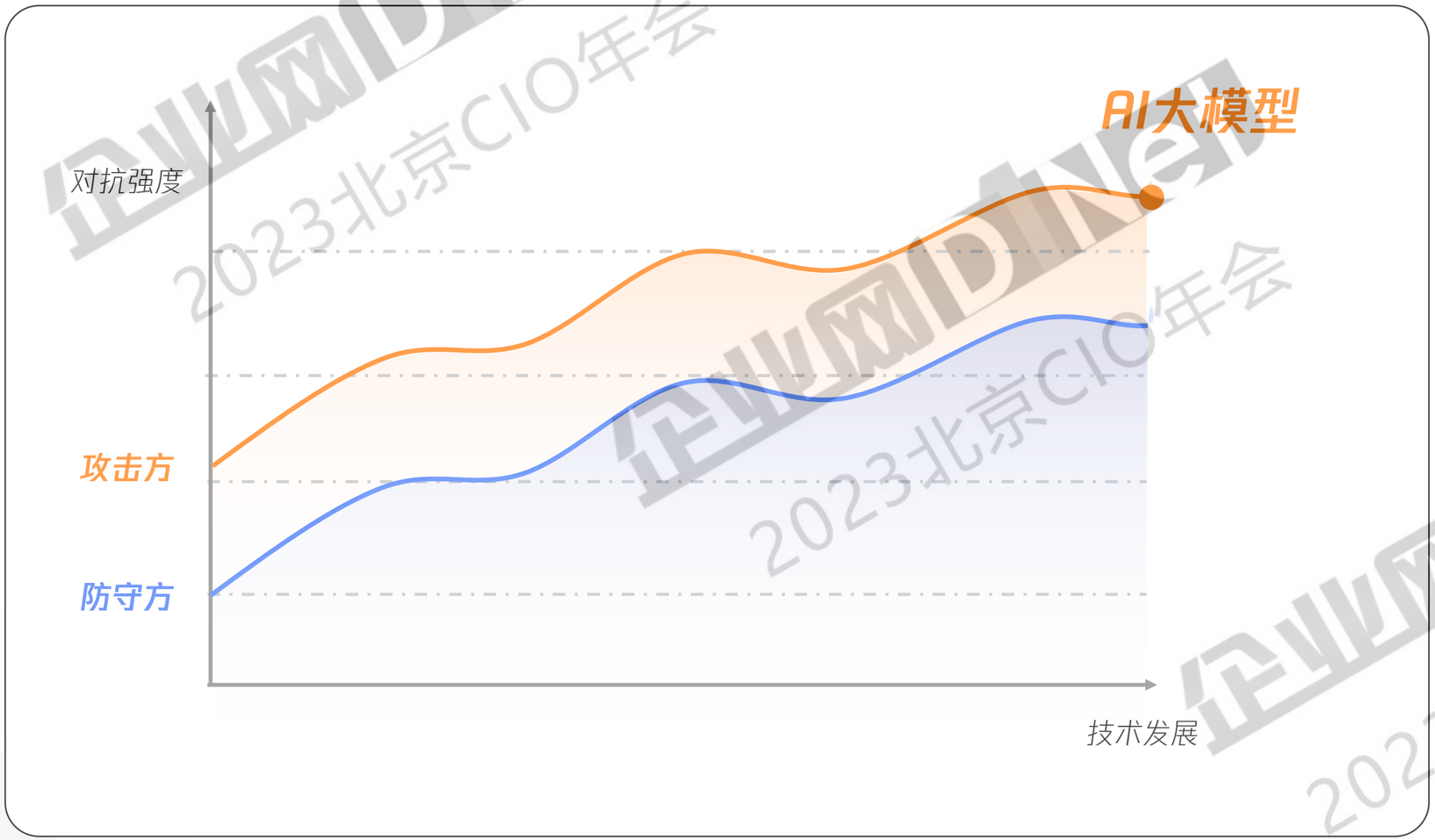
Tencent 腾讯 | 腾讯云 腾讯安全

大模型技术下
安全运营的应用和实践

腾讯云安全架构师 王倜

大模型“智能涌现”，开启新一轮“攻强守弱”



135%

攻击者利用生成式 AI
让社会工程攻击量增加了 135%

17%↑

ChatGPT发布后
钓鱼电子邮件的平均语言复杂度提升

1.69亿

ChatGPT发布后
钓鱼邮件大幅增加，环比增长260%

来源：Darktrace：2023年研究报告
Vade：2023年2月9日《2022年第四季度网络钓鱼和恶意软件报告》

智能化时代，企业面临四大安全挑战

反应窗口期缩短

- 黑客攻击从周→天→小时
- 传统回合制攻防变成即时战争

防御半径增加

数据量激增，暴露更多风险

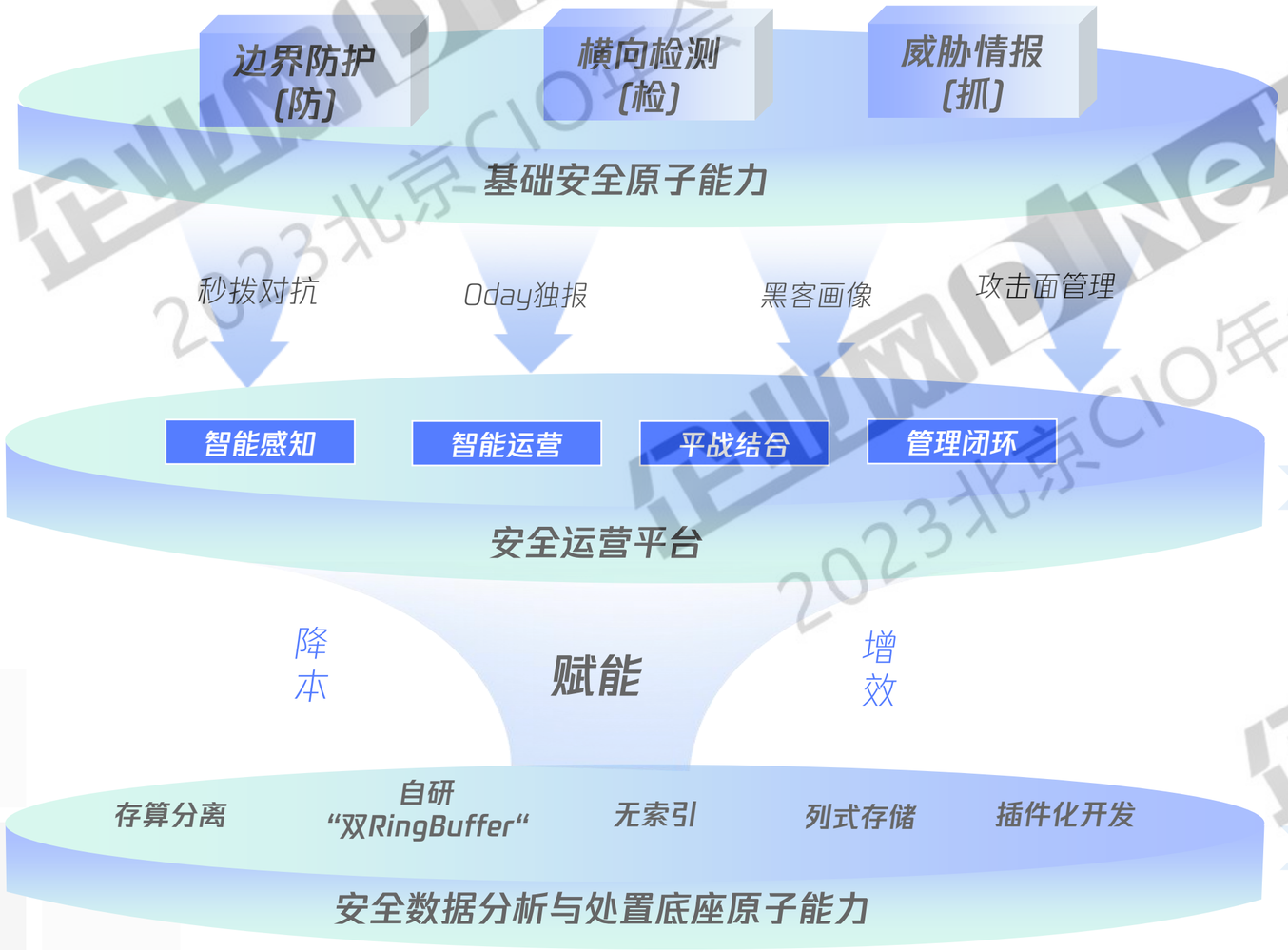
“情报库”失效

- AI随时随刻产出新行为/样本
- 传统基于“过去行为”预测“未来行为”安全策略失效

区分人和机器难度增大

黑灰产利用AI提升模拟真实用户行为的效率，企业难以辨别

实践之路：持续进化、强化保护的安全架构，让安全回归本质



技能进化

- 以串接独立防护--》联动式旁路防护
- 以防御为核心--》以检测为核心
- 以漏扫为安全检测--》以攻击面管理验证威胁

智力进化

- 依赖本地安全模型--》基于全球威胁情报的智能进化
- 平台跨网联动不足--》防、检、抓闭环
- 过去通报为主--》以赋能协作升级

算力进化

- ES索引2-3倍开销--》无索引和高压缩
- 安全平台数据封闭--》插件化赋能，建安全应用生态
- 实战攻防日志分析分钟级--》PB及秒级查询

API灵活联动传统安全设备,非侵入旁路阻断攻击行为，闭环处置（99.99%阻断率）

四大专项边界防护场景

实时阻断

- 实时监测，秒级响应（协议优化腾讯专利）
- 支持封禁策略100万条，支持IPv6，完美满足HW需要
- 支持第三方联动，提升整体攻防效能

秒拨IP对抗

- 利用AI算力+AI算法自动化方法，即实时提取网络流量中的行为模式作为指纹特征
- 动态生成黑指纹库，并基于指纹特征进行攻击判定及阻断
- 自动将同一秒拨IP群的攻击载荷快速聚合，结合可视化应对这类网络攻击。

热补丁

- 快速响应漏洞：无需等待开发厂商的补丁包，只需及时调整策略即可。
- 快速修复：无需重启系统，无须停机窗口，策略一旦调整完毕实时起效。
- 非侵入式：通过虚拟补丁方式修复数据库漏洞，无需更改数据库环境，无额外成本，大大减轻测试和部署补丁的工作。

反测绘

- 主流开源扫描工具指纹特征全录入
- 各类开源及非开源扫描工具行为特征自动优化
- 通过向测绘流量IP的客户端发送RST包或回假数据包进行反制

已有的安全产品不能阻断，联动API完成阻断

天幕提供了阻断API，能让客户以前的安全设备(生态厂商)接入天幕的阻断能力，帮客户整合了以前采购的安全产品，不造成浪费

领先的未知威胁检测能力对抗绕过与0day, APT检测实现攻击全面感知

- 联合安全实验室从攻击视角提供规则和AI检测模型，覆盖常见的绕过手段。
- 0day检测和横移检测能力突出；如通用规则检出 java反序列化漏洞0day，用友ERP 0day、域渗透攻击、变种webshell等。
- 本地动态沙箱，支持XP,win7, win10,linux等系统，对未知文件进行实时检测。
- 专家自定义策略管理，可调整精准度和覆盖度，专业用户可通过自定义做策略精细化运营。

（一）识别未知威胁能力

模型效果

数万测试样本

精确率: 99.67%

召回率: 99.03%

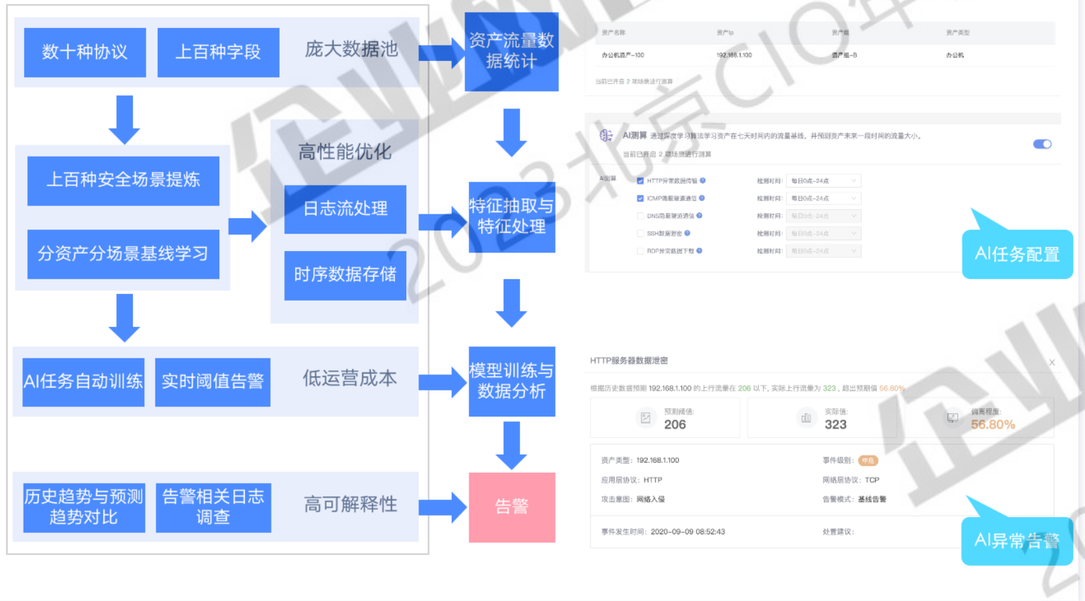
HW攻防实战

相比传统方案，提升20%检出率

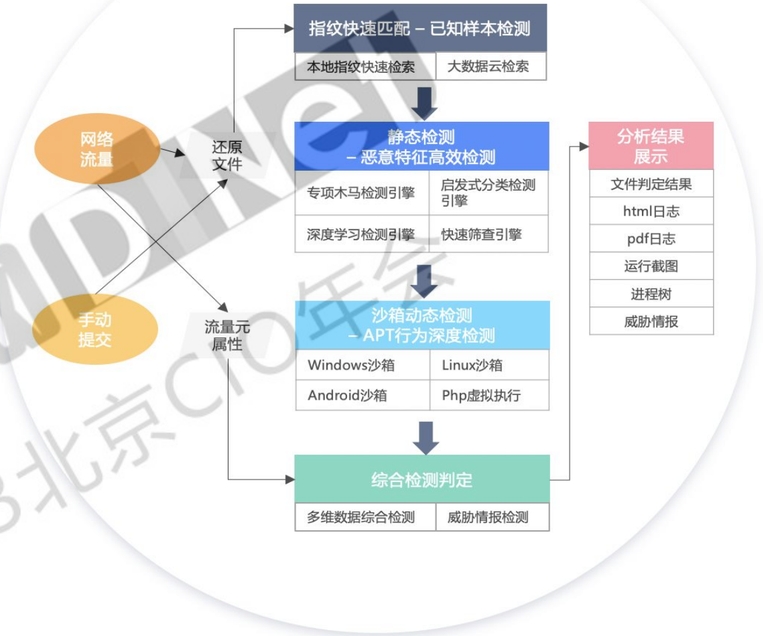
专利

基于人工智能的恶意流量文件的检测方法、装置及电子设备

（二）提升攻击检测能力



AI检测能力

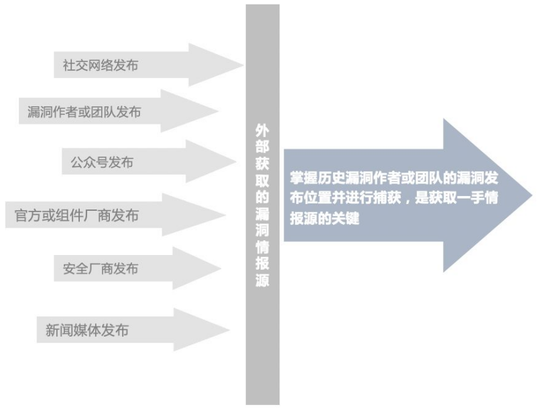


沙箱检测能力

结合腾讯安全玄武实验室域渗透研究成果，扩展东西向流量检测，覆盖域控攻击场景是QAX天眼的4.5倍：御界防御49种攻击手法，QAX天眼11种。

腾讯御界：数据情报分析，贡献一条日志，可以把敌人看的更清楚

- 最全的互联网漏洞监测机制，广泛获取最新的漏洞信息。
- 实验室共建高危漏洞共享机制，0day和1day漏洞发现更快。
- 结合腾讯威胁情报及时发现恶意IP、境外访问、失陷主机等。
- 涵盖云、PC端、移动端、实验室威胁情报体系，国内最大的威胁情报库。



已覆盖国内外500+个情报源

全球文件样本库	IP信誉库	域名信誉库	DNS信息库	第三方情报
• 总样本 150亿+ • 日均新增 900w • 白名单 100亿+ • 黑名单 40亿+	• 总数量 20亿+ • 日均新增 100w • 白IP数量 1亿+ • 黑IP数量 100w+	• 总数量 10亿+ • 日均新增 100w+ • 白名单 1亿+ • 黑名单 100w+	• DNS解析记录 100亿+ • 日均新增100w+ • 18年+Whois信息存储	• 每日抓取3000+全球情报源（博客，Twitter，Osint，安全厂商等等） • 每日监控暗网内敏感信息
腾讯云 • 承受针对国内头部互联网公司的攻击流量 • 网络攻击防护成功率超99.995% • 拦截国内最大的1.2T的DDOS攻击	**腾讯电脑管家** • 用户累计安装超过8亿 • 病毒检出235w/日 • 国内用户覆盖率40% • Google Virus Total首家沙箱分析系统供应商	**腾讯手机管家** • 中国市场份额第一，覆盖主流手机品牌。 • 移动安全软件市场份额第一 • 月活跃用户2亿	**全球杀毒评测** • 赛可达测试：从2016年至今荣获六次第一 • VB100测试：连续26次通过 • AVC测试：获得20个A+最高评级，国内唯一满分厂商	**腾讯全系产品安全保护** • 微信、QQ、邮箱、腾讯云、游戏、企业微信等产品URL、文件安全鉴定支持

腾讯安全

安全运营效果和效率需要持续智力进化

看不清风险：
Github、暗网、影子IT、互联网暴露

→ 从攻击者视角看清风险

- 攻击面管理
- 数据遥测
- 威胁情报

攻击多样化：
0day多发、恶意文件、域横移攻击、内部异常行为

→ 应对新型攻击和威胁检测

- 0Day漏洞防护
- 未知威胁防护
- 内部威胁与违规
- 文件沙箱

安全运营挑战：
告警多无法运营、检索分析性能低

→ 提升运营效率和效果

- 安全大数据湖
- 海量数据分析引擎
- AI算法/模型
- 安全专家知识

实时对抗需求：
缺乏实时对抗响应能力

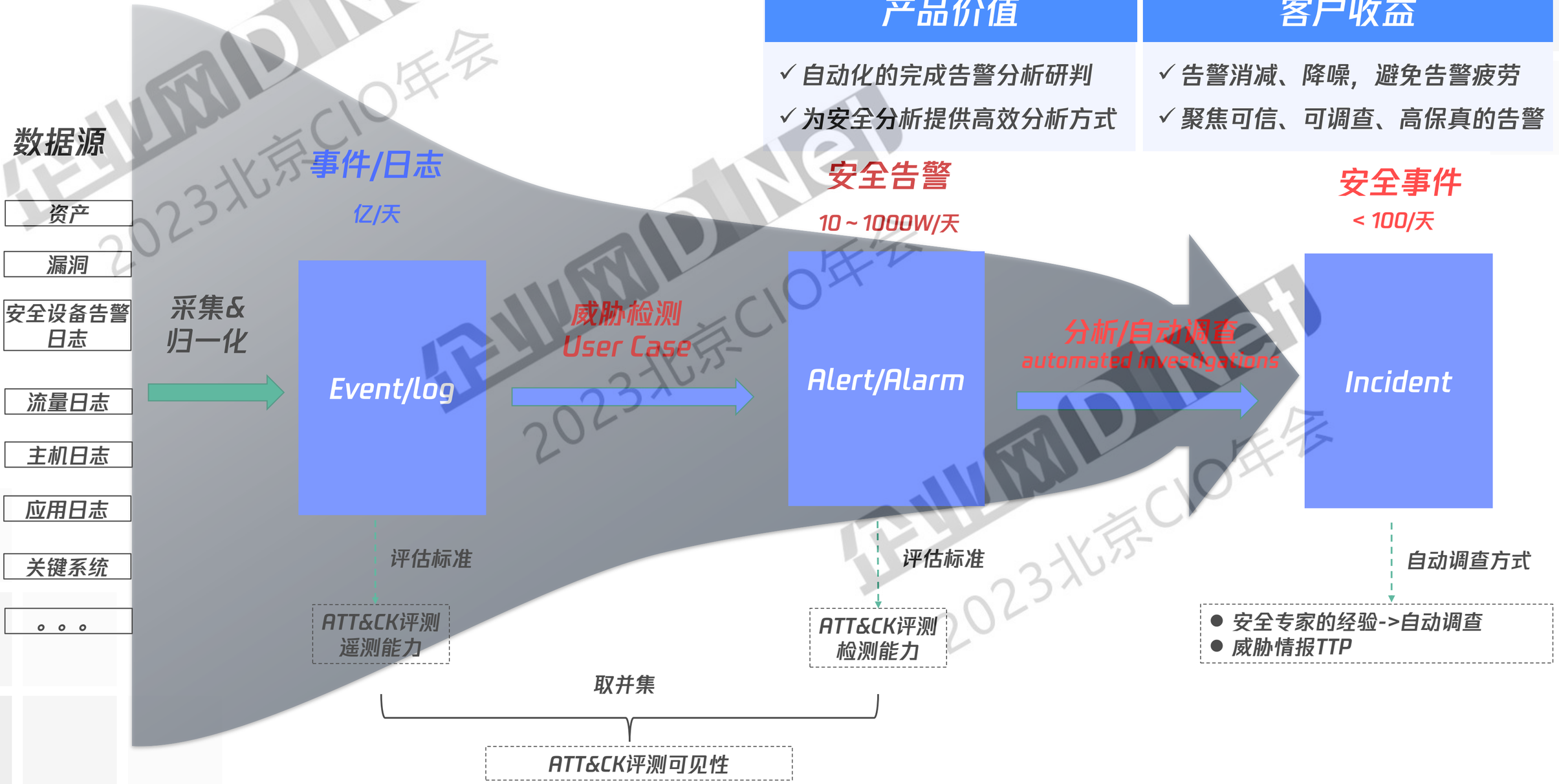
→ 提供敏捷响应能力

- “插件式”安全能力扩展
- 旁路阻断

腾讯安全

日志>告警>事件自动化自治系统，实现海量安全日志降噪

产品价值	客户收益
✓自动化的完成告警分析研判	✓告警消减、降噪，避免告警疲劳
✓为安全分析提供高效分析方式	✓聚焦可信、可调查、高保真的告警



腾讯安全

UEBA核心引擎的三大特性，带来灵活、智能的行为分析能力

UEBA典型场景

社工攻击
导致凭据泄露

漏洞攻击
导致设备失陷

黑客进入内网
进行渗透

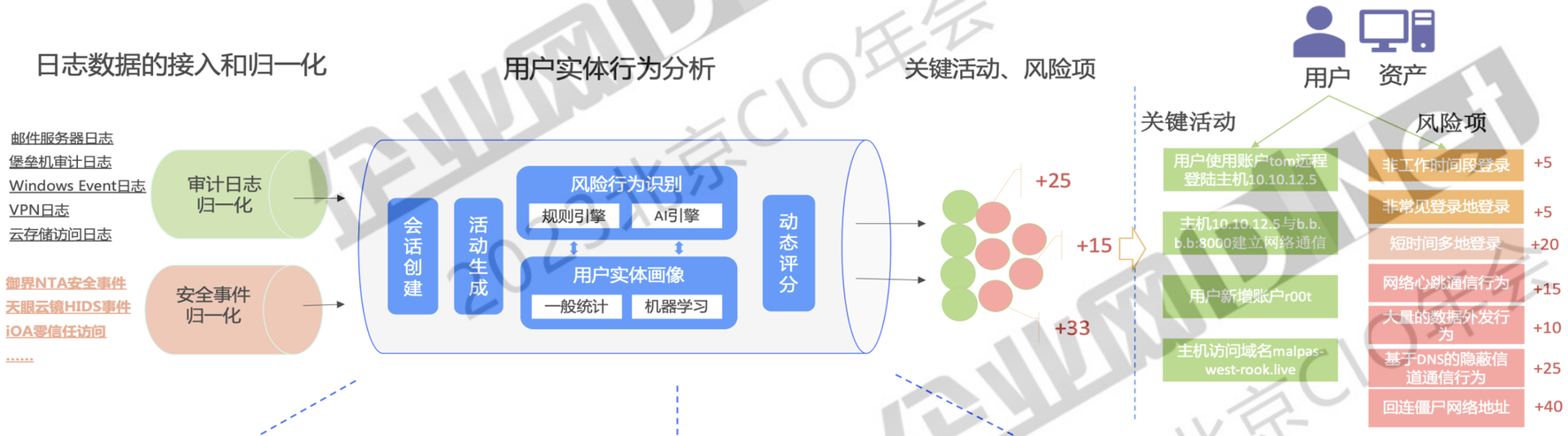
内部人员进行
数据泄露

产品价值

- ✓基于规则、画像、AI三大引擎
- ✓覆盖已知威胁，聚焦行为风险
- ✓自研风险量化算法，智能评分

客户收益

- ✓防范社工攻击
- ✓管控内部风险
- ✓降低安全运营难度



1 行为精准关联到UE

- 基于日志、HR信息，实现人、账号、设备的精准关联，并富化到行为日志，有效应对行为分析中动态IP、账号和设备隔离等挑战

2 大时间范围的行为分析

- 使用数学统计和机器学习对日志进行长时间范围的分析，形成用户实体画
- 克服规则匹配、小窗口统计等检测方法的局限性

3 灵活的安全场景扩展能力

- 基于内置安全场景模板，选择数据源即可新增安全场景
- 基于规则引擎、AI引擎新建一般安全场景
- 动态引用学习到的画像结果，配置基于规则、AI的智能分析场景

腾讯安全

基于新一代安全大数据分析与处置能力与安全运营平台底座结合，实现降本增效

新一代云原生高性能、分布式、专为日志分析打造的高性能底座，为用户提供数据源接入、采集、处理、存储、分析和检索等功能，具备“插件化”应用开发能力，上层应用可根据需求定制，并通过平台+APP+合作伙伴构建完整的日志数据应用生态体系。

高性能

列存储，向量化执行引擎。
无索引避免摄入时索引开销。

高可靠

数据多副本，支持多节点自动故障切换。

灵活弹性

分布式架构，灵活、可扩展，应对海量数据的挑战。

易使用、易运维

丰富的组件，采集、存储、可视化，以及运维监控。

易开发

REST API 、各种开发语言的SDK。
通过“插件化”的场景组装构建安全产品/应用。

腾讯安全

实现数据的高压缩，大大降低硬件资源成本，支撑应用灵活编排调用

某业务成本对比：在同等性能下资源消耗为ES的1/5，存储与服务器资源投入成本首年降低30%

日志平台	节点数量	节点配置
ES	7〔集群〕*10〔节点〕= 70	24核96G 10T
安全数据湖平台	20	64核128 G 7T

无索引

- 避免索引带来的成本开销
  ES索引大小是原始数据2～5倍，安全数据湖产生的摘要大小是压缩后数据的1/10

列式存储

- 相同类型压缩比高： 10～20压缩比
- 列中重复数据越多，压缩率越高
- 不同数据类型采用不同压缩算法，进一步提升压缩性能

支持COS

- COS支持容灾备份+冷数据存储，存储成本对比SSD节约88%

某客户业务全量数据
压缩比：16.92

某安全日志归一化表
压缩比：15.61

某流量数据表
压缩比：17.84

海尔集团多分支一体化安全运营中心项目

腾讯安全

腾讯威胁情报中心
（云端）

情报数据下发

客户诉求

- 多源数据集中存储与管理
- 构建内外部威胁情报体系
- 建立符合客户的安全分析
- 安全态势感知大屏可视化
- 对接内部系统做联动响应
- 落地一体化安全运营体系

实现效果

- 21个风险规则策略构建
- 多分支混合云统一监测
- 大幅提升安全攻防与运营能力

统一态势监控与运营

可视大屏呈现

态势感知大屏

安全数据

态势感知、统一资产、漏洞、事件运营

腾讯安全运营中心SOC

对接

集团总部已建系统

IAM　工单系统　防御系统

CMDB　漏扫系统　基线系统

账号、资产、事件、漏洞、资产数据订阅

账号、资产、事件、漏洞、资产数据订阅

账号、资产、事件、漏洞、资产数据订阅

xxx-二级单位

xxx SOC

流量日志、告警日志　事件、漏洞数据　资产数据　第三方日志、漏洞数据

流量检测
NTA

其他安全产品
主机安全、云堡垒机、云数据库审计等

第三方产品
防火墙、漏洞扫描器等

镜像流量

xxx网络

资产管理
CMDB

xxx-二级单位

xxx 云SOC

流量日志、告警日志　事件、漏洞数据　资产数据　第三方日志、漏洞数据

流量检测
NTA

其他安全产品
主机安全、云堡垒机、云数据库审计等

第三方产品
防火墙、漏洞扫描器等

镜像流量

xxx公有云

资产管理
CMDB

xx-二级单位

腾讯 云SOC

流量日志、告警日志　事件、漏洞数据　资产数据　第三方日志、漏洞数据

流量检测
NTA

其他安全产品
主机安全、云堡垒机、云数据库审计等

第三方产品
防火墙、漏洞扫描器等

镜像流量

腾讯公有云

资产管理
CMDB

深交所态势感知项目

项目背景及客户需求

- 项目背景：目前深交所及下属单位的安全告警事件分散、不同类型的安全告警事件主要依靠人为流程和手段进行协同，难以在海量、分散的流量及日志中去挖掘有效的攻击信息，溯源攻击链及支撑安全事件的处理，无法有效应对高强度的攻防对抗时期。
- 尤其看重：1、多级部署；2、威胁预警，3、威胁情报；4、安全运营能力。5、快速响应能力

方案价值

- 预测
  - 通过内部威胁预测、外部威胁情报等手段，进行平台暴露面分析，监控外部威胁，实现攻击预测、提前预防的目标；
- 防御
  - 面对持续攻击，降低受攻击面，实现“攻击减速”的目标；
- 检测
  - 针对XX交所业务系统，进行7*24小时在线检测和响应，减少威胁停留时间，及时发现并控制事件，防止事件升级；
- 响应
  - 深度威胁分析，联动响应与处置，并结合安全服务人员的实时监测，对发生的重大安全事件进行回溯分析，实现及时处置、止损、追踪溯源的目标。

解决方案

网络安全态势感知系统采用三层架构实现多级部署能力，建设闭环安全运营体系。

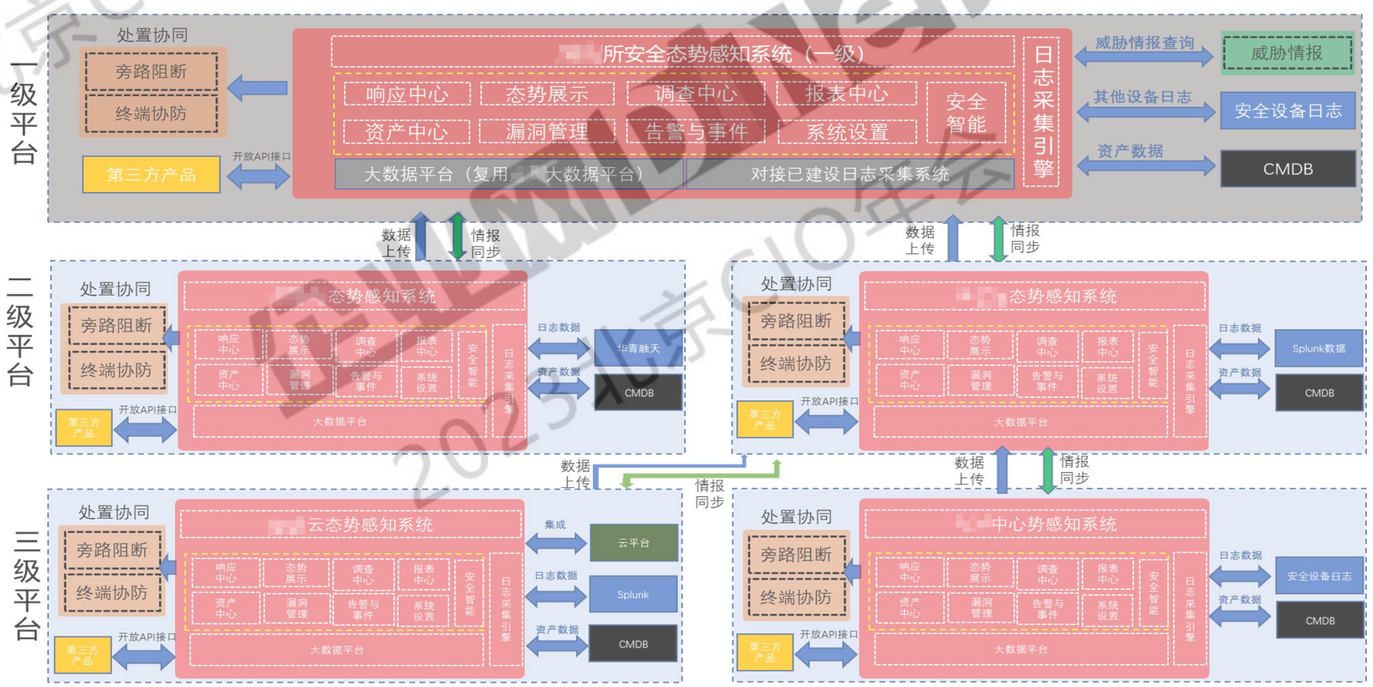
查：通过**御界**，覆盖网络入侵〔南北向为主、部分东西向〕监测、流量日志存储需求

防：通过**天幕**，覆盖多产品策略集中响应，快速封堵攻击来源

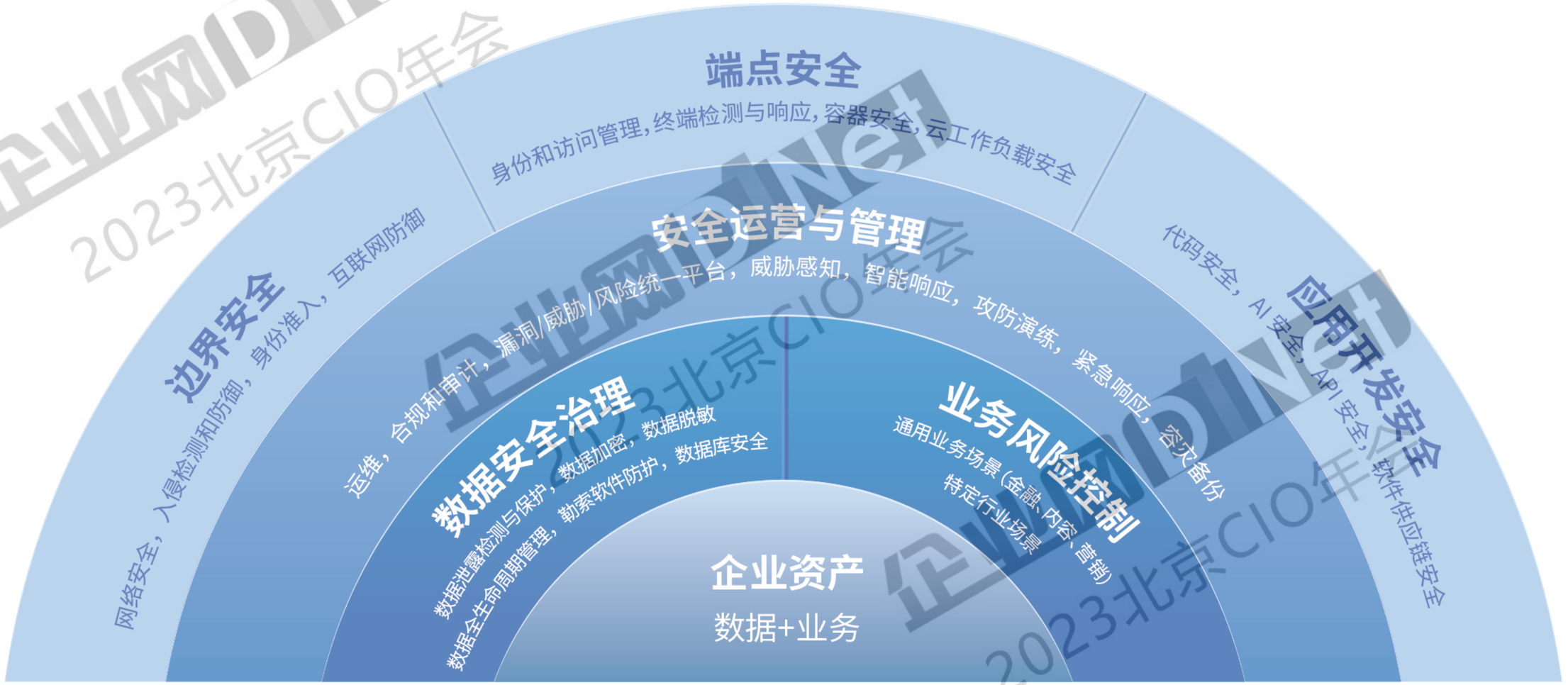
控：通过**御见**，覆盖综合态势，多租户租户视角需求

情：通过**威胁情报**，预测各方攻击态势，提前进行防护

服：通过**腾讯安全团队**，统筹各方人员，发挥1+1>2的能力优势



腾讯安全构建企业数字安全免疫力，守护企业生命线



静态安全 ➡ 弹性、自适应、可扩展

治已病 ➡ 治未病

被动防御 ➡ 主动安全

Tencent 腾讯 | 腾讯云 腾讯安全

THANKS

谢谢观看