How to Choose a Data Discovery Solution

GROUND LABS

# Table of Contents

GROUND LABS

What is Data Discovery?

Consumers, employees, enterprise clients, and many other key stakeholders trust organizations with their most sensitive personally identifiable information (PII). This includes social security numbers, addresses, health records, birth dates, and much more. The volume of PII organizations are trusted with has increased exponentially in recent years, with no signs of letting up: in fact, in the next three years, we will create more data than we did over the past *three decades*.[1]

At the same time, organizations must ensure their data storage and handling practices maintain compliance with a broad range of data privacy regulations. All organizations face a multitude of mandatory industry and global data management obligations, irrespective of how and where they store and process their data. These obligations fuel data-related challenges around complexity, hygiene, process, and reporting.

GDPR, CCPA, CPRA, PDPA, HIPAA, LGPD, PCI DSS

GDPR, CCPA, CPRA, PDPA, HIPAA, LGPD, PCI DSS — in today's global economy, the alphabet-soup of data privacy regulations continues to grow. Each year, more regions and more industries enact new rules that require compliance.
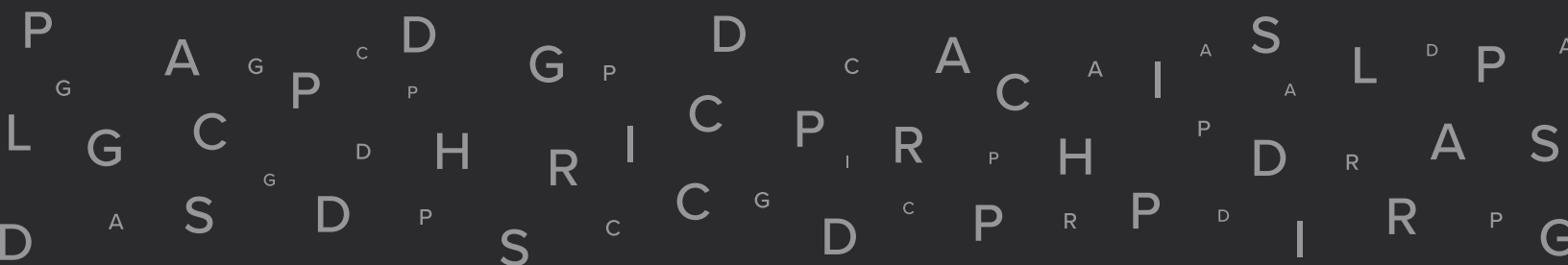
Data discovery is a process that enables organizations to identify and locate both structured and unstructured data they are storing, with the goal of securing or remediating any sensitive data. As an essential part of any security plan, data discovery helps organizations to achieve their compliance goals, secure sensitive information, protect customers and employees, prevent data breaches, and deliver trust to customers, employers, and shareholders.

Effective data discovery needs to be an ongoing process. Compliance regulations are constantly evolving and ever-growing customer and employee bases mean the data your organization is storing is changing too. Continuous data discovery helps security teams maintain an ongoing proactive understanding of where all sensitive data is stored.

GROUND LABS

Why Your Organization Should Be Leveraging an Effective Data Discovery Solution

Companies store their data in so many locations that it is impossible to search for it all manually. The majority of organizations are unable to pinpoint where their data resides. This is especially applicable when it comes to personal or sensitive data. They assume that all of their customers' PII data is stored in one or two databases, while they are actually unknowingly storing data in a myriad of locations. As a result, these companies draw conclusions and establish policies based on inaccurate assumptions around what they think their data storage should be rather than how it actually is processed and stored.

Companies often unknowingly store PII in many locations, including:

Cloud Storage Providers

Databases + Servers

Email

Workstations

An effective data discovery solution provides organizations with insights into their current and evolving organizational needs, giving security teams control over their data. Data discovery solutions can help your business achieve the following security goals:

Meet Compliance Obligations

Compliance with privacy regulations needs to be a top priority for every organization. Depending on your industry and the geographic regions your business operates in, there might be several compliance laws you need to adhere to.

128 countries around the world have implemented data privacy legislation, and many other regulations exist at the local and industry-specific level.[2] Here are a few examples of these data privacy regulations that apply to a wide variety of businesses:

GDPR   PCI DSS 4.0   CCPA   HIPAA

Data discovery solutions can help your team scan servers for PII, the first step towards achieving compliance with most privacy laws. Global and regional requirements are ever-changing, and a PII discovery tool ensures organizations avoid liability and risk. They can also help organizations comply with subject access requests (SARs) when individuals request a copy of the data the organization has stored from them.[3]

Mitigate Risk

Today, risk management and risk mitigation are not simply board level discussions: CISOs and CTOs have to try to manage risk across multiple aspects of an organization, including firewalls, endpoint antivirus, VPNs, networks, and more. The core thing being protected by risk management and mitigation policies, is, in many cases, data. Yet where that data resides is often a secondary consideration. When looking at data as a key asset, and not just as what gets generated, organizations can start mitigating risk to enhance their security posture.

Data discovery should be part of every organization's data asset and data management policies. This will allow security teams to drive change management policies, such as leveraging data insights to improve staff productivity and deficiencies.

Understanding where your data resides is particularly important when your company is going through an acquisition or divestiture. If your company is going through a merger or acquisition, you will likely take on a lot more data all at once. Data discovery can help make the M&A transition process more smooth and secure by helping your team find, keep track of, and secure all that new data.

As every business is becoming a cloud first organization, data discovery is also a critical tool to help security teams understand what their organization is transitioning to the cloud. Data discovery will help your organization establish good data hygiene before the transition, and ensure you are only moving the appropriate data to the cloud. This allows you to avoid a lift and shift strategy, lowers the cost of storage, and minimizes legal exposure.
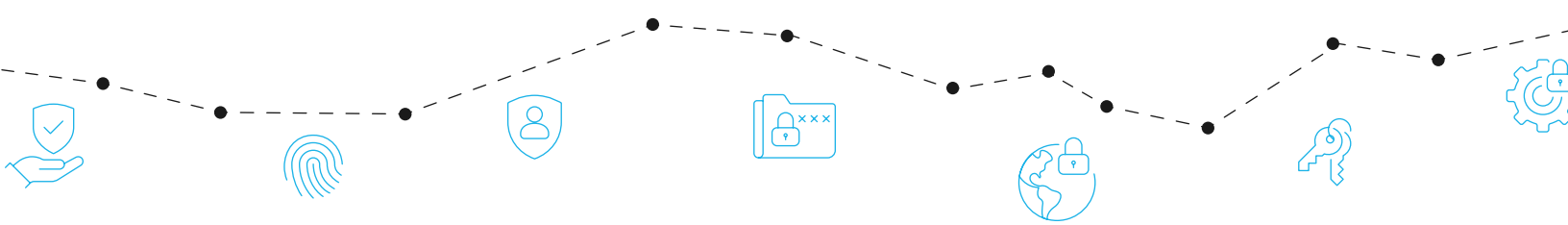
Maintain Customer & Employee Trust

Companies that experience a data breach often experience a loss of customer trust and lost business. A privacy law fine imposed after a data breach might seem small and manageable for an organization, but losing your customers' trust can have a devastating impact on your brand and shareholder value. In 2020, the average cost due to business loss from a data breach was $1.52 million — an amount that can have a significant impact on a company's bottom line.[4]

Data discovery solutions allow your team to build and execute a proactive approach to data security — as opposed to a reactive approach that relies on damage control post-breach — to build a stronger foundation of trust within your organization.

GROUND LABS

What to Look for in an Enterprise-Grade Solution

When choosing a data discovery solution, you want to select a solution that addresses the specific needs of your organization, while also expanding its capabilities as your needs grow. Some foundational things to look for are whether the solution will allow you to accomplish the scan in the timeframe you need, if it can connect *to the targets that hold your data, and whether it can handle unique data at your organization.*

You want a data discovery tool that is not a stand alone solution, but one that works to mitigate risk by integrating with tokenization and encryption tools, API frameworks, and BI reporting solutions. Ensure you are considering not just the reporting tools and frameworks you use now, but others you might want to use in the future.[5]

Primary Factors to Look For

Class-leading accuracy

Discover both personal and sensitive data

Lack of false positives

Speed across network with little or no network impact

Scope of targets natively supported

Ease of use and remediation capability

Risk analysis and mapping capabilities

Reporting tools the solution integrates with, such as ODBC, Power BI, etc.

Future-proof technology

APIs for tokenization and encryption

Diverse ecosystem of targets and data types

The number and types of target systems where the solution can perform data discovery *(Can the solution scan all the systems in your environment?)*

Ability to add custom data patterns and exclusions

Ability to scan images (OCR scanning)

What to Avoid

Avoid data discovery solutions that simply look at a sample of data, instead of your entire data source. Any tool that uses a sample will inevitably miss critical data. You also want to avoid solutions that do not allow you to create filters to prevent false positives. For example, AAA automobile club numbers look similar to credit card numbers. If you are not able to filter out AAA numbers, your data discovery solution will register them as credit card numbers.

Why Choose Enterprise Recon from Ground Labs?

With Enterprise Recon by Ground Labs, organizations can find and remediate personal and sensitive information across the broadest range of structured and unstructured data, whether it is stored across servers, on desktops, email, and databases, on prem and in the cloud. Enterprise Recon enables organizations worldwide to seamlessly discover all of their data and comply with an extensive range of data compliance standards, including GDPR, PCI DSS, CCPA, HIPAA, and Australian Privacy.

Enterprise Recon is powered by Ground Labs' proprietary, award-winning GLASS Technology™. GLASS Technology™ is the quickest and most accurate data discovery solution on the market, with speeds between 20x - 6,000x faster than the legacy data discovery technology from RegEx. Enterprise Recon comes with over 300 predefined patterns out of the box, and makes it easy for you to set up custom data patterns unique to your organization's needs, reducing the number of false positives. Enterprise Recon enables data discovery, risk scoring, and data classification across the broadest set of platforms available.

With Enterprise Recon by Ground Labs, organizations can:

Identify more than 300 data types of structured and unstructured data including pre-configured, compliance-specific personally identifiable information (PII) patterns

Demonstrate compliance with custom reporting and analytics available in Enterprise Recon

Scan immediately and quickly thanks to a low-impact distributed design, complementing and strengthening your data loss prevention strategy

Accurately map data across networks, servers, and platforms to keep tabs on PII data and more easily respond to consumer compliance requests

Easily build custom data types and search platforms to locate and remediate unique data types to address your organization's unique needs

Search within both structured and unstructured data sources including files, databases, emails, cloud, big data and more

Easily view and analyze the access permissions for sensitive data locations and immediately take action to minimize risk by managing and controlling access to those locations

Establish a 'Risk Profile' based on a Risk Mapping/Scoring feature, enabling the tagging of high, medium and low data risks across your network

Execute a proactive approach to data security — as opposed to a reactive approach that relies on damage control post-breach — to build a stronger foundation of trust within your organization

Ground Labs offers award-winning customer service 24 hours a day, 5 days a week. Over 5,500 customers trust Ground Labs for their data discovery needs, including Thales, McDonalds, Verifone, Wynn Casinos, Dufry, Pilot Travel Centers, Global Partners LP, Woodforest National Bank, City West Water Corporation, Jackson College and Fidelity International.

"**Organizations today need to be aware of what data they handle, where they store it and what controls they have to protect it. Ground Labs develops products that fit this requirement. The tools are easy to use yet provide incredibly valuable information that can be acted on for further analysis or remedial efforts. The applications support most popular operating systems, databases and also a number of online applications."**

— **Murray Goldschmidt,**
    COO, *Sense of Security*

"**After exhaustive due diligence and market alliance, we chose to partner with Ground Labs for meeting our PCI DSS obligations, through unmatched accuracy. Based on their expansive data discovery features in Enterprise Recon we're also able to meet our growing needs for PII as well."**

— **Angel Galvez Caballero,**
    Global IT Security Head, *Dufry*

Conclusion

Whether you are running a single machine or 100,000 systems, Ground Labs has the proven, trusted technology to help you discover all your data and meet evolving compliance regulations. Book a demo with a member of the Ground Labs team by visiting: **https://calendly.com/ground-labs-global-sales-team.**

GROUND LABS

The References

[1] "IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data," IDC, May 8, 2020, https://www.idc.com/getdoc.jsp?containerId=prUS46286020#:~:text=By%20 2024%2C%20IDC%20expects%20this%20ratio%20to%20be%201%3A10.&text=Productivity%2Fembedded%20 data%20is%20the,somewhat%20by%20COVID%2D19%20dynamics.

[2] "Data Protection and Privacy Legislation Worldwide," United Nations Conference on Trade and Development, February 2020, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[3] "What is a Subject Access Request?: Everything You Need to Know," Truyo, https://insights.truyo.com/what-is-a-subject-access-request.

[4] "Cost of a Data Breach Report," IBM, 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

[5] Richa Pathak, "3 Ultimate Tips to Choose the Right Sensitive Data Discovery Tools," Tech Web Space, April 29, 2020, https://www.techwebspace.com/3-ultimate-tips-to-choose-the-right-sensitive-data-discovery-tools/.

GROUND LABS