WHITE PAPER

Data Security with Rubrik Laminar

Table of Contents

HERE’S THE PROBLEM

Businesses have innovated how they use cloud data, but not how they secure it. Cloud data gets created, copied, shared, and moved rapidly. Legacy manual or connector-based techniques cannot keep pace.

THE RESULT?

Security has little to no oversight over one of the fastest-growing sources of risk in the business—the drastic expansion and replication of data. This is the Security Execution Gap—a fast-growing gap between the agility needed to safely create value with cloud data, and traditional (slow, limited, manual) data security controls.

Securing your cloud data is completely different from securing your infrastructure. Not only do you need a data-centered tool for the job, you need an agile cloud native approach to keep up with your users.

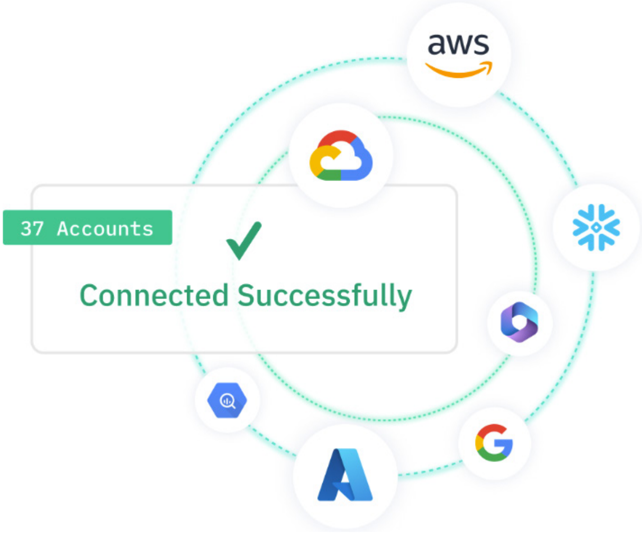
THE LAMINAR PLATFORM

To secure all of your data, Laminar provides agile data security across multi-cloud environments using cutting-edge preventive and detective controls for posture management, access governance, threat monitoring, and response.

One integrated solution enables complete data protection and lets your teams keep pace with the rapid changes in your cloud environment and protect what matters most—your data.

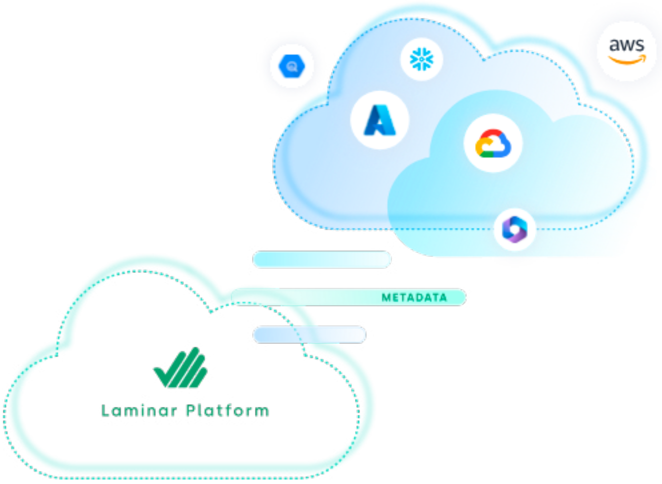
ARCHITECTURAL PILLARS

Comprehensive and continuous visibility
Laminar autonomously and continuously discovers all cloud-resident data, not just known or manually tagged assets. Laminar comprehensively detects data in managed and self-hosted assets, embedded in virtual instances, Shadow Data, data caches, data pipelines, and Big Data. Without requiring credentials, the platform leverages multi-step contextual validation to precisely identify and classify sensitive data such as PII, PHI, and PCI, living in Amazon Web Services (AWS), Microsoft Azure, Microsoft 365, Snowflake, Google Cloud Platform (GCP), and Google workspace environments.



Secure scanning

Laminar's industry-leading technology integrates into your cloud infrastructure and is developed to keep your data safe. Data safety is ensured because Laminar's role structure prevents data from leaving your cloud environment. Discovery and classification occur in your Cloud account so that data always remains within your environment. Only metadata is extracted.

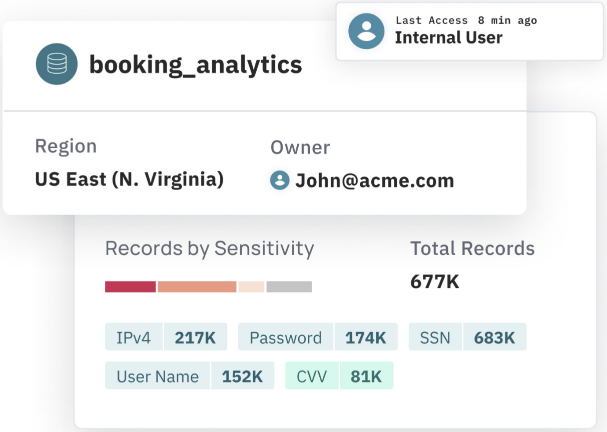


Agentless architecture

Laminar deploys effortlessly, with no need for an agent or connectors, and utilizes serverless functions that leverage CSP APIs to asynchronously scan your environment - without impacting performance (and data never leaves your environment).

Rational, high-fidelity AI classification

Laminar employs AI smartly to optimize classification accuracy while keeping your data secure in your own environment. Dynamic ML models combine usage telemetry and Laminar Labs research to deliver low false positive data tagging in the most cost-effective manner. This means you gain contextual understanding, data insights, and awareness of the data owner, the content type, object size, location, creations and last accessed dates, top users, posture, and more.


Last Access 8 min ago
Internal User

booking_analytics

Region
US East (N. Virginia)

Owner
John@acme.com

Records by Sensitivity

Total Records
677K

IPv4	217K	Password	174K	SSN	683K
User Name	152K	CVV	81K		

SOLUTION USE CASES

Data intelligence

Businesses operating in the cloud are processing massive and growing amounts of data. The result is a vast and complex ecosystem that rarely has a clear organizational owner. Instead, CIOs, CISOs, and CPOs share this responsibility. Under these circumstances, it's easy to see how blind spots and nearly unchecked data proliferation can occur.

Laminar's data intelligence solution delivers data discovery and classification that provides you with end-to-end visibility into your cloud ecosystem; contextual insight and easy-to-consume data mapping are available on data sources. There is no need for connectors, access credentials, or lists of data assets.

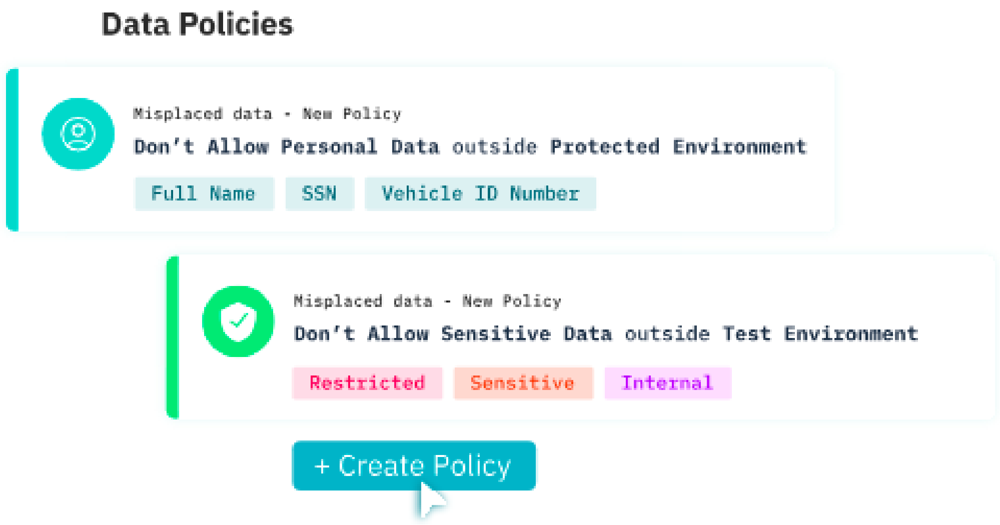
Asset and data discovery gives you insight into what assets and data live in your environment:

- A comprehensive view of all assets that generate data or host data in your organization is continuously and autonomously updated.
- Get granular visibility into the assets where data resides, for example, information on asset risk levels, asset ownership, and asset sensitivity levels.

Data classification provides granular visibility into critical contextual information such as Data categories, Data types, Data sensitivity levels and more.

Data security posture management (DSPM)

Laminar provides Data Security Posture Management (DSPM) that enforces data security best practices and data policies. Use DSPM policies to have visibility into overexposed, misplaced, redundant, and unprotected data. To meet the specific needs of your security and business environment, you can also create custom policies.

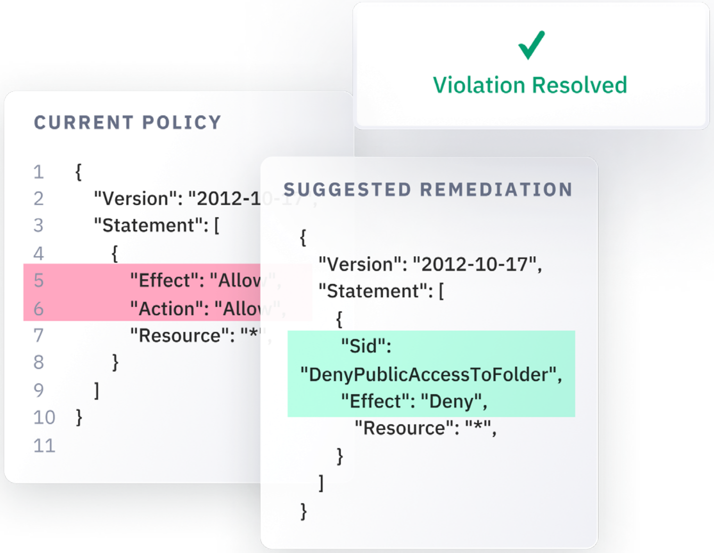


Data Policies

Misplaced data - New Policy
Don't Allow Personal Data outside Protected Environment
Full Name | SSN | Vehicle ID Number

Misplaced data - New Policy
Don't Allow Sensitive Data outside Test Environment
Restricted | Sensitive | Internal

Get a full analysis of why a security or compliance violation exists, supporting evidence, and expert step-by-step technical fix recommendations, saving time and reducing complexity.



CURRENT POLICY

```
{
  "Version": "2012-1
  "Statement": [
    {
      "Effect": "Allov
      "Action": "Allov
      "Resource": "*"
    }
  ]
}
```

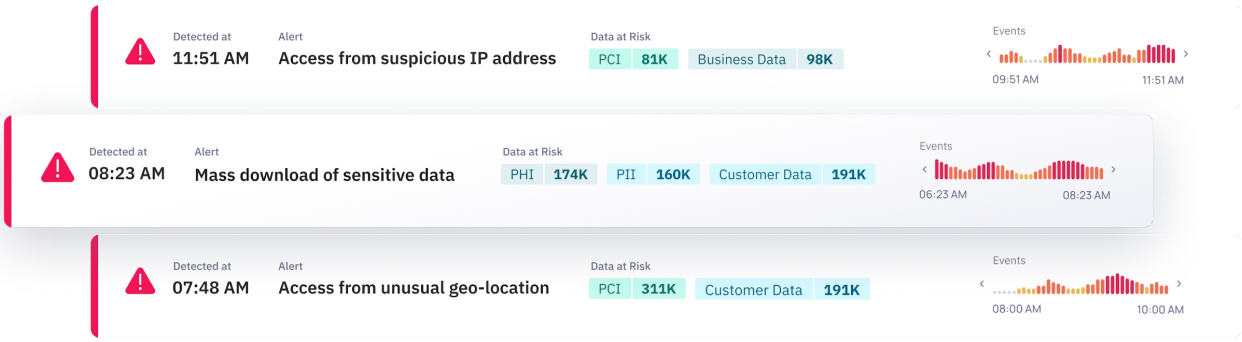
SUGGESTED REMEDIATION

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
"DenyPublicAccessToFolder",
      "Effect": "Deny",
        "Resource": "*",
    }
  ]
}
```

Data detection and response (DDR)

Laminar's data detection and response (DDR) solution lets you detect data breaches as they occur and quickly contain active threats to minimize damage. Laminar identifies anomalous data access and behavior—alerting you on data exfiltration, suspicious third-party access, insider threats, accidental data leaks, data misuse, and other threats.

Laminar's DDR solution finds data threats other solutions do not. Laminar monitors your sensitive data no matter where it resides or moves across your multi-cloud environment and SaaS applications – eliminating blind spots encountered with other solutions that don't monitor data at its source.

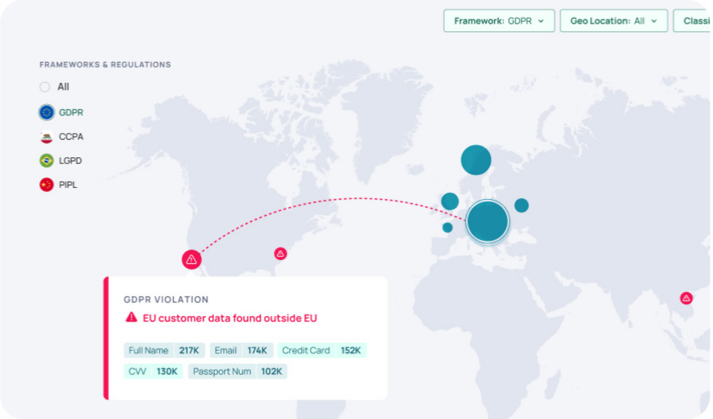


Detected at	Alert	Data at Risk	Events
11:51 AM	Access from suspicious IP address	PCI 81K Business Data 98K	09:51 AM – 11:51 AM
08:23 AM	Mass download of sensitive data	PHI 174K PII 160K Customer Data 191K	06:23 AM – 08:23 AM
07:48 AM	Access from unusual geo-location	PCI 311K Customer Data 191K	08:00 AM – 10:00 AM

Data privacy and governance frameworks

Compliance is a daunting task, but with proper evidence, it can make things much easier.

- Streamline evidence collection for internal and external privacy and governance stakeholders through autonomous data discovery and classification of your sensitive and regulated data. For example, detect where you have stored PII, PHI, PCI. Learn more about discovering sensitive and regulated data.
- Utilize Laminar's data policy engine to continuously enforce regulatory compliance and standards requirements for data, regardless of the underlying technology or location. Easily ensure all data is properly owned and tagged to fast-track evidence collection for records of processing activities (RopA) and answer data subject access requests (DSAR). Learn more about using policies to regulate privacy and governance.



Framework: GDPR

Geo Location: All

GDPR VIOLATION

⚠ EU customer data found outside EU

Full Name 217K · Email 174K · Credit Card 152K · CVV 130K · Passport Num 102K

LAMINAR PARTNERSHIPS

- AWS Foundational Technical Review (including AWS Well-Architected Framework)
- AWS Security Competency Partner in the Data Protection category
- AWS RDS Ready Product Designation
- AWS Built-in Partner Solutions
- Launch Partner for Wiz Integration (WIN) Platform
- Launch Partner for Amazon Security Lake

LAMINAR SOC II TYPE 2 CERTIFICATION

Laminar is SOC II Type 2 certified, which guarantees its capacity to safeguard sensitive and proprietary information. Laminar prioritizes the security and confidentiality of clients, employing established protocols and frameworks to ensure the protection of data.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

wp-data-security-with-rubrik-laminar / 20231128