

# Discovering Dark Data

The Elusive Security & Privacy Risk in the Cloud

With multi-cloud frameworks commonplace, organizations can now create, store and manage enormous volumes of data in the cloud.

Despite the growing trend, businesses often have little to no visibility into the data, residing in these clouds.



Organizations rely on multi-cloud environments

## The Culprit | Dark Data

The massive volume of unstructured, untapped, and ungoverned data, residing in organizations' multi-cloud environments but never used or analyzed.

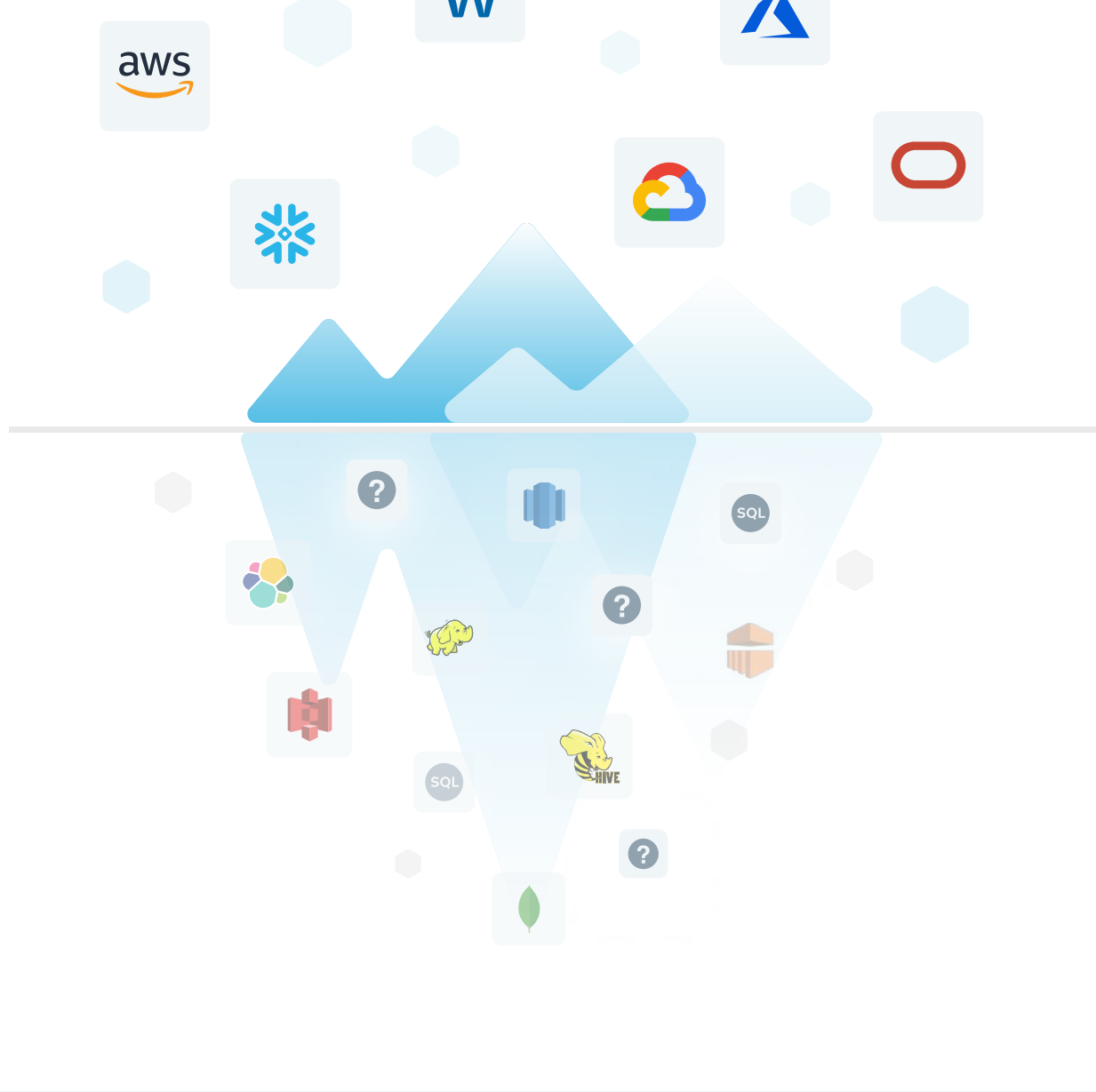
### Top Dark Data Security & Privacy Risks

- Single-platform cloud inventory tools fail to discover and detect Dark Data outside their own environment.
- Due to the exploding volume of unstructured data systems, a lot of Dark Data goes under the radar.
- Lack of visibility into the sensitive data makes it difficult to monitor & remediate security posture.
- Unmanaged and unmapped data increase the chances of non-compliance with privacy obligations.
- Lack of security control and governance frameworks further leads to non-compliance with global data regulations.

## Six Critical Steps to Stamping Out Dark Data

### 1 Data Discovery

Detect shadow and native data assets, residing across the multi-cloud, and extract them into an asset catalog with mapping/tagging of the data inside each system.



### 2 Risk Detection

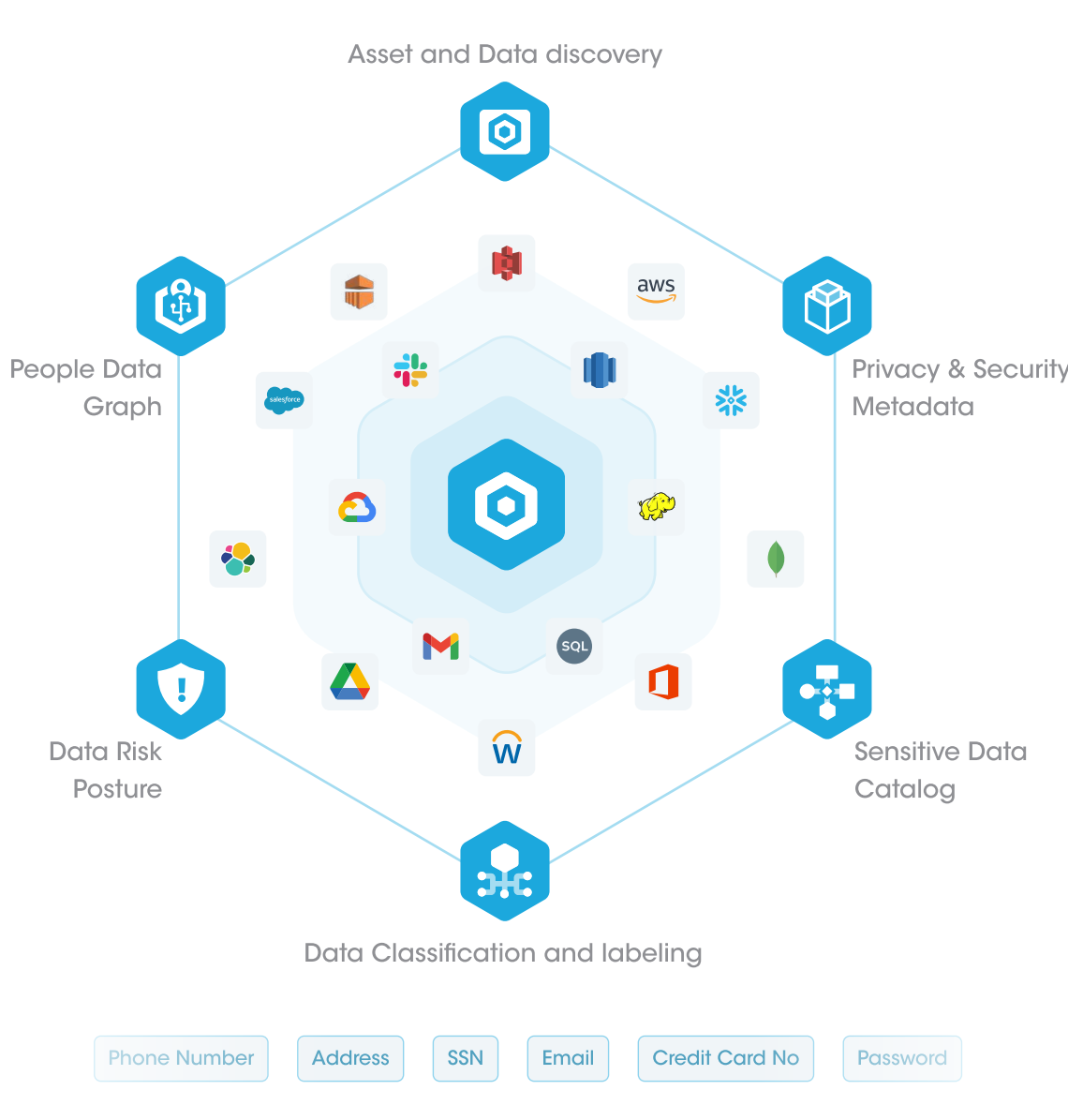
Discover security posture and compliance risks associated with dark data assets, and remediate exposures.

Restrict and Encrypt all PD on Oracle Cloud with 'Very High Risk'

SECURITY	RISK	RESTRICT	ENCRYPT
Email	Moderate	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card	Very High	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SSN	Very High	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

### 3 Sensitive Data Intelligence

Visualize the sensitive data elements across structured and unstructured systems to populate metadata.



### 4 Access Governance

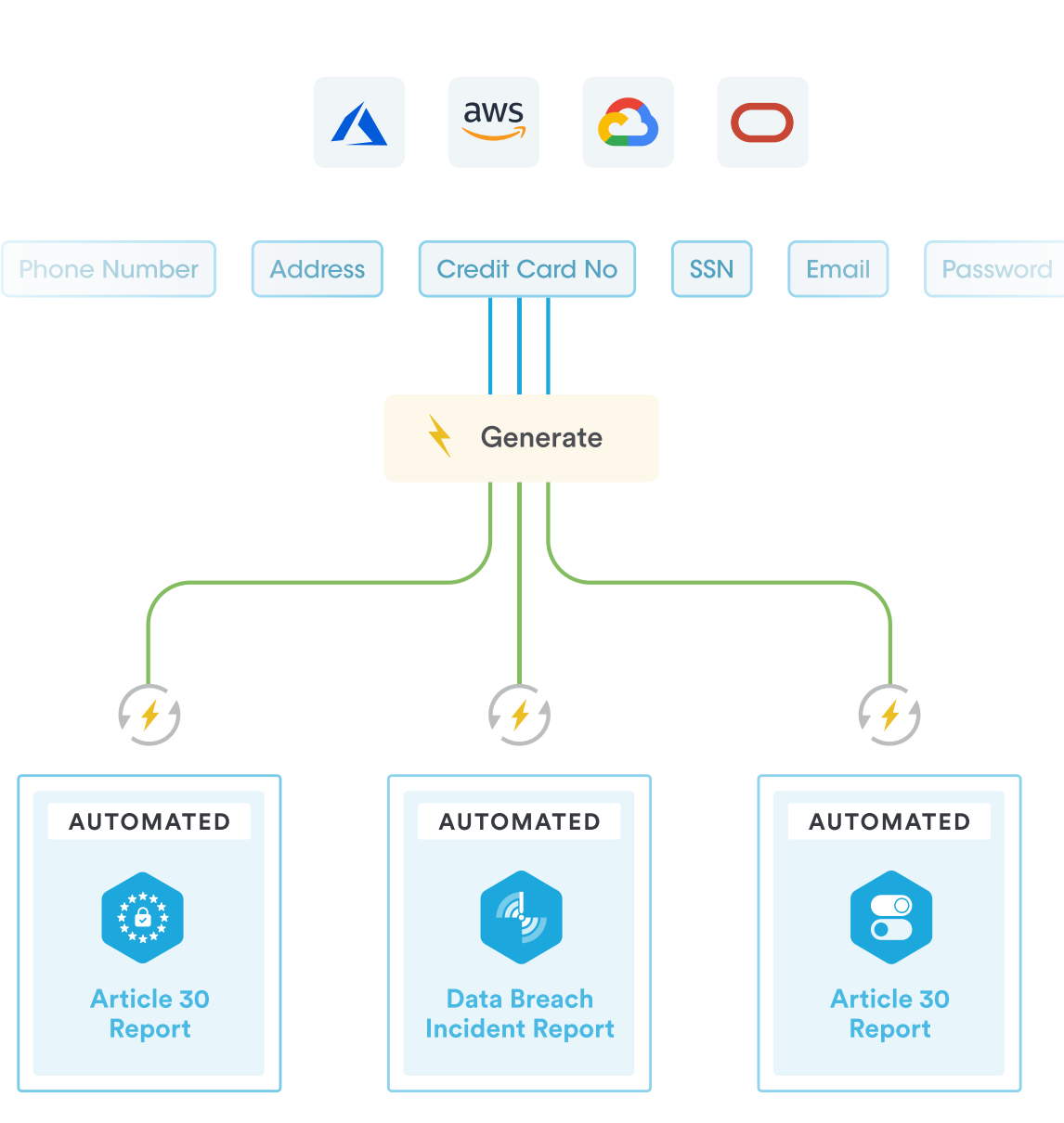
Map discovered personal data and its owners to understand security risks and define appropriate access controls.

Access Controls for Oracle Cloud

TABLE	RISK	ACCESS
Sales_Data	Moderate	
Customer_Data	Very High	Blocked
Transaction_Data	Very High	Blocked
Employee_Data	Moderate	

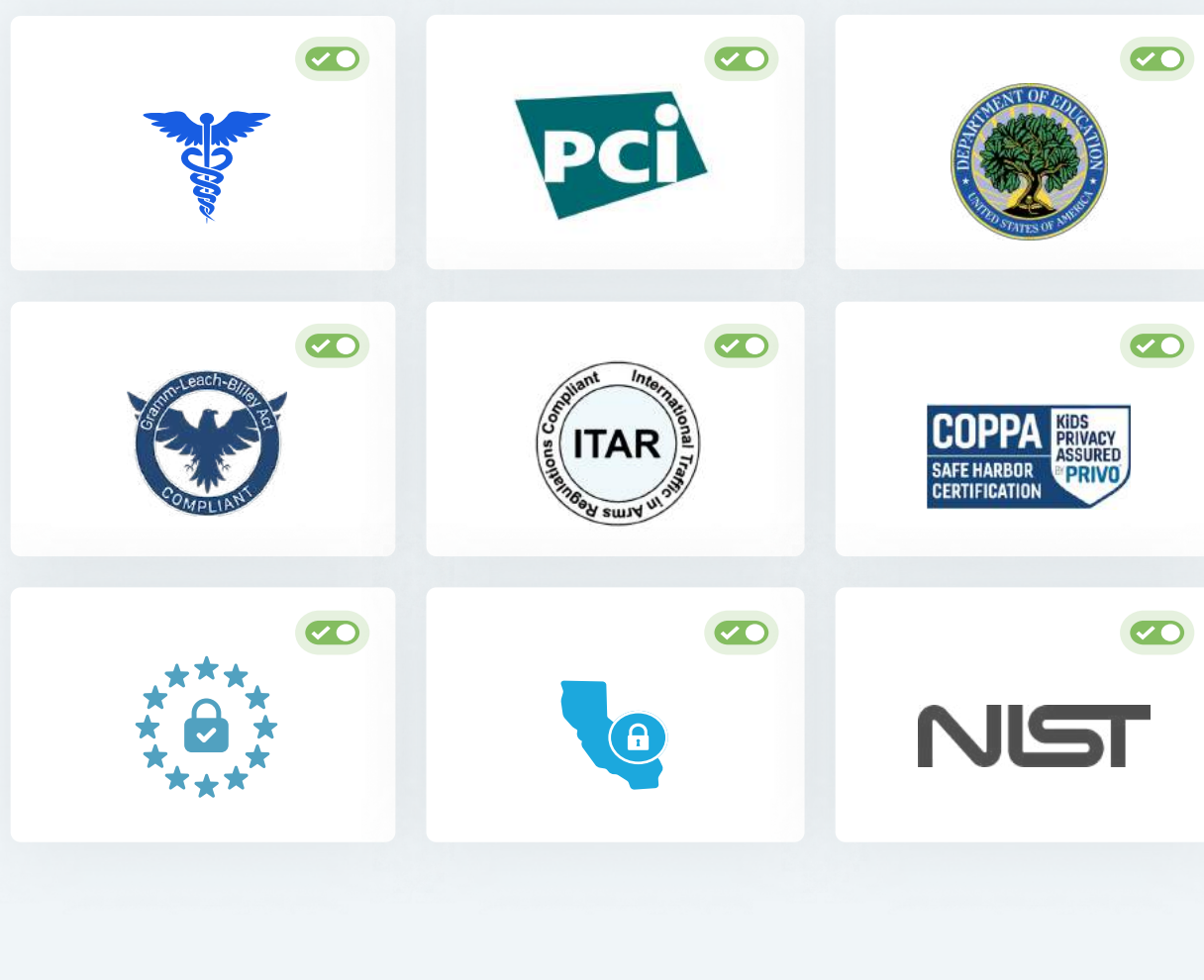
### 5 Privacy Obligations

Use personal data mapping to fulfill data subject requests (DSRs), breach notifications, and consent reports.



### 6 Regulatory Compliance

Automate processes and workflows to comply with global privacy laws and industry-specific mandates.



Make no mistake, shedding light on dark data can help your organization adopt a more enlightened approach to **security, privacy, and governance.**



[Request a Demo](#)

- WINNER** "Most Innovative Startup" RSAC 2020
- Forrester Wave **LEADER** in Privacy Management
- WINNER** "HPE-IAPP Innovation Award" 2020
- WINNER** "Most Innovative" Frost & Sullivan
- FORBES** Top 10 Most Promising Cyber Security Companies