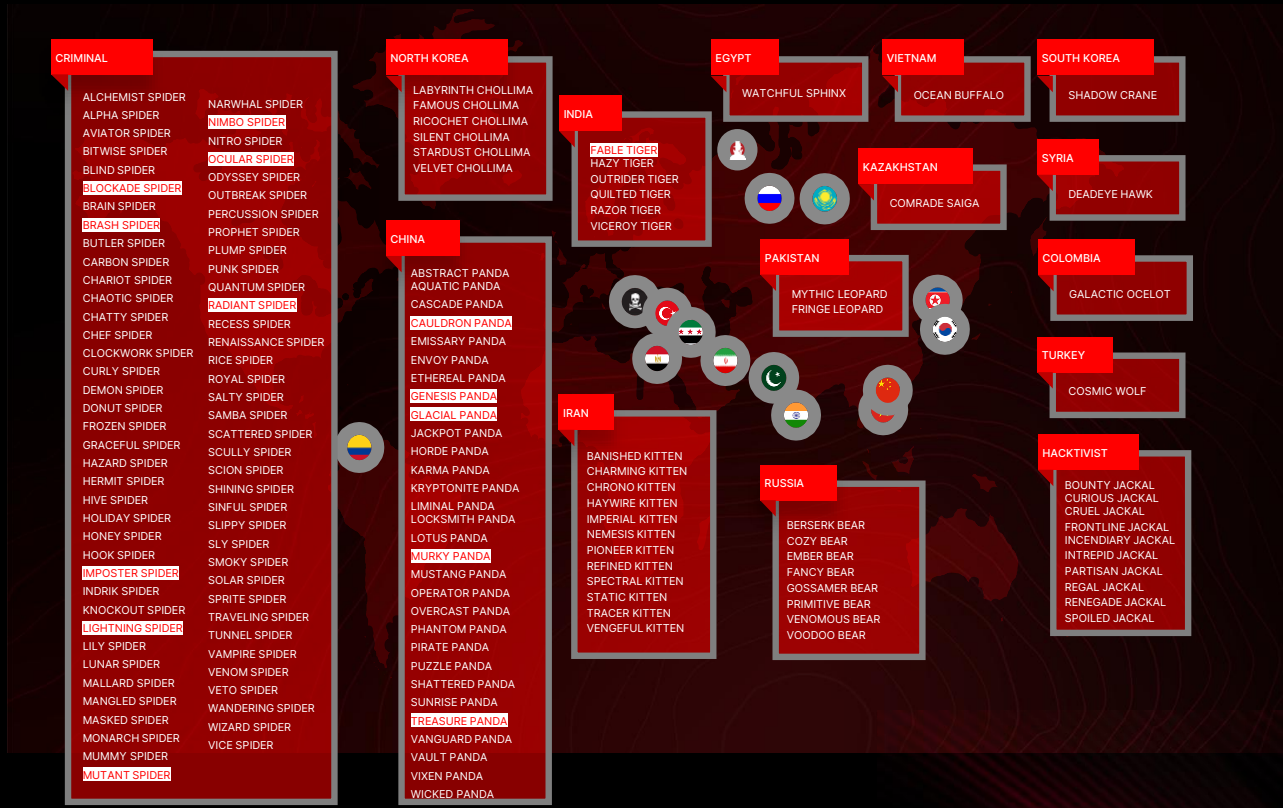
How CrowdStrike Falcon NG-SIEM and Cribl Are Reshaping the SIEM Journey

One Platform to Stop Breaches

Global Adversaries

The Growing Threat Actor Landscape

- 14 New Adversaries
- 265+ Total Tracked
- 150+ Malicious Activity Clusters



CROWDSTRIKE

CROWDSTRIKE

2025 Global Threat Report

Threat Landscape by the numbers

INITIAL ACCESS

442%
Increase in Voice Phishing (Vishing) in 2024

50%
Increase in Access Broker Activity

52%
Vulnerabilities observed related to Initial Access

LATERAL MOVEMENT

51s
Fastest Breakout Time

STEALTH

79%
Detections were Hands-on-Keyboard

CURLY SPIDER

attack in under 4 minutes

INITIAL ACCESS

Network

Help desk imposter tricks user into installing a remote access tool and connecting to adversary's cloud infrastructure

3m 43s

EXECUTION

Endpoint

Uses curl to download malicious scripts and runs scripts to set registry keys

PERSISTENCE

Endpoint

Creates a backdoor user and executes final payload

0m 06s

DEFENSE EVASION

Endpoint

Removes forensics artifacts to erase traces of intrusion

0m 06s

<4

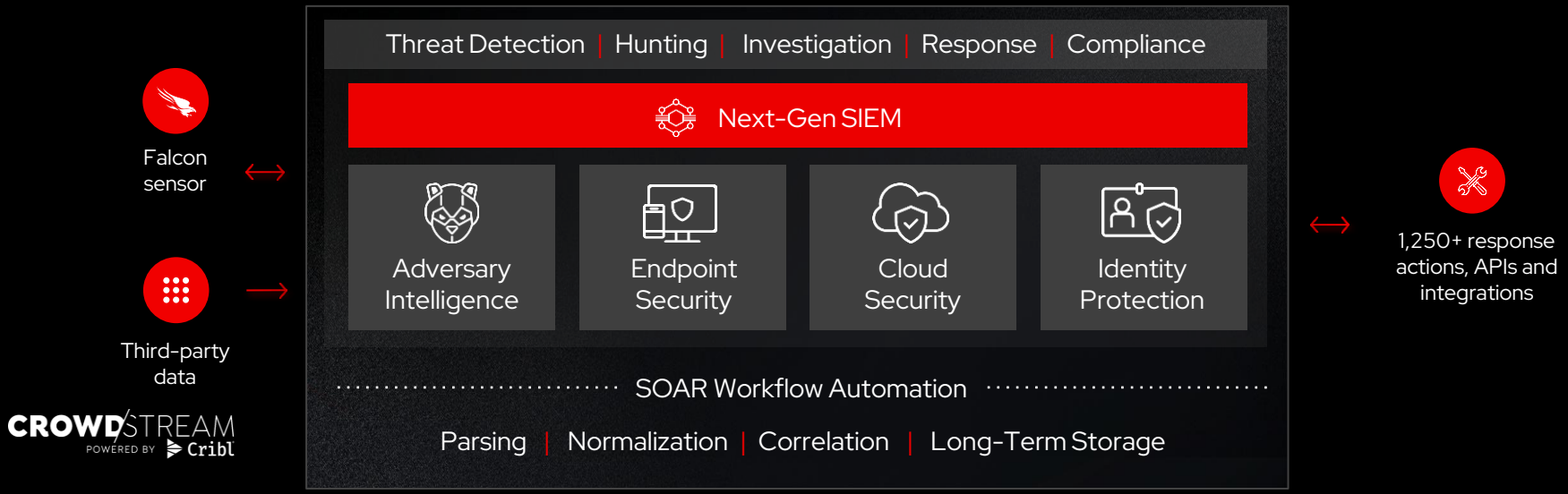
minute to conduct attack and establish back door

Source: CrowdStrike 2025 Global Threat Report

CROWDSTRIKE

Legacy SIEMs give adversaries the advantage.

Transform your SOC with Falcon Next-Gen SIEM



Stop breaches
with the world's best prevention, detection, intelligence and AI

Reduce response time
with blazing-fast search and workflow automation

Cut costs up to 80%
by unifying SecOps on one platform with one console[1]

1. These numbers are projected estimates of average benefit based on recorded metrics provided by customers during pre-sale motions

CROWDSTRIKE

Cribl

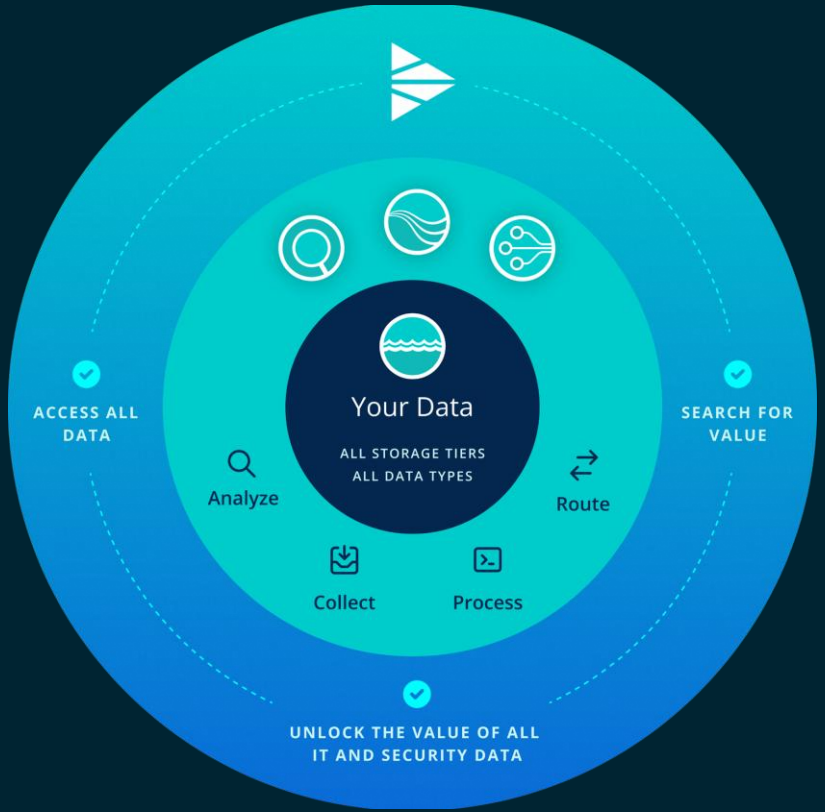
IN DATA SPERAMUS

The Data Management Dilemma

Dominika Kanczik

September 2025

Who we are.



Technology Innovator

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

Hyper Growth Company

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

Solid Financials

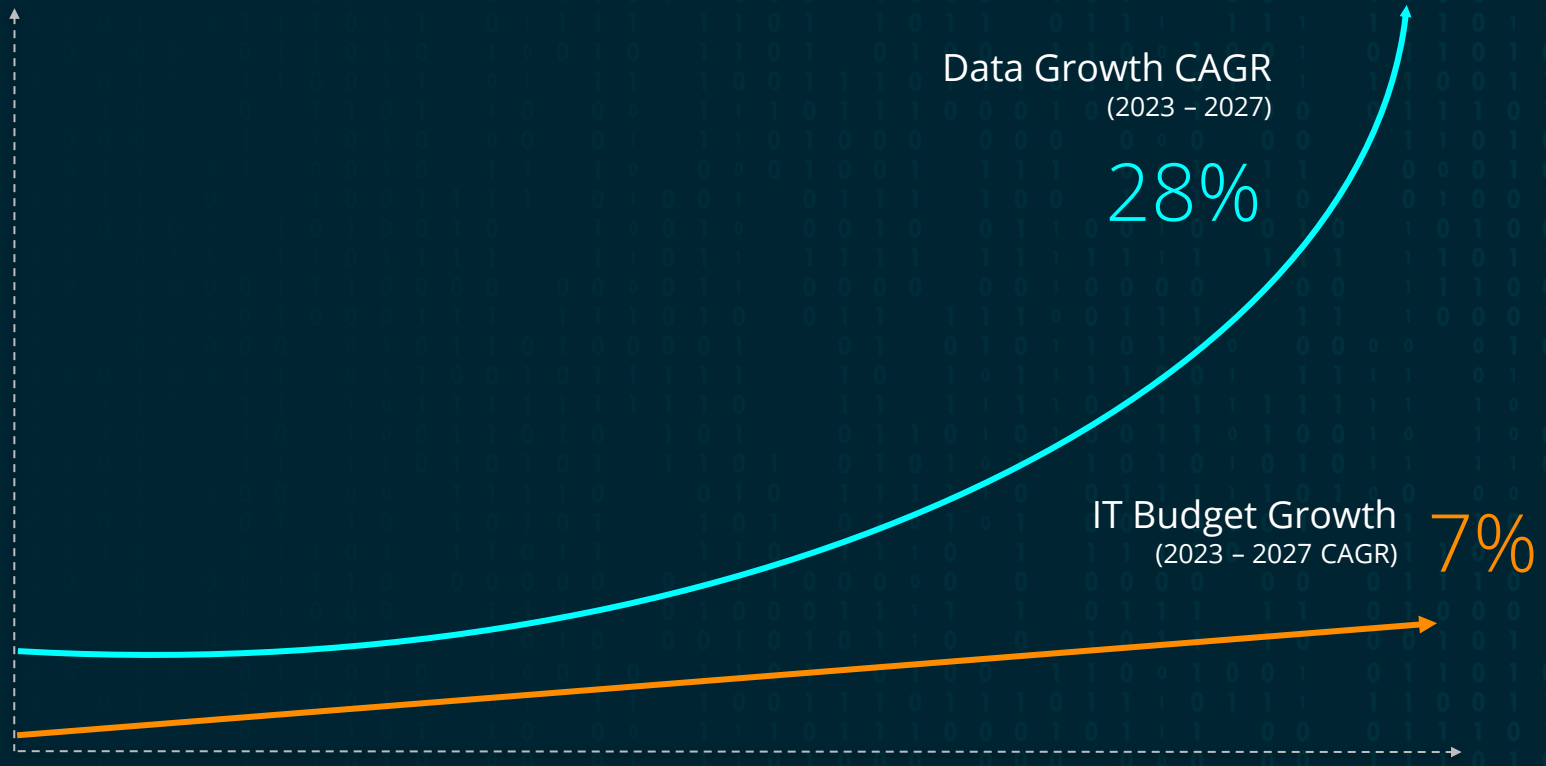
- 4th fastest $1M to $100MM ARR in Silicon Valley*
- $600M+ in funding

The Data Challenge

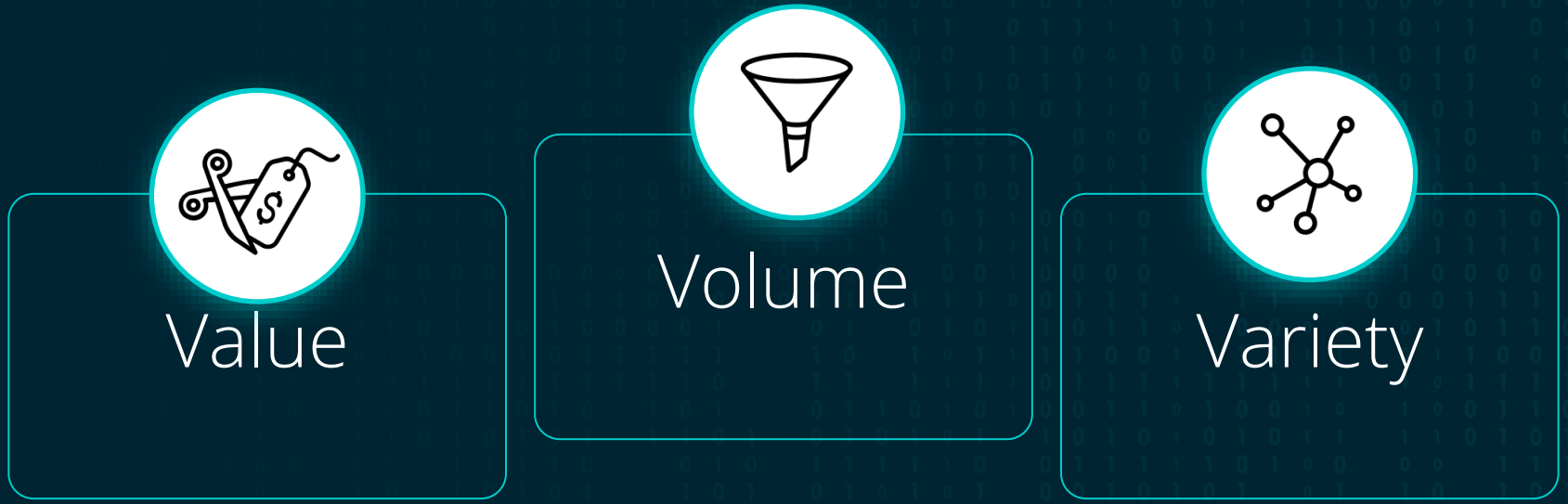
IN DATA SPERAMUS

Cribl

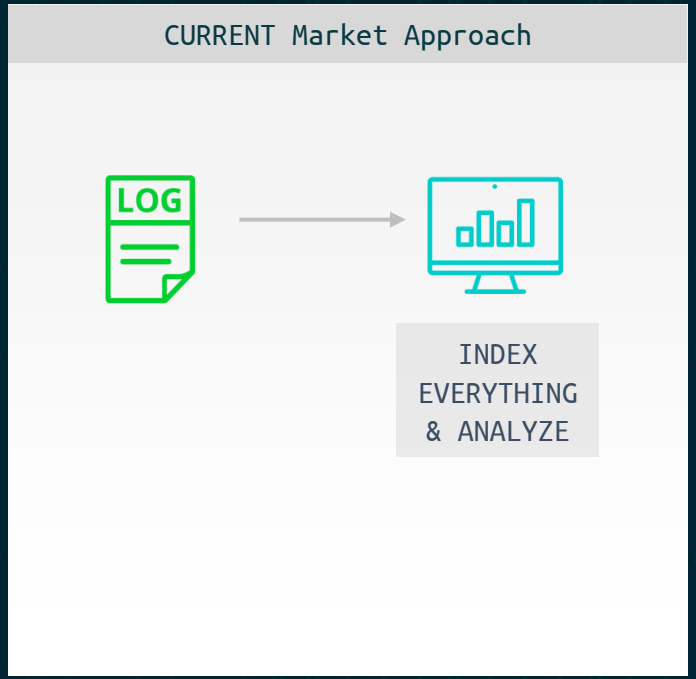
IT & Security face a tidal wave of diverse data



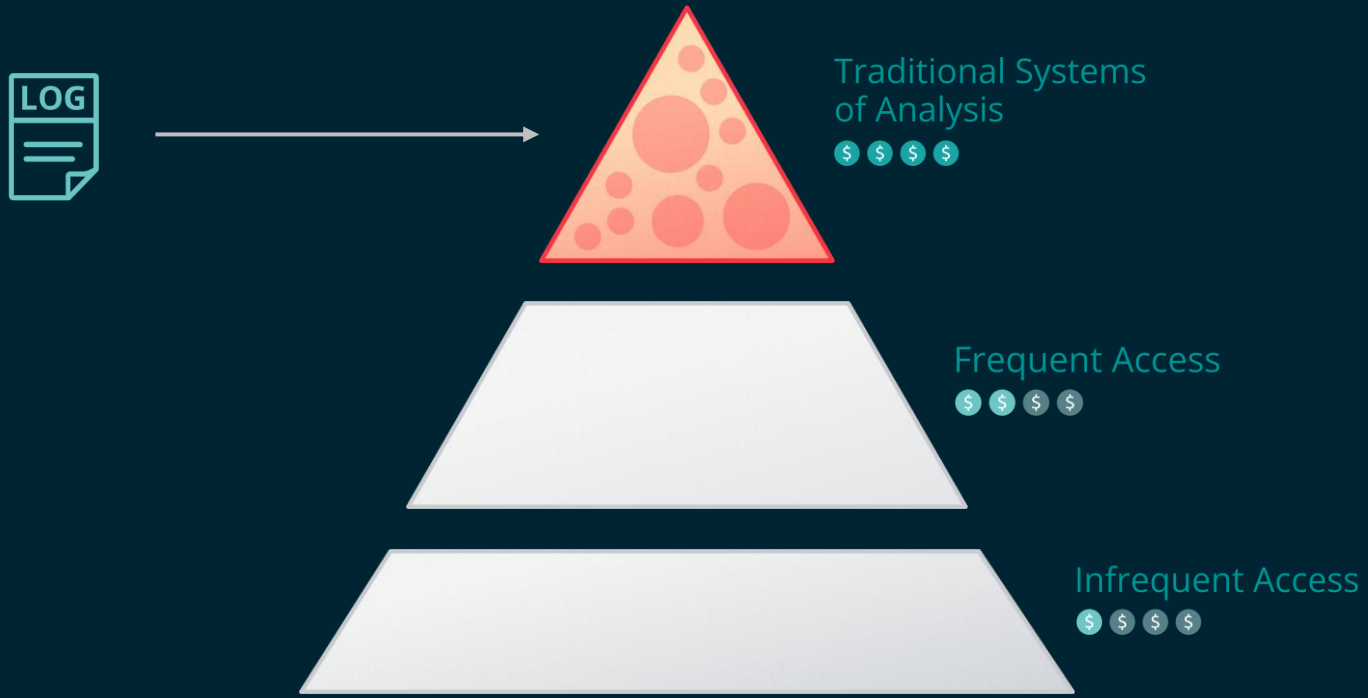
And that data is **different…**



What got you to 2025 won't get you to **2035**



Same cost for all workloads?



Recent Gartner survey shows 11% of organizations use their SIEM just for storage.

Gartner - April 2025

KEY FINDINGS

- The growing volume of logs increasing the financial pressure on IT
- Log data is often distributed without a centralization strategy - such as a telemetry pipelines - analysis is inefficient
- Organisations struggle that the right data is available to the right actors at the right time

RECOMMENDATIONS

- Maximize the value of log data by implementing a telemetry pipeline architecture to enrich, transform and normalize logs and regulate the flow of logs to analysis systems. This also reduces operational overhead.
- Increase cost and data efficiency by managing the content location and retention of log telemetry

Source: **Gartner Market Guide for Log Monitoring and Analysis Solutions**
https://www.gartner.com/en/documents/6337479

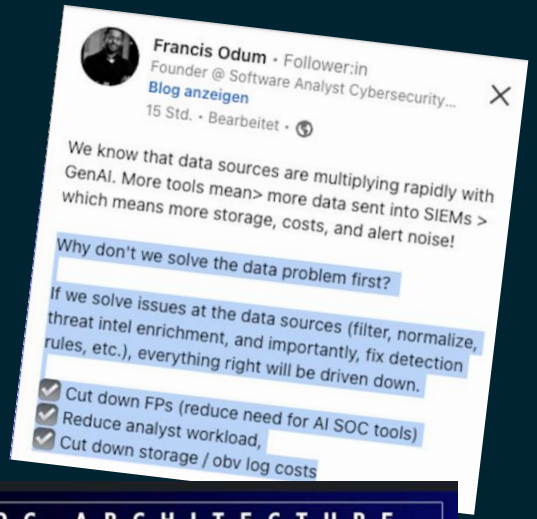
Voices of the Market …

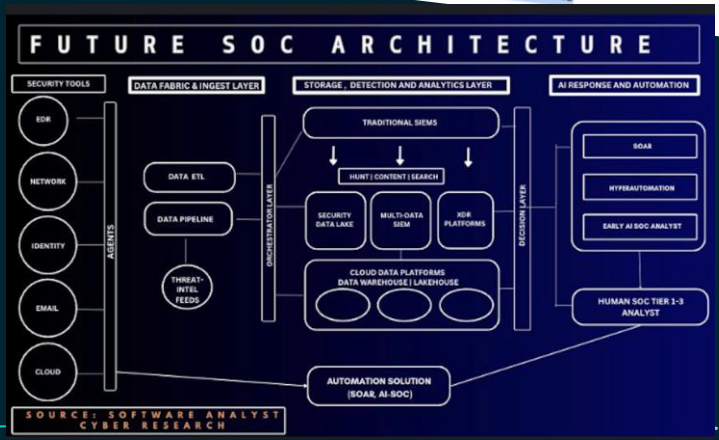
FORRESTER®

If You're Not Using Data Pipeline Management For Security And IT, You Need To

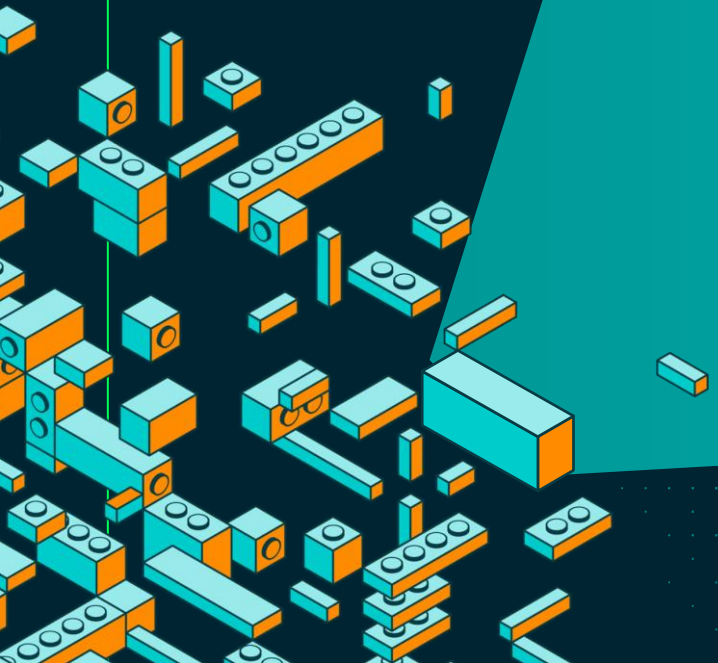
Gartner

Innovation Insight: Telemetry Pipelines Elevate the Handling of Operational Data





New Data Lifecycle Management Approach Needed!



Wait, what? Why? How?

Data Management Modernization Is a Journey

Cribl

Lifecycle of **Data Management**




Discovery

Discover
Collect
Forward
Monitor

Processing

Shape
Transform
Route
Replay

Storing

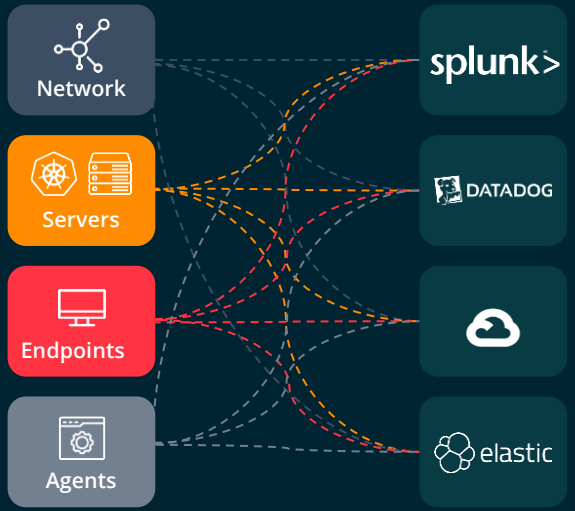
Store
Access
Optimize
Manage

Exploring

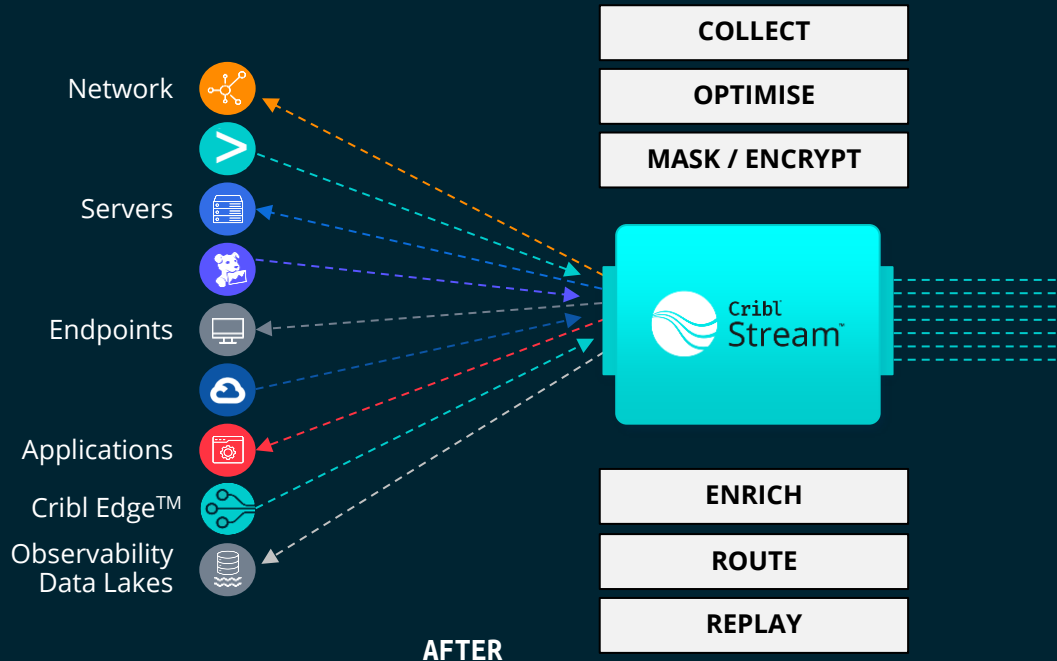
Explore
Query
Visualize
Alert

Step1 to **Modern Data Management**

From scattered agents, forwarders, and servers to streamlined collection



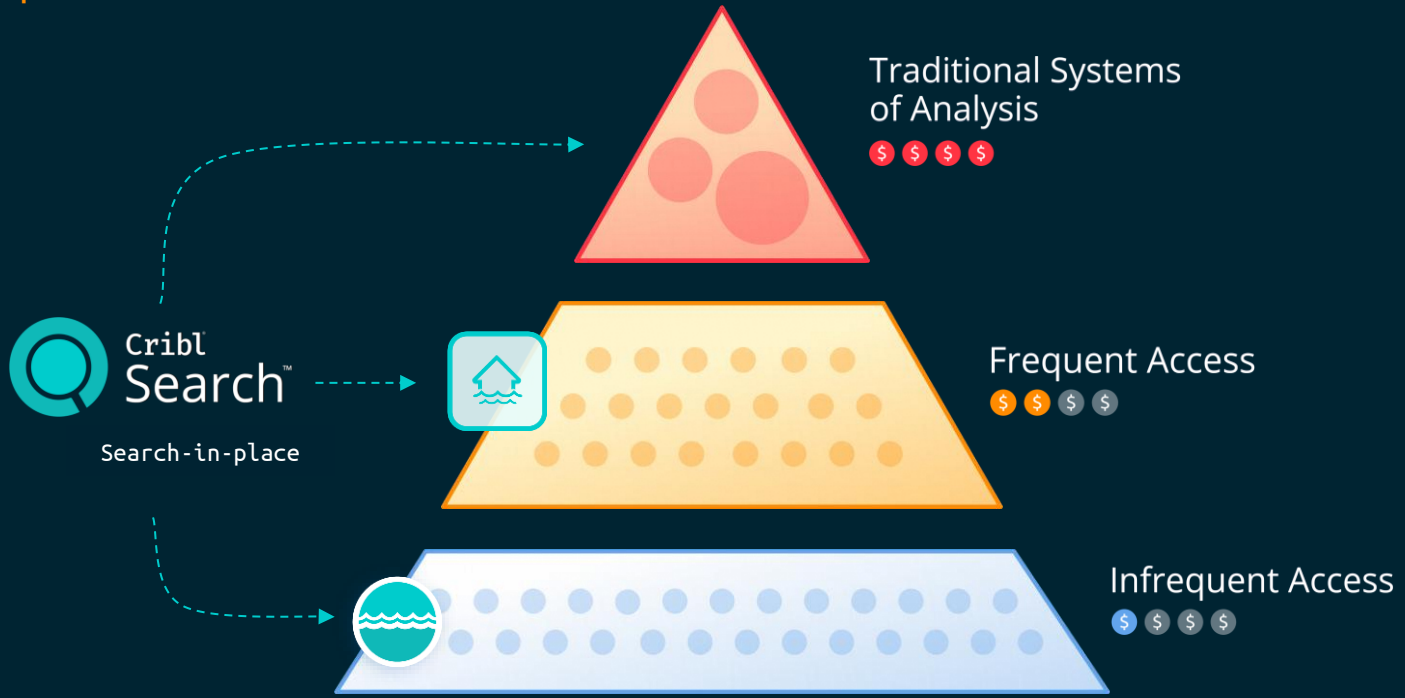
BEFORE



AFTER

Step2: **Tiered Data Management**

Cost-optimized workloads

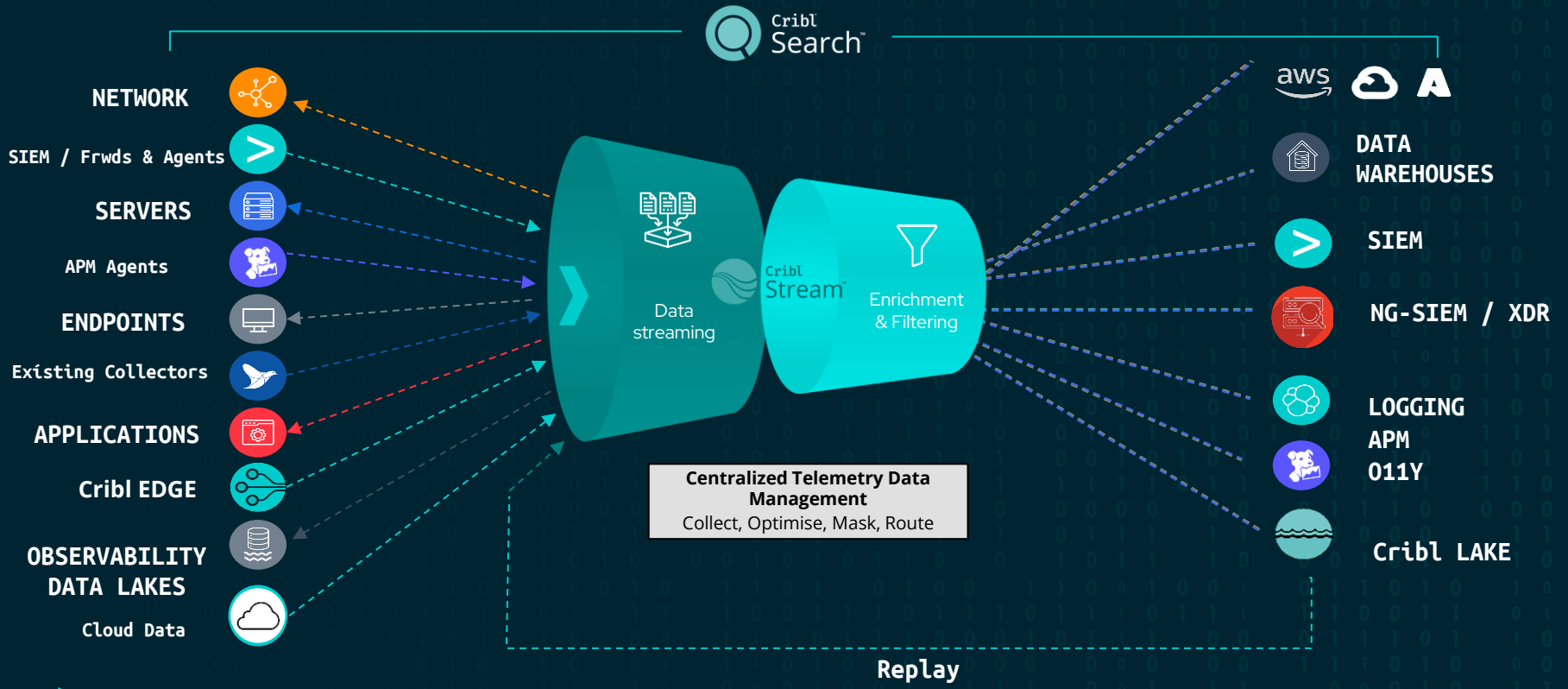


Cribl

The Data Engine for IT & Security

Cribl Approach to **Data Management**

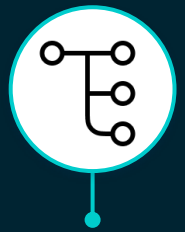
Easily onboard and route data to multiple destinations & be vendor agnostic



Re-thinking data strategy

What got you to 2025 **won't** get you to 2035

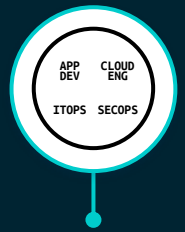
Control data
in motion centrally



Consolidate
telemetry collection

Implement tiered
data storage

Optimize full fidelity
data analysis



Distribute, isolate,
and optimize data
processing

Thank you