Laminar

USE CASE BRIEF

# Conquer Shadow Data

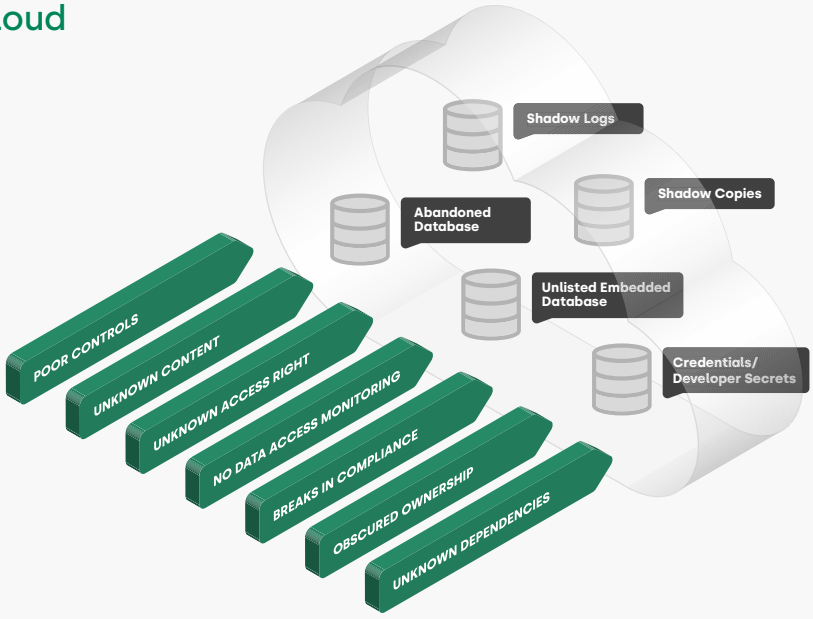
Discover and secure Shadow Data in multi-cloud environments

## Challenges

While the cloud maximizes flexibility to develop, distribute, backup, and manage all kinds of sensitive data, security teams are facing a deadly combination of a geometrically increased attack surface and near zero visibility, especially of the "Shadow Data" created by ongoing operations. Challenges include:

- Unknown Data Assets: Lacking programmatic discovery of data assets, the full range of data assets is unknown.
- Insufficient Controls: Data is often moved outside of the compliance guidelines (across geos) or without copying source controls.
- Unclassified Content: The sensitivity of the data types are not discoverable without manual investigation.
- Lack of Context: Context such as asset owner, usage, and application dependencies is not known due to turnover or gaps in documentation.
- No data access monitoring: Access rights are not known and accesses to data are not monitored much less analyzed for anomalies.
- Lack of Detection: Lacking the above information, leakage of Shadow Data such as data stores, logs / caches, and credentials / developer secrets is not detected.

## Shadow Data in the cloud




*Shadow Data is spawned throughout the cloud as part of everyday operations.*

## Cloud Shadow Data security with Laminar

Our industry-leading platform embeds into your environment to provide data security for everything you build and run in the cloud, including Shadow Data. Highlights:

- Discover all data: Autonomously discovers all data assets used in the cloud without requiring access credentials.
- Classify the data: Classifies data and identifies PII and PCI automatically.

- Prioritize by risk: Prioritizes data assets that pose a high security or governance risk.
- Deliver actionable context: Provides actionable information including data owner, history, and application dependencies.
- Highlights Inactive data: Highlights inactive data that may be deleted or archived.
- Recommends remediation: Recommends remediation such as encryption or quarantine.

## How Data Security Teams Work With Laminar

With Laminar, Security teams find the data security attack surface is reduced and visibility is enhanced. With Laminar, Data Security teams:

- Monitor usage: Monitor real-time cloud data usage and trends even in multi-cloud environments using Laminar's dashboards.
- Understand data assets: Understand each data asset in detail from the information presented by Laminar in drilldown windows and reports.
- Validate conformance: Ensure that assets are in conformance with security policies.
- Investigate: Investigate prioritized and questionable assets by contacting the owner and the creator of the data.
- Prioritize protections: Ensure that PII, PCI, and other sensitive data receives higher levels of protection.
- Request Action: Request IT or Development take specific actions such as encrypt based on Laminar's recommendations (manually or via API integrations).
- Respond to Data Leaks in real time: Take action in real time in response to a detected incident (via the organization's tools or API integrations).
- Remediate: Remediate by taking action such as encryption or quarantine (via the organization's tools or API integrations).

Laminar is the first and only cloud data security platform that provides:

- **Autonomous** discovery and classification for all cloud data assets including Shadow Data
- **Agentless** architecture that operates asynchronously to avoid performance impacts
- **Continuous** monitoring to identify new risks, provide Data Leak Protection (Cloud DLP), and uncover security anomalies in real time
- **Embedded** functions within the customer's cloud so that sensitive data never leaves

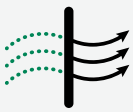
## Benefits

### Provide Defense in Depth for Cloud Data

Provides preventive and detective controls for your data including active defenses and data security attack surface minimization.

### Match security to value

Data security can be ramped to ensure that "crown jewel" data assets receive the highest levels of security controls .



### Detect Shadow Data leaks

Detects all forms of Shadow Data across the environment and pinpoints both data leaks and unauthorized infiltrations.

ABOUT LAMINAR

Laminar's Cloud Data Security Platform is first in the market to protect data in everything you build and run in the cloud across cloud providers (AWS, Azure, and GCP) and cloud data warehouses such as Snowflake and Databricks. The platform autonomously and continuously **discovers** and **classifies** new datastores for complete visibility, **prioritizes** risk based on sensitivity and data risk posture, **secures** data by remediating weak controls and actively **monitors** for egress and access anomalies. Designed for the multi cloud, the architecture takes an API-only approach, without any agents, and without sensitive data ever leaving your environment. Founded in 2020 by a brilliant team of award winning Israeli red team experts, Laminar is proudly backed by Insight Partners, TLV Partners, and SentinelOne. To learn more please visit www.laminarsecurity.com. www.laminarsecurity.com