HCLTech | Supercharging Progress™

Strengthening security with real-time insights for a global logistics company on Google Cloud

HCLTech helped a global logistics company strengthen its security posture by providing rich data insights with 15% cost savings

A global logistics company had a huge inflow of security log data from multiple sources. The company wanted to strengthen its security by drawing insights from this data. On the advice of HCLTech, a longstanding partner in their managed services program, it leveraged the data analytics capability of the Google Cloud Platform. By migrating data from its on-premise source systems and applications to the cloud, the global logistics company was able to improve its security posture by drawing rich, real-time insights from advanced analytics based on artificial intelligence and machine learning (AI/ML). The company also saved 15% in costs through customized data ingestion pipelines with an additional monthly savings of $25,000 through cost optimization.

The Challenge: Drawing insights from a massive inflow of data

Data, the lifeblood of organizations, is being generated on an exponential scale – locating, classifying and analyzing it is a significant challenge. In this case, the company had over 20GB of security log data flowing in every day from 25 different sources. The volume of this data inflow from its various cybersecurity systems was expected to double to 40GB each day over the next three to four months. But the company's existing on-site systems were unable to analyze this in a meaningful way to gain valuable insights that would help improve its security posture.

The Objective: Migration of on-premise systems to Google Cloud

The company wanted to ingest this massive amount of data to improve its security systems. To do this, it needed an advanced data analytics platform that could be leveraged to slice the data and analyze it to track anomalies and better visualize areas of concern through AI/ML. Google Cloud was the obvious choice, with Big Query, Looker analytics and AI/ML capabilities. By migrating its on-premise systems to Google Cloud, the company gained a better and more comprehensive perspective on how to strengthen its security system.

The Solution: Advanced analytics and AI/ML for anomaly detection on Google Cloud

HCLTech delivered the technology transformation and enabled the migration of the on-premise source systems and applications to the Google Cloud Platform. The solution covered real-time data ingestion with batch and history data loading, data processing and data analytics features. AI/ML solutions were designed to manage and monitor high-risk events and alerts.

Using Google Cloud Platform Machine Learning, AI/ML models were developed to leverage Privileged User Behavior Analytics (PUBA) for anomaly detection. In addition, data lakes and data marts were developed leveraging the AI/ML models. The engagement, which began with simple use cases, quickly expanded into more mission critical areas as the ease of visualizing desired elements from the data significantly improved.

The Impact:
Stronger security through real-time insights plus cost savings

Empowered with real-time insights and advanced analytics, the company saw significant benefits from the migration. Google Cloud's analytics provided insights that were not previously visible in the on-premise systems. The transformation helped the company gain a better understanding of anomalies, threat intrusions and areas of concern such as fraudulent logins. These insights enabled better anomaly detection and threat detection across the company's global network.

The migration to Google Cloud also provided relief from the huge costs of the previous on-premise landscape. It created a faster, more flexible model enabling 15% savings in cost and effort. In addition, the team's proactive approach to utilizing Google Cloud best practices led to $25,000 in monthly savings through cost optimization.

The positive impact resulted in an ongoing fine-tuning of the company's security systems across the world. In view of its vast benefits, the program has been extended for another two years.

A faster, more flexible model enabling **15%** savings in cost and effort

Monthly cost optimization savings of **$25,000**

Insights enabled better anomaly detection and threat detection.