# Splunk Federated Data Management Workshop

## Learn How to Filter, Mask, Route, & Metricize Your Data with Ingest Processor, Edge Processor and Ingest Actions

splunk>
a CISCO company

# Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

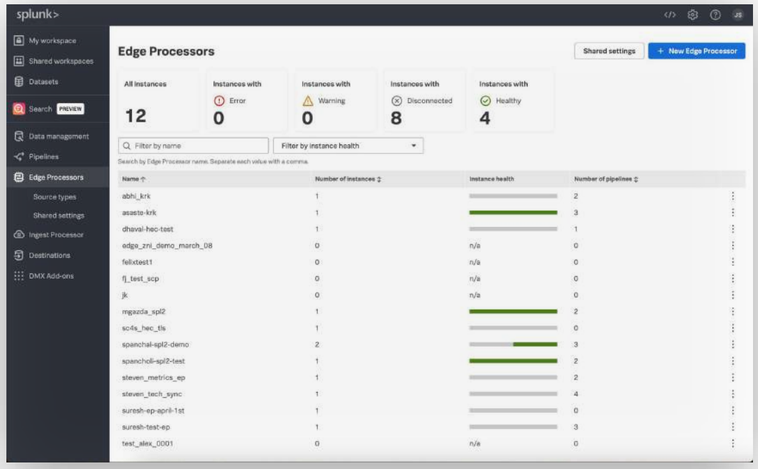


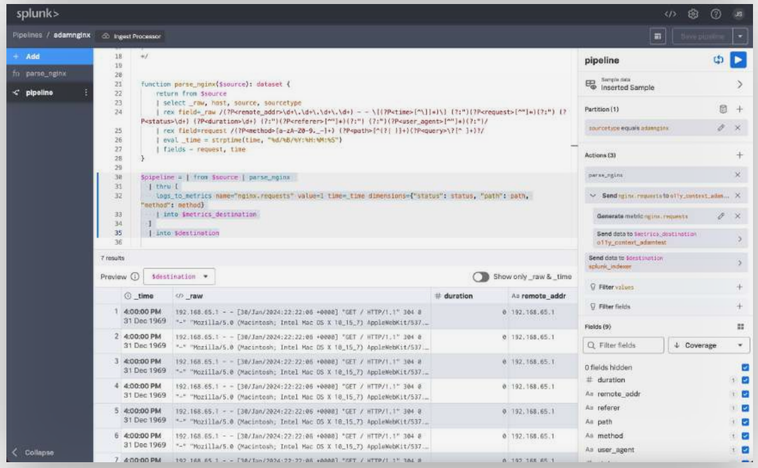
splunk> a CISCO company

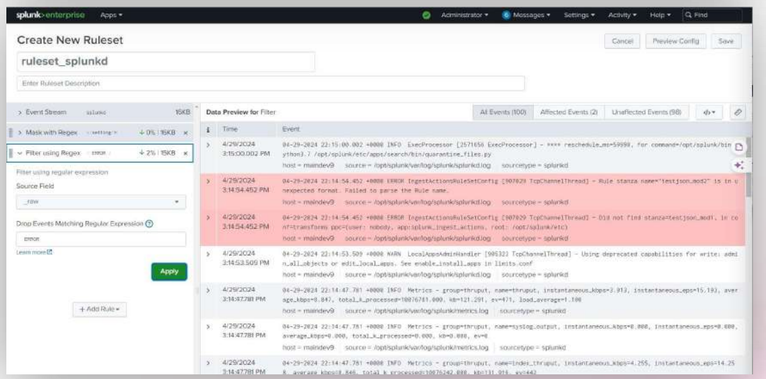
# Why?

Quickly manage your data.

- Learn what tools exist and how to use them.
- Learn how to manage data from your browser.
- Learn to filter, mask, transform, enrich, and route data to multiple destinations.
- Learn you can get faster feedback that your changes are working.



# Workshop Structure

## One base use case for three labs

- Reduce noisy logs.
- Mask sensitive data.
- Route data to S3.
- Route data to a Splunk index.

## Ingest Actions Lab

- Federated Search for AWS S3.

## Splunk Edge Processor Lab

- Enrich data with lookups.

## Ingest Processor Lab

- Logs to metrics.

## Short recap and Q&A after each lab

# Ingest Actions

Filter, Mask, and Route

Easy to deploy simple ingest-time transformation and routing rules using existing Splunk indexing and forwarding technology

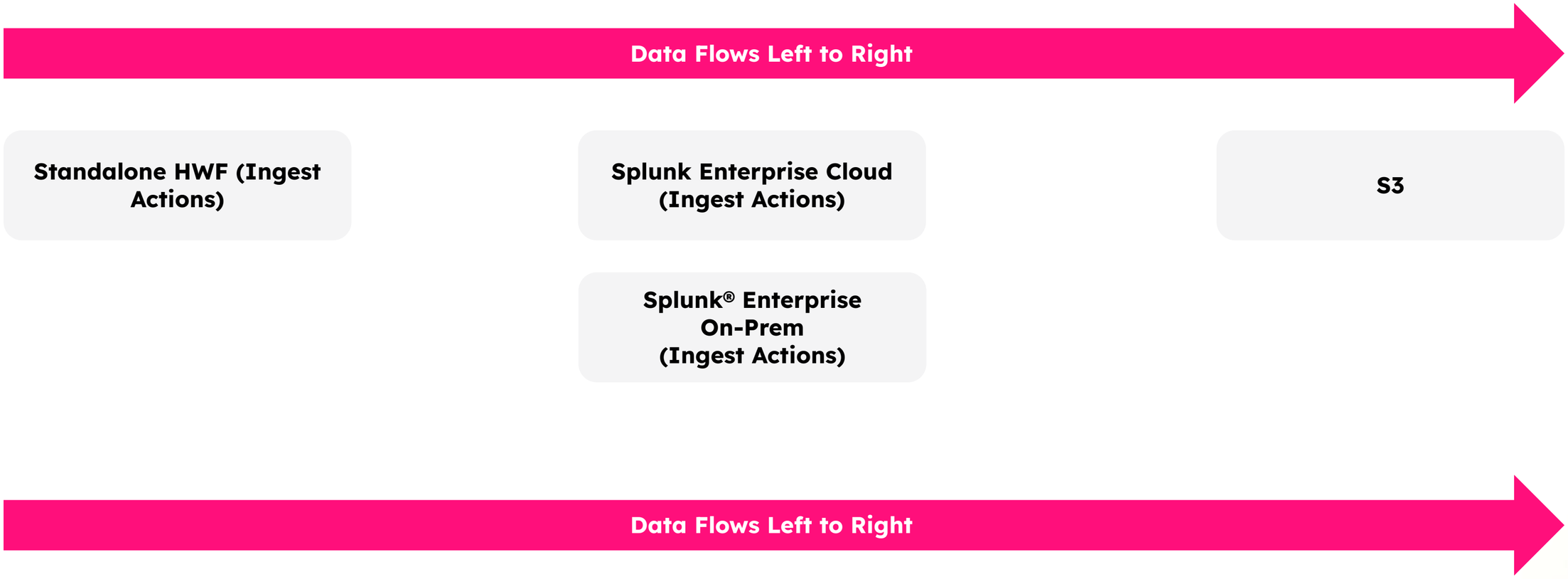
ON-PREM CLOUD

# Ingest Actions

## Data Admin / UI Power User

| WHEN TO USE | HOW IT'S DONE | WHAT YOU NEED |
| --- | --- | --- |
| • Reduce noise / volume → | • Filtering | • Good data quality<br>  – sourcetype, source, host |
| • Redact sensitive data → | • Masking | • Simple → medium complexity use cases |
| • Send to indexes / S3 → | • Routing | |

# Ingest Actions Dataflow



# Enroll in Today's Workshop

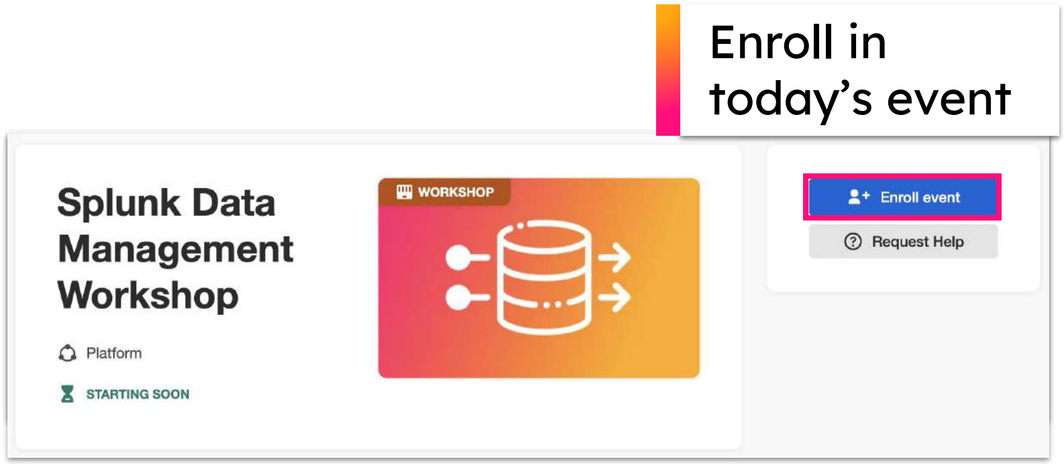
## Tasks

1. Get a splunk.com account if you don't have one yet:
   https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event:
   https://show.splunk.com/event/<eventID>
3. Download the hands-on lab guide:
   https://splk.it/DM-Lab-Guide

   Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:
   https://splk.it/DM-Attendee

## Goal

Enroll in today's event



Workshop


# Ingest Actions

# Ingest Actions Recap

What did you learn?

- How to target and manipulate events using the Ingest Actions UI.
  - No need to edit .conf files.

# Ingest Actions Recap

What did you learn?

- How to target and manipulate events using the Ingest Actions UI.
  - No need to edit .conf files.
- How to mask specific fields in events.
  - PII stays safe from view.

# Ingest Actions Recap

What did you learn?

- How to target and manipulate events using the Ingest Actions UI.
  - No need to edit .conf files.
- How to mask specific fields in events.
  - PII stays safe from view.
- How to route data to S3.
  - Lower cost to store.
  - Great for:
    - Compliance and audit.
    - Low value / high volume data.
  - Can use Splunk Federated Search for S3.

# Ingest Actions Recap

What did you learn?

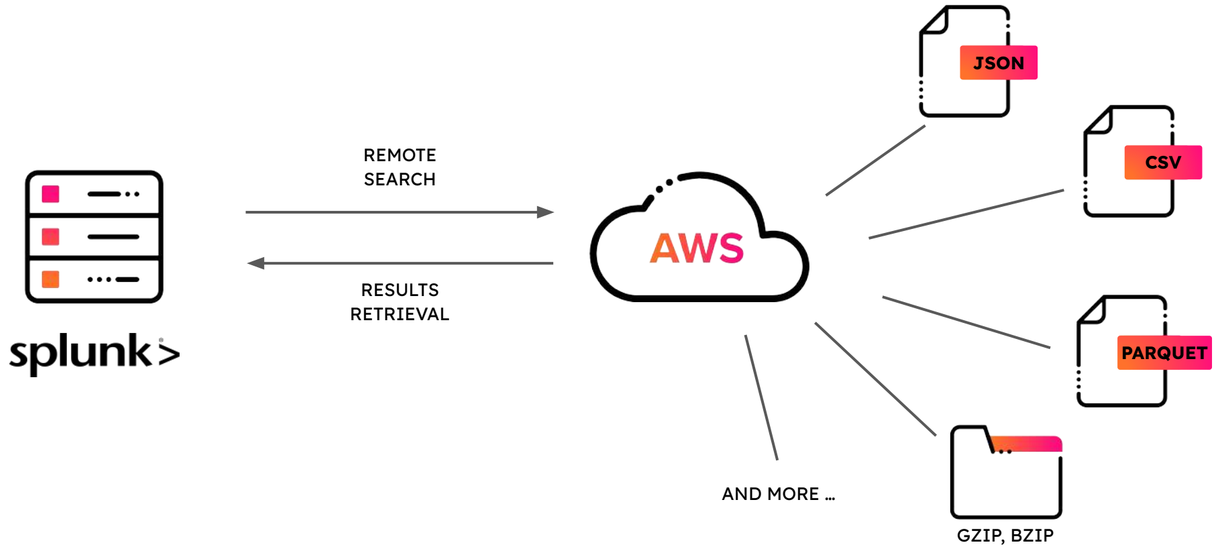
- How to target and manipulate events using the Ingest Actions UI.
  - No need to edit .conf files.
- How to mask specific fields in events.
  - PII stays safe from view.
- How to route data to S3.
  - Lower cost to store.
  - Great for:
    - Compliance and audit.
    - Low value / high volume data.
  - Can use Splunk Federated Search for S3.
- How to route data to Splunk indexes.
  - Store data you need for immediate searching.

# Ingest Actions Questions

# Federated Search for Amazon S3

Read datasets from your Amazon S3 buckets directly in Splunk® Cloud Platform!

Federated Search for Amazon S3 is a search capability that allows you to perform a **remote search** on your Amazon S3 buckets and retrieve the search results directly in your **Splunk® Cloud Platform** instance for investigations, enrichment and analysis.

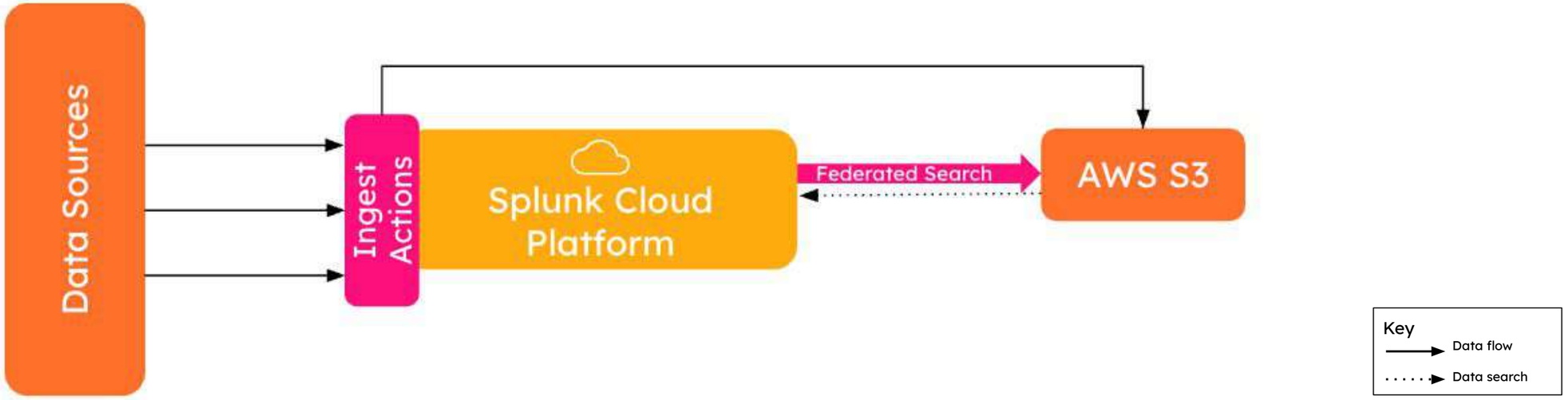


# Scenario

Read data from AWS S3 bucket (Data Ingested by Ingest Actions from Lab 1)

“Search all data on AWS S3 bucket leveraging partitioning with AWS Glue, or using a specified location in Amazon S3 path.

```
| sdselect * from federated:fss3_cisco_index
```



# Edge Processor

Filter, Mask, Enrich, Transform, and Route

Works at the edge of your network to filter, mask, enrich, and transform your data close to its source before routing the processed data to external environments.

HYBRID

# Edge Processor

Data Admin / SPL2 User

## WHEN TO USE

- Reduce noise / volume
- Redact sensitive data
- **Add data via lookups / evals**
- **Add indexed fields**
- Send to indexes / S3

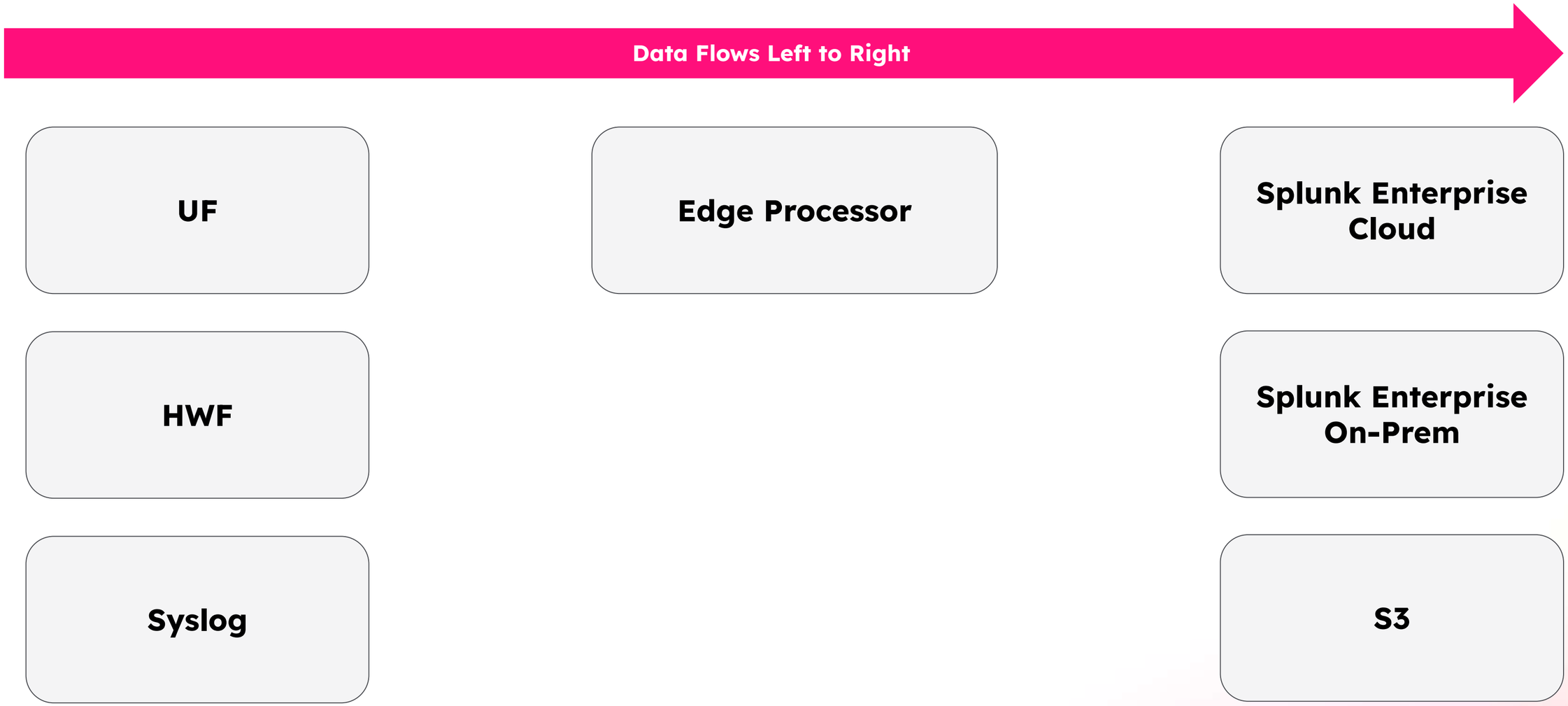
## HOW IT'S DONE

- Filtering
- Masking
- **Enriching**
- **Transforming**
- Routing

## WHAT YOU NEED

- Edge Processing nodes in your own network
- **Cloud stack for pipeline authoring and management of Edge Processing nodes**
- Defined sourcetypes

# Edge Processor Dataflow



# Workshop

14:41

# Edge Processor

# Edge Processor Recap

What did you learn?

- Reinforced what you learned in the Edge Processor Lab.
  - Using SPL2.

# Edge Processor Recap

What did you learn?

- Reinforced what you learned in the Edge Processor Lab.
  - Using SPL2.
- How to author and manage SPL2 pipelines using Edge Processor service UI.
  - No need to manage the Edge Processor nodes.

# Edge Processor Recap

What did you learn?

- Reinforced what you learned in the Edge Processor Lab.
  - Using SPL2.
- How to author and manage SPL2 pipelines using Edge Processor service UI.
  - No need to manage the Edge Processor nodes.
- How to enrich data using lookups as it passes through the Edge Processor.
  - Move data enrichment to the edge.

# Edge Processor Questions

# Ingest Processor

Filter, Mask, Enrich, Transform, and Route

Data processing capability that is fully hosted and managed by Splunk. Use to configure data flows, control data format, apply transformation rules prior to indexing, and route to destinations.

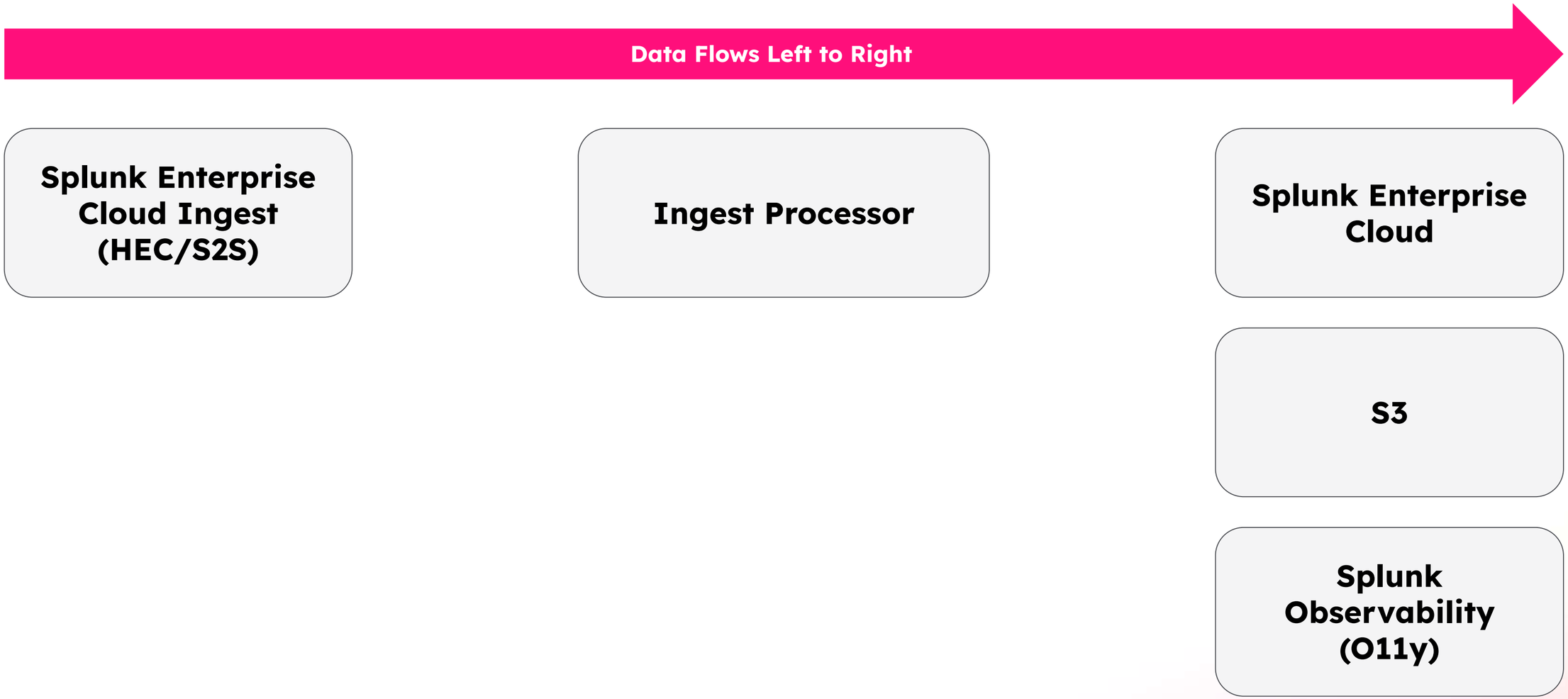
CLOUD

# Ingest Processor

## Data Admin / SPL2 User

| WHEN TO USE | HOW IT'S DONE | WHAT YOU NEED |
| --- | --- | --- |
| • Reduce noise / volume | • Filtering | • Cloud stack |
| • Redact sensitive data | • Masking | • **No infrastructure setup required** |
| • Add data via evals | • Calculated enrichment | |
| • **Logs to O11y metrics** | • Transforming | |
| • Send to indexes / **O11y** / S3 | • Routing | |

# Ingest Processor Dataflow



# Workshop


# Ingest Processor

# Ingest Processor Recap

What did you learn?

- Reinforced what you learned in the Ingest Processor lab.
  - SPL2 processing fully in cloud.
  - No infrastructure needed.

# Ingest Processor Recap

What did you learn?

- Reinforced what you learned in the Ingest Processor lab.
  - SPL2 processing fully in cloud.
  - No infrastructure needed.
- How to author and manage SPL2 pipelines using Ingest Processor service UI.
  - No need to synchronize to edge nodes.

# Ingest Processor Recap

What did you learn?

- Reinforced what you learned in the Ingest Processor lab.
  - SPL2 processing fully in cloud.
  - No infrastructure needed.
- How to author and manage SPL2 pipelines using Ingest Processor service UI.
  - No need to synchronize to edge nodes.
- How to preview snapshot data.
  - No need to upload sample data.

# Ingest Processor Recap

What did you learn?

- Reinforced what you learned in the Ingest Processor lab.
  - SPL2 processing fully in cloud.
  - No infrastructure needed.
- How to author and manage SPL2 pipelines using Ingest Processor service UI.
  - No need to synchronize to edge nodes.
- How to preview snapshot data.
  - No need to upload sample data.
- How to convert logs to metrics.
  - Reduce log data.

# Ingest Processor Questions


# Workshop Recap

- You learned what you can do with Ingest Actions, Edge Processor, and Ingest Processor that helps you with your data.


# Workshop Recap

- You learned what you can do with Ingest Actions, Edge Processor, and Ingest Processor that helps you with your data.
- You learned when you should use Ingest Actions, Edge Processor, and Ingest Processor to process data.


# Workshop Recap

- You learned what you can do with Ingest Actions, Edge Processor, and Ingest Processor that helps you with your data.
- You learned when you should use Ingest Actions, Edge Processor, and Ingest Processor to process data.
- You learned where Ingest Actions, Edge Processor, and Ingest Processor components reside.


# Workshop Recap

- You learned what you can do with Ingest Actions, Edge Processor, and Ingest Processor that helps you with your data.
- You learned when you should use Ingest Actions, Edge Processor, and Ingest Processor to process data.
- You learned where Ingest Actions, Edge Processor, and Ingest Processor components reside.
- You learned how Ingest Actions, Edge Processor, and Ingest Processor work and where they do data processing.


# Workshop Recap

- You learned what you can do with Ingest Actions, Edge Processor, and Ingest Processor that helps you with your data.
- You learned when you should use Ingest Actions, Edge Processor, and Ingest Processor to process data.
- You learned where Ingest Actions, Edge Processor, and Ingest Processor components reside.
- You learned how Ingest Actions, Edge Processor, and Ingest Processor work and where they do data processing.
- You learned why you should use Ingest Actions, Edge Processor, and Ingest Processor instead of editing configuration files.

# Workshop Questions

# Thank you

splunk> a CISCO company