

# 高升科技案例

## 高升科技公司简介

高升科技成立于2006年，是中国领先的云基础服务提供商，专注于基础云平台产品的研发与运营，主要向客户提供IDC（互联网数据中心）、CDN（内容分发网络）、APM（应用性能管理）和增值云服务。公司在全国积累了80多个机房和近4500G的带宽资源，服务网络可靠性达99.99%。已在中国大陆建立了150多个CDN节点，运营带宽达1200G，并针对视频、广电、游戏等行业推出了CDN加速解决方案。

## 业务挑战

随着高升科技CDN（内容分发网络）业务不断增长，在全国建立了150多个CDN节点，拥有上千台服务器，为200多家用户进行服务，日增数据达到1.2TB左右，高升科技不仅要为用户提供稳定的CDN服务，基于海量数据，还要为用户提供相应的数据业务支持。日增达到1.2TB的海量数据中，高升科技面临以下三大挑战。



### 跨地域数据整合难

如何将全国150多个CDN节点，上千台服务器中的数据进行统一的汇总，并在汇总过程中，对数据进行ETL的工作，进而保证数据的质量和完成性，是高升科技面临的第一个挑战。



### 数据的实时性差

基于CDN（内容分发网络）服务，高升科技需要为用户提供用户网站的访问数据，在日增TB级的海量数据中，分别为200多家用户提供实时的数据分析，是高升科技面临的第二个挑战。



### 无法实现灵活的多维度统计

基于网站访问数据，高升科技提供PV、UV和流量等维度的数据分析，上述维度已经不能满足用户对数据分析的需求，如何针对用户需求变化，灵活的设定统计维度是高升面临的第三个挑战。

## ALEIYE解决方案



## 数据整合

Aleiye 数据采集引擎LASSOCK是数据整合基础。通过数据采集器、文件上传、协议传输，脚本采集，API等手段将分散的、异构的数据进行实时的收集、拆解并整合进入平台。企业通过定义的采集规则，通过对数据进行拆解、过滤等手段进行预处理，并保证数据的实效性，完整性及准确性，为数据的关联、分析以及挖掘打下基础。

## 实时分析

Aleiye结合数据属性以及用户需求，对实效性要求的较高的数据进行实时的数据流处理。基于Aleiye的检索引擎，通过类似百度和谷歌的关键字检索（使用布尔代数AND、OR、NOT及括号）进行任意的组合实现数据实时检索，通过检索结果，快速生成可视化报表，从而自定义分析维度及指标，为分析结果提供高扩展性和灵活性。

# 中国移动案例

## 中国移动简介

中国移动通信集团公司（简称“中国移动”）于2000年4月20日成立，基站总数超过220万个，客户总数超过8亿户，中国移动全资拥有中国移动（香港）集团有限公司，由其控股的中国移动有限公司（简称“上市公司”）在国内31个省（自治区、直辖市）和香港特别行政区设立全资子公司，并在香港和纽约上市。

## 业务挑战

中国移动拥有4A、安全域、ISMP等业务系统，每个业务系统对应着独立的数据库，随着业务快速扩展，基于传统的数据库，已经无法支撑其系统运转，存在数据丢失，无法进行复杂的业务计算。



### 多业务系统数据整合

基于中国移动中的多个业务系统，每个业务系统的数据都是独立的，无法实现全部整合，除业务数据外，安全设备数据需要与业务数据进行关联、补全等操作，当前业务数据和设备数据的整合是中国移动面临的第一大挑战。



### 数据标准化

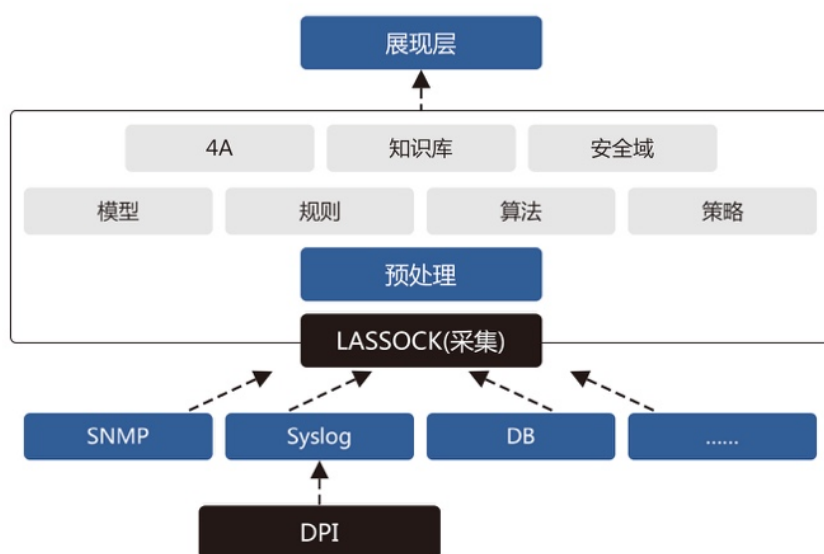
数据在整合过程中，需要对数据库数据、安全设备数据进行统一标准化管理，由于数据格式存在差异，且在数据源中，存在大量的重复信息、不可信的信息和不重要的信息，这些问题将会直接导致最后分析结果的准确性降低，如何将业务数据和设备数据进行标准化管理是中国移动面临的第二大挑战。



### 复杂的规则告警

中国移动的数据不断增加，在传统的数据库的支撑下，很难保证数据的实时性，其次无法实现业务逻辑复杂的规则性告警，如何实现上述问题是中国移动面临的第三大挑战。

# ALEIYE解决方案



## 数据整合

Aleiyee 数据采集引擎LASSOCK是数据整合基础。通过数据采集器、文件上传、协议传输，脚本采集，API等手段将分散的、异构的数据进行实时的收集、拆解并整合进入平台。企业通过定义的采集规则，通过对数据进行拆解、过滤等手段进行预处理，并保证数据的实效性，完整性及准确性，为数据的关联、分析以及挖掘打下基础。

## 数据预处理

原始日志采集之后，需要进行数据预处理的过程。Aleiyee通过标准化配置，对数据源进行明确的数据类型划分，将日志格式进行统一转化和分类，根据划分好的数据类型进行过滤、归并、补全等规则操作，为后续数据处理提供信息。最终输出明确的事件类型和各字段属性及补全后的信息等内容的标准事件。

## 基于规则库的关联告警

基于Aleiyee自带的规则库，将解析后的数据与规则进行关联匹配，一旦数据传输过程中，符合规则库中的业务逻辑，便会触发告警信息，从而重构整个攻击场景，降低误报率，帮助安全监控人员分析出网络中潜在的安全隐患。

# VIPKID客户案例

## 客户介绍

VIPKID是一家新兴的互联网教育科技公司，旨在为中国孩子提供最好的美国小学线上课程，凭借强大的国际化师资团队、精细化运营管理以及个性化、全流程化的服务助力业务的高速发展，服务学生数量达到3万人，是中国科技教育行业的Rock Star，曾在硅谷与美国团队同台竞技，获得国际顶级投资机构投资。

## 业务挑战



### 多源异构数据源无法整合：

数据来源于不同的数据库、web服务器日志以及其他软件、业务系统等，数据孤立导致无法深层次挖掘数据价值；



### 传统数据库无法支撑复杂的业务分析：

基于VIPKID的销售漏斗模型，在传统数据库的支撑下，其复杂的业务指标查询速度极慢，甚至无法进行关联查询。无法保证销售漏斗模型的数据支撑，直接影响业务发展。



### 非结构化数据无法分析：

随着企业的不断发展积累了大量的数据，其中大部分为非结构化数据，其中包括设备日志、文本文字等非结构化数据无法进行价值掘金；



### 业务快速发展对客户转化率的要求不断提高：

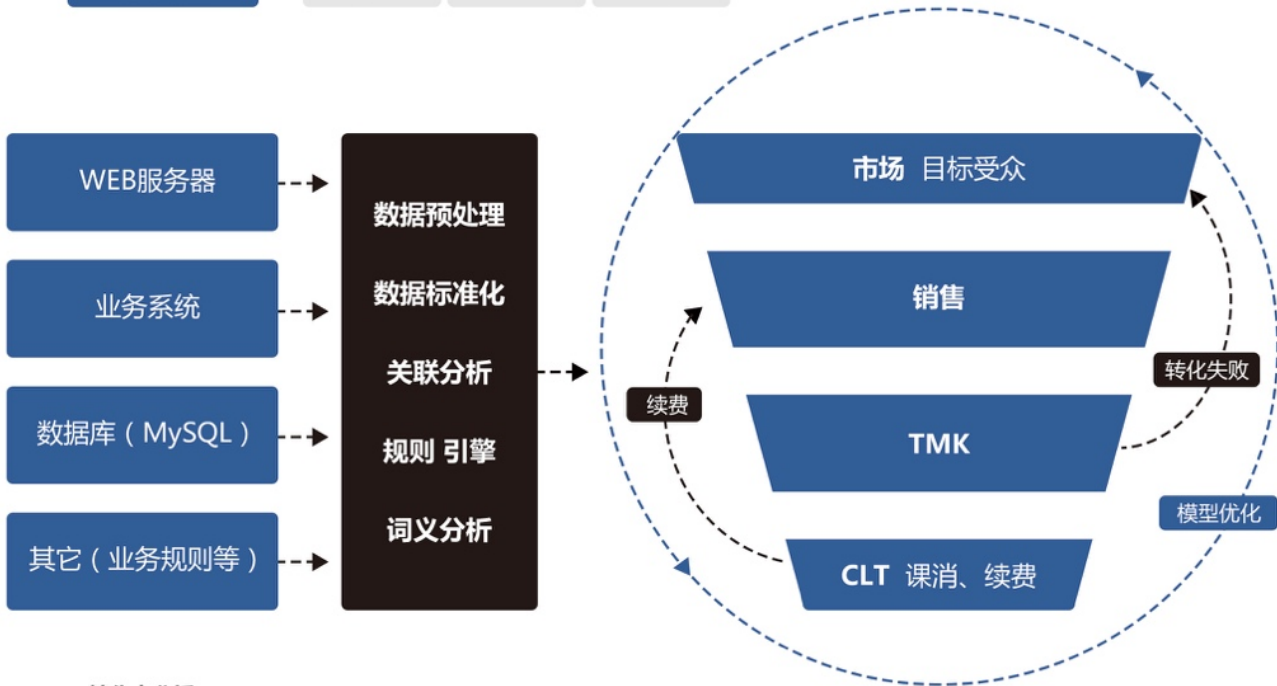
面对高速的业务发展，与此同时也面临着业务运营带来的巨大压力；企业各部门只能依赖于简单的数据库查询进行决策支撑；



### 分析成本高、人力投入不断增加：

随着业务的迅速发展，其业务指标的复杂性不断增加，根据业务增长需求，对数据支撑依赖度不断增加，在传统数据库的支撑下，其指标扩展性差，导致数据分析部门人力成本不断投入。

# ALEIYE解决方案



## ● 转化率分析：

Aleiye平台基于强大的数据处理能力结合VIPkid业务模型进行业务流程的持续优化，为用户运营的精益化管理提供数据支持；

1. 提升新客户转化率：对市场 - 销售 - TMK各个环节的学生数量、地域等属性进行分析以及对沟通过程中的文本记录进行语义分析，从而更精准的识别需求客户，降低不必要的人员投入成本，提高新客户转化率；
2. 促进课程消费：结合CLT - 销售 - 教师等各环节学生的空暇时间、兴趣偏向、成绩等数据，优化学生的课程安排，在提升服务质量的基础上，促进学生消费预付的课程费用；
3. 提升客户黏度：通过学生的兴趣偏向、成绩、地域分布等多个属性制定个性化的学习方案，提升服务质量、进而提升客户黏度；

## ● 模型优化：

打破以往数据竖井的限制,对业务各个环节数据以及运营数据的深度关联，进行业务模型的持续优化；

## ● 情感分析：

结合Aleiyed数据挖掘模型对用户销售各环节的沟通记录文本进行词语分析，快速提取有效信息，为销售漏斗模型转化提供数据支持；

# 客户收益

作为一家处于成长期的互联网企业，业务转化率的提升以及业务流程的持续优化是我们现阶段的首要目标；Aleiyed提供的数据分析对我们帮助很大，数据分析已经成为我们经营决策一把标尺，在运营管理中可知其然、知其所以然；洞察新机会以及建立数据化运营管理体系将是发展中又一个新的制高点。



# 北京银行用户案例

## 客户介绍

北京银行目前是中国第二大城市银行及北京地区第三大银行，雇有3,600多名员工，通过其116家支行为个人与公司客户提供服务。同时，北京银行还在其覆盖网点设立了272台自动取款机，并建立了快速增长的电子银行业务。

## 业务挑战

安全事件分析，通过对多品牌、多类型的安全设备进行整合，找到安全事件之间的关联关系及影响程度。



### 故障分析

故障定位凭借人的经验进行机械化工作，故障定位于解决速度慢，希望提高到分钟级别



### 容量规划

可以对设备的使用情况进行监控，但是无法进行负载分析，需要为设备的使用情况提供量化指标



### 趋势分析

对服务器硬件CPU、流量等实时监测，为硬件升级或带宽升级提供数据依据。

## Aleiye解决方案

将北京银行过去分散在各个系统中的信息集中，其中包括资产信息、设备运行状态、日志、安全事件等全部通过syslog和snmp的方式存储到aleiye数据平台。在平台中，通过字段扩展、统计、预测、关联资产、日志规则分析等手段完成集运维与安全的高效办公平台。



### 资产信息

资产信息源自于北京银行内部的IT设备管理系统。通过数据采集的方式同步到数据平台中，并在平台中可进行任意的扩展。是所有业务分析的基础数据。



### 日志

包括网络日志、安全日志、系统日志及应用日志，涉及到多个类型和多个品牌的百余种日志，完美的统一存储在Aleiy数据平台。



### 深度分析

将采集到的多种数据进行交叉关联，日志与日志，日志与设备、日志与业务同时进行关联，准确定位故障、发现安全事件、描述发展趋势。

## 网络运维管理

在银行体系里，各系统及各服务器网络情况是日常管理的重中之重，Aleiyee大数据分析平台可以帮助用户从以下几个方面完成管理，包括：



### 网络事件管理

网络因传播性，同一事件往往会产生大量日志。大量日志不但不会为事件的定位和分析带来好处，反倒会成为影响事件分析的障碍。aleiye通过微时间窗口内的日志间的关联关系，将日志压缩为事件，事件是用户分析和管理的原子。



### 接口级网络拓扑

提供网络设备间接口级别的连接拓扑，接口连接信息可直接进入资产信息，并提供交互式管理接口。为网络事件提供更细粒度的分析维度。



### 容量规划

通过对设备监控的同时，讲历史的数据通过负载分析算法综合评价设备的使用情况。为设备升级、带宽升级及资源合理化利用提供量化指标



### 故障定位

根据事件的产生时间，位置及关联资产信息。再通过实时的流数据分析，主动发现事件间存在的共性进行快速定位，并且对故障对服务的影响进行分析。



### 告警

告别传统的一日志一告警的方式，将关键事件（RET）直接变成以报告为主要内容的综合告警。

## 安全事件分析管理



### 统一管理

多类型，多品牌aleiye平台提供统一的采集、存储、分析平台。兼容主流品牌的安全设备分析功能。



### 标准化

安全设备原始日志之后，需要预处理，通过标准化、过滤、归并、信息补全，将原始日志转化为格式统一、分类明确，并进行过滤与归并，为关联分析输出告警提供一句；最终输出已明确事件分类、各字段属性正确赋值，并补全了安全事件信息。



### 关联分析

通过安全事件关联分析完成以安全事件为触发，结合安全资产信息、漏洞情况、安全防护状况等信息进一步挖掘有用信息，直到产生具有较高可信度、明确的问题描述以及具体的处理方式的报告。

## 客户收益

通过成熟的Aleiyee大数据分析平台作为管理工具，利用专业化的网络、系统、应用存储方案，将北京银行现有的业务进行整合、标准化，全面的进行关联分析，异常实时告警、业务趋势分析。并且把网络、系统、应用三者的运维工作进行集成，以仪表板的型式集中展现，完成统一管理。



# 民族证券用户案例

## 客户介绍

中国民族证券有限责任公司（以下简称“公司”）成立于2002年4月，是经中国证监会批准的综合类证券公司，注册地北京市。2013年，股东政泉控股、乐山国资公司、兵工财务等完成对公司增资后，注册资本44.87亿元人民币。2014年8月，民族证券与方正证券重大资产重组工作获批，公司原股东成为方正证券股东，方正证券成为公司股东。公司总部位于北京市朝阳区盘古大观，是上海证券交易所、深圳证券交易所的会员单位。在北京、上海、深圳等 18 个大中省市和经济发达地区设立了51家分支机构。

## 业务挑战



数据分布在多个区域；



人力不足，突发事件解决困难；



每天增量上千万；



审计机动性大，只能通过大量手工方式处理；



业务类型多，并每个季度都会有业务数据类型产生；



多年的大量数据存在硬盘上，不知道如何利用；



产生的数据无法量化，从而淹没数据。

## Aleiye解决方案



高性能分布式多功能采集系统。



全类型接入，统一数据平台管理。



灵活检索模式，应对突发事件及审计。



任务调度机制，让机器覆盖日常的事务性工作。

## 客户收益



高效运维与审计减少人员投入。



新业务上线，日志无缝接入平台。



良好的数据可视化效果，量化数据更直观。



科学的数据分析方法，对数据价值的挖掘产生了新的想法。