SpyLogix for
Active Directory
Data Sheet

IDENTITYLOGIX™

Enhanced Visibility and Operational Security Awareness for Active Directory

HIGHLIGHTS

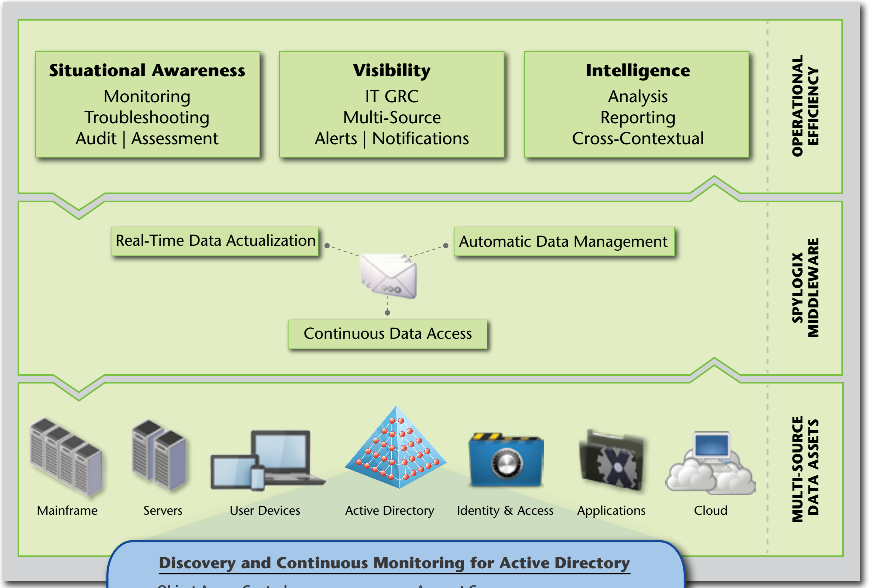
- **Security Intelligence**
  - Situational Awareness
  - Enhanced Visibility
  - Object Analysis and Reporting
    - Accounts | Identities
    - Objects | Attributes | Permissions
    - Privilege Governance
- **Continuous Data Access**
  - By API (no reliance on logs)
  - SpyLogix Message Design
- **Communication Services**
  - Message Broker
    - Multi-platform
    - Message Store/Forward
    - Message Mirroring
    - 1:Many Routing
  - Message Streaming
  - Web Services (data in)
- **Automatic Data Management**
  - Intelligent Data Handling
  - Historical Database
  - LINQ/Odata Enabled
- **Real-Time Data Actualization**
  - ActionLogix™
    - Policies
    - Alerts | Notifications
    - Event Synthesis
    - Message Forwarder
    - Extensibility Layer
  - Web Services (data out)
  - Report Scheduler
  - Interactive Console
    - Data Query and Filter
    - Data Analysis
    - Reports
    - Data Export | Sharing
- **SpyLogix Enterprise**
  - SpyLogix Platform
  - SpyLogix Modules
    - User Security
    - Active Directory
    - Windows Server
    - VMware vSphere
    - Microsoft FIM 2010
    - LDAP Directory
    - CA SiteMinder
    - Radiant Logic
    - IdF Gateway (IBM System z and i)
    - Module SDK

SpyLogix for Active Directory is a module that provides agent-less discovery and continuous monitoring of Microsoft's Active Directory Domain Services. Active Directory is the central location for configuration information, authentication requests, and information about all of the objects that are stored within your forest for securing user access to enterprise business information. Using SpyLogix for Active Directory this ubiquitous security control point may be efficiently and effectively managed   Complete visibility and accountability for security provided by Active Directory is simplified and substantially enhanced with SpyLogix for Active Directory module and it's prerequisite SpyLogix Platform server.

Primary features of Microsoft® Windows server security model include user authentication and access control. Active Directory is a primary user entry point and ongoing authorization security control point for accessing network shared resources and enterprise information systems; it is a resource that helps administrators effectively manage these features easily and efficiently. Active Directory is flush with capabilities for security control, which gives rise to much complexity.

Complexity introduces security exposures without clear visibility for current users and access privileges inside Active Directory. Along with user authentication, administrators are allowed to control access to resources or objects on the network. To do this, administrators assign security descriptors to objects that are stored within an advanced inheritance model in Active Directory. While tools are available to analyze Active Directory, they are cumbersome for viewing object security settings and lack a broader perspective.

An enterprise depends on Active Directory for managing its information-driven business. SpyLogix for Active Directory provides industry-leading robust security information natively from Active Directory; working in conjunction with its prerequisite SpyLogix Platform server, SpyLogix provides an efficient and effective means to continuously monitor and on-demand audit Active Directory without reliance on log data or log data settings. SpyLogix is an essential tool for enabling continuous information governance, risk control, and compliance initiatives.



Discovery and Continuous Monitoring for Active Directory

Object Access Control
- **All Objects | Attributes | Permissions**
  - Periodic Baseline
  - Continuous Change Tracking
- **Security Descriptors (ACL)**
  - DACL | SACL
  - ACE Enumeration
  - 0 vs. NULL DACL Delineation

Common Object Types
- User | Group | OU
- File | Shared Folder
- Computer | Server | Printer

Account Governance
- Orphaned Accounts
- Administrative Accounts
- Power | Remove Users

Security Principal Governance
- Who owns an object?
- Who can access it and in what way?
- What types of access are audited?

Security Service Process Enablement
- Orphaned Account Vigilance
- Least Privileges Analysis | Monitoring
- Privileged User Management

OVERVIEW

SpyLogix for Active Directory is a module for continuously monitoring (for changes) Active Directory agent-lessly and with no reliance on physical log data. An on-demand discovery feature creates a baseline to which all changes may be compared.

Security data may be used to assist with account governance tasks such as orphan, administrative, power/remote user account management. Security service process enablement for least privilege analysis or privileged user management initiatives. Detailed security principal governance enables answers to questions such as:

- Who owns an object?
- Who can access it and in what way?
- What types of access are audited?

SpyLogix Platform server is prerequisite software that enables enterprises to efficiently and effectively use natively acquired the data. *(See SpyLogix Enterprise for a more information.)*

- Native Data Access
- Advanced Communications Services
- Automatic Data Management
- Real-Time Data Actualization

Native Data Access

The SpyLogix Module is component provides for on-demand discovery and continuous monitoring of Active Directory data used to control access to Windows family resources.

Security data includes object access control, such as:

- All Objects | Attributes | Permissions
- Security Descriptors (object ACL)
  - DACL | SACL
  - ACE Enumeration
  - 0 vs. NULL DACL Delineation
- Common Object Types
  - User | Group | OU
  - File | Shared Folder
  - Computer | Server | Printer

All data is mapped into standardized well-formed messages for subsequent treatment.

Note that it is possible for a security descriptor to have no DACL (also known as a NULL DACL); this gives unconditional access to everyone. A security descriptor with an empty DACL gives no access to anyone.

In Windows NT, allowing everyone unconditional access to an object would necessitate object creation with a NULL DACL — that is, without a DACL. In Windows 2000 and later, it is still possible to create objects with a NULL DACL, but code that does this must set the SE_DACL_PROTECTED security descriptor control flag to prevent the object from acquiring a DACL through inheritance. In the worst case, forgetting to protect a NULL DACL can result in an empty DACL if the parent object has no inheritable permissions. The result would be to allow no access to anyone, exactly the opposite of what the object's creator intended.

Best practice is not to use NULL DACLs at all. If you are developing for Windows 2000 or later and want to give everyone unconditional access to an object, create a DACL with one ACE that grants Everyone full control. In Windows Server 2003, the Everyone group no longer includes Anonymous Logon; therefore you might also want to include a second ACE that grants Anonymous Logon full control.

SpyLogix for Active Directory will enable granular object ACL on-demand audit and continuous monitoring to ensure proper security policy is maintained.

Communications Services

The communicaton services component safely and efficiently communicates messages from SpyLogix for Active Directory to Data Management and Actualization layers of SpyLogix Platform for advanced processing and use. See SpyLogix Enterprise web pages and data sheet for more details.

Automatic Data Management

The automatic data management component processes all messages to eliminate burdensome IT staff work and improve "time-to-value" when managing diverse security data. Well-formed messages are 100% parsed. A Translator feature may be invoked to automatically change non-human readable data types into human readable form. All data types are supported. Parsed or translated data with identifying meta-data is passed to the Data Engine feature, a high performing component that ensures all data types are persistently recorded non-redundantly with proper date/time context. Data is assessable via the included Interactive Console feature or any Odata compatible query tool such as PowerPivot for Excel 2010.

The following examples illustrate the Translation feature and is a sample of SpyLogix User Account Control pre-processing:

SpyLogix UAC Event	AD Reported	Event Description
UAC: Script Executed	0x00000001	Logon script executed
UAC: Account Disabled	0x00000002	User account is disabled
UAC: Lockout	0x00000010	Account currently locked out
UAC: Interdomain Trust Account	0x00000800	Account from a trusted domain
UAC: Smartcard Required	0x00040000	user log on requires smart card

The following is a sample of object ACL pre processing performed by translating ACE bitmasks into discrete SpyLogix fields.

SpyLogix Permission	ACE Bitmask Description
Delete	The right to delete the object
CreateChild	The right to create children of the object
DeleteChild	The right to delete children of the object
ReadProperty	The right to read properties of the object
WriteDACL	The right to modify the DACL in the object Security descripton

The real-time data actualization component includes features that enable efficient leverage of messages and persistently recorded security data, effectively making all security data actionable and useable by people, processes and technologies.

ActionLogix™

ActionLogix is a series of features provided to process messages and invoke pre-programmed actions.

- **Policy Engine** feature uses rules to filter all messages for specific data. Identified message data may then use the ***alerts | notifications*** feature to write to email, RSS message or any text dissemination method.
- **Plug-in** feature is provided for taking dynamic programmatic actions to remediate uncovered issues.
- **Synthesizer** feature synthesizes events by dynamically translating message data re-saving an event that is human readable. For example, SpyLogix detects when the ***Last Login Time*** attribute changes and re-saves the message data as a "Logon" event in the database.

The following is a sample of how new events are recorded and illustrates simplification of user events by SpyLogix:

SpyLogix Simplification	***Audit Data Conditions***
Bad Password	if badPwdCount changed and badPasswordTime changed
Logon	if logonCount changed and lastLogon changed
Password Reset	if pwdLastSet changed

Active Directory identity object changes are not easily detected through logged events. SpyLogix simplifies these object changes.

The following is a sample of how Active Directory synthesizes identity events recorded by SpyLogix's postprocessor that are derived from a single AD edit operation by an administrator:

SpyLogix Identity Events	
User Created	User Deleted
User Added to Group	User Removed from Group
Group Created	Group Deleted
Group Added to Group	Group Removed from Group

NOTE: ***SpyLogix synthesized events would not appear in AD log data.***

- **Message Forwarder** feature selectively forwards messages to one or more SpyLogix servers. This feature is helpful for using data effectively with remote support teams or managed cloud service providers.

The following Data Actualization features are included to effectively use out-of-band persistently recorded security data:

Web Services

The Web Services feature provides an easy to use interface for sharing data with other software tools or information security processes.

Interactive Console

A graphical console enhances security intelligence by providing clear visibility into the complex security controls deployed in Active Directory. An easy-to-use tool is provided for data query, analysis, and reporting to share with management or other interested parties. Favorite data views may be saved and recalled for later re-execution.

Any Odata compatible tool may be used to query, view/analyze or report on recorded data, such as PowerPivot for Excel 2010 or SharePoint.

Scheduler

This feature generates reports from saved views in the background.

Additionally any generated output may be made to be managed by SpyLogix using the Module SDK and the Scheduler feature. For example, network security assessment tools or scripts may be scheduled and resulting output data managed using SpyLogix Enterprise.

SUMMARY

IdentityLogix for Active Directory enables:

- Fast and easy security intelligence
- Historical reference for identity & access management data
- Automatic data management to maximize efficiency
- Real-time data actualization to effectively leverage data