Laminar

# State of Public Cloud Data Security Report 2022

Amidst Shadow Data Explosion and Soaring Breaches, Companies Must Turn to Cloud-native Security Solutions for Better Protection

# Contents


| | |
|---|---|
| Executive Summary | **1** |
| Growing Cloud Data Breaches Put IT and Security in a Defensive Position | **2** |
| Cloud Complexity is Getting Worse, Not Better | **3** |
| The Good News: There's Growing Buy-in for Data Protection among the C-Suite | **5** |
| Data Security Teams May Be Overconfident in Their Abilities and Tools | **6** |
| Cloud Data Demands a Different Security Approach — Cloud-native Tools | **7** |
| The Case for Laminar – Data Security at the Speed of Cloud | **8** |
| Appendix | **9** |

# Executive Summary

Over the past two years, companies' adoption of public cloud services has surged as IT teams enabled hybrid workforces and sped the development of digital products and services. As a result, spending on public cloud services has grown from $270 billion USD in 2020 to an estimated $397B in 2022.[1]

However, that fast-paced transformation was achieved with some compromises. Developers rapidly implemented new models, including hybrid work and cloud, which diluted security observability. As a result, security now lacks visibility into where cloud data is stored, whether data stores contain sensitive information, and if they're adequately protected. These conditions have all created the perfect conditions for cyberattacks.

Companies faced a 50 percent rise in attacks in 2021, and cyber risks are now the number-one concern for businesses of all sizes.[2] What's clear, then, is that companies need a better security strategy to enable digital business growth, while safeguarding their valuable cloud-enabled data stores.

It is against that backdrop that Laminar is proud to announce the release of the *State of Public Cloud Data Security Report 2022*. For the survey methodology and participant demographics, please see the Appendix.

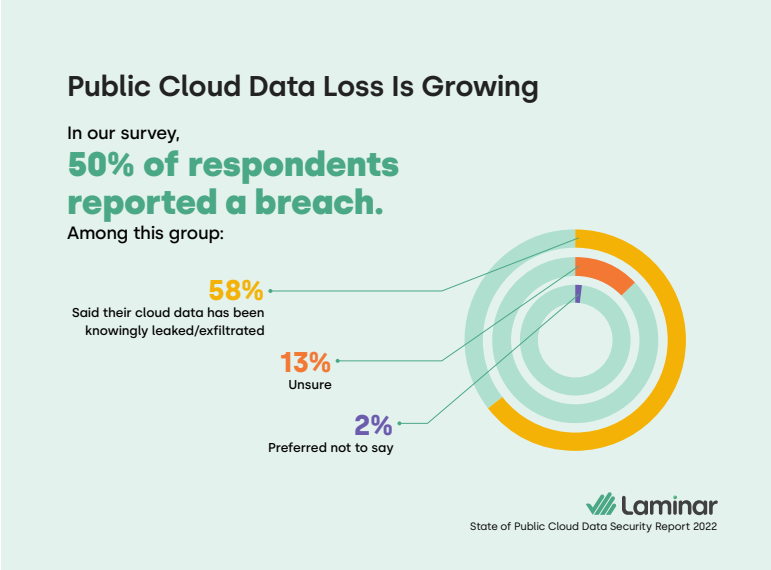
Our report provides compelling insights into the current weak and fragmented state of public cloud data protection and security's concern over lack of visibility. It also demonstrates the need for cloud-native security solutions that can provide full data observability, monitoring, and control across companies' multi-cloud environments.

We hope that these findings spur corporate IT and security teams to rapidly harden controls by adopting cloud-native security solutions to protect their fast-growing wealth of cloud data and related business processes.

Let's dig into the data now.

# Growing Cloud Data Breaches Put IT and Security in a Defensive Position

It's no surprise that public cloud data breaches are growing fast. In our survey, 50 percent of respondents acknowledged that their cloud environments were breached in 2020 or 2021, while 13 percent were unsure. In addition, five percent said they preferred not to answer, likely indicating that they, too, had been breached.




The growing number of data breaches is concerning because both B2B and B2C customers rely on their providers to protect their data and consider organizations' security posture in whether to do business with them.

With large-scale data breaches, cybercriminals are building on past results. They're creating detailed profiles on individuals on the dark web, buying and selling user credentials, and mining data for further vulnerabilities. As a result, cybercriminals are able to commit greater harm or launch repeat attacks by reusing breach data in new ways.

The recent SolarWinds supply chain hack and Microsoft Exchange hack shook many security teams to their core. That's because attackers leveraged multiple breach techniques to compromise literally thousands of organizations across the enterprise, utility, and government verticals.

Along with breach rates, costs of breaches are rising — by more than 10% in 2021 alone. While the typical cost to remediate a breach was $4.24 million in 2021,[3] costs are obviously higher in heavily regulated industries, such as financial services and healthcare.

Successful attacks on cloud providers are worse yet, as they impact scores of customers. That's why threat actors are increasingly targeting cloud providers. Nation states gain access to leading organizations' data and intellectual property.[4] Cybercriminals, on the other hand, gain privileged credentials and other data they can use to infiltrate hyperscalers' customers with ransomware or launch other types of attacks.

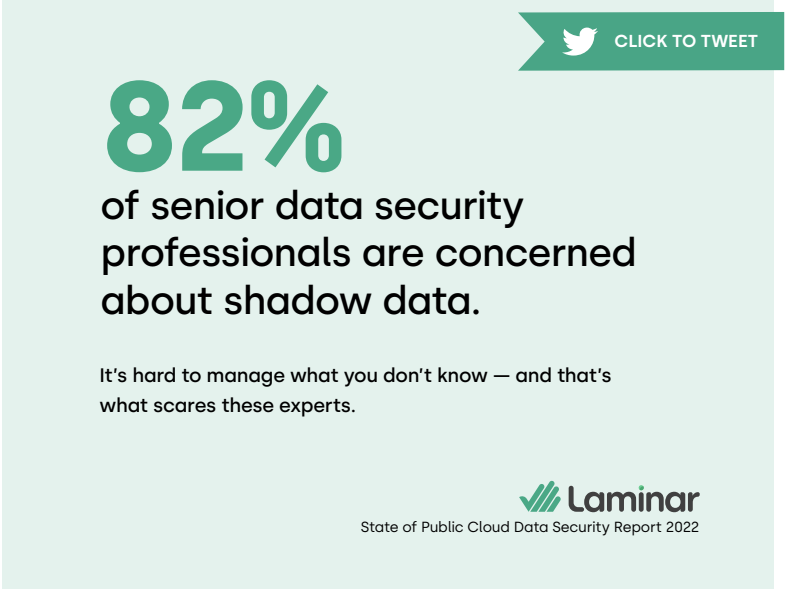
Companies are developing data-centric and zero-trust strategies and architectures in response, and one key place to start is with cloud-native security tools. In the next section, we explore why.

> By 2025, 60% of organizations will consider cybersecurity risk as one of their main criteria in deciding whether to do business with third parties.
>
> Source: Gartner[10]

# Cloud Complexity is Getting Worse, Not Better

Over the past two years, many companies adopted public cloud services to digitize their business and increase operational resilience. In the process, they drove much faster growth.

The five leading cloud providers — Amazon Web Services (AWS), Google Cloud Platform, Microsoft Azure, IBM Cloud, and Oracle — have gained the majority of companies' cloud business. Each of these five hyperscalers offers hundreds of services, meaning that there are literally thousands of cloud services on the market today.




Companies typically engage with more than one vendor to gain access to a broader mix of capabilities, align spending with a chosen vendor's expertise, and reduce risk. In our survey, we found that **56 percent of organizations work with two or more cloud service providers**. As a result, most companies today have cloud infrastructures that are complex by design.

Thus, it's hardly surprising that our survey found 82 percent of respondents are extremely or fully concerned about shadow, or unmanaged, data. That's well-founded, because only 49 percent have full visibility when developers spin up new data repositories. Some 35 percent have partial visibility, while 12 percent have no visibility, and five percent are unsure.

At companies today, both IT and business users can self-provision cloud services and stand up instances for application development and testing. They also use cloud-enabled data every day for a wide array of business purposes. Shadow data now includes database copies in test environments, unmanaged backups, toxic application logs and caches, analytics pipelines, stale unmaintained databases, and unlisted embedded databases.[5] All of these sources create exposure risks if they are not protected and managed proactively.

In our eBook, *How to Achieve Data Protection at the Speed of Cloud*, we note, "All data is accessible from anywhere, given the right credentials or tokens. There's no longer a single choke point to protect and monitor."[6] Thus, data security professionals need to be able to see all data holdings across the public cloud, gaining the ability to discover and classify all sensitive data, in both managed and unmanaged data stores as well as compute.

# How Your Organization Creates Shadow Data

**Shadow data is everywhere. Here are some common reasons your teams create it — and then forget it, increasing your organization's risks of data leaks.**

1. A developer creates a database copy to run a test in a development environment and forgets to delete it.

2. A structured query language (SQL) database is moved to a public cloud in a "lift and shift" project. It then gets refactored into a cloud-managed relational database service (RDS), but the original SQL database is never removed.

3. An application is decommissioned, but the backup database that was associated with the defunct application is left behind.

4. A developer spins up an embedded database inside an Amazon Elastic Compute Cloud (EC2) instance but doesn't tell security. To IT this database looks like a compute instance. These team members don't know that the EC2 instance is actually a data storage source.

Laminar

# The Good News: There's Growing Buy-in for Data Protection among the C-Suite

Among this gloom and doom — growing cyberattacks on cloud services and the rise of unmanaged cloud data — there is some good news. Data protection has joined cybersecurity as a C-suite priority.

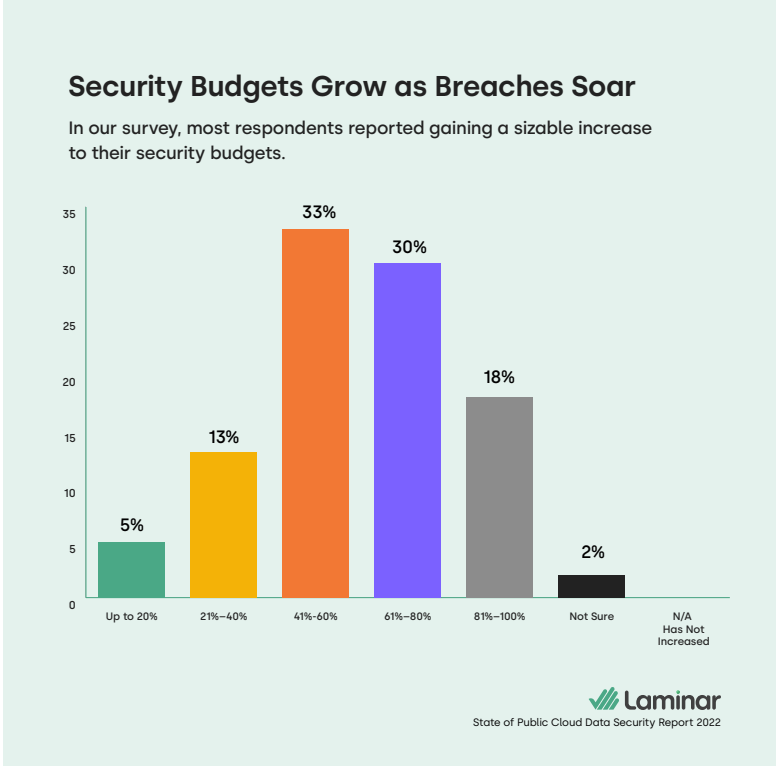
Our survey found that:

- **Executive buy-in is increasing:** The growing number of cloud data breaches in 2020 and 2021 has increased executive and board of directors' buy-in for cybersecurity at 50 percent of the companies surveyed. Some 29 percent, however, say buy-in has not increased. An additional 21 percent don't know, meaning that there is still work to be done to ensure that security teams have the authority they need to evolve key processes.
- **Security budgets have increased:** Given high-profile breaches, it's not surprising that 81 percent of respondents have reported a >40 percent increase in security budget since January 2020. Most of this group has witnessed significant increases, enabling them to rapidly evolve programs. This means that senior leaders truly understand the strategic importance of cybersecurity to enabling and growing a digital business with data at its core and are willing to fund these initiatives.
- **Data protection has its own team:** Finally, data protection is emerging as a key player for the future. Some 58 percent of organizations now have a dedicated team for these efforts. Among this group, 32 percent report to the chief information security officer (CISO), 36 percent report to privacy leaders, and 30 percent report to governance heads. These findings indicate that while data protection's role is emerging, there is no clear consensus yet on the ideal organizational structure and reporting mechanisms for this new function.

All of these developments are extremely positive and will help ensure that data security efforts have the executive sponsorship, visibility, and funding they require to be more successful.

However, this recent success may be creating complacency on the part of IT and security. Let's read on to learn more.

> Some **58 percent of organizations** now have a dedicated team for data protection



# Data Security Teams May Be Overconfident in Their Abilities and Tools

To be human is to often hold opposing positions on the same issue. So, it's not too surprising that our survey found similar disconnects. However, these findings could indicate dangerous overconfidence on the part of data security teams at a time when they should be rethinking their approach amidst ongoing cyberattacks.

Our survey found that 41 percent of respondents say they are fully confident they have total visibility into their public cloud data holdings. That's a rather shocking response given that 82 percent said they were concerned about shadow data. More realistically, 36 percent said that they were somewhat confident, 19 percent of respondents were not too confident, and four percent were not confident at all that they controlled all of their company's data.

Companies are innovating so fast that they are experiencing data sprawl. It's not uncommon for security teams to know about their primary production databases, but lack visibility into other data sources. That means there are typically multiple shadow data stores that are unknown, unmonitored, and can be easily infiltrated by malicious parties.

**65%**

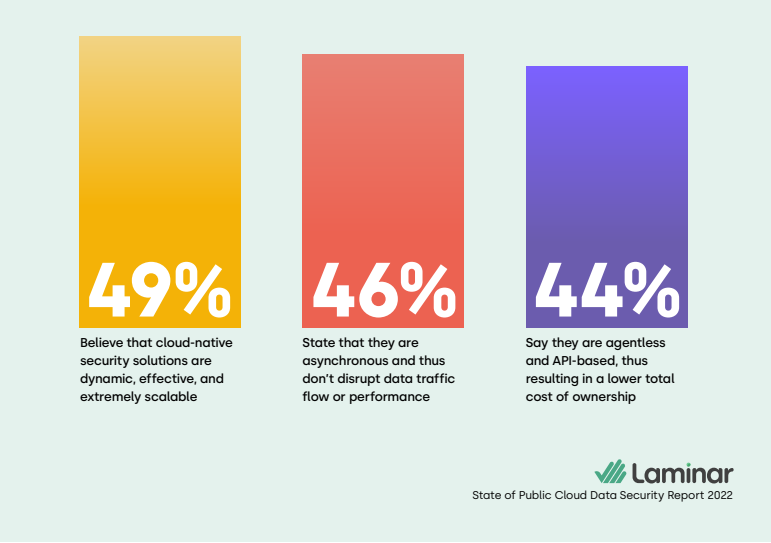
agree that cloud environments are different enough from on-premises infrastructures to warrant unique solutions

That disconnect appears again when data protection professionals are asked about their security solutions. Some 77 percent are extremely (32 percent) or very (43 percent) confident that on-premises security solutions can address cloud data security challenges. Yet 65 percent also agree that cloud environments are different enough from on-premises infrastructures to warrant unique solutions. This latter finding is on the money. Let's explore why.

# Cloud Data Demands a Different Security Approach — Cloud-native Tools

It's clear from our survey that data security professionals are struggling to match pace with cloud data growth. And that predicament will worsen. The amount of corporate data stored in the cloud has now reached 50 percent[7] – and more will be moved to the cloud as companies refactor legacy applications or retire on-premises business applications in favor of flexible and scalable cloud architectures.

It is clear that data professionals understand the benefits of cloud-native security solutions. Our survey found that among respondents:




As a result, 61 percent of data security professionals have now adopted cloud security tools. They are looking for these solutions to address the following data protection challenges:

- **Accommodating diverse storage architectures:** Some 43 percent of respondents want to be able to oversee diverse cloud environments, including hosted, managed and embedded data stores. Using the right cloud-native platform allows data professionals to manage increasing amounts of cloud data, while still tightly enforcing security policies. With cloud-native automated solutions, data security can implement a "trust but verify" approach that enables the business to grow safely.
- **Managing internet-facing resources without a defined perimeter:** Business users love SaaS applications, and their use is outpacing cloud business process and infrastructure growth.[8] Given the business's increasing control over IT spending, data security teams can't and shouldn't try and stop this trend. However, with the right cloud-native platform, data security teams can automatically discover, govern, and secure the data stored in these applications.
- **Reducing shadow data:** With the right cloud-native solution, teams can automatically discover and inventory all of their shadow data, enforce policies and controls, and retire unneeded sources. In addition, prioritized remediation and alerts ensure that teams can proactively focus on high-risk data, quickly reducing the attack surface.
- **Providing developers with self-service capabilities:** Developers need the ability to spin up new data stores safely and securely. Data security teams can allow that, while asynchronously monitoring these new holdings with a platform that doesn't harm data performance. As a result, developer teams can execute process-intensive work, such as running big data analytics, without experiencing latency.

# The Case for Laminar – Data Security at the Speed of Cloud

It's clear from media reports and our survey that companies are in a time of transition. They're rapidly evolving their businesses, increasing their use and dependence on public cloud services and valuable data analytics. Yet, the reality is that 90 percent of data breaches occur in the public cloud.[9]

Data security teams can't put the genie back in the bottle, by reducing their use of public cloud services or consolidating vendors. Nor would they want to: Over the past two years, companies have achieved amazing gains by leveraging cloud services.

Yet, data security teams are mindful that they need to improve their ability to combat cloud data risks. Shadow data is a real and growing problem. The time is now to address it, and the best path forward is to use cloud-native security solutions that are high-performance and scalable; work asynchronously to avoid disrupting data flows; and are agentless and API-based, making them easy and fast to deploy.

However, not all cloud-native security platforms are created equally. Most cloud security tools today are focused on either SaaS apps or infrastructure, but not many are focused on data. That may be why some survey respondents express doubts about their efficacy. Among those who have adopted cloud security tools, 22 percent said they were not too confident these solutions provided the data protection they need, while five percent weren't confident at all.

Laminar provides a cloud-native security platform that's uniquely designed to protect sensitive data for everything you build and run in the cloud. Laminar works with all public cloud infrastructures, all cloud data types, and all data policies. As a result, teams gain a single solution to protect and control their multi-cloud data holdings. Laminar best practices include four steps:

- **Discover** – Data security teams can simply connect Laminar to any and all cloud accounts to gain full data observability and discovery across their entire public cloud stack completly autonomously and without an agent. Laminar characterizes and classifies the data, such as PII or credit cards with contextual validation. Providingcoverage for both managed and unmanaged data stores, as well as compute.
- **Prioritize** – Prioritizes data stores according to sensitivity, volume, data security posture (encryption, retention, configuration, and access controls), and access exposure per the Laminar risk model.
- **Secure** – Laminar enforces data security policy, reducing sensitive data exposure surface. As a result, data security teams can enforce data policies, as well as security best practices. Data context allows for guided remediation of data security posture with one-click controls.
- **Monitor** – Laminar provides asynchronous monitoring of data egress channels continuously and detects unsanctioned or risky activity without interrupting valid data flow.

## Sources


1 **"Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021," press release, Gartner, April 21, 2021,** https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021#

2 **Chuck Brooks, "Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats," article, Forbes, January 21, 2022,** https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/

3 **Drew Todd, "Ponemon Institute: Cost of Data Breach Hits Record High," article, SecureWorld, September 1, 2021,** https://www.secureworld.io/industry-news/cost-of-a-data-breach

4 **Bruce Schneier and Trey Herr, "Russia's Hacking Success Shows How Vulnerable the Cloud Is," article, Foreign Policy, May 24, 2021,** https://foreignpolicy.com/2021/05/24/cybersecurity-cyberattack-russia-hackers-cloud-sunburst-microsoft-office-365-data-leak/

5 **Adir Gruss, "The Largest Threat to Your Data You're Not Aware of is Lurking in the Shadows," blog, Laminar, January 17, 2022,** https://laminarsecurity.com/blog/the-largest-threat-to-your-data-youre-not-aware-of-is-lurking-in-the-shadows/

6 **Ibid.**

7 **"Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2021," chart, Statista, July 30, 2021,** https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/#

8 **"Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021," press release, Gartner, April 4, 2021,** https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021

9 **"Key cloud security statistics that will reshape your cloud perspectives," article, Cybertalk, October 20, 2021,** https://www.cybertalk.org/2021/10/20/key-cloud-security-statistics-that-will-reshape-your-cloud-perspectives/#

10 **Kasey Panetta, "The Top 8 Cybersecurity Predictions for 2021-2022," article, Gartner, October 20, 2021,** https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022

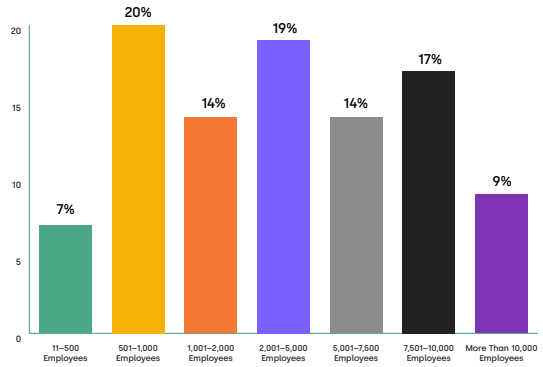

# Appendix

Our survey for the *State of Public Cloud Data Security Report 2022* was conducted in February 2022 by Censuswide.

## RESPONDENT DEMOGRAPHICS

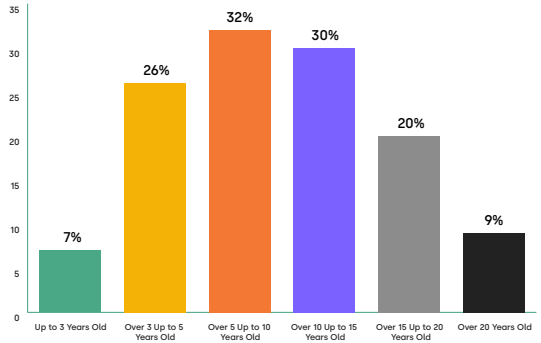
### Company Size

Q: What is the size of the company you currently work for?




### Age of Business

Q: How old is your business?



**ABOUT LAMINAR**

Laminar delivers data leakage protection for everything you build and run in the cloud. Laminar's Cloud Data Security Platform is the first solution on the market delivering data-centric cloud security that allows you to Discover, Prioritize, Secure, and Monitor your sensitive cloud data. Continuously Discover and classify new datastores for complete visibility, Prioritize actions based on data sensitivity and risk posture, Secure data by improving security posture and actively Monitor for egress and access anomalies. Complete data observability for everything running in your public cloud accounts. Both agentless and asynchronous monitoring of datastores, compute as well as data egress channels allows sanctioned data movements and alerts when something's wrong. Data protection teams can reduce the attack surface, detect real-time data leaks and get back in control of their data. 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 find out more please visit laminarsecurity.com.