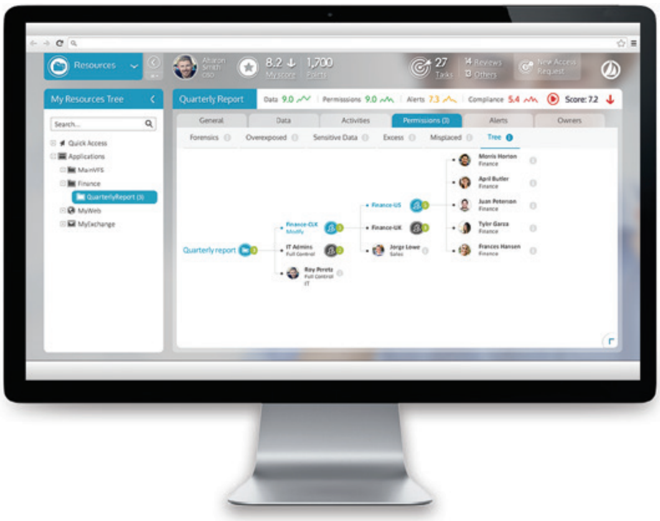
SecurityIQ

Complete Access Governance for Unstructured Data

SailPoint

Managing access to unstructured data is a growing problem. The amount of data stored in file servers and NAS devices, collaboration portals, mailboxes, and cloud folders has increased exponentially over the past few years. Yet, with no easy means to track, control, and protect unstructured data, organizations face growing security, legal and regulatory risks.

SailPoint, the recognized leader in identity and access management (IAM), helps organizations protect unstructured data with SecurityIQ, a business-oriented access governance solution that works seamlessly with SailPoint's IAM solutions to discover sensitive data throughout the enterprise and control access to it. With SailPoint, organizations can centrally manage and control access to both structured and unstructured data, applying consistent administrative processes, policies and controls.



Organizations with unmanaged, unprotected data face tremendous risks. SecurityIQ reduces risk by identifying where sensitive data resides, determining who has access to it and how they are using it, and putting effective controls in place to secure it. SecurityIQ helps organizations meet regulatory requirements by providing proof of compliance during audits and increases staff productivity by reducing time spent on diagnostics, forensics, and data administration tasks. It also simplifies the ongoing challenge of managing how users are granted access to unstructured data throughout a user's lifecycle within the organization.

Data Discovery and Classification

Find Where Sensitive Data Resides

In most organizations, sensitive information such as financial data, customer data, credit card information, and personal health information can be found in hundreds of places – on file shares, on SharePoint sites, in cloud storage services, and in email folders. SecurityIQ allows organizations to find and classify sensitive information, so that they can put effective controls in place to manage and protect it. SecurityIQ allows you to:

- Analyzes files for sensitive data using keywords, wildcards, and regular expressions
- Uses verification algorithms for common data types to improve accuracy and eliminate false positives
- Provides flexible methods for classifying sensitive data using content-based or behavior-based approaches
- Leverages activity monitoring to classify data based on how it is used

Permissions Management

Determine Who Can Access Sensitive Data

Access to unstructured data is impossible to manage and control without full visibility "effective access." SecurityIQ automatically collects and analyzes effective permissions across on-premise Windows file-servers, NAS devices, SharePoint and Exchange, as well as cloud-based portals, including: Office 365, Box, Dropbox, and Google Drive.

- Gain full visibility into effective access for all of an organizations' data from a single dashboard
- Identify and remediate overexposing access to sensitive data (open shares, sites, mailboxes, etc.)
- Report and remediate unused entitlements by cross-checking effective access with activity monitoring
- Ensure access management for unstructured data is aligned with best practices across the enterprise

Data Activity Tracking

Discover Who Accessed Sensitive Files and More

To prevent security breaches and information theft, or minimize the potential damage of this activity, organizations need real-time tracking of users that access sensitive files or change file permissions, as well as the ability to respond to violations in real-time. SecurityIQ captures events for all users on monitored resources, and enriches these events with user and machine details gathered from directories, IAM systems, HR applications, and any other data source.

Through its intuitive graphical interface and reports, SecurityIQ allows detailed forensic analysis and data usage auditing, addressing questions such as:

- Who has accessed this folder?
- What data has this user been accessing?
- Who accessed mailboxes not self-owned?
- Who changed this group's membership?
- What data is stale and for how long?

Complete Coverage

Extend Your IAM Strategy

SecurityIQ shares information with SailPoint IAM systems to provide comprehensive governance of access to unstructured data. By augmenting IAM data from structured systems with permission data from unstructured data targets, your organization can more quickly identify risks, spot compliance issues, and make the right decisions to strengthen controls.

- Provides centralized visibility across structured and unstructured data in the enterprise – all applications, all data, and all users
- Adds unstructured data targets to preventive and detective controls, such as access certifications and separation-of-duty (SoD) policy enforcement
- Automates provisioning of access to unstructured data repositories and revocation of inappropriate access
- Informs the IAM system with real-time activity data to improve risk mitigation and understand appropriate use

SailPoint

SecurityIQ Allows Customers to:

Mitigate Risk of Inappropriate Access

Improve Audit Performance

Decrease Operational Costs

Improve IT staff productivity

The difference is clear.

- SecurityIQ delivers comprehensive discovery, classification, and monitoring of unstructured data – on premises and in the cloud.
- SecurityIQ shares information seamlessly with SailPoint's IAM solutions to centrally manage and control all enterprise applications and data (structured and unstructured).
- SecurityIQ can be up and running quickly with rapid deployment connectors monitoring and classification best practices delivered out-of-the-box.

Corporate Headquarters

11305 Four Points Drive
Building 2, Suite 100
Austin, Texas 78726

512.346.2000
USA toll-free 888.472.4578

www.sailpoint.com

Global Offices

UK	+44 (0) 845 273 3826
Netherlands	+31 (0) 20 3120423
Germany	+49 (0) 69 50956 5434
Switzerland	+41 (0) 79 74 91 282
Australia	+61 2 82498392
Singapore	+65 6248 4820
Africa	+27 21 403 6475

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 portfoliooffers 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.