GC | CYBERSECURITY

Compliance And Posture Enforcer (CAPE)

Version 1.0

Comprehensive Data Compliance and DSPM Platform

Compliance And Posture Enforcer (CAPE)

Version 1.0

The compliance industry's first DSPM platform based on Domain Language Modeling with Knowledge and Data Objects that dramatically reduce data risk and cost of sensitive data ownership.

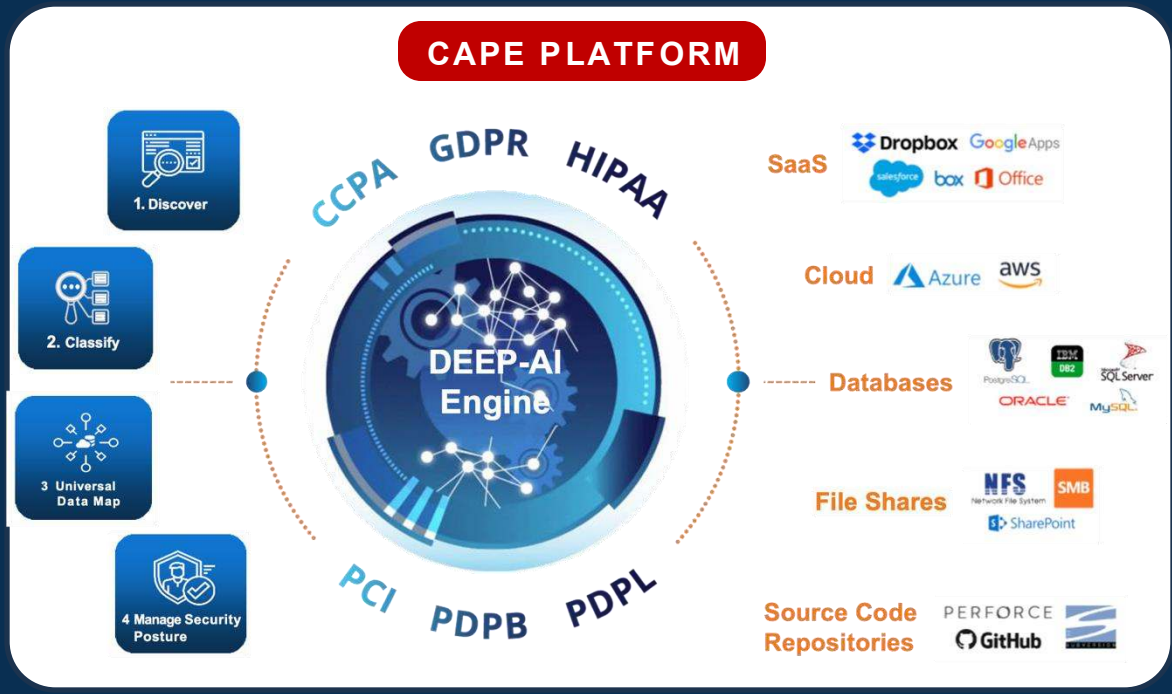
GC Cybersecurity's CAPE platform offers comprehensive Data Compliance and Data Security Posture Management (DSPM) based on Knowledge Objects and a patented Domain Language Model. Its advanced, intelligently automated features include Enterprise Data and Knowledge Discovery, Classification, Mapping, Scoring and Observability. These features, powered by a Deep-AI engine, offer the highest discovery accuracy and scale at petabyte speeds while eliminating false positives.

Deep-AI Powered Engine

CAPE boasts the industry's most sophisticated AI discovery engine specifically designed to use multiple disciplines of AI to solve the challenges, constraints and limitations of current and legacy DSPM solutions.

Differentiating Technology & Benefits

- Knowledge and data objects - comprehensiveness
- Domain language model – accuracy, low false positives
- Structured and Unstructured Data
- Any data type, or repository type, unlimited contexts
- On-prem, multi-cloud
- Basic or complex data & knowledge objects
- Ordered, unordered and sequenced data aggregations



AI-powered Auto- Discovery

CAPE employs a data and knowledge object layer to automate comprehensive discovery of known and unknown enterprise data. You cannot observe the security posture for data you don't know you have or cannot identify so our patented discovery algorithms let you discover mission-critical data, confidential and sensitive data, compliance-dependent data and even shadow or dark data.

AI-powered Auto- Classification

CAPE employs a unique Auto-Classification Engine that examines every Data, Knowledge and Information Object in repository corpuses, and using GCCybersecurity's patented algorithms - automatically classifies them into any Classification Types defined in a flexible Object Ontology. It can classify sensitive information at any number of levels - as granular as discrete words and phrases.

AI-powered Auto- Mapping

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

AI-powered Auto- Posture Scoring, Observability and Management

With comprehensive discovery, classification and mapping of a greater volume of enterprise data and corpuses, CAPE's Security Posture Scores let data security personnel score, track and manage DSPM for any single repository or across all repositories and all compliance mandates. In a single pass, personnel can now observe a comprehensive measure of risk across compliance mandates.

Key Features & Specifications

AUTO-DATA DISCOVERY 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 powerful Data Objects by combining Canonical Data Objects with: 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 & KNOWLEDGE

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

Universal Data Map (UDM)	Automatically creates a persistent Universal Data Map for the Data/Information objects that exist in the enterprise corpuses

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.

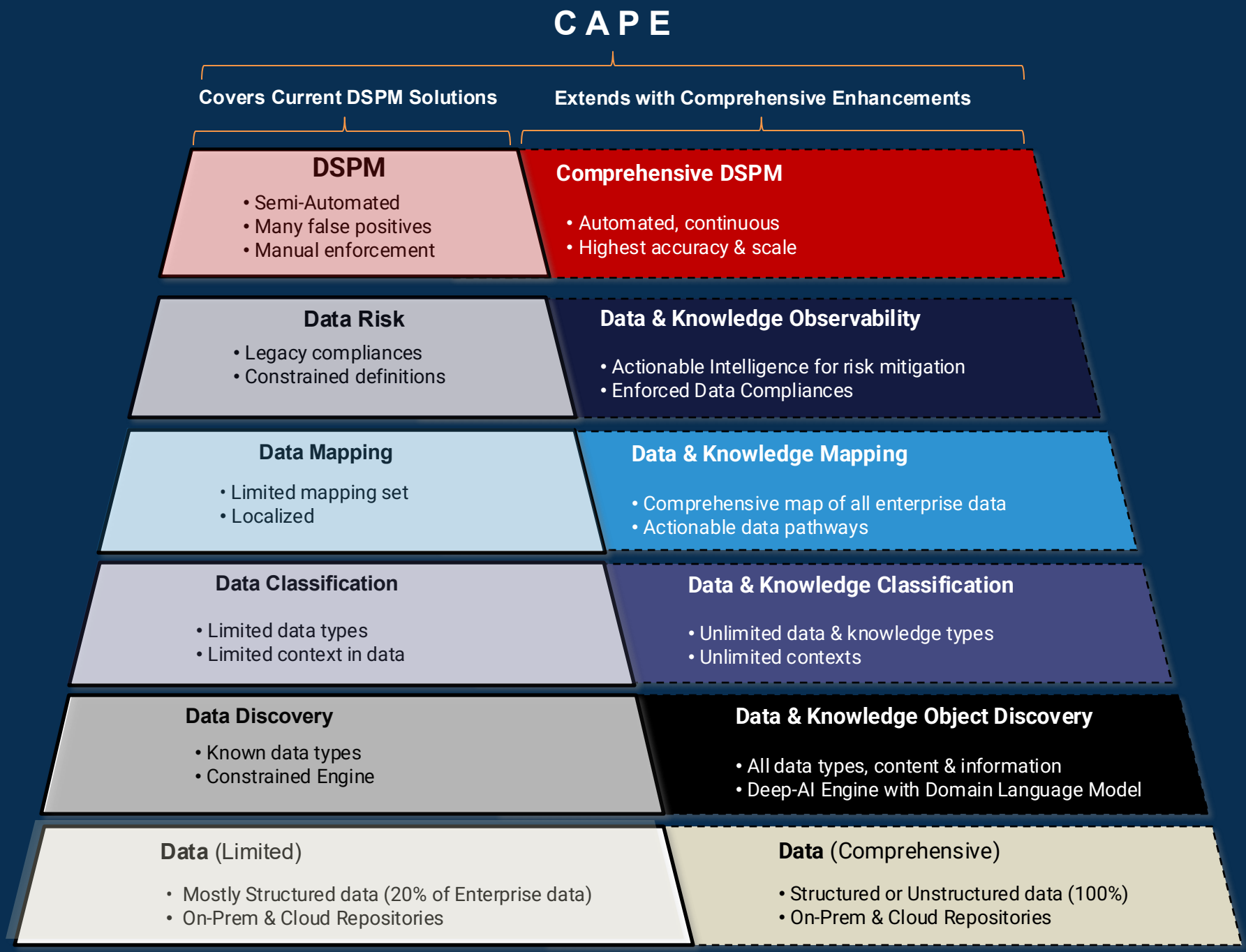
COMPLIANCES & REGULATIONS

Privacy Compliances	CCPA, GDPR, PDPB, DPDP etc.

DEPLOYMENT MODES

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

CAPE Differentiation: Comprehensive DSPM



Benefits of CAPE

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

Automated data discovery for compliance and privacy regulations

Lowest Total Cost of Ownership (TCO)

Protection against Data Breaches

Enterprise-wide Privacy Map

Repository & Data Analytics

Ease of Installation & Use

Petabyte Scale

Support for On-Prem & Cloud repositories

GC CYBERSECURITY

GC Cybersecurity, Inc.
2001, Gateway Place,
Ste: 710 West Tower

San Jose, CA-95110, USA.
www.GCCybersecurity.ai