

Identity Management from the Enterprise Perspective

Wednesday, 12/5 10:15am-11:30am

Description: Enterprise IdM often requires that organizations correlate multiple user accounts to a single person; manage accounts across many, often heterogeneous platforms; and create appropriate workflows to address multiple approvals and notifications. Learn techniques to introduce efficiency and stability, and improve security, through best IdM practices here.

 **OpenNetwork**[®]

Agenda



- Managing identity in a heterogeneous world –The Enterprise Perspective
- Organizational factors
- Automation through IdM Platform
- Sample Architectures
- Selection & Deployment Considerations

Agenda



- Managing identity in a heterogeneous world –The Enterprise Perspective
- Organizational factors
- Automation through IdM Platform
- Sample Architectures
- Selection & Deployment Considerations

Why Identity Management?

**Spends 1/3 of his day
resetting passwords**

**Has 7 passwords across
11 applications.**

**Has 34 requests for new user
accounts buried in a stack of
papers on his desk.**



**Terminated 4 months ago.
Just pulled all the customer
data from your CRM system.**

**Hired last week. Still waiting for
access to company systems.**

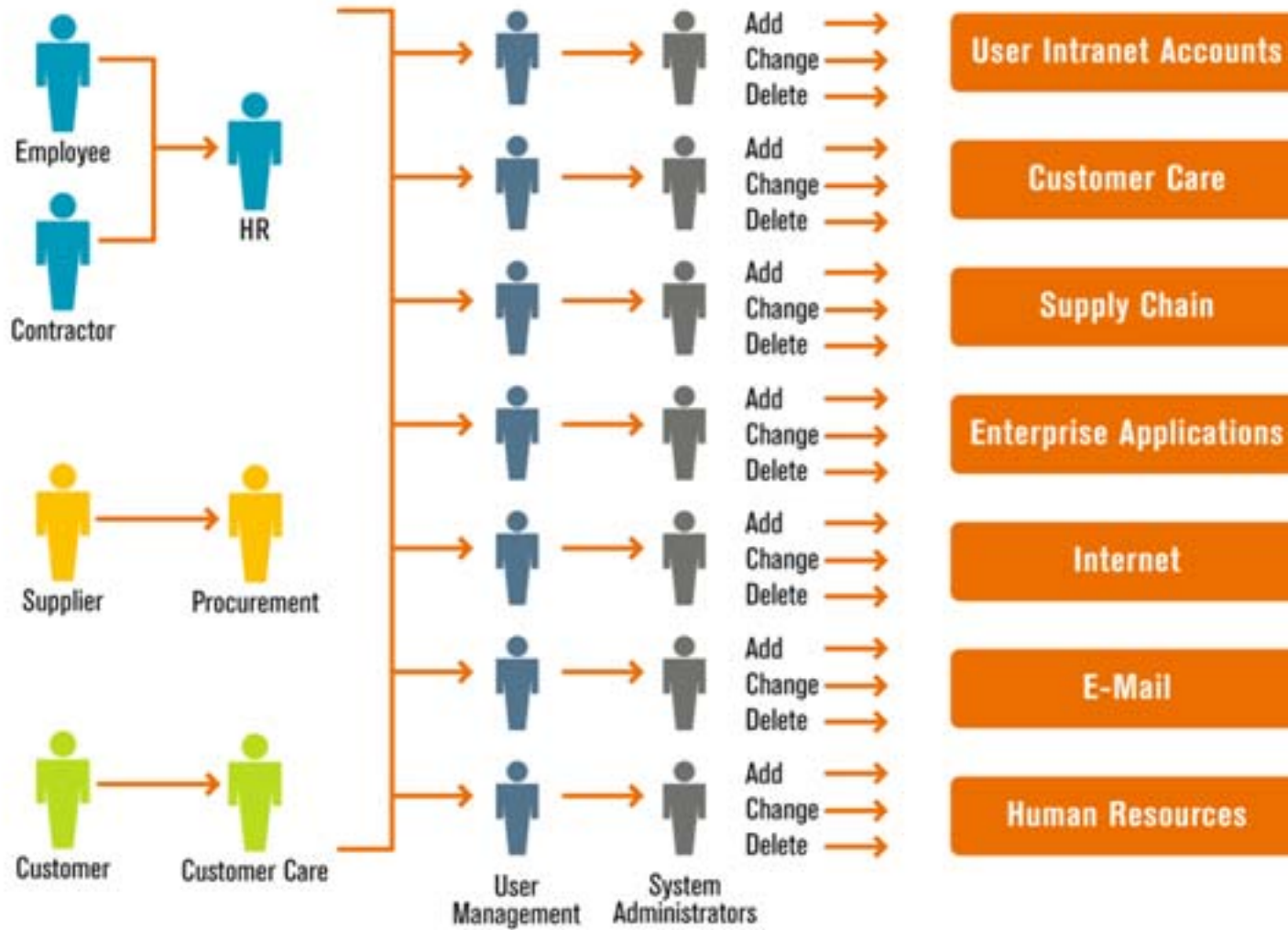
The Challenge

- ▶ Many users and applications
- ▶ Heterogeneous platforms
- ▶ Duplicate administrative interfaces
- ▶ Manual processes

Resulting in:

- *IT burden*
- *Inconsistent information*
- *Security risk*
- *Difficulty generating comprehensive audits and reports*
- *High support costs*
- *Productivity losses*

The Challenge



Identity and Access Management Drivers and Examples



Security

- 30% of users do not have access removed when they leave a company.

Efficiency

- 45% of help desk calls are for password reset.
- The elapsed time for new user provisioning is 6-29 hours.

Control

- On average, large enterprises have as many as 75 applications, databases and systems.

Accountability

- 48% of survey respondents were unsure of their readiness for Sarbanes-Oxley compliance.

Identity and Access Management Drivers and Examples



Security

- Avoid average losses of over \$2 million**

Efficiency

- Reduced help desk costs: \$75 per user per year*
- Quicker access to applications: \$1,000 per new employee, \$350 per year per existing employee*

Control

- Improved data management – \$350 per user per year*

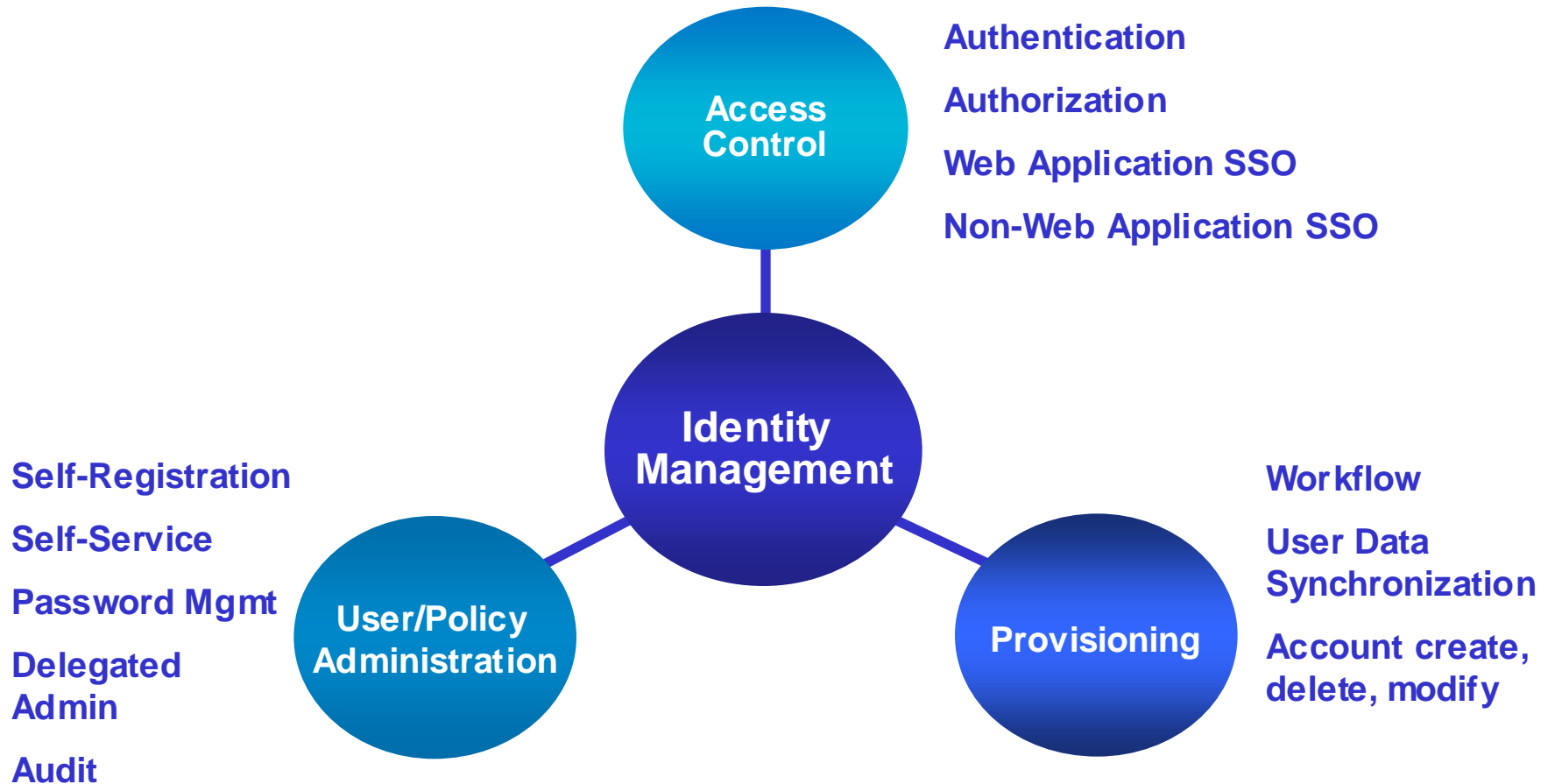
Accountability

- Audit savings: \$4,000 per security audit*

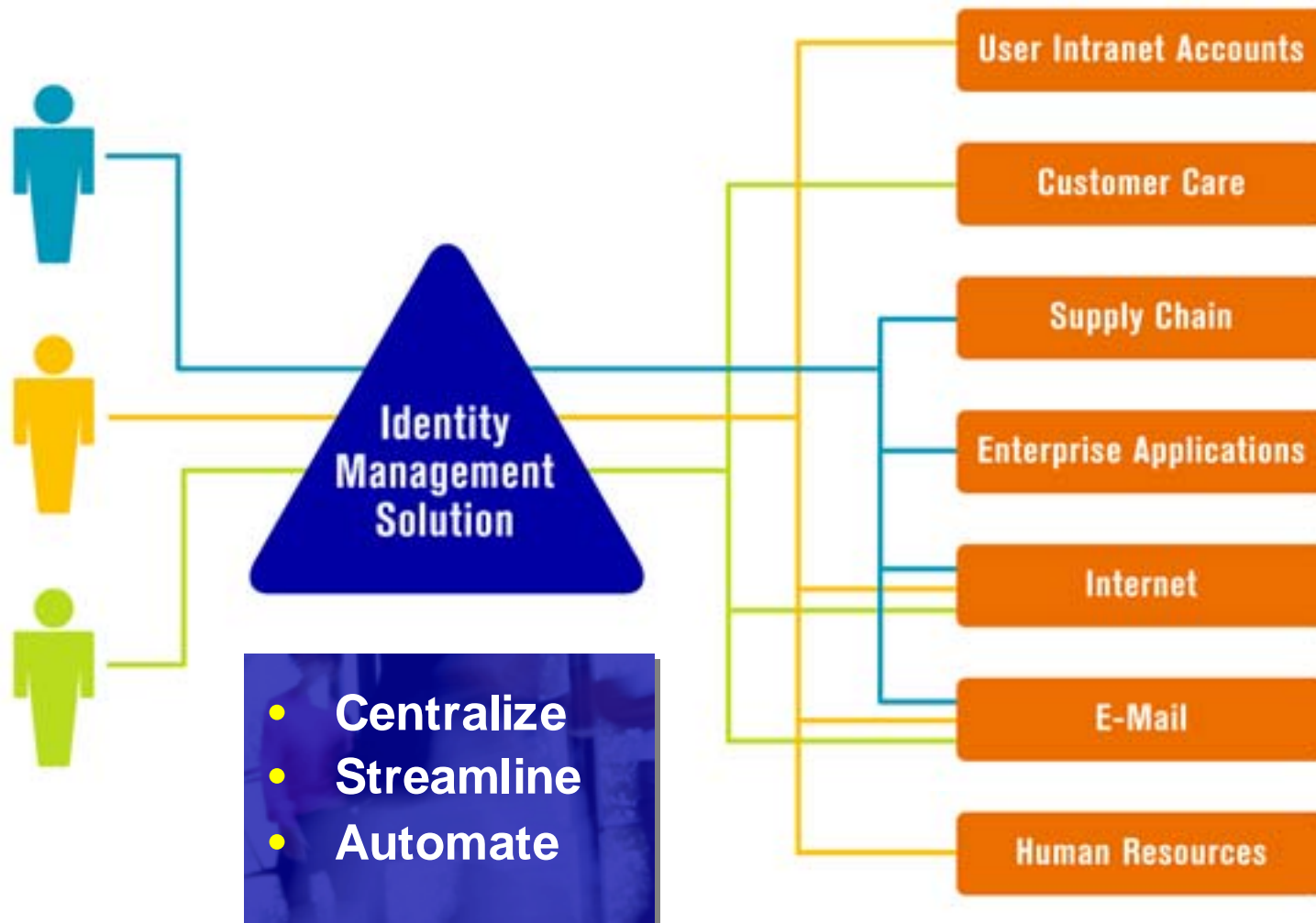
*Giga Information Group**

*2002 CSI / FBI Computer Crime and Security Survey***

What do Enterprise Customers need?



The Solution: Identity Management Defined



Agenda



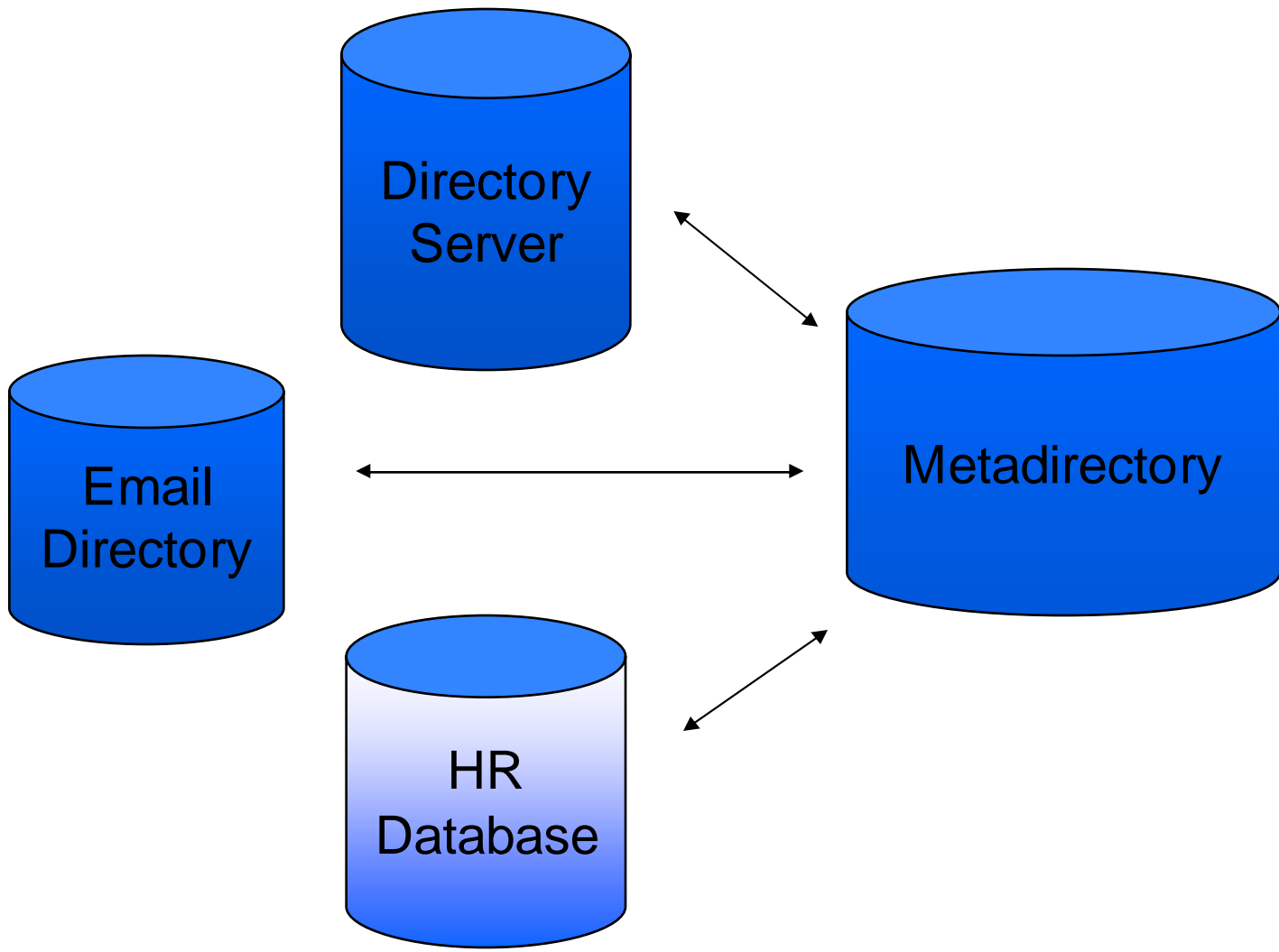
- Managing identity in a heterogeneous world –The Enterprise Perspective
- **Organizational Factors**
- Automation through IdM Platform
- Sample Architectures
- Selection & Deployment Considerations

The HR Factor



- Organizational resistance – HR systems are often off limits to IT staff
- Cooperation is hindered by confidentiality of data and regulatory compliance
- Technical incompatibilities often also exist as HR systems have not been designed to share data
- HR data is often incomplete lacking records for contract staff
- Most organizations have islands of user data stored in additional non-HR systems
- No comprehensive view of users & their access control

Need for Aggregation of Identity Data



Agenda



- Managing identity in a heterogeneous world –The Enterprise Perspective
- Organizational Factors
- **Automation through IdM Platform**
- Sample Architectures
- Selection & Deployment Considerations

Identity Management Capabilities

Role-based
provisioning/
deprovisioning

Workflow

Password
Management

Self-Service

Delegated
Admin

Auditing

Universal Identity Platform
Service Oriented Architecture

MIS Management Agents

OpenNetwork Connectors

MIS data synchronization

Identity Management Influences the Application Environment

Applications

Databases

Application
Servers

Authorization Services
(APIs, Connectors, Web Services)

Identity and Privilege Management

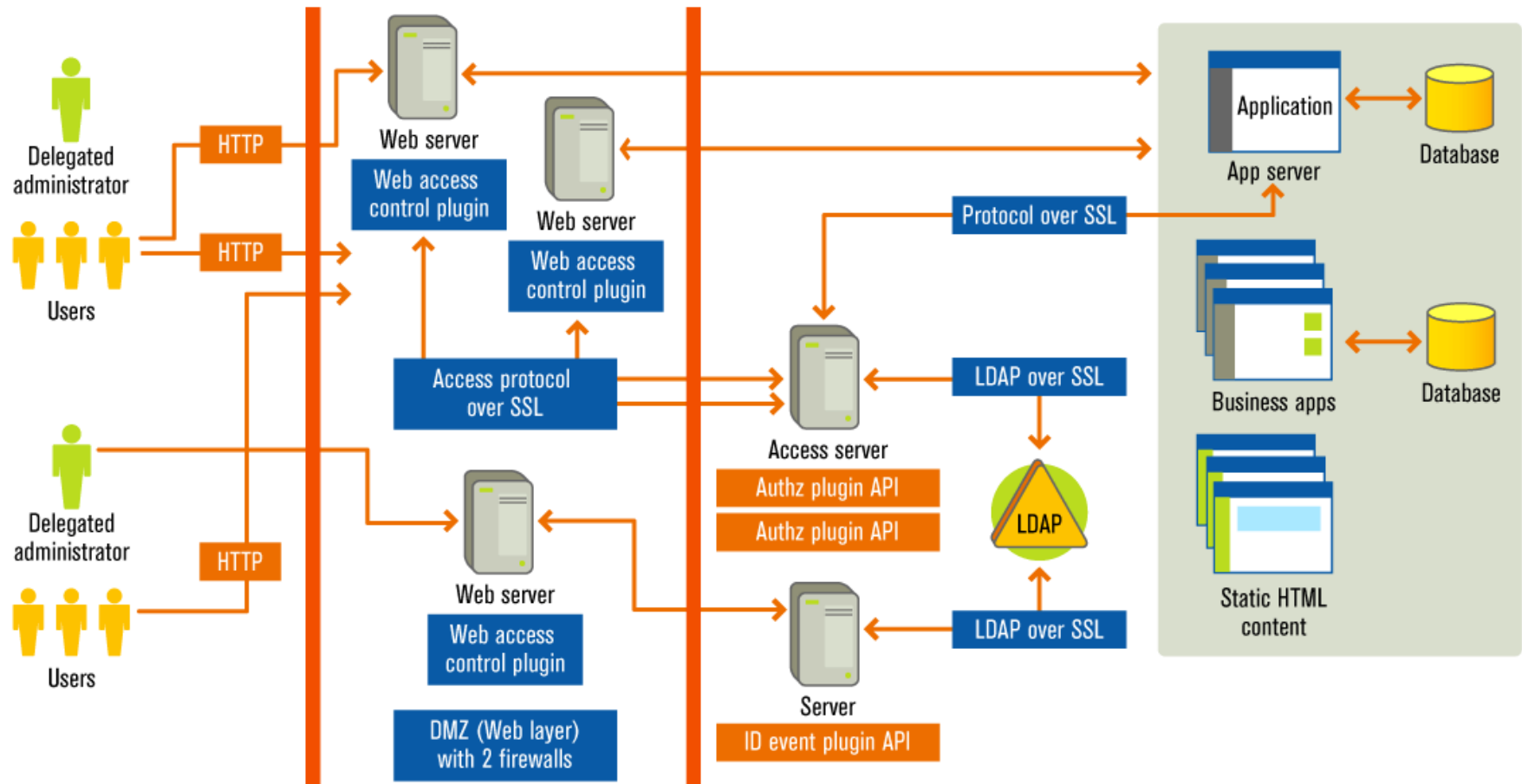
Identity Management Infrastructure
(Database, Directory, Meta-Directory)

Agenda

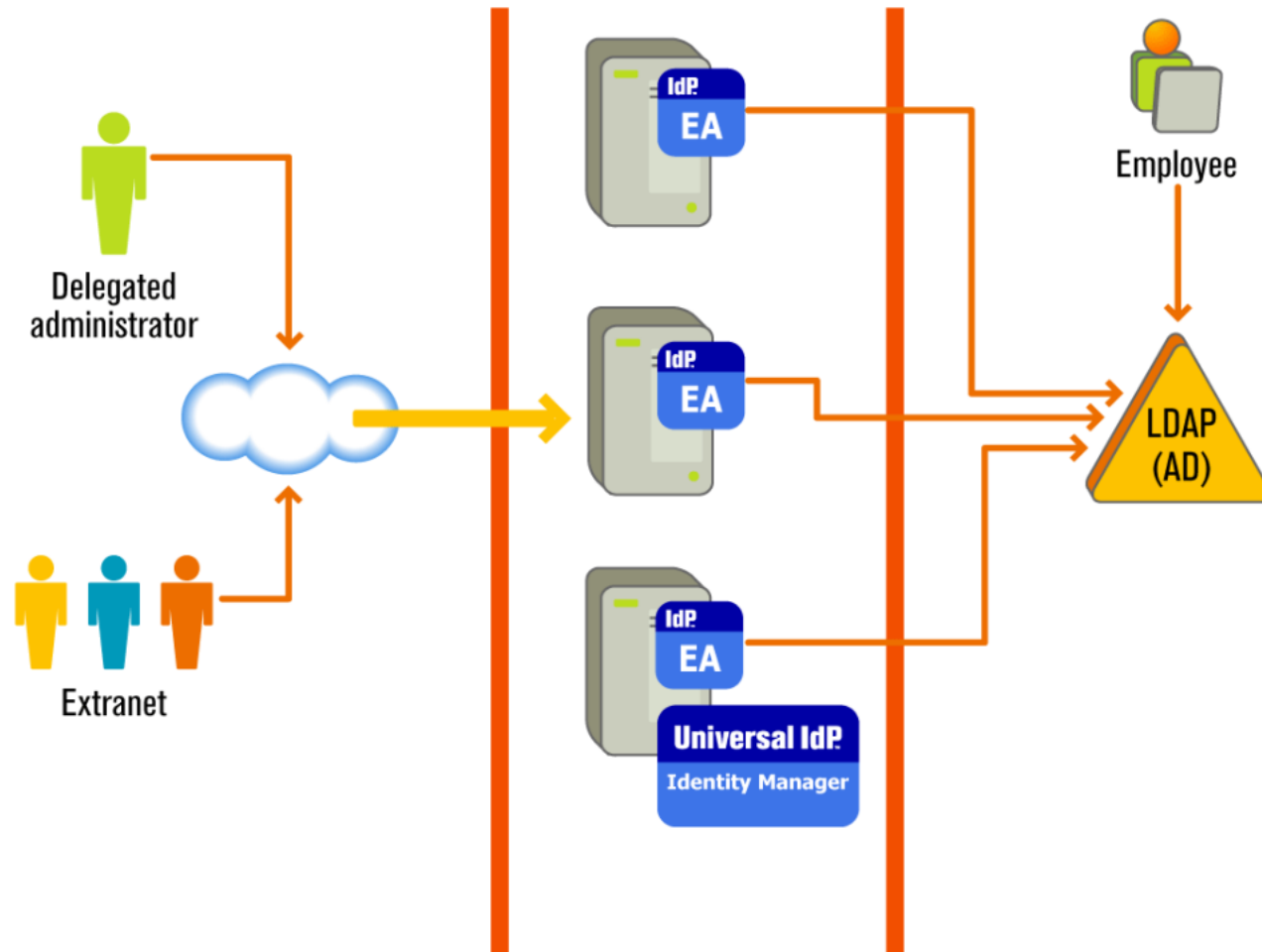


- Managing identity in a heterogeneous world –The Enterprise Perspective
- Organizational Factors
- Automation through IdM Platform
- **Sample Architectures**
- Selection & Deployment Considerations

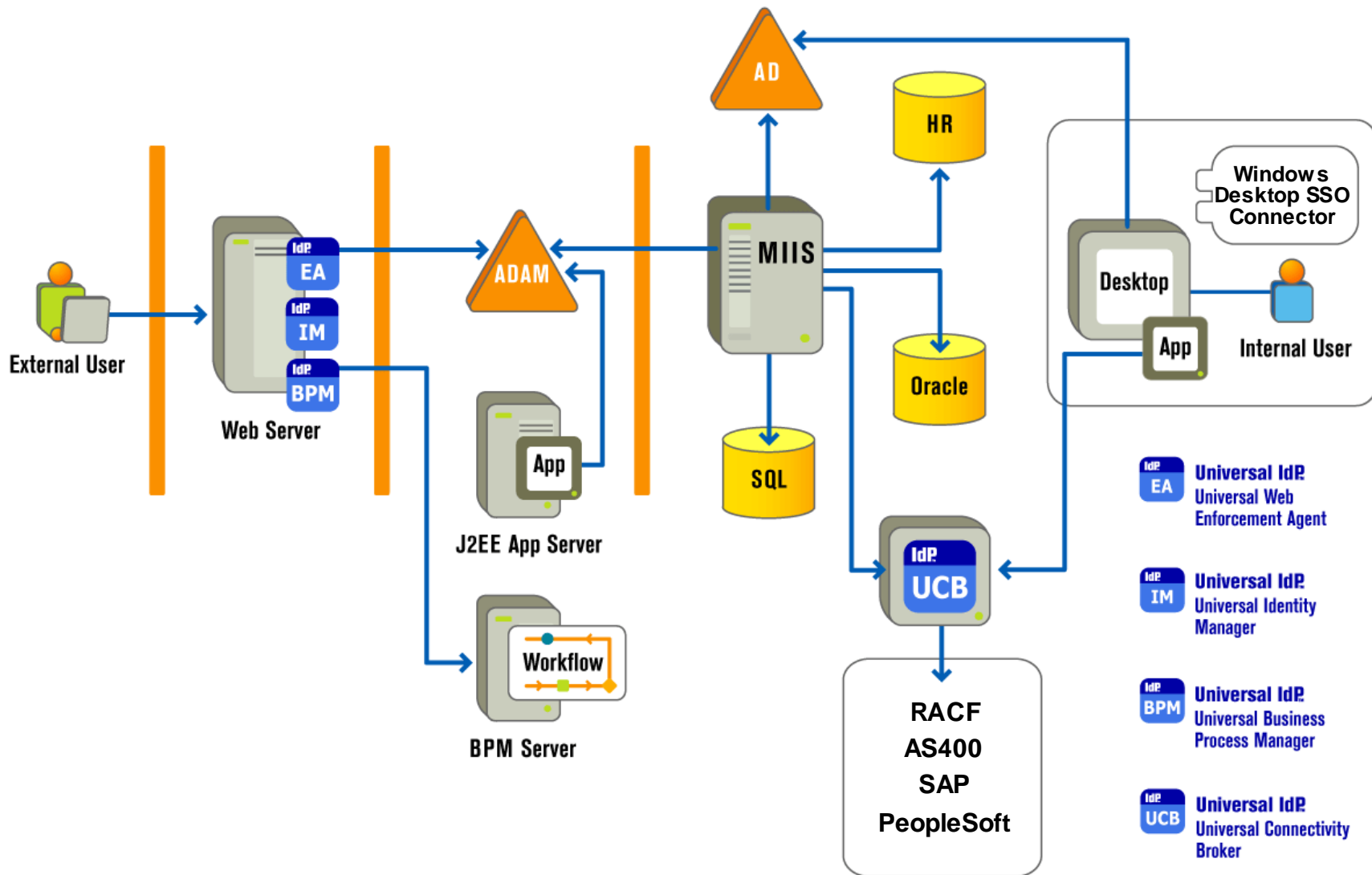
It's About Reducing Complexity... Not Introducing It!



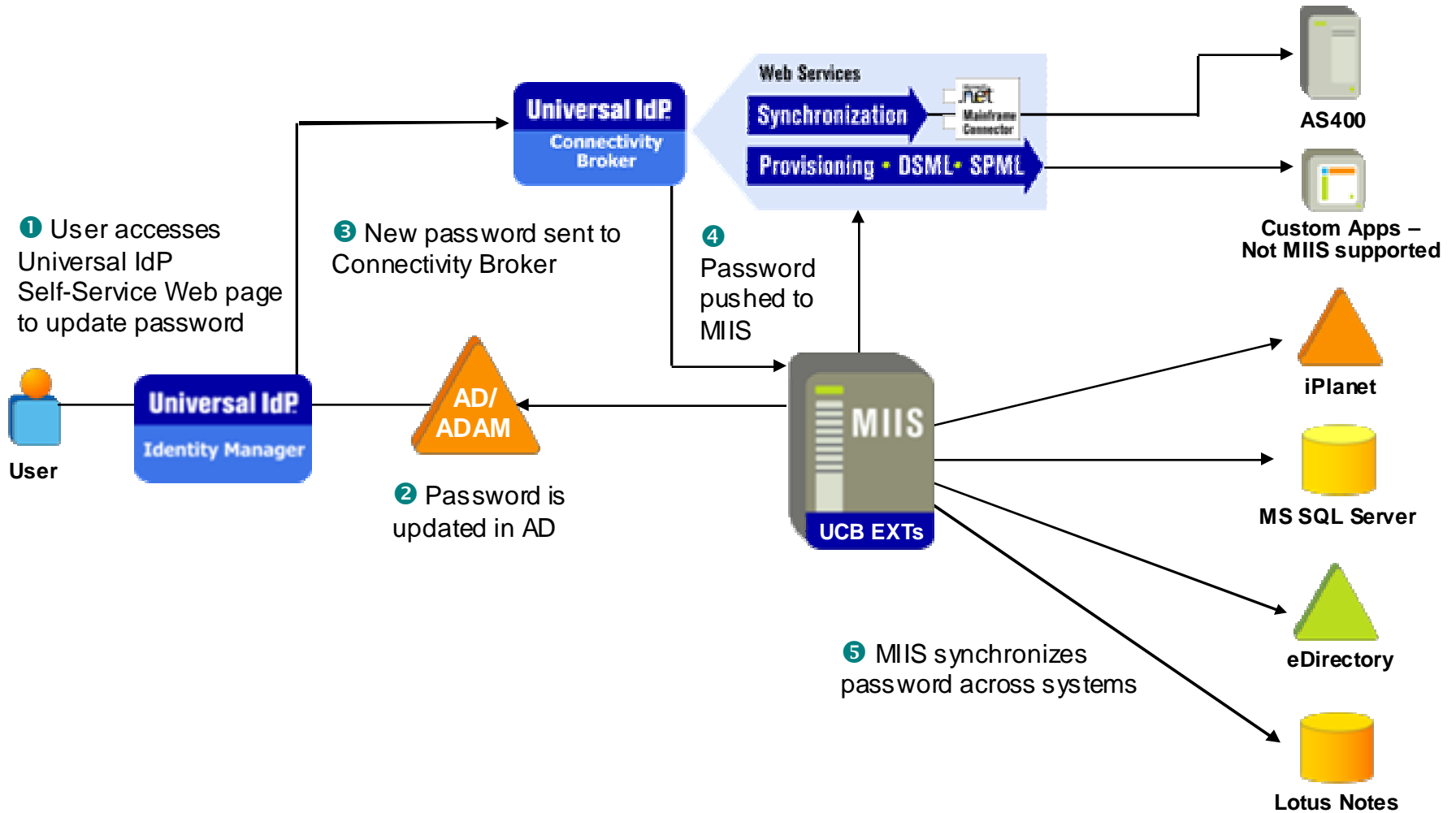
Sample IT Environment – Universal IdP Access and Identity Management



Sample IT Environment – Universal IdP End-to-End Identity Management



Use Case: Password Reset via Universal IdP



Agenda



- Managing identity in a heterogeneous world –The Enterprise Perspective
- Organizational Factors
- Automation through IdM Platform
- Sample Architectures
- **Selection & Deployment Considerations**

Typical Requirements for an Identity Management Solution



- Accuracy
- Automation / Self-Service
- Consistency
- Audit Compliant
- Platform Diversity
- Extensibility
- Ease of Deployment and Scalability
- End-to-End Functionality
- Simplicity of Management

Top 10 problems affecting Identity Management Deployments



1. Lack of Identity Management vision that is inclusive of process, technology and people
2. Ad-hoc approach to implementing IdM platform – lack of phased delivery
3. Low understanding of existing processes
4. Maintaining the defined scope of first release
5. Changing management's view of application security
6. Undocumented technical designs for many of the deployed custom applications
7. Lack of upper management support and buy-in at project inception
8. Lack of strong support from vendors
9. Adding infrastructure complexity
10. Lack of proper due diligence in technology selection

Calculating ROI

- Password management costs
 - Resources spent on help desk call
- Provisioning & workflow costs
 - Resources associated with integrating ERP, email systems and other applications
- IT management costs
 - Managing user attributes on ERP, NT/2000 including mail systems
- Development cost savings
 - Costs of developing front-end identity management services
 - Costs associated with ad-hoc user repository synchronization
- Indirect cost savings
 - Yearly costs associated with security breaches, exit cost, etc
 - Time spent on troubleshooting Help Desk
 - Time spent administrating Applications
 - Regulatory Compliance

Summary

- Lower costs, reduce complexity and improve security
 - Common administration
 - Common security policies
 - Common workflow

... *across Heterogeneous environments*
- Leverage and extend existing Microsoft technology investments
- Deploy the solution you need today – migrate easily to the solution you need tomorrow

Where to go for more information...



- Download whitepapers at:
www.opennetwork.com/goto
- Download an evaluation copy of Universal IdP at: www.opennetwork.com/eval
- Visit Microsoft at:
<http://www.microsoft.com/business/security/access/default.mspx>
- Find out more about standards at:
<http://www.oasis-open.org/home/index.php>