TAG CYBER

PROTECTING DATA IN PUBLIC CLOUD ENVIRONMENTS: AN OVERVIEW OF LAMINAR

DR. EDWARD AMOROSO, TAG INFOSPHERE

Laminar

PROTECTING DATA IN PUBLIC CLOUD ENVIRONMENTS: AN OVERVIEW OF LAMINAR

DR. EDWARD AMOROSO, TAG INFOSPHERE

Organizations routinely store and manage critical data in public cloud services such as Amazon Web Services, Microsoft Azure, Google Cloud Platform and Snowflake. As a result, data security solutions are required to address risks in these shared environments. The Laminar platform implements an effective cloud data security platform for modern enterprise architectures.

INTRODUCTION

When security experts are asked about cloud security, their response often focuses on infrastructure-related controls. The cybersecurity industry, for example, relies on cloud security methods such as cloud access security broker (CASB) and cloud security posture management (CSPM), both of which are excellent solutions for cloud misconfiguration, unintended use, poor service visibility and so on.

A challenge, however, is that these cloud controls tend to ignore the vital task of protecting the data stored in cloud services and infrastructure. Perhaps this should not be a surprise, since protecting legacy data in traditional environments was originally handled by protecting the infrastructure at the perimeter. Moving the business focus to the cloud certainly doesn't solve the protection problem automatically; attention is required, usually with the assistance of a modern cloud data security platform.

In this report, we outline the key aspects of the cloud data security equation, emphasizing how enterprise teams can support data security, governance and privacy requirements for data stored in cloud workloads and apps. We illustrate the approach in the context of the commercial solution from Laminar, which offers effective support for data security in Amazon Web Services, Microsoft Azure, Google Cloud Platform and Snowflake.

DATA SECURITY RISKS IN THE PUBLIC CLOUD

The security community has long understood the need to protect the systems and infrastructure associated with major public cloud offerings. What is more recently clear, however, is the importance of addressing data security risks that arise in such environments. This emphasis on data security risks in the public cloud is directly addressed by Laminar's platform and helps explain the motivation and purpose for creating the solution.

Major categories of data security risks that are commonly exposed to enterprise teams include the following:

- *Sensitive Data Disclosure* – When data breaches occur in public cloud systems, the potential emerges for sensitive or critical data to be compromised by unauthorized entities. This is a particular challenge since the attack will occur off-premise and hence might not be easily visible to security teams.
- *Privacy Issues* – When data breaches from both external actors and compromised insiders occur in public cloud services, the potential is high for privacy issues to emerge. These issues can cause problems for teams that must comply with regulations such as the GDPR or other major privacy frameworks or laws.
- *Third-Party Security* – When data is managed by third parties in public cloud environments, the risk is considerably more difficult to address. The need is thus present for all participants in data management, including first parties, customers and third parties, to ensure proper data security, privacy and governance.

METHODS FOR ADDRESSING CLOUD DATA SECURITY

While generally accepted frameworks for data security in the cloud have yet to emerge across the compliance community, we can identify several fundamental protection controls that should be present in any effective program. It is worth mentioning that the threats under consideration here are data security, governance and privacy as opposed to availability threats targeting cloud networks or service infrastructure.

The major categories of cloud data security controls referenced here are driven by extrapolating best practices in non-cloud contexts to the unique functional characteristics of modern public cloud services—namely, the ubiquity of public access, shared underlying infrastructure and outsourced service administration. Given these assumptions, we propose the following five methods as being mandatory for cloud data security:

- *Data Inventory* – Cloud data security solutions must support the discovery of the data requiring protection. Most enterprise teams struggle with this inventory task across their ecosystem, especially in the cloud. Nevertheless, discovery is a mandatory requirement for cloud data security.
- *Priority Marking (classification)* – Cloud data security solutions require the ability to mark and prioritize discovered data in public infrastructure. Such prioritization is necessary to properly define access policy and enforce controls. The organizational mission will influence how data priorities are established.
- *Data Security Posture Assessment* – Data security policies exist for each type and sensitivity of data in terms of required security controls and governance and privacy requirements. Cloud data security solutions must automatically assess and validate the data security policies.

- *Access Policies* – Cloud data security solutions must include basic security controls that will enforce defined policies for access based on the identities of requesting entities. Establishing an access policy requires a mature understanding of identity and many organizations struggle with this aspect of their security infrastructure.
- *Activity Tracking* – Cloud data security solutions must include a means for monitoring data use, including any meaningful transactions that could have a security impact. This capability is essential for audit and incident response and should include a way to normalize the audit data with other logging systems.

These five requirements for cloud data security must connect to the organization as follows: Cloud data inventory must integrate with corporate inventory repositories, cloud data priority marking must accept input from business units, access policies must define end-user access, security posture assessment identifies the risk and activity tracking must be connected to security information and event management (SIEM) and security operations center (SOC) infrastructure (see Figure 1).

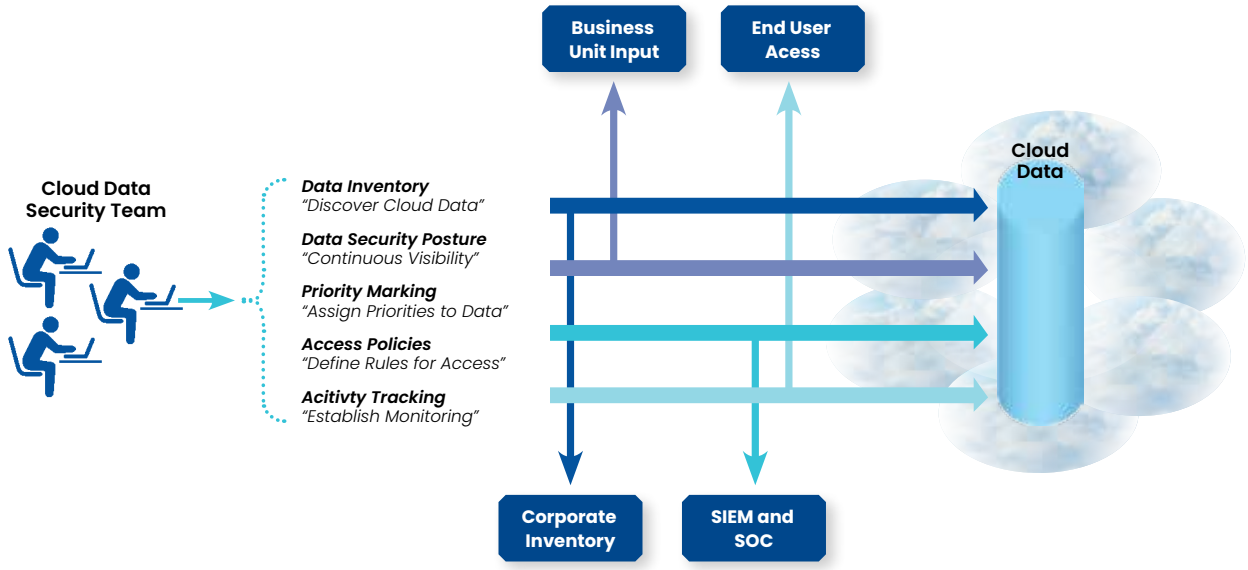

Figure 1. Required Cloud Data Security Functions

The discussion thus far has been mostly notional, based on high-level views of cloud data security. In the next section, we introduce and illustrate a practical commercial offering from data security vendor Laminar that implements cloud data security concepts in a realistic computing environment. The goal is to demonstrate that cloud data security controls can be practically implemented in a typical enterprise.

OVERVIEW OF LAMINAR

Founded by Amit Shaked and Oran Avraham, and emerging from stealth in 2021, Tel Aviv-based cybersecurity startup company Laminar provides a commercial solution for securing data in public clouds. The company addresses the growing challenge of leaks and other cyber threats to public cloud-hosted enterprise data. The platform currently focuses on Microsoft Azure, Google Cloud Platform, Amazon Web Services and Snowflake.

Platform Features

The Laminar platform is designed specifically for data security posture management for cloud-hosted data in a manner consistent with the discussion above. The commercial solution exhibits several functional capabilities that ensure seamless integration with enterprise customer security architectures, which increasingly include cloud-hosted data. The more important capabilities are listed below:

- *Autonomous Discovery* – The platform is designed to find and classify data in the cloud without the need for human involvement; no prior knowledge is needed.
- *Agentless Architecture* – An agentless, API-only architecture supports asynchronous operation and zero performance impact as data never leaves the environment.
- *Continuous Monitoring* – The protection from Laminar is ongoing so that dynamic environmental changes are captured and leaks from cloud services are avoided.
- *Secure by Design* – The Laminar solution is integrated and embedded directly into the customer's cloud infrastructure to avoid data proliferation.
- *Data Context Awareness* – The platform analyzes access and use patterns and relevant contexts such as data owners and cloud tags to aid in threat detection and remediation flows.

The Laminar platform protects the most sensitive data, but enterprise teams should find value in all their cloud-hosted data. This includes both known data and unknown shadow data that might reside in one of the major cloud services. Such comprehensive visibility is important for threat reduction as well as emerging security and privacy compliance frameworks.

Platform Architecture

The cloud-native Laminar platform includes direct integration for data security with AWS, Azure, GCP and Snowflake. Within each of these environments, the objective is to support the discovery, prioritization, security and monitoring of cloud-hosted data. A key technology used is Laminar's autonomous and continuous discovery and classification of cloud-resident data without the data ever leaving the customer's environment.

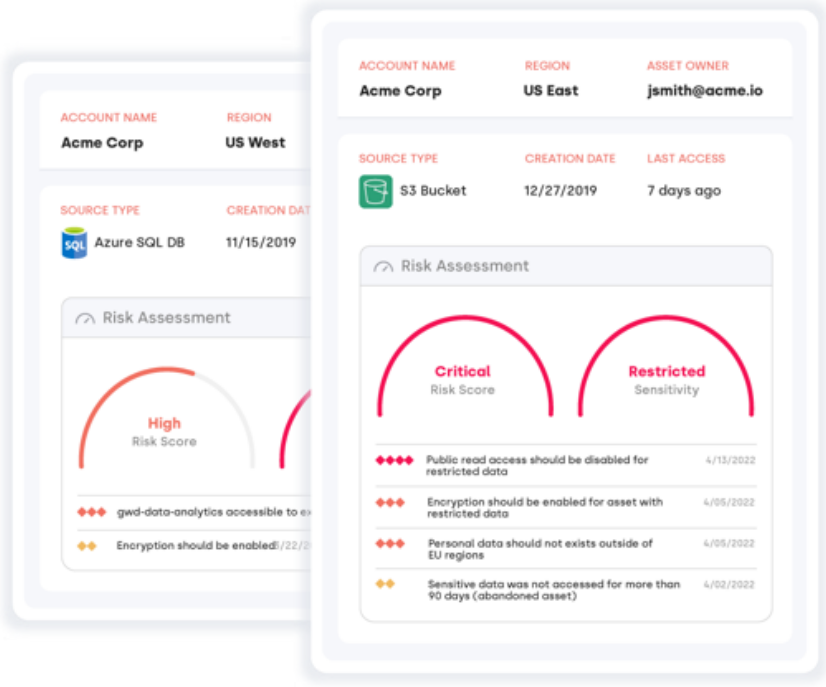

Figure 2. Laminar Customer Reporting Interface Examples

The customer reporting interface includes a rich set of telemetry values including the account name, region and asset owner for discovered data. It also includes the source type, creation date and last access for this cloud-resident asset. A risk assessment is provided that addresses issues such as public read access configurations, encryption settings, geographical region hosting and frequency of data access. In addition to out-of-the-box policies, customers can configure custom policies to fit their needs.

Platform Use

The Laminar platform is used for three primary cases. First, the solution helps customers determine where their data is currently stored and hosted. This is a complex process due to the rapid rate of change for sensitive data stored in the cloud, and the challenges of handling both known and unknown, or shadow, data repositories. Without proper cloud data visibility, teams don't know where the data is to protect it.

Second, the platform ensures that data security policies are properly enforced. This is superior to manual, user-defined approaches and it reduces the risk of unintentional proliferation of data since security controls do not travel with data and shadow copies are now well protected. The Laminar platform not only enforces this policy but also verifies that it is working.

And finally, the Laminar platform supports ongoing data access monitoring. Most existing approaches only monitor the known data sources, but it is the unknowns that are typically under-protected and unmonitored. Laminar's automation is required not only for coverage but also to keep up with the volume of cloud data access and interactions that occur in a typical environment.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.