Customer Success Story

ALLURE SECURITY

CUSTOMER STORY

Allure Security Uses Hydrolix on AWS for Better Application Performance at a Better Price

Allure Security provides brand impersonation detection across all digital platforms. The company monitors tens of millions of pages of internet content, about fifty petabytes a day, looking for signals of fake websites.

Business Challenge

Allure Security's software monitors the many components of a company's digital assets, and detects unusual activity that may indicate a brand impersonation. It monitors logos, taglines, fonts and other components that may have indicators of fraud. The company uses log data as part of its operations to keep the components of its software in sync and fast. The logs also show where bad activities are happening and how behaviors are changing.

Some of that log data, however, was getting thrown away due to the cost of retaining data, and log limitations set by Allure's existing observability provider. Allure had bought a limit of logs. If the log amount crossed that limit, the provider shut off its platform entirely, which led to lost log data. Allure could only use about 30 days' worth of data with its provider, and had to be conscientious about logging events that may not have been valuable. Also, as the log amount increased, costs spun out of control to the point where it became difficult to run the business in a performant way.

The prohibitive cost coupled with limiting log data created challenges in mitigating persistent impersonation attacks over time. Without ingesting and retaining all log data for an extended period, the company could not identify the root cause of issues nor collect the evidence needed to build a complete story of incidents. It's also critical to keep all data hot so searching for indicators is fast, a matter of seconds. Allure's existing observability provider could not deliver data insights quickly enough, causing a loss of certain records.

"Working with Hydrolix, I have less concerns about my ability to scale my data, data ingestion, and which logs I collect. I don't have to be selective."

—

Josh Shaul, CEO, Allure Security

Solution

Allure turned to Hydrolix on AWS for the backend of its observability needs. The company continued using its existing provider for its UI but used Hydrolix for log ingestion, long-term retention, and always-hot data for rapid querying and analysis. With Hydrolix, Allure can ingest and retain all log data for at least 15 months and the license fee is less than half of what the company paid its other observability provider.

Hydrolix ingests terabyte- to petabyte-scale data and shows insights within ten seconds, which means Allure can spot indicators of impersonated sites in real time, reducing the time to mitigation. With Hydrolix, Allure doesn't have log limitations, so it can spot root causes and build an evidential story about incidents.

Results

- No logging limitations, ingest all data as needed
- 15+ month data retention at less cost
- Ingestion to insights in less than 10 seconds, subsecond querying
- Spots indicators of brand impersonation in real time to reduce MTTR
- Better performance at a better price
- Always-hot data
- 24-7 customer support

If you are interested in learning more about how Hydrolix can help you find and fix performance and security issues before they disrupt your business, contact us today.

Or find us on the AWS Marketplace by clicking here.

FOR MORE INFORMATION, VISIT > HYDROLIX.IO/HYDROLIX-FOR-AWS