

Pulse
Comes to You



IBM.

Managing the World's Infrastructure

Tivoli Security

Risk and Compliance Management

Tim Birdsall, Business Unit Executive, AP Growth Market
Scott Henley, AP Tivoli Security Technical Sales

Goa, India, April 25th, 2009



© 2009 IBM Corporation

Security: today's key investment

- threats and challenges

The Tivoli Security Solution

- Welcome to the Smart Planet

Delivering on IBM's strategy

- Identity and Access Management
- Data and Application Security
- The Enterprise Hub

Tivoli Security Stands Out from the pack

Announcing the new offerings



<http://www.youtube.com/watch?v=jev-Y10MJcw>

Security Threats and Challenges

Credit Card Numbers Stolen From Movie Theater Computer Merrimack Police Say Numerous People Report Credit Card Problems

POSTED: 5:05 pm EST December 10, 2008

Extra 12/12/2008 10:00 AM ET

msn money

Businesses see rise in employee theft

Security - eWeek

eWEEK.COM [SUBSCRIBE TO eWEEK](#) [RSS Feeds](#) [Print](#) [Newsletters](#)

SEARCH

enterprise

erger from them to cope with tough financial times. One surprise: Often guilty parties.

HOME NEWS REVIEWS DATA STORAGE SECURITY DESKTOPS/NOTEBOOKS MOBILE/WIRELESS APP DEV BLOGS VIDEOS THE CHAMP

Security News | Security Reviews | Security Blogs | IT Infrastructure | Government IT | Linux & Open Source | Enterprise Networking | Applications

Home > Security > Citigroup's Account Management Nightmare: 50,000 Layoffs Means Closing Up To 1 Million Accounts

Security

Citigroup's Account Management Nightmare: 50,000 Layoffs Means Closing Up To 1 Million Accounts

By Brian Prince
2008-11-19

30 Days Most Popular

MOST READ

1 - Intel Arms Len
New Anti-theft Test

2 - Wireless Secur
Wireless Security

3 - It's Time to Sig
(2444)

Police seize gang tied to US\$62m credit fraud

Rasha Abu Baker
Last Updated: December 16, 2008 12:28PM UAE / December 16, 2008

TheNational

Berlin Bank Accused of Country's Largest Data Leak

13.12.2008

Consumers in Germany have been affected by what is being calling the country's largest data leak. A Berlin bank has reportedly lost data on thousands of credit card customers -- including their PIN numbers.

HP, Symantec warn employees after laptop thefts

It's an embarrassment to the companies, says analyst

Robert McMillan

December 11, 2008 ([IDG News Service](#)) Technology vendors [Hewlett-Packard Co.](#) and [Symantec Corp.](#) are warning employees that their names and Social Security numbers may have recently fallen into criminal hands after two separate laptop thefts.

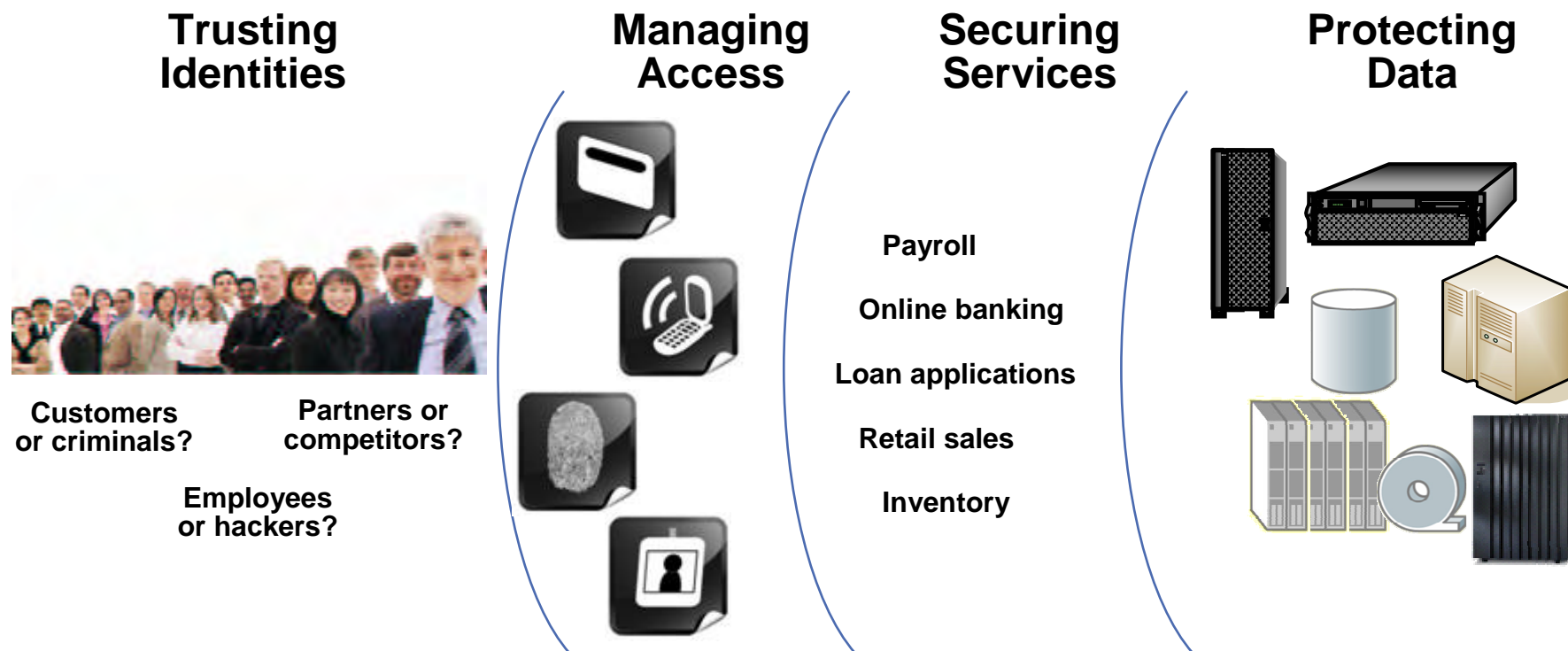
Global market forces are impacting us all

- Reality of living in a globally integrated world
 - Widespread impact of economic downturn and uncertainty
 - Energy shortfalls and erratic commodity prices
 - New customer demands and business models
 - Information explosion and risk/opportunity growth
- Businesses are under increasing pressure to effectively:
 - Manage operational cost and complexity
 - Deliver continuous and high-quality service
 - Address security risks intensified by innovation, emerging technologies, data/information explosion, etc.

According to a survey by SearchCIO, non-essential IT projects are being put on the backburner but security has a "1% or less chance of being affected by the economy."



Today's Security Challenges



Security has to be applied within a Business context and fused into the fabric of business and not as a widget to solve the next security threat

Security Threats and Challenges

- **Web applications have become the Achilles heel of corporate IT security**
 - 54.9% of all vulnerabilities are Web application vulnerabilities, 75% of those have no patches available
 - Number of malicious Web sites in the 4th quarter of 2008 alone surpassed the total number seen in all of 2007
 - X-Force 2008 Trend and Risk Report
- **Threats continue to rise: mergers, acquisitions, layoffs. 59 percent of workers who left their positions took confidential information with them.**
 - 24% of these former employees responding to the survey said they still had access to their former employer's computer systems after they left,
 - 50% between one day to a week,
 - 20% more than a week.
 - study by Ponemon Institute
- **Weak passwords are easily compromised by insiders.**
 - Internal attacks cost 6% of gross annual revenue -- costing USD 400 billion in the U.S. alone.
- **30% of all help desk calls are password related.**
 - Password resets can cost as much as \$20-\$25 per call.



Welcome to the smart planet...



Globalization and Globally Available Resources

Billions of mobile devices accessing the Web



Access to streams of information in the Real Time



The planet is getting instrumented, interconnected and intelligent.



New Forms of Collaboration

**New possibilities.
New complexities.
New risks.**

Managing risks introduced by new opportunities



Emerging technology

- Virtualization and cloud computing increase infrastructure complexity.
- Web 2.0 and SOA style composite applications introduce new challenges with the applications being a vulnerable point for breaches and attack.



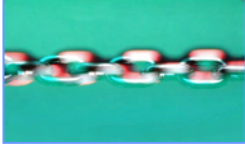
Data and information explosion

- Data volumes are doubling every 18 months.*
- Storage, security, and discovery around information context is becoming increasingly important.



Wireless World

- Mobile platforms are developing as new means of identification.
- Security technology is many years behind the security used to protect PCs.



Supply chain

- The chain is only as strong as the weakest link... partners need to shoulder their fair share of the load for compliance and the responsibility for failure.



Clients expect privacy

- An assumption or expectation now exists to integrate security into the infrastructure, processes and applications to maintain privacy.



Compliance fatigue

- Organizations are trying to maintain a balance between investing in both the security and compliance postures.

IBM Tivoli Security delivering on the IBM Security Strategy



Identity, Access & Audit Management

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

Data & Application Security

- Protect Business Information & Reputation by safeguarding data in use or at rest

Enterprise security hub

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

Why Identity, Access, and Audit Management?

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 reset requests
- More efficiently manage restructuring
- ERP deployments / upgrades

Manage Risk

- Privileged & Shared IDs
- Failed audits,
- Insider breach
- SOA, SharePoint, cloud computing, Portal, DataPower
- Recertification, entitlements management
- National ID / Trusted ID – provisioning of strong / trusted credentials.
- Unauthorized IT change detection



Identity, Access, and Audit Management

Tivoli Capabilities

- User provisioning & role management
- Unified single-sign-on
- Application entitlement management
- Privileged user activity audit & reporting
- Log Management
- Directory and integration services
- 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)

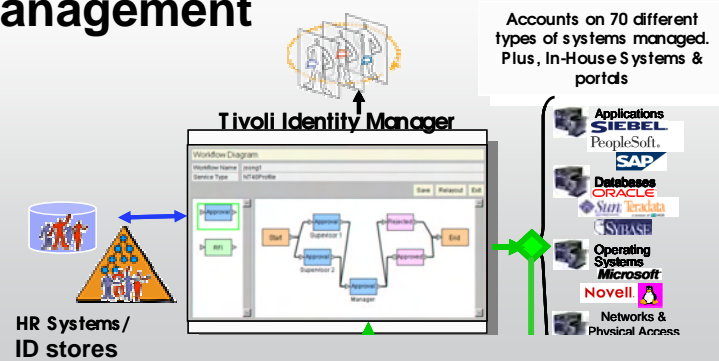


Getting started with Identity, Access and Audit Management

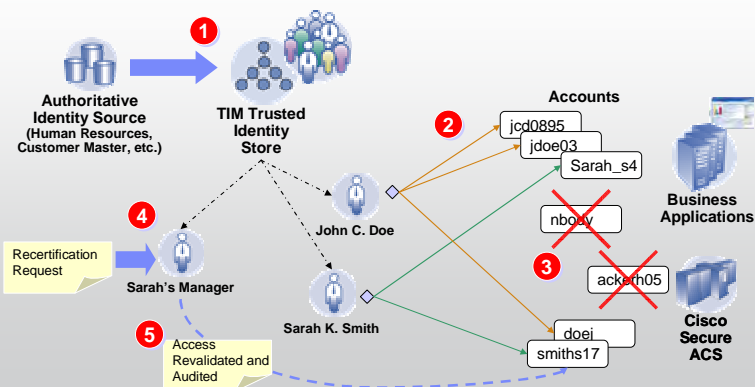
Single Sign On & Password Management



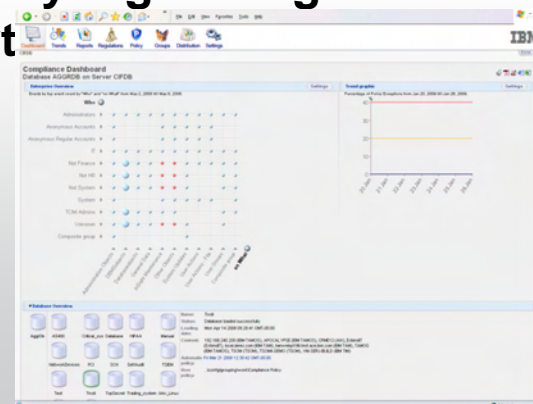
User Provisioning / Role Management



Access Attestation



Security log management & report



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

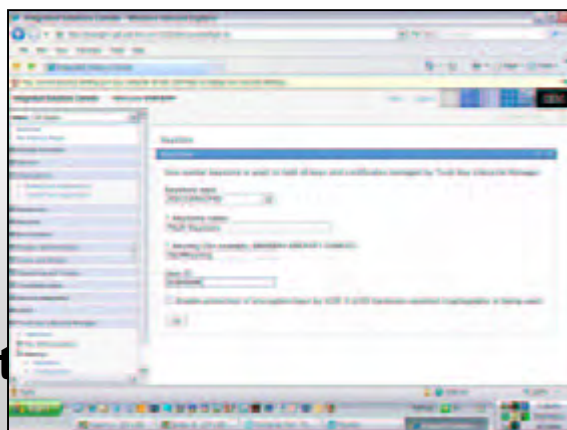
Manage Risk

- Data disclosure / privacy regulations
- Failed audits, insider breach in industry
- Lost backup tapes / laptops
- SOA, SharePoint, DataPower, Portal

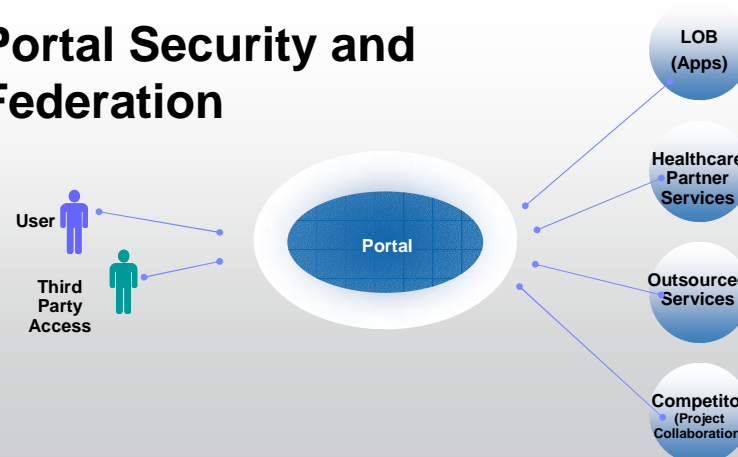


Getting started with Data and Application Security

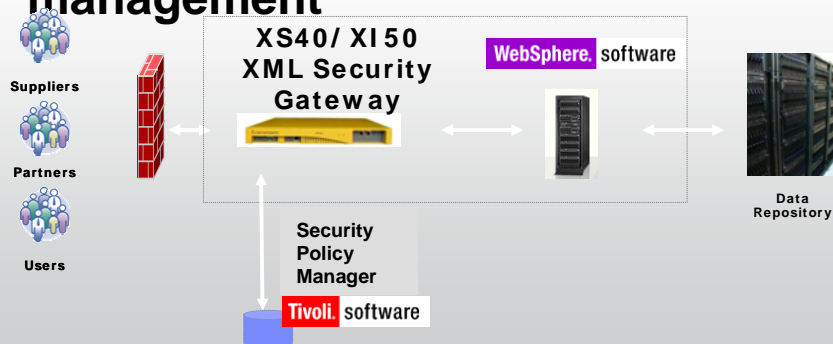
Encrypted Disks & Archive Tapes with Key Management



Portal Security and Federation



SharePoint / DataPower management



Security log management & reporting



Solution: Data & Application Protection

- 1 **Security Policy Management and Security Services**
- 2 **Application & Data Entitlements Management**
- 3 **Encryption Key Management for tape and disk**



Data and Application Security

- **Tivoli 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**

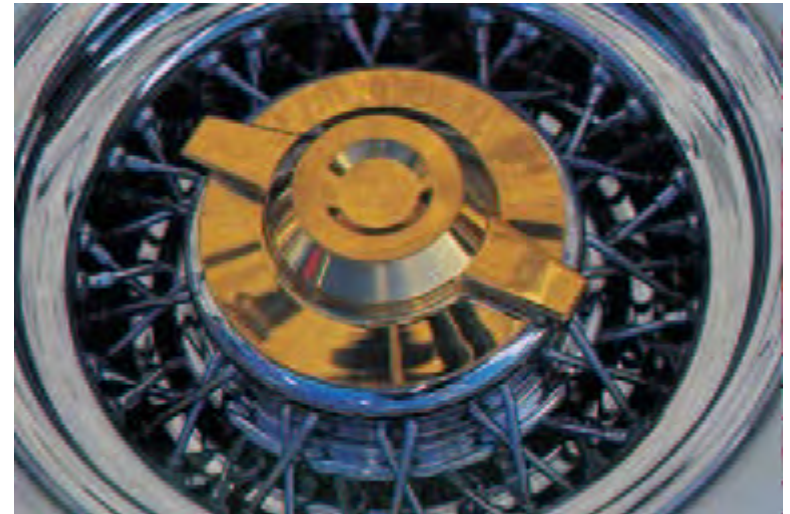


Why an Enterprise Security Hub?

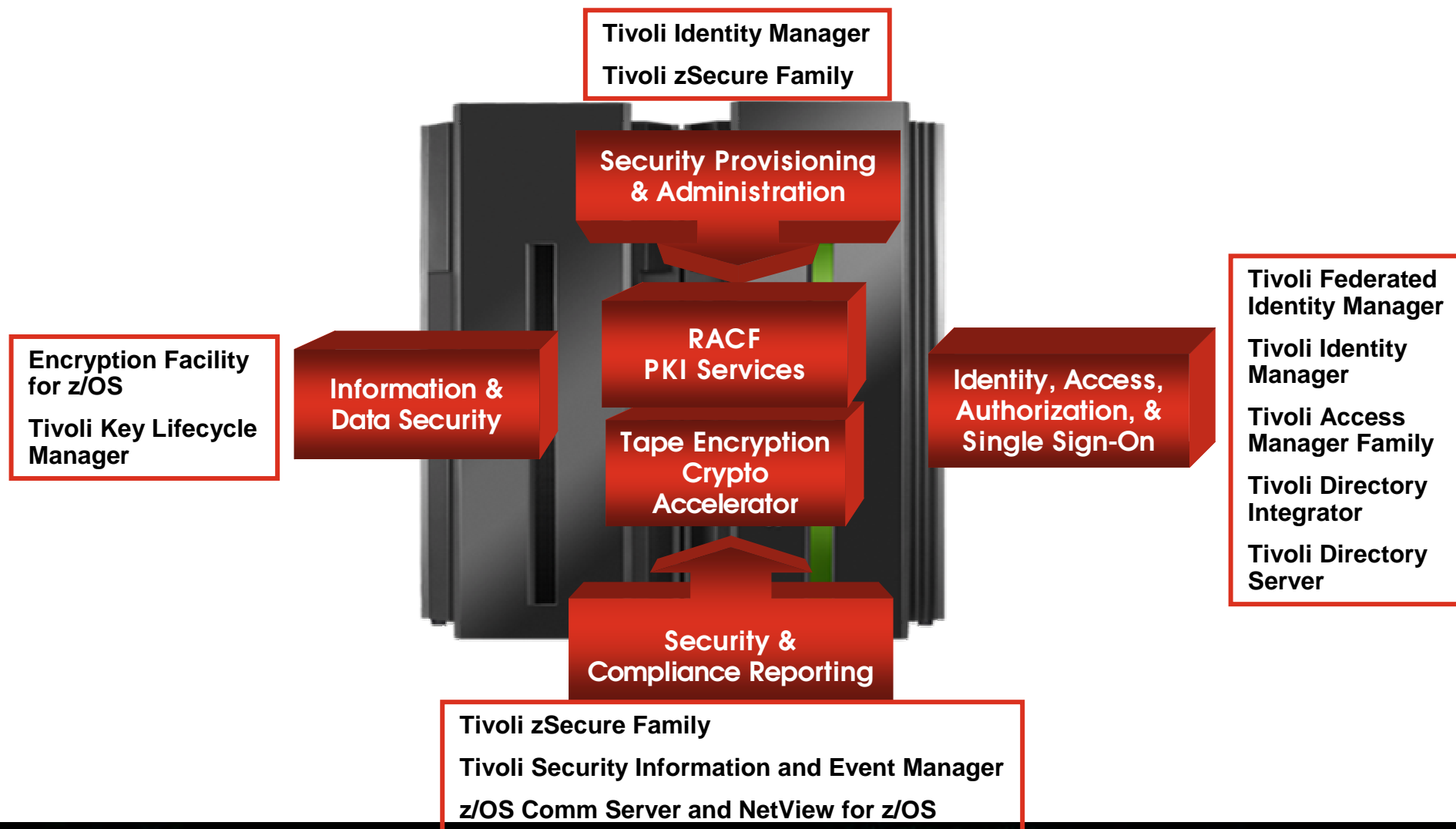
- **Improve service**
 - Leverage the most secure platform in the enterprise

- **Reduce cost**
 - Datacenter consolidation
 - Workload consolidation on Linux on System z
 - Cloud
 - Reduce “cost of compliance”

- **Manage risk**
 - Data disclosure / privacy regulations
 - Failed audits, breach in industry
 - Lost backup tapes



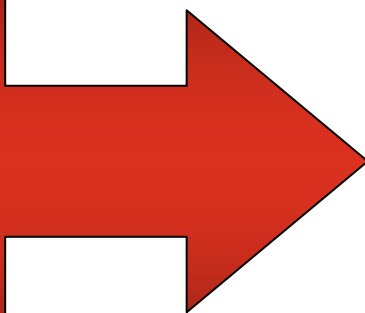
Tivoli Security: the mainframe as the Enterprise Security Hub



Establishing an Enterprise Security Hub

Tivoli Capabilities

- RACF administration and auditing
- Centralized user provisioning and access mgmt
- Centralized key management
- Auditing and reporting infrastructure



Benefits:

- Secure critical mainframe hosted data and transactions
- Comply with regulations
- Improve service availability
- Enable workload consolidation through improved, centralized security management

| | IBM. | ORACLE | ca | Sm | Novell. | Representative Customer | |
|--|------|--------|----|----|---------|-------------------------|--|
| Mainframe Security | ✔ | ✘ | ✔ | ✘ | ✘ | | |
| Deep System z audit + SIEM | ✔ | ✘ | ✔ | ✘ | ✘ | | |
| <i>Extended Capabilities (not in this bundle):</i> | | | | | | | |
| WAM/User Provisioning on z | ✔ | ✘ | ✘ | ✘ | ✘ | | |
| Encryption Key Mgt | ✔ | ✘ | ✘ | ✘ | ✘ | | |

IBM Service Management enables customers to manage the world's infrastructure *securely*

▪ Visibility

- The ability to see everything that's going on across the infrastructure
 - Sensitive user compliance and data access dashboard and alerting
 - Compliance initiative reporting
 - Board level transparency required



▪ Control

- The ability to keep the infrastructure in its desired state by enforcing policies
 - Consistent Processes for User Access to Business Applications



▪ Automation

- The ability to manage huge and growing infrastructures while controlling cost and quality
 - Automated process for granting and removing users right to access applications and resources
 - Self service password resets
 - Policy driven identity governance



IBM Tivoli : why we stand out from the pack...

IBM is only vendor that truly enables the mainframe to serve as the Enterprise Security Hub

- Broad strategy that brings unified security process across the mainframe and distributed environments
- Improved administration, security processes, Audit and Compliance and end to end identity mgmt (zSecure, RACF, TFIM, TIM)

Closed loop SIEM & IAM integration offers offers end to end identity management across the lifecycle

- This includes PROOFING a user before issuing them credentials (IBM Identity Resolution, IBM Relationship Resolution)
- This also includes continual monitoring of users, their rights and what users have done with those rights (Tivoli SIEM and Tivoli IAM integration)

IBM offers a broad and flexible portfolio of application and business process security capabilities across a range of applications and platforms.

- Closed-loop user management and compliance (even privileged users!)
- Integration with applications controls vendors (Approva, SAP-GRC)
- SOA Security
- Closed loop App Security with TAMEb and Rational AppScan
- Strong Authentication integration





IBM Tivoli Security: why we stand out from the pack...

- The *only security vendor* in the market with end-to-end coverage of the security foundation
- 15,000 researchers, developers and SMEs on security initiatives
- 3,000+ security & risk management patents
- 200+ security customer references and 50+ published case studies
- 40+ years of proven success securing the zSeries environment
- \$1.5 Billion security spend in 2008



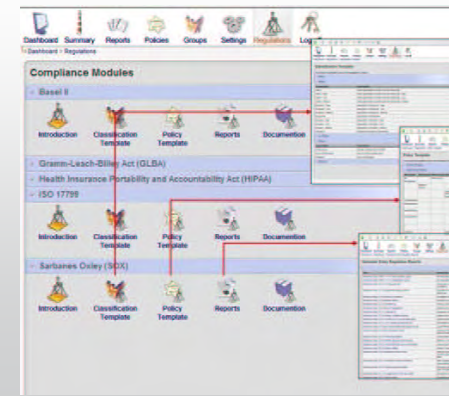
IBM Tivoli Security: why we stand out from the pack...

A leader in security standards work

- Open standards: OpenID, OASIS, XACML
- OpenSource: Eclipse Project Higgins
- IBM Delivery of Standards Support:
 - Project Higgins: TSPM, TFIM 
 - OpenID exploitation: TFIM 

compliance initiative support

- ISO 27001
- PCI
- HIPAA
- SOX
- Basel II
- And more...



part of a comprehensive Security strategy



and an integral part of Service Management



IBM Tivoli : why we stand out from the pack...

- **The Facts**

- Projected 50% reduction in the number of administrators assigned to support identity management processes within 18 months
- Anticipated 25% savings in help-desk administrative costs
- Reduce turn-on time for new users from 10 days to less than 24 hours
- Reduce time and cost associated with regulatory reporting by 50%
- 75% reduction in security incidents that affect business and customer outage, 98% reduction in time to mitigation of incidents
- Increased visibility into the root causes from 25% to approx 90%
- Reduced time to mitigate worm outbreaks - Zotob was remediated **across the company in less than 1 day**



IBM Tivoli Security delivering on the IBM Security Strategy

Tivoli Security Solutions New!



Tivoli Identity and Access Assurance 1.0

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

Tivoli Data & Application Security 1.0

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

Tivoli Security Management for z/OS 1.10

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



New security solution suites provide greater customer value and competitive differentiation

| Identity and Access Assurance | | Data and Application Security | | Security Management for z/OS | |
|--|--|--|---|--|---|
| Value Prop | Provide efficient and compliant access for right people to right resources | Value Prop | Protect integrity and confidentiality of business data and transactions | Value Prop | Secure critical business services with your most trusted and resilient platform |
| Problems Solved | | Problems Solved | | Problems Solved | |
| <ul style="list-style-type: none"> • Reduce help desk OPEX • Comply with regulations • Improve user productivity • Reduce risk from privileged insiders • Respond quickly to business initiatives (e.g. new applications, M&A, restructuring) | | <ul style="list-style-type: none"> • Data disclosure and privacy compliance • Application security and agility • Secure 3rd party collaboration • Protect IP / data-in-use • Secure storage / data-at-rest | | <ul style="list-style-type: none"> • Secure critical mainframe hosted data and transactions • Comply with regulations • Improve service availability • Enable workload consolidation through improved, centralized security management | |

| | IBM | ORACLE | MS | Novell |
|----------------------------|-----|--------|----|--------|
| WAM / User Provisioning | ✔ | ✘ | ✔ | ✔ |
| ESSO | ✔ | ✘ | ✘ | ✔ |
| OS Security Policy/Control | ✔ | ✘ | ✘ | ✘ |
| SIEM | ✔ | ✘ | ✔ | ✔ |



| | IBM | ORACLE | MS | Novell |
|----------------------------|-----|--------|----|--------|
| Federated Identity Mgt. | ✔ | ✔ | ✔ | ✔ |
| Encryption Key Mgt. | ✔ | ✘ | ✘ | ✘ |
| OS Security Policy/Control | ✔ | ✘ | ✘ | ✘ |
| Entitlements Management | ✔ | ✘ | ✘ | ✘ |
| SIEM | ✔ | ✘ | ✔ | ✔ |



| | IBM | ORACLE | MS | Novell |
|------------------------------|-----|--------|----|--------|
| Mainframe Security | ✔ | ✘ | ✔ | ✘ |
| Deep System 2 audit - SIEM | ✔ | ✘ | ✔ | ✘ |
| WAM / User Provisioning on z | ✔ | ✘ | ✘ | ✘ |
| Encryption Key Mgt. | ✔ | ✘ | ✘ | ✘ |



Pulse

Comes to You



Managing the World's Infrastructure

Tim Birdsall, Business Unit Executive, AP Growth Market

- tim.birdsall@au1.ibm.com

Scott Henley, AP Tivoli Security Technical Sales

- scott.henley@au1.ibm.com

- Ramgopal Gandhekar India Security Leader

- rgandhek@in.ibm.com

- Mahesh Narkar Program Manager, Tivoli Security India Software Lab, Pune

- manarkar@in.ibm.com



© 2009 IBM Corporation