

# Apache Doris 与 Elasticsearch 在实时分析场景下的深度对比

肖康

Apache Doris PMC 成员

# 目录

01 为什么对比两者

02 深度对比

03 典型案例

01

# 为什么对比两者

# 为什么对比两者

## Doris 实时数仓

- 运维领域：可观测性
- 安全领域：安全分析
- 业务领域：在线报表、用户画像、湖仓一体

## Elasticsearch 搜索引擎

- 运维领域：可观测性
- 安全领域：安全分析
- 业务领域：搜索与分析

相似的应用场景：实时分析



02

# 深度对比两者

# 从用户角度多维度深入对比

## 1 开源开放

对用户的开放性和使用约束

## 2 系统架构

可选的部署形态和依赖要求

## 3 实时写入

数据写入的方式和性能

## 4 实时存储

数据存储的功能和性能

## 5 实时查询

查询的功能和性能

# 1 开源开放

## Apache Doris

### 一直是 Apache 2.0 License

- 开放
- 商业友好
- 长期持续

### 项目运营

- Apache 开源软件基金会

## Elasticsearch

### 多次变更 License

- Apache License 2.0
- Elastic License
- AGPL License

### 项目运营

- Elastic 公司



## 2 系统架构

### Apache Doris

#### 支持3种部署模式

- On-Premise
- Cloud SaaS
- Cloud BYOC

### Elasticsearch

#### 支持2种部署模式

- On-Premise
- Cloud SaaS



## 2 系统架构

### Apache Doris

支持存算一体和存算分离，多种弹性

- 计算-计算分离：workload group
- 存储-存储分离：冷热分层
- 存储-计算分离：存算分离

### Elasticsearch

仅支持存算一体，有限弹性

- 计算-计算分离：thread group
- 存储-存储分离：冷热分层
- 存储-计算分离：不支持

### 3 实时写入

#### Apache Doris

支持实时写入与更新，吞吐高

- 写入**吞吐高**：多副本一次索引，向量化
- 支持 Push: HTTP REST / MySQL
- **支持 Pull**: Kafka, CDC

#### Elasticsearch

支持实时写入与更新，吞吐低

- 写入**吞吐低**：多副本多次索引
- 支持 Push: HTTP REST
- **不支持 Pull**：需借助 logstash 外围工具

## 4 实时存储

### Apache Doris

#### 支持3种存储模型

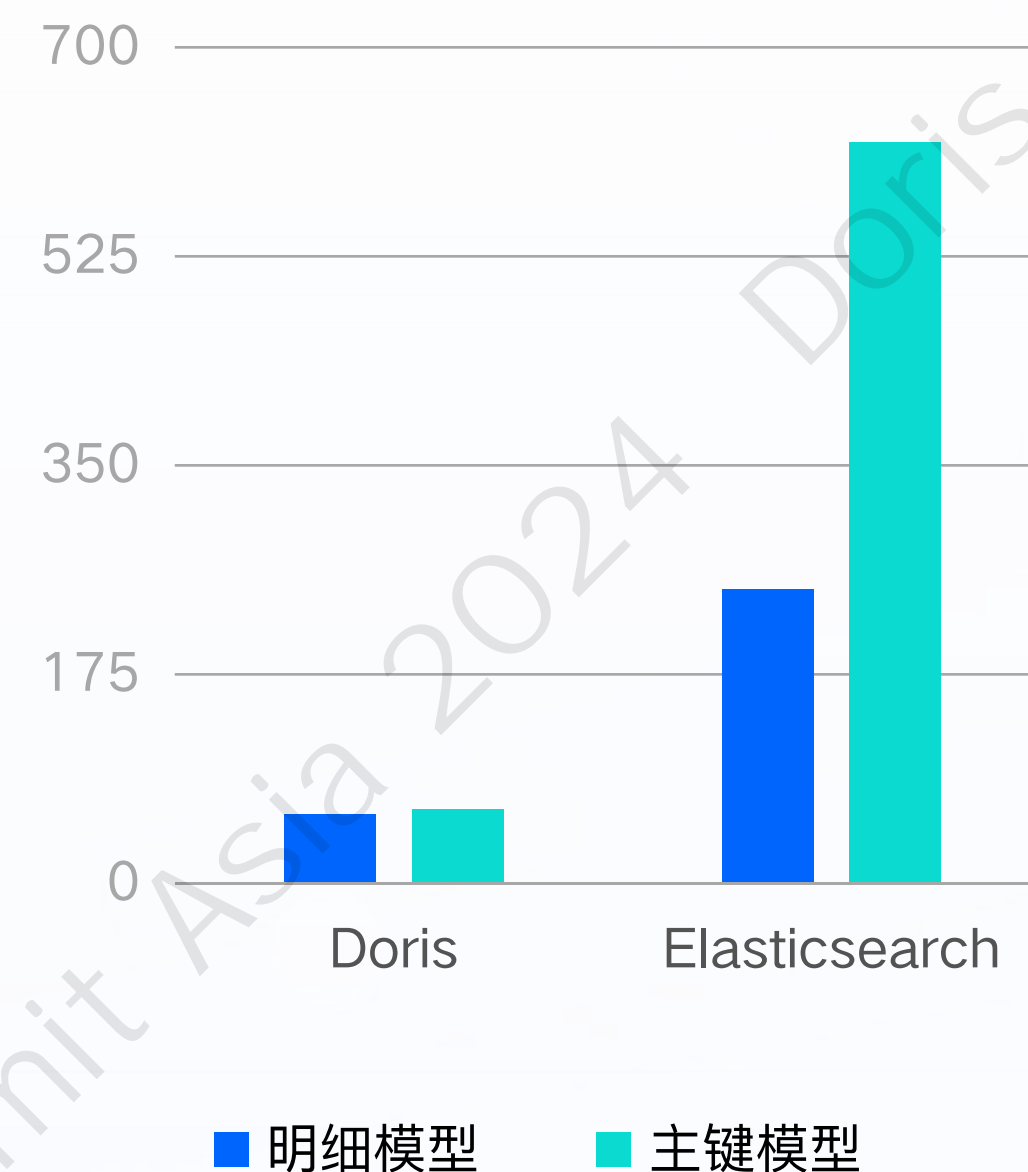
- 明细模型
- 主键模型
  - MOW 写优化 MOR 读优化两种模式
  - 主键去重写入性能**仅降低 10%**
  - 支持**多字段**联合主键
- 聚合模型

### Elasticsearch

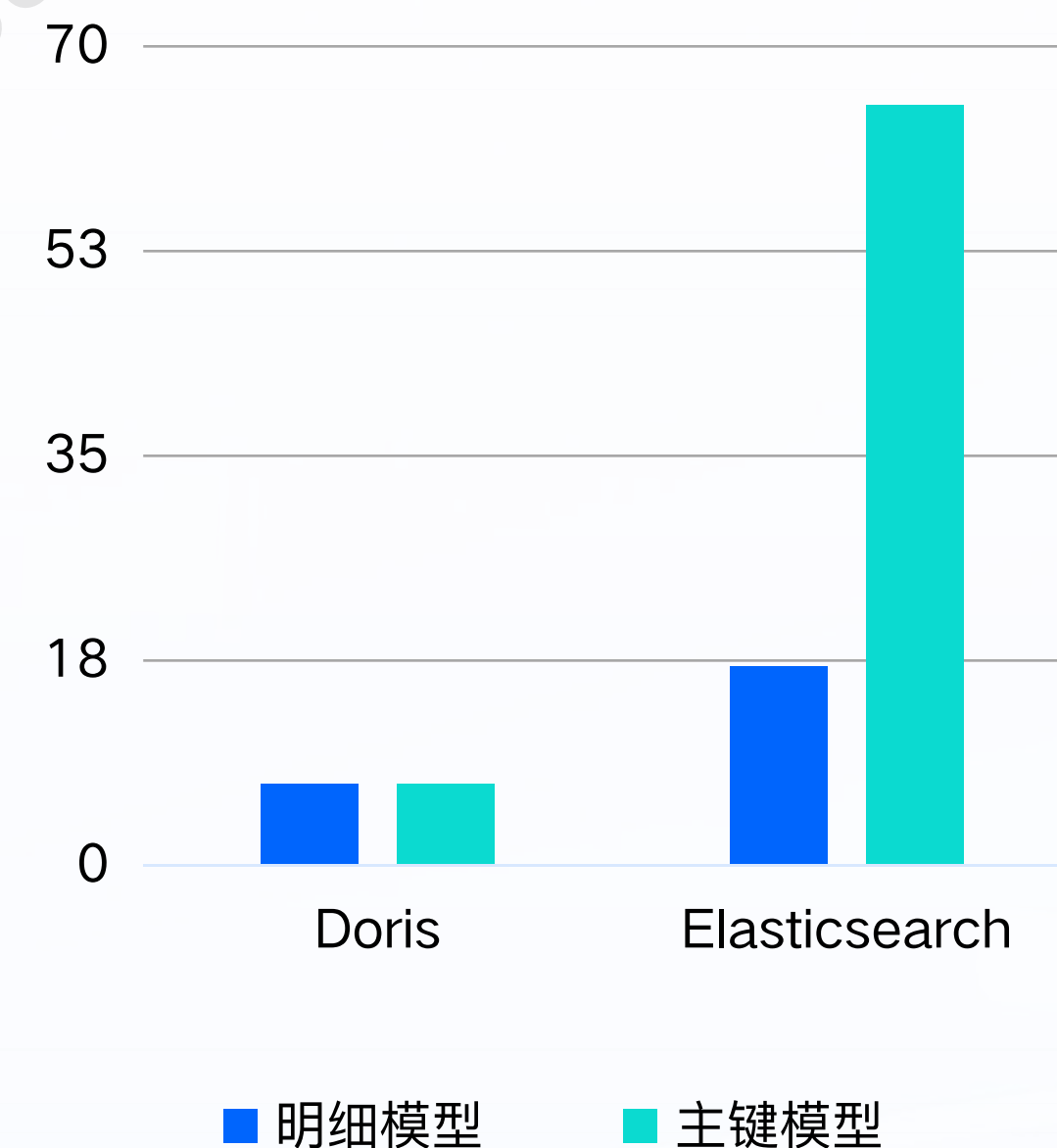
#### 支持2.5种存储模型

- 明细模型
- 主键模型
  - 仅支持 MOW 写优化模式
  - 主键去重写入性能**大幅降低3倍**
  - 主键仅支持**1个字段**，不能用于**聚合和排序**
- 聚合模型

httplogs 数据集重复导入时间对比 (单位: 秒)



tpch 100G customer 表重复导入时间对比 (单位: 秒)



## 4 实时存储

### Apache Doris

#### 支持3种存储模型

- 明细模型
- 主键模型
- 聚合模型
  - 同步**强一致**聚合
  - 支持**更新**
  - 原始 + 聚合 和 仅聚合 **两种模式**

### Elasticsearch

#### 支持2.5种存储模型

- 明细模型
- 主键模型
- 聚合模型
  - 异步**最终一致**
  - **不支持**更新
  - 聚合数据替换原始数据，**不能共存**



## 4 实时存储

### Apache Doris

#### 存储空间占用低

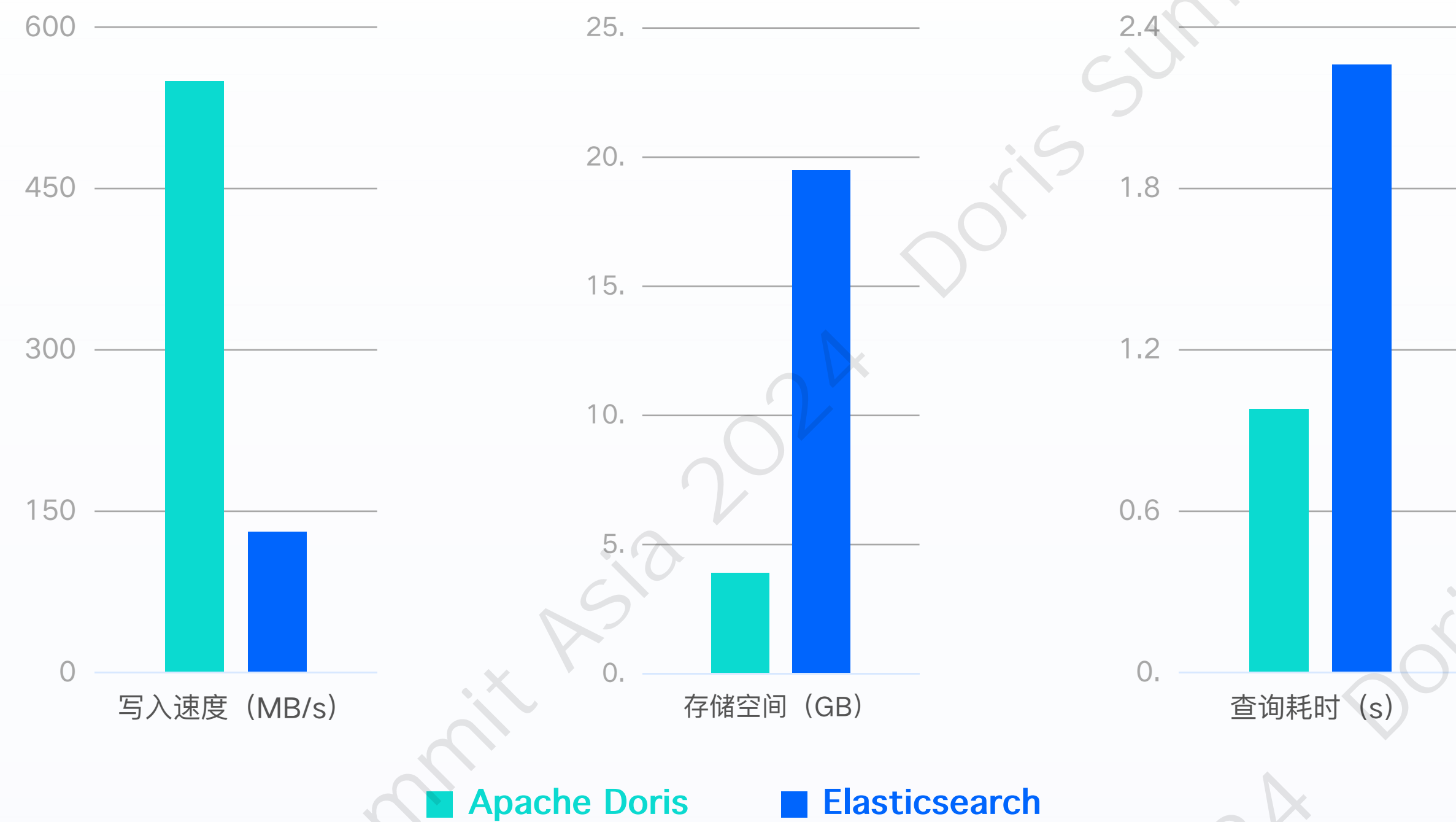
- 列存 + 简化倒排索引
- LZ4/GZ/ZSTD 压缩算法
- 整体压缩率高 1:5 ~ 1:10

### Elasticsearch

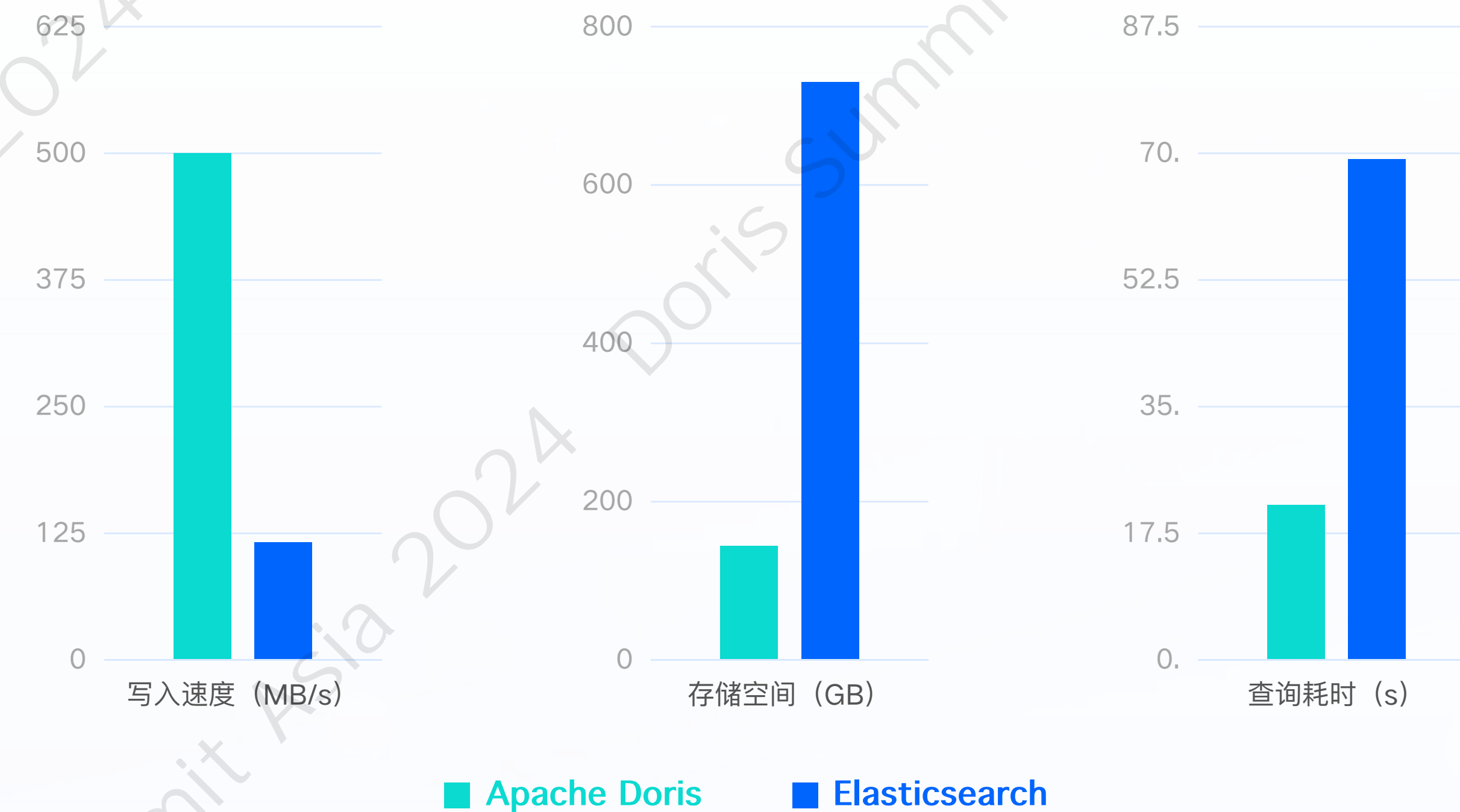
#### 存储空间占用高

- 行存 + 列存 + 倒排索引
- LZ4/GZ 压缩算法
- 整体压缩率低 1:1.5

### 3 实时存储



ES 官方 benchmark httplogs 测试集, 32GB、2.47亿条数据, 11个查询



Microsoft Azure logsbench 测试集, 1TB、40亿条数据, 10个查询

## 4 实时存储

### Apache Doris

#### 支持灵活 schema change

- 秒级动态增加字段
- 秒级动态删除字段
- 秒级动态增加索引
- 秒级动态删除索引
- 后台增量构建索引
- 秒级修改表名、字段名

### Elasticsearch

#### 支持有限 schema change

- 秒级动态添加字段
- **不支持**删除字段
- **不支持**增加索引
- **不支持**删除索引
- **不支持**增量构建索引
- **不支持**修改表名、字段名

## 5 实时查询

### Apache Doris

开放的查询接口，使用简单

- 标准的 SQL
- 开放的 MySQL 生态
- 学习门槛低，熟悉后容易盲写

### Elasticsearch

专用的查询接口，使用复杂

- 定制的 DSL
- 私有的 ES 生态
- 学习门槛高，熟悉后仍然参考手册和样例



## 5 实时查询

### Apache Doris

```
1 SELECT hour_floor(timestamp) as hour, count()  
2 FROM table1  
3 WHERE timestamp >= '1998-05-01 00:00:00'  
4 AND timestamp < '1998-05-02 00:00:00'  
5 AND message MATCH 'error'  
6 GROUP BY hour  
7 ORDER BY hour
```

### Elasticsearch

```
1 {  
2   "size": 0,  
3   "query": {  
4     "bool": {  
5       "must": [  
6         {  
7           "range": {  
8             "timestamp": {  
9               "gte": "1998-05-01 00:00:00",  
10              "lt": "1998-05-02 00:00:00"  
11            }  
12          }  
13        },  
14        {  
15          "match": {  
16            "message": "error"  
17          }  
18        }  
19      ]  
20    }  
21  },  
22  "aggs": {  
23    "by_hour": {  
24      "date_histogram": {  
25        "field": "timestamp",  
26        "calendar_interval": "hour"  
27      }  
28    }  
29  }  
30 }
```

## 5 实时查询

### Apache Doris

#### 支持 JOIN 等丰富的分析能力

- 支持完整的多表 JOIN 和优化
  - INNER / OUTER / CROSS JOIN
  - LEFT / RIGHT SEMI JOIN
  - LEFT / RIGHT ANTI JOIN
- 支持更多复杂分析能力
  - UDF, 子查询, 窗口函数, 逻辑视图, 物化视图, 湖仓一体 ...

### Elasticsearch

#### 支持搜索和聚合查询

- 不支持多表 JOIN
- 不支持更多复杂分析能力



# 5 实时查询

## Apache Doris

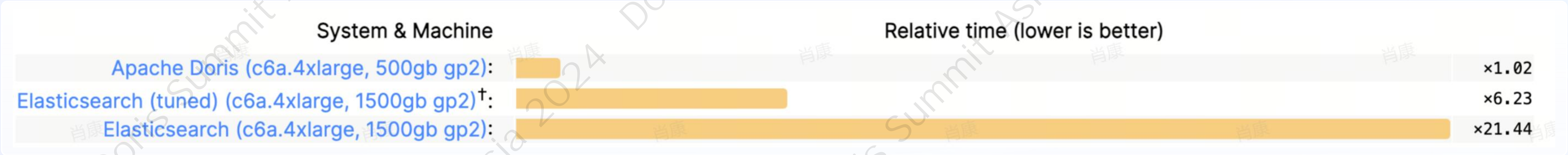
多种负载上有极速响应

- 点查性能高：行存 + 主键 + 倒排索引
- 分析性能高：列式存储、向量化、跳数索引和物化视图

## Elasticsearch

点查性能高，分析性能低

- 点查性能高：行存和倒排索引
- 分析性能低：列存和简单查询引擎



# 对比总结

## 1 开源开放

最开放的 Apache 基金会  
和 Apache License

## 2 系统架构

Run anywhere  
存算分离 + 存算一体

## 3 实时写入

写入性能提升 4倍  
支持 Push 和 Pull

## 4 实时存储

存储空间降低 70%  
更新性能提升近 10倍

## 5 实时查询

分析性能 6倍  
支持 SQL 和 JOIN



03

# 典型场景和案例



# 典型场景



## 可观测性

保障服务稳定 提升用户体验



## 网络安全

降低安全风险 提升系统安全性



## 业务分析

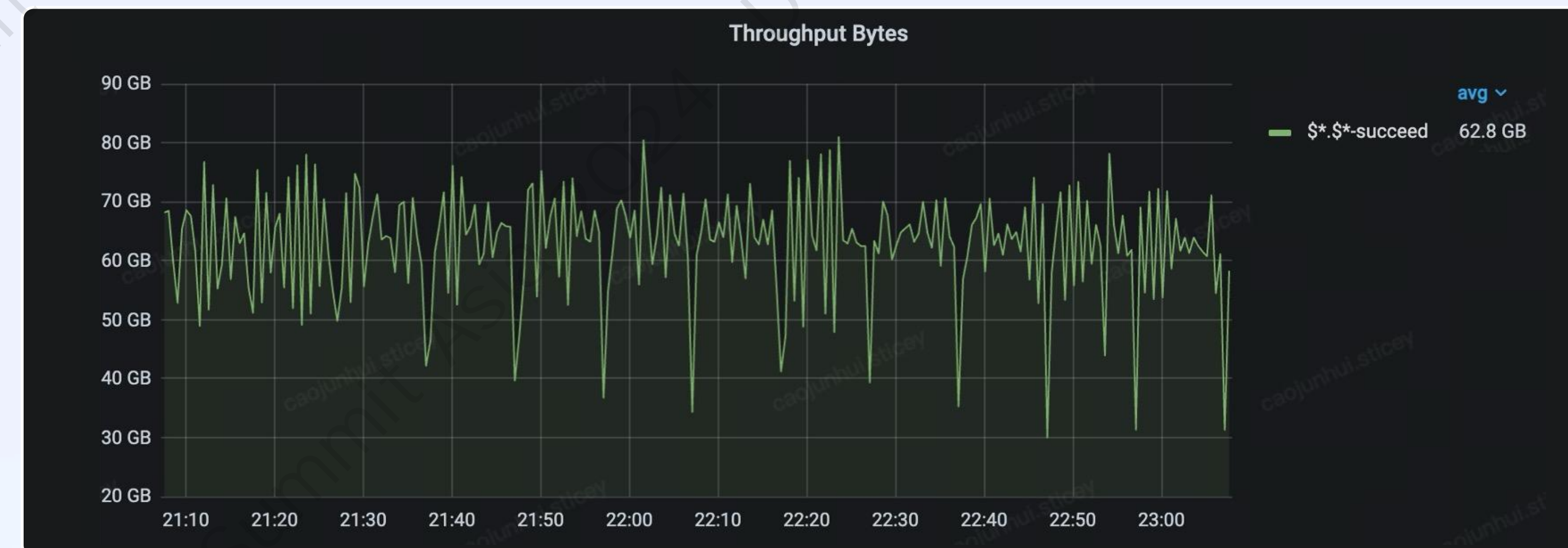
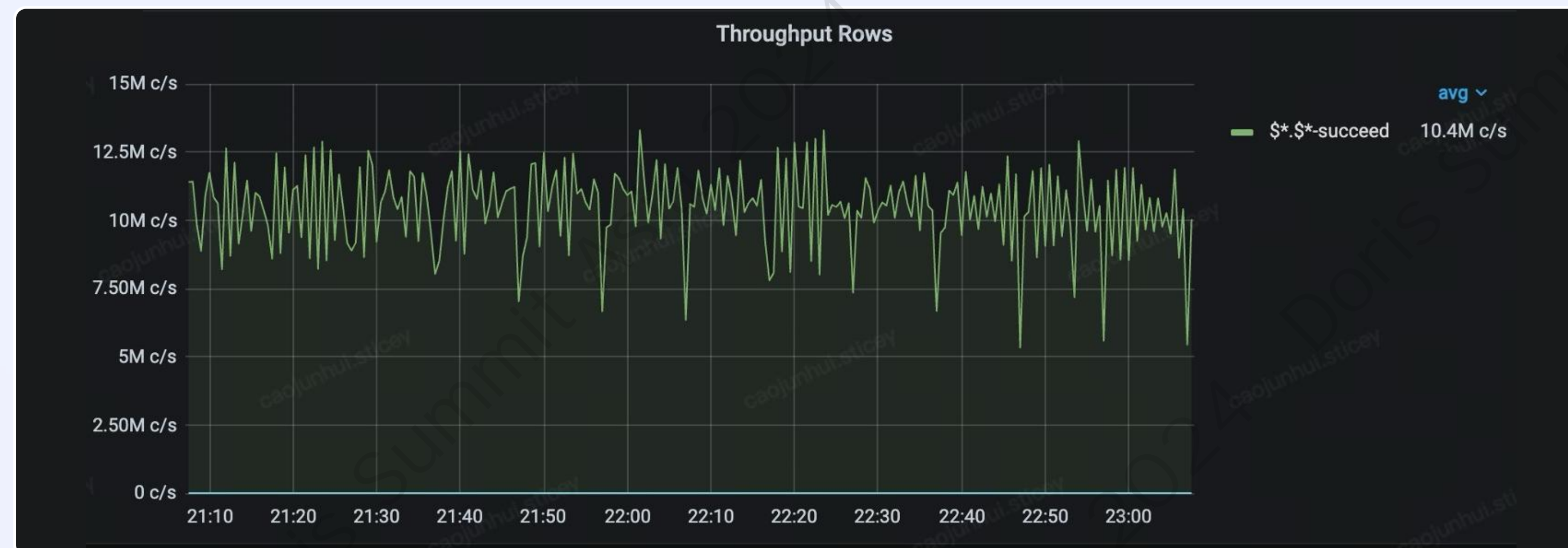
支持业务分析 加速业务增长



# 可观测性场景 — 案例1 抖音

日增数据量 **8000亿条 500TB**，写入均值 1000w/s 60GB/s，峰值 **3000w/s 90GB/s**

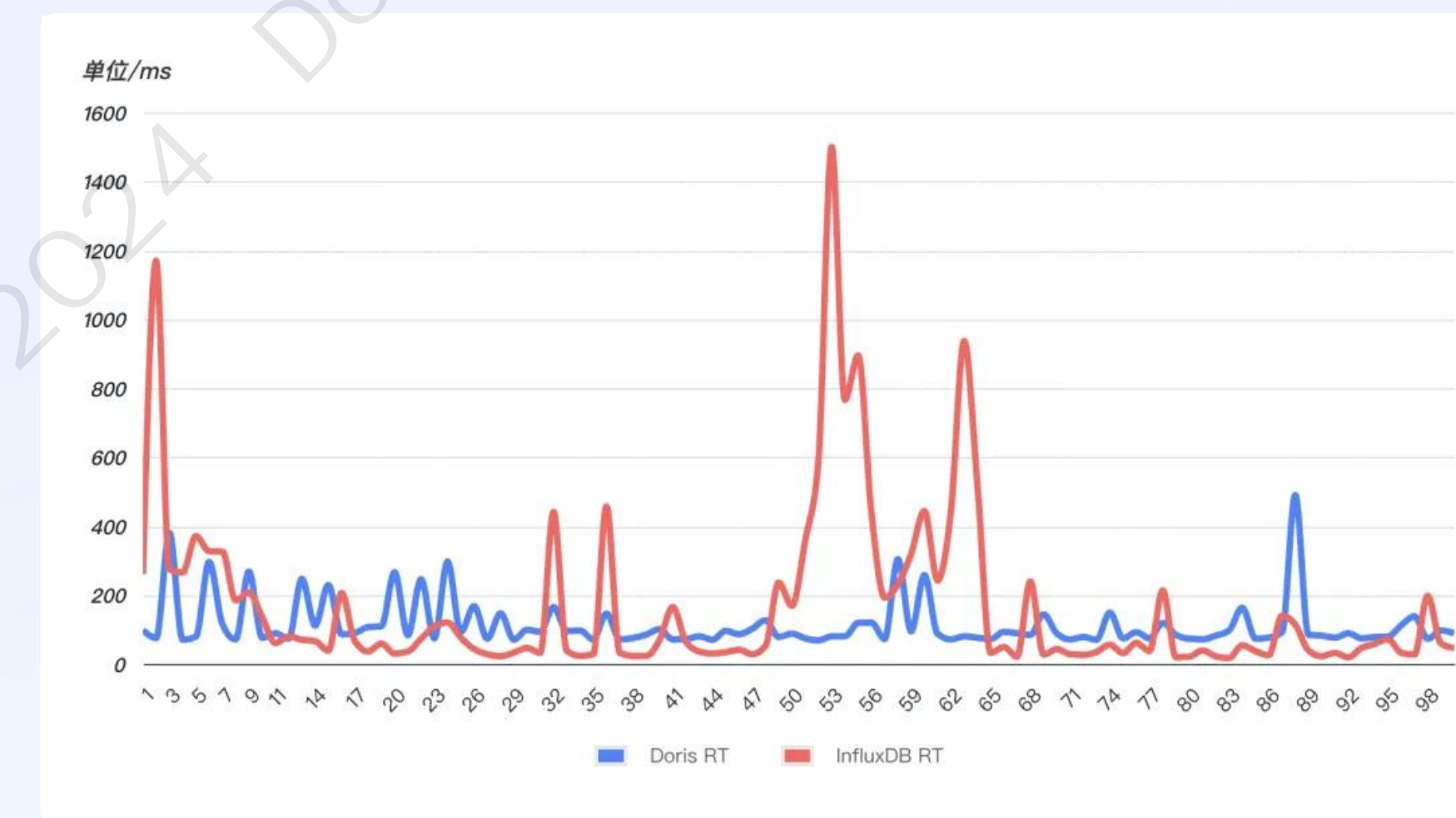
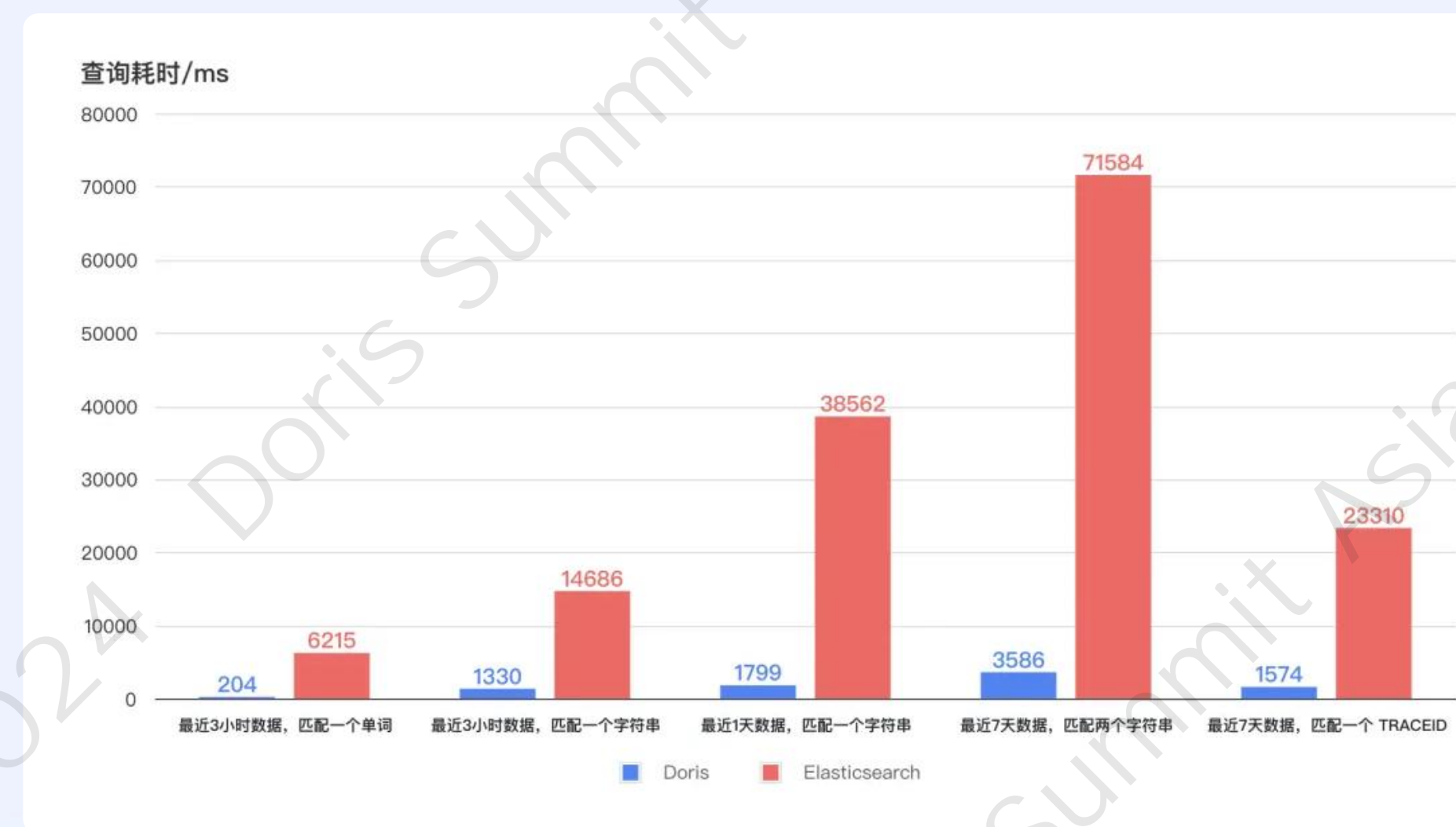
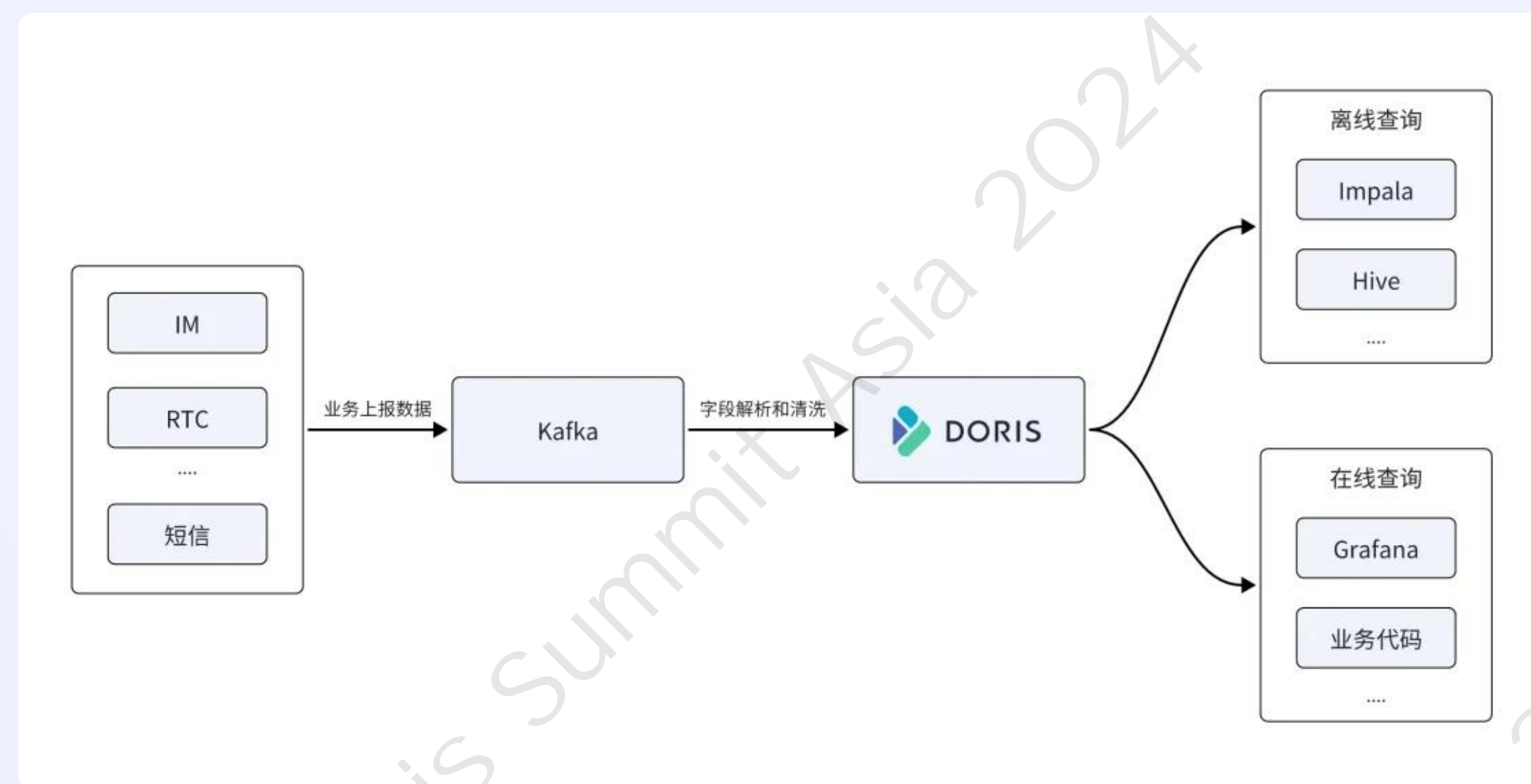
Log Trace 场景能够完全支持，标志着 Doris 几乎能扛住抖音集团绝大部分场景的导入性能需求



# 可观测性场景 — 案例2 网易

日志场景替代 ES，存储空间降低到原来 **1/3**，查询效率获得 **10** 倍提升

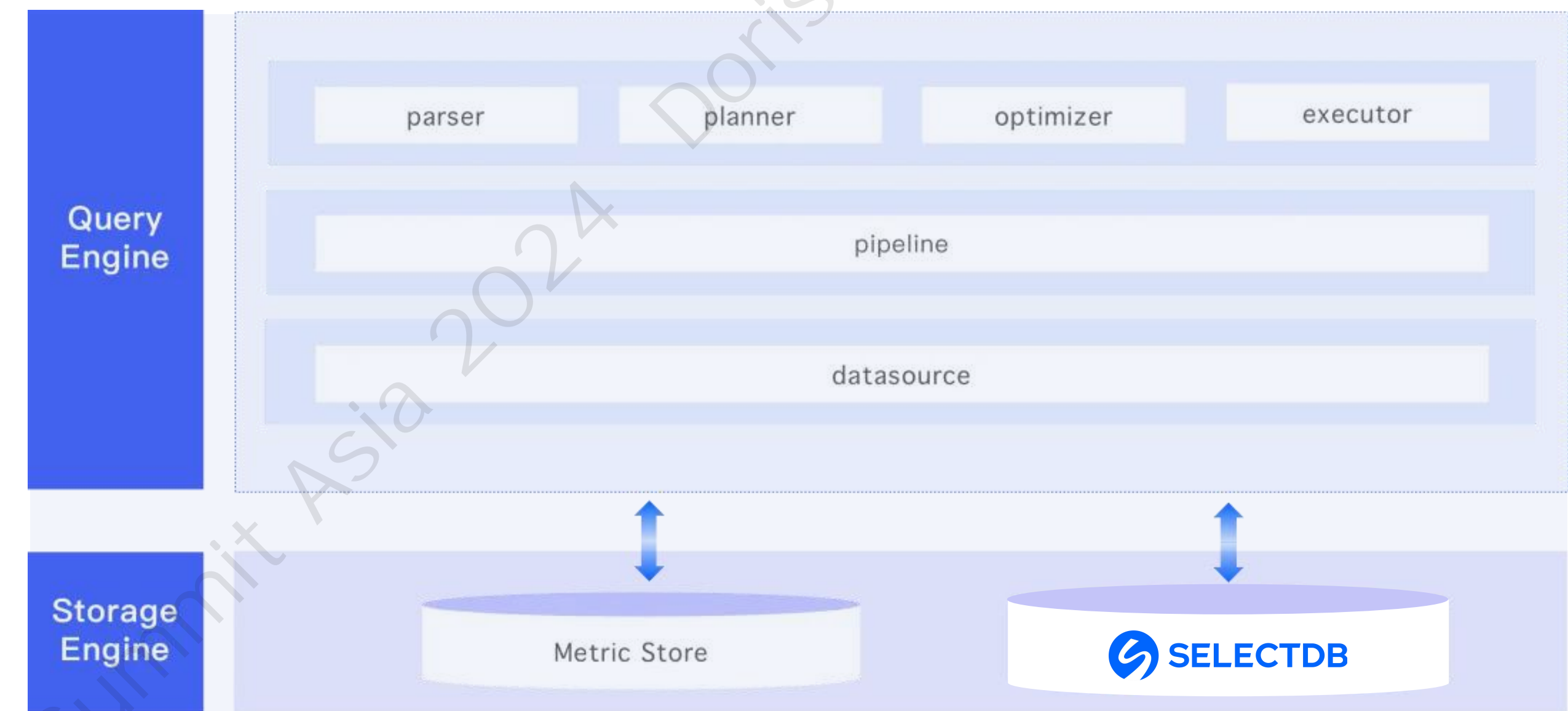
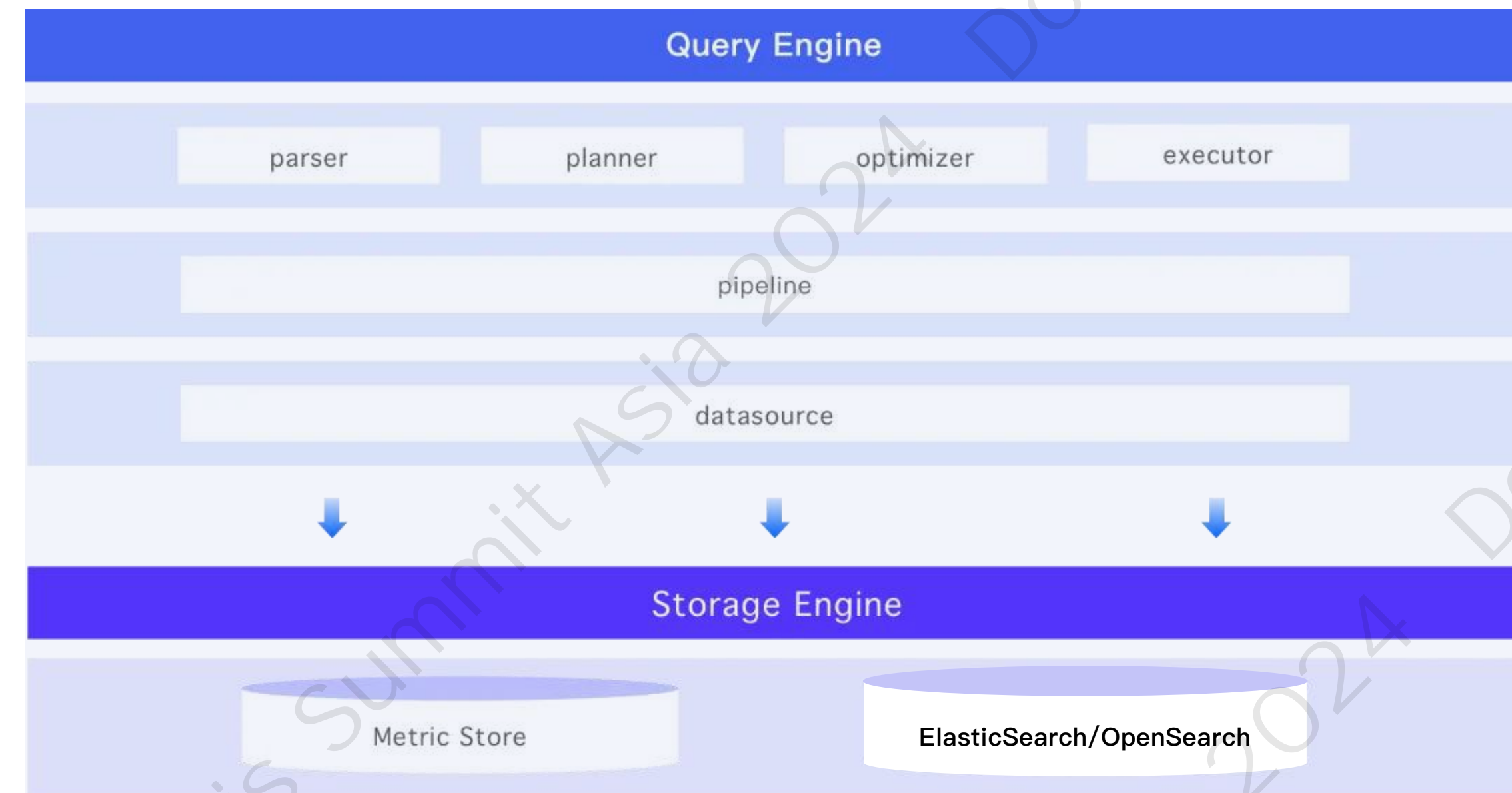
时序场景替代 InfluxDB，服务器节省 **50%**，存储空间降低 **67%**





## 可观测性场景 — 案例3 观测云

SelectDB 提供了适合 Log Trace 的半结构化类型 variant，相比云上ES 成本节省 **70%**，全文检索性能提升 **2-3倍**





# 网络安全场景 — 案例1 奇安信

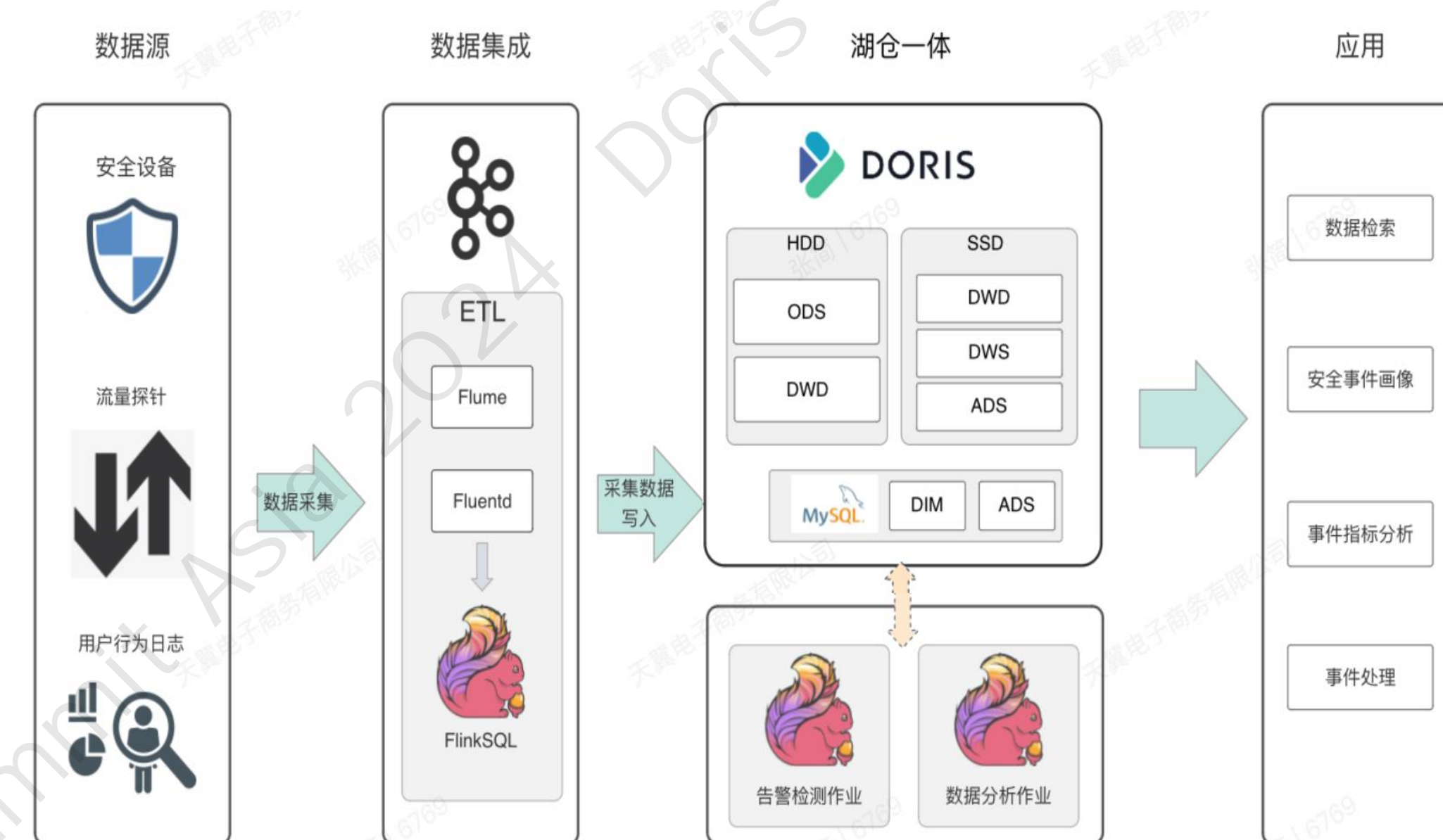
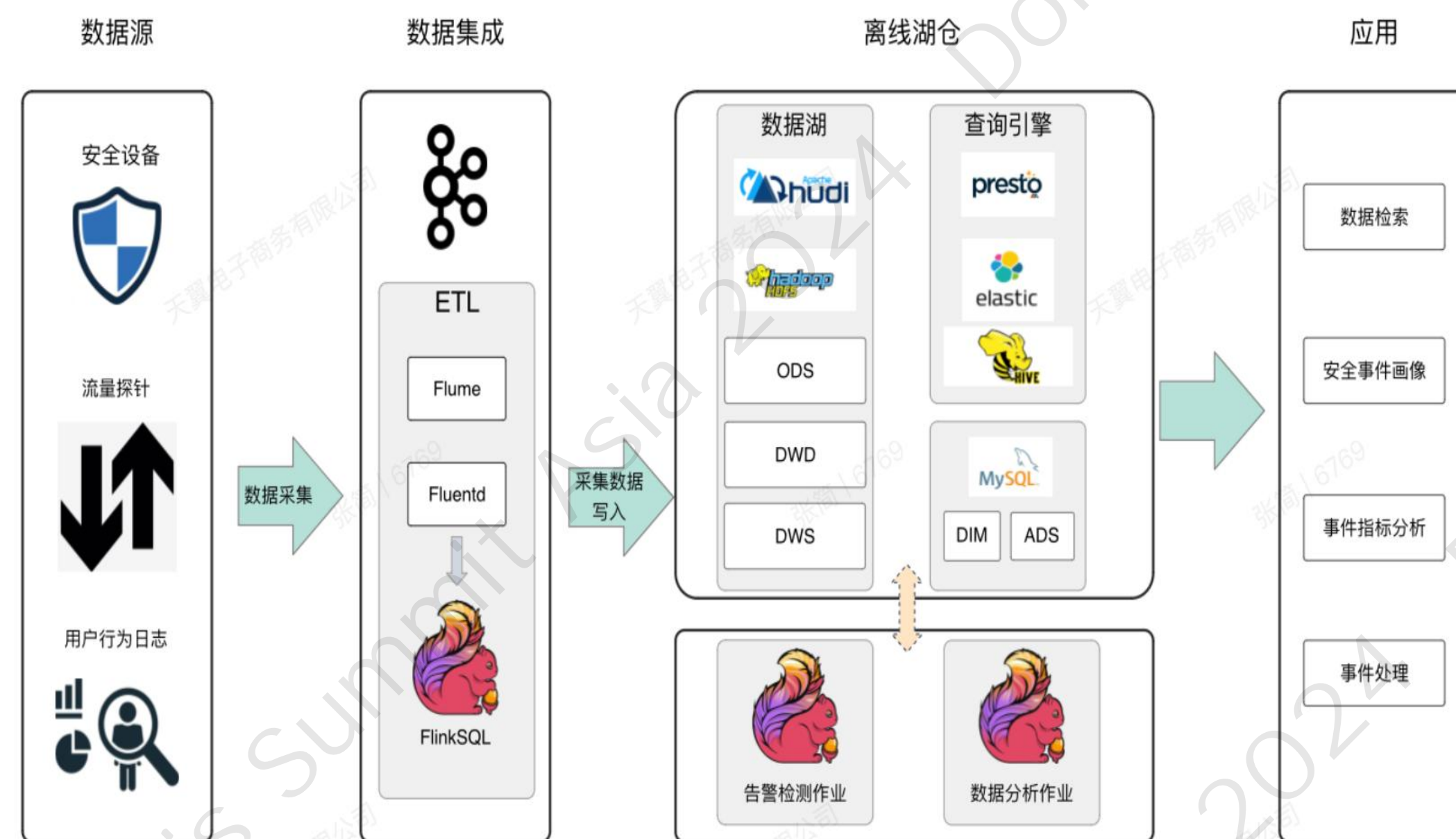
基于 Doris 的安全日志存储空间节省 **40%**，写入性能提升 **2倍**，查询同时支持 **全文检索 聚合统计 多表JOIN**





# 网络安全场景 — 案例2 中国电信翼支付

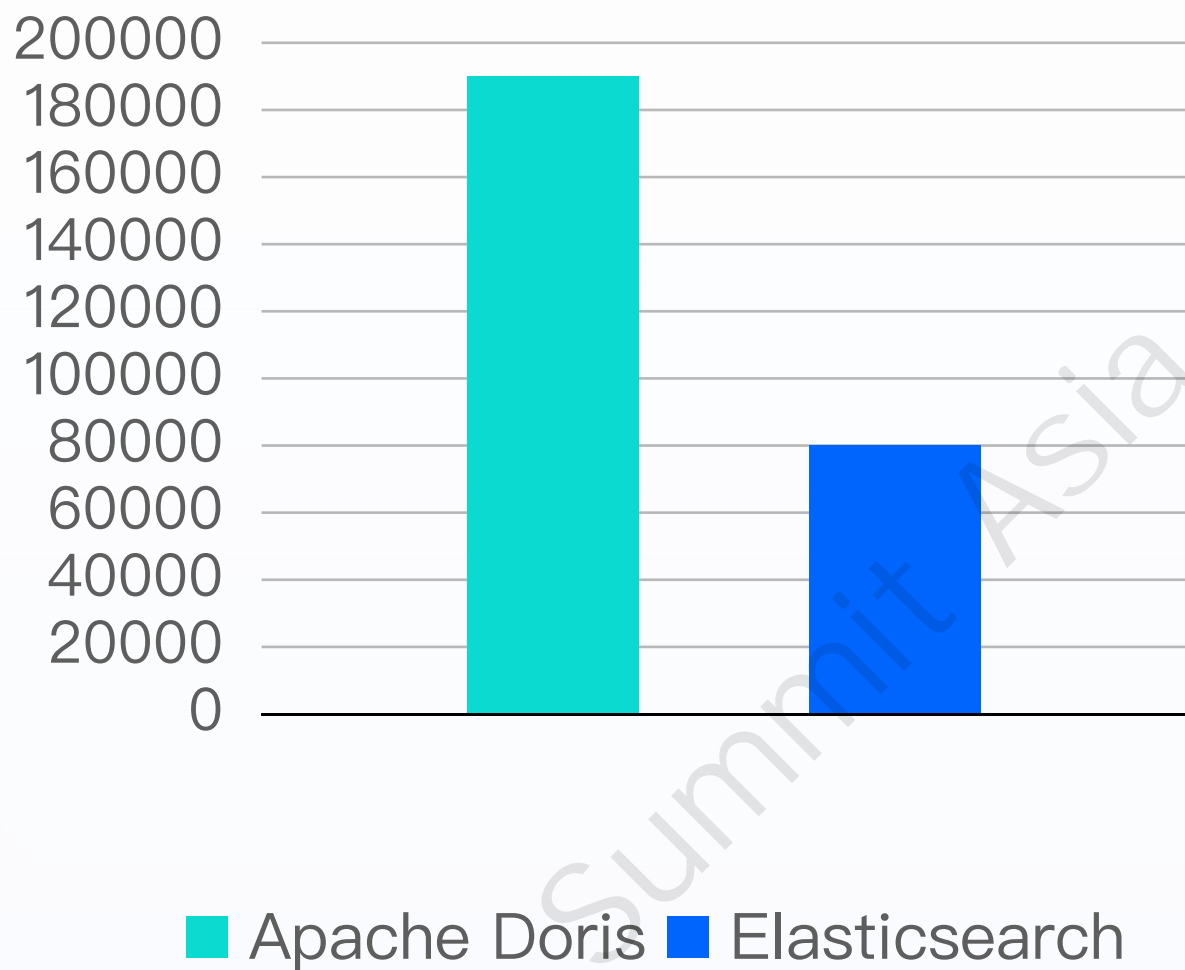
基于 Doris **统一** 安全数据存储，导入性能提升 **4倍**，存储空间节省 **50%**，查询性能提升 **3倍**



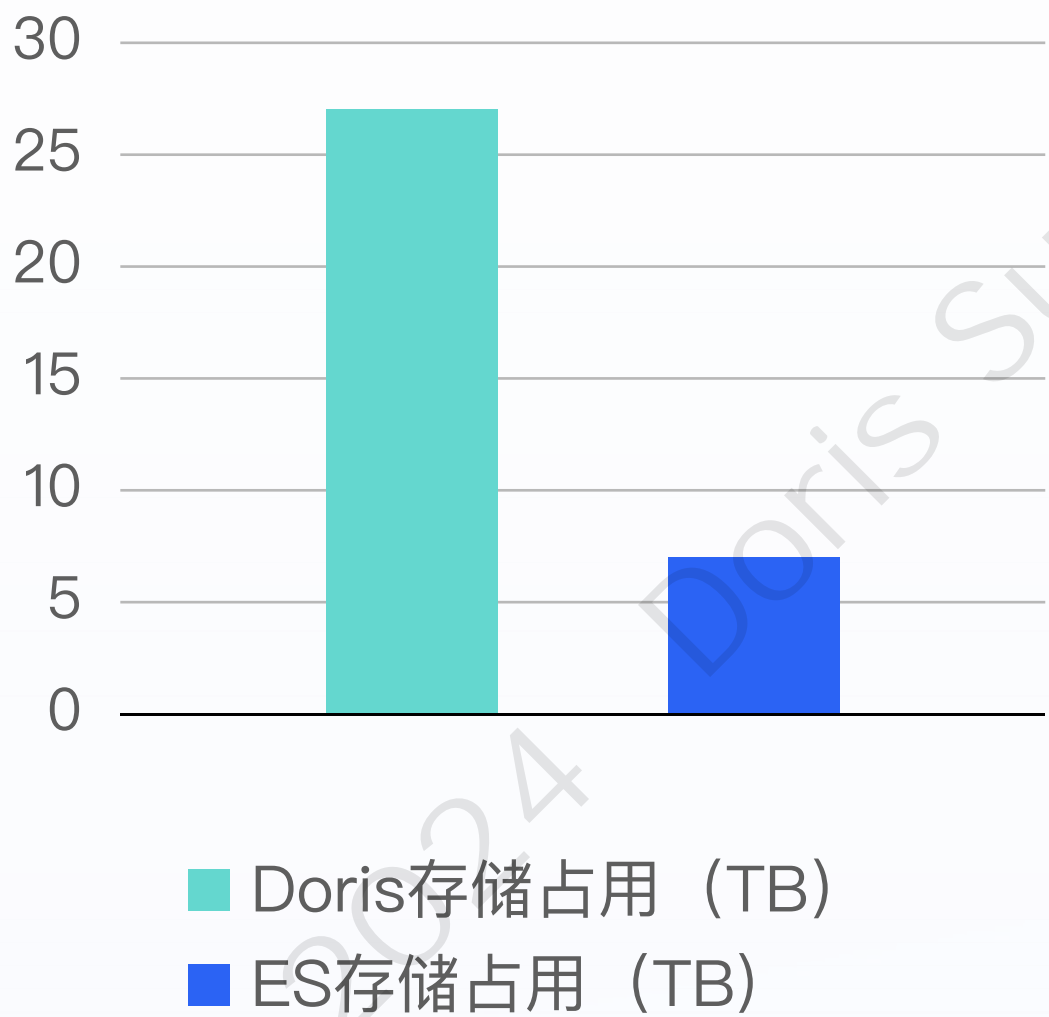
# 网络安全场景 — 案例3 安恒信息

Doris 相对于 ES 写入性能提升 **2倍**，压缩率提升 **4倍**，查询性能提升 **4倍**

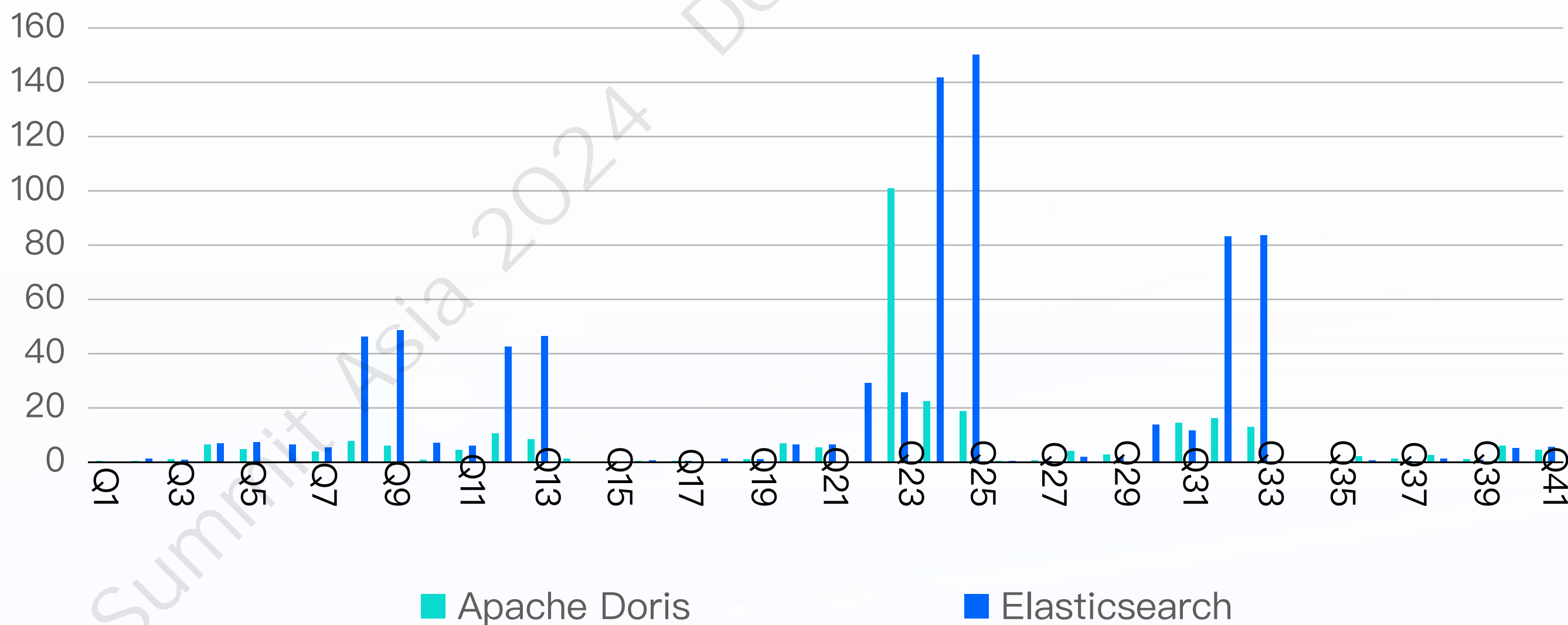
入库性能



相同数据量存储占用对比



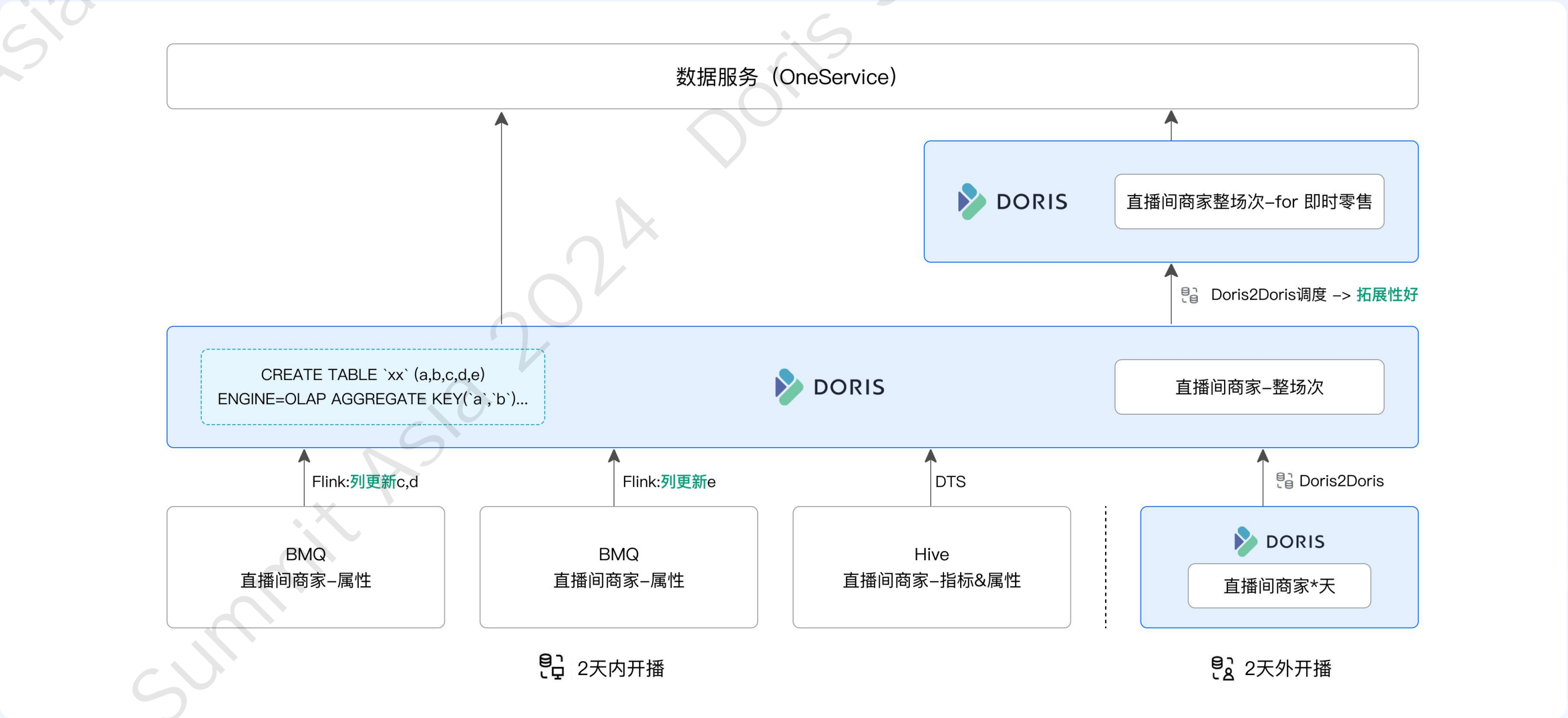
查询平均耗时 (s)





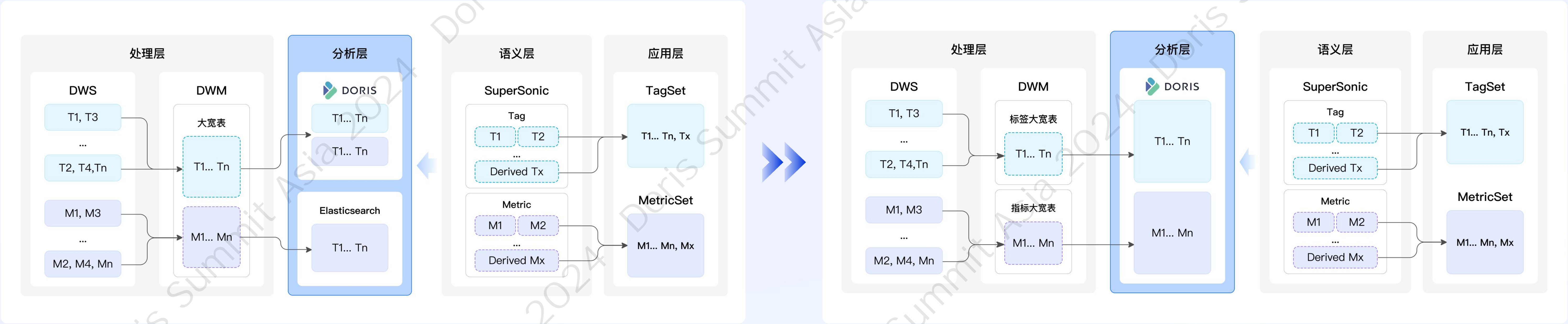
# 业务分析场景 — 案例1 抖音电商

直播详情页实时写入性能提升3倍：**30w/s->100w/s**， 查询并发提升4倍：**500QPS -> 2000QPS**



# 业务分析场景 — 案例2 腾讯音乐内容库

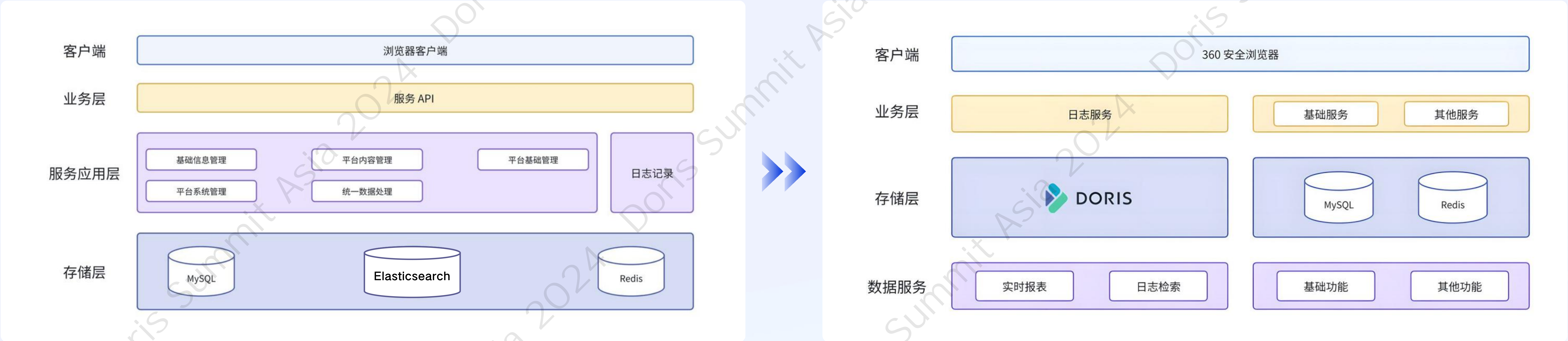
Doris 替换 ES 和 CK，同时满足 **搜索和分析** 的需求，存储成本降低 **80%**，写入性能提升 **4倍**，支持 **复杂分析**





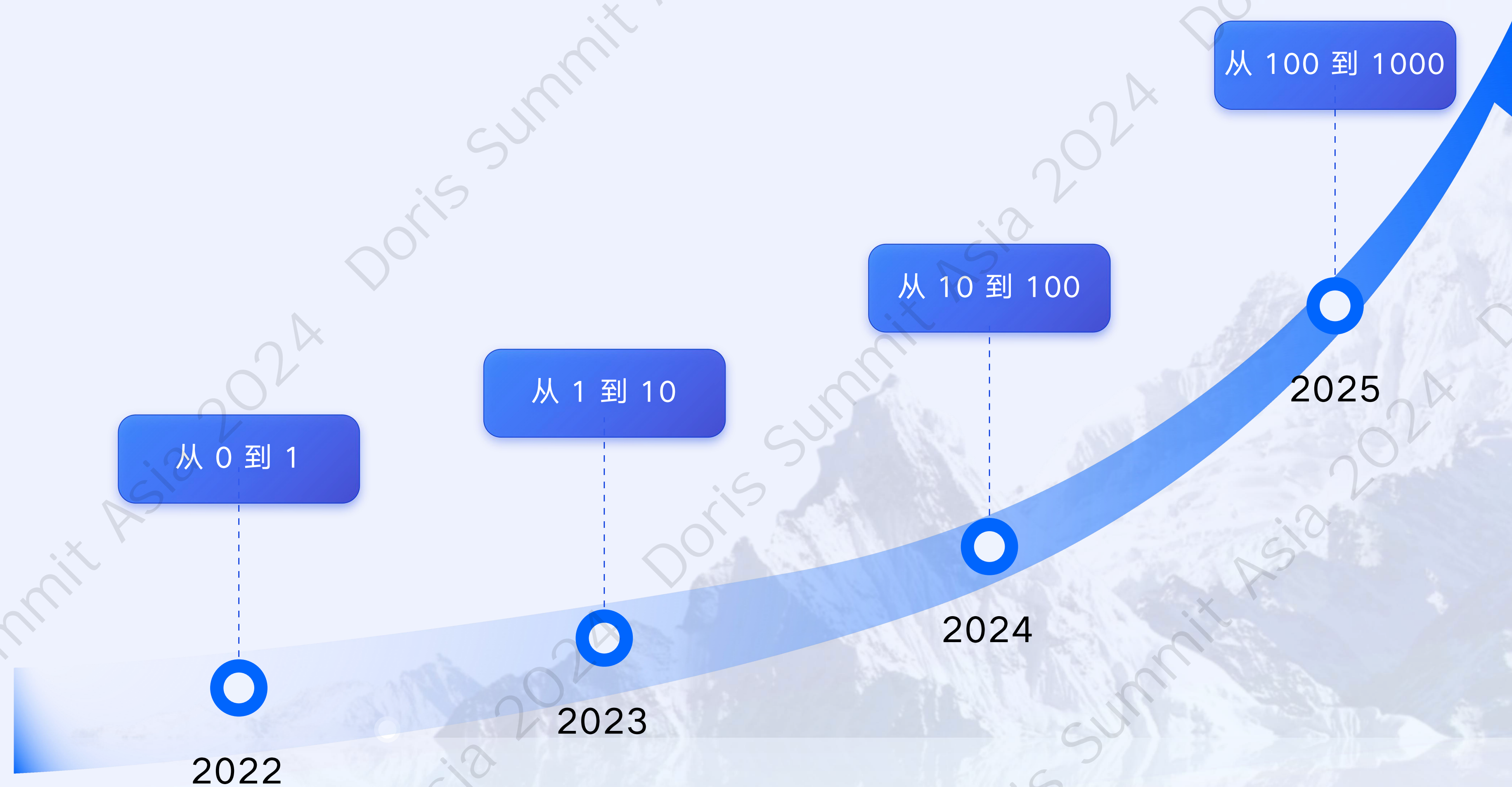
# 业务分析场景 — 案例3 360企业安全浏览器

Doris 统一了日志检索和报表分析，聚合分析效率提升 **100%**，存储空间降低 **60%**，SQL 开发效率提升**1倍** 以上





# 携手共建，勇攀高峰



欢迎加入专项群交流





Thanks for Watching!