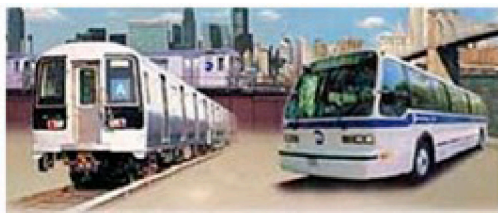


Corporate Transformation Through Identity Management

New York City Transit I-Vault Project

Ben Goodman
Director,
Identity & Security Management
East Area

June 4, 2007



MTA New York City Transit

Novell[®]

About New York City Transit

Established June 15, 1953, New York City Transit is the largest agency in the MTA regional transportation network.

Rolling stock: The largest subway car fleet in the world.

Equipment: More buses than any other public agency in North America.

Features: All NYC Transit subway cars and buses are air-conditioned and either new, remanufactured, or overhauled.

Ridership: Ridership on NYC Transit is approximately seven million daily - more than 2 billion annually.

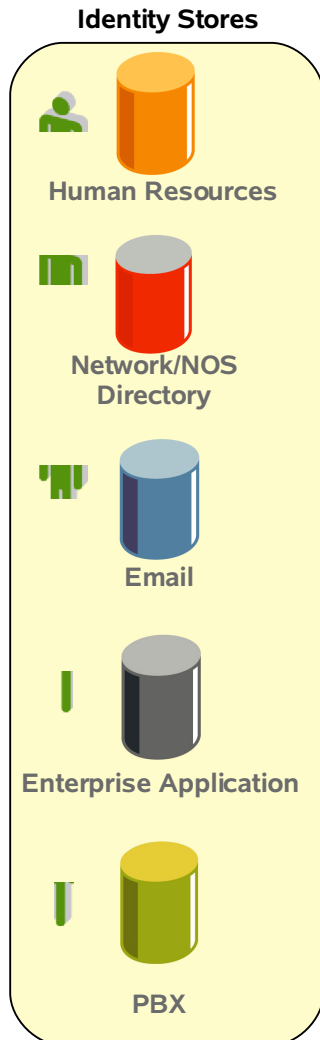
Work Force: NYC Transit employs nearly 47,000 people in more than 20 major departments and divisions.

Identity Management Project High-Level Goals

- Create a centralized repository of identity information for NYCT— I-Vault
 - Increase the quality of identity information by synchronizing identities across multiple identity stores
- Reduce the cost and complexity of managing multiple separate user stores
 - Leverage common services, e.g. authentication
 - Developing more efficient ways to provision and manage users
- Improve user satisfaction
 - Implement reduced sign on capabilities
 - Implement employee self-service
- Improve audit capabilities
 - Logging of events, tracking, and reporting
- Improve overall data security
 - Better access controls, improved password policies,



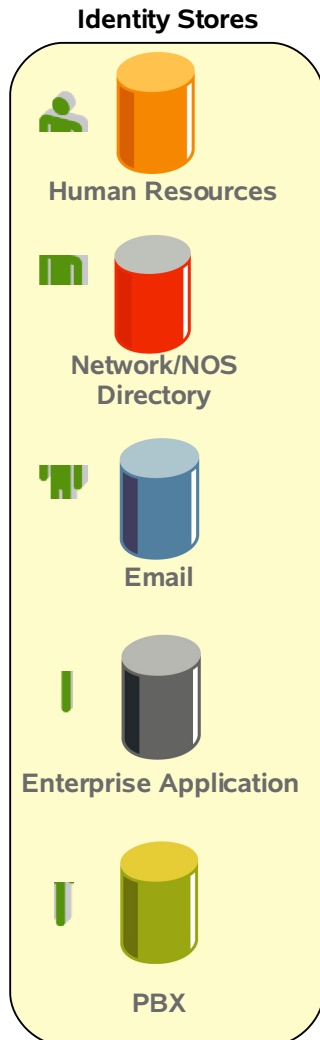
NYC Transit Has many Identity Stores



Many of your Enterprises application own a piece of the user's Identity.

- This Identity data can be expensive to Maintain.
- The Data may not be shared by everyone who needs it.
- This Data may not be accurate, consistent or kept up to date.

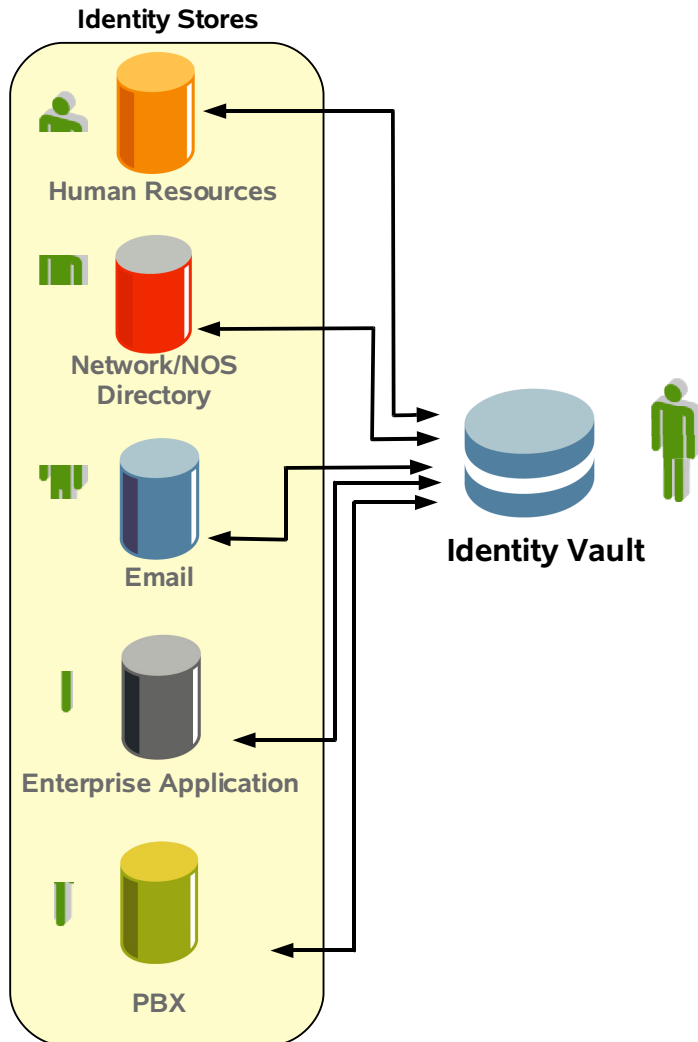
A Central Identity Vault



Identity Isolation problems can be solved by creating an Identity vault.

- A location for centralized identity management
- Many applications share the same identity data and authentication and authorization functionality
- Lays foundation for access control
- Provides basis for role-based personalization based on rights

Identity Synchronization Services

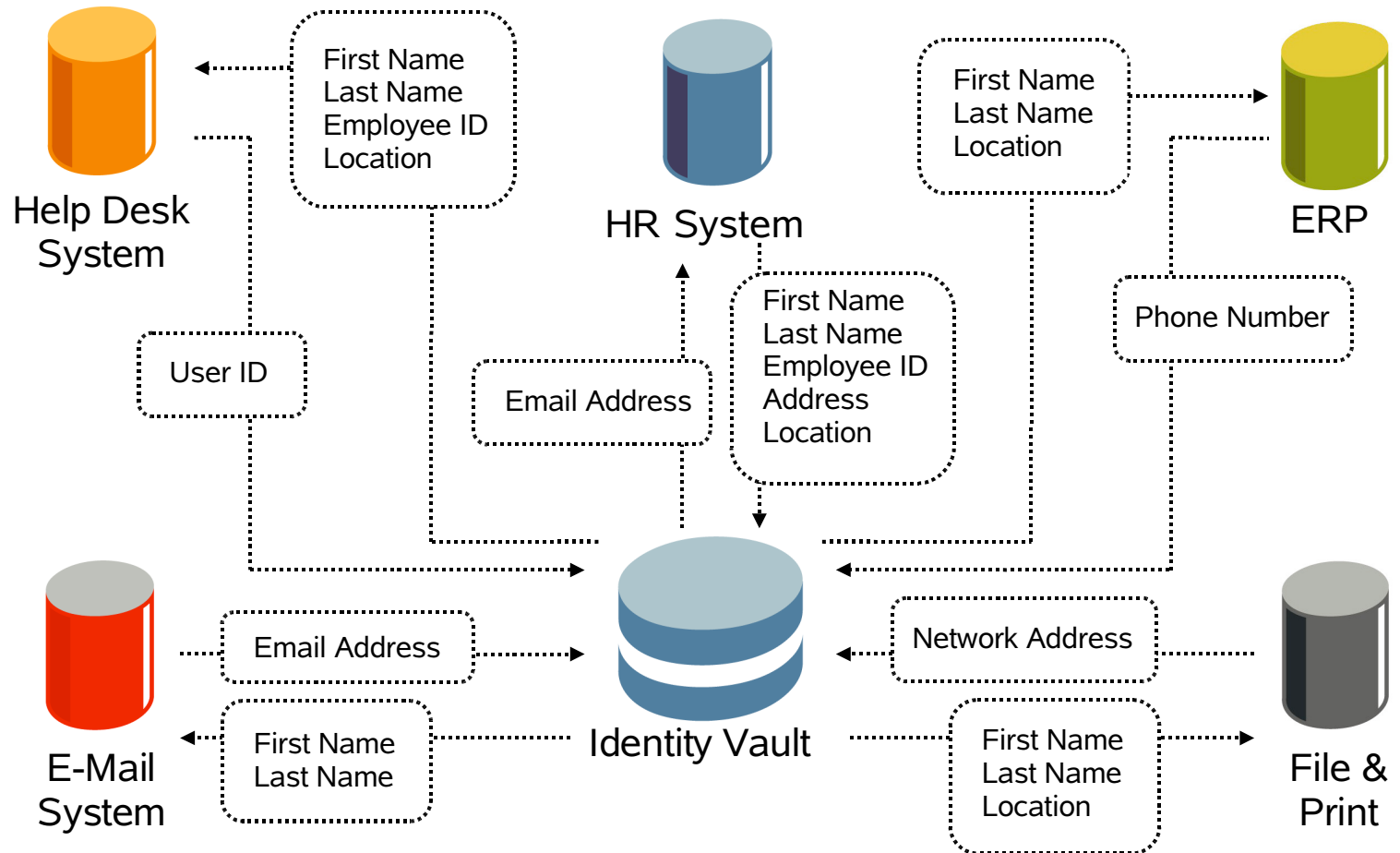


In order to aggregate this identity data into the Identity Vault we utilize Identity Synchronization technology.

- This allows you to utilize data owned by many systems to create a single rich identity.
- It allows for distributed ownership of portions of an identity, while allowing a single, centralized identity that can be leveraged by a myriad of systems.

Distributed Ownership of Data

a Centralized view



Key messaging- Why I-Vault?

3 Core Fundamental benefits of I-Vault

New applications can take advantage of I-Vault

- For authentication – Single User ID/Password
- Applications can now take advantage of a single security framework

Many applications can leverage I-Vault data

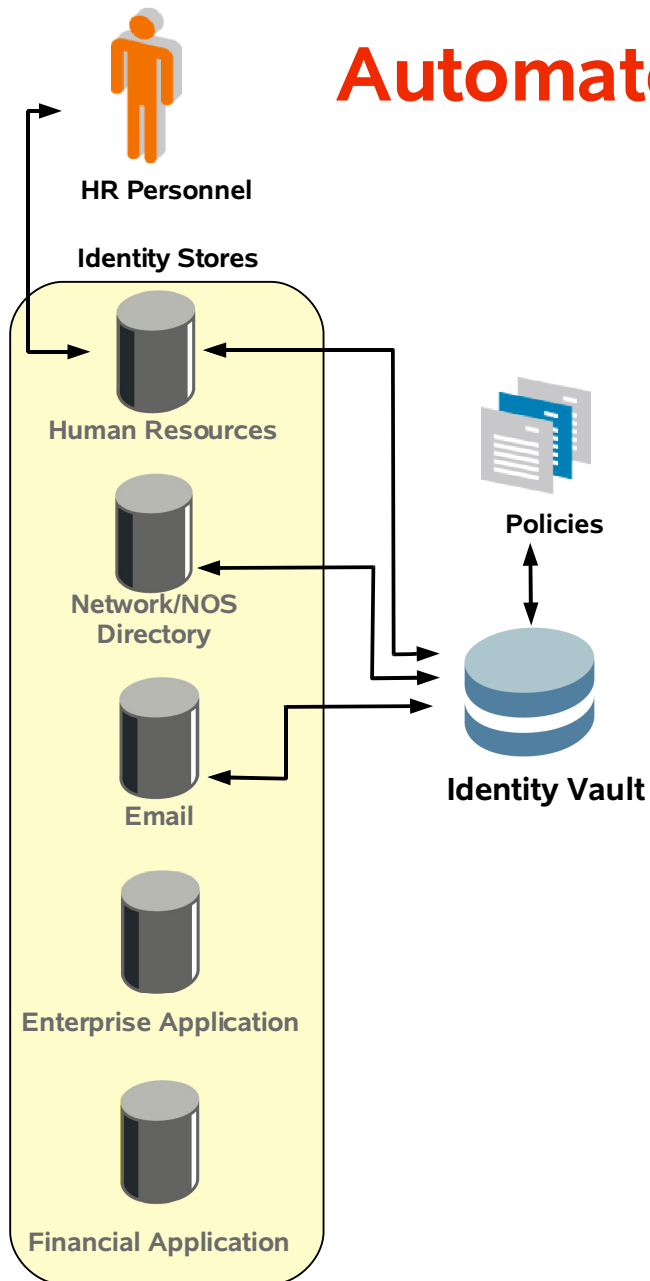
- Applications can consume data stored within I-Vault
- Better data quality, authoritative data synchronized across enterprise

User account workflows can be leveraged to enhance provisioning capabilities

- Better controls and greater efficiency
- Improved service to users by real-time provisioning and online security approvals
- Reduced effort to manage user accounts by applications staff



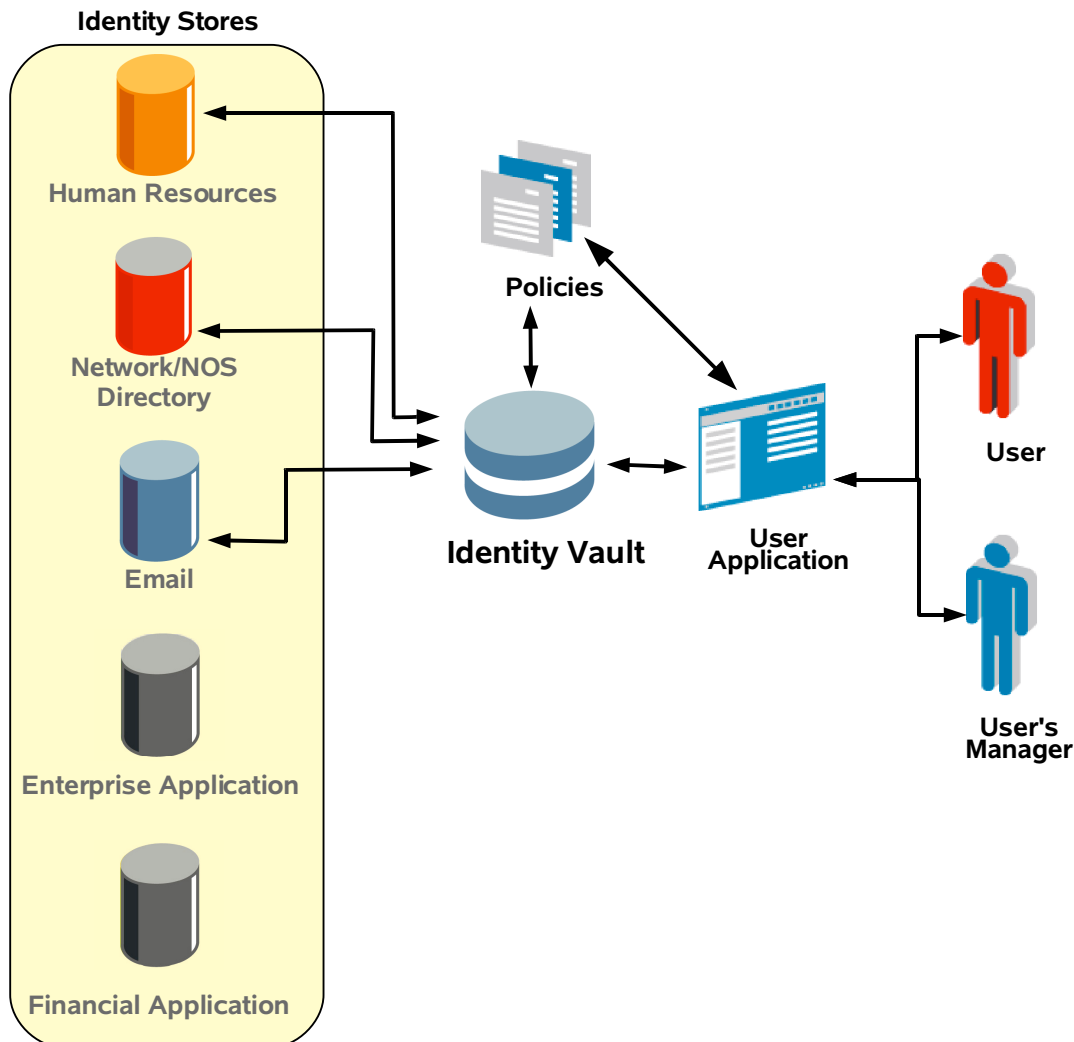
Automated Provisioning



In order to give user's access to the resources they need we utilize dynamic provisioning capabilities.

- This allows Identity Manager to capture events that occur in an authoritative system such as an HR system.
- The Identity Management system provisions user in realtime based on on policies.

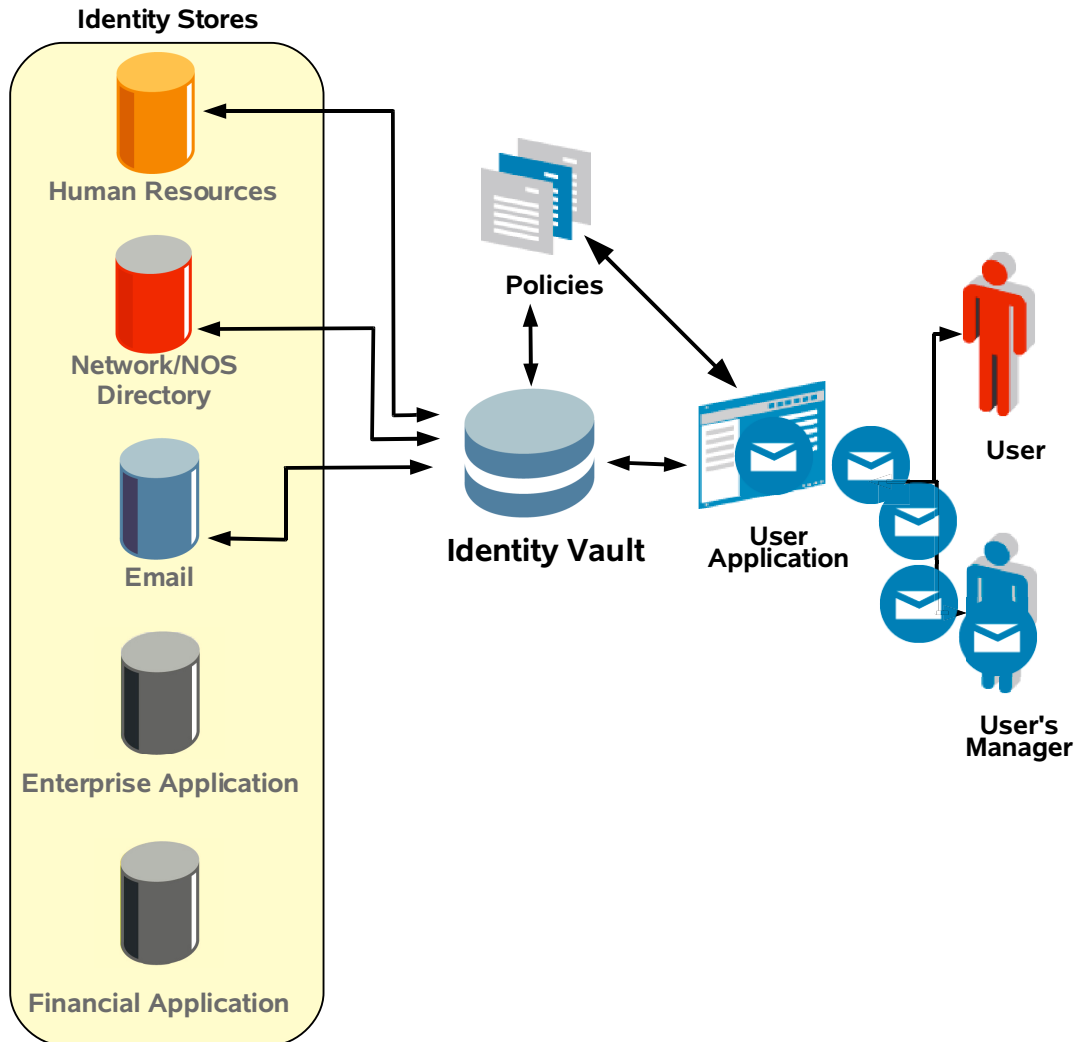
Workflow Based Provisioning



In situations where access to resources should require approval, a user facing provisioning environment is created.

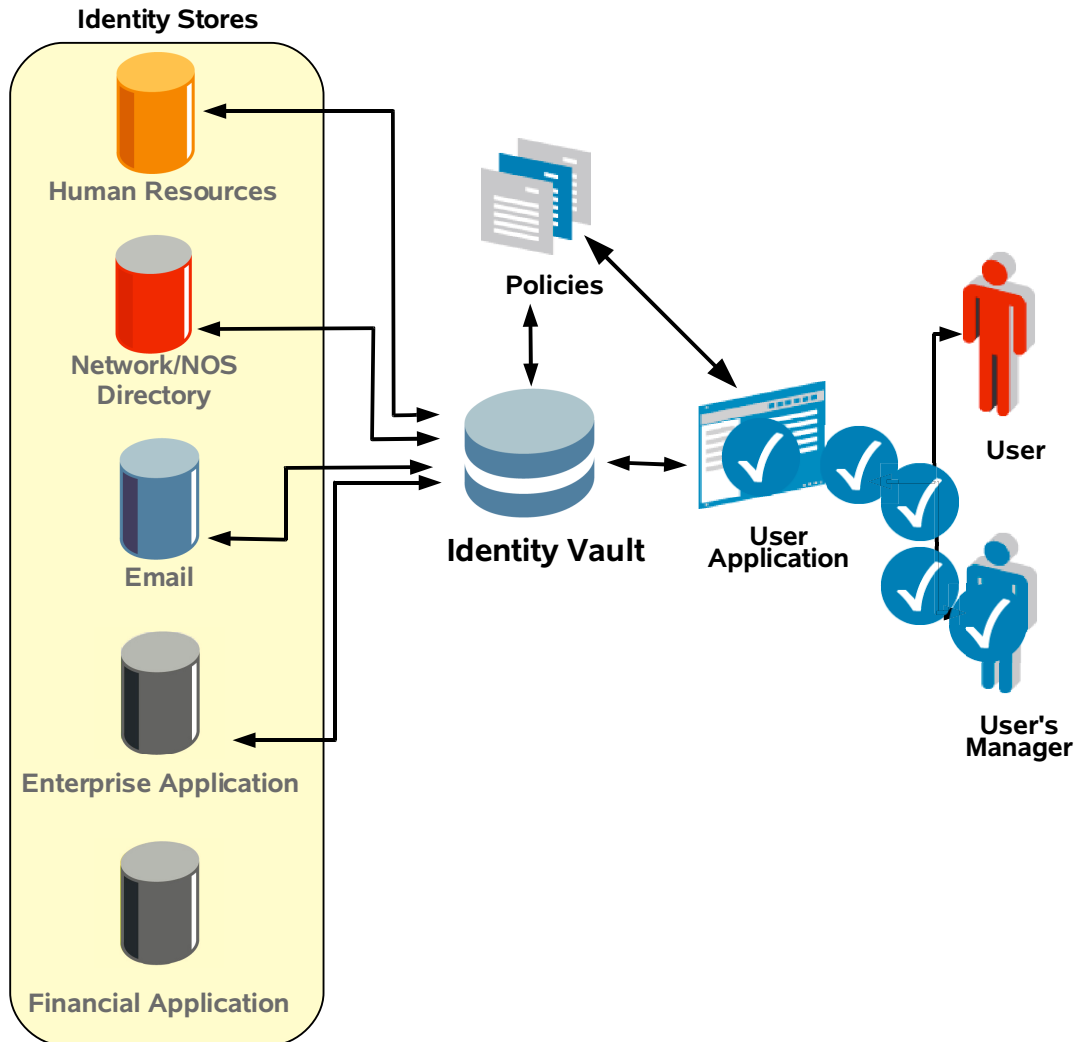
- Users only see the resources that they can request based on their Identity.
- Policies determine who should approve access to the resource.

Workflow Based Provisioning



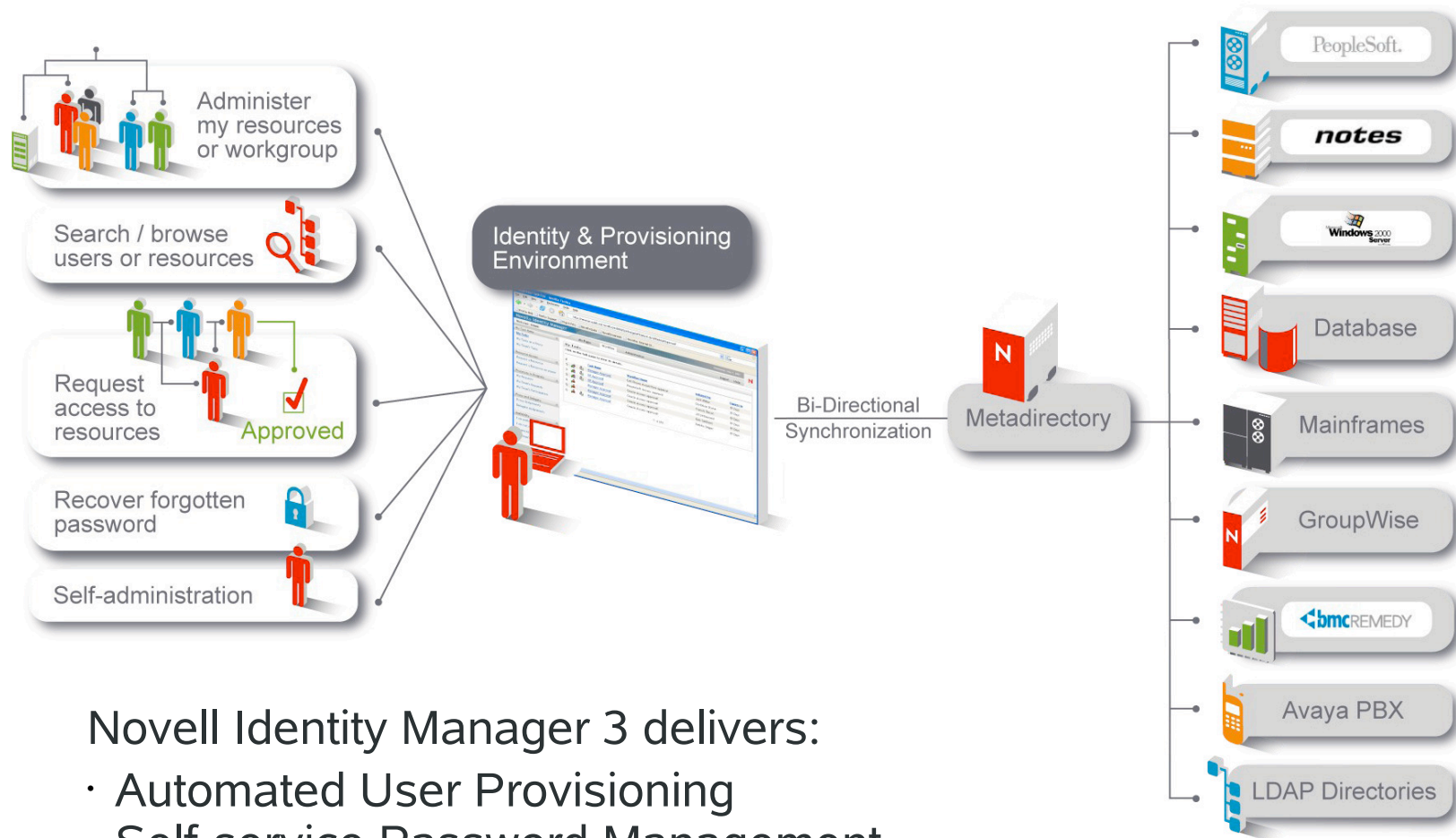
Users can be notified there is a request awaiting their approval in a variety of ways including email.

Workflow Based Provisioning



A link in the email can forward the user to the Provisioning User Application. Here the manager can deny or approve the request.

Novell Identity Manager 3



Novell Identity Manager 3 delivers:

- Automated User Provisioning
- Self-service Password Management
- Secure Logging, Auditing and Reporting

Across platforms: Linux, Windows, Solaris, HP-UX, AIX & NetWare

Who's Doing This Today?





Why Novell's Solution is Unique

- Real-time event monitoring & reporting, a superior management console and more out of the box functionality than any other integrated solution.
- Support for mixed-platform environments and built on open standards for maximum openness and ease of connectivity.

“Novell has probably the **most intuitive** and **polished user interface** of the bunch... **We were already sufficiently impressed, and then they pulled out Designer**”

InfoWorld Review of Identity Management Suites
- October 10, 2005



Award-Winning Technology

Ahead of the competition



The Identity Management Challenge

- October 10, 2005 Oliver Rist & Paul Venezia

In a recent shootout of competitive identity management solutions from Novell®, Courion*, IBM*, Microsoft*, Sun*, and Thor Technologies* **Novell emerged victorious.**

“Novell Identity Manager proved to be one of the **easiest-to-use** solutions in the roundup. The addition of Designer adds **even more intuitive functionality** on top of this suite.”

“Designer gives the Novell solution **a definite ooh-aah factor not found in any of the other products here.**”

What is user account workflow?

The electronic routing and tracking of request / approval tasks associated with resource provisioning, using defined business rules and policies, together with identity attributes (relationships, roles, job functions, identity data, etc.)



Identity-based workflow can include:

- Auto-initiation based on HR triggers, manager initiation, employee initiation
- Delegation, proxying, dynamic routing, and escalation based on business rules
- Logging and reporting for compliance purposes
- Tracking, aging, and other process monitoring metrics
- The ability to manage group provisioning, quorum approvals, and team claiming of tasks
- Recertification of existing privileges and accounts
- Incorporation of digital signatures for non-repudiation of approvals

26 Identity Management Initiatives identified

- I-Vault
- Authentication and Author
- People
- eBenef
- Photo connect
- Passw
- Excha
- RACF mainfr
- Junipe engine
- NetWare Connector
- Authentication service
- Reduced Sign on
- White Pages and self service
- Remote Access

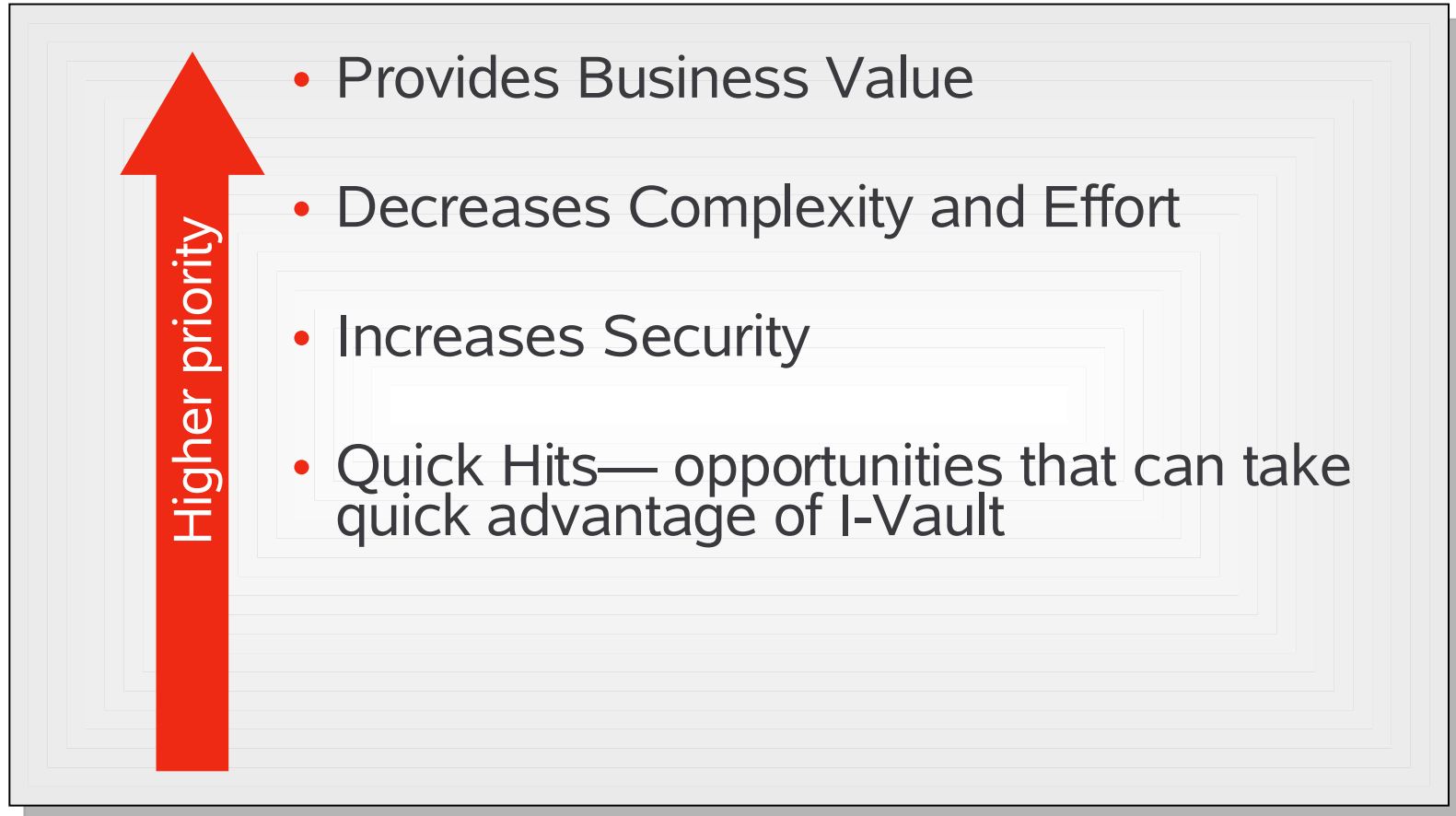
Extremely Diverse Initiatives

- From Physical to Logical
- From Legacy to Web based
- From Managing Employees to Contractors and Retirees

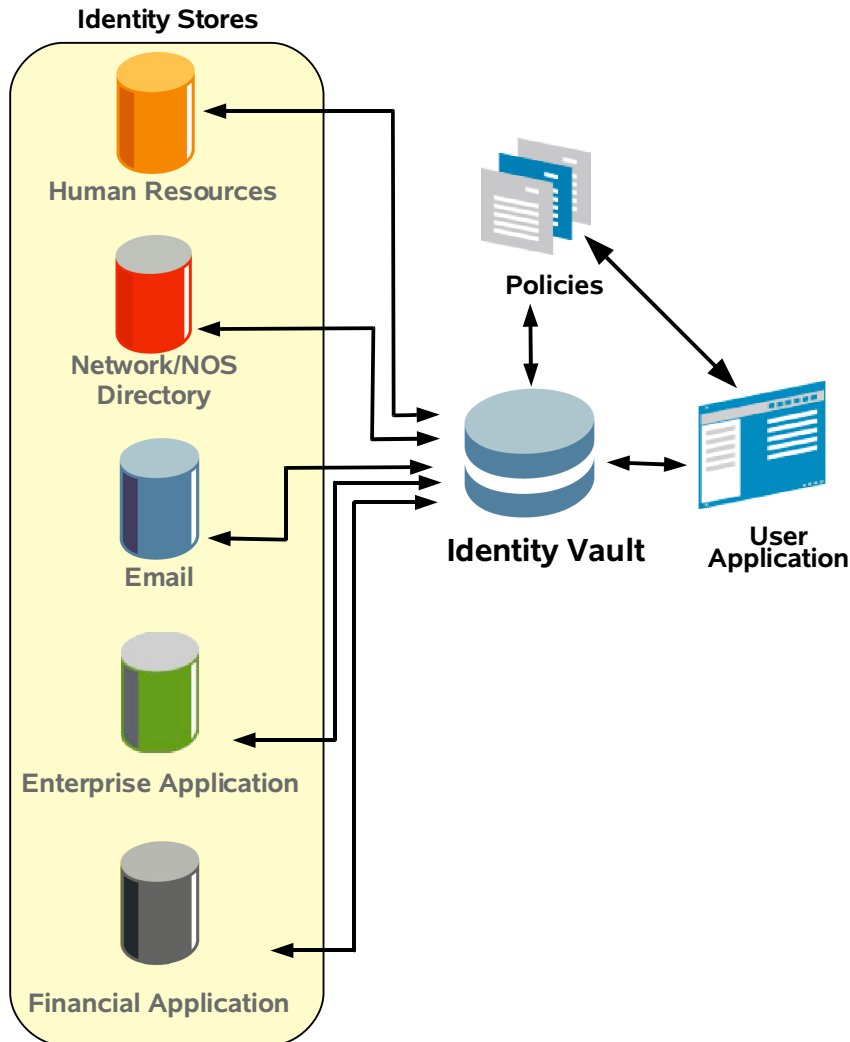
ng
er
tions

- Unix/Linux platforms
- Spear single sign on
- Access Control (new)

I-Vault opportunity prioritization criteria



Identity Event Management



Identity Management creates many events which need to be logged, audited and reported on.

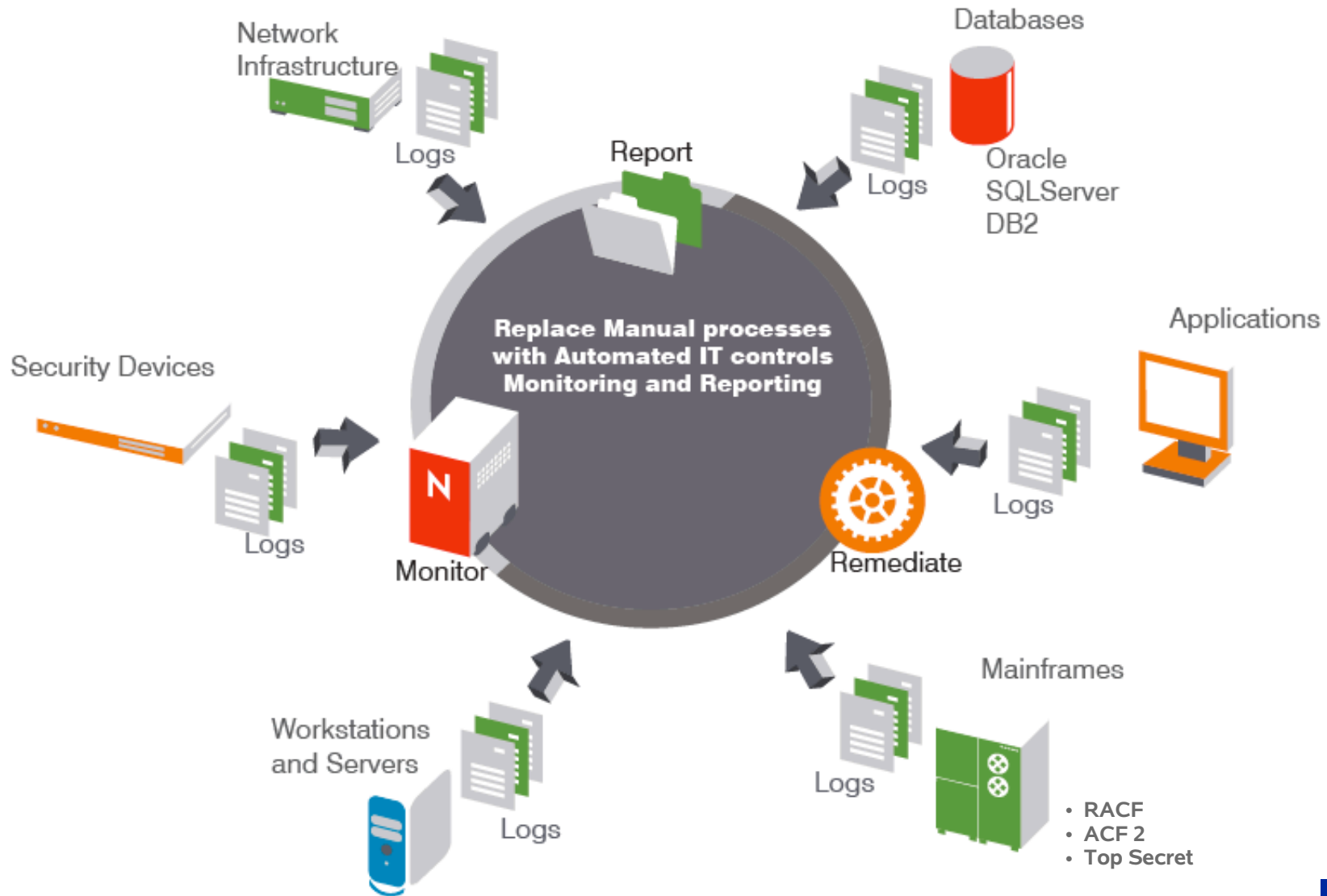
- User Creations
- Requests for access
- Approvals of access
- Access Given
- Change of attributes
- Changes of role
- Deletion of Accounts
- ETC...

Silos of Data, Manual Processes, So Little Insight

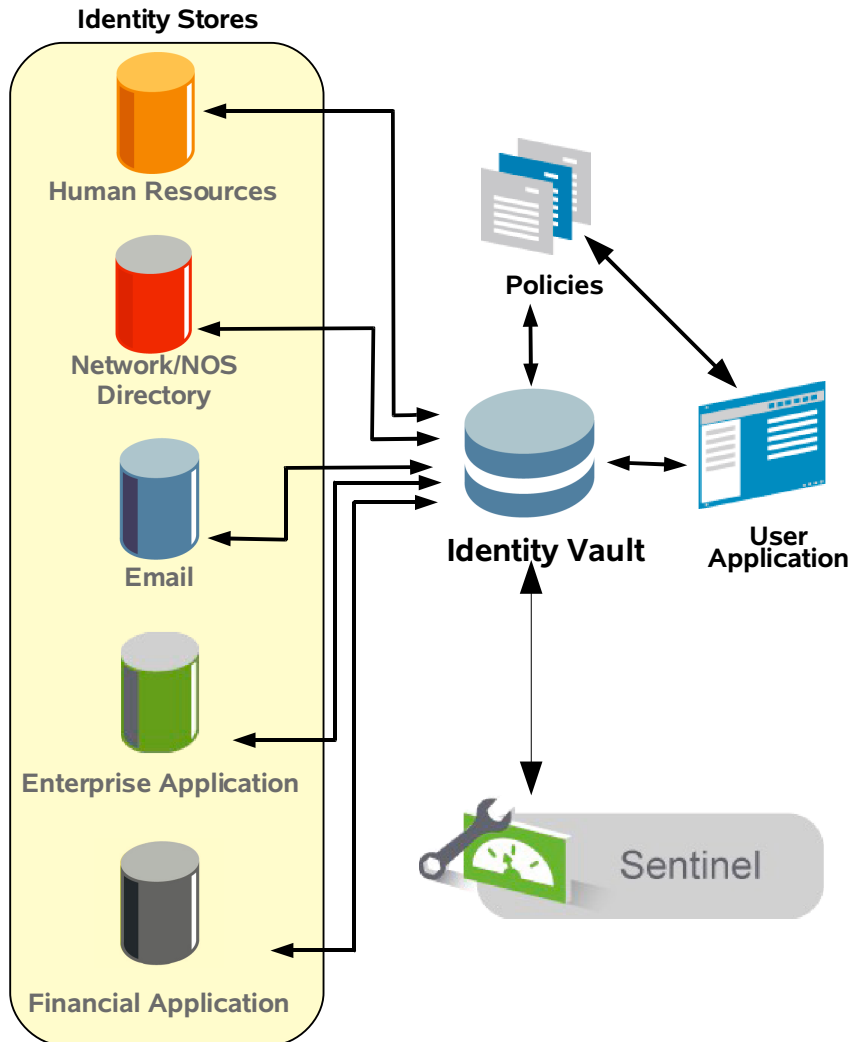




With Sentinel™...



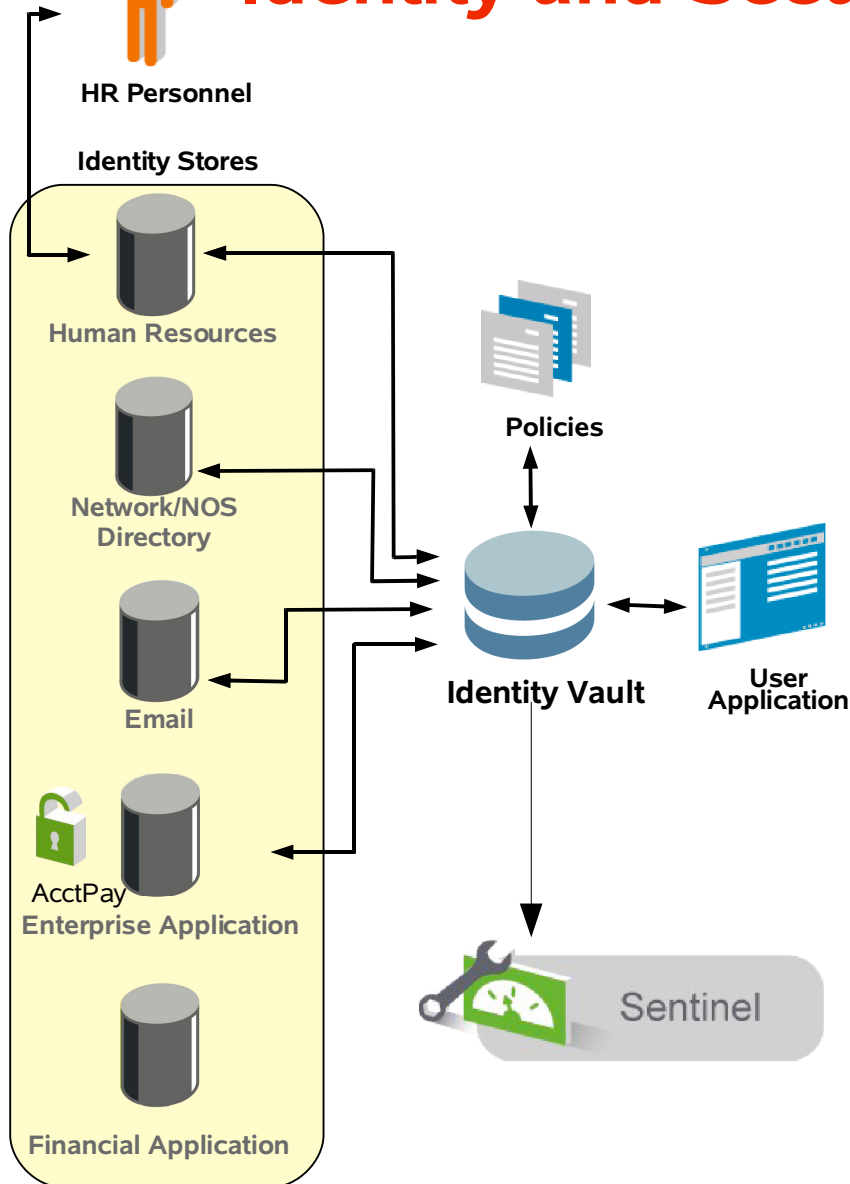
Enter Novel Sentinel



- Sentinel provides real-time infrastructure to monitor, manage and automate security and compliance related to identity, information and network resources.
- Identity Manager enriches collected events with identity specific business relevance.
- Bi-directional ties into the provisioning features of Identity Manager allows automatic account updates as a part of remediation.

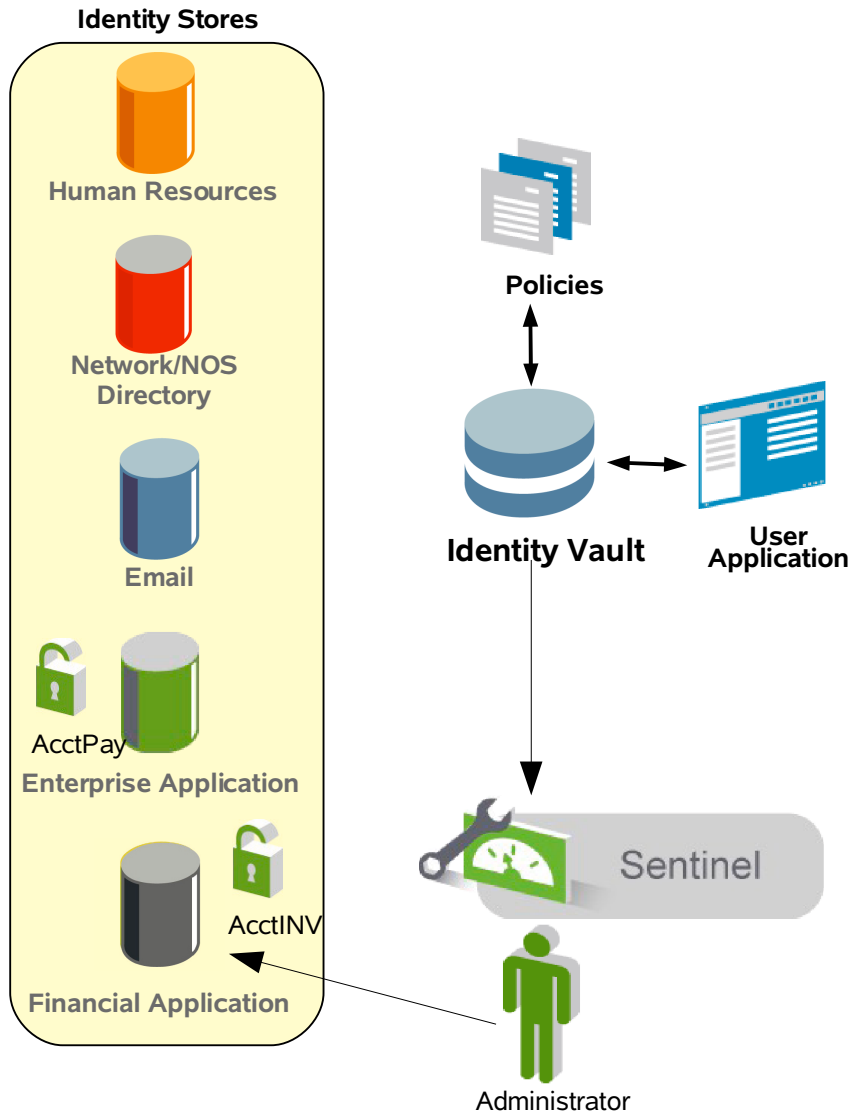


Identity and Security Convergence



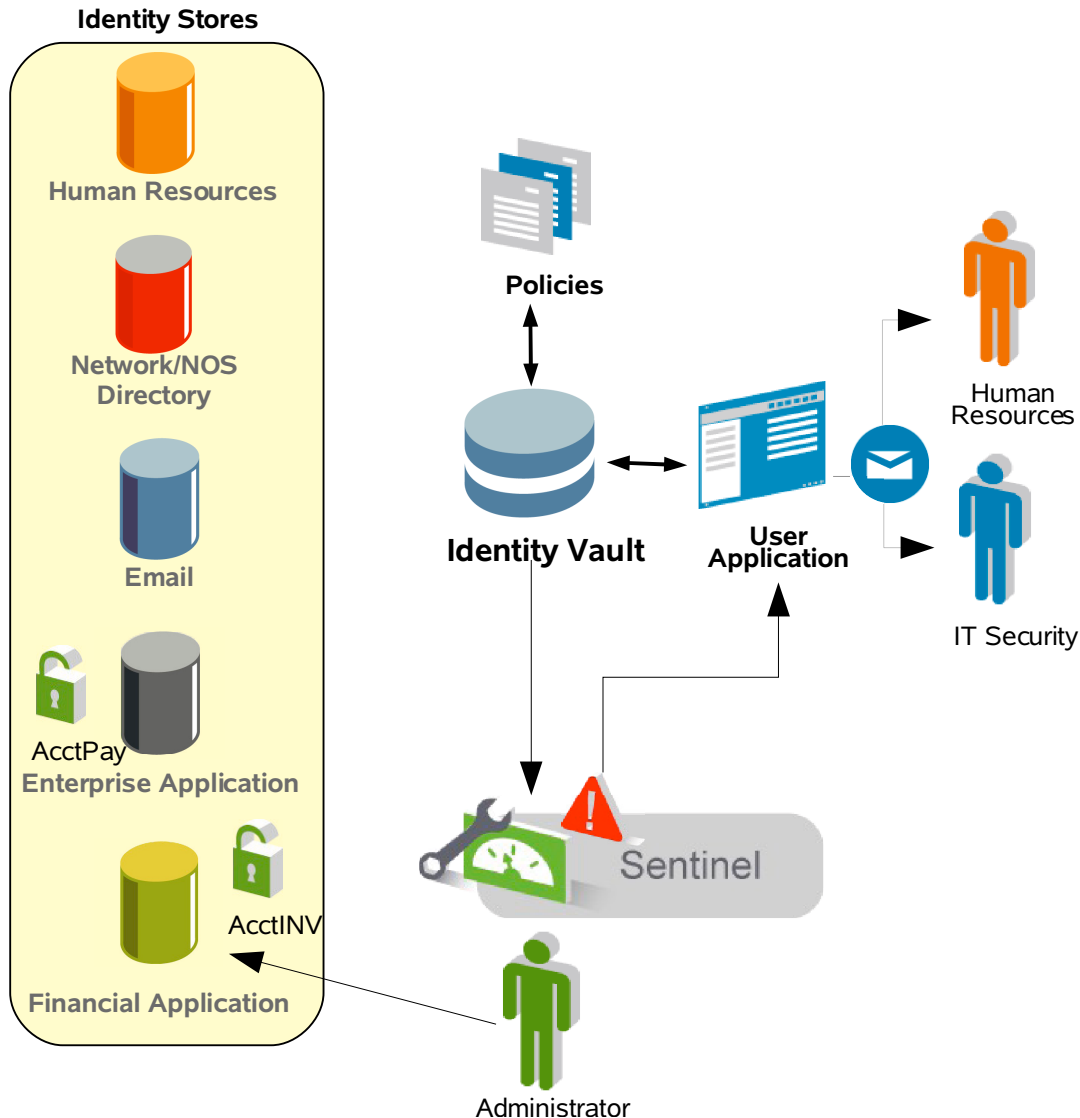
- Jeff joins company in Accounts Payable and is provisioned into the ERP Application in the AcctPay group.
- All of his Provisioning events are monitored and logged by Sentinel.

Identity and Security Convergence



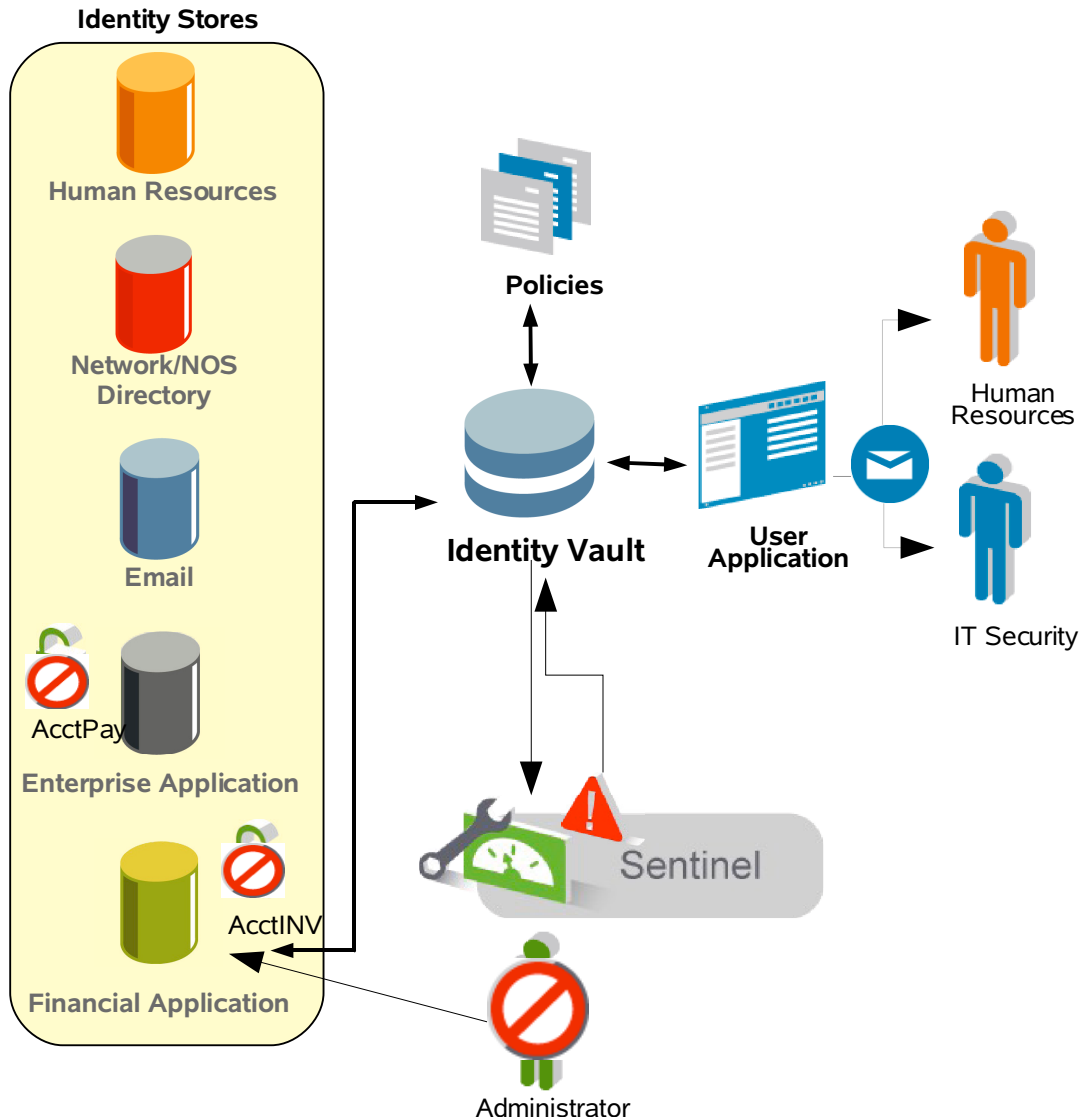
- Due to “Segregation of Duties” policies Jeff can not be part of both the AcctPay in the ERP Application and AcctInv in the Finance Application.
- Jeff, wants to close out accounts at the end of the quarter. He asks a friend in IT to add him to the AcctInv group in in the Financial application
- His friend, the admin adds him to the group violating the Segregation of Duties policy.

Identity and Security Convergence



- The addition of Jeff to the AcctInv group is picked up by Sentinel and evaluated against a Separation of Duties ruleset.
- The rule is triggered and initiates a workflow for IT security to evaluate. The correlation engine can also perform additional actions such as an email notification to Human Resource.

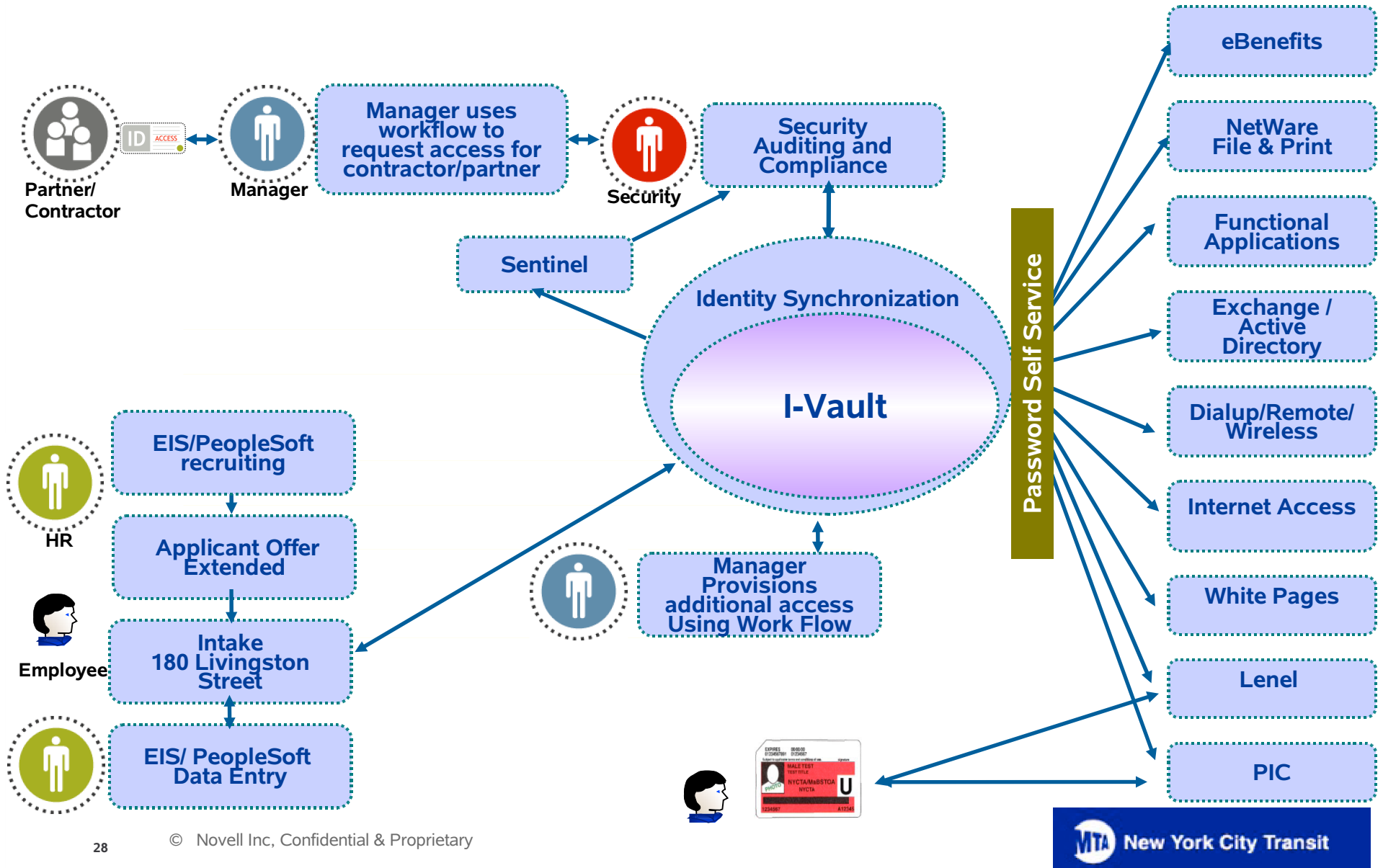
Identity and Security Convergence



- While the situation is being evaluated by Human Resources and IT security, Sentinel informs the identity management system of the violation.
- The Identity Management system initiates account suspension of the admin's account and Jeff's account via IDM.
- These account suspension events are logged to Sentinel as well.

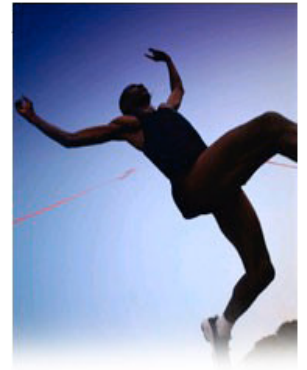


High Level Identity Management Vision



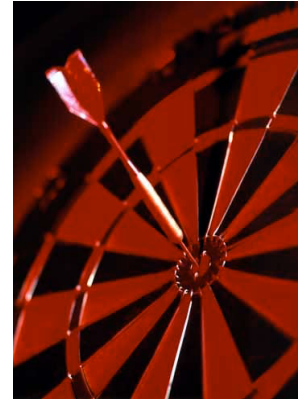
Current Status

- I-Vault Infrastructure
 - Identity enabling platform is in production
 - Contains 85,000 employees and retirees
 - Connections from EIS and PIC for new updates to employee information
 - 2 LDAP Authentication service directories in place
- User Registration & Password Self-Service
 - Updated user interface – myaccess.nyct.com went live on May 18
- Application Support
 - AskHR application authentication
 - eBenefits authentication
 - IVR authentication
 - Kronos
 - Lenel
 - Access Control for Subways
 - eMail and Active Directory
 - NOS (NetWare) file and print share Tree
- Governance Plan Implemented



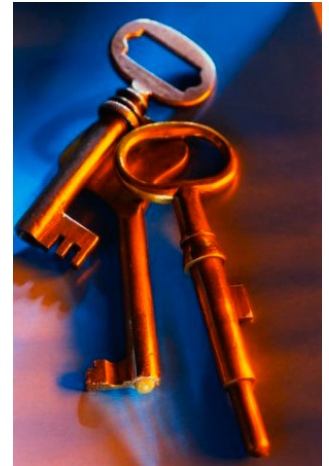
The goals of I-Vault governance NYCT

- Deliver a common set of technical and business capabilities across NYCT to reduce costs, increase productivity and efficiency, improve security, and assure conformance
- Drive standardization needed to achieve business benefits while encouraging adaptability, flexibility, and innovation
- Ensure that I-Vault concepts and benefits are understood and supported by NYCT leaders, managers, and stakeholders
- Involve and represent needs of all affected parties and provide transparency in decision-making
- Provide clarity in identity management standards, processes, roles, and accountabilities
- Measure and communicate results, drive continual improvement



Keys to effective identity governance

- ✓ Enterprise-level executive sponsorship
- ✓ Necessary structure to represent key stakeholders
- ✓ Cross-functional / cross-organization involvement
- ✓ Necessary processes to fulfil governance mission
- ✓ Defined charter—mission, goals, measures of success
- ✓ Clear roles and responsibilities for leadership, management, and operation
- ✓ Consensus based, not silo based decision-making
- ✓ Dedicated resources with clear mission and goals
- ✓ Defined and measurable policies and processes
- ✓ Solid communication plan



Summary of 2007 changes and key benefits

• Increase Efficiency

- User Account workflows replace key paper request forms
- Support migration to new File/Print and AD infrastructure

• Improve Security

- Support provisioning / deprovisioning
 - Kronos, Lenel, Access Control
 - File/Print and Active Directory/Exchange
- Obtain PIC photos for security applications
 - Access Control, and Lenel in future

• Improve Audit capabilities

- Log requests and approvals for access