

aws marketplace

Cribl

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 9

Other Solutions Considered..... 10 - 11

ROI..... 12

Use Case..... 13 - 15

Setup..... 16 - 20

Customer Service and Support..... 21 - 23

Other Advice..... 24 - 26

Trends..... 27 - 28

About PeerSpot..... 29 - 30

Product Recap



Cribl

Cribl Recap

Cribl optimizes log collection, data processing, and migration to Splunk Cloud, ensuring efficient data ingestion and management for improved operational efficiency.

Cribl offers seamless log collection directly from cloud sources, allowing users to visually extract necessary data and replay specific events for in-depth analysis. It provides robust management of events, parsing, and enrichment of data, along with effective log size reduction. Cribl is particularly beneficial for migrating enterprise logs, optimizing usage, and reducing costs while streamlining the transition between different log management tools.

What are Cribl's most important features?

- **Real-Time Data Transformation:** Enables immediate data processing for accurate insights.
- **Simplified Log Collection:** Gathers data from diverse sources effortlessly.
- **Powerful Data Reduction:** Reduces log size without losing critical information.
- **Inbuilt Packs:** Ready-to-use functions simplify complex tasks.
- **Live Testing:** Allows testing before production deployment for reliability.
- **Master Node Updates:** Manages worker groups efficiently for consistent performance.
- **Advanced Data Processing:** Offers robust data serialization and coding perspectives.
- **Easy Plugin Configurations:** Facilitates direct integration with reduced setup time.

What benefits and ROI should users look for?

- **Optimized Usage:** Ensures effective resource management and cost reduction.
- **Streamlined Migration:** Simplifies the transition between log management tools.
- **Enhanced Data Management:** Improves data quality and processing efficiency.
- **Reduced Time and Effort:** Direct-to-production capabilities save operational time.

Cribl is widely implemented in industries requiring extensive data management, such as technology and finance. Users leverage Cribl to handle log collection, processing, and migration efficiently, ensuring smooth operation and effective data analysis. It aids in managing temporary data storage during downtimes and better handling historical data, preventing data loss and allowing extended periods for viewing statistics and monitoring trends.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“When it comes to the product's installation phase, it is not tough for people who have good knowledge...The tool is worth the investment.”



Phanindra Ponnada

Splunk SME at Sbase Technologies India PVT Lmtd



“Cribl definitely helps with the complexity because you don't have to push for deployment—they provide the interface where you can mimic what the output will look like, and you can see that in real time when setting up the Cribl configuration, which definitely helps considerably.”



Verified user

Lead Engineer at a manufacturing company with 10,001+ employees



“Cribl offers easy plugin configurations and source collection settings, allowing us to collect logs from any source.”



Hariram G

Lead Engineer at a tech vendor with 1-10 employees



“My favorite option in Cribl is the Stream product.”



Carlos Moreno Buitrago

Splunk Consultant at a pharma/biotech company with 201-500 employees



“The platform's most valuable feature is the ability to transform data in real-time within the pipeline without sending it to a destination.”



Feroz Khan Peer Mohamed

Splunk / Cribl Consultant at HynoonTech LLC



“Features such as Cribl Stream, Cribl LogStream, and Cribl Edge have been the most beneficial. The Cribl LogStream, in particular, is valuable for routing data, creating firewalls on pipelines, and putting security measures in place to ensure data reaches its destination without issues.”



Kenekchukwu Murphy Ezeoka

IT Support Specialist at Convergys Corporation



“The support team was very helpful and managed to get everything production-ready.”



Maciej Grabowski

Architect at Sii Polska

What users had to say about valuable features:

“One of the biggest things I love about Cribl is that you can actually see the output in real time before you push anything to production. The UI makes it super easy to work with, and honestly, it saves a ton of time. Plus, it’s way easier to collaborate—everyone’s on the same page, and you’re not guessing what the data’s gonna look like once it’s live.”

Verified user

[Read full review](#) 

Lead Engineer at a manufacturing company with 10,001+ employees

“My favorite option in Cribl is the Stream product. It is the best use case for us and our customers. Additionally, the community on Slack is excellent for solving questions and getting ideas..”

Carlos Moreno Buitrago

[Read full review](#) 

Splunk Consultant at a pharma/biotech company with 201-500 employees

“Cribl's ability to handle high volumes of diverse data types is exactly the purpose that we took it for, and as far as I have seen for the last nine months, it is handling well without issues. Connectivity-wise, there is some problem, but I'm not sure whether it's from the Cribl end or the SIEM end; we are working on both ends right now, so I don't see any problems concerning that. Cribl has helped in reducing informational logs between the main entity of our SIEM and the external entity, so that actually helped..”

Kumbesh Rajagopal

Senior Security Delivery Analyst at Accenture

[Read full review](#) 

“The feature I appreciate most about Cribl is that it is really easy to use and quick to replicate data models on different data sets. We have over 1,000 log sources, and currently, we have to configure them individually with their own architecture. Cribl allows us to do a copy and paste architecture and saves us a lot of development time. It also makes it easy to add any sort of extra data parsing to specific lines. Ease of use is really our biggest benefit from it..”

Verified user

Works at a manufacturing company with 10,001+ employees

[Read full review](#) 

“It helped us to completely remove the monopoly on Splunk, as we previously couldn't have any control over logs and how to optimize them. When we had Cribl in place, it provided a vision and a platform for us to control what we send and how we send it in terms of data passing, data enrichment, and many more things, with massaging the data. It also helped us to open up to many tools where we could send the data to various destinations, as it is vendor-agnostic..”

Verified user

[Read full review](#) 

Works at a tech vendor with 10,001+ employees

“My favorite feature is Cribl Stream. That's probably the only Cribl product I have a lot of experience with, and Cribl Stream makes it very easy to identify where all the customer's log sources are and to quickly connect them to a destination source such as Microsoft Sentinel and Microsoft Azure Data Storage.

Cribl Stream does two things: not only does it make it easy to connect one log source or one dataset to multiple storage locations, but it also has compression features, which greatly reduce the storage cost for that data. It strips out and compresses data so that only the absolute information remains and not any duplicates. Dual destination and compression are the two top features..”

Joe Cicero

[Read full review](#) 

Director of Strategic Alliances at security risk advisors

Other Solutions Considered

“There are other solutions like Azure and Splunk, and each has its strengths. Cribl stands out due to its streaming data model and integration for security use..”

Kenechukwu Murphy Ezeoka

IT Support Specialist at Convergys Corporation

[Read full review](#) 

“Currently, we are using Logstash, and we are also exploring a POC with DataBahn. DataBahn is a newer company. They are not as sophisticated as Cribl, and the performance is probably not there, but they make up for it in cost..”

Verified user

Works at a manufacturing company with 10,001+ employees

[Read full review](#) 

“Cribl is the first tool that I'm using for this particular data pipelining. We do have Dynatrace, but we use it for a different purpose, for monitoring. Cribl is for streaming purposes only, so the purpose is different. I'm not sure if there is a competitor for this particular tool or not, as I haven't worked with any competitor so far..”

Kumbesh Rajagopal

Senior Security Delivery Analyst at Accenture


[Read full review](#) 

“I am not really sure if there are any competitors to Cribl at the moment. I would say Cribl had used its marketing strategy in a better way to advertise its brand than its competitors, and maybe that is why every company thought about it more. I did not see that much advertisement from Datadog. Most of the people still don't know about Datadog.

Datadog is famous for application performance monitoring. I would disagree with those who use it to reduce their costs, as most people would prefer to use Cribl. Cribl's major agenda is to reduce the need for Splunk licenses..”

Phanindra Ponnada

Splunk SME at Sbase Technologies India PVT Lmtd

[Read full review](#) 

“The only alternative I can compare Cribl to would be Azure Data Transformation, Azure Data Time configuration rules and policies, basically making the storage source sort the data, and that is very painful. I don't see any next-best options when it comes to Cribl. They seem to be a leader and standing alone in their service offering, specific to Cribl Stream. For other products such as Cribl Lake, there's now Microsoft Sentinel Lake, which is a competitor, and I haven't really analyzed the pricing to see how competitive that is. But regarding Cribl Stream, there's no close competitor. The closest is extremely painful, requiring about 20 pages of configuration to even get close..”

Joe Cicero

Director of Strategic Alliances at security risk advisors

[Read full review](#) 


ROI

Real user quotes about their ROI:

“Cribl is indeed a cost-effective solution, saving thousands of dollars for our clients. It provides value through cost savings and time efficiency once users know how to effectively use the platform..”

Verified user

Security Engineer at a tech services company with 51-200 employees

[Read full review](#) 

Use Case

“I use Cribl to ingest logs from different platforms. These logs could come from sources like Mimecast, Windows, or CrowdStrike logs. It acts as a pipeline to send data to our destinations and also helps in reducing the amount of logs sent by applying different functions on them..”

Verified user[Read full review](#) 

Security Engineer at a tech services company with 51-200 employees

“In this particular situation, we use Cribl to deploy data to various destinations. My role is to create and analyze data and deploy it to the appropriate location required by the organization. I also monitor data to manipulate or adjust it as needed. Additionally, we use it to amend or remove some lookup in the data or to add some phrases, ensuring it meets the organization's requirements. Overall, we use it for daily data management activities..”

Kenechukwu Murphy Ezeoka[Read full review](#) 

IT Support Specialist at Convergys Corporation

“We use Cribl Stream to collect logs from multiple sources, transform and enrich them, filter out unnecessary data before sending them to SIEM. We also use Cribl to route logging to data lake. .”

Verified user

[Read full review](#) 

Lead Engineer at a manufacturing company with 10,001+ employees

“Entire logs from my organization go through Cribl and get routed to Splunk and various other destinations. I use it on a large scale in my organization. Cribl Stream is one of my favorite parts. I use Cribl to route the logs to various destinations. It helped us to completely remove the monopoly on Splunk. Not only firewall logs, but also cloud trail logs and many other logs were processed through Cribl..”

Verified user

[Read full review](#) 

Works at a tech vendor with 10,001+ employees

“I am using Cribl to have everything centralized in one tool in terms of data collection. We were working with different Splunk customers, and Cribl helps collect data and then send it to an S3 bucket or Amazon Web Services (AWS) response plan..”

Carlos Moreno Buitrago

Splunk Consultant at a pharma/biotech company with 201-500 employees

[Read full review](#) 

“For Cribl, we use only Stream, which we are using as a data pipeline in between our environment and the SIEM console. We have two SIEMs: one is a cloud SIEM and one is an on-prem SIEM. On-prem, we are using another user and entity behavior analysis tool, so we have a redirection or a copy of a log for user login and logout information. Then we have a SIEM console, and we have redirections to the SIEM through Cribl. From the environment, we have a load balancer, and from the load balancer, we have this data pipeline configured to different SIEMs, and then we have that data transferred to two different SIEMs..”

Kumbesh Rajagopal

Senior Security Delivery Analyst at Accenture

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“The initial setup of Cribl was straightforward, often taking as little as thirty minutes for deployment. Cribl has QuickConnect features that simplify the process significantly. However, we preferred using routing and pipelines for more control and security measures..”

Kenechukwu Murphy Ezeoka

IT Support Specialist at Convergys Corporation

[Read full review](#) 

“The initial setup with Cribl is much easier. Upgrading versions, especially in cloud environments, is almost a single-click process. Upgrading is also straightforward for on-premises setups—updating the leader node automatically distributes the upgrade to all worker groups and nodes. This makes upgrading, maintaining, and installing Cribl relatively simple compared to other tools.

Additionally, Cribl offers free training for users and administrators. The existing learning materials are comprehensive enough to support effective use and deployment..”

Hariram G

Lead Engineer at a tech vendor with 1-10 employees


[Read full review](#) 

“Setting up Cribl for basic training is straightforward and effective. You can easily configure it on your laptop by downloading the binaries and using simple command-line instructions to set it up in different modes, like leader, edge node, or single deployment. Adding a worker node is also simple; just run a script generated in the UI, and it's up and running.

The enterprise setup process is more complex, and there are significant documentation challenges. Despite the system eventually being available, the process involved many support calls and workarounds. Getting everything set up for a production-ready enterprise deployment was long and challenging..”

Maciej Grabowski

Architect at Sii Polska

[Read full review](#) 

“When it comes to the product's installation phase, it is not tough for people who have good knowledge. I would like to highlight a similarity between Splunk and Cribl. Their official site's documentation makes even a layman's job easy. Just following the documentation, they can install the tool, but they still have to do it under some supervision.

The solution is deployed on the cloud and on an on-premises model. When you talk to the tool's global support, you can have the cloud version provided as a SaaS solution, or you can also have an enterprise-level version where you can have it in your own environment. If you have your own data center setup, you can buy Cribl's enterprise version, and you can install it, so it all depends on the requirements..”

Phanindra Ponnada

[Read full review](#) 

Splunk SME at Sbase Technologies India PVT Lmtd

“It's straightforward. They have a really nice user interface, and their service engineers will guide you through the initial setup. Since they are compensated based on product usage, they ensure that we are properly onboarded and that our experience is as successful as possible.

To deploy Cribl probably took an hour. Identifying all the different log sources that we wanted to bring in took about another eight hours of human work as it was a data exercise of determining which log sources are important to us, and where we can get the best compression or data size reduction. You can connect to them all automatically, but you want to have the thought process of which ones matter and what actual data you need.

It does not require any maintenance on my end. The big thing is just checking connector health to make sure everything is running and that logs aren't dropping and that there haven't been any changes. In case there's any outage, putting in a ticket for any outage issues is very minimal. It's set it and forget it, and then just monitor to make sure nothing's bad or nothing has gone wrong. .”

Joe Cicero

[Read full review](#) 

Director of Strategic Alliances at security risk advisors


“We employed a hybrid strategy, setting up Cribl Cloud as the head node in their environment. For data processing, we used worker nodes within the client’s environment, which are closer to the data sources. This setup allowed us to process data locally before sending it to our destination. For cloud assets, such as SaaS applications like Salesforce, we used the cloud-hosted Cribl instance to handle that information. Meanwhile, the on-premises data was processed by the hybrid worker nodes.

We encountered delays due to third-party issues, extending the timeline to six to seven months. Without these issues, it likely would have taken around three months, depending on the speed of obtaining API keys, authorizations from networking teams, and other factors. Under ideal circumstances, a three-month timeframe would be more accurate.

You need to maintain the pipeline, which includes data processing, before it reaches its destination. When onboarding new data, managing and rotating API keys as needed is important. Maintaining these aspects ensures faster and more efficient deployments.

If you want to reduce log ingestion or route data to multiple destinations, consider using an on-premises or cloud solution. Your choice will depend on your organization’s network constraints. For example, if critical assets on your network need to connect to the internet, your network team might have restrictions. Weigh the benefits of cloud versus on-premises options to determine what best fits your needs..”

Jai Chudasama

[Read full review](#) 

Security Engineer at a tech services company with 201-500 employees

Customer Service and Support

“Everything works, but it required a lot of support. The setup wasn't easy, but the support team was very helpful and managed to get everything production-ready. .”

Maciej Grabowski

Architect at Sii Polska

[Read full review](#) 

“They are very good in terms of solving issues. Regarding availability over other time zones, since it is mostly focused on Europe and US, they are starting to build up in New Zealand and other places..”

Verified user

Works at a tech vendor with 10,001+ employees

[Read full review](#) 

“I haven't contacted them in terms of paid support. That said, the community, including the engineering and sales teams, is available on Slack and is very supportive..”

Carlos Moreno Buitrago

Splunk Consultant at a pharma/biotech company with 201-500 employees

[Read full review](#) 

“I would rate Cribl's customer service and technical support as nine and a half out of ten. We have worked with various teams to address some issues, and the support has been exceptional..”

Kenechukwu Murphy Ezeoka


IT Support Specialist at Convergys Corporation

[Read full review](#) 

“I never got the chance to contact the solution's technical support, but my counterpart, who is a direct employee in the company, had contacted Cribl's support team, and it seems we get pretty good support..”

Phanindra Ponnada

Splunk SME at Sbase Technologies India PVT Lmtd

[Read full review](#) 

“We've engaged their customer service and support, and anytime there's an outage, they've been very receptive. They've quickly escalated our tickets and helped us get resolution. We've never felt we were waiting for a response or that they didn't know what was going on. I think it's maybe because we were an early customer. I would assume it's the same for all customers, but we've gotten great treatment.

I would give them a 10 out of 10 for support. They are very responsive. We deal with a lot of other cloud solution providers who have tried to save money on support. It could be that because Cribl is new and they really want to make sure all new customers are being successful, but we really hope this continues. We don't feel we're alone..”

Joe Cicero

Director of Strategic Alliances at security risk advisors

[Read full review](#) 

Other Advice

“It has been able to perform to the best of its capabilities. They are able to handle everything with their non-shared architecture. On a scale of 1-10, I would rate Cribl a solid nine..”

Verified user

Works at a tech vendor with 10,001+ employees

[Read full review](#) 

“Utilize the documentation to ensure Cribl fits your use case, and join the Cribl community for any questions or recommendations.

I'd rate the solution ten out of ten..”

Carlos Moreno Buitrago

Splunk Consultant at a pharma/biotech company with 201-500 employees

[Read full review](#) 

“Cribl gives us way more control and flexibility than we ever had before. We deal with massive volumes of telemetry data, and honestly, a lot of it is just noise. Cribl allow us to easily filter, transform, and route that data exactly how we want. It’s made a big difference..”

Verified user

Lead Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

“For everything, my suggestion and limitation as I told, if it were there, I would give Cribl 10 out of 10; since it's not, I'm giving nine out of 10. I am just a user of Cribl; my company has a license with them. I'm not sure if they have a partnership with Cribl or not. I rate Cribl nine out of 10..”

Kumbesh Rajagopal

Senior Security Delivery Analyst at Accenture

[Read full review](#) 

“I would rate Cribl a ten out of ten. I truly appreciate them as partners. They genuinely feel like they're with us on this journey to manage the increasing volume of data. It's been exciting to watch them grow. At first, I thought I was a bit of a nerd for being an early adopter, but seeing so many others come on board after us reassures me that we made the right decision..”

Joe Cicero

Director of Strategic Alliances at security risk advisors

[Read full review](#) 

“We are using around 25% of what Cribl offers, mainly focusing on log parsing, which is what Cribl started with. We use [AWS](#) as our main source of ingestion.

There is little flexibility in pricing. It is simply the market price, and you either pay it or you do not. Cribl has significant capacity to handle high volumes of diverse data types, such as logs and metrics. Cribl can handle almost anything we throw at it, as long as budget is not an issue.

There is a team in my company that uses them, but they are part of a separate company. We do not have any partnership with them yet.

On a scale of 1–10, I rate Cribl an 8. .”

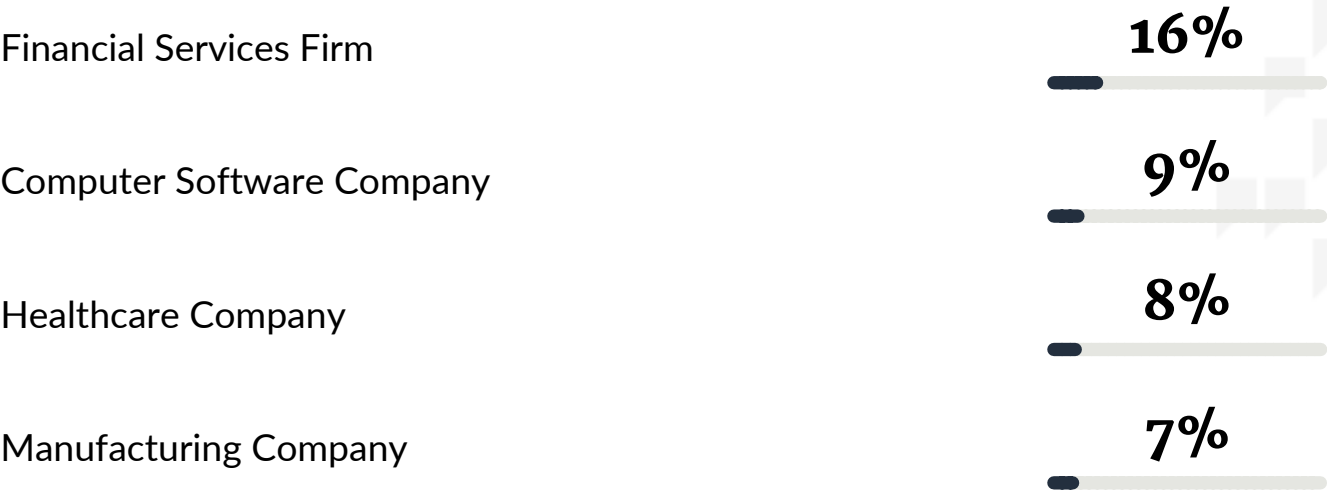
Verified user

Works at a manufacturing company with 10,001+ employees

[Read full review](#) 

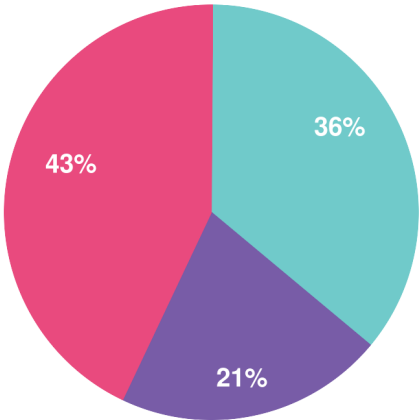
Top Industries

by visitors reading reviews

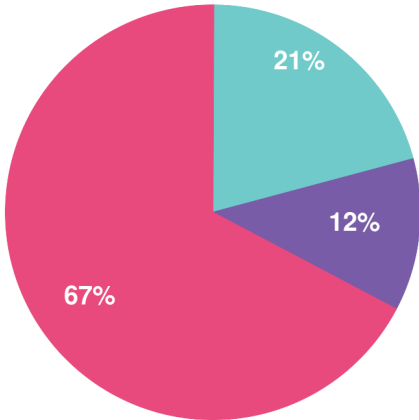


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944