SpyLogix for User Security
DATA SHEET

HIGHLIGHTS

- Continuous User Activity Monitoring
- Track Session State Changes
- Track Directory Edits
- Track Client Applications Executed
- Data Loss Detection
- View, Analyze, and Report
- 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

IDENTITYLOGIX™

Dynamically audit and monitor user activity real-time...

SpyLogix for User Security monitors users accessing business data from Windows clients for improved information security transparency.

Businesses rely on information exchange to enhance overall efficiency and effectiveness. The Windows client is the alpha and omega for users accessing business information. It is also a computer with data processing capabilities that continually improve. Businesses must ensure that the risk of empowered users seeking business information is properly managed.

Proper information security risk management depends on collecting data about the process of users accessing business information assets. Security data can support answering questions related to information security, such as:

- Who requested access to information assets?
- What assets were used to access information?
- When were online resources available to users?
- Where did they initiate access from?
- Why was information accessed?
- How was information assets accessed?

SpyLogix for User Security provides a fast and easy way to begin answering these questions as business data is accessed using layers of information technologies employed to enable information security.

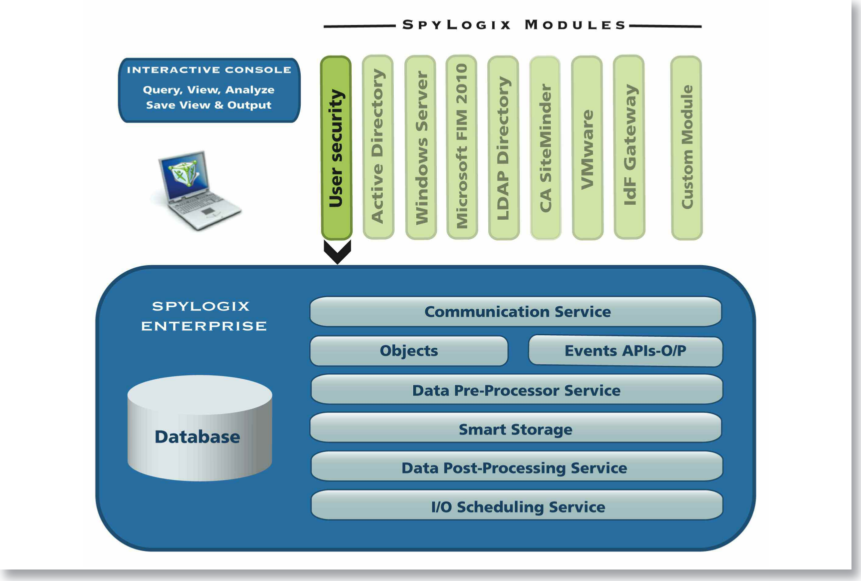

Figure 1. SpyLogix Enterprise Platform

SpyLogix for User Security

When businesses manage risks associated with ubiquitous access to information for operational efficiencies and effectiveness, SpyLogix for User Security works to enable information security.

OVERVIEW

SpyLogix for User Security facilitates information security risk management by providing Windows client user security data for:

- Sessions (logon, logoff, lockout, etc.)
- Data loss detection
- Client (user) activity tracking

Users begin accessing business information using a computer by establishing an "electronic presence," or session, to begin using multiple layers of information technologies needed to mitigate proper data access and use. User sessions can be created in a variety of supported ways, each with unique associated risks.

When computers are used to access information, there are many ways by which business data can be compromised or removed from a secured business network.

In some cases data loss by users with special privileges, which can be inadvertent or intentionally malicious, involves changes made to underlying identity systems employed for controlling user access to local network, web, or legacy mainframe application realms.

By monitoring users or programs that edit Active Directory or other directories using LDAP, changes are recorded for governance and compliance.

SpyLogix for User Security records user activities to make governance and compliance easier. Security administrators can spend less time documenting changes. Malicious activity can be detected faster and with more detail, even when an attacker shuts logging off to hide activities.

SpyLogix for User Security includes capabilities that compliment traditional end-point security solutions.

KEY MONITORING FUNCTIONS

Session State Changes

SpyLogix records Windows client user session state changes,

including logon/logoff events, to assist in determining more precisely the means by which a user accessing business data online. This information helpful for:

- Understanding the ways users enter networks for access to business data
- Forensic studies to identify trends
- Identifying potential nefarious activities

Online user session state changes are recorded when

A session connected to the console terminal
A session was disconnected from the console terminal
A session was connected to the remote terminal
A session was disconnected from the remote terminal
A user has logged on to the session
A user has looged off the session
A session has been locked
A session has been unlocked
A session has changed it remote controlled status*

*Note: _This system metric is used in Terminal Services environment to determine if the current Terminal is being remotely controlled_

Data Loss Detection

When a user inserts a portable storage device or media capable of storing data outside of the protected network environment, SpyLogix records an event.

This data can be cross referenced with file monitoring records to understand when the potential for sensitive data loss exists.

Client-Spy

When privileged accounts initiate activity, this user will be recorded with all ongoing activity events synthesized by the Client-Spy feature. This feature is needed when it is important to understand the identity of users making key changes, especially so for compliance purposes.

Client-Spy will record programs executed and other key data. Internal or malicious users may use non-standard means (scripts or tools) for editing directories needed to control access to business data. When log data is unavailable, monitoring is needed to continuously collect this data.

When malicious users shut down logging to cover their tracks, or another problem causes log records to be unavailable, monitoring use of the LDAP API will provide necessary compliance data or a history for forensic analysis.

Client-Spy may be used for addressing special Windows application activity tracking that had not been originally designed for an application.

In summary, Client-Spy is a DLL for recording data from client program executables that are not readily available from Windows. Client-Spy will record:

- User account initiating activities
- Windows client or server programs executed
- LDAP client API invocation (by tools or scripts). Directory edits are confirmed (using SpyLogix) with Windows Server log events, with an alert for unconfirmed edits. *Unconfirmed edits occur when logs are improperly configured, encounter unforeseen collection issues, or logging is turned off.*
- Windows application activity

SPYLOGIX ENTERPRISE

SpyLogix for CA SiteMinder and all SpyLogix modules leverage centralized automated data management and information exchange features of SpyLogix Enterprise, including:

- Network Services
- Message Handling
- Data Synthesis
- Smart Storage
- Alert/Action Triggers
- View, Analyze and Output
- Scheduling Service
- Integration

SpyLogix for CA SiteMinder is designed to work with SpyLogix Enterprise, a platform for managing 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.

Operating Environment

- Windows Server 2003 or 2008
- Windows XP, Vista, or W7
- SpyLogix for User Security requires SpyLogix Enterprise as a prerequisite.

SpyLogix enables businesses to manage risks associated with making information available so businesses can operate efficiently and effectively.

For more Information

To learn more about IdentityLogix SpyLogix for User Management, please visit Identitylogix.com.