Cribl | SWISSLOS

>SOLUTION BRIEF_

Swisslos Leverages Cribl Stream and Edge to Optimize Kubernetes and Enhance Splunk Performance

Swisslos is a Swiss lottery company that offers lotteries, sports bets, and instant tickets in Switzerland. A growing number of sports bets and live events has been increasing their data volumes to keep the platform performant–and increasing their daily profit, which is now up to $4 million daily.

An enormous amount of data is generated from all the physical and online stores selling Swisslos' offerings. A few years ago, the team switched to Kubernetes services to help automate the deployment, load balancing and scaling of their containerized applications. It helped to automate the IT team's workload, but soon the security team at Swisslos noticed that the number of logs generated each day—primarily from web application firewalls (WAF) and other critical applications-was growing at an unsustainable rate. The team needed to come up with a strategy to keep pace with rapid data growth while staying lean as a team and keeping costs for tools relatively flat.

Swisslos decided to bring in Cribl Stream to tackle the challenges posed by the increasing volume and fidelity of logging infrastructure.

Easy Management of and Reduction of Splunk License

With the increase in log volume and variety also came more complicated logs and several formatted in JSON— all of which took up valuable space in Swisslos's Splunk license. Most of the logs and the information within them weren't useful, so reducing unnecessary data was the first thing the team focused on.

Cribl Stream enabled them to filter their data effectively and store only what was necessary, helping to optimize their log storage and usage.

> "By using Cribl Stream, we were able to reduce the growth of our Kubernetes cluster by 35% – and we reduced our web application firewall and web logs by over 50%."
>
> — **Joris Vuffray**, Head of Network & System Management

HIGHLIGHTS

- Reduced size of Kubernetes cluster by 35%.
- 50% reduction in WAF and web logs.
- 3-5x return on admin time.

> “The pricing is very attractive, and the return on investment was really fast. It made a measurable difference within a couple of weeks.”

In addition to reducing that data, Joris and his team also use Cribl’s sampling feature, which allows them to bring in just enough data that their analysis remains statistically significant. This way, they can do any necessary troubleshooting from a small portion of data that is representative of the entire pool that was generated.

Increased Spunk Performance

Joris is making use of Cribl Stream’s enrichment capabilities as well, using lookups to do things like changing product IDs to product names. They also have an easier time adding GeoIP information using Cribl Stream instead of Splunk.
With less data overloading the application and better quality data going into it, Joris has noticed a huge improvement in Splunk’s performance.

> **“Everything we’re doing now in Cribl was done on the indexer or heavy forwarder before, so those parts of the Splunk installation have much less to do. Cribl helped us to significantly increase the performance of Splunk.”**
>
> — **Joris Vuffray**, Head of Network & System Management

Easy Access to Live Data In Real Time

The team at Swisslos was pleasantly surprised at how fast it was to set up and install Cribl Stream.

> **“We had Cribl Stream up and running within a few hours, and there was essentially no learning curve. In Splunk, we had to be creative and use some tricks to do everything we needed. It’s the opposite with Cribl.”**
>
> — **Joris Vuffray**, Head of Network & System Management

To see live data in Splunk, they had to change configs and restart it every time they wanted to see those changes. With Cribl, they’re able to see changes in real time.

> **“The most important benefit from Cribl is being able to see live data and the impact changes will have on the data in real time. The integrated change tracking is also pretty cool.”**
>
> — **Joris Vuffray**, Head of Network & System Management

Less Time Spent on Admin Work

One of the benefits of making these kinds of changes so quickly is the time that system admins get back in their day. The added flexibility is having a big impact on the organization.

> **“Our admins can do their work 3-5 times faster with Cribl. We can provide solutions for test or dev teams easier than before, when we had to check configurations and restart the Splunk installation every time we made big changes.”**
>
> — **Joris Vuffray**, Head of Network & System Management

Increased Visibility Into Kubernetes

Before implementing Cribl Stream, Swisslos struggled with managing the vast amount of data that needed to be logged out of their Kubernetes cluster. Keeping all of their data in the same place made security monitoring difficult, and they were looking for an easier way to route data to specific indexes within Splunk. Cribl gives them the ability to route and retain data in different indexes with specific time retention to speed security investigations, and optimize the teams’ time.

> **“In Splunk, we had to use loads of regexes to rewrite formats, source types, and indexes. We can do this live in Cribl and send it to Splunk very easily, already sorted and routed to the right index or source type.”**
>
> — **Joris Vuffray**, Head of Network & System Management

Faster Incident Response Times

Swisslos can also respond faster to security incidents since making Cribl Stream a part of their infrastructure. They resolved a recent security issue in a fraction of the usual time with the help of Cribl Stream. They could quickly isolate the data necessary for the investigation and because it was already enriched, searches populate faster helping analysts to reduce mean time to remediation (MTTR).

> **“It only took a few minutes to gather the information we needed to respond to the security attack. We took care of it on the phone in one afternoon, when normally it would have taken two weeks. We just took care of it.”**
>
> — **Joris Vuffray**, Head of Network & System Management

> **“Deploying an application in a testing environment used to generate hundreds of GBs in 15 minutes. We can now sample it in a couple of seconds to make sure we’re still compliant with our Splunk license.”**

Staying Ahead of Regulatory Requirements

GDPR compliance regulations aren’t as strict in Switzerland as they are in the rest of the EU, but since Swisslos has customers in Lichtenstein, they do have some compliance requirements they need to follow. They’ve also begun experimenting with Stream’s encryption and masking capabilities to prepare for the inevitable, stricter regulations that are on the way.

> **“When it comes to regulations, we don’t always know what will be required in the future. But with Cribl Stream in place, I don’t really have to worry about it. My management can just tell me what information needs to be masked or encrypted, and it will be done in a few clicks.”**
>
> **— Joris Vuffray**, Head of Network & System Management

Using Cribl Edge to Pull Data From Kubernetes

Swisslos is also using Cribl Edge, so they won’t have to rely on using Fluentd to gather data from Kubernetes. Edge offers automatic discovery of host, container, and application data on endpoints and gives users extra processing power with its functions and pipelines. The UI allows you to explore, preview, and build configs before forwarding data to any of the many supported destinations. Compared to Fluentd, not only is the combination of Cribl Edge and Stream faster and easier to use, it’s also turnkey–significantly reducing the long term build and maintenance workload for the team.

> **“We have Cribl Edge installed on all of our test Kubernetes nodes to gather logs and metrics. So far, it’s already a lot easier than deploying the Splunk forwarder. It deploys in five minutes, and then it’s done.”**
>
> **— Joris Vuffray**, Head of Network & System Management

TL;DR

- Decreased growth of Kubernetes cluster by 35%.
- Reduced web application firewall and web logs by over 50%.
- Improved Splunk performance with higher quality data.
- Recovered admin time .
- Increased visibility into Kubernetes with live, real-time changes in Cribl Stream.
- Faster incident response times from easy searches with Stream.
- Easy compliance with GDPR and other regulatory requirements.
- Reduced MTTR by 95%.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl’s vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl’s product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry’s leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry’s first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

©2024 Cribl, Inc. All Rights Reserved. ‘Cribl’ and the Cribl Flow Mark are trademarks of Cribl, Inc. in the United States and/or other countries.
All third-party trademarks are the property of their respective owners.

CS-0010-EN-2-0624