Laminar

CHECKLIST

Cloud Data Security Platform Evaluation

Today there is enterprise data security on-premises and cloud security for infrastructure, but there is nothing that secures data for everything that you build and run in the cloud. While developers and data scientists have free reign to capture, copy and manipulate sensitive data in public cloud environments, security teams have lost visibility much less control over data in the cloud. That's why it's important to add a cloud data security platform to your cloud security stack.

However, when choosing new technologies it's important to choose wisely from the outset to avoid solutions that are not suited for the environment, that are incomplete, or that are too much effort for the value received. Not all cloud data security platforms are created the same, so take care when selecting among vendors. Here is a checklist of things to look for.

- [ ] **1. Multi-Cloud View:**
  Your organization likely has a multi-cloud strategy, and you need a cloud data security platform that provides consistent security and governance across multiple public cloud services. Whether you're running AWS, Azure, GCP or Snowflake, you need a single, consistent view of your cloud data across clouds, geographies, and organizational boundaries. This single view also helps you evaluate the risk to your data across them all, rather than individually.

- [ ] **2. Secure by Design Architecture:**
  When evaluating a data security platform the last thing you need is another source of risk. That's why you should look for a solution that does not extract your data from your environment.

- [ ] **3. No Impact on Production:**
  When it comes to cloud infrastructure that drives and powers the business, you simply cannot slow it down or disrupt it. Look for a cloud-native data security solution that is agentless and asynchronous, implemented using the cloud's APIs, is not inline, and has no impact on production. Utilizing that cloud-native APIs gives complete visibility of every data instance.

- [ ] **4. Discovery of All Data, Known & Shadow:**
  You can't protect what you can't see and you can't accurately assess, evaluate and mitigate the risk to your data until you have a full picture. Your data security platform needs to see all of your cloud data, including managed and unmanaged data assets, data caches, data

pipelines, Big Data environments, and, most importantly, the Shadow Data previously unknown to IT and security. And it should do this:

- continuously, without any manual effort or any prior knowledge of the environment or access credentials. It must be completely hands off.
- autonomously, without the need for a known, fixed list or target resources.

---

5. Precise Classification of Data & Context:

You need to know where your most sensitive data, like PII, PCI or company financial records are located, all without manual effort. Look for data security solutions that provide automated and accurate data classification. Data classification must go through multi-step contextual verification to avoid false positives. Additionally, to take action on data that puts your organization at risk, you'll want an offering that gives you critical contextual metadata such as resource owner, consumers of the data, and more.

---

6. Prioritization Based on Risk:

No one wants more security alerts. Look for a cloud data security platform that sifts through all of the risk posed by your data assets and prioritizes those that are highest risk based on several factors, such as sensitivity, volume, data security posture and exposure.

---

7. Guided Posture Improvement:

Easy handoffs between teams are key to good results in data security. Time is wasted or remediation does not happen when security needs to manually search through hundreds if not thousands of developers for who to talk to. Look for a solution that facilitates this with detailed, specific guidance on the asset and the actions necessary to mitigate risk.

---

8. Ongoing Monitoring & Data Leak Protection:

Data security requires constant vigilance, so continuous, ongoing monitoring on your most sensitive data is paramount. You want to have constant eyes on your "crown jewels" (e.g., your company's most critical data). Look for a solution that continuously monitors your crown jewels, detects suspicious anomalies that may signify a data leak in real time and offers immediate notification and remediation guidance.

Get to know the Laminar cloud data security platform today. **Click Here**