SailPoint

DATASHEET

Identity Governance for **Microsoft Exchange**

Microsoft Exchange infrastructure is often a target for malicious activity as it has grown in global popularity. A successful data breach involving Microsoft Exchange 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 protect the unstructured data stored in Microsoft Exchange, organizations need a technology to provide them with full visibility into who can access folders and who is actually accessing them. A solution must have a complete understanding of the Microsoft Exchange activities and permissions model, while not affecting the performance of the protected environment.

Dramatically reduce security risk and increase compliance by:

- Determining who has effective access to data, how they are using it and putting real-time controls in place to secure it
- Providing proof of compliance during audits and reducing time spent on forensics
- Extending the IGA strategy to provide 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

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 full 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 personal and public folders, including Send As and Send on Behalf permissions. Aside from answering who has access to what data, 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 the key to ensuring access is granted on a "need-to-know" basis. Streamline access requests and manage 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.

Microsoft Exchange Server and Online Support

To ensure your entire Microsoft Exchange infrastructure is protected, IdentityIQ File Access Manager covers both Microsoft Exchange on-premises and online by the same license. IdentityIQ File Access Manager fully supports hybrid architecture where some public folders are on-premises while others are in the cloud.