Laminar

State of Public Cloud Data Security Report 2023

Public Cloud Data Breaches, Shadow Data Concerns Show Steep Rise Over Last 12 Months. To tackle skyrocketing cloud data security issues, 97% of organizations now have a dedicated data security team

Contents

Executive Summary

The race to the cloud is accelerating. Investments are soaring, and hybrid, multi-cloud infrastructures are the norm for organizations today. Public cloud spending in 2022 outpaced estimates by more than $150 billion[1] to reach $490.3 billion in 2022 and is projected to reach $591.8 billion in 2023, according to Gartner. Organizations are accelerating cloud adoption to equip remote workforces, boost innovation, increase business agility, and maintain market competitiveness. By 2025, 95 percent of all new digital workloads will be deployed in the cloud.[2]

However, cyberattacks have also soared, resulting in a growing number of data breaches. Laminar surveyed security professionals for its **State of the Public Cloud Data Security Report 2023**, finding that 77 percent of organizations have had their public cloud data accessed by an adversary over the past 12 months, up from 51 percent the year before. It's no wonder that the World Economic Forum cites cybersecurity as one of the world's seven most pressing risks for 2023.[3]

Also compared to last year, shadow data is taking center stage as the No. 1 challenge in protecting cloud data overtaking both managing varied storage architectures as well as overseeing internet facing resources.

However, there is good news amidst the gloom. Our report reveals that security professionals have a growing awareness of these critical issues and how to solve them, and 97 percent of organizations now have a dedicated data security team to begin to tackle cloud data issues.[4] This is up significantly from 58 percent in 2022.

When compared to last year's results, security professionals have made significant strides in setting up teams and governance to mitigate these risks and increasing budgets to buy solutions and scale security operations. More are now turning to cloud-native security solutions to gain a single, consistent view of data across multi-cloud environments; improve monitoring; and enforce security controls that enable defense-in-depth strategies.

Yet, a contradiction in the research emerges: More respondents had increased visibility into public cloud data stores, yet we saw a significant increase in shadow data worries as 93 percent of respondents are concerned about shadow data, up from 82 percent last year.

Security Professionals:

Shadow Data Worries Grow, Despite Greater Visibility into Public Cloud Data Stores

86%

of respondents said they have increased visibility into public cloud data stores, up from **77%** last year.

80%

of respondents are very confident they have full visibility into all cloud data, up from **77%** who said the same in 2022.

86%

are confident they can see new data repositories, up from **49%** in 2022.

→

Despite this confidence, almost all

93%

are concerned about shadow data, up from **82%** last year.

Security professionals believe that their business is transforming faster than tools and processes can keep pace, creating gaps and vulnerabilities they can't see. As a result, nearly a third of respondents said they can't be certain that publicly exposed buckets do not contain any misplaced sensitive data.

Their concerns are valid. Here's why.

> Two key trends -- the fast pace of cloud transformation and the democratization of data -- have created an innovation attack surface, or a growing number of entry points for attackers to access company data.

The innovation attack surface is a new threat vector that most organizations unconsciously accept as the cost of doing business. It refers to the continuous unintentional risk cloud data users, such as developers and data scientists, take when using data to drive innovation. In contrast to traditional attack surfaces determined by external forces (including bad internal actors) seeking to exploit vulnerabilities to gain illicit access to protected information, the innovation attack surface results from the massive, decentralized, accidental risk created by the smartest people in the business.

This is driven by multiple trends, including:

- **Cloud storage use is growing:** Organizations are adopting cloud storage services across multiple vendors. These technologies are often configured differently, resulting in numerous architectures that are hard to manage, are constantly changing, and require deep cloud expertise.
- **Data is proliferating:** Developers are spinning up or copying entire data stores at will in the cloud, resulting in fast-growing data volumes, including shadow, or unknown, unmanaged data stores.
- **The traditional perimeter is now dead:** Organizations are managing expansive core-to-edge networks, where data is easily accessible to global users. As a result, the risk of sensitive data exposure is growing.
- **Software release cycles are faster:** Release cycles are now happening in weeks, days, and hours rather than months or years. Security teams are either left out of the development processes or have to respond quickly to ensure that ready-to-release code adequately protects data.
- **Security's role is changing:** Security must protect data without hindering innovation. However, security teams are chronically understaffed and may lack the bandwidth to keep up with rapid changes in cloud data technology.

Gaps are emerging, including misconfigured or abandoned cloud data stores; misplaced data; and other issues that attackers are exploiting to access cloud services and exfiltrate data. OWASP says that security misconfigurations plague up to 90 percent of the web applications it's tested.[5]

Humans are often implicated in attacks, either due to malicious intent, negligence, or errors. The "human element" continues to be the root cause of most (82 percent) of all attacks.[6] However, humans make mistakes and require process and technology to enforce guardrails that reduce risk and enforce proper preventive controls.

With breaches rising, there is clearly work to be done if organizations are to reduce attack surfaces, repel malicious access attempts, and protect their data and intellectual property.

We hope that our research helps security teams make a strong case for prioritizing public data security for the cloud and deploying cloud-native solutions to protect their organizations' fast-growing data and analytics wealth.

Let's look at the results now.

Increasing Visibility into Public Cloud Data Holdings

As organizations deploy multi-cloud infrastructures, their data landscape is becoming more complex and difficult to manage. Business teams are using SaaS applications that access corporate data in the cloud, DevOps teams are spinning up database instances and creating multiple versions of cloud data, and data teams are creating data lakes to enable cloud-based analytics. Data is now everywhere. In addition, organizations are in the early stages of empowering business teams to create their own big-data analytics and data mesh solutions.

The pace of change and relentless rate of data innovation are increasing organizations' innovation attack surfaces. Previously, security teams enforced perimeter controls with on-premises systems. Now, they must protect cloud data that is highly distributed, across actors, infrastructure, and applications and extremely dynamic, being constantly created, moved, modified, analyzed, and deleted. And while the traditional attack surface was determined by outside-in activity, the new risk environment is being created by inside-out activities -- legitimate internal actors who are creating new data risk as an unintentional byproduct of value-creating activities.

Despite this challenging new reality, security teams have made significant progress since last year.

Claims of visibility up

In 2023, **86% of respondents**

said that they now have complete visibility into new data repositories, up from 49% in 2022

But respondents know they don't know.

That progress is good news.

However, teams know that shadow data -- and their organizations' innovation attack surface -- is increasing due to data proliferation spurred by the pace of change and agility of cloud technologies.

These challenges will only increase due to the fast rate of change. Organizations have accelerated transformation strategies to stay competitive. That means more data workloads proliferating in the cloud at a faster pace, leaving security struggling to catch up.

> This is called the **security execution gap** -- the divergence between agile cloud data activities that contribute to innovation and the static and manual data security activities intended to protect the business. And it is only getting wider.

As a result, the problem of shadow data in the public cloud is increasing exponentially. Teams need a cloud-native data security solution that is agile and will scale with data volumes and monitor and manage cloud data wherever it's located -- across multi-cloud storage technologies, in analytics pipelines, or even in cloud storage recycle bins.

Setting Up Dedicated Data Security Teams

Most organizations now have dedicated teams to oversee public cloud data security programs, as CISOs seek to combat rising risks and threats.

These findings indicate that leaders realize the scope of their public cloud data security problem and are investing in people to address it. Data and cloud security teams can work together to ensure the proper monitoring, maintenance, and remediation of public cloud data, but only if they have the right tools to support this important mission.

C-suite leaders like the CISO and CDO can champion the cause of cloud data security to the board and other members of the senior leadership team. By doing so, they can gain long-term stakeholder support, budgets, and the authorization to continually enhance tools and skills to safely enable data innovation at the same time rappelling attacks and preventing devastating data breaches.

Staffing Up to Solve the Data Security Challenge

In 2023,

97% of respondents

reported that they had a dedicated data security team,

up from

58 percent in 2022.

Understanding Shadow Data Risks

Do data and cloud security teams know what they're up against? Our survey asked respondents if they knew what shadow data is. Shadow data is organization data that is copied, backed up or housed in a data store that is not governed, under the same security structure, nor kept up-to-date by security or IT.[7]

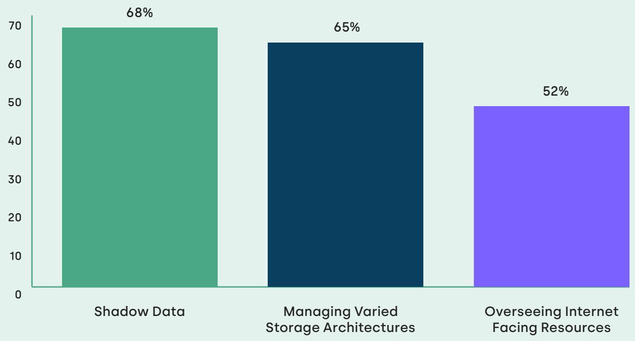
Here are some different ways shadow data occurs across organizations.[8]

- **Copied data lives on in test environments:** Most organizations maintain partial copies of production or databases in development or test environments. Developers may take a snapshot of data but fail to properly remove or secure copied data. Or they may forget about it altogether.
- **S3 backups disappear from view:** Organizations maintain at least one backup data store, which provides an exact copy of production data that can be restored in the event of a breach or operational issue. However, these backup data stores are often less well-monitored and maintained than active data stores.
- **Legacy data isn't deleted after a cloud migration:** After moving on-premises databases to modern cloud data stores, teams may forget to delete legacy data.
- **Data logs can become toxic:** Developers and log frameworks inventory sensitive data. This activity creates sensitive files that are not classified as sensitive. These files can be easily exposed because they lack proper access control and encryption.
- **Data is stored in analytics pipelines:** Many organizations will store data in an analytics pipeline created using Snowflake or AWS, so that they can easily access and run analytics on demand. These can be out of sight of the application/business owner.

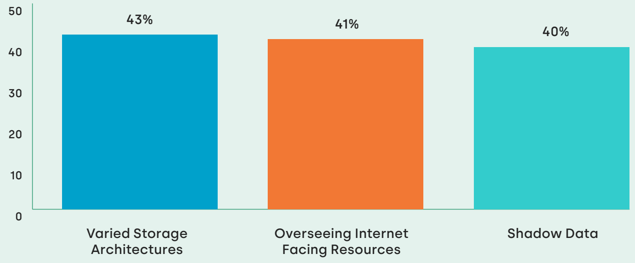
The Growing Risks of Shadow Data

#1 Risk up from #3 in 2022

Two-thirds of security professionals say that shadow data is the greatest challenge to protecting cloud data



2022:



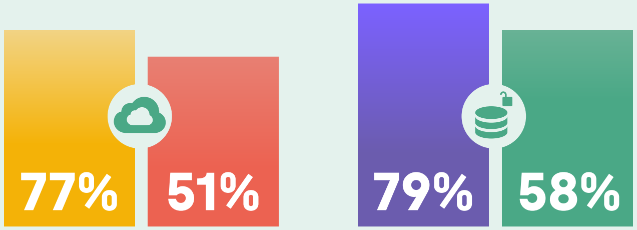
Rising Data Breaches Challenge Security Professional Confidence

We shared earlier that respondents said they had growing confidence they could see new data stores and all cloud data, but that almost all were concerned about shadow data risks. We also shared evidence that a third aren't confident that publicly exposed buckets don't contain any misplaced sensitive data. Rising data breaches are revealing the limits of security professionals' confidence.

This finding indicates that organizations' current strategy of racing to the cloud without implementing next-generation security controls isn't working. It's likely that current security solutions don't actually provide holistic visibility and may lack the full set of tools organizations need to prioritize and remediate the sensitive data stores most at risk for exposure.

Another group is likely more realistic about the scope of the public cloud data management challenge. One in five (20 percent) of security professionals said that they are only somewhat or not very confident that they have full visibility into their public cloud data stores. Last year, 23 percent said the same, meaning that visibility worries are mitigating slightly.

3 in 4 Organizations Hacked in 2022



More than three-fourths (77 percent) of respondents said their organization's public cloud data has been accessed by an adversary in the last 12 months, versus 51 percent the year before.

Of those who were breached recently, 79 percent were aware that data had leaked or been exfiltrated versus 58 percent the prior year.

Responding to Possible Cloud Data Exfiltration

Security professionals' rising concerns about shadow data are well-placed. When Laminar Labs scanned public-facing cloud storage buckets, we were able to detect sensitive personally identifiable information (PII) in 21 percent of these buckets.[9]

Exposed data is obviously at significant risk for exfiltration by a malicious party. So, what happens when the worst happens?

> Unfortunately, 20 percent of security professionals say they are only somewhat confident that their organization will be able to respond to an incident in a timely and efficient manner.

They're likely aware that their current security practices won't be able to keep pace with cyberattackers' more sophisticated strategies.

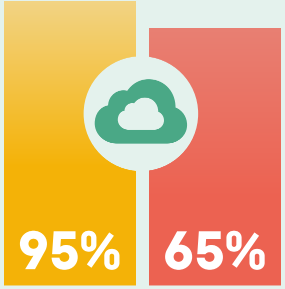
An IBM data breach report found that 43 percent of respondents are still in the early stages or have not started applying security practices across their cloud environments. When these organizations are breached, they pay $660K more in clean-up costs than those who have more mature security processes for cloud environments.[10] And those organizations that use automation had a 74-day shorter breach lifecycle and saved more than $3M than those who didn't have those capabilities.[11]

Investing in Better Cloud-Native Data Security Solutions

With breach rates rising, the pressure is on to improve cybersecurity tools and practices. While hyperscalers provide infrastructure security, organizations must secure their own cloud data.

Security professionals realize that they need fit-for-purpose tools to create full data observability, monitoring, and control across their multi-cloud environments. Cloud-native systems enable agile data security across growing cloud infrastructures, whereas legacy on-premises systems are connector-based and are not equipped for cloud sprawl.

Settling the Debate over Cloud Versus On-Premises Systems



Nearly all (95 percent) of respondents believe that cloud environments are different enough compared to on-premises ones to require unique solutions, up from 65 percent in 2022.

In addition, nearly all (92 percent) of respondents say that the uptick in cloud data breaches has increased executive and board level buy-in for best-of-breed cybersecurity platforms, up from 50 percent in 2022. It's likely that many leaders and teams have learned the hard way that their legacy tools aren't up to the challenge of securing cloud data. In addition, they may realize that breach clean-up costs vastly exceed the cost of deploying fit-for-purpose cloud-native data security solutions.

> As a result, two-thirds (66 percent) of organizations have increased security budgets by 41 percent or more in the past year. However, that figure is down year-over year, as 81 percent of organizations had increased budgets by this amount in 2022.

CISOs may be trying to do more with less in this challenging economic environment, as many organizations are cutting costs and focusing on operational improvements over enhancing business capabilities. Solutions that leverage automation, like cloud-native solutions for data security, improve workforce productivity, enhance operational efficiency, and save money.

The Industry's Need for Data Security Posture Management (DSPM) Solutions

Nearly a third (29 percent) of respondents say they are only somewhat or not very confident that their existing on-premises security solutions can meet the challenges of improving cloud data security, up from 24 percent in 2022. This finding indicates that security professionals have a growing awareness that cloud-native solutions are required to combat the growing problem of data security.

A recent Gartner report on data security posture management (DSPM) describes the business, technical, regulatory, and security risks that can occur when cloud data isn't effectively secured and controlled.

"Identifying meaningful data risk is impossible to solve without combining metrics from data sensitivity, data lineage, infrastructure configurations that create data risks and access risk into a common view," states Gartner[12]

> The emerging field of DSPM "provides visibility as to where sensitive data is, who has access to that data, how it has been used and what the security posture of the data store or application is."
>
> Gartner.

Although DSPM solutions have "transformational" capabilities, they have been adopted by just 1% of the market to date.[13]

When asked who should oversee new DSPM solutions,

41%
of survey respondents

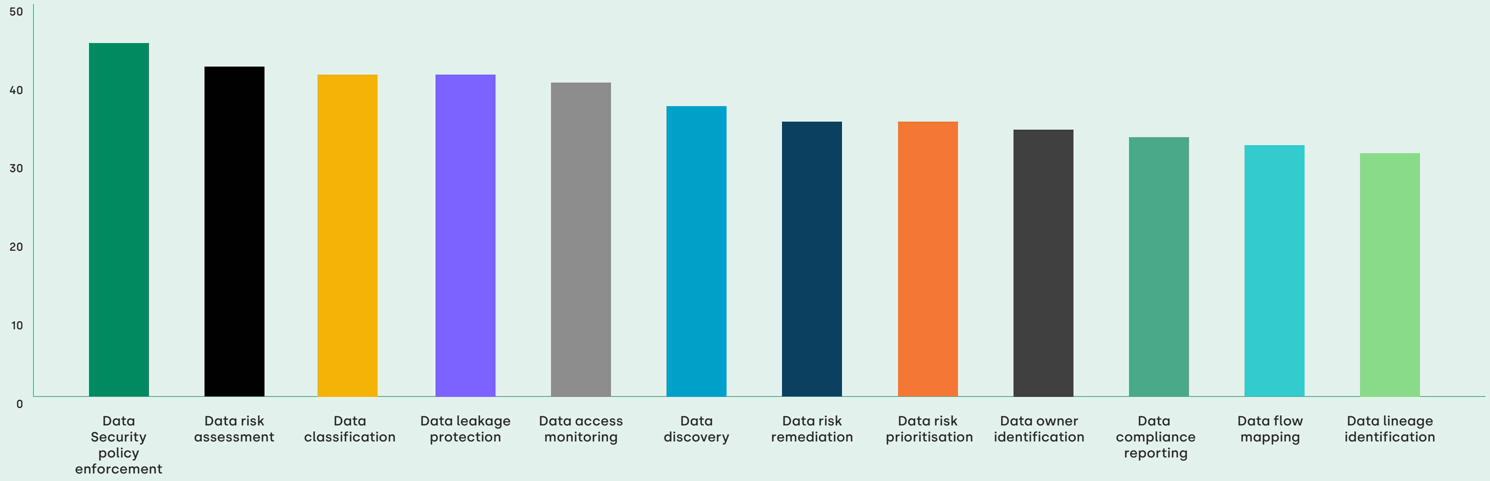
said that data security would be the appropriate primary owner.

This finding indicates leaders' evolving thinking that cloud data security risks are significant enough to warrant their own team and tools.

Capabilities a DSPM Solution Should Provide

Respondents said they need 12 different capabilities from a DSPM solution. Organizations can use these criteria to vet new solutions to see if they can handle their full set of public cloud data security requirements.

What are the components of a DSPM solution?



Advantages of Deploying Cloud-Native Security Solutions

Security professionals are right to question whether on-premises security solutions are up to the challenge of managing ever-growing, constantly moving data stores across multi-cloud infrastructures. As a result, they're taking a fresh look at cloud-native security solutions.

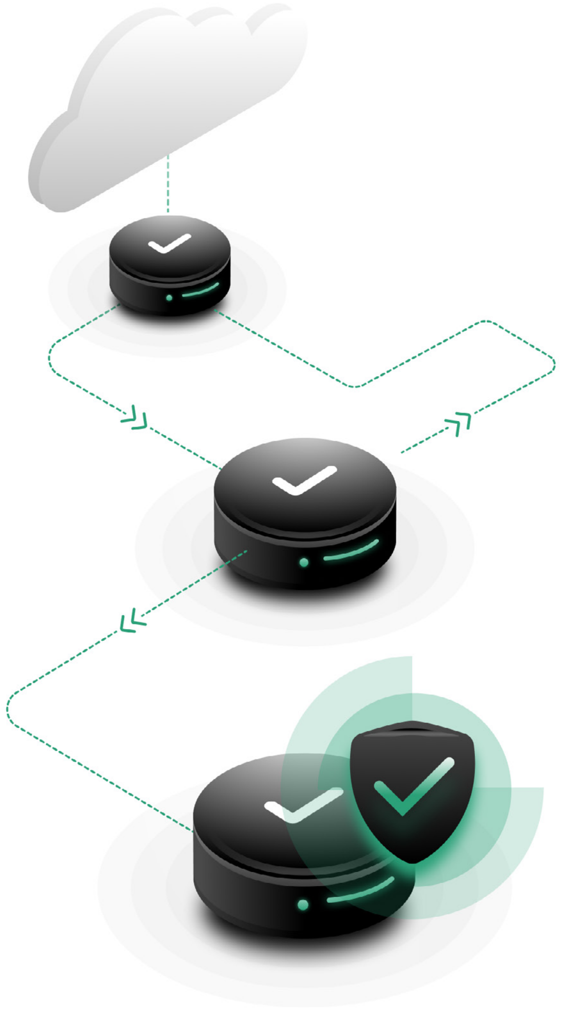
Survey respondents said the benefits of adopting these platforms include:

- **Enabling autonomous scanning:** Nearly three-quarters (71 percent) of respondents said they need a cloud-native security solution to run independently and not require any ongoing setup, maintenance, or configuration. The solution should automatically discover and classify all cloud data assets across multi-cloud infrastructures, including shadow data. (This question was not asked in 2022.)

- **Providing a dynamic, performant platform:** Nearly two-thirds (63 percent) of respondents want to deploy a highly reliable, scalable platform that can accommodate fast-paced cloud adoption and cloud data growth. In 2022, 49 percent of respondents felt the same.

- **Offering asynchronous operations:** More than half (54 percent) of respondents said that the cloud-native security solution should operate asynchronously to avoid performance impacts that harm data availability and usage. In 2022, 46 percent of respondents agreed.

- **Providing an agentless architecture:** As API-based solutions, agentless cloud-native security solutions offer a lower total cost of ownership compared to installed on-premises solutions. That quality is valued by 53 percent of survey respondents versus 44 percent in 2022.



Why Choose Laminar to Protect Cloud Data

After years of torrid cloud adoption and data growth and rising breaches, security leaders and teams are increasing their efforts to protect cloud data. They rightly recognize faster cloud adoption as the path to future-proofing their organizations' business models. However, security professionals also understand that they must become more agile to meet business, regulator, and customer expectations for safeguarding cloud data.

Legacy, on-premises solutions that are connector-based aren't equipped to meet the challenge of discovering, monitoring, classifying, and prioritizing data assets by the risk they present. Only agile, cloud-native security platforms can handle these mission-critical tasks.

As the leading enterprise DSPM provider, 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.

Cloud-Native Platforms Protect Data, Enabling Teams to Innovate More

Laminar's mission is to help teams close the security execution gap by protecting data and empowering value creators to innovate faster and safer than their competitors. Our DSPM solution marries environmental agility with the controls required to safeguard sensitive, regulated, and proprietary data in the cloud, closing this gap.

As a result, developers and data scientists can innovate freely, creating new products and services with public cloud data, while CISOs improve security outcomes and get to focus on other strategic priorities.

Request Demo

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] "Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences," press release, Gartner, November 10, 2021, https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences

[3] Gayle Markovitz, "Global Risks Report 2023: We know what the risks are - here's what experts say we can do about it," blog, World Economic Forum, January 11, 2023, https://www.weforum.org/agenda/2023/01/global-risks-report-2023-experts-davos2023/

[4] For information on the Laminar survey respondent demographics, please see the Appendix.

[5] "OWASP Top 10," website list, undated, https://owasp.org/www-project-top-ten/

[6] https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

[7] Dan Eldad, "How to Combat Shadow Data—The Data Security Risk Lurking in the Shadows," blog, January 7, 2022, Laminar, https://laminarsecurity.com/blog/the-largest-threat-to-your-data-youre-not-aware-of-is-lurking-in-the-shadows/

[8] Ibid.

[9] Gali Lazarovsky, "New research finds that 21% of publicly facing cloud storage bucket contain sensitive PII data," blog, Laminar, November 17, 2022, https://laminarsecurity.com/blog/new-research-finds-21-of-publicly-facing-cloud-storage-buckets-contain-sensitive-pii-data/

[10] "IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High," press release, IBM, July 27, 2022, https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High

[11] "Cost of a data breach 2022," IBM website, https://www.ibm.com/reports/data-breach

[12] Brian Lowans, 2022 Gartner Hype Cycle™ for Data Security Report, pages 7-8, Laminar website, https://laminarsecurity.com/forms/gartner-hype-cycle-for-data-security-all/

[13] Ibid.

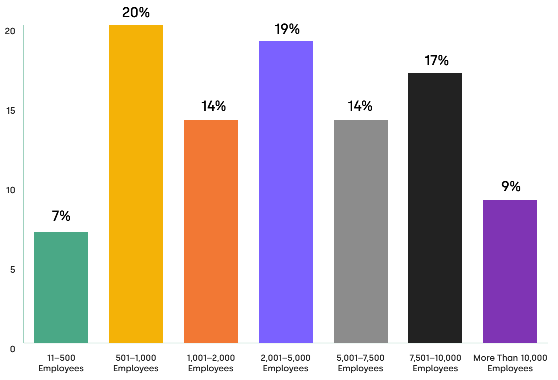
Appendix

Our survey for the *State of Public Cloud Data Security Report 2023* was conducted in February 2023 by Censuswide.

RESPONDENT DEMOGRAPHICS

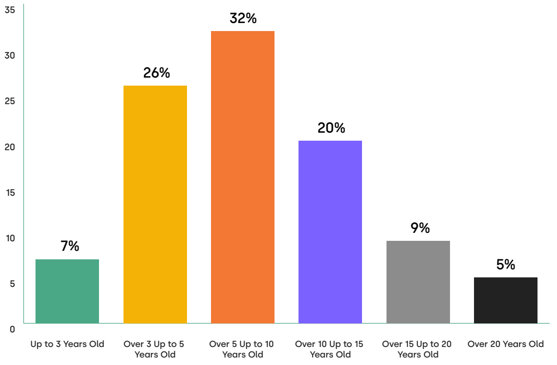
Company Size

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



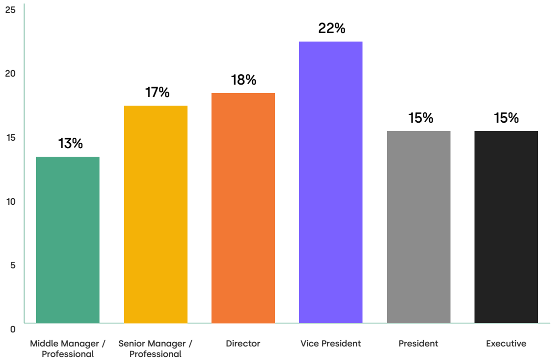
Age of Business

Q: How old is your business?



Level of Employment

Q: What is your current level / status of employment?



ABOUT LAMINAR

Laminar is the leading agile data security platform and provides organizations the visibility and control they need to achieve data security, governance, and privacy in the cloud. Our cloud-native Data Security Posture Management (DSPM) solution continuously discovers and classifies all cloud data, structured and unstructured, across managed and self-hosted data stores, including unknown shadow data, without the data ever leaving your environment. It analyzes access, usage patterns, and security posture, and provides actionable, guided remediation for data security risk. Laminar connects to your multi-cloud environment including AWS, Azure, GCP, and Snowflake via APIs and is agentless, asynchronous, and completely autonomous. To find out more please visit laminarsecurity.com.