SpyLogix for
VMware vSphere
Data Sheet

IDENTITYLOGIX™
Continuous Situational Awareness, Visibility and Security Intelligence For Virtualized Enterprises

HIGHLIGHTS

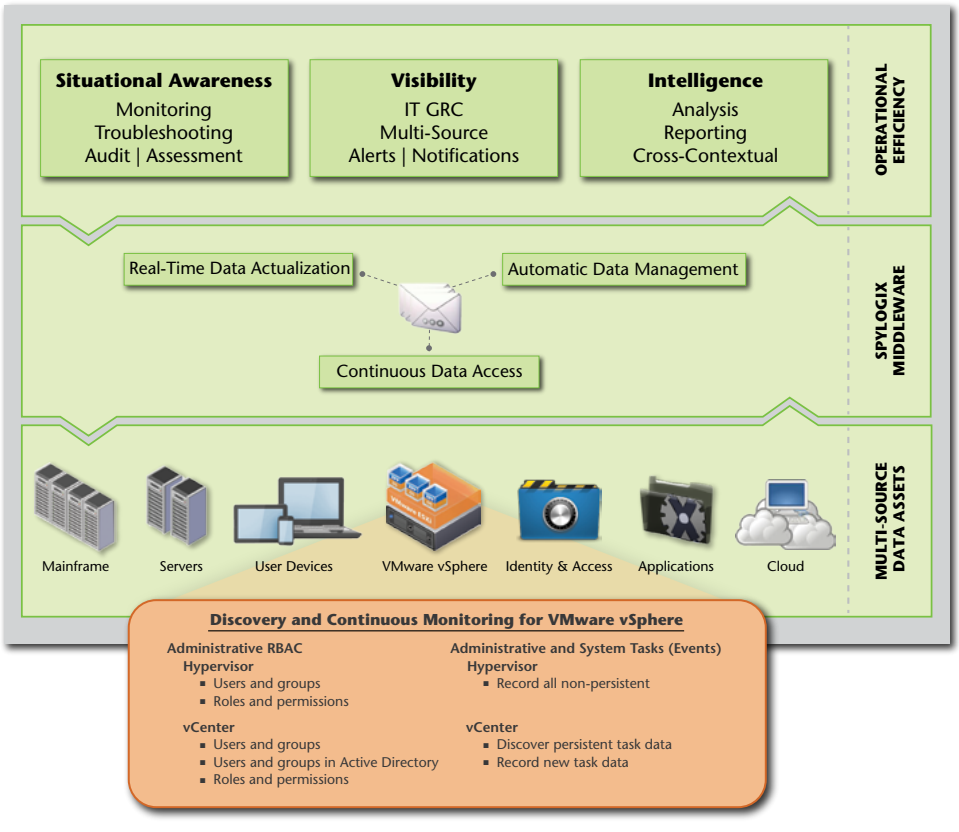
- **Security Intelligence**
  - Situational Awareness
  - Enhanced Visibility
  - Analysis and Reporting
    - Administrative RBAC
    - Administrative Tasks
    - System Tasks
- **Continuous Data Access**
  - By API (no reliance on logs)
  - SpyLogix Message Design
- **Communication Services**
  - Message 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™ for VMware vSphere improves vSphere virtualized infrastructure security by continuously monitoring key security objects and data. A secure virtualized business can operate more efficiently and its people will be empowered to perform information security tasks with greater efficiency. Virtualized infrastructure support costs and "time-to-value" are reduced by making complex support tasks simple and easy. Business information security is improved due to simplification of security support and ready access to new information supporting virtualized infrastructure governance, risk control and compliance (GRC) initiatives.

As virtualized infrastructures grow, the simplicity of spawning new virtual machines (VMs) makes security management more difficult with time. Managing VM administrative access rights and daily activities (tasks or events) can become challenging. In fact, the industry has coined a phrase "VM sprawl" to characterize generally these new management challenges. VM sprawl complicates virtual machine security administrative rights and activity tracking. SpyLogix for VMware vSphere will discover and monitor administrative role based access control (RBAC) settings across multiple supported identity and access management stores controlling access to the vSphere virtualized enterprise.

Governance, risk control and compliance initiatives within vSphere infrastructures have evolved to depend on continuous recording of activities (tasks) being performed by administrators and the vSphere system components. In some entry VMware virtualized infrastructures task activity is not persistently recorded. For robust virtualized enterprises using vCenter tasks are persistently recorded. SpyLogix for VMware vSphere will discover and monitor both persistent and non-persistent administrative and system activity (tasks or events) data.

SpyLogix for VMware vSphere enhances virtualized server infrastructures security using its unique capabilities for continuous operational awareness, visibility, security intelligence and real-time data actualization. Current administrative role based access control (RBAC) settings, defined as privileges required for invoking an operation or viewing a property, and tasks (activity or events) are recorded. vSphere is continuously monitored for administrative RBAC changes, which may be added to persistently stored baseline data or previous changes, and new task activity.



OVERVIEW

SpyLogix for VMware vSphere is a data access module designed to continuously monitor vSphere security. All administrative RBAC security settings are first discovered, and then monitored continuously for changes. Administrative and system tasks (activity or events) are also continuously recorded. RBAC and task data are automatically accessed over a network using native vSphere APIs (without agents) from a central server running SpyLogix for VMware vSphere.

VMware vSphere security data is mapped into well-formed, standardized messages and communicated via a broker to any companion SpyLogix Platform (prerequisite) server for advanced processing.

SpyLogix Platform capabilities may be summarized as follows:

- Messages may be received
  - Locally,
  - Sent to remote support teams, or
  - Routed to cloud security-as-a-service providers.
- Data management automatically processes and smartly stores parsed data persistently.
- Data actualization leverages data to make it efficiently usable.

See the SpyLogix Enterprise data sheet for more information on automated data management, actualization, interactive console and more features included with prerequisite SpyLogix Platform software.

Administrative RBAC Management

VMware administrative role-based access control (RBAC) security involves:

- Privileges required to invoke an operation or view a property.
- Roles or predefined sets of privileges and
- Permissions which are assigned to roles for performing activities on objects.

With RBAC security the possible combinations available to control administrative access quickly grows to unmanageable levels.The possibility of improperly configured RBAC administrative privilege can put VMware vSphere complex data security at risk. Due to the inherent complexity, misaligned (with enterprise policy) administrative privileges can go undetected for extended periods of time.

Furthermore, VMware vSphere allows for RBAC data to be stored in vCenter, Active Directory and ESXi, which sets the stage for possible conflicting authentication and authorization settings. SpyLogix for VMware vSphere will enable RBAC controls to be tracked and remain manageable.

When RBAC is leveraged to control administrative access to VMware vSphere environments, having answers to questions such as:

- Who has what authority for securing the VMware vSphere virtualized complex?
- Are all authentication and authorization changes documented for IT audit readiness?
- Who made critical changes recently?

Administrative and System Task Management

VMware vSphere generates both persistent and non-persistent (in the case of ESX/ESXi only) task data. SpyLogix for VMware vSphere will access and centrally provide for advances task management through its companion (prerequisite) software SpyLogix Platform.

SpyLogix for VMware vSphere provides a discovery ability for using existing vCenter persistently stored tasks to form a baseline record of historical activity. Task discovery forms a baseline from which new activity may be compared.

The VMware vSphere environment is continuously monitored natively using VMware vSphere APIs for centralized "future-proof" and reliable task data management.

VMware vSphere Security Best Practices

As the size of the virtualized infrastructure grows, it becomes more difficult to efficiently manage proper administrative RBAC. Use SpyLogix to continuously monitor and review (for compliance) account privileges and institute automatic "closed-loop" provisioning and de-provisioning process control monitoring in lieu of "straight-line" monitoring for "least privilege" or "privileged account" managment.

- **Discover** all users, groups, roles and permissions wherever they are stored within VMware vSphere to form a baseline of who has what authority from day one.
- **Monitor** RBAC changes, wherever it is stored, and activity continuously for optimal business information security. Periodic review of task data is insufficient for information security governance, risk and compliance processes.
- **Automate** monitoring of critical tasks and generate alerts or notifications to maintain good information flow.
- **Continuously** audit authentication and authorization controls employed by other VMware management tools using the SpyLogix Module SDK.

Continuously track all administrative and system activity for proper governance, risk control and compliance support.

SUMMARY

SpyLogix for VMware vSphere organizes and leverages the administrative RBAC, wherever it resides, and persistent and non-persistent task data to enable greater management control over virtualized enterprises. It can be positioned nicely as an innovative and enterprise extensible security middleware solution for continuous visibility for administrative users, groups, roles, permissions, as well as, administrative and system tasks. People and IT services processes supporting VMware vSphere can become more efficient and effective.

IDENTITYLOGIX™ Purdue Technology Center 9800 Connecticut Drive, Crown Point, IN 46307 ■ +1.219.379.5560 ■ info@idenitylogix.com