LACEWORK

CASE STUDY

DataVisor scales multicloud security & compliance for customers

DATAVISOR

Challenges

- Securing a multicloud (GCP/Azure/AWS) environment to meet the demands of expansion
- Required a highly efficient approach to real-time monitoring and protection

Solutions

- Anomaly detection that operates at the host level
- Daily reporting and detailed compliance reporting

Results

- Increased overall efficiency and productivity of their existing security operations
- Allows the security team to quickly identify issues and close them almost immediately

> "Lacework enables us to easily scale our cloud security with an anomaly-based host intrusion detection system that operates at the host-level."

Avinash Raju, Principle Security Engineer at DataVisor

The company and its business

DataVisor is a leading provider of AI-based fraud and risk management solutions for large enterprises. As a pioneer in real time fraud detection using unsupervised machine learning, DataVisor is now a global company whose solutions are deployed in multiple clouds. DataVisor monitors over 4 billion user accounts to detect and identify both known and unknown fraud signals.

The growth challenge

DataVisor was initially operating in the AWS environment that hosts a large number of instances and clusters. Their cloud footprint was continuously changing and expanding. As their business continues to grow and expand into multiple other clouds such as GCP and Azure, they want to extend the tight security to these new cloud environments, which requires a highly efficient approach to real-time monitoring and protection. This is where Lacework came to help. "We needed something that would save us time and effort in terms of both monitoring and compliance for multiple clouds, and we wanted a solution that would deliver real-time security event alerts to help us thwart a wide range of attack types over all cloud environments," Raju explains.

Choosing Lacework

DataVisor's Engineering and Management teams considered their options for gaining the visibility and efficiencies they needed across all of their growing environments. One was to develop all the functionality in-house, which would have been a huge task. Instead, they chose Lacework as the solution that would fulfill their needs. Raju notes that, "Features, efficacy, consistency, pricing and support are all part of our evaluation criteria, and it's these factors we look to when assessing the extent to which we're seeing desirable return on our investment."

Rapid, efficient detection and response

Currently DataVisor uses Lacework to monitor activity in their cloud environments, generate alerts, and for compliance reporting. Lacework automatically provides reports of non-conformations to defined compliance policies. Additionally, Lacework reports network/IAM/Bucket/Cloud Watch security violations on a daily basis. This has enabled them to save both time and money, which has increased overall efficiency and productivity of their existing security operations.

Raju explains how this works: "Lacework enables us to easily scale our cloud security with an anomaly-based host intrusion detection system that operates at the host-level. Because data is collected at the host-level, security teams can more accurately and effectively detect insider attacks that otherwise wouldn't be identified in network traffic. Lacework identifies all activity happening across all cloud workloads and accounts. Lacework alerts on security events and non-conformations daily. This allows the security team to identify issues and close them almost immediately."

Find out more at lacework.com