**SailPoint**

MANAGING THE BUSINESS OF IDENTITY

# SecurityIQ for Microsoft Exchange

## BENEFITS:

- Identify who has effective access to what data, and who is actually using it
- Track and respond to real-time activities on Exchange
- Reduce risk by addressing overexposed data and excess access requests
- Minimize response time to breaches and minimize damage
- Manage the access lifecycle for unstructured data across the organization
- Engage business users to protect the data they own
- Cut costs by eliminating stale data and accounts and automating audit requirements

Email has become the most common way for employees to collaborate both with each other and the outside world. The Microsoft Exchange infrastructure is often a target for malicious activity as it stores vast amounts of sensitive data. Additionally, spoofing an identity over email could cause serious damage, e.g. sending fake emails as a company's CEO. Microsoft Exchange is particularly vulnerable; every user owns his own mailbox and could unintentionally overexpose it. A successful data breach is very likely to result in sensitive data exposure, heavy direct financial loss, serious reputation damage and increased audit requirements.

## How SecurityIQ Can Help

To effectively protect the unstructured data stored in Microsoft Exchange, organizations need a technology to provide them with full visibility into who can access mailboxes and folders, and who is 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.



SecurityIQ dramatically reduces security risk and increases 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
- Electing the rightful data owners and enabling them to protect their own data
- Extending the IAM strategy to provide access governance to unstructured data

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

## SecurityIQ Key Features and Benefits

### Context-Aware Activity Monitoring with Real-Time Alerting

Time is of the essence when it comes to data security, so activity monitoring in SecurityIQ is done in real-time. Every monitored activity is enriched with its full security context from in place security systems (Active Directory, IAM or any other data source). The full context is crucial to identify violations and respond to them in real-time, and it is also available when performing forensics and activity policies.

### Permissions Collection and Analytics

SecurityIQ automatically collects and analyzes all granted entitlements on user mailboxes, 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. SecurityIQ is the only product on the market to utilize crowdsourcing techniques to elect the rightful data owners. The elected owners are provided with a set of dedicated dashboards to enable 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. SecurityIQ streamlines access requests and manages periodic and risk-based access reviews for unstructured data. The system can also automate provisioning and revocation of access (access fulfillment) to reduce costs, IT workload and to avoid potential human errors.

### Microsoft Exchange Server and Online Support

To ensure your entire Microsoft Exchange infrastructure is protected, SecurityIQ covers both Microsoft Exchange on-premises and online by the same license. SecurityIQ can also be used to clean an on-premises environment before moving to Microsoft Exchange online to align with best practices, reducing risks and costs. SecurityIQ fully supports hybrid architecture where some mailboxes and public folders are on-premises while others are in the cloud.

## About SailPoint

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of global organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices and in the cloud. The company's innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning and access management delivered on-premises or from the cloud (IAM-as-a-service). For more information, visit www.sailpoint.com.