

Novell® Secure IT Tour

May 9, 2006



Novell®

Agenda

- 8:30 - 9:00 Breakfast and Registration
- 9:00 - 9:30 Introduction: Automating Identity Management for Greater Security & Compliance
- 9:30 - 10:30 Identity & Access Management in Action:
 - > Automated provisioning and reporting
 - > Secure access and single sign-on
- 10:30 - 10:45 Break
- 10:45 - 11:30 What's Your Next, Best Step?
 - > Security and Identity Management Best Practices
- 11:30 - 12:15 Case Study and Questions

WHY ARE YOU HERE?

- What are YOUR business challenges?
- Does your organization face regulatory pressures?
- Is information theft a current concern?
- Do you need to reduce costs?
- What are you hoping to learn today?

Security Challenges Today...

Information Theft
Privacy Concerns

The collage includes several articles:

- Information Theft:** An article from TechnologyPost.com mentioning Kessler International and information theft losses doubling in three years.
- Hotmail Policy Raises Privacy Concerns:** An article from PC World by Tom Rabinelli, dated Friday, May 17, 2002, discussing Hotmail users and privacy.
- Minimize Securities Litigation Risks -- Guidelines For Designing Your Web Site:** An article from FindLaw.com by Meredith Landy of Brobeck Phleger & Harrison, discussing web site design and litigation risks.
- Sarbanes-Oxley COMPLIANCE JOURNAL:** A section titled "Embracing Compliance" dated 2005-06-24 12:00:00.0 CDT by Reed Harrison, discussing the pressure of federal regulations.
- Special report on IT globalization:** An article from ITworld.com dated 3/22/01, discussing global expansion and IT management challenges.

Litigation Risks
Compliance Violations
Growth Challenges

...Lead to Opportunities

Security & Compliance

Secure sensitive information & meet regulatory demands

Agility & Cost Containment

Enable growth while controlling costs

“Identity and access management projects are much more than technology implementations - they have real business value by reducing direct costs, improving operational efficiency and enabling regulatory compliance. “

Business Drivers of Identity and Access Management

- Roberta Witty, Gartner Group November 2003

What is Required?

1

Manage
Complexity

2

Enforce
Security and
Compliance

3

Maximize
Agility

...across all your systems and platforms

“In three to five years, every large organization will have an access management middleware layer that knows the identity of every user and device, and manages who can talk to what, when and how.”

The hottest business you never heard of
- *CNET Perspectives, May 18, 2005*

Who's Doing This Today?



Automating Identity Management for Greater Security & Compliance

The Challenge:

How can you enable your business to be more open and agile without limiting security or control?

- Enforce consistent security policy across all systems
- Enable centralized management and reporting
- Deliver real-time automated access management

Strategic Implications

- Can't afford **cost** of administering users & IT resources
- Shouldn't manage **compliance** without auditable IT controls
- Won't let **complex security** policy limit business **agility**

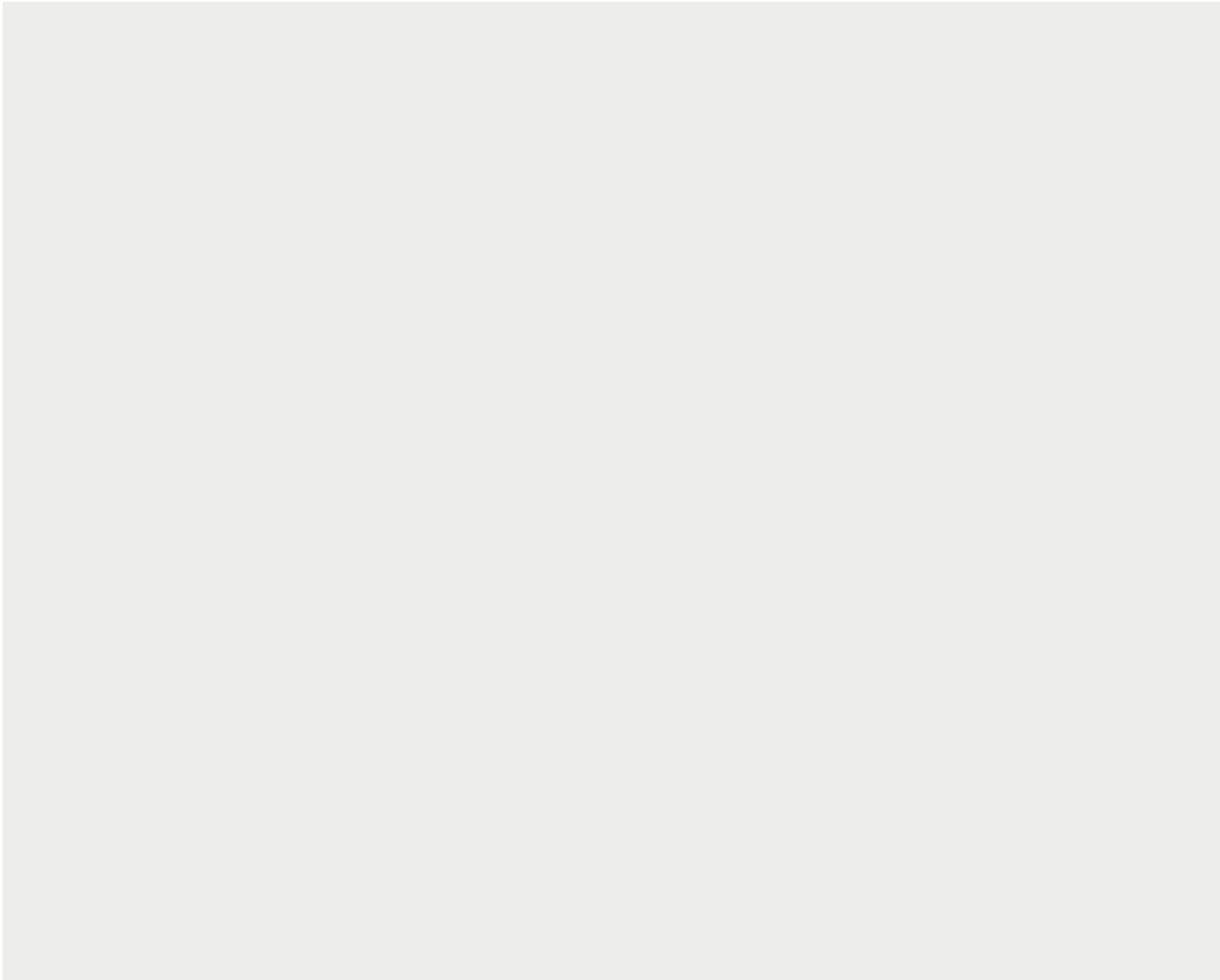
The Solution:

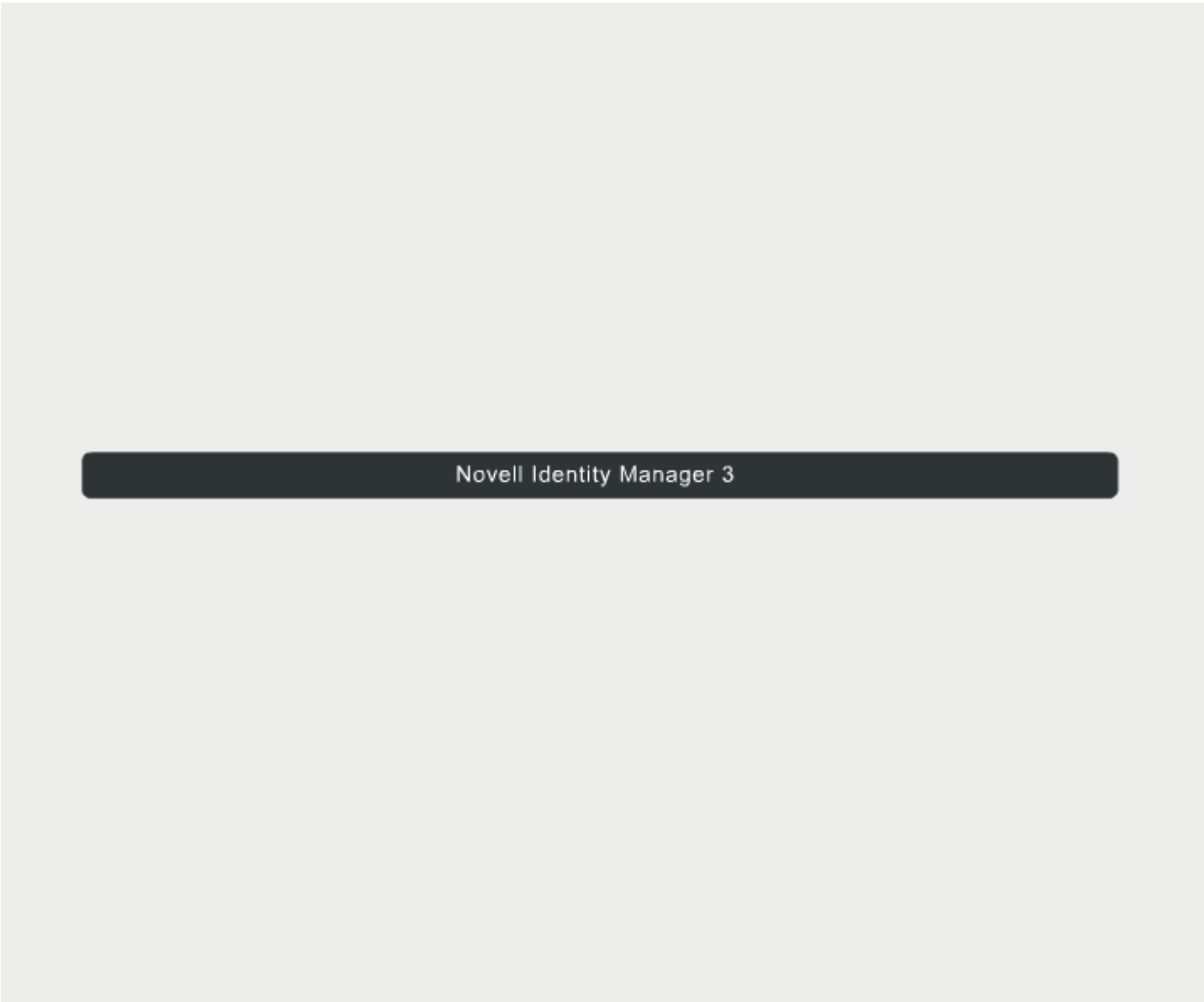
Automated Provisioning

It's about:

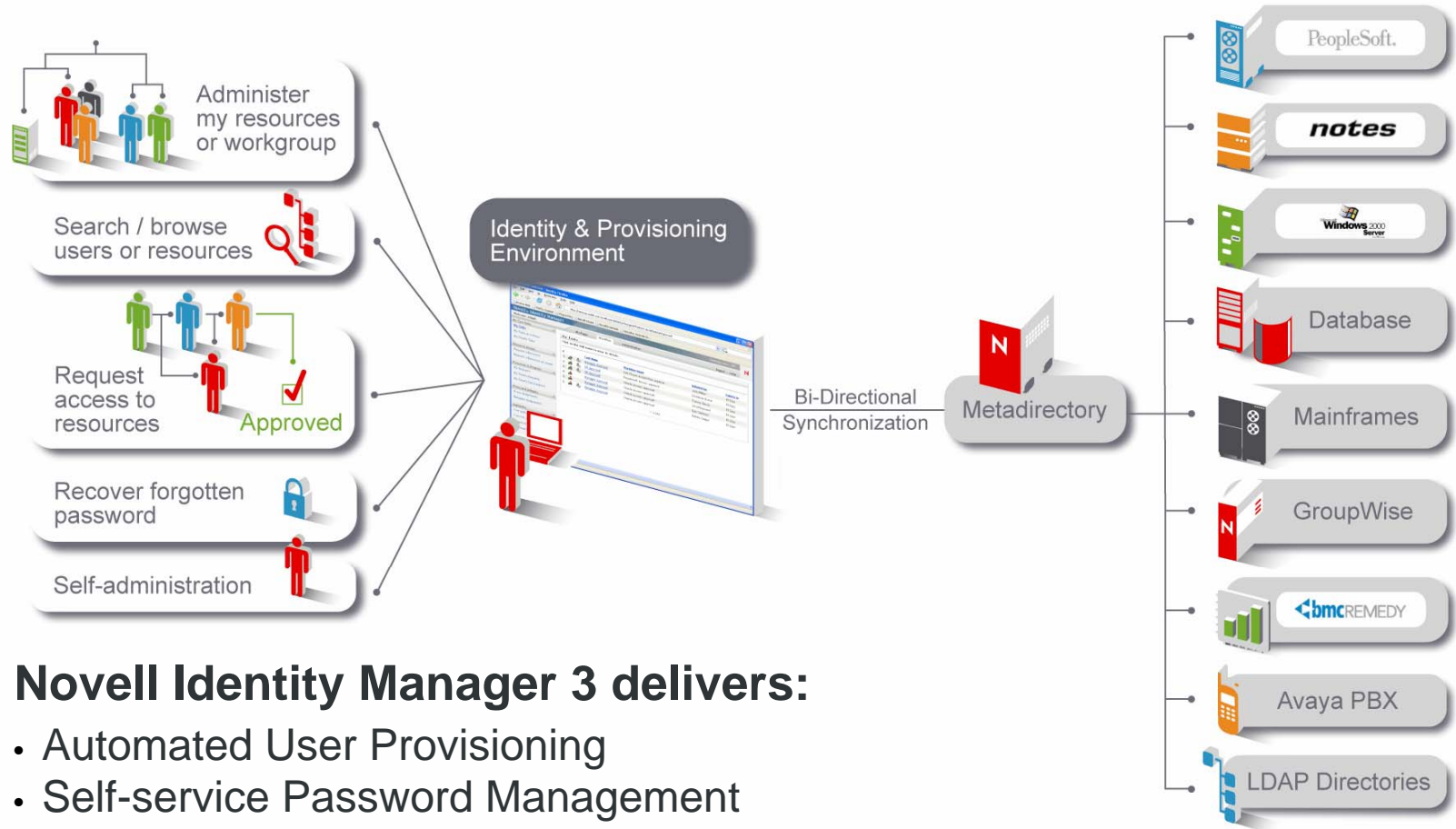
- Immediate Access
 - Instant On
 - Rapid time to productivity
- Security Confidence
 - Instant Off
 - Eliminate known and unknown exposures
- Real Cost Savings
 - Integrated, distributed identities
 - Reduced points of administration

Novell Identity Manager 3





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®

Managing the Complete User Lifecycle



Top Three Features & Functions

1. Simplified Configuration & Administration

- Automated Provisioning Workflows
- Self-Service Provisioning & Password Management
- Identity-driven Business Applications
- Visual Toolkit for Identity Management

2. Automated Compliance

- Automated Audit, Reporting & Documentation

3. Secure & Scalable Architecture

- Encrypted Identity Vault
- Bi-directional, Real-time Synchronization
- Open Standards-based/Cross-platform Support
- Unlimited Connectivity

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.**”

Demonstration Automated Provisioning & Reporting

Demonstration Secure Access & Single Sign-on

Does This Sound Like You?

- **I would like a single solution that controls access to my web and enterprise applications**
- **I need to quickly deploy protected services, while reducing management overhead**
- **I need to reduce risk of non-compliance with User Privacy and other regulations.**
- **I need to inter-operate with internal and external business partners**
- **I need a way to quickly enable services due to recent acquisitions**

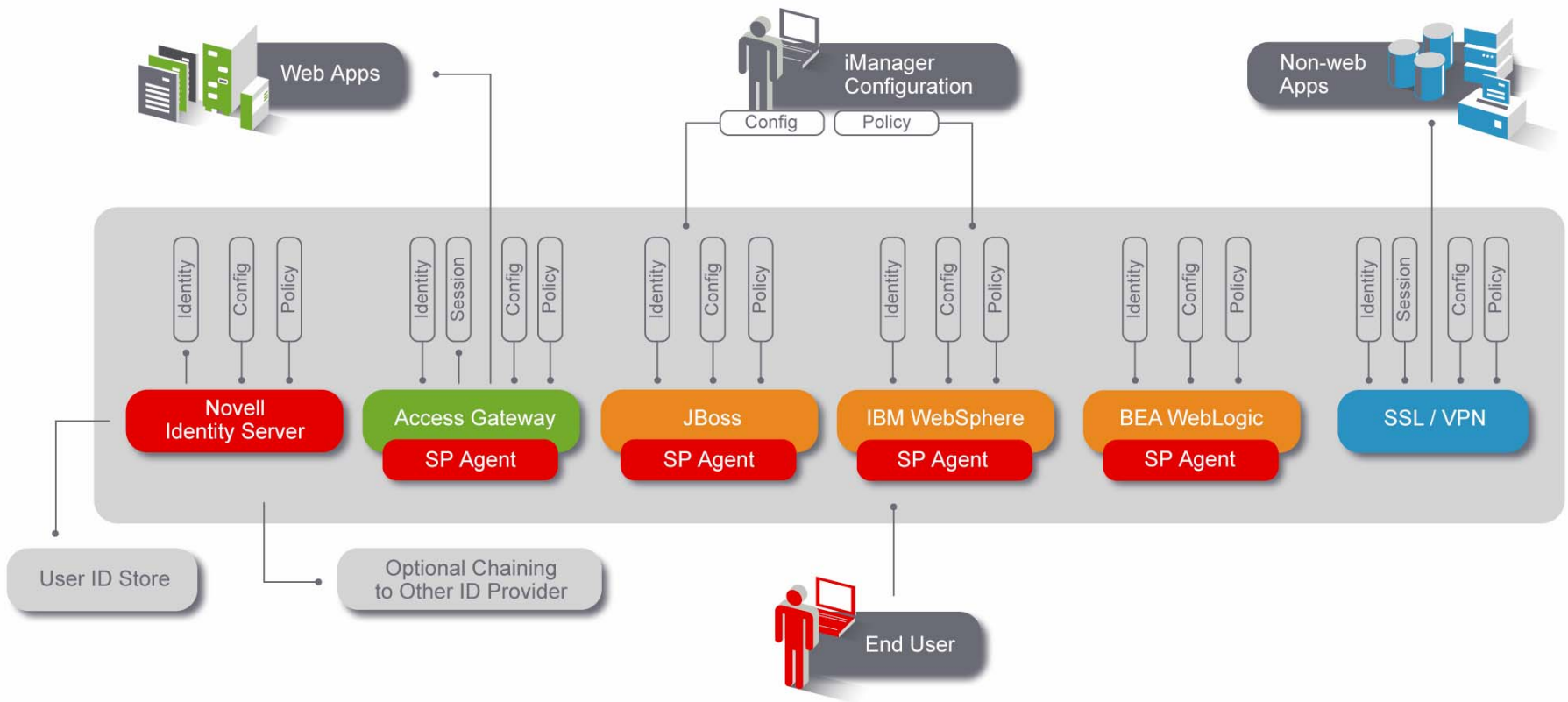
Introducing Novell® Access Manager

The Future of Novell® iChain

Next-generation Access Management Solution

- Secures HTTP applications via Access Gateway
- Secures non-HTTP applications via SSLVPN
- EJB and Servlet fine grained access control via Java* Agents
- Extensible policy engine
- Identity federation (SAML and Liberty Alliance)
 - > No need to modify Web applications to take advantage of new federated identity standards

Novell® Access Manager



Best Practices Security & Identity Management

Think About Where You Are Today



Your First Identity-driven Project: What to look for and how to succeed

1. What should I be evaluating?
2. Lessons learned for managing your first identity and access management project

Solution Components:

8 Features to look for:

1. Integrated roles, rights & rules across product suite
2. Modular access management
3. Secure auditing, flexible reporting
4. Workflow – automated, manual & self service
5. Password management
6. Integrated identity vault
7. Connectivity
8. Platform performance

1. Integrated Roles, Rights & Rules

What should be evaluated?

The ability to:

- Associate access rights with a role within the organization
- Dynamically assign and automatically change access rights based on changes in user role
- Mix manual and automatic roles and rights assignments
- Report on roles, rights associated with roles and users associated with roles
- Use defined organizational information to dynamically route workflow and approvals

2. Workflow: Self Service & Administration ^N

What should be evaluated?

- Web-based tool for requesting resource access
- Ability to use defined organizational information to dynamically route workflow and approvals to the “right” role/person.
- Ability to delegate approval authority to another
- Automatic escalation of request to alternative approver as time elapses

3. Access Management

What should be evaluated?

- Adherence to open/industry standards
- Protection of private user information
- Secure process for transmitting changes in access rights over the internet.
- Reporting of user access events, changes in access rights
- Web and client-based SSO
- Integrated management console for identity & access management administration

4. Audit

What should be evaluated?

- Datastore that supports non-repudiation – “Tamper-proof”
- Time stamped records for changes in access rights, roles and each sequence in approval workflows
- Multi-factor, easy to build reports for users, systems, administrators workflows and time periods

5. Password Management

What should be evaluated?

- Ability to reach user self service through the Web without logging into the network.
- Ability to implement password policy across the entire enterprise
- Password synchronization across the entire enterprise (including legacy systems)

6. Integrated Identity Store

What should be evaluated?

- Ability to connect to multiple data stores to build “one view” of the user
- Ability to detect and respond to changes in the identity store in real time
- Ability to detect and roll back changes made to user attributes automatically, based on policy, in identity store or application
- Ability to prevent the creation of orphan accounts through policy

7. Connectivity

What should be evaluated?

- Availability of connector development tool
- By-directional synchronization
- Ability to define and connect application and identity data at any object or attribute level
- Web services functionality & standards-based
- Event-based
- Legacy support

8. Platform

What should be evaluated?

- Web-based administrative systems for remote management or integration into existing portals
- All components should be configured for high availability including disaster recovery and fault tolerance
- Ability to operate on secure platforms like Linux
- XML-based extensibility for interaction with external systems
- Demonstrated performance on loads exceeding likely performance environment
- Doesn't require rip & replace of existing systems

Lessons Learned: Your First Identity Management Project

Project Steps:

1. Discovery & Design
2. Proof of Concept
3. Production Prep, Pilot & Rollout
4. Installation
5. Documentation

1. Discovery & Design

- Determine if pre-existing conditions need to be addressed before project launch
- Develop a “solution roadmap” of what your world will look like after project completion
- Including Line of Business Units that “own” applications in the RFP creation. Examples: HR, Accounting etc.
- Define the business processes you are looking to automate
- Map your existing enterprise data model

2. Proof of Concept

- Focus on access to legacy or silo-ed applications
- Identify vendor customization requirements
- Consider paying for a more detailed POC/proposal – with the price being credited towards final purchase
- Focus success factors business requirements not technical minutia

3. Production Prep, Pilot & Rollout

- Set realistic organizational timeline expectations
- Make sure solution can support “rollback”
- Create centralized identity “vault”
- Find project champions within user groups and train them first

4. Installation Sequence

- Install software
- Set up connected systems
- Activate the software
- Configure password management
- Configure entitlements
- Configure audit and reporting
- Configure workflow & user application
 - based on business policies

5. Documentation

- Detail design and implementation
- Ensure documentation addresses audit/compliance needs
- Automate documentation production

Additional Thoughts

- Identity & access management projects are obtainable if taken in stages
- Not all technologies may be initially required, but most are ultimately used, very little shelfware
- Avoid solutions that disrupt existing systems during deployment
- Align early stage deliverables to primary business driver to highlight quick win ROI and build internal support for project
- Focus on the total cost of the project over time - not just cost of software or support

Customer Case Study State of Michigan

Michigan State Police Priorities

- • Increase Homeland Security
- Improve Public Safety
- Save Lives
- Reduce Crime
- Speed Arrests

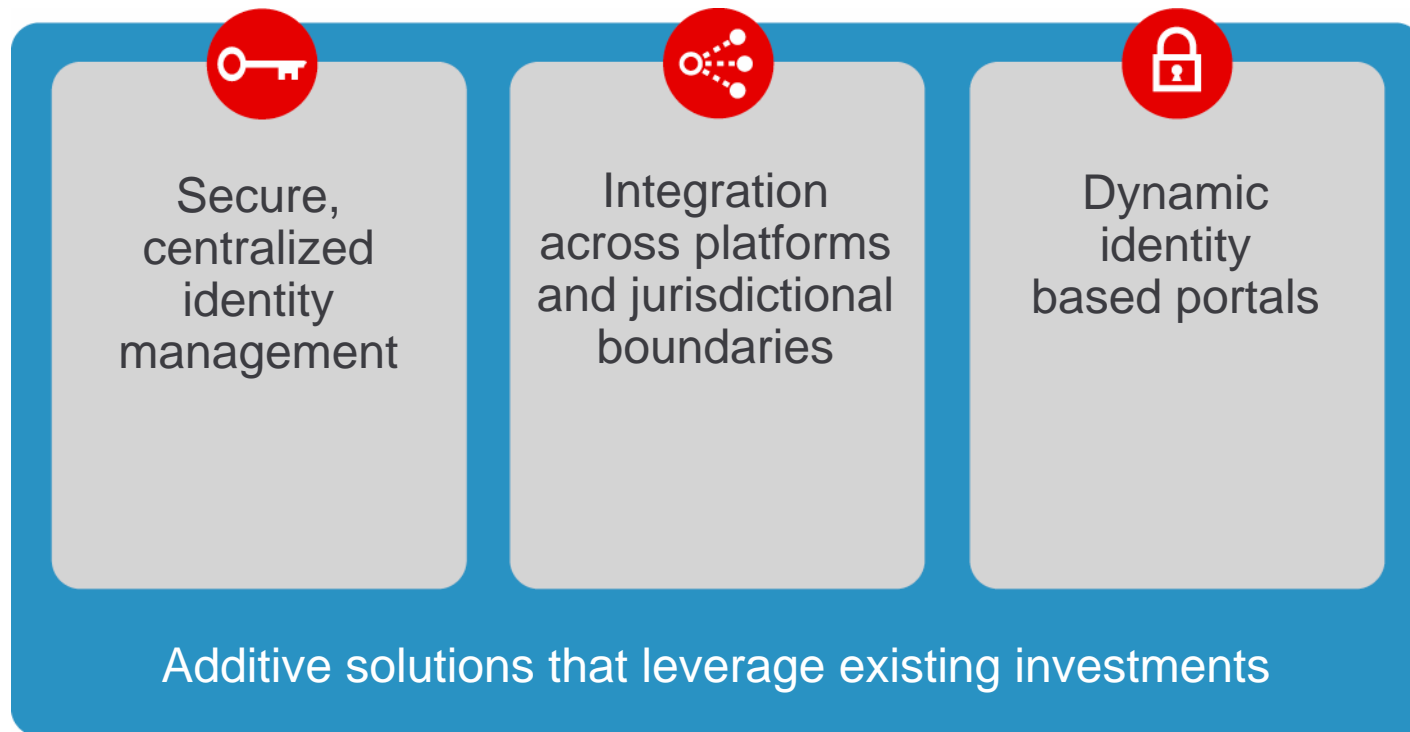
Michigan State Police Challenges

- Rising Costs - managing criminal justice applications was becoming costly and inefficient
- Unnecessary Security Risks - users sharing IDs and passwords at common terminals
- Compliance - new requirements necessitate unique, identity-based authentication for users
- Controlled Access - users need access to legacy and server-based applications
- “Do More with Less” - shrinking budgets for IT expenditures

Project Objectives

- Reduce the cost and time of managing identities, passwords and applications
- Comply with new security regulations
- Build a security infrastructure that will scale for statewide use
- Enable secure Web access to criminal justice applications
- Grant users access to applications based on their identity

Design Points



Approach

- Requirements assessment conducted to define a plan of attack
- Centralize user identity information
- Synchronize user identity information across multiple applications
- Integrate more than 50 applications through an identity-based portal
- Build a secure portal to provide troopers with access to applications from their office or their car
- Create an infrastructure to support the incorporation of applications from other state agencies

Centralized Identity Management



Desired Outcome

A single, comprehensive view of user identities

Cross-platform identity integration

Role-based identity management

Audits and tracks user access to information

Distributed and delegated administration

Supports multi-factor authentication (RSA)
(certificate, token and biometric forms of identification)

Integration



Desired Outcome

Web-enable legacy systems

Extend and maximize existing investments

Enable application and information sharing between federal, state and local jurisdictions

Create a single comprehensive view of criminal justice community information

Establish the identity of every person requesting sensitive information

Control access based on roles and responsibilities

Dynamic Identity-based Portals



Desired Outcome

Provide quick, convenient and secure access to mission critical information

Grant access based on individual roles, responsibilities and established security policies

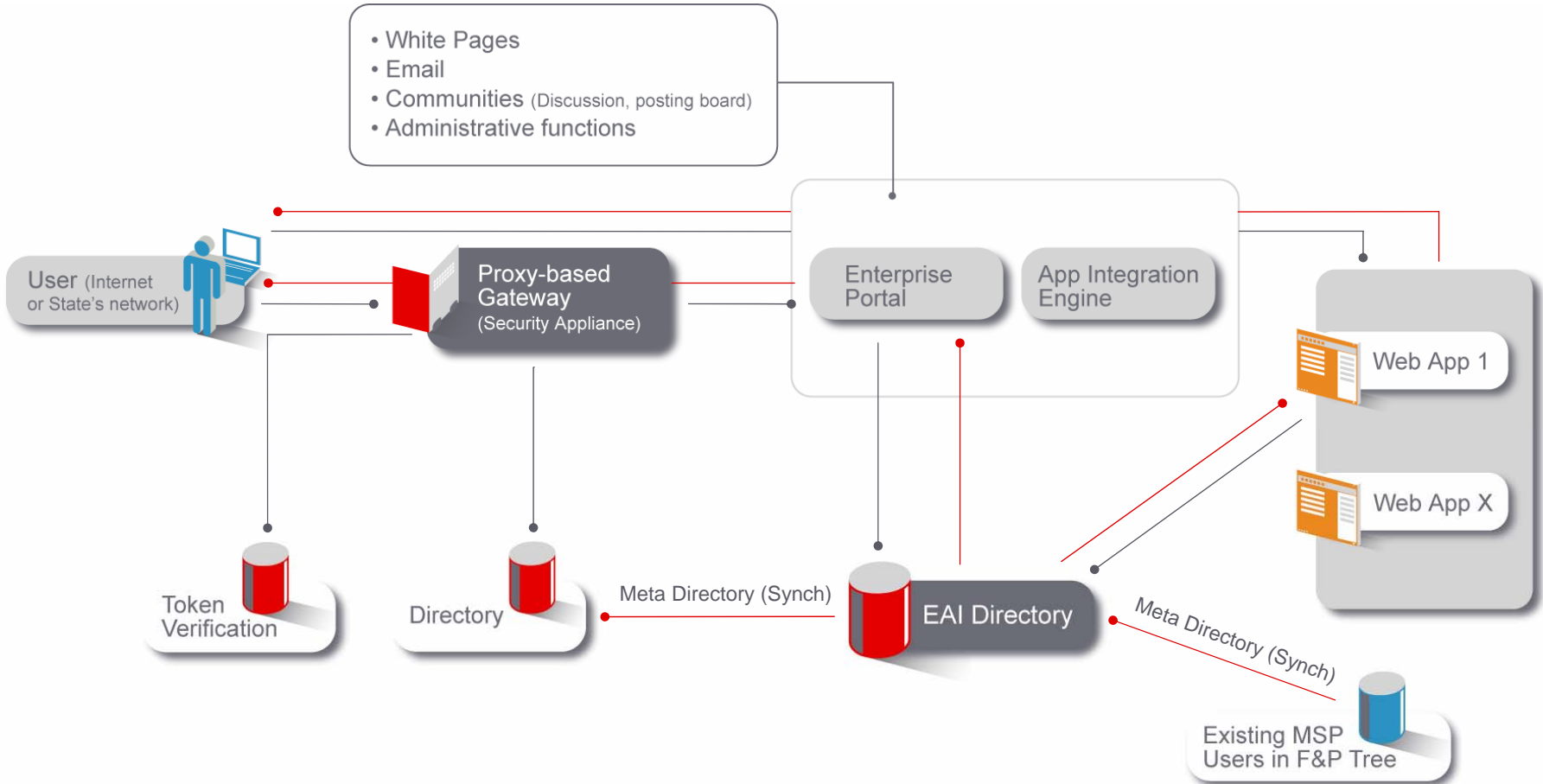
Provide access across systems & organization boundaries

Support federated, identity-based authentication


Deliver comprehensive information to support rapid decision making

Control access based on roles and responsibilities


Michigan State Police Architecture



Results

-  1,500 state troopers can access 10+ applications over the Internet
- Single sign-on to all applications and resources
- Improved productivity and crime-fighting capacity
- Improved security
- 40% reduction in identity management integration costs
- Distributed administration

Evolution - Beyond Michigan State Police

-  Incorporated additional agencies and applications into the portal environment
 - **CVISN**: Commercial Vehicle Information Safety Network
 - **CHR**: Criminal History Records
 - **E-Team**: Emergency Management

Q&A

Novell.[®]

Unpublished Work of Novell, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Novell, Inc., makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

