using security policy management Jose is able to decrease his workload and still implement specific entitlement

- **Common authorization framework**
- **Consistent enforcement & centralized policy mgmt**
- **Improved administration and developer experience**

= Authorization

Thank you!