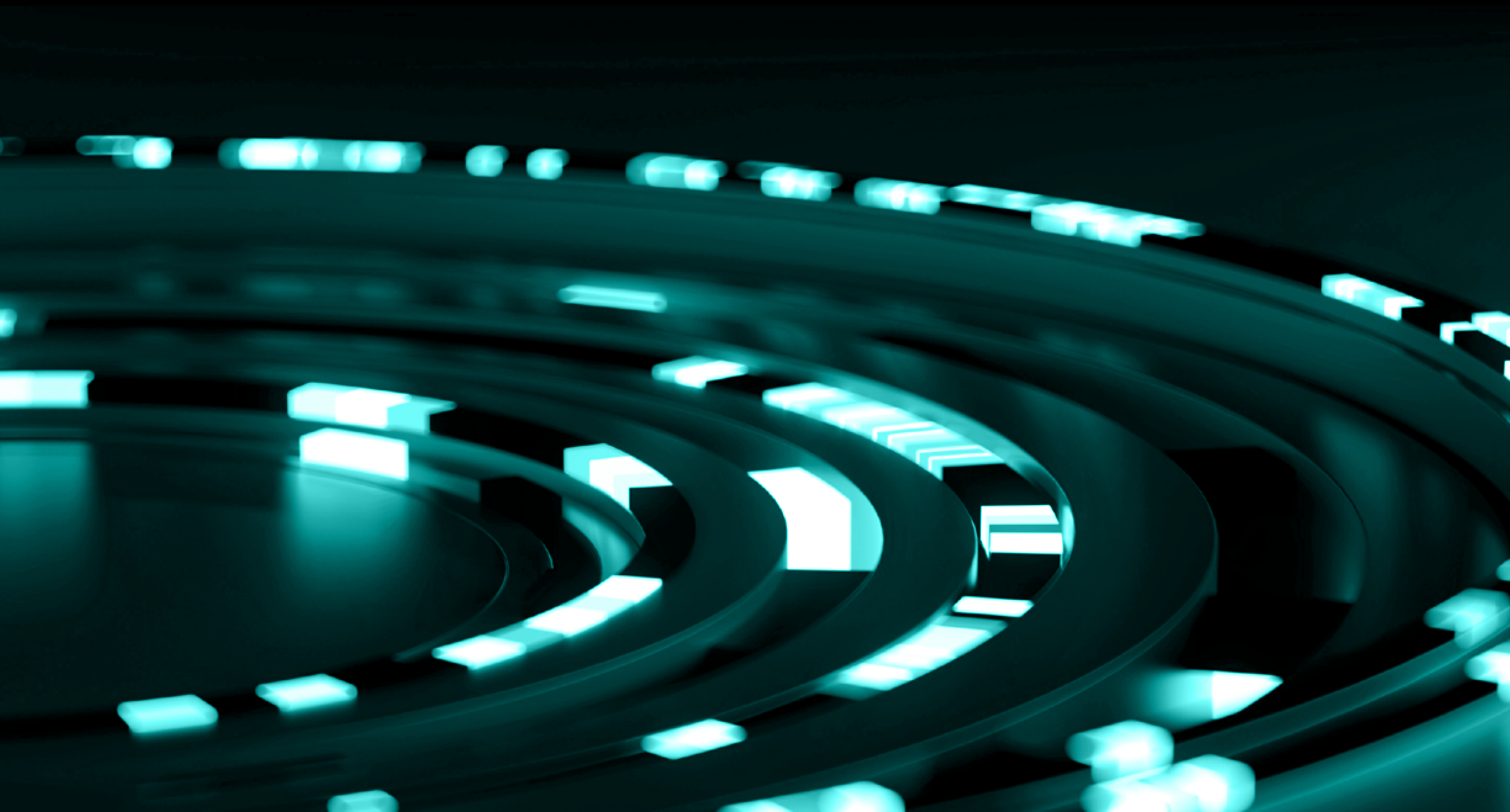
Cribl

WHITE PAPER

Using Cribl Stream Cloud to Integrate SaaS Platform Logging Into Your Analytics and SIEM Platform



THE CHALLENGE

Enterprises need to securely consume more and more data from Cloud SaaS platforms which is a challenge due to operational complexity around data and security concerns around increased attack surface.

THE SOLUTION

Cribl Stream Cloud provides an easy to use cloud native solution to solve both complexity and security challenges.

THE BENEFITS

- Reuse your existing data sources and agents to route observability data to the Elastic Stack
- Achieve big savings by retaining observability data in lower-cost object storage
- Make it easier to migrate your data from older versions of Elastic
- Easily execute data migrations at scale from one tool to another
- Eliminate data with little analytical value before sending to Elastic to control costs

WHITE PAPER

Using Cribl Stream Cloud to Integrate SaaS Platform Logging Into Your Analytics and SIEM Platform

With the proliferation of Security SaaS platforms, such as Cloudflare, Proofpoint, and PingOne, enterprises must figure out how to integrate third-party data that is shipped over the internet into their analytics and SIEM platforms. This requirement to integrate third-party data raises a host of security, infrastructure, and data quality questions. Enterprises can lower risk, and complete projects faster, by using Cribl Stream Cloud to solve their challenges in managing third-party SaaS platform data.

Overview

KEY CHALLENGES

Enterprises have a common set of questions and concerns about SAAS logging integration:

1. *How do we securely exchange data with SAAS platforms over the Internet?*
2. *How do we support protocols such as syslog that do not support authentication?*
3. *How do we manage allowed lists with SAAS platform source IP addresses constantly changing?*
4. *How do we support a number of data delivery options with no clear standards, more formats means more overhead?*

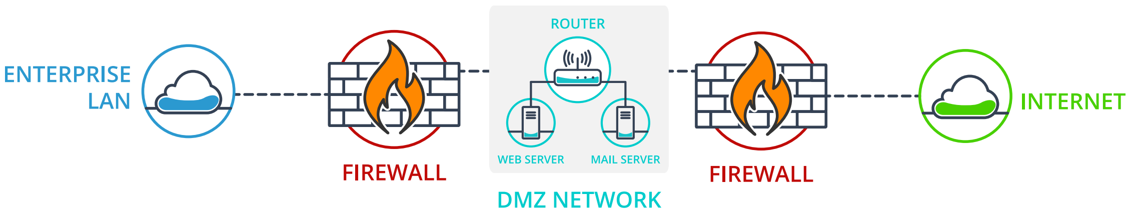
Enterprises have a common set of questions and concerns about SAAS logging integration:

1. *Deploy server and load balancer resources to the DMZ*
2. *Setup logging tools that are then exposed over the Internet to support logging*
3. *Add every possible logging source to an allow list, deny all other sources*
4. *Put in other controls as required to ensure DMZ resources are secure*

CRIBL CLOUD REDUCES THE ENTERPRISE THREAT SURFACE TO JUST THE ENTERPRISE PERIMETER AND CRIBL CLOUD. SMALLER THREAT SURFACE EQUALS LESS RISK.

CRIBL CLOUD CAN ONBOARD NEW LOGS IN MINUTES, SAVING PRECIOUS TIME AND FREEING UP ENGINEERING FOR MORE HIGH VALUE WORK.

DMZ NETWORK ARCHITECTURE



This approach can have a number of operations and security challenges. Maintaining firewall access groups for every cloud logging source is a non-stop job. Your network team will not be pleased. With the usual change process, you are looking at 7-10 day of delay which could compromise your logging by not getting data you need.

Putting infra in the DMZ creates risk with more exposure to potential security issues and the associated delay for many companies with deploying onprem infrastructure. Does your logging tool support all the different logging options SAAS platforms can offer? Staffing and skill set are always an issue, which means even more delay and a growing backlog.

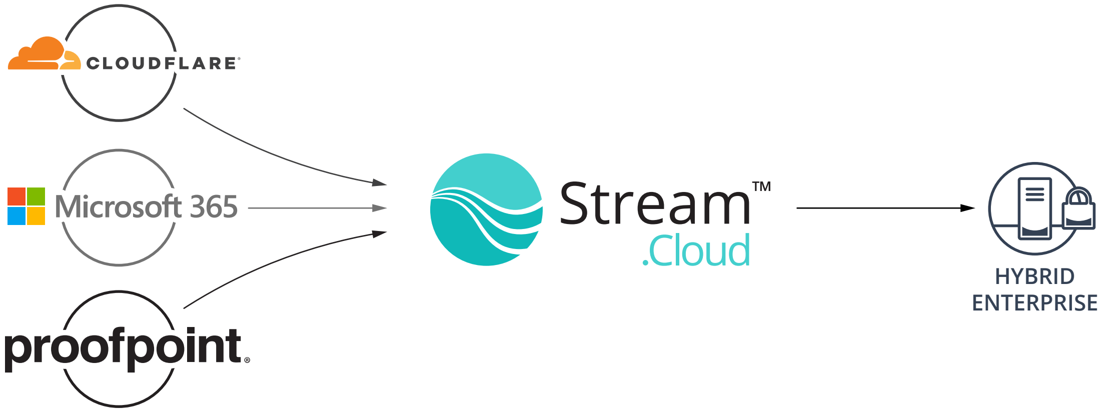
Recommendations

MADE EASIER IN THE CLOUD

These challenges get easier with the release of Stream Cloud. Use Stream Cloud to handle connections from all of your SaaS data sources. Then transform the data to your preferred format and ship it to your logging platform.

Instead of managing an allow list for potentially thousands of IP addresses, only manage sources from Cribl Stream Cloud. Instead of exposing your infrastructure to the Internet, only allow access from Cribl Stream Cloud. Instead of deploying different solutions or home grown scripts to consume different data sources, use the Stream Cloud's flexible framework to handle everything. Instead of deploying substantial infrastructure to handle logging, only deploy enough to consume the output from Stream Cloud.

Your enterprise gets the benefit of fast deployment and Cribl Stream Cloud manages the security risk of interfacing with different SAAS platforms. You can lower risk and get fast results.



CIBL CLOUD HELPS SIMPLIFY YOUR NETWORK ARCHITECTURE BY GIVING YOU AN OPTIONS BASED APPROACH TO INTEGRATING WITH EXTERNAL DATA SOURCES.

HELP “JOHN” OUT BY UPDATING YOUR FIREWALL ACCESS POLICIES TO SUPPORT THE EXTERNAL DATA SOURCES.

A Story About John

This is an allegory and not based on actual events....

This could happen to any overworked engineer; John, the firewall admin, has request after request to add SAAS logging sources to the DMZ firewall to enable platforms, like Cloudflare, to push data to the Enterprise logging platform. The task is quickly becoming a problem with thousands of potential sources and some platforms unable to provide a static list of sources at all.

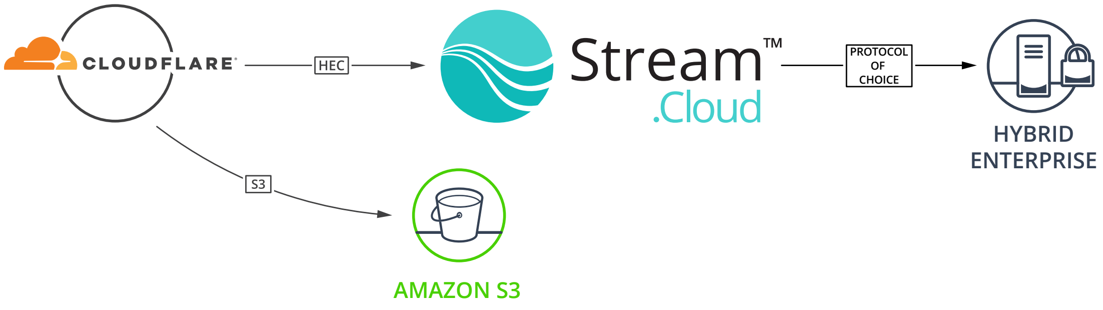
BACKGROUND

John’s enterprise has a policy to strictly define source IP and destination IP for every firewall rule. This is a fairly standard process for legacy enterprises, but does not scale well to account for SAAS platforms that constantly scale and change on demand. Cloud technologies like autoscaling and service migration across regions – reasons why companies use Cloud in the first place – make these types of policies unrealistic in cloud or hybrid environments. Policy definitions quickly fall out of date, leading to misconfigurations and potentially exposing your company to a security breach.

Back to our overworked firewall admin .... John had a request to add hundreds of IP addresses to the DMZ firewall to support a new SAAS platform. The requestor made a mistake and the request contained IPs addresses that were instead owned by cyber criminals operating out of Russia. John was too busy creating enormous object groups to support the enterprise firewall policy and could not verify every IP address was actually owned by the SAAS platform. A few hours after the change, servers out of Europe and Africa started probing the exposed external interfaces for the logging platform and found an issue with the API and compromised the logging platform. The hackers were able to pivot off the DMZ and into the heart of the network.

How do enterprises get the best of both worlds where risk is minimized and capabilities are maximized?

BASIC CRIBL STREAM CLOUD INTEGRATION WITH CLOUDFLARE

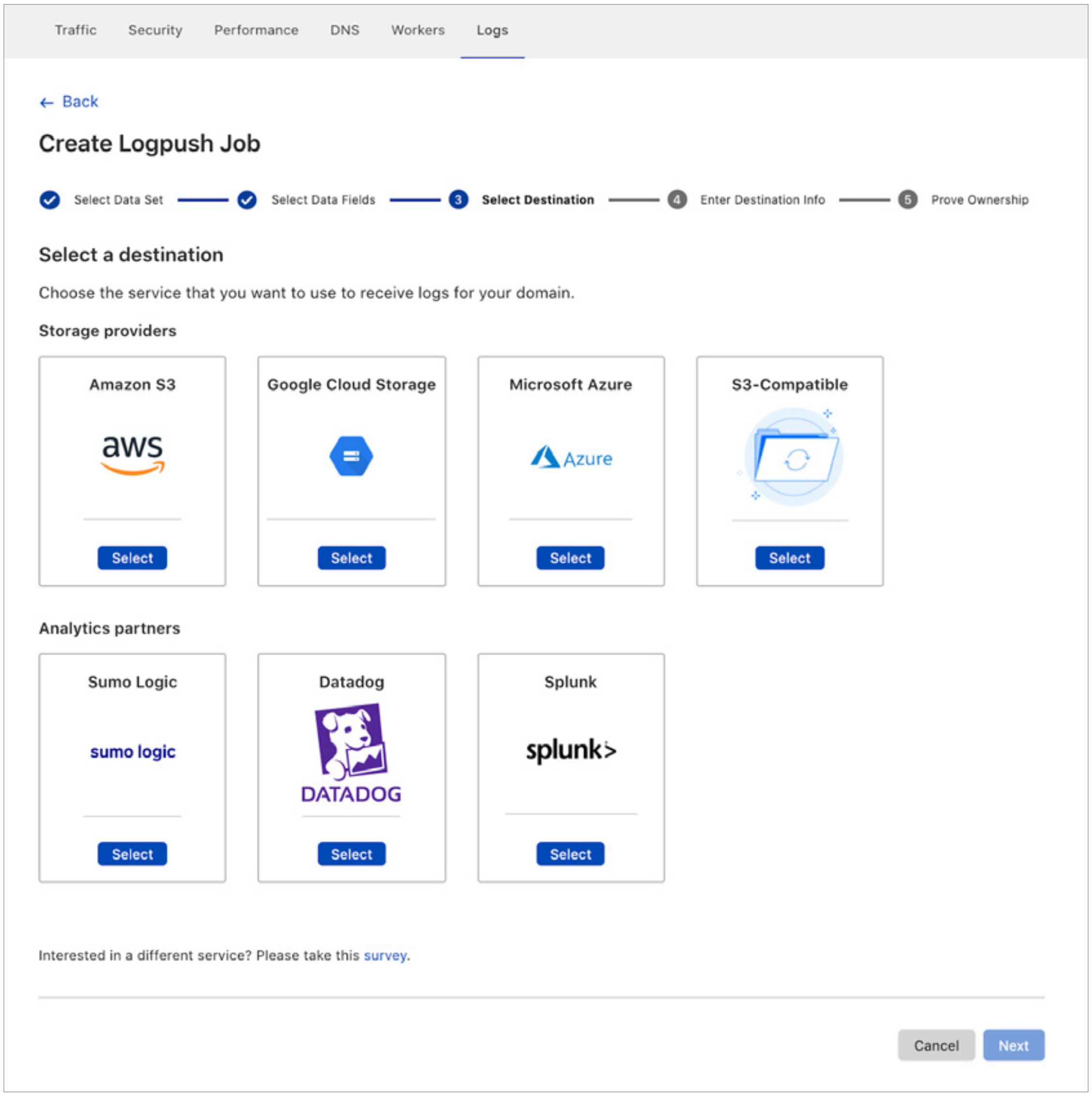


ONBOARD CLOUDFLARE LOGS IN MINUTES USING CRIBL CLOUD.

Cloudflare is a very popular SaaS platform that provides a number of services including managed DNS, CDN, WAF, and DDOS mitigation. It has enormous scale, and provides detailed data that any enterprise would want in its analytics and SIEM platforms.

If your enterprise requires Cloudflare logging, it only needs to do the following to integrate Cloudflare into Stream Cloud:

1. *Create an allow list for Stream Cloud data sources to reach your logging platform, either in the Cloud or on-prem. Platform docs can supply a list and/or a block of IP addresses.*
2. *Create a Stream Cloud account: https://cribl.cloud/*
3. *Review Cloudflare documentation at: https://developers.cloudflare.com/logs/*
4. *You have two options for ingesting Cloudflare logs with plus/minus for either approach:*
    - *AWS S3 bucket – Cloudflare writes data to your S3 bucket, and Stream Cloud consumes the data and pushes it to your destination.*
    - *Splunk HTTP Event Collection (HEC) – you create a HEC source in Stream Cloud. Splunk HEC is a secure, high-volume alternative if AWS S3 is not an option.*



Create Logpush Job

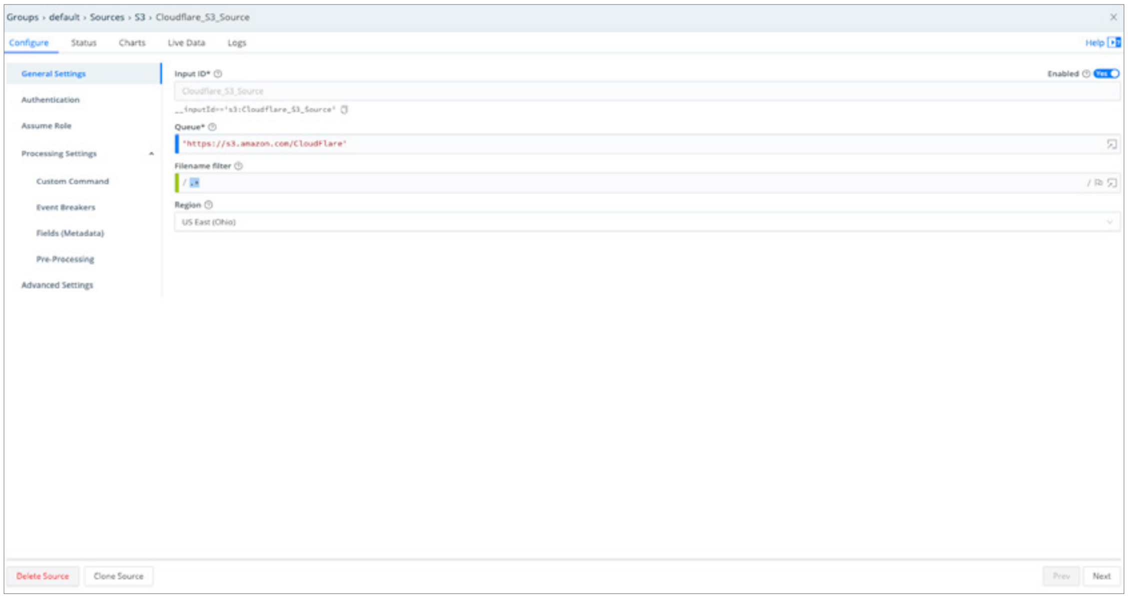
Select a destination

Choose the service that you want to use to receive logs for your domain.

Interested in a different service? Please take this survey.

CRIBL CLOUD SUPPORTS BOTH S3 AND SPLUNK HEC DATA SOURCES.

5. *If you choose the AWS S3 bucket option, then create a Stream S3 Source. See: https://docs.cribl.io/docs/sources-s3*



Input ID* Cloudflare_S3_Source

Enabled Yes

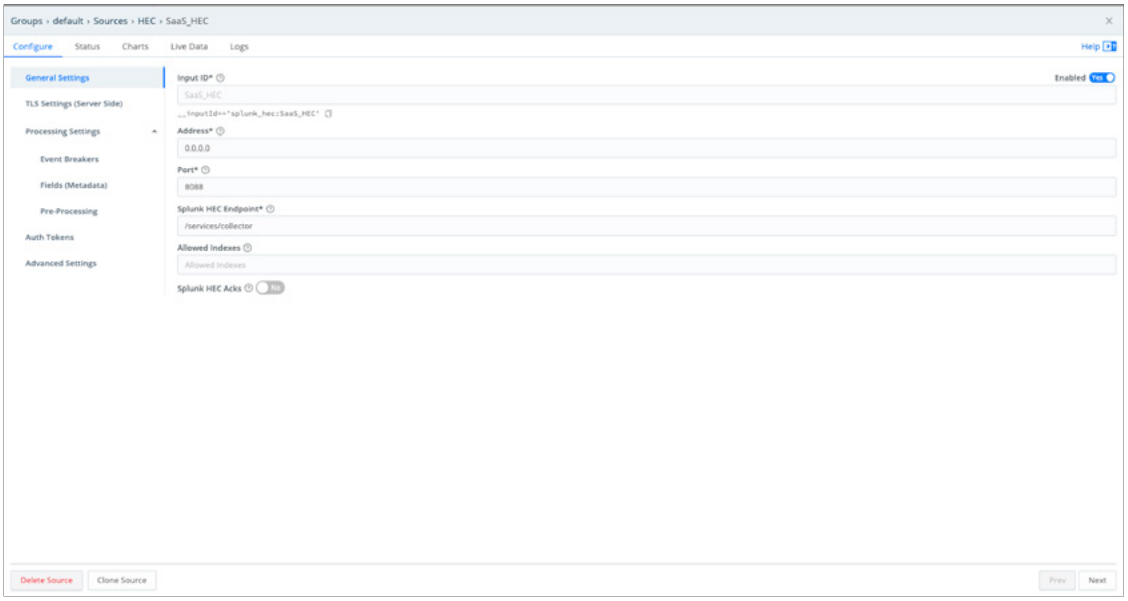
`__inputId=='s3:Cloudflare_S3_Source'`

Queue* `'https://s3.amazon.com/CloudFlare'`

Filename filter `/.*/`

Region US East (Ohio)

6. *If you choose Splunk HEC, then create a Splunk HEC Source. See: https://docs.cribl.io/docs/destinations-splunk-hec*



Input ID* SaaS_HEC

Enabled Yes

`__inputId=='splunk_hec:SaaS_HEC'`

Address* 0.0.0.0

Port* 8088

Splunk HEC Endpoint* /services/collector

Allowed Indexes Allowed Indexes

Splunk HEC Acks No

7. Use the Cloudflare console to configure logging per your data-source decisions: *https://developers.cloudflare.com/logs/get-started/logpush-dashboard*

8. Once you make your ingest decision, then you determine your format:
    - *The data is in JSON by default.*
    - *Most platforms fully support JSON, but with Stream, you have transformation options.*

9. *Finally, ship the data securely – using the method of your choice – back to your analytics platform. See: https://docs.cribl.io/docs/destinations*

SAVE YOURSELF TIME AND LIMIT RISK TO YOUR ENTERPRISE BY USING CRIBL CLOUD TO INTEGRATE EXTERNAL DATA SOURCES WITH YOUR ANALYTICS PLATFORM.

We will provide you with more examples for SAAS integrations in future blog posts.

*Back to John....*John only had to make one firewall change to support the enterprise using Cribl Stream Cloud. John is instead working on customer facing requests and adding value to the business instead of chasing the impossible task of controlling thousands of cloud ip addresses. The logging team is able to add new SAAS data sources in hours and days instead of weeks. The needs of the business benefit from speed to solution and less time spent on

Bottom Line

Adopting Stream Cloud to integrate SaaS logging reduces risk, and increases speed to solution. Giving enterprises easier, faster access to SaaS platform data, while maintaining a strong security posture. Want more information? Join the **Community Slack**, and sign up for Cribl Cloud, free up to 1 TB/day, at **https://cribl.cloud/**.

ABOUT CRIBL

Cribl makes open observability a reality for today's tech professionals. The Cribl product suite defies data gravity with radical levels of choice and control. Wherever the data comes from, wherever it needs to go, Cribl delivers the freedom and flexibility to make choices, not compromises. It's enterprise software that doesn't suck, enables tech professionals to do what they need to do, and gives them the ability to say "Yes." With Cribl, companies have the power to control their data, get more out of existing investments, and shape the observability future.Founded in 2017, Cribl is a remote-first company with an office in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.