

onetrust

Discovering and De-risking Sensitive Data

Phil Donaus, Solutions Engineer, OneTrust

September 19, 2023

Agenda

- 01.** How things have changed with regard to data and security
- 02.** Cross-functional challenges & initiatives
- 03.** Steps to protect

Today's data landscape

The attack surface continues to expand

How to control risk and enable the business?

- Data is a valuable asset, which means bad actors are trying to steal it
- The cloud and decentralization of IT means that data may live in dozens of different places
- New privacy and data security regulations are introduced on a near-monthly basis
- Data footprint has exploded with a rise in redundant, duplicate and siloed data
- Persistent, overwhelming threat to the brand



The way of doing business with data is evolving



Visibility and validation
are critical to solve
challenges

Does this feel familiar? Similar initiatives carried out in silos

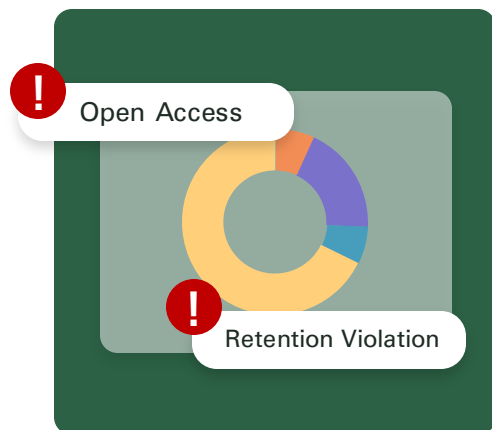


Lack of visibility means wasted effort and inefficiencies, duplicate data, and security challenges in managing that data

Visibility and validation solve for these challenges

Security

Identify and de-risk sensitive data, monitor controls and risk



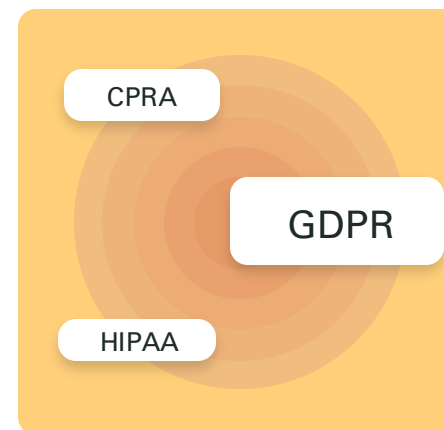
IT

Ensure resources are properly utilized



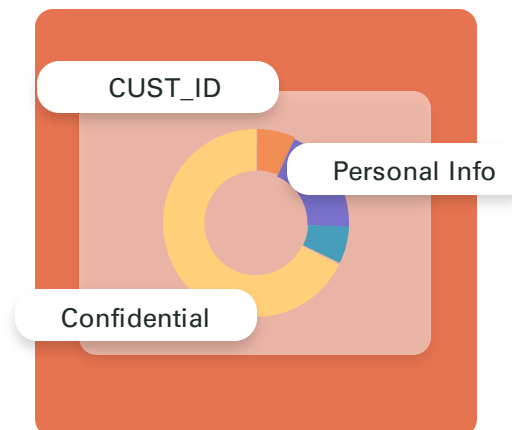
Privacy

Comply with global privacy laws



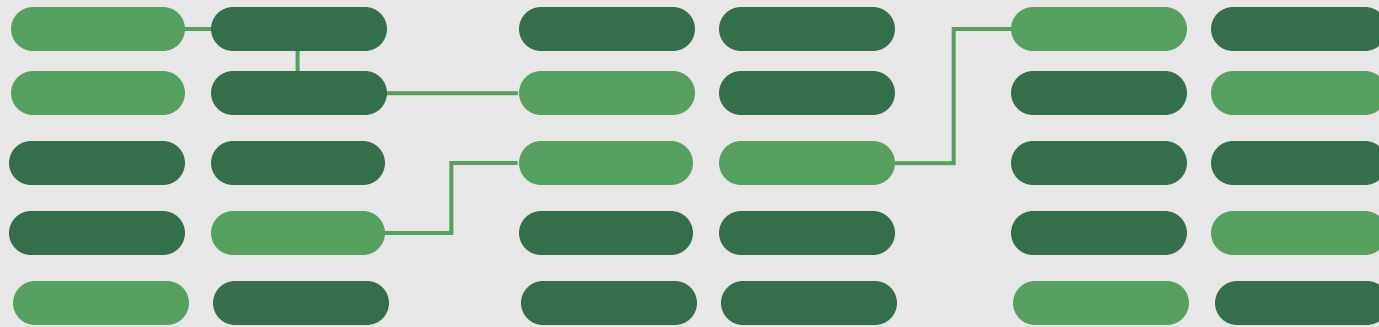
Data Governance

Enrich data catalogs & streamline stewardship



Visibility reduces risk and improves efficiencies

Centralized architecture to understand the what, why, where and how across Data Governance, Privacy and InfoSec



Focused automation provides intelligence, controls drift and enables fact-based decisions

What can I do to get started?

Visibility and control are needed to reduce data risk



Discover

Intelligently discover and classify sensitive data to gain central visibility into data risk



Control

Effectively protect & govern sensitive data through automated policy orchestration & remediation actions



Enable

Enable privacy, data, and business teams to automate compliance activities and use data responsibly

Some key questions to think about

What data do I have?

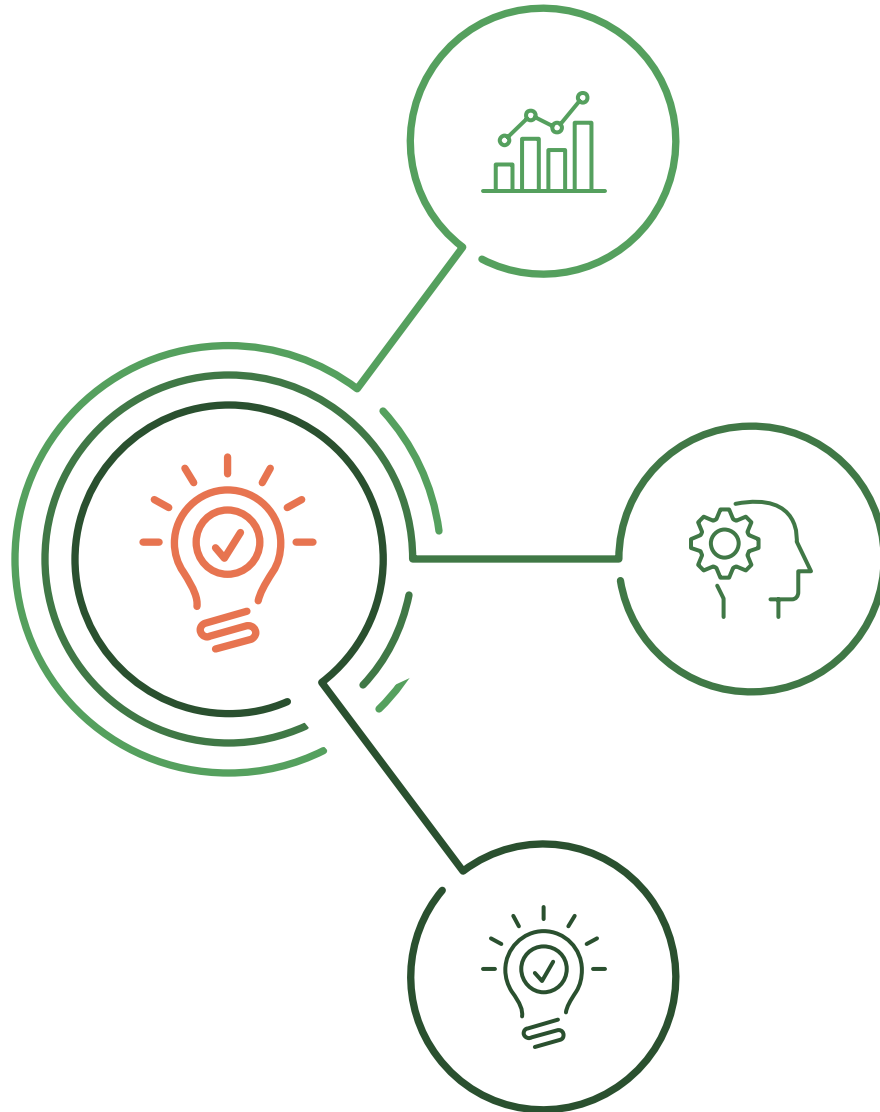
Where is it?

What is the purpose for having the data?

How effective are my data controls and policies

What is the most impactful fix?

What should you prioritize to reduce risk?



1. Locate and inventory sensitive data

What sources contain my most high-risk data?

Do I have sensitive data stored in systems outside of governance policy?

2. Automate remediation

What processes and policies do I need to use to reduce risk?

Automatically apply and enforce them at scale across all of your data

3. Report progress & risks to stakeholders

Communicate risk reduction and process improvements to the business

Examples of processes and how to implement them

Technical control validation

Detect at risk data



Initiate controls like encryption, masking, access



Retention orchestration

Document retention schedules



Enforce deletion in downstream systems



Data usage requests

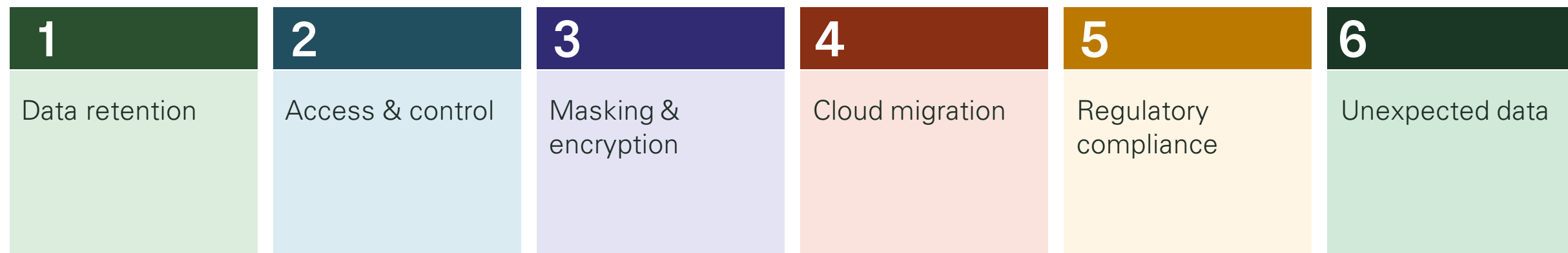
Enable customers and employees to make requests



Take action in downstream systems



What other activities and governance processes does automation and discovery help implement?



Visit onetrust.com

Email me: pdonaus@onetrust.com

All Resources: onetrust.com/resources/

Request a Demo: onetrust.com/request-demo/

onetrust