SpyLogix
ENTERPRISE
Data Sheet

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

HIGHLIGHTS

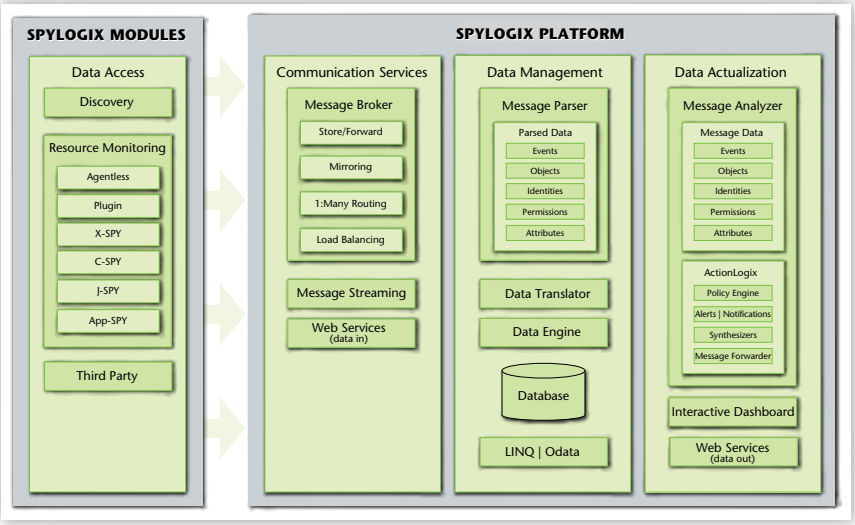
- **Security Intelligence**
  - Enhanced Visibility
  - Situational Awareness
  - Analysis, Visualization and Reports
- **Continuous Data Access**
  - Native Data Access (by API)
  - SpyLogix Message Design
- **Communication Services**
  - Message Streaming
  - Message Broker
    - Multi-platform
    - Message Store/Forward
    - Message Mirroring
    - 1:Many Routing
  - Web Services (data in)
- **Automatic Data Management**
  - Intelligent Message Parser
  - Historical Data Storage
  - LINQ/Odata Enabled
- **Real-Time Data Actualization**
  - ActionLogix™
    - Policies
    - Alerts | Notifications
    - Event Synthesis
    - Message Forwarder
    - Extensibility Layer
  - Interactive Dashboard
    - Data Query and Filter
    - Data Analysis
    - Data Visualization
    - Reports
    - Data Export | Sharing
  - Web Services (data out)
- **SpyLogix Enterprise**
  - SpyLogix Platform
  - SpyLogix Modules
    - CA IdentityMinder
    - CA SiteMinder
    - IdF Gateway (IBM System z and i)
    - LDAPv3 Directory
    - MS Active Directory
    - MS FIM 2010
    - MS User Security
    - MS Windows Server
    - RadiantOne VDS
    - Sun Java System Directory Server
    - VMware vSphere
    - Module SDK

SpyLogix Enterprise is a new paradigm for simplifying and enhancing enterprise information security management and control. Digital security assets are continuously monitored using SpyLogix Enterprise "security middleware" services. Efficient management of enterprise security data is realized through standardization, centralization and automation approaches for lowering costs, saving time and improving information security effectiveness. Multi-sourced native data are collected into standardized messages, centralized for employing automatic data management, and readied for proactive analysis in real-time via provided services.

Benefits include improved "time-to-value" for people working to keep business information safe, more efficient IT service processes, and less technology complexity to boost staff effectiveness. Now a single enterprise security intelligence system can support enterprise security monitoring, real-time data for forensics, trending analysis and can be used as a powerful operational tool for quick and accurate issue resolution.

SpyLogix Modules provide continuous multi-sourced enterprise security data access and communication to one or more SpyLogix Platform server(s) in a standardized way, which facilitates automated centralized middleware services.

SpyLogix Platform servers offer middleware services for processing message data streamed from SpyLogix Modules interfacing with enterprise sources, forming an effective security data intelligence and actualization system that enhances threat responsiveness and process quality.



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 security data characterized by variety, volume, and velocity. Variety of security data comes from lack of standards in the way identity, access management and application activity data are defined and stored. Volume of security data grows exponentially as demands of business processes expose sensitive information online. Velocity of enterprise security data increases as the sources and types of security data streams (i.e access management, performance data, etc.) evolve to maximize leverage of information for proper business advantage.

SpyLogix is designed to assist enterprises with efficient management and effective use of multi-sourced security data from users, identity systems, file and application systems. Activity and identity and access management data are continuously monitored directly (using native APIs) from accessible digital asset sources to a central server for automatic and real-time processing. For example, data from client domain logon/logoff activity, user access rights, historical object permission changes, and application events are easily managed for advanced analysis or shared with enterprise IT security processes.

Business and IT staff tasked with keeping business information safe benefit by improved management/control, timely troubleshooting, insightful operational monitoring, risk mitigation with 360° visibility and enhanced compliance support.

SPYLOGIX ENTERPRISE KEY COMPONENTS

SpyLogix Modules for Continuous Data Access

Source specific Data Access modules are designed to continuously centralize data from multiple disparate information security resources to SpyLogix Platform. Data Access modules provide capabilities including:

Discovery of objects managed by monitored resources on-demand for pro-actively maintaining a true data baseline from which changes may be readily detected and compared.

Resource Monitoring using available native vendor APIs is provided for detecting object or data changes by employing:

- **Agentless** modules that interface with source data accessible via a network connection by "subscription" or proactive query.
- **X-SPY** modules that are cross-OS (Windows, Linux and UNIX) and designed for efficient, direct integration with high-capacity sources.
- **J-SPY** modules are designed to integrate with JAVA environments.
- **App-SPY** modules enable developers to manage application events.
- **C-SPY** module is designed to collect Windows OS client or server user activity, such as user logon and logoff events.

Third Party modules enable vendors to leverage SpyLogix capabilities for application events, network security report output or any 3rd party security data input.

Data Access modules all employ a standardized approach for collecting data from native APIs into well-formed messages that are continuously sent to one or more centralized SpyLogix Platform server(s) using existing enterprise network communication services.

SpyLogix Platform Communication Services

Communications Services components leverage today's enterprise networks for effectively centralizing messages. Data is safely communicated in standardized, well-formed messages from multiple SpyLogix modules which are continuously consumed and processed by SpyLogix Platform servers in real-time employing:

- **Message Streaming** mode designed for efficiently moving messages continuously over high-speed enterprise networks.
- **Message Broker** communications for data store/forward, mirroring, 1:many routing or load balancing. All these features include optional safe delivery of messages over less reliable networks, enable high-availability configurations or cloud-based managed service delivery.
- **Web Services (data in)** easily facilitating external data input from applications, unmanaged network security output reports or any IT service process.

SpyLogix Platform Automatic Data Management

Data Management components automatically processes all incoming messages. Message data is parsed, selectively translated and smartly stored.

- **Parser** feature automatically parses all data types.
- **Translator** feature may be selectively invoked to automatically change non-human readable data types into human readable form.
- **Data Engine** feature persistently records parsed data with date/time context.
- **LINQ/Odata** service makes recorded data accessible to the Interactive Dashboard, PowerPivot for Excel 2010 or Odata compatible business intelligence (BI) tools.

SpyLogix Platform Real-Time Data Actualization

Data Actualization components provide real-time services for leveraged data query, analysis and sharing with enterprise IT service processes. Real-time data services improves IT service quality, "time-to-value" and process efficiency.

ActionLogix™ is a series of widgets that analyze streaming messages in real-time, and then trigger configurable programmatic actions.

- **Policy Engine** employs configurable policies that monitor streaming messages in real-time. Policy development expedited using a graphical interface and exposed message meta-data properties including:

Basic Filters (by meta-data tags)	State Filters (by object state)	RBAC Filters (by identity)	Utility Filters
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 | Notifications** are embellished messages generated by blending standardized text with selected message data passing Policy Engine rules, and then written to email, RSS, net send, a file, an application, Windows Event Log, SQL RDBMS or other custom target.
- **Synthesizers** derive new data analyzing message payload, drawing measured conclusions and re-storing new persistent data. For example, when a user's last login time changes, a "logon" event is created and stored in the database.
- **Message Forwarder** communicates selected messages to other network-connected SpyLogix Platforms; this feature is appropriate for cloud computing with distributed specialized support teams, managed service providers or aggregation for data mining.

Interactive Dashboard is a graphical user interface enabling insightful security intelligence through powerful real-time or historical data visualization. Simple to use features include:

- **Query** panels enable access to multi-sourced data
- **Analysis** using streaming data via grid and charts
- **Report Designer** reporting combines text, data and charts
- **Alert | Notification** graphical configuration interface

A single interface facilitates management information, operational collaboration with colleagues or continuous compliance management initiatives. Visualization using streaming graphs, charts, heat maps, and granular security data properties reveal intrinsic relationships and ready comprehension of multidimensional data. Saved data grid/chart views are available for offline output generation.

Web Services (data out) implements a RESTful-style interface for easily sharing data outward with other software tools or IT processes.

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