Laminar

Top 3 Reasons Cloud Data Security Belongs in 2023 Security Budgets

Data has become the new currency

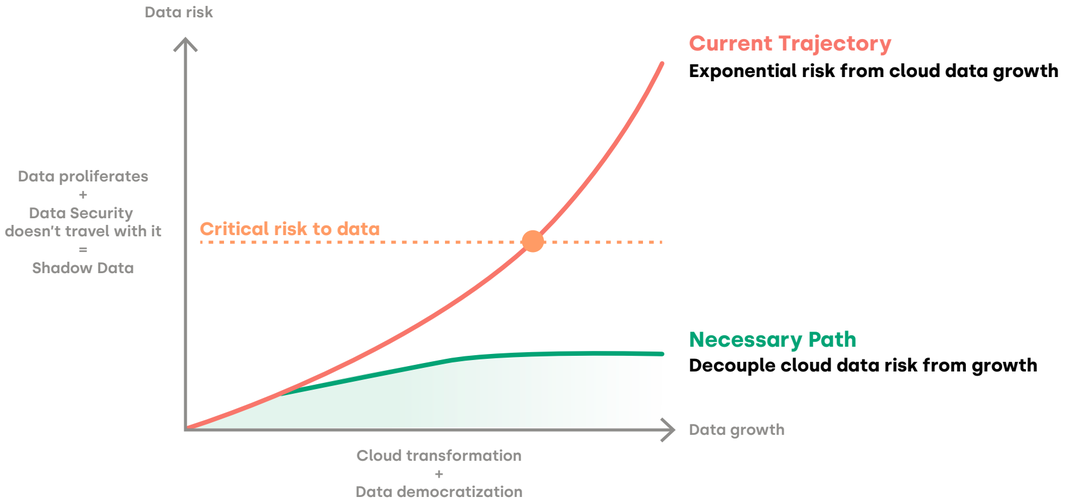
From 2020 to 2022 the amount of enterprise data will more than double, from one petabyte to just over two petabytes. More than 60% of this data is generated in the cloud. Far more than ever before.

Cloud data has facilitated innovation that uses AI or machine learning and data science to solve new challenges or old challenges in new ways. It feeds everything from customer experience improvements like increasingly personalized user playlists on streaming platforms to internal process efficiencies like narrowing in on the most impactful words in sales calls. With all of the many innovations that it can empower, data has become the new currency.

Despite its benefits, data growth also poses a risk: the more corporate data there is out there, without proper controls, the easier it is for attackers to steal. We see this in the corresponding growth in the size and scale of breaches—1,862 last year alone, a 68% increase from the year before.

Security teams should work to enable the acceleration of business, but they must also ensure that their organization's most sensitive data is protected. In order to achieve this delicate balance, they need to decouple the exponential growth of data from the risk presented to the enterprise by its proliferation.

Enable data democratization, safely



What's the answer?

Cloud-native, data-centric security solutions that are focused on enabling organizations to continuously protect their data by following the data as it proliferates in the hands of developers and data scientists who need to copy and move large volumes of sensitive data in the cloud to support innovation.

In this guide we review the top 3 reasons why you should include cloud data security in your 2023 cloud security budget. After all, if data is the new currency—isn't it time to rethink your cloud security budget?

1. Cloud data security is different than data security
2. Tedious manual efforts don't work in the cloud
3. What you're doing now is not working

Laminar

Reason 1

Cloud data security is different than data security

As organizations digitize to compete, the cloud enables them to move faster, be more agile, and process data at amazing speeds to gain new insights. Yet organizations still rely on their on-premises security solutions to support the new paradigm. The hard truth is that these legacy solutions simply won't work in the cloud. The growing frequency of data breaches is clear evidence of this fact. The cloud requires new security solutions, especially data-centric security solutions. We can look to the complementary area of cloud infrastructure security and the emergence of cloud security posture management for evidence of the need for cloud-native security solutions. Now is the time to add data-centric solutions as well.

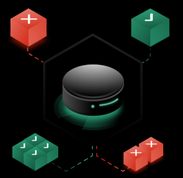
The cloud has brought the issue of security versus utility to a tipping point. Why? Because with the ease with which developers and data scientists can now spin up cloud assets, they hold all of the power. Developers no longer ask for permission when they want to create new workloads or storage assets, they just do it. This means security teams no longer have the visibility or the chance to ask important questions and to implement and enforce policies that can protect the data before that data is copied, moved, or created.

Think of it this way: giving developers free reign in the cloud is like you've handed over the keys to a Ferrari to a 20-something-year-old. Do you really think they have any thoughts of staying safe while they are tooling around in this crazy-powerful machine? No. They do not. Developers are just trying to get where they need to go, in this case, delivering value to the business, as quickly as possible. The result:

1. **Data proliferates -** data is moved, copied, and created instantly.
2. **Change is rapid and constant -** cloud services can be spun up, changed, and moved at the click of a button.
3. **Data access is used freely -** to enable innovation, data must be accessible to the developers and data scientists who need it.
4. **Data is easily exposed -** but this freedom and accessibility also means that data, especially the most sensitive data, is not nearly as secure as it was in an on-premises environment.

In the cloud when data proliferates and changes are constant security teams lose visibility to where the data is and how it is secured. The old adage is true: you can't protect what you can't see. New realities call for new solutions. In this case, the new reality of cloud data proliferation, rapid change, free use, and exposure of data call for data-centric solutions that are purpose-built for the cloud.

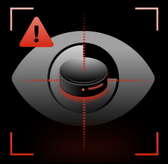
The Four Data Challenges of Cloud



Data proliferates

Change is rapid and constant

Data access is used freely



Data is easily exposed

Reason 2

Tedious manual efforts don't work in the cloud

Let's face it, the old way of manually doing things doesn't work when developers and data scientists can spin up new services at the push of a button. Security breaks down. Compliance suffers. Unfortunately, when data is copied, moved, or backed up, security controls don't travel with it, and they have to be redone. To remain secure, keep up with the pace of innovation and reduce friction between security and DevOps teams—organizations need to automate, automate, automate.

There are five main reasons that manual data security efforts don't work in the cloud and an automated solution is needed:

1. Manual efforts can't keep up with the agility of today's digitally transformed businesses. When done manually, data inventory efforts are out of date days after completion and are not accurate due to employee and contractor turnover.

2. Security is blind to "shadow" data, the hidden sensitive files that occur when data is copied, backed up or housed in a data store that is neither governed under the same security structure, nor kept up to date. In the cloud, this kind of hidden data is all too frequent.

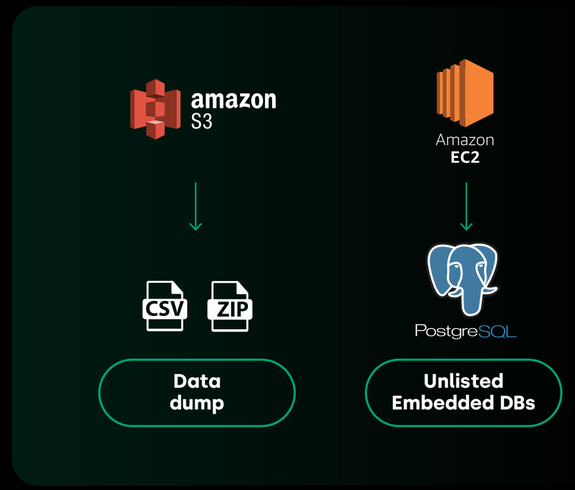
3. There is no way to validate or enforce data security policies. Data security often has to rely on written policies with little to no verification or enforcement. Instead of automated approaches to enforce policies, they have to trust that developers will understand standard policies and properly implement them.

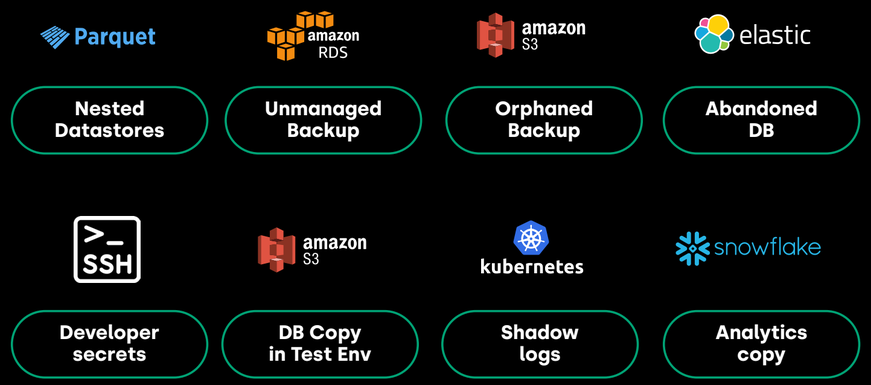
4. Security has no ability to identify "crown jewels" and put proper monitoring in place. Because of the inability to identify the crown jewels the impulse is to turn monitoring on for everything, but that is way too expensive, so the reality is to turn monitoring on for nothing. Manual efforts will never lead to a complete and accurate inventory of your most sensitive data.

5. There is no ability to easily understand exposure at the data element layer and how to limit access. In the cloud, with multiple disparate forms of access control to data that have developed over the last decade, the computation to figure out who has access to a specific data file is exceedingly complicated and an impossible task using manual efforts. Knowing whether "Bob" has access is easy. Knowing everyone who has access and who has used their access is much more challenging.

Shadow data

10 customer examples





Reason 3

What you're doing now is not working

It's a sad fact that while the cloud security spend has increased: estimates tell us that the market is growing at a rate of 25.1% year over year, from $10.98 billion in 2021 to 13.73 billion in 2022, so too has the number of cloud data breaches. As has the cost. The average cost of a data breach in 2022 is $4.35 million, up 12.7% from 2020, and the 2021 Data Breach Investigations Report from Verizon found that 90% of data breaches target the public cloud.

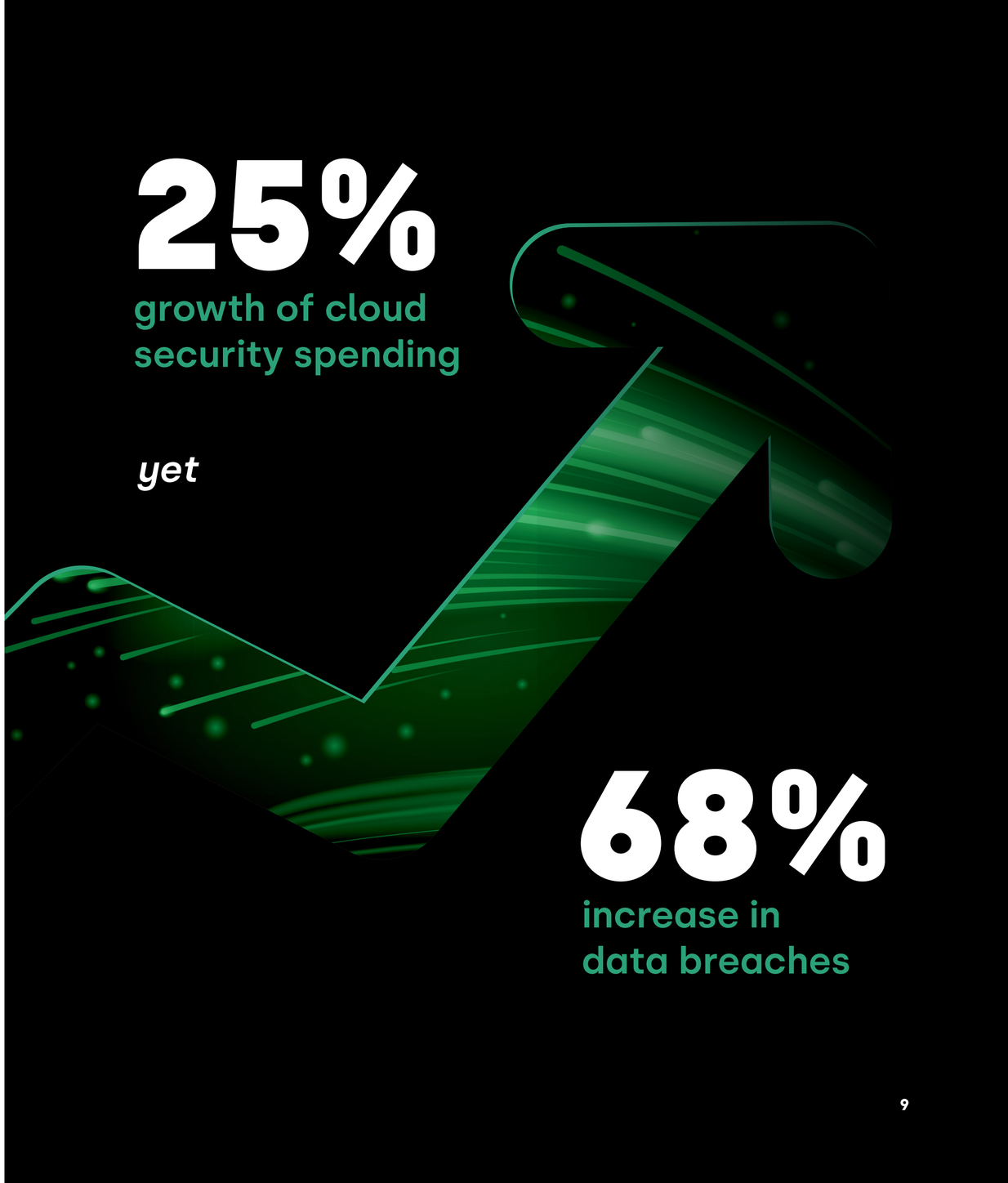
Large brands have come to face this reality: SEGA Europe with their massive data breach after someone inadvertently stored secure, sensitive files in a publicly accessible AWS S3 bucket. Twitter when users' personal information and passwords were stored in a readable text format on the company's internal system rather than disguised by their hashing process. Marriott in their July 2022 data breach, on top of breaches in 2020 and 2014, a pattern of repeated attacks.

If current security tools kept your data secure, wouldn't the number of data breaches decrease over time? Albert Einstein is credited with saying, "Insanity is doing the same thing over and over and expecting different results." So if your current solutions aren't working, isn't it time to consider a completely new approach to protecting your data in the cloud?

Cloud data security is a new, evolving discipline that has emerged to fill the gap in cloud security. Until now, there were either legacy data security solutions that didn't address the cloud or cloud security solutions that only focused on securing cloud infrastructure.

Now there are solutions solely dedicated to keeping your cloud data safe. They are designed to address the challenges of data proliferation in the cloud and discover not just the data you know about but importantly, the data that you don't. In fact, best-in-class cloud data security platforms will prioritize sensitive data that is most at risk, allowing you to focus on what really matters to the business and less on the noise, freeing up your already overburdened security teams for more strategic work. The right cloud data security solution will ensure your organization's data is protected so that we as a collective whole can successfully decouple data growth from data risk.

We bet you haven't tried cloud data security out yet. We think it's time to do so.



It's time to add cloud data security to your 2023 budget

The amount of sensitive data going into the cloud is increasing exponentially and so is your risk—unless you start thinking differently today. Cloud data security is not just a nice-to-have in your security toolkit, but a must-have. So we challenge you—if it's not already in your cloud security budget for the coming year, why not?

Laminar

Why Laminar for cloud data security

Unlike those legacy data security solutions that don't address the cloud or cloud security solutions that only protect your cloud infrastructure but do nothing to protect your data, Laminar's cloud data security platform was purpose-built to discover, prioritize, secure and monitor all your known and unknown data across your multi-cloud environment.

Laminar is the only cloud data security provider to deliver multiple capabilities in a single platform so you don't need to worry about managing siloed point solutions that don't talk to each other and miss the most critical aspect of cloud data security—context.

Our cloud security platform combines:

1. **Data Catalog for Cloud Security** that automates the discovery, classification, and prioritization of cloud data, enabling teams to remediate the security issues that put sensitive data at risk.
2. **Cloud Data Security Posture Management (CDSPM)** that converts data policies into specific technical configurations and uncovers policy violations, prioritizes issues for resolution, and provides actionable remediation recommendations.
3. **Cloud Data Access Control (CDAC)** to visualize and understand which entity or entities have an access path into sensitive data, and which sensitive data can be accessed by which entities.
4. **Cloud Data Detection and Response (CDDR)** that monitors and detects in real time anomalous behavior that may indicate a data leak or potential breach of sensitive data.

And the Laminar platform does all of this autonomously, agentlessly, and continuously without impacting performance or data flow. The platform does not require an agent, does not impact performance, and is implemented using the cloud's APIs in minutes without disruption to production.

Laminar

Contact us →

to talk about how cloud data security can help your organization level up or request a demo of our industry-leading cloud data security platform.