▶ Cribl

Cribl
Insights

Cribl Insights lets IT and security teams know exactly what's happening with their data—built for a future where monitoring is increasingly automated and agent-driven.

Security and IT teams struggle with getting the visibility they need:

Partial data drops go unnoticed:
Existing tools only alert when data stops completely, but a drop from 100% to 10% or even 2% can still mean terabytes are lost — leaving significant issues undetected.

Difficult trend detection:
Identifying meaningful increases or decreases requires analyzing patterns over multiple days, to avoid misleading spikes or lulls.
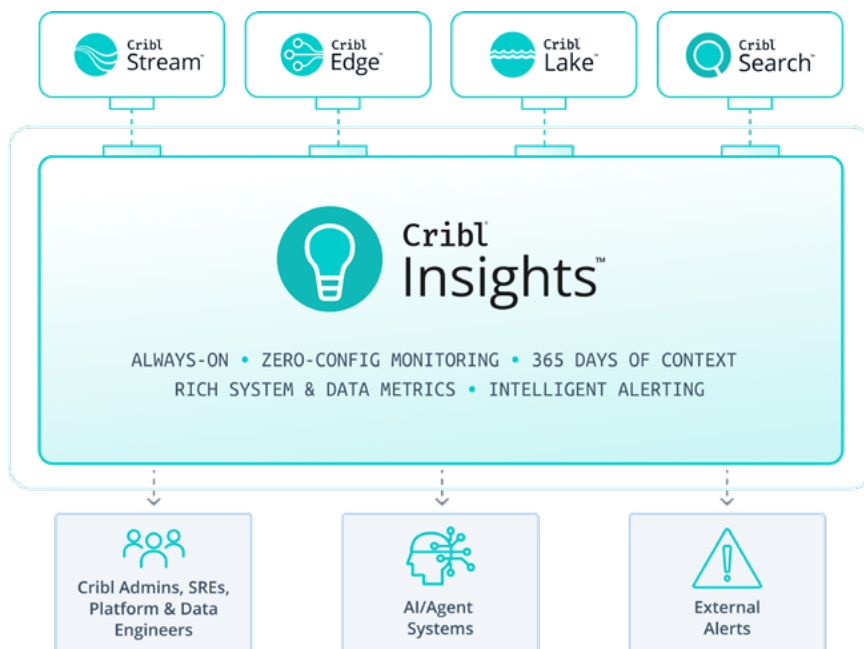
Scattered monitoring:
Alerts and visibility are spread across multiple products, requiring too many clicks and constant context switching.

Lack of centralized insight:
Customers need a single, at-a-glance view to monitor data flow, spot anomalies quickly, and scale with their environment.

Cribl Insights offer a central hub for monitoring and alerting so it's easy to understand the usage, performance, and health of your data.

Benefits

BETTER VISIBILITY
Understand upstream and downstream activity, catch issues instantly, and never let data slip through the cracks.

INCREASED PRODUCTIVITY
Proactively prevent outages, detect and resolve issues faster, streamline operations, and reduce downtime.

STORYTELLING & CONTEXT
Translate anomalies into clear insights your whole team can understand and act on.

UNIFIED CONTROL
Keep oversight of system & data insights, as well as alerting all in one place.

RESOURCE OPTIMIZATION
See where capacity is over- or under-utilized, save on costs while making smarter scaling decisions.

Product Features

SYSTEM INSIGHTS

Granular visibility into the operational health of products and worker groups

Stream

- **Detailed worker-level monitoring** – View metrics by worker group or individual worker.
- **Throughput and health monitoring** – Track events and bytes in/out, events in/out, queuing activity, dropped events, and processing errors to quickly assess pipeline health.
- **Source and destination visibility** – Identify top data sources consuming bandwidth and top destinations receiving data to understand usage patterns and cost drivers.
- **Pipeline and routing insights** – See which routes, Packs, and pipelines contribute most to event volume and throughput.
- **Job execution tracking** – View scheduled and running jobs to understand background activity and operational impact.
- **Infrastructure insights for SREs** – Monitor CPU load, memory usage, and worker distribution across your Cribl deployment.
- **Log-level investigation** – Access logs directly and filter events by time range to support faster root cause analysis.

Edge

- **Events per second and bytes per second** – Monitor ingestion rate and data volume in real time.
- **Top sources and destinations** – Identify the highest-volume sources and destinations by events and bytes.
- **Top packs by events** – Understand which packs are driving the most data processing.
- **Top pipelines by events** – See which pipelines handle the greatest workload and impact throughput.
- **Fleet and node visibility** – Track Edge fleets and individual nodes to quickly assess scale and health.
- **Routing and pipeline views** – Visualize routes, pipelines, sources, and destinations to understand how data moves end to end.

Search

- **Query performance and volume** – Track how often searches are run and how efficiently queries execute.
- **Search performance metrics** – Monitor end-to-end search latency and responsiveness.
- **I/O rate and throughput** – Understand data read/write activity and overall search capacity.

- **Queue size** – Identify backlogs and contention that may impact search responsiveness.
- **Search health** – Quickly assess system stability and operational status.
- **Billable CPU hours** – Gain clear insight into resource consumption and cost drivers.

Lake

- **Storage utilization visibility** – Monitor data stored per day and analyze storage consumption trends over time.
- **Cost awareness and optimization** – Understand how storage is consumed across different time periods to optimize retention and spending.

DATA INSIGHTS

End-to-end visibility into how data flows

- Visualize data as it moves from **source to preprocessing, post-processing, and destination**, eliminating black boxes across the pipeline.
- **Source- and worker-level filtering** – Drill into specific worker groups or individual sources to understand exactly how data is routed and processed.
- **Interactive volume and flow analysis** – Click into data volume views to see event counts flowing through each stage—from source to destination—with clear visibility into where data changes.
- **Data in, data out transparency** – Inspect events and bytes in and out at every step, including data freshness (lag) and data shape (fields in vs. fields out).
- **Drop and filter detection** – Identify where events are being dropped, filtered, or rerouted—intentional or accidental—before downstream tools are impacted.
- **Trend analysis by dataset and source** – Track volume and freshness trends over time to spot anomalies and understand normal behavior.
- **Cost and pipeline optimization** – Use insights into routing, filtering, and tiering to optimize pipelines and control storage and processing costs.

ALERTING

Centralized, intelligent alerting

- **Out-of-the-box alerts** – Enable or disable default alerts based on use case, including system health, data anomalies, and failures.
- **Customizable firing conditions** – Set thresholds and severity levels (Critical, Warning, Info) to trigger alerts and reduce false positives.

- **Notification management** – Send alerts to Slack, PagerDuty, SNS, email, webhooks, or custom targets. Configure policies per product, per alert, or by severity.
- **Alert visibility and tracking** – See all active and historical alerts, including query details and triggering conditions. Filter by product, alert type, or severity.
- **Mute and schedule alerts** – Temporarily mute alerts for specific periods, with naming and time-range options to reduce noise.
- **Actionable insights** – Fewer alerts, faster response, and less noise—help teams detect issues early, resolve them efficiently, and stay proactive.

TECHNICAL REQUIREMENTS

System

- Cribl Insights is available as a service at https://cribl.cloud

Browsers Supported

- Firefox 65+, Chrome 70+, Safari 12+, Microsoft Edge