SpyLogix Enterprise Platform
DATA SHEET

Security Intelligence and Data Actualization System for Continuous Monitoring and Real-Time Processing of Security Data from Enterprise Information Systems

HIGHLIGHTS

- Continuous Security Intelligence
  - User Access Rights (e.g. RBAC)
  - User Activity
- Interactive Console
  - Query
  - Analyze
  - Report
- Automated Data Management
  - Message Handling
  - Pre- and Post-Processing
  - Smart Storage
- Report Scheduling
- Alerts and Actionable Triggers

IDx Enterprise Suite

- SpyLogix Pro
- SpyLogix Enterprise
- SpyLogix Modules

SpyLogix Modules

- User Security
- Active Directory
- Windows Server
- Microsoft FIM 2010
- LDAP Directory
- CA SiteMinder
- VMware
- IdF Gateway (Mainframes)
- Custom Module Toolkit

SpyLogix Enterprise Platform is a security intelligence and data actualization system that works in conjunction with one or more SpyLogix modules or IDx applications to continuously centralize and automatically manage real-time security data feeds from multiple IT resources deployed to secure business information assets. Now a single enterprise security intelligence system can support IT GRC, provide access to real-time data for forensic and trending analysis and can be used as a powerful administrative tool needed for quick and accurate issue resolution.

SpyLogix unlocks security intelligence information from enterprise information delivery systems, including:

- User end-points
- Active Directory
- LDAP Directories
- IBM Manframe
- Web Applications
- Virtualized Servers
- Network infrastructures
- Windows Server folders and files
- Unix/Linux applications
- iSeries / AS400
- Identity & Access Management systems
- Cloud based application systems

SpyLogix Enterprise Platform is designed to organize and leverage use of centralized security data fed from multiple sources. Security data feeds can include user login and logoff events, user application access permissions (e.g. RBAC) from identity systems, application activity events, API output, security assessment tool or home-grown script output.

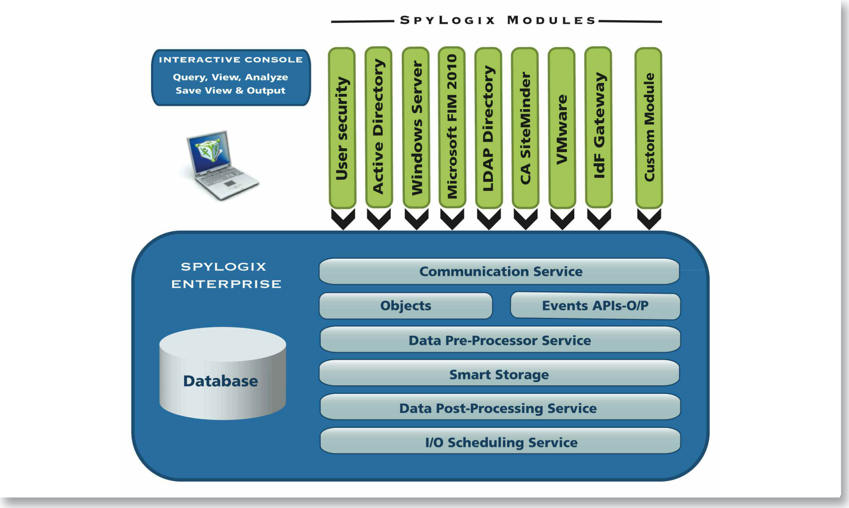

Figure 1. SpyLogix Enterprise Platform

SpyLogix Enterprise Platform (Continued)

All centralized security data is processed using a sophisticated multi-faceted architecture designed for automation, complex information security threat detection and remediation, troubleshooting, electronic forensics, and support of IT GRC initiatives. Thus enterprise information security transparency is enhanced for compliance or improved operational control over who has access to data and what activities have been performed which affect business information security.

Today multiple tools are used to obtain this information, each with a unique interface for viewing or reporting on a single source, or intensive log data aggregation and processing to find needed information. These solutions are either too narrowly or broadly focused, expensive, time consuming to support, and can miss key trends or events. 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 inappropriate business data exposure.

SpyLogix Enterprise Platform with its companion SpyLogix suite of modules can make an immediate impact and solidify a strategy to capture and leverage information for securing business data assets enterprise wide. Business and IT staffs are more productive. New information security initiatives can be initiated. Automation features help drive down costs and improve productivity.

OVERVIEW

Multi-sourced security data from enterprise business information systems require specialized handling to keep cost and complexity at a minimum. All security data types are input into SpyLogix Enterprise Platform in a standardized way.

Regardless of the source of security data being monitored continuously, all security data employ standardized message formats. A standardized message format enables dynamic real-time processing of security data centrally, thus automating data management for any security data input source, and keeping support costs minimal.

Centralized security data from multiple disparate sources facilitates an effective security intelligence system for managing today's threats affecting the safety of business information assets.

SPYLOGIX ENTERPRISE PLATFORM COMPONENTS

Interactive Console

An interactive multi-function software console is provided for accessing recorded security data. Time and metadata based queries enable selective access to the data. Secondary filters offer a further refinement of viewed data. Viewed data may be analyzed easily using familiar "drag-and-drop" grouping, column sorting and searching. Resultant favored views may be saved and re-run on-demand. Pre-saved views are provided.

The interactive console is capable of accessing and analyzing millions of recorded security data types in seconds, with no special technical skills needed. Reports are easy to create and may be output in many popular formats for sharing with others via email, collaboration software, or hardcopy. A scheduler is available to generate reports unattended.

Network Communication Service

Enterprise wide cross platform security data feeds must be centralized effectively to build an enterprise security intelligence system. Network Communication Services are designed with extensive data throughput optimization to centralize multi-sourced and cross platform messages with robust security data payload:

- Asynchronous message transport for high-performance
- Data throttling enables control over network pipeline bandwidth
- Buffer control keeps messages from being lost.
- Automatic push and/or pull data harvesting optimizes network capacity and business needs
- Crypto option for sensitive message payload using 128-bit AES encryption
- Delivery confirmation protocol option ensures data is not lost by centralization.

Message Handling

Incoming messages are automatically handled uniquely per each contained data type. Data handlers are available to process messages containing common data types: string, integer or floating point numeric, Boolean, binary, and array representations for all data types, including 2D array and matrix representations are supported. For example, LDAP directory multi-valued attributes are fully supported for granular access rights analysis using the Interactive console.

Representative message sources include:

- Identity Systems:
  - Security objects and attributes
  - Entity permissions
- Event messages
- Event or audit API messages
- Network scanning tool output messages
- Homegrown script output messages

Messages containing named data types are automatically defined within the SpyLogix database. This scheme preservation processing further simplifies IT staff support responsibilities as new security data is fed into SpyLogix, such as AD scheme changes or new application events.

Data Pre-Processing

Data types may be selectively and dynamically processed. The data pre-processor function translates non-human readable data types into human readable form. For example, incoming Active Directory User Account Control (UAC) bit flags are transformed into human readable text.

Data Smart Storage

Each multi-sourced data type scheme is preserved by automatically storing each data type with its original name and up to six software assigned metadata tags to facilitate rapid retrieval and eliminate security data management time, money, and resources.

- Date/time context is preserved
- Redundant security data is eliminated to make retrieval faster
- More data maintained online for security intelligence, troubleshooting, electronic forensics, or IT GRC process enablement.

DATA Post-Processing

Once message data is smartly stored, new data may be synthesized, for example, a user login event is synthesized and recorded in SpyLogix when a user's last login time attribute is updated in Active Directory.

Any and all security data types are actulized by ActionLogix, a dynamic expert system incorporating simple rules or fuzzy logic for powerful analysis and automatic control of complex information security service processes.

ActionLogix can share data with other tools, such as reporting tools, help desk, workflow applications, email, or SMS text messaging of noteworthy occurrences.

Input and Output Scheduling Services

APIs that provide access to security data, such as RBAC, audit or event data, may be queried initially to record a baseline, and then periodically for data updates.

Tools or homegrown scripts may be scheduled to run for purposes of generating more periodic security data and recording the output in SpyLogix.

Pre-saved reports using the interactive console may be scheduled to run in the background.

SUMMARY

SpyLogix Enterprise Platform improves enterprise security intelligence by providing a single independent system or record for enhancing information systems security:

- Continuous monitoring
- Historical baseline and change record
- Automated data management
- Actualized data to enhance threat detection
- Easy access to real-time security data
- Scalable for SMB's or large enterprises

OPERATING ENVIRONMENT

- Windows Server 2003, 2008 and 2008 R2
- See specific SpyLogix modules for source specific requirements