>CASE STUDY_

How Vijilan is Future Proofing Data Management with Cribl

HIGHLIGHTS

- Reduced AWS infrastructure costs through data filtering
- Gained the ability to offer competitive pricing for different retention needs
- Opened opportunities for new revenue streams for MSP partners in regulated industries
- Reduced time-to-market for new data sources from one month to one week

Vijilan Security

Vijilan Security is one of the industry's leading Managed Extended Detection and Response (mXDR) providers, serving over 200 MSPs and over 750 end customers. The Vijilan team found that customer data volume was growing year-on-year and becoming increasingly difficult to manage and expensive to store. Cribl Stream helped them overcome these challenges.

Looking ahead to the next three to five years, the Vijilan team anticipated an even greater data deluge. They realized it was time to move away from their existing log management solution and adopt a more modern approach. Using Cribl Stream for data ingestion and Cribl.Cloud to deploy dedicated workspaces in each end customer environment, Vijilan has reduced infrastructure costs, streamlined parser development, achieved better control over data, and even provided new revenue streams for its partners.

Greater Control Over Data

Vijilan's founder and CEO, Kevin Nejad, explored several other log ingestion solutions before settling on Cribl Stream. For him, the control over data Cribl Stream offers sets it apart.

> **"I love the fact that Cribl gives you complete control over data from the point of ingestion up to its destination. You can control its entire journey. Some of the other technologies out there can't do that. This is really important because things do change, things do evolve; there's always the possibility of a sudden change in the way you want to store and manage data."**
>
> —**Kevin Nejad**, founder and CEO at Vijilan Security.

Moreover, with traditional log management solutions, changes in log formats - such as the ongoing shift from syslog to ADI and JSON - would require Vijilan to replace technology in end customer environments, which requires considerable work. Cribl Stream, however, offers the flexibility necessary for Vijilan to adapt to evolving data formats without overhauling existing technologies.

> **"In life, only three things are inevitable: death, taxes, and change. With Cribl, we are certain that if data formats change or the way we collect data changes, we don't have to overhaul the technology in end customer environments. Or even if we decided to provide a service for serviceability, not just cybersecurity, we could use the same technology for that."**
>
> **—Luis Medici**, CPO at Vijilan Security.

Reduced Infrastructure Costs

As Vijilan's partners primarily cater to small and medium-sized businesses, cost-effectiveness is everything. Before data hits expensive components like SIEM platforms and other costly areas, Cribl Stream allows Vijilan to filter data before ingestion, significantly reducing AWS infrastructure costs by minimizing unnecessary data and lowering storage, compute, and data transfer expenses.

> **"By being able to filter data and control what we're ingesting, we're able to lower our AWS infrastructure costs, which has a significant impact on our gross profit margin."**
>
> **—Luciana Furtado**, co-founder and CFO at Cribl.

New Revenue Streams

The ability to filter and mask data before ingestion has also opened up new revenue streams for Vijilan's MSP and MSSP partners. Vijilan's previous log management solution lacked the data masking and filtering capabilities necessary for MSPs to penetrate more regulated industries. Cribl Stream, however, does have these capabilities, opening up new revenue streams for Vijilan's partners.

> **"When I talk to our partners, they're all about providing solutions that meet compliance requirements. When I told them that, with Cribl Stream, our solution would include data masking and filtering capabilities, they were ecstatic. They weren't aware that this kind of technology existed for MSPs. It's helping them gain access to industries that were previously out of reach."**
>
> **—Kevin Nejad**, founder and CEO at Vijilan Security.

Similarly, Cribl Stream's data filtering capabilities allow Vijilan's partners to offer more tailored, affordable solutions - for example, not all end customers need to store raw logs or maintain data over extended periods. Filtering data before ingestion allows MSPs to minimize unnecessary data storage, tailoring offerings to customers who only need short-term storage or smaller data sets, meaning they can expand into new markets.

Reduced Time to Market for New Data Sources

Since adopting Cribl Stream, Vijilan has also significantly reduced the time to market for new data sources. For example, creating a parser for a new vendor was a complex and time-consuming process. Thanks to Cribl Stream's user-friendly UI, Vijilan has reduced the time to create a new parser from a month to just one week.

> **"We developed a methodology using Cribl to collect sample data and have cybersecurity experts use these samples to create new packs. Previously, we relied on live customer data to build parsers, which was challenging. With Cribl, we can use sample files, making the process faster, simpler, and more efficient."**
>
> **—Luis Medici**, CPO at Cribl

TL;DR

- Filtering data before ingestion minimizes unnecessary data, cutting AWS infrastructure costs
- Ability to offer tailored solutions based on different data retention needs, improving affordability for customers.
- Data masking and filtering capabilities help MSP partners access regulated industries and expand offerings.
- Reduced parser creation time from one month to just one week using Cribl's user-friendly UI.
- Cribl Stream offers control over data from ingestion to destination, adapting to changing formats without significant overhauls.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Powered by a data processing engine purpose-built for IT and Security, Cribl's product suite is a vendor-agnostic data management solution capable of collecting data from any source, processing billions of events per second, automatically routing data for optimized storage, and analyzing any data, at any time, in any location. With Cribl, IT and Security teams have the choice, control, and flexibility required to adapt to their ever-changing data needs. Cribl's offerings–Stream, Edge, Search, and Lake–are available either as discrete products or as a holistic solution.

Learn more: www.cribl.io | Join us: Slack community | Follow us: LinkedIn and X (formerly Twitter)