

FROM DISCOVERY TO DEFENSE AT MACHINE SPEED

Why keeping discovery, policy, ownership, decisions, and protection in one governance plane is critical in the age of AI.

AI is compressing the time between exposure and exploitation. Security and governance teams cannot afford to discover risk in one tool, search for policy in another, locate the right owners manually, and then begin a separate protection process.

Speed Is Now a Governance Requirement

AI-enabled attacks are increasing the speed and automation of real breaches. That changes the value of governance. Finding sensitive data is essential, but discovery by itself does not protect anything. The advantage comes from reducing the time required to understand the exposure, determine what policy applies, identify who must make the decision, and execute the protection.

ASSESS	PLAN	REACT	EXECUTE
What is exposed?	What should happen?	Who must act?	How is it protected?
Scanner and catalog results identify sensitive data, impacted assets, classifications and concentration of risk.	Policies, ownership, stewardship, business context and impact are available together to determine the right response.	Security, privacy, data owners, governance and application stakeholders can work from the same governed context.	Connected workflows and APIs can carry the decision into protection, with the outcome retained as governance evidence.

Why Fragmented Governance Slows the Response

Fragmented approach	IDMC / CDGC governance context	Speed advantage
Results live in a scan report.	Discovery results become governed catalog context alongside classifications, relationships and asset details.	Teams begin with shared facts instead of reconciling separate reports.
Policies are stored elsewhere.	Policies and governed assets can be related directly to the data they affect.	The applicable control is visible when the exposure is being evaluated.
Owners are found manually.	Stakeholders, owners and governed responsibilities are associated with assets and workflows.	The right people can be engaged without rebuilding the contact chain.
Protection is a separate project.	IDMC services, workflows and APIs can connect governance decisions to downstream action.	The path from decision to execution is shorter and more repeatable.

The Objective

Keep the evidence, business context, policy, people, decision, and protection path together so the organization can move from exposure to action at the speed the risk demands.

IDMC as the Governance Plane: From Finding Risk to Closing It

Informatica Cloud Data Governance and Catalog (CDGC) brings discovery, classification, business context, stakeholder and policy management, dashboards, lineage and governance workflows into the IDMC platform. ASP delivers its Intelligent File Scanner and Test Data Management solutions into that same governance context so the organization does not have to break the protection process across disconnected tools.

1	2	3	4	5	6
DISCOVER	CLASSIFY	CONTEXT	DECIDE	PROTECT	PROVE
Sensitive data	What it is	Policy + owner	Required action	Execute control	Show enforcement

Why ASP Delivers the Solutions in the Same Place

ASP INTELLIGENT FILE SCANNER

Extends content-level discovery into enterprise files and repositories, publishes classifications into CDGC, and supports dashboards that connect discovered sensitive data to the policies it impacts.

ASP TEST DATA MANAGEMENT

Uses governed classifications and masking rules to automate protection of sensitive non-production data, with CDGC attributes and application/global dashboards providing evidence that security policy is enforced.

The Combined Operating Model

- **ASSESS:** ASP File Scanner identifies exposed sensitive information across enterprise files and publishes classification context into CDGC.
- **PLAN:** CDGC brings the classifications together with business context, affected policies, asset relationships, ownership and stakeholder information.
- **REACT:** Security, privacy, governance and application teams can evaluate the same governed evidence and determine the required control.
- **EXECUTE:** ASP TDM can use classification/rule assignment and masking APIs to apply protection to non-production data rather than leaving the decision as a manual follow-up.
- **PROVE:** CDGC custom attributes and ASP dashboards can show where masking rules are assigned, application/global progress, and the enforcement of security policy.

The Strategic Advantage

The value is not simply having more features in one platform. It is eliminating the handoffs that consume time between knowing there is a problem and actually protecting the data.

In the age of AI, the winning metric is time-to-protection. Keeping discovery, policy, ownership, decision context, automation and evidence together in IDMC gives organizations a shorter, more defensible path from exposure to control.

Sources

Informatica - Cloud Data Governance and Catalog data sheet: discovery, classification, stakeholder and policy management

Informatica - Cloud Data Governance and Catalog Data Stewardship & Curation, April 2026

Informatica - CDGC workflows: stakeholder involvement, policy assets, risk mitigation and auditing

Informatica - What's New in Data Governance and Catalog, April 2026: dashboards and workflow enhancements

IBM - Cost of a Data Breach 2026: AI-enabled breach findings

ASP capability statements reflect current ASP Intelligent File Scanner and Test Data Management positioning as of September 2026.