LightBeam.ai

Data Privacy Automation for the ZenDesk Application

Reference Architecture

Table of Contents

Executive Summary

The key to meeting the requirements of today's privacy regulations and protecting personal information (PI) from unauthorized use and disclosure lies in understanding and managing the use of personal information within an organization's data environment. Spread across a multitude of repositories and application data sets, PI use can be difficult to manage through written policy alone.

We at LightBeam.ai believe the best way to implement policy across an organization is to supplement written policy with technical controls designed for specific applications and functions. By working with our clients we have developed several applications and function-specific controls focusing on discovering, analyzing, and enforcing control over the use of personal information within popular applications.

Zendesk is a company that provides software-as-a-service products related to customer support, sales, and other customer communications. Using service tickets to interact with customers, Zendesk tracks lots of information about service requesters and stores it long-term as part of the service record. Guided by the privacy principle to only keep PI for as long as is needed, LightBeam.ai has developed controls specific for how Zendesk uses and stores personal information.

Our AI-driven platform engine LightBeam Spectra can easily be configured to review all service tickets to automatically discover, analyze, and enforce privacy policies regarding sensitive information stored in service tickets. By finding and redacting PI in tickets that have been closed, organizations can reduce privacy risk and meet retention requirements for data that is no longer needed. By then automating the execution of these control policies, Privacy Officers can develop custom rule sets that continually scan, monitor, and control how PI is used and controlled within Zendesk. The details of how this happens are discussed below.

Audience

This document is intended for organizations that have implemented Zendesk and whose processing with Zendesk uses personal information. It is meant for both technical and non-technical audiences. Privacy Officers, CISOs/Security Architects, and Support leaders within organizations using Zendesk will find this reference architecture useful in automating data privacy controls.

Purpose

This document provides greater details on the problem of processing personal information within Zendesk and how LightBeam can be used to manage the use of PI and reduce the risk posed by long-term storage of PI.

Zendesk Overview

Zendesk is an award-winning customer service software platform in use by 200K+ customers. A leader in customer relationship management (CRM), the Zendesk platform gathers customer information from multiple sources and creates interaction tickets, centrally storing tickets as the service is in progress. A workflow engine allows for the creation of custom workflows for various business processes exposing the information to anyone that has access. Zendesk supports multiple channel inputs and can receive contact via Email; Social media like Facebook; or social messaging like WhatsApp, WeChat, Twitter Direct, etc. creating support tickets from multiple sources across the organization.

Used across a multitude of business types, Zendesk supports many different process types. Many customer interactions require the use of PI and the type of PI will vary by process type. Common fields like Name, Address, and Phone may be stored in structured fields while other information like credit card information for one-time use can be captured and stored in open text fields. Long-term storage of

PI in closed tickets creates a risk that should be addressed to support the key privacy principle of minimum necessary.

LightBeam Data Privacy Automation Platform

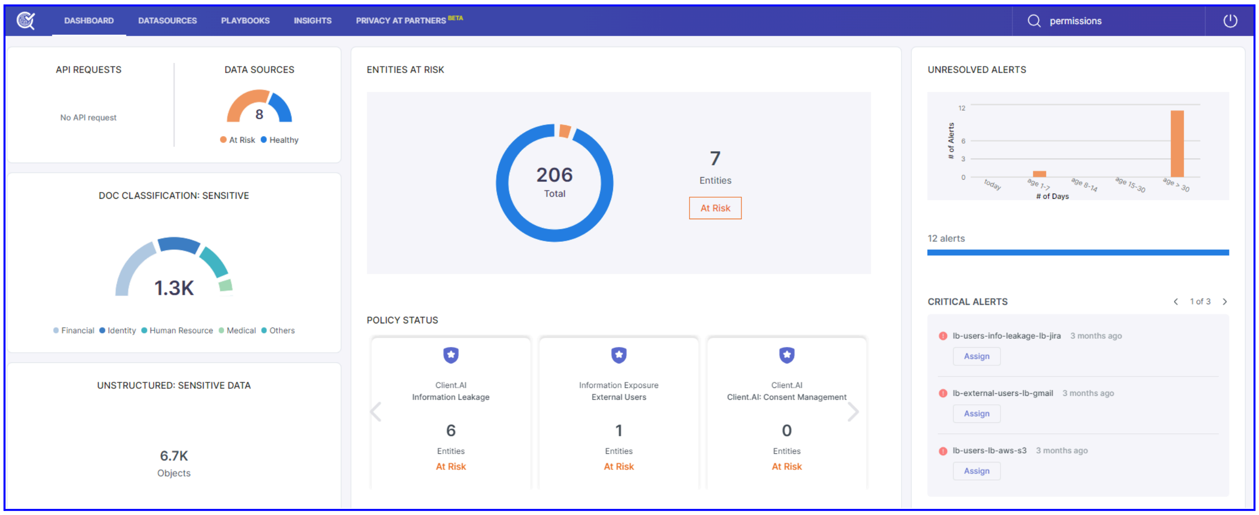
A pioneer in the data privacy automation (DPA) category, LightBeam is on a mission to empower organizations to manage and access their sensitive data securely. Leveraging its identity-centric discovery & classification engine, Spectra, LightBeam ties data cataloging, access, and sharing into a unified privacy control platform.

LightBeam empowers privacy and compliance executives to keep their organizations under continuous compliance for GDPR, CCPA, HIPAA, and PCI-DSS among others, while information security executives can finally rest assured that sensitive data is being used, accessed, and stored securely.

LightBeam's 360 view of the data environment provides an up-to-date accurate dashboard of data sources, data attributes, Entities (identities), control policies, and permission lists. The following is a quick look at how LightBeam brings an unparalleled view of the PI and SPI that an organization carries within a myriad of data repositories.

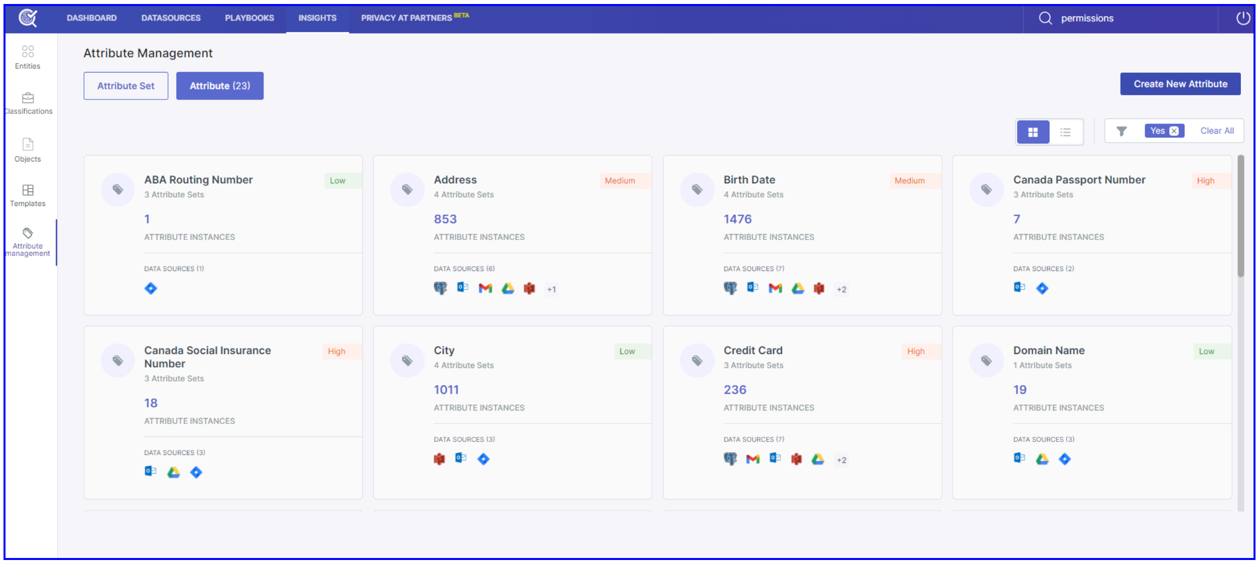
Main Dashboard

The main dashboard provides a high-level view of all data sources where sensitive data is present, the entities (customers/employees/patients et al) whose sensitive data is being carried, and any alerts that might need attention.



Attribute View

LightBeam has over 200 pre-configured sensitive attributes (sometimes called fields/columns) in its system and is capable of recognizing their identifiers (sometimes called Values) from all the data sources; moreover, users can also add their own attributes to the system and make it learn from various sources.
These attributes have 3 sensitivity levels based on their weight in the system i.e. High, medium & low
Examples of attributes are US Social Security Number, Loan Account Number, Medical Record Number, and so on.



Attribute Management

ABA Routing Number — Low
3 Attribute Sets
1
ATTRIBUTE INSTANCES
DATA SOURCES (1)

Address — Medium
4 Attribute Sets
853
ATTRIBUTE INSTANCES
DATA SOURCES (6)
+1

Birth Date — Medium
4 Attribute Sets
1476
ATTRIBUTE INSTANCES
DATA SOURCES (7)
+2

Canada Passport Number — High
3 Attribute Sets
7
ATTRIBUTE INSTANCES
DATA SOURCES (2)

Canada Social Insurance Number — High
3 Attribute Sets
18
ATTRIBUTE INSTANCES
DATA SOURCES (3)

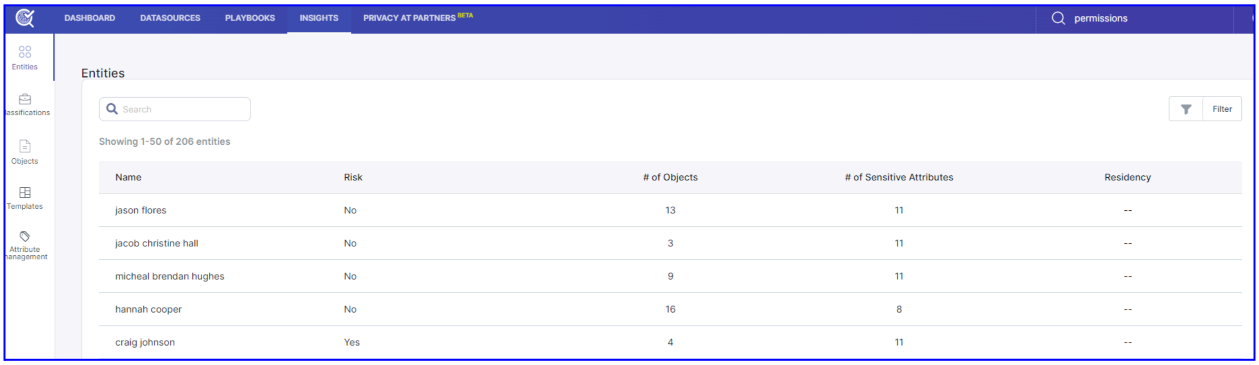
City — Low
4 Attribute Sets
1011
ATTRIBUTE INSTANCES
DATA SOURCES (3)

Credit Card — High
3 Attribute Sets
236
ATTRIBUTE INSTANCES
DATA SOURCES (7)
+2

Domain Name — Low
1 Attribute Sets
19
ATTRIBUTE INSTANCES
DATA SOURCES (3)

Entity View

Centered on the individual, the entity view provides a precise breakdown of what data is being held for any individual, in what data sources, and if there are any known associated risks. This view supports GDPR, CCPA, and other individual rights requests.



Entities

Showing 1-50 of 206 entities

Name	Risk	# of Objects	# of Sensitive Attributes	Residency
jason flores	No	13	11	--
jacob christine hall	No	3	11	--
micheal brendan hughes	No	9	11	--
hannah cooper	No	16	8	--
craig johnson	Yes	4	11	--

LightBeam Operational Phases

LightBeam's Spectra DPA platform employs a three-phase approach to managing privacy risk. These phases include Detect, Enforce, and Automate. Each of these phases builds on the previous phase to create a fully automated privacy management system that can;

1. Understand the existence and use of PI
2. Create control policies with resulting actions.
3. Create automated tasks to execute control policies.

Detect

The initial LightBeam deployment step is to gain an understanding of the data environment. This includes connecting to applications and repositories to discover sensitive data elements called "attributes." Attributes are contained in applications and repositories and are duplicated across the environment based on the relevant business processes. LightBeam uses API connections to analyze structured and unstructured repositories and identify the data attributes, attribute types, the related sensitivity levels. Then, an Entity is resolved from the data related to an identified individual or "entity".

By understanding which data exists in the environment, LightBeam learns which data is important to an organization and its business processes. With this understanding as a foundation, LightBeam is able to then set policies as to how that data is stored, shared, and viewed.

During the detect phase, LightBeam natively recognizes and classifies;

- 200+ common attributes including the common identifiers from a variety of countries.
- Industry attribute type sets like (Financial, Healthcare, Identity…)

- Unlimited client-specific attributes - every LightBeam customer is unique and may carry sensitive data that is unique to them. LightBeam enables customers to add custom attributes. (e.g. Customer account number, employee number, member numbers, SKUs, and other values)
- Document classification of type and sensitivity of data contained in attachments in a service ticket.
- Sensitive attributes detected across multiple data repositories are linked using a machine learning algorithm to see if they belong to a single entity. The cross-linking of fragments of information to a central identity is a unique capability that helps customers understand not only if sensitive data is at risk but more importantly, whose data it is that might be at risk.
- The DETECT phase helps create data maps, RoPA reports, and a 360-degree view of all information that's present about customers within an organization's systems.

Enforce

The enforce phase is used to establish the rules for data usage. There are four primary control components in the enforce phase. These include Policies, Permissions, Alerts, and Redaction.

Policies

LightBeam Policies are configured to track both internal and external data sources. Each policy may contain multiple rule sets that define the search criteria and details about the data including; attribute sets and types, data sources, alert level settings, and the associated relevant regulations, and are configured via a query selection screen.

Policies include;

- Types of policies. Policy types include Internal, External, and Leakage.
- The contact information for whom an alert should be sent.
- The setting of permissions list for whitelisting if approved data sources.

Permissions

- Permission lists (also sometimes referred to as Permit Lists) establish and maintain an inventory of approved repositories and uses of PI
    - Approved repositories are added to a permission list and used to compare new scan results.
    - Alerts can be raised when a new instance is not found on a permission list.
    - Workflows are initiated by an alert to approve new instances and update the permission list so future findings will not raise an alert.

Alerts

Alerts are used to notify system owners and others that a policy has been violated and that action may be needed.

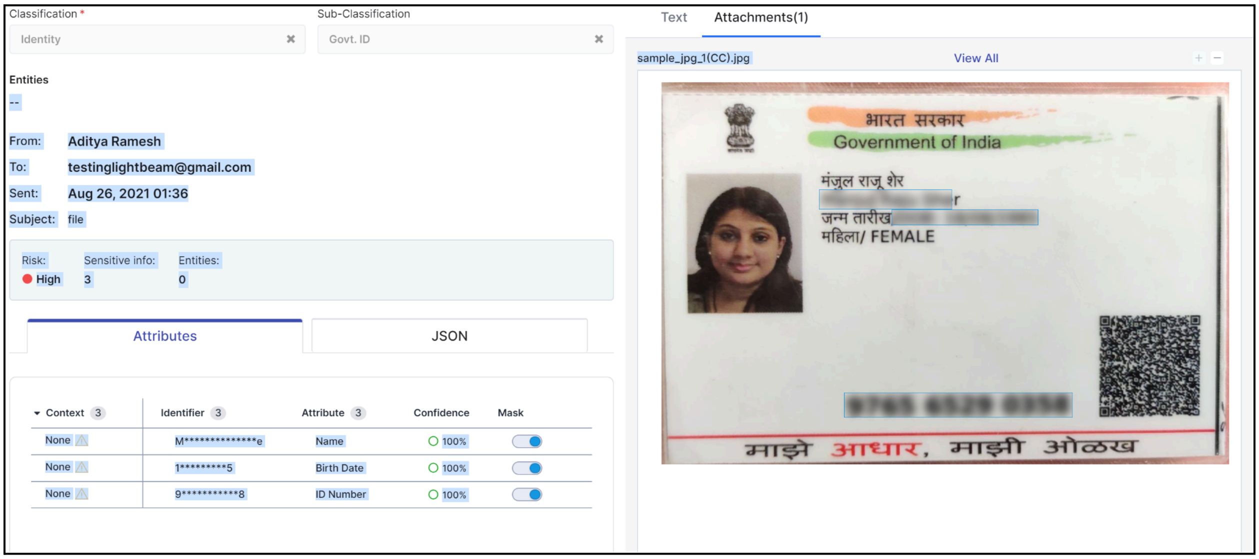
- Alerts are triggered based on rule sets inside policies.
- Alerts can be set for specific applications or all connected applications.
- Alerts can trigger a workflow to drive a review and approve cycle

Redaction

An example of automation is LightBeam's ability to redact the presence of sensitive data within data repositories.

- The redaction control is used to maintain accurate processing records while reducing the use and risk of PI by obfuscating select fields from view.
    - Redaction control works on many document types including image files.
    - Redaction control can be set to obfuscate any sensitive data fields while keeping the rest of the process information intact in LightBeam
    - Redaction filtering can be role-based for eyes-only operations.

In the example below a government ID is redacted of sensitive fields with some less sensitive information un-redacted. LightBeam can learn and scan images as well as documents and repositories.



Classification * Identity ✖

Sub-Classification Govt. ID ✖

Entities

--

From: Aditya Ramesh

To: testinglightbeam@gmail.com

Sent: Aug 26, 2021 01:36

Subject: file

Risk:	Sensitive info:	Entities:
● High	3	0

▾ Context 3	Identifier 3	Attribute 3	Confidence	Mask
None ⚠	M**************e	Name	○ 100%	●
None ⚠	1*********5	Birth Date	○ 100%	●
None ⚠	9***********8	ID Number	○ 100%	●

sample_jpg_1(CC).jpg

भारत सरकार
Government of India

मंजुल राजू शेर
[redacted]r
जन्म तारीख [redacted]
महिला/ FEMALE

[redacted]

माझे आधार, माझी ओळख

Guided by LightBeam's established policies, the scanning engine, Spectra, continuously scans the data environment looking for changes to the data. New copies and uses can quickly be identified and either added to a permissions list, redacted or removed. By automating the execution of enforcement controls like alerting and redacting on a continual basis, an always-on accurate inventory of personal information is created. The process maintains an identity-centric index that can be used to facilitate the retrieval of an Individual's PI and aid in the processing of Individual Rights Requests. Additionally, DPA allows for duplicated data to be easily monitored and controlled reducing data leakage.

Data Privacy Automation for ZenDesk

Automate

Utilizing LightBeams DPA technology to execute privacy process controls to continually scan, monitor and control data usage is a powerful tool for today's Privacy, Compliance, IT, and IT Security teams. Automated monitoring of IT system controls has long been a part of most modern IT and security programs. Now the monitoring of sensitive data usage through automated processes greatly expands visibility, control, and understanding of an organization's sensitive data use across the data lifecycle.

LightBeam customers can configure policies to trigger actions to manage the use of PI in Zendesk. The Zendesk use case is centered on the Zendesk service tickets and the PI stored in them. Spectra can discover PI in both the body of a ticket as well as any attachments that are a part of the ticket. LightBeam will identify any of the 200+ common attributes and any client custom attributes in those tickets. LightBeam will identify tickets containing PI and based on the rule set of the control policy that is in force automatically take steps to;

1, Raise an alert and initiate a review and approve workflow

And/or

2. Redact the PI stored in the ticket Zendesk.

As an example A client may want to redact any sensitive information in any part of a service ticket but only after the ticket has been closed. To accomplish this Spectra would first analyze a ticket to see if it meets a certain criteria. Select all closed tickets that contain any sensitive information. All sensitive data in the selected tickets would be redacted. These tickets would appear as if a black marker was used to cross out the information

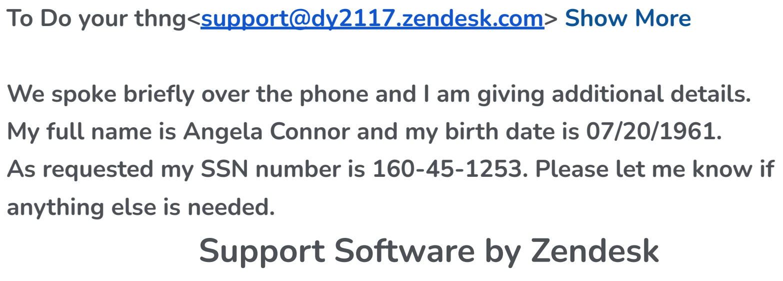
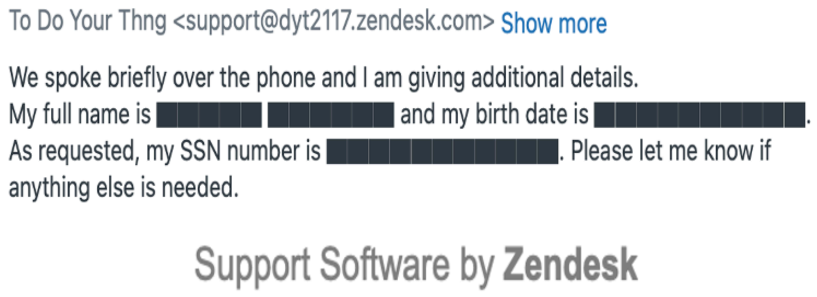
Zendesk Redaction

LightBeam can recognize sensitive data in the body and attachments in Zendesk tickets.

- By scanning and analyzing Zendesk support tickets, sensitive data selected for redaction is identified.
- Masking selectors allow for document-specific redaction rule-sets to be turned on or off providing access to the selected attributes.

- ○ PI is obfuscated after the ticket has been completed. This is removed after the retention period has been met and the data is no longer needed.
- ○ Support tickets can safely be archived with all sensitive data redacted.

Zendesk tickets may contain the personal details of a requester that are needed to provide support and service the ticket.

Before Redaction
 To Do your thng<support@dy2117.zendesk.com> Show More We spoke briefly over the phone and I am giving additional details. My full name is Angela Connor and my birth date is 07/20/1961. As requested my SSN number is 160-45-1253. Please let me know if anything else is needed. Support Software by Zendesk
After Redaction
 To Do Your Thng <support@dyt2117.zendesk.com> Show more We spoke briefly over the phone and I am giving additional details. My full name is [redacted] [redacted] and my birth date is [redacted]. As requested, my SSN number is [redacted]. Please let me know if anything else is needed. Support Software by Zendesk

By establishing Policies, Rule sets, and Permission lists in LightBeam, automated monitoring not only provides visibility of the data inventory, it also continually enforces the data management rules to manage privacy risk. By having a tool that automatically removes PI from all closed tickets, privacy officers have reduced their PI footprint and reduced their risk of inappropriate loss or disclosure.

Connecting Zendesk to LightBeam

Connecting any ZenDesk instance as a data source to LightBeam is a simple 3 step process.

1. Create a new ZenDesk data source.
2. Connect to the new Gdrive
3. Configure scan preferences

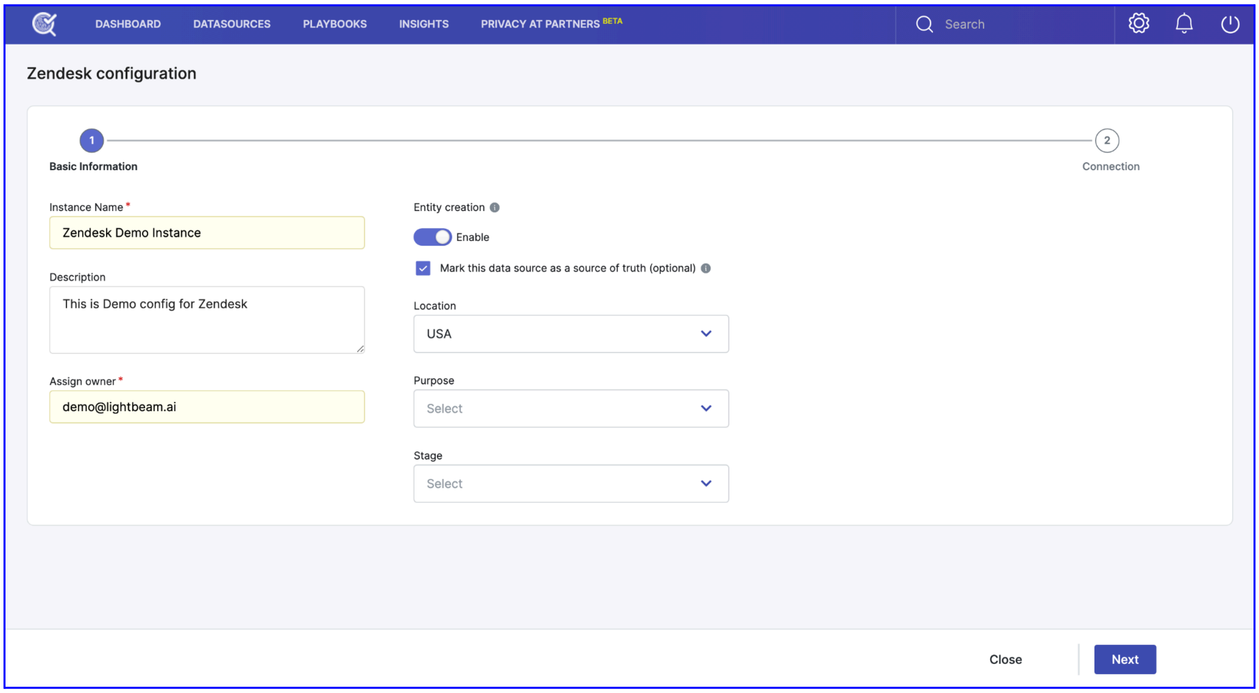
To begin from the LightBeam home dashboard, select DATA SOURCES. From the DataSource home screen select Add Data Source from the top right of the page. From the application list select New ZenDesk and continue with the steps below.

Step 1:

Complete the Basic Information page to create a new data source. Keep the following guidance in mind when creating a new data source:

1. Ensure the name is not repeated, as it acts as metadata for the data source and must be unique. E.g., Zendesk_Support
2. Use the description to explain the kind of information the data source contains. E.g., All customer support tickets
3. LightBeam uses the email ID stated as the Primary Owner to send alert notifications.
4. You can add another email for notifications using the co-owner button. Remember to check the ‘send notification to all owners’ box.
5. Entity Creation: Enable to create entities out of this data source
6. Location tells where the data source is located
7. Purpose tells for what purpose is this data source storing or processing data for

8. The stage tells what stage the data belongs in, which could be source, processing, transactional, archival, etc.



Zendesk configuration

1 Basic Information

2 Connection

Instance Name * Zendesk Demo Instance

Description: This is Demo config for Zendesk

Assign owner * demo@lightbeam.ai

Entity creation: Enable

☑ Mark this data source as a source of truth (optional)

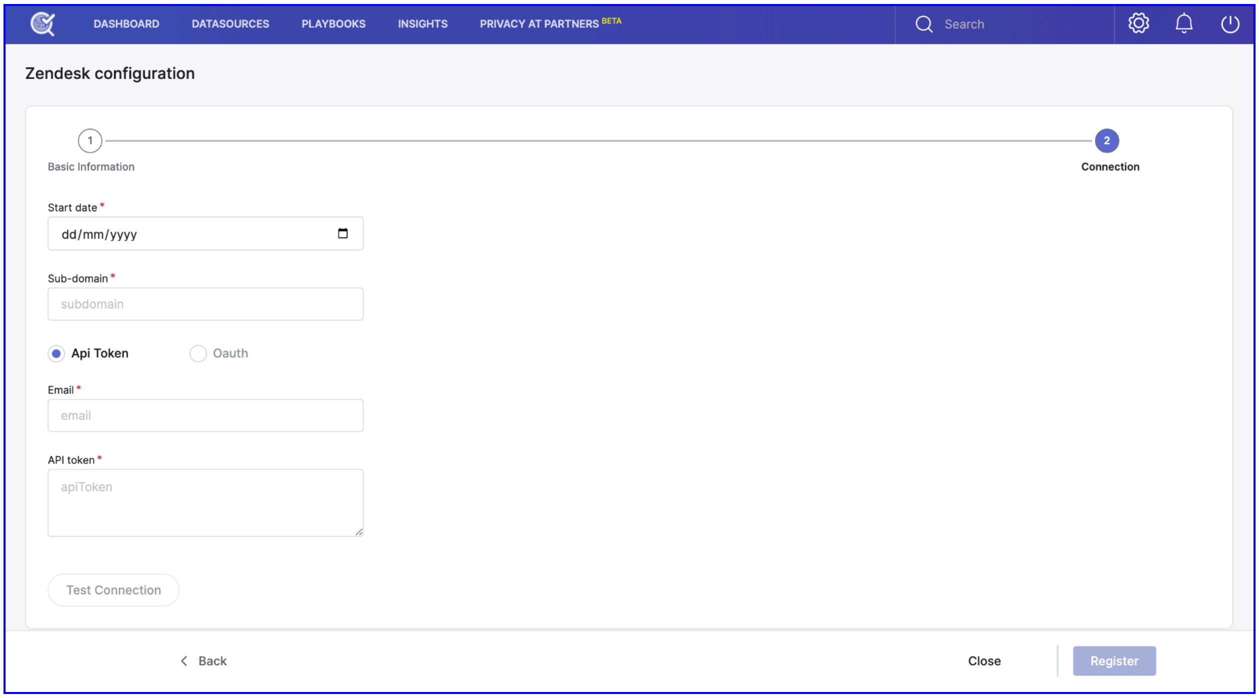
Location: USA

Purpose: Select

Stage: Select

Step 2: Connection Details

1. Select the start date from when you want to start scanning the tickets
2. Add subdomain name
3. Configure API Token for authentication
    a. Add the Email ID from which the API token has been created
    b. Add API token
4. You can test the connection and see if the connection really went through



Zendesk configuration

1 Basic Information — 2 Connection

Start date * dd/mm/yyyy

Sub-domain * subdomain

● Api Token ○ Oauth

Email * email

API token * apiToken

Test Connection

Step 3: Scan Settings

1. Scan ZenDesk instances

Conclusion

Managing the appropriate use of personal information is challenging for any organization. Administrative controls like policies, procedures, and employee training are only as good as their execution which is often an afterthought in many organizations. By using the power of AI to diligently scan and monitor data applications and repositories, data officers can apply significant technical control over how data is stored and processed. This in turn provides privacy teams with new accurate pictures of how sensitive data is used in the organization. By understanding all sensitive data in an organization LightBeams 360 degree view allows for more advanced reviews and proactive actions to be taken to manage privacy operations and reduce overall privacy risk.

Appendix

Revision History

Reference Architecture Update	Date	Author
First generally available version.	11/30/2023	Bill Schaumann

About LightBeam

With its focus on Data Privacy Automation (DPA), LightBeam is pioneering a unique identity-centric and automation-first approach to the data privacy and data security markets. Unlike siloed solutions, LightBeam's Data Privacy Automation (DPA) ties together sensitive data discovery, cataloging, access, and data loss prevention (DLP), and makes the right (sensitive) identity-centric data available to the right people and teams. It becomes the privacy control tower providing a 360-degree view of PII/PHI sensitive data sprawl. LightBeam enables privacy officers to set policies to automate their enforcement, while information security executives can finally rest assured that sensitive data is being used and accessed securely.