SailPoint

DATASHEET

Identity Governance for **File Shares**

Today, more than 80% of organizational data is unstructured. This content doubles in size every two years and is spread across geographical locations, located both on-premises and in the cloud. File shares enable collaboration with this data. From a risk perspective, the vast amount of data maintained in file shares makes it a target for any malicious activity. A successful data breach is likely to result in sensitive data exposure, heavy direct financial loss, serious reputation damage and increased audit requirements.

How IdentityIQ File Access Manager Can Help

To effectively protect the unstructured data within file shares, organizations need technology to provide them with full visibility into sensitive data stored within it, including who can access it and who is accessing it – a complete understanding of file servers and network attached storage activities and permissions model.

Dramatically reduce security risk and increase compliance by:

- Identifying where sensitive data resides, who has effective access to it, how they are using it, and putting effective controls in place to secure it
- Providing proof of compliance during audits and reducing time spent on forensics
- Electing the rightful data owners and enabling them to protect their own data
- Extending the identity strategy to provide comprehensive access governance to unstructured data

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

Key Features and Benefits

Data Classification

Visibility into all users, applications, and data ensures the right people have the right access to the right applications and systems improving security and reducing the risk of data leakage or breach is especially crucial when workers are onboarding, moving to a new job role, or leaving the company. Employees have visibility (and access) to all applications, cloud and on-premises alike, from the Microsoft Azure AD Access Panel.

Context-aware Activity Monitoring with Real-time Alerting
Activity monitoring is done in real-time. Every monitored activity is enriched with its full security context from in place security systems (Active Directory or any other data source). The context is crucial to identify violations and respond to them rapidly, and is also available when performing forensics and activity policies.

Permissions Collection and Analytics
Automatically collect and analyze all granted entitlements on your Windows, Hitachi, EMC, or NetApp environments, while considering users, groups and custom permissions. The process also reveals overexposed data, other implemented access management violations and bad practices.

Business Users Involvement and Data Ownership
Business users are the true owners of an organization's data. Electing the rightful data owners requires a deep understanding of the business – one that lies only in the minds of the employees. The elected owners are provided with a set of dedicated dashboards to equip them with actionable intelligence about the data they own.

Access Lifecycle Management
Access lifecycle management is key to ensuring access is granted on a "need-to-know" basis. IdentityIQ File Access Manager streamlines access requests and manages periodic and risk-based access reviews for unstructured data. Automated provisioning and revocation of access reduces costs and IT workload while avoiding potential human errors.

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.

DS1143-1903