

# Enterprise Directories: A Foundation to Protect and Improve Your Business

Eric Baize  
16 July 2002

Email: [ericbaize@yahoo.com](mailto:ericbaize@yahoo.com)  
Phone: 978-549-3256



## *About the Presenter*

- ✍ Over 12 years of experience in information security and access control
- ✍ Technical and business experience
  - Security architecture, product management & strategy
- ✍ Holder of US patent 6,317,838 on secure Internet access
- ✍ Author of international security standards
  - Co-author of Internet Standard RFC 2478 implemented in Microsoft Windows 2000
- ✍ Frequent presenter to domestic and international security conferences and global 2000 executives
- ✍ Email: [ericbaize@yahoo.com](mailto:ericbaize@yahoo.com)



# *Agenda*



- Concepts and History
- Benefits of a directory based architecture
- Implementing directories in an enterprise
- Conclusion

## *What Is a Directory ?*

### *A Widely Accepted Definition*

- ✍ A specialized database
- ✍ Intended for publication
  - More “Read” than “Write”
- ✍ Shared between multiple applications
- ✍ Highly distributed
- ✍ Can be replicated
- ✍ Easily extendible

*“LDAP isn't a replacement for relational databases (and never will be)”*

**Tim Howes -  
Co-author of the LDAP protocol**



*Specialized Directories Are Designed for a Limited Functionality or a Reduced Number of Applications*

- ✍ DNS (Domain Name Server) for Domain Name and IP address resolution
- ✍ Network Operating Systems
  - Novell Netware 4
  - Microsoft NT 4.0
  - Banyan Vines
- ✍ Mail directory
  - Lotus Notes



## *General Directories Are Dominated by LDAP Based Directories*

### ISO ITU-T X.500

- Perfect but Heavyweight architecture
- e.g: Critical Path, Siemens

### LDAP v3

- Simplified version of X.500
- Dominates the market
- Sun ONE (iPlanet)
- Microsoft Active Directory
- Novell NDS




## *LDAP Directories Are Often Used to Store User Related Information*

- ✍ Easily accessible user information storage
  - e.g. certificates for PKI
- ✍ Can act as an authentication server
  - on Bind operation
  - Password or certificate (LDAP-S)
- ✍ Provide an effective framework for application security but ...
  - Only applicable to LDAP compliant applications
  - Interoperability requires a common schema of data

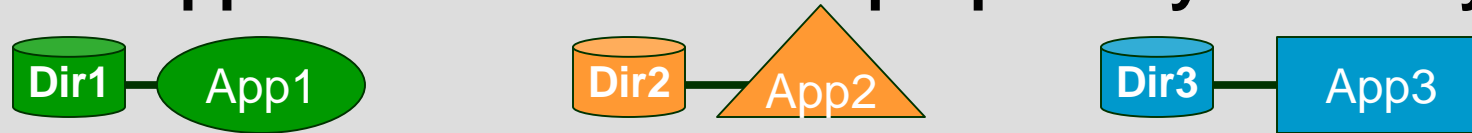


# *Agenda*

- Concepts and History
-  – Benefits of a directory based architecture
- Implementing directories in an enterprise
- Conclusion

## *Multiple Application Specific Directories Increase Costs and Weaken Security*

**Each application has its own proprietary directory**



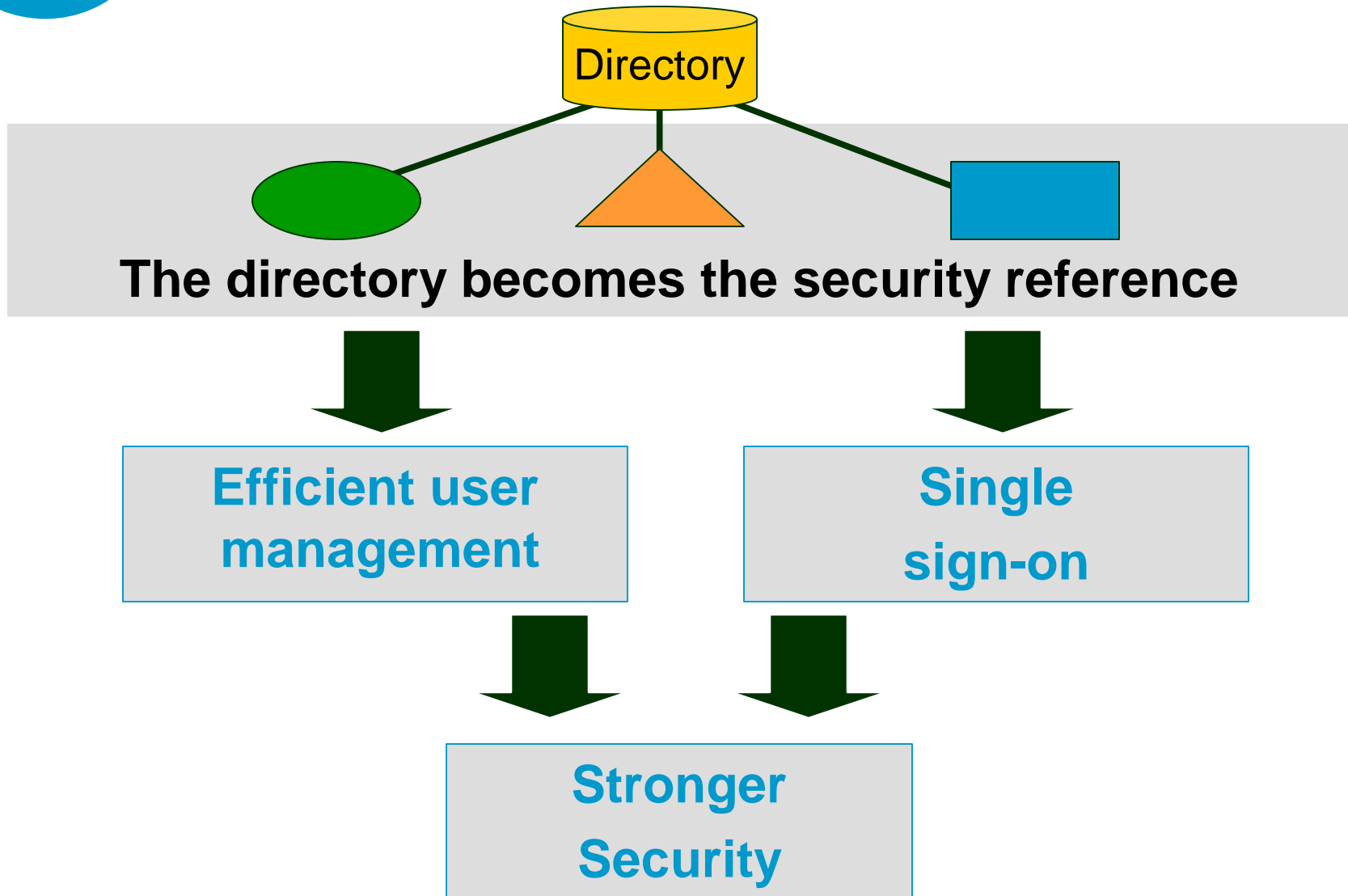
### **Overloads administrators**

- Security is defined by each application administrator
- Limited tracking of user accounts
- Dead accounts are not removed

### **Weakens overall security**

- End-users have too many passwords
- Weak passwords
- Former employees can still access applications
- No coherent access policy

# *A Directory Secures Applications And Streamlines User Administration & Access*



# *An LDAP Directory Enables Efficient User Management for Directory Enabled Applications*

## *Applications*

### *Objectives*

|                                 | <b>Directory enabled applications</b>  | <b>Other applications</b> |
|---------------------------------|--|---------------------------|
| <b>User Management</b>          | <ul style="list-style-type: none"><li>– Users are immediately disabled or enabled</li><li>– Coherent security rules across applications</li><li>– Delegated administration</li><li>– Role based policy</li></ul> | <b>N/A</b>                |
| <b>SSO &amp; Access Control</b> | <ul style="list-style-type: none"><li>– Enforce strong password policy</li><li>– One set of credentials to remember</li><li>– No access control enforcement</li></ul>  | <b>N/A</b>                |

*An LDAP Directory Enables Efficient User Management for Directory Enabled Applications*


*Applications*

*Objectives*

|                                 | <b>Directory enabled applications</b> | <b>Other applications</b> |
|---------------------------------|---------------------------------------|---------------------------|
| <b>User Management</b>          | <b>100%</b>                           | <b>0%</b>                 |
| <b>SSO &amp; Access Control</b> | <b>50%</b>                            | <b>0%</b>                 |



# *Agenda*

- Concepts and History
- Benefits of a directory based architecture
-  – Implementing directories in an enterprise
- Conclusion

*In Most Large IT Environments, All Applications Cannot Easily Interface With a Directory*

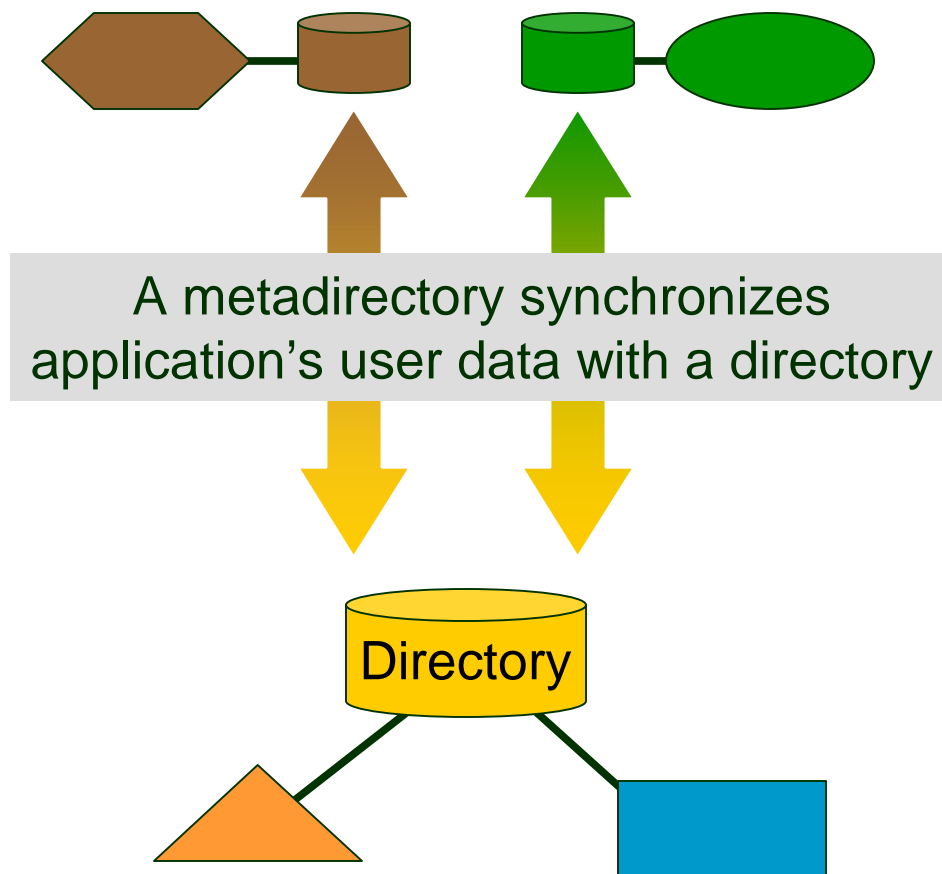
**Directories help enforce a strong security policy across several applications**

**Enabling technology is required to extend directory benefits to all applications**

**Some applications cannot benefit from a directory:**

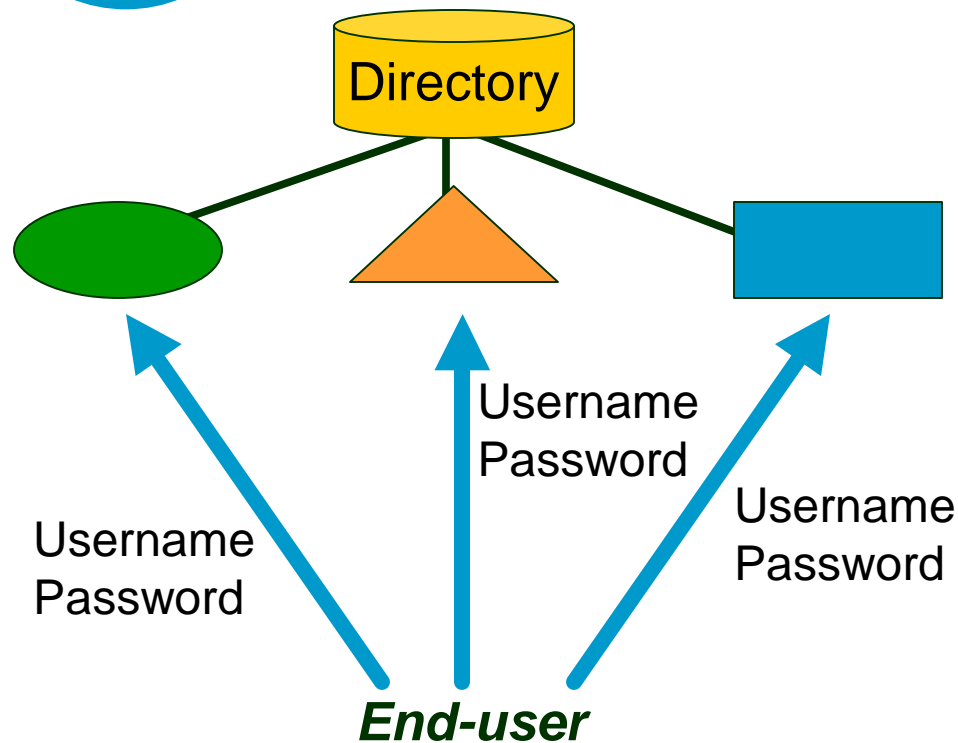
- Technical incompatibility
- Cost concerns: Migration of local information into a directory would be too expensive

# *The Metadirectory Extends Directory-based Security Management to All Enterprise Applications*



- ✍ Synchronizes changes in user status across all applications
  - Email, database, ERP...
- ✍ Extension of directory benefits across multiple applications
  - End to end business oriented user management
- ✍ Vendors: Microsoft, Novell, Sun (iPlanet), Critical Path

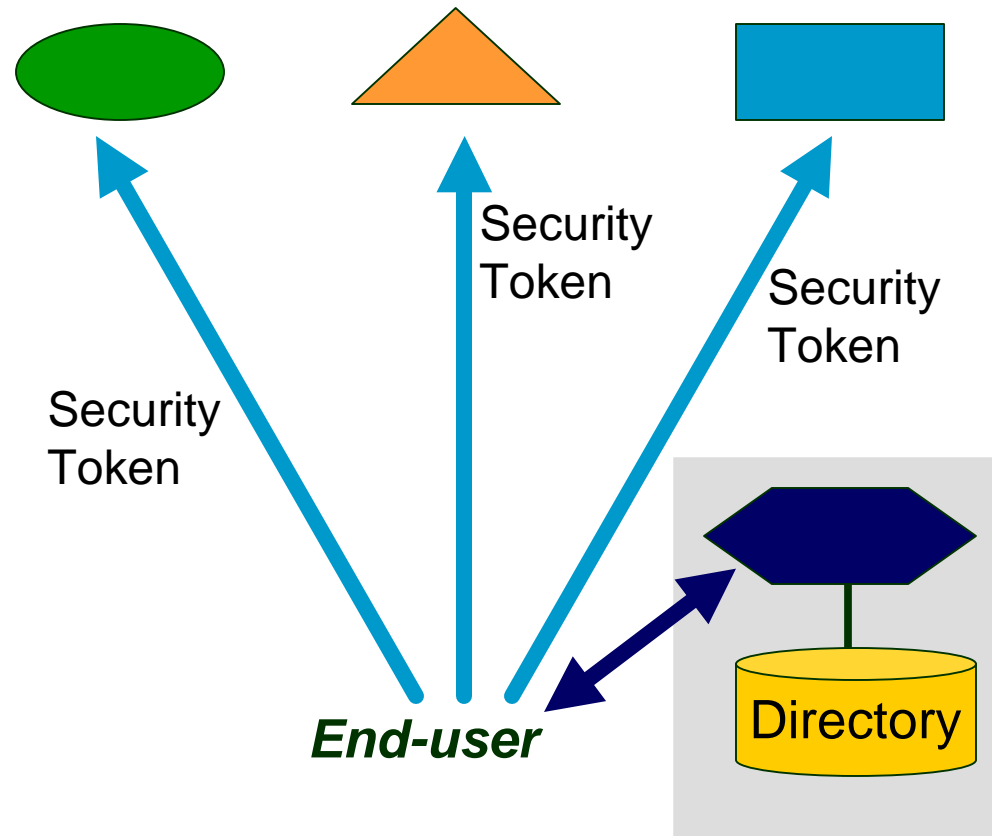
*With a Directory, End-users Have to Re-enter the Same Username and Password for Each Application*



A directory unifies user name and password across directory enabled applications but ...

- ✍ Directories do not maintain an authentication session across LDAP enabled applications
- ✍ End-users have to retype user name and password at each different application access

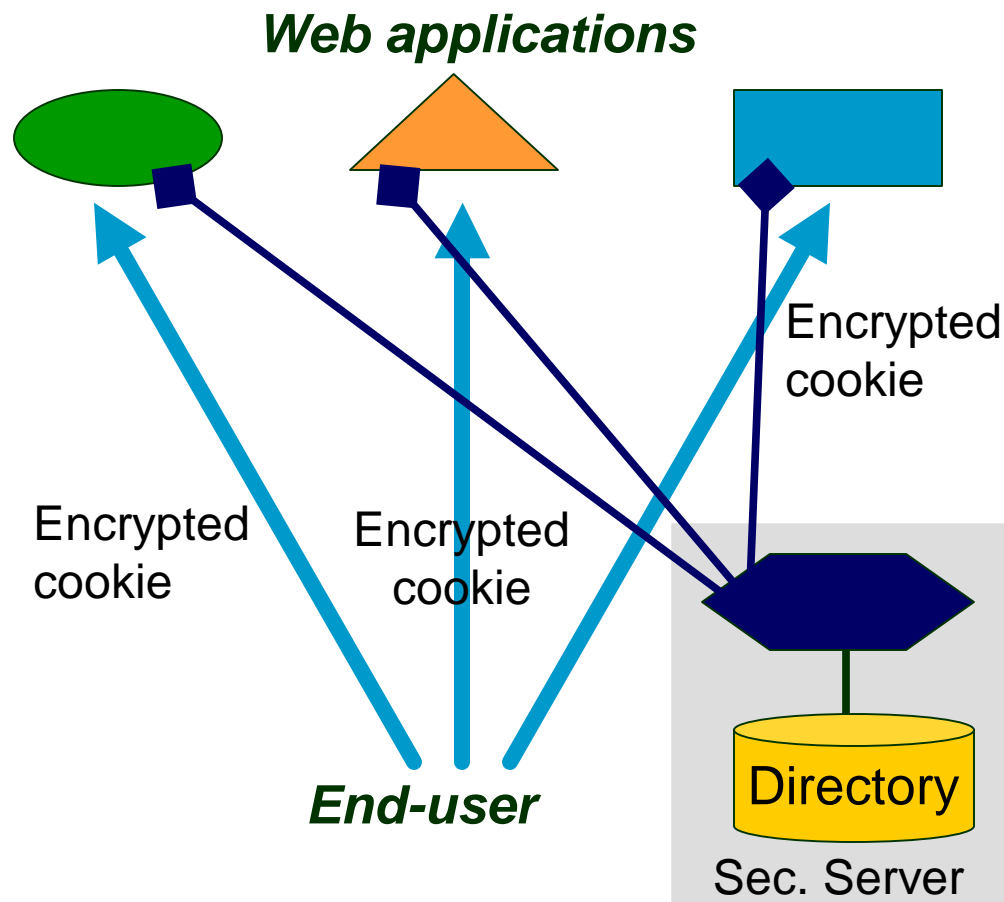
## *A Distributed Authentication Framework Maintains a Single Directory Based Authentication Across Applications*



Authentication is performed by an independent entity - Security sessions are maintained through encrypted token

- ✍ Examples: Kerberos, PKI
- ✍ Web access control
  - Agent based architecture
  - Proxy based architecture
- ✍ Also provides access control and communication encryption
- ✍ Only applies to “token aware applications” e.g.
  - Certificate based
  - Kerberos based
- ✍ Legacy SSO products are required for full SSO
  - Passlogix, Evidian

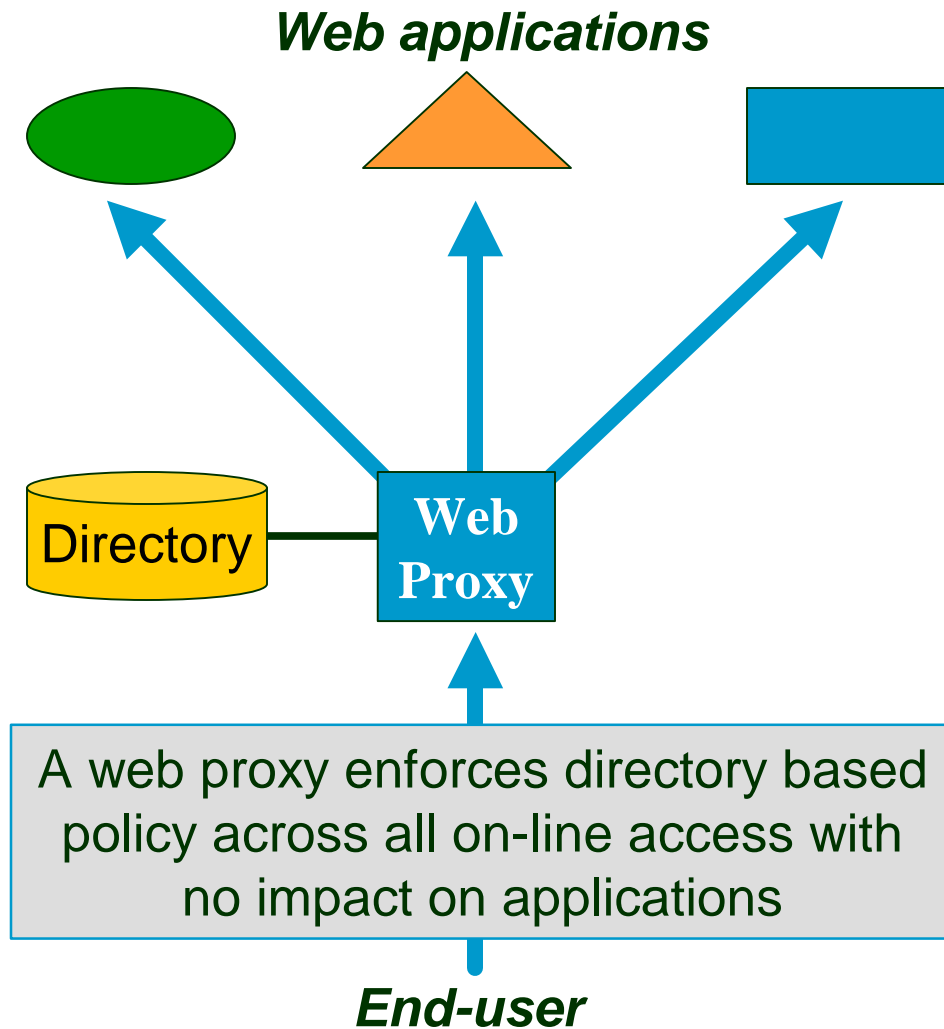
## *Agent Based Web Access Control Products Enforce Access Control and SSO Across Web Enabled Applications*



Agent on applications enforce security with a directory based security server

- ✍ Examples: Netegrity, RSA/Security, Oblix
- ✍ Enforce directory based access control policy to Web applications
- ✍ Provide SSO
- ✍ Agents are deployed on secured applications
- ✍ Security session is maintained through an encrypted cookie
- ✍ Also provide communication encryption

## *Proxy Based Web Access Control Products Enforce Directory-based Security Policy With No Impact on Applications*



- ✍ Examples: Apache, Microsoft, Evidian, Netegrity
- ✍ Extend directory benefits to web access
  - Web proxy enforces directory rules for all web access through the portal
  - No change in the applications
  - Often coupled with a firewall
- ✍ Add strong security features
  - Worm and virus protection
  - Internet traffic encryption

# A Directory Alone Is Not Enough

Web applications

Applications

Objectives

|                      | Directory enabled applications | Other applications  |
|----------------------|--------------------------------|---------------------|
| User Management      |                                | Meta Directory      |
| SSO & Access Control |                                | Legacy SSO products |


Web Access Control

Distributed Authentication Framework



# *Agenda*



- Concepts and History
- Benefits of a directory based architecture
- Implementing directories in an enterprise
-  – Conclusion



## *Summary*

- ✍ A directory is intended to publish and share information across applications
  - A directory is not a replacement for a relational database
- ✍ A directory is a first step towards enforcing enterprise-wide security policy
  - Helps simplify administration and improve security
  - Ideal for new applications
- ✍ Directory alone are not enough - Enabling technology is required:
  - For non directory enabled applications
  - To enforce access control and SSO

**Policy specification and enforcement are not technology issues and remain the critical success factors of a directory based policy project**



## *References*

- ✍ LDAP: Use as Directed by Tim Howes  
(Network Magazine)
  - <http://www.networkmagazine.com/article/DCM20000502S0039>
- ✍ Understanding and Deploying LDAP Directory Services, T.A. Howes, M.C. Smith, G.S. Good