

SURIDATA.AI

DATA MANAGEMENT FOR SECURITY



INFORMATION SECURITY

Discover and classify your data at speed and scale. Enhance your security and threat response platform.

DATA GOVERNANCE

Assure the integrity of your data. Limit access to sensitive data to only those who need it. Realize its value.

PRIVACY & COMPLIANCE

Reduce the cost of regulation on your business. Automate reporting and compliance documentation.

- **Label and classify sensitive** information to precisely enforce Zero Trust policies and wisely allocate security resources.
- **Ensure only authorized users can access** customers' information, employees' records, financial statements and other sensitive data.
- **Harvest your information assets** to gain operational efficiency and competitive advantage.
- **Reduce the cost and disruption** of compliance with GDPR, HIPAA, PCI, and CCPA. Automate Subject Access Requests.



Suridata autonomously discovers sensitive, private, or other target information across an enterprise's data infrastructure. This breakthrough AI-driven discovery and classification engine is based on Natural Language Processing (NLP) technology. Data is reviewed and analyzed in a human-like manner. Classification is based on content and context.

No rules to write. No keyword dictionary to be defined. No Regex to be coded. No agents to be deployed. Suridata can be implemented quickly with no business disruption.

The Suridata solution can discover and map data stored on prem or in the cloud. It can analyze both structured and unstructured data. It can classify data at rest and in motion. Suridata software is offered as SaaS or a subscription that can be hosted in your cloud or on your premises.

Suridata provides a complete map and inventory of your most sensitive data. It provides visibility and control across the enterprise from a single pane of glass.

Accurate classification enhances your security platform's ability to prevent data leakage and mitigate security risk by focusing your resources on the areas that represent the greatest threat.

Improve data governance by controlling access to sensitive info. Support your legal team by ensuring appropriate retention. Help your data science team apply information assets to improve operational efficiency and competitive edge.

Automate and reduce the burden of compliance with regulations like GDPR, HIPAA, PCI, CCPA and more.

HIGHLY ACCURATE

Suridata goes beyond rule-based file type and pattern recognition to grasp the true nature of each file's content – which means less false positives and zero disruptions to your business operations.

EFFECTIVE

Accurate classification enhances your security platform's ability to prevent data leakage, implement data governance, and reduce the cost of regulatory compliance.

FAST TIME TO VALUE

No rules to write. No keyword dictionary to be defined. No Regex to be coded. No agents to be deployed. We do in weeks what others take months to achieve.

For more information on our disruptive technology, please visit us on the Web at: www.suridata.ai



THE NLP ADVANTAGE



Autonomous learning of your data unique to your organization is what makes our technology better. Natural Language Processing (NLP) is the basis of our machine learning discovery and classification engine. It understands your data the way a human would. Classification is based on content and context.

The engine's innate understanding is further honed by training the machine learning platform. Simply drag & drop a few sample files containing sensitive data and let our engine independently learn and discover similar files across all your data sources. This process results in precise discovery and mapping of your true data assets, with a fast time to value and a very low false positive

Eli Vidavsky
IT & Cyber Director

Deloitte.

“By using Suridata.ai's solution I am confident that our customers' data is protected. I'm capable of gaining this peace of mind with minimal resources. Their unique ability to label sensitive information, allows me to locate our most valuable data.”

THE FOUNDATION OF ZERO TRUST

A variety of technologies including DLP, CASB, Identity Governance (IGA), Email Management and more seek to limit data access or transmission according to file content. These technologies need a reliable source of truth to base their decisions on what information to restrict and what should be allowed to flow freely to prevent business disruption.

By providing consistent data classification across the enterprise, Suridata provides a foundation for these technologies to ubiquitously apply Zero Trust policy and enforcement.



DATA SOURCES

Suridata will find and classify data that resides on prem or with cloud service providers such as:

