SailPoint

DATASHEET

Identity Governance for **Active Directory**

Microsoft infrastructure, prevalent in businesses around the world, is reliant on Active Directory to provide a global model for users, groups, and resources. This centralized directory carries inherent risk: it is an attractive target for malicious activity. A successful attack on an Active Directory installation is likely to result in security exposure, heavy direct financial loss, serious reputation damage and increased audit requirements.

How IdentityIQ File Access Manager Can Help

To effectively protect Active Directory, organizations need technology to provide them with full visibility into the users, groups, resources, and activity associated with it.

Dramatically reduce security risk and increase compliance by:

- Providing proof of compliance during audits and reducing time spent on forensics
- Monitoring and responding to activity in real-time
- Extending the identity strategy to provide comprehensive access governance to unstructured data

Demonstrate ROI by identifying and cleaning up stale accounts, automating audit requirements, and streamlining access reviews and requests
to reduce the IT workload.

Key Features and Benefits

Context-Aware Activity Monitoring

Activity monitoring is done in real-time. Every monitored activity is enriched with its full security context from in place security systems and other data sources. The context is crucial to identify violations and respond to them rapidly, and is also available when performing forensics and activity policies.

The following activities may be monitored by IdentityIQ File Access Manager:

- Object Actions: Create, Undelete, Move, Delete, Modify (Attribute), Added Permission, Removed Permission
- Audit Policy Change
- FSMO Role Change

- Domain Policy Change
- Account Lock
- Reset Password
- Account Logon
- Group Policy Object (GPO) Actions: Status Modify, Security Filtering Modify, Property Modify, Link Modify, Link Added, Link Removed, Before / After Policy Changes

Real-Time Alerting

Activities monitored by IdentityIQ File Access Manager can prompt action to be taken to address risk-inducing behavior. This includes notification by email, actions such as certifications or modification of access, and remote actions initiated by an alert sent from IdentityIQ File Access Manager into a SIEM or other infrastructure. Alerts can be used to take governance actions such as notifications, suspension of all accounts related to an identity, and event-driven certifications.

Permissions Collection and Analytics

Automatically collect and analyze all entitlements on your Active Directory environments. Aside from answering who has access to what data, the process also reveals access management violations and bad practices. IdentityIQ File Access Manager can also assist in remedying Active Directory installations that may have latent governance issues such as toxic combinations of groups and permissions and may assist in the removal of cyclical groups.

**SAILPOINT:
THE POWER
OF IDENTITY™**

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.