SpyLogix for

IDF GATEWAY

Data Sheet

IDENTITY LOGIX™ IdentityForge

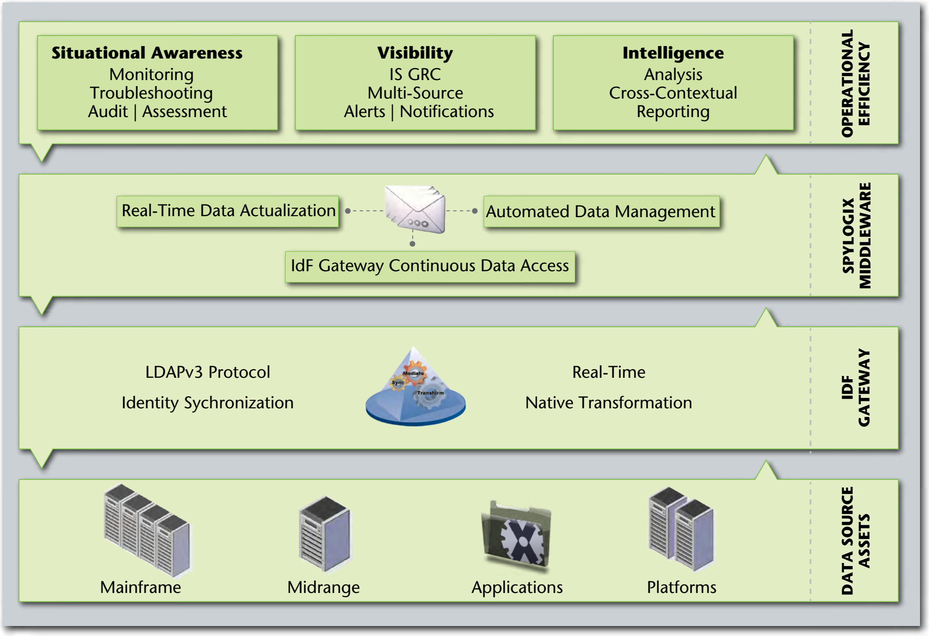
Continuous Situational Awareness and Real-Time Security Intelligence for Enterprise Systems

SpyLogix for Identity Forge (IdF) Gateway is a solution for continuous situational awareness and visibility for security data from mainframe security managers (IBM RACF, CA ACF2 or Top Secret), z/OS, IBM iSeries (AS400), platforms and other business application systems. SpyLogix uses standards and automation to simply security data management and reduce complexity and substantially improve ease of use. Now a single enterprise security intelligence system can support IT GRC, provide access to real-time data for forensic studies, trending analysis and used as a powerful administrative tool for rapid issue resolution.

Enterprise resources store security data in multiple formats, use different means/ interfaces to access and use this information needed to solve problems and for IT GRC. The Identity Forge (IdF) Gateway provides a unified bi-directional means of interfacing with this disparate data using LDAP V3 protocol. For example, identity management tools can use the IdF Gateway to manage mainframe security objects.

SpyLogix for IdF Gateway provides a separate out-of-band server that provides a historical record of security objects and changes. An interactive console allows SpyLogix data to be queried and analyzed centrally and offline from the run-time production resources. Programmable logic gateways facilitate real-time automated software based monitoring. A message based architecture facilitates scalability, flexibility and automation to maintain ease of use. Security data objects and associated attributes are proactively discovered to form a baseline to which new changes could be compared. This forms a “chain of custody” of sorts for access rights which appeals to auditors or IT staff performing troubleshooting. Flexible output options facilitate sharing of information with other people or IT service processes.

SpyLogix is a solution for organizing and using IBM and other enterprise security data efficiently and effectively. SpyLogix leverages standardization, centralization, and automation to eliminate complexity and burdensome IT support normally associated with security data management. Security data management is automatic; data analysis and reporting is easy and flexible reducing time, money and resources needed to support enterprise security intelligence, identity assurance and IT GRC initiatives.


OPERATIONAL EFFICIENCY

Situational Awareness
Monitoring
Troubleshooting
Audit | Assessment

Visibility
IS GRC
Multi-Source
Alerts | Notifications

Intelligence
Analysis
Cross-Contextual
Reporting

SPYLOGIX MIDDLEWARE

Real-Time Data Actualization
Automated Data Management
IdF Gateway Continuous Data Access

IDF GATEWAY

LDAPv3 Protocol
Identity Sychronization
Real-Time
Native Transformation

DATA SOURCE ASSETS

Mainframe
Midrange
Applications
Platforms

HIGHLIGHTS

- **Continuous Security Intelligence**
  - Information Security Visibility
  - Identity Intelligence
  - Audit and Monitor
    - Users & Groups
    - Datasets | Facilities
    - Alias | Catalogs
    - Security Activity
- **Automated Data Management**
  - Message-Based Design
  - Intelligent Data Handling
  - Historical Database
- **Real-Time Data Actualization**
  - Policy Engine
  - Alerts
  - Event Synthesis
  - Message Forwarder
  - Report Scheduler
- **Interactive Console for Data**
  - Query
  - Analysis
  - Reporting
- **SpyLogix Enterprise**
  - SpyLogix Platform
  - SpyLogix Modules
    - User Security
    - Active Directory
    - Windows Server
    - VMware
    - Microsoft FIM 2010
    - LDAP Directory
    - CA SiteMinder
    - Radiant Logic
    - IdF Gateway
    - Module SDK
- **Operating Environments**
  - SpyLogix for IdF Gateway:
    - Windows Server 2003, 2008 and 2008 R2 (recommended)
    - Windows XP or W7
  - IdF Gateway:
    - IdF Gateway 4.5 or higher

OVERVIEW

SpyLogix obtains IBM security data using Identity Forge's Gateway solution. An on-demand discovery step by SpyLogix records a baseline of objects, attributes and events.
Objects include users, groups, datasets and resources, along with the unique attribute set stored for each objectClass. Events are recorded with data for user logins, commands, and IP address used.

With on-demand baseline ability and continuous monitoring for changes to security objects and attributes or events, and automated security data management, SpyLogix enables IBM systems security auditing or monitoring initiatives. IBM systems security intelligence is simplified, putting the right information in the hands of the right people, with minimal ongoing IT staff support burden.

DATA QUERY, ANALYSIS AND REPORTING

An interactive multi-function software console is provided for accessing IBM security data. Time and metadata based queries enable selective access to the data. Secondary filters offer a further refinement 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.

Secure Data Recorded
Users
Groups
Attributes
Datasets
Resources (Facilities)
CICS Authoritzations
Alias/Catalog Management

User Audit Recorded
Date and Time User Login
User Usage
Terminal Session
Terminal Session
User IP Address
Issuing User

The interactive console is capable of accessing and analyzing millions of stored IBM security objects or user events in seconds, with no special technical skills needed. Reports are easy to create and output. Reports 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.

AUTOMATIC DATA MANAGEMENT

Security data is centralized for simplicity and cross-contextual historical security data management. SpyLogix fully parses all enterprise security data for fine-grained analysis. Data elements may be pre-processed, usually for enhanced human readability using the interactive console. Data elements are then smartly stored, so as to eliminate storage of redundant data, and maximize historical baseline and change data stored for analysis and reporting purposes.

SpyLogix collects IBM security data, fully parses data, and then processes data elements into well-formed messages. Messages are communicated to a central processing service, whereby message data elements may be pre-processed, usually for enhanced human readability using the interactive console. Data elements are then smartly stored, so as to eliminate storage of redundant data, and maximize historical baseline and change data stored for analysis and reporting purposes.

REAL-TIME DATA ACTUALIZATION

With enterprise security data safely stored, SpyLogix post-processing occurs. All data may be automatically filtered using programmable logic gateways. New events may be synthesized programmatically. Object, attribute or event changes can trigger alerts by email or SMS text. Changes are detected and alerts or other actions may be generated based on the stored data, including programable actions.
Multi-source baseline and continuous change monitoring is combined to yield better information for management and control of business data security.

SpyLogix Enterprise is 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