

WHITE PAPER

# Cloud Data Security Strategies for 2023

By Jack L. Poller, Senior Analyst  
Enterprise Strategy Group

May 2023

# Contents

What Comprises an Effective Framework for Cloud Data Security? .....	5
Protecting Cloud Data Demands a Platform that Combines All of These Capabilities .....	6
The Laminar Cloud Data Security Solution .....	7
Conclusion .....	7

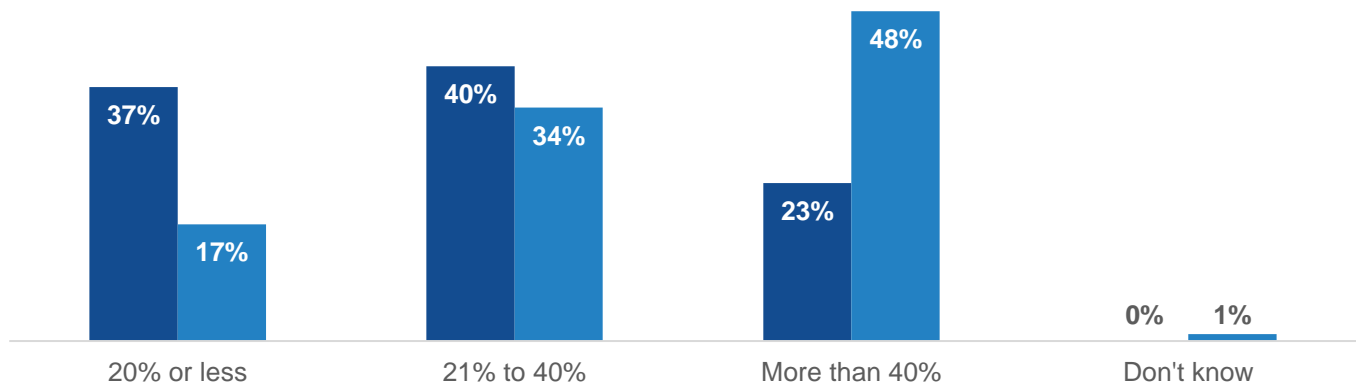
## Cloud Security Is a Focal Point

Organizations are moving rapidly to the cloud, and according to research from TechTarget’s Enterprise Strategy Group, the growth of cloud resident applications will continue: Currently, only 23% of organizations reported that more than 40% of their applications are cloud resident, but in the next three years, 48% of organizations expected to have more than 40% of their application in the cloud (see Figure 1).<sup>1</sup>

**Figure 1. Public Cloud Usage Is Ubiquitous, and Usage Is Deepening**

**Of all the business applications used by your organization, approximately what percentage is currently public cloud-resident? How do you expect this to change – if at all – over the next 36 months?**  
(Percent of respondents, N=742)

- Percent of applications that are public cloud-resident/delivered today
- Percent of applications that will be public cloud-resident/delivered 36 months from now



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

However, securing cloud-resident data has not kept up with infrastructure or application security. Unlike on-premises environments, the cloud environment is constantly and rapidly changing in response to the needs of the business and the use of agile methodologies. Further, analytics, data re-use resulting in data sprawl and multiple silos of data, the ever-increasing volume and velocity of data, and the use of APIs to expose data impose new and different security challenges.

The megatrend of data democratization, where more individuals and accounts gain valuable insights from the use of data, is vital for business innovation. However, this results in more data, in more places, used by more people, and creates a more difficult security challenge.

Lost data, whether exfiltrated by an external attacker or inadvertently corrupted or maliciously exploited by an internal worker, can be catastrophic to an organization. The reputational risk of data leaks, compliance and regulatory penalties, and other negative results from data loss cannot be ignored.

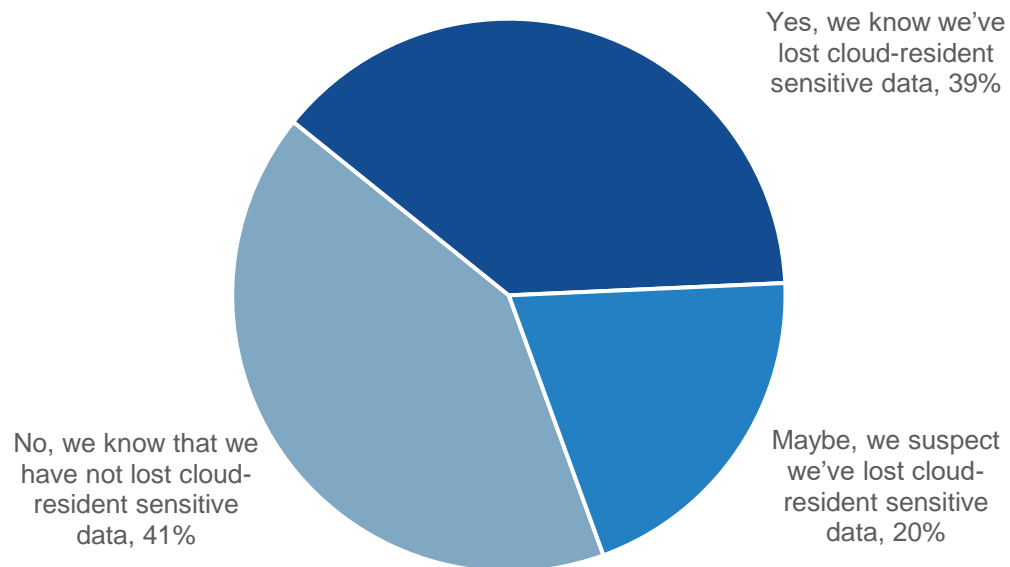
<sup>1</sup> Source: Enterprise Strategy Group Complete Survey Results, [2023 Technology Spending Intentions Survey](#), November 2022.

As with applications moving to the cloud, more sensitive data is moving to the cloud. According to Enterprise Strategy Group research, 31% of organizations said that more than 30% of their cloud-resident data is considered sensitive today. With the rapid shift to the cloud, 67% of respondents said that more than 30% of their cloud-resident data will be sensitive in the next two years.<sup>2</sup>

The cloud data security gap is a very real problem. More than half of respondents (56%) said they believed that between 21% and 50% of their sensitive data in the cloud is insufficiently secured. Further, as shown in Figure 2, data residing in the cloud is often lost. Worse yet, one-fifth (20%) of respondents believe they have a problem with losing sensitive data, but don't know for sure because they haven't deployed adequate security controls.<sup>3</sup>

**Figure 2.** Loss of Cloud-resident Data

**Has your organization experienced any data loss of its cloud-resident sensitive data the last 12 months? (Percent of respondents, N=387)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Securing data in the cloud is difficult because cloud environments are exceptionally dynamic, data usage is unrestricted, and the cloud erases the concept of an easily defensible perimeter. Cloud data storage architectures are more complex, intertwined, and change rapidly as cloud service providers (CSPs) develop a multitude of different storage solutions, each with its own set of controls and configurations, for different use cases. These challenges cannot be met by existing legacy data security solutions or cloud infrastructure security tools. Organizations need a new set of controls and automated processes designed and purpose-built specifically for protecting data in the cloud.

A data security platform built for the cloud must address four important challenges unique to cloud:

- **Visibility**—Organizations need to have visibility into all data repositories in the cloud, regardless of repository type (files, databases, data warehouses, data lakes, etc.). Unfortunately, the cloud lends itself to the rapid proliferation of data stores and data copies, and this can result in shadow data—any data that is unknown, not

<sup>2</sup> Source: Enterprise Strategy Group Complete Survey Results, [The Cloud Data Security Imperative](#), April 2023.

<sup>3</sup> Ibid.

governed, has no oversight, and may not be kept up to date. Because it is unknown and ungoverned, shadow data is not subject to standard security policies and controls and is at greater risk of loss or exfiltration.

- **Classification**—Agile methodologies and the rapid proliferation of new applications, services, data store types, data stores, and shadow data makes it hard for security practitioners to classify data and identify data owners, both of which are critical pieces of information necessary to develop and apply the correct security policies.
- **Access governance**—The cloud makes it easier for users to access more of the organization's sensitive data. And developers are continuously creating new business apps and services that use and analyze vast swaths of sensitive data. The volume and speed of data access, often by machine or service accounts, makes it difficult for security teams to correctly identify and attribute activity (i.e., determine who accessed what data and when).
- **Data leak detection**—Legacy data security was based on the concept of a well-defined perimeter. By placing controls at perimeter crossing points, the security team could catch inadvertent or malicious data loss. The cloud, however, has an amorphous perimeter that is constantly changing with new apps and services. This makes it harder for security controls to detect when data has left the organization.

## What Comprises an Effective Framework for Cloud Data Security?

At the outset, organizations have a fundamental need for a single, cloud-native, comprehensive framework/stack that works across all cloud services, providing automated, always-on monitoring of their environment. A single stack, natively integrated into an organization's cloud, delivers consistent protection and reporting to reduce operational complexity and ensure comprehensive protection. Using different, unrelated, and siloed security tools can result in unexpected gaps in coverage. Consistent application of data security policies is also an important part of meeting many compliance and regulatory requirements.

Protecting data, not infrastructure, is the focus for cloud data security. These are two different use cases: Infrastructure-centric security ensures the cloud infrastructure configuration is secure and maintained, regardless of the data that it contains, while data-centric security ensures data is secure, regardless of where or how the data is stored and ensures data security policies move with data. Both infrastructure-centric and data-centric security are necessary for effective protection.

Protecting cloud data includes several critical capabilities:

- **Continuous and autonomous discovery and classification of data**—This is essential to successfully protecting the data, and without this information, organizations will have blind spots, making data much more vulnerable. You can't protect what you can't see, and data security teams have lost visibility of where their company's sensitive data lies in the cloud. The ease and speed of creating and copying data in the cloud demands both autonomous and continuous discovery, as manual processes cannot keep up.
- **Consistent application of infrastructure-agnostic data security policies**—Ensuring that cloud data is secure regardless of where it's stored or how it proliferates is necessary and differs from on-premises approaches. The cloud makes it easy for users and developers to create or copy data stores. But are these new data stores protected with the correct security policies? Today, there is no automated way to verify that policies are consistently and comprehensively applied, leading to gaps in security.
- **Fine-grained access controls**—These controls are necessary due to the flexibility, complexity, and power of cloud infrastructure. Administrators can create elaborate rules and policies to strictly control access. However, this complexity makes it difficult for an administrator to understand exactly who can access any data object. Further, access is often automated, and it can be hard to decode access privileges for machine or service accounts. Because of the structure of cloud identities and privileges, it can be difficult, if not impossible, for a

security practitioner to answer the question, “Who can access personally identifiable information (PII) records across all data assets?”

- **Data-centric detection and response**—Having the context through monitoring to detect anomalous changes to data or access patterns ensures that the data security controls can rapidly detect potential attacks. Data visibility and classification are prerequisites for monitoring—the organization needs to identify their most critical and sensitive data—their crown jewels. This helps to allocate resources, as monitoring all data can be cost prohibitive and generate too many inconsequential alerts, and monitoring too little data can leave critical data stores unprotected.

## Protecting Cloud Data Demands a Platform that Combines All of These Capabilities

An effective cloud data security platform combines four fundamental capabilities: cloud data landscape, a data security posture management engine, data access governance, and data detection and response. Together, these form a cohesive cloud data security strategy. But to be truly effective, all four capabilities must be present.

- **Cloud data landscape**—Securing sensitive data starts with the process of cataloging the data and identifying all data stores in the cloud. It is imperative that organizations identify all unknown and unowned data stores. The next step is to classify the data, identifying at a gross level if it is sensitive and then further refining into specific categories such as PII, financial, account numbers, etc. The goal is to answer questions about the data, including the key questions, “What data is stored in the cloud?” and “Where is that data?”

The scale and dynamic nature of the cloud demands automation and autonomy. The solution must continuously discover new data stores regardless of type (e.g., databases, files, object storage, data embedded in apps, etc.) and classify and catalog the data. Discovery and classification need to be cloud-native and agentless, as the cost and complexity of maintaining agents in dynamic cloud infrastructures is untenable.

- **Data security posture management (DSPM)**—DSPM provides a set of controls and policies that ensure data always has the correct security posture regardless of the infrastructure or how the data moves or is copied. DSPM is similar to cloud security posture management (CSPM). While CSPM focuses on the posture of the cloud infrastructure, DSPM focuses on the security posture of the data.

The core of DSPM is a data-centric policy engine that ensures the correct policies are applied to all data at all times. This includes the necessary governance and compliance demands for specific data types. For example, one policy might require that all PII is encrypted, regardless of where or how the PII is stored. DSPM ensures that this policy is enforced even when the PII data is copied or a new data store containing PII is created.

DSPM must support fine-grained policies to detect and prevent overexposed, under-protected, misplaced, and unmanaged/unprotected data. DSPM will send alerts when it detects policy violations, and security analysts need to be able to incorporate measures of risk into policies and alerts to aid in triaging and prioritizing responses.

- **Data access governance (DAG)**—DAG answers the question of which entities have access to specific data elements and data stores. Cloud access control technologies have evolved over the years, and current access controls provide multiple overlapping options for defining and maintaining element access. Thus, using visualization to understand which entities have access to data elements or the full scope of data makes it easier to protect data. For example, when a DSPM has found a case of overexposed data via third-party access, the security analyst will also need to know who else has access and what else that third party can access. DAG can help visualize the answers to both questions, simplifying the investigation and mitigation of the issue.

DAG is similar to cloud infrastructure entitlement management (CIEM). While CIEM focuses on access to the cloud infrastructure, DAG focuses on access to the data.

- **Data detection and response (DDR)**—DDR monitors how data is currently being accessed and used and alerts on behavior that is indicative of data loss or the possibility of a breach. It is imperative that the organization identify and prioritize monitoring the most critical and sensitive data. Monitoring all data will consume precious resources and create too much noise with immaterial alerts regarding unimportant data.

DDR needs to detect issues and provide alerts in real time to enable security or operations teams to respond quickly and terminate data exfiltration attempts as soon as possible. Response teams can use DDR data access logs as well as DAG access visualizations to triage and prioritize alerts as well as respond to and mitigate security incidents.

## The Laminar Cloud Data Security Solution

Laminar's Cloud Data Security platform works across the major cloud services (AWS, Azure, Google, and Snowflake) to discover, prioritize, secure, and monitor data with consistency. It is an agentless solution that connects to the cloud service providers' APIs, seamlessly scanning the environment while ensuring no impact on performance. With a single cloud data security solution that is utilized across all cloud services, organizations can be assured that data is discovered and policies are consistently applied, enabling data growth without increasing data risk.

This offering is designed specifically as a full-stack solution to address modern cloud data security challenges. It supports the four essential components—data landscape, DSPM, data access governance, and data detection and response—that comprise a holistic cloud data security solution. It is also possible to link Laminar's Cloud Data Security Platform with SIEM, CSPM tools, ticketing and workflow systems, and other cloud security products, simplifying cloud operations and delivering faster identification of potential or real problems. One of the key benefits of the Laminar solution is that it's agile and works autonomously and continuously without any prior knowledge or inputs from the security staff or operators.

Laminar's service also ensures that the policies and process for protecting data are consistent across cloud services and instances, an important attribute for any organization subject to compliance with regulations and standards.

## Conclusion

The impact of two megatrends—cloud transformation and data democratization—is rapidly increasing the amount of cloud-resident data, along with the number of users, apps, and systems accessing this sensitive data. Organizations need a cloud data security platform to decouple data risk from data growth. Protecting data in the cloud requires different tools than are used to protect on-premises data, and organizations need a purpose-built cloud data security solution.

Laminar provides a comprehensive, cross-cloud data security solution that includes the four necessary capabilities for delivering effective data security. The Laminar platform provides security and operations teams with a single tool for securing all their cloud data, and Laminar's automation reduces the demand on scarce staff and provides for rapid identification and resolution of issues.

For organizations that need to protect cloud-resident sensitive data, Enterprise Strategy Group recommends comprehensive cloud data security platforms that include data landscape, data security posture management, data access governance, and data detection and response. Enterprise Strategy Group recommends organizations explore solutions like Laminar that provide a holistic approach to the entire process of securing data in the cloud and provide unified and integrated data security across multiple clouds.



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

---

#### **About Enterprise Strategy Group**

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

 [contact@esg-global.com](mailto:contact@esg-global.com)  
 [www.esg-global.com](http://www.esg-global.com)