SpyLogix
ENTERPRISE
Data Sheet

IDENTITYLOGIX™
Continuous Security Intelligence and Real-Time Data Actualization for Enterprise Information Assurance

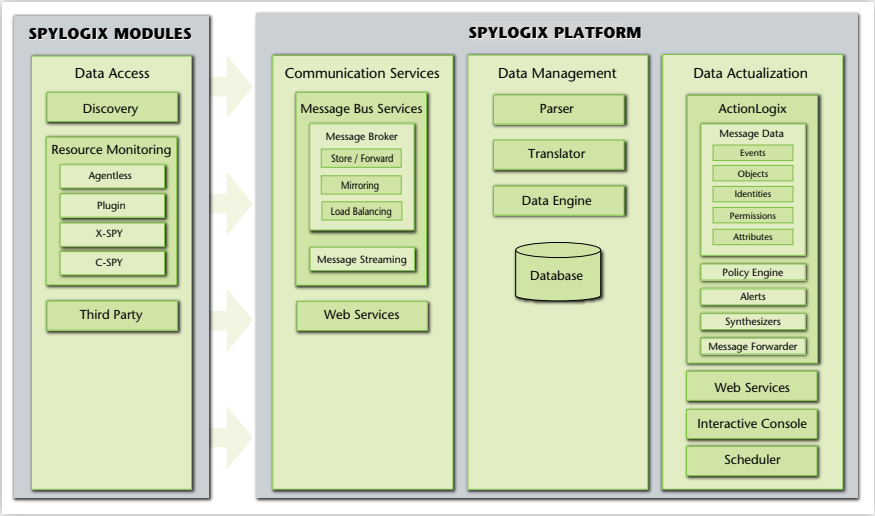
HIGHLIGHTS

- **Continuous Security Intelligence**
  - Information Security Visibility
  - Identity Intelligence
  - Activity Monitoring
- **Automated Data Management**
  - Message-Based Design
  - Intelligent Data Handling
  - Historical Database
- **Real-Time Data Actualization**
  - Policy Engine
  - Alerts
  - Event Synthesis
  - Message Forwarder
  - Report Scheduler
- **Interactive Console for Data**
  - Query
  - Analysis
  - Reporting
- **SpyLogix Enterprise**
  - SpyLogix Platform
  - SpyLogix Modules
    - User Security
    - Active Directory
    - Windows Server
    - VMware
    - Microsoft FIM 2010
    - LDAP Directory
    - CA SiteMinder
    - Radiant Logic
    - IdF Gateway (IBM System Z and i)
    - Module SDK
- **Operating Environments**
  - SpyLogix Platform:
    - Windows Server 2003, 2008 and 2008 R2 (recommended)
    - Windows XP or W7
  - SpyLogix Modules:
    - Modules run on Windows Server 2003, 2008 or R2
    - Optionally, modules run on Windows XP or W7
    - Modules supporting sources hosted on Windows, Linux, UNIX may require an included cross-platform client

SpyLogix Enterprise is security middleware for simplifying continuous management and control of enterprise information security employing enhanced visibility and data actualization. Benefits include improved IT process efficiency and staff effectiveness. SpyLogix Enterprise is comprised of SpyLogix Platform with companion SpyLogix Modules. Now a single enterprise security intelligence system can support IT GRC, real-time data for forensics, and trending analysis and can be used as a powerful administrative tool needed for quick and accurate issue resolution.

SpyLogix Platform organizes data collected or streamed from multiple enterprise sources simultaneously to form a security intelligence and data actualization system for enhanced threat responsiveness and process quality.

SpyLogix Modules are companion software technologies that provide continuous multi-sourced security data to SpyLogix Platform in a standardized way to facilitate security data processing automation.



SpyLogix organizes and leverages data from any data source, such as:

- User end-points
- Directories
- UNIX/Linux
- IBM System Z
- Web Applications
- Business Applications
- Virtualized Servers
- Windows Server folders and files
- AS400 / iSeries / System i
- Databases
- Identity & Access Management systems
- Cloud based application systems

SPYLOGIX ENTERPRISE OVERVIEW

SpyLogix Enterprise is designed to efficiently organize and effectively use enterprise access control and activity data. Security data is continuously streamed directly from each source to a central server for real-time processing. For example, data from user login/logoff activity, identity system discovery or changes, and application activity is easily handled. A message based design enables automatic continuous data management and actualization for information security threat detection and remediation, troubleshooting, electronic forensics, and IT governance, risk control and compliance enablement.

Today multiple tools are used to obtain enterprise security data – mostly involving management of log files. These solutions can be too narrowly focused, expensive, time consuming to support, and can miss key trends or activities. Finding the right security information can be "like trying to find a needle in a haystack." Lack of information timeliness or lost context can result in missed opportunity or improper business data use.

Enterprise information security (IS) visibility is enhanced by continuous direct monitoring of resources and real-time actualization of data. Business and IT staff tasked with IS governance, risk control, and compliance responsibilities can execute efficiently and improve operational control over business information access.

SPYLOGIX ENTERPRISE COMPONENTS

Data Access technologies are designed to centrally acquire, map, and send security data in a standardized way to SpyLogix Platform for processing. SpyLogix Modules acquire security data from any programmatically accessible enterprise source using the most direct and effective means possible. Security data is mapped into a standardized message format, and then communicated efficiently and safely for automatic processing by one or more SpyLogix Platform Server(s).

Individually, SpyLogix Module technologies compromising Data Access may be described as:

Discovery Modules are used to pro-actively create a baseline of security data to which monitored changes may be subsequently compared.

Resource Monitoring technologies are designed to continuously collect data form IT sources:

Agent-less monitors consume source data fed over a network connection;

Plug-in monitors query a resource, then consume source data fed over a network connection;

X-SPY monitors are designed to accept source data fed at high rates from an efficient and high-capacity cross-OS (Windows, Linux and UNIX) universal companion agent;

C-SPY monitors are specially designed to accept Windows OS security data from a proprietary client agent, including qualified user logon and logoff events, Event Viewer events, program executables, and LDAP API invocations. The C-SPY agent is highly extensible for customized end-point monitoring tasks.

3rd Party monitors may be customized to consume data from any 3rd party source.

Communication Services are available for safely communicating well-formed messages to the Message Services layer. Message Streaming efficiently moves messages to the Data Management layer for persistent storage. Message Handling process incoming messages employing either SpyLogix binary protocol or XML format; it automatically supports safe mode delivery of messages over less-reliable networks. Web Services (data in) interface is provided to easily send external data into SpyLogix Platform. Threading enables higher SpyLogix Platform throughput when utilizing multi-CPU servers.

Data Management processes all incoming message data. Well-formed messages are 100% parsed. Selectively, Translator may be invoked to automatically change non-human readable data types into human readable form. All data types are supported. Parsed and translated data with complete meta-data is passed to the Storage Engine, a high performing component that ensures all data types are persistently recorded non-redundantly with proper date/time context.

Data Actualization provides multiple post-storage processing services to effectively use incoming messages in real-time:

ActionLogix™ is a series of components used to automatically analyze (filter) message content and trigger an action (see Alerts), synthesize events or forward messages to another SpyLogix Platform(s):

Policy Engine Policy Engine employs configurable programmatic logic gate (PLGs) incorporating Boolean logic or Python scripts to automatically process message data. PLG deployment is expedited using message meta-data, including: basic, state, RBAC, and utility. Any message passing PLG processing may trigger an action, for example, generate an Alert.

Basic (by meta-data tags)	State (by object state)	RBAC (by identity)	Utility
Service Name	Added	RBAC added	Counter
Service Category	Moved	RBAC Deleted	Timer
Event Class	Modified	RBAC Added to	
Object Class	Deleted	RBAC Deleted From	
Object Name	None		
Identity			
Time			
Location			
Attribute (new)			
Attribute (old)			

Alerts are embellished messages generated by blending standardized text with selected message data passing the Policy Engine rules, and then written to email, RSS, net send, a file, an application, Windows Event Log or SQL database. New output targets may be easily added.

Synthesizers are Module-specific events that are generated by analyzing message payload, drawing measured conclusions and re-storing a synthesized event persistently.

Message Forwarder communicates intact well-formed messages to another network-connected SpyLogix Platform. This capability is appropriate for cloud computing infrastructures or distributed SpyLogix Platform message aggregation for security data mining or monitoring purposes.

Web Services (data out) provides as easy to use interface for sharing data with other software or IT processes.

Interactive Console enhances security intelligence visibility through an easy to use tool for data query, analysis, reports and sharing within collaborative workgroups.

Scheduler generates Interactive Console reports in the background. Additionally, network security assessment tools or scripts may be scheduled for Data Management and Actualization.

SpyLogix Enterprise is an innovative software technology for continuous management of enterprise security data.

For more information or to learn more about SpyLogix Enterprise, please visit
www.identitylogix.com

IDENTITYLOGIX™ 9800 Connecticut Drive, Crown Point, IN 46307 ■ +1.219.379.5560 ■ info@idenitylogix.com

v1.10_10/2011