LightBeam.ai™

Breach Response Service

From Chaos to Coordination

Unauthorized data breaches pose significant risks to organizations. These breaches occur when bad actors gain access to sensitive or confidential information, including personal, corporate or production data. The consequences for businesses can be severe, affecting their customers, employees, and business partners.

A Modern Approach to Breach Response

While traditional methods require hundreds of hours to understand data exposure, LightBeam uniquely automates cataloging of data, and the identities (individuals) that may be at risk due to a breach, leading to a quick, targeted and effective response strategy.

Breach Perimeter

Know **WHAT** data may be at risk across Cloud, SaaS and On-prem apps.

Breach Identity

See **WHOSE** data may have been impacted (customers, employees, vendors).

Breach Notification

Notify exactly the **PEOPLE** and **PARTNERS** who may have been impacted.

LightBeam can help you assess the exposure and prepare a response strategy with just three simple steps aligned with your incident response plan:

Execute a mutual non-disclosure agreement (MNDA)

Rest assured that all information you share will be treated with due respect and confidentiality.

Deploy or Connect to LightBeam (with full data residency)

Deploy LightBeam in your environment (AWS, Azure, GCP, VMware, Nutanix), or connect to your dedicated LightBeam SaaS instance.

Identify Impacted Resources, Remediate and Notify

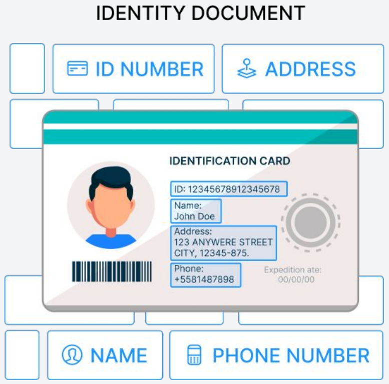
Scan the at-risk data sources/repositories to understand the scope of exposure, and generate reports for further action.

Defining Your Breach Perimeter

Resources | Identity | Reporting

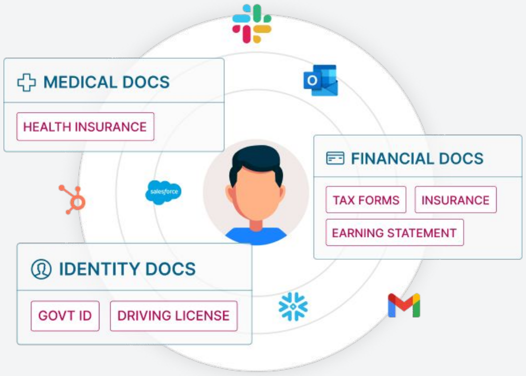
Assess Breach Perimeter: Catalog all sensitive assets and resources.

- Discover and classify all files with sensitive data (PII/PCI/PHI/Others, Financial/ Legal/Medical etc.).
- Visibility into disparate data repositories across Cloud (AWS, Azure, GCP), SaaS (SharePoint, Gdrive), and On-prem (file servers) locations.



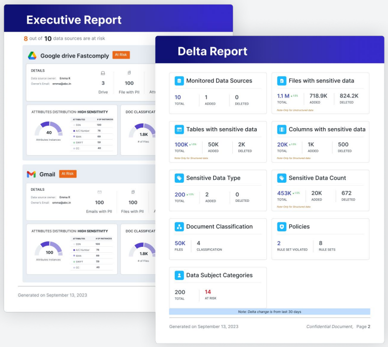
Assess Breach Identity: Automatically identify all individuals and partners at risk of information exposure.

- Individuals - Customers, Patients, Employees, Executives etc.
- Organizations -Partners, Vendors, Clients etc.



Generate Reports: Provide actionable information to your incident response team.

- Sensitive data element report highlighting the sensitive data that's part of the exposure including where such data elements reside within the organization.
- Entity report capturing the details around people and organizations that need to be notified.



Executive Report

8 out of 10 data sources are at risk

Google drive Fastcomply At Risk

DETAILS

Data source owner: Emma R

Owner's Email: emma@abc.in

3 Drive | 100 File with PII

ATTRIBUTES DISTRIBUTION: HIGH SENSITIVITY — 40 Attributes Instances

ATTRIBUTES	# OF INSTANCES
SSN	100
A/C Number	78
IBAN	69
SWIFT	59
CC	40

DOC CLASSIFICAT — 1.8K # of Files

Gmail At Risk

DETAILS

Data source owner: Emma R

Owner's Email: emma@abc.in

100 Emails with PII | 100 Files with PII

ATTRIBUTES DISTRIBUTION: HIGH SENSITIVITY — 100 Attributes Instances

ATTRIBUTES	# OF INSTANCES
SSN	100
A/C Number	78
IBAN	69
SWIFT	59
CC	40

DOC CLASSIFICAT — 1.8K # of Files

Generated on September 13, 2023

Delta Report

Monitored Data Sources: 10 TOTAL | 1 ADDED | 0 DELETED

Files with sensitive data: 1.1 M ▲1.5% TOTAL | 718.9K ADDED | 824.2K DELETED — Note-Only for Unstructured data

Tables with sensitive data: 100K ▲1.5% TOTAL | 50K ADDED | 2K DELETED — Note-Only for Structured data

Columns with sensitive data: 20K ▲1.5% TOTAL | 1K ADDED | 500 DELETED — Note-Only for Structured data

Sensitive Data Type: 200 ▲1.5% TOTAL | 2 ADDED | 0 DELETED

Sensitive Data Count: 453K ▲1.5% TOTAL | 20K ADDED | 672 DELETED — Note-Only for Structured data

Document Classification: 50K FILES | 4 CLASSIFICATION

Policies: 2 RULE SET VIOLATED | 8 RULE SETS

Data Subject Categories: 200 TOTAL | 14 AT RISK

Note: Delta change is from last 30 days

Generated on September 13, 2023 — Confidential Document, Page 2

www.lightbeam.ai
info@lightbeam.ai | +1 (650) 224 8706
460 California Ave Suite 205 Palo Alto, CA 94301

Try out LightBeam now at:
www.lightbeam.ai/securenow

From Chaos to Coordination

Staying ahead of FUD

Review your incident response plan

Your incident response plan is the best place to start. It will outline the areas of responsibilities, the action owners, the expected urgency of actions amongst others.

Designate individual(s) for internal and external communication

Breaches need to be handled with speed. Fear, uncertainty and doubt (FUD) naturally creep in. A proactive communication approach for need-to-know individuals and teams is recommended.

Execute on your legal responsibilities

Consult your legal counsel on your responsibilities for notifying internal/external parties in compliance with your local/national/global obligations.

Predictable Pricing

Time is of the essence in responding to breaches. LightBeam offers a pre-packaged solution to organizations via its **SNAP (SecureNow Assessment Program)** to help you respond effectively and quickly to an unfortunate data exposure event.

SNAP offers a fixed price limited duration LightBeam license to get you the data you need quickly to act on the exposure. SNAP includes:

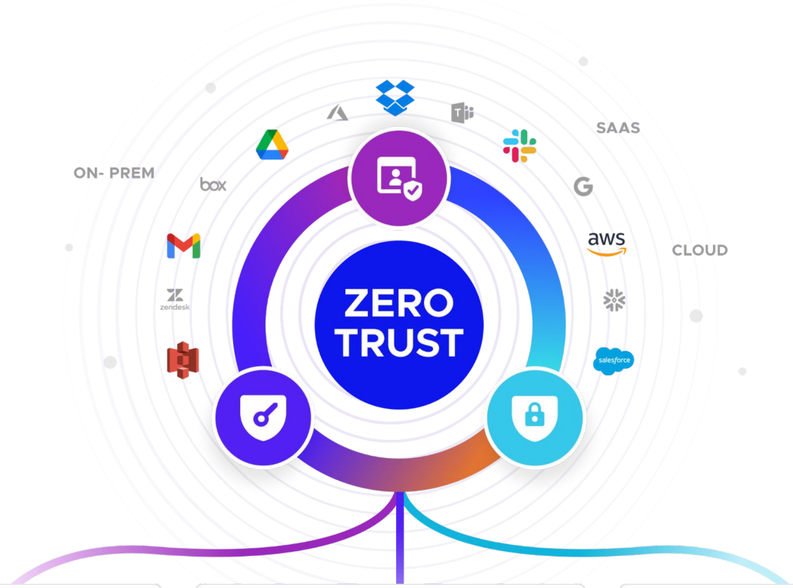
- Discovery, Classification and Cataloging of exposed data for up to 3 applications.
- Results and reports starting the first day of scanning.
- Up to 5TB of capacity scanned for each application.
- Up to 500 users’ data scanned for Microsoft M365 or Google Gsuite apps.
- Modular pricing option to tailor and extend licensing to meet your specific needs.

For continuous peace of mind, LightBeam also provides subscription licenses that customers may consider once their breach response is behind them. . For more details on SNAP or Subscription licenses, contact your LightBeam reseller/partner or sales@lightbeam.ai

LightBeam.ai™

Zero Trust Data Protection

Discover, Classify and Control Access to Sensitive Data



SECURITY

DATA DISCOVERY

- Structured data
- Unstructured data
- Semi-Structured data

RISK REMEDIATION

- Redaction
- Archival
- Deletion

PRIVACY

- Data Subject Request
- Consent Management
- Record of Processing Activity
- Privacy Impact Assessment
- Third-party risk management
- Right to be Forgotten
- ADMT

GOVERNANCE

- Labeling
- Cataloging
- Retention
- Life cycle
- Access
- Residency

About LightBeam

LightBeam.ai converges data security, privacy, and AI governance, so businesses can secure their data across cloud, SaaS and on-prem locations. Leveraging generative AI, LightBeam ties together sensitive data cataloging, control, and compliance across structured (databases), unstructured (file repositories), and semi-structured (ticketing systems) applications. LightBeam enables you to start down the road of your zero trust data protection journey.

LightBeam is on a mission to create a secure privacy-first world.

www.lightbeam.ai
info@lightbeam.ai | +1 (650) 224 8706
460 California Ave Suite 205 Palo Alto, CA 94301

Try out LightBeam now at:
www.lightbeam.ai/securenow