



When Identity Meets Data

Data Access Governance Solutions for the Enterprise

Nicola Venditti, SailPoint Partner Enablement Manager

- 
- 1. Our point of view to data security and governance**
 - 2. The GDPR challenge**
 - 3. How we help with GDPR compliance**



SailPoint approach to data security



71%

of staff have
access to data they
should not see

Ponemon Institute Report

80%

of company data is
held in unstructured
content

Forbes Report

1 in 7

employees will sell
their credentials for
\$150

SailPoint Survey

89%

believe they are
now at risk from
insider threat

IT Governance Report



Do you know **WHERE** your (Sensitive) data is?



Do you know **WHO** has access to it?



Is the access **APPROPRIATE**?



Can you **PROVE** it?

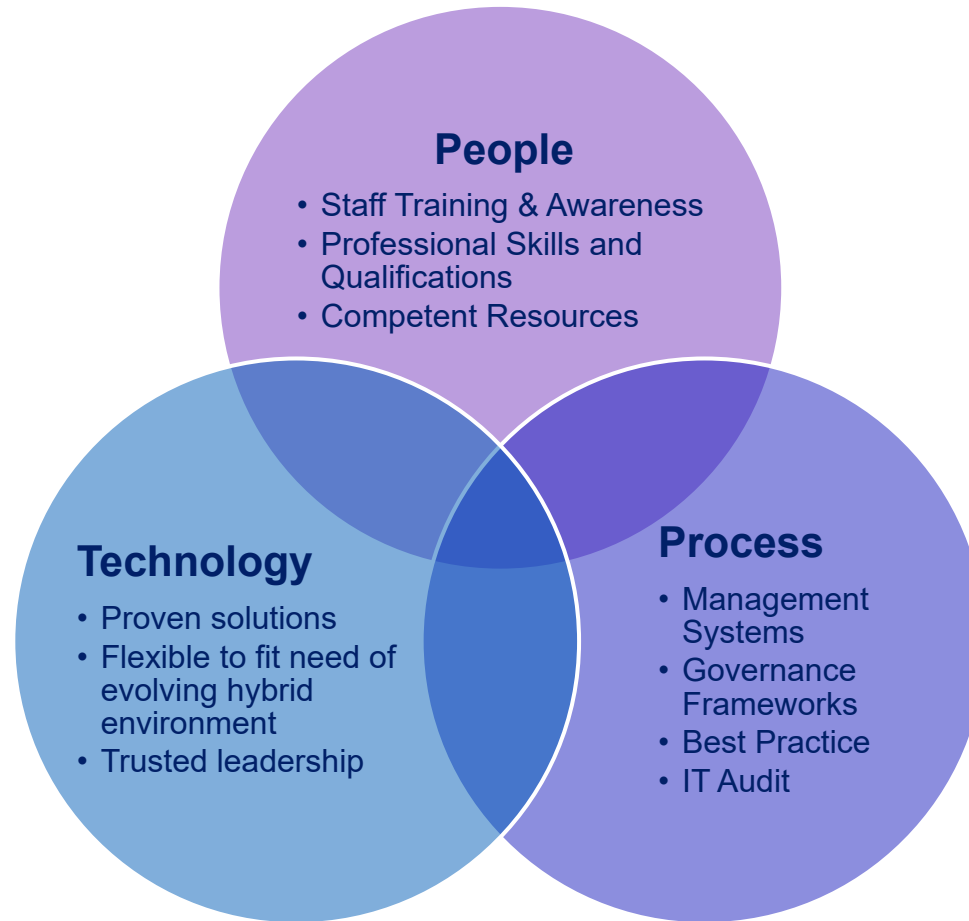
**\$158 per lost or
stolen record**

2016 Cost of Data Breach Study: Global Analysis -
Ponemon Institute© Research Report



The GDPR Challenge

GDPR Solution: It's not just Technology



Highlights

Consent

Breach
notification

Right to access

Right to be
forgotten

Data portability

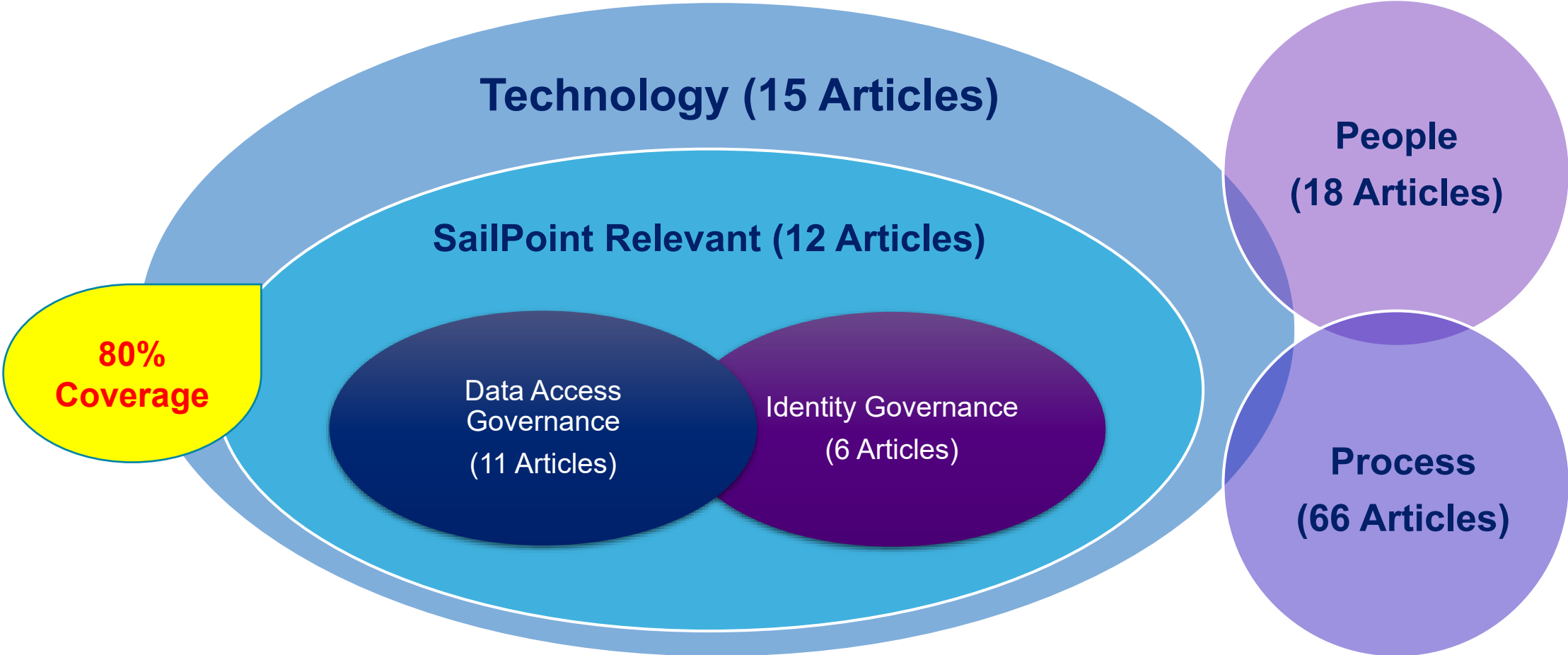
Privacy by design

Personas

GDPR Compliance

- ✓ Worldwide application of a European data protection law
- ✓ Stringent rules for the protection, management and control of any EU citizen personally identifiable information (PII)
- ✓ Significant financial penalties for data breaches involving EU citizen PII, ranging from a minimum of €20 million up to 4% of an organization's global annual revenue
- ✓ Required material changes in how and where organizations store customer data
- ✓ A new data breach notification requirement
- ✓ New data privacy governance, data mapping and impact assessment requirements
- ✓ A requirement to implement "privacy by design and by default"

Technology Relevance to GDPR





How SailPoint helps with GDPR compliance

SailPoint's Four Stage Approach

VISIBILITY

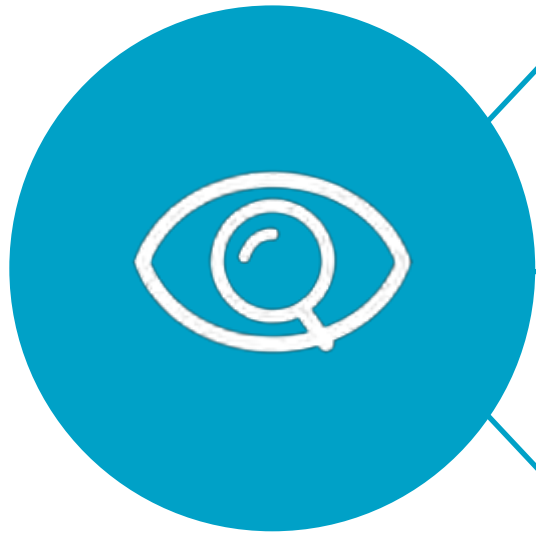
CONTROL

COMPLIANCE

REMEDIATION

STAGE 1: Visibility

You can't protect what you can't see



PERMISSION ANALYSIS

Identify who has access to what data (direct & indirect)

IDENTIFY WHO IS ACCESSING DATA

**Monitor activity in real-time on-premises and in the cloud
Enrich with Identity Data to enhance queries**

LOCATE SENSITIVE DATA

Classify data based on content or behavior

Over-Exposed Resources

The screenshot displays the SailPoint interface with the 'Permissions' section selected. The 'Overexposed View' is active, showing a list of resources with their respective permissions and sensitive data indicators. The 'Resources Tree' on the left shows the hierarchy: All Applications > SIO - Windows File Server > XS > Data. The main table lists the following resources and permissions:

Path	Permission Subject	Permission Type	Sensitive Data
\\siq\XS\Data\TestData\TestData\Healthcare Data	siq\Users	Read & Execute	PCI \ General
\\siq\XS\Data\TestData\TestData\Healthcare Data	siq\Users	Create folders / Append Data	PCI \ General
\\siq\XS\Data\TestData\TestData\Healthcare Data	siq\Users	Create files / Write data	PCI \ General
\\siq\XS\Data\TestData\TestData\Credit Card Tests	siq\Users	Read & Execute	PCI \ General
\\siq\XS\Data\TestData\TestData\Credit Card Tests	siq\Users	Create folders / Append Data	PCI \ General
\\siq\XS\Data\TestData\TestData\Credit Card Tests	siq\Users	Create files / Write data	PCI \ General
\\siq\XS\Data\Share	siq\Users	Read & Execute	
\\siq\XS\Data\Share	siq\Users	Create folders / Append Data	
\\siq\XS\Data\Share	siq\Users	Create files / Write data	
\\siq\XS\Data\Departments\Accounting\Acct_2015\Q4_15	Everyone	Full Control	

At the bottom of the table, it indicates 'Showing 1-10 of 1 Results' with navigation buttons for 1, 2, and 3 pages.

Granular Permission Visibility

The screenshot displays the SailPoint user interface, specifically the 'Permissions' section. The top navigation bar includes 'Dashboard', 'Resources', 'My Tasks', 'Reports', 'Goals', and 'Settings'. A secondary navigation bar shows 'Dashboard', 'Activities', 'Permissions', 'Data', 'Alerts', and 'Owners'. A 'New Access Request' button is visible in the top right corner.

The main content area is titled 'Permissions > Tree View'. It shows the 'Resource: project_X' with the following details:

- Application: SERI - Windows File Server
- Path: \\ad-resource\Data\Projects\project_X

The permissions tree for 'project_X' is as follows:

- project_X
 - Everyone: Read & Execu...
 - Everyone: Full Control
 - Everyone: Share FullC...
 - Training: SERI, Read & Execu...
 - Michelle Per...: SERI, Human Resour..., Full Control
 - SYSTEM: NT AUTHORITY, Full Control

On the right side, a list of users is shown with their roles and permissions:

- Elizabeth Ta...: SERI, Human Resour..., Read & Execu...
- Kevin Philli...: SERI, Human Resour..., Read & Execu...
- Laura Turner: SERI, Human Resour..., Read & Execu...
- Michelle Per...: SERI, Human Resour..., Read & Execu...
- Sarah Campbe...: SERI, Human Resour..., Read & Execu...

A context menu for Elizabeth Taylor (SERI) is open, showing the following options:

- Revoke This Permission
- Revoke All Permissions
- Add Permission
- Show User's Permission Paths

The left sidebar contains a 'Resources Tree' with a search bar and a 'Quick Access' section. The 'All Applications' section is expanded to show 'SERI - Windows File Server' > 'Data' > 'Projects' > 'project_X'.

Locating Sensitive Data with Classification

Two types of Data Classification

Classify Based on Content



Classify Based on Population



Configuring Data Classification Policies

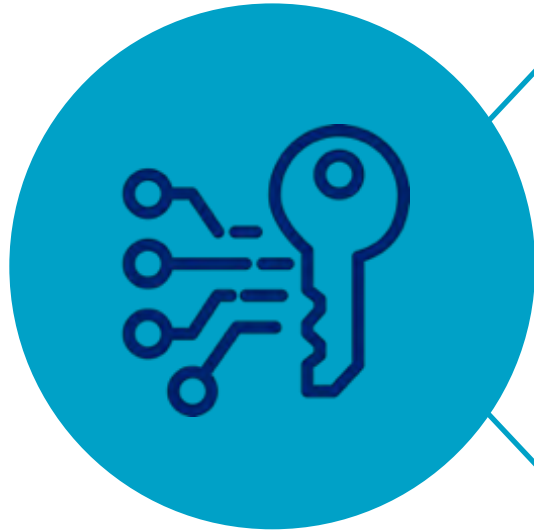
The screenshot shows the SailPoint interface for configuring a Data Classification Policy. The top navigation bar includes the SailPoint logo, menu items like 'GDPR Dashboard', 'Resources', 'My Tasks', 'GDPR Reports', 'Compliance', 'Forensics', 'Goals', and 'Settings', and a user profile for 'SERIAdminstr...'. A secondary navigation bar shows 'Access Certification' and 'Data Classification'. The main content area is titled 'Edit Policy' and contains the following sections:

- Policy Name***: A text input field containing 'General Data Protection Regulation (GDPR)'. To its right is a toggle switch labeled 'Activate / Deactivate Policy' which is currently 'Active', and an 'Owner' field with the value 'System'.
- Description**: A text area containing the text 'Detect personal information relating to residents of the European Union (EU), as required by GDPR.'
- Scope**: A section with a note: 'Note: Default scope of this policy is 'All'. You can narrow it down by selecting specific application or application type'. It includes a 'Scope Type' dropdown menu set to 'Application type' and an 'Application type' search box with '0 Selected' items and a 'Clear Selection' link.
- Rules Assigned (6 active rules)**: A list of six system rules, each with an active toggle switch and a dropdown arrow:
 - EU Phone Number (System Rule | Type - Content)
 - EU IBAN Bank Code (System Rule | Type - Content)
 - EU ID Number (System Rule | Type - Content)
 - EU ID Terms (System Rule | Type - Content)
 - EU Zip Codes (System Rule | Type - Content)
 - EU License Plate (System Rule | Type - Content)

At the bottom right, there is an 'Activate Windows' watermark and a 'Save' button.

STAGE 2: Control

Establish business accountability over data



AUTOMATE DETECTION AND RESPONSE

Respond in real-time to policy violations

STREAMLINE ACCESS REQUESTS

Ensure only the people who need the access get it

DATA OWNERS ELECTION AND ENABLEMENT

Utilize targeted crowdsourcing for the best accuracy

Real-Time Access Policies

The screenshot displays the SecurityIQ web interface. The top navigation bar includes 'Activities', 'Compliance', 'Permissions', 'Policies', and 'System'. The left sidebar shows a navigation tree with 'Access Policy' selected. The main content area is titled 'Access Policy' and shows a list of sub-resources for 'SERI - Windows File Server'. A modal dialog box titled 'Welcome to the Edit Rule Wizard' is open, displaying the 'Rule Requirements' configuration screen. The dialog prompts the user to 'Please add at least one requirement to the rule in order to continue'. It features a 'Create a Requirement' section with dropdowns for 'Question', 'Attribute', 'Operator', and 'Value'. An 'Add Rule Requirement!' button is located at the bottom of this section. To the right, a 'Rule Requirements' list shows three configured requirements: 'Action Type Equals Read File', 'File Extension Equals secret', and 'User Name Not Equals Administrator'. The dialog also includes 'Cancel', 'Back', 'Finish', and 'Next' buttons.

Data Owners: Choosing The Right Person

The Traditional Approach



The SecurityIQ Approach (Patent-Pending)



Owner Election

SailPoint Dashboard Resources **My Tasks** Reports New Access Request My Requests 1 Amanda Ross (S...

Access Certification Access Request Compliance Control **Owners Election** My Requests

Owners Election

Who owns the following resource?
 \\ad-resource\Data\Projects\project_X

Files you used in this resource:

- X_MovedFile.txt (0 minutes ago)
- X_NewFile.txt (0 minutes ago)
- X_Project_Plan.txt (9 minutes ago)
- Animals.txt (0 minutes ago)
- PCI.txt (9 minutes ago)
- fish1.txt (9 minutes ago)

Vote for the user(s) who would be the most suitable owner(s) of the resource

SERI\Administrator Vote	Amanda Ross (SERIAma...) Regional Operations Vote	I don't know Vote
Ernest Wagner (SERIEm...) Information Technology Vote	Albert Woods (SERIAiber...) Engineering Vote	Suggest other user Add
Alice Ford (SERIAlice.Ford) Information Technology Vote		

[Discard](#) [Commit](#)

STAGE 3: Compliance

Automate data access compliance controls



AUTOMATE PROOF OF COMPLIANCE

Implement audit controls for GDPR, SOX, PCI, etc.

STREAMLINE ACCESS REVIEWS

Grant access on a “need-to-know” basis

STALE DATA DETECTION

Comply with regulations and reduce storage costs

Setting up a Review Campaign

SailPoint | GDPR Dashboard | Resources | My Tasks | GDPR Reports | **Compliance** | Forensics | Goals | Settings | [New Access Request](#) | | SERI/Administr...

Access Certification ▾ | Data Classification ▾

Everyone Access to Folders

[End Campaign](#) [Hide Details](#)

Template : No Template **Owner :** Me **Type :** Permissions **Status :** ⌚ Review In Process

Start Date : 10/16/2017 **Due Date :** 4/16/2018 **End Date :** No End Date Yet

Description : This campaign targets folders where everyone has access

[Pending Records Per Reviewers](#) | [All Records](#)


[Bulk Actions](#) ▾ [Filters](#)

<input type="checkbox"/>	Reviewer	Level #	Level Name	Pending Records	Actions
<input type="checkbox"/>	Michelle Perez	1	Owner	104	
<input type="checkbox"/>	Paul Walker	2	Security Council	53	
<input type="checkbox"/>	Dorothy Robinson	2	Security Council	53	

Show Per Page Showing 1-3/3 Results [«](#) **1** [»](#)

[Close](#)

Access Review

SailPoint Dashboard Resources **My Tasks** Reports New Access Request My Requests 1 

Access Certification Access Request Compliance Control Owners Election My Requests

Access Certification - Departments Folder Certification Progress: 0 / 6 complete (0%)

Bulk Actions View graph Filters (1)

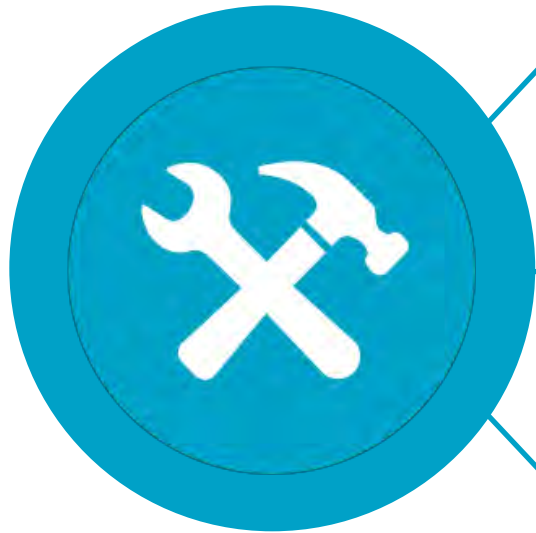
Business Resource Name	Business Resource Full Path	User Name	User Display Name	Group Na...	IIQ Employee Type	IIQ Job Title	IIQ Department	IIQ	Actions
Departments	\\ad-resource\Data\Departments	Administra...							Approve Reject Comment More
Departments	\\ad-resource\Data\Departments	SYSTEM							Approve Reject Comment More
Departments	\\ad-resource\Data\Departments	Aaron Nic...	Aaron Nichols		Employee	Operations M...	Executive Man...	1c	Approve Reject Comment More
Departments	\\ad-resource\Data\Departments			Everyone					Approve Reject Comment More
Departments	\\ad-resource\Data\Departments			Everyone					Approve Reject Comment More
Departments	\\ad-resource\Data\Departments	Administra...		Domain A...					Approve Reject Comment More

Show 10 Per Page Showing 1-6/6 Results 1

6 permission(s) pending commit Close Commit (6)

STAGE 4: Remediation

Eliminate risk with actionable intelligence



ACTIONABLE DASHBOARDS FOR IT & BUSINESS

Enable every stakeholder to act on risks

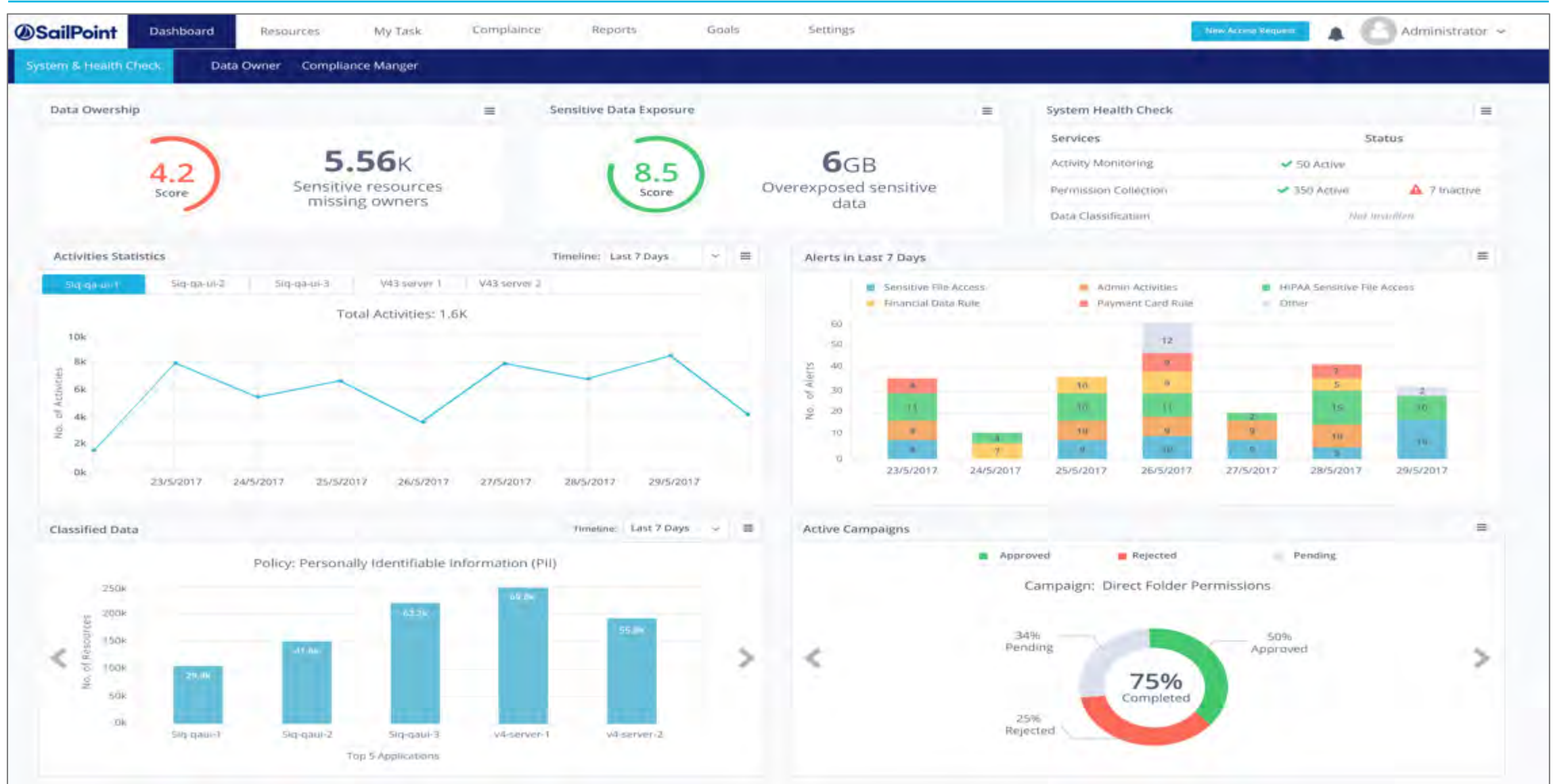
ACCESS NORMALIZATION & CLEANUP

Simplify access structure to enable automatic fulfillment

AUTOMATED ACCESS FULFILLMENT

Avoid human errors while reducing IT workload

Dashboard



SecurityIQ – Functional Summary

VISIBILITY

Discovery & Classification
Where does the sensitive data reside?

Real-time Activity Monitoring
Who is accessing what data?

Permissions Analysis
Who has access to what data?

Identity Enrichment – Adding business context to permissions and activities

CONTROL

Data Owners Election
Who owns the data in a resource?

Real-time Access Policies
Who validates access policies?

Access Requests
Avoid access management chaos

COMPLIANCE

Compliance Insights
Who validates compliance controls?

Access Reviews
Which permissions are stale/ excess?

Access Simulations
What if impact analysis to ID risks

REMEDIATION















Access Normalization
Align with best practices

Access Fulfillment
Save time and avoid human errors

Actionable Dashboards
For IT, data owners & business users

*** Relevant to GDPR**

SecurityIQ – Supported Endpoints

SecurityIQ for Windows File Shares (CIFS)	 Windows	 HITACHI DATA SYSTEMS	 EMC²	 NetApp
SecurityIQ for Unix/Linux File Shares (NFS)	 EMC²	 NetApp	NFS	DFS
SecurityIQ for Exchange	 Exchange	 Exchange Online	 Office 365	
SecurityIQ for SharePoint	 SharePoint	 SharePoint Online		
SecurityIQ for Cloud Storage	 box	 Google Drive	 Dropbox	 OneDrive for Business

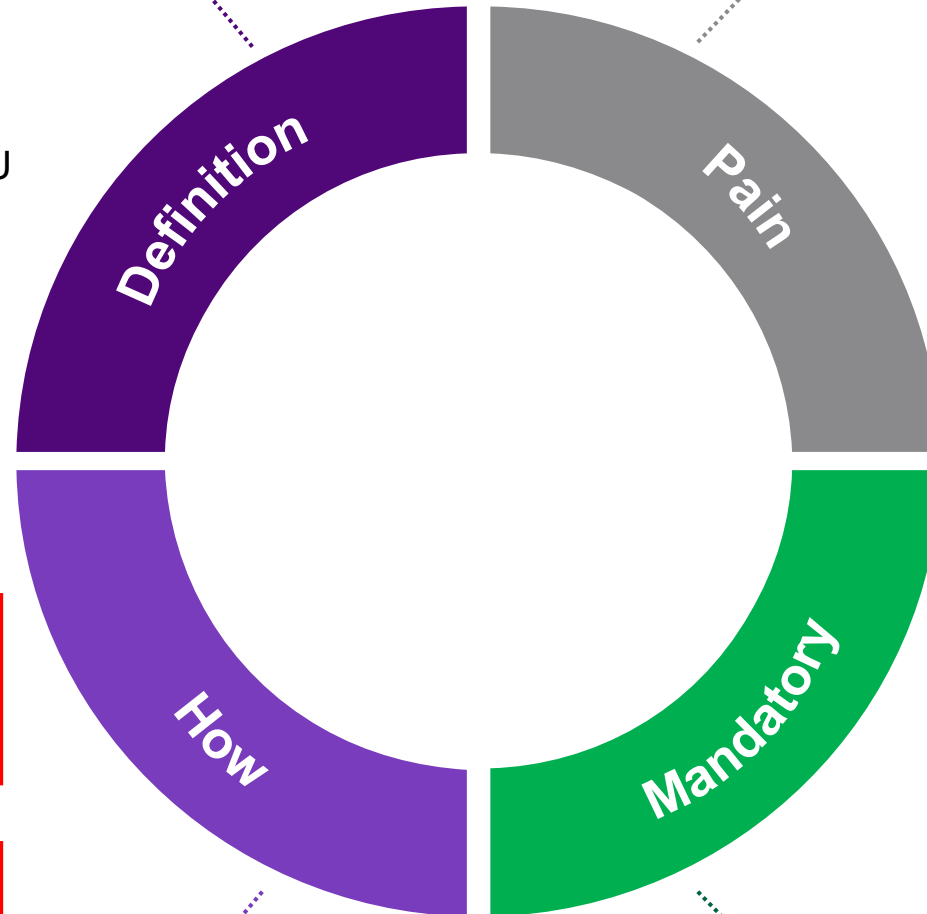
GDPR Coverage

What is it?

- Homogenous Data privacy law
- All organizations processing EU citizen data
- Live date May 2018
- Unstructured data in scope
- 28 PII conventions

Data Access Governance

- Privacy Policies
- Data Discovery
- Need to know basis access
- Retention Policies
- Breach detection & Disclosure



Sanctions & litigation risk

- Fines: 4% of annual revenue or €20m
- Breaches notified to regulator within 72 hours
- Citizen compensation lawsuits
- Audit, Clean up, reputation

Governance & Compliance

- Data Protection Officers
- Data owner accountability
- Least privilege principle
- Breach disclosure
- Fine grained audit trails

Why Customers Choose SecurityIQ



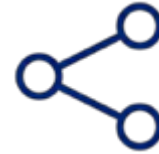
Business Focused

Enable and Empower
Best User Interface



Innovative

Crowdsource
owner election



Connectors & Coverage

Supports On-
Premises and
Cloud



Powered with Identity

Dynamic content
enrichment

More info:

1. **GDPR Compliance:**

<https://www.sailpoint.com/business/gdpr-compliance>

2. **(Free ebook) Step-by-step Guide GDPR Compliance with Identity Governance:**

<https://www.sailpoint.com/resources/gdpr-compliance-identity-governance-guide>

3. **(Free ebook) Meeting the Challenge of GDPR Compliance:**

<https://www.sailpoint.com/resources/meeting-challenges-of-gdpr-compliance/?elqct=Blog&elqchannel=MeetingGDPRReq>

4. **(Podcast) Mistaken Identity Episode 9 (GDPR):**

<https://www.sailpoint.com/blog/mistaken-identity-episode-9-gdpr>

5. **(Video) Sailpoint Youtube Channel:**

<https://www.youtube.com/user/IdentityIdol/search?query=gdpr>



Thank You