

The Future of DLP is Automation

GhangorCloud

Increasing
Accuracy and
Control through
Automation

Multiple Stages of Automation

- *Automation* delivers speed and accuracy that is not possible with manual systems.
- *Automation* also delivers cost benefits by reducing or eliminating the time required for manual processes.



The evolution of automation for any type of system goes through multiple stages.

- The first stage is usually completely manual
- The second stage automates one or more of the functions
- The third stage automates more functions
- The fourth stage relies on strategic input and then fulfills most of the functions automatically.

Four Generations of Automation for Automobiles

4th Generation Automobiles:



→ The human makes high level decisions. The system executes automatically and informs the human.

3rd Generation Automobiles:



→ The human must make some of the decisions. The system executes some functions automatically.

2nd Generation Automobiles:



→ The human must make all the decisions. Single element to coordinate.

1st Generation Automobiles:



→ The human must make all the decisions. Multiple elements to coordinate.

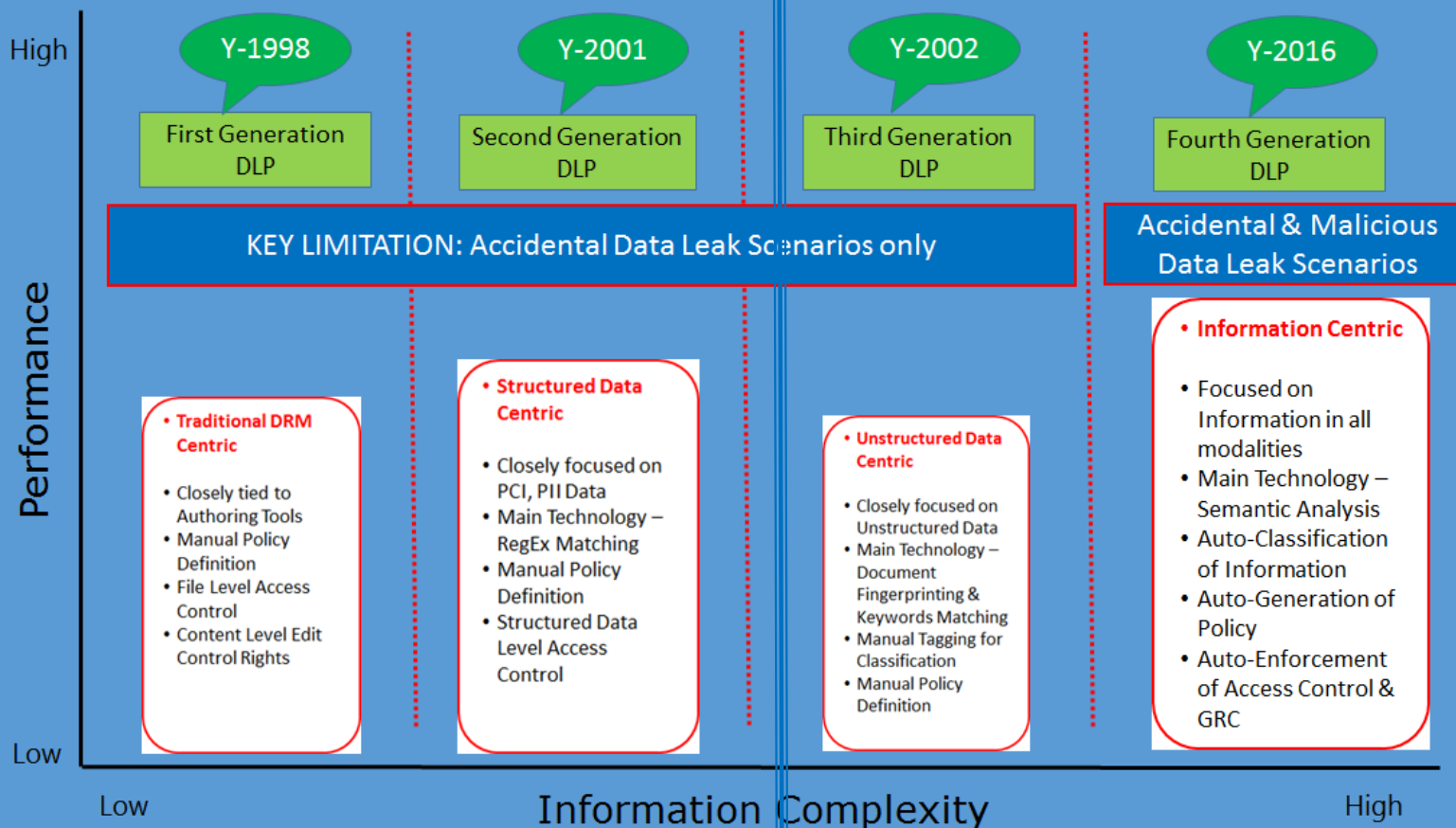
Four Generations of Evolution for DLP

First Generation DLP - DRM Centric

Manual identification and marking of all sensitive documents.

Second Generation DLP - Structured Data Centric

RegEx Matching based identification of all sensitive Data



Fourth Generation DLP - Information Centric

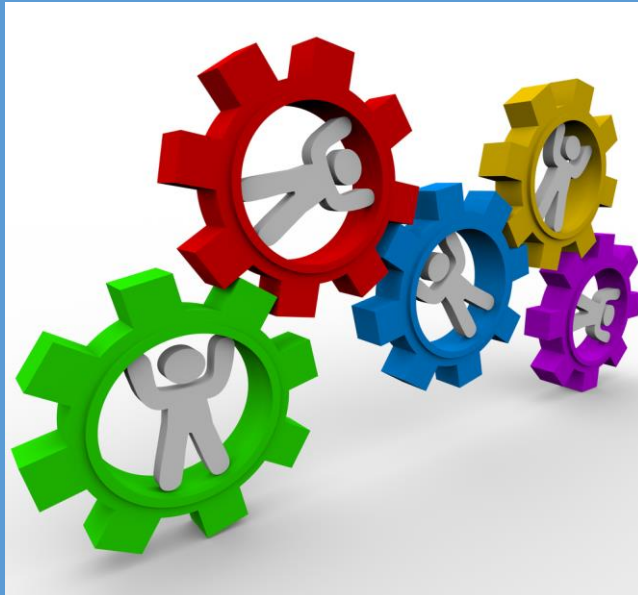
Automated identification of all sensitive data & documents. Enterprise provides initial high level specification about who has access to what. The system automatically identifies the data/information and enforces policies.

Third Generation DLP - Unstructured Data Centric

Manual Tagging, Keyword Matching, Fingerprinting based identification of all sensitive documents

4th Generation DLP Products need to...

- *Automatically* classify information
- *Automatically* classify Actors and Actions
- *Automatically* correlate multiple types of information
- *Automatically* use multiple data sources to enforce correct actions based on risk assessment



Information Security Sensitive Businesses and Security Agencies Will...

- Use multiple data sources to determine risk
- Automatically correlate information from multiple sources
- Automate actions based on correlations
- Automatically deliver real time enforcement from multiple platforms



Core Automation Technologies for 4th Generation DLP

Auto-Classification of Data & Content

4th Generation DLP system must be able to recognize and Auto-Classify confidential and/or mission critical data in any format without human intervention.

NOTE: Auto-Classification Engine must be able to perform *Automatic Data Identification*. To this effect, sophisticated data identification techniques are imperative. Simple Keyword and Lexical Matches are NOT enough as they have been proven to be error prone resulting in high False Positive rates.

Auto Classification Technology must exhibit following characteristics;

No Manual Intervention

No Manual Processing of data/content such as *Pre-Tagging* or *Pre-Marking* of data/content.

No Pre-Processing of data/content such as *Document Fingerprinting* or *Hashing* of Data/Content.

No Manual Heuristic Training The Auto-Classification process should NOT require manual heuristic training.

-
- Traditional Data Classification systems that require “Manual Input” are greatly *ineffective* as they are not only error-prone and unscalable but actually highly susceptible to Malicious Data Leak scenarios.



Core Automation Technologies for 4th Generation DLP

Auto-Generation of Policies

4th Generation DLP system must be able to Automatically Generate comprehensive set of Policies for enforcement of data leak prevention based on Role-based Content Access Control.

NOTE: DLP Policy definition is the single most critical process for successful deployment of a DLP regime. DLP Policies are inherently more complex and require deeper understanding of sophisticated use case scenarios in order to ascertain acceptable level of “Completeness” and “Use Case Coverage”.

Auto Policy Generation Technology must exhibit following characteristics;

No Manual Intervention in the Policy Generation process. All relevant *Policy Primitives* should be automatically generated thus eliminating human error and inconsistency.



No Post-Processing such as *Manual Policy Embossing* of Data/Content.

No Manual Heuristic Training of the Policy Parameters to perform Incident Correlation.

-
- Traditional DLP systems are typically limited to manual policy creation process which is not only tedious but also error prone and costly.

Core Automation Technologies for 4th Generation DLP

Auto-Access Control

4th Generation DLP system must be able to Automatically Generate comprehensive set of Access Control Primitives.

NOTE: Traditional DLP systems are either dependent on extensive manual enumeration of Access Control Primitives or rely heavily on the Policy definition process – both of the two approaches is extremely cumbersome and constrained in its ability to provide the requisite coverage of “Use Case Scenarios” in sophisticated real-life DLP deployments.

Auto Advanced Access Control Technology must exhibit following characteristics;

Identity and Role driven Access Control wherein access rights and corresponding violations are automatically deduced from the identity and functional role of an actor (i.e. employee, application or device).

Contextual-Conceptual Correlation algorithms to perform sophisticated reasoning (i.e. who should have access to what type of information?) for detection and pre-emption of complex data leak scenarios.



Core Automation Technologies for 4th Generation DLP

Auto-GRC Enforcement

4th Generation DLP system must be able to Automatically Enforce Governance & Regulatory Compliance .

NOTE: Traditional GRC Systems are typically focused on document routing and workflow. They are either dependent on third party data security tools or rely heavily on the Standard Operating Procedures – both of the two approaches is extremely cumbersome and constrained in its ability to provide the requisite coverage of “Use Case Scenarios” in sophisticated real-life DLP deployments.

Auto GRC Enforcement Technology must exhibit following characteristics;

Segmentation of Duty (SoD) based Information Control

wherein dissemination, exposure and routing of data/information is automatically controlled according to pre-defined Business Standard Operating Procedures.

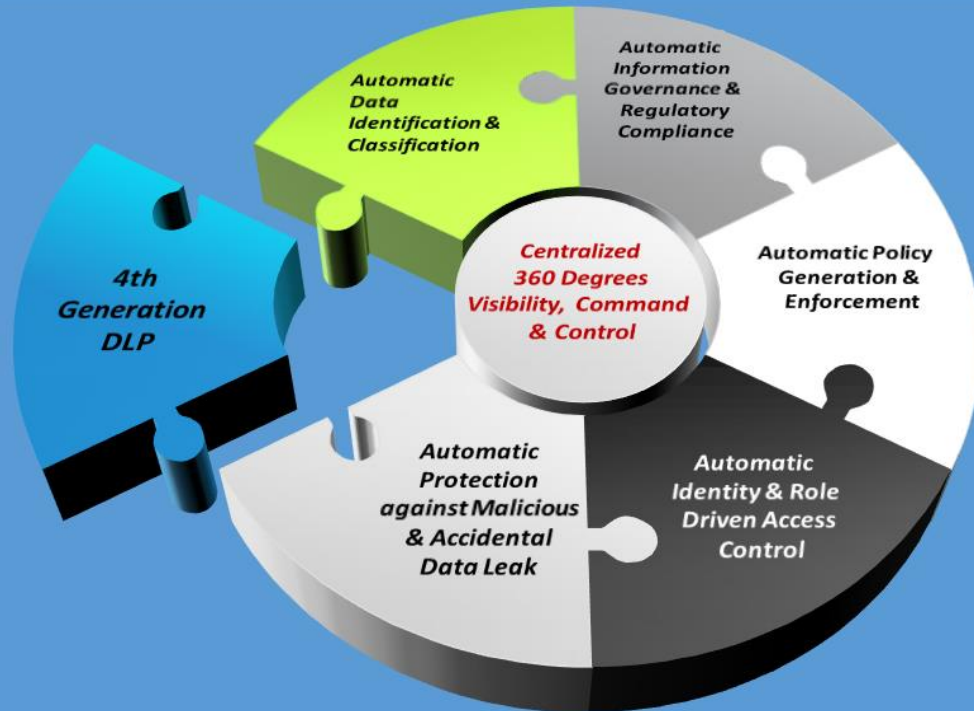
Regulatory Compliance Enforcement wherein all domain specific compliance guidelines are automatically enacted.



GhangorCloud Technologies for Automated Security



GhangorCloud *Key Solution Features*



GhangorCloud Delivers 4th Generation Automated DLP for Your Organization

- Auto-classification of Information
- Auto-classification of Actor Risk Posture
- Multi-variable Correlation – Actors-Information- Operations
- Auto-synthesis of Policy
- Centralized Command Control Collaboration & Intelligence

4th Gen DLP for Enforcement

- Industry's most advanced
- No Manual Tagging
- No Pre-processing of Data

Auto Classification

- Auto Identification of Data
- Auto Classification of Data

Identity & Role Driven Solution

- Industry's First
- Protects Data from Malicious or Accidental Leaks

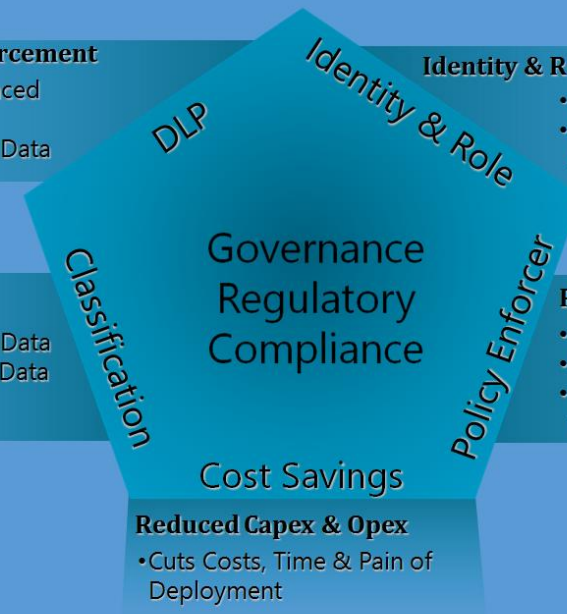
Policy Automation

- Most advanced Policy engine
- Automatically generates policies
- Dramatically reduces deployment time

Cost Savings

Reduced Capex & Opex

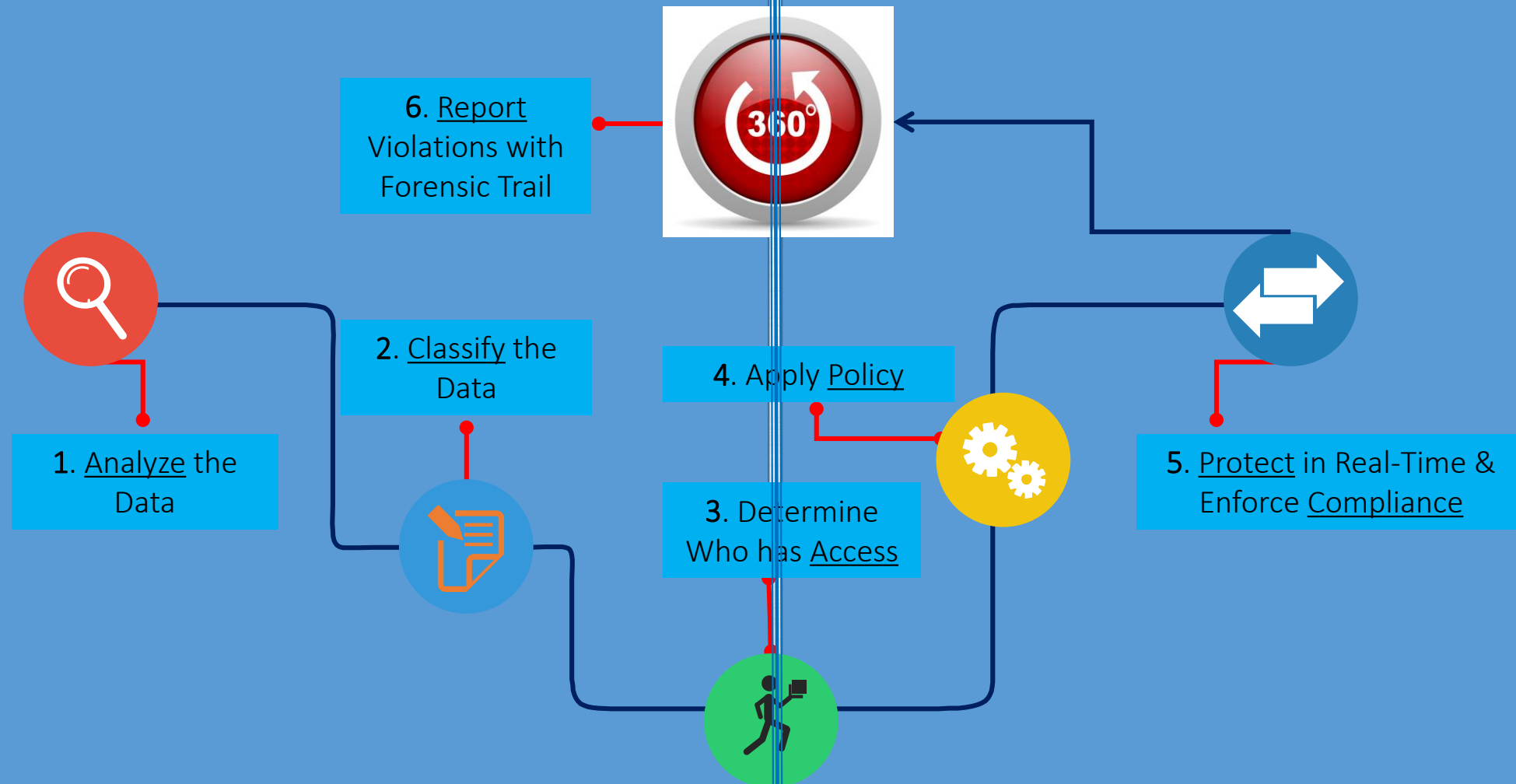
- Cuts Costs, Time & Pain of Deployment



GhangorCloud's 4th Generation DLP Product

GhangorCloud *How Does It Work?*

Automated & in Real-time



Let us show you how
4th Generation Data Leak Prevention
can secure your sensitive data.



GhangorCloud

Contact:

GhangorCloud
2001 Gateway Place
Suite 710, West Tower
San Jose, CA 95110
+1 408-713-3303
info@ghangorCloud.com