

Data Management and Federation

cisco Live !

Manage SOC Data Your Way with Splunk

Jayant Kripalani
Senior Security Solution Architect – Splunk,
APJC

Session ID: BRKSEC-2544

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2544>

Agenda

- 01 List placeholder
- 02 Lore ipsum dolor sit amet
- 03 Ut laoreet dolore magna
- 04 Duis autem vel eum iriure
- 05 Dolore magna sit
- 06 Lore ipsum dolor sit amet
- 07 Ut laoreet dolore magna
- 08 Duis autem vel eum iriure

Growing data volume makes it harder to be resilient

\$200M

Yearly cost of
system downtime

\$4.9M

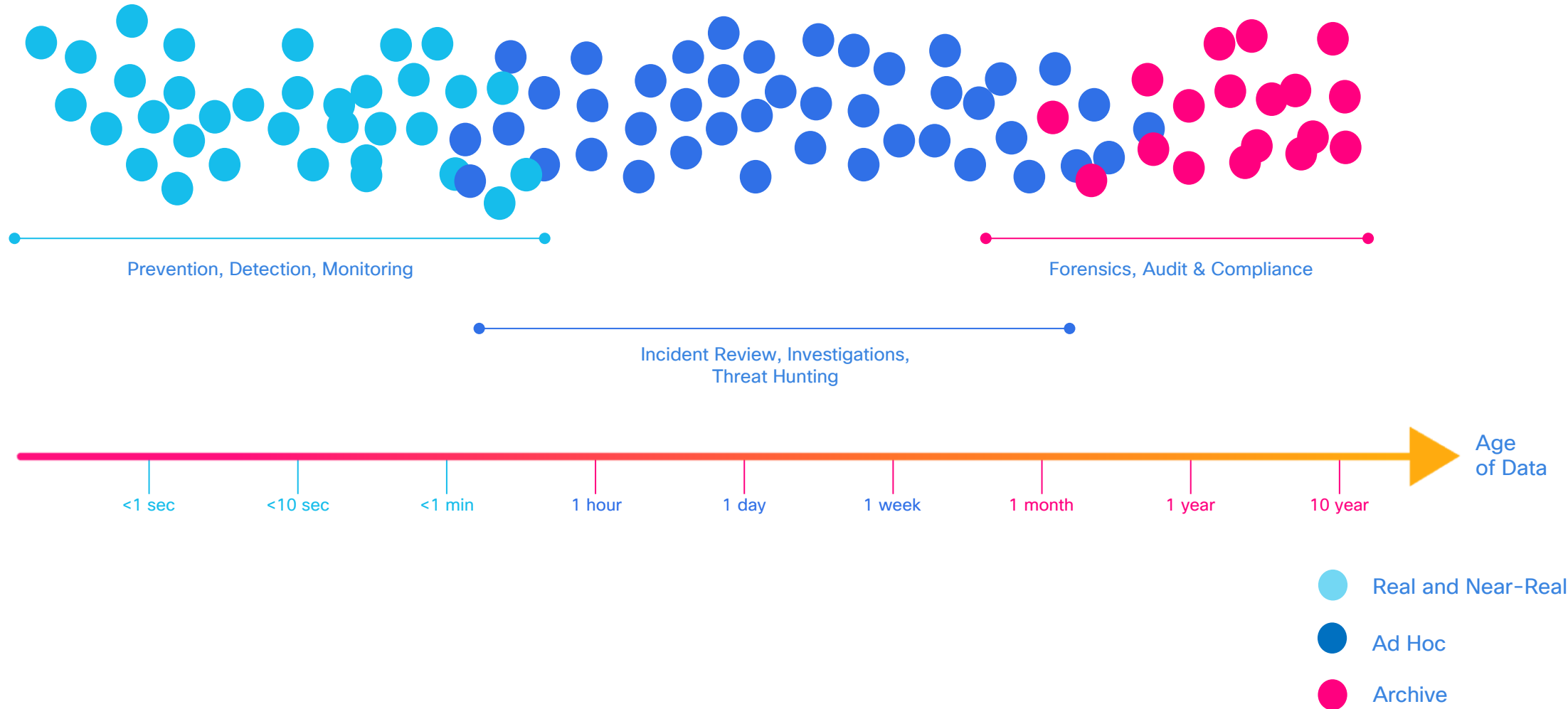
Average cost of a
data breach

90%

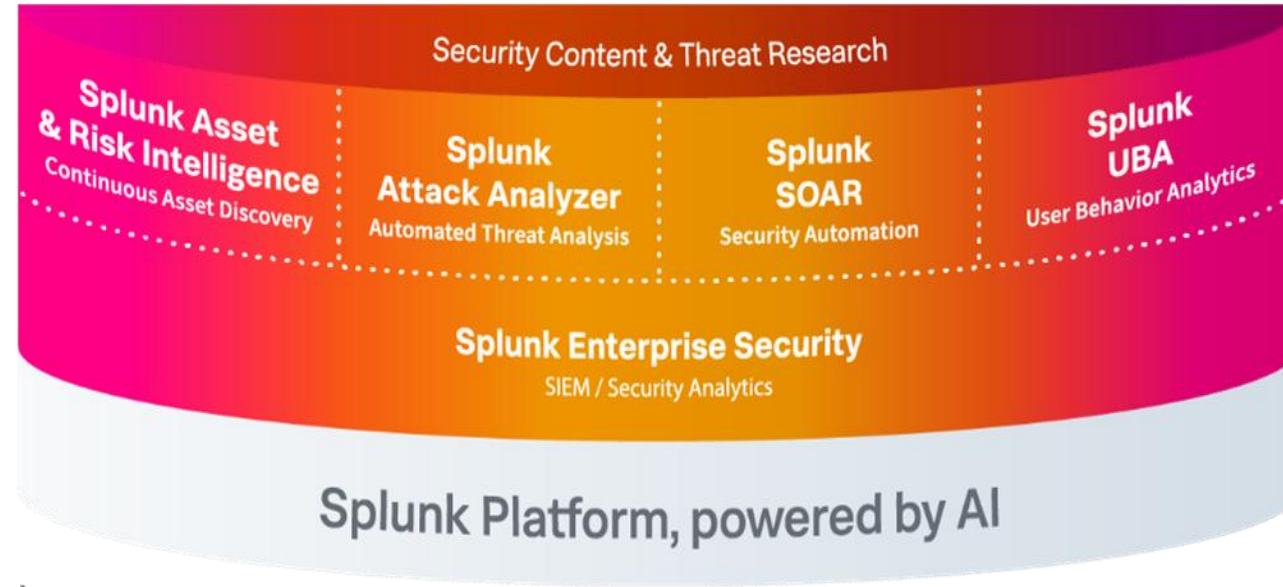
data created past 2
years; accelerating
demand due to AI

Splunk Hidden Cost of Downtime
IBM Cost of a Data Breach 2024

Not all data is created equally



Unified Threat Detection, Investigation & Response



Access
the right
Data



Seamlessly manage and access data
across diverse data stores

Apply
the right
Analytics



Leverage multiple detection
methodologies from signatures to
ML-driven anomaly detection

Accelerate
the right
Actions

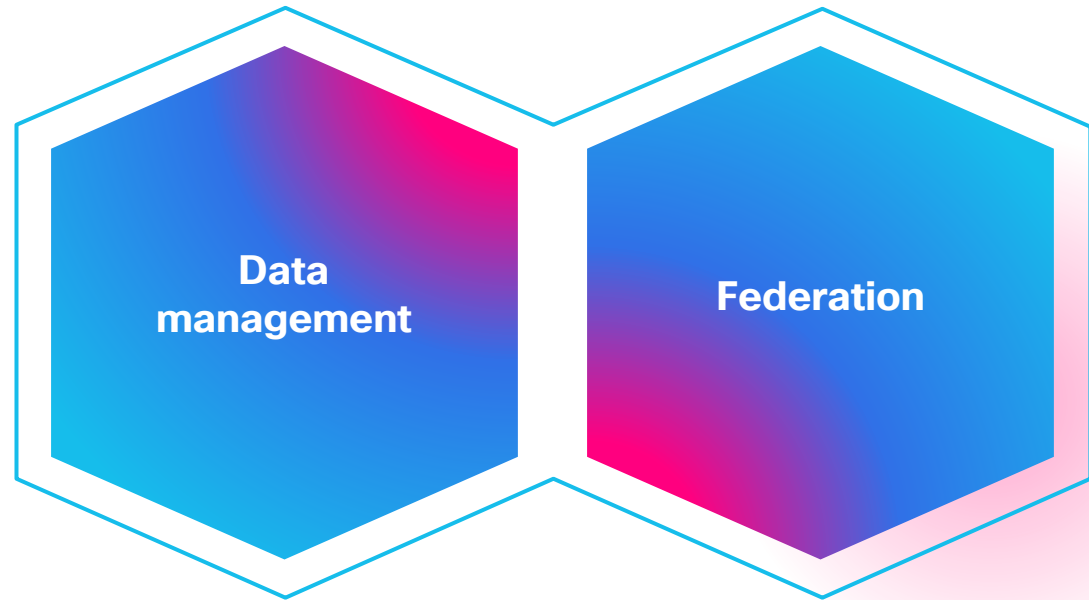


Seamless coordination and
collaboration across the TDIR
lifecycle. Automate workflows in a
single, unified analyst experience

The Data Platform is the foundation

Highly scalable, **unified data management** and **federation** to optimize distributed enterprise data including events, metrics, logs and traces.

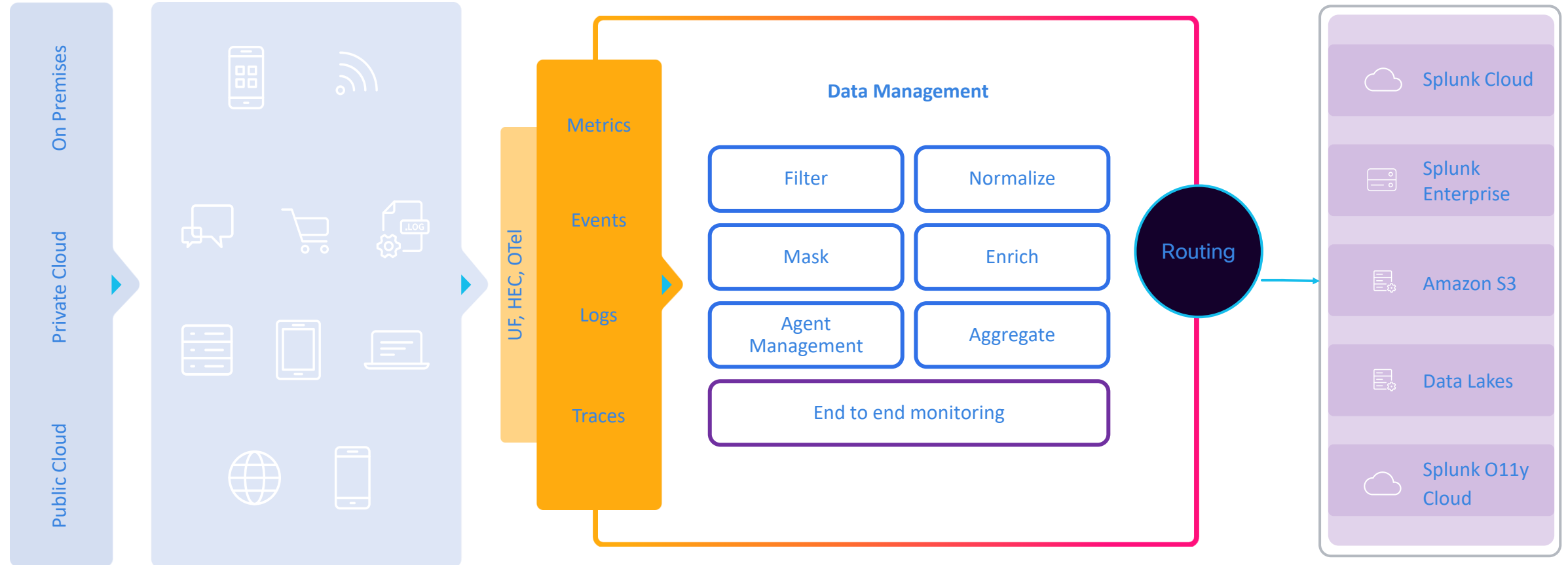
Data is **VISIBLE** from Splunk, without having to **LIVE** in Splunk.



Data Management



Unified data configuration, processing and management

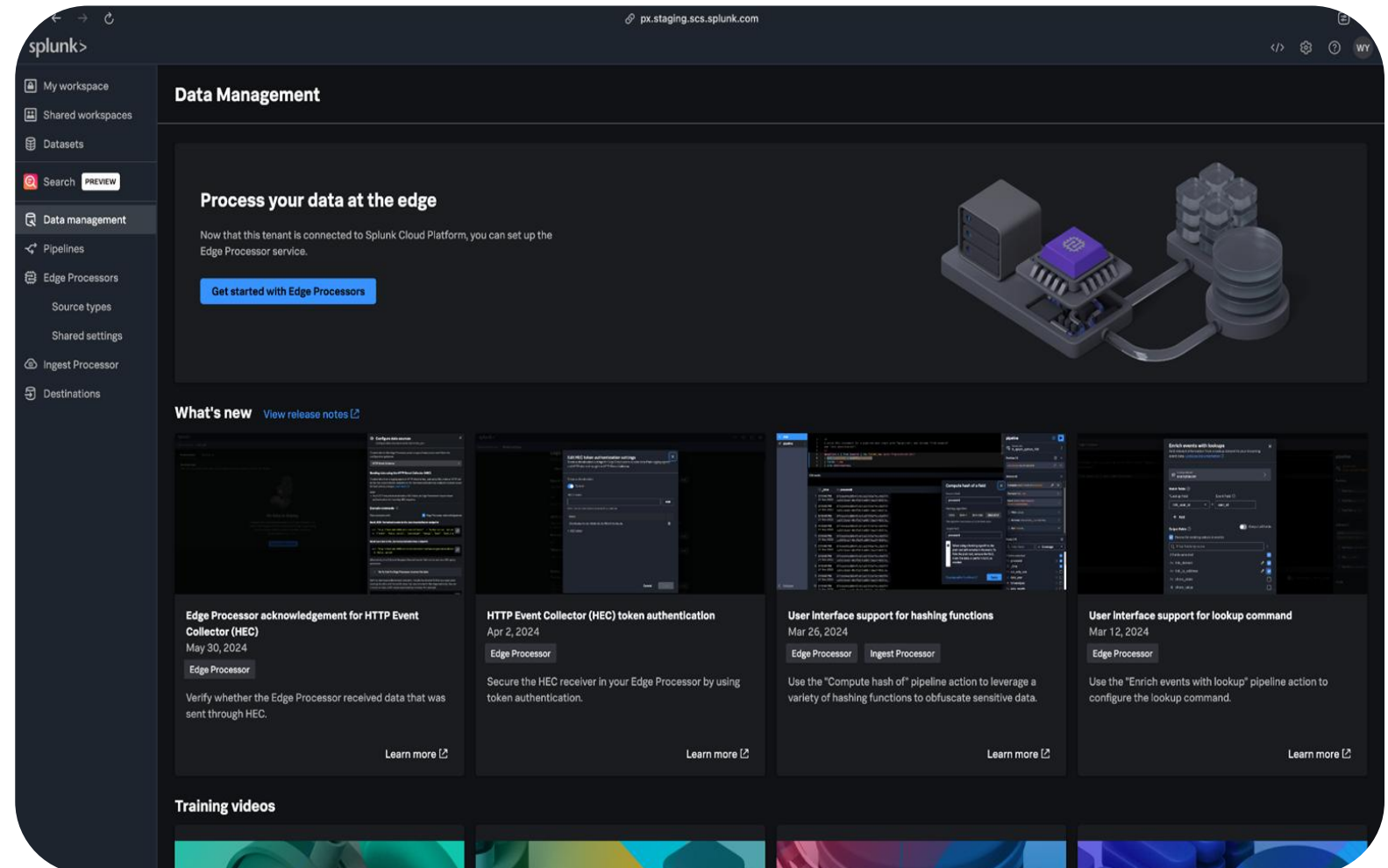


Data Management Experience (DMX)

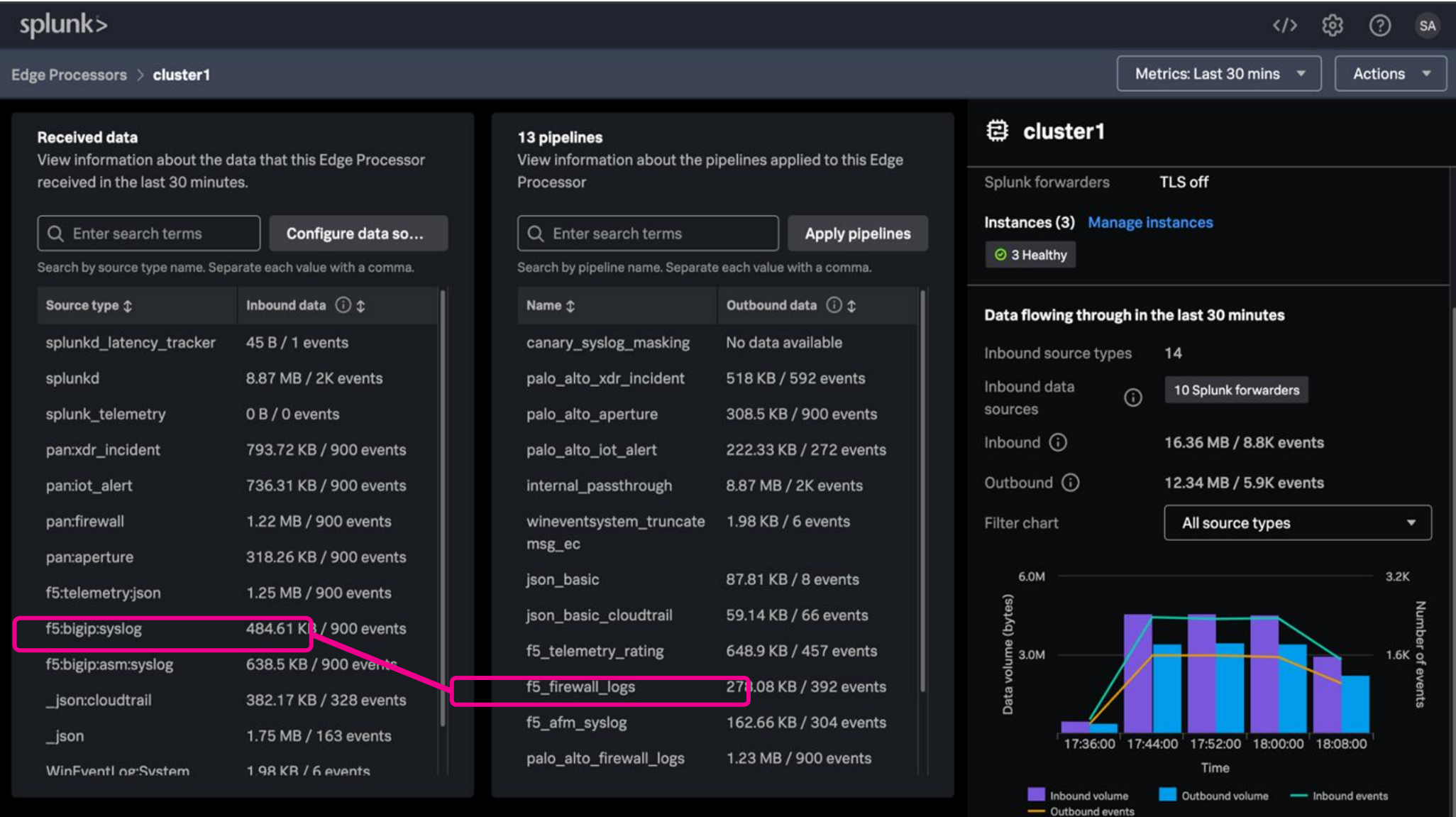
End-to-end data management



- Delivered through a single, modern UI experience
- Powered by SPL2
- Offered through two deployment methods:
 - **Ingest Processor** as a Splunk hosted SaaS offering, great for customers all-in on cloud
 - **Edge Processor** as a customer-hosted offering, great if you want more control at the edge

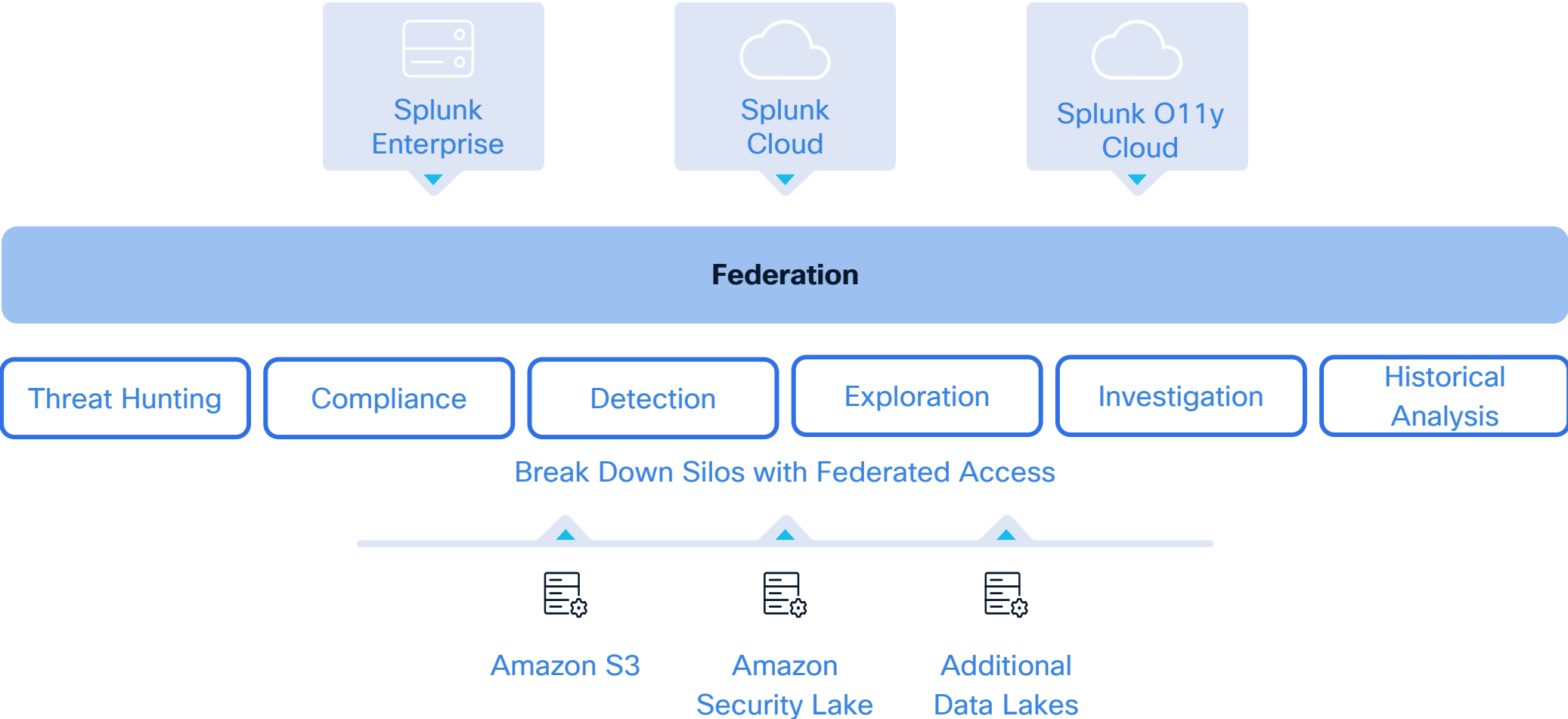


Edge Processor



Federation

Break down silos with federated access

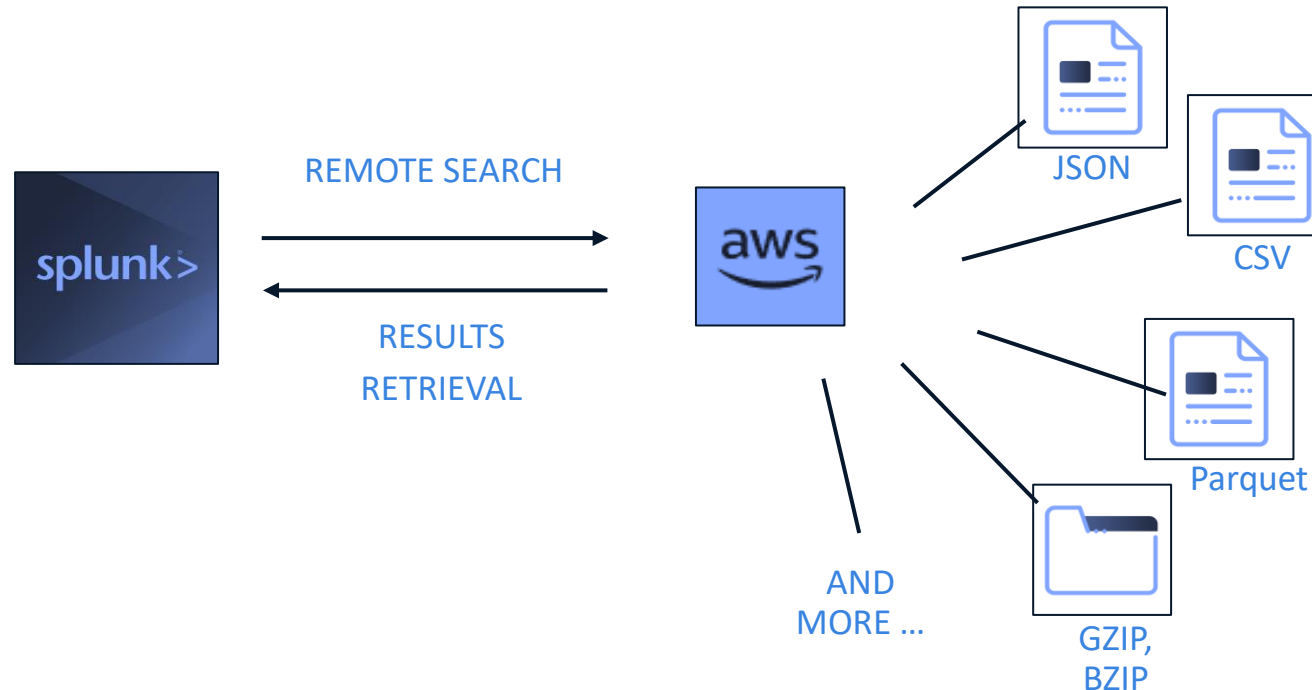


Federated Search for Amazon S3

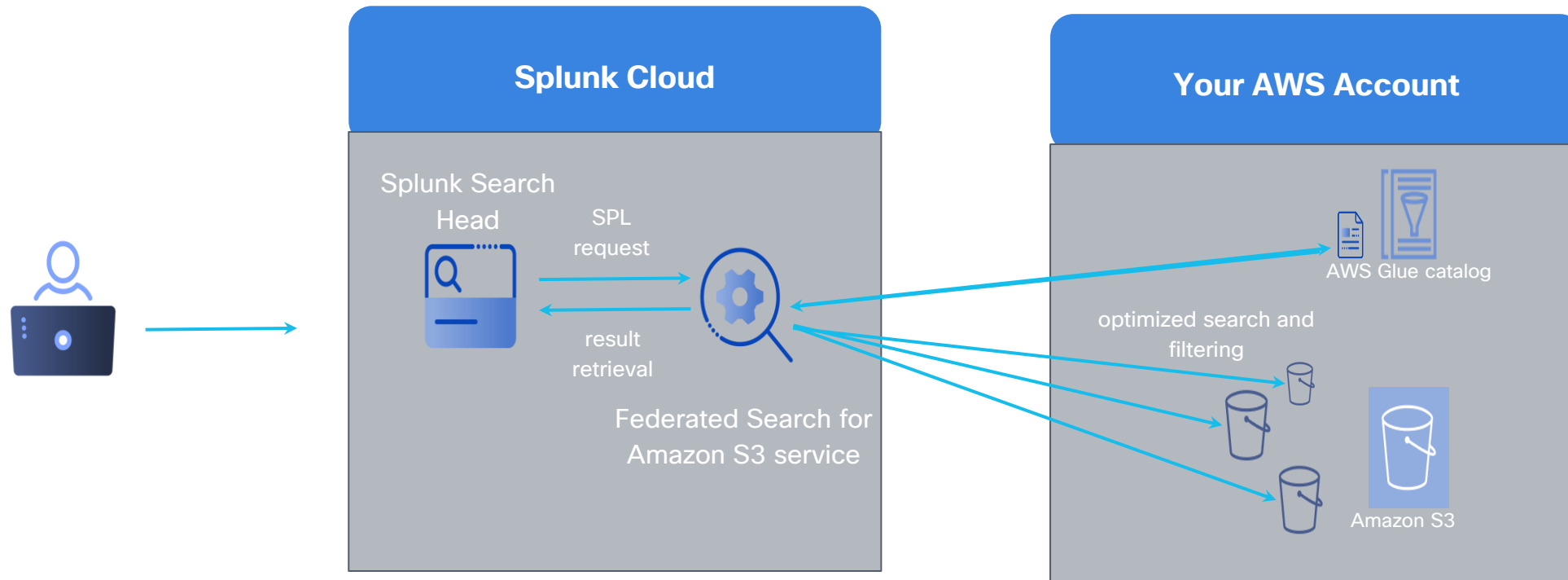
Read datasets from your Amazon S3 buckets directly in Splunk Cloud Platform!



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 correlation, enrichment and analysis.

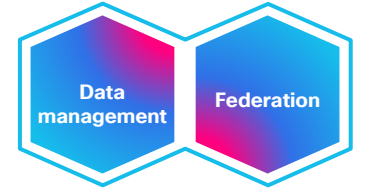
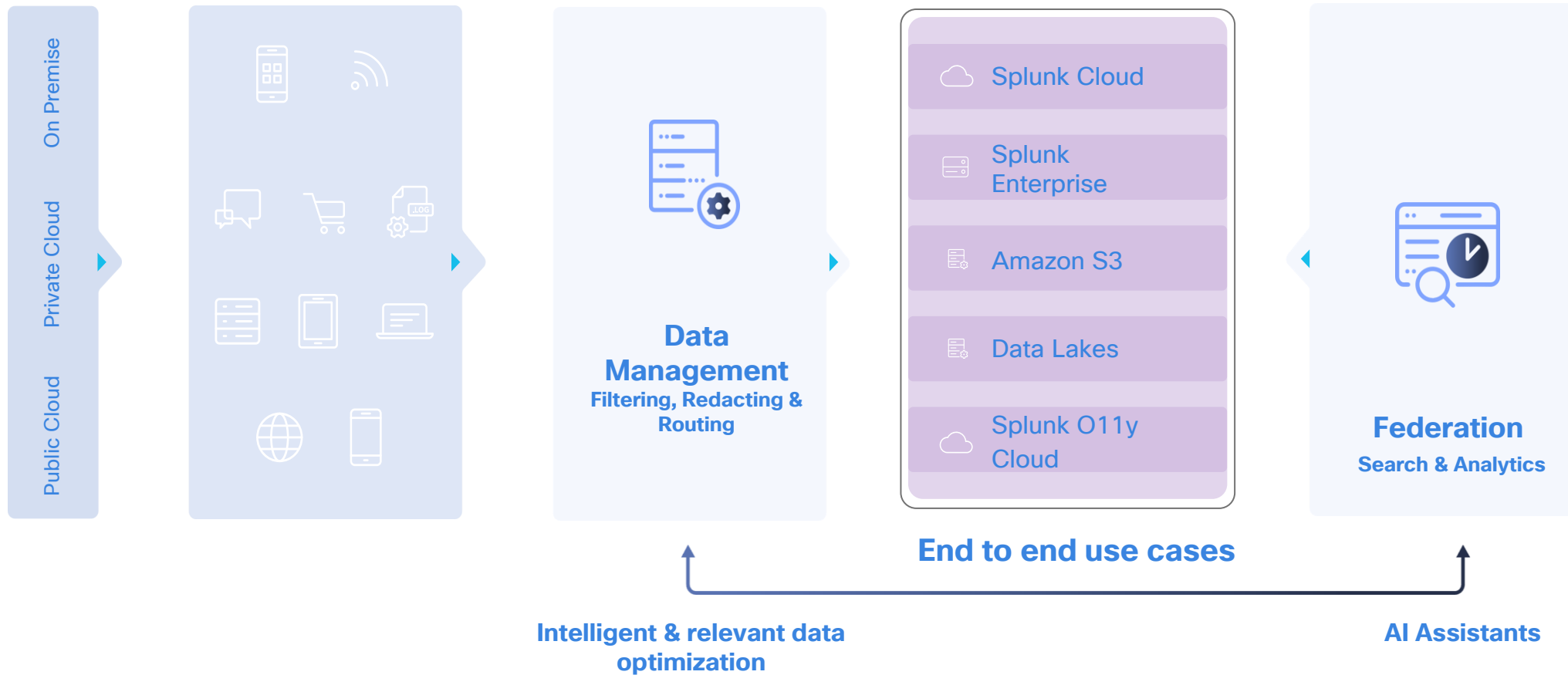


How does it Work?

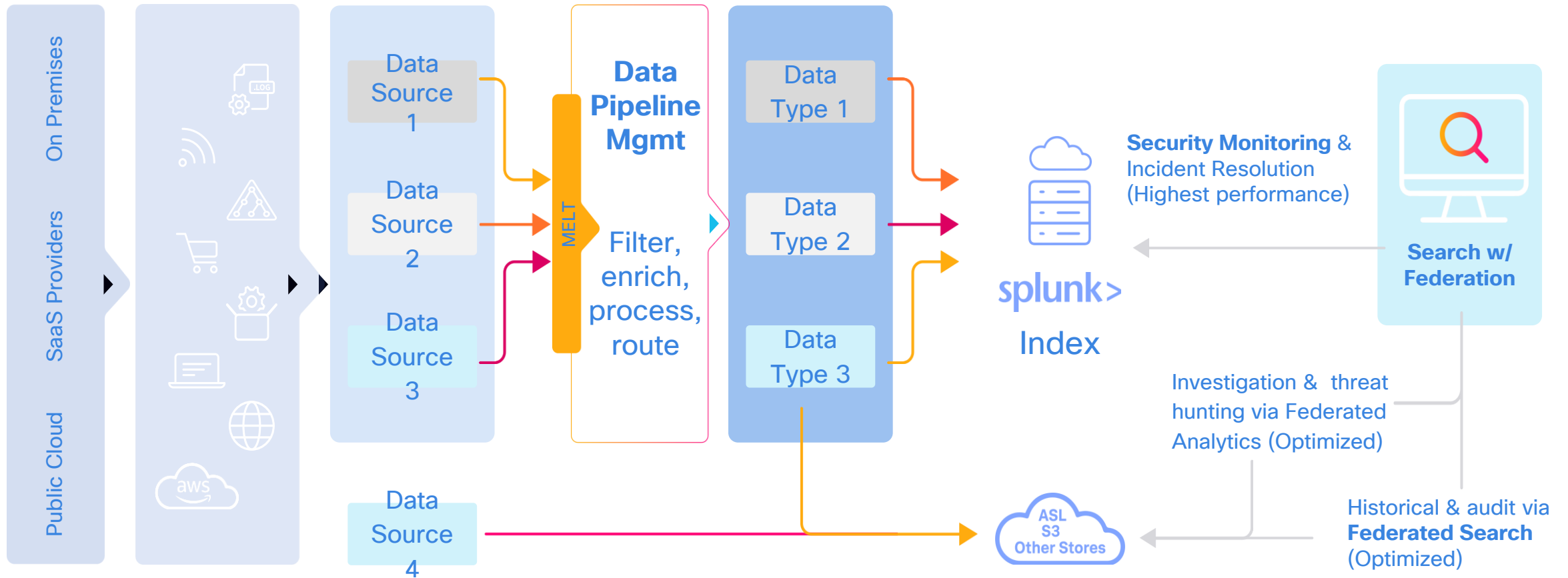


Data Management and Federation

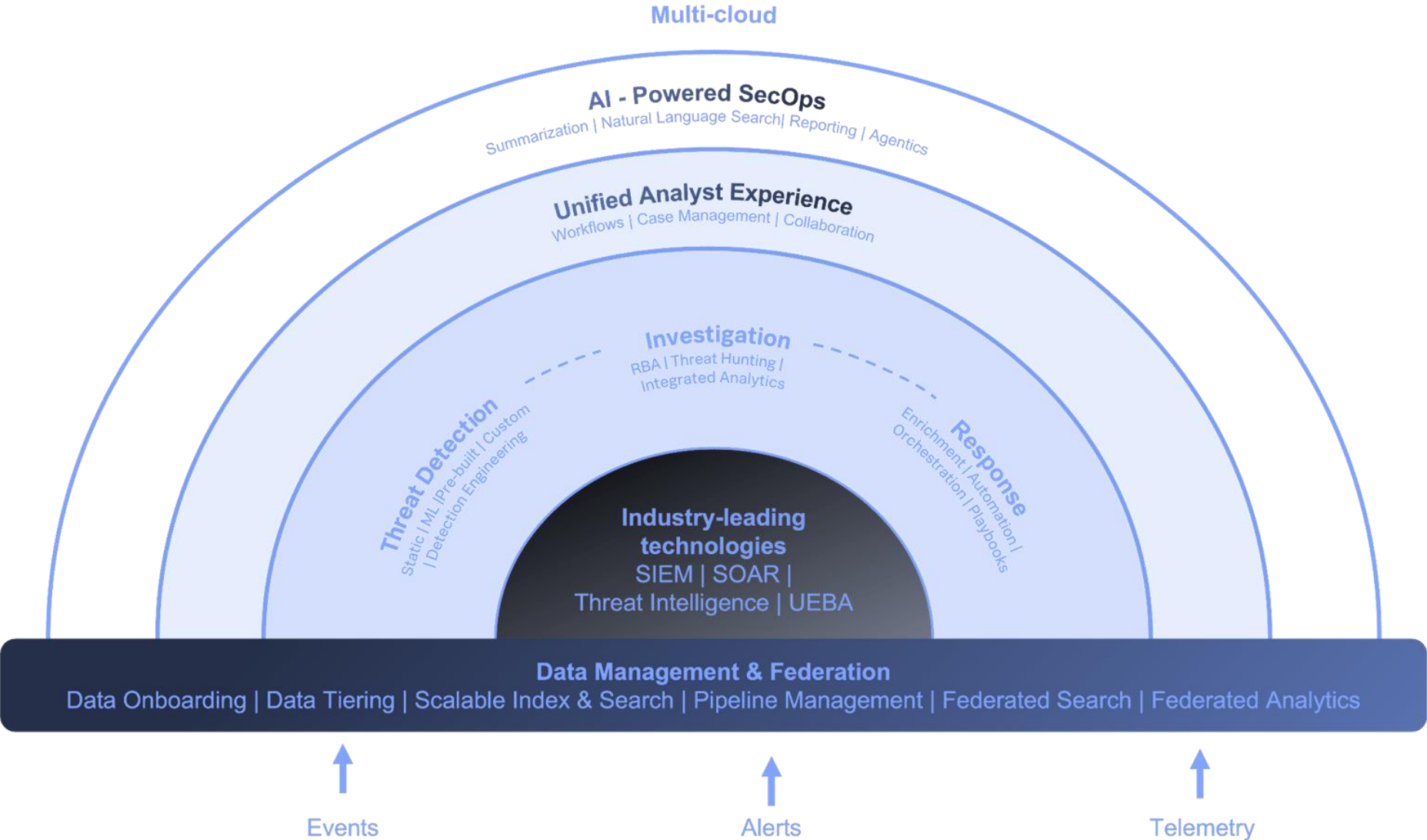
Enable a broader range of use cases



Optimized data design across use cases

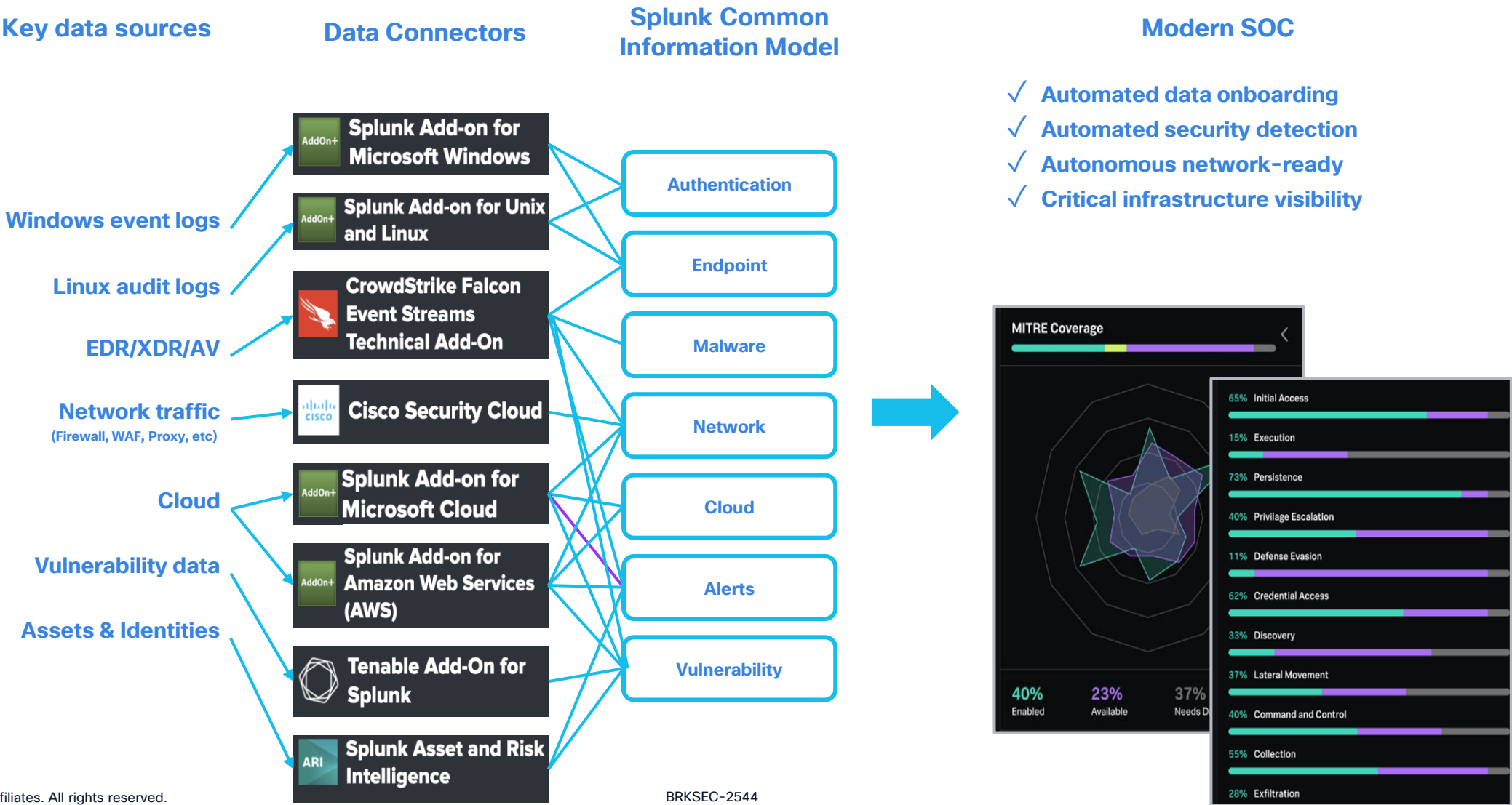


Splunk Enterprise Security



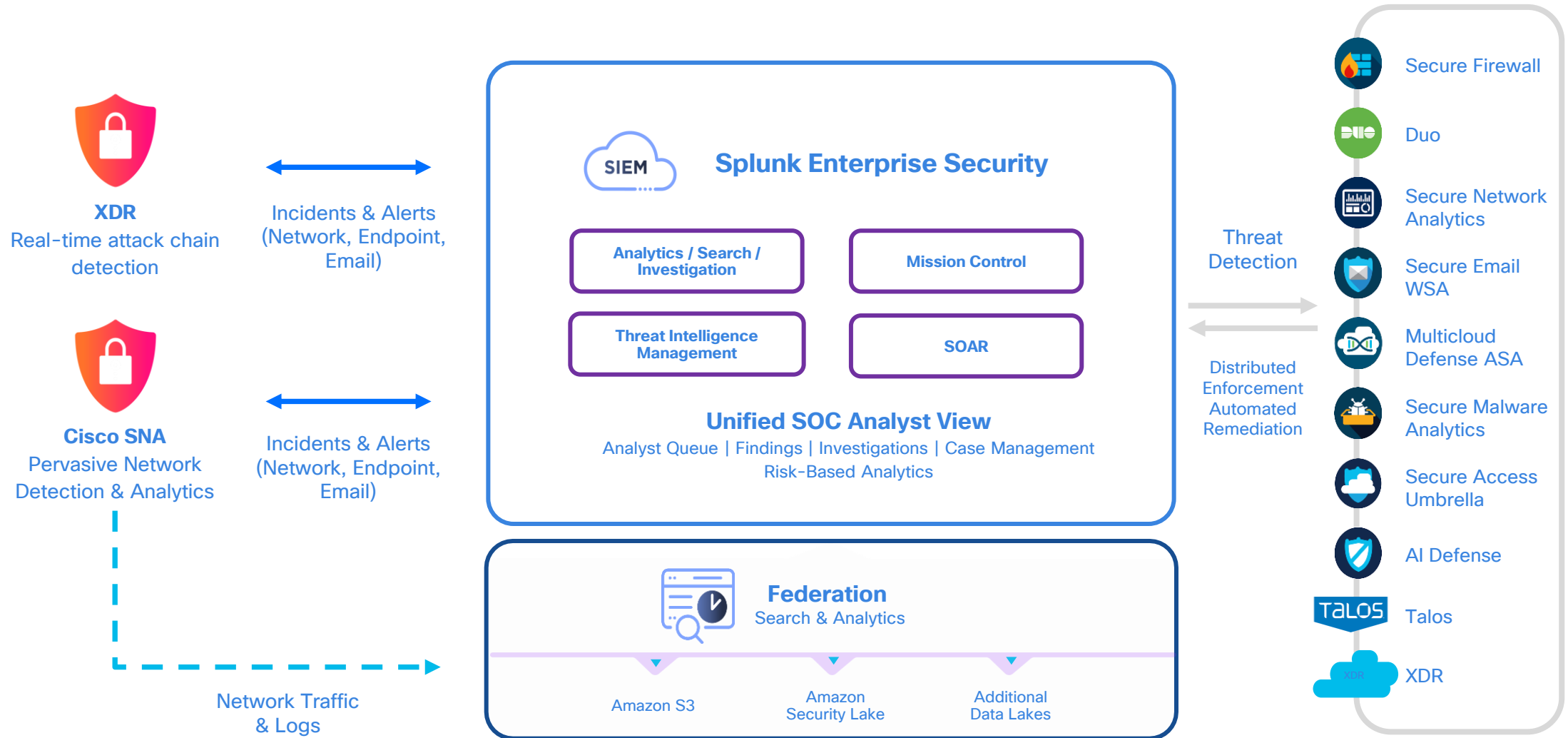
Security Logging Baseline

Logging policy based on visibility of critical business systems



Unifying Threat Detection, Investigation and Response

Splunk Enterprise Security: The Core of the Unified TDIR Experience



SOC Overview Dashboard



Disposition

True Positive

4

0.6%

Suspicious Activity

Benign Positive

2

0.3%

Suspicious but expected

False Positive

2

0.3%

Inaccurate data

False Positive

2

0.3%

Incorrect Analytic Logic

Undetermined

619

97.9%

Unassigned

1

0.2%

Other

0

0.0%

Incident Analysis

Owner

6

unassigned 621

sc_admin 2

splunker 2

sgeetarfunk 2

soar_admin 2

lthomson 3

Status

4

New 480

In Progress 149

Resolved 2

Pending 1

Urgency

5

Critical 181

High 117

Medium 188

Low 145

Informational 1

Disposition

7

Undetermined 619

False Positive - Incorrect Analytic Logic 2

True Positive - Suspicious Activity 4

Other 2

False Positive - Inaccurate Data 2

Benign Positive - Suspicious But Expected 2

Unassigned 1

MITRE ATT&CK Techniques by Risk Object

hash_values

host_artifacts

network_artifacts

system

user

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

privilegeEscalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Privilege Escalation

How to maximize value

With unified data management and federation

High Performance

Prevention, Detection, Monitoring

Search Tier: Search & Analytics for highest performance with configurable data retention

Data Management: Enrich, mask, and transform

Performance at Cost

Incident Investigation, Threat Hunting

Search Tier: Federated Analytics for performance on data <30 days, subject to data lake latency

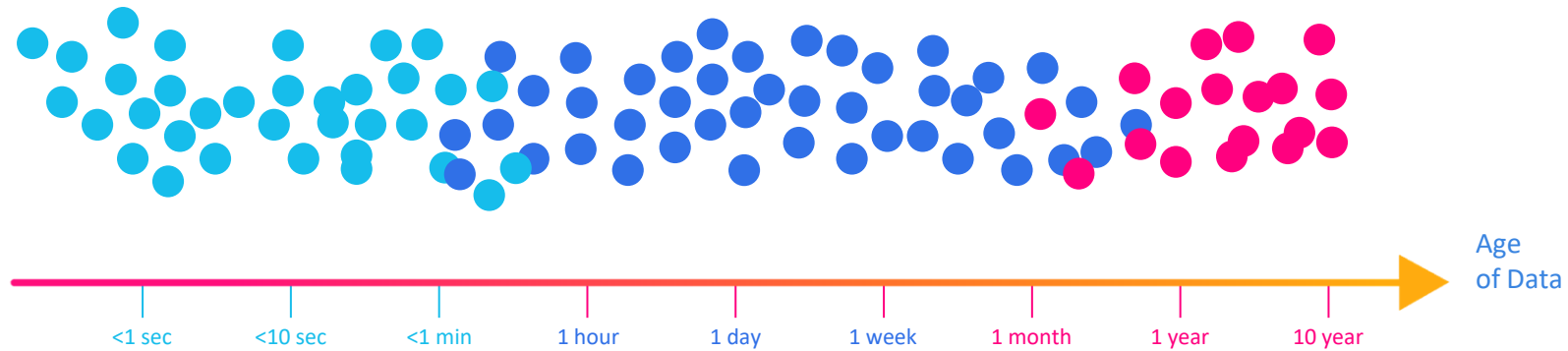
Data Management: Ingest Processor
Metricisation, Lookups

Compliance

Audit, Forensics, Compliance

Search Tier: Federated Search for less performant scanning of archived & long term data

Data Management: Filter & Route with Edge Processor



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

