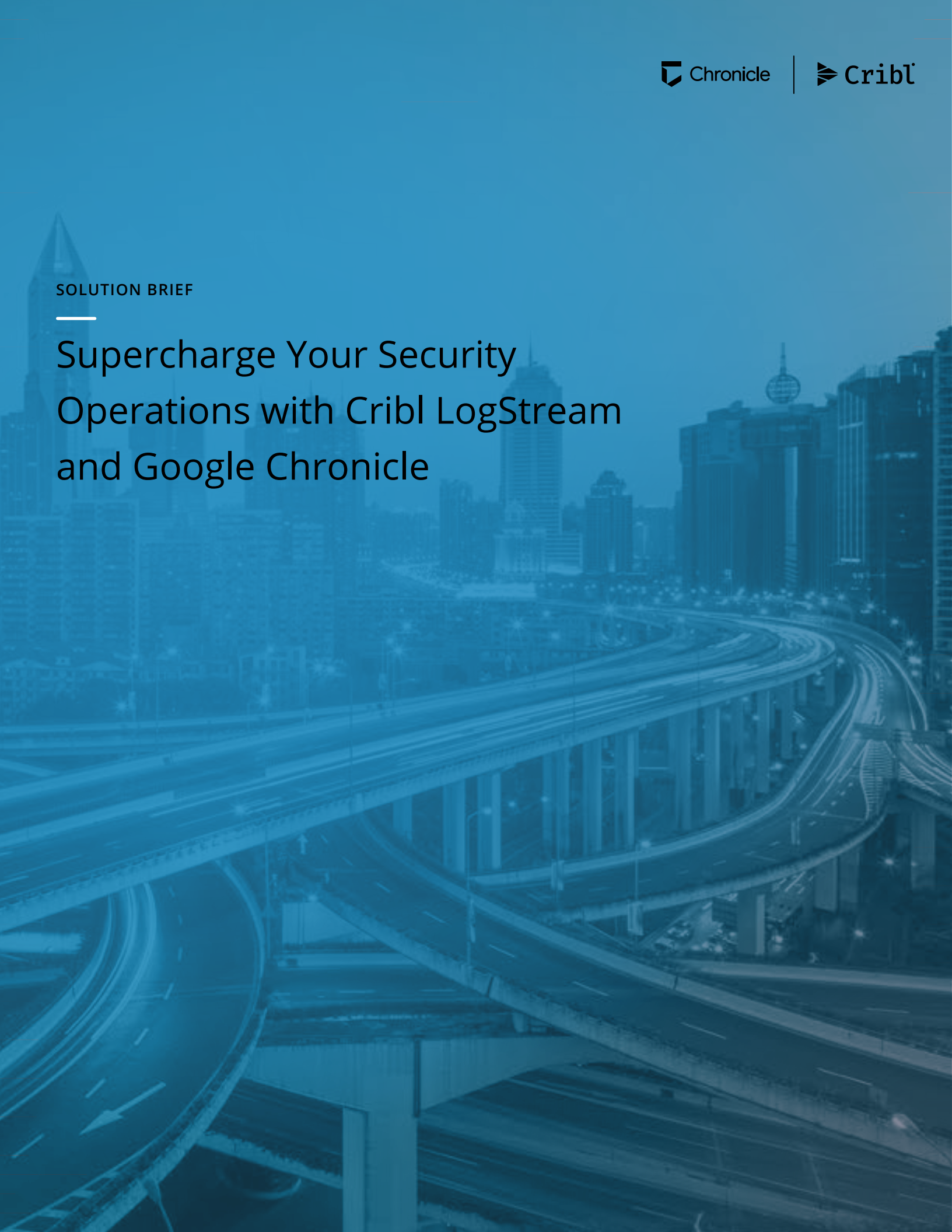
Chronicle | Cribl

SOLUTION BRIEF

Supercharge Your Security Operations with Cribl LogStream and Google Chronicle



SOLUTION BRIEF

Supercharge Your Security Operations with Cribl LogStream and Google Chronicle

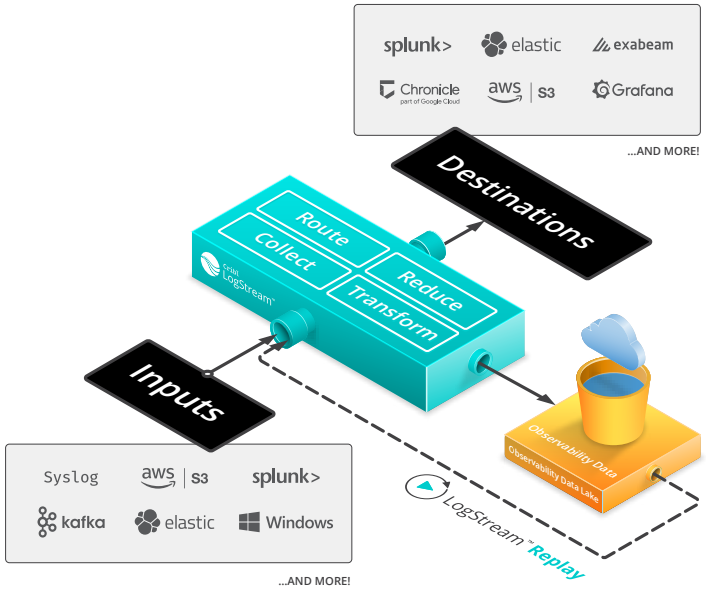
Together, Cribl LogStream and Google Chronicle provide a way for SecOps teams to support massive amounts of data regardless of retention level, increasing efficiency and improving outcomes in the Security Operations Center (SOC).

The Power of Google Chronicle and Cribl LogStream

Chronicle was made for organizations that want to manage petabytes of data in the cloud – at unprecedented retention levels. It's a powerful platform that runs on core Google infrastructure, meaning they don't have to exhaust all their resources managing data systems at scale. Google Cloud Threat Intelligence for Chronicle gives these enterprises global-scale threat intelligence; BigQuery and Looker provide them with a way to visualize that security data via dashboards and more.

Those same organizations are turning to Cribl LogStream for similar reasons. They need an observability pipeline with the flexibility to get data into multiple tools from multiple sources without adding new infrastructure and agents. These companies also need a cost-effective strategy for retaining data long-term. At the same time, they need an observability solution that gives them the flexibility to make new business decisions and test out new use cases at scale, regardless of the amount of data they have.

Together, Cribl LogStream and Google Chronicle provide a way for SecOps teams to support massive amounts of data regardless of retention level. When you further combine LogStream and Chronicle with Google Cloud Threat Intelligence, Looker, and BigQuery, security teams unlock a powerful toolset to create brand new visual workflows, increase efficiency, and improve SOC outcomes.



THE CHALLENGE

Companies using Google Chronicle to manage multi-petabyte cloud data systems need an observability pipeline to match – giving them the flexibility to try new tools, test out new use cases, and make new business decisions at scale.

THE SOLUTION

Cribl LogStream is an essential part of any observability solution, providing a pipeline that works with all tooling at any scale, making it the perfect complement to Google Chronicle – and unlocking a powerful toolset that increases efficiency and improves SOC outcomes.

THE BENEFITS

- Easily try out new SIEM vendors, like Google Chronicle
- Pull events from Chronicle and leverage webhooks to convert them into actionable events for further investigation
- Get data into Chronicle without the added licensing costs and resource usage of Chronicle Forwarder
- Integrate Chronicle, Google Cloud Threat Intelligence, BigQuery, and Looker with any other tool in your stack

WITH LOGSTREAM, YOU CAN NORMALIZE BOTH STRUCTURED AND UNSTRUCTURED DATA IN-FLIGHT, ENSURING IT ARRIVES IN CHRONICLE IN THE FORMAT YOU NEED.

The Benefits of using Chronicle with LogStream

EASILY TRY OUT NEW SIEM VENDORS, LIKE GOOGLE CHRONICLE

LogStream can send data to and from anywhere, helping you further avoid vendor lock-in and test out new tools. Wanting to evaluate Chronicle for your organization? Use LogStream to route the same data to both your current SIEM and Chronicle for a pain-free assessment.

PULL EVENTS FROM CHRONICLE AND LEVERAGE WEBHOOKS TO CONVERT THEM INTO ACTIONABLE ALERTS FOR FURTHER INVESTIGATION

With Cribl LogStream's built-in integration for Chronicle, you can pull security events straight from the SIEM and leverage webhooks to get alerts on the tool of your choice for further investigation and faster incident response.

GET DATA INTO CHRONICLE EASILY – WITHOUT ADDED LICENSING COSTS AND RESOURCE USAGE

Getting certain data in Chronicle can be tricky: Chronicle accepts both structured and unstructured data, meaning it often needs special formatting prior to forwarding. With LogStream, you can restructure and normalize data in-flight, ensuring it arrives in Chronicle in the format you need. No additional software required.

INTEGRATE CHRONICLE, GOOGLE CLOUD THREAT INTELLIGENCE, BIGQUERY, AND LOOKER WITH ANY OTHER TOOL IN YOUR STACK

Because Cribl LogStream is a universal receiver and router, you can smoothly and securely integrate Chronicle, Google Cloud Threat Intelligence, BigQuery, and Looker with any other tool in your environment – regardless of vendor.

Summary

Looking for a better way to affordably manage multi-petabyte data systems in the cloud, many enterprises are turning to Chronicle – and later implementing Google Cloud Threat Intelligence, Looker, and BigQuery to create new visual workflows, increase efficiency, and improve SOC outcomes. These same enterprises now need an observability tool to match: flexible, cost-effective, and reliable. Cribl LogStream is an observability pipeline that provides the simplicity, flexibility, and control to work with any tooling, reduce the cost of long-term storage, and perform well with even the largest amounts of data – making it the perfect complement to Chronicle.

With Cribl LogStream, anyone can:

- *Easily try out new SIEM vendors, like Google Chronicle*
- *Pull events from Chronicle and leverage webhooks to convert them into actionable events for further investigation*
- *Get data into Chronicle easily – without added licensing costs and resource usage*
- *Integrate Chronicle, Google Cloud Threat Intelligence, BigQuery, and Looker with any other tool in your stack*

TOGETHER, CRIBL LOGSTREAM AND GOOGLE CHRONICLE PROVIDE A WAY FOR SECOPS TEAMS TO SUPPORT MASSIVE AMOUNTS OF DATA REGARDLESS OF RETENTION LEVEL, INCREASING EFFICIENCY AND IMPROVING OUTCOMES IN THE SECURITY OPERATIONS CENTER (SOC).

Together, Cribl LogStream and Google Chronicle provide a way for SecOps teams to support massive amounts of data regardless of retention level. When they further combine LogStream and Chronicle with Google Cloud Threat Intelligence, Looker, and BigQuery, security teams unlock a powerful toolset to create brand new visual workflows, increase efficiency, and improve SOC outcomes.

To get started with Chronicle and Cribl LogStream today, **click here to sign up for LogStream Cloud**. The **Cribl Slack Community** is also a great place to connect with leaders from other teams leveraging both Chronicle and Cribl.

ABOUT CHRONICLE

Cybercrime now affects billions of people globally, and the organizations responsible for protecting critical information and systems need more help to keep up. Cybersecurity needed a moonshot. Chronicle was born in 2016 as a project within X, Alphabet's moonshot factory. As an Alphabet company, we bring unique resources and talent to the goal of giving enterprises, and the people within them, the tools to win the fight against cybercrime. We see a future where enterprise security teams can find and stop cyberattacks before they cause harm. By applying planet-scale computing and analytics to security operations, we provide the tools teams need to secure their networks and their customers' data. We turn the advantage to the forces of good. For more information, visit **chronicle.security**.

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 observability 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.