



## XDR网络安全监测与分析 关键技术创新产业化实施项目

---

国内首家SOAPA创新架构XDR技术  
解决的实战化网络安全运营商





# 目录 CONTENTS

This is a subtitle for your presentation



● 项目介绍

● 商业模式

● 项目团队介绍

● 融资计划



## 项目介绍 ▶

About us

## 政策与事件催生服务和实战需求——高效运营

### 政策

- 《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》明确了到2023年，行业规模超过2500亿元
- 关键行业安全预算占比大幅度提升（三法、两规、两办法）



### 事件

- “滴滴出行”App存在严重违法违规收集使用个人信息问题。国家互联网信息办公室，应用商店下架“滴滴出行”App



超过100万用户的APP赴海外上市需经过监管审查

## 已知威胁数量庞大，水下威胁更令人担忧

- 境外恶意程序攻击数量大幅增加

单位：万个



数据资产  
高效管理  
迫切需求

- 重点被攻击行业



通信



金融



交通



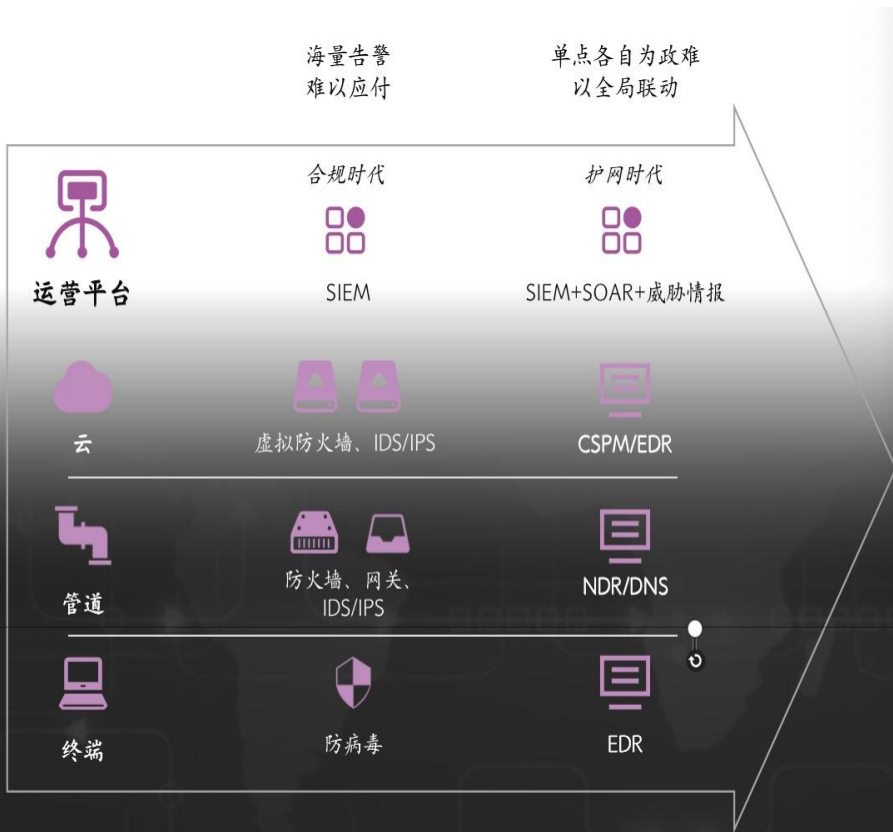
能源



国防

# 客户已完成安全产品堆砌采购，如何“用起来”成为头号难题

安全建设发展路径



产品各自为政，安全运营割裂，依赖安全专家

一体化运营，全局态势感知

优化告警，提高运维效率

全工具化，摆脱专家依赖

交互溯源，还原威胁全貌

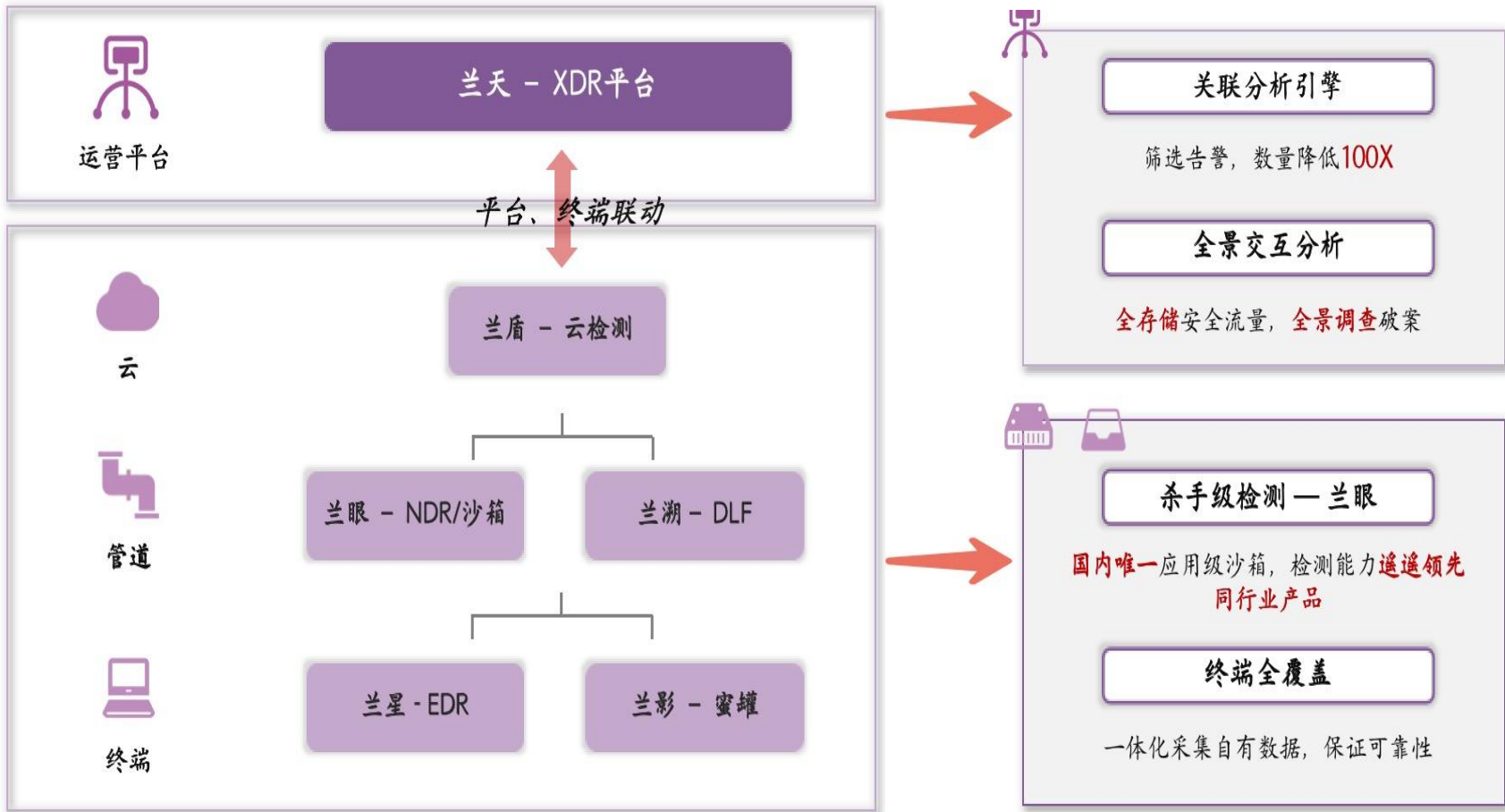
优化策略，降低处理难度

产品化高效处理已知&未知威胁，摆脱专家依赖

解决  
现有  
产品  
联动  
运营

补强  
产品  
整体  
运营  
方案

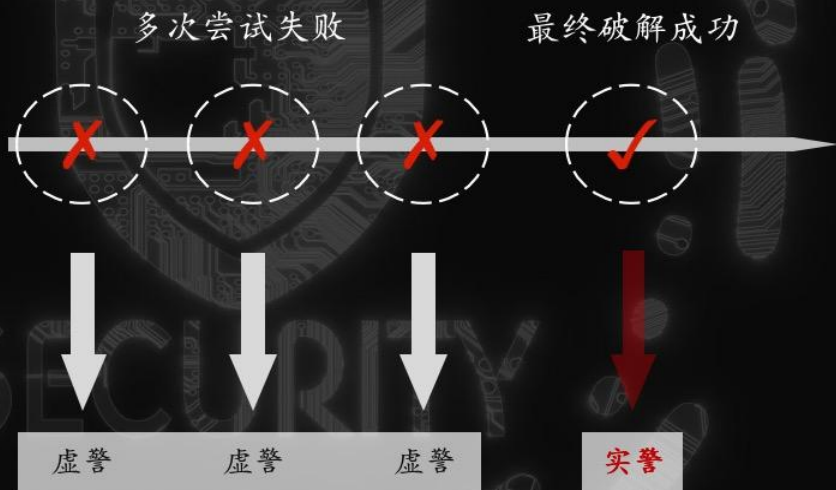
# XDR平台 + 终端联动，兰云实现安全运营一站式高效管理



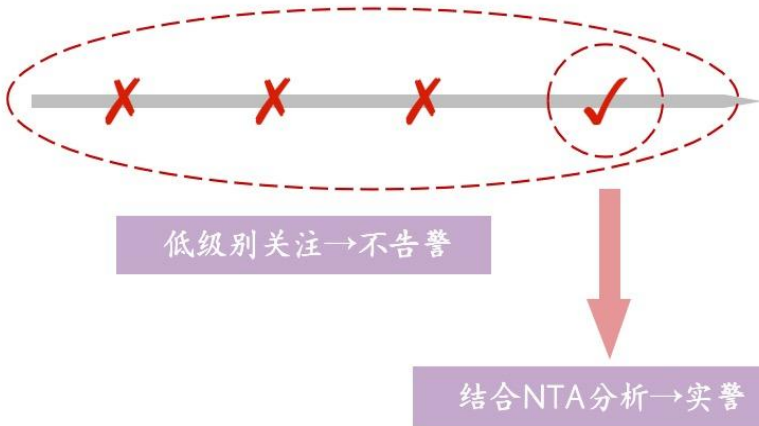
# 几何级降低海量告警管理难度——关联分析业内领先

以多次恶意尝试密码登陆为例：

## 主流分析逻辑——多次告警



## 兰云分析逻辑——一次告警



- 真实告警被掩盖在了大量虚警中
- 友商缺乏关键节点产品，从而出现漏报

- 告警量下降为原来的1/100，颠覆性的逻辑构建
- 通过关联分析事件序列筛选真实威胁，解决重大实战需求

国内唯一工具化交互调查，深度发现水下威胁。

## 还原攻击全景——快速锁定目标

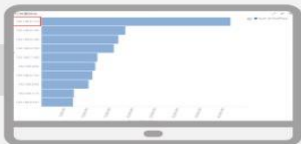
甲方安全运维人员视角：在兰天平台展开威胁调查

出现告警



- 经关联分析引擎筛选后出现告警

定位异常设备



- 发现一台闲置设备出现了大量的数据通信

自动筛选异常应用



- 此闲置设备正在频繁向境外IP发送邮件

自动分析异常流量



- 发送邮件的速度是每秒1000封

交互分析其它感染资产



- 同步发现出现此类问题的其它资产，迅速阻断



2016

- 完成天使轮融资
- 国家级贵阳大数据与网络安全攻防大赛获得防守方第一名



- 完成A轮融资
- 出色完成厦门“金砖会议”重点保障
- 2017 WitAwards “年度创新产品奖”

2017



2018

- 中国网络安全技术对抗赛第三名
- 2018年中国网络信息安全最具成长力企业奖




2019

- 2019CNCERT恶意脚本检测能力测试第一名
- 北京大兴国际机场态势感知平台圆满验收
- 与华三建立唯一战略合作伙伴



- 与中兴通讯达成唯一战略合作伙伴
- 北京高速公路联网收费系统态势感知项目圆满验收



2020

- 东南大学全球创新创业大赛“麒麟杯”总决赛第一名
- 科创中国创新创业大赛第二名
- 布局省代模式，完成全国区域化销售网络
- 完成IPO初调，业务及财务规范化运营开始

2021

PRESENT



## 国产化支持



...

## 国内唯一应用级沙箱



WEB  
沙箱



Office  
沙箱

沙箱行为规则: 500+

静态流检测规则: 2w+

## XDR技术国内领先

首家SOAPA架构体系创建者

关联分析 交互分析

数据运营一体化整合技术

## 全面调查分析

- 失陷主机分析
- 可疑主机分析
- 业务情况分析
- VPN登录用户行为分析

## 全面行为审计

- 全网络会话
- 邮件收发
- Web访问
- DNS请求
- 文件传输

## 内网服务器资产梳理

- 了解以开放的业务端口
- 提供有效的回收机制
  - 内部应用管理
  - 权限管理



# 兰云科技 部分行业客户展示

交通



金融



运营商&渠道



军队&其它

部队&军工客户





# 盈利模式



北京大兴机场 首都公路发展集团 中国移动 阳光保险 北京地铁

标杆大客户——行业渗透 样板  
点复制 垂直行业管理

战略合作伙伴——资源互补 基  
础设施重点拓展 开发大项目

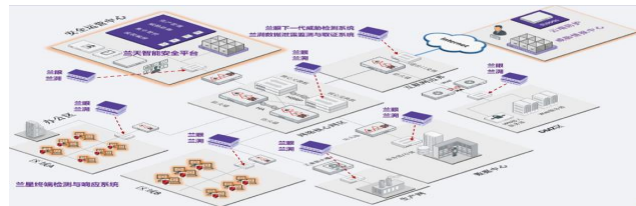


华为 新华三 中兴通讯 中国联通 中国电信



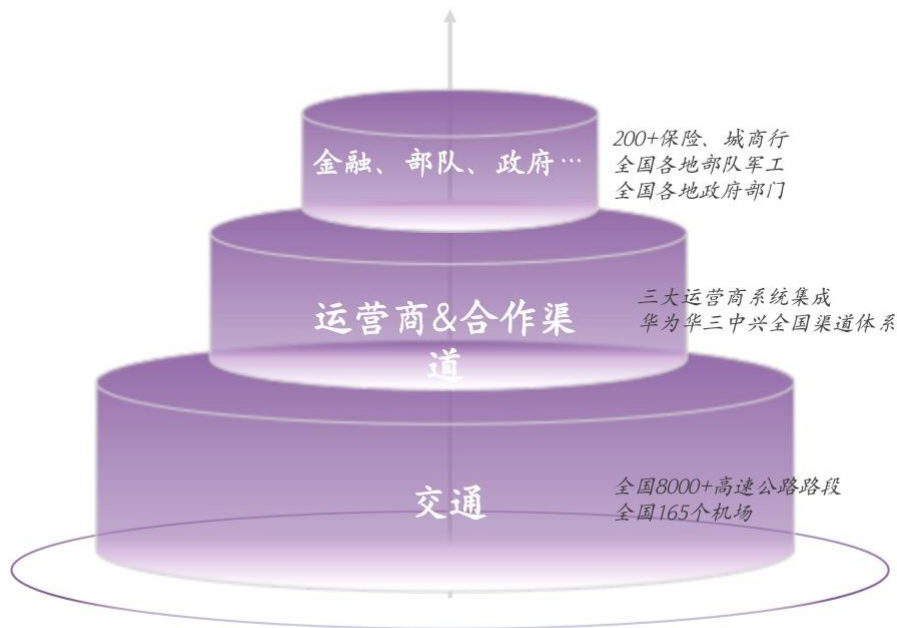
区域子公司模式——全国销  
售体系建设 业务快速响应

省代模式——地方政企维护  
行业深耕细作





全面的产品线 → 多样的切入点



### 业务拓展区 - 优势产品单点突破再渗透

- 用户痛点：应对护网等场景，亟需实战攻防能力补强
- 销售策略：终端产品为主，逐渐渗透平台产品

### 高速增长区 - 得天独厚的资源优势

- 渠道痛点：渠道解决方案需要更有竞争力的产品补充
- 销售策略：平台 + 终端产品，提供更完整的打包方案

### 品牌基本盘 - 国内交通领域NO.1

- 用户痛点：高速公路路段中心过往采购了大量合规产品产生的海量告警无人处理
- 销售策略：平台 + 终端产品，一体化安全运维



项目团队



## 领军人介绍

董事长&CEO

易建超



### 华为15年 | 华为赛门铁克杭州研究所所长

- 东南大学计算机系2001年硕士毕业，师从东南大学校长、中国工程院院士顾冠群教授
- 曾任华为赛门铁克杭州研究所所长、移动互联网安全国家重点实验室理事，曾主导华为中低端安全、高端安全、大数据安全等领域业务
- 华为经历：
  - 曾获华为金牌个人奖（TOP 3%）
  - 2012年国内首创的盒式万兆防火墙产品荣获华赛公司产品最高成就奖
  - 2014年高端防火墙获NSS LAB全球首款推荐级TB防火墙
  - 2015年Anti-DDoS产品在德国全球ICT峰会作为华为近2000款产品的四个重量级代表产品之一面向全球发布
  - 2015年开创华为大数据安全业务，所带领的华为安全板块业绩平均每年保持30%增长，华为安全业务在2016年上半年登上《中国网络安全企业50强》榜首



CTO

周宏斌

19年 | 反APT专家

- 曾任华为安全专家
- 深入研究终端、边界、网络安全
- APT检测专家
- 国内单向网闸首创者
- 拥有多项安全领域发明专利



VP

肖洪亮

16年 | 安全专家

- 华为AntiDDoS产品创始人，现在该产品竞争力仍处于全球领先
- 分管销售，曾主导多个重大市场项目的落地和运营



CSA

朱国峰

23年 | 架构专家

- 22年架构设计及开发经验
- 具备丰富大型软件产品和项目的开发和性能调优经验
- 曾作为核心成员参与研发IBM、CISCO、VMWare多款核心产品



融资计划



# 势能积蓄完毕，兰云通过资金杠杆快速放量冲刺IPO

2022 ~ 2025

质变期 - 冲刺IPO

2017 ~ 2021

量变期

各个行业标杆客户案例积累

亿元成熟单品 + 多产品线组合

军密资质 + 各行业渠道资源

复制 + 增销

- 交通：全国复制
- 军工：军种内复制
- 金融：已进入客户增销
- 政企&能源：更多渠道合作触达

管理甲方预算

- 复制XDR+NDR的成熟方案
- 提升EDR能力
- 夯实数据安全产品线
- 打造一体化解决方案

渠道放量 + 直销体系建立

- 华为、华三渠道资源放量
- 各省建立直销+服务抓手
- 渠道代理模式建立

2025年完成IPO

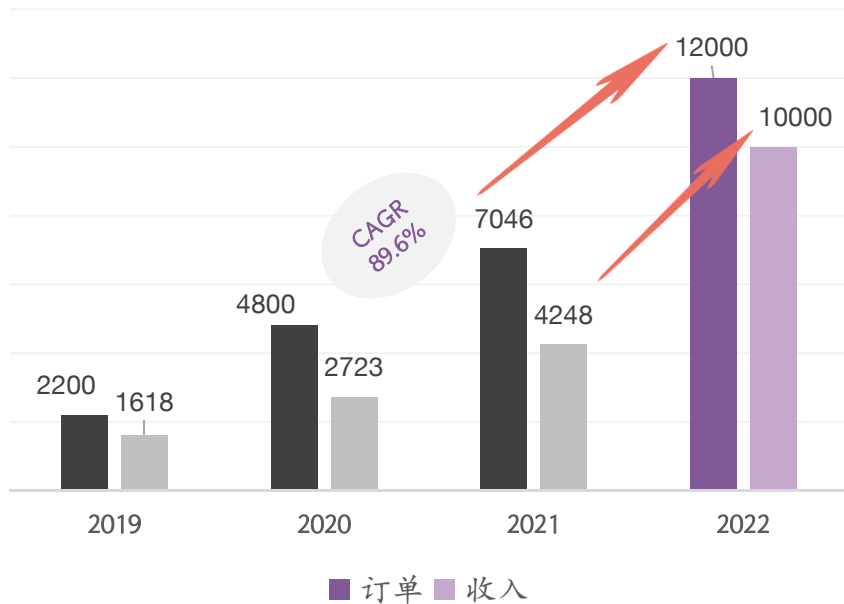
\*具体详见财务预测模型

8亿收入

60-80亿估值

# 业绩逐年翻倍，兰云增速大幅领先同业竞争对手

业绩逐年翻倍增长，22年迎来大幅跃进



2022年订单分布预测：



2022年业绩增长逻辑：

- **核心团队的扩充：**公司在2022年引入了多位核心销售成员，获取更多扎实的销售资源
- **销售渠道的打通：**兰云创始团队的背景使得2022年公司在华为、华三、运营商等渠道方面获得了大规模的突破
- **销售资质的获得：**军密资质的获取使得公司在部队领域的订单得到增长
- **行业口碑的裂变：**大兴机场、首发高速等标杆项目通过部委的认可得到了大规模的复制

本轮计划融资1亿人民币  
加强工具化、平台化、服务化、运营化集成建设



40%

产品研发



40%

市场拓展



20%

管理&其它



不可运维 → 可运维

运维效率质变飞跃

IPO确定性极高



唯一自动化溯源分析 + 安全服务

唯三全流量检测 + 云管端防护

历史四年业绩持续翻倍



创始人为华赛杭研所所长  
高层创业资源加持

千人团队、百条产品线管理经验  
华为、华三、运营商、政企军方  
高层资源

国家级标杆案例背书  
行业多样化规模放量

大兴机场态势感知平台  
厦门金砖会议国家级态势感知  
HJ军、W军、H军等  
首发高速全国交通标杆

东南大学战略加持  
联合W军共建实验室

- 共建研发
- 人才输送
- 战略投资&顶层辅助销售



# 感谢领导聆听

创新、专注、懂安全——愿与您携手共创辉煌

易建超：18611661166