SpyLogix
ENTERPRISE
Data Sheet

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

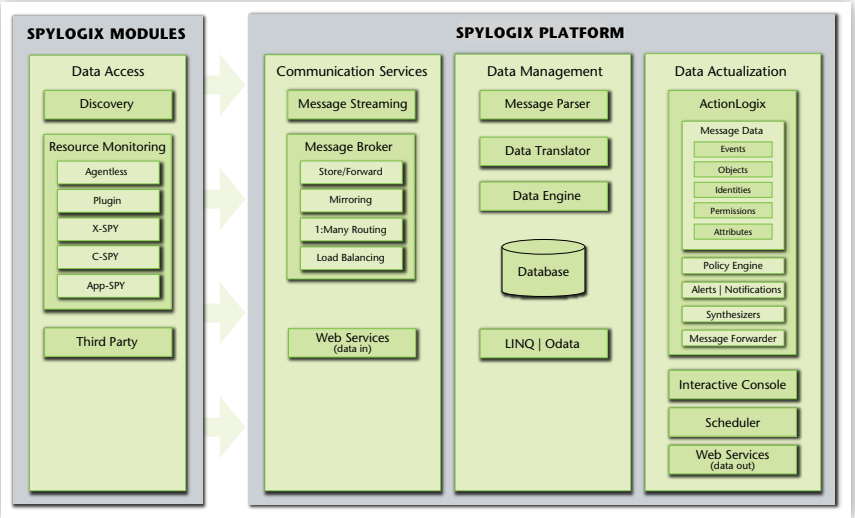
HIGHLIGHTS

- **Security Intelligence**
  - Situational Awareness
  - Enhance Visibility
  - Analysis and Reporting
- **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 Enterprise is security middleware designed for simplifying and enhancing enterprise informtion security management and control. New multi-sourced digital assets are natively monitored continuously, security data are automatically processed centrally for efficient historical data management, and proactively analyzed in real-time (referred to as "data actualization") via provided services to leverage data effectively for the enterprise. Benefits include improved "time-to-value" for people working to keep business information safe, more efficient IT service processes, and less technology complexities to boost staff effectiveness. 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 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 is stored. Volume of security data grows exponentially as online data grows to enable business efficiency. Velocity of security data increases as the sources and nature of (performance data) security data is needed 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. Access and activity data is continuously collected directly (using native APIs) from any accessible source 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. A message based design enables automatic data management and real-time actualization for simplified 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 intelligence is enhanced by continuous direct monitoring of key of resources and real-time actualization of data. Business and IT staff tasked with security governance, risk control, and compliance responsibilities can execute efficiently and improve operational control over business information access.

SPYLOGIX ENTERPRISE COMPONENTS

Continuous Data Access technologies are one or more SpyLogix Modules designed to natively acquire data, map it, and safely deliver as standardized messages security data to one or more SpyLogix Platform servers for advanced 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 Module technologies for ***Continuous Data Access*** include:

Discovery Modules that 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 natively form accessible IT sources using the most efficient means, including:

- **Agent-less** monitors consume source data accessible via 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 to capture back door identity system changes. 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 from SpyLogix Modules to Automatic Data Management and Real-Time Data Actualization layers of SpyLogix Platform for advanced processing and use.

Message Streaming efficiently moves messages directly to the Data Management layer for persistent storage. Furthermore, messages are made available for Action-Logix processing in real-time.

A cross-platform communications broker facilitates message store/forward, 1:many routing, mirroring, and load balancing. Message broker communications enables confirmed safe mode delivery of messages over less-reliable networks and high availability configurations, or cloud-based managed services.

A Web Services interface is provided to enable applications to easily send external data into SpyLogix Platform or share data externally with other applications or IT service processes.

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 is assessible via the included Interactive Console, any Odata compatible query tool, such as PowerPivot for Excel 2010, or through simple Web Services calls.

Real-Time Data Actualization provides multiple post-storage processing services to effectively use incoming messages and persistently stored security data in real-time:

ActionLogix™ is a series of components used to enact policies in real-time based on message content and use data effectively with other software or to take automated actions.

- **Policy Engine** employs configurable policies to monitor message data automatically in real-time. Boolean logic and Python scripts may be used for advanced message data processing or customized programmed actions. Policy development expedited using exposed message meta-data, including: basic, state, RBAC, and utility.

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 | Notifications** are embellished messages generated by blending standardized text with selected message data passing the Policy Engine rules, and then can be 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. For example, when a user's last login time changes, a "logon" event is created and stored in the database.
- **Message Forwarder** communicates only selected messages to another network-connected SpyLogix Platform. This capability is appropriate for cloud computing infrastructures with distributed specialized support teams, managed service providers, or data aggregation for mining or enterprise 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™ Purdue Technology Center 9800 Connecticut Drive, Crown Point, IN 46307 ■ +1.219.379.5560 ■ info@idenitylogix.com