SOLUTION OVERVIEW

Spirion Enhanced Analytics (SEA) Service

For smarter insights about your sensitive data risk posture, turn to the SEA

Companies eager to rein in runaway data volumes and minimize their organization’s risks are turning to Spirion Sensitive Data Platform (SDP). With Spirion SDP, Privacy-Grade data discovery and purposeful classification act as the foundation of your data security and privacy program. It quickly and automatically discovers, classifies, and remediates almost any form of sensitive data or personally identifiable information (PII) anywhere—on-premises, in the cloud, and on endpoints like employee workstations and laptops.

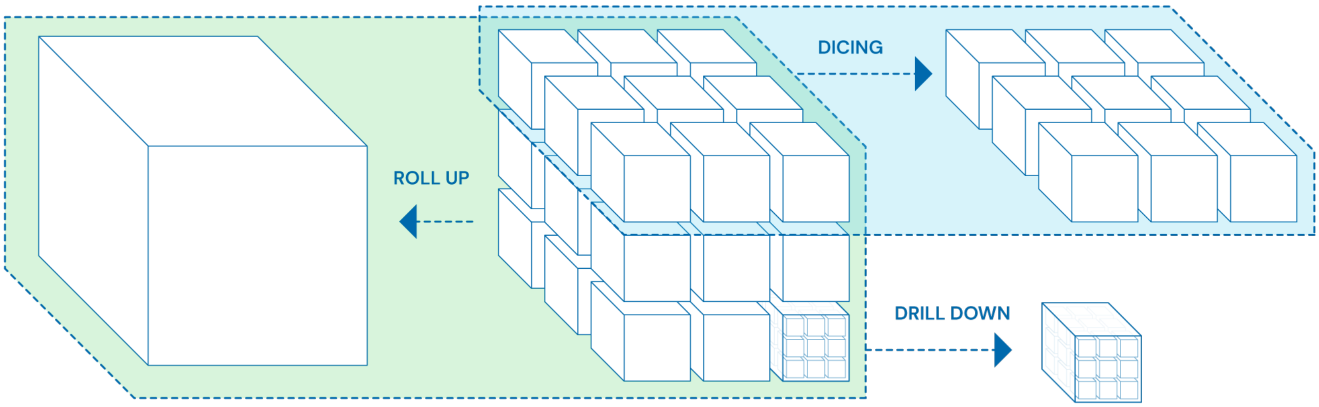
To help you gain clarity and insight into organizational risks associated with your sensitive data, Spirion offers out-of-the-box reports and risk-based dashboards. These analytics support data-driven decision making to prioritizing data protection initiatives, prove compliance, demonstrate progress on initiatives, report on cyber risks to executives and boards, and more.

The SEA Dives Even Deeper

For even more control and customization in managing your data environment, Spirion Enhanced Analytics (SEA) delivers a powerful pipeline to easily build your own data models and visualizations. This new add-on option to Spirion Sensitive Data Platform (SDP) can analyze hundreds of millions of records with enterprise-grade data model capabilities from nearly any analytics platform. Data is processed at the SEA level, so you can conduct powerful, complex analyses in seconds. Merge SDP data with metrics from your other data management systems for a holistic view of your organization’s security and privacy key performance indicator (KPIs). Instantly analyze months or years of historical data to track progress and detect patterns.

The SEA will perform queries very quickly, deliver high data throughput, and provide enough flexibility for end users to “slice and dice” the data for closer examination to meet a variety of demands—whether at a high level or at a very fine, detailed level.

Once you’ve created your views, your reports are automatically refreshed, so the most recent information is always available. With SEA, spend your time creating, implementing, and tracking well-informed data protection strategies—instead of wrangling, sorting, and filtering reports every month that are already obsolete by the time you create them.



Key Capabilities

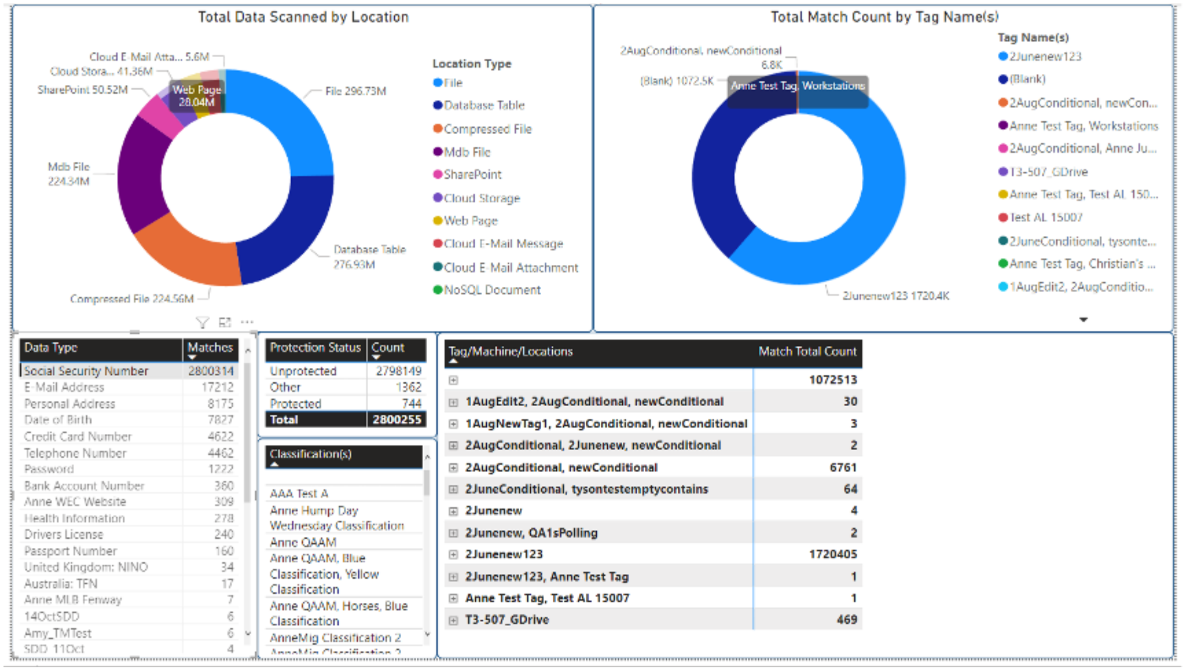
- **Standardized, multi-dimensional data warehouse** – Efficiently consolidate and analyze large volumes of data efficiently in ways that a traditional database cannot; slice and dice, conduct ad hoc queries, model what-if scenarios, and more
- **Access to full schema to derive results** – Draw connections between data points extracted from SDP and other sources to create a single semantic model, providing a structured, streamlined view of your data
- **Platform connectivity** – Simple ODBC connectivity to analyze data from nearly any platform, including BI tools (e.g., Power BI and Tableau), SIEMs (e.g., Splunk), and other applications
- **Performance** – The SEA can quickly analyze and return results from even the most data-intensive, complex queries.
- **Self-service analytics** – User-friendly interface enables data analysts to quickly navigate the SEA to create custom reports
- **Scalability** – As your organization evolves, so too do requirements around data and data usage; as the data volume grows, the SEA can scale up to meet the analytics and performance needs of any organization
- **Integrated** – The SEA integrates SDP data, your existing spreadsheets, and source systems into one, enabling you to populate models, reports, and spreadsheets with real-time actuals data for a holistic view of your data privacy and security programs
- **Time-variant** – View the shifting tides in your data landscape with the SEA; view changes over months or even years to track progress and to pinpoint trends and emerging risks
- **Automatically refreshed** – Reports are continually updated so you always have access to the most current content

Benefits

- Pull critical security and privacy insights across SDP and other platforms for a comprehensive view of your sensitive data risk posture
- Powerful data warehouse processing to quickly return results from even the most complex, data-intensive queries
- Spend less time on manual data management and more time deriving insights
- Monitor key trends and metrics over time to track the progress of your risk reduction initiatives
- Develop visualizations and forward-looking business intelligence to better understand your organization's and teams' performance and predict future risks
- Continually refreshed analytics keep pace with today's rapidly evolving privacy and security environments
- Analyze data in your favorite BI or SIEM platform to create reports and visualizations that transform data into actionable findings
- Empower end-users to run their own analyses and visualizations for more impactful insights
- Run "what-if" scenarios and view historical trending to inform practical decisions based on more comprehensive analysis

Model Reports from these Attributes

VARIABLE	DESCRIPTION
Scan Type	Final action taken; how the issue was resolved, e.g., sensitive data was quarantined, redacted, encrypted, etc.
Scan Name	Name assigned to the scan
Date/Time (Discovered)	First date/time the location/match was found
Date/Time (Most Recent)	Date/time the location/match was most recently found
Playbook(s)	Playbook used in scan that found the match/location
Playbook Status	Complete, Incomplete, Error, etc.
Data Type	Type of data found (credit card, social security number, etc.)
Classification(s)	Classifications applied by Playbook for sensitivity and other context
Location	Full string that defines data object (e.g. file with folder path)
Resolution	Final action taken; how the issue was resolved, e.g., sensitive data was quarantined, redacted, encrypted, etc.
Total Location Match	Count of matches in a specified location (e.g. file)
Agent	Scanning Agent that found match/location
Target	Name of machine being scanned
File Owner	Name of person who owns file
Assignee	Match/location assignment from Playbook
Tag Name(s)	Tag groups that have been assigned to the target asset
File Type	Type of file identified (PDF, docx, etc.)
Database Column Name	Name of column containing match in database target
Database Primary Key	Primary key value for matches found in database targets
Location Type	General type of asset (Gmail, local machine, etc.)
Last Modified Date	Date when file was last modified
Last Accessed Date	Date when file was last accessed as indicator of whether file is still being used
Match Total Count	Total count of matches in the location
Locations Scanned Total	Count of total locations scanned


Total Data Scanned by Location
Cloud E-Mail Atta... 5.6M
Cloud Stora... 41.36M
SharePoint 50.52M
Web Page 28.04M
File 296.73M
Mdb File 224.34M
Database Table 276.93M
Compressed File 224.56M
Location Type
● File
● Database Table
● Compressed File
● Mdb File
● SharePoint
● Cloud Storage
● Web Page
● Cloud E-Mail Message
● Cloud E-Mail Attachment
● NoSQL Document
Total Match Count by Tag Name(s)
2AugConditional, newConditional 6.8K
(Blank) 1072.5K
Anne Test Tag, Workstations
2Junenew123 1720.4K
Tag Name(s)
● 2Junenew123
● (Blank)
● 2AugConditional, newCon...
● Anne Test Tag, Workstations
● 2AugConditional, Anne Ju...
● T3-507_GDrive
● Anne Test Tag, Test AL 150...
● Test AL 15007
● 2JuneConditional, tysonte...
● Anne Test Tag, Christian's ...
● 1AugEdit2, 2AugConditio...

Data Type	Matches
Social Security Number	2800314
E-Mail Address	17212
Personal Address	8175
Date of Birth	7827
Credit Card Number	4622
Telephone Number	4462
Password	1222
Bank Account Number	360
Anne WEC Website	309
Health Information	278
Drivers License	240
Passport Number	160
United Kingdom: NINO	34
Australia: TFN	17
Anne MLB Fenway	7
14OctSDD	6
Amy_TMTest	6
SDD 11Oct	4

Protection Status	Count
Unprotected	2798149
Other	1362
Protected	744
Total	**2800255**

Classification(s)
AAA Test A
Anne Hump Day Wednesday Classification
Anne QAAM
Anne QAAM, Blue Classification, Yellow Classification
Anne QAAM, Horses, Blue Classification
AnneMig Classification 2

Tag/Machine/Locations	Match Total Count
⊞	**1072513**
⊞ **1AugEdit2, 2AugConditional, newConditional**	**30**
⊞ **1AugNewTag1, 2AugConditional, newConditional**	**3**
⊞ **2AugConditional, 2Junenew, newConditional**	**2**
⊞ **2AugConditional, newConditional**	**6761**
⊞ **2JuneConditional, tysontestemptycontains**	**64**
⊞ **2Junenew**	**4**
⊞ **2Junenew, QA1sPolling**	**2**
⊞ **2Junenew123**	**1720405**
⊞ **2Junenew123, Anne Test Tag**	**1**
⊞ **Anne Test Tag, Test AL 15007**	**1**
⊞ **T3-507_GDrive**	**469**

Executive-level visualization was created in Power BI. It shows how many sensitive data matches were found and protected to understand the total impact of the risks, since a single file may contain hundreds of personal data records.

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion has relentlessly solved real data protection problems since 2006 with accurate, contextual discovery of structured and unstructured data; purposeful classification; automated real-time risk remediation; and powerful analytics and dashboards to give organizations greater visibility into their most at-risk data and assets. Visit us at spirion.com