SPIRION

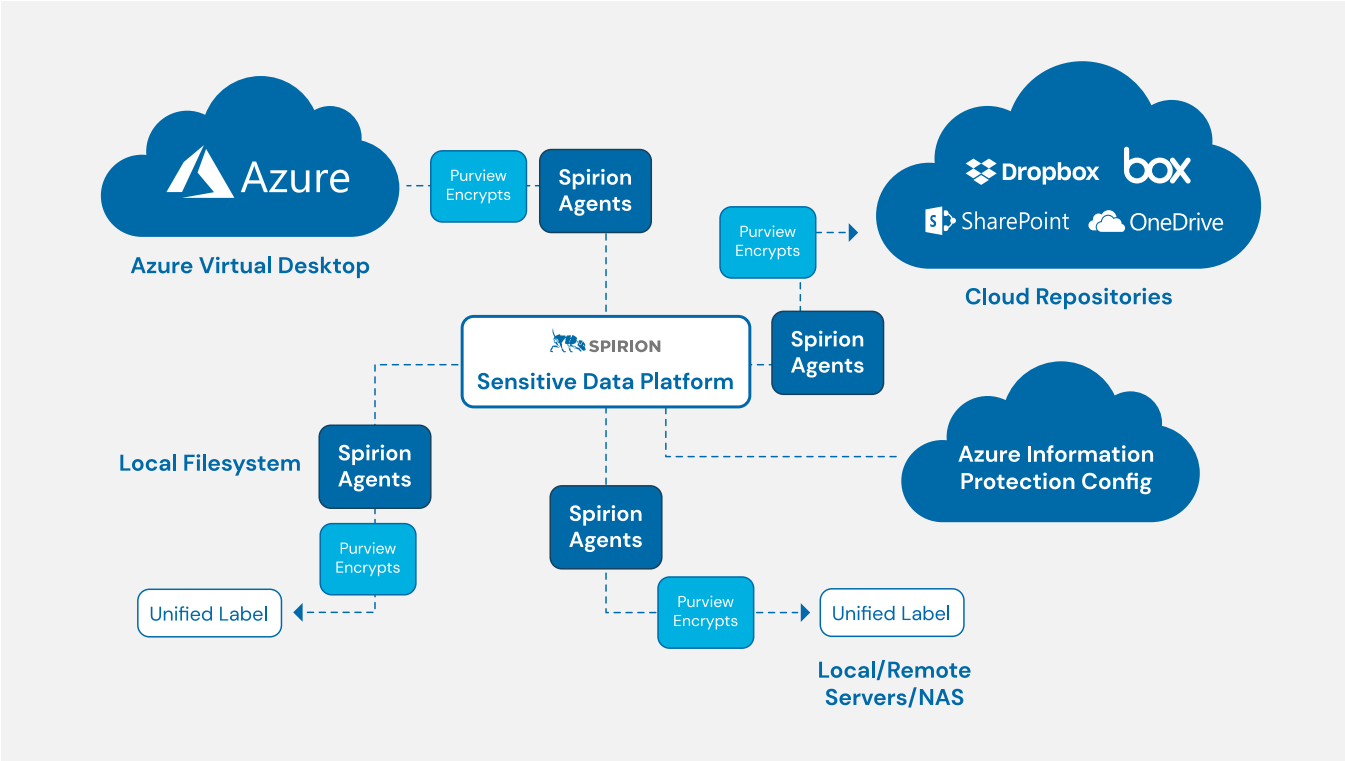
WHITE PAPER

Complete Your Microsoft 365 Data Protection Stack

With Spirion Accuracy and Automation

Complete your Microsoft 365 Data Protection Stack with Spirion Accuracy and Automation

Spirion + Microsoft Purview Information Protection Delivers Extended Coverage and Accuracy for Rights-Managed Encryption and the Remediation of Sensitive Data



Locate and classify all your sensitive and confidential data using one set of rules. Spirion partners with Microsoft to extend data protection and labeling to systems they don't secure—your file servers; non-Microsoft cloud technologies;, other non-Microsoft on premise cloud databases; SaaS apps; and Microsoft, Mac, and Linux workstations.

Protecting Data in Today's Modern Environments is Challenging

Data is the lifeblood of your organization, enabling everything from new product and service development to large-scale analytics, and every imaginable use in between. But with greater access to a greater volume and diversity of data, IT security and privacy professionals face increasing challenges around properly protecting throughout its lifecycle and across expansive IT footprints.

Today's enterprises feature complex IT landscapes that spread sensitive personal information (SPI) and personally identifiable information (PII) beyond their primary environments. Recent trends including remote work, adaption of multi-cloud strategies, business investments in SaaS applications, and expanding and ever-evolving data privacy compliance needs all require a greater understanding of the data in your organization and how it's being used than ever before.

Employees and Contractors are Spread Across the Globe

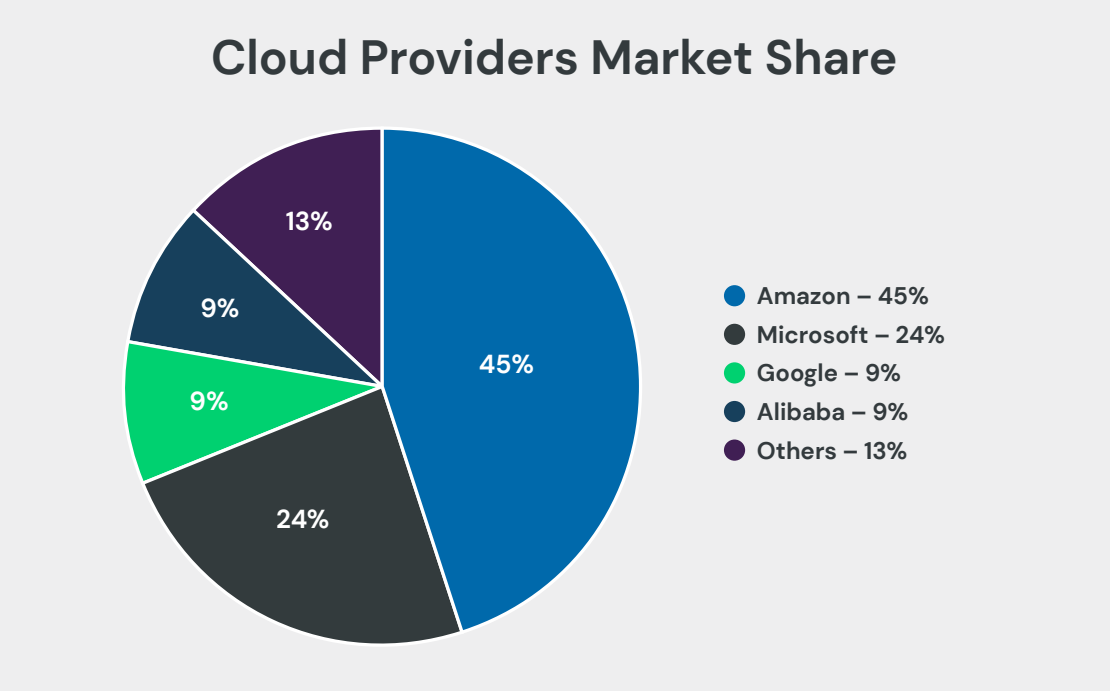
Driven by the Covid Pandemic, remote work is becoming the norm with 66% of U.S. employees now working from home at least part-time.[1] And work isn't always done by your employees. Many of your company's functions are likely performed by contractors working in India, China, or the Philippines. The global business process outsourcing market forecasted to be $620 billion by 2032. The most popular outsource functions include IT, payroll and other financials, and call centers – putting troves of valuable, sensitive data in the hands of third parties. The scattering of modern workforces now extends an enterprise's sensitive data footprint to hundreds or thousands of remote workstations and laptops and workstations.

66% of U.S. employees work remotely, at least part-time – driving data across 1,000's of endpoints and obliterating network perimeters.

Data is Diverse and Spread Out

Today's workplaces no longer consist of a single mainframe computer sitting in a back office. In practice, enterprise data can reside in a number of places:

- Across platforms and operating systems, including Windows, MacOS and Linux endpoints
- In various cloud storage applications, such as Box, Dropbox, G-Suite or Microsoft SharePoint
- In multi-cloud environments, including Azure, Google Cloud Platform, and Amazon Web Services (AWS)—Today, 92% of organizations have a multi-cloud strategy in place or underway, and 82% of large enterprises have adopted a hybrid cloud infrastructure. On average, organizations are using 2.6 public and 2.7 private clouds.[2]
- Within unstructured files created using productivity suites such as Microsoft Office, in a data store such as a File Server or Cloud Storage, and in structured objects such as relational databases
- Throughout hundreds of disparate SaaS applications—The average enterprise has 364 applications in use, proliferating data to hundreds of disparate platforms. While Microsoft is certainly a behemoth in enterprise applications, the market is so dispersed that even Microsoft only has a 13% share of enterprise applications leaving hundreds of applications potentially unprotected with a vendor-centric approach to security.



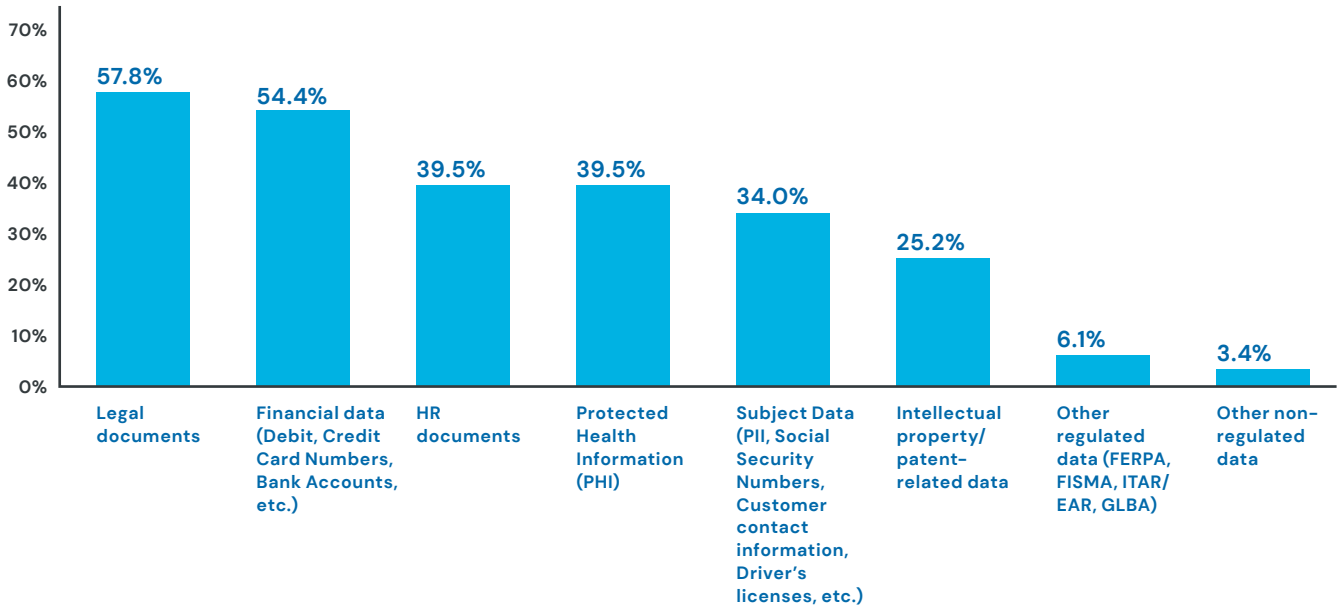
Organizations are taking a multi-cloud approach, with an average 2.6 public and 2.7 private clouds deployed.[2]

Complicating matters is that this data is spread across myriad formats and locations. It's saved to unstructured objects such as productivity documents and email in structured objects like relational databases. It can be found in multiple cloud environments, in file servers, in data lakes utilized by data scientists, and even on employee workstations and laptops.

Storing data across varying file formats, operating systems, and storage environments, can make it nearly impossible for enterprises to efficiently discover where their data resides, let alone understand its contents. Only once data is understood that appropriate steps can be taken to classify it and apply appropriate usage restrictions—i.e., remediation. The entire process requires either intensive manual searching or specialized tools to locate it.

This chart, using data from Spirion's Data Privacy Survey, highlights the diversity of sensitive data, especially unstructured data types and locations.

What types of sensitive data makes up your organization's unstructured data?



Data Controls Vary by Type and Purpose

It's clear that data itself isn't homogeneous, so it's important to understand that each category of data will require different standards around which people and other systems can see it, access it, utilize it, or otherwise modify it. These controls need to ensure security and compliance, while allowing business to get done. They may include:

- Visibility controls that dictate whether or not a user is allowed to view a certain set of data
- Accessibility controls that limit access to employees or systems with specific roles
- Openness controls that allow data enrichment and monetization, such as with analytics or aggregation

Privacy parameters can differ even by use case, data type, and even state or country where the data subjects reside or where the data is processed. For example, highly sensitive personal information like social security numbers, addresses, credit card numbers, bank accounts or health records may require special controls based on company policy, industry standards, and government regulations.

Governing your data to comply with this myriad of regulations and policies requires that your data is classified with the necessary context to properly control it, including its sensitivity, applicable regulations, locations, purpose of the data, business processes where it is being used, data consumer preferences, and other contextual information.

Existing Information Protection Solutions Aren't Enough

These sensitive data management challenges are driving IT and privacy professionals to look at new methods to discover, classify, and remediate sensitive information beyond the confines of a particular app or environment. It is becoming apparent that the objective of securing data effectively cannot be achieved by a single-vendor suite. In response, many forward-thinking IT security and privacy professionals are looking to augment their vendor-specific information protection tools with enterprise-grade, built-for-purpose infrastructure, and tools to gain visibility and transparency into their data across systems and platforms, which will enable them to better preserve both the privacy and the security of data in support of regulatory compliance, corporate policies, and customer expectations.

57% of organizations house over ¾ of their data outside their Microsoft or Azure environment.[3]

Microsoft Purview Information Protection (MPIP) Data Discovery and Classification

Many tools on the market offer sensitive data discovery and management capabilities to varying degrees. If your organization has a Microsoft E5 license, you may already have one such tool available to you. Microsoft Purview Information Protection (MPIP) is a data discovery and management product that enables you to discover, classify and label sensitive information across a variety of locations. You can customize your classification and labeling taxonomy to meet your specific needs and apply a range of protection actions to your data based on its sensitivity—such as encryption, access restrictions, or visual markings.

If your organization primarily or exclusively uses Microsoft applications and security software and Azure for your data stores, you may find MPIP to be sufficient for data discovery and classification. But for the vast majority of hybrid, multi-cloud organizations with a broad diversity of non-Microsoft applications, MPIP alone may leave you with blind spots in your management of sensitive data.

Although the system has limitations, if your only concern is the classification of documents that MPIP will label within the Microsoft 365 environment, then MPIP has to be your prime candidate.

Gartner, Inc., "Improving Unstructured Data Security with Classification"[5]

Spirion Extends Sensitive Data Discovery Across Your Data Landscape

Because data lives across so many systems, clouds, file formats, and applications, solving the challenge of data discovery, classification and protection requires great insight—and partnership. For Microsoft users already deploying MPIP, adding Spirion Sensitive Data Platform (SDP) can extend your security ecosystem to other, non-Microsoft environments and platforms enterprise-wide. Spirion SDP applies context-aware sensitive data detection and purposeful classification using a range of techniques not possible with simple RegEx pattern matching, immature artificial intelligence, or manually applied classification technologies. SDP can discover sensitive personal information contained within structured data in relational databases as well as unstructured data on fileshares, cloud repositories, and endpoints.

Spirion SDP can automate enforcement of your access, use, and privacy policies across every platform, app, or instance where that data resides. Spirion's data-centric, platform-agnostic solution goes beyond simply securing data from unauthorized access at the perimeter by accurately identifying and classifying sensitive, private, and regulated data where it lives—at the database and individual data record level (e.g., a Microsoft Word or PDF file) —so it can be stored, protected, and used in the safest, most compliant means possible. Spirion finds data at rest in years-old unknown, ungoverned files and documents, including those on local servers, enabling you to proactively make holistic decisions about your data estate, rather than simply handling data already in motion, or as it's being created or edited on an ad hoc basis.

Spirion SDP is built upon a highly-scalable cloud architecture that brings discovery closer to the source of the data, leveraging containerized microservices to deliver high-efficiency results.

For many clients, the complicating factor is budget rather than technology. If you already have an E3 or E5 license, why would you spend more for what looks like the same capability?

The answer lies in scope, accuracy, additional functionality, user experience, and classification requirements that MPIP may not cover. In this case, a third-party tool that integrates with MPIP (such as Spirion) may provide the additional scope you need. Privacy requirements, such as DSARs, require the technical capability that vendors such as Spirion can address.

Gartner, Inc., "Improving Unstructured Data Security with Classification"[5]

Microsoft Purview + Spirion: Better Together

As a member of Microsoft Intelligent Security Association (MISA), Spirion extends protections provided by MPIP to deliver comprehensive data discovery, classification, and remediation across your diverse and multi-Cloud / on-premise data estate:

	MPIP CAPABILITIES	+ SPIRION
Multi-cloud and SaaS support	Native support for classifying data in the Azure cloud environment; limited support is also available for AWS. Can scan Microsoft applications and PDF files for sensitive data. A limited number of connectors are available for some non-Microsoft applications, but they require separate third-party licenses and data must be ported to the data owner's Exchange folder for scanning and remediation. This duplication of data may increase cloud costs and could have performance implications.	Provides holistic visibility needed for enterprise decision-making around sensitive data. Discover, classify, and remediate sensitive data at the source, anywhere it lives–on-premise, at endpoints, and in multiple cloud environments, across 280+ systems and applications, including file shares, Big Data, SaaS, NoSQL, RDBMS, collaboration tools, ERP, and more.
File Formats Supported	Microsoft file protection supports about 20 file types: Microsoft Office and PDF. It modifies file extensions for non-Office file types (e.g., txt to ptxt), which may confuse users or cause issues with security applications and firewalls.	Discovery across hundreds of data formats, including images without modification to the file extensions, including Microsoft and other SaaS apps, full OCR image support, scripts like Java, log files and more. Users can open all files in their native application. It does not modify file extensions, which means applications that rely on native file extensions for scanning or other purposes keep working.
Endpoint Data Discovery	Lacks agents that can support endpoints like workstations, remote worker laptops, and local file servers. Instead, endpoint data is ported to Azure for scanning, which may increase cloud costs.	Spirion agents scan data directly at the endpoint with support for endpoints running Windows, Red Hat Linux (RHEL) operating systems. Spirion supports both Intel, M1 and M2 versions of Ventura, Catalina, Big Sur, and Monterey.
Accuracy	• Accuracy has been pegged at 60-80%, which results in false positives and missed results. • To enhance performance, only samples of files are scanned. • AI/ML training classifiers are available for Microsoft-native environments, e.g., Excel and Word, to assist with accuracy	Discovery uses branching algorithms with leading-edge recognition techniques and validations for fewer false positives (below 2%) across any data format or location. The entire file is scanned to ensure that sensitive data is not missed.
Data-at-Rest Discovery	Designed to find sensitive data when it's created or edited	Spirion's data-at-rest approach proactively locates the sensitive information that is often buried in archived documents proliferating across your organization.

Context-Sensitive Classification	Sensitivity classification can be performed automatically within Microsoft applications (with E5 license) or manually by end-users (with E3 or E5 license). Watermarking and Classified headers / footers is available for Microsoft documents.	• Spirion extends automated classification beyond your Microsoft environment providing a single source of truth for your data. • Multiple businesses and governance drivers may require numerous labels applied to a single data object. Spirion context-rich classification offers context beyond just sensitivity labels. • Classification is persistently embedded in the file's metadata to protect data at its source. • Visual classifications appear as markers on files as guidance for end-users, extending watermarking beyond Microsoft documents.
Reporting	Limited reporting capabilities constrain your ability to derive insights about your data to create smart, proactive strategies. Developers may need to write complex PowerShell scripts for needed insights. Lacks insight around many of your non-Microsoft environments.	Spirion reports offer insights across your data estate with numerous turnkey reports and risk-based dashboards available, as well a new data warehousing option offering enterprise-grade data model capabilities from your favorite BI/ analytics platform.
Data Protection Settings	Protection settings are only encryption, data headings, and rights enforcement permissions	Remediation / protection offerings are broad; Playbooks automate enforcement of organizational policies and regulatory mandates, including GDPR, CPRA, HIPAA, PCI-DSS, and more.
Deployment Options	Microsoft Purview is a cloud-based service.	Spirion can be deployed as a fully managed SDP, within an Azure private cloud, or on-premises

Spirion SDP Key Capabilities

Data discovery across non-Microsoft environments and applications

You can't protect their sensitive data if you don't know where it exists. And only a portion of enterprise applications are Microsoft. That's why Spirion interrogates your data wherever it lives, including both unstructured and structured data, across on-premise and multi-Cloud environments. Discover sensitive data across 280+ file shares, Big Data, SaaS, NoSQL, RDBMS, collaboration, ERP, and more. Spirion also supports hundreds of file formats, including full PDF and Optical Character Image (OCR) recognition to find text within images and PDFs, which comprise over 60% of most company's data. MPIP sensitive data scanning is limited to Microsoft and Azure offerings and AWS S3.

Other third-party sources lack full functionality. For instance, popular sources like Snowflake only offer technical metadata discovery, which lacks insights into whether the data is sensitive. As well, data for non-Microsoft applications must be ported to Azure or Exchange in order to scan it for sensitive data, resulting in redundant cloud costs. Other functionality, such as the new ML-based Advanced Trainable Classifiers is only available for Microsoft-native applications and may lack maturity or require extensive training by the end-user. An MPIP-only approach will also miss many structured SQL databases, such as Oracle.

Endpoint data discovery supports locally saved data and today's remote workforces

Microsoft Purview is designed for Cloud-first companies, where data is encrypted, secured in the Cloud, and end-users interact with it via their edge device (laptop, mobile device, etc.) or browser. Data created locally is assumed to always be backed up to OneDrive or other Azure data stores, where it can be scanned for sensitive data. Email messages can be scanned for sensitive data as they are sent. Real-world environments aren't usually so simple. Employees create and download documents on their local drives. Millions of old sensitive records may reside on an inactive, years-old local server. Employees use their laptop for personal tasks. If you're not addressing sensitive data-at-rest everywhere locally, bad actors may find it before you do.

Spirion's agents go directly to the end-user workstations – PCs, remote employee laptops, local file servers, and more - to find and protect data directly at its source. Agent-based approaches are necessary because endpoint systems are often disconnected from the corporate network. Uniquely, Spirion can locate and protect sensitive data on Windows, Mac OS, and Red Hat Linux (RHEL) environments. Microsoft Purview can only scan endpoints for data loss protection purposes by porting data to Azure, which may result in additional cloud costs.

Proven 98.5% discovery accuracy reduces false positives and missed results

Sensitive data discovery across disparate platforms, applications, file formats, and other variables is difficult. Without finely tuned algorithms, false positives -- when the system thinks it found a match that really isn't a match -- are far too common. Too many false positives may render your data discovery worse than useless. Productivity is needlessly hampered when they users can't save or share a document thought to have sensitive data. Precious IT resources are wasted chasing down non-issues and true alarms may not get resolved with an out-of-control backlog. Even worse, less-than-perfect matches may result in missed results, leaving your organization's sensitive data unprotected.

Spirion achieves industry-leading precision via Branching Validation Algorithms rather than with a single verification – e.g., simple RegEx pattern matching. These algorithms are comprised of dozens of predefined and linear classifiers, procedural validators (search results can be precisely validated

using tree traversal so that the results of early validations can determine whether any and which additional validations are executed), checksums, Boolean logic formulas, decision trees, exact data matches, dictionaries, and a user-defined rule builder for custom queries.

While other vendors scan samples of your data for faster results, the likely result will be that sensitive data is missed. Spirion scans and validates the entire file to ensure accurate, comprehensive results.

With Spirion, your organization can find any type of sensitive data anywhere it exists with independently-verified 98.5% accuracy,[4] so that it can be properly protected and ethically used, an outcome we call "PrivacyGrade™ Data Discovery."

Proactive, data-at-rest approach protects sensitive data at its source

While it's important to understand what data is sensitive as it's created and is traversing your network, data at rest can't be ignored. The average organization is storing 2.2 petabytes of data. IDC estimates that 80 percent of enterprise data is unstructured, and 90 percent of that data hasn't been analyzed for its sensitivity. If your company isn't capturing data at rest, you could have significant blind spots in your security posture. Spirion proactively scans data at rest, protecting it at its source, and simplifying the burden of your other security tools that can now more easily and accurately identify which data is sensitive and needs to be protected – wherever it may travel and without impacting network performance.

Organize and define your data estate with automated, consistent, context-rich classification

MPIP auto-labeling is limited to Microsoft and Azure applications and a small handful of non-Microsoft sources, while Spirion scans across 280+ structured and unstructured data sources. Through integration with MPIP, Spirion extends the ability of Microsoft customers to automatically apply labels and policies defined through MPIP to all sensitive and personal data – including data outside of Microsoft infrastructure, such as Snowflake or Dropbox.

Spirion SDP offers persistent classification, meaning it's added to the file's metadata – so it travels with the document - protecting it wherever it goes. Whether the file is copied, shared, downloaded, etc., the classification remains. Further, while some file types (particularly Microsoft Office and PDF files) have room and formal support for tagging in headers or document properties, many other file types have no such attributes. Tags must be entered in the file's body as plain text, and some file types are not capable of being labeled internally at all. Spirion tags your files with visual markers and icons to help end-users understand data's sensitivity and other context and treat it appropriately.

Multiple businesses and governance drivers may require numerous labels applied to a single data object. Spirion offers context-rich labeling to support even your most complex data security policies. In addition to sensitivity classifications that set confidentiality levels, Spirion offers additional categories to enhance understanding of the data and provide the utmost flexibility in how you organize and define it. The categories include business processes where data is being used, purpose for collecting information about an individual, consumer preferences for how data about them can be used, associated regulations that would govern the data (CPRA, GDPR, HIPAA, PCI-DSS, etc.), or your own custom labels.

Quantify, monitor, track, report, and prioritize data risks with in-depth reporting

Understand your sensitive data landscape at a glance. Spirion SDP dashboards and reports are your single source of truth to view and make decisions about your entire data estate and comply with

audits and regulations. MPIP reporting is more limited and complex PowerShell scripting may be required to get the reports you need. Spirion SDP Data Asset Inventory (DAI) tracks where you store data and what security you have implemented for their protection. Easily determine what data types you have scanned for. SDP even points out what you haven't yet scanned. An array of out of the box reports give you awareness needed to make smarter decisions around your sensitive data.

Spirion SDP offers better insights on data security risks than anyone, including the proprietary SDV³™ Sensitive Data Risk Dashboard. SDV³™ provide quantitative measurements of data risk that is directly tied to the sensitivity of personal and classified data stored on IT systems and in the cloud. Sharpen your focus to what matters most—spotlighting the riskiest data assets so you can objectively manage trade-offs and quantify your success. For executive and board-level reporting, Spirion's C-Suite dashboard directly ties your team's activities to business outcomes with a monetary-based view of risks. Easily demonstrate value or highlight the need for additional resources. Reports can be automatically generated, and findings published to your clients to comply with regulations.

With Spirion Extensive Analytics (SEA), you can develop your own insightful reporting, analytics, and visualizations on your data with enterprise-grade semantic data model capabilities for business intelligence (BI), data analysis, and reporting applications. Use SEA to define the key metrics associated with your security and privacy programs to monitor for maximum value and risk reduction. Simple ODBC connectivity allows the data to be consumed from nearly any platform including BI tools like Power BI and Tableau, SIEM devices (e.g., Splunk) and more

Playbooks offer consistent, cross-platform data protection

Once your organization's data is properly understood and classified, you can apply the appropriate controls to protect your sensitive data and reduce your sensitive data footprint. With Spirion SDP, securely process personal data from collection through disposal. Control how personal data is retained, logged, generated, transformed, disclosed, and shared. And collect and provide the evidence necessary for defensible deletion. Spirion SDP Playbooks automate policies associated with controlling sensitive data aligned with your organization's security goals and regulatory mandates, extending protections beyond the Microsoft environment.

Use Spirion's visual, intuitive, no-code interface to easily design even the most complex scenarios. For instance, if sensitive data is found on a laptop, it can be automatically relocated to a more secure location and the owner notified. Or if data was created more than three years ago and hasn't been accessed in more than one year, notify the data owner and delete it. Orchestrations are available to delete, organize, anonymize (mask), redact, encrypt, relocate (quarantine), encrypt, and more. Playbooks can also interact with the rest of your security stack. The ability to share labels with Microsoft for information rights management (IRM) and encryption is just one example.

A single source of sensitive data intelligence across your IT stack

In addition to the MPIP integration, Spirion provides the single source of sensitive data truth required to generate improved return-on-investment (ROI) from your organization's existing data security and privacy technology implementations. Spirion's mission to discover and protect sensitive data works in tandem with the rest of your IT security stack to help keep sensitive and restricted data away from external malicious actors and insider threats. The platform is inherently extensible with support for add-ons that bring additional functionality that includes ongoing data analysis or support for data subject access requests (DSAR)

Spirion's accurate discovery and context-rich classification capabilities provide the identity necessary for Information/Data Rights Management (IRM/DRM) encryption, Security Information and Event Management (SIEM) incident workflows, data de-identification of structured data, and

interoperability with Data Loss Prevention (DLP), NGFW, and CASB tools. Spirion offers pre-defined interoperability solutions with many popular platforms, or you can create your own Playbook scripts to interact with any other proprietary tools in your environment.

Flexible deployment options

Microsoft Purview is a cloud-based service. Due to regulatory compliance or security reasons, you may need additional flexibility in how your data protection solution is stored. Spirion can be deployed as a fully managed SDP, within an Azure private cloud, or on-premises.

> **"I can now honestly present to the Board of Directors that we have full command and control of our sensitive data throughout our global organization. As a CISO, I can easily and cost effectively update the CEO and CIO with detailed metrics."**
>
> CISO, Pharmaceutical Wholesaler

Prevention is Better than Cure

Today's businesses create and manage more data than at any point in history. But as data volumes grow and the ways it's utilized continue to evolve, organizations face new and more sophisticated challenges around minimizing risk and maintaining compliance with company policy and government regulations.

While many of the information protection solutions available today play an important role in protecting high-value or highly sensitive information, enterprises need to extend the reach and capabilities of their single-vendor solutions by adding platform-agnostic, enterprise-grade information protection solutions. Combining native tools with expansive third-party platforms like Spirion provides end-to-end coverage across the data universe, as well as the visibility and transparency businesses need to keep every byte of data secure, compliant, and ethically used.

Member of
Microsoft Intelligent
Security Association

Microsoft

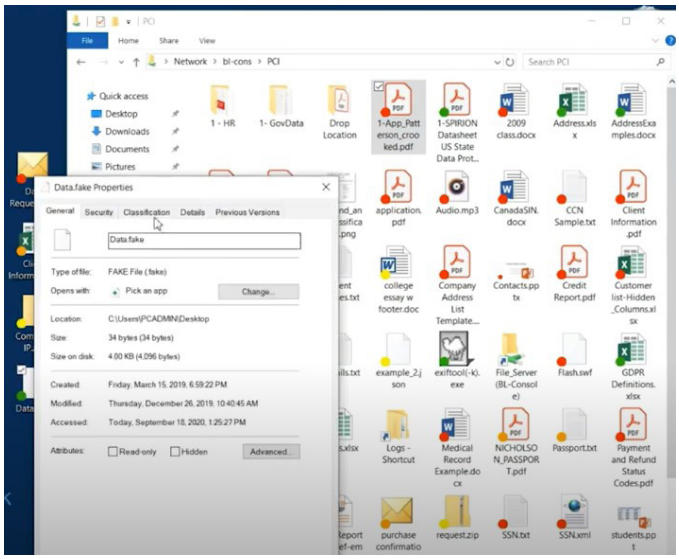
Quotes from Spirion Customers:

"We did a pilot on NAS SharePoint and clearly had a lot of sensitive data. Millions of records. Somebody had five Excel spreadsheets with the entire download of our master database. A single file in this case was almost deadly."

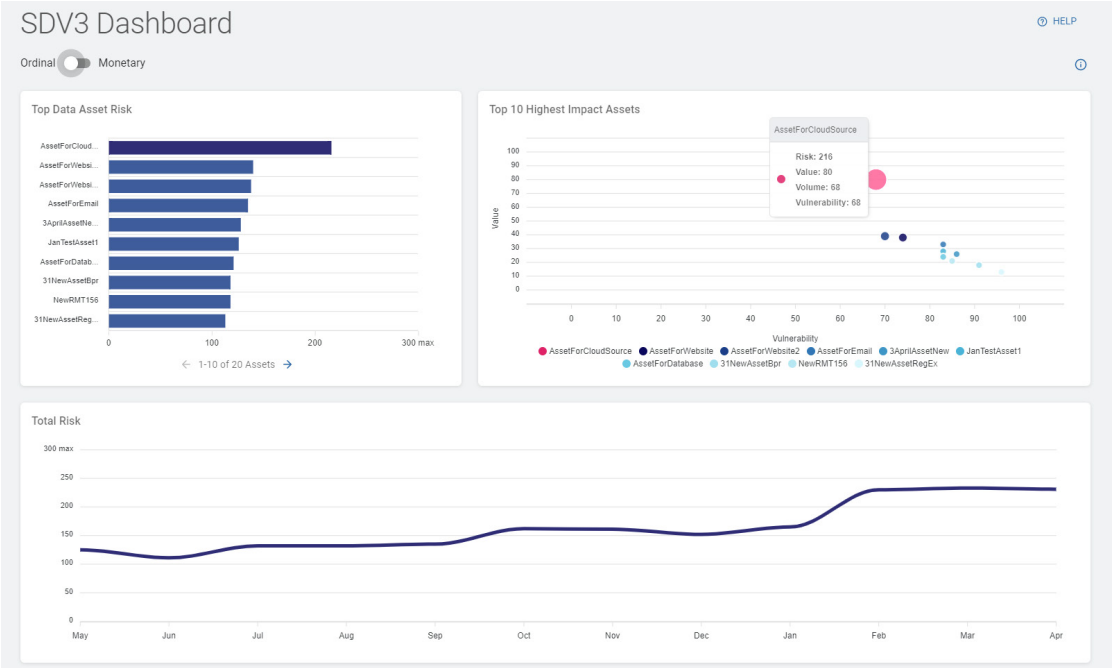
"During the inspection of a file server, the partner found hundreds of SSNs alongside tax returns in a container holding site construction folders."

"In looking at our results after scanning some of the workstations, I found 6 SSN, 12 BANs, 2 DLNs, 10 DOBs and 53 passwords. Looking at DOB actually gave light to another document that had personal health information we weren't initially looking for but that actually contained 1,400 records of personal health information in leave of absence requests. If we had rolled this out to all of our stores, it would have exposed us to $1.6M of risk."

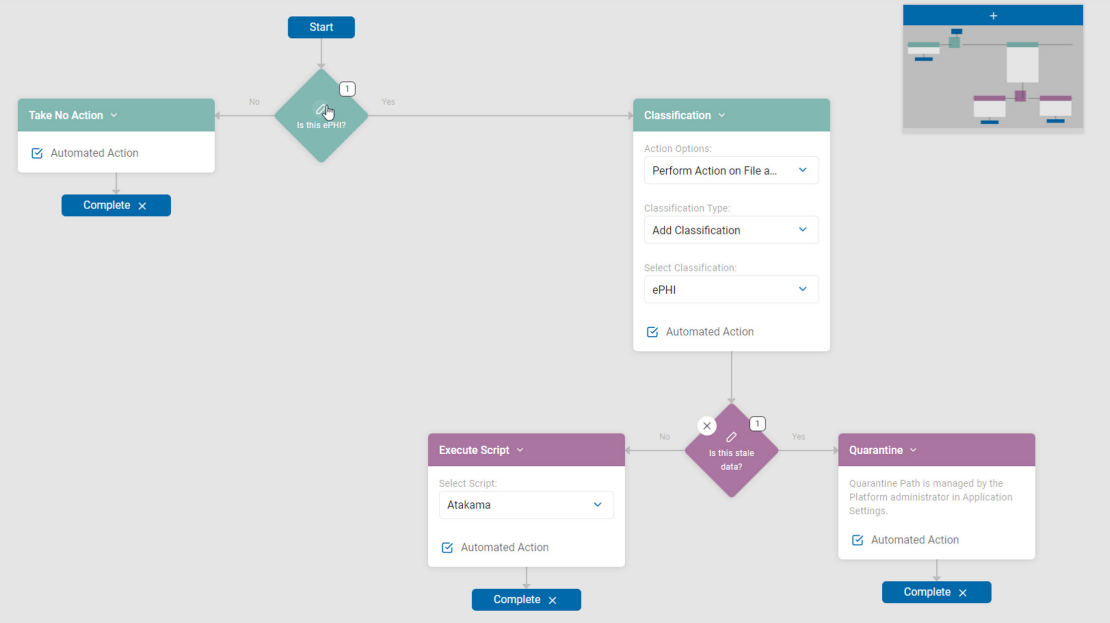
"After scanning approximately half the workstations in the environment, Spirion has located over 140 million results. One single workstation had over 110 million results stored locally on its C: drive."



Spirion SDP context-rich classification extends beyond sensitivity labeling to deliver greater insights around your data, such as relevant regulations, business processes, and more. Classifications are added as metadata to the documents so that security travels with the data, as it proliferates across your organization. As shown in the illustration above, visual markers including icons and color-coding are displayed at the individual file level to provide end-users with immediate understanding of which documents are sensitive.



Spirion SDP dashboards incorporate Spirion's proprietary SDV³™ risk score that helps organizations understand, track and prioritize their sensitive data risk remediation efforts based on data value, volume, and overall vulnerability.



Spirion Playbooks offer a no-code workflow solution to enforce your data policies by enabling you to select actions when sensitive data is found, including notify owner, quarantine, encrypt, create an MPIP label, remediate, mask, encrypt and more

1) Zippia, "25 Trending Remote Work Statistics (2023): Facts, Trends, and Projections," by Jack Flynn, Oct. 16, 2022
2)Gartner, Inc., "Market Share: Enterprise Public Cloud Services, Worldwide, 2021," by Colleen Graham, Fabrizio Biscotti, et al, May 22, 2022, ID G00766742
3) Spirion, "Data Privacy Annual Research Report." Spirion.com. November 2020
4)Tolly Group Report: "Spirion Data Accuracy Evaluation," #221104 January 2021. Commissioned by Spirion, LLC
5)Gartner, Inc., "Improving Unstructured Data Security with Classification," May 30, 2022, by Mac Howell, ID G00765468

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