BlueVoyant | Cribl

CASE STUDY

BlueVoyant Offers Next-Generation Cybersecurity Services, Backed By Cribl

CASE STUDY

BlueVoyant Offers Next-Generation Cybersecurity Services, Backed By Cribl

BlueVoyant is a cybersecurity service provider specializing in advanced technologies that support world-class offerings designed to protect organizations from today's agile, well-financed attackers.

In the aim of protecting their customers, Blue Voyant's technology teams process and cross-correlate staggering quantities of data from hundreds of different data sources, processing over 3 million events per second in their threat intelligence practice alone. A system capable of parsing, routing, and analyzing security telemetry and massive internet metadata at this scale requires not only tremendous power but also tremendous flexibility. BlueVoyant chose to work with the team at Cribl to leverage some of Cribl LogStream's special talents — smart routing, field extraction, data masking, and real-time detection at the edge, all manageable from a central console — when designing the architecture of their custom data processing pipeline for their managed security services offering.

HIGHLIGHTS

LogStream™ helps keep BlueVoyant ahead of a 1000x increase in attacks since March 2020.

With Cribl, new data sources are onboarded rapidly to add to BlueVoyant's arsenal.

The team at BlueVoyant trusts Cribl's deep expertise and architectural input.

Boosting performance to stay ahead of escalating trends in cybersecurity

As a result of the current Covid-19 pandemic, many more workers than usual are connecting to business networks from home systems, resulting in a vastly-expanded attack surface for bad actors. The analyst teams at BlueVoyant are detecting and combating a thousandfold increase in the levels of domain impersonations and other attack types taking advantage of businesses needing to operate with strained technical resources.

Resilience and speed are critical to successful outcomes when a live threat is in play. Using Cribl LogStream, the BlueVoyant team leverage blazing-fast, real-time detection of critical events, accelerating time to understanding and resolution.

> *"Detection at the edge is critical, we don't have to wait for saved searches, indexing, or lookups to run." — Chris White, BlueVoyant Chief Security Officer*

As more data is brought in to grow BlueVoyant's ability to detect and stop malicious activity, the need to scrub, restructure, and mark it up rapidly becomes vital. Errors in onboarding new sources are costly, and normalizing the data would typically take precious time without Cribl.

THE CRIBL TEAM UNDERSTANDS OUR BUSINESS REQUIREMENTS; IT'S A GREAT DESIGN PARTNERSHIP."

– CHRIS WHITE, CSO, BLUEVOYANT

"Doing this normalization would be a lot of work, but LogStream makes it very simple for us. We can fork the data and play with it, and only THEN put it into production, when it's right."
— Jake Vance, BlueVoyant Head of Splunk Operations

A rapidly-growing number of data sources and use cases in play means a profusion of agent configurations to manage, but with LogStream, it's not an issue.

"Cribl simplifies everything; we can manage it all from a central location. Before, we were managing props and transforms all over the place."
— Jake Vance, BlueVoyant Head of Splunk Operations

A trusted and verified design partnership leads to greater insights for the customer

The systems architects at BlueVoyant work with the Cribl team as design partners as they expand and scale their service, leveraging LogStream to both take advantage of Splunk's strengths and mitigate its shortcomings at scale.

"The Cribl team understands our business requirements; it's a great design partnership. They understand how a given change will impact us— how to scale it out effectively and safely for our hundreds of clients." — Chris White, BlueVoyant Chief Security Officer

Because their custom cybersecurity platform is built to leverage the speed and precision of LogStream, the BlueVoyant team is able to do greater things for their customers.

"LogStream allows us to offer our customers significantly more insight into the cybersecurity implications of their data, well beyond compliance. Our clients are getting substantially greater security value out of the data they have, with our use of Cribl's technology."
— Chris White, BlueVoyant Chief Security Officer

Find out how your business can implement an observability pipeline to parse, restructure, and enrich data in flight, while cutting costs and simplifying operations.

Get Cribl, and take control of your data.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and machine data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.