



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

CRIMINAL

ALCHEMIST SPIDER
ALPHA SPIDER
AVIATOR SPIDER
BITWISE SPIDER
BLIND SPIDER
BLOCKADE SPIDER
BRAIN SPIDER
BRASH SPIDER
BUTLER SPIDER
CARBON SPIDER
CHARIOT SPIDER
CHAOTIC SPIDER
CHATTY SPIDER
CHEF SPIDER
CLOCKWORK SPIDER
CURLY SPIDER
DEMON SPIDER
DONUT SPIDER
FROZEN SPIDER
GRACEFUL SPIDER
HAZARD SPIDER
HERMIT SPIDER
HIVE SPIDER
HOLIDAY SPIDER
HONEY SPIDER
HOOK SPIDER
IMPOSTER SPIDER
INDRIK SPIDER
KNOCKOUT SPIDER
LIGHTNING SPIDER
LILY SPIDER
LUNAR SPIDER
MALLARD SPIDER
MANGLED SPIDER
MASKED SPIDER
MONARCH SPIDER
MUMMY SPIDER
MUTANT SPIDER

NARWHAL SPIDER
NIMRO SPIDER
NITRO SPIDER
OCULAR SPIDER
ODYSSEY SPIDER
OUTBREAK SPIDER
PERCUSSION SPIDER
PROPHET SPIDER
PLUMP SPIDER
PUNK SPIDER
QUANTUM SPIDER
RADIANT SPIDER
RECESS SPIDER
RENAISSANCE SPIDER
RICE SPIDER
ROYAL SPIDER
SALTY SPIDER
SAMBA SPIDER
SCATTERED SPIDER
SCULLY SPIDER
SCION SPIDER
SHINING SPIDER
SINFUL SPIDER
SLIPPIY SPIDER
SLY SPIDER
SMOKY SPIDER
SOLAR SPIDER
SPRITE SPIDER
TRAVELING SPIDER
TUNNEL SPIDER
VAMPIRE SPIDER
VENOM SPIDER
VETO SPIDER
WANDERING SPIDER
WIZARD SPIDER
VICE SPIDER

NORTH KOREA

LABYRINTH CHOLLIMA
FAMOUS CHOLLIMA
RICOCHET CHOLLIMA
SILENT CHOLLIMA
STARDUST CHOLLIMA
VELVET CHOLLIMA

CHINA

ABSTRACT PANDA
AQUATIC PANDA
CASCADE PANDA
CAULDRON PANDA
EMISSARY PANDA
ENVOY PANDA
ETHEREAL PANDA
GENESIS PANDA
GLACIAL PANDA
JACKPOT PANDA
HORDE PANDA
KARMA PANDA
KRYPTONITE PANDA
LIMINAL PANDA
LOCKSMITH PANDA
LOTUS PANDA
MURKY PANDA
MUSTANG PANDA
OPERATOR PANDA
OVERCAST PANDA
PHANTOM PANDA
PIRATE PANDA
PUZZLE PANDA
SHATTERED PANDA
SUNRISE PANDA
TREASURE PANDA
VANGUARD PANDA
VAULT PANDA
VIXEN PANDA
WICKED PANDA

INDIA

FABLE TIGER
HAZY TIGER
OUTRIDER TIGER
QUILTED TIGER
RAZOR TIGER
VICEROY TIGER

EGYPT

WATCHFUL SPHINX

VIETNAM

OCEAN BUFFALO

SOUTH KOREA

SHADOW CRANE

SYRIA

DEADEYE HAWK

KAZAKHSTAN

COMRADE SAIGA

PAKISTAN

MYTHIC LEOPARD
FRINGE LEOPARD

COLOMBIA

GALACTIC OCELOT

TURKEY

COSMIC WOLF

IRAN

BANISHED KITTEN
CHARMING KITTEN
CHRONO KITTEN
HAYWIRE KITTEN
IMPERIAL KITTEN
NEMESIS KITTEN
PIONEER KITTEN
REFINED KITTEN
SPECTRAL KITTEN
STATIC KITTEN
TRACER KITTEN
VENGEFUL KITTEN

RUSSIA

BERSERK BEAR
COZY BEAR
EMBER BEAR
FANCY BEAR
GOSSAMER BEAR
PRIMITIVE BEAR
VENOMOUS BEAR
VOODOO BEAR

HACKTIVIST

BOUNTY JACKAL
CURIOUS JACKAL
CRUEL JACKAL
FRONTLINE JACKAL
INCENDIARY JACKAL
INTREPID JACKAL
PARTISAN JACKAL
REGAL JACKAL
RENEGADE JACKAL
SPOILED JACKAL



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

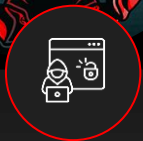
79%

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

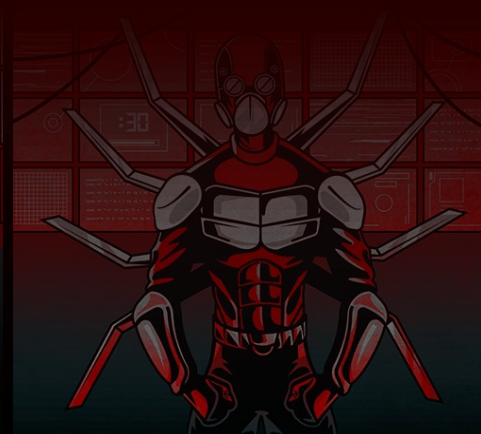
0m 06s

<4

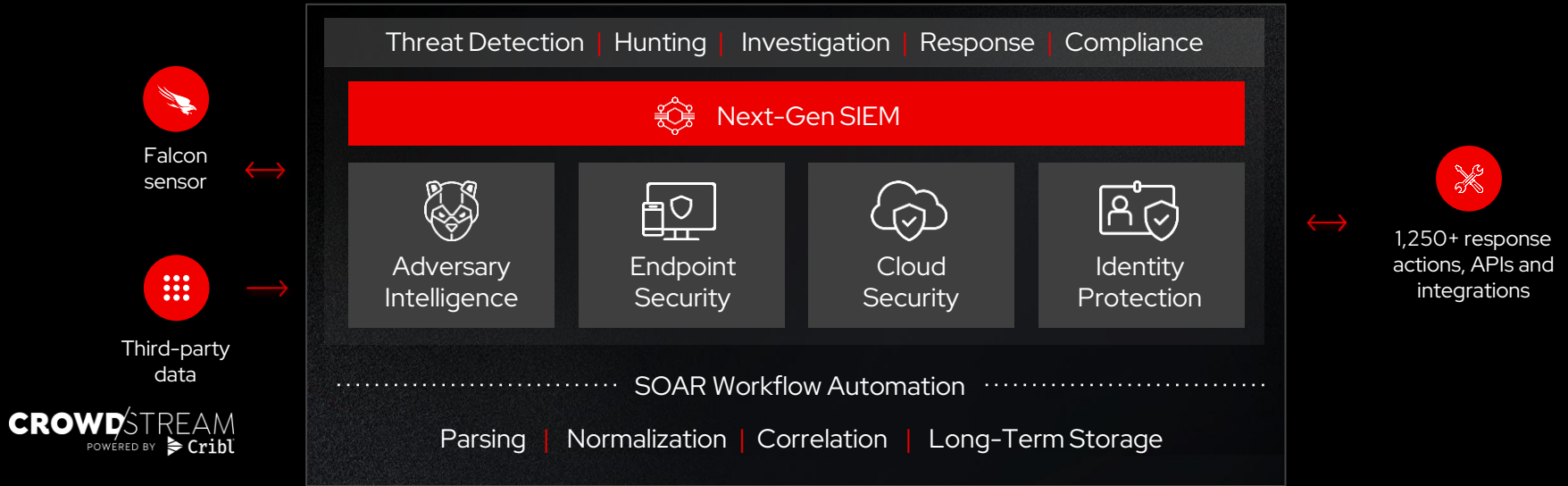
minute to conduct attack and establish back door



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 console¹

1. These numbers are projected estimates of average benefit based on recorded metrics provided by customers during pre-sale motions
© CrowdStrike, Inc. All Rights Reserved



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

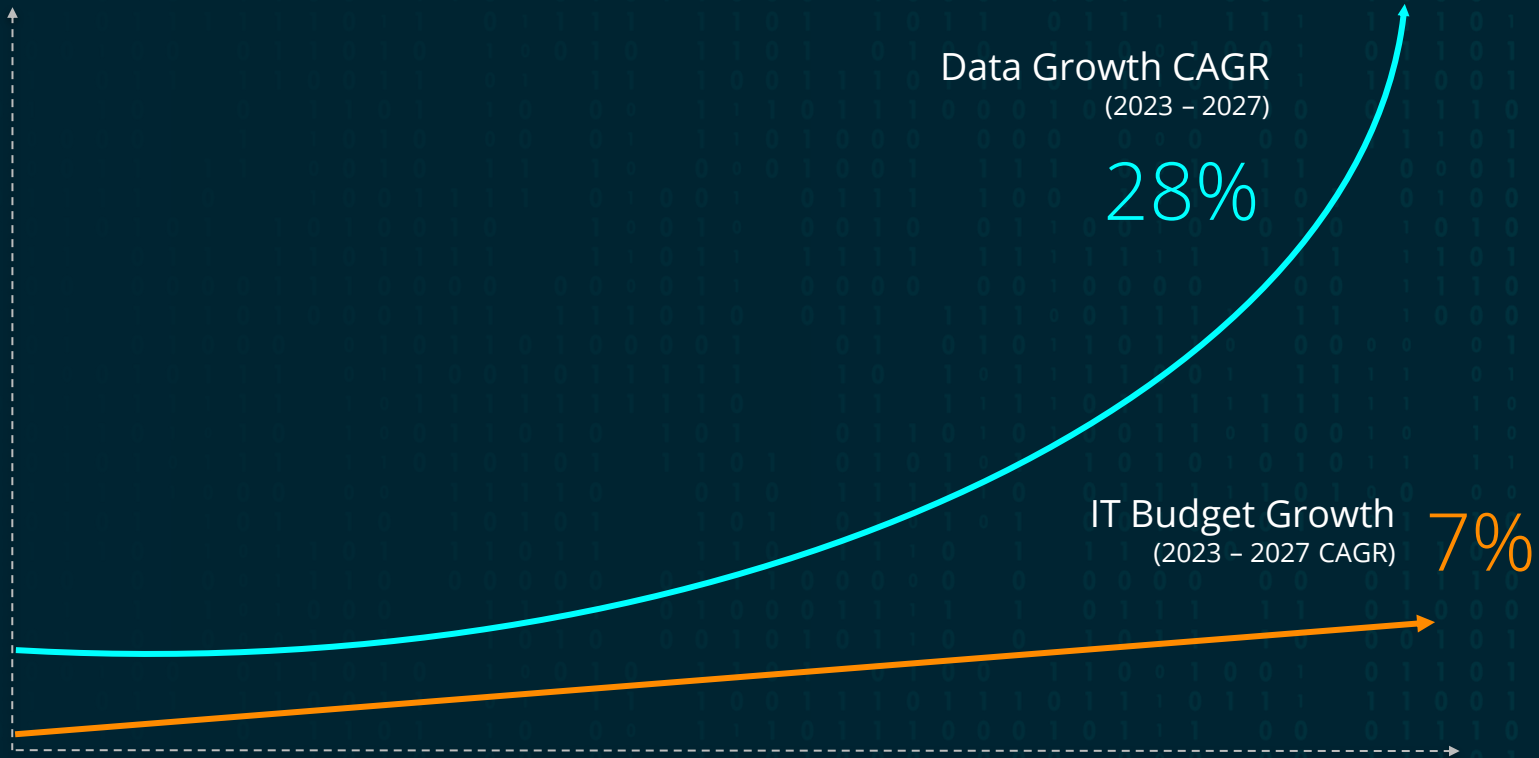
- 4th fastest \$1M to \$100MM ARR in Silicon Valley*
- \$600M+ in funding

The Data Challenge

IN DATA SPERAMUS



IT & Security face a tidal wave of diverse data



And that data is **different...**



Value

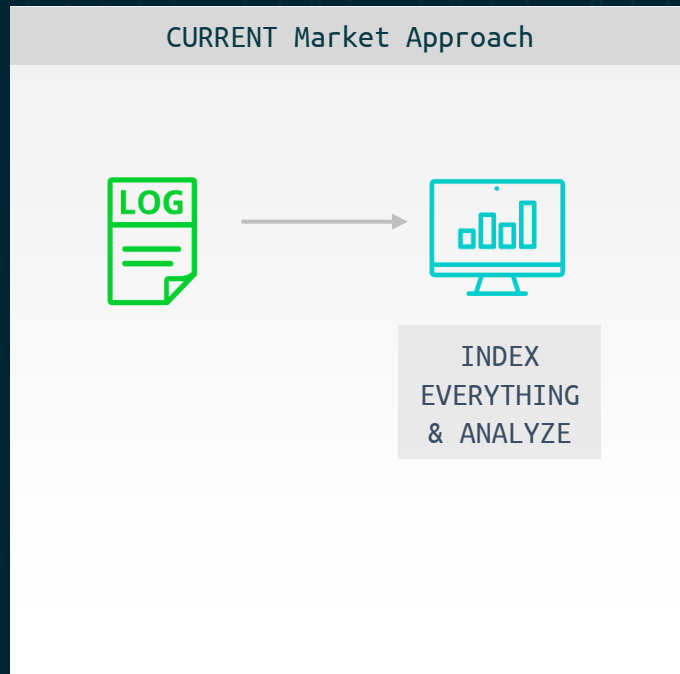


Volume

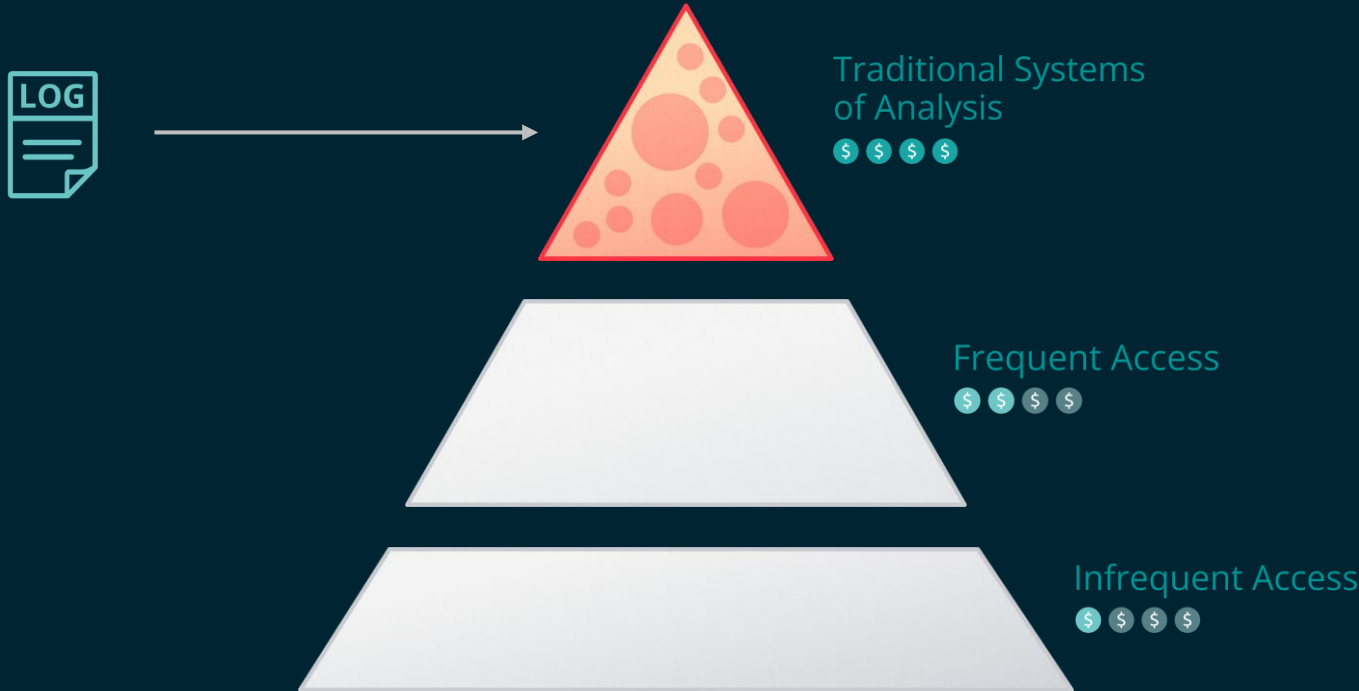


Variety

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 ...



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

Francis Odum · Follower · in
Founder @ Software Analyst Cybersecurity...
[Blog anzeigen](#)
15 Std. · Bearbeitet ·

We know that data sources are multiplying rapidly with GenAI. More tools mean > more data sent into SIEMs > which means more storage, costs, and alert noise!

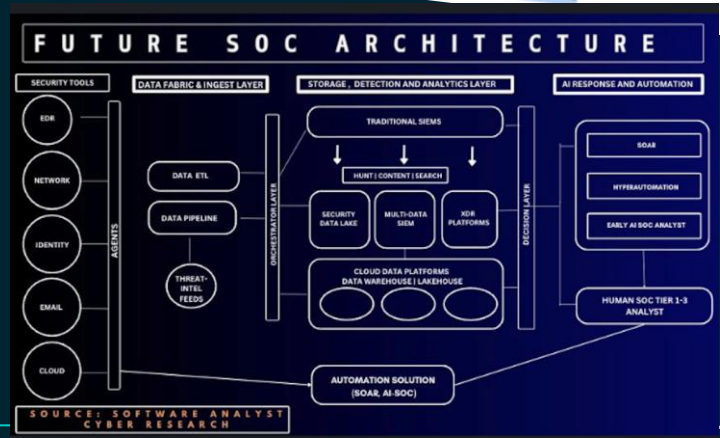
Why don't we solve the data problem first?

If we solve issues at the data sources (filter, normalize, threat intel enrichment, and importantly, fix detection rules, etc.), everything right will be driven down.

- ✓ Cut down FPs (reduce need for AI SOC tools)
- ✓ Reduce analyst workload,
- ✓ Cut down storage / obv log costs

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



Lifecycle of **Data Management**



Discovery



Discover
Collect
Forward
Monitor



Processing



Shape
Transform
Route
Replay



Storing



Store
Access
Optimize
Manage



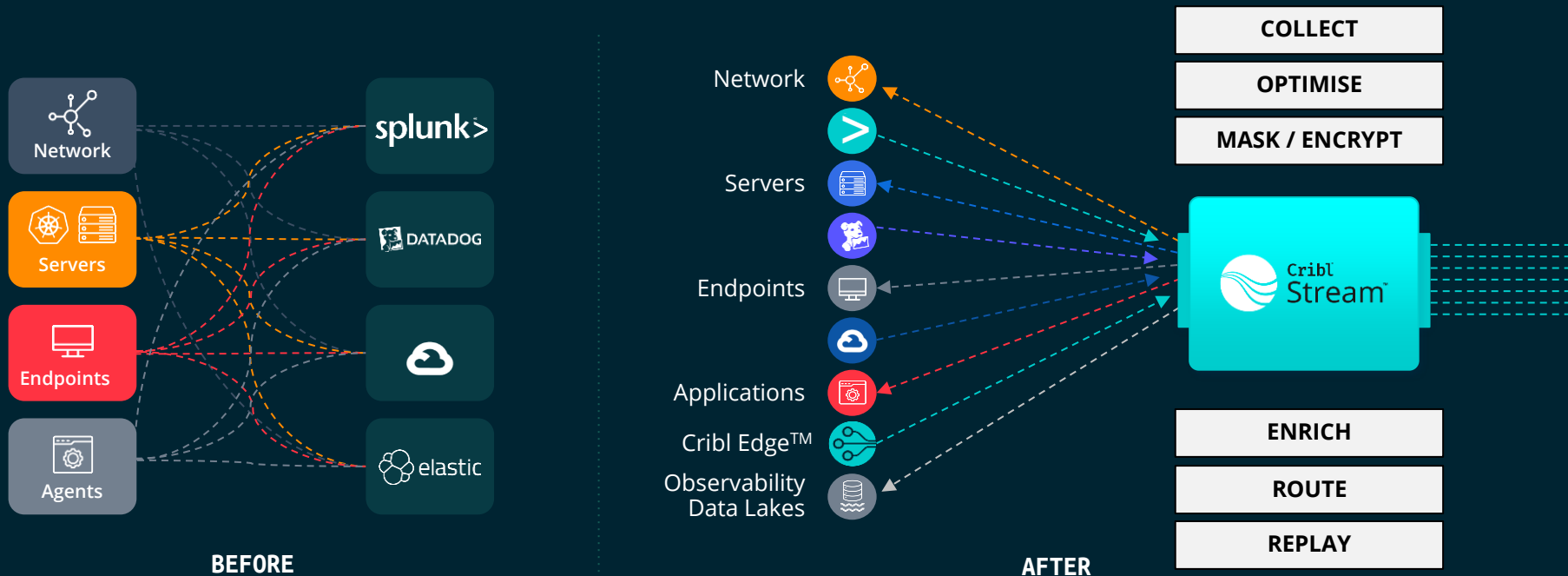
Exploring



Explore
Query
Visualize
Alert

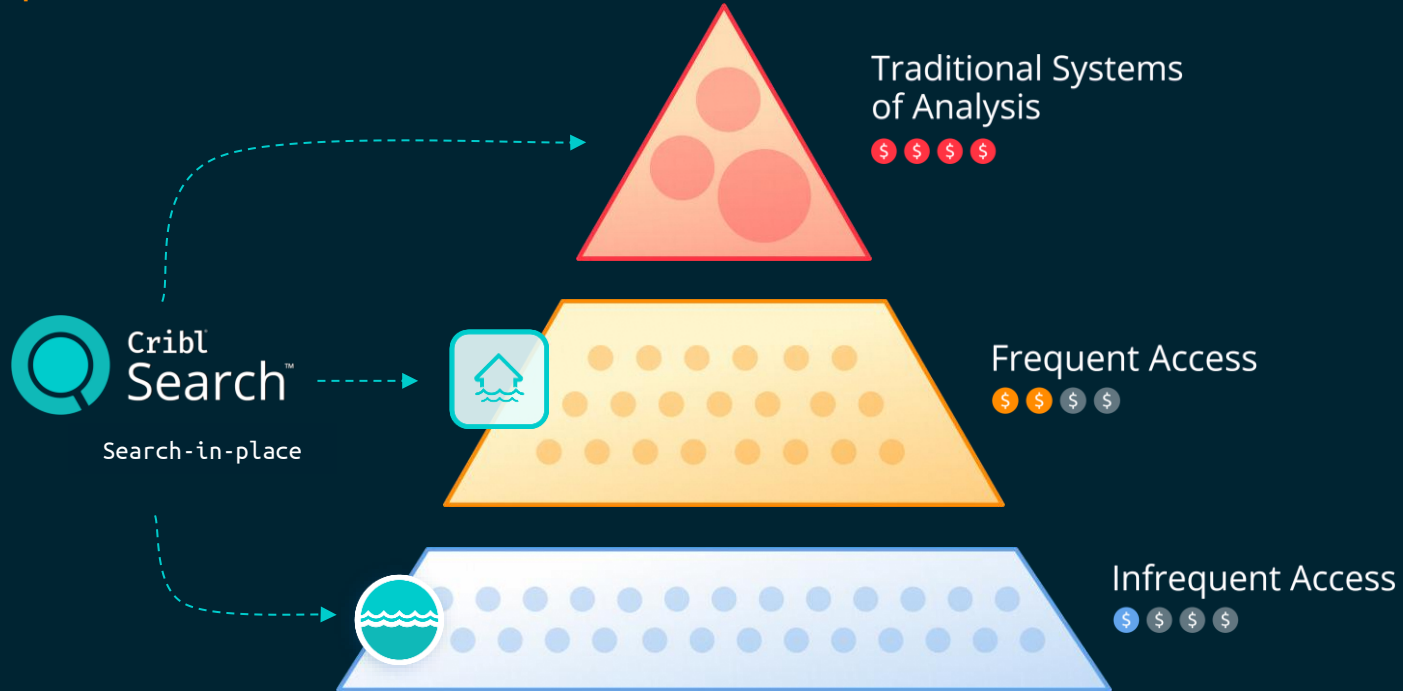
Step 1 to Modern Data Management

From scattered agents, forwarders, and servers to streamlined collection



Step2: Tiered Data Management

Cost-optimized workloads



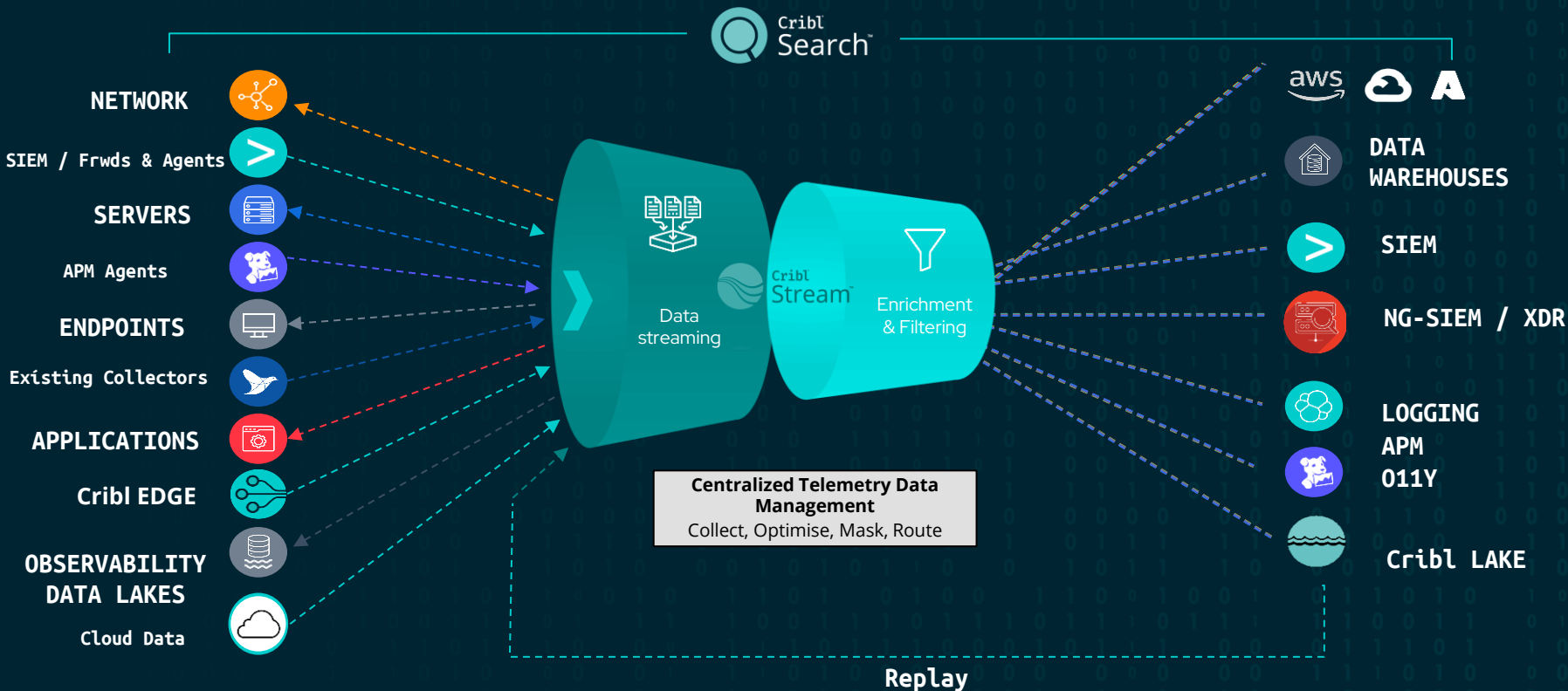


The Data Engine for IT & Security



Cribl Approach to Data Management

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

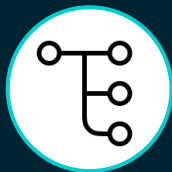


Re-thinking data strategy

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



Control data
in motion centrally



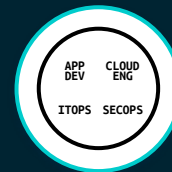
Consolidate
telemetry collection



Implement tiered
data storage



Optimize full fidelity
data analysis



Distribute, isolate,
and optimize data
processing





Thank you

