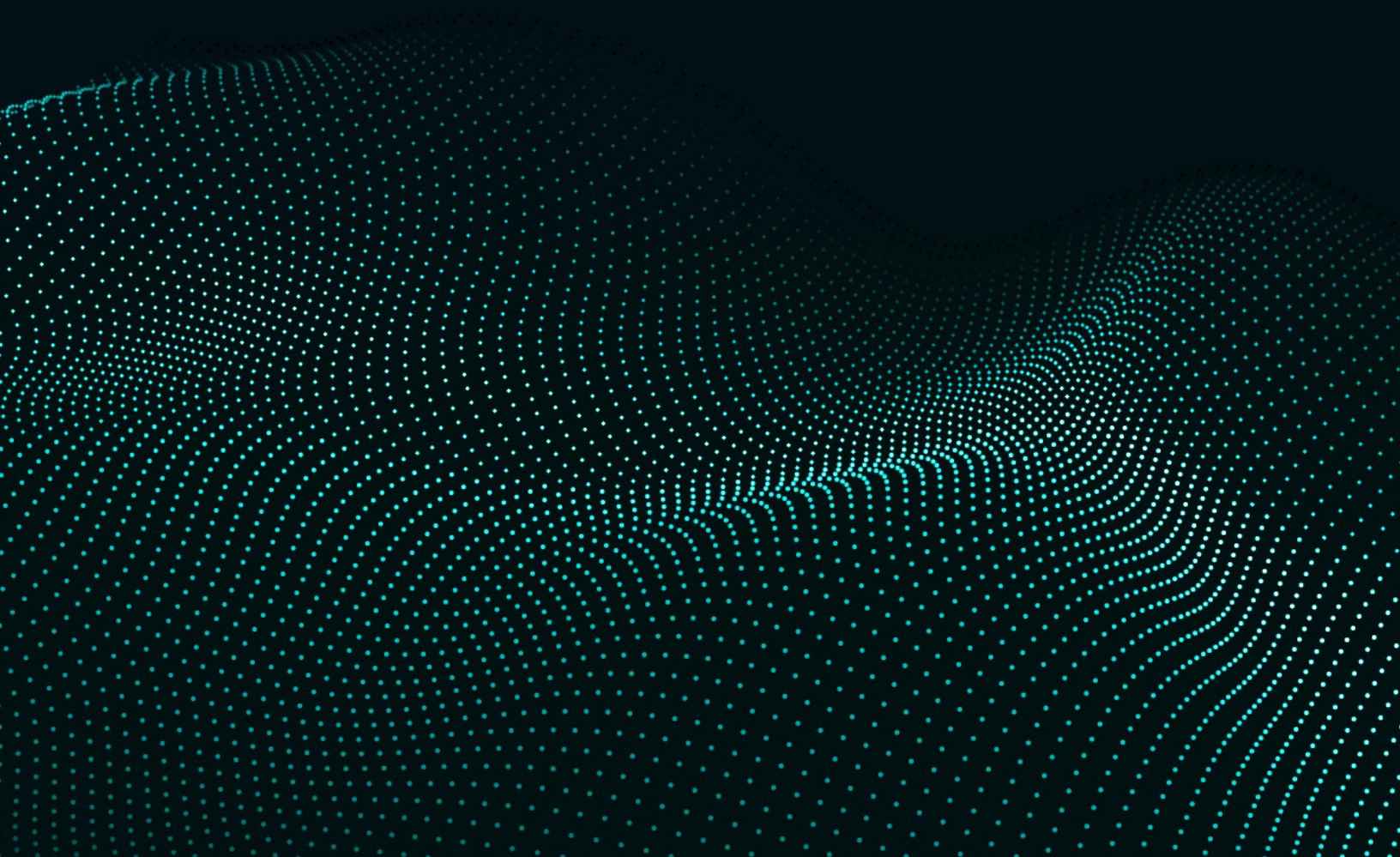
Nightfall™ | Cribl

SOLUTION BRIEF

Data Protection and Cost Reduction with Cribl Stream™ and Nightfall AI



SOLUTION BRIEF

Data Protection and Cost Reduction with Cribl Stream™ and Nightfall AI

THE CHALLENGE

Enterprises using Cribl to reduce log volume want to remove sensitive data from logs before it is sent and stored within platforms such as DataDog and Splunk.

THE SOLUTION

Nightfall's machine learning Developer Platform (DLP) engine detects and labels or redacts sensitive information in logs (secrets and keys, PHI, PII etc.) that are sent through Cribl Stream.

THE BENEFITS

- Detect and redact or level sensitive information in logs
- Support compliance regimes through Cribl + Nightfall including HIPAA, FERPA, PCI, GLBA, GDPR, and more
- Log batching to make fewer requests to the Nightfall API
- Find and label problematic logs automatically

Together, Cribl and Nightfall AI provide security and protection of sensitive data throughout your observability platform.

The Challenge

Data observability is a core tenet of building strong software systems. However, when sensitive data makes its way into logs inadvertently or as metadata on traces/metrics, this opens up vulnerability to potential attacks. Security problems may quickly and quietly arise in observability environments due to:

- *Limited access controls in observability platforms when compared to their associated application environments*
- *Multi-tenanted nature of observability environments*
- *Potentially exposed nature of observability environments to the internet*

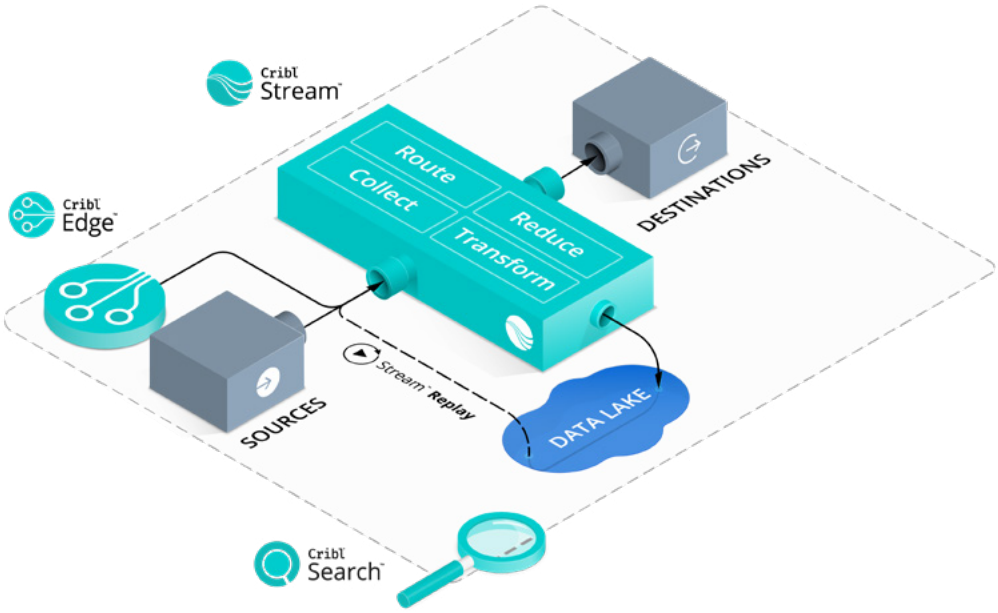
Security issues exacerbate when observability data contains sensitive information because there is usually no fine-grained access control. For teams that work with large data pipelines integrated across their tech stack, it's remarkably easy for sensitive data to be ingested into observability platforms, even when data hygiene best practices are followed.

The Solution

Cribl's observability pipeline, Cribl Stream, provides a vendor agnostic routing system to shape data from any source to any destination. Stream can send data to Nightfall's machine learning-powered data detection and redaction engine to protect sensitive information in logs (secrets and keys, PHI, PII etc.). This helps ensure information is not ingested and replicated across other platforms throughout your organization.

DLP by Nightfall AI, available in the Cribl Dispensary as a pack, is intended to solve security issues by allowing for an easy implementation of data loss prevention (DLP) within Stream. With the Nightfall pack, you can monitor your pipelines in real-time for logs and traces that include common types of PII, PCI, PHI, secrets and other sensitive information.

TOGETHER, CRIBL'S OBSERVABILITY PIPELINE COUPLED WITH NIGHTFALL'S DLP ENSURE THAT YOUR ORGANIZATION REMAINS COMPLIANT WITH DATA SECURITY REGULATIONS AND BEST PRACTICES



The Benefits of Using Nightfall with Cribl's Observability Solution

ROUTE AND SANITIZE YOUR DATA THROUGH THE NIGHTFALL PIPELINE

Nightfall is deployed as a pack through the Cribl Dispensary and works like any pipeline within Cribl Stream, allowing you to route data from any of your existing sources and redact sensitive text from content before sending it off to your intended destinations. The added functionality of Nightfall's Developer Platform (DLP), a machine learning engine, allows you to fully customize what Nightfall detects and redacts with a high level of detection accuracy.

FULLY CONTROL AND CUSTOMIZE HOW YOUR DATA IS SANITIZED

Once installed, you can modify settings for the Nightfall pack in the processing tab of Cribl Stream including:

- *Adding custom detection rules created in the Nightfall DLP dashboard to specify when sensitive text should be redacted from the content entering Stream.*
- *Establishing trigger flags whenever Nightfall detectors redact or detect sensitive data. These tags can be used to create custom workflows for how the sanitized data within the Nightfall pipeline should be routed or handled.*
- *Enabling log batching to make fewer requests to the Nightfall API and reduce sampling to minimize Nightfall API data usage.*

LEVERAGE DETAIL RICH ALERTS FROM THE NIGHTFALL DEVELOPER PLATFORM

Having full access to the Nightfall DLP means that you can receive detail-rich alerts via Slack or email whenever data matching your specific detection rules enters the pipeline in Stream. Alternatively, use a webhook to send alerts to a SIEM or through another pipeline within Cribl, where you can route or replay data from any destination including low-cost storage.

Summary

As the volume of data sources organizations leverage grows, so too will the risk of sensitive data accumulating and spreading across data pipelines. Cribl is the premier platform for scaling observability data for cloud-first organizations, and Nightfall is an easy and effective way to ensure this data doesn't accumulate in the first place, ensuring that your organization remains compliant with data security regulations and best practices.

With Cribl and Nightfall, customers can:

- *Detect and redact sensitive information in logs, such as secrets and keys*
- *Support compliance regimes through Cribl + Nightfall including HIPAA, FERPA, PCI, GLBA, GDPR, and more*
- *Use log batching to make fewer requests to the Nightfall API*
- *Find and label problematic logs automatically*

To get started with Nightfall and Cribl Stream today, **click here to download Stream** and **click here to create your Nightfall account**. The **Cribl Slack Community** is also a great place to connect with leaders from other teams leveraging both Nightfall and Cribl.

ABOUT NIGHTFALL

Nightfall's mission is to bring efficiency and efficacy to data protection. Organizations depend on Nightfall to discover, classify, and protect sensitive data across cloud services via machine learning & natural language processing (NLP). As the industry's first cloud-native data loss prevention & data classification platform, Nightfall has scaled rapidly to a broad set of customers across the globe, ranging from hyper-growth tech startups to Fortune 100 enterprises. Nightfall's SOC 2 Type 2 compliant platform has been deployed across consumer-facing and highly regulated industries like healthcare, insurance, and education to address data leakage and compliance risks around HIPAA, GDPR, CCPA, and more. Nightfall is backed by Bain Capital Ventures, Venrock, Webb Investment Network, and a cadre of high-profile operators, including CEO/executives at Okta, Splunk, FireEye and Salesforce. For more information on Nightfall and Cloud Native DLP, please visit **nightfall.ai** or contact us at **hello@nightfall.ai**.

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.