



Introduction to Access Management

J. Tony Goulding CISSP, ITIL

Security Solution Strategist, CA Inc.

tony.goulding@ca.com

Goal of This Session

- *Access Controls* are at the heart of many regulations. In this presentation you will gain an understanding of:
 - Identity & Access Management
 - Where Access Controls fit into the common regulation landscape
 - Where Access Controls fit in the larger Identity & Access Management (IAM) world
 - Common Access Control models (web-based and host-based)
 - What aspects of Access Control demand auditing

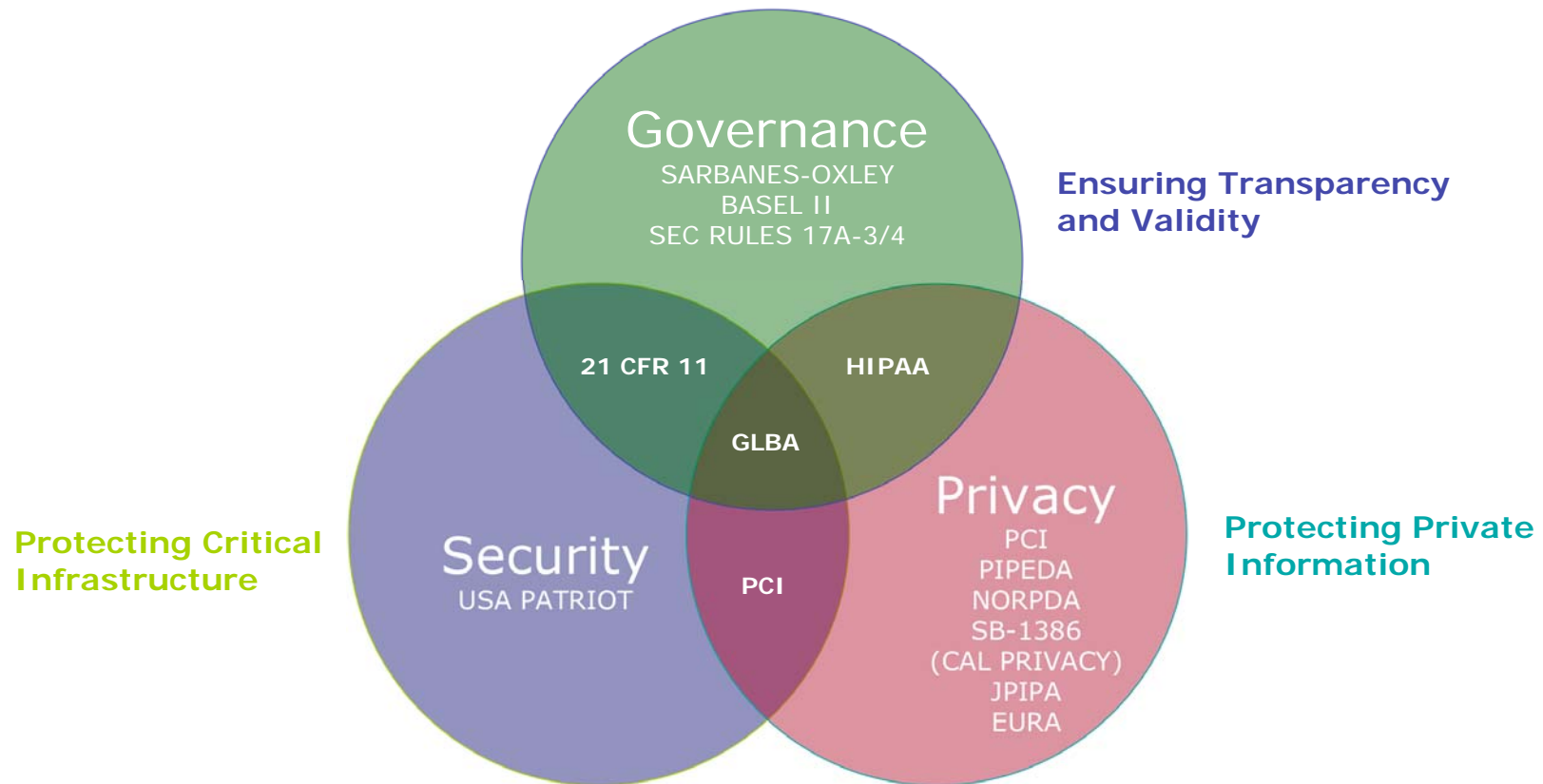


The Regulatory Landscape

Major International Laws/Regulations

Vertical	Regulation	Summary of Regulation
Financial Services	Gramm-Leach-Bliley (GLB)	Defines privacy requirements for customer personal financial information.
	Basel II	Defines requirements for risk management within a capital framework. The higher the risk, the more capital is required for a bank.
Healthcare& Life Sciences	HIPAA	Governs privacy and security of private user health information.
	21 CFR Part 11 (FDA)	Defines requirements for storage and access to data relating to drug development cycles.
Cross-Sector	EU Data Directive	Provides a framework of data protection and privacy requirements that is to be reflected in national law by all member states to provide a minimum level of protection throughout the European Union nations.
	Payment Card Industry Data Security Standard (PCI DSS)	Collaboration between leading credit card institutions to ensure consistency of security standards for card issuers and assure security of account information.
	UK Data Protection Act	Provides additional data protection and privacy requirements over and above what is required by the EU Data Directive.
	ISO 17799 (BS 7799)	Standard that sets out requirements for an “best practices” Information Security Management System (ISMS).
	Patriot Act	Requirements to combat and report money-laundering activities.
	Sarbanes-Oxley Act	Requires a company to document internal controls that relate to financial reporting.
	California Privacy Act	Defines requirements for notification of suspected breaches of personal information. Applies to any company doing business in California.
	NORPDA	Establishes a national standard for notification of consumers when a database breach occurs.
	PIPEDA	Controls use of personal information by corporations (Canada)

Major Types of Regulations and Laws



Common Elements - Security

The most common element of all regulations is a ***strong set of internal controls***. An internal control is a set of procedures that can ensure the successful operation of a business practice or transaction.

These controls must provide:

- **Accountability** – who performed an action, who approved it, when was it done, and what was the result?
- **Transparency** – all business processes and controls must be fully understood, and clearly documented. Opaque processes are, by definition, non-compliant.
- **Measurability** – All internal processes must be able to be measured and evaluated as to success or failure. Measurement is done through auditing, logging, correlation, and visualization.

The Importance of Security for Compliance

Regulation Technology	SOX	HIPAA	Gramm-Leach Bliley	Sec 17A-4	21 CFR Part 11	Basel II	USA Patriot Act	CA SB 1386	Canada PIPEDA
Financial Compliance	✓								
Business Intelligence & Data Warehousing	✓								
Document / Content Management & Access	✓	✓	✓	✓	✓	✓	✓	✓	
Records Management	✓	✓		✓	✓	✓			
Archiving	✓	✓	✓	✓	✓	✓	✓	✓	
Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage	✓	✓		✓	✓	✓	✓		

Example: Sarbanes Oxley

Most Common Problems in SOX Compliance:

- “... there were 28 disclosures of weaknesses in internal controls. 10 of those disclosures specifically mentioned deficiencies in **user access controls or segregation of duties.**”
 - Compliance Week, April 6, 2004
- “If you haven’t found **user access control and segregation of duties** violations yet, you just haven’t looked hard enough.”
 - Senior Manager, Big 4 Audit Firm; ISACA Sarbanes Oxley Conference, April 6, 2004
- “My Two Biggest Sarbanes Issues are **User Access Controls and Segregation of Duties.**”
 - CIO, Finance; Fortune 70 Manufacturer

Top 10 IT-Related Control Deficiencies

- #10 System documentation does not match actual process
- #9 Inadequate documentation, identification and tracking of IT assets
- #8 *Custom programs, tables, & interfaces unsecured***
- #7 Posting periods not restricted within GL application
- #6 *Terminated employees or departed consultants still have access***
- #5 *Large number of users with access to “super user” transactions in production***
- #4 *Development staff can run business transactions in production***
- #3 *Lack of “transparency” over changes made to Financial Applications***
- #2 *Database (e.g. Oracle) and Operating system (e.g. Unix) supporting Financial Applications or Portal not hardened***
- #1 *Unidentified or unresolved segregation of duties issues***

7 of Top 10 Deficiencies are IAM-Related!

* Ken Vander Wal, National Quality Leader, E&Y ISACA Sarbanes Conference, 4/6/04



Where Access Control Fits in the Larger IAM Landscape

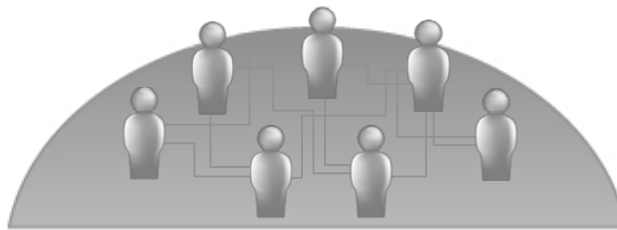
What is IAM? Top-Down...

- Drivers that bring people to IAM:
 - Reduce Risk – do things more securely
 - Reduce Cost – do things more cost-effectively
 - Improve Service – happy people are sticky people!
- Linking PEOPLE to RESOURCES via PROCESS and TECHNOLOGY
 - People: internal users; customers, vendors, partners....
 - Process: password reset, user registration, account creation...
 - Technology: stuff that makes all this happen

Identity & Access Management

The Challenge

- > Difficult to admin access rights
- > High Help Desk costs

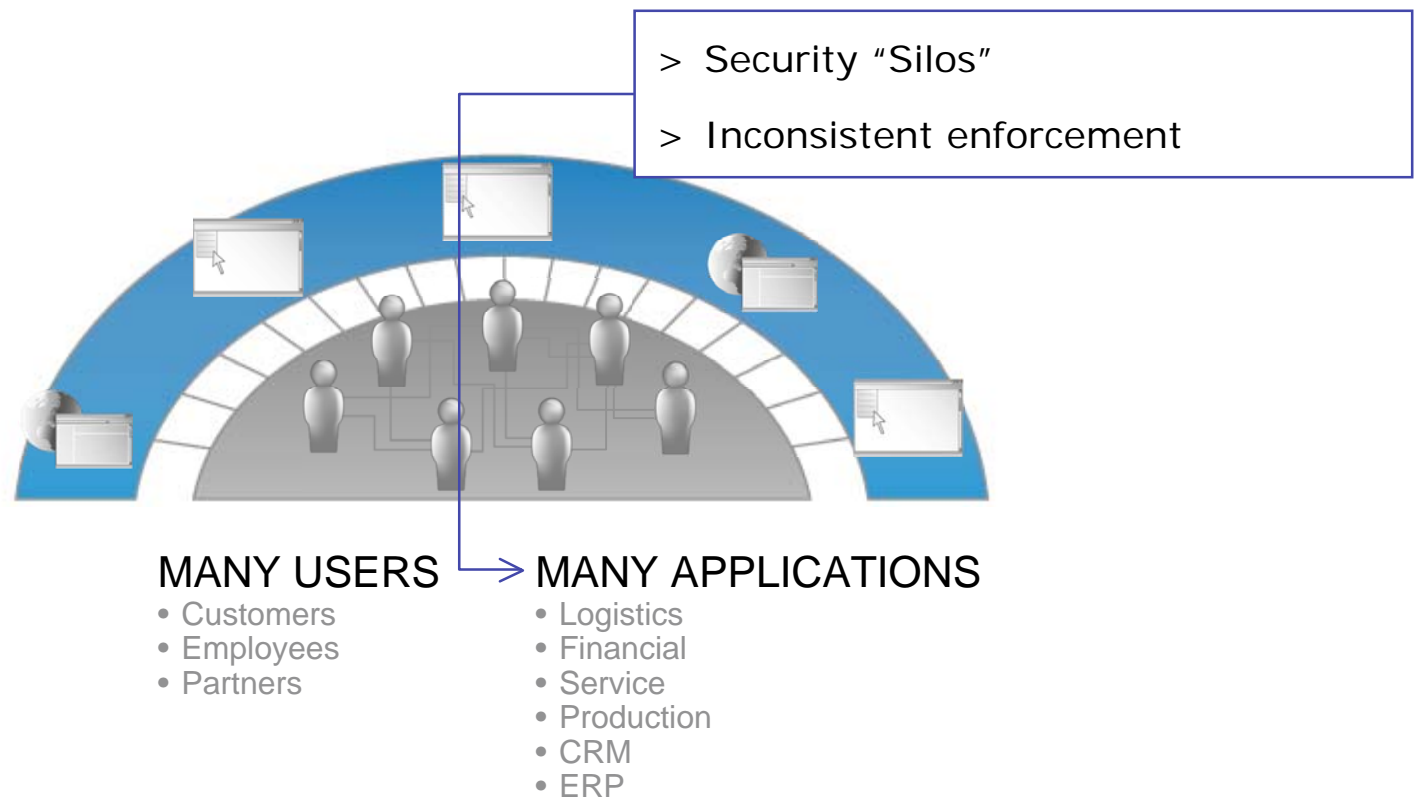


→ **MANY USERS**

- Customers
- Employees
- Partners

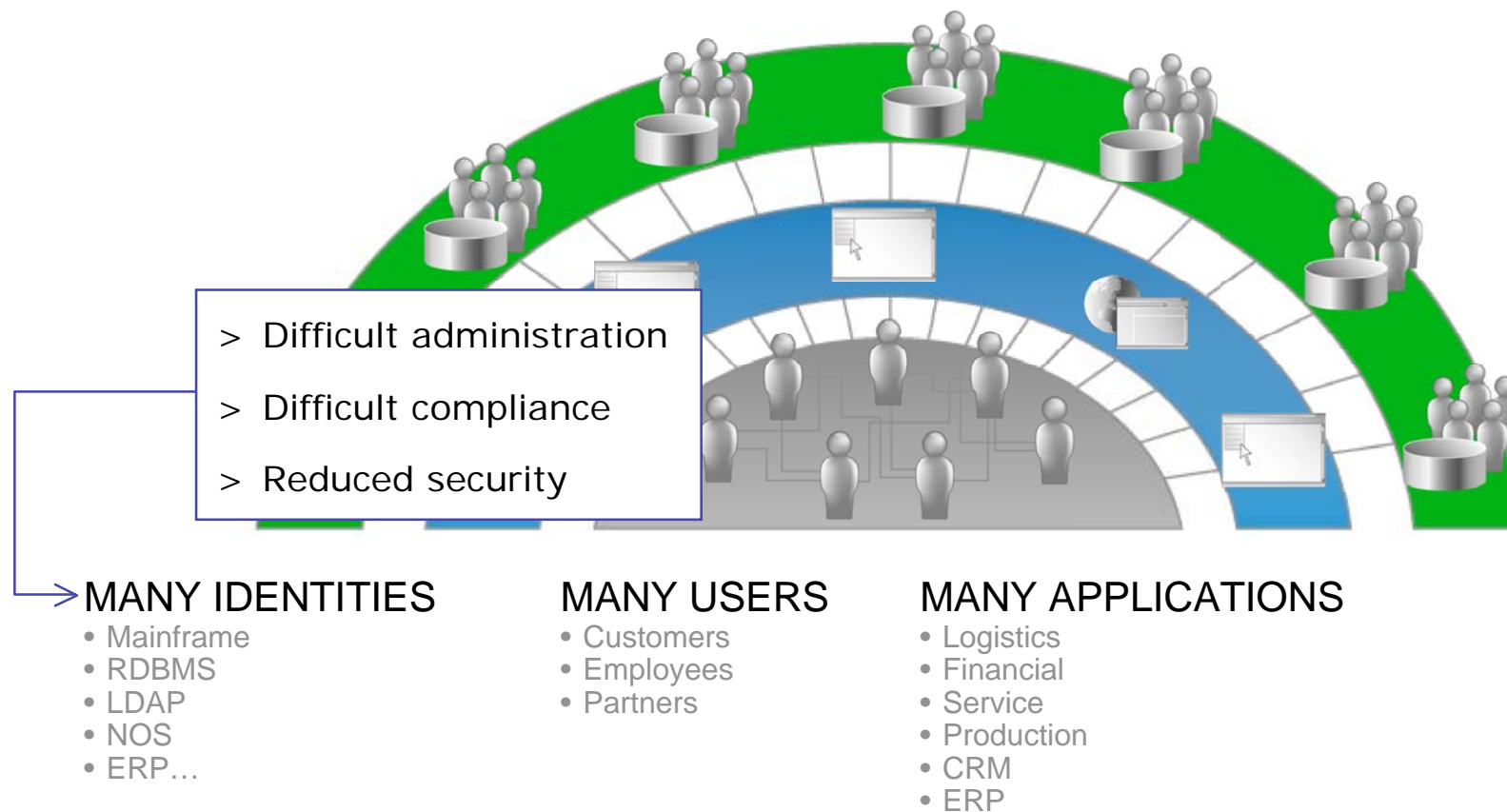
Identity & Access Management

The Challenge



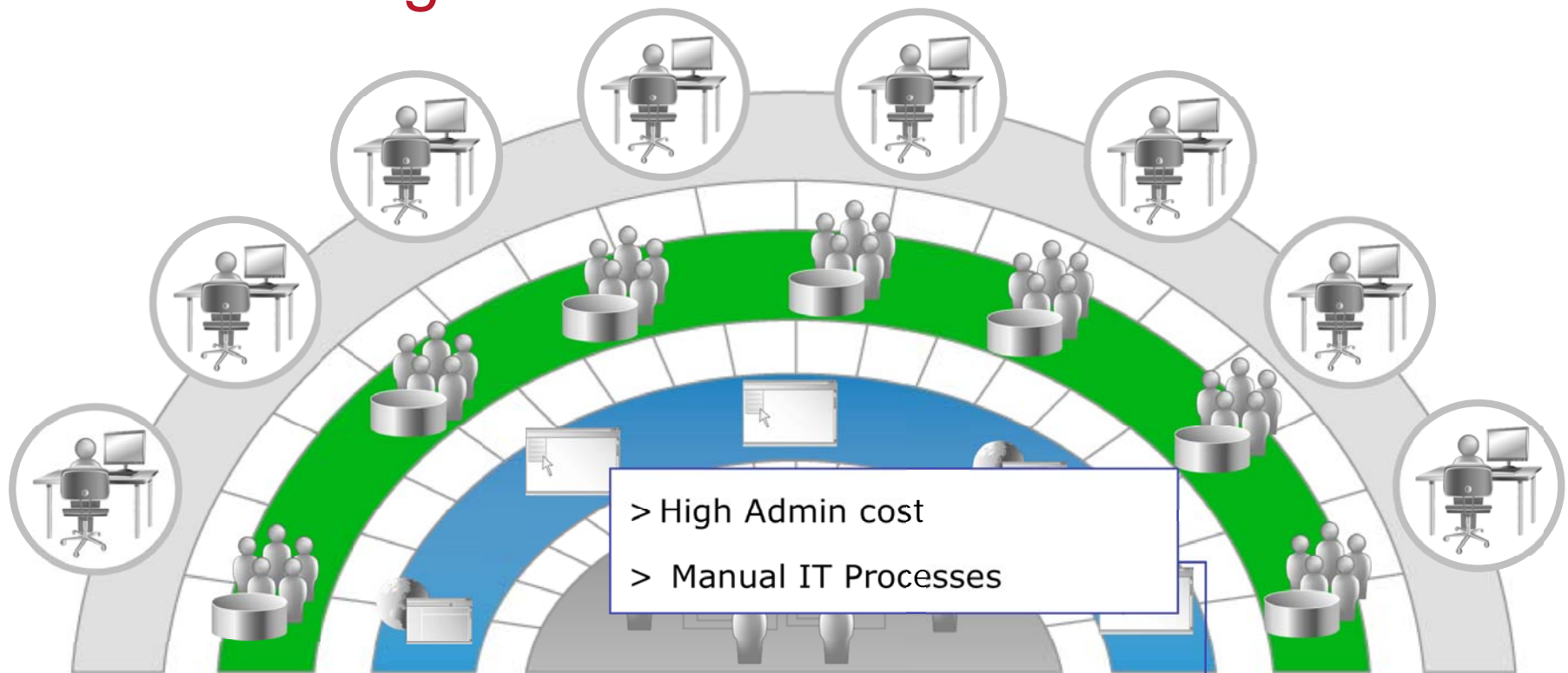
Identity & Access Management

The Challenge



Identity & Access Management

The Challenge



MANY IDENTITIES

- Mainframe
- RDBMS
- LDAP
- NOS
- ERP...

MANY USERS

- Customers
- Employees
- Partners

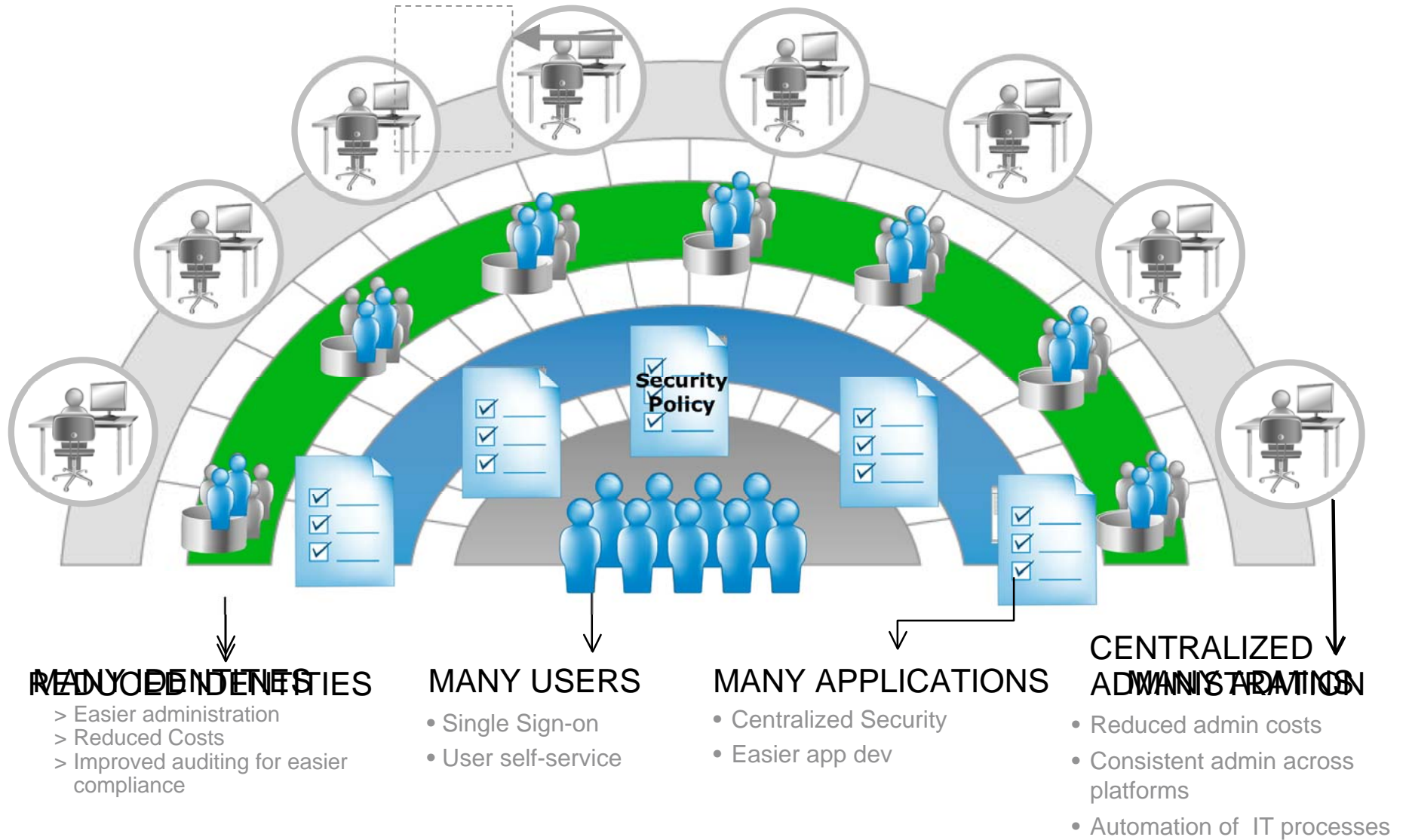
MANY APPLICATIONS

- Logistics
- Financial
- Service
- Production
- CRM
- ERP

MANY ADMINS

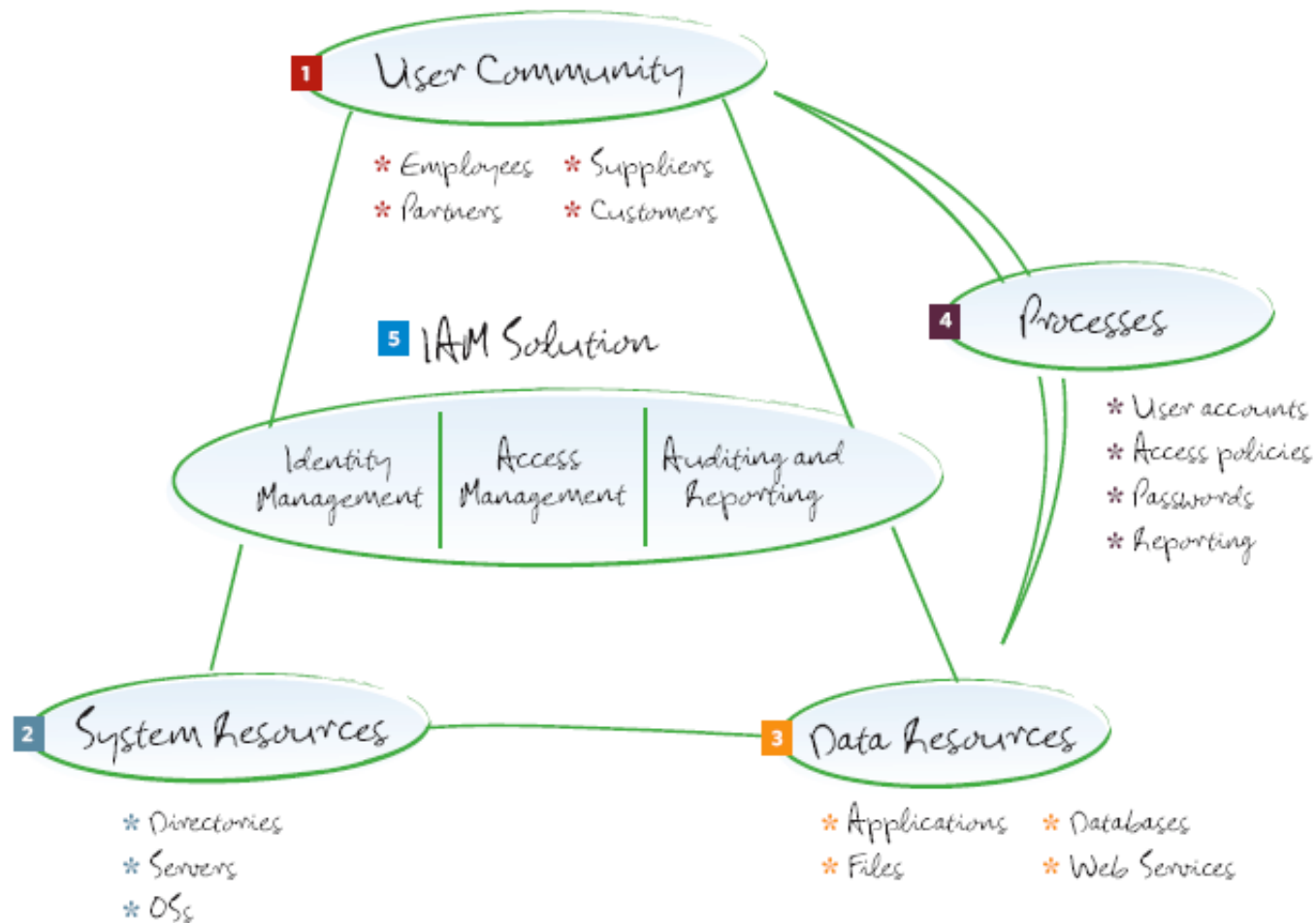
- Many tactical issues
- Managing users, passwords, etc.

Identity & Access Management The Solution



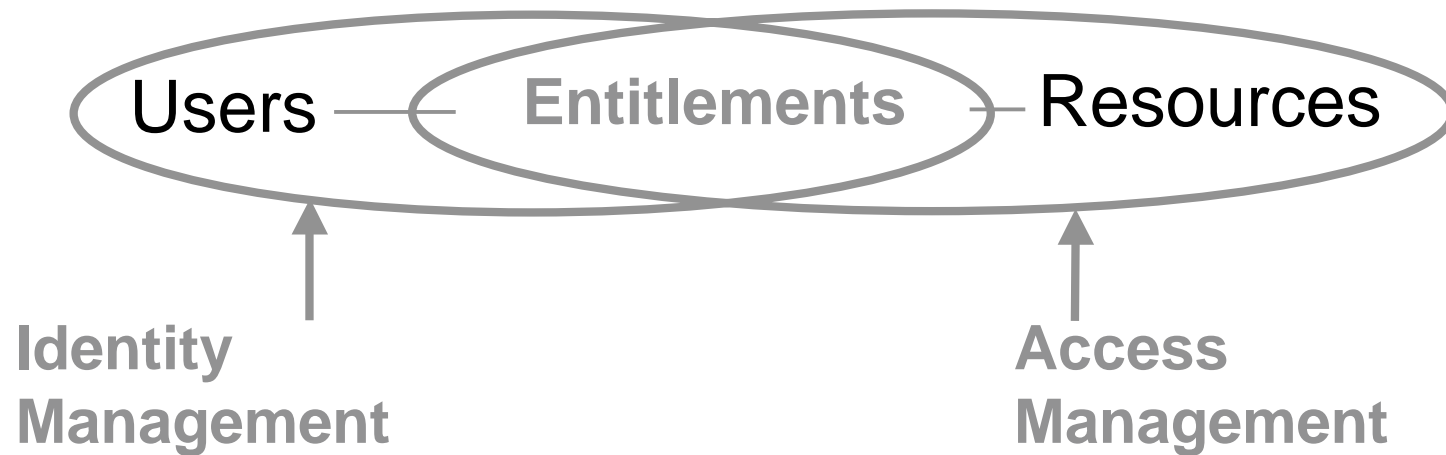
Obligatory Picture...

Obligatory Picture



Identity & Access Management

- Identity Management and Access Management are two sides of the equation to manage and enforce information access



“Entitlements Administration”

Entitlements:

- Managed
- Granted/Denied
- Enabled
- Approved



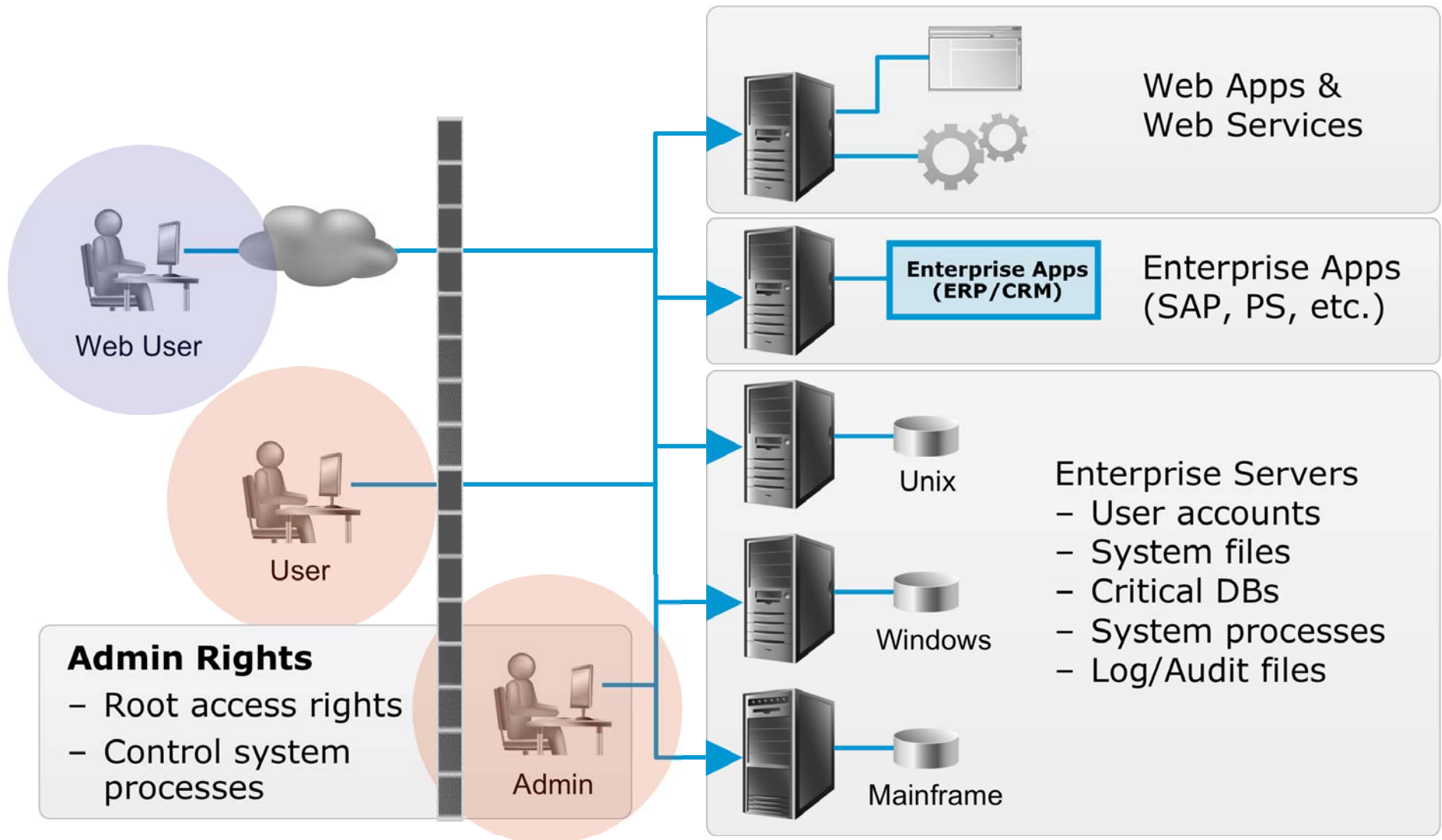
“Entitlements Enforcement”

- Policy enforced
- Access controlled
- Single sign-on



Focus on Access Control

Access Control = ~~Asset Protection~~ *Business enablement!*

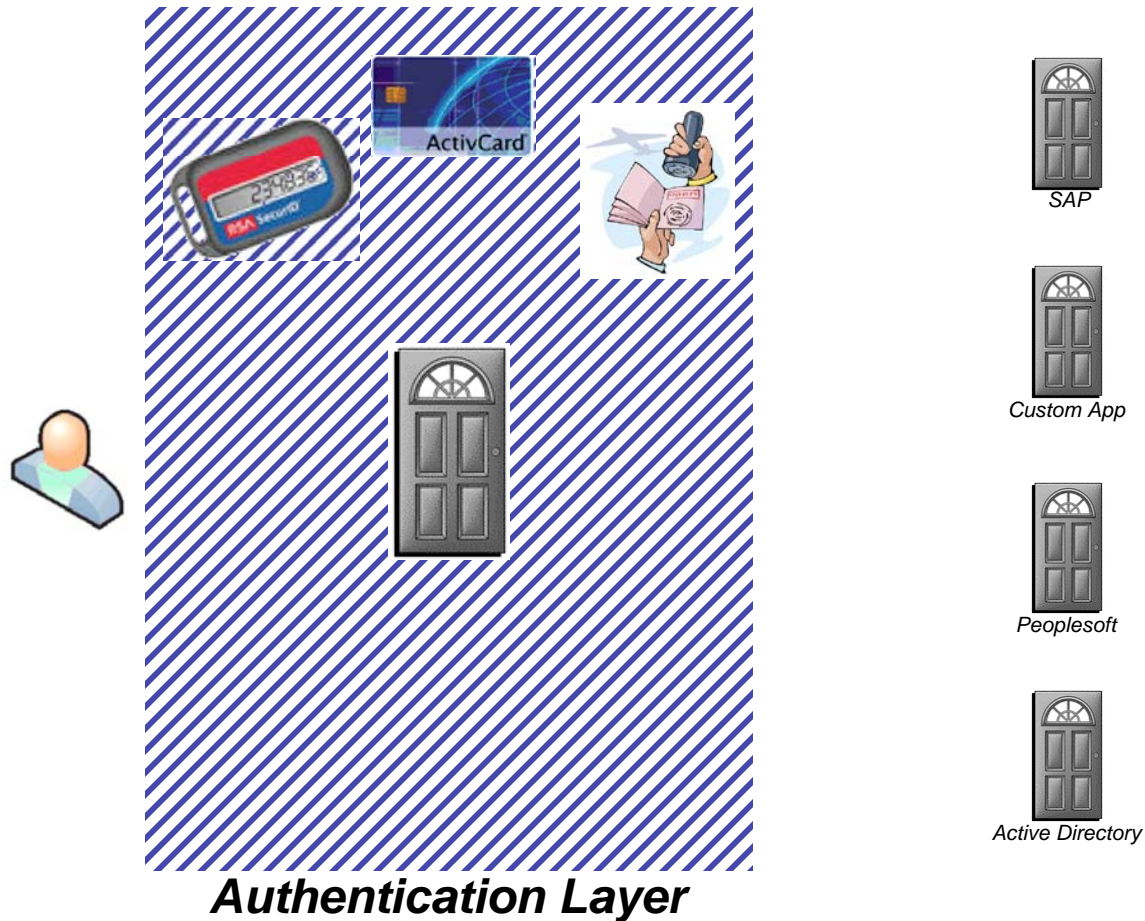


HOW?

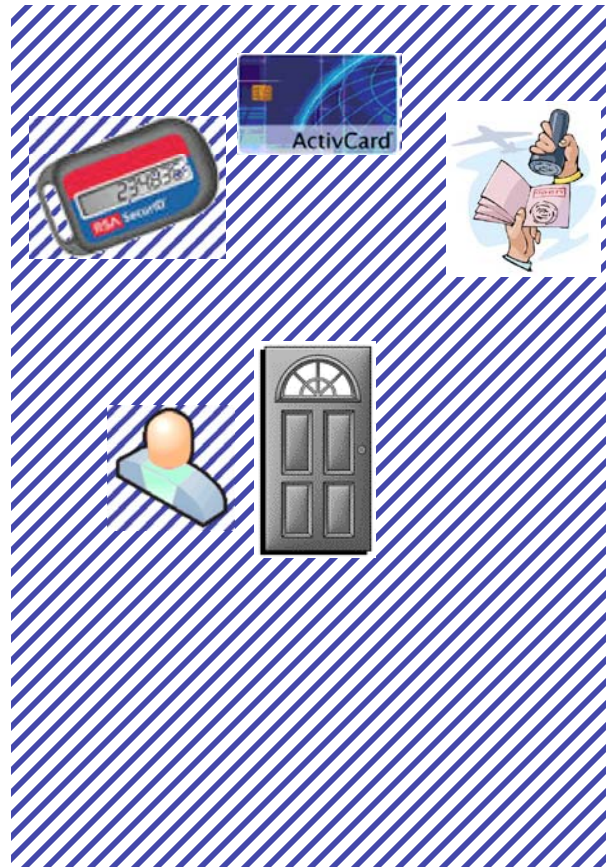
AAA

- Authentication
 - WHO ARE YOU?
- Authorization
 - WHAT ARE YOU ENTITLED TO DO?
- Audit
 - WHAT HAVE YOU DONE?

Authentication + Authorization



Authentication + Authorization



Authentication Layer



SAP



Custom App



Peoplesoft

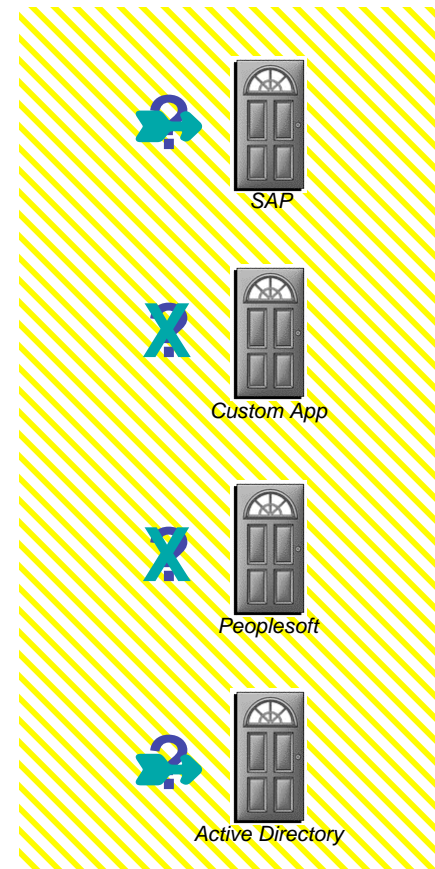


Active Directory

Authentication + Authorization

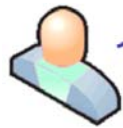


Authentication Layer



Authorization Layer

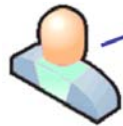
Role-Based Access Control



- Active Directory account
- Consulting Knowledge Base acct
- Intranet Portal account
- Single Sign-On account
- UNIX login account on server XYZ

**ROLES = BASIC +
CON1 + SSO**

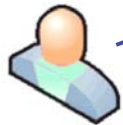
ROLE = BASIC
• AD Account
• Intranet Portal
account



- Active Directory account
- Consulting Knowledge Base acct
- Intranet Portal account
- UNIX login account on server XYZ

**ROLES = BASIC +
CON1**

ROLE = CON1
• Con KB acct
• UNIX XYZ logon



- Active Directory account
- Consulting Knowledge Base acct
- Intranet Portal account
- Single Sign-On account
- Sales Database account

**ROLES = BASIC +
CON1 + SSO +
CON2**

ROLE = CON2
• Sales DB acct

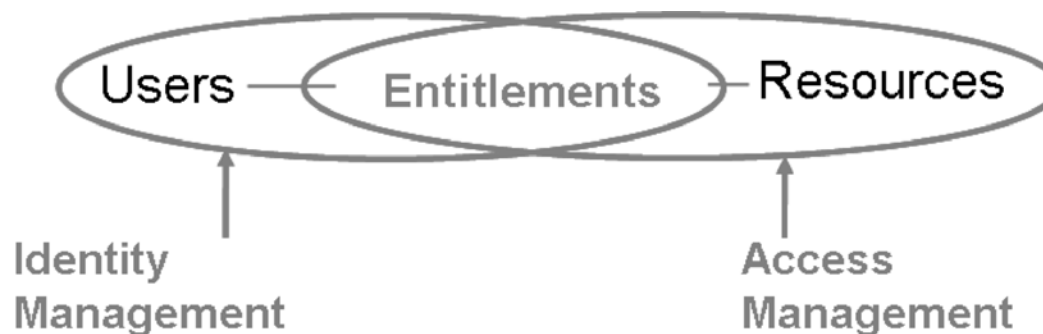
ROLE = SSO
• SSO account

Access Management Summary

- An essential element of any regulation is effectively and securely controlling the access to all protected resources by all users.
- Role-based access control is required for a range of corporate resources:
 - Web applications
 - Web services
 - Systems and platforms
 - System files and repositories
 - Critical system services
 - Granular Root access privileges
- Key Access Management Functions
 - Authentication (and Single Sign-On)
 - Authorization
 - Audit

Another Reminder About Identity Management

- Don't forget, Identity Management is also a strong source of relevant auditing information. E.g.:
 - Who delegated access to whom?
 - What SOD violations were captured?
 - Who approved giving the role of Accounts Receivable to John?
 - When was Tony deprovisioned?
 - What accounts were removed when Mary left the company?
 - Etc...





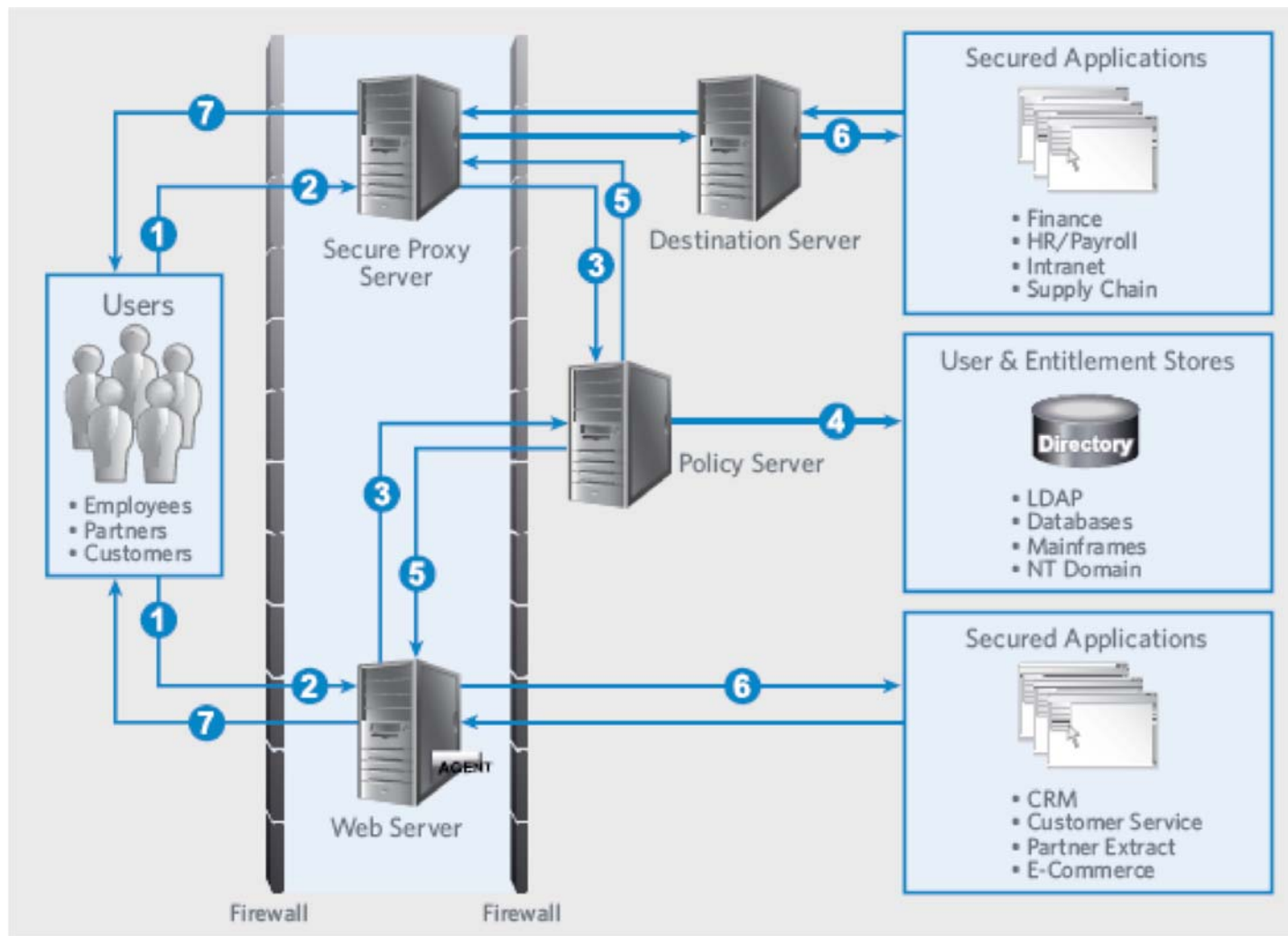
Access Control Models

Web Access Control

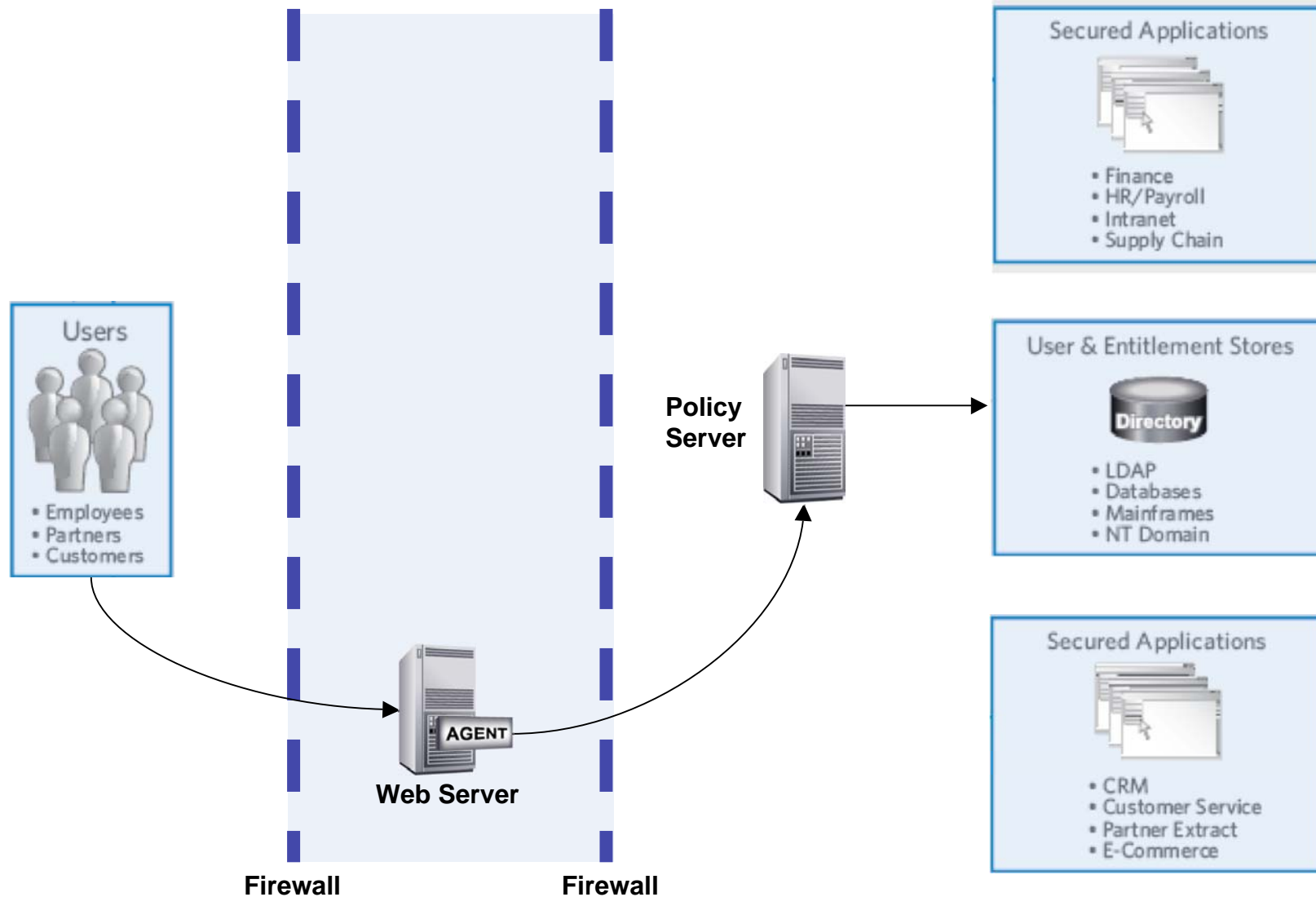


Access Control Models

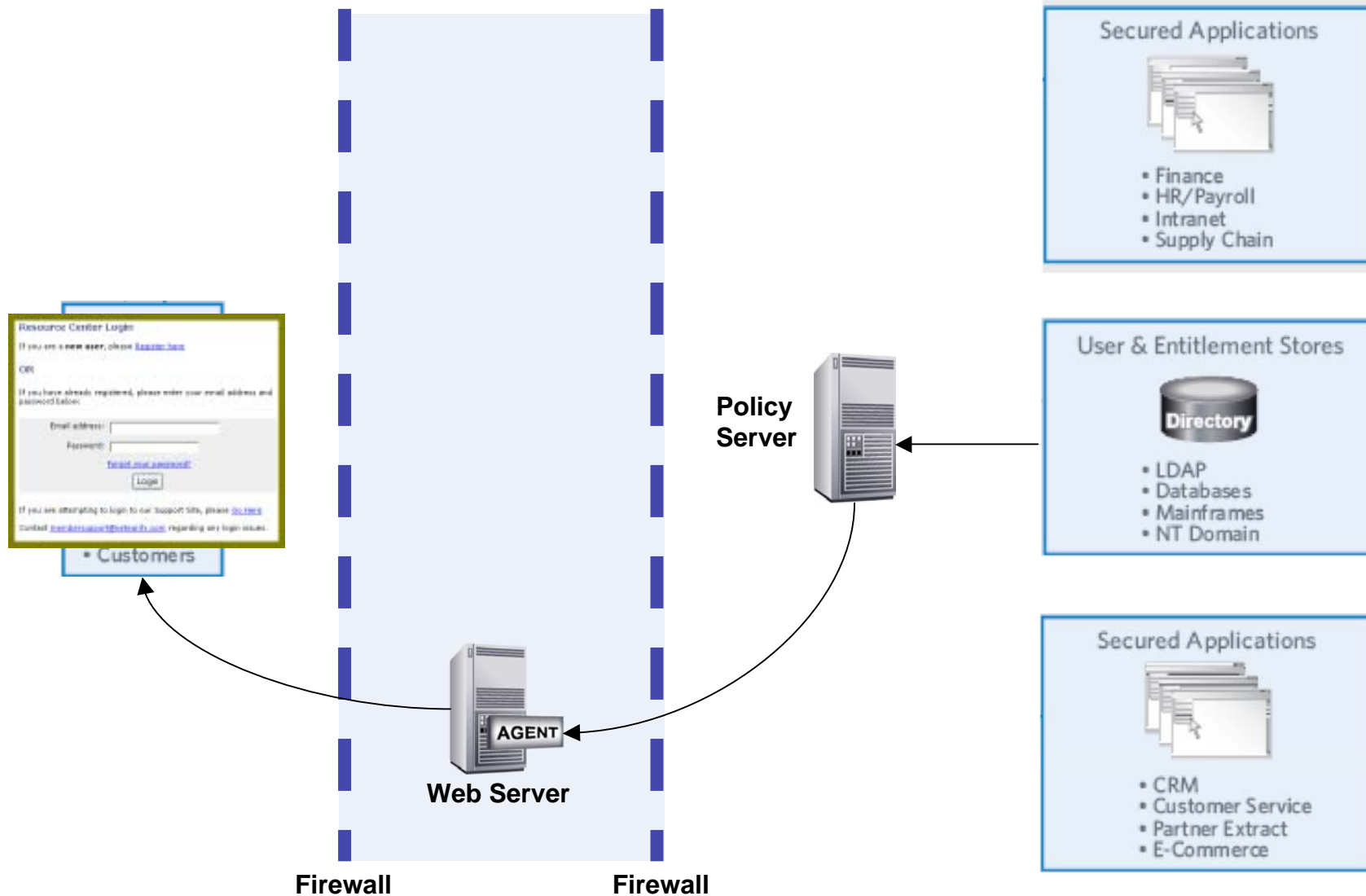
Web-Based Access Control



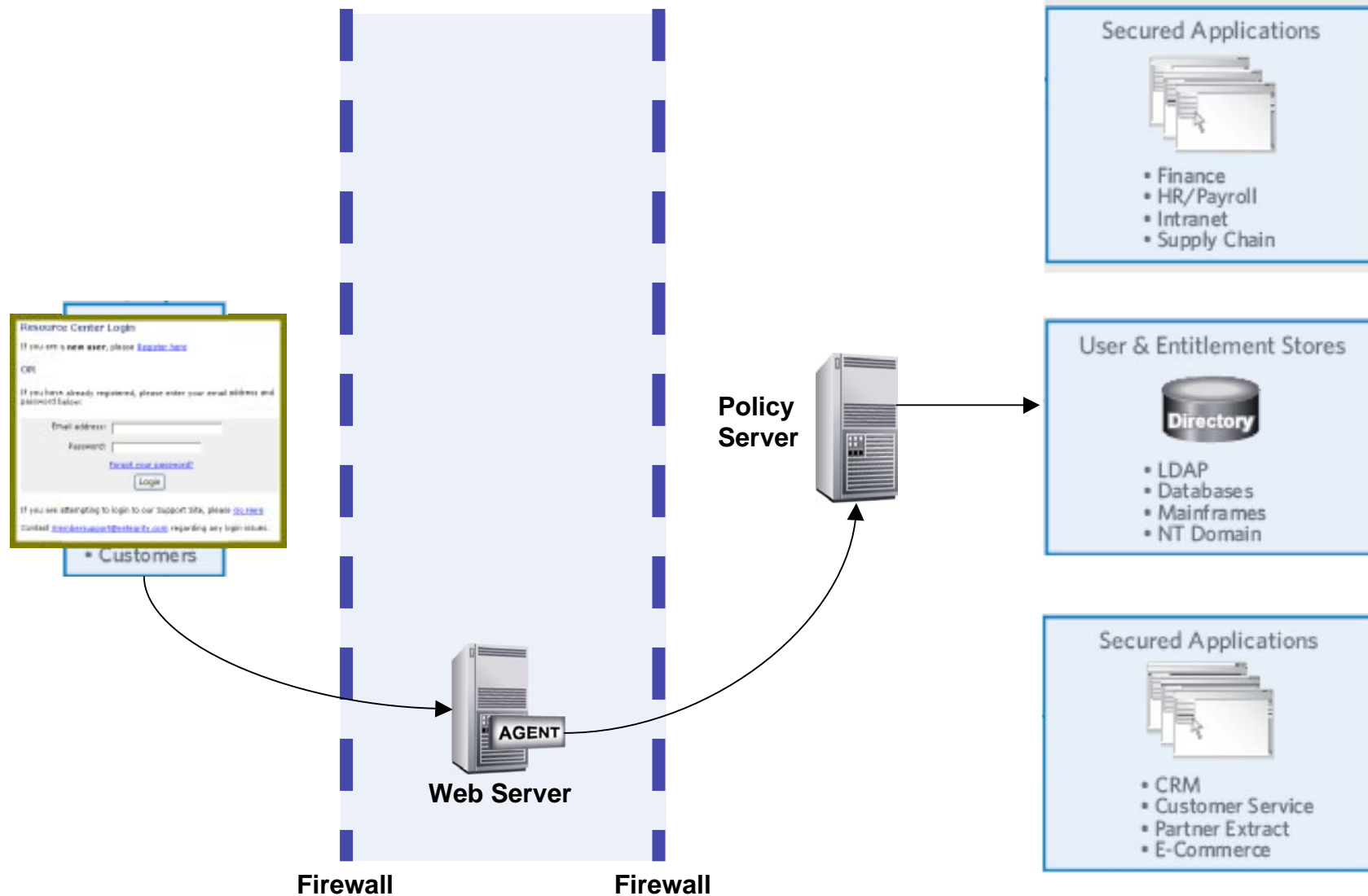
Typical Use Cases



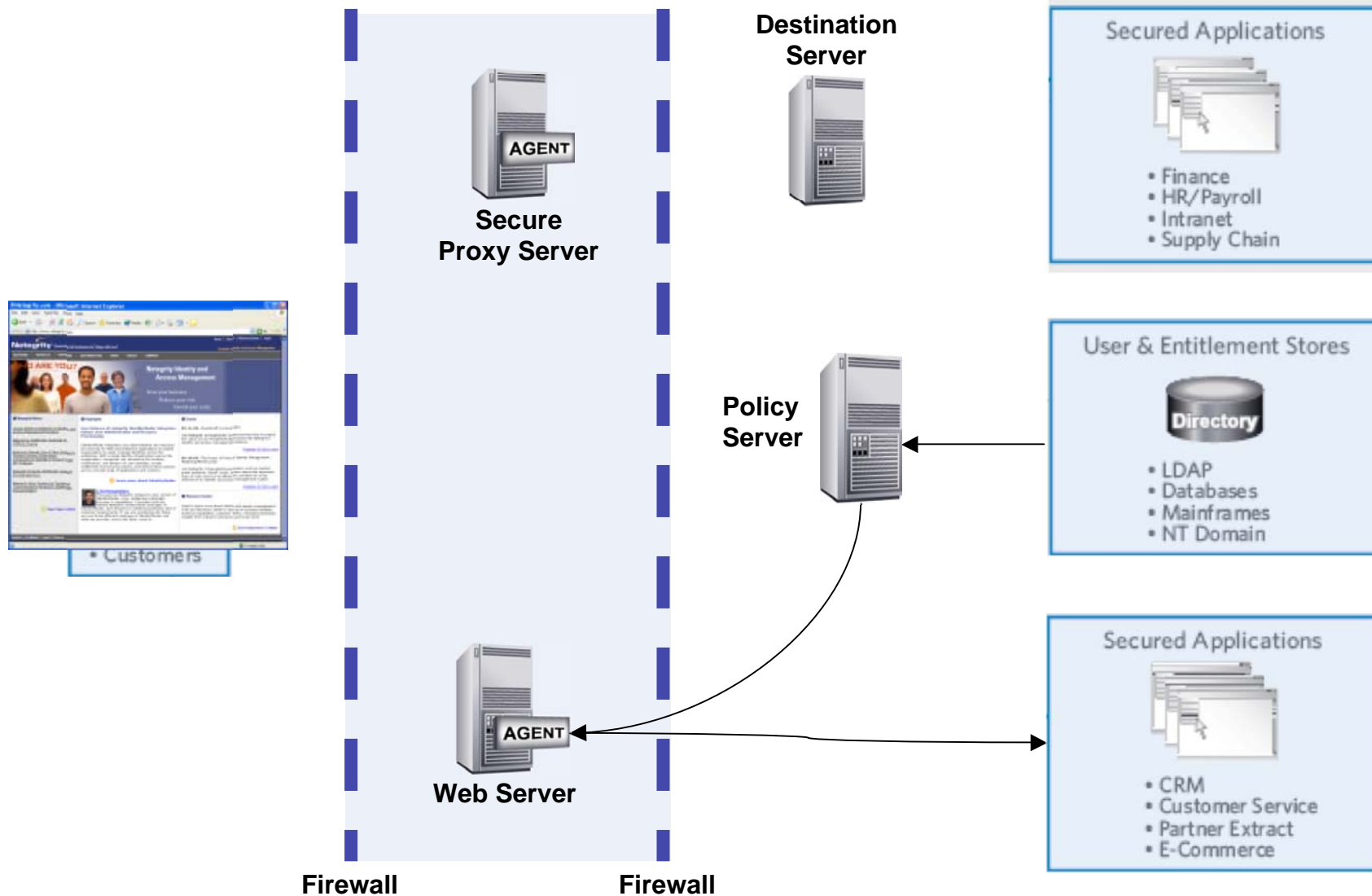
Typical Use Cases



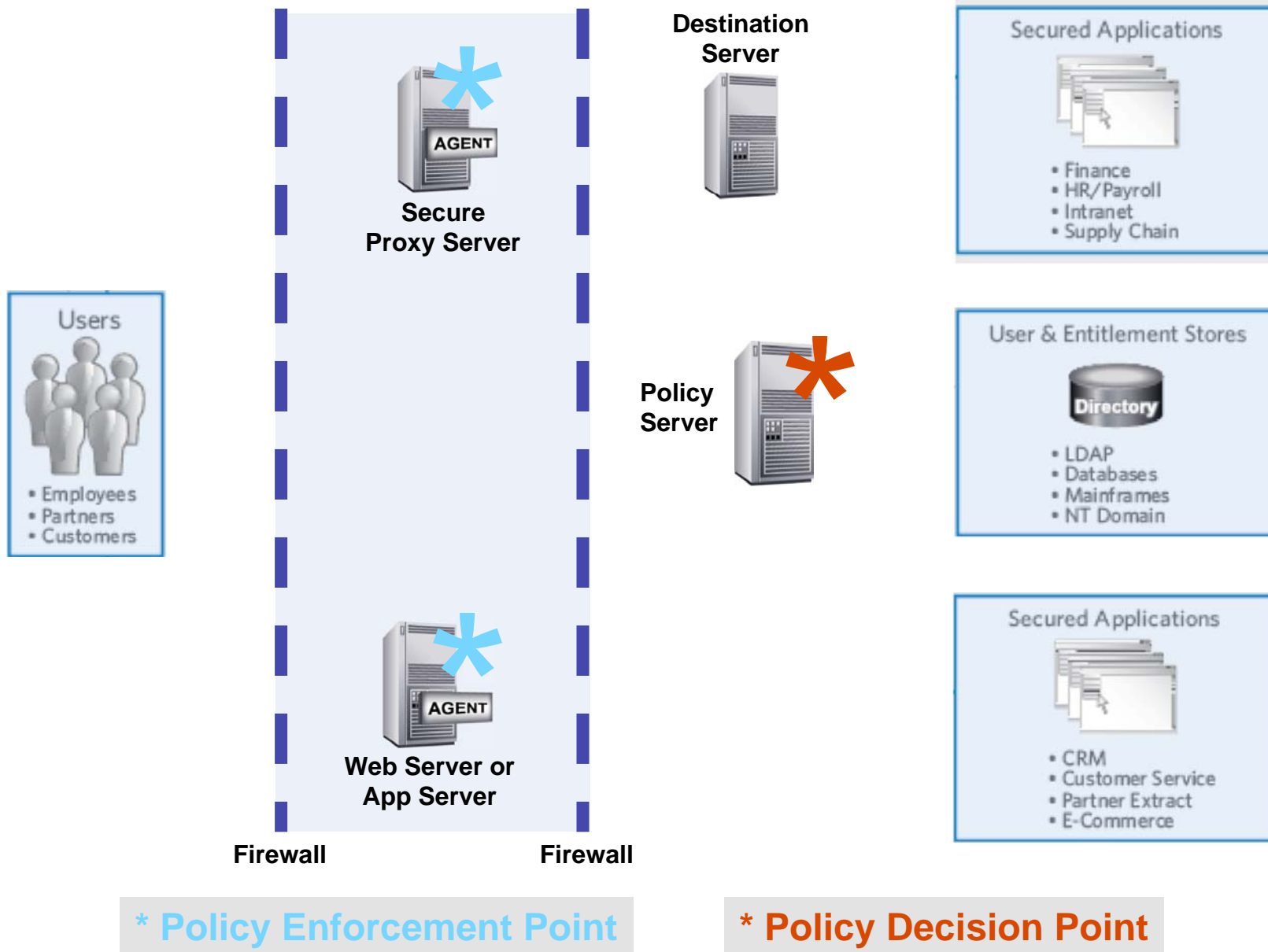
Typical Use Cases



Typical Use Cases



Audit Points



Auditing in WAM Model

- Each AC PEP/PDP typically maintains local logs
- Potential for many logs on different systems (web servers, proxy servers, application servers)
- May also leverage other logs (web server, app server...)
- Typically find PEP and PDP separate, so correlating the events can be challenging
 - Is there a SIM/SEM solution? May not be big enough problem to warrant this (see Host AC later)



Access Control Models

Host-Based Access Control

Host Access Control Functions

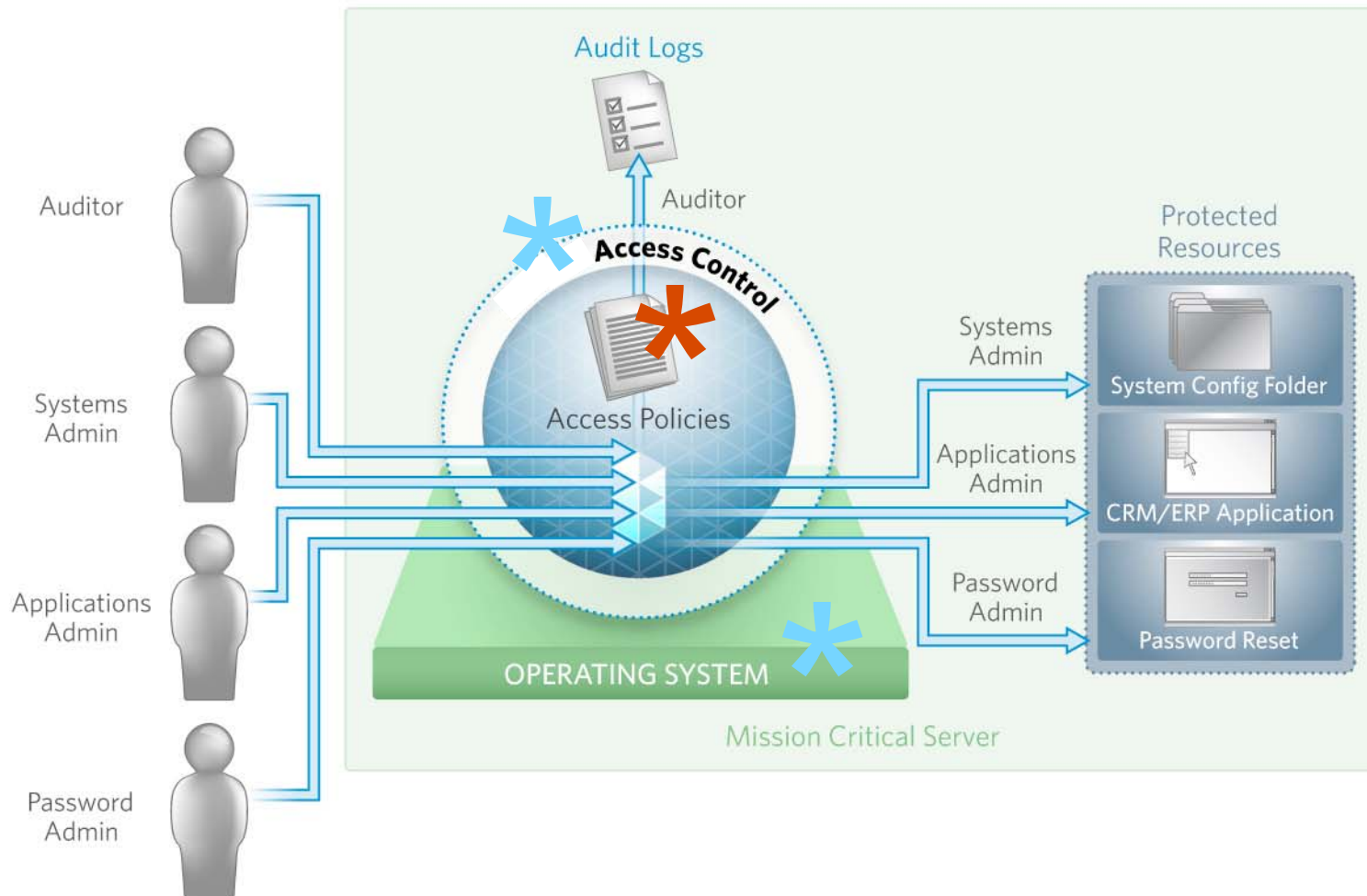


Fine-Grained Access Control

- Lock Down
 - Enforcement access control policies to protect files, folders, processes...
- Containment
 - Decompose the super user
 - Control all critical access by location, method, time
 - Limit privileges to minimal set necessary
- Separation of Duties
 - Provision rights by role
 - Eliminate shared accounts

Fine-Grained Access Control

Example: Separation of Duties



* Policy Enforcement Point

* Policy Decision Point

Auditing in Enterprise/Host Model

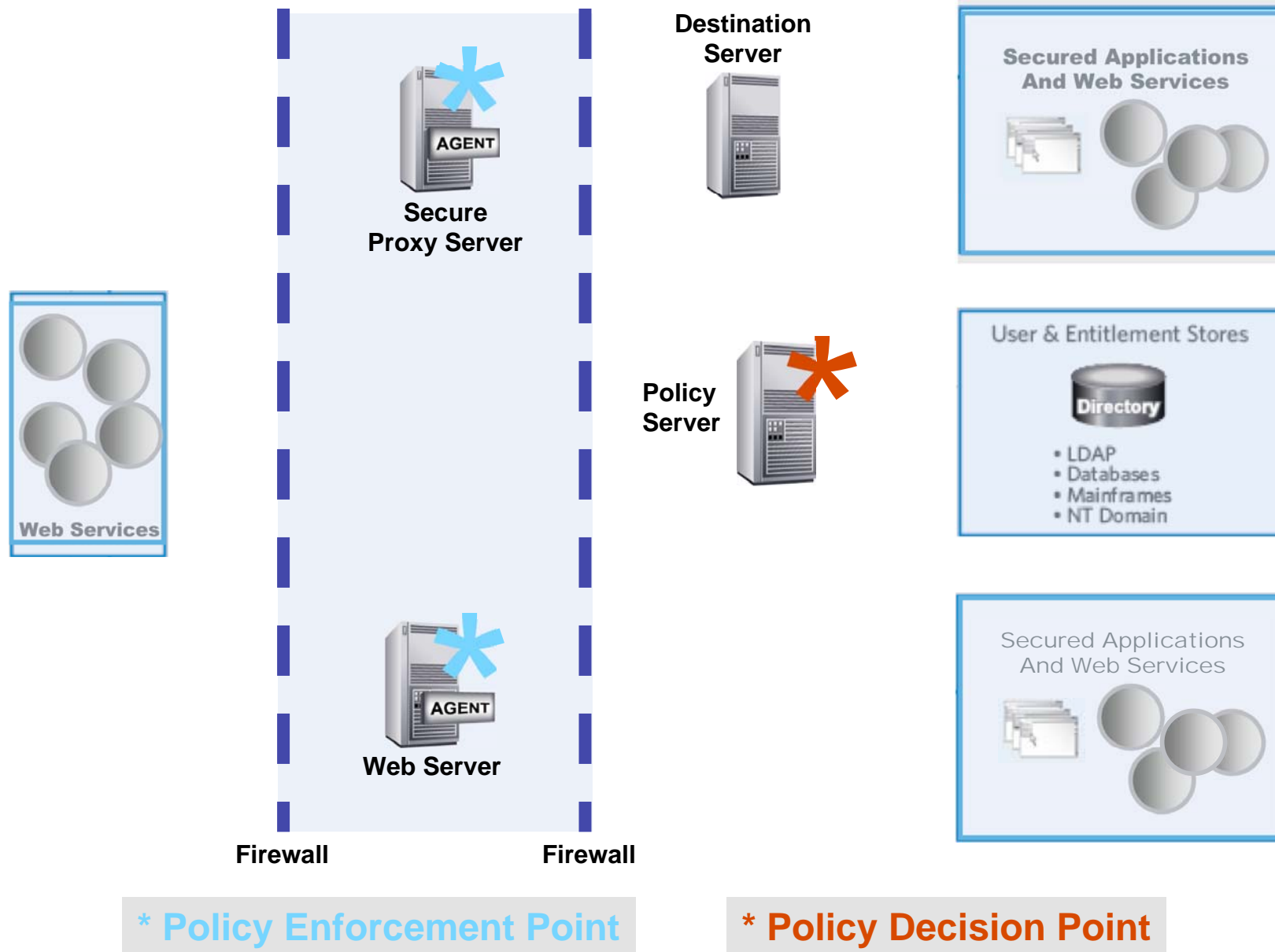
- Each host AC PEP/PDP typically maintains local logs
- Potential for hundreds of hosts
- Order of magnitude greater than WAM model
- May also leverage OS-level logs (syslog...)
- May find a SIM/SEM solution in place:
 - Harvest log file data
 - Perform data reduction, aggregation, normalization, correlation
 - Store data centrally for central reporting, auditing, operations
- If so, can make auditing much easier



Access Control Models

Web Services

Similar to WAM

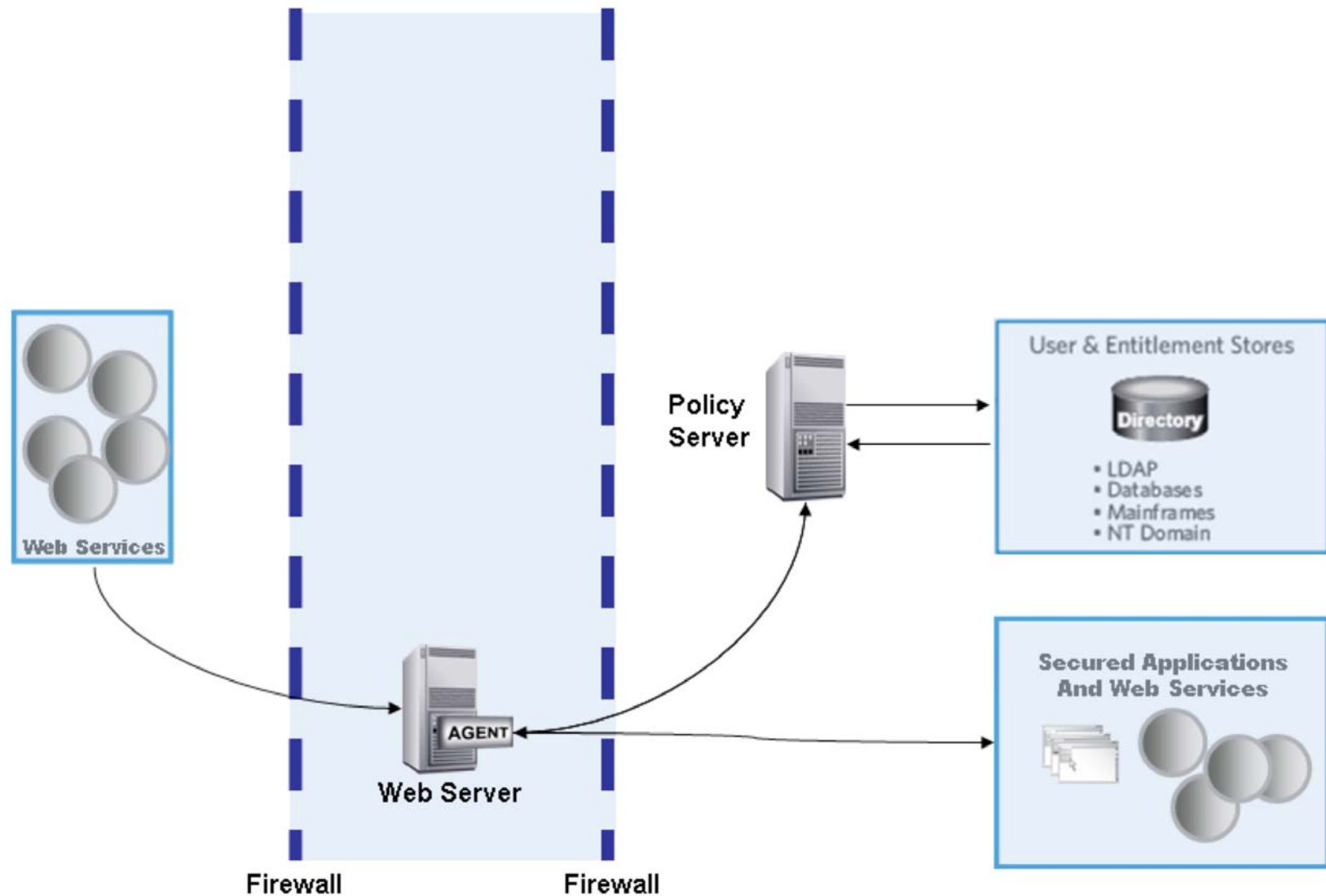


Web Services Security – Compounded Challenges

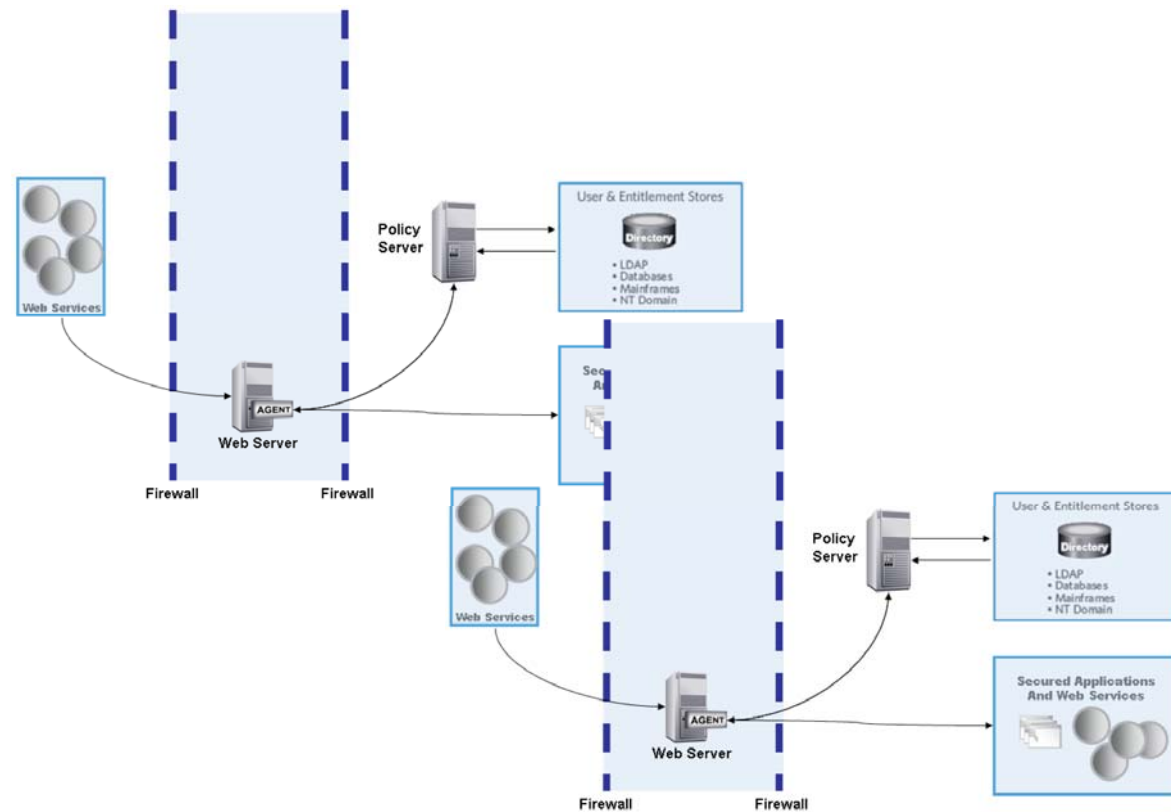
- Typical Web services use cases:
 - Single Web Service Request
 - Chained Web Service Requests
 - Multi-Step Web Service Requests
- Unlike WAM, more likely to involve multi-step transactions*

* WAM model may involve Federation, which can also result in chained events

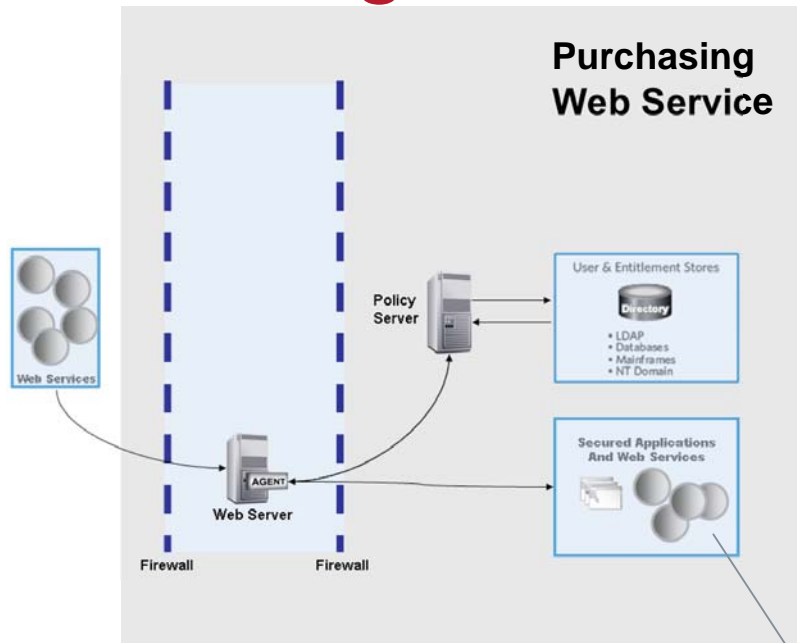
Chaining Web Services



Chaining Web Services

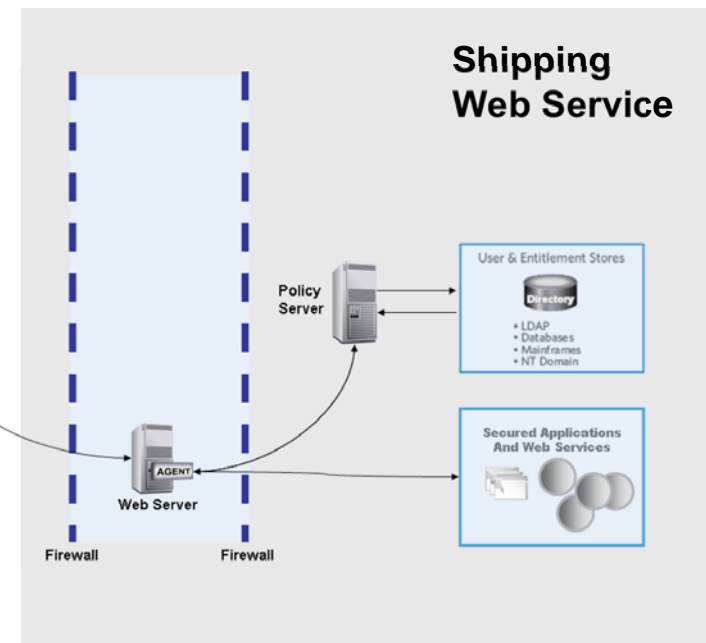


Chaining Web Services



- Multiple PDP's and PEP's

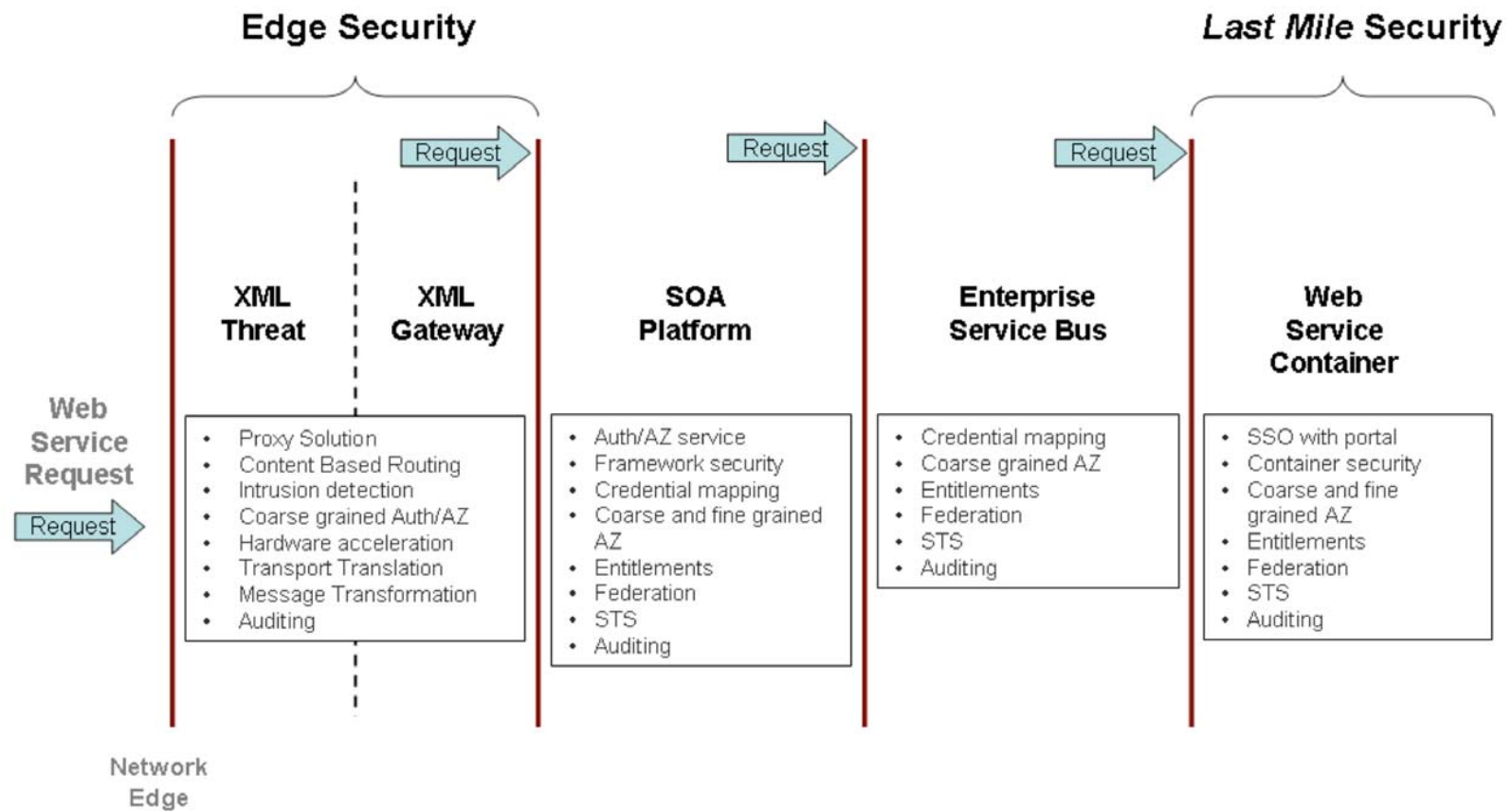
- Multiple points of audit



PEPs

- Web Service Container
 - App Server - .NET, WebLogic, WebSphere, JBOSS, CA SOA Security Manager
 - Web Server – IIS, Apache, SunOne, CA Security Manager
- Enterprise Service Bus (ESB)
 - Tibco, MQSeries, SonicMQ, webMethods
- SOA Frameworks
 - BEA AquaLogic, Oracle Fusion
- Edge/XML Firewall
 - Forum Systems, IBM (DataPower), Cisco (Reactivity), Vordel, Layer 7, CA SOA Security Manager
- More Layers
 - Mainframe, database, etc

Various Layers



Auditing in Web Services Model

- Similar to WAM model, unless architecture is NOT built off WAM architecture (e.g., different policy server PDP)
- PEP may be at the application level, the container level or third-party solution (e.g., CA SOA Security Manager)
- Web Services/SOA implementations will likely involve other security components as additional PDP/PEP's at the edge – e.g., XML Gateway



Auditing Access Control

Auditing Access Control

- In each of the 3 AC models, we have seen the major auditing points
- Aside from ensuring that the technology is simply able to log events, there are other considerations
- The following slide are some recommendations CA makes to its customers
- The degree to which you will see these recommendations implemented will vary considerably

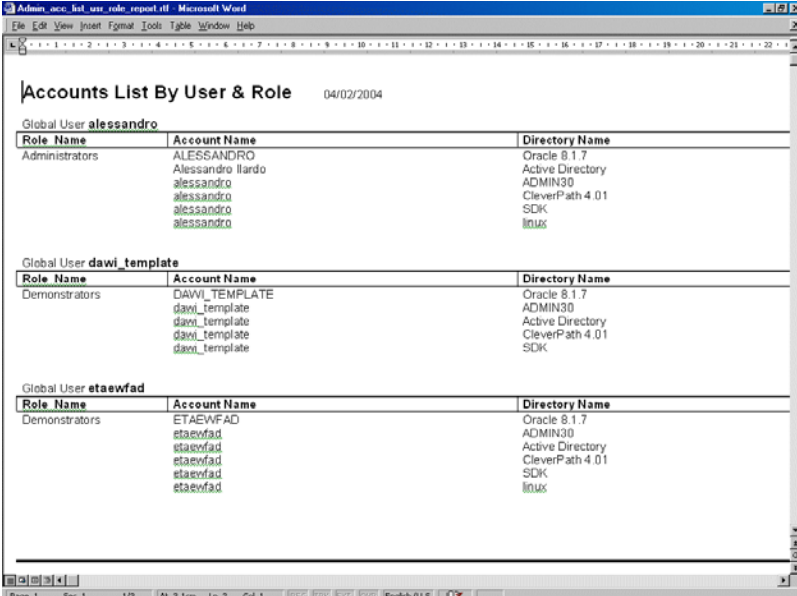
What We Tell Our Customers

- It is essential that all identity lifecycle management activities and access rights be audited
- The audit tools and information should fit within a recognised auditing methodology such as CobiT
- Activities include those of administrators as well as users, and cover the platforms, applications and administration tools
- It should be possible to link activities to the real identity of the people performing them rather than to anonymous system accounts
- It should also be possible to see the access rights belonging to each individual and to trace how those rights were acquired and under what authority
- The collection process should be tamper proof. E.g., administrators should not be permitted to disable auditing of their activities, or to alter the log of what they did
- The audit information should be transmitted across the network and stored securely
- Reports on the activities for different uses should be accessible
- It should be possible to raise alerts in real time when certain actions are detected (for example repeated failed access attempts)

If they follow our advice, this is what you should expect to see!!

Auditing/Monitoring: Proving Compliance

- User Based Reporting
 - What Accounts and Rights
- Role Based Reporting
 - Which Users
 - What Policies
- Policy Based Reporting
 - What Rights
 - Which Users
 - Accounts out of Policy
- Resource Based Reporting
 - Which Users
 - Which Policies



Accounts List By User & Role 04/02/2004

Global User alessandro

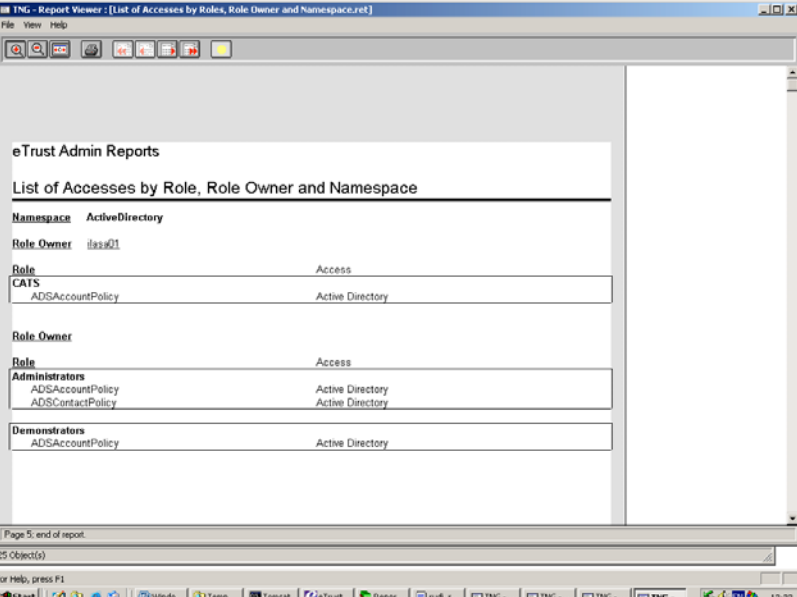
Role Name	Account Name	Directory Name
Administrators	ALESSANDRO	Oracle 8.1.7
	Alessandro Ilardo	Active Directory
	alessandro	ADMIN30
	alessandro	CleverPath 4.01
	alessandro	SDK
	alessandro	linux

Global User dawi_template

Role Name	Account Name	Directory Name
Demonstrators	DAWI_TEMPLATE	Oracle 8.1.7
	dawi_template	ADMIN30
	dawi_template	Active Directory
	dawi_template	CleverPath 4.01
	dawi_template	SDK

Global User etaewfad

Role Name	Account Name	Directory Name
Demonstrators	ETAEWFAD	Oracle 8.1.7
	etaewfad	ADMIN30
	etaewfad	Active Directory
	etaewfad	CleverPath 4.01
	etaewfad	SDK
	etaewfad	linux



TNG - Report Viewer: [List of Accesses by Roles, Role Owner and Namespace.rtf]

eTrust Admin Reports

List of Accesses by Role, Role Owner and Namespace

Namespace	ActiveDirectory
Role Owner	ilasso01
Role	Access
CATS	ADSAccountPolicy
	Active Directory
Role Owner	
Role	Access
Administrators	ADSAccountPolicy
	Active Directory
	ADSContactPolicy
	Active Directory
Demonstrators	ADSAccountPolicy
	Active Directory

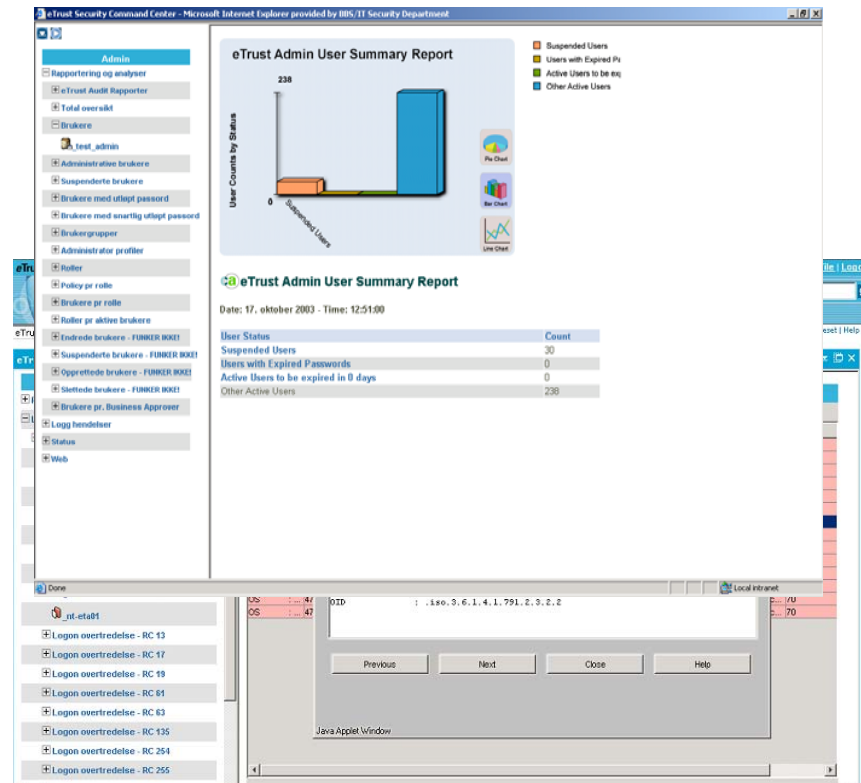
Page 5: end of report.

25 Object(s)

For help, press F1

Auditing – Who Did What?

- Changes
 - What changes were made
 - Who Requested Changes
 - Who Approved Changes
 - Who Made Changes
 - ...
- Access Attempts
 - Who logged on
 - Failed logons
 - Resource Access
 - Failed Accesses
 - ...



Summary

- Compliance is a fact of life, and it will only grow (more regulations are on the way!)
- The key to compliance automation is a comprehensive, integrated identity and access management platform
- Identify the AC Model – Web, Host, and Web Services
- Identify the Policy Decision and Policy Enforcement Points
- Don't forget the other half of the equation – Identity Management
- Log files are critical; they must be protected (AC and SOD) and ideally shipped away to a secure, centralized repository



THANK YOU

Introduction to Access Management

J. Tony Goulding CISSP, ITIL

Security Solution Strategist, CA Inc.

tony.goulding@ca.com

