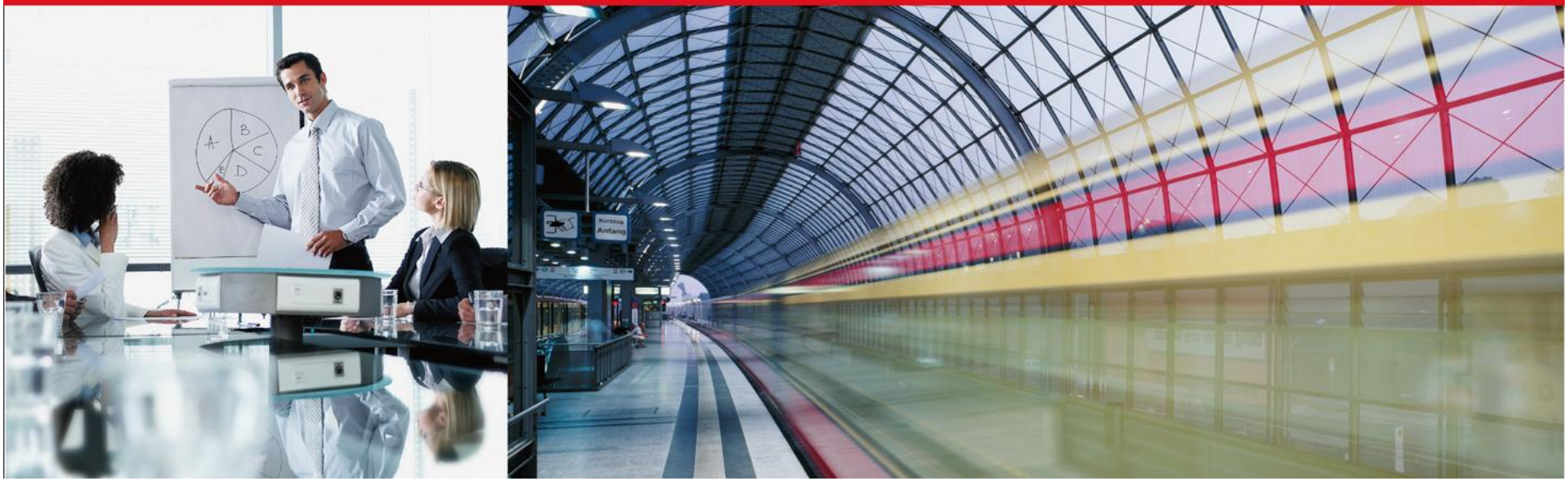
EXPO 2010 SHANGHAI CHINA

IBM

中国2010年上海世博会高级赞助商

IBM服务管理体验之旅

高效管理随需而变 优化服务实践共赢



构建统一的身份安全架构，保障企业信息安全

杨振宇

IBM 资深技术顾问

yangzy@cn.ibm.com

演讲主题： 构建统一的身份安全架构，保障企业信息安全

议程：

- 身份管理和访问控制 - 概述
- IBM Tivoli身份管理解决方案
  - 集中身份管理
  - 集中访问授权
  - 特权用户行为审计

信息安全成为企业CTO/CEO最为头疼的问题

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Massive Insider Breach at DuPont

February 15, 2007 – A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706 more …

"The best way to guard against insider breaches is for companies to ***monitor database and network access for unusual activity*** and set thresholds that represent acceptable use for different users."

发生的安全问题:

- 数据被窃取
- 访问关键数据库
- 账号多人共用

Carnegie Mellon CERT Comments:

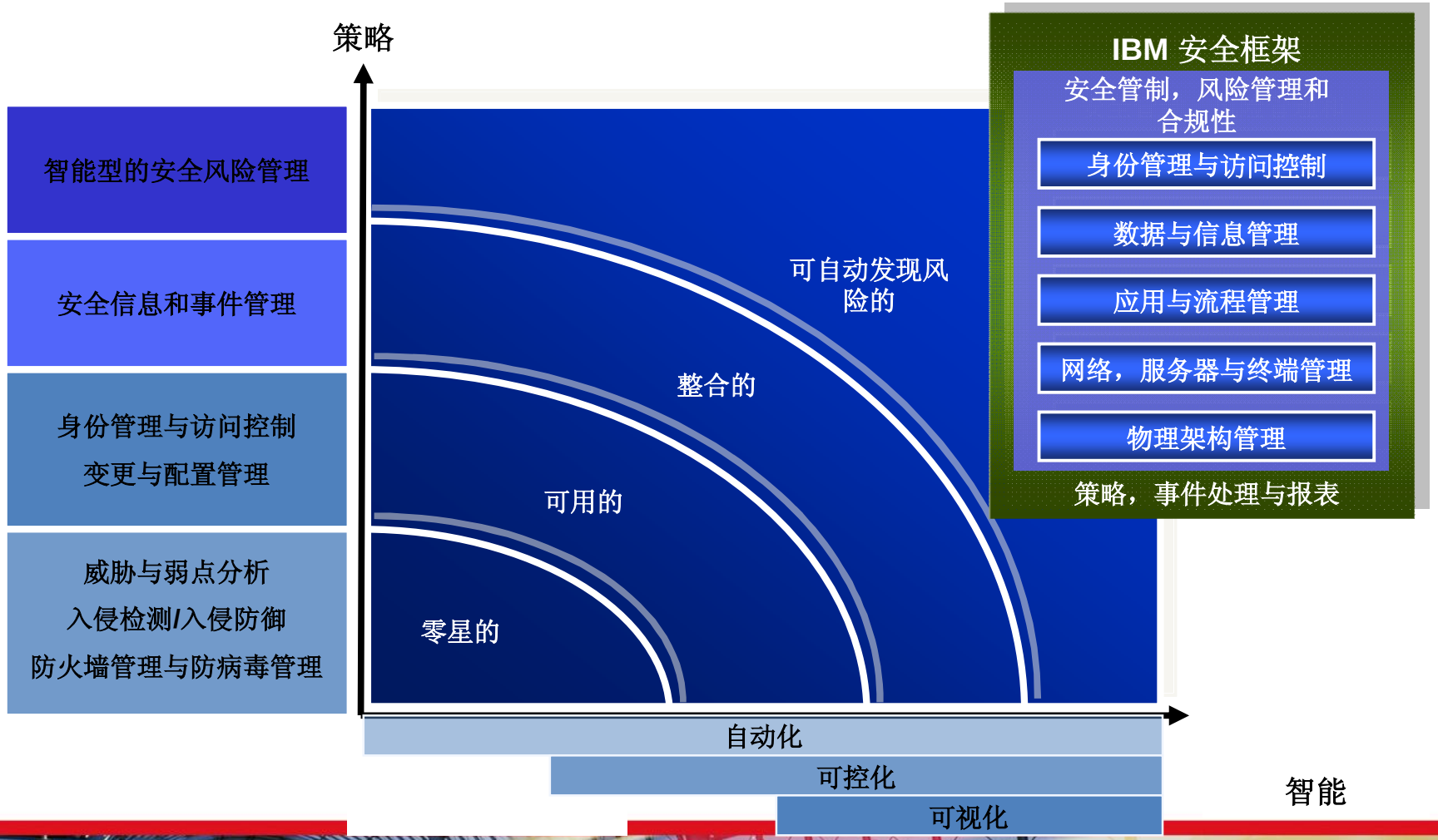
- "75% of … confidential information thefts studied … were committed by current employees"
- "45% had already accepted a job offer with another company"

如何处理：

- 对于内部访问有更为清晰的了解
- 增加身份控制
- 集中化的监控和审计

Source: InformationWeek, Feb. 15, 2007

IBM安全管理战略 -
从及时响应的安全管理到企业风险意识和控制



身份安全在企业的需求 ....

- 企业往往有大量的内部应用和对外应用
- 企业应用系统有各种类型访问用户
- 企业需要管理流程来保障身份管理
- 企业需要满足各种安全策略、标准

身份管理与访问控制 (Identity & Access Management)

- **身份管理 (Identity Management)** - 建立身份和帐号的关联关系；管理每个用户的整个生命周期以及围绕用户管理的各种自动化的业务流程。它包括了：
  - 用户帐号的供应与管理，包括创建、修改、检查、删除等
  - 用户自我服务 (如更改用户个人信息或密码)
  - 工作流(Workflow)支持不同的用户管理及审批条件
  - 删除用户帐号，当该用户不再需要访问系统时

- **访问管理 (Access Management)** - 实现用户对应用资源和系统资源的访问与授权。
  - 什么人(by role)可以用什么资源 ？
  - 该角色被授权执行何种作业 ？
  - 该角色有什么样的授权和限制 ？

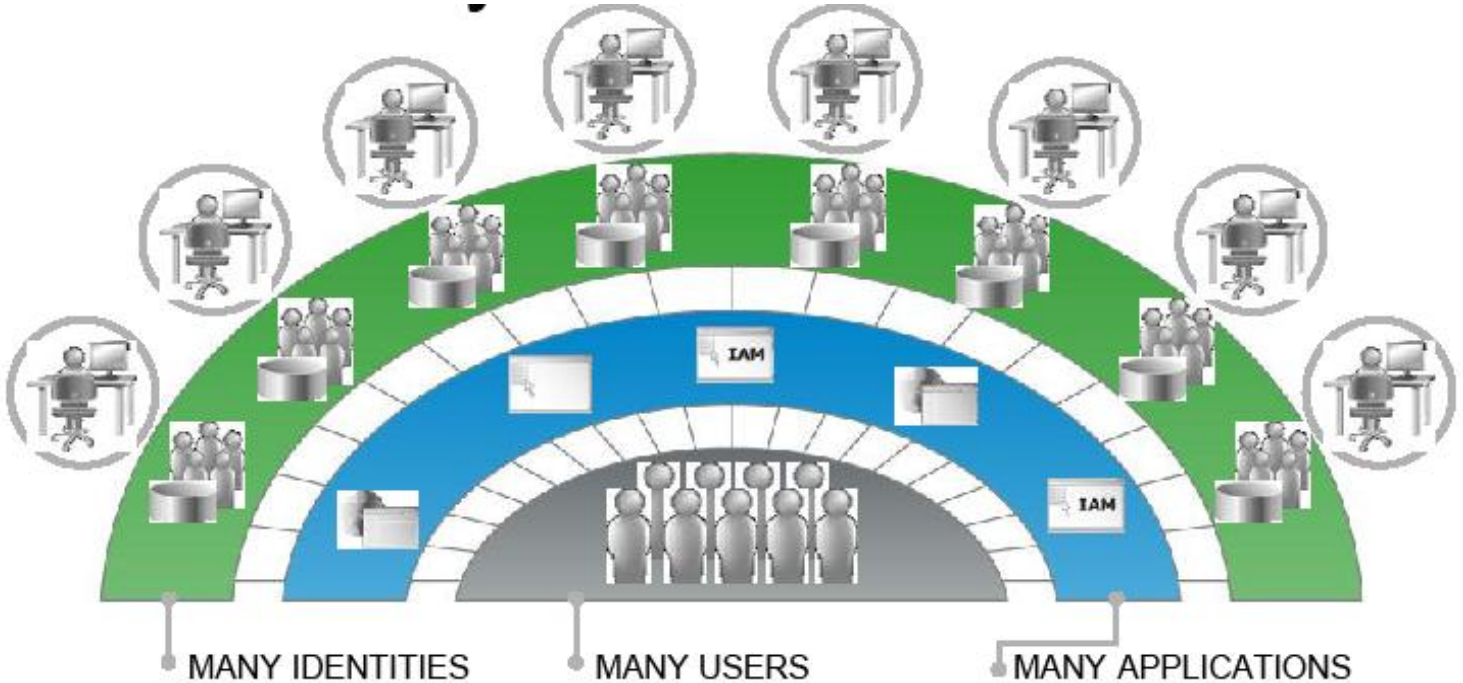
身份管理与访问控制 – 目的与价值

- 账号、授权管理将纳入统一。实现对各业务支撑系统的帐号、认证、授权和审计的集中控制和管理。
- 实现集中化、基于角色的的主从帐号管理。用户权限的分配符合安全策略要求，拥有完成任务所需要的最小权限。
- 用户生命周期的管理，均可在一个平台上进行管理。用户的工作变动情况及时在支撑系统中得到体现。
- 用户一次登录即可方便地访问被授权的系统，提高工作效率。
- 实现安全审计管理，收集、记录、管理用户对业务支撑系统的高敏感度的数据访问和关键操作行为记录。

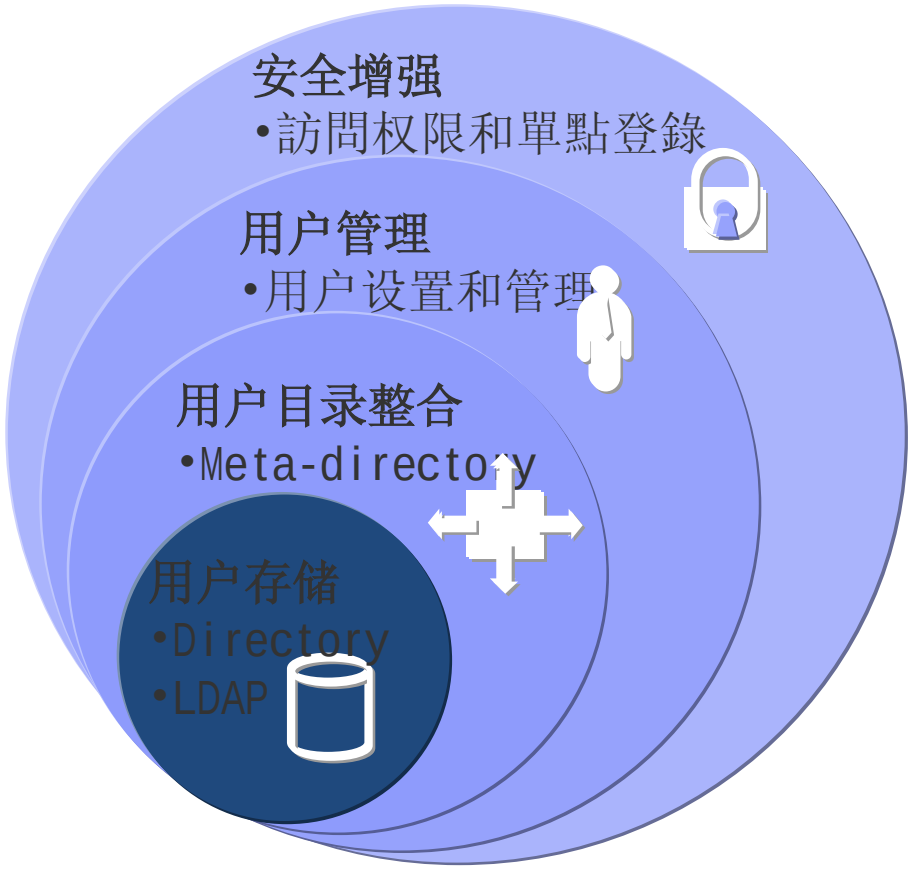
身份管理和访问控制（IAM） - 企业面临的困难与需求

- 大量的操作系统、应用系统和网络设备，分别属于不同的部门和不同的业务系统。缺乏一集中的资源授权管理平台。
- 现有系统帐号共用、授权过大等情况严重，安全风险超出可控范围。
- 人员入职、变更和离职时，不能及时对帐号和授权进行更新。原本应删除的无效用户帐号依旧存在。
- 支撑系统多，帐号口令多，用户需要在各个系统之间多次登录，用户体验差，安全性差。
- 各系统独立运行、维护，缺乏集中统一的访问审计系统。

企业在身份管理的困难：系统多，用户类型多，管理问题突出，运维成本高，…



身份和访问管理（IAM）解决方案的组件有哪些 ？



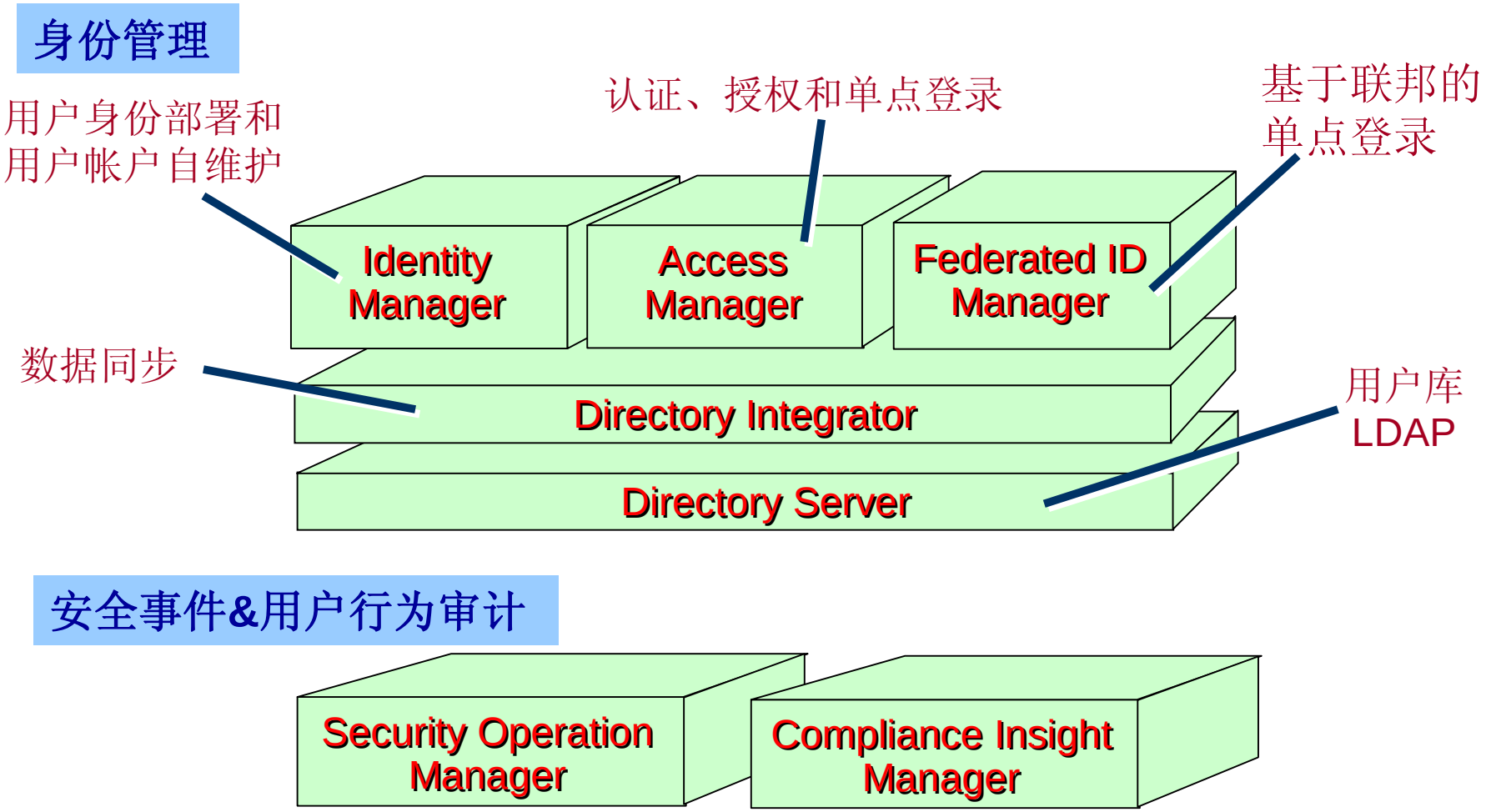
IAM方案的组成部分必须具备高度稳定性和灵活性

- 目录
  - 必须扩展至几百万个用户
  - 需要复制和分发目录数据，以提高可用性
- 身份管理
  - 标准 IT系统（操作系统、目录、数据库）的界面应该可以测试并支持各种选项和场景
  - 必须能以灵活的方式处理复杂供应场景
- 访问管理
  - 必须能支持高身份验证率
  - 单点登录和访问控制对于应用程序非常关键，必须具有高度可用性

议程：

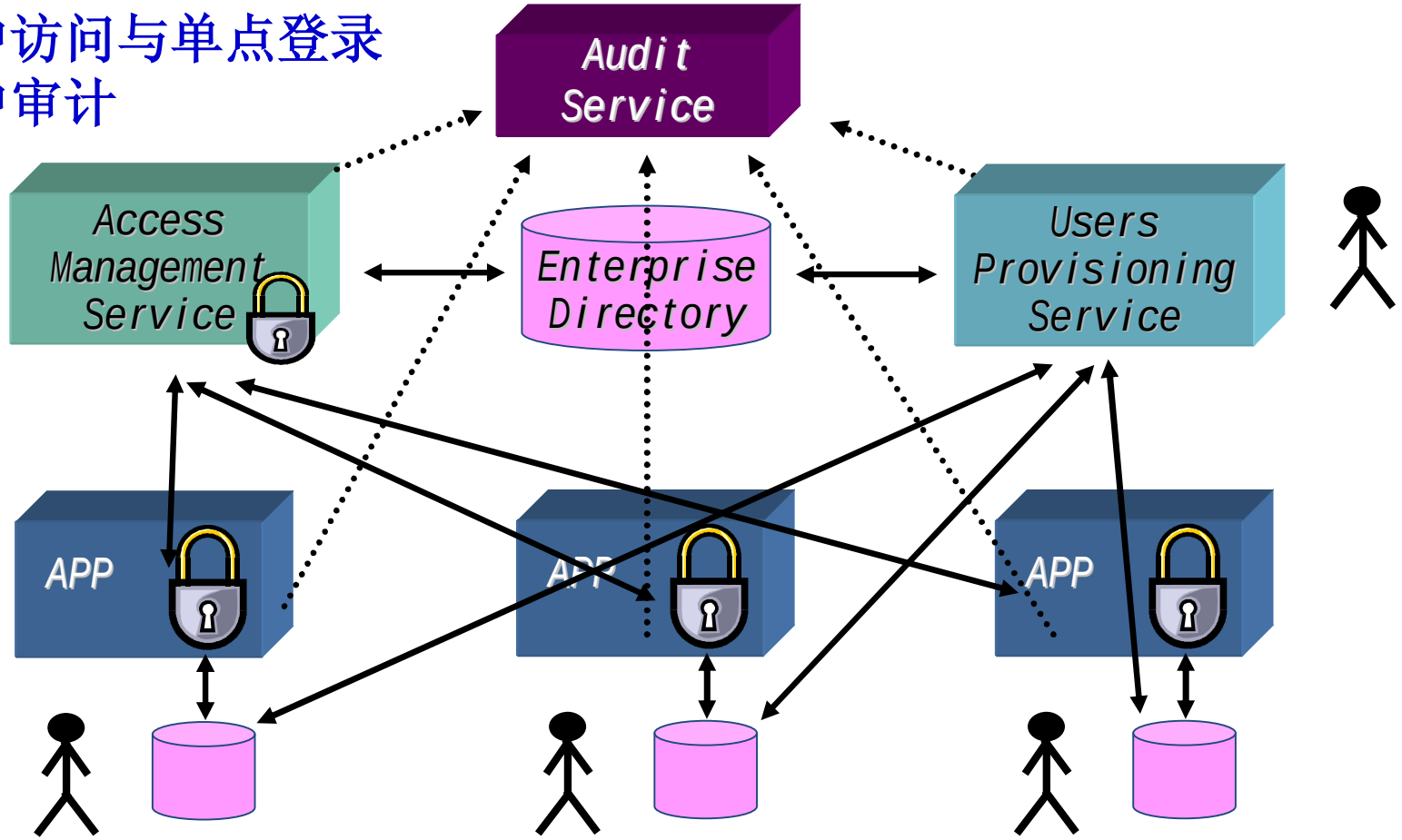
- 身份管理和访问控制 - 概述
- IBM Tivoli身份管理解决方案
  - 集中身份管理
  - 集中访问授权
  - 特权用户行为审计

Tivoli安全解决方案、产品和功能

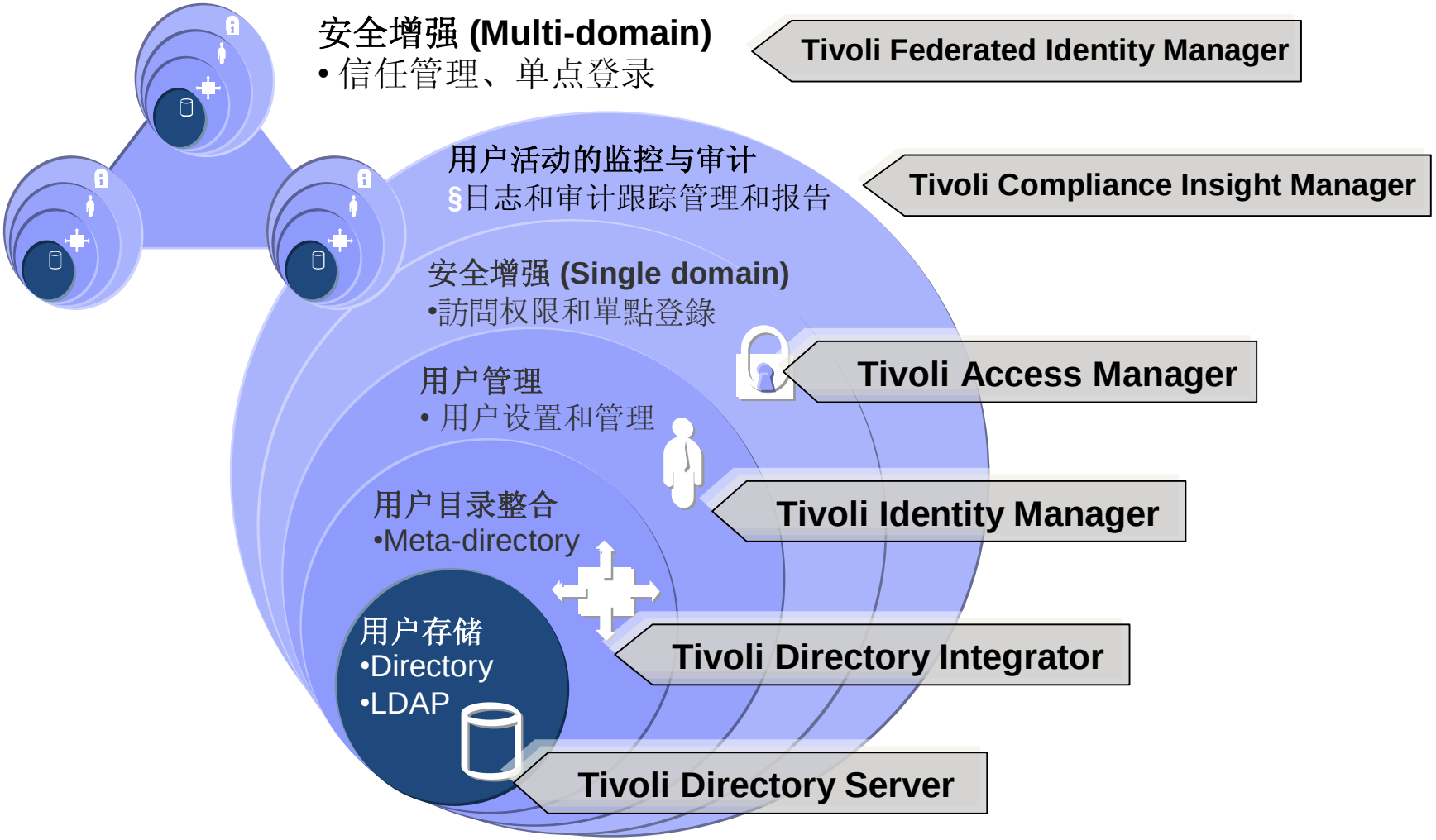


集中的安全管理框架：满足当前和未来身份管理发展的需要

- 集中用户管理
- 集中访问与单点登录
- 集中审计

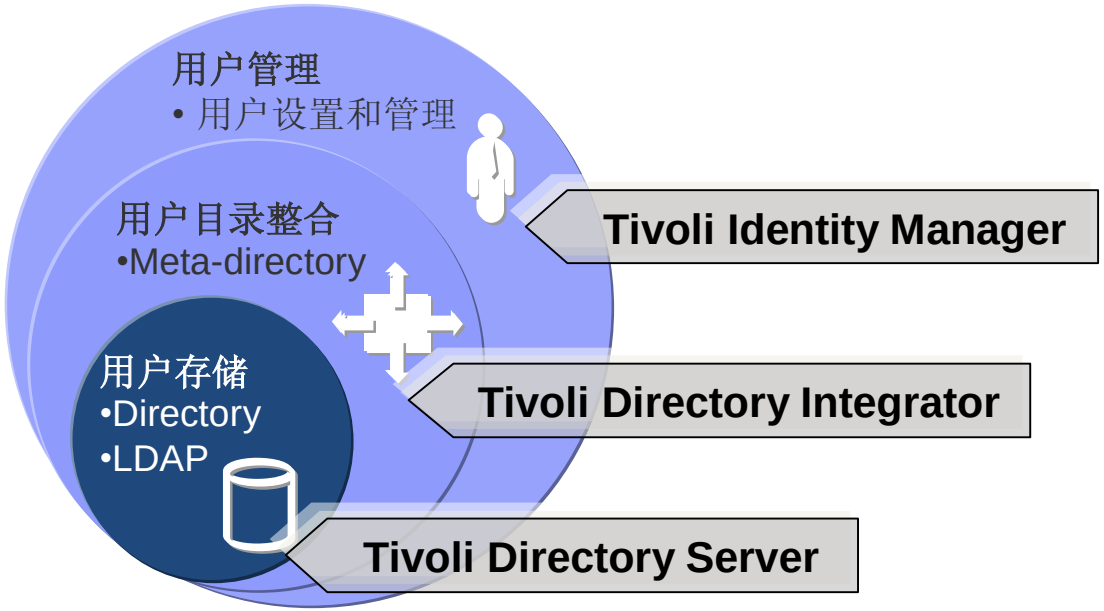


Tivoli 身份管理和访问授权解决方案构建模块

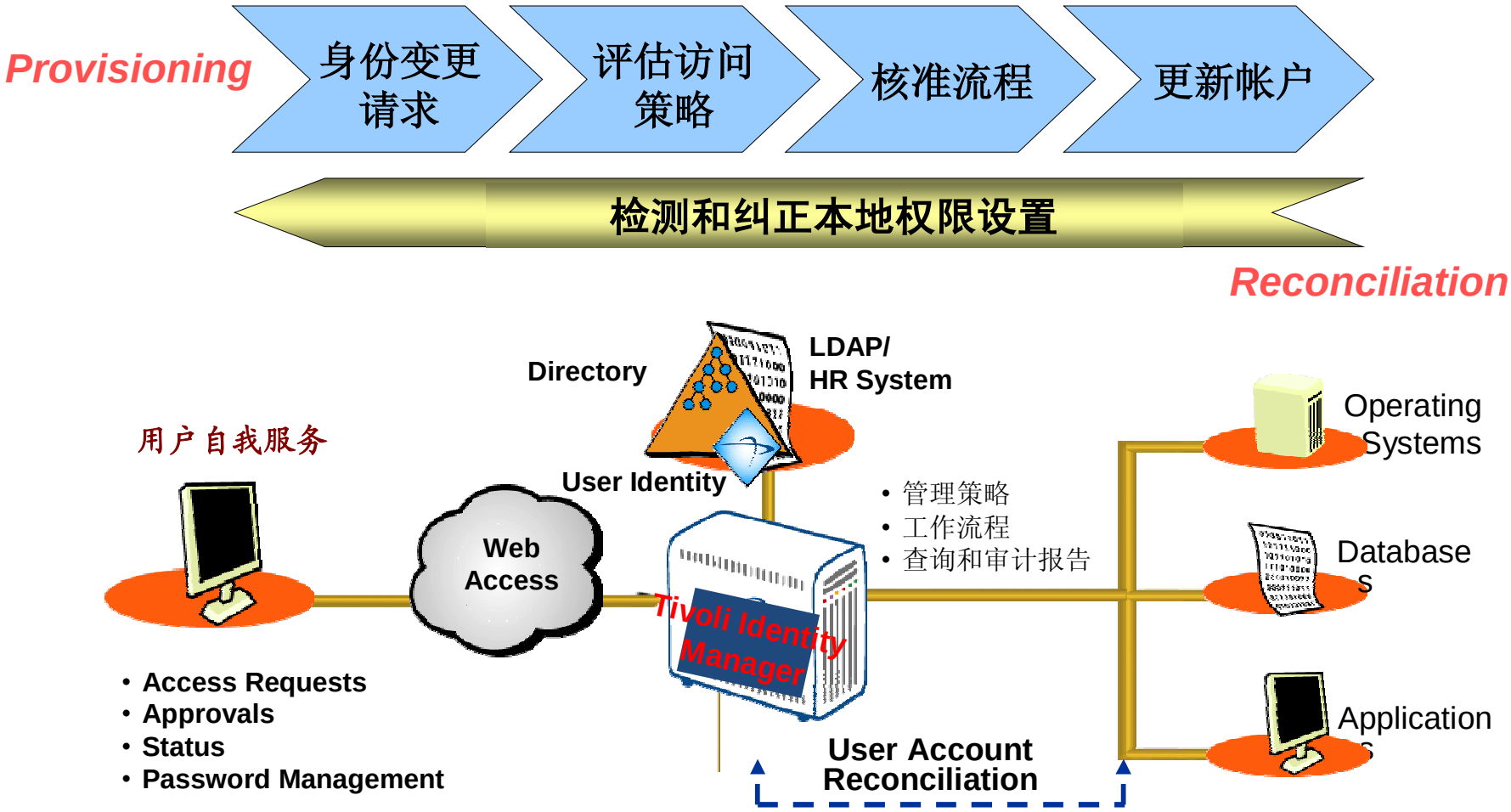


身份管理应用模式：统一用户身份管理

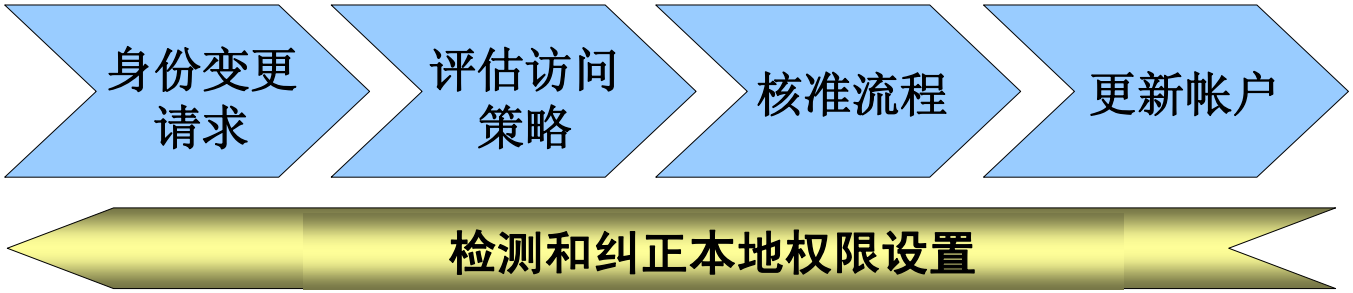
解决客户问题
- 太多的ID管理点，高昂的身份管理费用
- 薄弱的/不一致的管理，存在安全和符合性问题
- 满足审计的要求



Tivoli Identity Manager - 自動化身份生命周期管理



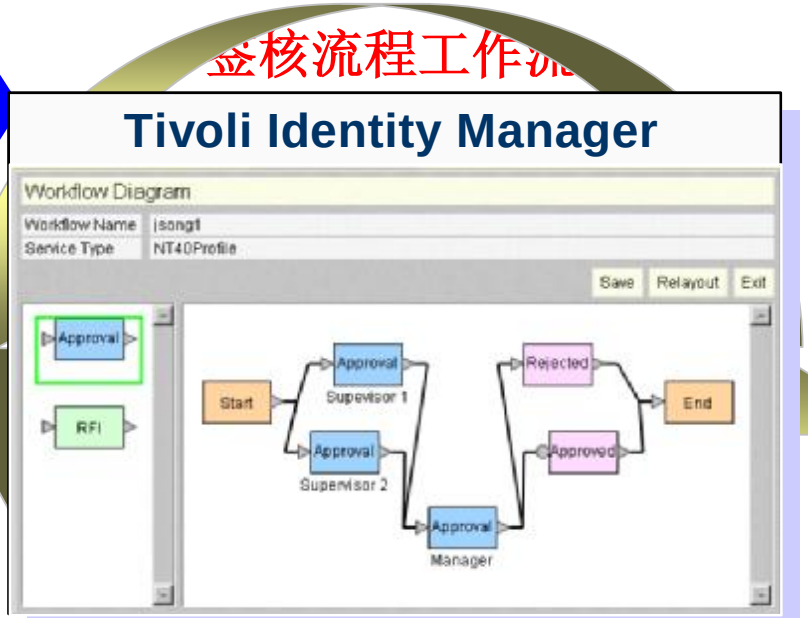
Tivoli Identity Manager - 工作流



新进员工/新使用者
自我注册、登记

使者用部门
或任务更动

重新认证使用者



新增

删除

异动

Account
Notif.
Policy
Role
User
Ext Sys

Tivoli Identity Manager - 用户密码管理

降低帮助台成本

所有系统的用户密码自助服务

密码规则检查

- 根据目标要求检验制度遵从情况
- 跨越所有资源添加规则

提问-回答机制，用于恢复被忘记的密码

*重新设置密码的帮助台成本为 **$20/呼叫***

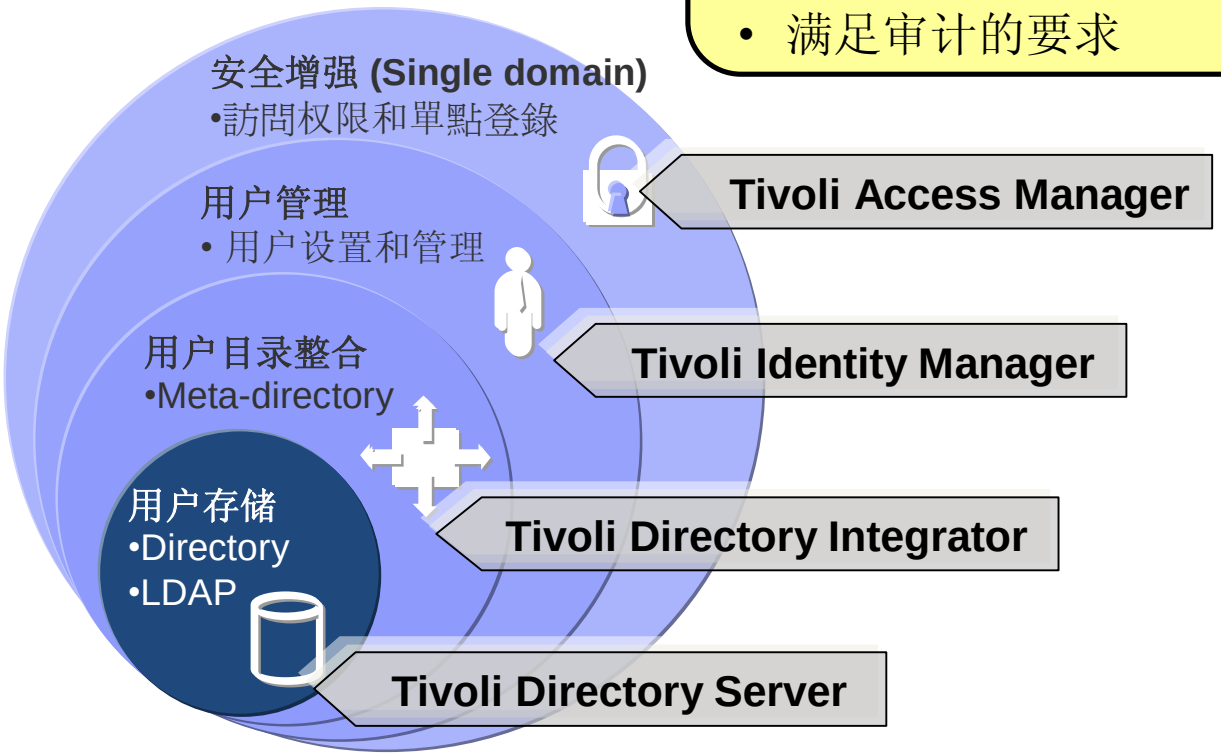
*员工每年的重新设置请求平均为 **3-4次***

Meta Group

身份管理应用模式：安全访问和认证授权

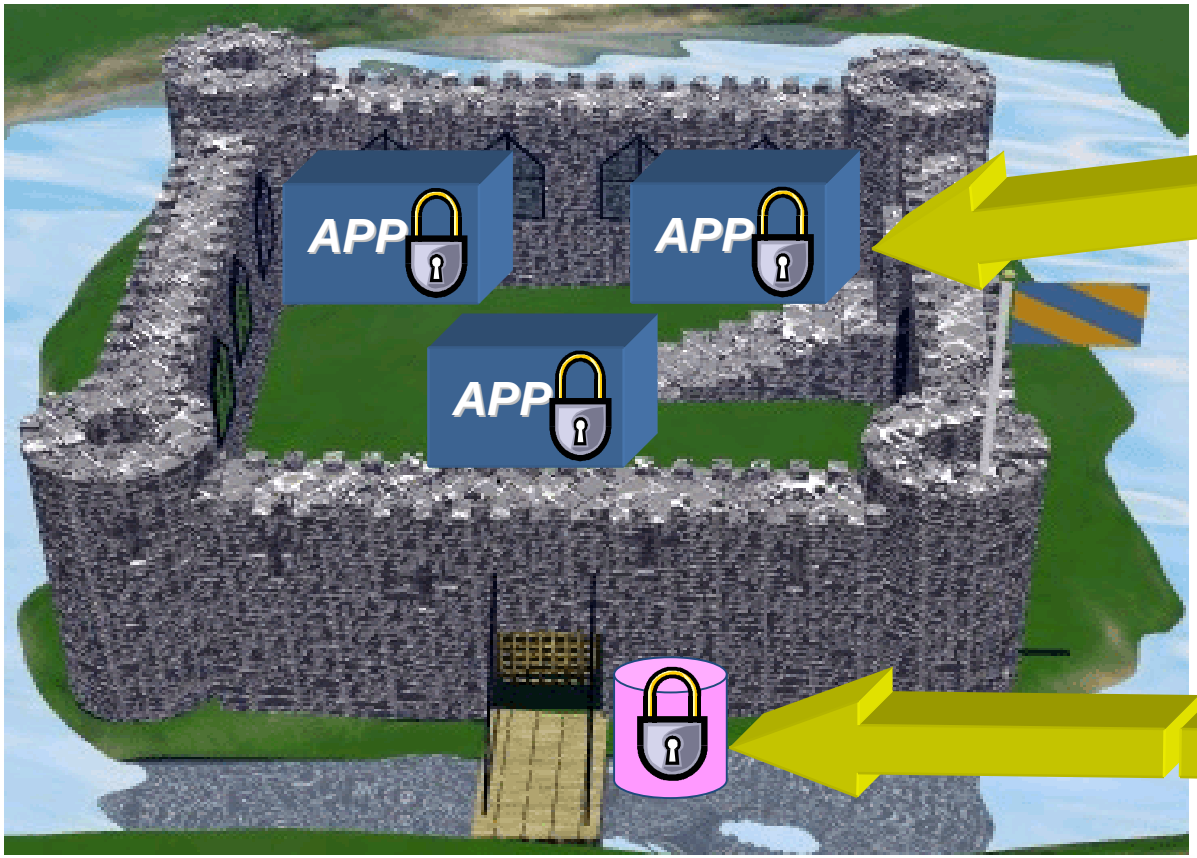
解决客户问题

- 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



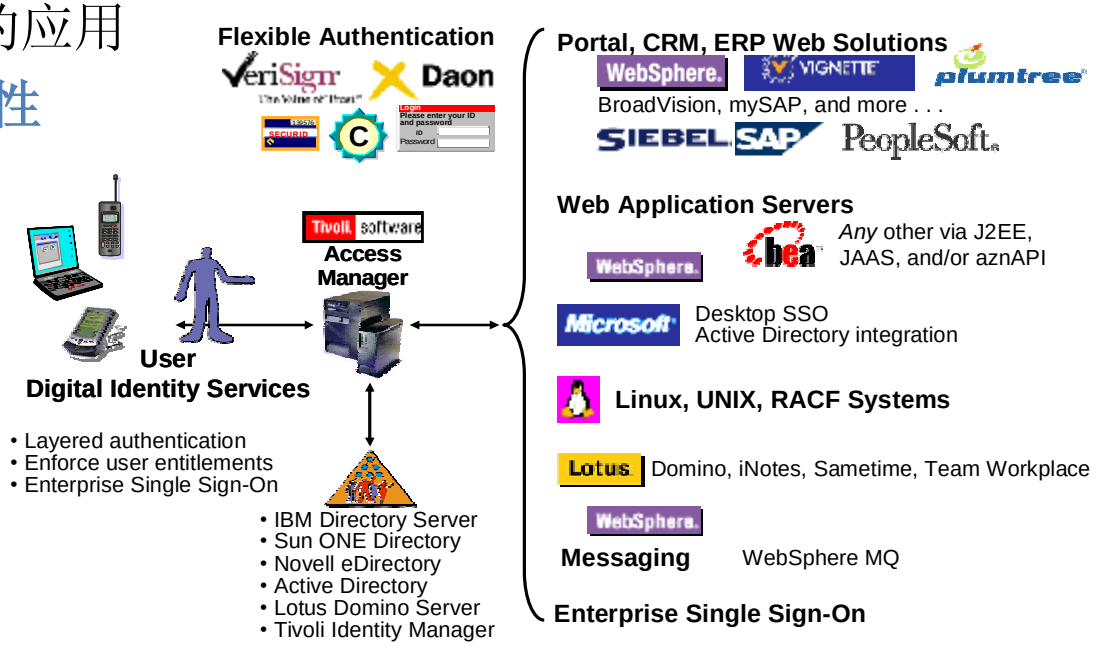
企业架构模式

面向整个企业的所有应用，架构应用系统安全平台

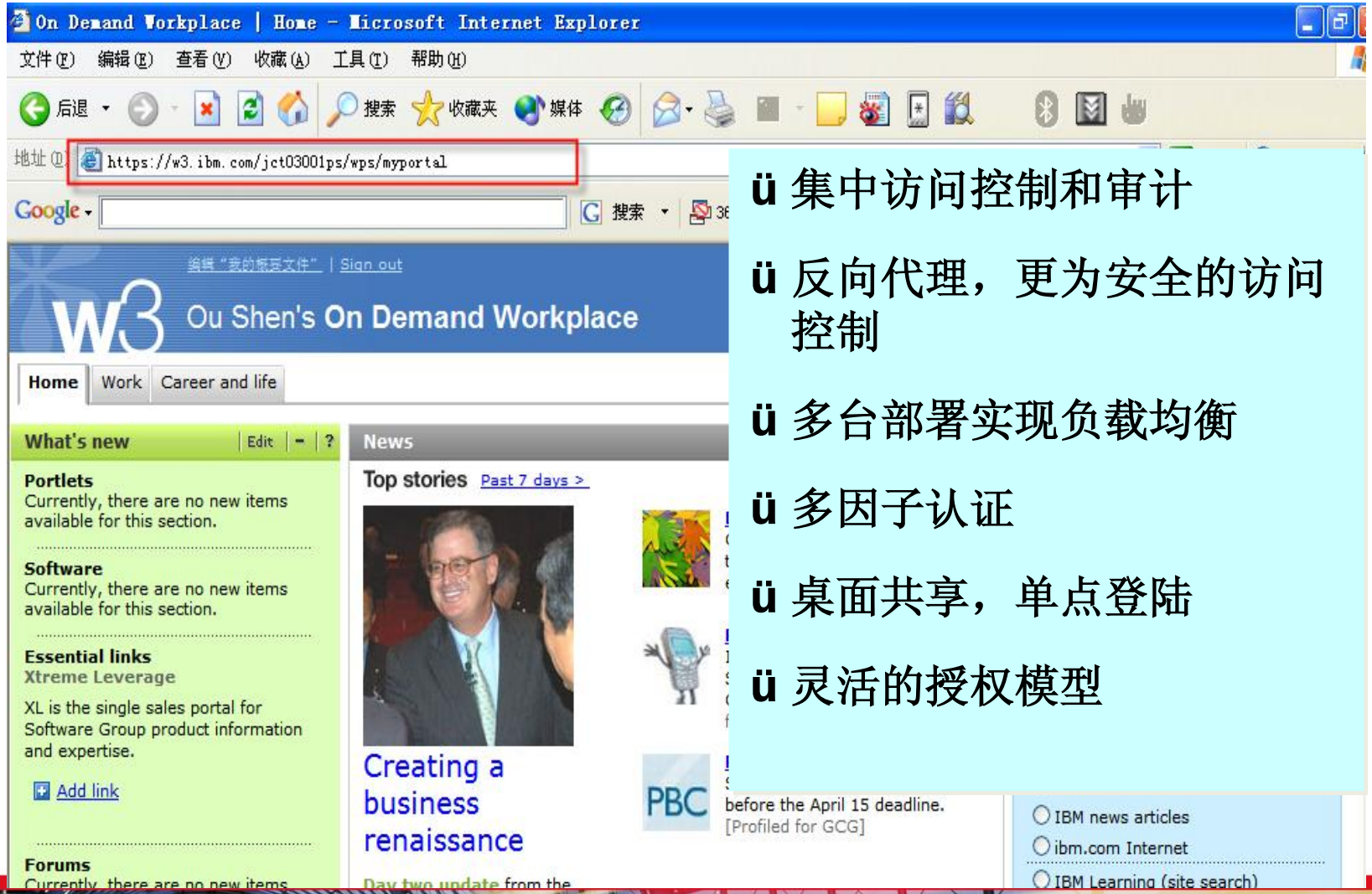


集中的应用访问认证和授权服务
Tivoli Access Manager for e-Business (TAMeB)

- 控制对系统、应用、数据和信息的访问
- 提供基于策略的管理
  - 用户、门户、Web 应用、定制应用
- 支持单一登录基于 Web 的应用
- 解决安全问题并确保可用性

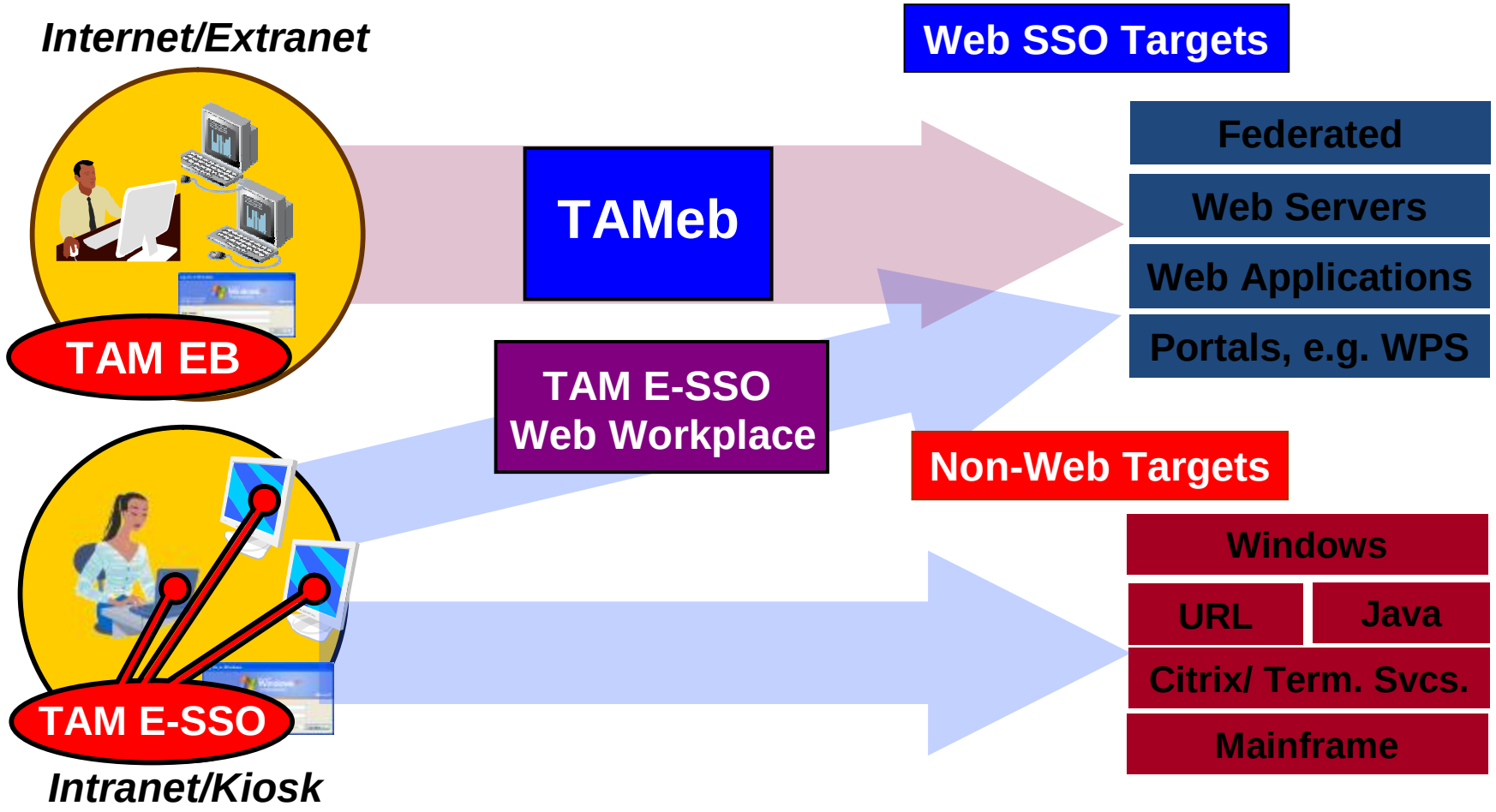


Tivoli Access Manager对Portal的加强

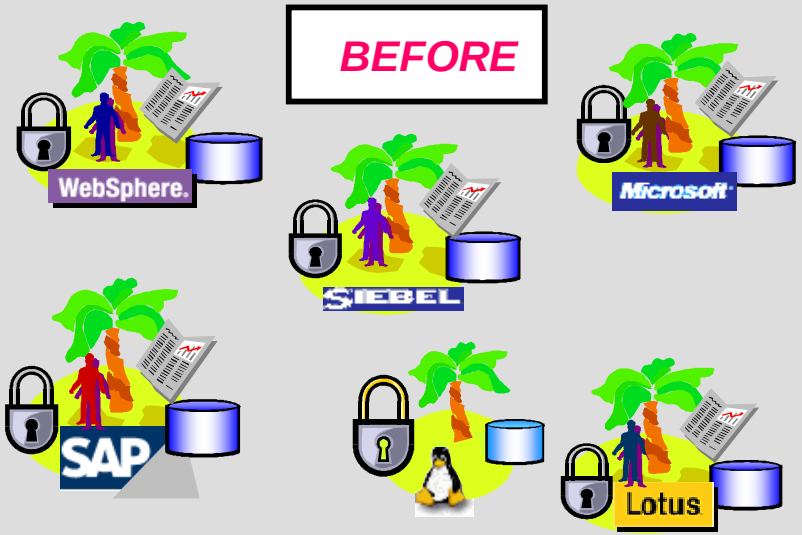


- ü 集中访问控制和审计
- ü 反向代理，更为安全的访问控制
- ü 多台部署实现负载均衡
- ü 多因子认证
- ü 桌面共享，单点登陆
- ü 灵活的授权模型

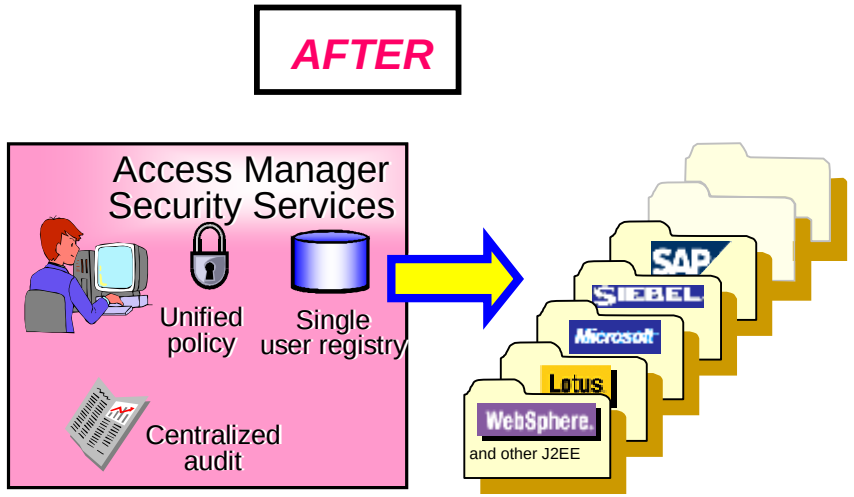
完整的单点登录(Single Sign-On)
Tivoli Access Manager



Tivoli IAM – 功能与价值



§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
§安全成为应用开发者的任务
§策略依从性?

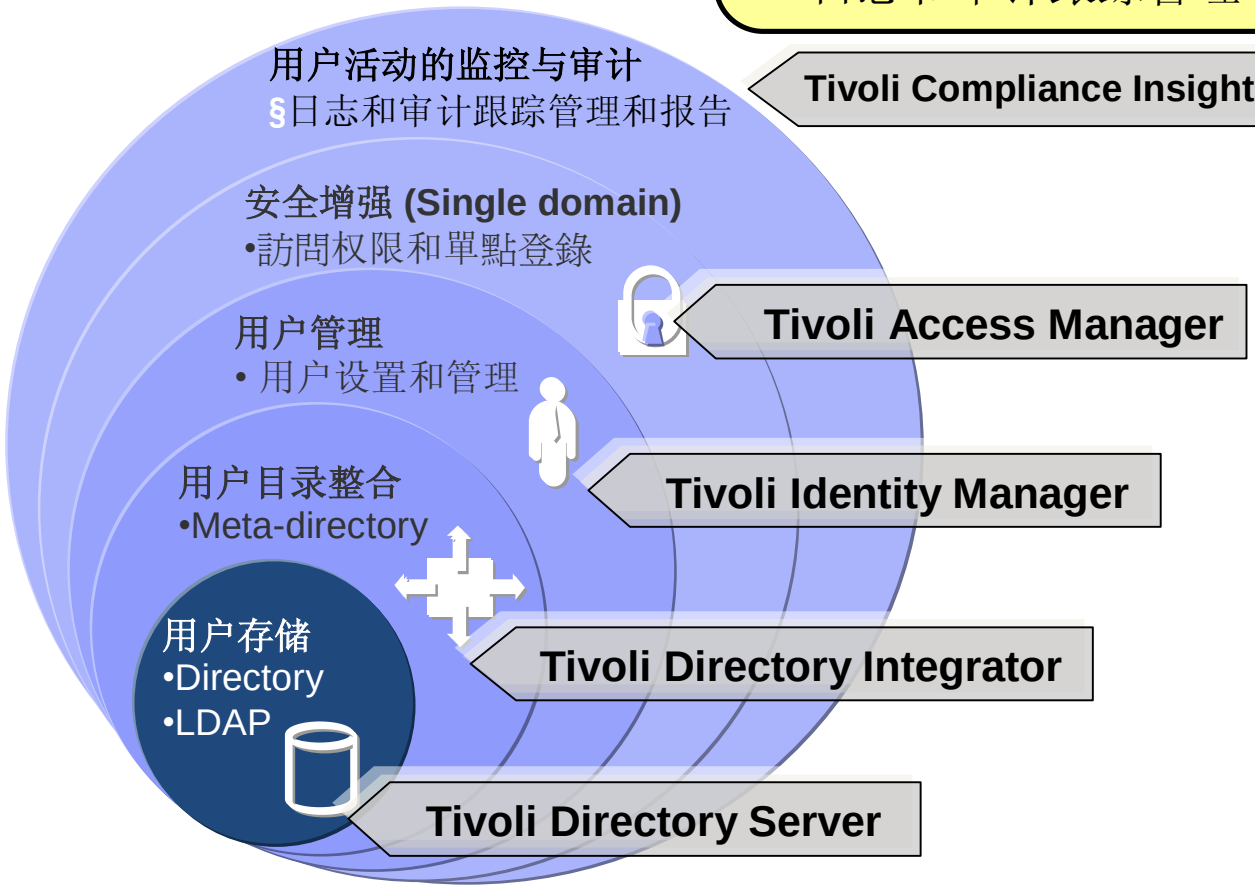


§Web单点登录，单一工具完成访问控制
§单一安全域，或是基于单一工具的委派管理
§集中的用户和安全信息
§策略+审计=策略依从
§建立安全标准，具有高度扩展性

= 安全策略　　= 用户和组的信息　　= 审计

身份管理应用模式：用户

- 安全制度遵从情况的显示板和报告
- 特权用户的监控与审计
- 数据库的监控和审计
- 日志和审计跟踪管理

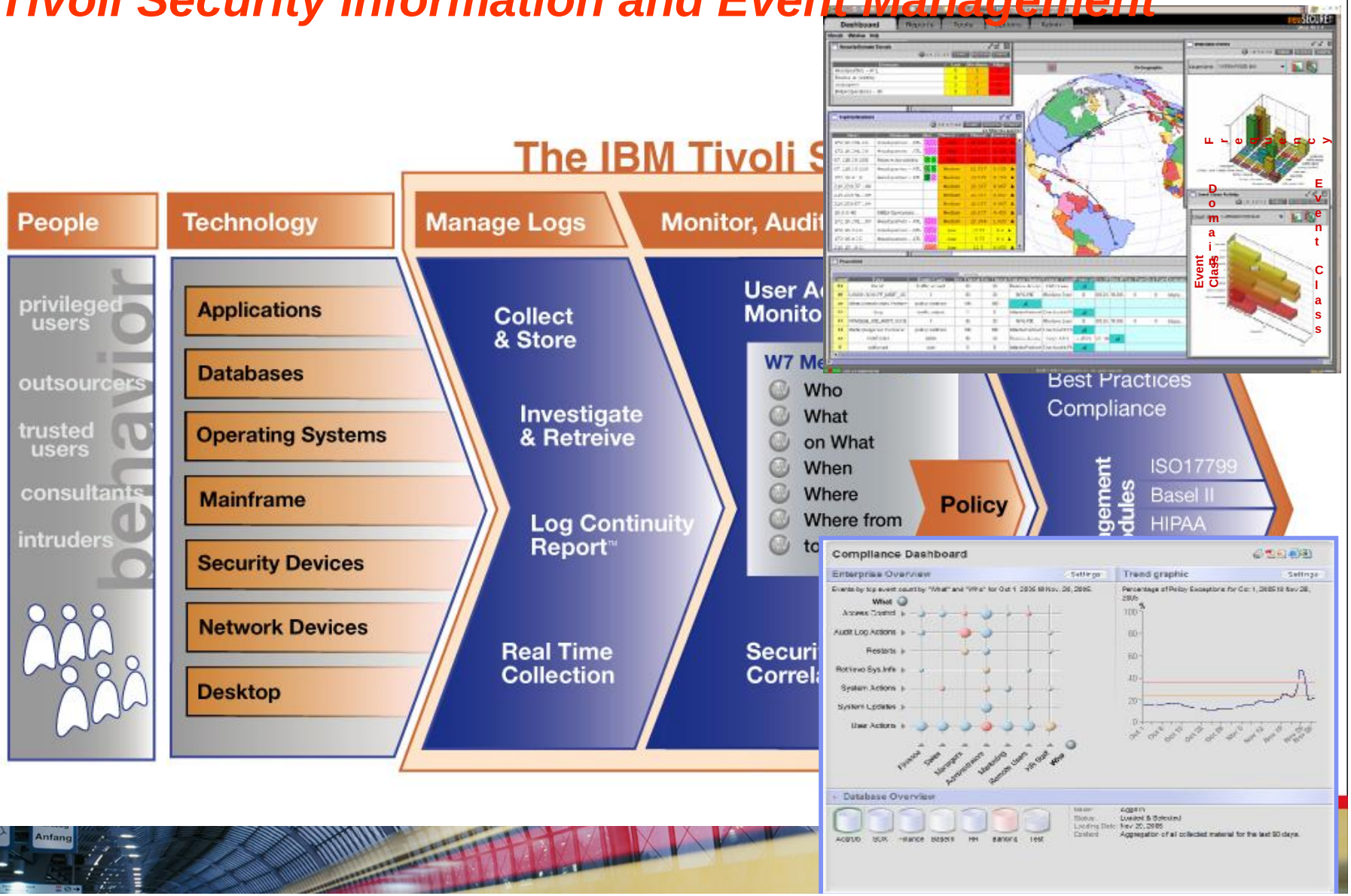


内部威胁

- 在引起资产损失的安全事故中，有 70% 的事故涉及内部威胁。（Gartner）
- 33% 的信息安全攻击来自于内部员工，而 28% 来自前雇员和合作伙伴（PricewaterhouseCoopers）
- 平均情况下，员工拥有的访问权要比实际需要多出 35%（Insider Threat）
- 在 87% 的情况下，恶意内部用户会使用简单的、合法的用户命令。（U.S. Secret Service and Carnegie Mellon）
- 出现数据破坏后，有 50% 的公开上市公司的市值损失超过 20%。（Deloitte）

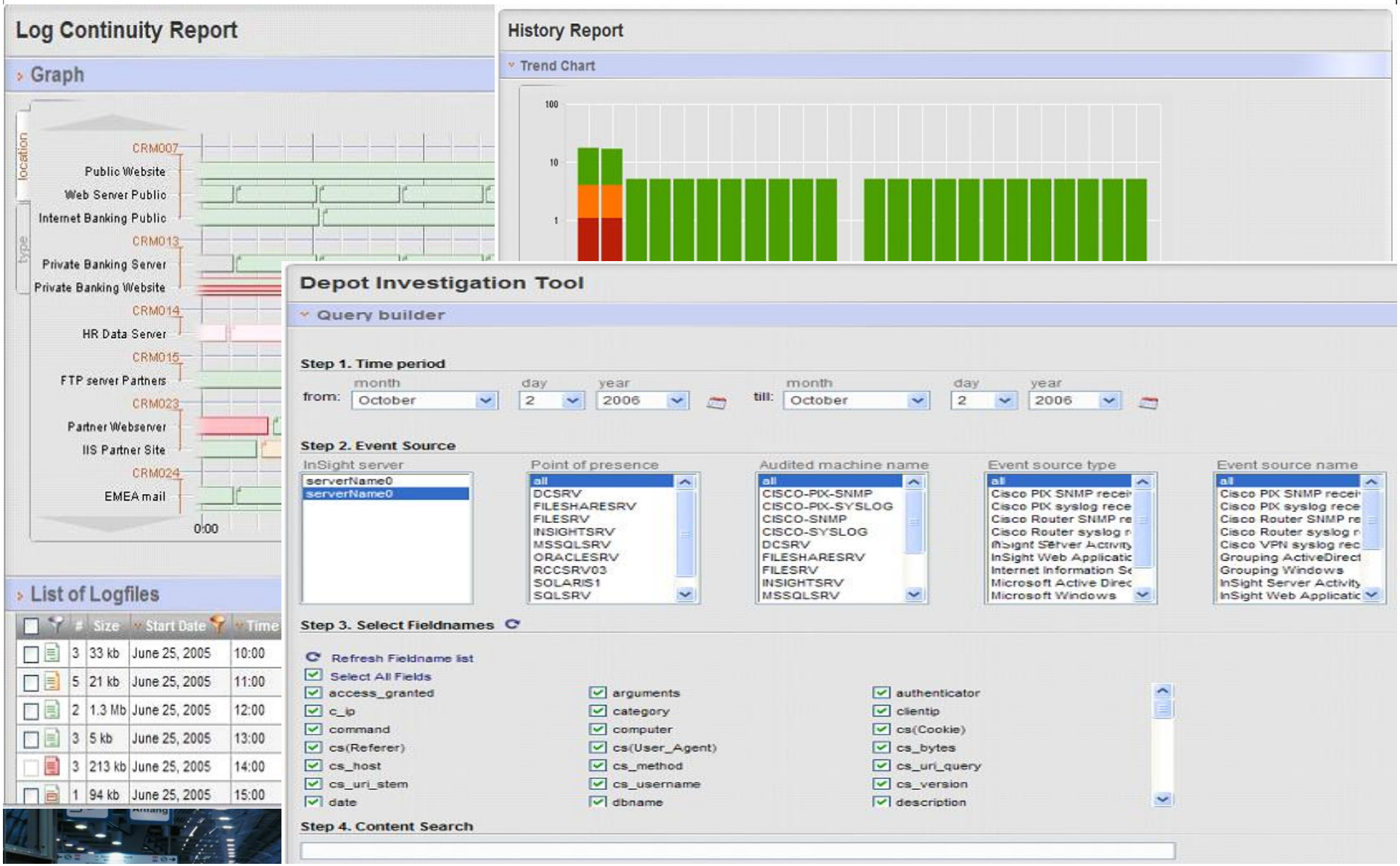
实时信息管理和事后审计管理

Tivoli Security Information and Event Management



日志管理

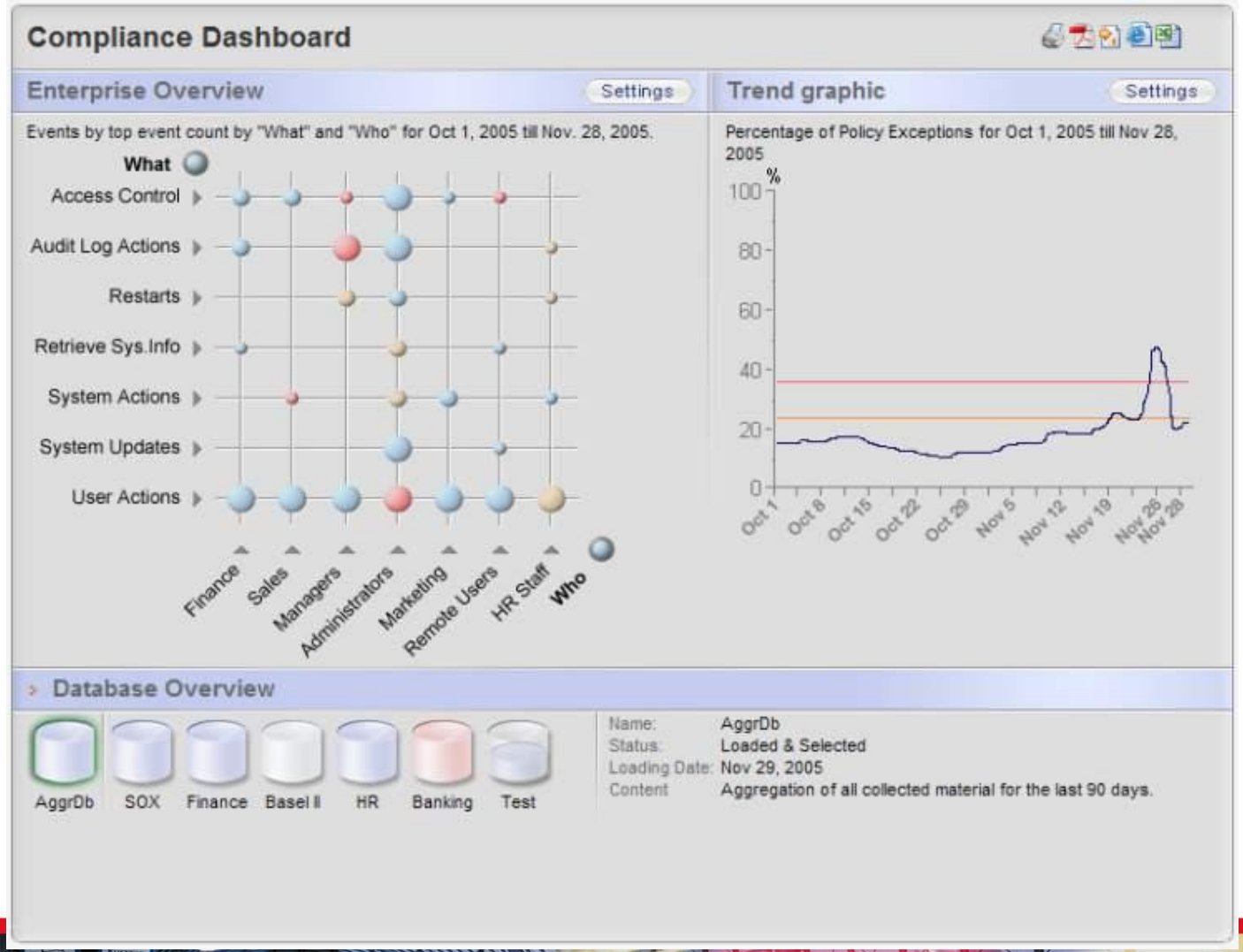
日志连续性及历史报告，
可即刻向管理及审计人員证明日志管理程序的完整性和持续性。



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！

TCIM – 使用制度遵从显示板提供监控

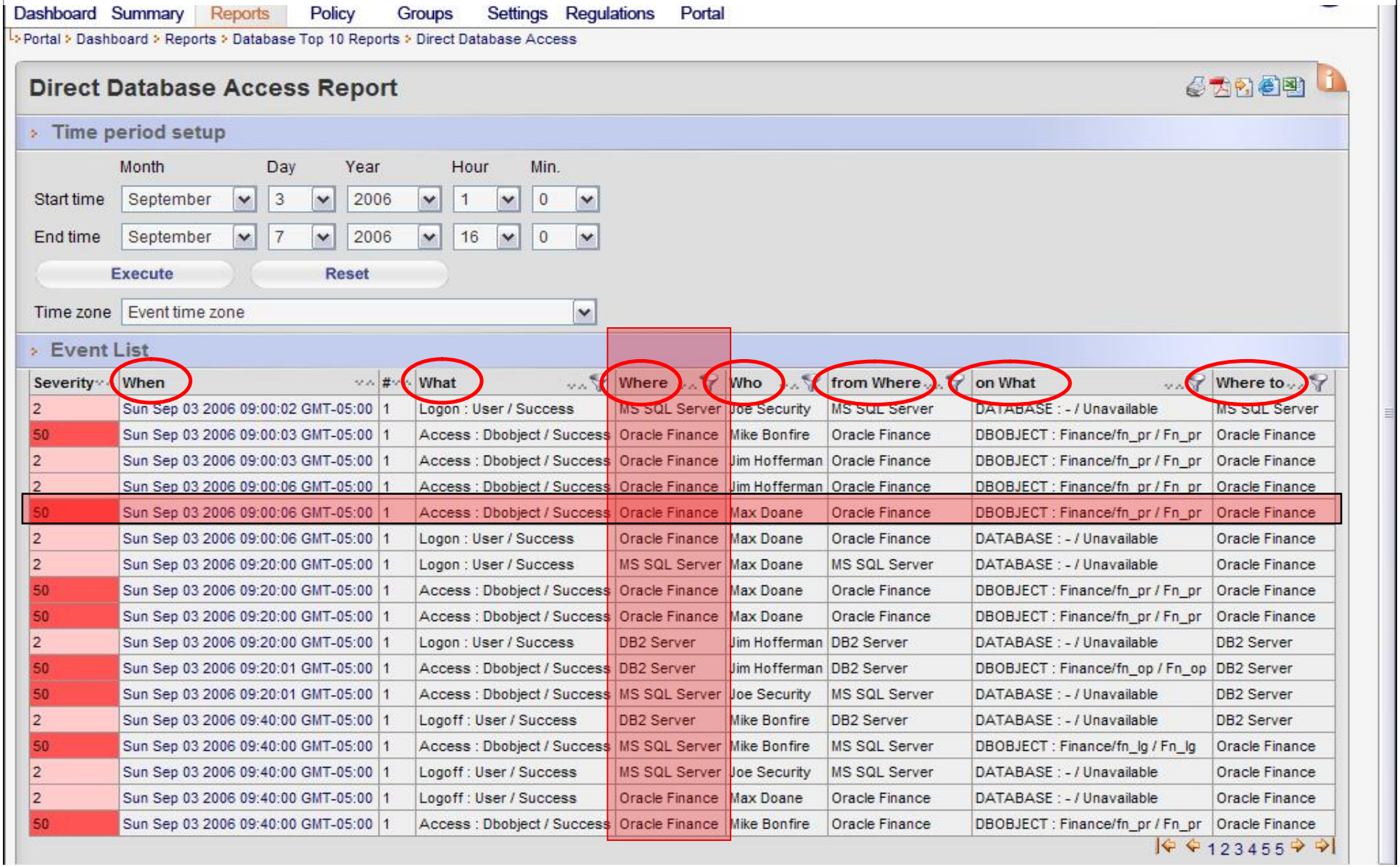


- 快速深入察看细节
- 违规
- 特别提示
- 故障
- 趋势
- 报告数据库
- 汇聚数据库
- 企业概述
- 报告分发
- 自助审计

Database Monitoring and Audit

W7 事件列表

注意! DBA Max Doane正在读取工资单



Dashboard Summary Reports Policy Groups Settings Regulations Portal

Portal > Dashboard > Reports > Database Top 10 Reports > Direct Database Access

Direct Database Access Report

Time period setup

	Month	Day	Year	Hour	Min.
Start time	September	3	2006	1	0
End time	September	7	2006	16	0

Execute Reset

Time zone: Event time zone

Event List

Severity	When	#	What	Where	Who	from Where	on What	Where to
2	Sun Sep 03 2006 09:00:02 GMT-05:00	1	Logon : User / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	MS SQL Server
50	Sun Sep 03 2006 09:00:03 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:03 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Jim Hofferman	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Jim Hofferman	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Logon : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
2	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	MS SQL Server	Max Doane	MS SQL Server	DATABASE : - / Unavailable	Oracle Finance
50	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	DB2 Server	Jim Hofferman	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbobject / Success	DB2 Server	Jim Hofferman	DB2 Server	DBOBJECT : Finance/fn_op / Fn_op	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbobject / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	DB2 Server
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	DB2 Server	Mike Bonfire	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Access : Dbobject / Success	MS SQL Server	Mike Bonfire	MS SQL Server	DBOBJECT : Finance/fn_lg / Fn_lg	Oracle Finance
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	Oracle Finance
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
50	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance

1 2 3 4 5 5

IBM Tivoli身份管理解决方案优势

- Tivoli IAM解决方案包括构建解决方案所需的IBM中间件
  - 數據庫(DB2)、应用服务器(WAS)、目录服务(TDS/TDI)
- 功能完善，一个方案解决所有关键需求。
  - 集中用户访问和单点登录
  - 集中用户管理
  - 集中日志审计
- 利用即成产品缩短实现价值的时间
  - 通过配置可以实现更多的定制功能，不需要开发新软件组件
  - 丰富的API集合可供客户环境所需的定制集成所用
  - 高可用性、可扩展性、稳定性、审计和日志等非功能需求会大大提高开发成本，这些功能都已经在产品中提供
- IBM专业安全服务团队，长期的安全伙伴
  - 无论行业或地理位置，IAM要求跨组织的高度通用性

案例：中国太平洋保险集团

客戶名稱	中國太平洋保險集團 (CPIC)
客戶需求	建立身份帳號管理流程 管理全國8萬個內部用戶帳號設立變更和刪除需求 支持公司主要應用系統的安全訪問與單點登錄 確保集團內安全策略的有效執行，對帳號管理的審計
解決方案	身份帳號配置與管理：Tivoli Identity Manager 訪問授權與單點登錄：Tivoli Access Manager
項目內容	集中身份帳號管理、訪問授權與單點登錄：8萬員工 集中訪問授權：Lotus, OracleERP, Cognos, HR, 保險核心系統, …. 集中身份認證：用戶名/口令、數字証書

案例：上海大众汽车

客戶名稱	上海大众汽车 (CSVW)
客戶需求	集中管理内部员工、供应商、经销商三类用户及其应用账户 三个门户系统应用的访问统一认证和单点访问 理清访问控制策略，确保安全策略的执行和审计
解決方案	身份帳號配置與管理：Tivoli Identity Manager 訪問授權與單點登錄：Tivoli Access Manager
項目內容	集中三类用户的身份、应用访问授权：1 万员工 集中应用访问认证和授权：Lotus, SAP、EAI、WCM、DMS、E-Scheduling …. 集中身份认证：用戶名/口令、Token、VPN集成


Thank
You


Kurzzug
Anfang