Industry-leading data discovery with Spirion

Accurate, efficient data discovery across formats and environments

Enterprise data continues to proliferate at breakneck speeds, driven by the nearly limitless supply of compute capacity, surge in cloud-based apps and platforms, and billions of new connected endpoints worldwide.

It's a double-edged sword for business leaders and their teams. The data can be either a goldmine of revenue-generating intelligence and insights or a source of increased risk compliance headaches — assuming it can even be found.

In today's IT environment, data is dispersed across numerous on-premises and cloud environments while taking on a range of forms and formats. Not only does that make it harder for line of business and operations teams to use it to the company's advantage, but it also increases the degree of difficulty for CISOs, CIOs, COOs, and database or IT administrators to try and protect it.

Leaving any data undefined or outside the scope of a company's data security and privacy efforts exposes the information and the organization to risk of unauthorized access or use. But accurately and efficiently discovering sensitive data is challenging, since it comes in structured, unstructured, semi-structured, and even synthetic formats.

What is required is a set of purpose-built, privacy-grade discovery tools to provide organizations with the intelligence required to quickly, easily, and accurately discover every byte of data within their ever-growing IT environment so they can classify and remediate it in a timely manner for optimal security and privacy protection.

175 ZB

By 2025, 175 zettabytes (175 trillion gigabytes) of new data will be created around the world.[1]

Many formats, diverse environments

IT and data security professionals are quickly realizing that unstructured data is becoming the primary front in the data protection battle. As much as 90%[2] of today's data is unstructured — productivity documents, emails, photos, social media posts, and more.

The explosion of remote work has accelerated an already rapid adoption of cloud storage and compute, while massive growth in connected devices means enterprise data now lives across a range of cloud environments, hard drives, and personal devices. As a result, this data is notoriously hard to discover and index, due in large part to the diverse locations where it lives and the relatively little context traditional discovery tools have to find it.

1. Seagate Technology. "DataAge 2025 – The Digitization of the World." Seagate.com. Retrieved 11/30/2020.
2. Davis, Dwight. "AI Unleashes the Power of Unstructured Data." CIO.com. July 9, 2019.

81%

81% of enterprises have a multi–cloud strategy in place.[3]

Existing data protection tools such as Microsoft AIP and MIP have proven valuable for enterprises with single–vendor environments or a close IT perimeter. But for others who prioritize multi–cloud and hybrid IT strategies — now more than 80% of global enterprises — the solutions' limited breadth and scope means teams can only ascertain certain bits of information, which can create massive visibility gaps and a startling rate of false positives.

Spirion brings a new and innovative approach to sensitive data discovery, applying advanced techniques to efficiently discover sensitive data in all formats to enable organizations to effectively apply purposeful classifications and federate remediation policies across different platforms, networks, and endpoints from a single, integrated platform.

Discovery is key to preventing many inappropriate uses of data:

- Selling end user data like DNA profiles, personal finance stats, and purchase histories to third–parties against the data owner's wishes

- Using personal information in a variety of ways, some above board and others nefarious

- Using personal data to train automated AI programs without consent

- Targeted advertising without permission

- Doxxing and harassment[4]

Higher accuracy, greater efficiency discovery with Spirion

Spirion, a pioneer in enterprise data privacy and compliance, has released its cloud privacy–grade solution, Spirion Sensitive Data Platform (SDP). Built on 15 years of industry–leading experience protecting on–premises architecture, Spirion SDP offers visibility into sensitive data,

wherever it lives, with the highest demonstrable accuracy, without disrupting business processes.

The company's discovery process identifies personal information contained within unstructured objects in data stores such as a File Server, Cloud Storage, or Object Storage, as well as in structured objects in relational databases. It delivers an unprecedented level of visibility that helps enforce better business practices associated with the collection, storage and sharing of sensitive data throughout the data lifecycle.

Sensitive data comes in many forms, with differing levels of legal protection. Here are five common examples of sensitive data to be aware of:

- Personally Identifiable Information (PII): information that allows a person's identity to be directly or indirectly inferred, including social security numbers, driver's license numbers, financial information, and healthcare information

- Personal Health Information (PHI): information collected by the healthcare industry, as well as information employers store in their network such as allergy information and emergency contact information

- Payment Card Industry Data Security Standard (PCI DSS): any form of credit card data, including Primary Account Numbers, cardholder name, card expiration date, and authentication data like PINs

- Biometric data including fingerprints, facial recognition, retina scans, and voice recognition

- Consumer behavior data, such as purchase records, browsing history, search history, and any information regarding an individual's interaction with a website, application, or advertisement

3. Wilcze, Marc. "IT governance critical as cloud adoption soars to 96 percent in 2018." CIO.com. April 2, 2018.
4. Hay Newman, Lily. "What to do if you're being doxed." Wired.com. December 9, 2017.

How it works

Spirion moves discovery closer to the data, leveraging containerized microservices on a scalable cloud architecture to deliver efficient, accurate results. It finds sensitive data that is stored and operated in all sources, locations, and file types, including any operating system or local device, any cloud, data stores such as storage area networks, network-attached storage, SharePoint, and document management systems for personal data.

Contextual, automated detection processes allow Spirion to find any kind of data, including:

- Personal
- Financial
- Health
- Government credentials
- National security clearances
- Custom data types

Its policy-driven searches find personal data efficiently and accurately, enabling organizations to keep up with increasing data velocity.

Advanced discovery tools increase accuracy and efficiency

Spirion applies advanced discovery tools for efficient, accurate results, including:

- Pattern matching to identify strings matching a pattern for social security numbers, credit card numbers, or other sensitive data
- Branching algorithms go beyond manual or single verification algorithms like RegEx, reducing false negatives and false positives to under 2%
- Distributed computing to bring discovery processes closer to the data
- Vector analysis that takes context clues into account
- Regression analysis to increase detection accuracy
- Supervised and unsupervised learning (AI/ML)

New features enable compliance and security

- Spirion's Advanced Identity Association allows you to ingest, search, and analyze disparate personal identifying information and automatically create associations between discovered data elements and their associated persons and identities.

- Its Identity-centric discovery allows automated Subject Rights Requests (SRRs), using AI techniques including keyword matching, partial document matching, structured data fingerprinting, and proximity rules to avoid false positives. This increases the speed and accuracy of SRRs, which are often done manually and can take up to a month to complete at an average cost of $1,400[5].

SRRs at-a-glance

SRRs are about more than just finding, amending, or deleting someone's data. While GDPR and CCPA suggest that users should have the "right to be forgotten," in many cases other regulations will supersede a consumer's right to erasure. Proper data identification and tagging of an organization's entire inventory can be helpful in effectively handling SRRs because it prescribes exactly what they can and can't do with the data they find.

- Continuous proactive Discovery Teams™ distributed cloud agents move the discovery of cloud data closer to the data location. Elastic agent on-premise architecture intelligently distributes workloads.

The industry's most accurate discovery for greater legal and financial protection

Spirion enables enterprises to easily and automatically discover any type of potentially sensitive personal data no matter where it lives in the IT environment. This enables faster and more accurate data discovery for context and risk. It identifies sensitive data with independently verified 98.5% accuracy and the lowest false positive rate in the industry, then automatically applies appropriate cures and controls.

Its automated discovery eliminates blind spots to dramatically reduce risk of breach or unauthorized access and use, without interrupting business workflows.

As a result, you'll minimize the time your analysts spend locating sensitive information over an ever-expanding big data footprint, and significantly improve compliance with virtually any data governance standard including GDPR, HIPAA, HITECH, CCPA, PCI DSS, and others.

You'll also enjoy benefits beyond the reduced legal and financial exposure. Data breaches can also damage your organization's reputation. And understanding the sensitive data you have in your organization's footprint means you can reduce the sensitive data on hand, and increase your ability to more efficiently spend data security budgets.

Unrivaled discovery for unparalleled protection

Data protection is a chief concern for today's privacy, security, and risk management professionals. But so many are unable to protect their most vulnerable information because they simply don't know it exists or can't find it even when they do.

Spirion's suite of privacy-grade data solutions provide unrivaled end-to-end data lifecycle coverage and protection. Many security professionals are turning to Spirion. This capability delivers an efficient, integrated, and automated solution that can discover any type of data, in any corner of the IT environment quickly, accurately, and with precision.

About Spirion

Spirion exists to protect what matters most – the sensitive personal data of our colleagues, customers, and communities. The forefront provider of information security solutions for modern enterprises, its clients include forefront organizations in higher education, health care, financial services, manufacturing, and eCommerce.

To learn more, read about how at **http://www.spirion.com/spirionatksu** or schedule a demo.

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