Laminar: The Leading Data Security Posture Management (DSPM) Solution

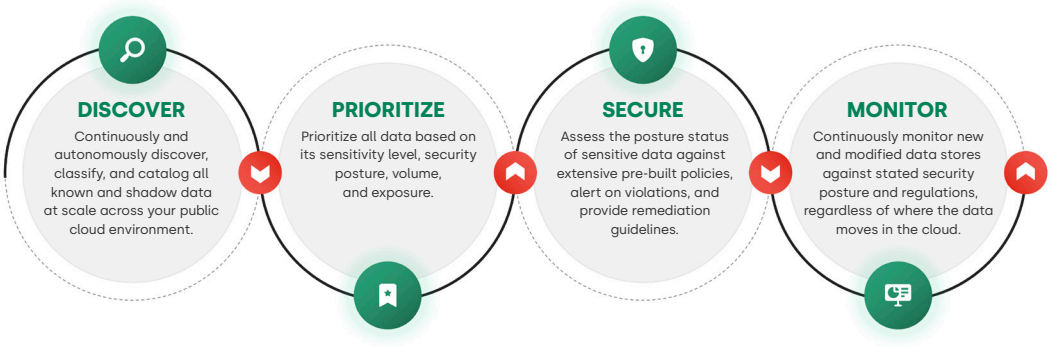
For everything you build and run on AWS, Azure, Google Cloud, and Snowflake.

Businesses move to the cloud to obtain a competitive advantage, but for all the limitless potential of cloud transformation, the source of that advantage comes down to two elements: the data you have and what you do with it. Unfortunately, the activities that create the biggest advantages for cloud-based businesses are the same activities that introduce the most risk.

Cloud data is magnitudes larger, more distributed, and more dynamic than on-prem data. Every day developers and data scientists create, move, modify, and delete data in pursuit of innovation. And they leave a trail of unintentional risk in their wake. As sensitive data propagates across the public cloud, risk grows, creating the innovation attack surface.

Security must reduce risk while enabling innovation with on-demand security provisioning that proactively discovers all cloud data, intelligently classifies it by sensitivity and business impact, identifies and alerts on data security policy violations, and provides actionable remediation recommendations.

This is agile cloud data security. This is Laminar.



"Implementation, connection, and deployment was easy. Laminar accurately discovered, classified, and cataloged all the data in our environment and assessed our risk in just a few days. It was a totally hands-off experience."

Yaniv Toledano
VP, Global CISO & IT
Pagaya

 |

The Laminar Advantage – Data Security at the Speed of Cloud

Autonomous – Laminar automatically discovers new and modified data stores without access credentials or any input from you.

Always-on – Laminar continuously monitors your environment for changes and automatically scans new cloud accounts, new data stores, and new data added to existing data stores.

Zero disruption – Laminar is agentless and runs in asynchronous mode, so there is no impact on cloud performance.

Risk-free – Laminar utilizes serverless functions that leverage APIs to scan your environment, so data never leaves your cloud environment for maximum security and privacy.

Fast time-to-value – Laminar deploys in 5 minutes and presents comprehensive findings of your at-risk sensitive and regulated data within a week.

Context-aware – Laminar prioritizes sensitive and regulated data by considering multiple risk factors (e.g., sensitivity levels, exposure), enabling you to protect your high-risk data first.

KEY USE CASES

Discover and classify data – discover, classify, and categorize all known and unknown data, including shadow and abandoned data, across all cloud accounts.

Automate policy validation and enforcement – find, prioritize, and fix policy violations for all your cloud data as it travels through the cloud.

Protect sensitive data from public exposure – pinpoint all your exposed sensitive data and remediate. Whether it's misplaced data, misconfigured controls, or overexposed access.

Ensure data sovereignty – detect and create alerts when sensitive and regulated data violates data residency requirements.

Enforce environment segmentation – segment the environment based on data privacy requirements (e.g., PCI DSS, HIPAA) and business needs.

ABOUT LAMINAR

Founded in 2020 by a brilliant team of award winning Israeli red team experts, Laminar is proudly backed by Tiger Global, Insight Partners, Battery Ventures, and Salesforce Ventures To learn more please visit laminarsecurity.com.