规划IT蓝图 提升业务价值

IBM服务管理用户大会

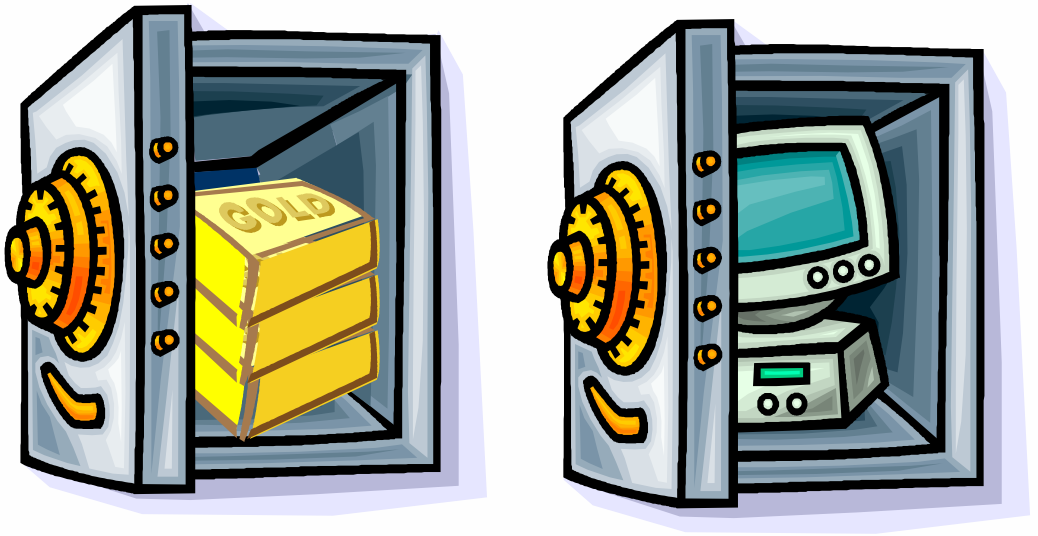
面向IT治理，多方位提升安全管理能力

IBM Tivoli安全解决方案概述

提纲

- **IBM安全解决方案定位**
- **IBM Tivoli 身份管理解决方案**
- **IBM Tivoli 风险及符合性管理**

身份管理、风险和符合性管理
Identity, Risk and Compliance Management



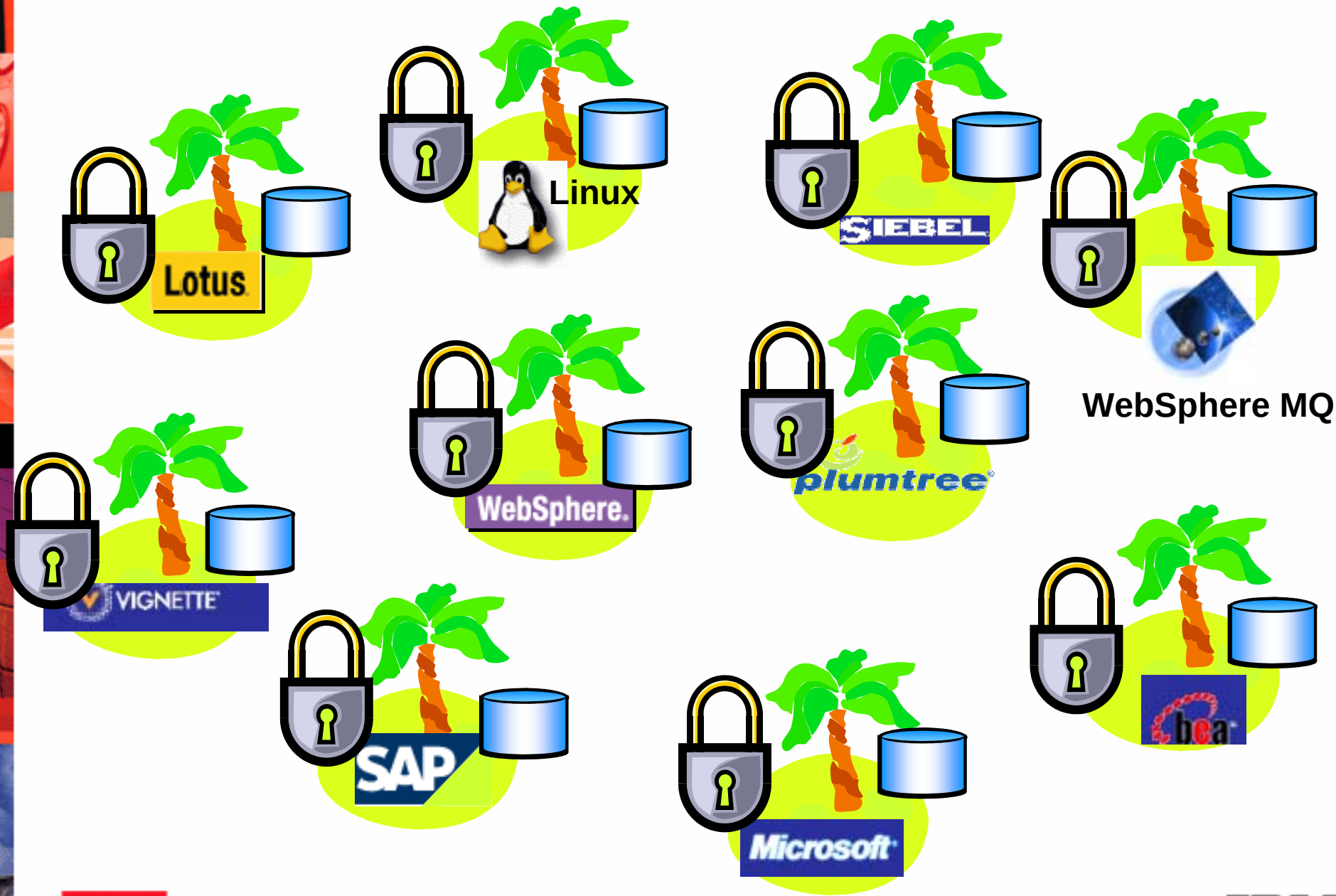
“IT Security is like guarding Fort Knox” . . .

U.S. Gold Bullion Depository in Kentucky.

典型IT安全的定义

任务	Fort Knox的观点	IT安全定义
基础 "It's in there"	*保卫金子"*	• *控制数据以确保私有性、完整性和保密性*
	在需要的时候可以到金子"	• *在需要的时候和地点提供信息I信息服务*
身份管理 Tivoli	*"需要访问? 给我看你的ID!"*	• *检验身份，并且控制访问*
	设置安全策略，并且遵照策略进行管理"	• *定义安全策略、规则，并且遵照执行*
网络安全 IGS *符合性管理* Tivoli	*"知道谁对于金子做了什么操作"*	• *跟踪动作I事件以鉴别每个人I实体的行为*
	"监控以确保所有任务都在正常工作"	• *检验以确保所有的都按照设计在进行工作*

业务不断发展，越来越多的安全孤岛，帐号多，认证多，授权复杂，审计分散...



安全孤岛的问题和管理需求

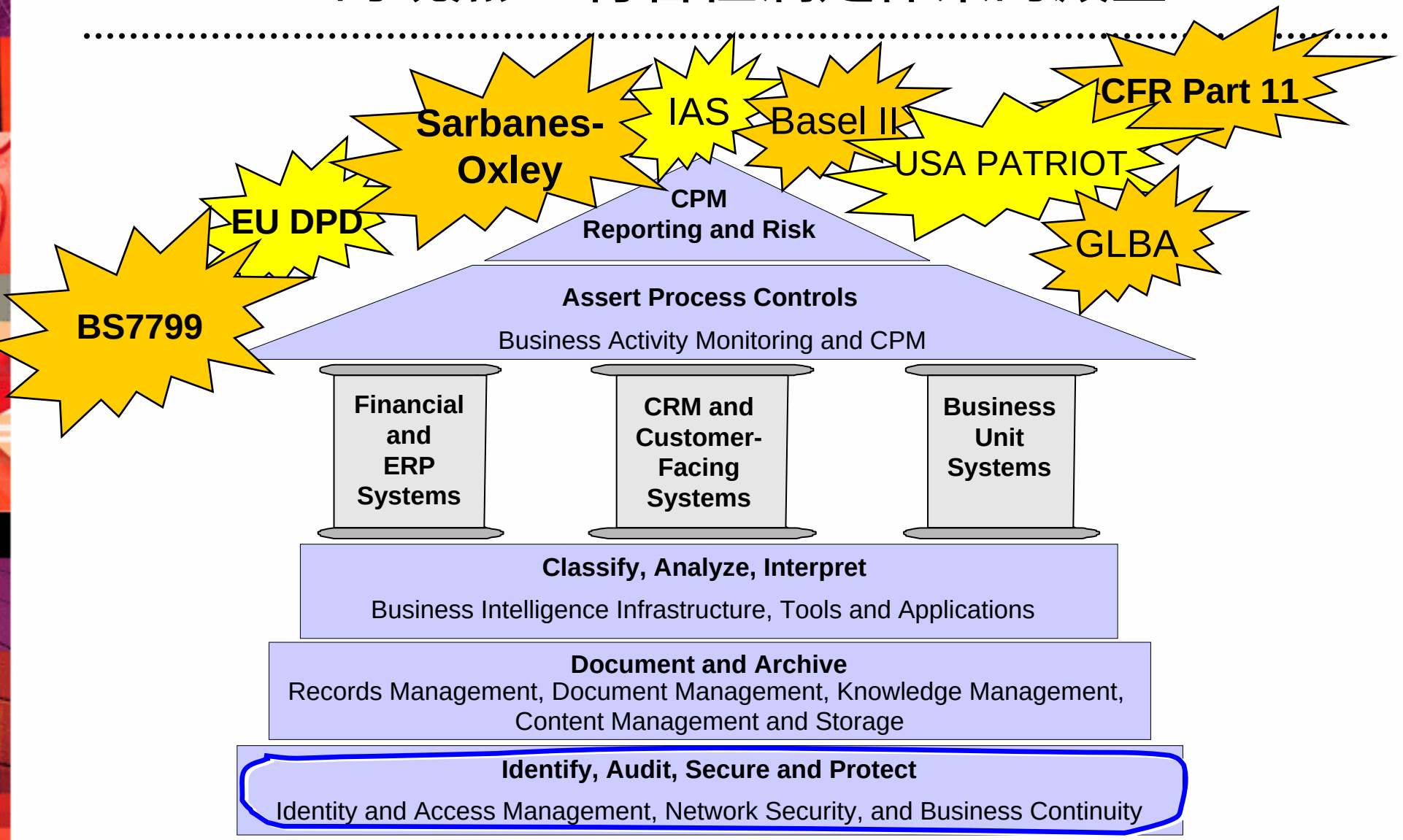
<u>身份管理</u>

- 太多的身份存储，错误数据 & 安全暴露
- 太多的身份管理点，居高不下的身份管理费用
- 薄弱的/不一致的管理，安全/符合性问题
- 太多的口令—工作效率,安全 & 符合性问题
- 分散的, 不一致的授权/访问控制
  - 一般企业：安全和符合性问题
  - 大型企业: 同上问题 + 进入新市场的挑战
- 审计的安全，安全的审计

<u>网络安全和符合性管理</u>

- 网络安全暴露 外部/内部的攻击
- 服务器 & 桌面系统违反安全策略
- 对于攻击反应迟缓，无法及时作出判断
- 内部攻击，对内部特权用户无法作出安全、全面的审计

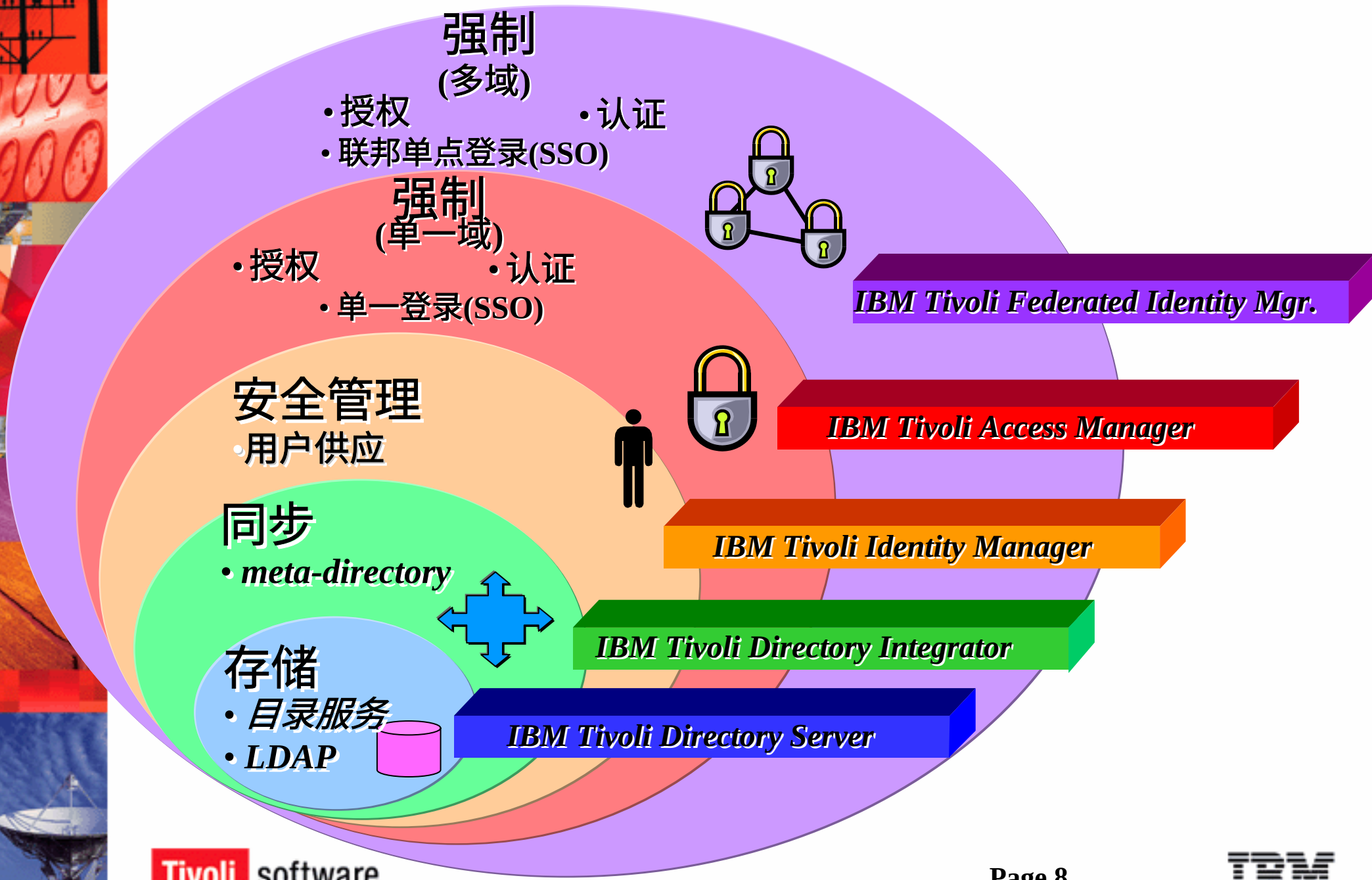
Gartner's 的观点— 符合性满足体系的殿堂



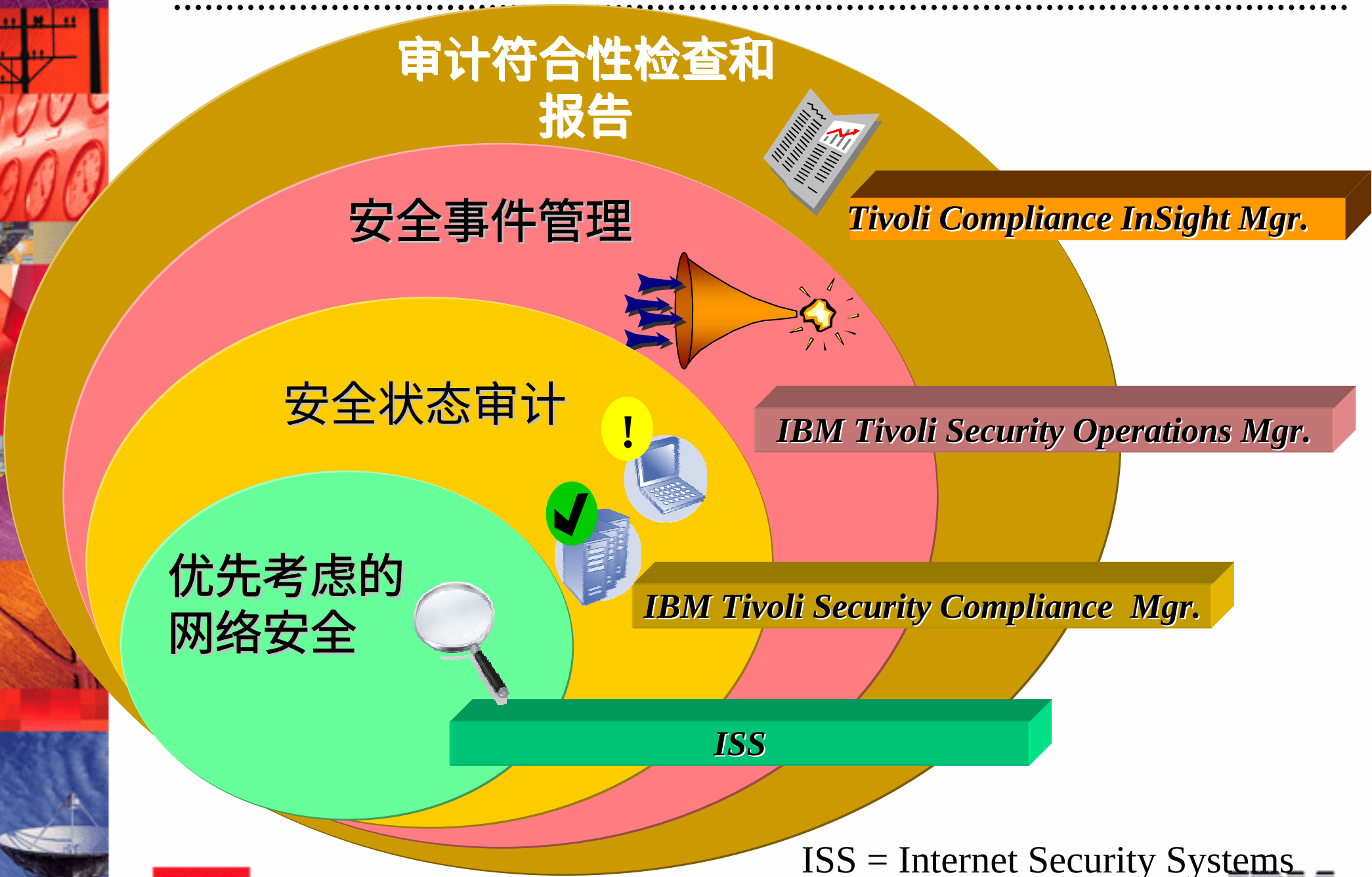
Acronym Key

CFR = Code of Federal Regulations
CPM = corporate performance management
CRM = customer relationship management
ERP = enterprise resource planning
EU DPD = European Union Data Protection Directive
GLBA = Gramm/Leach/Bliley Act
IAS = International Accounting Standards

基于身份的安全管理


强制
(多域)
• 授权
• 认证
• 联邦单点登录(SSO)
强制
(单一域)
• 授权
• 认证
• 单一登录(SSO)
安全管理
• 用户供应
同步
• meta-directory
存储
• 目录服务
• LDAP
IBM Tivoli Federated Identity Mgr.
IBM Tivoli Access Manager
IBM Tivoli Identity Manager
IBM Tivoli Directory Integrator
IBM Tivoli Directory Server

优先考虑的网络安全和符合性管理



ISS = Internet Security Systems

Tivoli software

IBM

Tivoli software

IBM

Tivoli 身份管理解决方案

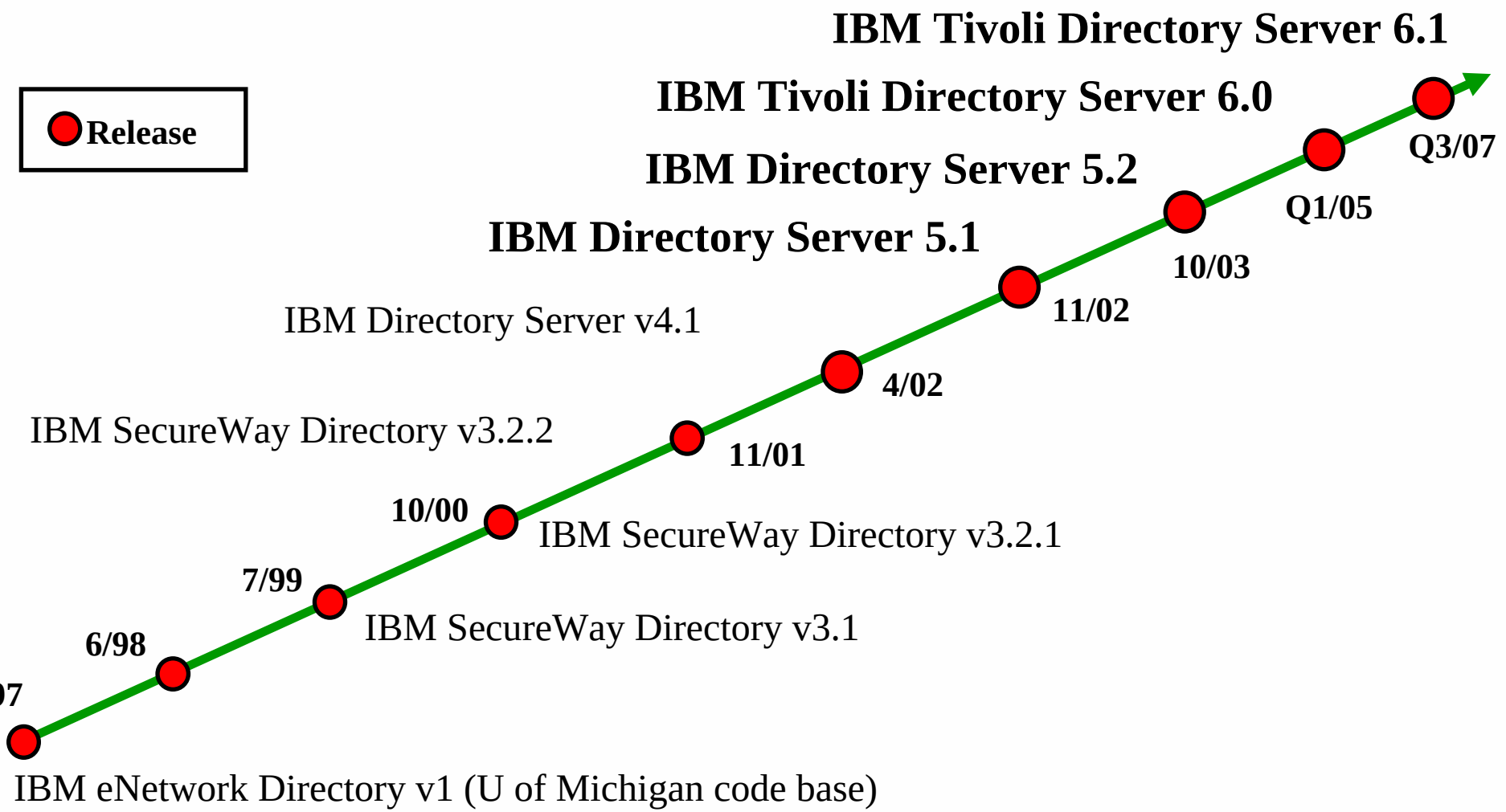
e business software

IBM Software Group

身份管理之一、用户目录

解决客户问题
- 太多的身份存储， 错误数据, 安全问题暴露和高昂的费用

Tivoli Directory Server，遵循LDAP v3标准的目录服务器



IBM Directory Server

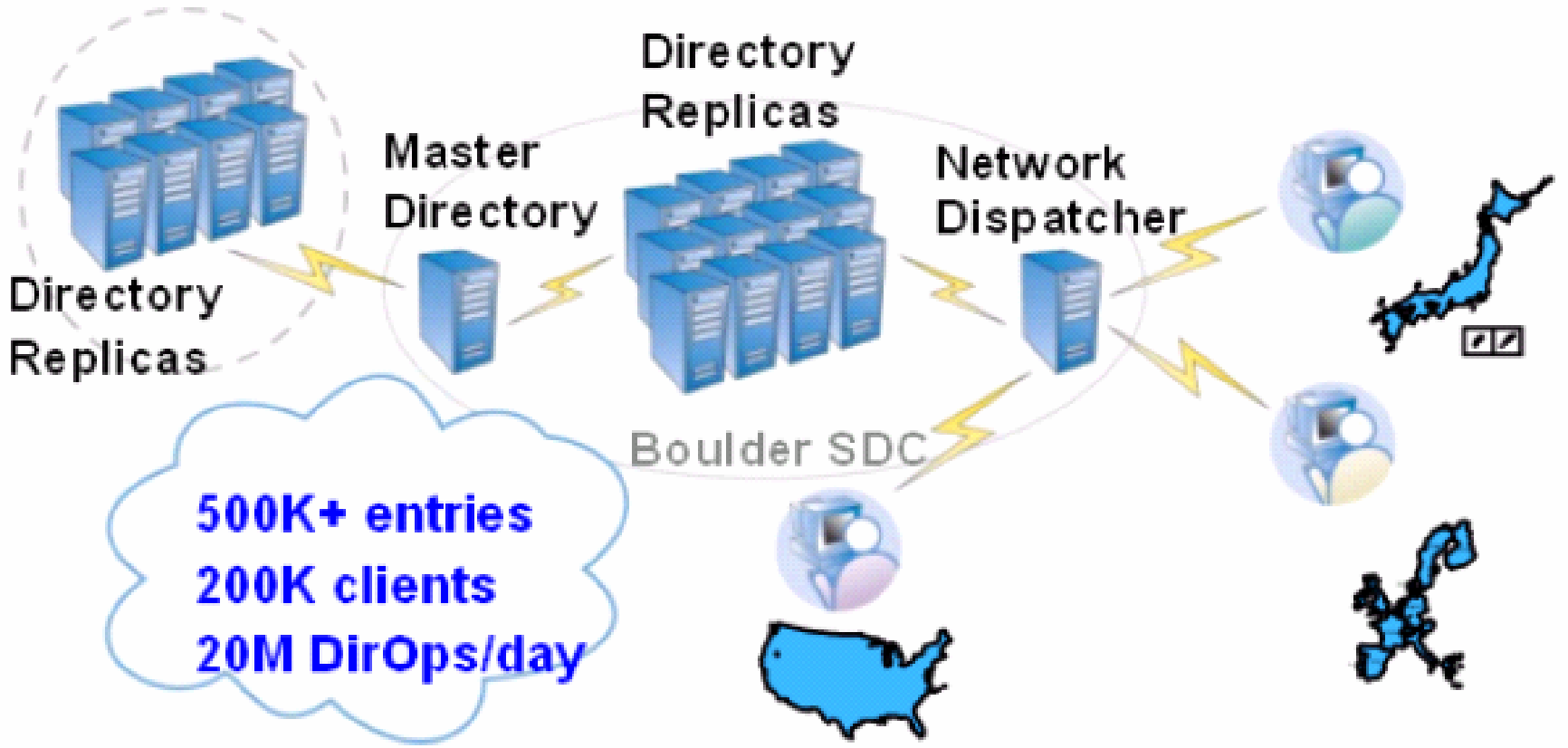
- 一个具有高度可靠性的、可扩展的、基于标准的LDAP服务器
- The Open Group LDAP v3 认证

- 运行在多种平台上，包括UNIX、Linux、Windows、AS/400等

- 多种复制模式，(S-M，M-M)
- 提供多种复制和高可用性机制
- 支持按属性进行复制机制

- 提供多种数据加密算法
- 支持关键属性加密

w3.ibm

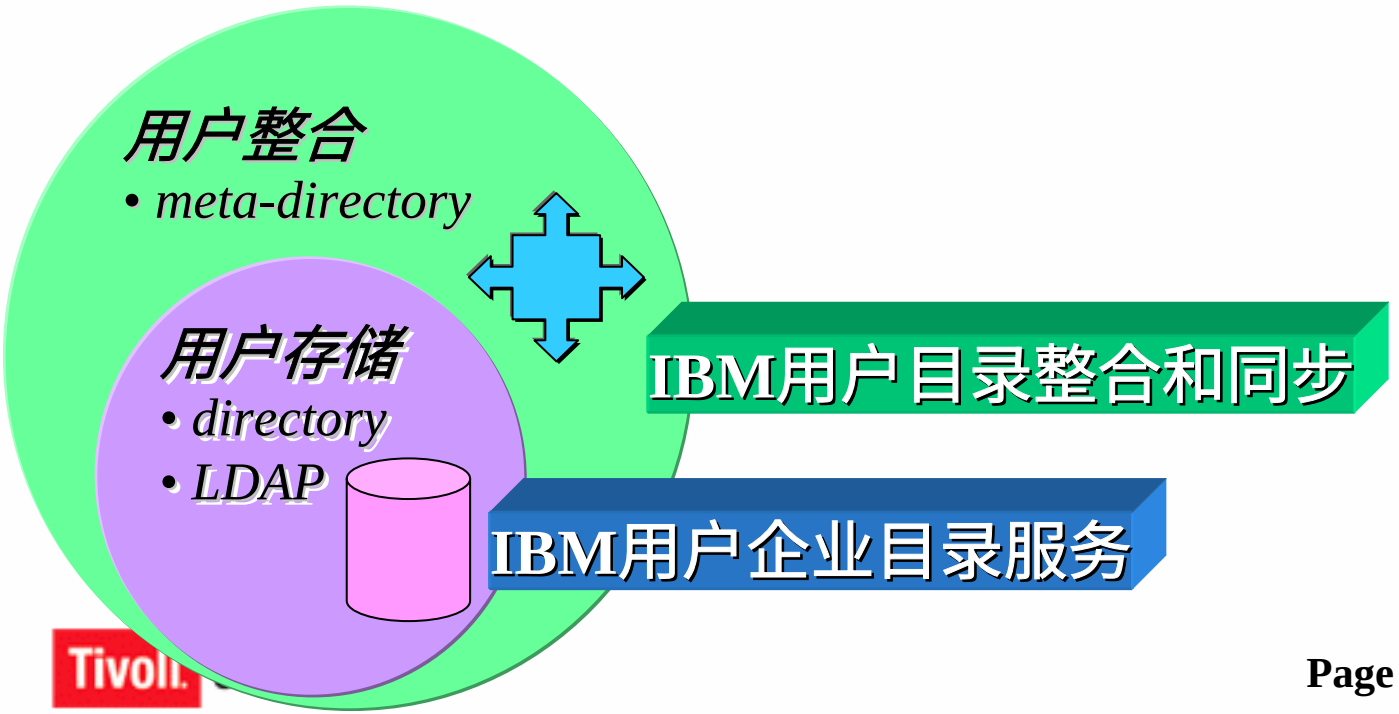


IBM directory-exploiting applications

Blue Pages, Common Web Authentication, PBCs, Expenses, Mobility 2000, Sametime Messaging, etc.

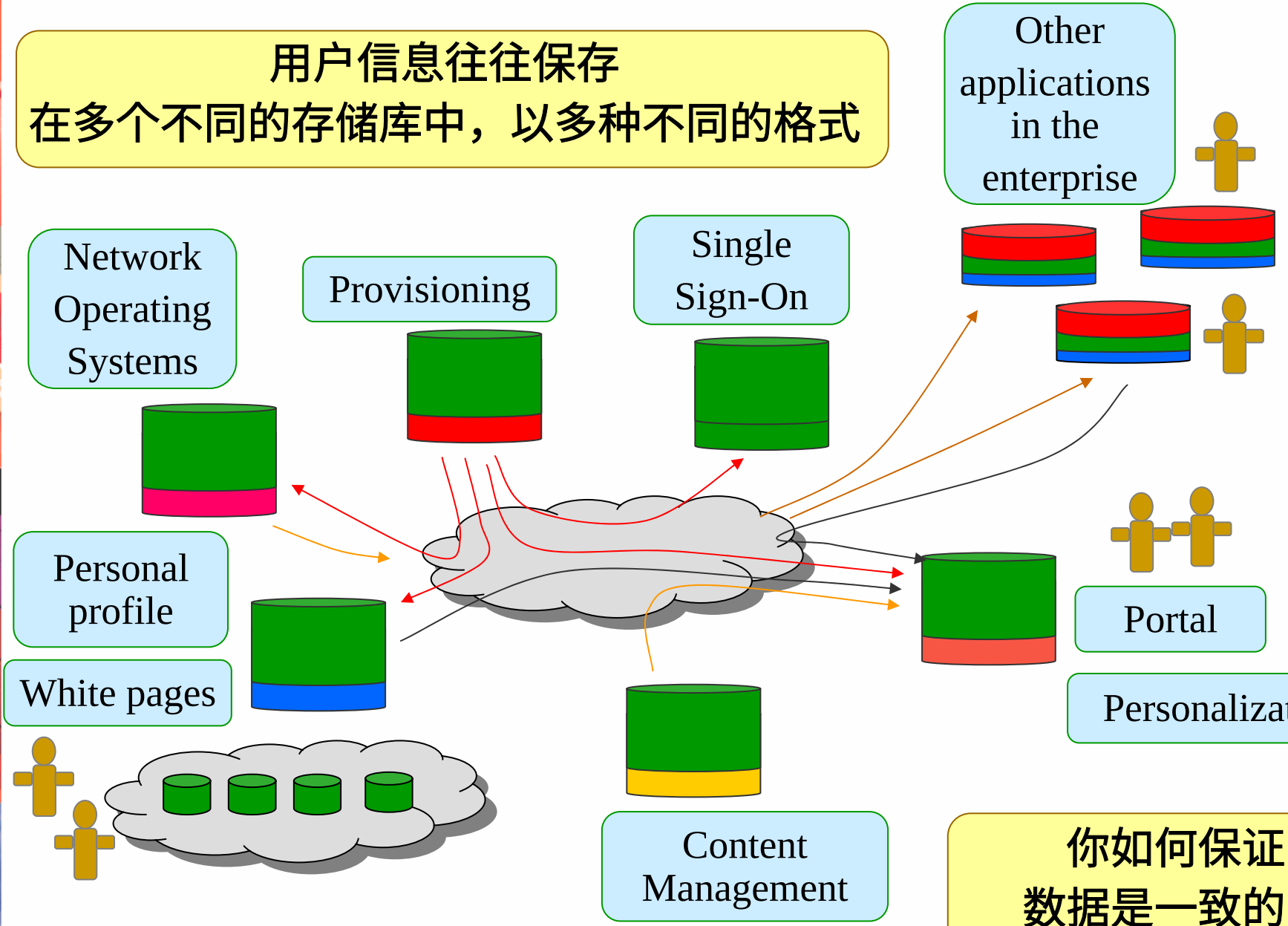
身份管理之二、用户信息整合

解决客户问题
- 太多的身份存储，数据难以同步和纠错, 安全问题暴露



用户目录保持一致性的困难

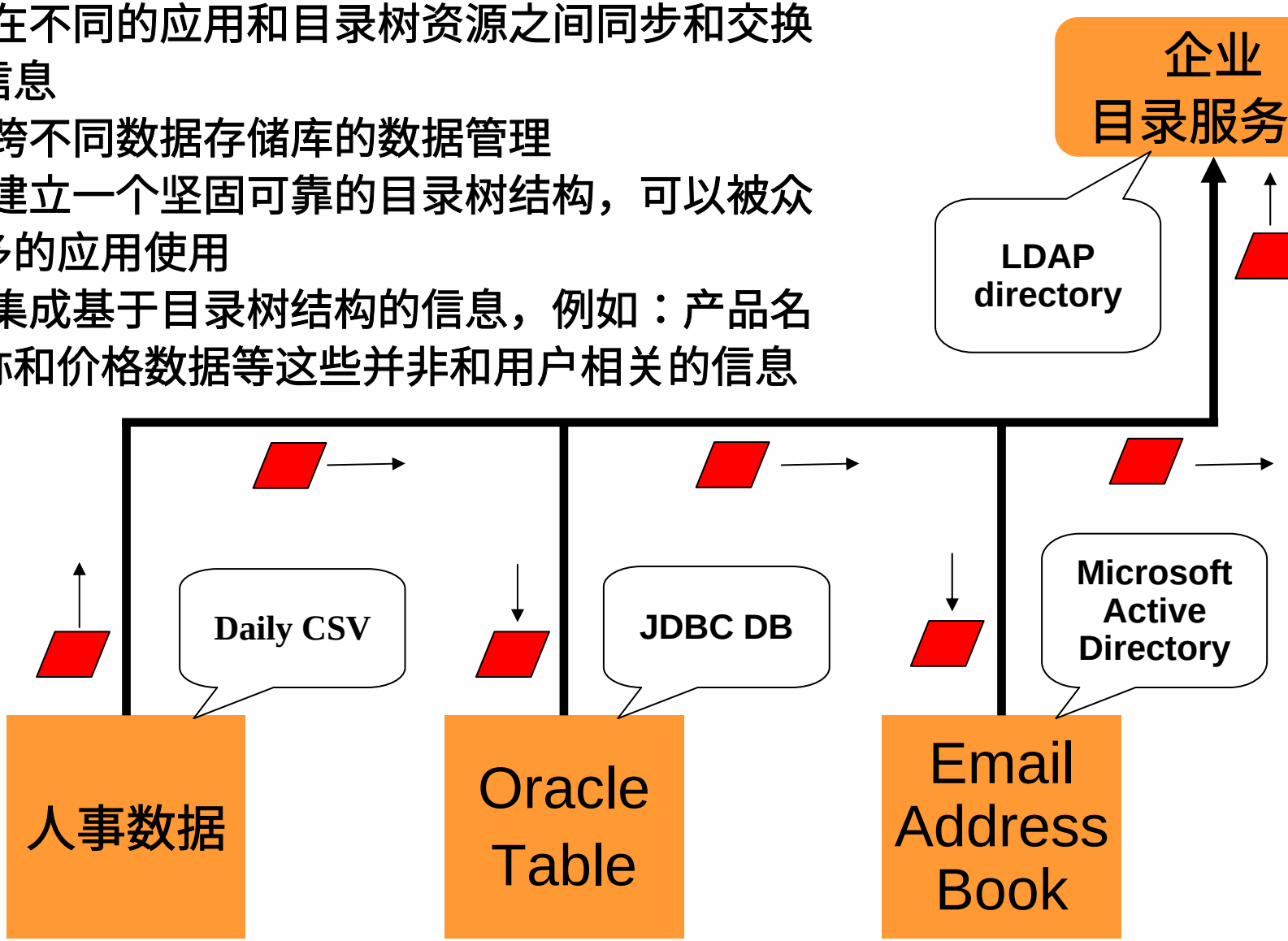
用户信息往往保存
在多个不同的存储库中，以多种不同的格式



你如何保证
数据是一致的？

IBM Directory Integrator：目录整合工具

- 基于策略的应用目录信息单向/双向同步
- 在不同的应用和目录树资源之间同步和交换信息
- 跨不同数据存储库的数据管理
- 建立一个坚固可靠的目录树结构，可以被众多的应用使用
- 集成基于目录树结构的信息，例如：产品名称和价格数据等这些并非和用户相关的信息



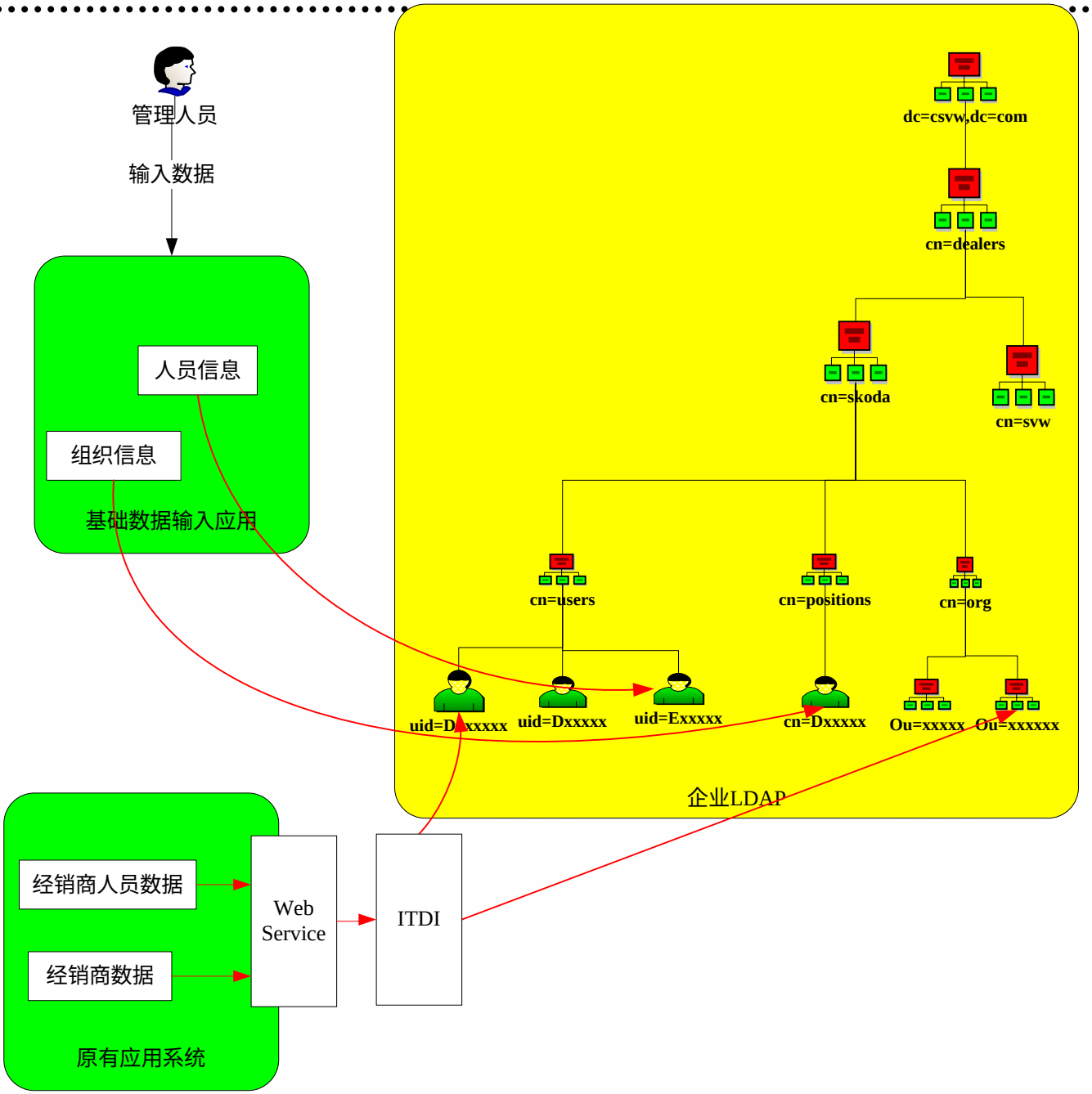
IBM Directory Integrator特性

- 纯Java产品，支持多种平台
- 配置文件基于XML文件，易于移植
- 提供超过三十种的数据连接器

• Active Directory LDAP	• IBM Tivoli Access Manager	• Lotus Notes
• Active Directory Changelog	• “Sub” AssemblyLine Caller	• HTTP Client
• Command Line	• IBM Tivoli Identity Mgr. Agent	• Old HTTP Server
• DSML v2	• JDBC	• PeopleSoft
• Domino Change Detection	• JMS Pub/Sub	• Persistent Entry Store (PES)
• Domino R5 & R6	• JNDI (Generic)	• RDBMS Changelog
• Domino Users	• LDAP Server	• SAP R/3
• FTP Client Connector	• MQe Password Store	• Siebel 7.5.3
• File System Connector	• Mailbox	• SNMP
• HTTP Client	• IBM MemQ	• Script
• HTTP Server	• Memory Stream	• TCP
• TDS/iPlanet/… LDAP	• XML/XSL Handlers	• Timer
• TDS/iPlanet/… Changelog	• CSV & Fixed Format Parsers	• URL
• Domino LDAP	• “In-Flight” Data Transformers	• Web Service Client
• Domino Changelog	• Cronjob/Timer	• Web Service Server

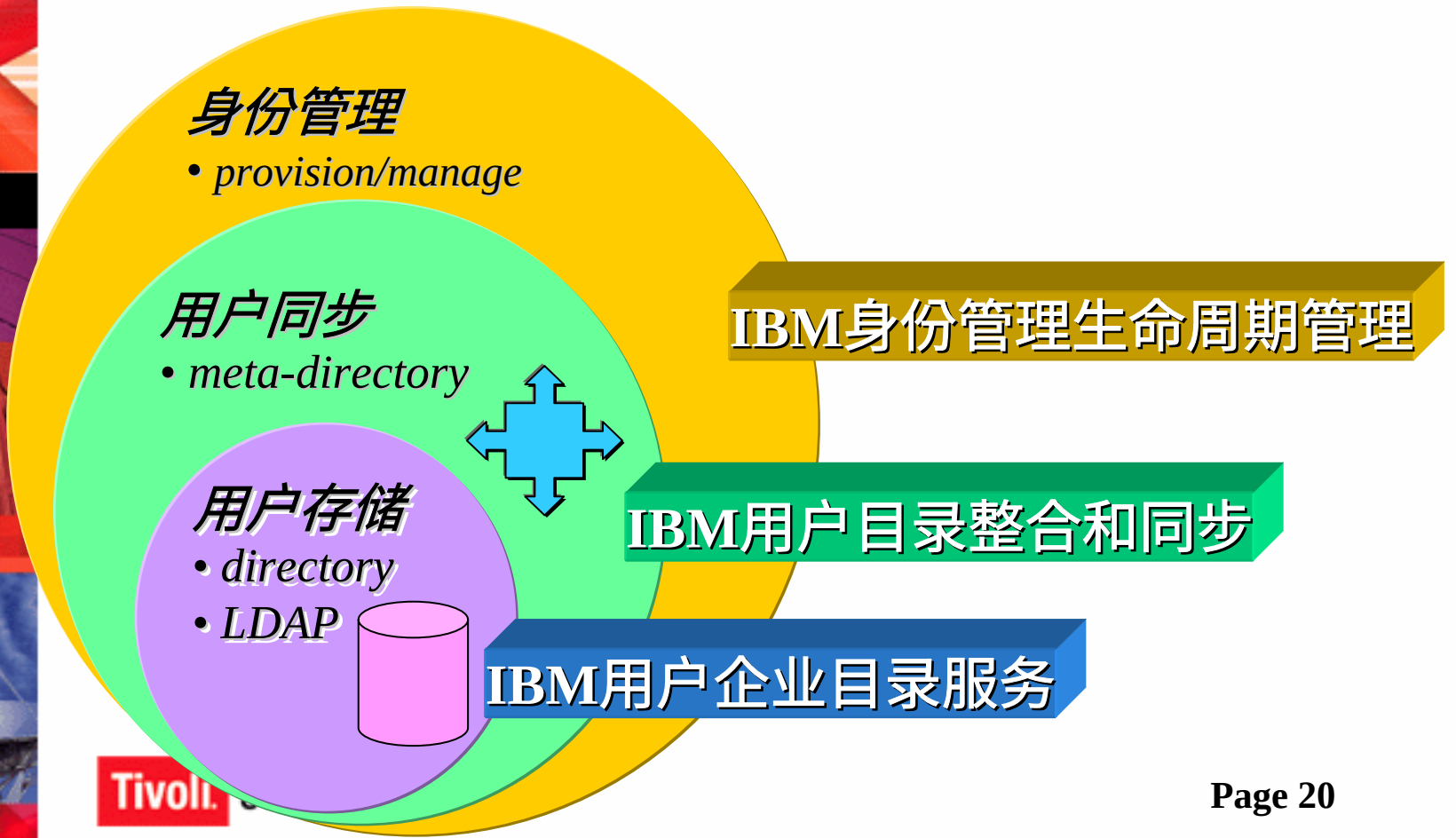
- 提供对商业逻辑的处理机制
  - 多种的驱动机制
  - 错误处理HOOK机制
- 基于Java/Java Script的扩展
- 服务器模式提供长期运行监控

TDI提供目录数据的策略同步服务



身份管理之三 ：统一用户身份管理

解决客户问题
- 太多的ID管理点，高昂的身份管理费用
- 薄弱的/不一致的管理，存在安全和符合性问题
- 满足审计的要求



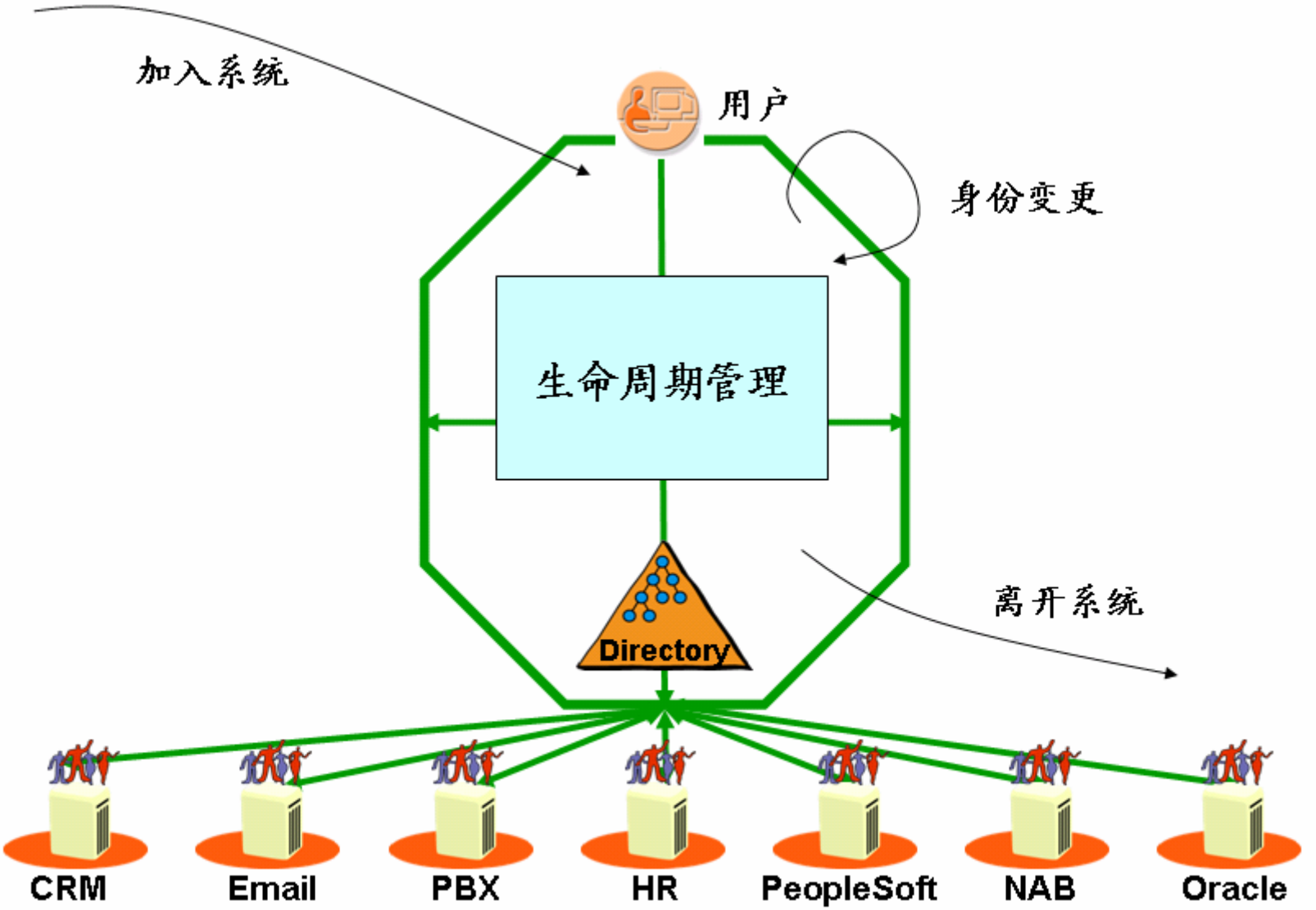
理想的企业身份管理平台是能够建立身份和帐号的关联关系，保护信息资产。

身份注册创建 → 帐号分配和授权 → 用户访问和审计 → 清理和身份中止

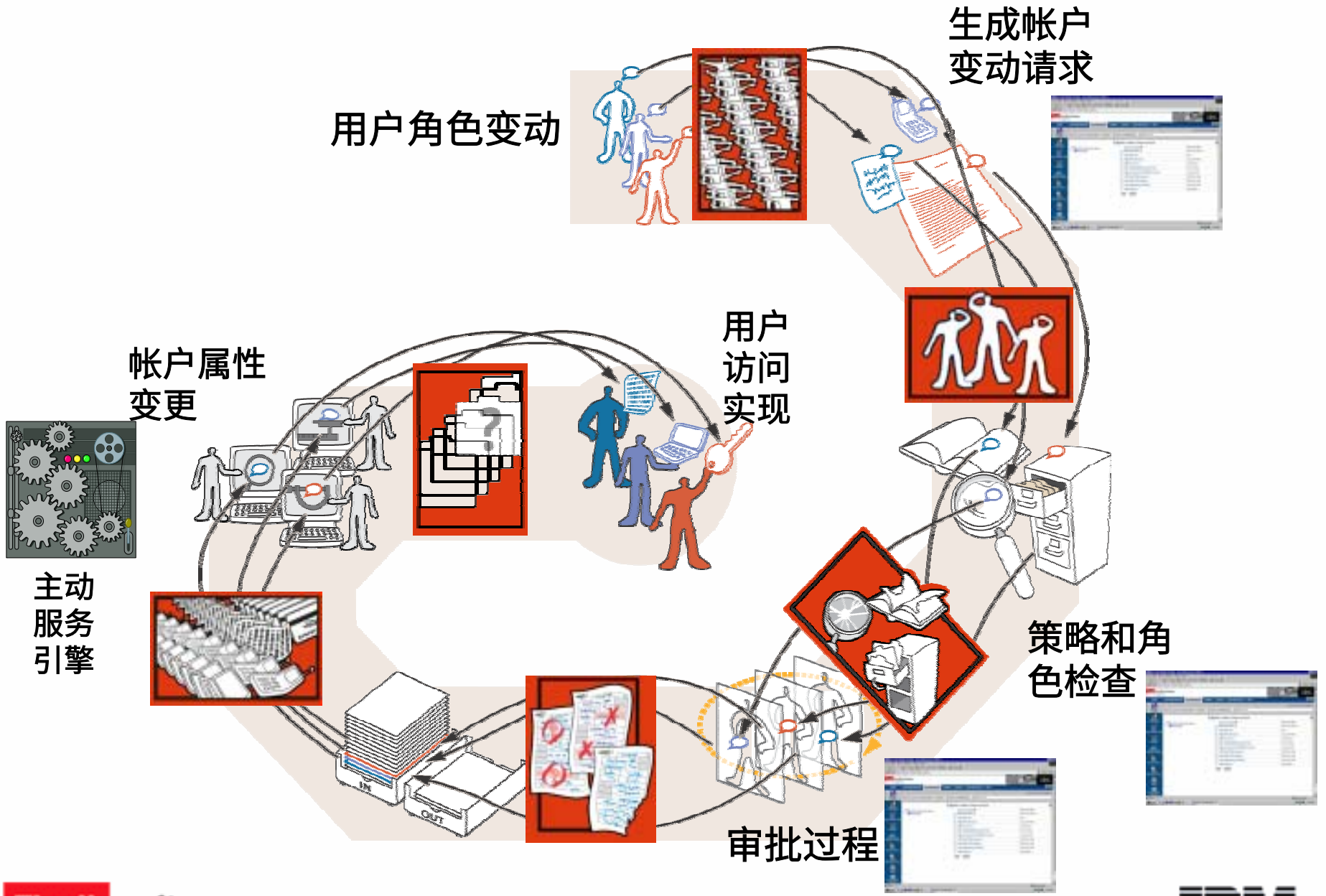
- 为用户创建身份和角色信息。
- 基于角色和职责，为用户创建相应的帐号和密码。
- 用户安全的、简单的访问IT系统。
- 挂起或中止用户身份和相应帐号。

用户角色变更

Tivoli Identity Manager 提供用户身份生命周期管理

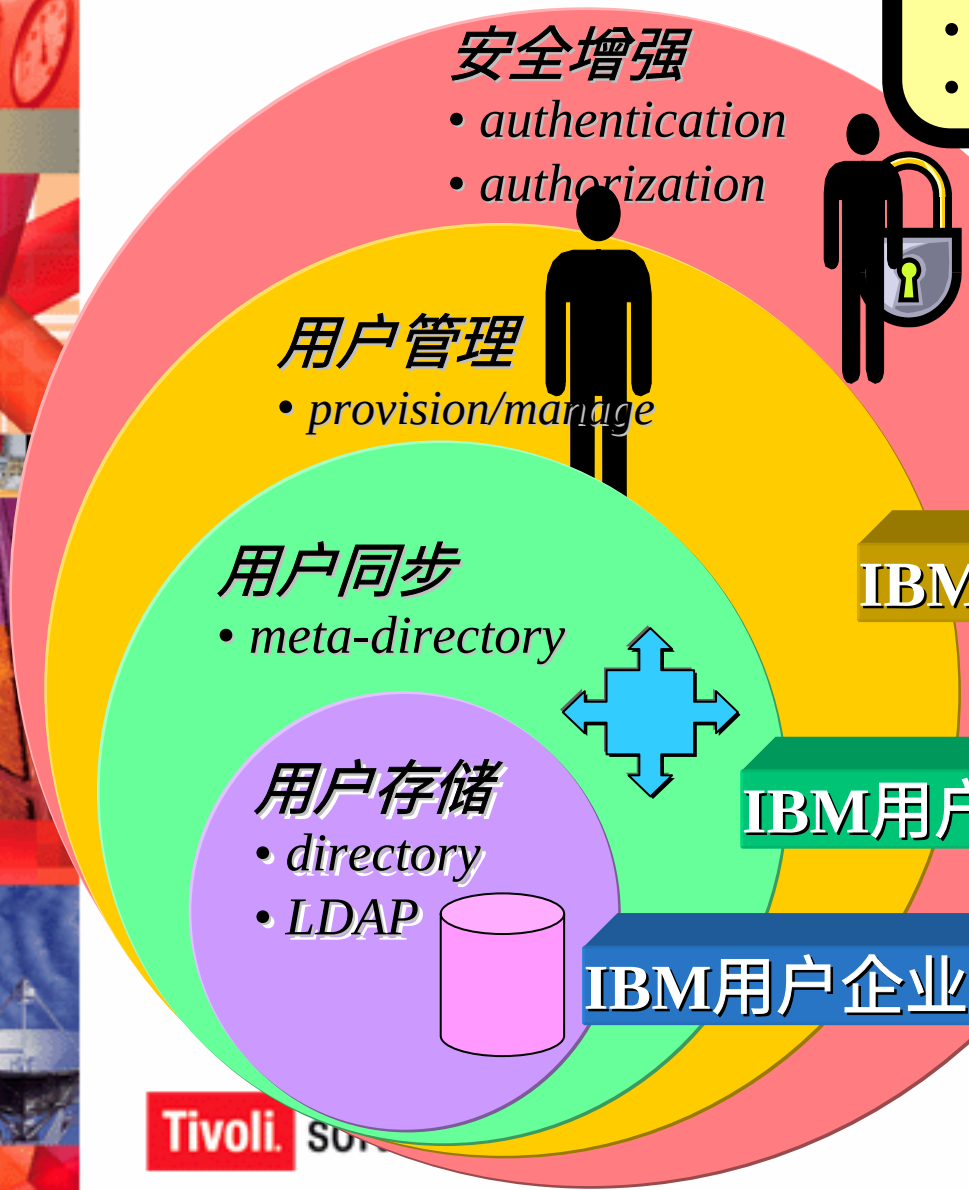


基于用户角色的用户身份主动服务



身份管理之四：安全访问和认证授权

解决客户问题
- 薄弱的/不一致的管理
- 分散的, 不一致的授权/访问控制
- 提高访问效率和管理效率
- 满足审计的要求



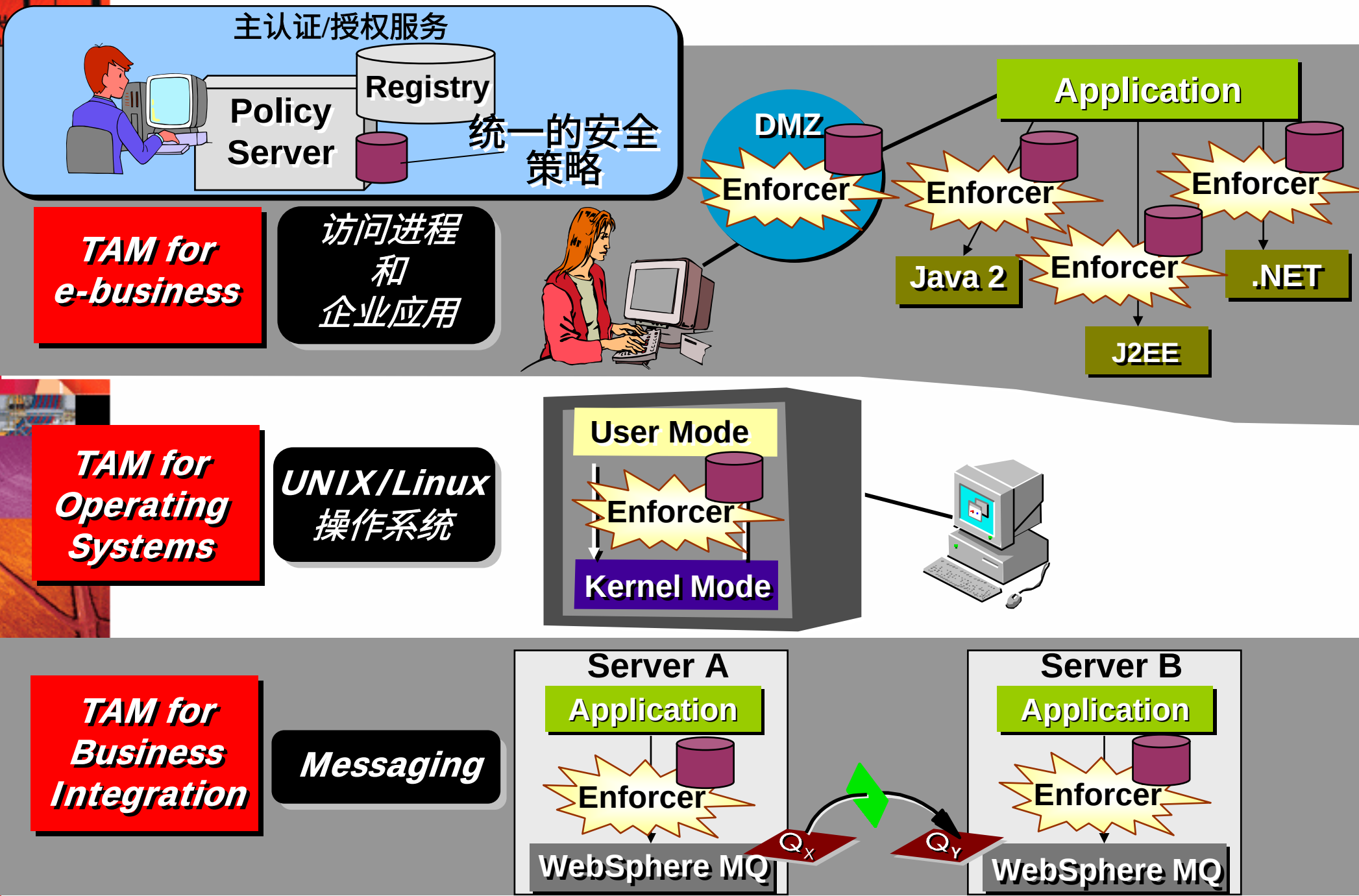
IBM应用访问集中认证和授权服务

IBM身份管理生命周期管理

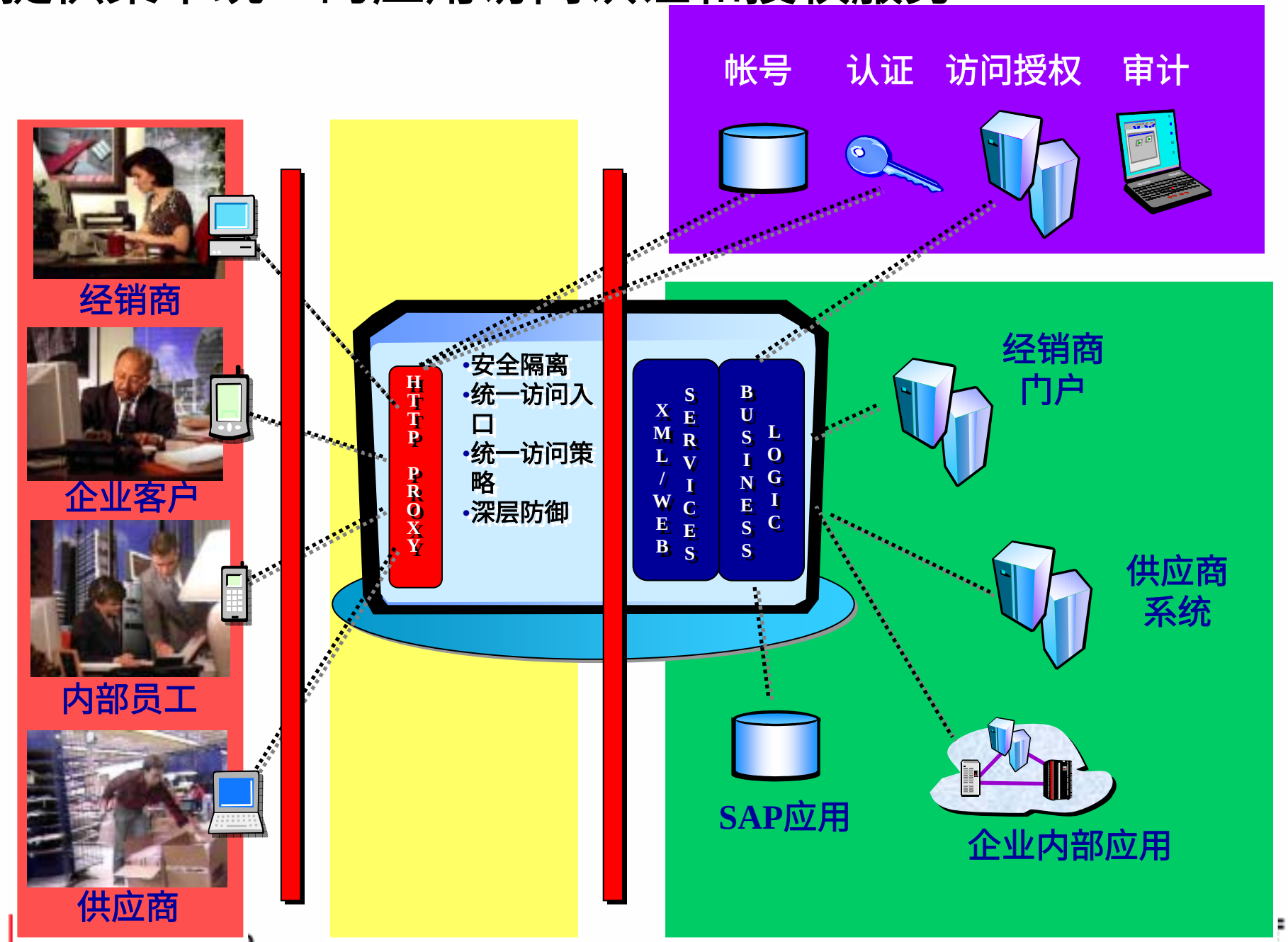
IBM用户目录整合和同步

IBM用户企业目录服务

TAM产品家族—单一策略、多个强制控制点

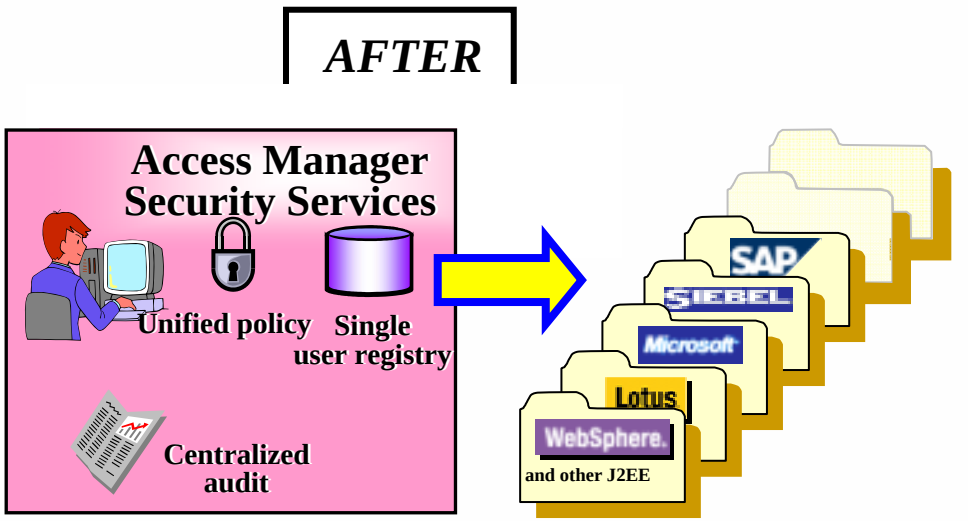


Tivoli Access Manager for eBusiness
提供集中统一的应用访问认证和授权服务



Tivoli的访问控制解决方案

- 太多的口令需要记忆
- 多个管理域，多个访问控制工具
- 到处都是用户和访问控制信息
- 策略依从性?



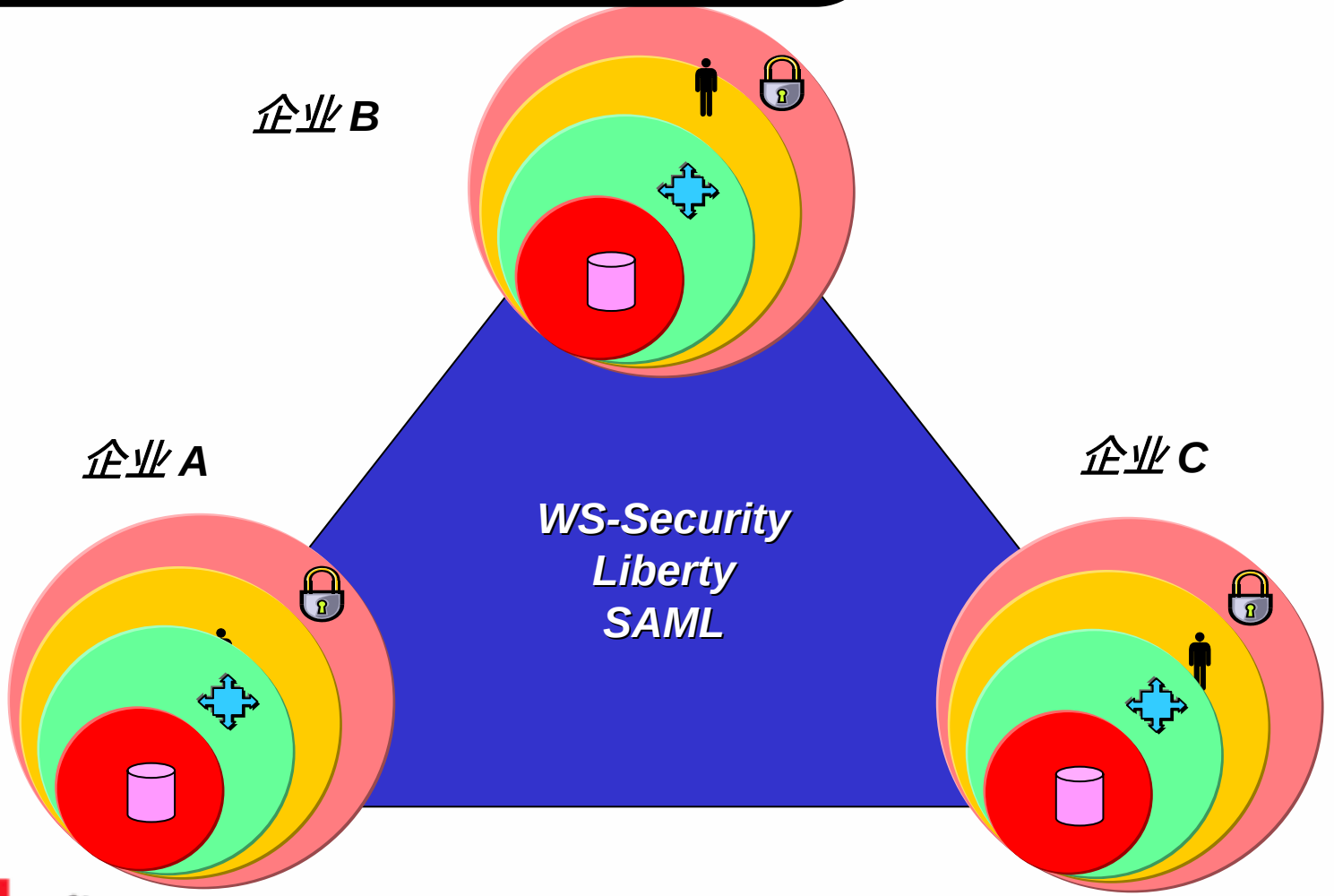
- Web单点登录
- 单一安全域，或者是基于单一工具的委派管理
- 集中的用户和安全信息
- 策略+审计=策略依从

= 安全策略　= 用户和组的信息　= 审计

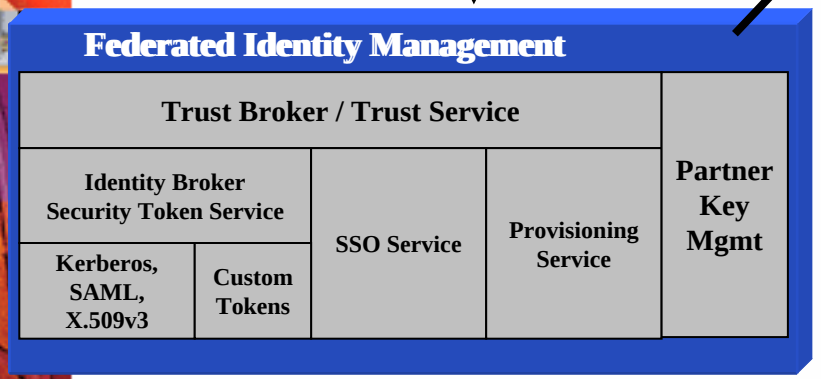
身份管理之五：联盟关系

解决客户问题

- 跨企业的业务开展带来的身份管理问题
- 企业整合中的身份管理问题
- 提高访问效率和管理效率
- 满足审计的要求



基于联邦身份协议的跨企业的身份认证和单点登录.....



1. 用户登录abc.com
   - TAMeb认证用户，创建session
   - TAMeb控制用户访问和进行Session管理.

2. 用户点击连到第三方supply.com的链接
   - 链接为Liberty, WS-Fed, or SAML进行配置

   TAM 调用 FIM

3. FIM 执行到3rd party site的SSO
   - FIM创建SSO Token user session

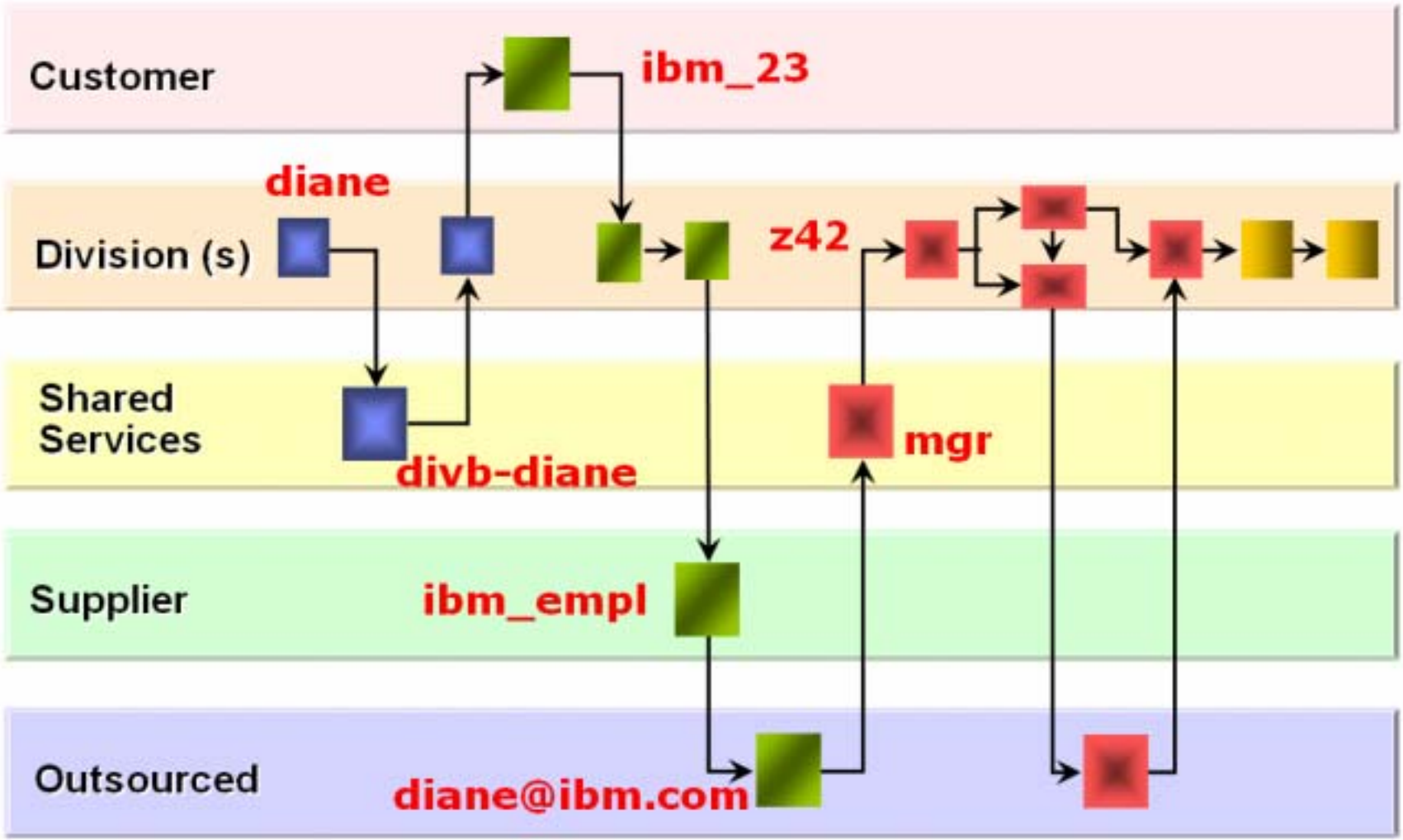
4. supply.com 映射token到本地用户身份库

*** 用户拥有到第三方的透明的SSO ***

SSO
- SAML
- Liberty
- WS-Federation

Service-Oriented Architecture 带来的新的安全问题务

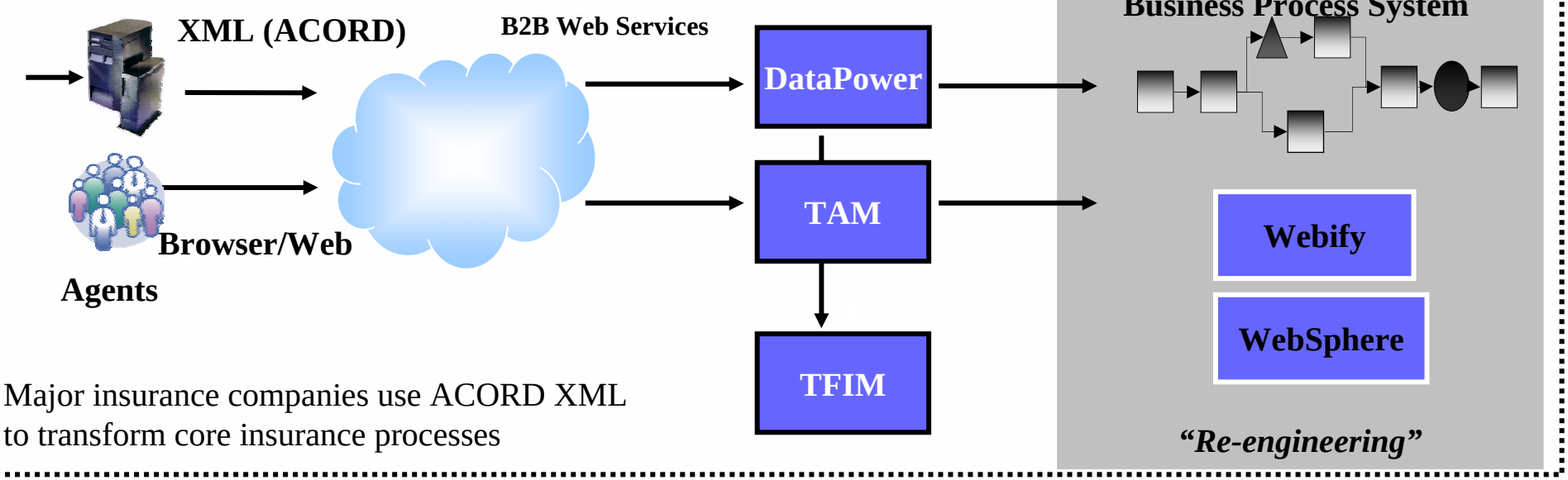
身份数据如何在这些服务之间进行流动和验证?



利用TFIM来实现SOA的安全架构

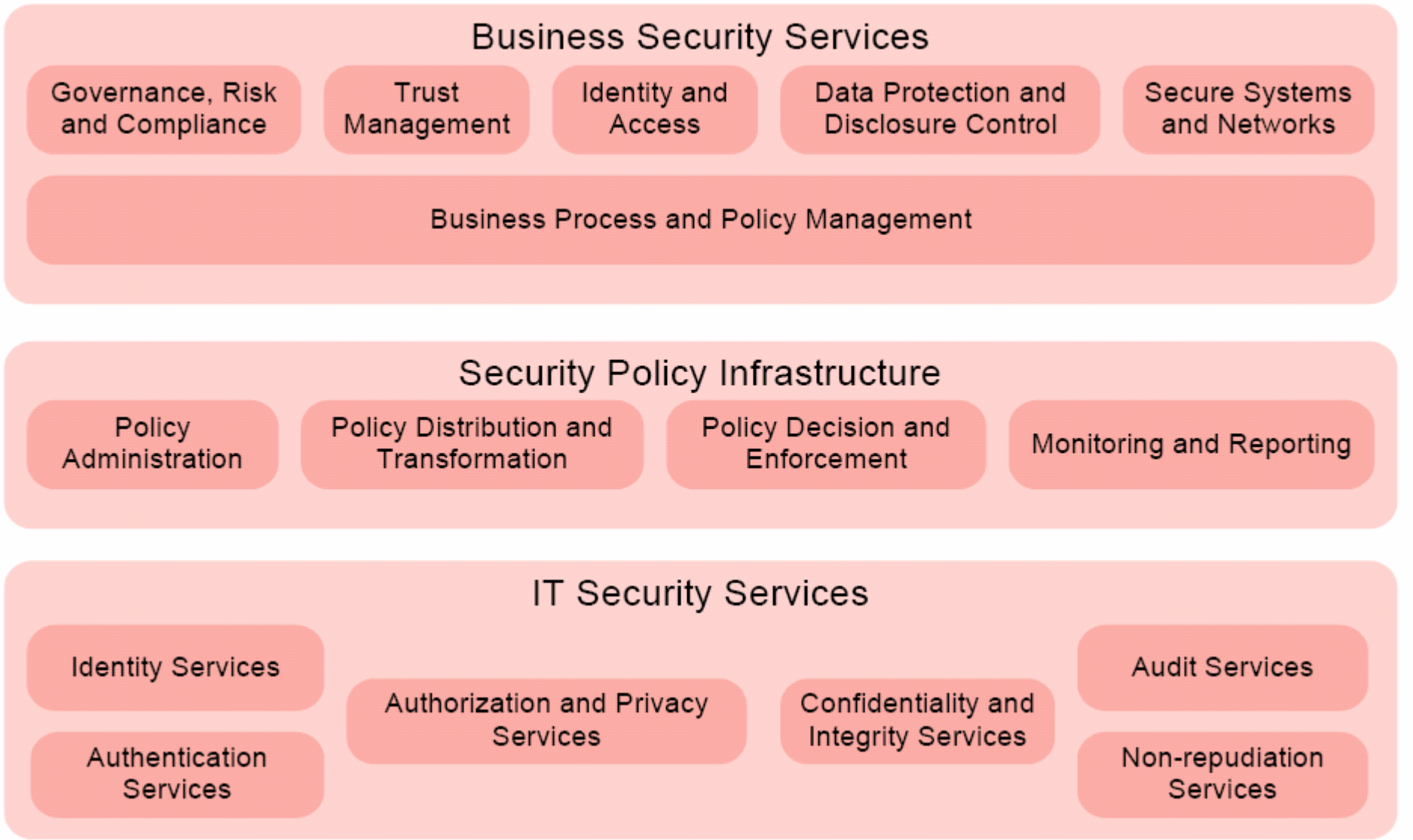
解决方案

- 端到端的SOA安全管理能力，支持service creation、service connectivity和service aggregation等多种模式，从而确保对客户业务流程的提升，并且减少由于SOA架构所代理的可能安全隐患



Major insurance companies use ACORD XML to transform core insurance processes

IBM SOA安全参考模型(v1.0)



Tivoli software

IBM

Tivoli 风险及符合性管理解决方案

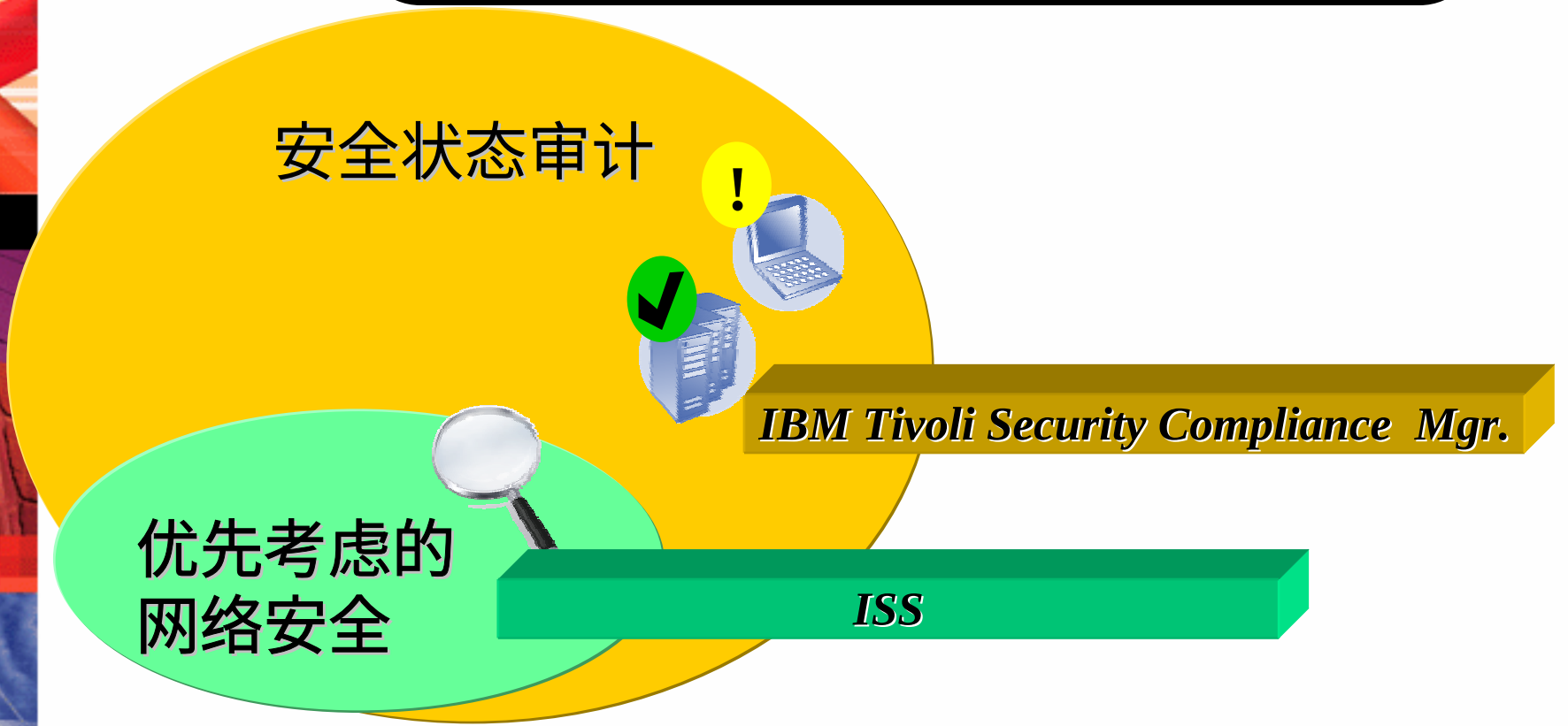
e business software

IBM Software Group

优先考虑的网络安全和符合性管理

解决客户问题

- 服务器、桌面系统是否违反企业安全策略
- 对于新的符合性要求能够提供更为快速的检查
- 满足审计的要求



什么是企业安全策略

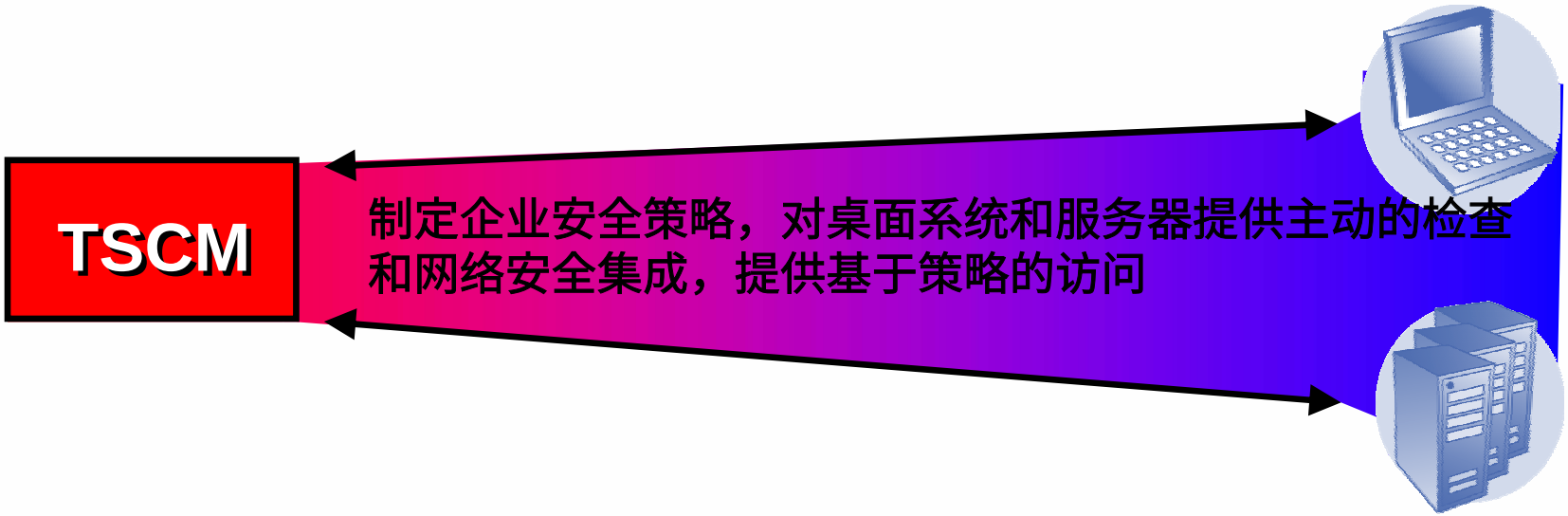
企业安全策略

Click Here to View Detailed Security Report

Performed check	Required result	Your system setting
Power-On Password ✓	Activate a power-on password	Password is set
Hard disk Password (Thinkpads only) ✗	Activate a hard disk password	Password is not set Password is not set
Screen Saver ✓	Set a password protected keyboard/screen lock. Inactivity period should be no more than 30 minutes.	Account: SLX-TPT40-XP\shenou; Screen Saver is active: yes; Screen Saver is password protected: yes; Inactivity period: 5 minutes
Norton AntiVirus ✓	Install and run an IBM-approved AntiVirus program. Run Norton AntiVirus LiveUpdate at least weekly.	Version of installed AntiVirus: 7.61.954; AntiVirus running: yes; LiveUpdate period: daily
Personal Firewall ✓	Install and run an IBM-approved personal firewall program on your workstation if you directly connect the workstation to any customer network, or to the internet via DSL or cable modem, or to any external wireless LAN.	Version of installed Firewall: ZoneLabs Firewall 3.5.175.087; Firewall service running: yes; Firewall active: yes This data is for your information. It is your responsibility to install and run an IBM-approved personal firewall program if your workstation is connected as described in the **Required result** column.
File Sharing ✓	You must not allow any form of unauthenticated access on your network connected workstation.	Sharename / Localpath / Unauthenticated Access: no share published
Lotus Notes Local Database Encryption ✓	Encrypt Lotus Notes databases that contain IBM Confidential information. Local mail files, archives, and "MyAttachment" repositories are mandatory files to be encrypted.	C:\Lotus\Notes\Data\bookmark.nsf: *NOTE* C:\Lotus\Notes\Data\names.nsf: *NOTE* • Local mail files, mail archives, and "MyAttachment" repositories are mandatory files to be encrypted • Databases listed above with a black "no" are not currently encrypted. You must determine if any of these database contain IBM Confidential information. If they do, they must be encrypted • ***NOTE*: DO NOT encrypt these databases, as it will make them unusable.**
Microsoft Windows Accounts ✓	You must not allow Microsoft Windows operating system userids to be created without a password. A	User ID / Fullname / Password Set / Min. password length / Max. password age

Tivoli. SC

Tivoli Security Compliance Manager功能概貌

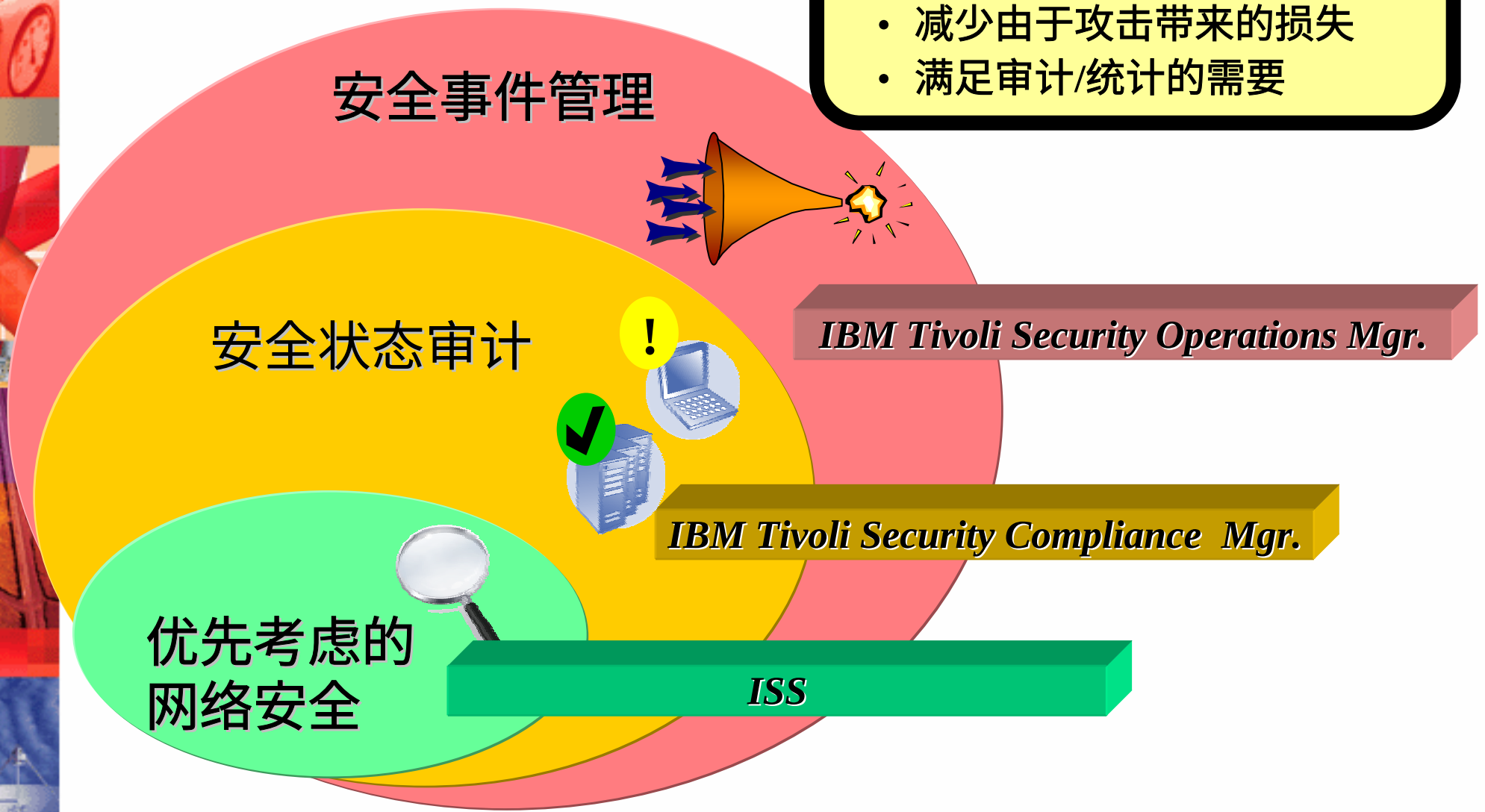


例子: PW strength, PW change frequency, inactive accounts, added or deleted services, mandatory services, forbidden services, forbidden applications, registry settings, application config files, patch levels, hot fix levels, incorrect or weak ACL/permissions, software versions (firewall, AV), . . .

优先考虑的网络安全和符合性管理

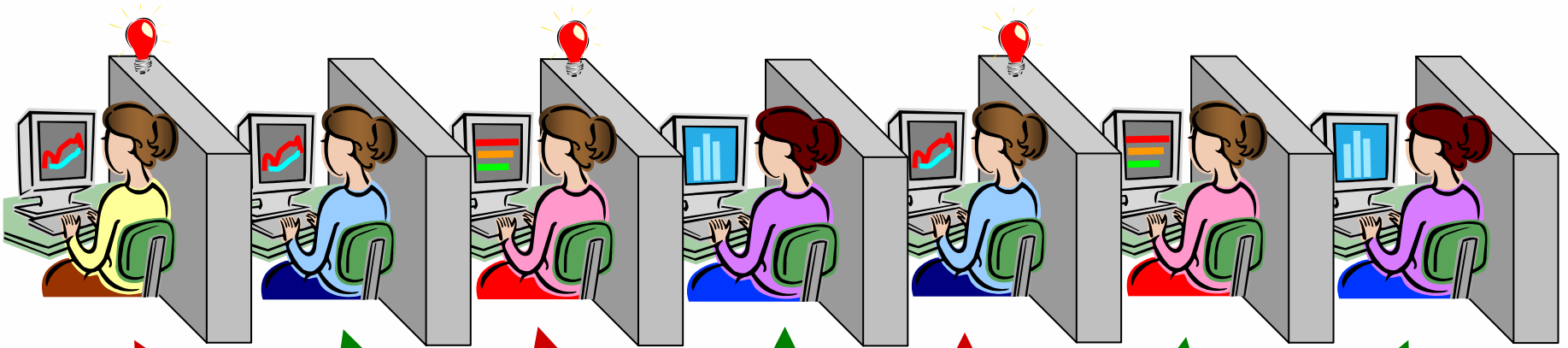
解决客户问题

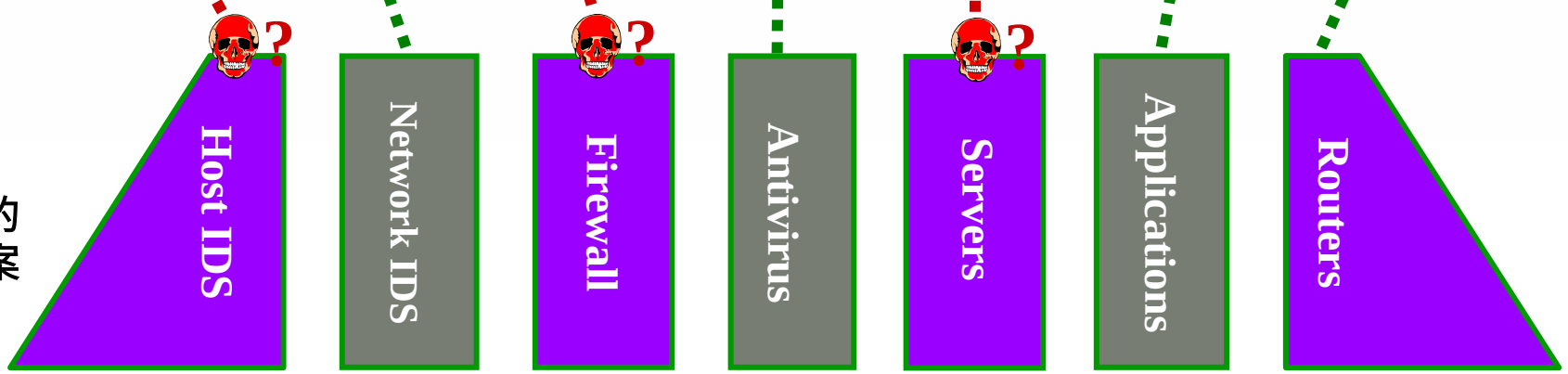
- 对于攻击的快速反应
- 减少由于攻击带来的损失
- 满足审计/统计的需要



典型的安全运维方式

孤立的管理　　众多窗口　　手工关联





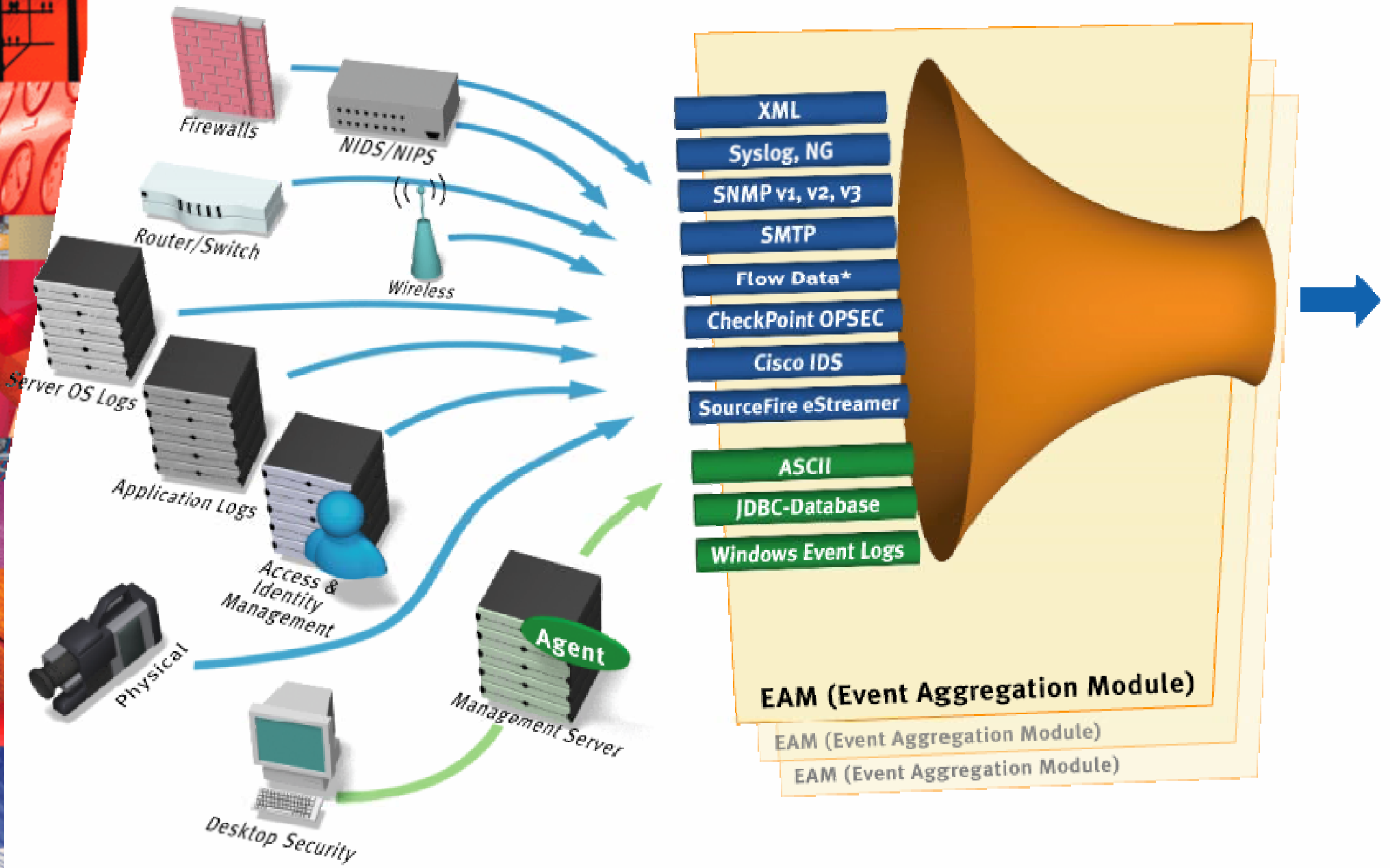
针对不同厂家的
单点解决方案

多厂商，多管理域

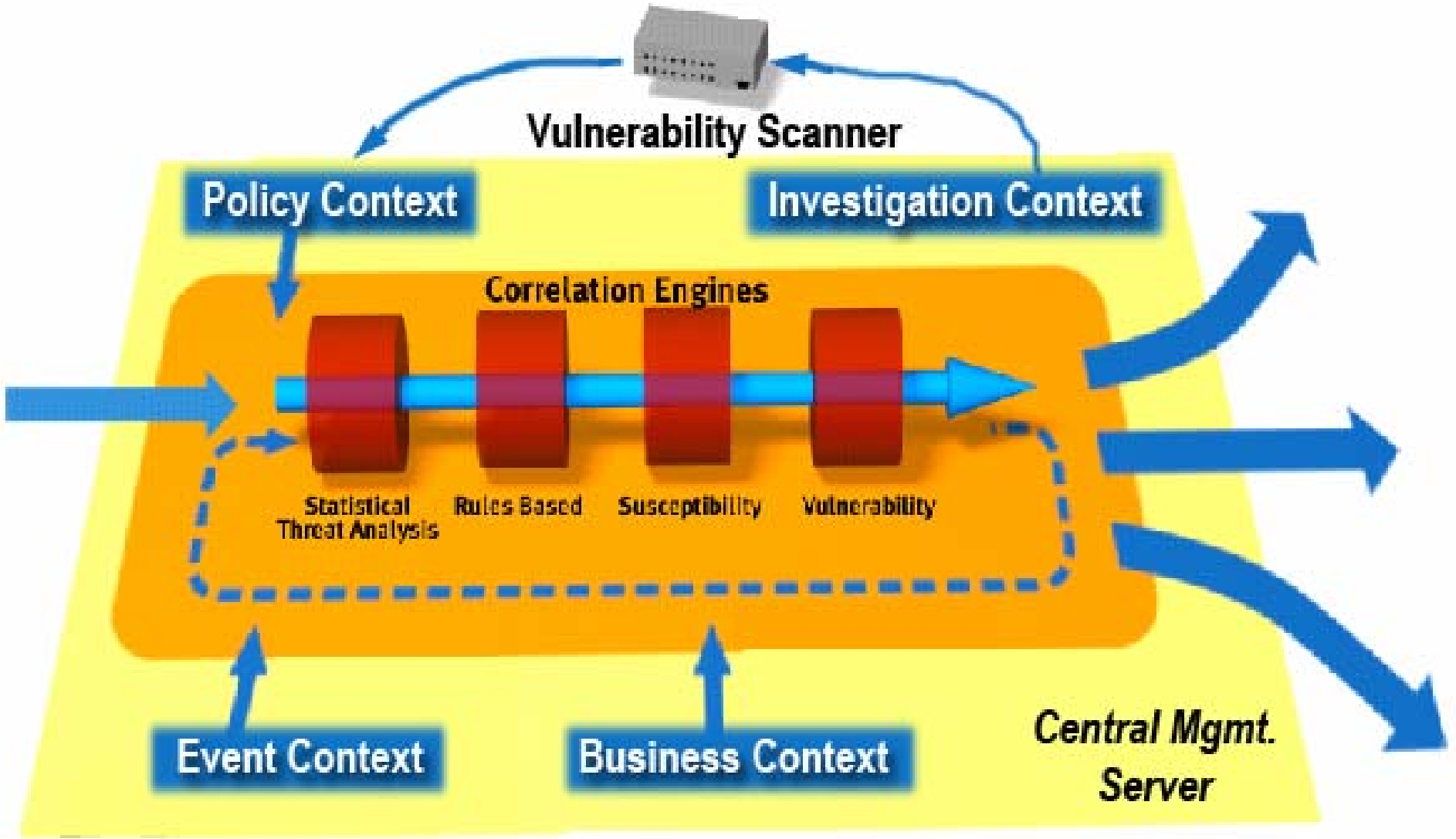
实时的安全事件管理中心

1：安全事件集中收集
2：安全事件的标准化
3：安全事件的关联分析和优先级处理
4：实时安全事件显示
5：自动响应和故障报警处理
6：报表和预测分析

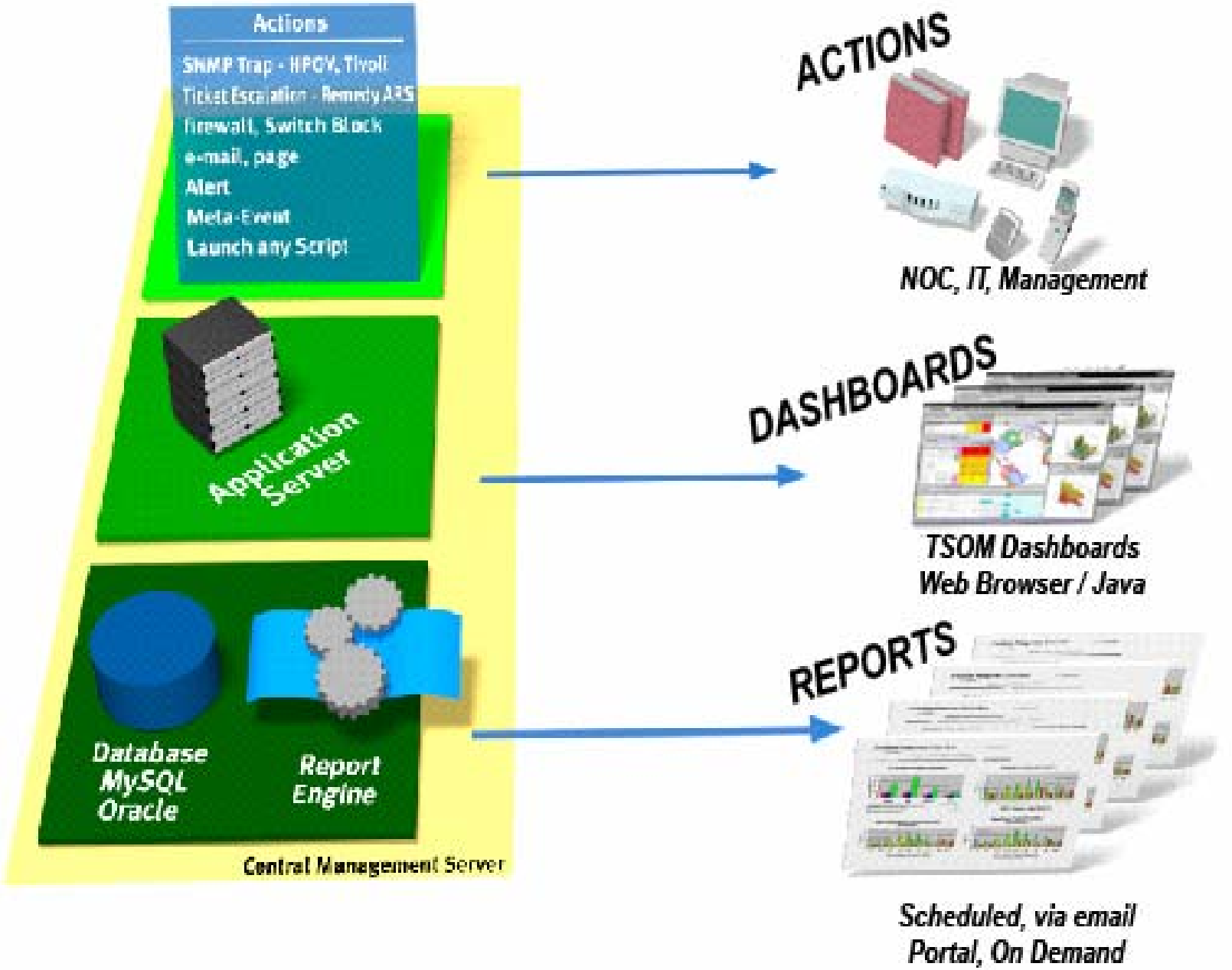
集成大范围的事件


Firewalls
NIDS/NIPS
Router/Switch
Wireless
Server OS Logs
Application Logs
Access & Identity Management
Physical
Agent
Management Server
Desktop Security
XML
Syslog, NG
SNMP V1, V2, V3
SMTP
Flow Data*
CheckPoint OPSEC
Cisco IDS
SourceFire eStreamer
ASCII
JDBC-Database
Windows Event Logs
EAM (Event Aggregation Module)
EAM (Event Aggregation Module)
EAM (Event Aggregation Module)

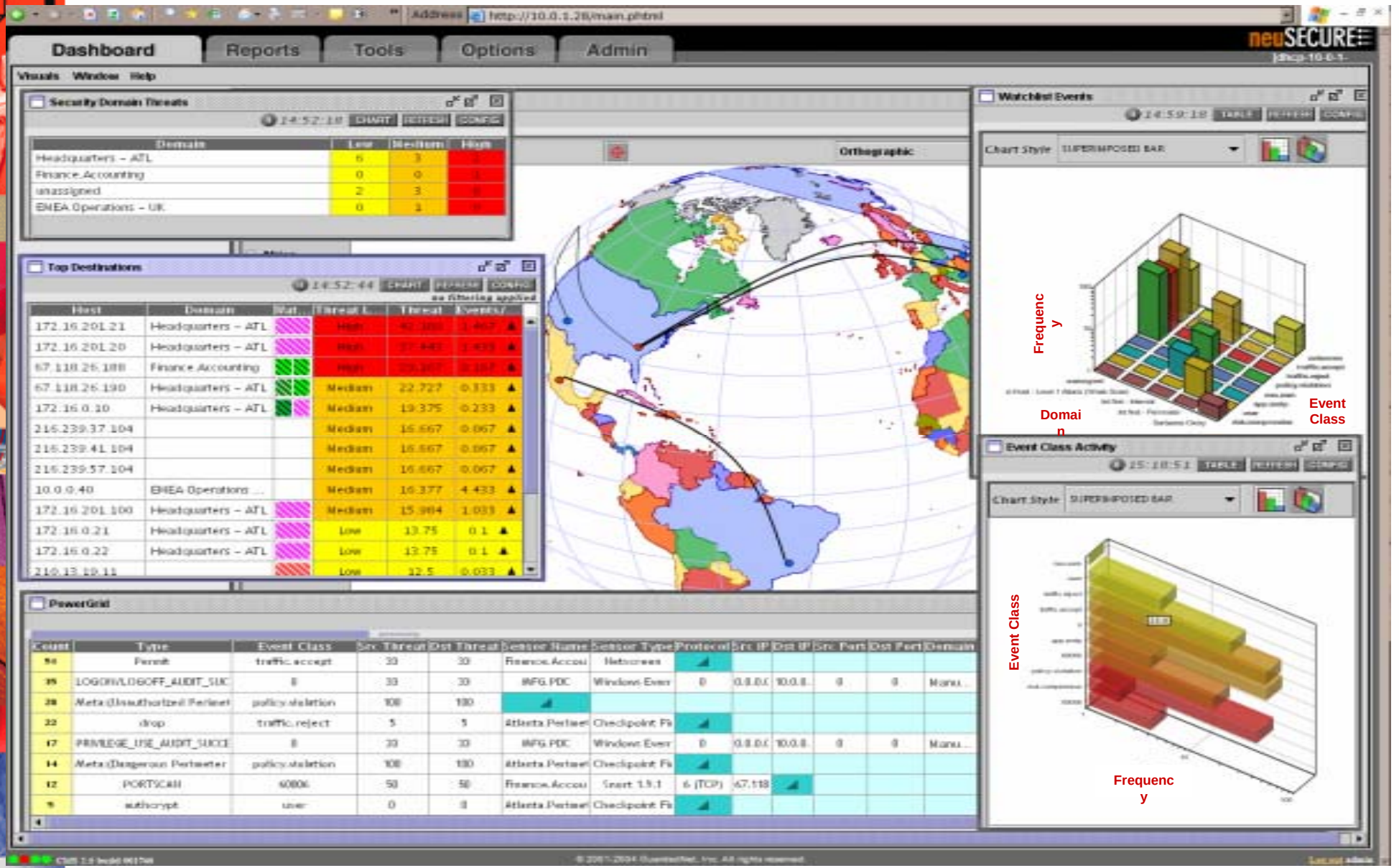
使用多种技术手段来实现事件关联



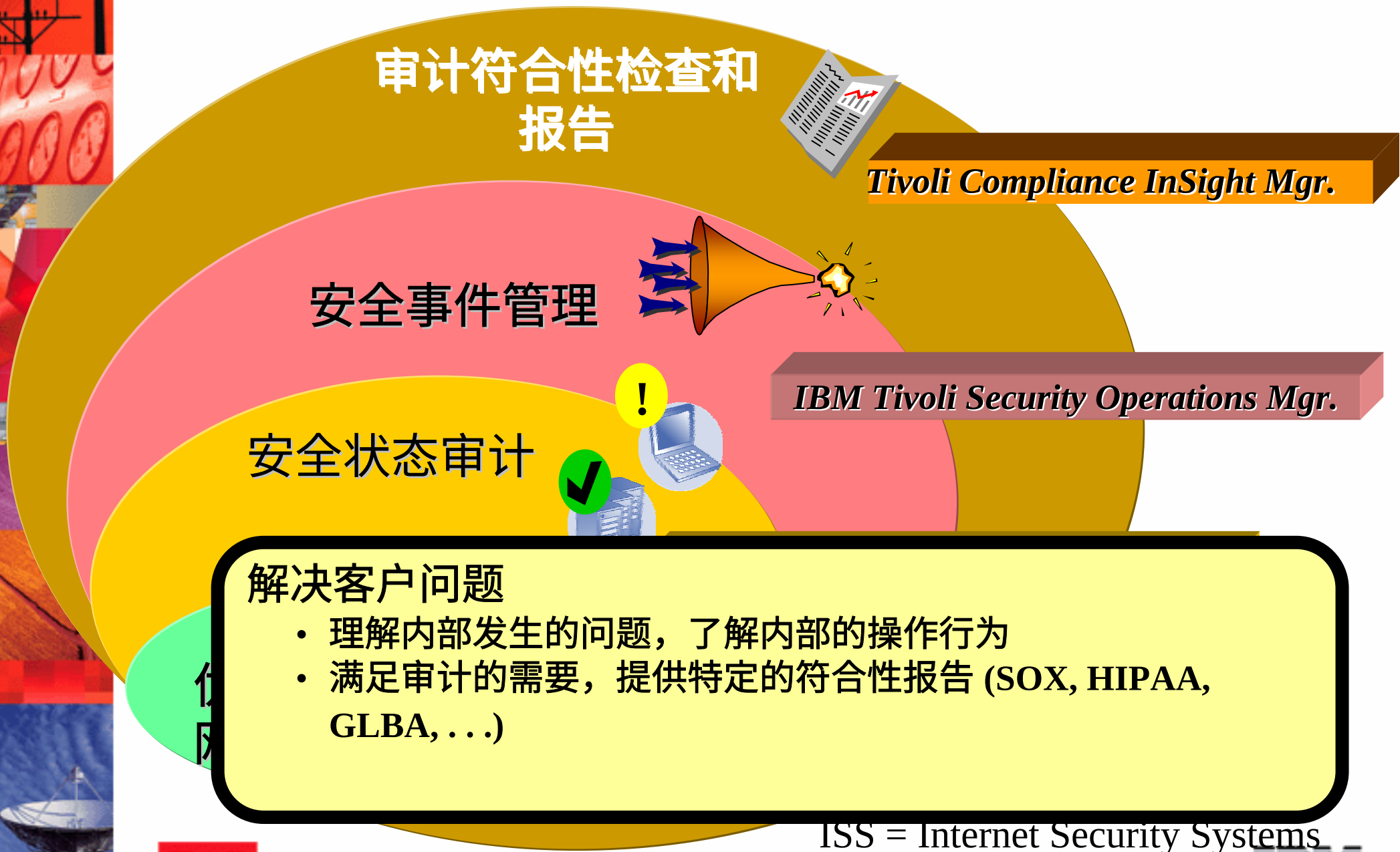
展现、动作和报告


Actions
SNMP Trap - HPOV, Tivoli
Ticket Escalation - Remedy ARS
firewall, Switch Block
e-mail, page
Alert
Meta-Event
Launch any Script
Application Server
Database
MySQL
Oracle
Report
Engine
Central Management Server
ACTIONS
NOC, IT, Management
DASHBOARDS
TSOM Dashboards
Web Browser / Java
REPORTS
Scheduled, via email
Portal, On Demand

IBM提供企业安全系统运行的全视图



优先考虑的网络安全和符合性管理

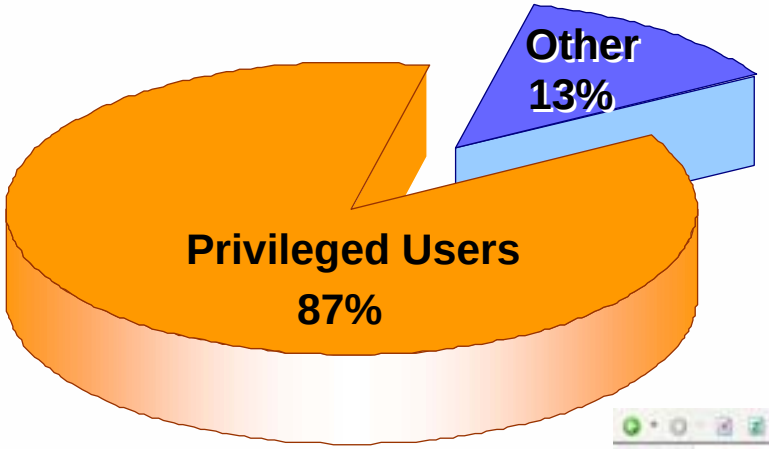


解决客户问题

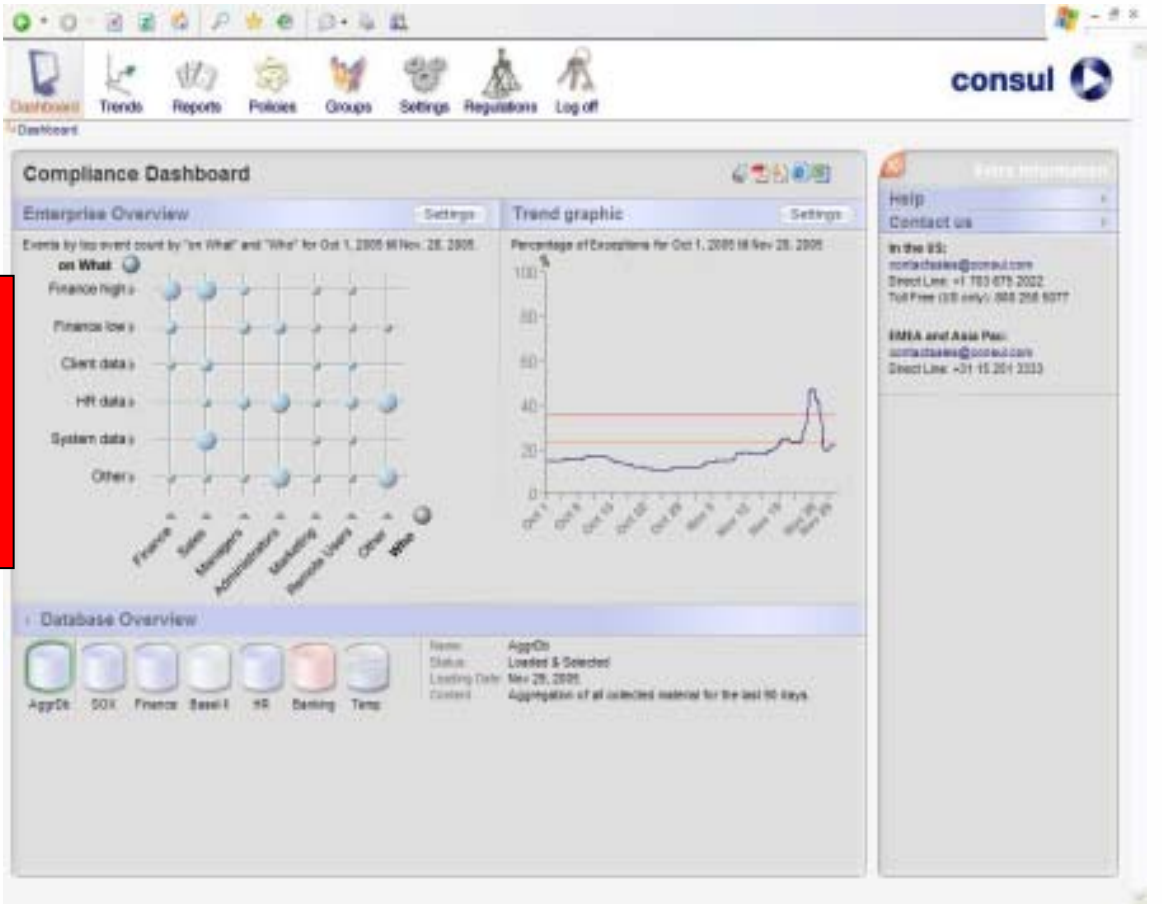
- 理解内部发生的问题，了解内部的操作行为
- 满足审计的需要，提供特定的符合性报告 (SOX, HIPAA, GLBA, . . .)

ISS = Internet Security Systems

加强对内部行为的了解不再是一个可选项了



制度遵从显示板
W7 处理器后的日志– 通过一个简单的图形汇总几十亿个日志文件！



W7 事件列表
注意!: 按照审计需要回放事件

Dashboard | Summary | Reports | Policies | Groups | Settings | Regulations | Log off

Dashboard > Reports > Events by Rule

Events by Rule

W7 Group selection

Who: Administrators | What: _ANY_ | When: _ANY_ | Where: _ANY_ | On What: _ANY_ | Where from: _ANY_ | Where to: _ANY_

Reset

GMT-05:00 New_York, Nipigon, Pangnirtung

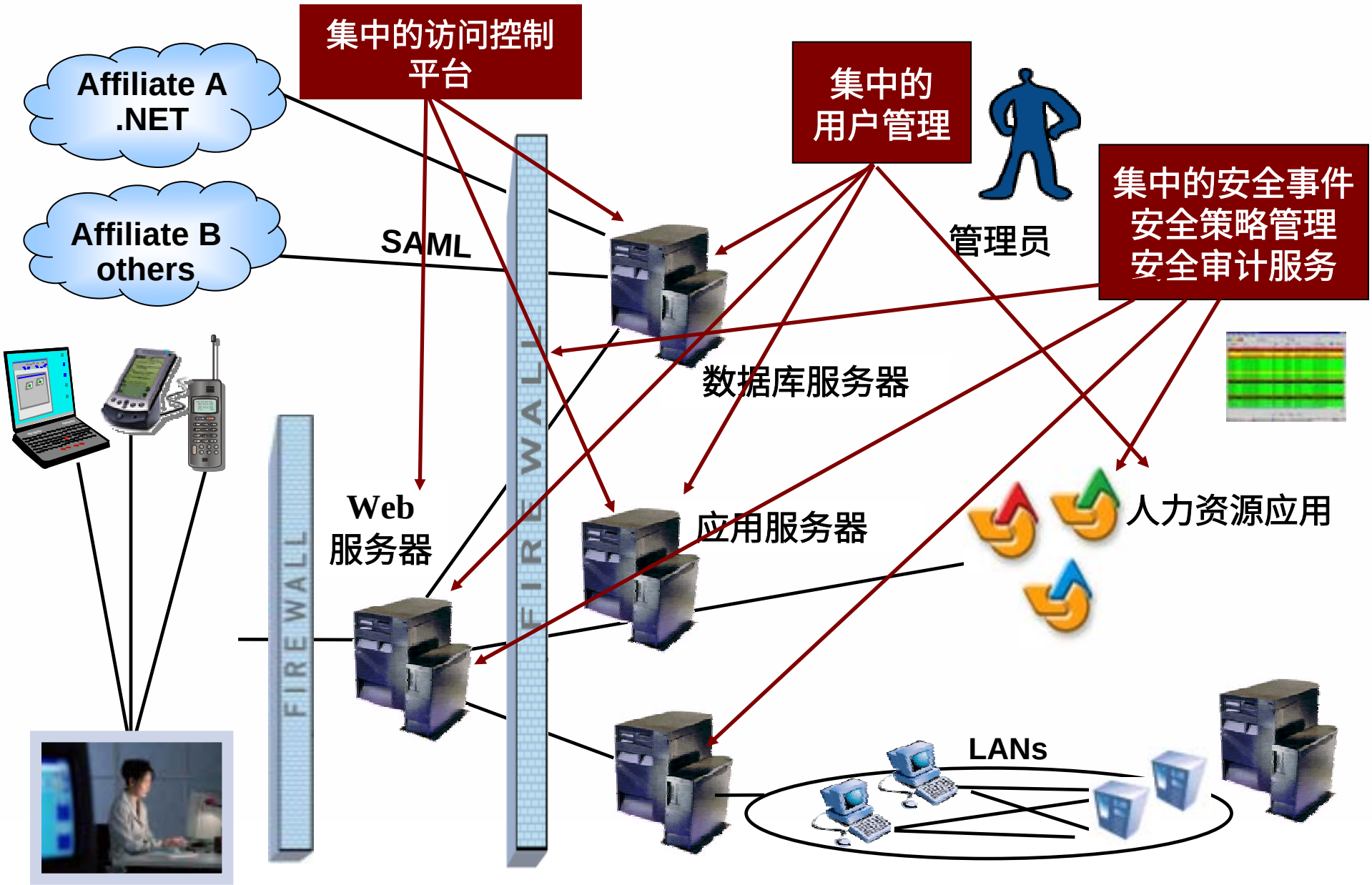
ANY
Users
Administrators
System
Management
Client Maintenance
FinAdmin Manager
FinAdmin Staff
Human Rescources
Salary Administratic
Auditors
IT Admin
Mobile user
IT
Database Admin
End User
Finance
Finance Admin
Finance Manageme
Helpdesk
HR
HR Admin
HR Management
Managers
Marketing
Network Admin
Operations
Operations Manage
Sales
Sales Admin

		#	What	Where	Who	from Where	on What	Where to
5	15:34:18 GMT -5	1	Start : Process / Success	Finance Server	Administrator	Finance Server	PROCESS : . / Notepad.exe	Finance Server
5	15:34:18 GMT -5	1	Clear : Auditlog / Success	Finance Server	ROOT	Finance Server	AUDITLOG : . / -	Finance Server
5	15:34:21 GMT -5	1	Complete : Process / Success	Finance Server	ROOT	Finance Server	PROCESS : . / Notepad.exe	Finance Server
5	15:34:28 GMT -5	1	Start : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Notepad.exe	Mainframe FIN
5	15:35:02 GMT -5	1	Complete : Process / Success	HR Server	ROOT	HR Server	PROCESS : . / Process2212024768	HR Server
5	15:35:02 GMT -5	2	Read : File / Success	Finance Server	Administrator	Finance Server	FILE : DataSmartinvest / *	Finance Server
5	15:35:24 GMT -5	1	Start : Process / Success	Mainframe FIN	James Patterson	Mainframe FIN	PROCESS : . / Runemacs.exe	Mainframe FIN
5	15:35:24 GMT -5	1	Start : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Emacs.exe	Mainframe FIN
5	15:35:24 GMT -5	1	Complete : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Runemacs.exe	Mainframe FIN
5	15:37:34 GMT -5	1	Start : Process / Success	Web Server	ROOT	Web Server	PROCESS : . / Eventvwr.exe	Web Server
5	15:37:35 GMT -5	1	Grant : Privilege / Success	Web Server	Tim Doberty	Web Server	OBJECT : . / Handle0	Web Server
5	15:37:41 GMT -5	1	Grant : Privilege / Success	Web Server	Administrator	Web Server	OBJECT : . / Handle0	Web Server
5	15:37:48 GMT -5	1	Grant : Privilege / Success	Web Server	Marcus Jacobs	Web Server	OBJECT : . / Handle0	Web Server
5	15:38:21 GMT -5	1	Grant : Privilege / Success	Web Server	Ross Hikkings	Web Server	OBJECT : . / Handle0	Web Server
5	15:38:28 GMT -5	1	Grant : Privilege / Success	Finance Server	Marcy Hoover	Finance Server	OBJECT : . / Handle0	Finance Server
5	15:38:28 GMT -5	1	Read : Access / Success	Finance Server	ROOT	Finance Server	FILE : DataSmartinvest / Default.cfg	Finance Server
5	15:38:28 GMT -5	2	Read : File / Success	Finance Server	Administrator	Finance Server	FILE : DataSmartinvest / *	Finance Server
70	Fri Nov 25, 2005 15:38:28 GMT -5	7	Read : Access / Success	Finance Server	ROOT	Finance Server	FILE : DataSmartinvest inadmin / *	Finance Server

1 2 3 4 5 6 7 8 9 10 11 12

Done | My Computer

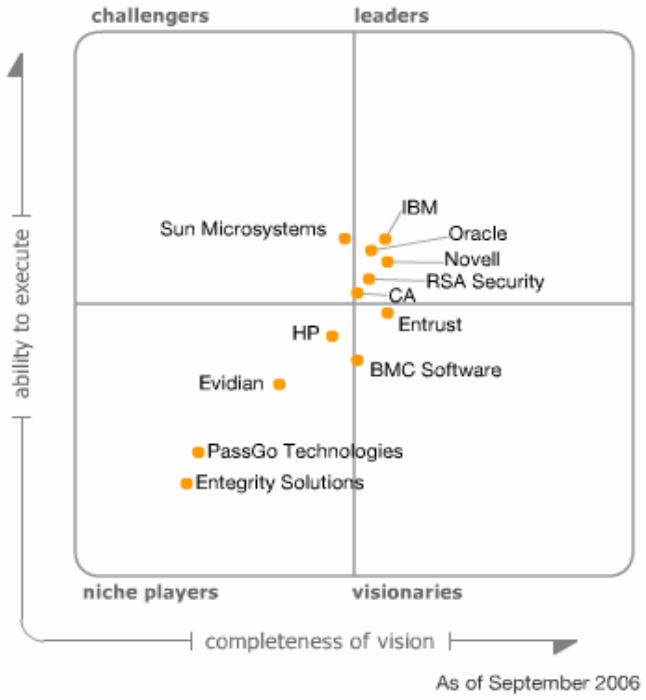
IBM Tivoli提供全面的安全管理



IBM业界领先厂商

- 全球身份管理市场
- 全球认证授权管理市场
- 全球日志管理市场

Figure 1. Magic Quadrant for Web Access Management, 2H06



Note: Formerly called the Magic Quadrant for Extranet Access Management
Source: Gartner (September 2006)

Tivoli software


Thank
You