MOLECULA

CUSTOMER CASE STUDY—

Molecula Powers Dynamic Segmentation to Better Understand User Logins

Business Challenge—

Q2, a secure, cloud-based digital banking solutions company needed to dynamically segment users at the time of login to identify and better understand anomalous attempts to access its banking platform so that it could better serve customers.

Q2's digital banking solutions include handling deposits, moving money, lending, security, and fraud protection for financial institutions. The end goal is a better, safer financial experience for account holders.

The Q2 websites have three types of visitors: consumers who are members of Q2's client banks, data aggregators, and malicious attackers. Q2 sought to identify the aggregators and bad actors hitting the platform in real time in order to identify the unwanted traffic, create a better experience for end users and free up the necessary resources for customer transactions.

Technology Challenge—

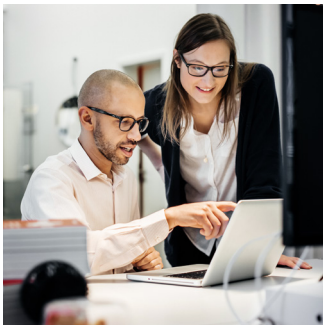
With over 100 million logins a month, the amount of data generated by Q2's system necessitated a multi-week process of aggregating, training, and producing the necessary analysis to be able to understand traffic based on threat levels. This slowed down detection model training and prevented real-time machine learning. As a result, Q2 was forced to overprovision in order to reliably serve customers. The massive amount of security, historical data, outcomes, and behavioral data was being stored in a data lake. Login-related data was streaming through a Kafka data pipeline.

Q2

KEY RESULT—

"Using Molecula (Pilosa) to analyze activity across our 100m+ monthly login events in real time gives us an entirely new view of our data. Without Molecula in our data pipeline, working with this volume of data would be effectively impossible."

— ADAM BLUE, CTO



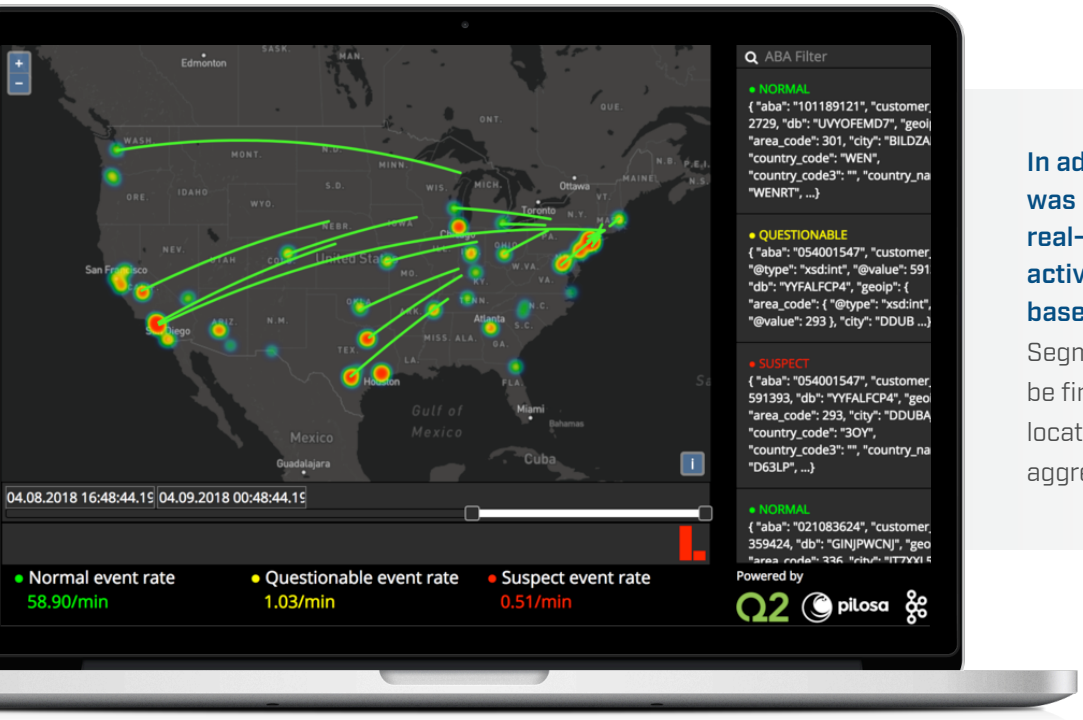
KEY OBSTACLE—

Q2 did not have the ability to query the combined data in real time and the traditional data infrastructure inhibited the speed with which detection models could learn and be put in production.

How Molecula Helped—

In this project, Molecula first began by integrating and ingesting the behaviors associated with Q2's 100 million monthly logins at the moment the transactions hit the bank's networks.

All historical data and outcomes were also ingested. Once Molecula virtualized all the data into Virtual Data Sources (VDSs), Q2 could perform dynamic segmentation queries in a fraction of a second and JOINs across these datasets with previously unthinkable speed. Q2 was able to run detection models using the combined data sets and could score each transaction's threat level in real time. Q2's models could now instantly combine in-house multi-factor and out-of-band authentication with proprietary behavioral and transactional analysis to improve its detection capabilities.



In addition to detecting threats, Q2 was able to use Molecula to power a real-time visualization of the login activity hitting Q2 to analyze traffic based on ad-hoc filtering criteria. Segmentation in the visualization could be fine tuned by threat level, time, location and type of login (consumer, aggregator, bad actor).

Business Outcome—

With this project led by Molecula, Q2 better understood its login traffic and how it could negatively impact the customer experience.

This continuously-updated dynamic segmentation system gave Q2 improved control over bad actors and the entire visitor experience was now informed by threat-level scoring based on complete, real-time datasets. With the new data insights, Q2 also improved overprovisioning strategies and realized cost savings while delivering a faster, safer, higher-quality service to the end user.