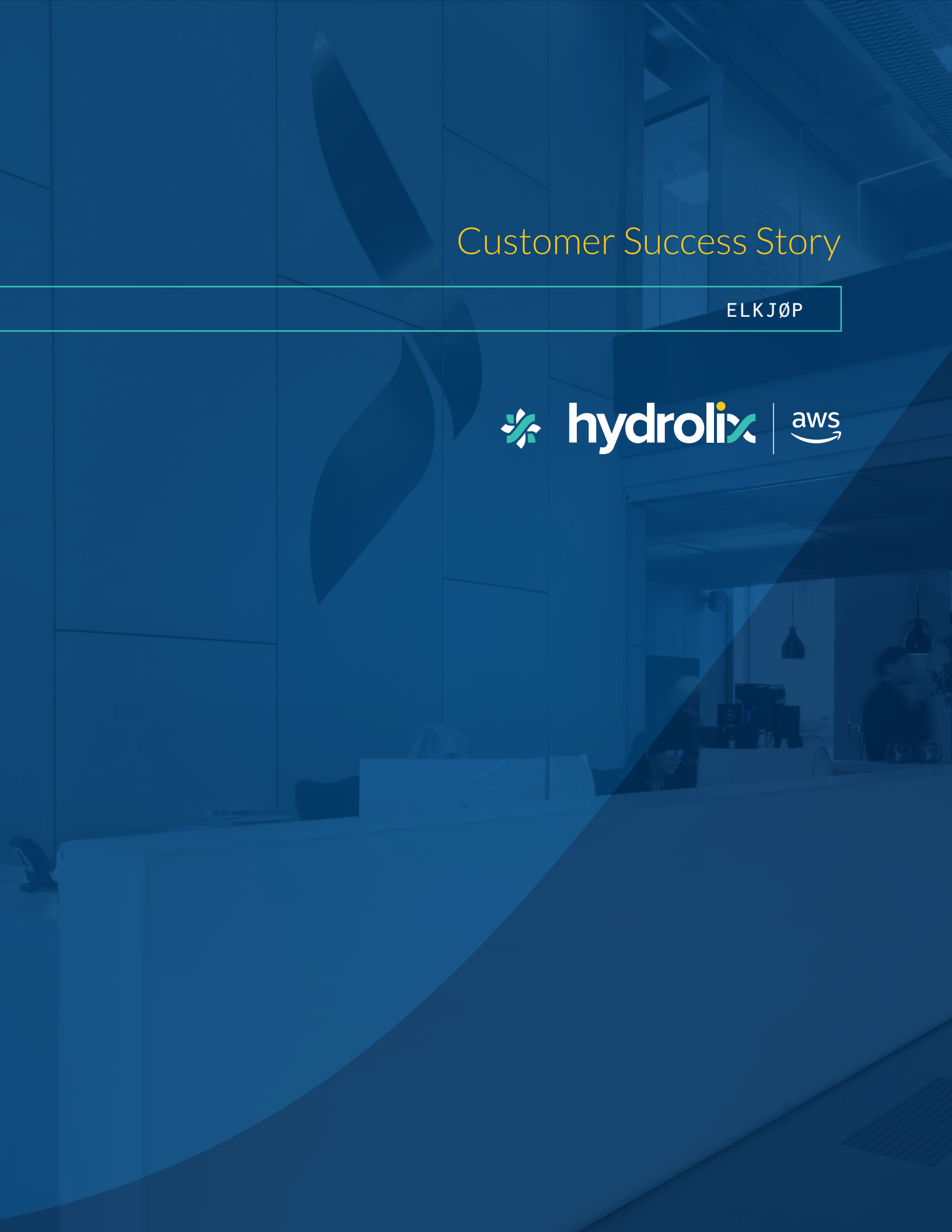

Customer Success Story

ELKJØP

hydrolix | aws

CUSTOMER STORY

How a large consumer electronics retailer stopped a massive DDoS attack without any business impact.

Jonas Petersson, Team Lead for eCommerce, Elkjøp Nordic AS January 2024

With more than 400 stores in the Nordic countries and a booming online retail business, the "Black Friday Weeks" campaign, which lasts for two weeks, is the peak season for the team at Elkjøp. Every year, it's "all hands on deck" to secure customers a smooth, fast, secure and reliable shopping experience.

Business Challenge

This peak season we wanted even more visibility into our traffic. During the past years it has been cumbersome to see traffic not hitting our origin servers. We wanted to better understand what traffic was hitting our cache and protection layers, enabling us to take necessary actions to protect our services even better. In other words, we wanted a complete picture of the traffic hitting the edge. Without solid insights, we wouldn't know where to prioritize our preparation efforts such as hardening our protection at the edge and our internal protection of our origin servers.

We needed a cost-effective solution that could show us pain points and areas to harden enabling us to mitigate them prior to the start of our "Black Friday Weeks" campaign, but also being able to tackle situations happening in real time. In addition, our requirement for a long data retention policy had to be met. At the time of assessing such a solution we were already using another provider for our applications on the backend.

However, moving our log data from our cloud platform into the provider's platform would make a significant hit on cost.

To achieve our goals, we needed an observability platform that allowed us to ingest, query and retain large amounts of data for a long period of time, at an affordable price point. Luckily, we found the perfect solution in Hydrolix, and in due time before Black Friday Weeks and a massive DDoS attack.

"Within just a few months, we resolved five different issues by simply having the extra visibility and ability to query on data patterns."

The Attack

Earlier this year we were introduced to Hydrolix, a managed observability service designed to ingest, monitor, query, store, and analyze massive amounts of data in real time. The platform, which is delivered as a managed service, seemed to check all our boxes so we launched a proof of concept. Within just a few months, we resolved five different issues using Hydrolix by simply having the extra visibility and ability to query on data patterns. After a successful proof of concept, we implemented the tool in our production environment a month before the peak season.

Then, during the "Black Friday Weeks" campaign, at the highest peak traffic time, we experienced an enormous DDoS attack. It involved 3000 IP addresses across 80 countries. Hydrolix spotted the attack immediately while our security services provider gave us the necessary protection to keep the attack contained. **The entire event from spotting to stopping the attack was instant. No sites went out of service and none of our customers experienced any impact whatsoever.**

We could clearly see the attack with Hydrolix and we could see that our preparation work had paid off since the security protection layer took most of the traffic, and the leftovers were handled by our origin servers.

Without Hydrolix we wouldn't have spotted the attack this early.

Hydrolix was also valuable to us in hindsight of the attack. Using the historical data

collected by the platform, we started an in-depth investigation, which led to remediations in our protection tools, some of which were deployed directly in connection to the attacks. The data Hydrolix collected was instrumental in piecing together what had happened. We could see that several attacks had hit different endpoints, trying to find different ways to bring down our sites. We looked at the traffic patterns and determined which actions to take to ensure a similar attack didn't happen again.

"Hydrolix has been working flawlessly and their support team has been very helpful and responsive."

Results

Using Hydrolix to find, contain, and remediate a massive DDoS attack in a very short time, without any impact to our users or sites crashing, speaks value in and of itself, although the platform helps in other ways too.

Our sites are dynamic. Many of our team members, from developers to content creators, in different countries, are making changes. It's difficult to get technical visibility into everything. When making new rules, Hydrolix supports us in creating rules correctly.

Hydrolix is fast and the query speed is great. We can rely on it to respond swiftly, and it has worked flawlessly since day one.

The Hydrolix support team has also been very helpful and responsive. At first, we had questions about features in the dashboards vs. the features other providers offer. The Hydrolix support team asked what we liked about a certain provider's dashboard features. Then that evening we received an email with a new dashboard that included many of the features we had said we enjoyed and were missing. The developers made a new dashboard quickly, just for us. We were very impressed.

Hydrolix has become an important part of our toolbox because it enables us to make better decisions to proactively reduce the risk on performance and security, while also reactively seeing what issues occurred and why.

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