FILESERVER SECURITYIQ INTEGRATION DATASHEET

SailPoint
MANAGING THE BUSINESS OF IDENTITY

SecurityIQ for File Shares

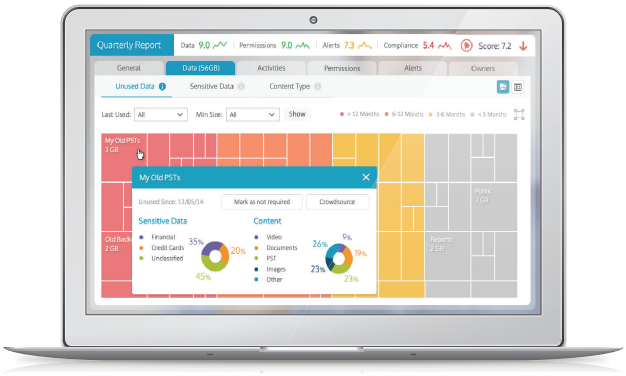
BENEFITS:

- Identify who has effective access to what data, and who is actually using it
- Track and respond to real-time activities on file shares
- Reduce risk by addressing overexposed data and excess access requests
- Minimize response time to breaches and minimize damage
- Identify where sensitive data resides to focus on the data you value most
- 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

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. It is everywhere, and out of control. File shares enable employees and contractors to collaborate and have access to data when and where they need it. From a risk perspective, the vast amount of data maintained in file shares makes it a high priority target for any malicious activity. 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 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 solution must have a complete understanding of file servers and network attached storage activities and permissions model, while not affecting the performance of the protected environment.



SecurityIQ dramatically reduces security risk and increases compliance by:

- Identifying where sensitive data resides, determining who has effective access to it, how it is used and putting effective 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 decide who should and shouldn't have access to the data that they know best
- Extending the IAM strategy to provide comprehensive access governance to unstructured data

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

FILESERVER SECURITYIQ INTEGRATION DATASHEET

SailPoint
MANAGING THE BUSINESS OF IDENTITY

SecurityIQ Key Features and Benefits

Data Classification

Data classification assists in locating your valuable, highly confidential information (HCI). SecurityIQ can search for common or proprietary data types in files based on their content (keywords, wildcards, regular expressions, and metadata) or on how the files are being used by an organization's employees. SecurityIQ is delivered with built-in verification algorithms (e.g. 'Luhn' for PCI data, etc.) to eliminate false-positives.

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 your file shares and network attached storage devices. It analyses effective permissions for NTFS folders while considering Share and Deny 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.

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.

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