SpyLogix Enterprise
DATA SHEET

HIGHLIGHTS

- Lower the cost of compliance by providing secure internal access and/or external delegation of audits and reports
- Real-time continuous monitoring of systems, applications and servers
- Real-time continuous monitoring of User Activity
- Interactive Console
- Smart Storage
- Analyze, Report and Output
- Scheduled Reporting
- Automate Alerts & Actionable triggers

IDx Enterprise Suite

- SpyLogix Pro
- SpyLogix Enterprise
- SpyLogix Modules

SpyLogix Modules

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

The SpyLogix Enterprise platform for protecting enterprise information assets through continuous real-time security data collection, analysis, assessment and automation.

SpyLogix Enterprise is a software platform for organizing and using centralized security data collected from multiple IT sources to help businesses do more with less time, money and resources. Security information is aggregated from key application realms prevalent in today's enterprise information systems: local/remote networks, Web (intranet and Internet), Unix/Linux, IBM main/mid-frame, and cloud based applications.

Access management and event data from sources, including users, identity systems, applications, and security tools are proactively collected and processed automatically. Thus information security transparency is enhanced for compliance or improved operational control over who has access to data and what activities have been performed affecting business information.

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 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. Business and IT staffs are more productive.
New information security initiatives can be initiated. Automation helps to drive down costs and improve productivity.

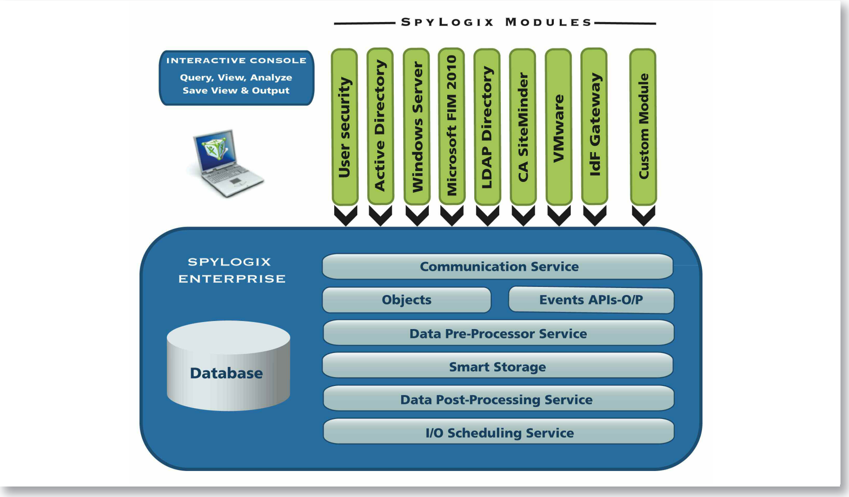

Figure 1. SpyLogix Enterprise Platform

SpyLogix Enterprise

SpyLogix Enterprise is for businesses to effectively automate burdensome tasks that impact compliance, security information, management and IT costs. The platform is designed to provide proactive actualization of security data and user activity information from any source in real-time (NOT static logs) normalizing, standardizing, centralizing, then providing analyzation and automation.

SPYLOGIX MODULES

SpyLogix modules proactively collect and centralize (feed) security data directly from users, identity systems, file servers, applications, and other event sources such as log files, that are involved with information security. Each module standardizes security data for immediate consumption by SpyLogix Enterprise, an enterprise security data management platform. SpyLogix modules are designed to work with SpyLogix Enterprise to centralize security information from key business application or data realms, such as local/remote networks, Web (intranet and Internet), Unix/Linux, IBM mainframe, midrange, and cloud based applications.

SpyLogix modules available include:

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

NETWORK SERVICES

This service finds well-formed (using SpyLogix modules) messages from multiple sources containing security data, and safely delivers each message centrally.

- **Scalability** - multi-threaded for high message throughput
- **Delivery Confirmation** - confirms delivery of messages from security data sources using a simple protocol
- **Message Routing** - delivers messages to source specific message handlers for proper processing

SpyLogix Enterprise a powerful platform providing real-time security and identity information for your risk and compliance needs.

For more Information

To learn more about IdentityLogix SpyLogix Platform, please visit identitylogix.com.

MESSAGE HANDLING

Advanced message handlers enable unique processing of needs of native object data, for example identities and permissions, as well as, simple structured data.

- Object Handler – directory data holding objects (e.g. users, groups, and computers) and associated attributes and permission data are parsed to enable further processing and simplified retrieval
- Event Handler – structured data from sources such as APIs, network scanning tools (e.g. NMAP) or log records
- All data is 100% parsed to facilitate custom processing and flexible retrieval options

DATA SYNTHESIS

Security data from objects or events is often in non-human readable form.

- Enables SpyLogix modules to identify non-human readable data in advance
- Transforms non-human SpyLogix module data into human readable forms
- Hidden security information is uncovered and made actionable for process automation and integration

For example, centralized event data gathered across multiple time-zones may be analyzed within the proper context by a person or in a report.

SMART STORAGE

Intelligently storing security data enhances the effect of using SpyLogix Enterprise to organize security data and deliver information.

- Six (6) levels of data classification for objects or events are interrogated to enable proper storage and subsequent flexible retrieval
- Ensures no redundant storage of security data to keep more security information online
- Retains proper historical context for querying, forensic studies or trend analysis
- Aliasing helps to associate related object or event data
- Supports both discovered and changed data

The Smart Storage data input/output design facilitates enhanced throughput with minimal hardware to lower overall cost of ownership.

ALERT/ACTION AUTOMATION

Automation is further realized by software plug-ins capable of analyzing data and enacting pre-programmed actions.

- Incoming or stored data is made actionable
- Object changes, such as adding a user to a group or permission elevation, can be detected
- Notifications may be sent when events occur, like a new application has been added to the network

By properly classifying, processing and storing parsed data centrally, enterprise users receive information faster, or real-time integration with other applications is enabled.

Information Security Benefits Summary

SpyLogix solutions improve efficiency and effectiveness of information security audit processes in three ways:

1. **Empower people with enhanced information**
2. **Automation of complex or burdensome tasks**
3. **Do more with less (time, money and resources)**

VIEW, ANALYZE AND OUTPUT

A software console is provided to access security information stored in the database.

- Easily query the database for information
- View and analyze security data
- View management
  - Pre-saved views
  - Filter, group, sort, +/- columns
  - Fine-grained secondary query filter
  - One-click wide column adjustment
  - Save as for creating new views
- Output data in popular formats

SCHEDULING SEREVICE

Once, favorite views and output formats are established, SpyLogix output may be automated by scheduling reports to run in the background and be distributed throughout the enterprise.

- Saved views may be scheduled for background execution
- Invocations are governed by date/time or designated frequency
- Output produced by home-grown or 3rd party tools can be periodically executed and processed by SpyLogix Enterprise

SpyLogix scheduling service feature is ready to leverage Microsoft's SharePoint collaboration server!

INTEGRATION

Stored data may be fed automatically or on demand to other programs.

- Existing reporting tools may receive data dynamically in expected formats
- Tools may make calls to extract just needed data
- Identity management tools can receive real-time identity changes for reconciliation
- Identity management tools can receive real-time identity changes for reconciliation

Robust integration preserves investments in other tools, and enables new information to be shared effectively.

KEY DIFFERENTIATORS

Fast | Easy

By designing a system for continuous IT security monitoring and automatic data management with no reliance on logs or log processing, information security transparency is made fast and easy. Continuous monitoring and processing of multi-sourced audit data feeds facilitate translation of disparate security data into actionable security information in real-time with full context.

Business or IT staff can easily view user security and activity reports periodically or on an ad hoc basis to keep business data safe. Self-service access, activity, and other security information is available quickly for compliance or operational information security easily, without impacting IT staff productivity!

Automation

Security data is 100% parsed and classified in a standardized way to enable automated processing of data in real-time. Non-human readable elements may be made human readable. Redundant elements may be eliminated to maintain more data online for analysis or reporting. Changes are detected and alerts or other triggers may be generated based on the stored data, including synthesized events. Multi-source baseline and continuous change monitoring is combined to yield better information for management and control of business data.

Centralization of multi-audit source information using IdentityLogix solutions lowers online security audit or compliance reporting costs and ongoing support complexities.

Security Intelligence and Action System

Automated security data management from access/identity systems, activity, audit API (on premise or cloud applications), and network security tool output assists businesses concerned with information security. Identity security attribute, permissions, and application event audit trails are simple to re-construct. Perimeter network security is stored. Audit data is stored with data/time reference to enable filtering. Historical attribute change history is preserved supporting forensic audit research.

An enterprise "security intelligence system" with historical reference empowers business process owners and IT staff with enhanced information for substantially improved information security transparency.

PRACTICAL APPLICATION

Compliance is widely regarded as the primary driver for new security investment by businesses. Information security controls show auditors that business data is safe and appropriate policies are in place. Ready access to security intelligence information helps answer questions such as:

- Who can access business information?
- What business functions or data can a user access?
- How and when do users access business data?
- Who has authority to make security changes?
- What security changes are being made right now?
- Are applications secure from outside attacks?

Business and IT staffs are tasked with answering these questions to enhance governance, manage business risk, and comply with regulations.

Business staff, such as IT auditors, application or data owners, can obtain information assurance reports for governance or compliance with minimal IT staff impact.

Security engineers will welcome a simple way to maintain "least privilege" or "privileged user management" initiatives. Ad hoc security reports or forensic studies may be responded to quickly.

Security administrators or identity management software solutions can automatically document actions "out-of-band" to enhance separation of duties (SOD) initiatives. Furthermore, "back door" identity system changes may be immediately reconciled.

Integration with help-desk systems independently confirm user access control actions received from HR or management. User problems may be proactively addressed with availability of improved security information driving 50% or more of new user problems.

Security engineers can aggregate output from vulnerability security assessment tools into a single output analysis and reporting system, including historical result trend analysis and remediation records.

Security intelligence information may be used by IT staff to improve data security governance. Management can validate changes using summary reports or automated notifications. Administrators can easily provide auditors needed reports for complying with regulatory mandates.