SPIRION

SOLUTION OVERVIEW

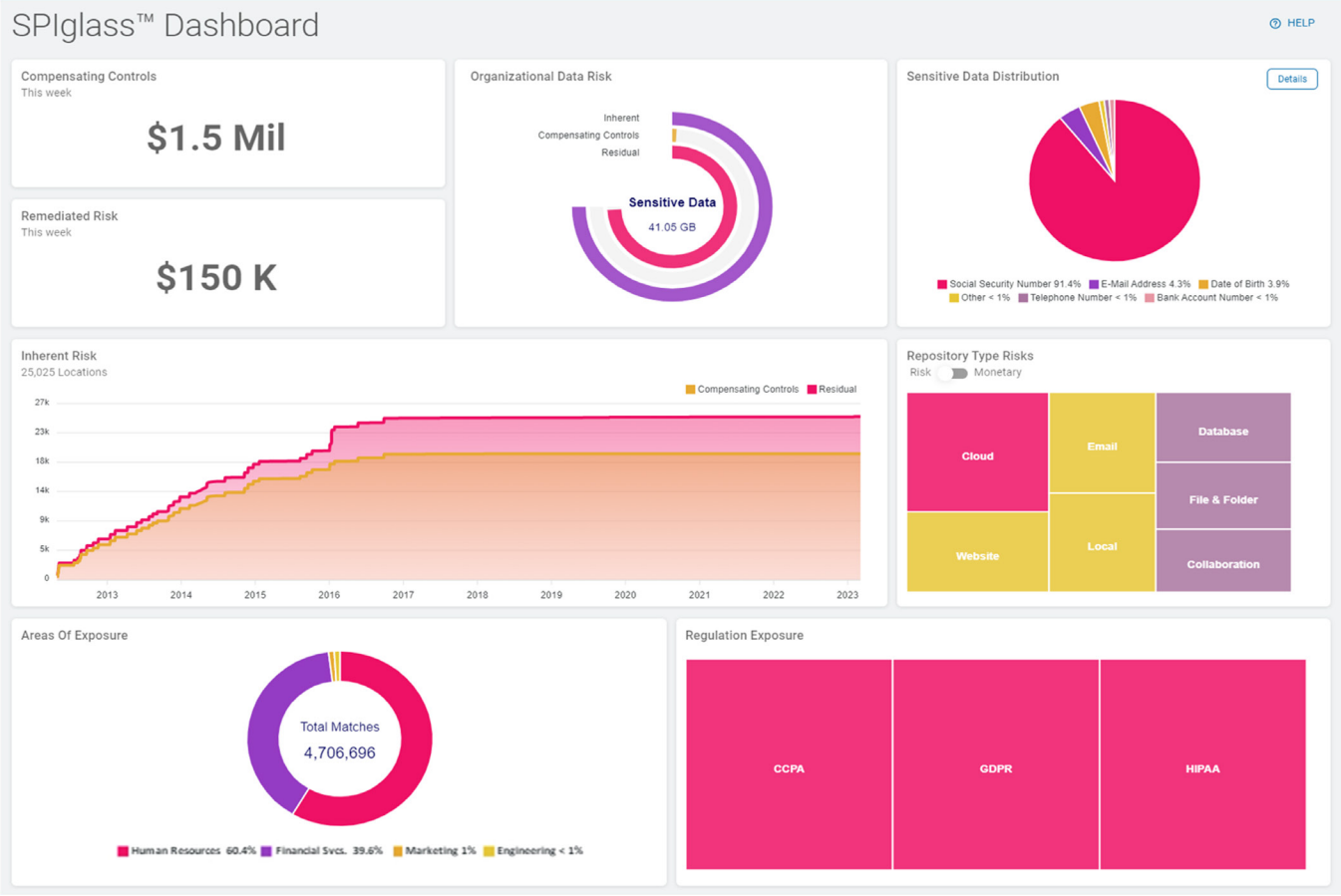
Spirion SPIglass™ Dashboard

Clearly Understand and Communicate Your Sensitive Data Landscape

Spirion SPIglass Delivers a Shared Understanding of Sensitive Data Risks Across Your Organization

As cyberattacks become more costly, frequent, and sophisticated and data privacy regulations have expanded globally, organizations face increasing risks from the sensitive data they collect and store. Protecting sensitive data is critical for maintaining the trust of customers, investors, and other stakeholders, as well as for avoiding legal and reputational damage.

Consequently, interest in cybersecurity and management of sensitive data is increasing at the board level, with 90% of security and risk management leaders having reported to the board at least once in the last year.[1]



To inform their strategic oversight, these leaders need to understand the types of sensitive data the company collects, processes, and stores, as well as the risks associated with each type of data. This might include personally identifiable information *(PII)* such as names, addresses, and social security numbers, financial data such as credit card numbers and bank account information, and confidential business information such as trade secrets and intellectual property. It's also important to outline the company's current data security practices and any gaps or vulnerabilities that need to be addressed.

With board directors recognizing the strong correlation between cybersecurity and business health, executive leadership is also increasingly focused on understanding and managing cyber risks through effective risk management and governance practices. They want to see risk and security financial impact *(Is it a $200,000 risk or a $25 million risk?)* and the likelihood of damage *(What is the probability of getting hacked?)*. Cyber risk quantification, which is the process of assessing and measuring cyber risks in financial terms, addresses these needs, helping organizations to:

- **Improve decision-making** – With a keen understanding of the potential financial impact of cyber risks, executives can make better-informed decisions about cybersecurity investments and risk mitigation strategies.
- **Communicate risks more meaningfully** – Provide a common language for discussing cyber risks with stakeholders, including executives, boards, regulators, investors, and insurers.
- **Enhance risks prioritization** – Better prioritize remediation efforts based on their potential financial impact, which can help focus limited resources on the most critical risks.
- **Comply with data privacy and security guidelines** – Demonstrate compliance and quickly spotlight pockets of risk in your compliance posture.
- **Improve risk transfer** – Cyber risk quantification helps assess the adequacy of your insurance coverage and negotiate better terms with insurers.
- **Increase accountability** – Financial metrics establish accountability for cyber risks at the executive and board level, which can encourage more proactive management of these risks.
- **Better track progress** – Actionable insights can concretely measure the impact of your team's operational and privacy security efforts, demonstrate ROI, and support financial business cases for new initiatives.

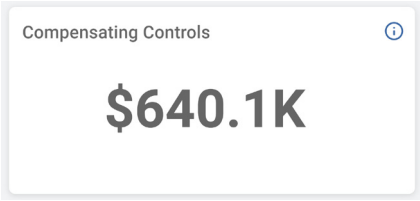
Introducing SPIglass: Insights Executive and Board Members Can Trust

Spirion® Sensitive Private Information Dashboard (SPIglass) Dashboard delivers these essential insights. The SPIglass dashboard presents sensitive data risk in metrics that are meaningful to the highest levels of your organization.

Now available as part of your Spirion Sensitive Data Platform (SDP) subscription, SPIglass gives views into the financial or ordinal impact that allows organizations to accurately understand, measure, and balance inherent risks within their respective teams. It pulls this essential information from SDP. The SaaS-based solution discovers, classifies, and protects sensitive data across your IT landscape — in unstructured and structured data formats, in the Cloud, on premises, and even residing in endpoints like employee laptops or local file shares.

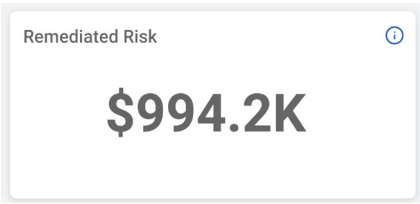
SPIglass is populated with risk-based algorithms pulled from SDP's patent-pending SDV$^{3®}$ risk scoring, which provides a quantitative measure of data risk that is directly tied to the sensitivity of personal data stored across IT systems. It scores the overall risk value of sensitive data assets and accurately assesses the potential costs of data exfiltration based on the three primary characteristics of sensitive data risk: Value, Volume, and Vulnerability. SPIglass metrics provide an immediate understanding of how well sensitive data is being managed and gaps that may exist in the enterprise's security posture.

Features:



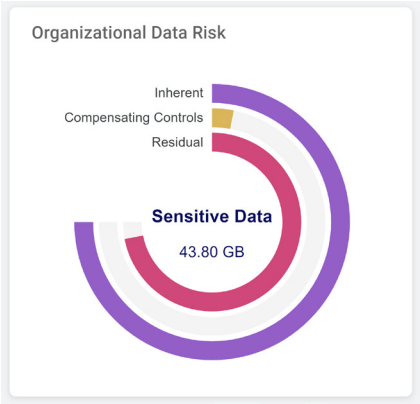
Current Compensating Controls

The total monetary value of all governed sensitive data with compensating controls this week and how the value has changed vs. the previous week. Also known as alternative controls, these are mechanisms that are enacted to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time. An example of a compensating control would be to quarantine the sensitive data to a more secure location.



Remediated Risk

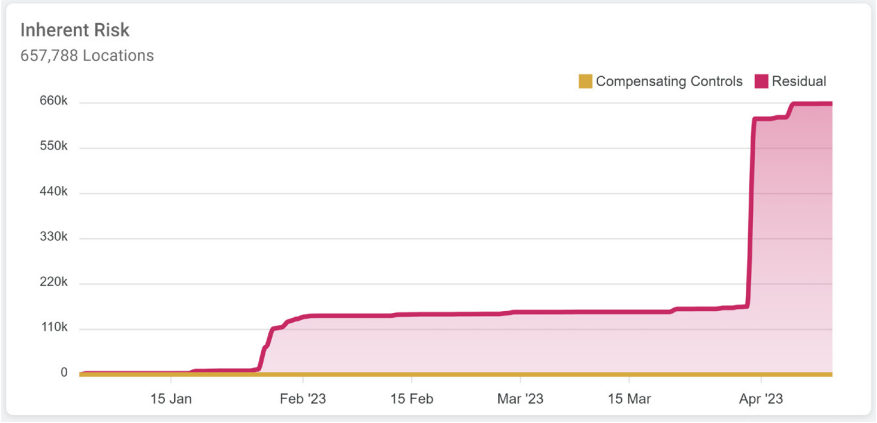
A financial measurement of the value of the sensitive data that has been protected or remediated this week and is no longer considered to be a risk; for instance, by deleting, encrypting, or masking it – along with how the value has changed vs. the previous week.



Organizational Data Risk

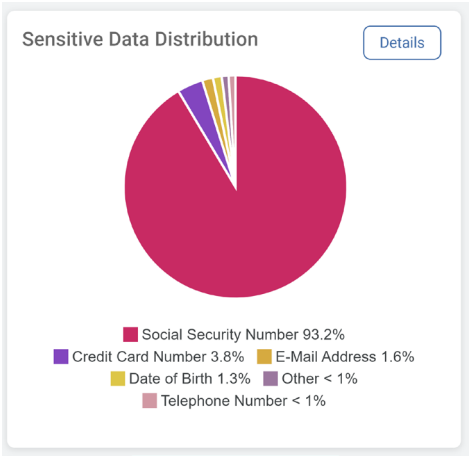
A current snapshot of how much sensitive data resides in your environment and how it is being governed to better control risks. The data is displayed by:

- **Inherent** – Total sensitive data risk. Compensating Controls + Residual Data = Inherent
- **Compensating Controls** – Data risk that has been addressed
- **Residual Data** – Ungoverned sensitive data



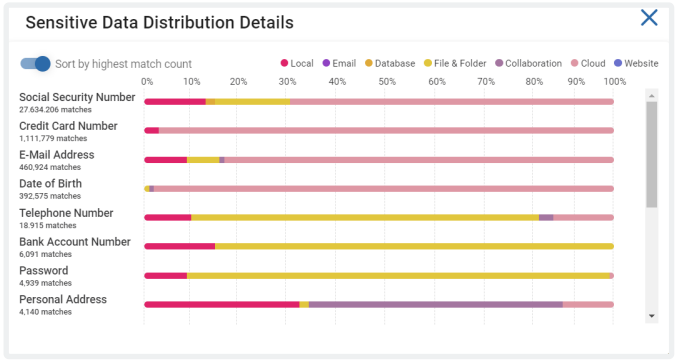
Inherent Risks

Track your organization's Inherent Risks over time broken into sensitive data with Compensating Controls and Residual Data to demonstrate progress and return on investment of your organization's security programs or understand how new risk has been injected into the data posture of the organization.

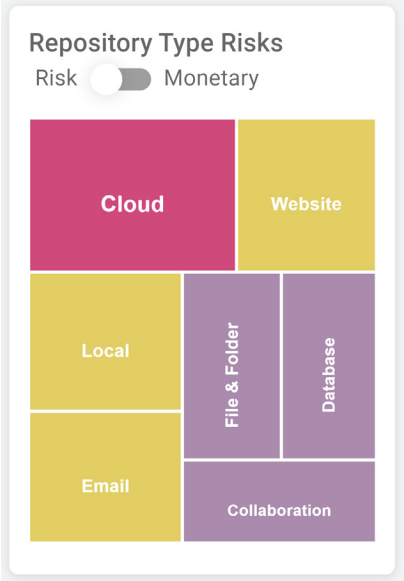


Sensitive Data Distribution

Understand what types of sensitive data are generating risks for the organization. This chart surfaces the top five data five data types *(e.g., credit cards, social security numbers, etc.)* and the remainder of the total data.



Click **Detailed Data** to display a specific category of data and its distribution

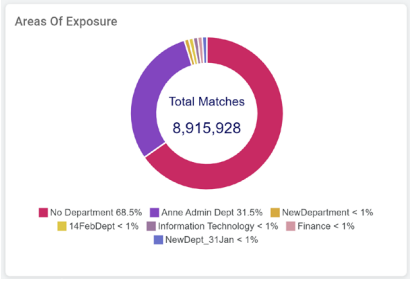


Repository Type Risks

Identify and prioritize data repositories at highest risk if breached, including Cloud and Local data stores, web sites, email, files and folders, collaboration platforms, and other data locations. Toggle to Monetary to see these risks in financial terms. The tree map is color coded by risk level to help prioritize the riskiest repositories for risk remediation.

Regulation Exposure

Ensure that data is stored, managed, and protected according to relevant local, regional, and global regulations. This widget sorts your data by total match count for applicable relations like CPRA, GDPR, and HIPAA to better understand what sensitive data is tied to which regulation and the value and volume of that data.



Areas of Exposure

Visualize and easily identify which departments have the largest volume of sensitive information under their purview in order to work with these departments to resolve potential risks.

Spirion is step one...

From automating zero-trust policies, understanding data-at-risk, to efficiently migrating to the cloud, Spirion is step one to developing an effective strategy to get your data under control.

With Spirion, you gain clarity as to what sensitive data you have and where it is located, control over how your data is stored and used, and confidence that your data is protected.

It all begins with our proven 98.5% accurate discovery and then enforced through our powerful and purposeful automated classification and remediation capabilities.

1 *Gartner, Inc. "Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer," by Sam Olyaei, and Jeffrey Wheatman, May 15, 2022, ID G00377323*

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

4142023 SO SPIGLASS-001