Applying Intelligence to Identity

IBM Security Systems

Chris Hockings

Rodney Dale, Philip Nye

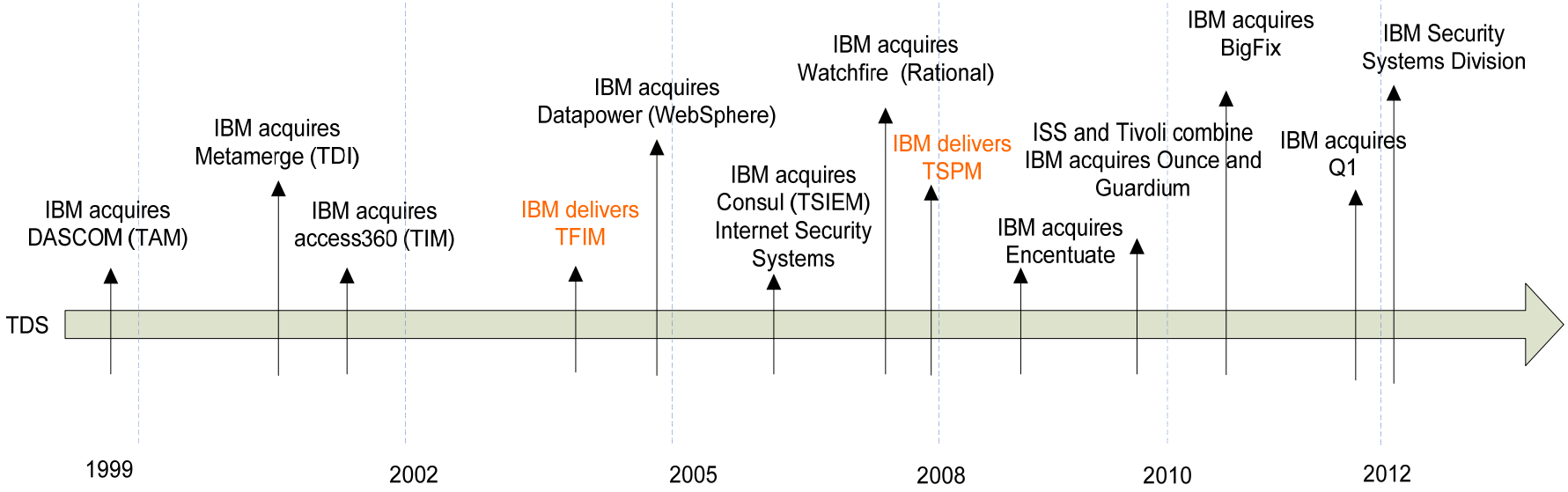
Pulse2012

Meet the Experts. Optimise your infrastructure.

May 31 – June1

Sheraton on the Park Hotel, Sydney

The new division is driving innovation and integration



A history built upon innovation through organic and acquired growth

IBM Security Systems Development Lab Gold Coast

- Background
  - Founded in 1996 with strong links to Queensland universities
  - September 1999 acquisition of DASCOM
- Profile
  - 90 technical staff
  - Design, development, test, project management, documentation, support
  - World class security expertise
  - Close to Asia Pacific Customers
- Product Development
  - IBM Security Heritage software
  - ISS software/hardware
  - Q1 (integration)
- IBM wide security components
- Integration Factory
- Customer Focussed
  - Lab Services
  - Support
  - SWAT

Agenda

- What is intelligence?
- Security intelligence within Identity and Access
- Identity and Access Roadmap
- Innovation examples
  - Privileged Identity Management
  - Role and Policy Modeler
  - Security Intelligence within Access Management
- The IBM Academy Advocacy program

Intelligence and Security

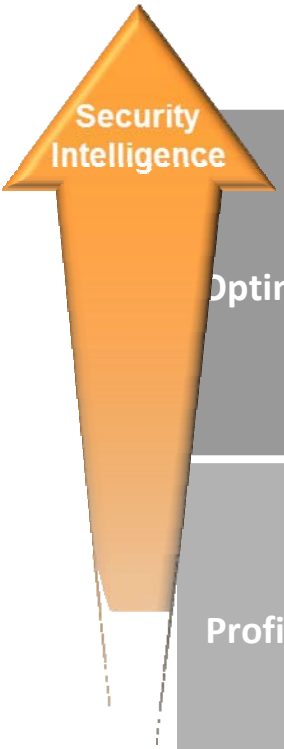
What is intelligence?

Sternberg & Salter	Goal-directed adaptive behaviour.
Lloyd Humphreys	"...the resultant of the process of acquiring, storing in memory, retrieving, combining, comparing, and using in new contexts information and conceptual skills."
Cyril Burt	Innate general cognitive ability
Hockings*	To lower the risk posed to a system by using historical and contextual information to influence decisions

Courtesy: wikipedia

*: Hockings definition has not been subjected to any scrutiny, and may be illegitimate

Focused on helping organizations' security to mature

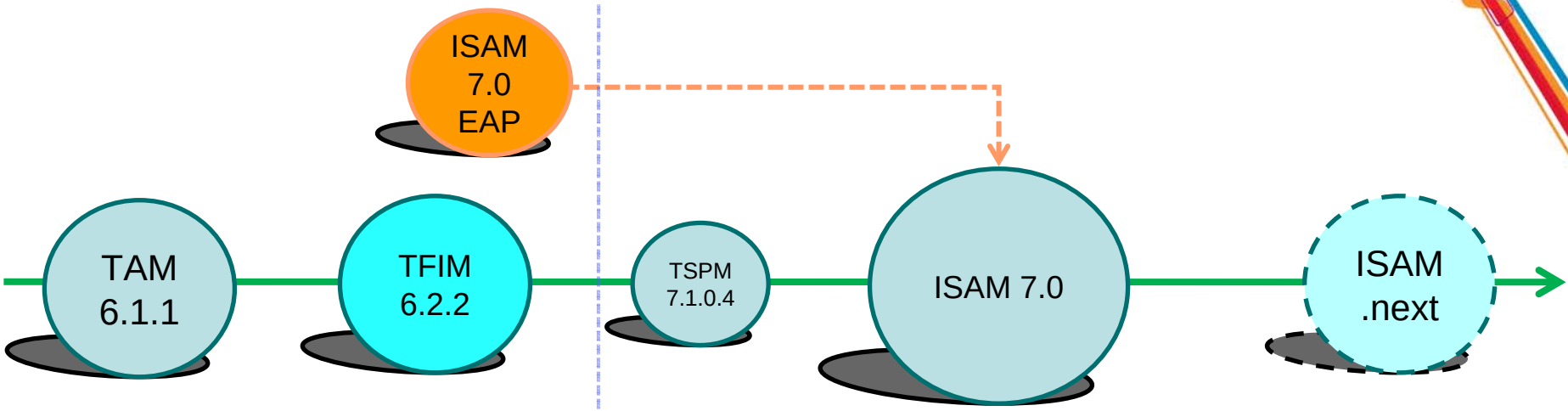


	People	Data	Applications	Infrastructure	Security Intelligence
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Securing systems	Advanced threat detection Network anomaly detection Predictive risk management
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management	Real-time event correlation Network forensics
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus	Log management Compliance reporting

Disclaimer:

The information on the new product is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information on the new product is for informational purposes only and may not be incorporated into any contract. The information on the new product is not a commitment, promise, or legal obligation to deliver any material, code or functionality. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Access Family Roadmap



Tivoli Access Manager
- SOA Integration

Tivoli Federated Identity Manager
- Enhanced standards support
- B2C support (OAuth)

IBM Security Access Manager
- TAM/WebSEAL virtual appliance (VMWare)
- Enhanced Microsoft integration
- Enhanced active client (e.g. AJAX) support
- 64-bit operating system support

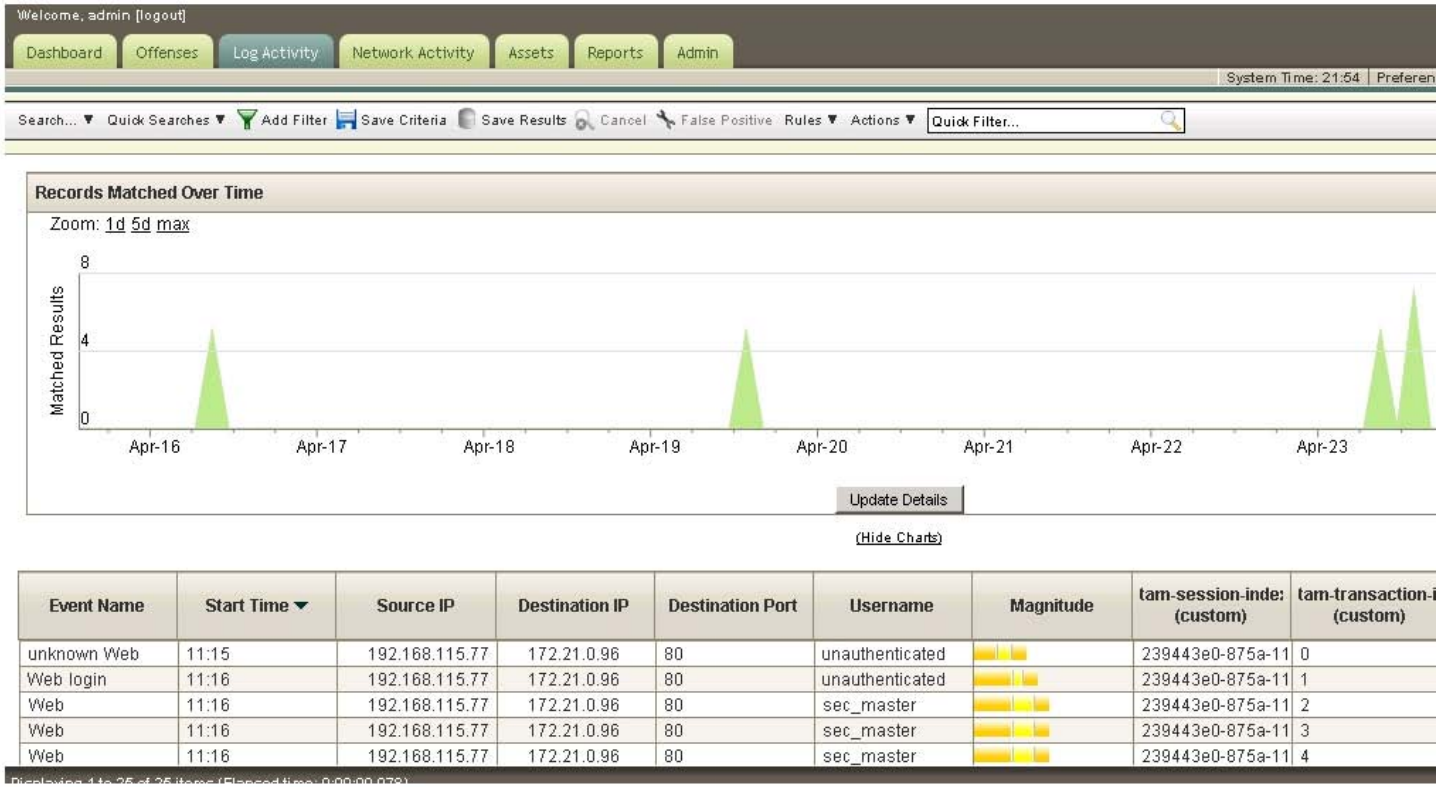
IBM Security Web Access Gateway
- TAM/WebSEAL hardware appliance
- WAF functionality (X-Force integration)

Risk Based Access (TFIM BG)
- Customizable Risk engine (externalized SPI)
- Risk evaluation based on location, device, and access pattern
- Integration with ISAM for Web (WebSEAL) including out of the box and 3rd party authentication factors

Today

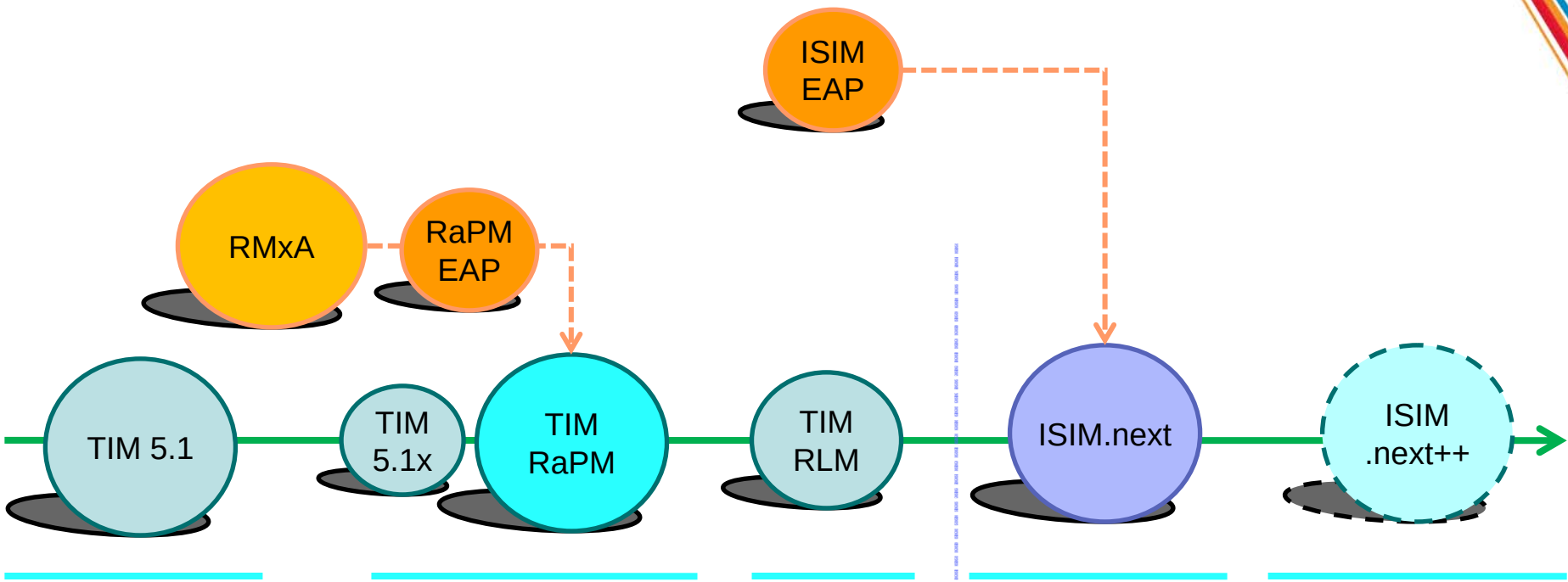
Using WebSEAL/QRadar to detect abnormal session behaviour

- Requirement to be able to gain more visibility of an entire web session
  - from unauthenticated to authenticated repeatedly
  - Anomoly detection can then be performed in cases of web based attack sequences



Event Name	Start Time	Source IP	Destination IP	Destination Port	Username	Magnitude	tam-session-inde: (custom)	tam-transaction-i (custom)
unknown Web	11:15	192.168.115.77	172.21.0.96	80	unauthenticated		239443e0-875a-11	0
Web login	11:16	192.168.115.77	172.21.0.96	80	unauthenticated		239443e0-875a-11	1
Web	11:16	192.168.115.77	172.21.0.96	80	sec_master		239443e0-875a-11	2
Web	11:16	192.168.115.77	172.21.0.96	80	sec_master		239443e0-875a-11	3
Web	11:16	192.168.115.77	172.21.0.96	80	sec_master		239443e0-875a-11	4

Identity Governance Roadmap



Operational Role and Access Compliance
SOD
Role Hierarchy
Group support
Access Certification
Reconciliation

Role and Policy Modeling
Role modeling and mining
File import and TDI adaptor
Business centric Web UI
TCR Reporting Analytics

Role Lifecycle
BPM
Approval templates

Integration Services
Check-in/out of shared IDs
Web Services

Future themes
Ongoing role mgmt
Analytics enhancements
UI/TTV improvements
Reporting improvements

Today

Traditional methods to address privileged access

Each administrator to have a userid on every system they administer

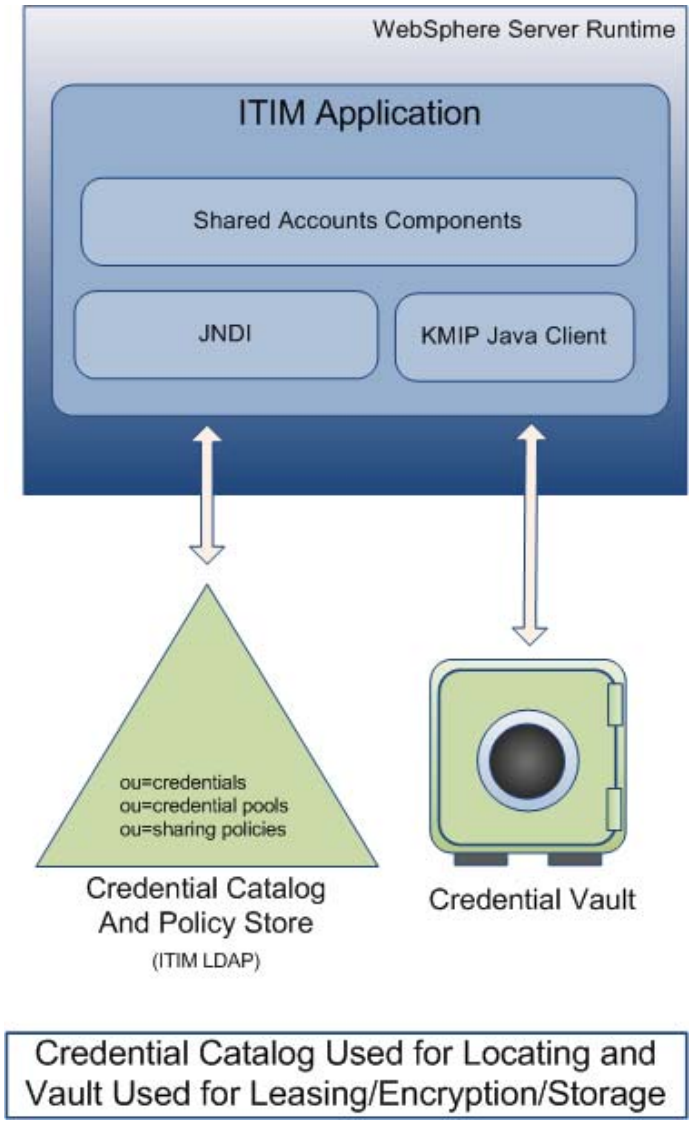
- Exponential increase in privileged userids
- Increased risk of mismanagement of privileged userids
- Increased userid administration costs

Administrators share privileged userids

- Risk of losing Individual Accountability
- Issues with password management and security
- Out of step with regulatory thinking

The strategic **reusable ID** solution provides a solution combining the best features of both approaches, without the disadvantages

Privileged Identity Management Solution Overview

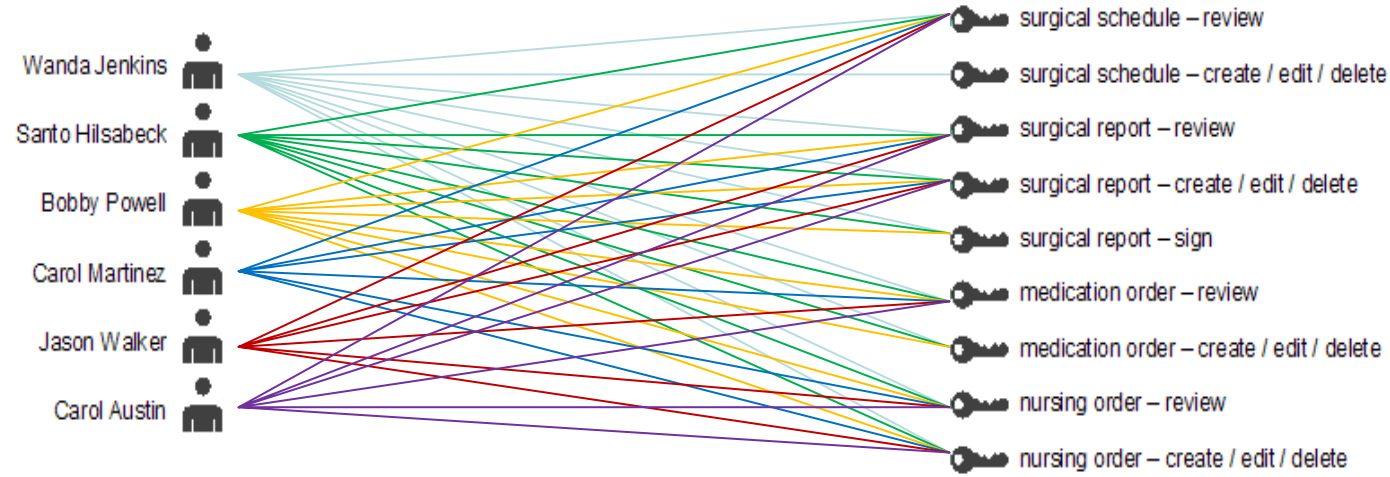


Credential Catalog Used for Locating and Vault Used for Leasing/Encryption/Storage

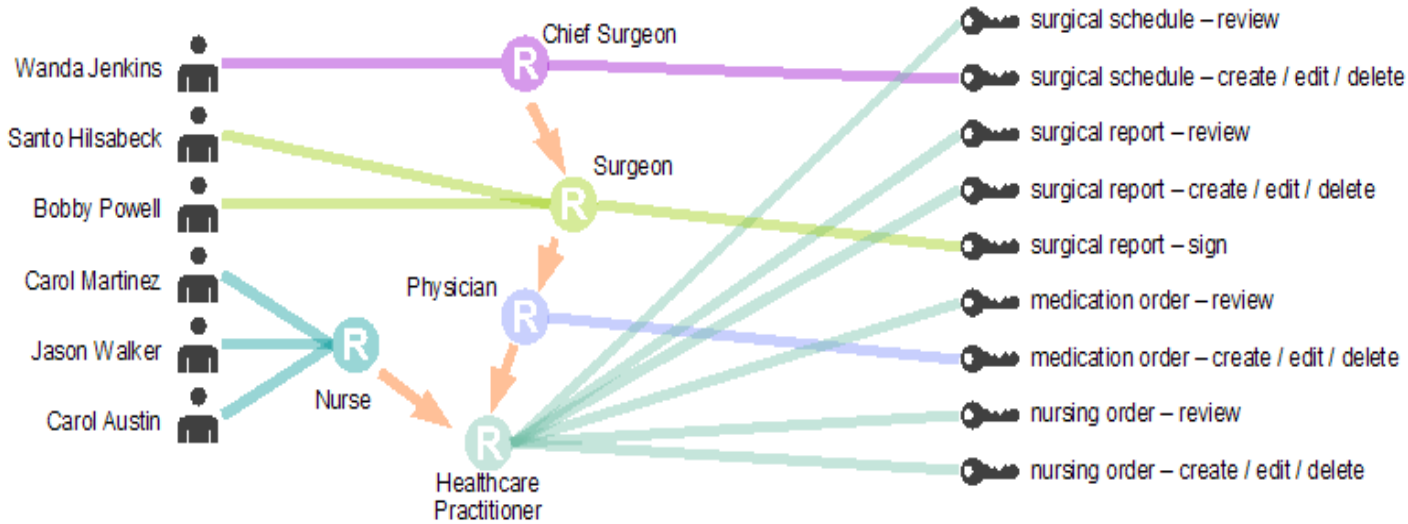
- Bundle Identity Mgr and ESSO to offer the PIM solution
- Access is shared via sensitive accounts.
- Credential Vault Administration
- Credential Pools
- Shared Privilege Policy
- Check In/Out of Shared Credentials
- Fine-grained audit reporting

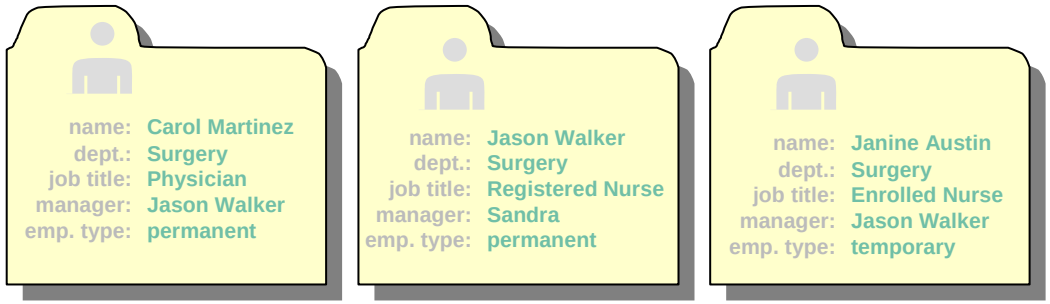
> Sharing access to sensitive accounts is inevitable… [However,] adequate control can mean the difference between disasters and effective operations." Forrester Research

Intelligence building Identities



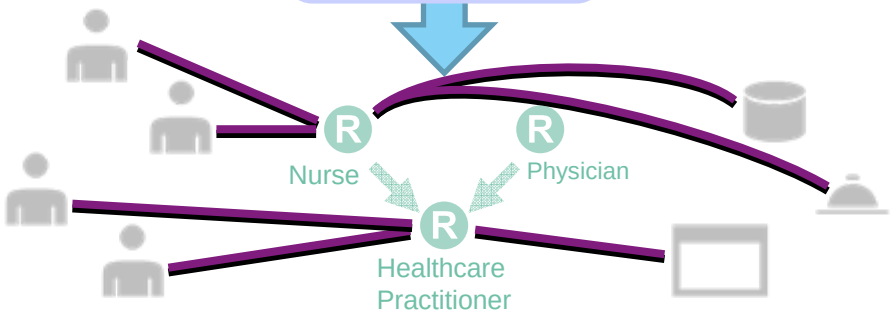
- **Simplify roles and access assignments**
- **Ability to handle growth and scale**
- **Facilitate accountability and compliance**

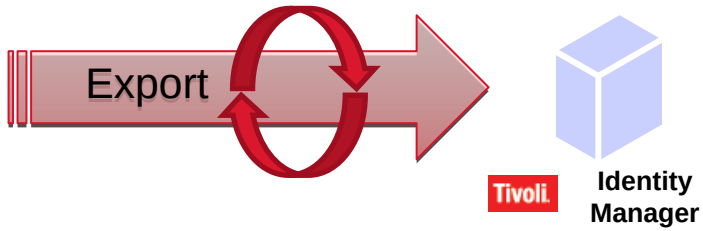




Record Feed - Identities

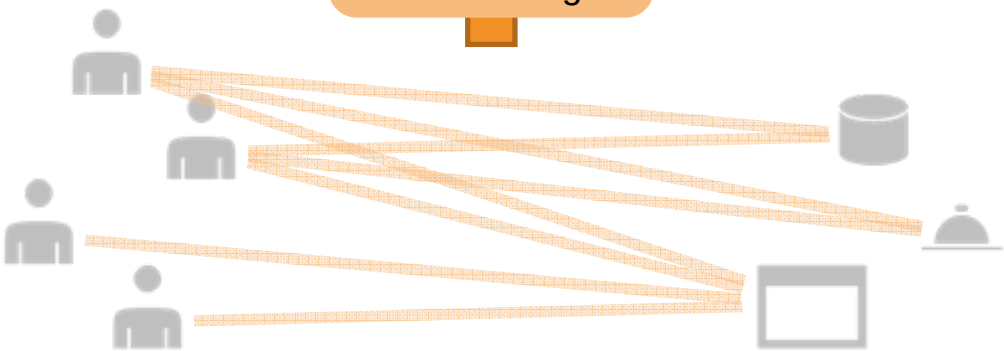
top-down
role modeling





bottom-up
role mining

Record Feed - Permissions



Engaging with IBM technologists

IBM Advocacy Program

- An initiative of the IBM Academy
  - A society of IBM's technical leaders organized to
    - advance the understanding of key technical areas
    - improve communications in and development of IBM's global technical community
    - engage clients in technical pursuits of mutual value
- Established in 1989, and loosely modeled on the National Academy of Science
  - transformed in 2009 for today's IBM
- Supports various forms of the advocacy:
  - Technical Advocacy Program (TAP)
  - Systems and Technology Group (STG) Advocacy program
  - Software Group (SWG) Advocacy
- Please discuss with the IBM Security Systems team if you'd like support from our development leaders

IBM Academy Of Technology

ibm.com/security

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.