Laminar

How to Achieve Data Protection at the Speed of Cloud

Table of Contents

DATA PROTECTION

The Soft Underbelly of Cloud Security

Laminar

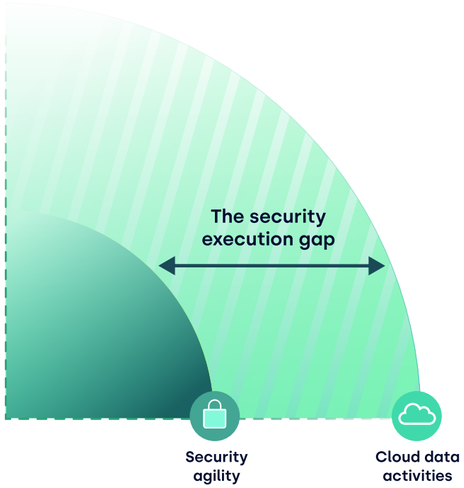
A Uniquely Cloud Challenge: The Security Execution Gap

The cloud has transformed the world, enabling multiple revolutions in the tech ecosystem. It allows us to dynamically scale up data resources, using them for everything from optimizing internal processes to developing new products. But there is a darker side to this great innovation boom.

We've seen a growing divide — what we call the security execution gap — between business innovation and the security practices needed to secure it.

To safeguard the business and empower internal innovation, security teams need to rethink their entire approach to data security.

This eBook describes the current challenges of running a data security program for the cloud and provides a roadmap for achieving agile data security, with real-world examples.



THE DRIVERS

How the Cloud Changed Data Protection

There are three major factors that significantly changed data protection in the cloud and contributed to the ongoing security gap.

01

Increasing adoption of cloud data technologies

Before the cloud, security professionals were tasked with securing data in controlled, on-premises environments. Every part of the architecture was owned and managed by the organization itself, and it was much easier to control who had access to which assets.

In today's world, businesses are adopting cloud technologies across multiple providers to store, use, and share data in the cloud. Each one is configured and used differently, and each comes with its own risks.

Not only are these new architectures complex and confusing, but they're also constantly changing.

Additionally, all data in the cloud is accessible from anywhere, given the right credentials or tokens. Unlike the traditional perimeter, there's no longer a choke point to protect and monitor, making it much easier to access sensitive data.

02

Proliferation of data

In today's agile cloud environment, developers and data scientists have free reign to spin up new datastores at any time and without any of the traditional gatekeepers. As they freely copy, share, analyze, and move data, inevitably, they will inadvertently move sensitive data to an environment that lacks appropriate governance and security measures.

And because this data proliferation is happening out of the security team's sight, they're often unaware of its existence and unable to secure it. These forgotten, unsecured datastores full of sensitive data are called **shadow data**, and it's the greatest threat to your data security.

03

Increasing pace of change

You may sense a theme here. Business in the cloud moves at a much faster rate than we've seen in the past. Now, release cycles happen in weeks or even hours, and security is either left out of the process entirely or isn't given adequate time to ensure data is appropriately protected.

This speed is a competitive advantage, but at what cost? Data security teams are struggling to find the right balance.

These factors have created the perfect storm,

resulting in a new threat vector called the innovation attack surface. It refers to the accidental but continuous creation of risk through the course of data innovation, and unfortunately, many businesses think it's the unavoidable cost of doing business.

NEW CHALLENGES

State of Cloud Data Protection Today

The market changes above and the lack of cloud-native solutions in place result in new challenges for data protection teams.

Laminar

Lack of visibility

Most data protection teams have no idea where their sensitive data is in their cloud environments or who has access to it. It's impossible to protect what you can't see, and security teams often don't have insight into their data security posture or risk level.

Increasing regulatory mandates

Data privacy regulations are on the rise, especially for those in highly regulated industries or who do business globally. While it's challenging to keep up with these shifting regulatory requirements, it's nearly impossible to enforce them without a detailed understanding of your data. Security teams need an overarching "single pane of glass" view to implement controls, monitor, and demonstrate compliance.

93% of security professionals are concerned about shadow data (up from 82% last year)*

Lack of automated controls

Cloud innovation requires that users be able to move and copy data at the press of a button, but data security policies don't travel with that data. These policies should govern how data is protected, where it's stored, and who has access, but with the dynamic movement of data, security teams have no automated way to implement these controls, let alone record violations.

Traditional approaches are insufficient

Manual, homegrown, and legacy solutions are not designed for the dynamic cloud environment. They require security teams to know where all their data is, which makes them cumbersome, resource-intensive, and rife with human error. They simply can't keep up with the speed of cloud.

EXAMPLE

Shadow Data Breach Example: Microsoft

There are many stories of the business risk caused by a lack of data visibility, this is just one example.

65K

entities from 111 countries potentially impacted

2.4 TB

of sensitive data exposed

In October of 2022, security researchers exposed a data breach in Microsoft's ecosystem. A whopping 2.4 TB of sensitive data was exposed, including prospect and customer names, email addresses, email contents, phone numbers, and other business files.

Researchers revealed that a misconfigured Azure Blob Storage caused the breach, rather than a security vulnerability. This exposure allowed unauthorized users to access business transaction data from 2017 to August 2022. The researchers claimed they could link the sensitive data to over 65,000 entities from 111 countries.

While no customer accounts or systems were compromised, bad actors could use the stolen data for extortion, blackmail, social engineering, and other nefarious purposes.

Data security could have avoided this breach if they had visibility into the security posture of this dataset, including what type of data it was and who had access.

Laminar Labs findings:

21%

of publicly exposed buckets contained sensitive data.

This finding further highlights the need to understand the access permissions of your cloud data storage, as well as the nature of the data within those buckets.

DATA SECURITY 2.0

Requirements for Data Security in the Cloud

To secure, govern, and maintain the privacy of sensitive data in the cloud, you need the visibility and control that can only be provided by a cloud-native DSPM (data security posture management) platform.

Your DSPM solution should offer these five capabilities:

Global data visibility

Your chosen DSPM solution should provide a comprehensive view of sensitive data across all cloud environments (including IaaS, PaaS, and SaaS services), answering:

1. Where and what sensitive data you have.
2. Who the data owner is.
3. Who has access to the data.
4. The data's current posture status.
5. How the data gets accessed.

Data access governance

Next, the DSPM solution should provide data access governance: identifying all internal/external users, roles, and resources with access to sensitive cloud data stores. Then, it should continuously track privileges based on each user's roles and responsibilities, including third-party access to data.

Data security risk control

In addition, your chosen DSPM solution should have the ability to detect data that is overexposed (e.g., public read access), unprotected (e.g., no encryption), or misplaced (e.g., sensitive data in the wrong environment). Then, it needs to provide remediation guidance, prioritized by risk.

Privacy and compliance

Lastly, your DSPM solution must detect and remediate regulatory and industry compliance violations. It should do this via a policy engine with common frameworks built into it. The DSPM should be able to generate audit-ready compliance reports to prove that your team successfully remediated these data violations.

Data hygiene

Your DSPM solution should provide data hygiene guidance, enabling users to locate and purge misplaced, redundant, and obsolete data. It should also be able to set policies that continuously maintain data quality in the future, in keeping with your organization's data governance framework.

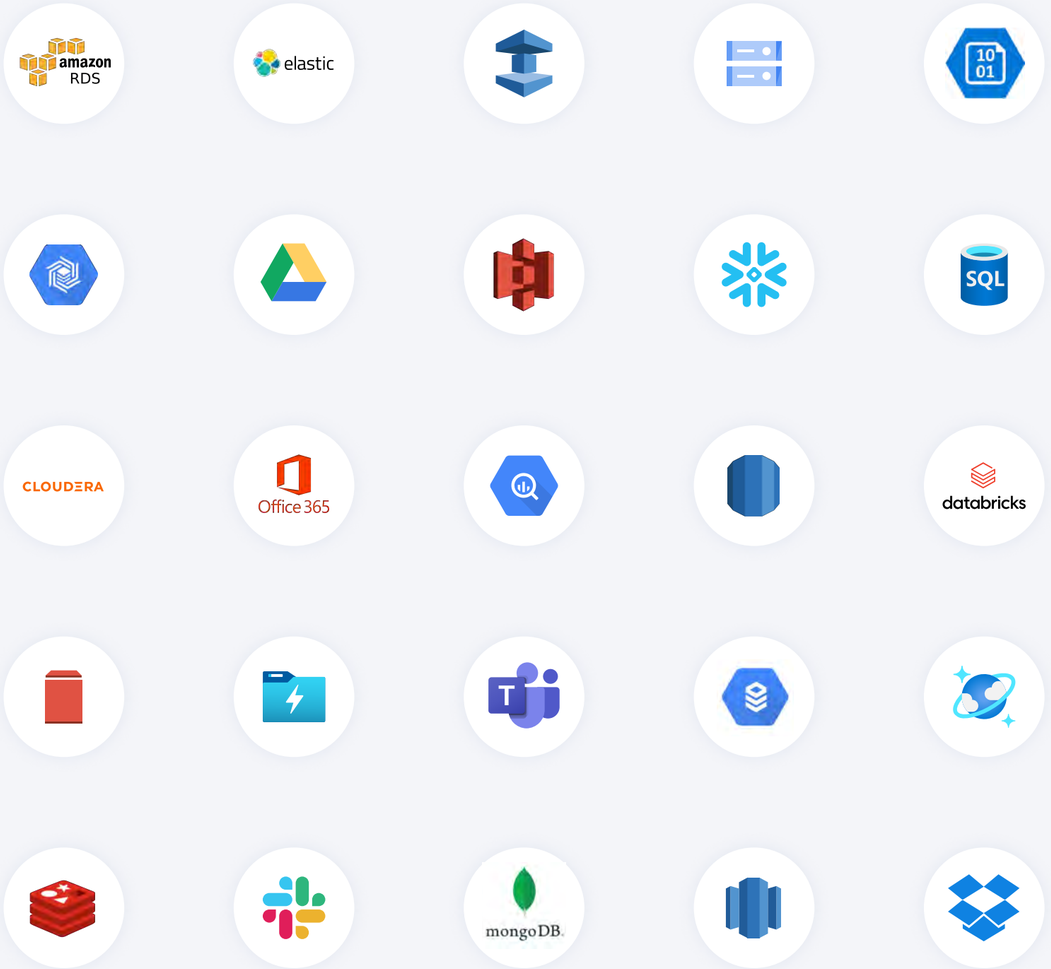
SPOTLIGHT REQUIREMENT

Solutions Must Cover the Sprawl of New Cloud Technologies

In a world where **over 87% of organizations have multi-cloud ecosystems,** with the majority deploying three or more cloud service providers (CSPs) and more than half employing data warehouse technology, it's more important than ever before that a DSPM solution covers this sprawl of technologies.

Additionally, within each CSP, there are a whole host of disparate object or asset-level technologies that may contain data, further complicating an already complicated challenge.

Here is just a taste of the vast array of cloud technologies:



DATA SECURITY 2.0

Why are Available Products Not Enough?

There are many data security solutions on the market that claim to secure data in the cloud, but most of them fail to meet the requirements listed above.

Manual solutions

We've discussed the proliferation of shadow data and the lack of visibility that security teams have into their multi-cloud environments, so it should be clear why manual cloud data security is inadequate. Again, you can't protect what you can't see.

Not only is manual data mapping and classification prone to human error, but it's also tedious, resource-intensive, out of date before it's even finished, and limited to the well-known and actively used datastores. Manual policy enforcement is equally resource-intensive and similarly ineffective due to its reliance on word of mouth to verify adherence to data security policies.

Legacy data security solutions

Legacy data security solutions were designed for on-premises IT environments, not today's dynamic cloud environments. They're connector-based, requiring manual connection to each data asset — often including access credentials — have high false positive rates, and are costly to maintain. It's also common that these solutions remove data from the environment, creating additional security risks rather than eliminating them.

CSPM / CNAPP solutions

Cloud security posture management (CSPM) and cloud-native application protection platforms (CNAPP) were designed to protect the cloud infrastructure and locate misconfigurations. While they're simple to install, they're unable to identify all shadow data such as misplaced or redundant data, detect a data leakage, or monitor access.

At best, these solutions provide basic data discovery capabilities but do not focus on privacy, compliance, or governance requirements. Even worse, they remove data from the environment, posing an additional security risk.

Homegrown solutions

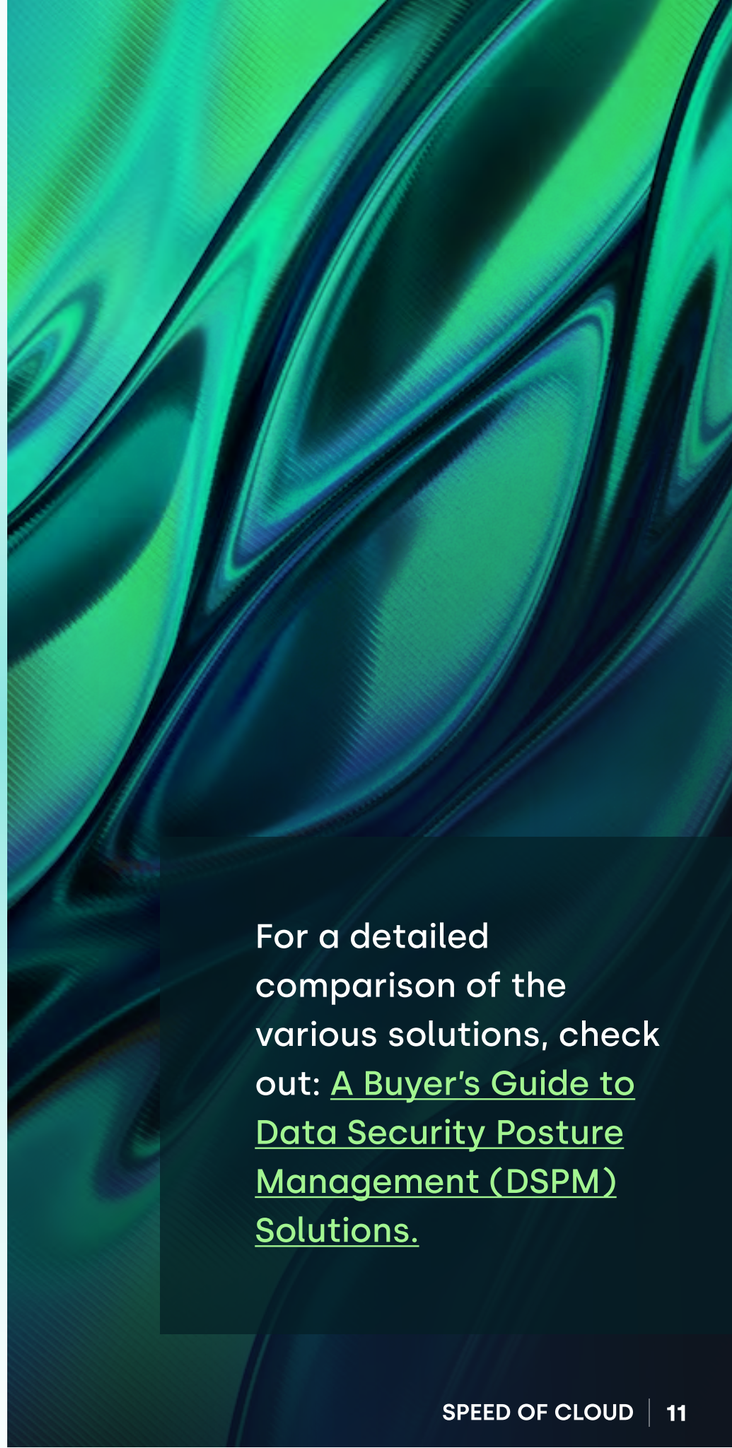
Like the manual approach, homegrown solutions are a massive drain on internal resources. Internal engineers must be pulled from more strategic security initiatives to configure connectors that allow for scanning, which also requires advanced knowledge of the location of these data assets.

This process is not only time-consuming, labor-intensive, and complex, but it leaves large amounts of sensitive data unaccounted for. Neither manual nor homegrown approaches are sustainable or scalable.

CSP-Native Solutions

Cloud Service Provider (CSP-native) solutions are offered directly by the CSP, and are mostly uni-cloud with limited asset support. For example, AWS Macie only supports S3 buckets + RDS snapshots to S3. Because they're uni-cloud, they typically require additional 3rd party solutions to secure (multi-cloud) assets.

CSP-native solutions traditionally have used full scan techniques — you have to know where data is to schedule the scan — and are therefore inefficient and difficult to configure. They miss shadow data entirely, and with a lack of smart scanning capabilities, they also incur high cloud operating costs. Lastly, CSP-native solutions do not provide data threat alerting or actionable remediation guidance.



For a detailed comparison of the various solutions, check out: A Buyer's Guide to Data Security Posture Management (DSPM) Solutions.

LAMINAR CASE STUDIES

Discover how Laminar's clients from diverse industries use DSPM to secure data in their multi-cloud environments.

RISE

CASE STUDY

Ad-Tech Company Establishes Data Security and Saves Cloud Cost with Laminar

"With Laminar's access analysis, we can identify unused data on our terms, such as identifying data with no read or write activities for the last 90 days. This allows us to be flexible in how and what we want to delete and better manage data that we store, as well as reducing the risk"

Challenge

Rise, an ad-tech company in media and publishing, had large quantities of data, originating from many different sources, that were being stored in their AWS environment.

They were looking for a solution that could provide the visibility they needed to ensure they were accessing the full potential of their data, improving development velocity, and reducing cloud expenditure.

Solution

Laminar gives Rise a comprehensive view of their data in S3, RDS, EC2, Elasticache, and DynamoDB, including a record of when and how it was accessed. By analyzing access at very high granularity levels, Rise now gets an unprecedented level of understanding of how the data is being used in its environment.

This results in better engineering, better cloud cost management, and a more secure data posture.

Read Full Case Study ▸

BOOKING HOLDINGS

CASE STUDY

An Innovative Global Travel Platform Achieves Complete Visibility and Data Security

Challenge

Agoda is one of the world's fastest-growing online travel booking platforms, providing a global network of over 3 million properties in more than 200 countries.

To meet compliance requirements and secure their customers' sensitive data, they needed better visibility into their security posture.

Solution

Laminar's platform continuously scans Agoda's cloud environment, discovering and classifying all data, and assessing their security posture status against an extensive set of prebuilt and custom security policies.

When Laminar detects a policy violation, the platform issues an alert and provides actionable remediation recommendations. This empowers Agoda to remediate risks within minutes, thus proactively maintaining its cloud security posture.

Read Full Case Study ▸

"Laminar enables us to grow our data in the cloud while effectively mitigating risk. They provided quick time to value and helped us discover all sensitive data, including the shadow data we uncovered."

Payability

CASE STUDY

Ecommerce Funding Platform Establishes Data Governance and Protects Business Agility with Laminar

"It took me three times longer to find the information I need in other tools, and I can trust the results I see thanks to [Laminar's] really low false positive rate."

Challenge

Payability, an ecommerce funding platform, recognized that good data governance is important to maintaining a cloud environment that fosters agility and innovation.

Without data governance, the accumulation of redundant, obsolete, or trivial (ROT) data clutters the cloud environment and increases cloud costs and the risk that bad data is accidentally used during the software development process.

Solution

Laminar gives Payability full and continuous visibility of its cloud data — without requiring connectors, access credentials, or any other input from the team — so they always have access to current information. They can see where data is stored, what type of data it is, who has access, how and where it's being used, and how it flows through the cloud environment, which includes S3, EC2, dynamoDB or RDS. The platform also prioritizes data based on its sensitivity level, security posture, volume, and exposure, guiding their security team to remediate the most critical issues first.

Read Full Case Study ▸

About Laminar

As the leading enterprise DSPM solution, Laminar gives organizations the visibility and control they need to support their data security, privacy, and governance initiatives in the cloud. The cloud-native platform provides autonomous and continuous data discovery, classification, and protection across a multi-cloud environment via a unified console. Laminar deploys in minutes and integrates with existing security stacks and process flows, empowering teams to deliver agile data security at the speed of innovation.

If you want to learn more about **Laminar's data security posture management** approach, contact us today for **a 20-minute demo!**

*Source: State of Cloud Data Security Report 2023

www.laminarsecurity.com