Tivoli Security, Risk & Compliance Management Solutions

Pierre G. Noel
Executive, Worldwide Risk Management & Information Security
pierre.noel@hk.ibm.com

Why Customers want our Security Bundles?

They need to address Increased Corporate Governance

They Buy solutions that Save Money, ***NOW***

They want to automate, and reduce Human Resources' impacts

Customers' Buying Patterns have evolved

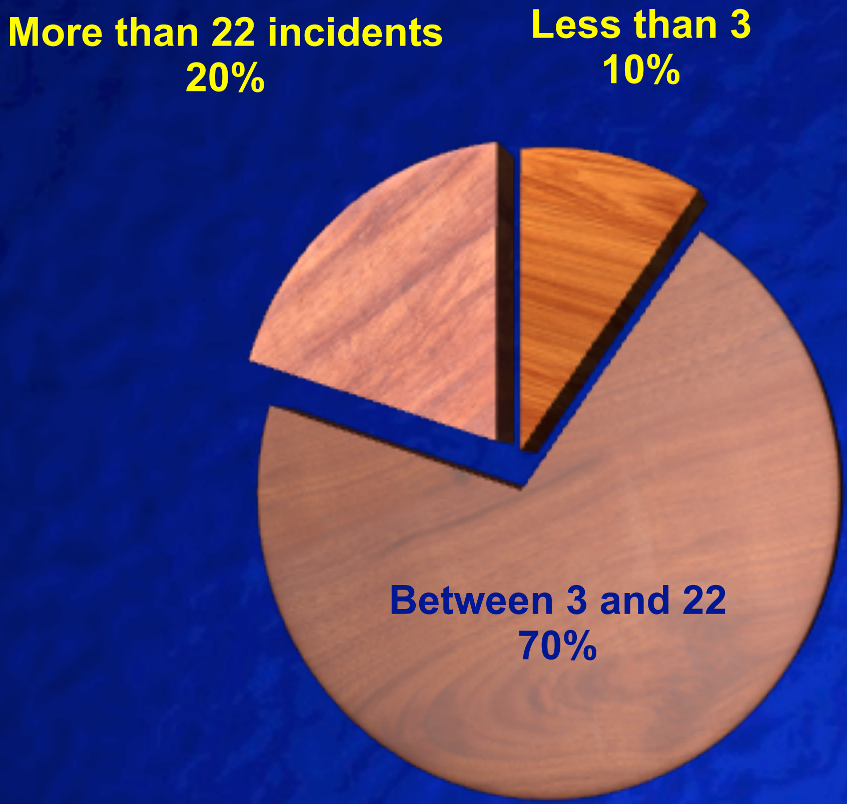
Mergers & Acquisitions

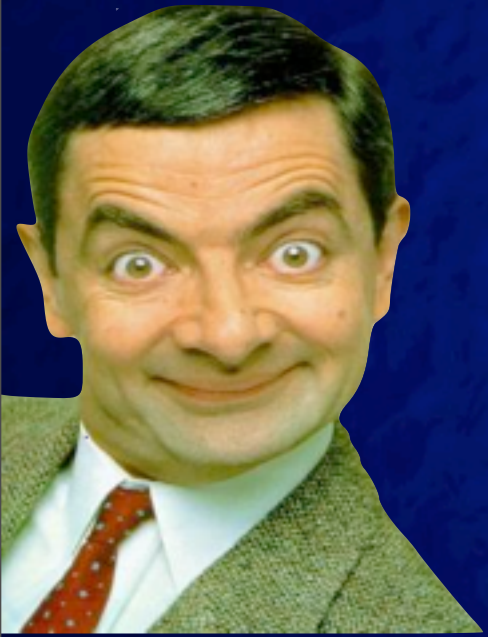
Layoffs

Incidents Increase

Security Requirements

Breaches of sensitive business data in past year:





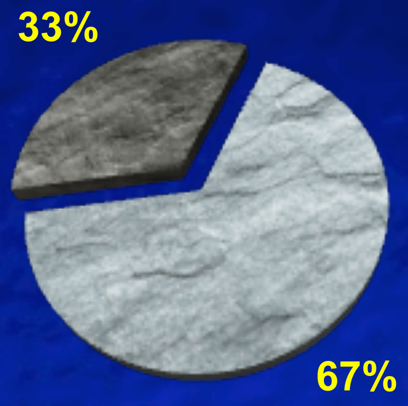
Source: 2006,07,08 survey by the IT Policy Compliance Group

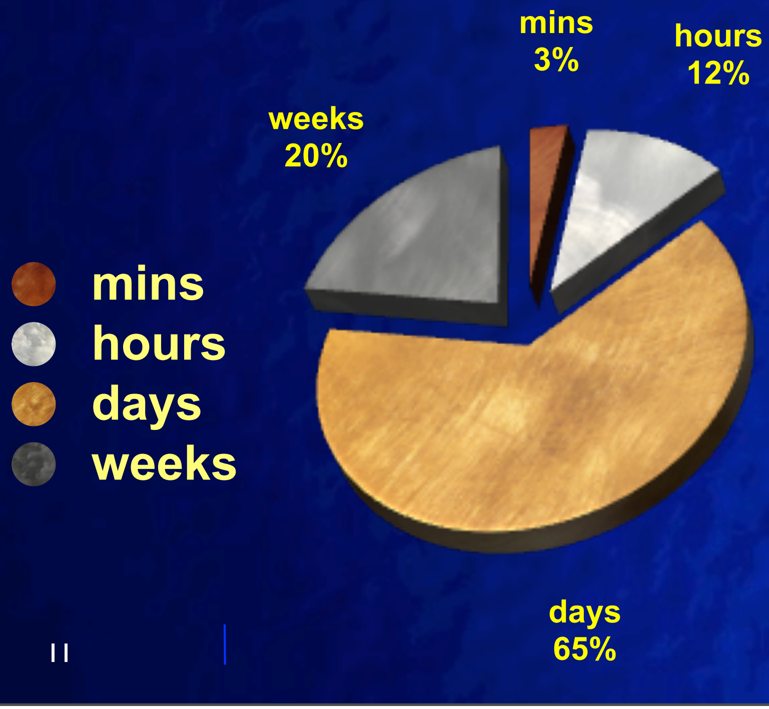
IBM

Another Threat to consider…

Improper Use of Corp Data

- 59% of workers who left their positions took confidential information with them
- 67% used their former company's confidential information to leverage a new job





Time to terminate access

- 24% still had access to Corporate Systems

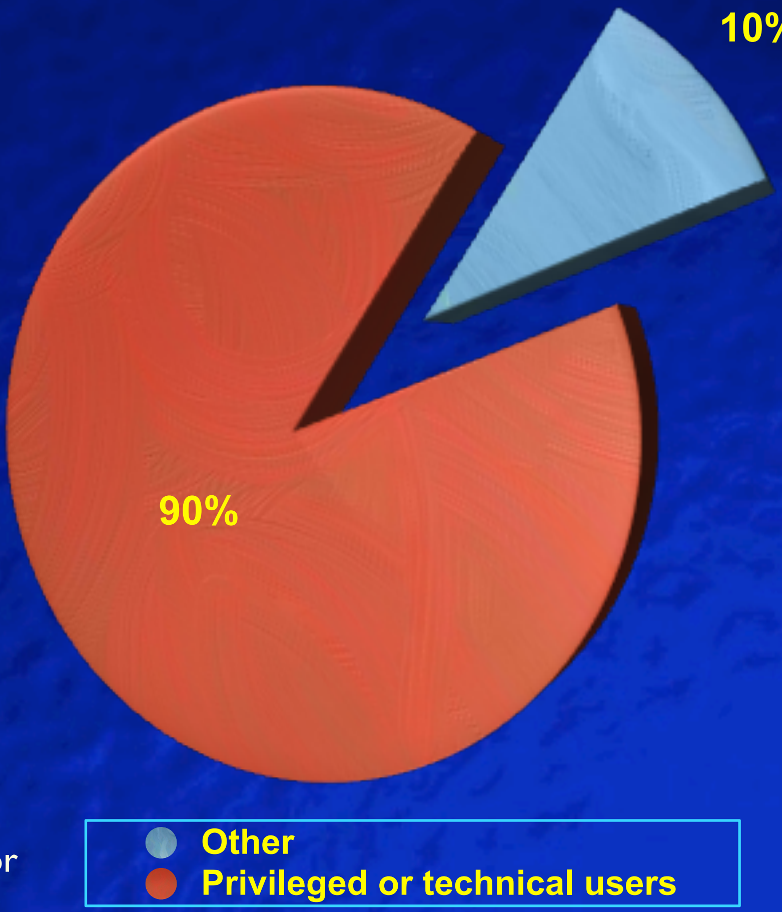
Source: "Data Loss Risks During Downsizing", Ponemon Institute LLC,Feb 23, 2009

Barbarians are Inside our Gates Already

What causes Internal Incidents?

The enemy is "us":

- **90% of insider incidents are caused by privileged or technical users**
  - **Most are inadvertent violations of:**
    - Change management process
    - Acceptable use policy
    - Account management process
  - **Others are deliberate, due to:**
    - Revenge (84%)
    - "Negative events" (92%)
  - **Regardless, too costly to ignore:**
    - Internal attacks cost 6% of gross annual revenue or 9 dollars per employee per day



Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005/6; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.

Tivoli Security Bundles

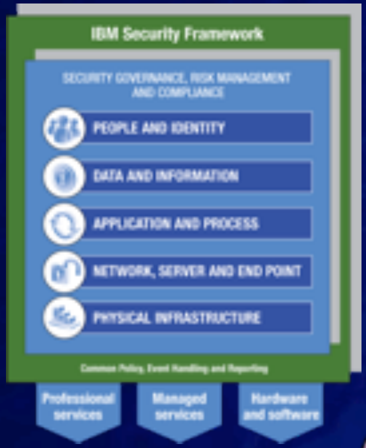
Addresses higher level pain points than point product sales

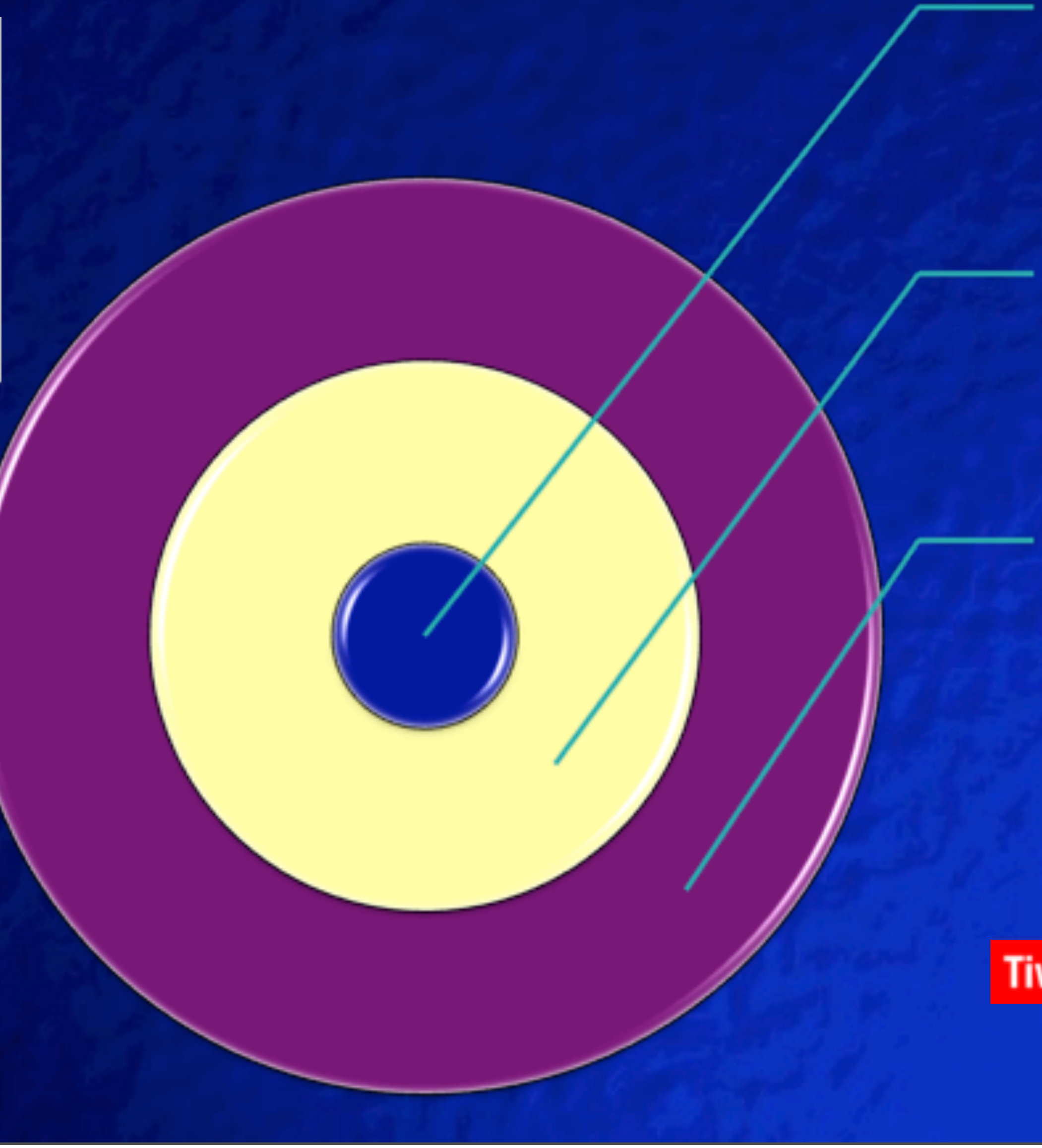
Provides clients greater value for the money in tough economy

Distinct competitive advantages and opportunities for take-aways

Simplified market messaging and ordering

Tivoli Security Solutions
Buying a car, not parts





Mainframe as my Bastion

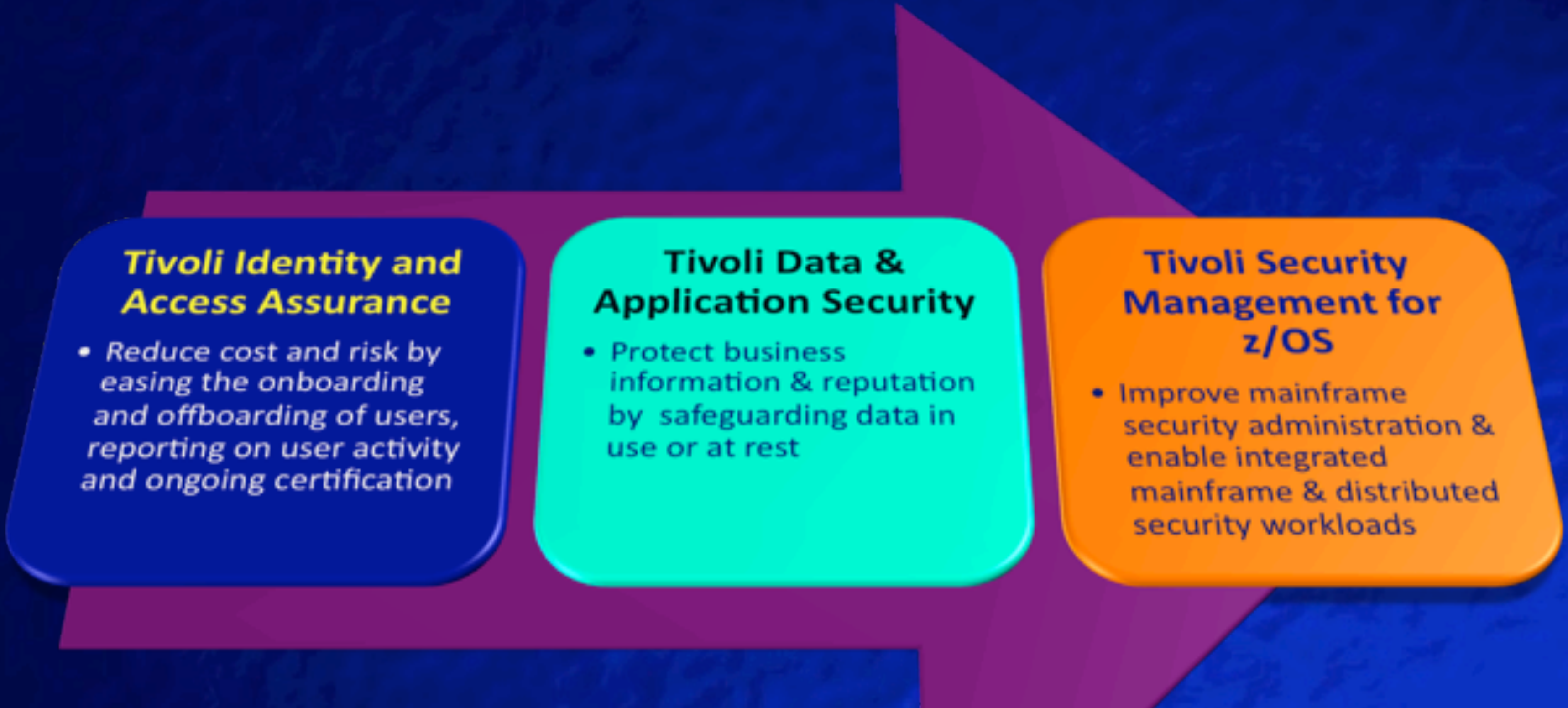
Securing Data & Applications

People approaching my critical information assets

Tivoli software

© 2009 IBM Corporation

IBM Tivoli Security Bundles



Tivoli Identity and Access Assurance

- *Reduce cost and risk by easing the onboarding and offboarding of users, reporting on user activity and ongoing certification*

Tivoli Data & Application Security

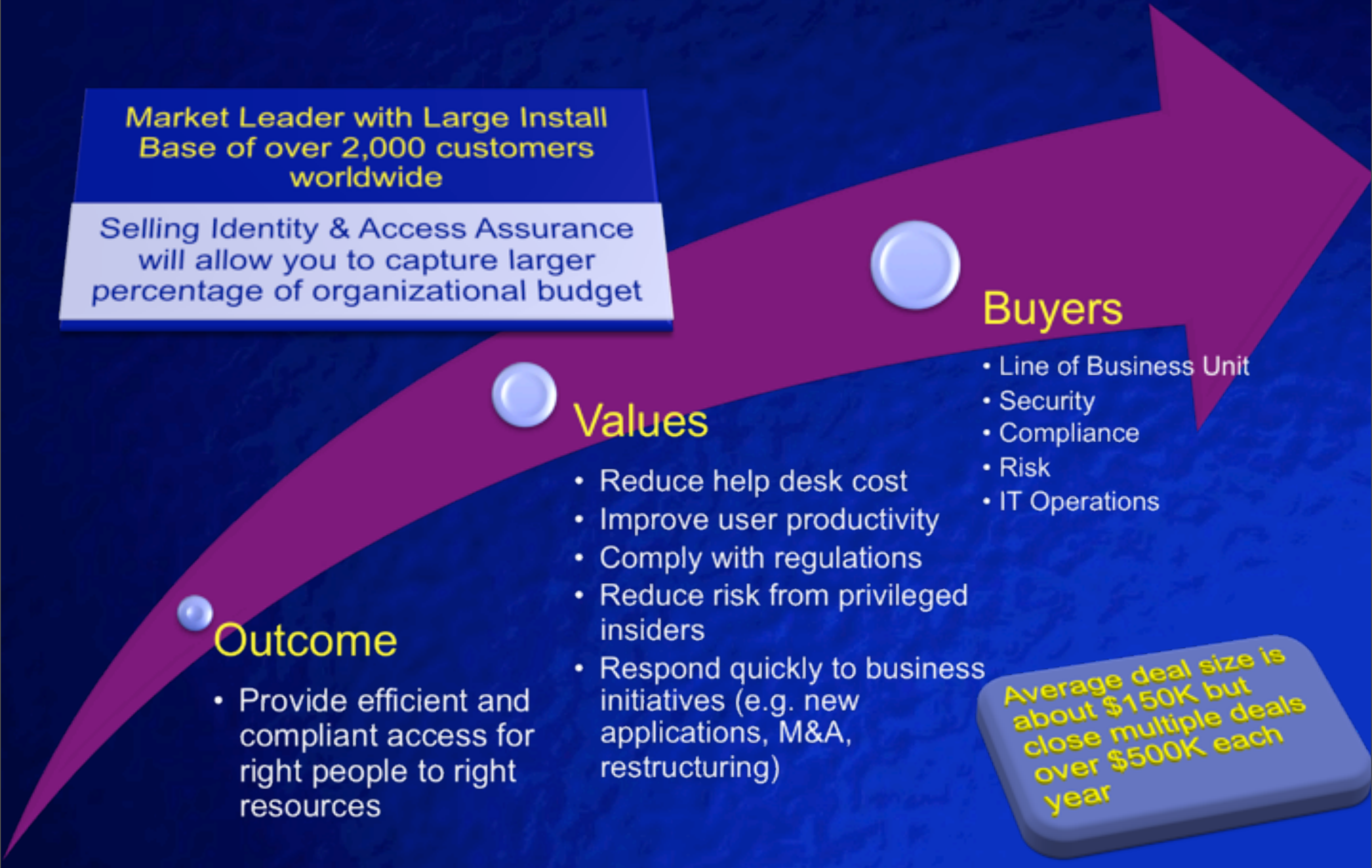
- Protect business information & reputation by safeguarding data in use or at rest

Tivoli Security Management for z/OS

- Improve mainframe security administration & enable integrated mainframe & distributed security workloads

IBM Security Framework
SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE
PEOPLE AND IDENTITY
DATA AND INFORMATION
APPLICATION AND PROCESS
NETWORK, SERVER AND END POINT
PHYSICAL INFRASTRUCTURE
Common Policy, Event Handling and Reporting
Professional services
Managed services
Hardware and software

Identity and Access Assurance



Market Leader with Large Install Base of over 2,000 customers worldwide

Selling Identity & Access Assurance will allow you to capture larger percentage of organizational budget

Outcome

- Provide efficient and compliant access for right people to right resources

Values

- Reduce help desk cost
- Improve user productivity
- Comply with regulations
- Reduce risk from privileged insiders
- Respond quickly to business initiatives (e.g. new applications, M&A, restructuring)

Buyers

- Line of Business Unit
- Security
- Compliance
- Risk
- IT Operations

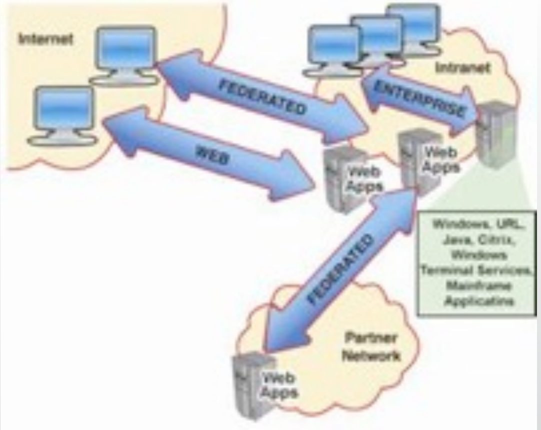
Average deal size is about $150K but close multiple deals over $500K each year

Why Identity and Access Assurance?

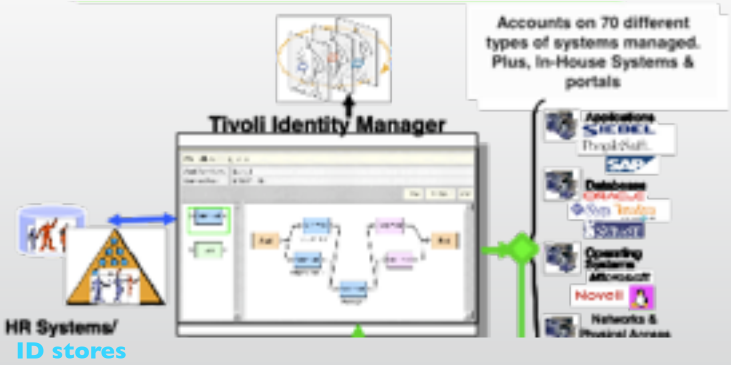
- **Improve Service**
  - Common IT Services Portal to offer ID services as well
  - Enable collaboration via role based portals with access to enterprise services and applications
  - Increase market reach with federated business models leveraging trusted identity information
- **Reduce Cost**
  - Reduce help desk costs, password resets
  - More efficiently manage restructuring
  - ERP deployments / upgrades
- **Manage Risk**
  - Privileged IDs
  - Shared IDs
  - Failed audits
  - Prevent insider breach
  - Recertification, Access Attestation
  - National ID / Trusted ID – provisioning of strong / trusted credentials.
  - Unauthorized IT change detection

Identity and Access Assurance in a nutshell

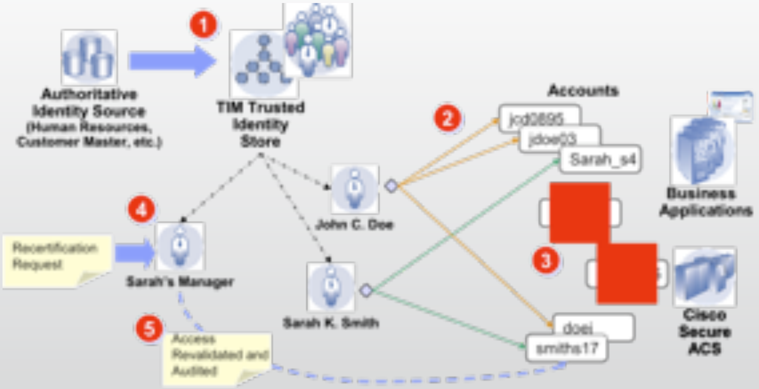
Single Sign On & Password Management



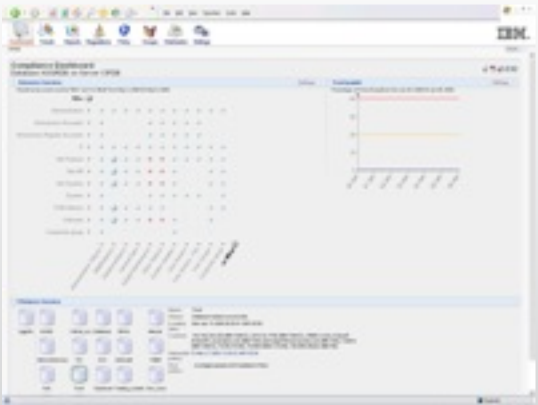
User Provisioning / Role Management

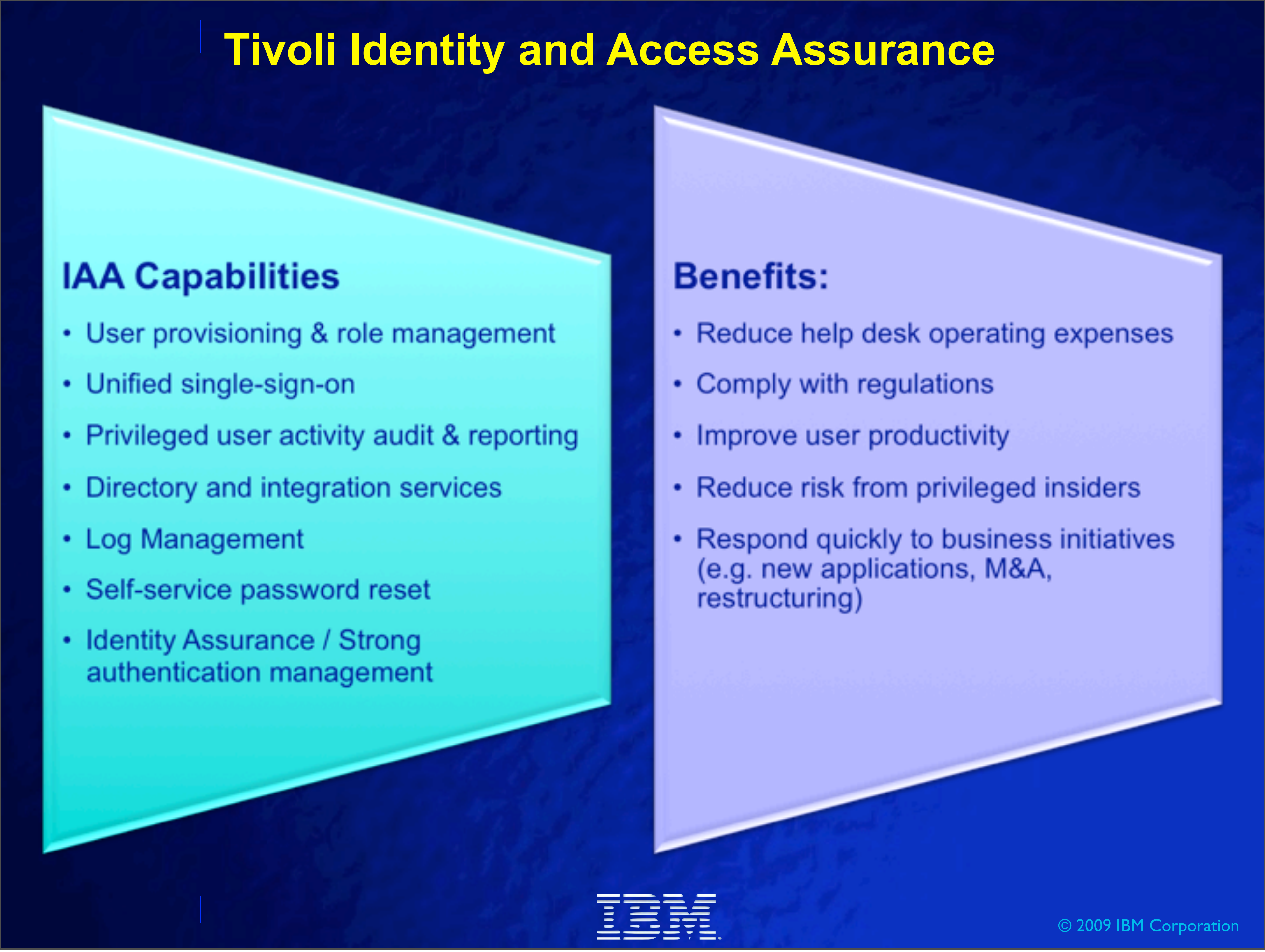


Access Validation & Compliance



Security log management & reporting





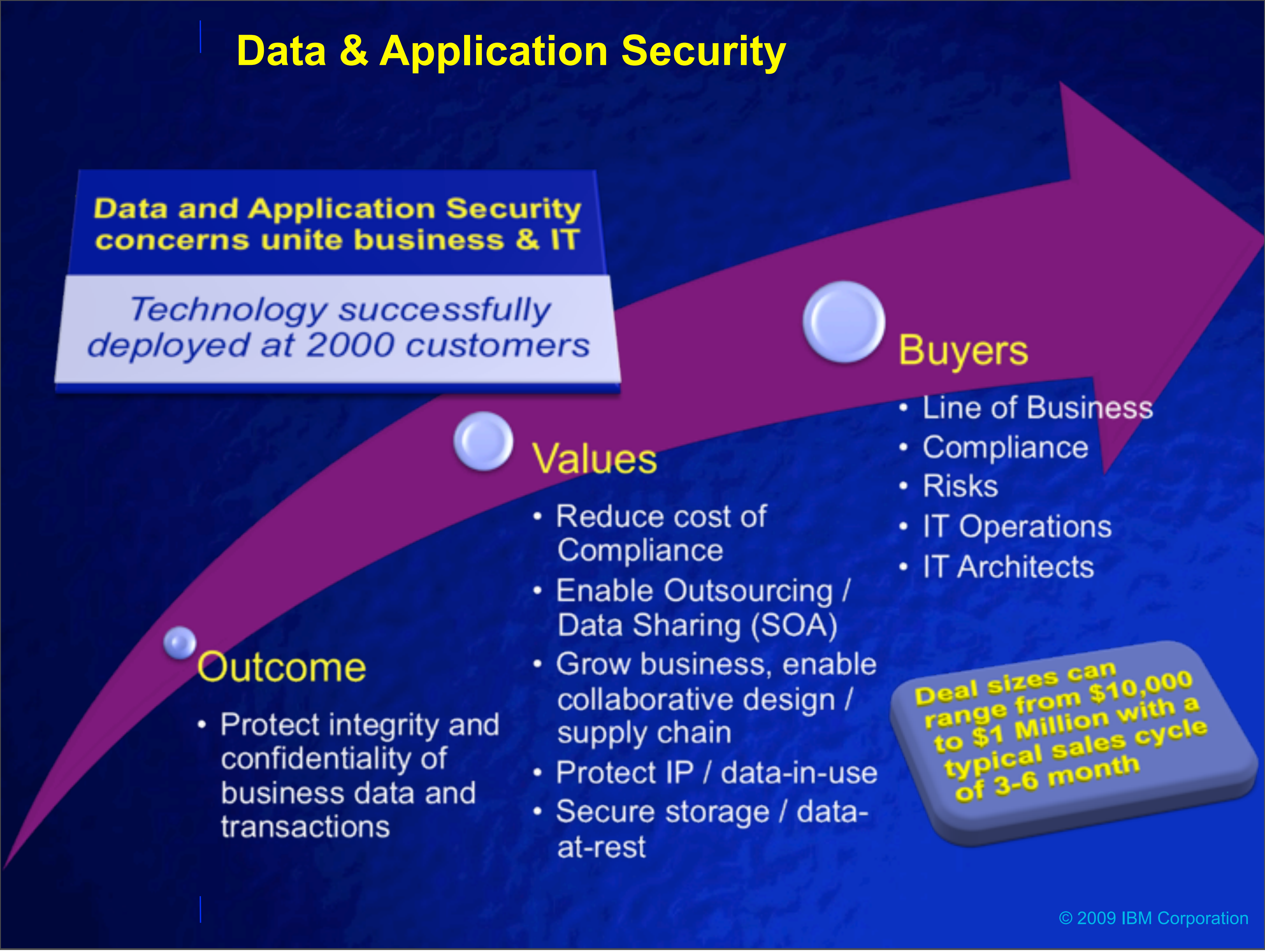
Tivoli Identity and Access Assurance

IAA Capabilities

- User provisioning & role management
- Unified single-sign-on
- Privileged user activity audit & reporting
- Directory and integration services
- Log Management
- Self-service password reset
- Identity Assurance / Strong authentication management

Benefits:

- Reduce help desk operating expenses
- Comply with regulations
- Improve user productivity
- Reduce risk from privileged insiders
- Respond quickly to business initiatives (e.g. new applications, M&A, restructuring)



Data & Application Security

Data and Application Security concerns unite business & IT

Technology successfully deployed at 2000 customers

Outcome

- Protect integrity and confidentiality of business data and transactions

Values

- Reduce cost of Compliance
- Enable Outsourcing / Data Sharing (SOA)
- Grow business, enable collaborative design / supply chain
- Protect IP / data-in-use
- Secure storage / data-at-rest

Buyers

- Line of Business
- Compliance
- Risks
- IT Operations
- IT Architects

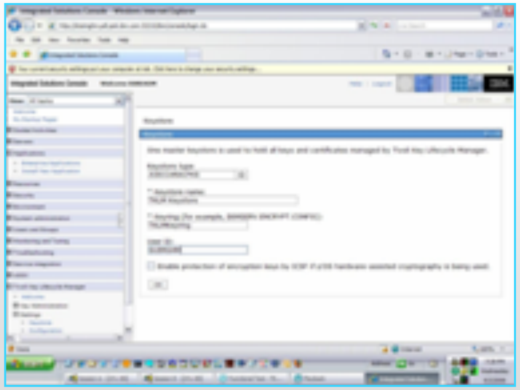
Deal sizes can range from $10,000 to $1 Million with a typical sales cycle of 3-6 month

Why Data and Application Security?

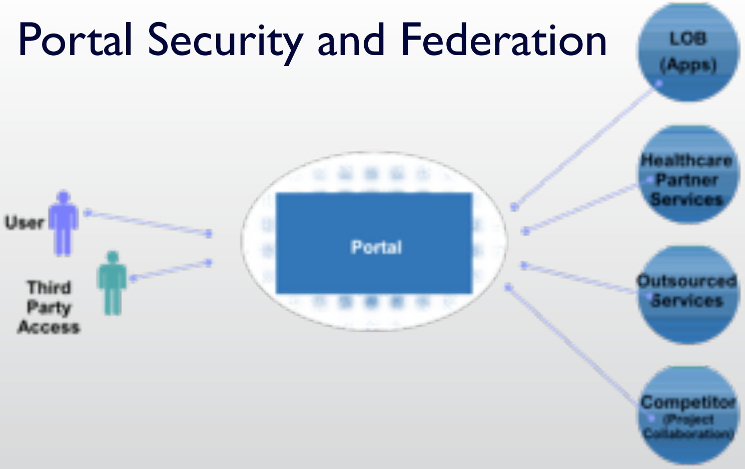
- **Improve Service**
  - Enable Outsourcing / Data Sharing
  - Grow business, enable collaborative design / supply chain
- **Reduce Cost**
  - Reduce “cost of compliance”
  - Ease storage upgrade / expansion by leveraging centralized security
- **Manage Risk**
  - Data disclosure / privacy regulations
  - Failed audits, insider breach in industry
  - Lost backup tapes / laptops
  - SOA, SharePoint, DataPower, Portal

Data and Application Security in a nutshell

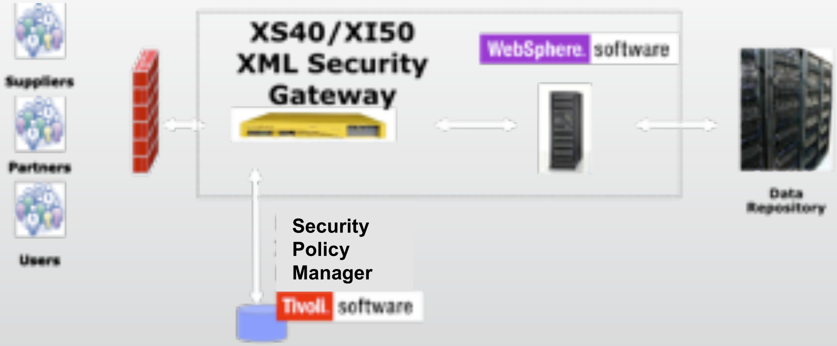
Encrypted Disks
& Archive Tapes
with
Key Management



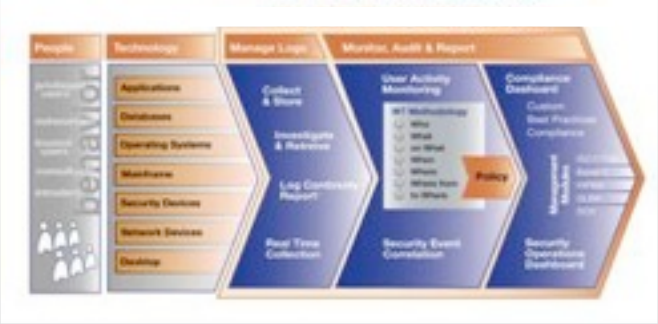
Portal Security and Federation

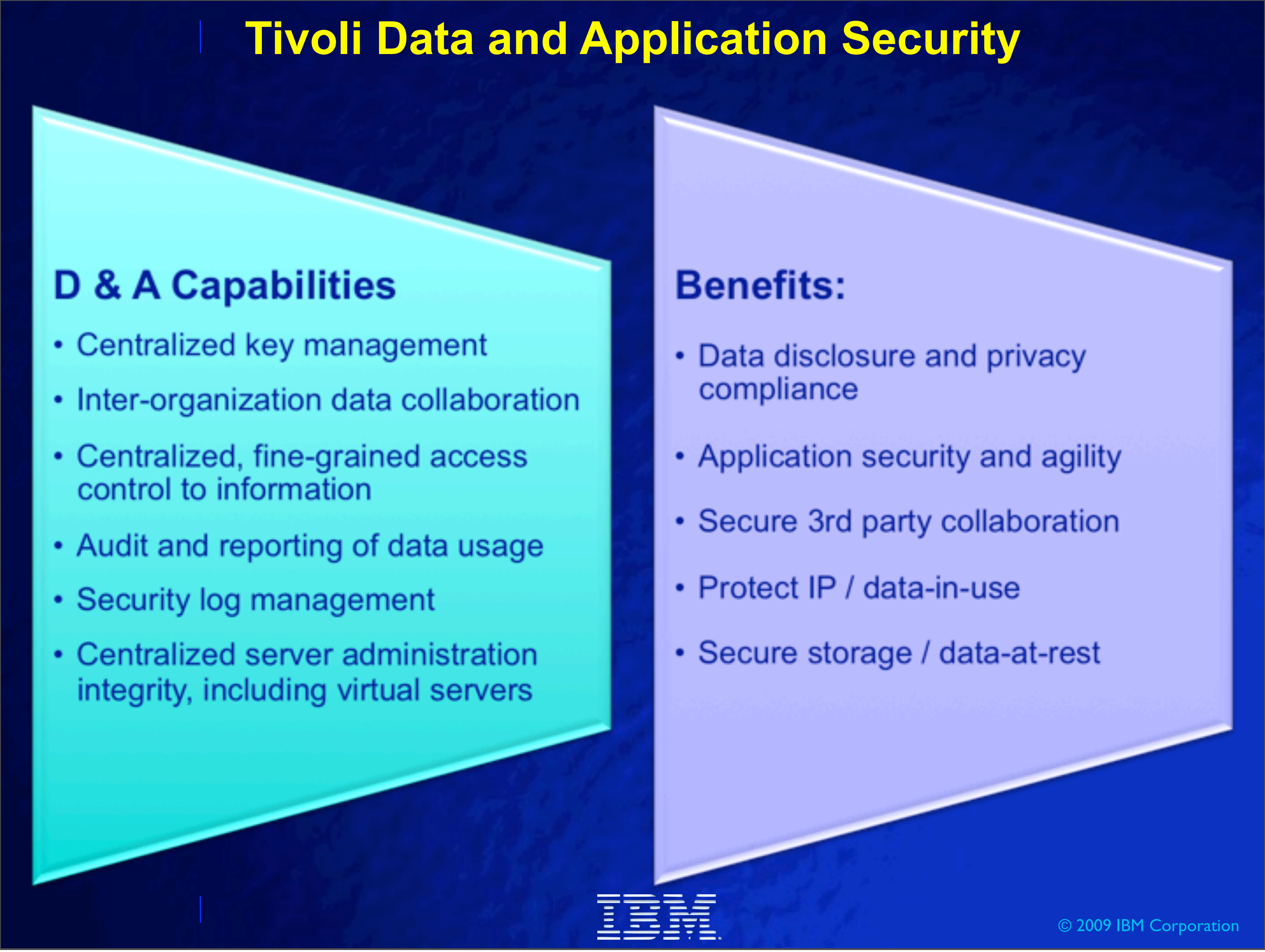


SharePoint / DataPower management



Security log management & reporting





Tivoli Data and Application Security

D & A Capabilities

- Centralized key management
- Inter-organization data collaboration
- Centralized, fine-grained access control to information
- Audit and reporting of data usage
- Security log management
- Centralized server administration integrity, including virtual servers

Benefits:

- Data disclosure and privacy compliance
- Application security and agility
- Secure 3rd party collaboration
- Protect IP / data-in-use
- Secure storage / data-at-rest

Security Management for z/OS

zSecure and Security on zLinux are huge opportunity areas. Large deals with relatively short sales cycle

Aviva $1.6m, Fiducia $2.0m, Vanguard $1.0m, Swiss re $2.0m, Large Telco $7.0m,

Outcome

- Secure critical business services with their most trusted and resilient platform

Values

- Secure critical mainframe hosted data and transactions
- Reduce "cost of compliance"
- Improve service availability
- Enable Data Center Consolidation

Buyers

- Service Owners
- Security
- Compliance
- IT Operations

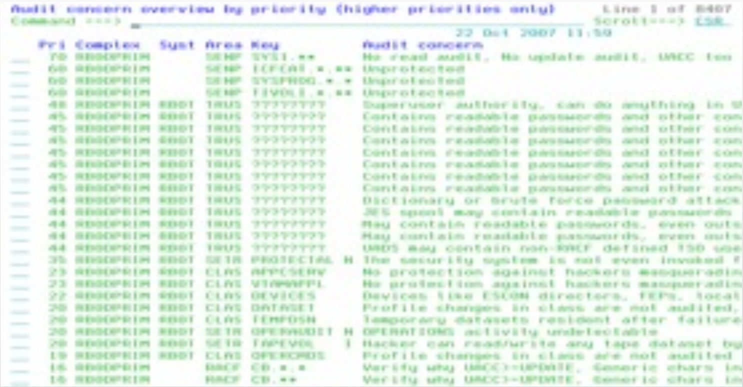
Average deal sizes can range from $50,000 to $1M+ with a typical sales cycle of 3-6 months

Security Management for z/OS?

- **Improve service**
  - **Leverage the most secure platform in the enterprise**
- **Reduce cost**
  - **Datacenter consolidation**
  - **Imbedded best practices**
  - **Reduce “cost of compliance”**
- **Manage risk**
  - **Data disclosure / privacy regulations**
  - **Failed audits, breach in industry**
  - **Lost backup tapes**

Security management for System z in a nutshell

Audit Concern Overview Reports

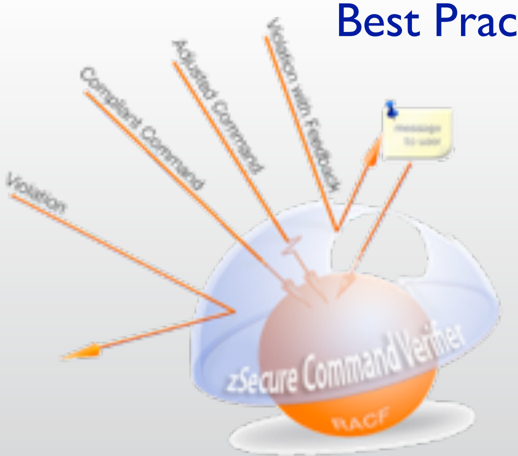


```
Audit concern overview by priority (higher priorities only)     Line 1 of 8407
Command ===> _                                                  Scroll===> CSR
                                                        22 Oct 2007 11:59
    Pri Complex  Syst Area Key            Audit concern
__   70 RBOOPRIM      SENP SYS1.**        No read audit, No update audit, UACC too
__   60 RBOOPRIM      SENP ICFCAT.*.**    Unprotected
__   60 RBOOPRIM      SENP SYSPROG.*.*    Unprotected
__   60 RBOOPRIM      SENP TIVOLI.*.**    Unprotected
__   48 RBOOPRIM RBDT TRUS ????????       Superuser authority, can do anything in S
__   45 RBOOPRIM RBDT TRUS ????????       Contains readable passwords and other con
__   45 RBOOPRIM RBDT TRUS ????????       Contains readable passwords and other con
__   45 RBOOPRIM RBDT TRUS ????????       Contains readable passwords and other con
__   45 RBOOPRIM RBDT TRUS ????????       Contains readable passwords and other con
__   45 RBOOPRIM RBDT TRUS ????????       Contains readable passwords and other con
__   45 RBOOPRIM RBDT TRUS ????????       Contains readable passwords and other con
__   45 RBOOPRIM RBDT TRUS ????????       Contains readable passwords and other con
__   44 RBOOPRIM RBDT TRUS ????????       Dictionary or brute force password attack
__   44 RBOOPRIM RBDT TRUS ????????       JES spool may contain readable passwords
__   44 RBOOPRIM RBDT TRUS ????????       May contain readable passwords, even outs
__   44 RBOOPRIM RBDT TRUS ????????       May contain readable passwords, even outs
__   44 RBOOPRIM RBDT TRUS ????????       UADS may contain non-RACF defined TSO use
__   35 RBOOPRIM RBDT SETR PROTECTALL   N The security system is not even invoked f
__   23 RBOOPRIM RBDT CLAS APPCSERV       No protection against hackers masqueradin
__   23 RBOOPRIM RBDT CLAS VTAMAPPL       No protection against hackers masqueradin
__   22 RBOOPRIM RBDT CLAS DEVICES        Devices like ESCON directors, FEPs, local
__   20 RBOOPRIM RBDT CLAS DATASET        Profile changes in class are not audited,
__   20 RBOOPRIM RBDT CLAS TEMPDSN        Temporary datasets resident after failure
__   20 RBOOPRIM RBDT SETR OPERAUDIT    N OPERATIONS activity undetectable
__   20 RBOOPRIM RBDT SETR TAPEVOL      I Hacker can read/write any tape dataset by
__   19 RBOOPRIM RBDT CLAS OPERCMDS       Profile changes in class are not audited
__   16 RBOOPRIM      RACF CD.*.*         Verify why UACC>=UPDATE, Generic chars in
__   16 RBOOPRIM      RACF CD.**          Verify why UACC>=UPDATE, Generic chars in
```

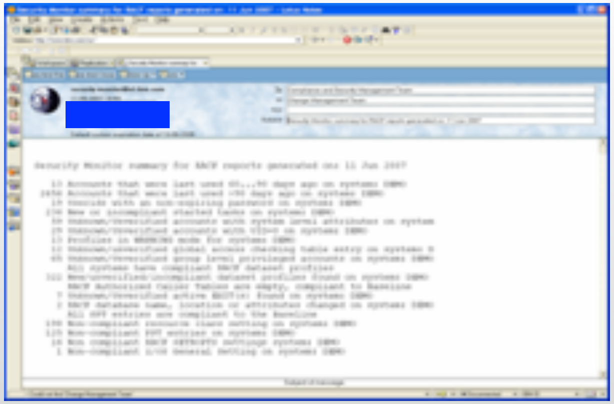
RACF database cleanup & improved manageability

```
Session A - [32 x 80]
zSecure Admin+Audit for RACF USER overview
```

Best Practices



Mainframe administration



[redacted]

```
Security Monitor summary for RACF reports generated on: 11 Jun 2007

   13 Accounts that were last used 60...90 days ago on systems IBM0
 1454 Accounts that were last used >90 days ago on systems IBM0
   19 Userids with an non-expiring password on systems IBM0
  134 New or incompliant started tasks on systems IBM0
   59 Unknown/Unverified accounts with system level attributes on system
   29 Unknown/Unverified accounts with UID=0 on systems IBM0
   13 Profiles in WARNING mode for systems IBM0
   12 Unknown/unverified global access checking table entry on systems I
   45 Unknown/Unverified group level privileged accounts on systems IBM0
      All systems have compliant RACF dataset profiles
  122 New/unverified/incompliant dataset profiles found on systems IBM0
      RACF Authorized Caller Tables are empty, compliant to Baseline
    7 Unknown/Unverified active EXIT(s) found on systems IBM0
    2 RACF database name, location or attributes changed on systems IBM0
      All PPT entries are compliant to the Baseline
  130 Non-compliant resource class setting on systems IBM0
  125 Non-compliant PPT entries on systems IBM0
   16 Non compliant RACF SETROPTS settings systems IBM0
    1 Non-compliant z/OS General Setting on systems IBM0
```

Tivoli Security Management for System z

Tivoli Capabilities

- More efficient and effective RACF administration, using significantly less resources
- RACF auditing that enables to automatically analyze and report on security events and detect security exposures
- Enforce compliance to company and regulatory policies by preventing erroneous commands
- Auditing and reporting infrastructure

Benefits:

- Secure critical mainframe hosted data and transactions
- Comply with regulations
- Improve service availability
- Implement z/OS security best practices

Pricing and packaging designed to be simple, comprehensive, and economical

Solutions would be delivered as a 'hard bundle'

Low break-even price points to stimulate solution suite purchases, trade-ups available

Available from IBM or IBM business partners

Services and hardware can be bundled by services partners for a single price

Identity and Access Assurance

Metric	Per User
Price	$125 per user value unit MOQ of 5,000 users
BOM	• Tivoli Identity Manager • Tivoli Unified Single Sign-On (FIM, TAMeb, ESSO) • Tivoli Compliance Insight Manager • Tivoli Access Manager for Operating Systems

Data and Application Security

Metric	Per Managed Resource
Price	$125K + additional RVUs to scale apps and storage
BOM	• Tivoli Security Policy Manager • Tivoli Key Lifecycle Manager • Tivoli Compliance Insight Manager • Tivoli Access Manager for Operating Systems • Tivoli Federated Identity Manager

Security Management for z/OS

Metric	Capacity-based
Price	$23K per MSU
BOM	• Tivoli zSecure Admin • Tivoli zSecure Audit • Tivoli zSecure Command Verifier • Tivoli Compliance Insight Manager for z/OS Auditing

Internal Use Only – Not for Use with Clients

More Information – Tivoli Security Sales Kit

- Identity & Access Assurance
  - http://w3-103.ibm.com/software/xl/portal/viewcontent?type=doc&srcID=CGSK&docID=S580595Q48163A23
- Data & Application Security
  - http://w3.ibm.com/software/xl/portal/viewcontent?type=doc&srcID=CGSK&docID=J972816R14730E22
- Security Management for z/OS
  - http://w3-103.ibm.com/software/xl/portal/viewcontent?type=doc&srcID=CGSK&docID=S880115Y30440U38
- Tivoli Security Virtual Sales Academy
  - http://w3-103.ibm.com/software/xl/portal/viewcontent?type=doc&srcID=T9&docID=X845088H35672Y50
- Tivoli Security Wiki
  - https://w3.tap.ibm.com/w3ki06/display/Main/TivoliSecurity
- Tivoli 3 Security Bundles (extended version)
  - http://cattail.cambridge.ibm.com/cattail/#view=bert.schaekers@be.ibm.com/files/80C3FCC0F1093DD8930E7B0F7F000001

Worldwide Security Sales

Sean Bergin/Austin/IBM

Worldwide Security Enablement

Pierre Georges NOEL/Hong Kong/IBM

Key Regional Security contacts

Americas: Kevin Williams/New York/IBM

Latin America: Max Rodriguez/Falls Church/IBM

CEEMEA: Jean-Michel Doudot/Switzerland/IBM

NE IOT: John Canny/Switzerland/IBM

SW IOT: Emmanuel Roeseler Rivera/Spain/IBM

Asia Pacific: Tim Birdsall/Australia/IBM

Japan: Keiko Nagatani/Japan/IBM

Pierre G. Noel
Executive, Worldwide Risk Management & Information Security
pierre.noel@hk.ibm.com