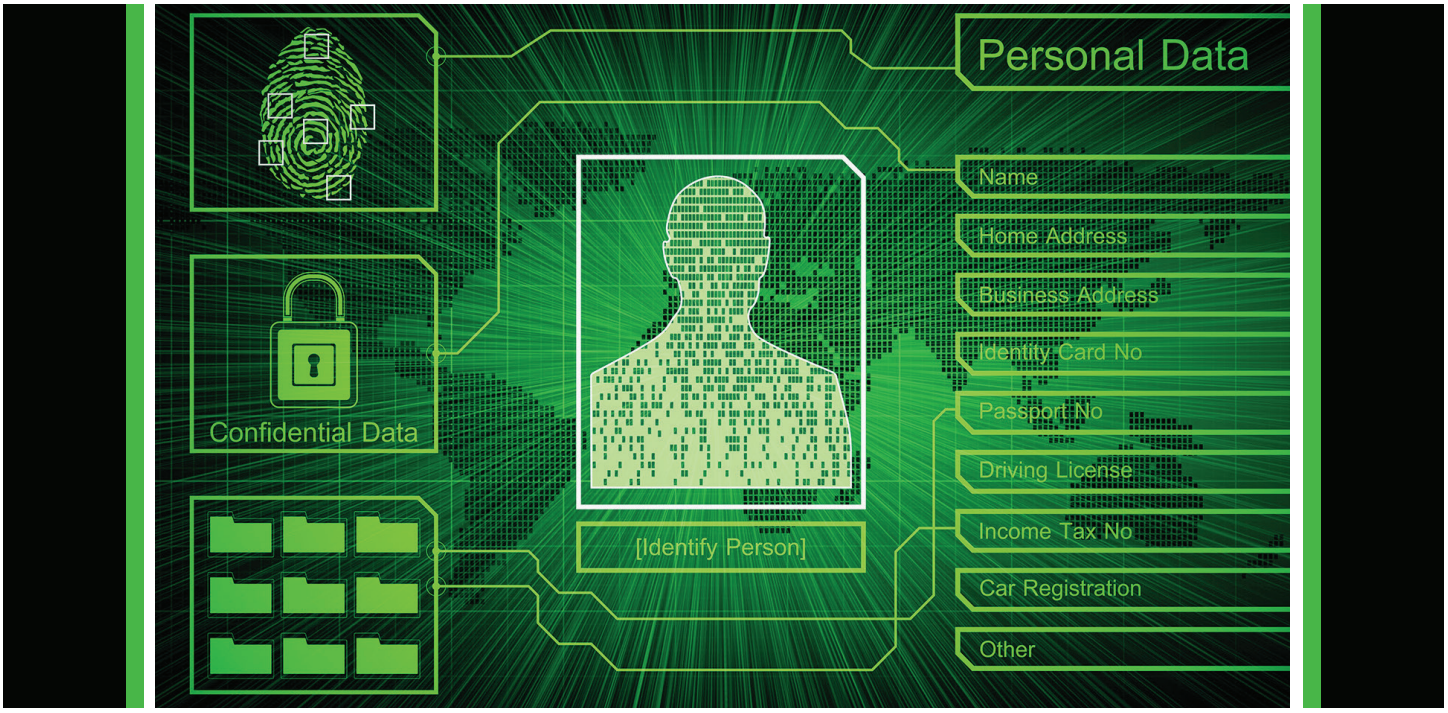
Data Protection Monitor :: Control Sensitive Data :: Ensure Compliance :: Enhance Trust



Compliance is more complex than ever with growing personal data and privacy regulations

Organizations must protect growing volumes of personal and sensitive data and comply with the nuances of a growing list of privacy regulations such as GDPR, CCPA, PCI, PII, and, HIPPA.

Highly publicized breaches dominate headlines, and cybercriminals' sophistication continues to grow. Organizations need to safeguard their reputation by monitoring data protection controls, which can be challenging, under the scrutiny of privacy-savvy customers, employees, and privacy-concerned partners.

As organizations update their data privacy policies to address the fast pace of regulatory change, they recognize the need for automated data protection controls in their information systems to address emerging compliance requirements, such as:

- Where personal and sensitive data resides and classify it according to its risk.
- Limit the number of people who have access to sensitive data and continuously monitor their access.
- Analyze data usage patterns that may signal potential abuses.
- Dispose of data that's no longer needed or valuable.
- Protect data from unauthorized access and misuse.

Capitalize on the business value of data privacy, and achieve sustained compliance

SafePaaS Data Protection Monitor transforms ad-hoc, manual and reactive data protection programs, recently adopted by many organizations, to meet the mandates of emerging new regulations into a holistic data protection process that is well-defined, continuously tracked, and optimized.

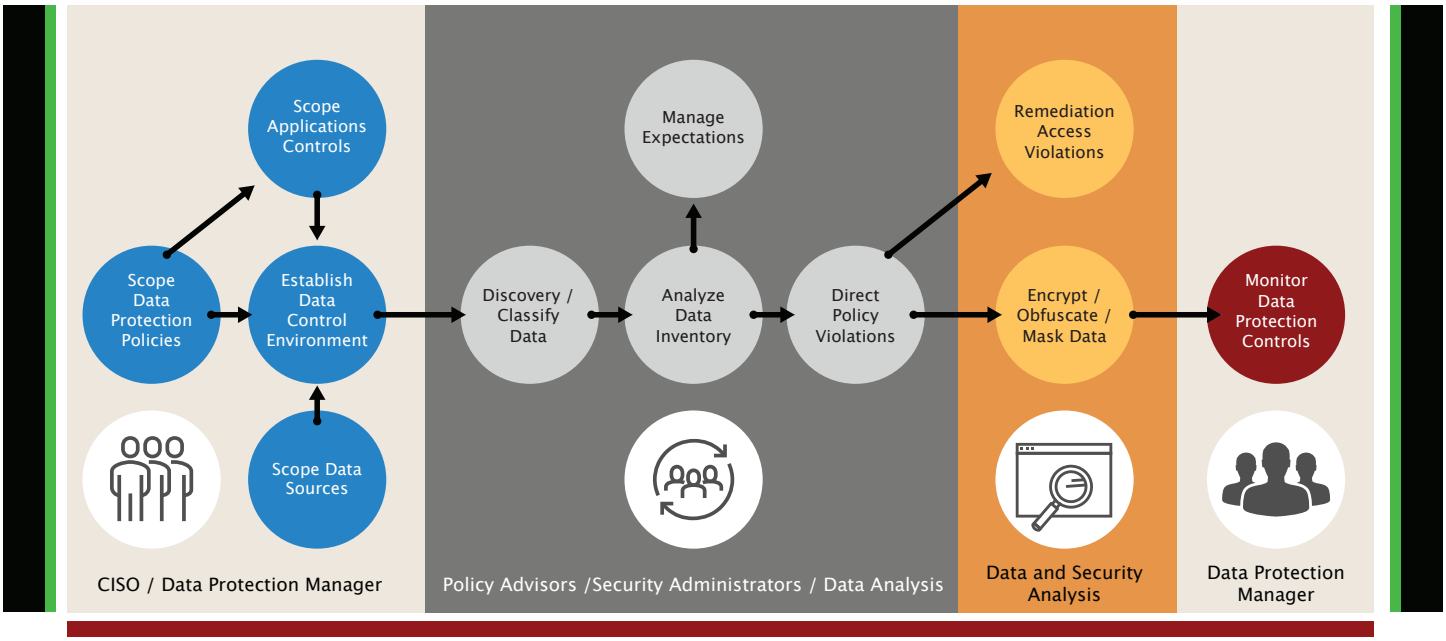
Organizations can rapidly deploy Data Protection Monitors to detect personal and sensitive data risks. The monitors generate risk incidents based on data privacy policies, which are automatically assigned to data protection owners for investigation and remediation. A closed-loop incident response workflow log maintains an effective control evidence log for independent audit of data protection policies and ensures sustained compliance.

Only firms that know where their data lives, can classify it and can deploy controls continuously and dynamically, can make the shift. Those with full confidence in their compliance abilities are more likely to have moved beyond simply defining their privacy processes to measuring and/or optimizing them too.

SafePaaS™

Copyright ©. SafePaaS, Inc.

Data protection process management best practices



Define Data Protection Policies

You can define your data protection policies in SafePaaS to build, oversee, and demonstrate sound privacy practices. Data protection policies provide data security rules to detect unauthorized access to data objects in information systems such as Human Capital Management, Financial Management, Customer Relation Management and Supply Change Management System. You can link data protection policies to legal definitions of data privacy policies that govern authorized access – who has it and who defines it.

Discover and Classify Data

Discover all the risks and appropriately classify data to map your organization's complete data lifecycle. Classifications may include Payment or Financial Information; Health, Biometric, or Genetic Information.

Maintain Data Inventory

The process to document the data lifecycle is referred to as a data inventory analysis. SafePaaS enables you to gather details about data collection, storage, usage, transfer, processing, and disposal. It helps you understand how the data is collected, how it is used, where it is stored, how it flows through and out of the company, who has access to it, and what protections are in place at each point.

Deploy Data Access Control to detect violations

Data access controls detect violations in specified data access activities, such as DML type commands and DDL type commands on the defined set of objects for all or specific users. You can define data access control as a snapshot of database activities that violate compliance or security rule. The result set of violations automatically delivers the access risk incident to the appropriate control owner on a scheduled basis by using workflow automation.

Deploy Encryption Controls to prevent violations

Prevent access to databases, files, and applications by encrypting or masking secure data residing in cloud, virtual, big data and ERP environments. Encrypt data-at-rest with centralized key management, privileged user access control and detailed data access audit logging that will help your organization meet compliance reporting requirements for protecting data, wherever it resides.

Monitor Data Protection Controls

Continuously monitor all data access operations in real-time to detect unauthorized actions based on detailed contextual information – the who, what, where, when, and how of each data access. Scan all data sources to detect vulnerabilities and suggests remedial actions. Protect sensitive or confidential data exposed in cloud and on-premise applications, without requiring changes to the application itself.

SafePaaS™

www. safepaas.com