Ghangor Cloud

Compliance And Privacy Enforcer (CAPE)

Version 1.0

Compliance And Privacy Enforcer (CAPE)

Version 1.0

GhangorCloud's CAPE is a full stack Privacy Compliance Enforcement Platform that incorporates advanced features to deliver reliable efficacy in automatic performance of Data Discovery, Data Classification, Data Mapping and Consumer Privacy Compliance Enforcement tasks in real-life Consumer Data Privacy Enforcement scenarios. CAPE platform is comprised of unique technology breakthroughs and sophisticated data security features.

AI Powered Data eDiscovery Engine

CAPE incorporates industry's most sophisticated Data Discovery Engine that has been built from ground up to address the deficiencies and constraints of previous generation Data Discovery solutions.

CAPE's disruptive eDiscovery technology provides for 3 major differentiated features:

01 Complex Data Object Definition for

a. Basic Data Object Types

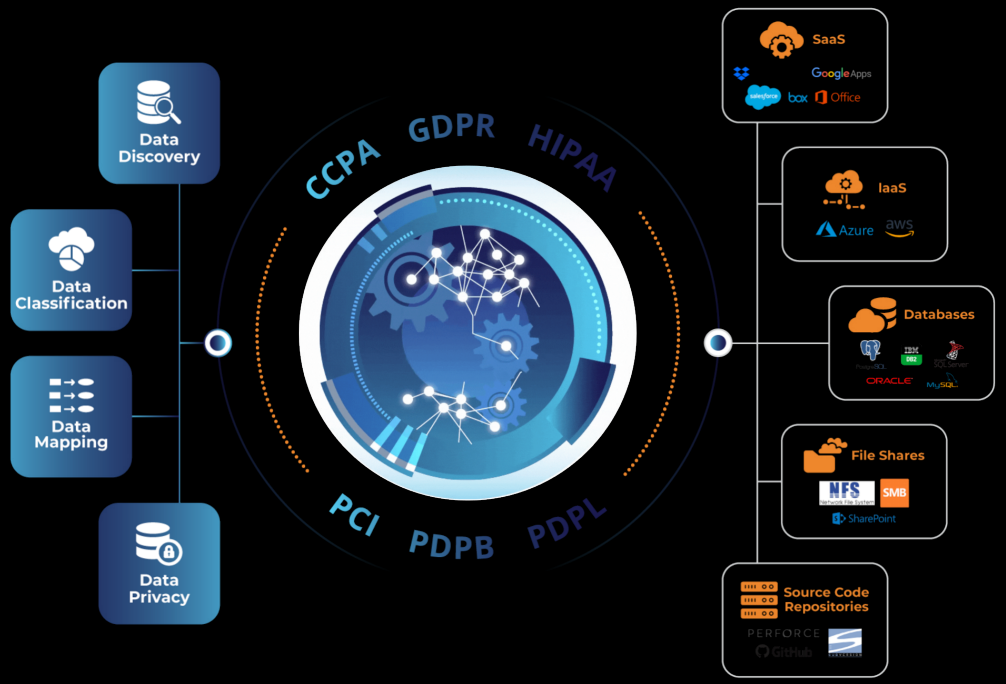
b. Complex Data Object Types

i. Unordered (non-sequenced) Data Aggregation

ii. Ordered and Sequenced Data Aggregation

02 Auto Data Identification

03 Auto Data Classification



AI Powered Data Classification Engine

CAPE incorporates a unique Auto-Classification Engine that examines every Data/Information Object in the corpuses and using GhangorCloud's patented algorithms automatically classifies it into one of the Classification Types defined in the Data Object Ontology. It can classify sensitive information as granular as specific words and phrases.

AI Powered Data Mapping Engine

CAPE incorporates a sophisticated Data Mapping Engine that automatically creates a persistent Universal Data Map (UDM) for the Data/Information Objects that exist in the enterprise corpuses. This is a crucial capability that greatly facilitates efficient navigation through large storage systems and corpuses following the 'Lineage' of any given Data/Information Object of interest.

AI Powered Automated Privacy Request Enforcement Engine

CAPE incorporates a unique fully automated Role-based (a) Data Subject Access Request - DSAR, and (b) Data Subject Request – DSR, Enforcement Engine. Using the patented AI Algorithms, the engine can automatically discretize the incoming DSAR or DSR jobs into corresponding sets of 'primitive' (or atomic) tasks. The 'primitive' tasks are then automatically 'serialized' into a Task Sequence using the Logical and Precedence Dependencies between these tasks.

CAPE incorporates an Actor Repository Map (ARM) that contains a correlation between Actors and the corresponding Repositories based upon the 'Segmentation of Duty' policies.

Key Features & Specifications

AUTO-DATA eDISCOVERY ENGINE

Data Types Supported	Structured, Semi-Structured & Un-Structured
Object Definitions Supported	Virtually any kind of data/information such as Structured, Unstructured, Semi-Structured or even Advanced Complex Data/Information Types such as Ordered / Unordered Set of Data and Data Sequences can all be '***modelled***' and, Automatically Identified and Classified by CAPE's Automated Data/Information Discovery Engine
BASIC Data Object Types	CAPE provides a default set of regular expressions and canonical classifications, used especially for PCI Compliance and PII (Personally Identifiable Information). Examples are credit card number formats, social security number formats, US zip codes, addresses, etc.
COMPLEX Data Object Types	CAPE facilitates creation of very sophisticated Complex Data Objects by combining the Canonical Data Objects through, a. Unordered (non-sequenced) Data Aggregation – this is analogous to creation of SET of Data Objects that may comprise of any number of Canonical and/or Complex Data Objects. b. Ordered and Sequenced Data Aggregation – this is analogous to creation of ORDERED and SEQUENCED combination of Canonical and/or Complex Data Objects.

AUTO-CLASSIFICATION OF DATA & CONTENT

Automated Semantic Analysis based Data Classification	Unique Intelligent Semantic Analysis based Classification system to perform Categorization & Classification without human intervention – No pre-tagging required.
Unstructured Data	Unique Security-based Semantic Analysis of Unstructured data with minimal or no human intervention required. Identify and protect Unstructured Data, such as text, memos, spreadsheets, emails, power-points, documents, images, Intellectual Property, etc. in real-time
Structured Data (Regular Expressions)	High performance Regular Expressions (Reg-Exes) matching algorithms for data such as Credit Cards, Social Security Numbers, Account No., Bar Codes, etc. – Expressions can be combined with wildcards and defined constructs
Pattern Matching & Analysis	Full support of Logical and Pattern-based occurrence analysis methodologies – Goes beyond traditional Statistical or Bayesian methods
Semi-Structured Data	Full keyword & phrase matching capabilities identify known data types
Easily Extensible	Customize and extend as new patterns and threats arise without re-deployment
Content Types Monitored and Controlled	Monitors data from databases, file systems, and desktops
Data Types/Format Monitored	Over 48+ content format decoders including Txt, MS-Word, PDF, PPT, XLS, XML, Images, Design Documents, etc.

AUTOMATIC DATA MAPPING & AUTOMATED DSR HANDLER

Universal Data Map (UDM)	Automatically creates a persistent Universal Data Map for the Data/Information objects that exist in the enterprise corpuses
Role-Based DSR/DSAR Enforcement Engine	Provides a fully automated Role-based DSR and DSAR Enforcement Engine
Actor-Repository Map (ARM)	Incorporates an Actor Repository Map (ARM) that contains a correlation between Actors and the corresponding Repositories based upon the 'Segmentation of Duty' policies
DSR and DSAR Workflow Generation – Step 1	Automatically Generates Primitive Tasks 1. Discretizes DSR/DSAR into 'Primitive Tasks' 2. Serializes 'Primitive Tasks'
DSR and DSAR Workflow Generation – Step 2	Automatically Assigns Primitive Tasks 1. Correlates UDM and ARM 2. Generates 'Segmentation of Duty (SoD)' based policies 3. Assigns 'Primitive Tasks' to Actors based on SoD
DSR and DSAR Workflow Generation – Step 3	Automatically Executes Workflow 1. Creates DSR/DSAR Workflow 2. Dispatches 'Primitive Tasks' to Actors 3. Executes Workflow

ON-PREM & CLOUD CONNECTORS

Online Storage	Amazon S3 Buckets, Dropbox, GoogleDrive, OneDrive etc.
File System	FILE, NFS, SFTP, SMB etc.
Database	DB2, MySQL, Oracle, PostgreSQL etc.
Mail	MS-Exchange, Office 365 etc.
IP and Source Code	GIT, Perforce, Subversion etc.

COMPLIANCES & REGULATIONS

Privacy Compliances	CCPA, GDPR, PDPB, PDSL etc.

DEPLOYMENT MODES

Enterprise Deployment	On Premise Enterprise Deployment
Hybrid Cloud	Hybrid Cloud based Deployment
Public Cloud	Large Scale Public Cloud based Deployment

Benefits of CAPE

Comprehensive Discovery & Insights for Enterprise Privacy, Security & Governance needs

Automated enforcement of compliance and privacy regulations

Lowest Total Cost of Ownership (TCO)

Protection against Data Breaches

Organization wide Privacy Map

Analytics for Data Subject Requests

Ease of Installation & Use

Petabyte Scale

Automated Workflows

Support for On-Prem & Cloud repositories

GhangorCloud, Inc.
2001, Gateway Place,
Ste: 710 West Tower
San Jose, CA-95110, USA.
www.GhangorCloud.com