SOLIXCloud

eBook

From Detection to Protection:

The Essentials of Sensitive Data Discovery and Security-Compliance Tools

Call to find out more
+1.888-GO-SOLIX

Visit our website for more
www.solix.com

Index

Why This Ebook?

The journey of sensitive data protection starts with effective discovery. Understanding what constitutes sensitive data, where it resides, and how it moves through an organization is the foundation of any data security strategy. This ebook comprehensively explores sensitive data discovery, from its definition and importance to the business case for its implementation.

We invite you to dive into the chapters ahead, where you'll discover the strategies and tools necessary to navigate the complex world of sensitive data security. Through this journey, you will be better equipped to protect your organization’s most critical assets and ensure your customers' and stakeholders' trust and confidence.

Welcome to the comprehensive guide on Sensitive Data Discovery and Security-compliance tool. Let’s begin this crucial journey together.

Chapter 1: Introduction to Sensitive Data Discovery

Sensitive data discovery involves identifying, categorizing, and managing sensitive information within an organization's data repositories. This data can reside in various forms, including structured databases, unstructured files, and even in transit across networks. The primary goal is to protect this data from unauthorized access, misuse, or exposure.

Sensitive Data

Sensitive Data refers to information whose disclosure could potentially harm individuals or organizations. This category includes personally identifiable information (PII), financial records, medical data, intellectual property, and confidential business details. Discovering sensitive data is crucial for maintaining data privacy, complying with regulatory requirements, and safeguarding the organization's reputation.

Types of Sensitive Data

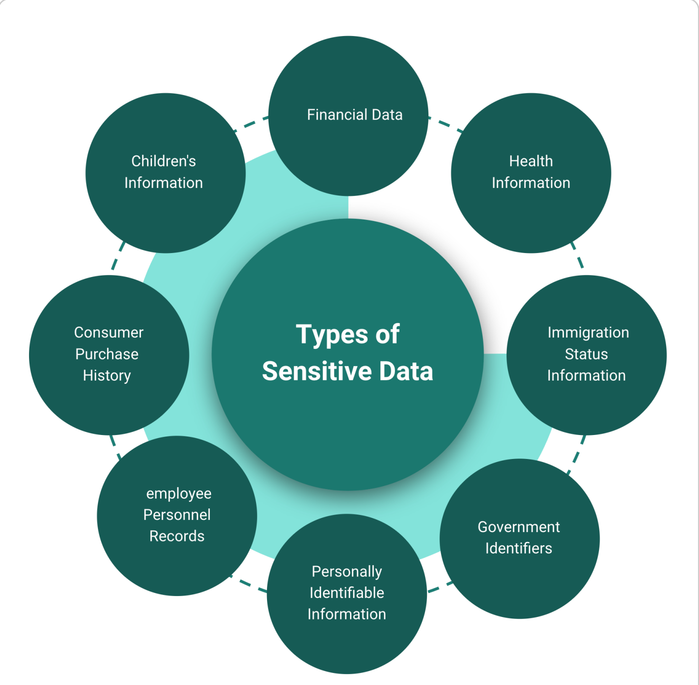

Financial Data
Children's Information
Health Information
Types of Sensitive Data
Consumer Purchase History
Immigration Status Information
employee Personnel Records
Government Identifiers
Personally Identifiable Information

image source: www.solix.com

- **Personally Identifiable Information (PII):** PII includes any data that can be used to identify an individual uniquely. This may include names, addresses, social security numbers, passport numbers, etc.
- **Financial Data:** It encompasses details related to an individual's or organization's financial transactions, such as credit card numbers, bank account information, transfers, investments, or financial statements.
- **Health Information:** Protected health information (PHI) includes medical records, health insurance details, or any other information related to an individual's health or medical treatment.
- **Biometric Data:** Biometric information includes fingerprints, retina scans, voice patterns, or any unique biological characteristics used for identification.
- **Government-Issued Identifiers:** This includes data like social security numbers, passport numbers, or driver's license information issued by government entities.
- **Children's Information:** This includes data relating to minors, such as their names, addresses, educational details, paternal details, or any other information that could be used for illegal purposes.

In addition to the sensitive data mentioned above, the list also includes employee personnel records, login credentials, location data, communication content, consumer purchase history, social media data, supply chain information, asset and inventory data, intellectual property (IP) data, trade secrets, research and development data, political affiliations, visitor and guest logs, voice recordings, immigration status information, emergency contact information, and more.

Chapter 2: The Business Case for Sensitive Data Discovery

As the amount of data expands rapidly, so do the risks and challenges associated with managing it. Investing in sensitive data discovery tools is not merely a technical necessity; it is a strategic business imperative.

Why Discovering Sensitive Data Matters

- **Enhancing Data Security:** Discovering sensitive data is the first protection step. Organizations can deploy suitable security measures to prevent unauthorized access and breaches by identifying sensitive data locations. This proactive strategy effectively minimizes the likelihood of data exposure and enhances overall security resilience.

- **Ensuring Regulatory Compliance:** Regulations like GDPR, CCPA, and HIPAA mandate protecting sensitive data. Compliance requires effective identification and management of this data. Non-compliance can incur hefty penalties and legal consequences, dictating necessary investments in data protection.

- **Operational Efficiency:** Sensitive Data Discovery automates identifying and classifying sensitive information, enhancing operational efficiency. This enables organizations to allocate resources effectively and streamline compliance processes by understanding data location and significance.

- **Trust and Credibility:** The data discovery and security-compliance tool allows organizations to showcase proactive efforts to secure data, fostering a positive reputation among clients and stakeholders and ultimately bolstering the organization's credibility in the eyes of the public.

The Risks of Unsecured Sensitive Data

- **Data Breaches and Their Consequences:** Unsecured sensitive data is a prime target for cybercriminals. Data breaches can lead to substantial financial setbacks, legal responsibilities, and erosion of customer confidence. For instance, the average data breach cost in 2023 was estimated at $4.45 million.

$1.8 Billion +	**250 +**	**$1.3 Million**	**<$200**	**500K +**	**100+**
2023 Penalties	**2023 Fines**	**Largest Fine**	**Smallest Fine**	**Data Privacy Officers**	**Countries with privacy laws**

- **Reputational Impacts:** The financial impact of a data breach extends beyond immediate losses to include regulatory fines, litigation costs, and long-term brand damage. A tarnished reputation results in customer loss and reduced business opportunities, highlighting the critical need for effective sensitive data discovery and protection.

> ***A leading cybersecurity firm found that a single privacy breach could cause 34% of customers to stop doing business with a company, as loyal users expect critical privacy obligations to be met.***

Chapter 3: How Sensitive Data Discovery Works?

It uses advanced technologies and methodologies to scan, analyze, and categorize data, empowering enterprises to comprehensively understand the sensitive data landscape. This process involves detecting patterns, keywords, and predefined criteria that signify sensitive information.

- **Data Source Scanning:** The process begins with a comprehensive scan of diverse data sources, including unstructured data repositories. It generally employs predefined criteria, such as patterns, keywords, and data formats, to identify potential instances of sensitive information.

- **Pattern Recognition and Keyword Analysis:** Advanced algorithms identify patterns, keywords, and data formats. The tool enhances accuracy using the latest technologies like regular expressions, machine learning, and artificial intelligence.

- **Contextual Analysis:** This discovery process often incorporates contextual analysis to enhance identification by considering surrounding data and relationships. Understanding sensitive information's interconnections enhances classification accuracy and reduces false positives.

- **Content Classification:** Once sensitive data has been identified, the tool categorizes it, aiding organizations in prioritizing and addressing high-risk areas for efficient data protection and ensuring a targeted approach.

- **Automated Reporting and Alerts:** The tool generates automated reports detailing the findings of the sensitive data scan. These reports include insights into the types of sensitive information discovered, their locations, and the associated risk levels.

- **Integration with Data Masking:** One key strength of sensitive data discovery is its seamless integration with data masking techniques. With insights from the discovery process, organizations can implement data masking to protect sensitive information throughout its lifecycle.

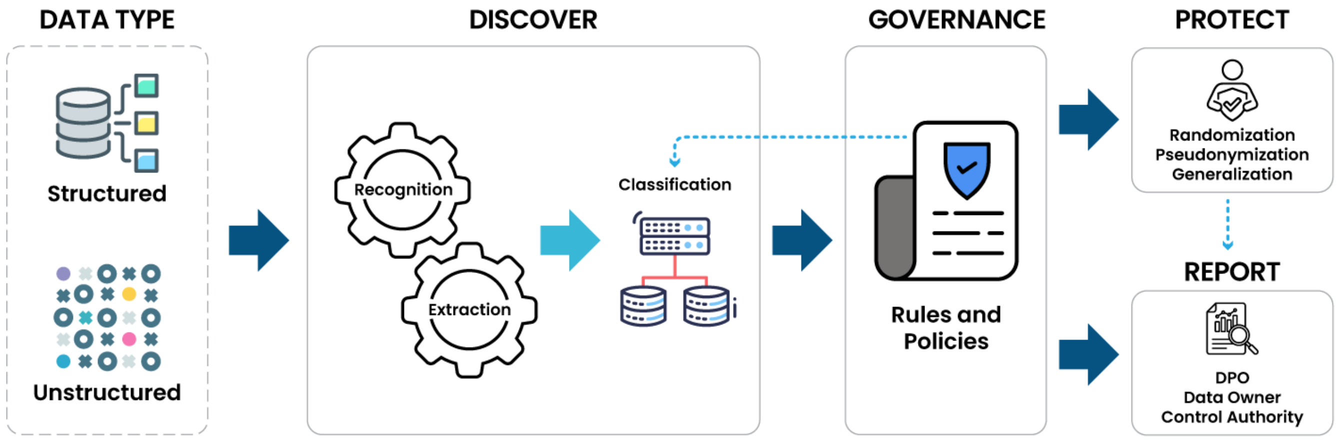


image source: www.solix.com

Chapter 4: Key Requirements of an Effective Data Discovery and Security-Compliance Tool

Effective data discovery and security-compliance tools are essential for navigating new data challenges and providing the foundation for comprehensive data protection strategies. An effective tool must go beyond basic functionalities.

Comprehensive Data Scanning

- **Data Classification:** Effective data discovery tools employ advanced techniques to classify data accurately. These techniques include pattern matching, machine learning algorithms, and contextual analysis to identify and categorize sensitive information across various data sources.

- **Data Mapping and Inventory:** Creating a detailed data map and inventory is essential for identifying all locations where sensitive data resides. This practice helps organizations maintain a comprehensive view of their data landscape, facilitating better management and protection of sensitive information.

- **Metadata Management:** Maintain detailed metadata for all data assets, including data origin, ownership, and lineage. This provides context and aids in effective data management and governance.

Data Privacy and Security

- **User Access Controls:** Organizations secure sensitive information by implementing strong access controls, ensuring only authorized personnel can access it. This approach effectively reduces the likelihood of internal threats and data misuse.

- **Data Masking and Encryption:** Data masking and Encryption techniques protect sensitive data by obfuscating it, making it unreadable to unauthorized users. This ensures that masked data retains zero value for attackers in a security breach, concealing sensitive information in its original form.

- **Compliance Reporting:** Capability to generate compliance reports and audit trails to demonstrate adherence to regulatory requirements and internal policies.

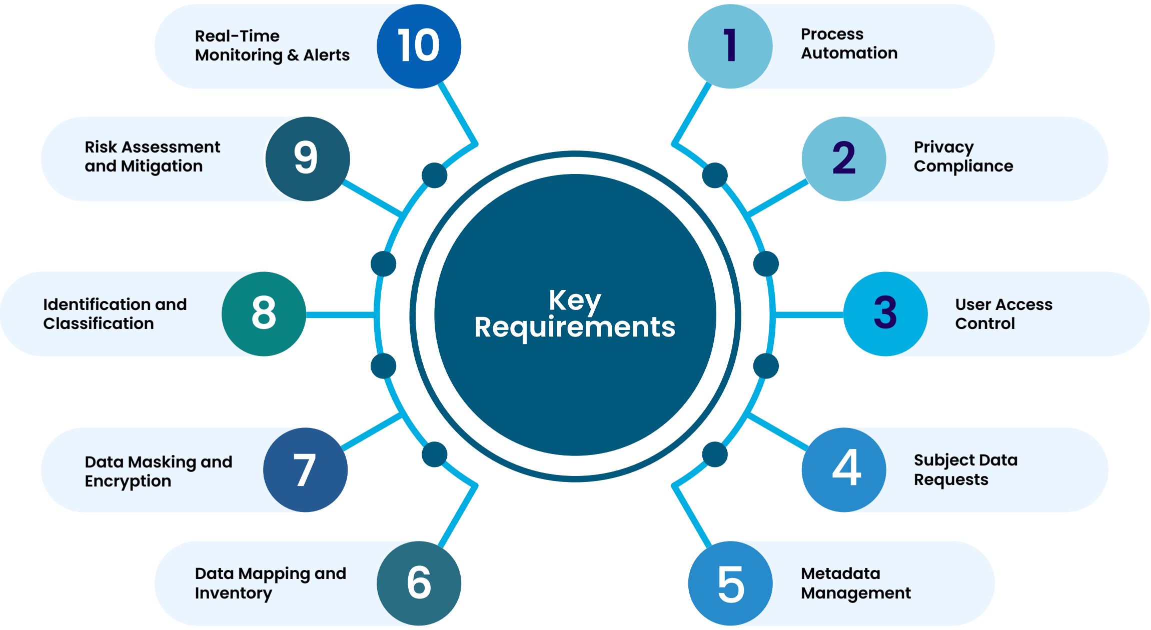

Key Requirements
1 Process Automation
2 Privacy Compliance
3 User Access Control
4 Subject Data Requests
5 Metadata Management
6 Data Mapping and Inventory
7 Data Masking and Encryption
8 Identification and Classification
9 Risk Assessment and Mitigation
10 Real-Time Monitoring & Alerts

image source: www.solix.com

Data Subject Requests

- **Streamlining Subject Data Requests:** A built-in subject data request feature can help organizations meet legal requirements such as GDPR, CCPA, and HIPAA, avoid fines, and mandate that individuals have the right to access, rectify, and delete their data. It demonstrates the organization's commitment to respecting user privacy and handling personal data responsibly.

Automation and Integration

- **Automation in Data Management:** Automation enhances efficiency and accuracy in data discovery. Automated tools can continuously scan for sensitive data, minimizing the potential for human error and ensuring that data discovery processes align with data expansion. It also frees IT resources, allowing them to focus on more strategic tasks.

- **Integration with Existing Systems:** For seamless operation, data discovery tools must integrate with existing IT infrastructure, including databases, file systems, and cloud storage. This integration ensures that all data, regardless of location, is subject to discovery and protection processes.

Real-Time Monitoring and Alerts

- **Importance of Continuous Data Monitoring:** Continuous monitoring is essential for maintaining data security in dynamic environments. Real-time monitoring allows organizations to promptly detect and respond to potential security threats, minimizing the exposure window and mitigating the impact of breaches.

- **Setting Up Effective Alert Systems:** Effective alert systems notify stakeholders of suspicious activities or policy violations in real time. These alerts should be configurable to prioritize critical issues and provide actionable insights for swift resolution.

Risk Assessment and Mitigation

- **Identifying Vulnerabilities:** A thorough risk assessment involves identifying potential data storage, access, and processing vulnerabilities. This involves assessing the efficiency of current security protocols and identifying gaps that could be exploited by attackers.

- **Developing Response Plans:** A robust response plan is essential for minimizing the consequences of data breaches. This plan should include incident detection, containment, eradication, and recovery procedures. Regular drills and updates to the response plan guarantee that the organization is ready to manage security incidents efficiently.

> ***51% - Organizations plan to increase their security spending, focusing on areas such as incident response (IR) planning and assessment, training employees, threat detection, and response tools, as per a recent study.***

Chapter 5: Implementation of Sensitive Data Discovery and Security - Compliance Tools

Implementing sensitive data discovery and security-compliance tools is a multifaceted process, as these tools are designed to provide comprehensive visibility into the data landscape, enabling organizations to detect and secure sensitive information across all environments, whether on-premise, cloud-based, or hybrid.

Steps to Deploy the Tool

- **Planning and Strategy:** Successful data discovery and security-compliance tool implementation begins with thorough planning. Key steps include defining the scope of discovery and security, identifying data sources, setting objectives, and allocating resources.

- **Assessment of Requirements:** Then conduct a thorough assessment of your organization's data landscape, including types of data stored, data sources (databases, file systems, cloud platforms), and regulatory compliance requirements (e.g., GDPR, CCPA).

- **Vendor Evaluation:** Research and evaluate different data discovery and security-compliance tool vendors based on your requirements, budget, scalability needs, vendor reputation, add-on services, and integration capabilities with existing IT infrastructure.

- **Consider Key Stakeholders:** Collaboration among stakeholders, including IT, security, and compliance teams, is vital to align goals and ensure successful deployment. The data privacy officer oversees compliance with regulations, the IT team manages technical deployment and integration, the security team assesses vulnerabilities, and the finance team validates ROI with shortlisted tools.

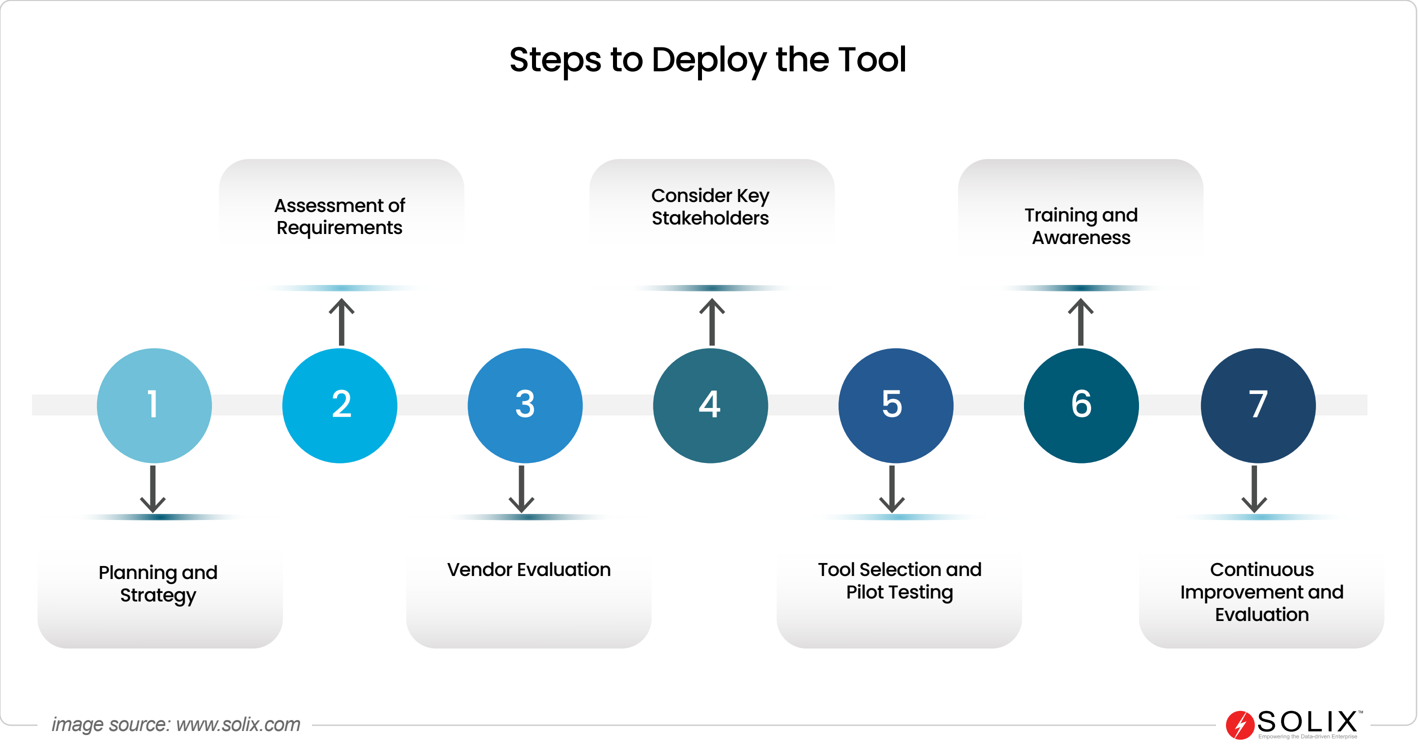

Steps to Deploy the Tool
Assessment of Requirements
Consider Key Stakeholders
Training and Awareness
1
2
3
4
5
6
7
Planning and Strategy
Vendor Evaluation
Tool Selection and Pilot Testing
Continuous Improvement and Evaluation
SOLIX
Empowering the Data-driven Enterprise

image source: www.solix.com

- **Tool Selection and Pilot Testing:** Select the tool that best suits your organization's needs and objectives. Before full deployment, conduct pilot testing in a controlled environment to assess the tool's performance in identifying sensitive data accurately, minimizing false positives, protecting sensitive data, and integrating seamlessly with existing systems.

- **Training and Awareness:** Provide thorough training sessions for employees on how to use and administer the tool. Educate them on the importance of data protection, regulatory compliance, and properly using sensitive data discovery features.

- **Continuous Improvement and Evaluation:** Establish regular reviews and evaluations of the data discovery tool's performance. Monitor its effectiveness in identifying sensitive data, addressing issues or gaps, and implementing necessary updates or enhancements.

Chapter 6: Overcoming Challenges in Data Discovery

Navigating the landscape of sensitive data discovery presents organizations with a myriad of challenges that extend beyond mere technological capabilities.

- **Ensuring Accuracy:** Automated data discovery tools may not always accurately identify sensitive data, leading to potential oversights or false positives that require manual verification. Implement a multi-faceted approach that combines automated scanning with manual verification.

- **Data Privacy Concerns**: Ensuring that data discovery processes do not violate privacy regulations is critical. Careful handling and processing of sensitive data are required to maintain compliance.

- **Integration with hybrid environments:** As organizations operate in hybrid environments, managing cloud-based and on-premise data presents challenges in discovering sensitive data. Integrating discovery tools across these environments is critical for comprehensive data protection.

- **Awareness and Training:** Employees' lack of understanding regarding the significance of data security and their responsibilities in securing sensitive information can hinder efforts in data protection.

- **Data Volume and Complexity:** The sheer volume and diversity of data sources, encompassing both structured and unstructured data, make it challenging to locate and classify sensitive information consistently. Effective tools and strategies are needed to handle the complexity and scale of modern data environments.

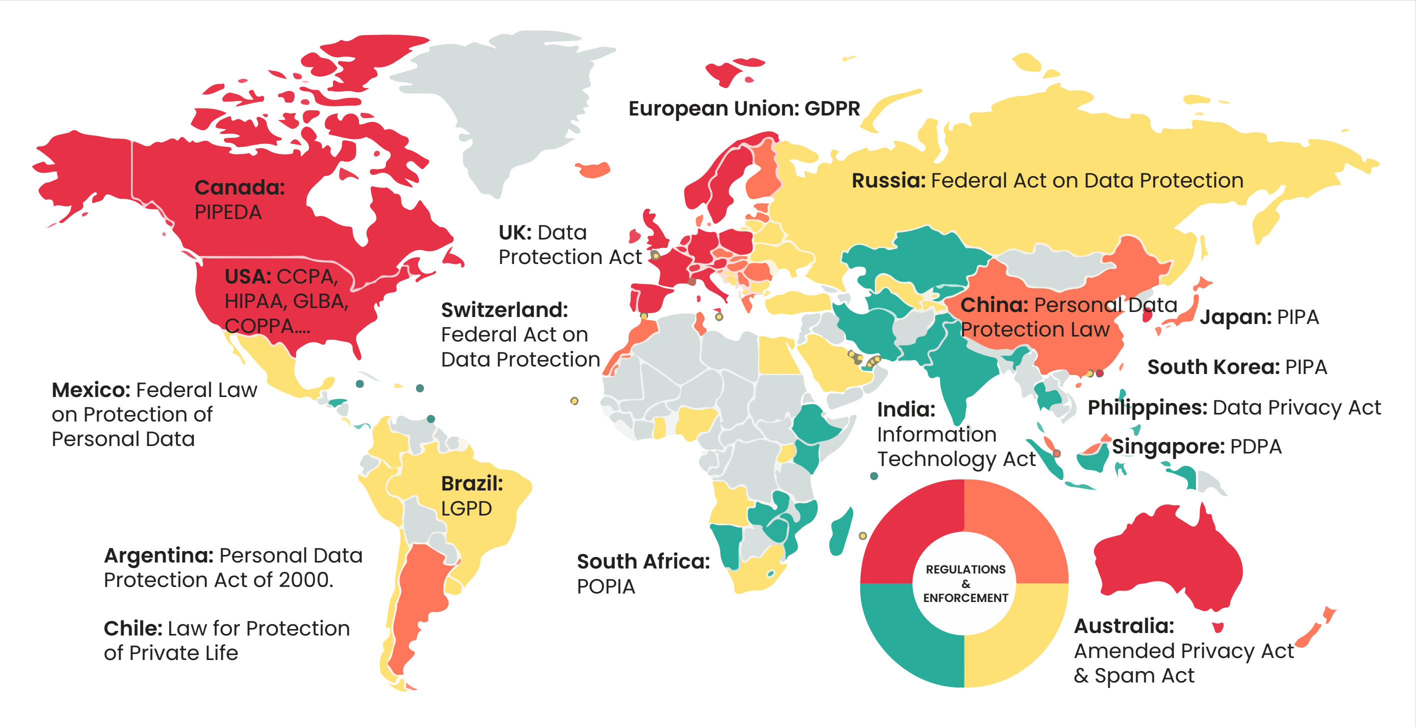
- **Data Fragmentation:** Data may be dispersed across multiple systems, databases, and cloud environments, complicating comprehensive discovery and creating potential blind spots.

> ***6\10 - Organizations report that around 21% to 50% of their sensitive data stored in the cloud lacks adequate security measures***

Chapter 7: Future Trends in Sensitive Data Discovery and Security-Compliance

The landscape of sensitive data discovery and security constantly evolves to keep pace with data storage's growing threats and complexities. Here are some anticipated future trends in this domain:

- **Ethical Data Practices:** Data ethics is becoming increasingly important as organizations handle more sensitive information. Ethical considerations in data management include respecting user privacy, ensuring transparency, and using data responsibly.
- **Emerging Regulations:** New data privacy regulations are continually emerging as governments recognize the importance of protecting personal information. Staying abreast of these changes is crucial for organizations to stay compliant and avert legal repercussions
- **Intelligent Data Classification:** Intelligent data classification systems use AI to categorize data based on its sensitivity and relevance automatically. This lowers the dependency on manual processes and improves the accuracy and efficiency of data discovery efforts.


European Union: GDPR
Canada: PIPEDA
Russia: Federal Act on Data Protection
UK: Data Protection Act
USA: CCPA, HIPAA, GLBA, COPPA....
Switzerland: Federal Act on Data Protection
China: Personal Data Protection Law
Japan: PIPA
South Korea: PIPA
Mexico: Federal Law on Protection of Personal Data
India: Information Technology Act
Philippines: Data Privacy Act
Singapore: PDPA
Brazil: LGPD
Argentina: Personal Data Protection Act of 2000.
Chile: Law for Protection of Private Life
South Africa: POPIA
REGULATIONS & ENFORCEMENT
Australia: Amended Privacy Act & Spam Act

- **Predictive Analytics in Data Discovery:** AI and machine learning technologies are revolutionizing data discovery by enabling predictive analytics. These technologies can recognize trends and patterns in data usage, helping organizations anticipate and mitigate risks before they materialize.

> *USD 1.76 million - The average savings for organizations that extensively utilize security AI and automation compared to those that do not.*

Chapter 8: Case Studies and Industry Insights

Benefits of Sensitive Data Discovery and Security-Compliance Tools

The benefits of sensitive data discovery and security tools can be significant, encompassing tangible and intangible benefits. Here are several aspects where ROI can be realized:

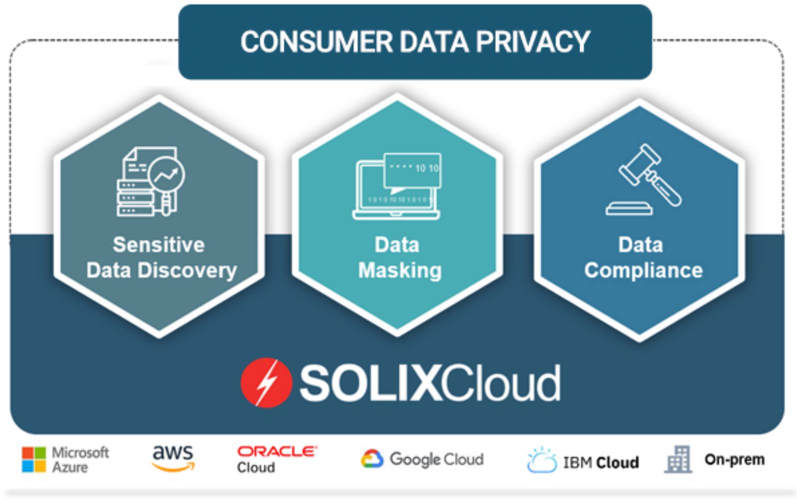
- **Improving Operational Efficiency:** integrating sensitive data discovery and security-compliance tools into business operations can streamline processes, enhance security posture, ensure regulatory compliance, and improve overall operational efficiency.
- **Improved Decision-Making:** Accurate and comprehensive insights from data discovery tools can inform better business decisions. Organizations can confidently leverage data-driven strategies, knowing that sensitive information is adequately protected.
- **Support for Digital Transformation:** As organizations undergo digital transformation initiatives, robust data discovery and security tools enable secure data sharing, collaboration, and innovation. This supports agile business practices and facilitates growth in competitive markets.
- **Cost Savings through Risk Mitigation:** Investing in sensitive data discovery and security tools can yield significant cost savings by preventing breaches and reducing compliance-related expenses.

> ***For instance, a study found that organizations using data discovery and security tools experienced a 20% reduction in data breach costs compared to those without such tools.***

Chapter 9: How Solix Solves Enterprise Security & Compliance Concerns?

Solix Technologies addresses the issues present within sensitive data via its product, SOLIX Common Data Platform (SCDP), a multi-cloud enterprise data management platform. In particular, a subset of SCDP, the Solix Consumer Data Privacy solution (CDPS), has been designed specifically for this purpose.

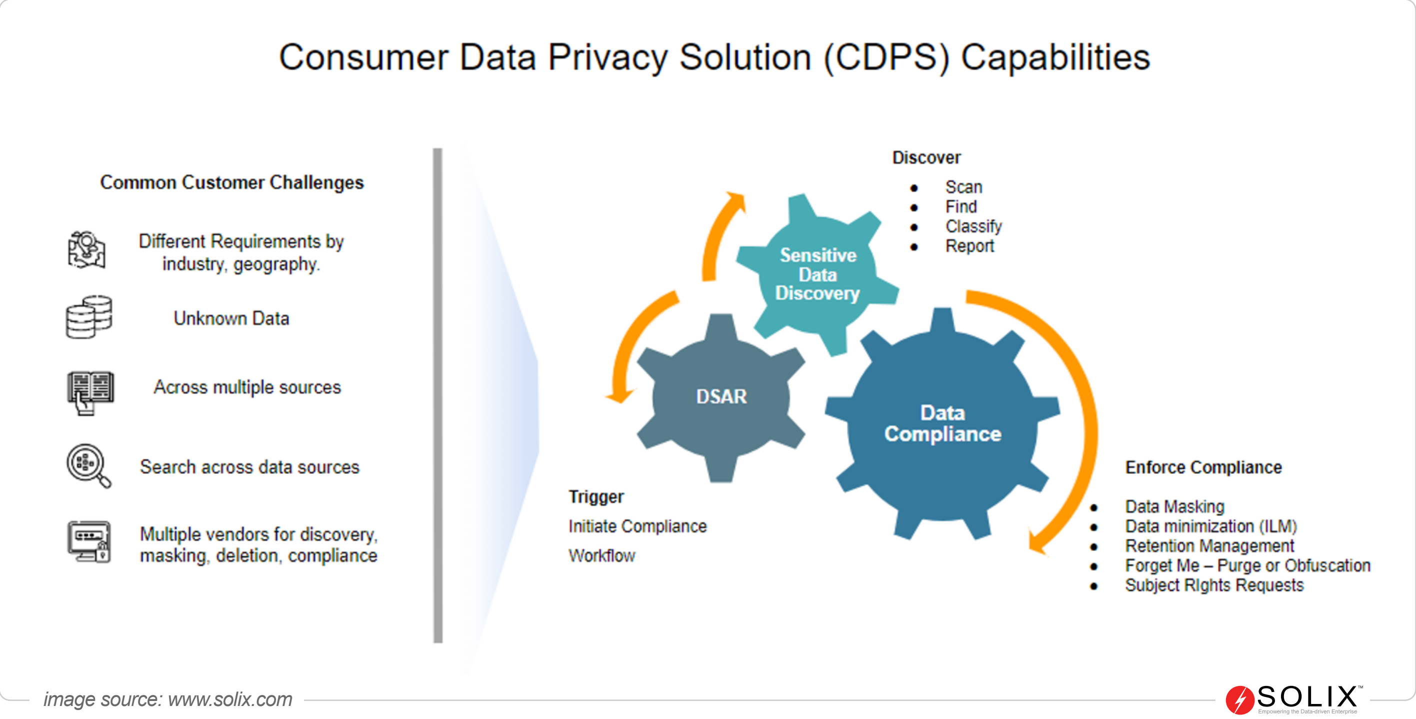
Solix CDPS is a solution for Sensitive Data Discovery, Data Masking, compliance, and policy management. These are wrapped in a layer of data governance and metadata management and bookended by extensive search and integration capabilities provided by Solix Search and Solix Connect. The latter provides connectors for hundreds of different data sources. Outgoing APIs are also available. The whole architecture is shown in Figure 1.



Solix CDPS offers comprehensive capabilities for finding, protecting, and governing sensitive data. The platform's further governance & compliance features include a data catalog, a business glossary, data lineage, lifecycle management, and more. Notable features include policy management, a legal hold that allows you to freeze information currently under request to prevent it from being edited or deleted, and a dedicated GDPR tool that will scan your enterprise and produce a report on your sensitive data and its compliance with GDPR in particular.

It also supports Data Subject Access Requests by producing all information about an individual and purging it from your systems on an essentially ad hoc basis.

To top it off, Solix CDPS comes with prepopulated discovery rules suitable for identifying PII, PCI, PHI, and other sensitive data elements, along with user-customizable rules.



Consumer Data Privacy Solution (CDPS) Capabilities

Common Customer Challenges

- Different Requirements by industry, geography.
- Unknown Data
- Across multiple sources
- Search across data sources
- Multiple vendors for discovery, masking, deletion, compliance

Discover

- Scan
- Find
- Classify
- Report

Trigger

Initiate Compliance

Workflow

Enforce Compliance

- Data Masking
- Data minimization (ILM)
- Retention Management
- Forget Me – Purge or Obfuscation
- Subject RIghts Requests

image source: www.solix.com

SOLIX™

At Solix Technology, we are committed to empowering organizations with the tools and knowledge necessary to navigate this complex landscape effectively. By leveraging our advanced data discovery and protection solutions, businesses can fortify their defenses, uphold regulatory standards, and build customer trust. We invite you to apply the insights earned from this ebook to your organization's data security strategy. Let's continue to innovate and prioritize data protection to ensure a secure and resilient future for all.

Download Ebook: [A Guide to Data Security and Data Privacy in Non-Production and Analytical Environments]

DEMO

REQUEST DEMO

WWW

VISIT WEBSITE

CONTACT US

info@solix.com

+1.888-GO-SOLIX

© 2024 Solix Technologies, Inc. All rights reserved.