
merlin group
March 11, 2025 | Washington, DC
XCCELERATE
Advancing Cyber Innovation for Government

Transforming Security Operations with AI and Data

Josh Brunvoll - Sr Solutions Engineer, Cribl

Deepak Badami – Pr Sales Engineer, ExtraHop

Analyze, collect, process, and route network insights at any granularity anywhere **in your Enterprise**

merlin group XCCELERATE 2025

ExtraHop

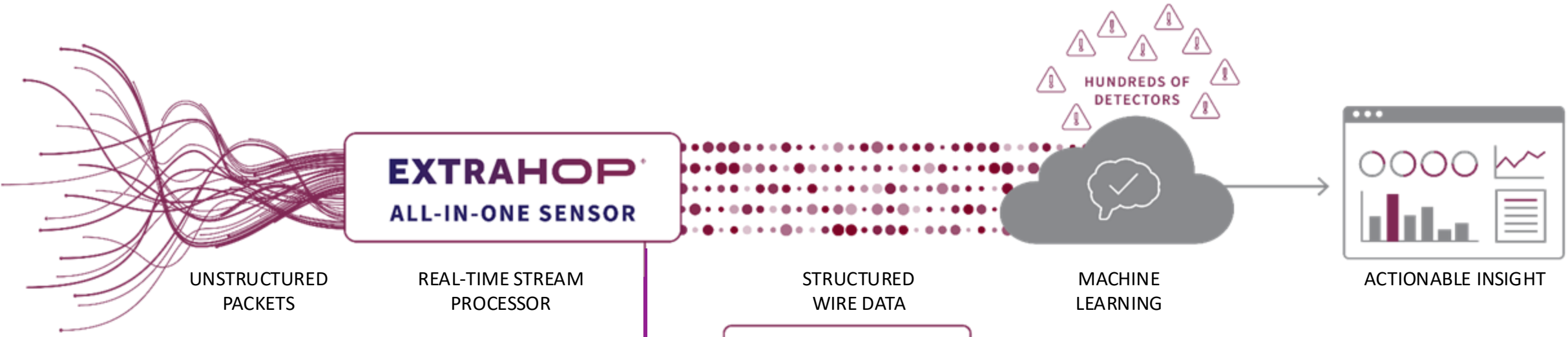
Cribl

Key Challenges and Requirements

- Mandates such as M-22-09 and M-21-31
  - Comprehensive logging and store
- Continuous Zero Trust Validation and Visibility
- Encrypted traffic
- Threat Detections and Incident response
- Correlation and faster Investigation
- Granular data = Better AI
- Log Standardization and storage
- Vendor neutral approach for SIEM/SIEM Vendor Lock in

Everything on Your Network, at Wire Speeds and Cloud Scale

One Platform, Many Use Cases



- Consolidate NDR, NPM, and IDS into a single powerful platform
- Instrument once, analyze for security, performance, and resilience
- One integration point to SIEM and EDR

METRICS

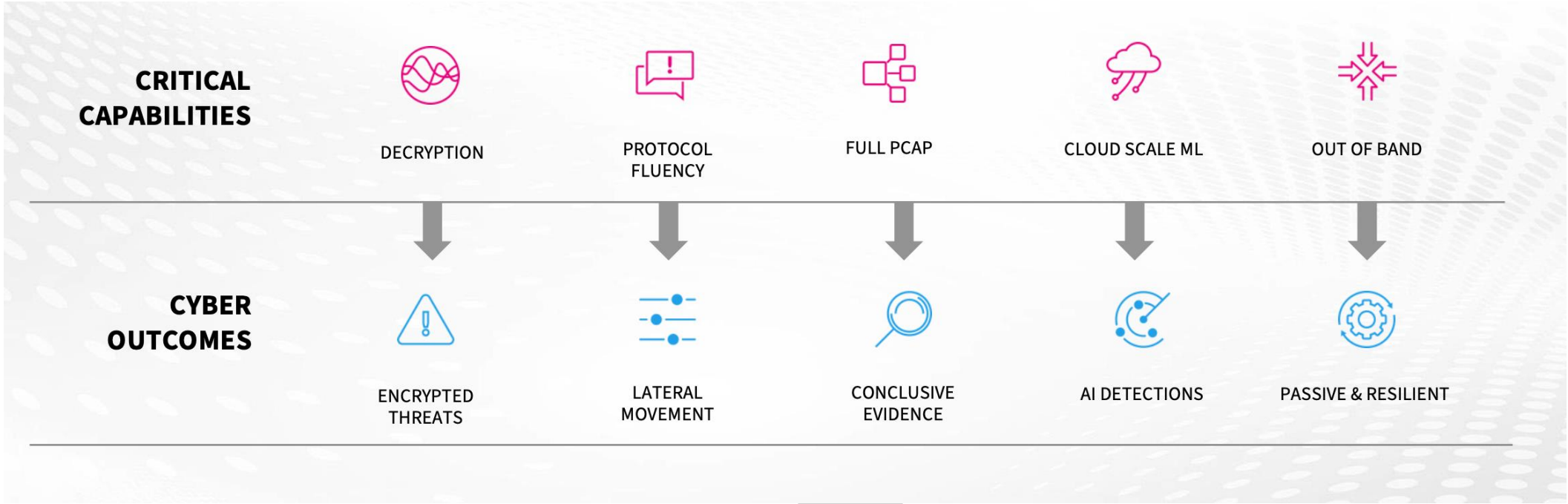
RECORDS

PACKETS

ASSETS

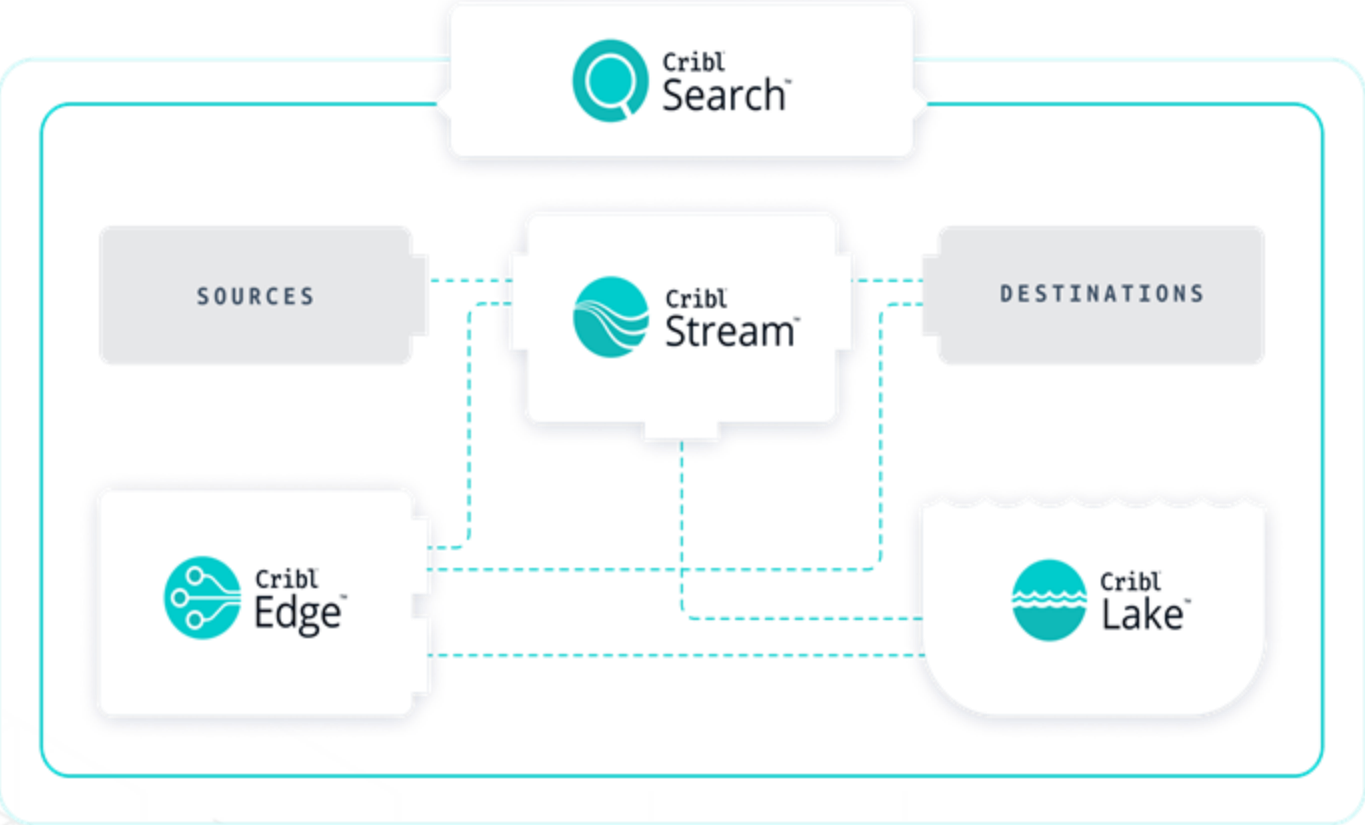
- 30, 60, 90, 180, 365 Days Lookback
- Cloud Scale Machine Learning
- Every packet, every application, for every conversation on the wire
- Cribl routing to long term frozen storage

ExtraHop NDR



AI SOC/SIEM/NG-SIEM

Cribl Overview



Technology innovator

- Data Engine for IT and Security
- Created industry's first Search-in-Place technology, purpose built for Cloud
- Defined Observability Pipeline Market
- Vendor-agnostic, hybrid-cloud approach

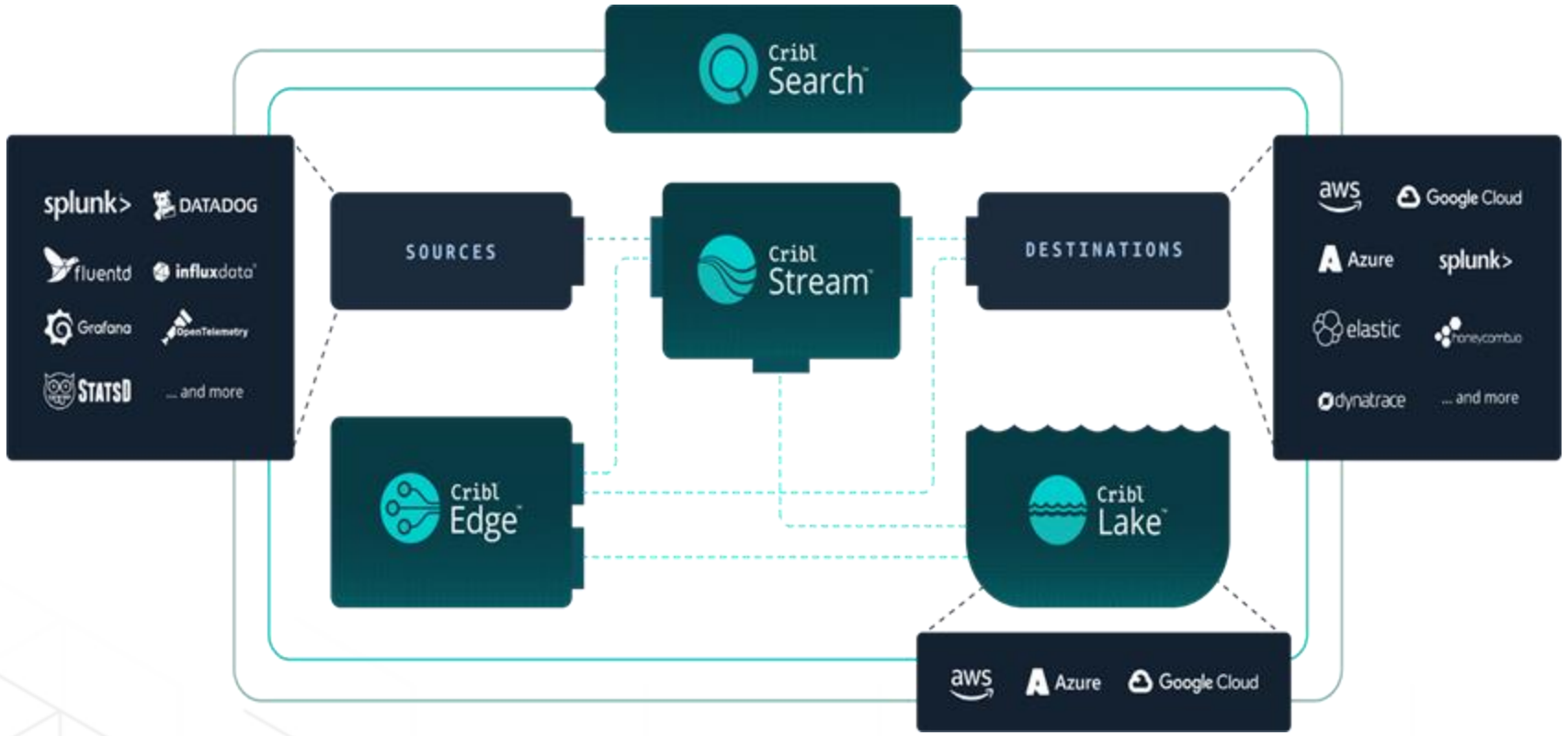
Hyper growth company

- 800+ employees globally
- Founders bring 30+ years of observability experience
- Strong leadership team with experience leading data, security, networking, and B2B companies

Solid financials

- 4th fastest $1M to $100MM ARR in Silicon Valley*
- $400M+ in funding

Cribl: Get data from any source into any SIEM



Reduce associated costs with your data

- Pre-process data before it is ingested into your system of analysis.
- Store data by default into a cost effective long term storage.
- Eliminate architectural overhead.

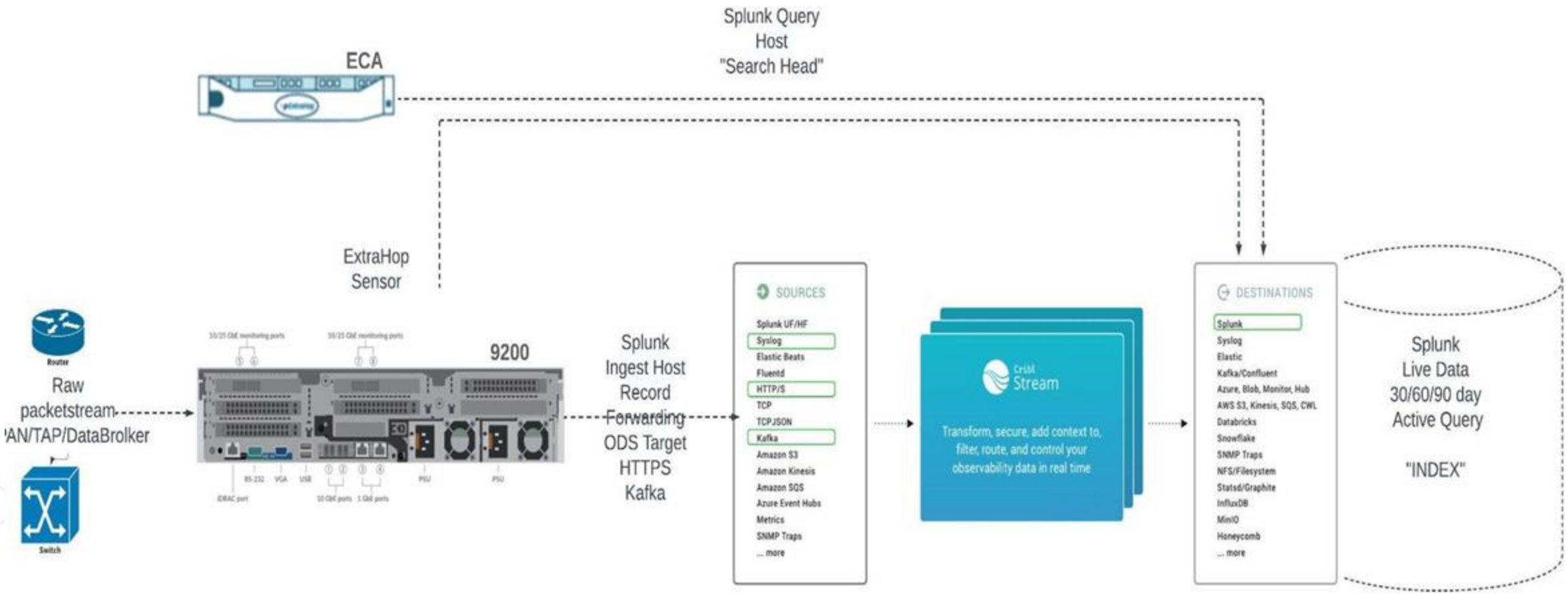
Promote interoperability with tools

- Leverage your data across existing tools.
- Store and utilize data where its meant to be.
- Easily conduct migrations between SIEMs or even to/from cloud

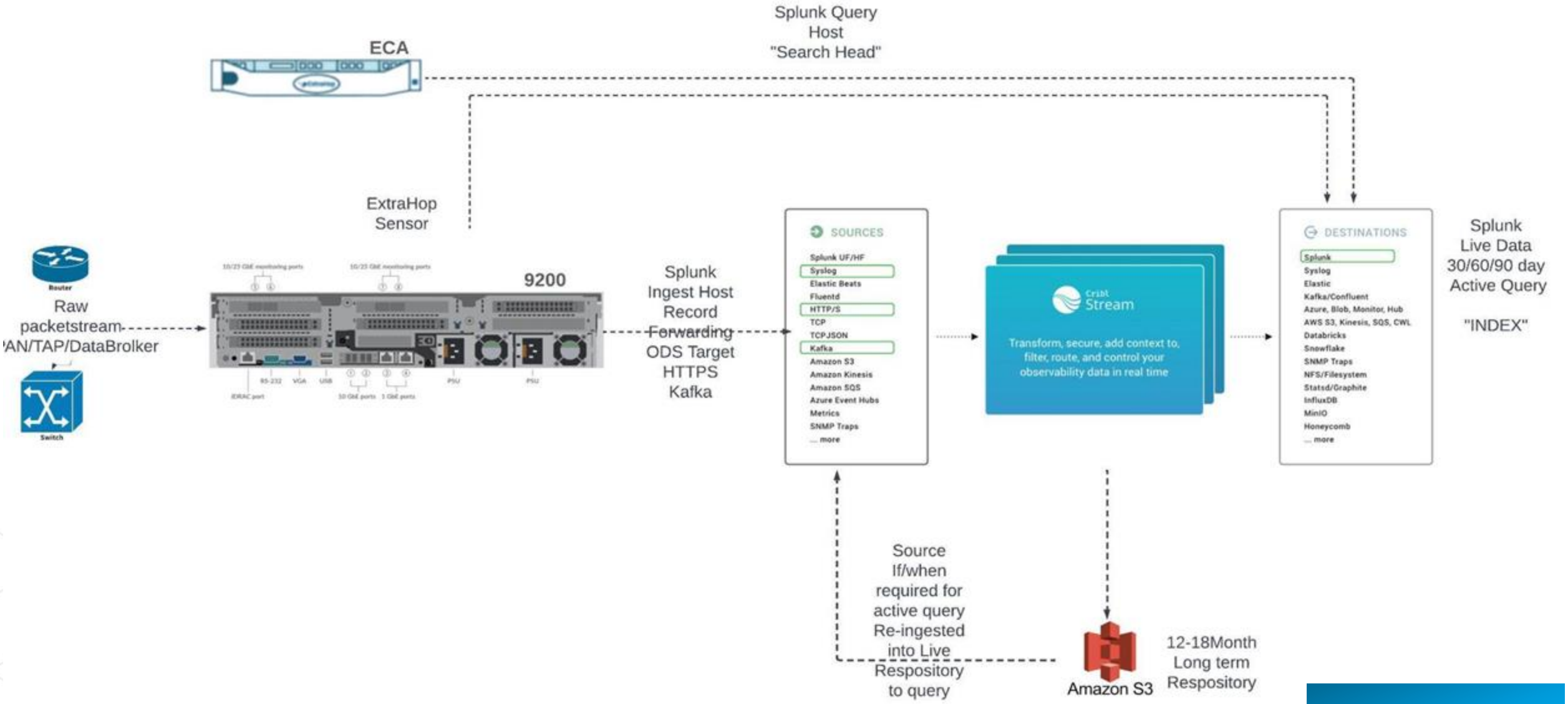
Arm your IT and Security teams

- Regain control of the data layer for choice and flexibility.
- Deny vendor lock-in. IT IS **YOUR** DATA!
- Enhance investigations with optimized and enriched data.

ExtraHop + Cribl: Standardize, Filter and Store



ExtraHop + Cribl : Long term Record Retention and Rehydration



ExtraHop + Cribl

- Identify and close visibility gaps
- Visibility into encrypted traffic and Lateral Movement
- Zero Trust Continuous Monitoring
- Granular network logs, detection and investigation for AI based SOC automation

- Promote Flexibility and Control of your data and the tools your organization uses.
- Reduce costs associated with your data; Storage, Infrastructure or data itself.
- Supercharge your data with enrichments and noise reduction.
- Enable your portfolio of tools to compliment each other