2024 REPORT

Navigating the data current

Exploring Cribl.Cloud analytics and customer insights

Cribl

INTRODUCTION

Welcome to the inaugural ***Navigating the data current*** report, providing insights into how IT and Security teams are modernizing their data management practices. This report explores where data is coming from, where it is going, and how teams are adapting to the changes.

KEY DISCOVERIES

Data sources on the rise

Not only are IT and Security teams dealing with more data volume, they're also managing an increase in the variety of data sources. **Year over year, the number of data sources ingested grew at an impressive 32%.** Nearly one-fifth of users are consuming from ten or more data sources.

IT and Security prefer a single cloud

An interesting counter trend uncovered in this year's data is around multi-cloud – or rather the lack of it. While it's common to hear that the majority of companies are using multiple cloud service providers (CSPs), we don't see this for IT and Security teams. **Only 11% of teams are sending data to destinations in more than one CSP.**

Expanding choice in SIEM providers

With the changes in the SIEM space over the last year, it's no surprise that IT and Security teams are checking out their options. **The number of companies sending data to multiple SIEM products increased a whopping 45% over the last year.** The number of security teams using multiple SIEMs grew from 11% to 16% year-over-year, with Google SecOps and Microsoft Sentinel showing significant gains.

CONTENTS

Why did we create this report?

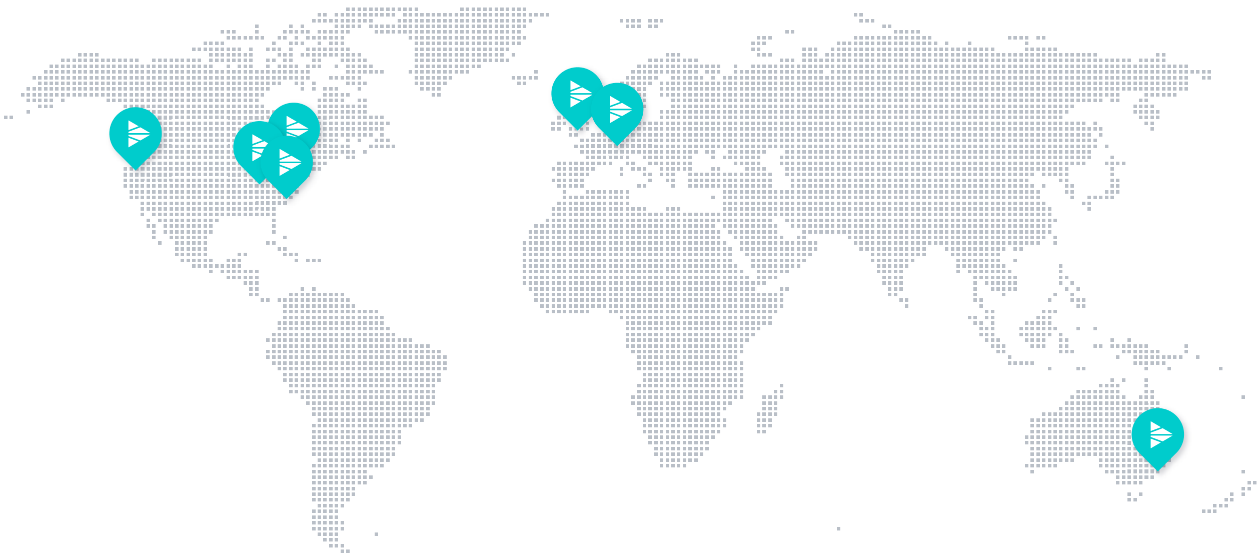
As the clear market leader, Cribl has more data than any other company about what IT and Security teams are doing with their telemetry data, and how those trends are changing. As the only vendor-agnostic company with purpose-built solutions for IT and Security, Cribl is uniquely positioned to offer you not only insights on these trends, but advice on what you should be doing about them in your own company.

Over the past year, we've witnessed customers discovering the power of managing their telemetry data at a broader scale than ever before. Challenges ingesting, processing, and protecting data are being overcome with better tools that offer the choice and control IT and Security teams need today.

Companies need choice and control beyond managing their telemetry data. As the product landscape constantly evolves through acquisitions, mergers, and divestments, IT and Security leaders want options. Insulating against punitive shifts in the market is a key driver in modernizing data management practices.

The data from customers using Cribl.Cloud shows an increasing range of not only data sources, but also destinations. This data tells a story of adaptability and experimentation, as well as a ruthless need to manage costs while simultaneously protecting and optimizing their enterprises.

Let's get started.



How we created this report

To create this report, Cribl, Inc. analyzed anonymized data from Cribl Stream instances within Cribl.Cloud. This data is based on telemetry data collected from Cribl.Cloud users. Our customers use Cribl's data engine for IT and Security to securely route, manage, store, and search their telemetry data. They span every major industry and size, from small enterprises to many of the world's largest organizations.

This data is only representative of Cribl.Cloud customers and the way they use Cribl Stream to connect telemetry data sources with their chosen destinations. The trends described in this report may differ from enterprises not using Cribl.Cloud. Unless otherwise specified, the data included in this report is limited to Cribl.Cloud customers with at least one pipeline deployed.

Unless otherwise noted, this report presents and analyzes data from May 1, 2023, to April 30, 2024, which we refer to as "this year," "today," and "in 2024." Similarly, when we refer to "last year" or "in 2023," we are referring to data from May 1, 2022, to April 30, 2023. "2023" refers to the same period in its respective year. When referring to company size, Cribl uses the term "Developing" to refer to companies revenue of less than $1B USD, and "Enterprise" to refer to companies with over $1B USD in revenue.

Rising tides of data sources

IT and Security teams have a clear appetite to consume a diverse array of data sources. From a pure usage perspective, Splunk remains the most popular source.

This isn't unexpected. Splunk's long history in the security and IT monitoring spaces means there is a large install base of agents. While end users are looking for more vendor-agnostic options to data collection, replacing an entrenched incumbent is always a challenge.

However, Splunk is also one of the slowest growing sources we see in Cribl.Cloud. Its popularity does appear to be waning as IT and security teams consume from a more diverse array of sources, which we'll look at in the next section.

Amazon S3 is the second most popular source. This may seem counterintuitive. After all, it's the Simple Storage Service. That certainly implies a S3 as destination. However, it's this popularity as a destination that has made Amazon S3 a popular source as well.

Several products, like CrowdStrike Falcon Data Replicator and AWS CloudTrail, write their data to S3. Once landed, it's common for IT and Security teams to distribute that data across multiple other platforms and destinations. This need to route data to multiple destinations is what makes Amazon S3 a popular and rapidly growing data source.

On a percentage basis, we witnessed huge year over year increases in Office365 sources, like Message Traces, Management Activity, and Services. Usage of Azure Event Hubs also increased over 300%, a clear indication that IT and Security teams are consuming from a range of Microsoft Azure sources. We'll see a similar trend when we look at destinations.

DATA SOURCES BY THE NUMBERS

32% — YoY increase in the number of sources consumed

18% — % of IT and Security teams consuming from 10 or more data sources

40% — YoY increase in the number of sources consumed for Cribl.Cloud users active over 12 months

> I've never had this kind of visibility. I get a daily health report, I can see all the data sources are up, and how they're doing. We've never had this level of insight into data stream status. We can just redirect any traffic where it needs to go. Usability has never been this good for a data product before.

Senior IT Director

Fortune 50 Company

How Cribl helps

By supporting over fifty different sources at the protocol level, Cribl allows IT and Security teams to ingest data from anywhere, in any format.

The best part? You don't have to create your own cumbersome integrations or deploy yet another agent to gather data. Cribl gives you the power to collect your data without compromise.

DIVERSE DATA CURRENTS BY COMPANY SIZE

Overall		Developing		Enterprise	
		(< $B in revenue)		(> $B in revenue)	
1	Splunk	1	Splunk	1	Splunk
2	REST	2	Amazon S3	2	REST
3	Windows Event Logs	3	REST	3	Windows Event Logs
4	Amazon S3	4	Windows Event Logs	4	Amazon S3
5	Azure Event Hubs	5	File Sources	5	Azure Event Hubs
6	File Sources	6	O365 Management Activity	6	O365 Management Activity
7	O365 Management Activity	7	Azure Event Hubs	7	File Sources

While certain data sources like Splunk and REST are universally popular, preferences for other sources like Amazon S3, File Sources, and O365 differ based on the company size.

Smaller companies favor cloud storage solutions and simpler data sources, while larger enterprises have a broader and more diversified data source usage, reflecting their complex infrastructure and management needs. This doesn't mean that developing companies abandon their simpler data sources as they grow.

One thing we've seen from working with hundreds of enterprises is legacy methods and products stick around. As developing companies turn into enterprises, these older data sources will persist, but they may become less prominent over time as new data sources grow in popularity.

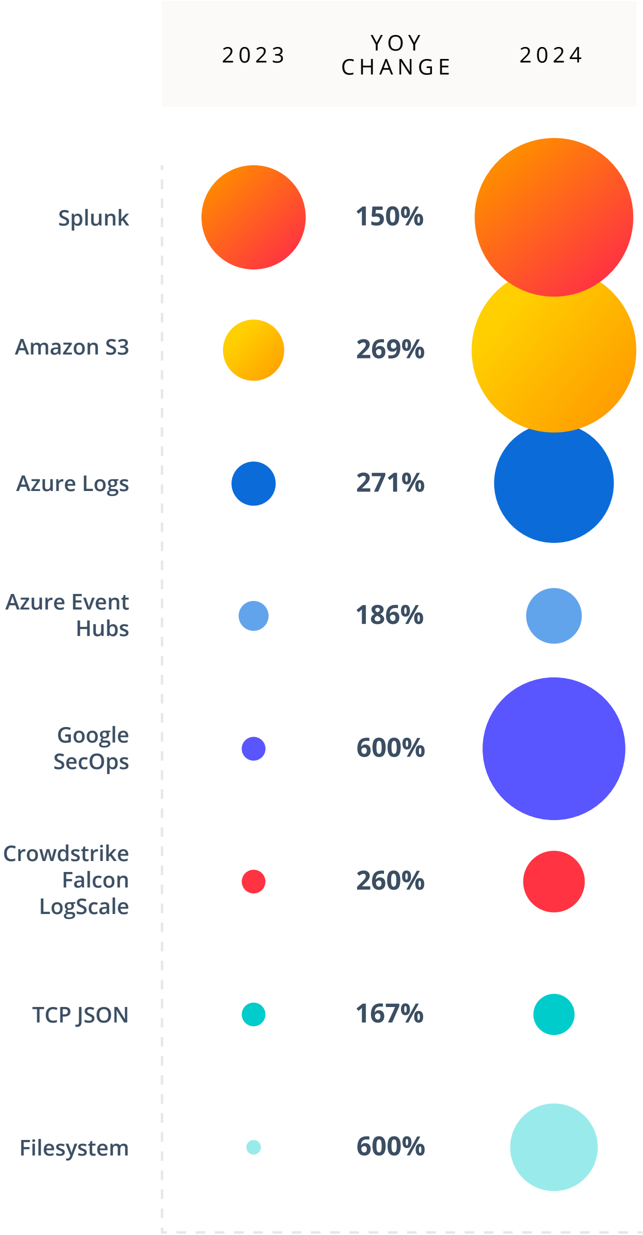
Navigating to key destinations

Much like the data sources, we see Splunk and Amazon S3 topping the list of most used destinations. Also like sources, we see Splunk's growth rate year over year as one of the slowest, with more modern platforms like CrowdStrike Falcon NG-SIEM (via CrowdStrike Falcon LogScale) and Google SecOps growing at much faster rates.

The pattern we see repeated time and again is tiering data based on forecasted use. Most organizations are sending data to at least two destinations as they separate their systems of analysis from systems of retention.

The rapid growth of security and storage destinations highlights the growing need for intelligent data management and infrastructure modernization.

This year, we saw the rise of Azure Event Hubs as a destination. In fact, Azure Event Hubs was the most popular messaging system across all of our data. This indicates a clear desire from companies to share data across the broader Azure ecosystem. Azure Logs also gained in popularity, with a 271% increase in usage across the Cribl user base.



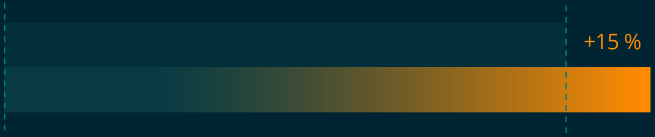
Fastest growing destinations by users

DESTINATIONS BY THE NUMBERS

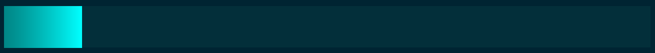
Unlike sources, destinations have grown more predictably year over year as companies seek to drive more value from existing platform investments by ingesting a broader range of data sources into them.

We see users adopting a pattern around data tiering—sending optimized, mission critical data to chosen systems of analysis, while full fidelity data lands in low cost data tiers, like object storage.

This full fidelity copy supports compliance, incident response, and, increasingly, direct search-in-place for ad hoc use cases.



15% YoY increase in the number of destinations used



12% of Cribl.Cloud users sending data to 4+ destinations

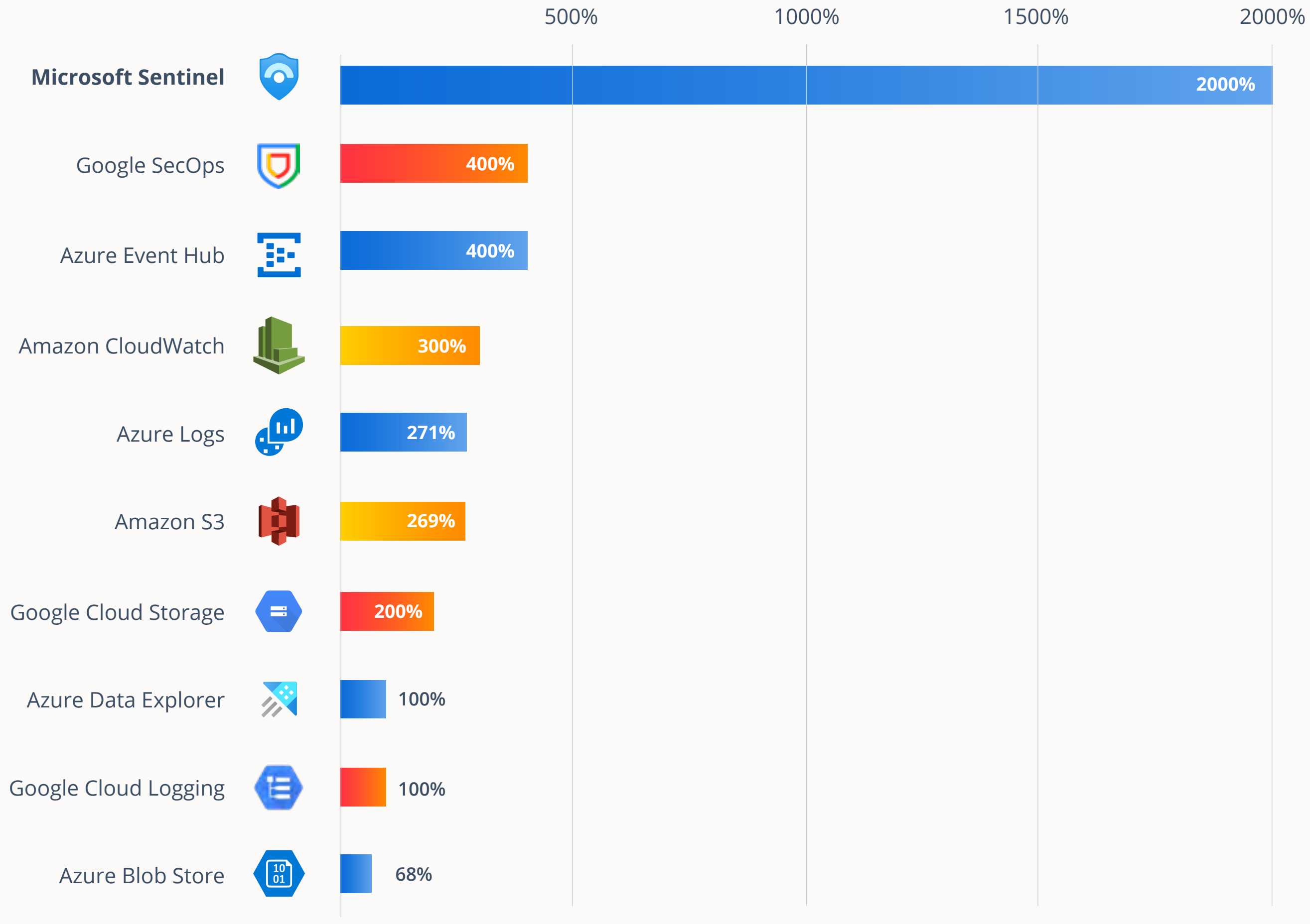
> Cribl Stream is an integral part of our logging and observability platforms, giving us the telemetry to deliver better business outcomes. The easy-to-use interface allows our engineers to easily route, enrich and trim data from our sources before we send it to multiple destinations. Stream adds to our agility and accuracy to ensure uptime and an optimal customer experience.

Steve Wojciechowski
IT Vice President, *Enterprise Holdings*

Microsoft Sentinel: The leading Cloud lighthouse

Turning our attention to the fastest growing CSP-native destinations, it’s hard to miss the growth in Microsoft Sentinel. Microsoft Sentinel is dominating many conversations with security teams and CISOs owing to Microsoft’s bundling of the product in its popular E5 premium subscription tier.

Across the destinations in the chart, Azure leads with four of the fastest growing destinations, while Google comes in second with three. Amazon, surprisingly, takes third place with two destinations.



Fastest growing CSP-native destinations

The growing wave of multi-SIEM deployments

Depending on the estimates you review, the SIEM market generates anywhere between $5.7 Billion and $6.2 Billion in annual revenue, growing somewhere between 7.7% and 13% CAGR. For such a small market, SIEM generates an outsized amount of interest. This interest is perhaps because of the perennial disappointment that security teams and CISOs have in both the cost and effectiveness of their chosen platform. They're always looking for options.

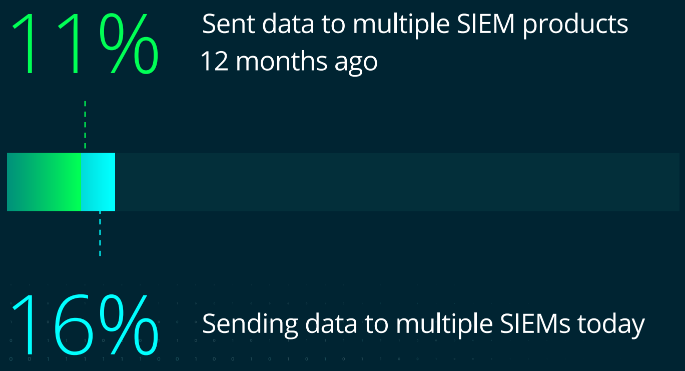
Now we have insight into which options they're exploring. Splunk, the clear market leader in SIEM, is under fire as teams most frequently send data to Google SecOps and CrowdStrike in addition to Splunk. This is understandable as there is significant uncertainty in the market after Cisco's acquisition of Splunk.

Exploring options doesn't mean teams are making wholesale migrations to new SIEM products. These migrations can take a year or more as alerts and rules are ported to new tools and teams integrate them into their existing security and business processes.

One thing is clear. The SIEM market is volatile and ripe for disruption.

MULTI-SIEM BY THE NUMBERS

One trend we see in our data is that the longer IT and Security teams have options, the more they take advantage of them. This is certainly true with SIEM. Last year, 11% of Cribl.Cloud users were sending data to multiple SIEMs. Of that original cohort, 19% of them are now sending data to multiple SIEMs—**a 73% increase!**



11% Sent data to multiple SIEM products 12 months ago

16% Sending data to multiple SIEMs today

> With Cribl Stream, we can get the data our old SIEM collected, as well as any other data we want to collect. It allows us to serve other platforms and other teams using their own processes with the right data. We can all work together now to collect data once and get it to everybody that needs it, in the optimal format.

Christopher Simpson
Senior Technical Architect
Edward Jones

How Cribl helps

Migrating to a new SIEM means taking on some risk because, without Cribl, it's a one-way door. Once you walk through it, you can't go back. You're committed to deploying new agents, training staff, updating alerts and other content, and, finally, cut over to the new product.

Cribl turns that migration into a two-way door. You can send data to different SIEMs in the format they expect with no loss of fidelity, and without weakening your security posture. Cribl customers migrate their detections and dashboards to compare products, ensuring the new SIEM works as well as the incumbent product. Even better? Keep the legacy product running for a time after the cutover. This takes all the risk out of the migration and accelerates it at the same time.

Compass points and resources

Based on the data we've explored in this report, IT and Security leaders should take the following actions to upgrade their telemetry data management strategy.

- **Optimize your data management strategy around your data,** rather than around your tools. Data, and its rate of change around volume and diversity of sources, will remain the constant in your enterprise, while tools are adopted or discarded as business needs change. Build your data strategy around how you will optimize your current array of tooling, as well as how you'll migrate away from those tools as your needs change.

- **Scope your data management challenges** by forecasting your enterprise's cybersecurity and observability data collection and analysis needs over a 12, 24, and 36 month horizon and contrast that with your forecasted IT budget growth over the same time period.

- **Adopt observability pipeline technologies,** like Cribl Stream, to abstract the sources of telemetry data from its native destination. This insulates you from market disruptions like onerous acquisitions, while also leveling the playing field when it comes to contract negotiations with your chosen platform vendors.

- **Avoid buying your observability pipeline product** from your cybersecurity or observability platform provider. Without a vendor-neutral position, these captive pipelines will further cement the vendor lock-in you're looking to avoid.

- **Use your pipeline's data routing and formatting capabilities** to test new tools and products without disrupting your incumbent solutions.

- **Leverage observability pipelines** in environments where data growth is forecast to exceed infrastructure budgets to implement a robust data tiering strategy.

- **Separate your systems of analysis from your systems of record** by creating a telemetry data tiering strategy that aligns data value and usage with the most cost-effective storage option.

- **Search for opportunities to consolidate** your cybersecurity and observability tools and platforms using the capabilities around a unified data approach leveraging open storage and access formats: from endpoint, to pipeline, to tiered storage, and search.

Resources

The following resources will help you modernize your telemetry data management strategy:

- See how IT and Security pros wield the power of Cribl for modern data management.
  https://cribl.io/clp/datamanagement/

- Read how escalating data challenges are reshaping IT and security operations and the offer a revolutionary approach to modernizing data management.
  https://cribl.io/clp/navigating-the-data-storm/

- Understand how to tackle the unsustainable skills challenge in cybersecurity and observability.
  https://cribl.io/blog/tackling-the-unsustainable-skills-challenge-in-cybersecurity-and-observability/

- Read how to simplify data management in the cloud.
  https://cribl.io/blog/simplifying-data-management-in-the-cloud-how-cribl-and-aws-strategic-collaboration-agreement-benefits-customers/

- Try Cribl for free up to 1TB/day.
  https://cribl.io/try-cribl/

- Get free in-demand knowledge for data pros that's easy to consume, convenient to access, and available at any time, at your own pace.
  https://cribl.io/university/

Steer toward your final course

Cribl's inaugural *Navigating the data current* report highlights a transformative period for IT and Security teams as they modernize their data management practices.

Cribl's comprehensive insights underscore the pivotal trends shaping the industry: the surge in data sources, the preference for single-cloud strategies, and the diversification in SIEM providers. This report not only illuminates the current landscape but also provides actionable guidance for organizations striving to optimize their data management. As we move forward, the ability to adapt, experiment, and manage costs while ensuring robust security will be critical. Cribl remains committed to supporting IT and Security teams with vendor-agnostic, purpose-built solutions that empower them to navigate these evolving trends confidently.

For more information, please visit at https://cribl.io/free-up-space-for-high-value-data.

Cribl®

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Powered by a data processing engine purpose-built for IT and Security, Cribl's product suite is a vendor-agnostic data management solution capable of collecting data from any source, processing billions of events per second, automatically routing data for optimized storage, and analyzing any data, at any time, in any location. With Cribl, IT and Security teams have the choice, control, and flexibility required to adapt to their ever-changing data needs. Cribl's offerings—Stream, Edge, Search, and Lake—are available either as discrete products or as a holistic solution.

Learn more: cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter (X)

RPT-0001-EN-2-0724