

Biometrics and Single Sign-On: The Next Step in Identity Management



Brian Mizelle, Vice President of Product Development
BioNetrix Systems Corporation



Network Authentication Today

- Organizations planning and starting to deploy advanced forms of strong authentication
 - Biometrics
 - Smart cards
 - Tokens
- Increasingly reliable and affordable
- Extends security to the network's edge
 - All infrastructure security inherently relies upon conclusive user verification



Biometric Management

- Large-scale biometric deployments are founded on an Authentication Management Infrastructure (AMI)
- AMI Principles:
 - Secure
 - Scalable
 - Agnostic to authentication methodologies
 - Ability to set policies based on: users, groups, channels, and/or applications
 - Audit and monitor access
 - Support for centralized or distributed management and administration

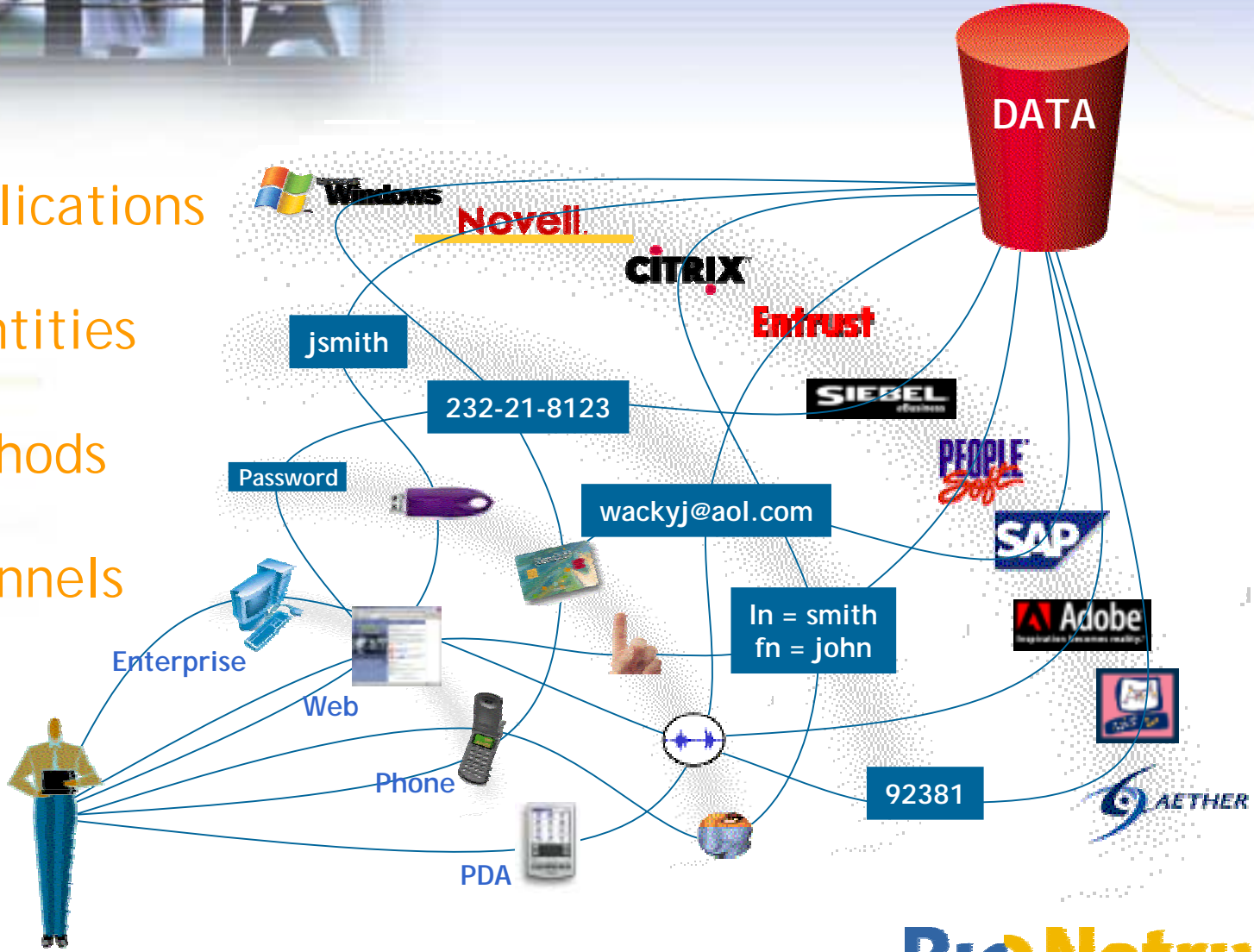
Current Process of Authentication

Applications

Identities

Methods

Channels





Identity Management Definition

- The full set of software-based administration tools for managing the lifecycle of digital user identities
- Contains Web Single Sign-on, Access Control, Personalization and Presentation, Account Management Automation and User Data Integration components
- Intended to maintain a person's complete set of information spanning multiple business contexts, establishing the relationship among these various identities
- Gartner: Will grow from \$2.8 billion in 2001 to \$9.5 billion in 2005, 28% CAGR

Identity Management Space

- **Components**

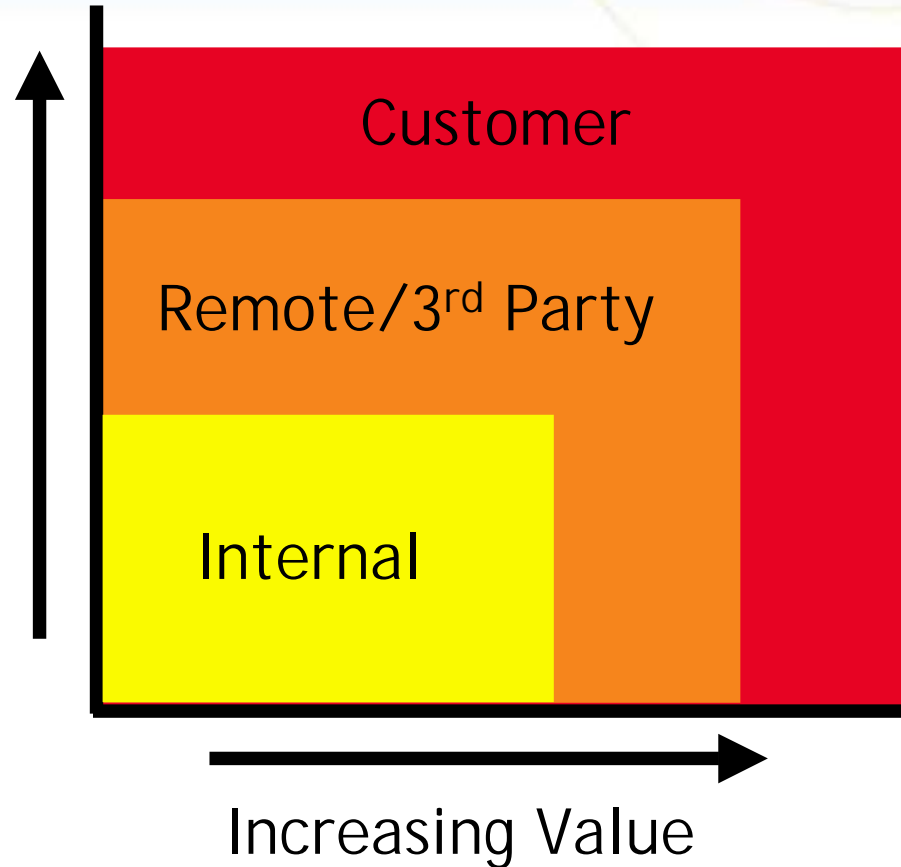
- User Authentication
- Enterprise Information Architecture
- Permission and Policy Management
- Enterprise Directory Services
- User Provisioning
- Identity Management Workflow



Identity Management Landscape

- New business processes/access modes
- External linkages and dependencies
- Market wants MORE options/convenience
- Market wants LESS cost/inflexibility
- Expanded role for unified identity management

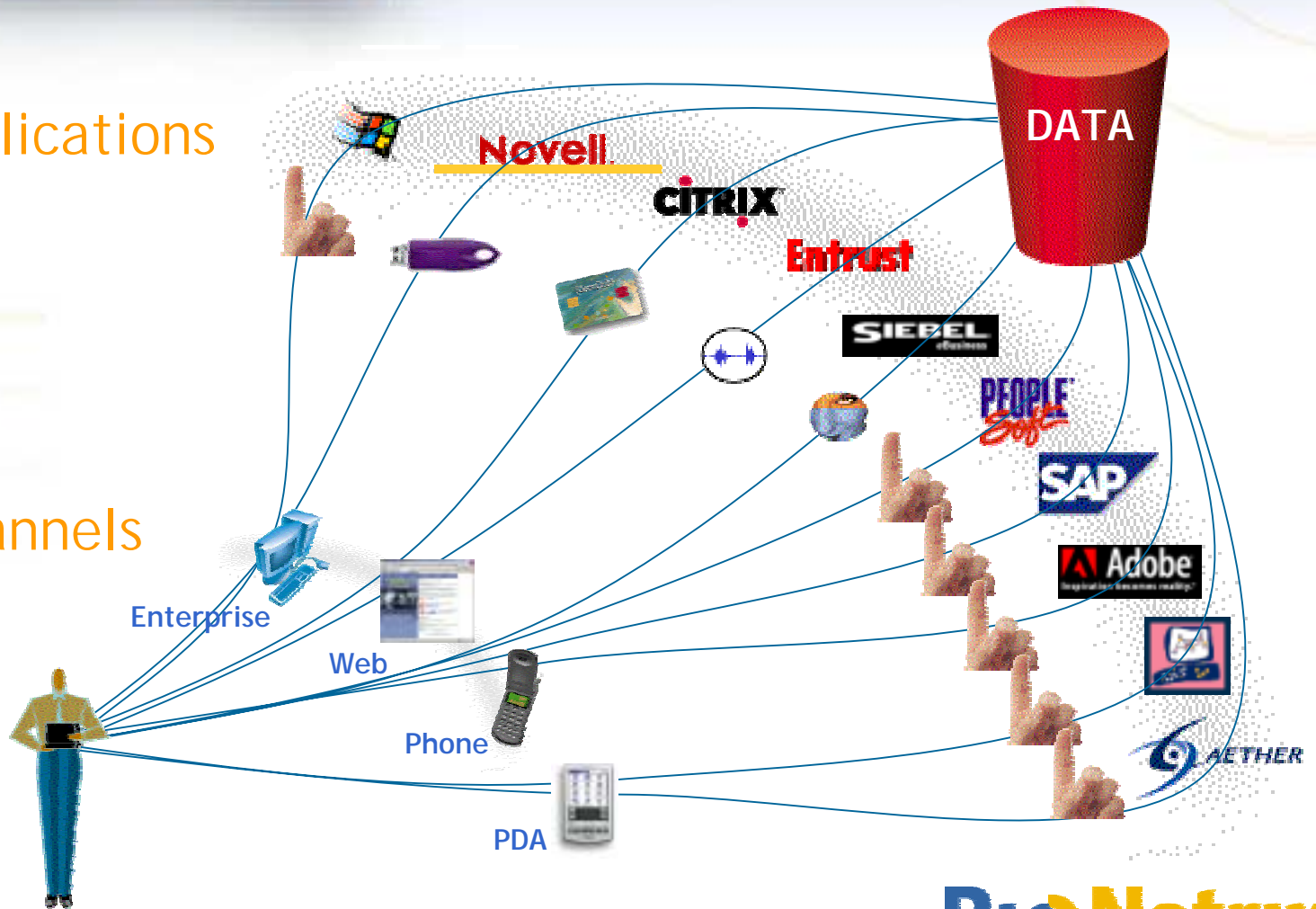
ID Management Disciplines



Strong Authentication

Applications

Channels



BioNetrix™

Security and Convenience



Single Sign-On

- One user ID/password
- Seamless workstation, network and application logon across enterprise and Web resources
- Currently provided by Privilege Management Infrastructure (PMI) authorization vendors
 - Authentication strategy dictated by select partnerships
- Gartner: “Using a Stronger Authentication Method Is Now a Prerequisite to Secure SSO”

Strong Authentication and SSO

Applications

*Intra-Session
Re-Authentication*

Novell

CITRIX

Entrust

DATA

Channels

Enterprise

Web

Phone

PDA

Secure
Single
Sign-On

SIEBEL

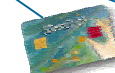
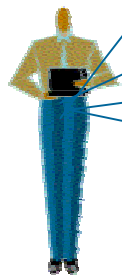
**PEOPLE
Soft**

SAP

Adobe



ETHER



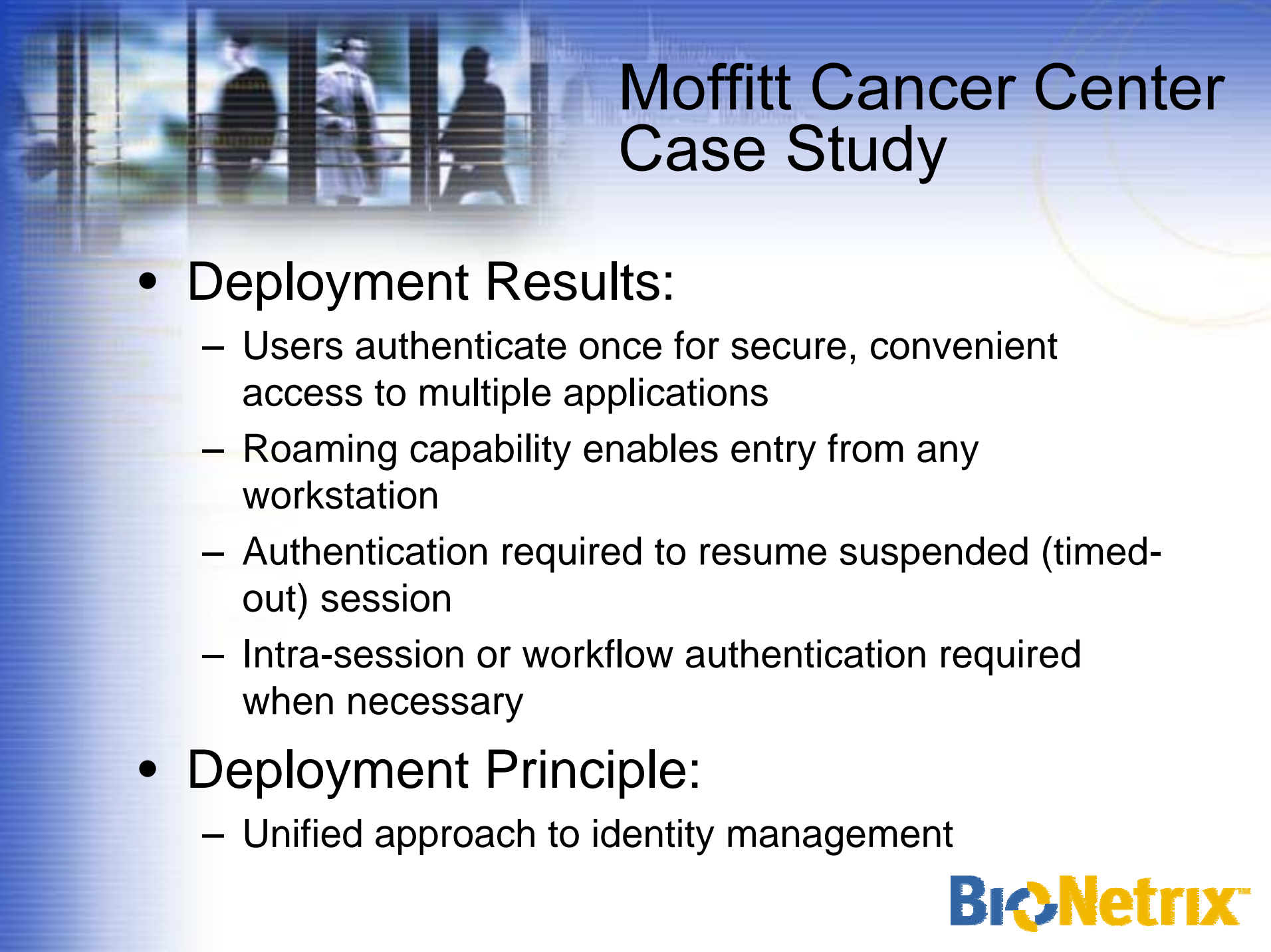
BioNetrix™

Ultimate Security and Convenience



Moffitt Cancer Center Case Study

- Deployed BioNetrix AMI with Single Sign-on for access to clinical applications and patient data
- Drivers:
 - Eliminate costly, time consuming password resets
 - Strengthen security and enhance patient privacy
 - Achieve HIPAA compliance
- Environment:
 - Citrix/NT environment
 - Cerner, SoftMed, Magic, Lawson, First Coast and Epic applications



Moffitt Cancer Center Case Study

- **Deployment Results:**
 - Users authenticate once for secure, convenient access to multiple applications
 - Roaming capability enables entry from any workstation
 - Authentication required to resume suspended (timed-out) session
 - Intra-session or workflow authentication required when necessary
- **Deployment Principle:**
 - Unified approach to identity management

Identity Management Outlook

- Current identity management solutions require – but often assume – a trusted user
- Strong authentication is the key to successful identity management
- Market is demanding an increasingly unified approach, based on conclusive user authentication

