A digital adoption platform secures sensitive assets across the entire cloud ecosystem

A Case Study

walkme

WalkMe's cloud-based Digital Adoption Platform enables organizations to measure, drive and act to ultimately accelerate their digital transformations and better realize the value of their software investments. The platform leverages proprietary technology to provide visibility to an organization's Chief Information Officer and business leaders, while improving user experience, productivity and efficiency for employees and customers

COMPANY SIZE
+1K employees

INDUSTRY
SaaS

CLOUD PLATFORMS
aws AWS

Azure

GCP

WalkMe has grown exponentially in the past few years, expanding its offerings to evolve into a full-fledged digital adoption platform.

This emerging new software category focuses on providing total visibility into SaaS application usage and user journeys. The WalkMe solution monitors internal software usage and executes onboarding, training, and adoption strategies. These features help customers with digital transformation and change management.

WalkMe's platform regularly deals with sensitive customer data as it enables customers to monitor and optimize their internal operations. The platform also provides walkthroughs that display customers' internal assets, sometimes including views of the sensitive data stored on these assets. Because of this, the WalkMe team wanted to prioritize data security as they continued to grow.

CHALLENGE

Securing a variety of cloud assets during continuous growth

WalkMe faced a challenge: handling continuous growth while ensuring the security of customer data They wanted to proactively ensure that their security controls in the cloud grew in tandem with their platform.

"As we grow, we have a lot of buckets, a lot of storage, and we need to keep an eye on them," said Dror Zilberman, Infrastructure & Cloud Team Lead at WalkMe. "We need to understand what type of data we have in each asset."

> "As we grow, we have a lot of buckets, a lot of storage, and we need to keep an eye on them, we need to understand what type of data we have in each asset"

The WalkMe team wanted to understand which data they possessed, its associated risk, and how to mitigate those risks. While they had a legacy solution for managing data security in the cloud, it only covered known S3 buckets. The solution left out the organization's other AWS data stores (RDS, EBS, etc.) as well as their entire GCP environment (including BigQuery). It also lacked data discovery capabilities, missing any unknown data (shadow data). The team's existing solution was also slow and hard to use, making it difficult for other departments, such as the DevOps team, to view findings and make actionable changes.

SOLUTION

Laminar discovers known and unknown data across WalkMe's entire cloud ecosystem

WalkMe saw apparent gaps in their existing approach and decided to evaluate Laminar alongside other DSPM security vendors. Laminar came out on top due to its speed and ability to discover publicly exposed sensitive data in areas the others didn't. For instance, Laminar can first discover and classify sensitivity of data so you know where it resides, and what your exposure is. It then can discover misplaced sensitive data (e.g. Personal information in a lower environment or in geographies requiring strict regulatory control, or publicly exposed sensitive information) to notify of segmentation violations. Laminar can also alert when a third party (perhaps, a supply chain partner) accesses sensitive information they normally wouldn't.

In Zilberman's words: "we needed something more intuitive, faster, and a better fit for WalkMe's needs. And this is where Laminar stepped in."

> "We needed something more intuitive, faster, and a better fit for WalkMe's needs. And this is where Laminar stepped in"

Rather than focusing on known infrastructure, Laminar locates known and unknown sensitive data across a multi-cloud environment. Then, it classifies this data by risk level and gives actionable recommendations for remediation (e.g., moving or removing sensitive data from lower environments). It also continuously monitors the entire ephemeral cloud environment for changed, moved, or copied data — and intelligently scans to keep constant vigil over new or emerging risks.

RESULTS

Data risk visibility, and actionable remediation guidance across the entire cloud

Over the past few months, Laminar and WalkMe have built a data security partnership. Laminar provides the platform and expertise, and the WalkMe team works directly with Laminar to tailor the solution to their unique needs.

Thanks to the Laminar platform, the entire WalkMe security team has visibility into data security threats and can take action to remediate potential risks. The DevOps team also uses the solution in collaboration with security.

"Thanks to prioritization, we had a lot of quick wins, working closely with our DevOps engineers on the hardening side: making sure encryption was enabled and that there was no over exposure and access to sensitive data."

> "Thanks to prioritization, we had a lot of quick wins, working closely with our DevOps engineers on the hardening side: making sure encryption was enabled and that there was no over exposure and access to sensitive data"

With Laminar, WalkMe can more readily assure their customers that they're proactively covering their sensitive data — an important selling point as they continue their efforts as category creators. In the future, WalkMe plans to use Laminar's data hygiene capabilities for removing unneeded buckets and reducing cloud costs.

See Laminar's Cloud-Native DSPM in Action

BOOK A DEMO