百度安全商业产品简介

-2023.12-

百度智能云 | 百度安全 有AI更安全

百度公司概况 | 战略业务：三大增长曲线 多引擎增长

积极稳健的成熟业务

移动生态

百度APP

6.57亿MAU

百度APP | 全网领先的以信息和知识为核心的综合性内容和服务平台

百度APP　百家号　智能小程序　百度营销　好看视频　百度问一问

有驾　百度百科　百度贴吧　百度联盟　度晓晓

高速增长的新兴业务

智能云

百度智能云

中国 TOP1

中国排名第一的AI公有云服务商

中国 TOP4

稳居中国四朵云之一增速远超行业平均水平

智能制造　智慧城市

智慧能源与水务

智慧金融　更多产业

基于新战略“云智一体，深入产业” 发布“云智一体3.0”架构

云智一体3.0形成了“芯片-框架-大模型-行业应用”的智能化闭环路径，做到端到端的优化

引领行业的前沿业务

智能驾驶与其它增长计划

apollo

全球 TOP1

全球最大自动驾驶出行服务商

全球 TOP1

自动驾驶总专利族数量全球第一

中国 TOP1

AI专利申请量及授权量中国第一

中国 TOP1

智能音箱出货量中国排名第一

小度

中国 领先

中国领先的云端全功能AI芯片

昆仑芯 KUNLUNXIN

全网 领先

全网领先的中文医疗健康科普平台

百度健康

领先技术

昆仑芯2代

第二代云端通用自研AI芯片

文心大模型

千行百业AI开发的首选基座大模型

飞桨

中国深度学习平台市场综合份额第一

百度智能云｜云智一体，深入产业

应用层
行业与应用

行业应用：

通用应用：

模型层
文心大模型

NLP大模型　CV大模型　跨模态大模型　生物计算大模型　行业大模型

框架层
飞桨

AI 中台

数据标注　部署运行　模型开发　模型管理　知识生产　知识管理

芯片层
昆仑芯

百舸·AI异构计算平台

高速互联　AI服务器　GPU虚拟化　AI作业调度　弹性训练　加速套件

2019　2023

云智一体1.0　云智一体2.0　云智一体3.0

百度安全 | 智能安全的新实践、新范式

百度安全简介

百度安全是百度公司旗下，以AI为核心为基础打造的安全品牌，是百度23年安全实践的总结与提炼。基于基础安全、数据安全、业务安全、车与IoT安全四大产品矩阵，业务覆盖百度各种复杂业务场景，同时面向合作伙伴输出安全产品与行业一体化解决方案，涵盖智能制造、智慧能源、智慧政务、智慧金融、智能汽车等领域，全面探索AI时代的新实践、新范式。

面向行业生态，一方面，发挥技术能力打击包括电信网络诈骗、赌博、隐私窃取在内的各类违法犯罪行为，协助公安机关破案数百起，涉案金额达数亿元人民币，一方面，以技术开源、标准驱动为理念，联合生态合作伙伴推动AI时代的安全生态建设。

百度安全产品矩阵｜云智一体，护航产业

服务行业

政务　互联网　金融　运营商　文娱　汽车　医疗　能源　制造

产品矩阵

基础安全

主机安全管理　安全检测服务　应用防火墙
DDoS防护服务　威胁狩猎平台　云堡垒机
流量审计分析　密钥管理服务　SSL证书
智能安全专家　AI模型安全评估　云安全专家服务
安全大脑

数据安全

点石隐私计算平台　智能数据安全网关
联邦学习平台　数据分类分级平台
数据安全沙箱　数据库审计
机密计算平台　数据脱敏　数据水印
图数据库及知识图谱

业务安全

智能风控　APP隐私合规　内容安全
号码安全服务　人脸认证安全　流量反爬
应用加固与安全检测　网址安全　安全短网址
大模型安全解决方案

车与IoT安全

整车威胁感知　车机攻击防护　安全OTA
数字证书　自动驾驶安全测试
车端数据合规

● 高成熟度标准产品

企业实践

安全防御体系　数据隐私合规　业务安全风控　等保合规

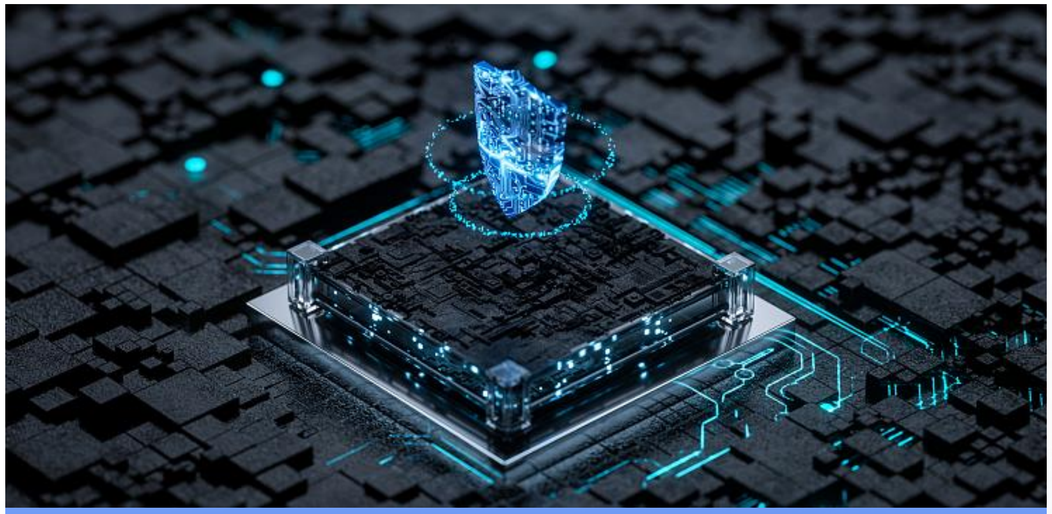
核心优势

全栈安全攻防实验室　全域安全大数据分析　大规模深度学习技术应用　安全大模型基础设施

生态共建

百度安全应急响应中心　政产学研合作　代码开源开放　威胁情报共享　黑产打击协同

百度安全 | 使命与愿景



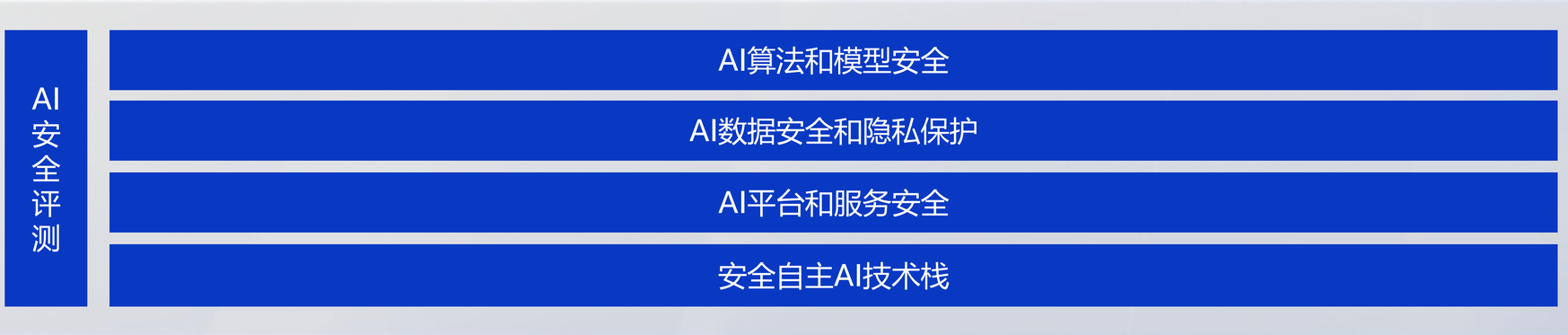
使命：让百度更安全 让用户更放心

愿景：成为深谙业务的智能世界安全引领者

百度安全技术优势 | AI安全底座 x 安全AI底座

AI Infra for Security
（AI安全底座）

Safe and Secure AI Infra
（安全AI底座）



百度安全 | 标准引领发展，认证保障合规

- 主要组织涵盖：国际级ISO/IEC、国家级TC260、行业CCSA、团体TAF等，主要有23家
- 累计参与标准编制353个，标准发布101个，在研标累计252个

  -其中国标标准8个，国家标准60个，国家标准研究2个，行业标准116个，团体标准65个，地方标准2个

  -网络数据安全相关标准68个，国家标准26个，行业标准33个，团体标准7个，地方标准2个
- 体系类资质认证共85项，其中网络数据安全类共10+项
- 产品类测评及认证共89项，其中数据安全类共10+项

《信息安全技术 生成式人工智能安全总体要求》
《信息安全技术 生成式人工智能预训练和优化训练数据安全规范》
《信息安全技术 生成式人工智能人工标注安全规范》
《信息安全技术 互联网信息服务深度合成安全规范》
《信息安全技术 敏感个人信息处理安全要求》
《信息安全技术 关键信息基础设施安全测评要求》
《信息安全技术 移动互联网应用程序（APP）个人信息安全测评规范》
《信息安全技术 关键信息基础设施网络安全应急体系框架》
《信息安全技术 关键信息基础设施边界确定方法》

部分重点标准参与情况

首批DSM数据安全管理认证的企业

国内首家获得DSMM四级的企业

数据安全治理能力评估优秀级

百度安全

有AI更安全

百度DDoS防护产品

DDoS防护产品-需求背景与攻击手法

DDoS （Distributed Denial of Service）

分布式拒绝服务攻击：控制2个或2个以上的机器向目标发起攻击，让其系统无法提供正常服务。

- 流量/反射攻击

简单粗暴，通过发起海量网络流量堵死网络出口

- CC攻击

高QPS并发攻击像网站等动态请求业务，拖死主机、数据库资源

- 混合攻击

以上两种加上其他黑客应用攻击如SQL注入、XSS等全方位多维度攻击

上述目标是要把受害者的在线业务搞跨！

DDoS防护产品-典型应用场景

1. 企业重大活动保障

当企业有重大活动时，可以提前启用DDoS云防防护，防范重大活动中可能出现的DDoS攻击行为，保障活动的安全进行。

2. 高风险业务常态防护

业务遭受超量DDoS攻击时，会导致网络延时上升、服务器资源耗尽、服务中断、客户流失，对于高风险业务，可以常态化的处于云高防之下，保障业务的稳定。

3. 本地云端联动防护

在机房署本地防御系统，当遇到小流量DDoS攻击时本地系统进行防御，攻击超量时，自动完成云防防御切换，提升防御效率。

DDoS高防IP简介

产品交付物

是一项基于SaaS的服务，用来防御各类大规模或超大规模的DDoS攻击，并提供数据报表展示攻击防御情况

付费形式

基础保底（按月、按年）防护套餐
+攻击超出保底弹性计费（按天）

适用的客户网络环境

- IDC环境（托管、自建）
- 云主机环境（百度云、阿里云、AWS等）
- 混合云

适用的客户业务

- 网站、 APP、游戏
- 视频（点播/直播）
- 金融
- 物联网（MQTT协议，需私有化部署）

产品优势-更强的防御技术，更低的拥有成本

1. 实时监测秒级防御

- 独有智能高敏数据包比例模型专利算法
- 最快100ms发现流量攻击，秒级执行防御

2. 完整联合防御方案

- 私有化部署本地防御系统，根据攻击量级联合高防、运营商分层防御
- 与智能云上EIP基础防护联动，超量攻击自动高防防御

3. 多维度精确缓解CC攻击

- 特有智能分析系统，实时提取攻击特征
- 辅助全网IP威胁库、攻击IP进行恶意请求拦截

4. 无限制防护，成本更低

- 高防CC防护量级无限制
- 支持全力防护方案，一站解决全部防御难题

DDOS防护产品-案例

某政企客戶：智能云EIP被超量攻击自动切入云高防防御

某政企客户业务平台，全部基础资源由智能云提供，包括BCC、BLB、EIP、数据库等，EIP默认仅具备5Gb的基础DDoS攻击防御能力，需要在遭受超过5Gb的攻击后，依然可以有效防御，确保业务可用。

智能云EIP被攻击：

- ✓ 小于5Gb由基础防护进行防御
- ✓ 超过5Gb攻击通过修改域名解析至高防IP，切入高防防御
- ✓ 云高防回源至客户源站EIP或备用EIP，完成正常用户数据交互

应用的产品：

- ✓ DDoS基础防护(EIP免费5Gb)
- ✓ DDoS高防IP

某游戏客户：常驻云高防防御

某游戏客户，经常被流量或CC攻击。平均每月超过10次，常常造成游戏掉线、无法登录。需要满足全国覆盖性能要求的防御能力，没有攻击时保证用户的访问速度，发生攻击时依然可以保证用户可正常快速的访问。

常驻高防防御：

- ✓ 30+线BGP线路，保证全国覆盖性能
- ✓ 毫秒级攻击监测秒级防御减少攻击影响，保证游戏不掉线
- ✓ 定制协议防御，非法请求不透过

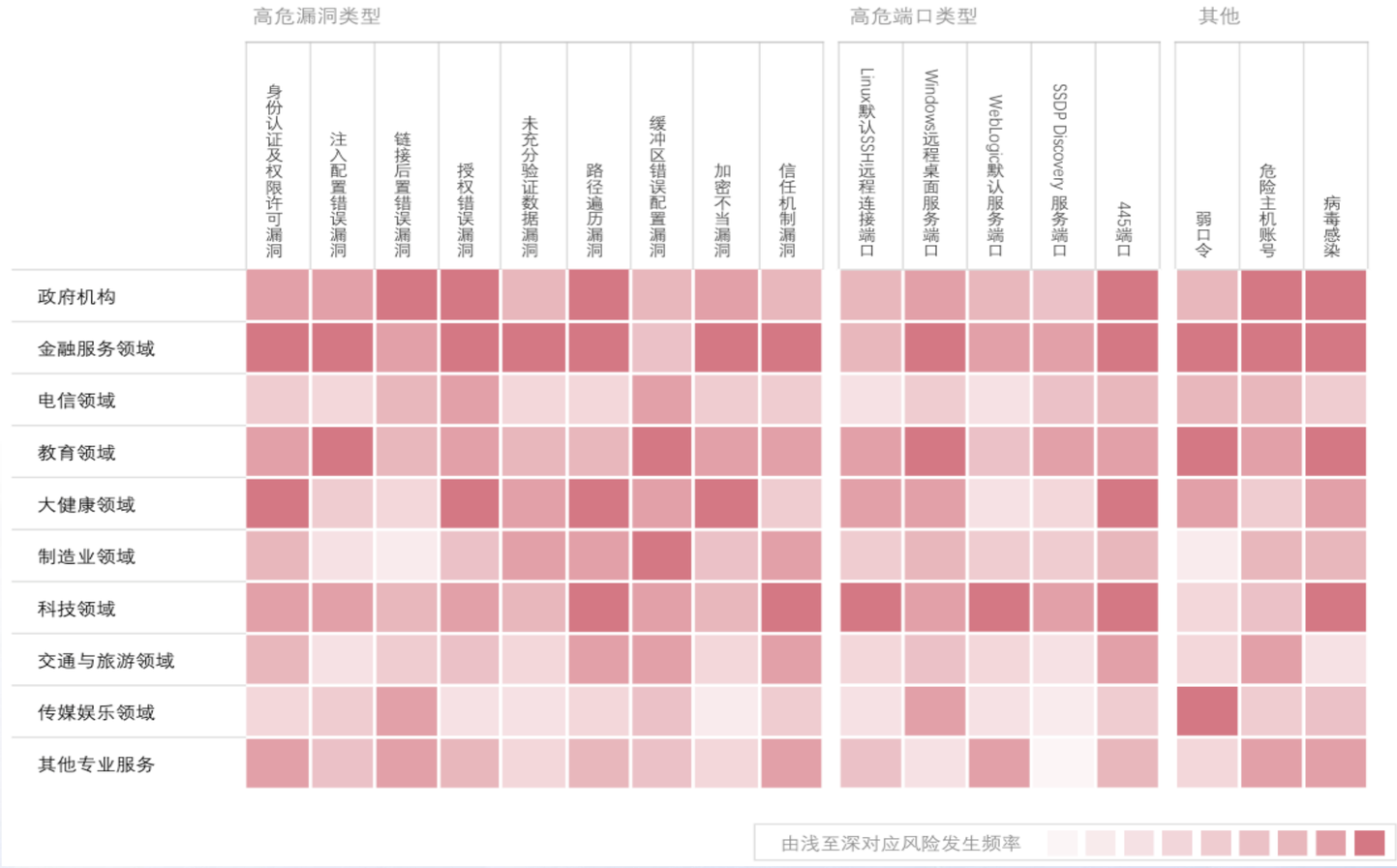
应用的产品：

- ✓ DDoS高防IP

百度主机安全产品

需求背景：主机安全威胁持续扩大

- 随IT产业和云服务市场快速升级扩容，**多云、跨云（公有云、私有云、混合云、容器云）**网络环境日趋复杂，**云主机攻击面持续扩大。**
- 多云环境下，云主机系统遭受恶意攻击的频率上升，**云主机被成功入侵平均时长缩短至约20小时。**
- 带有**开放端口和漏洞**的云端主机成为黑客攻击的首要对象。



数据来源：沙利文《2020年中国云主机安全市场报告》

云主机面临的**安全漏洞**包括**资源管理问题、代码失误、配置错误、代码注入等**，补丁修复缺失的**资产漏洞**成为入侵突破口。云主机端存在**大量易受攻击的资产端口**（包括远程连接服务端口、远程桌面服务端口、数据库端口、邮件服务端口等），亦面临较高的**勒索病毒及病毒变种攻击**风险。此外，**云主机软件弱密码、高危账号**（开放Root权限）、**补丁修复不及时**等问题使得**恶意网络攻击行为潜在控制面持续扩大。**

百度主机安全产品简介及产品架构

主机安全（HOSTEYE）是百度面向企业客户推出的云主机安全产品，**能够全面评估云主机的资产风险，快速建立云主机安全防护体系，助力客户满足云主机等保合规要求**，广泛应用在金融、交通、能源、互联网等行业。

应用场景

主机安全场景

安全合规

- **等保合规：**满足等保防护要求，提供的安全能力，如防病毒、入侵检测
- **行业合规：**诸如电力行业、运营商自身安全需要所固化的基线合规

安全运维

- 围绕资产、配置、漏洞、补丁的安全能力，如资产梳理、漏洞检测、配置核查等

安全对抗

- **应急响应：**勒索、挖矿病毒防治等
- **护网行动：**实战化的攻防演练
- **重保安全：**大型活动、节日的高级别安全检查与防护

优势特性

多云集中管控

混合云
私有云、公有云、IDC
集中管控

全方位主机防护

病毒查杀
入侵检测、漏洞扫描、基线核查

轻量级客户端

客户端
资源消耗与安装包
极小

高稳定性，高可用性

百度智能云
10万+
主机安全防护实践

金融行业客户案例

客户背景：

XX金融云为银行及各金融机构提供新一代互联网银行、银行核心系统、支付平台、新一代客服中心、票据平台、信贷平台等云服务，期望通过主机安全建设降低金融云内资产风险。

客户痛点：

服务器内存在网站后门、恶意漏洞；

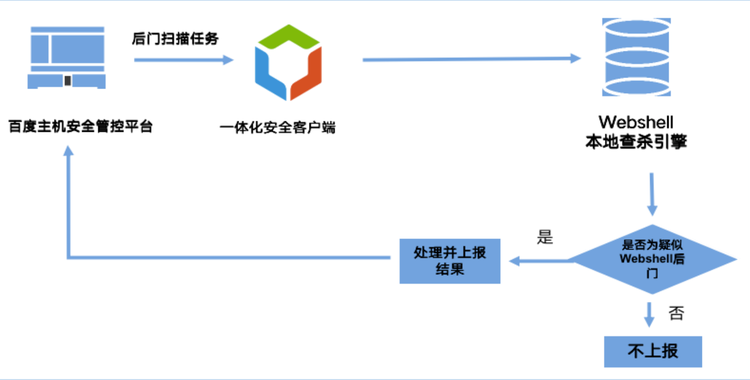
服务器内资产繁杂，难以进行精准管理。

使用效果：

实时检测网站后门、木马、蠕虫、挖矿、反弹shell等恶意行为；

能够及时发现服务器漏洞，识别潜在风险；

帮助用户梳理自身服务器资产。



制造业客户案例

客户背景：

某集团是中国领先的汽车制造商，百度 ABC stack 专有云行业版为某集团全世界的分支机构提供服务。期望通过主机安全建设，进行病毒查杀与异常登录管理等防护。

客户痛点：

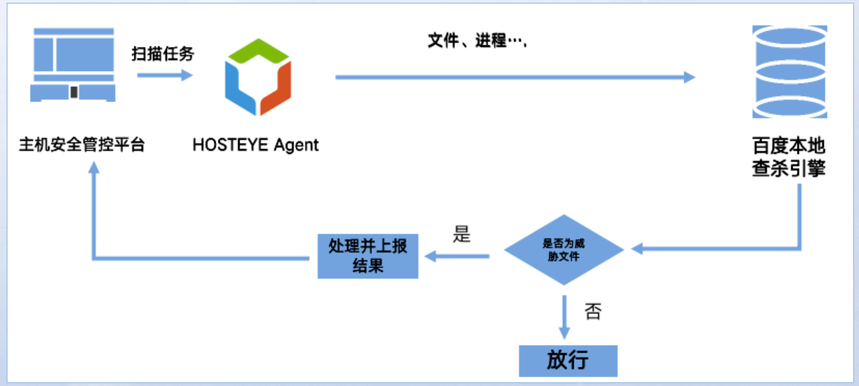
主机安全存在恶意进程风险；

账号登录管理不足，暴力破解、异常登录、异地登录等问题突出。

使用效果：

对恶意进程进行了有效查杀；

检测攻击者的暴力登录行为，及时封锁攻击源头，帮助用户规范登录行为，发现异常登录，及时告警。



百度应用防火墙WAF产品

WEB安全风险在哪?

百度安全总结当前WEB安全风险分为以下四个方向，企业独力面对需要投入大量成本，且不能保证收效。

- 服务器系统漏洞
- 中间件漏洞
- 代码本身漏洞

- 弱口令
- 安全策略无配置
- 应用权限越界

- 企业数字化转型
- 业务上云
- 使用大量SaaS

- 攻击工具泛滥
- APT组织增多
- 攻击成本低收益高

百度WAF功能一览

高效WEB攻击防御

独家自研规则引擎+AI业务自学习+语义引擎三管齐下，消灭防护死角

灵活的自定义规则

对于内置规则可灵活定义工作模式，精细到具体每一条漏洞规则，更可以根据业务实际需求自定义规则组合

网络资产全面纳管

对于公有云、私有云、混合云和本地IDC的资产均能接入流量，统一平台管理网络资产

详细的数据报表

企业可根据需求，自定义报表模板，一键生成报表，可精细化到每一条攻击报文

灵敏智能拦截

多维度自动化处置，可感知网络攻击并自动化拦截。同时内置AI业务学习模型，可积累业务数据并自动学习，优化防护能力

API网关/CC防护/反爬虫/防盗链（内测）

主动发现流量中API信息，进行URL级阻断。基于内置CC防护规则缓解HTTP Flood。基于用户指纹及行为特征阻击爬虫访问和盗链行为。

百度威胁情报数据共享

百度日常业务积累海量数据，包括IP信息库、设备信息库、社交信息库、攻击工具特征等

网页防篡改/敏感信息防泄露

锁定重要页面内容，防护页面内容浏览时不会被篡改。检测流量中身份证、银行卡、手机号等敏感信息，自动脱敏

百度WAF产品优势

企业级WEB安全防护

保障企业网站安全，有效防御各类WEB风险和攻击。荣获OWASP WAF攻防大师赛第一名好成绩。

满足等保合规要求

根据等保合规要求设计，全面满足等保防护和审计需求

灵活部署满足各类网络环境

支持软件、硬件不同的模式，对于公有云、私有云、混合云均可部署

简化安全运维工作

为企业安全运维赋能，帮助企业客户实时了解WEB安全情况，及时做出调整和规划安全资源分配

案例-某省公安厅网络安全防护项目

业务诉求：

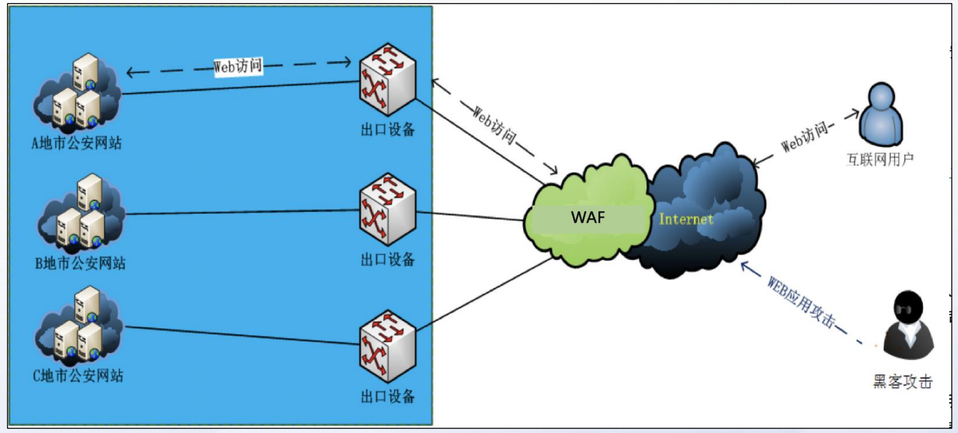
- 通过对部分省内各地市公安网站网站进行安全检测发现存在代码级的安全漏洞，省内各地市公安网站的安全防护措施都明显不足。
- 黑客可轻松获取网站的域名解析IP地址和服务器所在地，通过服务器所在机房对网站发起攻击。

合作价值：

发现目前业务的安全风险，解决公安网站的安全问题，保证网站和业务系统的可持续的安全运行。

解决方案：

本方案构筑了基于云计算的网站安全防护系统，实现对全省公安网站和信息系统的集中统一管理。



核心技术及产品：

- **百度WEB应用防火墙 度御关WAF**

以网站替身的形式为网站拦截各种SQL注入、XSS跨站、网站挂马、篡改、拖库等黑客攻击，并做到实时更新防护策略，第一时间防御各种0day漏洞，有效保护用户源站安全。

- **渗透测试/应急响应**

当发生黑客入侵、DDoS、数据窃取、木马病毒等事件时，提供包括抑制止损、事件分析、业务损失评估、系统加固、事件溯源的应急响应服务，降低安全事件对企业自身的影响与损失。

案例-某互联网教育企业

业务诉求：

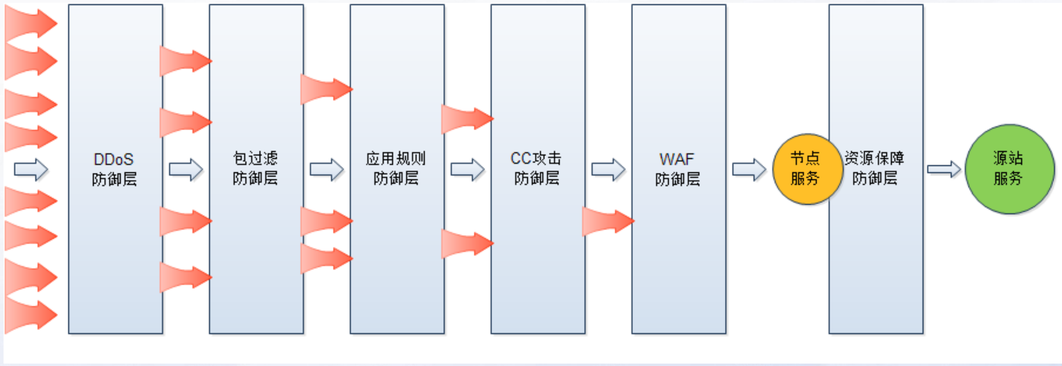
- 客户聚焦K12视频在线教育场景，尤其要保障在高峰的上课时间段保证业务系统流畅无卡顿。
- 业务系统中有核心的客户个人隐私数据，需要保证数据安全，防止黑客非法入侵服务器盗取。

合作价值：

- 成功的阻断了竞争对手或黑客的恶意大流量攻击，给予了客户良好的业务体验，提高了客户复购率。
- 保护客户数据资产安全，个人隐私数据不泄露，为业务系统公信度持续上升提供了有利保障。

解决方案：

- 在敏感时间段接入云抗D系统，将DDoS攻击化解在专业的第三方抗D中心内，保证了业务可用性。
- 在业务系统前部署WAF产品，阻断黑客攻击流量的同时保证正常业务流量通过。



核心技术及产品：

- **百度WEB应用防火墙 度御关WAF**

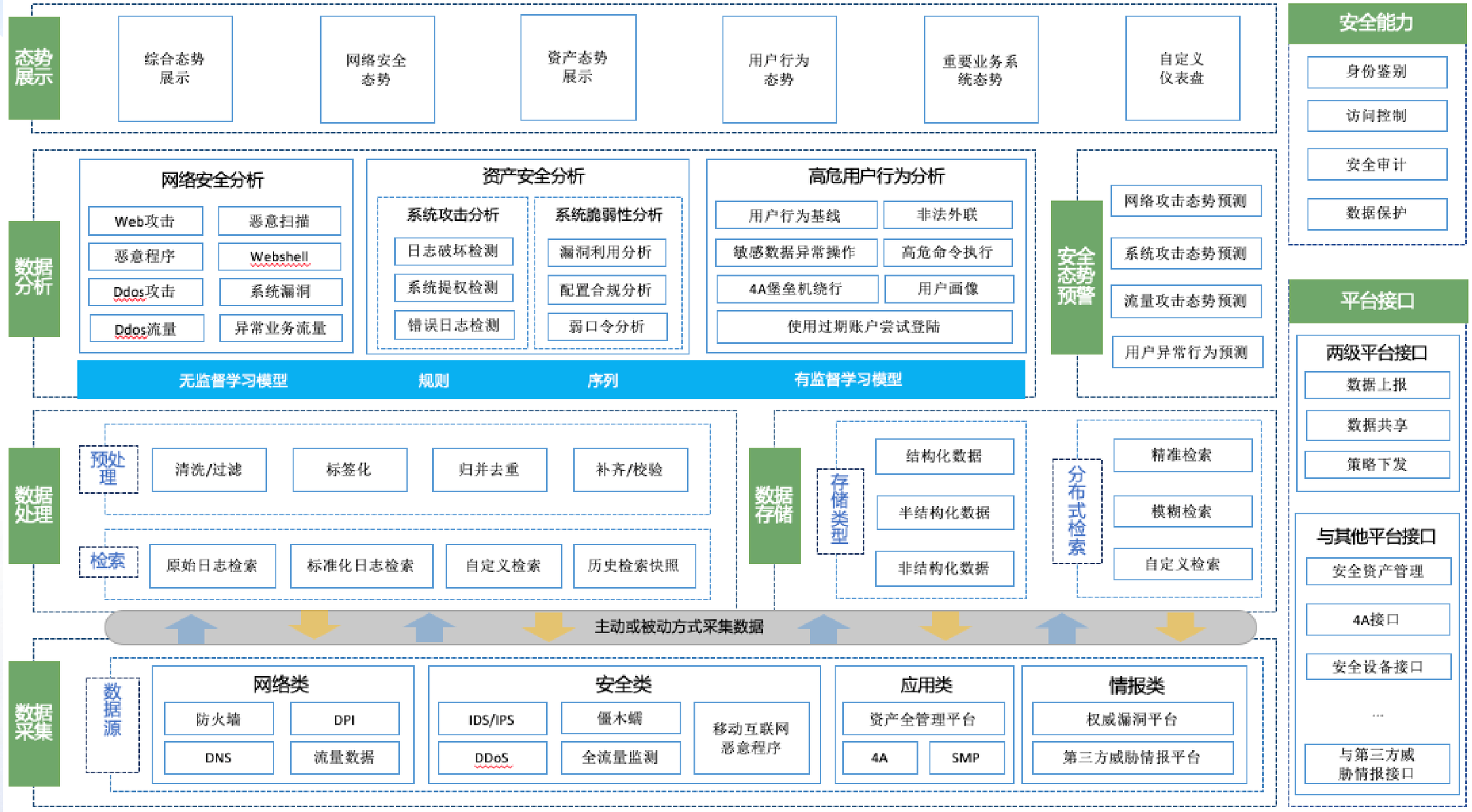
以网站替身的形式为网站拦截各种SQL注入、XSS跨站、网站挂马、篡改、拖库等黑客攻击，并做到实时更新防护策略，第一时间防御各种0day漏洞，有效保护用户源站安全。

- **DDoS防护**

具备1Tbps抗D能力，采用云端防护模式，客户无需购买或租用硬件清洗设备，按需使用；同时，百度安全团队全程支持防护；有效防御各类攻击，挽回因网站或业务服务中断造成的诸多损失。

百度安全大脑

百度企业安全大脑业务能力架构



百度企业安全大脑业务模块

安全数据管理

安全数据的集中采集、处理和存储，实现安全数据的汇聚和集中化管理

安全场景分析

场景化的分析能力，提供基于多种数据的安全分析场景，以实现分场景的安全告警和预警

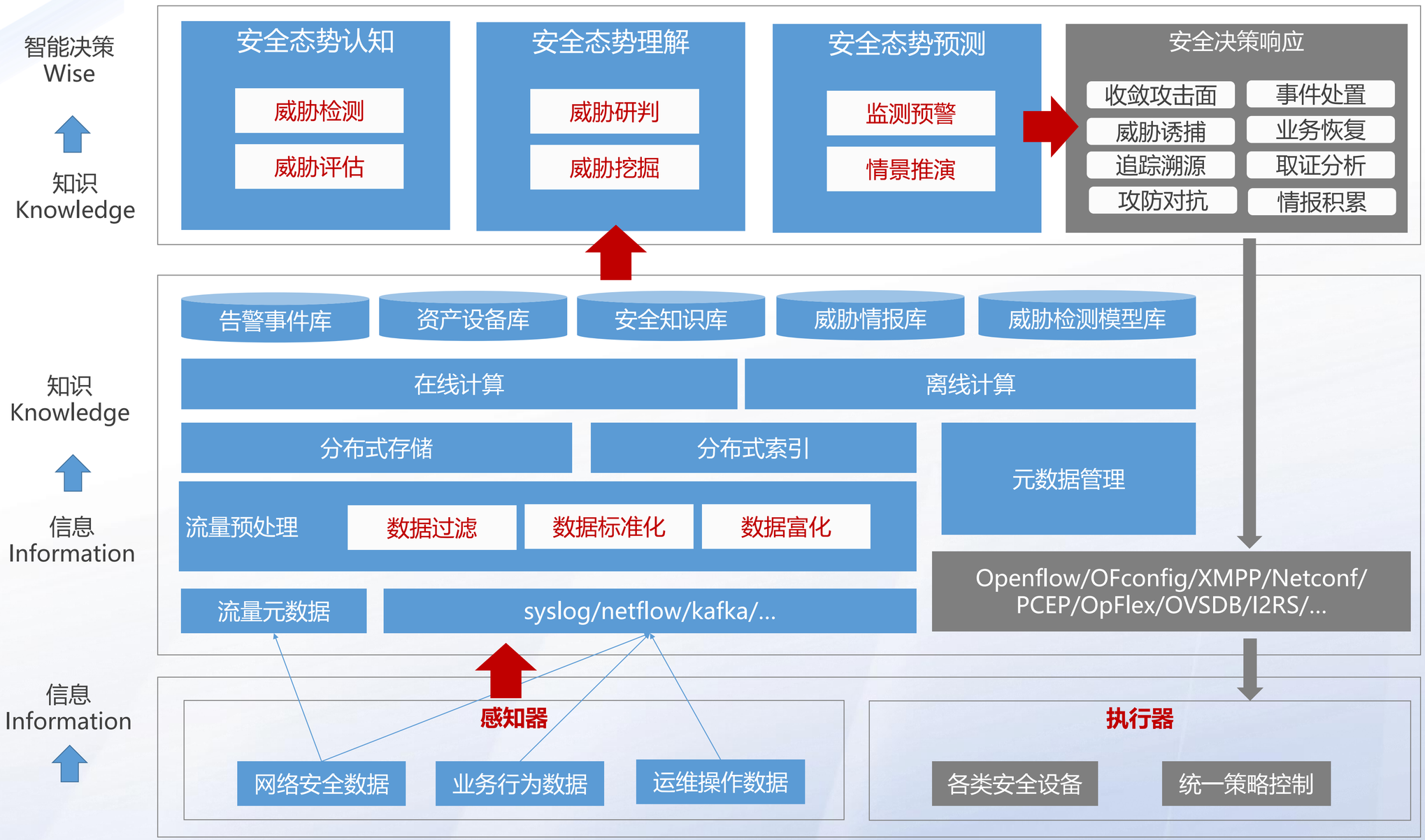
安全威胁预警与处置

提供资产脆弱性关联分析、网络攻击态势进预测，未知安全威胁发现能力。对预警进行自动联动或工单处置。

安全态势展示

作为网络安全态势感知平台可视化和分析的入口，提供安全态势分析综合视图和多种风险可视化展示

安全大脑技术框架


智能决策
Wise
知识
Knowledge
安全态势认知
威胁检测
威胁评估
安全态势理解
威胁研判
威胁挖掘
安全态势预测
监测预警
情景推演
安全决策响应
收敛攻击面
事件处置
威胁诱捕
业务恢复
追踪溯源
取证分析
攻防对抗
情报积累
知识
Knowledge
告警事件库
资产设备库
安全知识库
威胁情报库
威胁检测模型库
在线计算
离线计算
分布式存储
分布式索引
元数据管理
信息
Information
流量预处理
数据过滤
数据标准化
数据富化
流量元数据
syslog/netflow/kafka/...
Openflow/OFconfig/XMPP/Netconf/
PCEP/OpFlex/OVSDB/I2RS/...
信息
Information
感知器
网络安全数据
业务行为数据
运维操作数据
执行器
各类安全设备
统一策略控制

百度智能威胁狩猎平台

智能威胁狩猎平台-产品简介

依托AI+创新技术，通过攻防对抗等方式，帮助客户解决护网、安全运维管理、攻击溯源防护等痛点。

企业安全运维管理

网络攻击溯源防护

1、智能标识

基于智能标识功能实现**精细化分析、处置**，
例如：基于IP、用户、设备的三级封禁、
限速、溯源、分析

2、未知威胁检测

基于**AI白模型**的业务学习、训练，可检测
0day、Nday漏洞等未知威胁

3、用户异常行为分析

基于**AI用户序列异常检测**，可以提前发
现潜在攻击者

4、自动化的攻击引流

攻击者自动引流至内置蜜罐或外置蜜罐，
用于溯源、取证等。

5、攻击诱捕

通过**设置陷阱、识别黑客工具**，
实现诱捕攻击者，获取攻击者

6、东西向流量感知

通过东西向流量的学习服务器间相
互访问关系，一旦打破及时告警

7、API立体化防护

针对API提供全生命周期管理，
包括横向与纵向的立体化AI防护

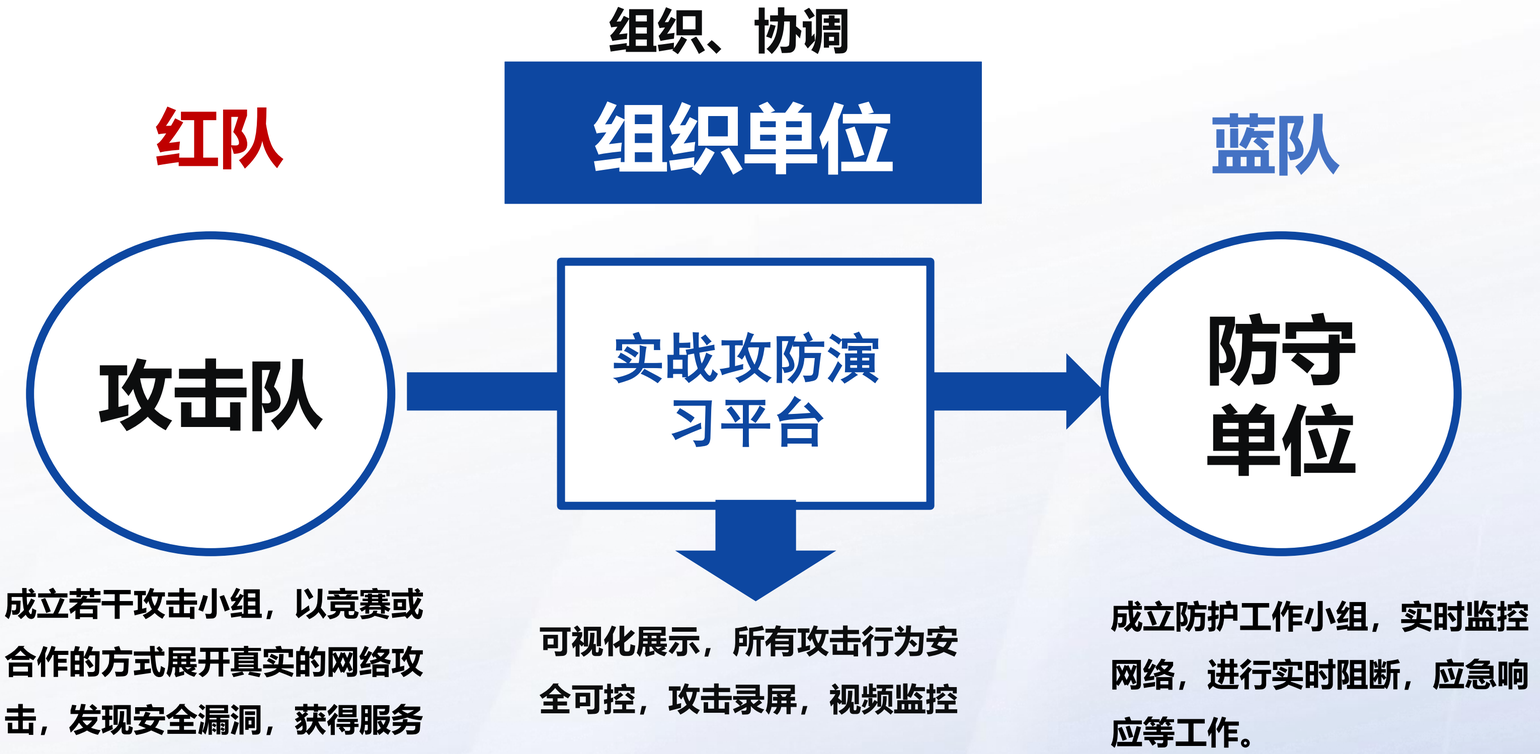
8、丰富的攻防工具箱

支持一键断网、一键静态化、
网页防篡改、区域封禁、
禁用JS检测、浏览器debug检测等

AI+创新技术

智能威胁狩猎平台-目标客群及其需求场景

实战攻防演练，又称护网HVV，在军事领域，是专指军队进行大规模的实兵攻防演习；在网络安全领域，是由公安部2016年发起的一年一度的“HW行动”所引申出常态化网络实战演习。该产品可有效满足客户的护网需求。



智能威胁狩猎平台-典型案例-政务与电力

在护网行动中，客户急需专业团队7*24协助监测和值守，避免被入侵攻破，提高得分能力和安全影响力。

某中央知名单位

业务诉求：

- 2020年由公安部组织的护网行动
- 护网期间，客户要求必须有人7x24值守
- 客户为了提高防护能力，提高得分能力

合作价值：

在帮助客户完成防护任务的同时，以百度智能威胁狩猎平台为中心，完成多份溯源报告。客户在2020年公安部护网行动中成绩排名优异。

某省级电网

业务诉求：

- 需要专业的安全技术人员+攻击防护监测产品进行7*24小时的防护值守，避免被入侵攻破
- 通过防守溯源反制，提交报告在公安部护网中取得较高的排名，提升安全建设影响力

合作价值：

在帮助客户完成防护任务的同时，以百度智能威胁狩猎平台为中心，完成多份溯源报告。2021年 树立电网行业标杆案例，取得第一名，得到领导表彰。

百度云安全专家服务

云安全专家服务-安全评估

安全评估是对信息资产（客户的整体硬件/软件/数据等资产的整体）所面临的威胁、存在的弱点、造成的影响以及三者综合作用所带来风险的可能性的评估。作为安全管理的基础，安全评估是组织确定信息安全需求的一个重要途径，属于组织信息安全管理体系策划的过程，可适用于重大社会事件/活动的安全专项检查等

对资产进行全面、细致的梳理，全面掌握现有资产状况
是保护被评估系统免受安全威胁的重要手段

安全风险是客观存在的威胁，没有绝对安全的系统，
所以需要整体全面的评估体系内存在的任何风险

安全服务团队成员主要由 CISP、CISSP等
经过资质认证的高级工程师组成，
日常负责百度内部系统及线上产品的安全评估工作

安全评估会输出评估报告，百度安全专家会
指导企业对发现的安全风险进行整改和负责

云安全专家服务-渗透测试

渗透测试是在客户授权许可的前提下，完全模拟真实黑客思维对授权目标(Web资产/系统/主机/APP等)发起攻击，采用可控、非破坏性质的方法和手段对系统进行深入的安全检测，发现系统或企业存在的最脆弱的环节，通过攻击链的形式展现系统从边界到内部网络的薄弱点

遵从业界OSSTMM与OWASP测试框架，
选取最佳实践进行操作，有效避免因过程
不规范导致的业务异常等风险

百度安全多年积累的漏洞库和应用库作为参考，
保证渗透全过程面准确

安全服务团队成员主要由 CISP、CISSP等
经过资质认证的高级工程师组成，
80%技术人员拥有5年以上的渗透测试经验

测试后，百度安全将提供渗透测试报告，
记录渗透全部操作步骤
并详细说明渗透测试过程中得到的数据和信息，
可根据客户需求安排漏洞复测服务

云安全专家服务-代码审计

代码审计指的是检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，
通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析。
代码审计是一种以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析，能够找到普通安全测试所无法发现的安全漏洞。

通过工具可以全面快速地发现代码中存在的缺陷问题，
代码扫描工具通过利用预先定义好的规则从数据流、
控制流、语义、结构、配置等几个方面对源代码进行分析

人工对扫描报告做进一步的分析，确认哪些漏洞是真正存在的；
同时，结合系统设计文档资料对系统业务流程进行跟踪分析，
重点分析代码中存在的工具不易发现的逻辑漏洞

可审计包括Java、PHP、C、C++、ASP、ASPX、
Python、Objective-C、Android等多种语言

测试后，百度安全将提供代码审计报告，
并详细说明代码审计过程中发现和分析出的风险，
可根据客户需求安排复测服务

云安全专家服务-安全加固

安全加固是针对主机和系统的安全保护手段，是对信息系统中的主机系统（包含运行在主机上的各种软件系统）与网络设备的脆弱性进行分析并修补。另外，安全加固同时包括了对主机系统的身份鉴别与认证、访问控制和审计跟踪策略的增强。安全加固通常建立在安全风险评估的基础上，参照安全评估结果对评估对象进行安全加固。

采取补丁修补，并优化和加强账号口令、日志审核、网络性能、文件系统、权限控制、服务和进程等的安全性能。
包括各种操作系统：Windows、Linux、各种Unix 等

采取补丁修补，并优化和加强账号口令、日志审核、网络属性、相关文件、数据库配置（存储过程）等的安全性能。
包括各种数据库系统：SQL Server、MySQL等

采取补丁修补，并优化和加强应用属性、日志审核、目录和相关文件等的安全性能。
包括常见的各种应用：Web、Mail、DNS 等

采取升级，并优化和加强访问控制、账号口令、网络属性、服务等的安全性能。
这些网络、安全设备包括各个厂商的路由器、交换机、防火墙等

云安全专家服务-应急响应

应急响应是在客户授权许可的前提下，当企业发生安全事件、紧急安全问题的情况下提供的远程/驻场技术支持服务。旨在协助客户在遭遇黑客入侵、数据泄露、数据篡改、挂马后门、勒索病毒等问题时，短时间内迅速排查问题、及时止损。协助企业找到入侵源头、还原入侵事件全过程，同时输出解决方案和应急响应报告内容，指导客户修复问题。

百度安全专家7*24小时值守，客户网络资产遇到紧急事件可第一时间响应，分析和抑制风险事件

百度安全对应急响应服务中存在的任何客户信息承担保密义务。承诺绝不会泄露至第三方组织或个人。

安全服务团队成员主要由 CISP、CISSP等经过资质认证的高级工程师组成，
80%技术人员拥有5年以上的安全服务经验

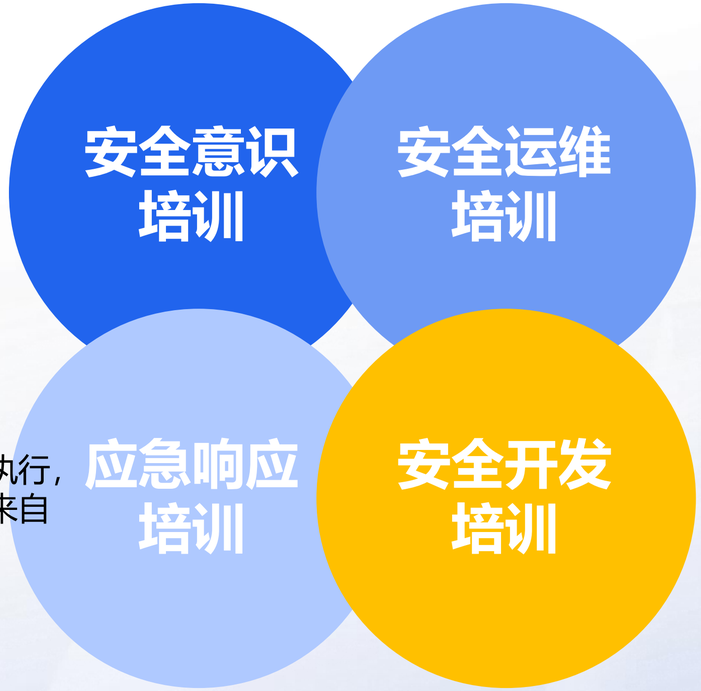
处置后，百度安全专家将提供应急响应报告，还原事件发生全过程，指导客户修复问题及时止损。

云安全专家服务-安全培训

安全培训服务是百度安全团队在保障百度自身复杂、庞大的业务中积累的实战经验和标准安全体系的系统化输出。

安全培训服务结合客户实际遇到的安全问题，为客户提供完整的培训，为客户赋能企业级安全意识及安全管理能力，以人为本打造最佳安全防线。

安全意识培训的目标是提高员工的信息安全意识，加深对信息安全的认识，加强识别信息安全风险的能力和信息安全风险防范技能。



让单位安全管理员了解网络安全漏洞的形成原理、利用方法，加深对信息安全的认识，加强识别信息安全风险的能力和信息安全风险防范技能。

培训企业安全运维人员，对突发的安全时间进行有效的预案执行，通过课程的培训，目的是让企业安全运维人员自身可以抵御来自网络的正在进行或进行后的侵害行为。

通过系列课程对企业研发进行培训，减少研发过程中产生的逻辑漏洞、引用的外部资源漏洞，提高代码安全质量。

云安全专家服务-典型案例

某大型银行

- **服务内容**

1、渗透测试服务（远程接入）

2、对客户测试环境的软硬件系统进行全面的渗透测试，内网渗透。

3、协助客户输出渗透测试/安全众测项目各类报告。

- **价值收益**

某大型银行每年均例行实施固定期的安全测试类项目，用来发现行内互联网系统的安全漏洞。百度安全已经连续第三年参与此大型银行互联网系统漏洞众测项目，以此来保障科技系统的安全性。三年的实施中在漏洞发现方面效果显著，深受客户好评。

某省级电网

- **服务内容**

1、安全评估服务（驻场）

2、于“护网行动2020”前中后期全程协助客户发现现存网络系统中系统级风险和威胁。

3、结合百度安全智能威胁狩猎平台产品，对网络攻击者精准溯源。

- **价值收益**

依赖百度安全驻场专家的服务以及智能威胁狩猎平台的溯源能力，我方输出的溯源报告助力国网某省电力取得了护网2020防守方得分第一名的好成绩。

百度点石数据安全隐私计算产品

应用场景1-内部数据安全可信共享

不改变数据所有权、打破壁垒，满足在安全合规条件下的数据共享交换

场景痛点

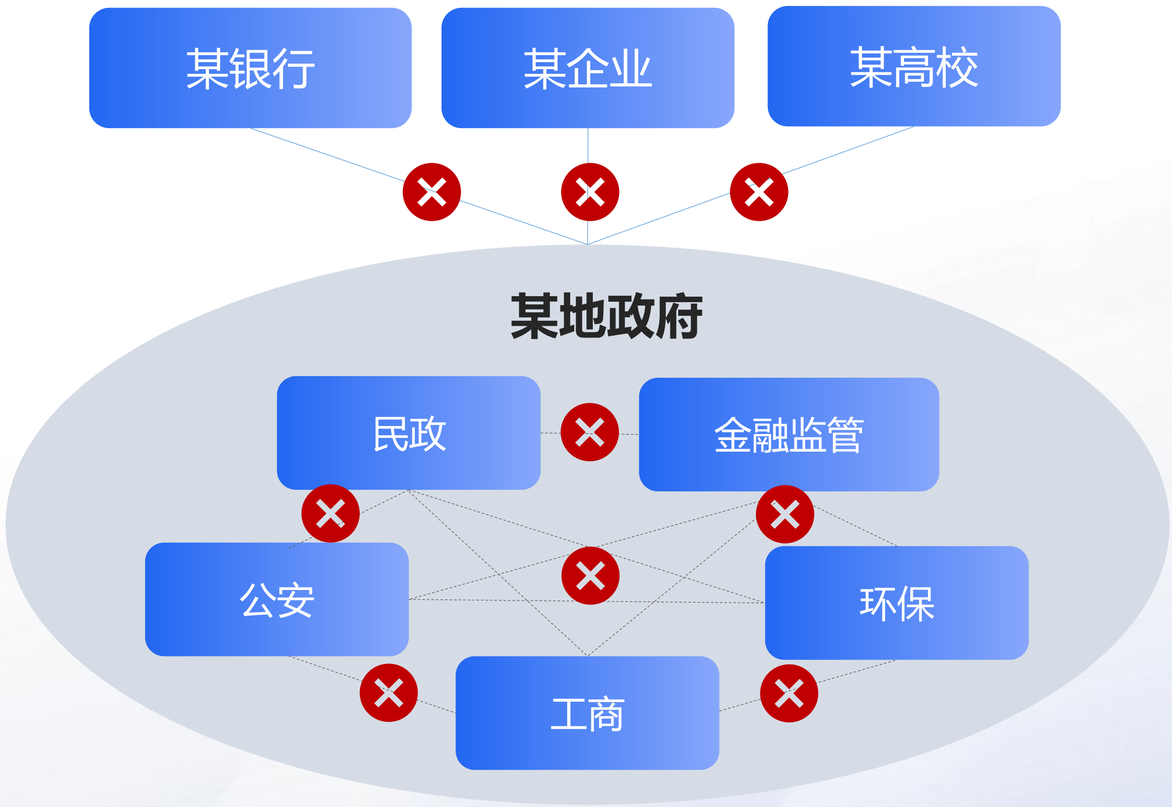
① **不愿共享：**内部各委办局/各部门重视自身数据权力，不愿共享

② **共享困难：**数据孤岛和壁垒严重，系统间难以打通缺少安全共享平台/技术，盲目共享容易造成数据安全风险

③ **泄露风险：**担心数据泄露、滥用、二次分发追责

应用场景2-跨机构数据价值释放

安全融合多方数据，打破数据孤岛，释放数据价值，助力业务创新



场景痛点

① **数据需求：**业务数字化转型趋势下，单方数据已不能满足业务创新需要

② **数据资源：**多方数据拥有方彼此不互信，缺乏共识

③ **安全手段：**多方数据融合互补，缺少安全合规技术/平台

④ **安全风险：**存在数据安全隐患，泄露风险高

……

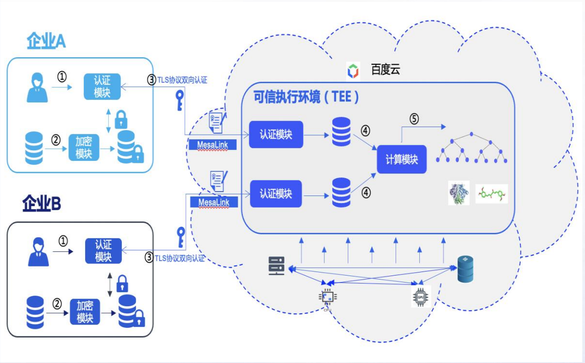
应用场景3-大模型训练、部署阶段的数据安全

大模型训练

在训练阶段，确保原始数据的隐私和机密性至关重要！

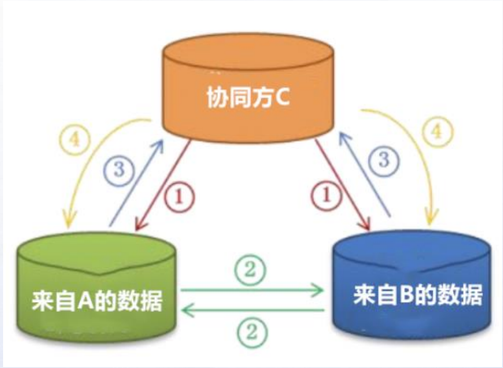
公有云场景

在云上大模型训练 、精调、推理时，如何解决敏感数据上云后的数据隐私保护?



私有化共建

在大模型的私有化共建时，可能涉及多个数据所有者之间的数据共享与计算?



大模型部署

- 攻击者可能通过攻击云服务器来窃取模型及其数据，或者反向工程模型参数以训练新模型。
- 大模型在部署过程中可能受到对抗性攻击的威胁，如对抗性样本攻击等
- 部署的模型在传输和存储过程中可能被篡改
- 如何建立访问控制机制，确保可信用户或系统可以访问模型和相关资源、以及AK/SK防滥用

点石隐私计算平台-需求场景

营销

联合精准拉新

联合精准推荐

联合深度转化

政务

政务数据安全交换

跨机构联合建模

敏感信息匿踪查询

高校&科研

教务数据校内共享建模

科研数据开放建模

科研数据创新开放大赛

医疗

DNA 联合测序

联合疾病早筛

联合电子病历

金融

黑名单共享

多头借贷发现

联合信用评估

总体架构

基于多方安全计算、联邦学习、可信执行环境（TEE）等技术能力，在数据安全与隐私保护的前提下， 满足多方数据安全共享、开放、融合及建模计算， 赋能政务、金融、医疗、教育、汽车、互联网等领域客户，解决数据融合应用困境。

应用层

政务、金融、医疗、教育、交通、互联网、零售、电商、旅游 ...

金融反欺诈	金融营销	产品精算定价	普惠金融	疾病风险检测	基因检测	核酸比对
营销旧客挖掘	人群分析	用户精细化运营	产学研用	临床辅助诊断	靶点筛选	... ...

功能层

联合建模			联合分析		在线服务		存证审计	
数据融合	特征工程	模型预测	数据统计	联合查询	在线安全查询	在线联合计算	数据上链	过程上链
数据处理	模型训练	模型评估	相关分析	数据核实	在线模型预测	在线隐私求交	审计溯源	存证取证

服务层

基于SMPC的安全多方计算引擎

PSI | SMC | LR/XGB | PaddleFL

多方安全计算 | 同态加密 | 差分隐私

基于TEE的安全可信计算引擎

MesaPY | SQL | Python | Paddle

MesaLock/RustSGX/MesaLink

Intel SGX | AMD SEV | ARM Trustzone

基于隔离域的安全隔离计算引擎

Notebook | Paddle | NLP | Vscode

生产环境 ⟷ 脱敏/置换/抽样 ⟷ 调试环境
逻辑/程序/模型

物理隔离 | 数据隔离 | 网络隔离 | 交互隔离

多方安全计算 | 联邦学习 | 可信执行环境（TEE） | 安全隔离域 | 大模型

数据层

机构 A			机构 B			机构 N
结构化	半结构化	非结构化	结构化	半结构化	非结构化	数据
云上数据	第三方	OpenAPI	云上数据	第三方	OpenAPI	

解决方案核心优势

NO.01

技术选型

安全多方计算
联邦学习
可信执行环境
安全隔离域
区块链

NO.02

全场景覆盖

联合营销
联合风控
政务数据开放
生物医疗
… …

NO.03

多项标准/认证

IEEE标准3项
国标3项
行标7项
认证6个
发明专利300+项
顶会论文20+篇

NO.04

代码开源

Teaclave
PaddleFL
HIGHFLIP

政务应用-某省会城市大数据工程服务项目

率先在省会城市采用**安全多方计算**的方式，打造政务数据基础设施，**助力政务数据安全共享与开放**

项目背景

- 某市级政府机构已有多个业务系统，各业务系统没有对大量政务数据聚通用，无法为业务提供应用支撑
- 各系统使用不同的网络（互联网、政务网、专网等），只能纵向运转，无法横向贯通
- 现有系统及数据无法满足系统间数据连通需求

项目目标

- 构建政务大脑：实现对市社会面风险态势、治安态势、舆情态势的全面感知；
- 构建政务大数据治理体系：拉通政府部门、相关政府职能部门、社会面数据的汇聚、治理与融合
- 完善政务业务应用生态体系：业务应用系统提档升级
- 构建政务大数据云：为政务大脑提供计算存储、通讯、安全、运行环境等基础设施

项目价值

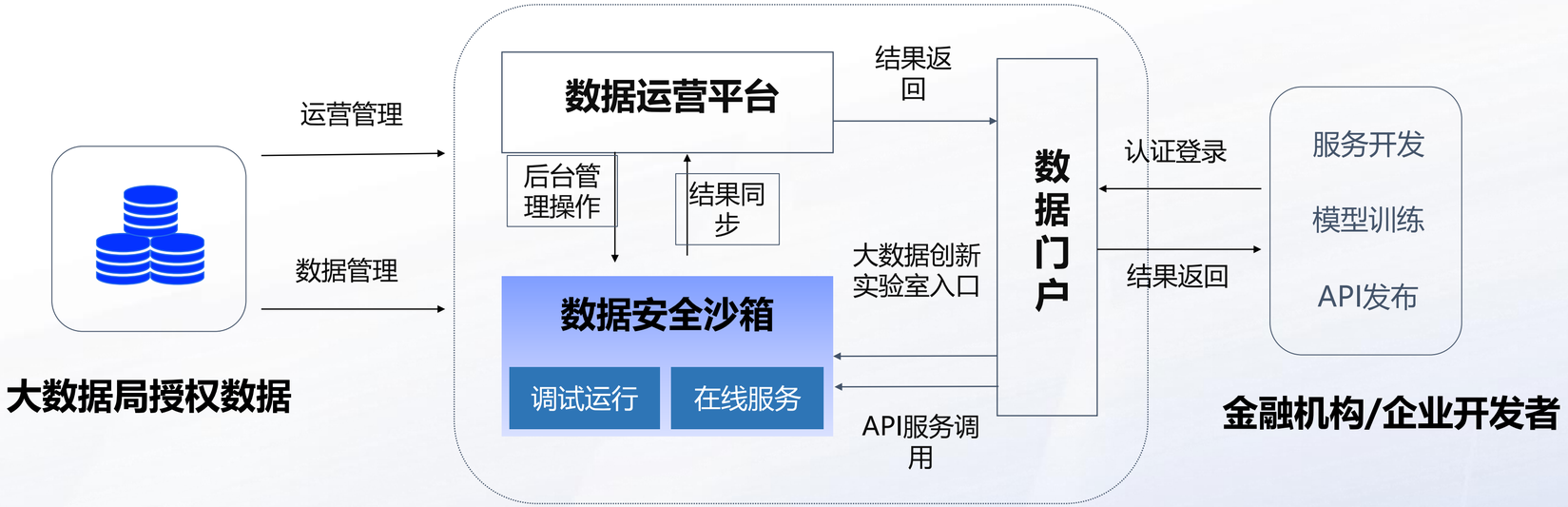
百度提供安全多方计算方案，在近50个委办局、社会面机构本地部署计算节点，满足各方“数据不出域”、“可用不可见”、网络连通诉求，成功拉通政府部门、相关体系、社会面数据的汇聚、治理与融合，为上层政务大脑、业务应用提供政务数据基础设施支持，实现政务数据安全共享与开放

政务应用-地方政务数据开放案例

业务场景：某国资数据运营公司建设了**数据运营平台**并搭建了数据门户，预期实现数据的对外开放和运营管理，但是该平台并不具备数据开放的安全能力、数据建模分析能力，无法在保证数据安全的前提下满足数据使用者建模、查询的数据需求。

核心诉求：在保护敏感原始数据不出域不可见的前提下，实现：

1. 充分调动金融机构/企业开发者们的开发能力，丰富数据利用场景。
2. 基于FAAS服务帮助开发者们快速实现服务开发和API发布。



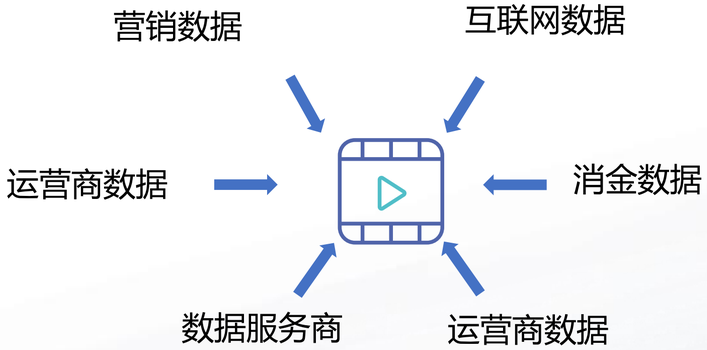
解决方案：将点石数据安全沙箱平台与数据运营平台进行对接：

- ✓ 沙箱平台负责数据统一接入、处理、开放、审计，提供建模和在线查询能力。
- ✓ 数据运营平台进行数据集开放管理、申请审核、权限管理等。
- ✓ 在实现了数据安全开放的同时，也满足了大数据局的业务管理诉求。

泛科技应用-某短视频平台引入联邦学习构建用户画像

应用场景：1、用户画像补充：引入外部数据，补充用户标签，提升用户留存率；2、人群定制：根据广告主业务场景，依据标签进行人群筛选。3、联合建模：广告主拥有用户Y值、平台拥有用户X值，双方数据融合、联合建模，提升投放效果。

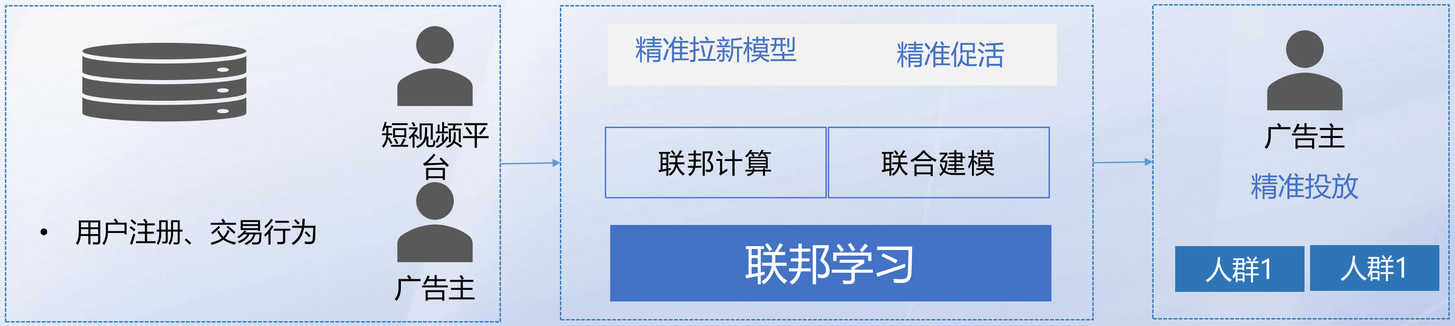
点石价值：客户存在上述业务需求，但数据敏感无法共享，点石联邦学习平台提供平台支持，可以在数据安全及隐私保护的基础上，安全打通多方数据。已协助引入5家数据源，1家广告主，还有8家数据生态正在进行联合测试。



客户合作方接入情况	
数据源	第三方数据服务商、某运营商
广告主	消费金融

用户画像补充/外部数据引入

联合建模（大客户/品牌客户）



百度智能数据安全网关产品介绍

数据安全的管控力度越来越大

国家与各行业推出数据安全建设标准与技术要求，整顿业务系统数据泄露问题，为数据安全中心提供了利好的政策环境。

全国人大

网络安全法
数据安全法
个人信息保护法

国务院

科学数据管理办法
重要数据管理办法
数据出境管理办法

网信办

数据安全管理办法
个人信息出境安全评估办法
（征求意见稿）

公安部

信息安全等级保护管理办法
网络安全等级保护条例

国家与各行业陆续推出了数据安全建设标准与技术要求

网络安全等级保护基本要求（GB/T 22239）、数据安全能力成熟度模型（GB/T 37988）、大数据安全管理指南（GB/T 37973）
政务信息共享数据安全技术要求（征求意见稿）、公安大数据安全总体技术框架、工业互联网平台安全白皮书

数据泄漏事件大多跟内部风险有关

部分员工由于安全意识淡薄进行误操作，或有意为之，加之薄弱的安全建设给不法攻击分子可乘之机，给敏感数据泄露造成了极大风险。

教育

- 郑州某高校近2万名学生个人信息遭到泄露
- 泄露信息包括姓名、身份证号码、专业、宿舍门牌号等高敏感数据

银行

- 浙江某农商行发生**内部人 员**泄露客户个人信息事件
- 银保监会罚款30万元，责任人禁业3 年

电商

- 国内某电商巨头发生**内外 勾结**倒卖用户数据事件
- 泄露数据达50亿条，相关人员获刑

医疗

- 胶州某医院**内部员工**泄漏6000名患者信息
- 3人被刑拘

数据安全中心-解决客户内部数据风险治理痛点

以AI为核心，构筑 “数据能看清、流转可监测、风险能感知、泄密可追溯”的核心能力。

通过简便的、开箱即用的模式，无需客户进行业务改造，便可帮客户落地系统数据安全管控能力，保护敏感信息，风险可追溯。

百度智能数据安全网关

盘家底

- 敏感数据资产分布
- 敏感资产生命状态

全监测

- 谁？什么时候？
- 访问什么敏感数据

智管控

- 敏感数据脱敏
- WEB水印威慑
- 异常行为处理

会运营

- 数据风险感知
- 安全态势可视

可追溯

- 泄漏事件溯源
- 定位到泄漏者

做到心中有底

事前全面预防

风险分析，推动修复

避免信息泄露

安全态势可视

事中持续保护

找到“内鬼”

事后精准溯源

数据安全中心-金融场景客户案例-某知名保险公司

客户内网业务多，存放着大量客户个人信息，希望在不改造业务系统的情况下，高效梳理敏感信息，定位数据泄露风险点，管控数据权限，监控并追溯到重要信息的泄露风险。该产品成功解决客户痛点并获“信通院优秀案例奖”。

【项目背景】

- 客户是一家涵盖保险、资管、医养三大核心业务的大型金融保险服务集团，在保险行业有较高影响力。

【客户痛点】

- 1、客户内网业务多、逻辑复杂，敏感信息难以梳理，无法定位数据泄漏的风险点；
- 2、客户业务中存放着大量客户个人信息，希望在不改造业务情况下，前端业务人员、后端管理人员等能够根据岗位职责或工作需求进行有限的客户信息访问，防止由于员工访问敏感信息范围过大而导致客户信息泄露。
- 3、监控员工的对内网敏感数据的访问行为，并且可以及时追溯。
- 4、内网发布的重要信息，总有员工通过拍照、截图方式泄漏出去，希望可以对这种数据泄露的行为进行追溯。

【百度方案】

- 1、通过敏感数据主动探测功能，帮助客户自动梳理敏感数据，定位数据泄露风险点。
- 2、基于用户权限的动态脱敏功能，无需业务改造，也不需要对接用户管理系统，实现用户粒度的敏感数据动态脱敏。
- 3、对用户访问敏感信息行为生成日志，记录谁、什么时间、访问过哪些敏感信息。
- 4、网页、文件水印和水印溯源，数据泄露追溯

【最终效果】

- 1、在本项目中，凭借产品成熟度与差异化优势，打败友商，**成功中标该项目；**
- 2、该项目获得信通院的优秀案例奖和idc cso20中国区优秀案例奖，成为**金融行业的标杆案例。**

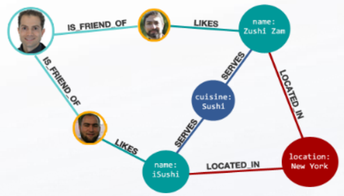
百度图数据库及知识图谱产品介绍

图技术背景

大数据和人工智能时代，数据管理技术遇到了前所未有的挑战。

图技术将数据按真实世界方式组织起来，按符合人类思维方式进行数据管理、处理和关联分析，深度挖掘数据价值。知识图谱是基于图的语义网络，是认知智能基础技术。

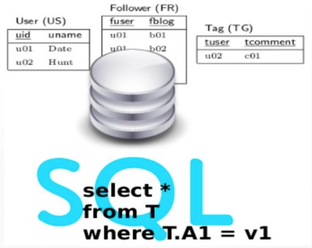
IOT



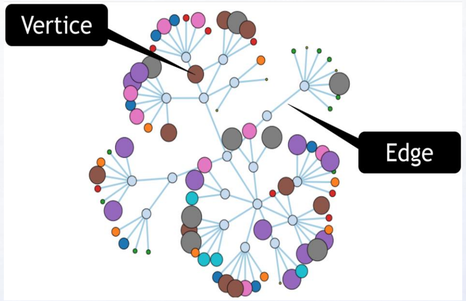
社交关系网络

指数级增长

复杂度、耦合性高



应运而生



HugeGraph

- 用户、系统和传感器产生的数据呈指数级增长
- 数据内部依赖和复杂度增加

- 关系型数据库不能满足海量数据存储、关联分析的需求
- 大数据平台在查询关联关系的场景下，速度过慢

- 图数据库可以存储海量的顶点和边
- 图数据库支持海量数据进行多维度、深链路的复杂关系分析能力

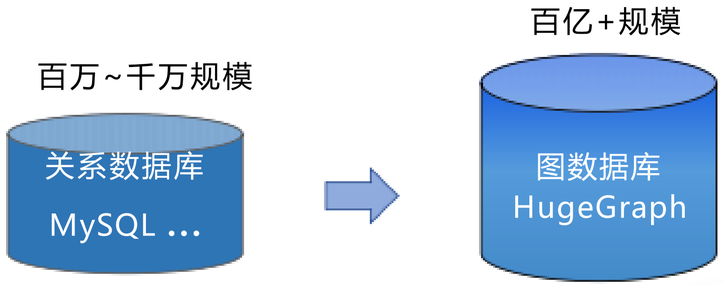
HugeGraph简介

HugeGraph是百度安全完全自主研发的一款易用、高效、通用属性图图数据库系统，实现了Apache TinkerPop3框架及完全兼容Gremlin、Cypher查询语言， 具备完善的数据导入导出、备份恢复、运维监控、可视化管理工具链组件，助力用户轻松构建基于图数据库之上的应用和产品。HugeGraph支持百亿以上的顶点和边快速导入，并提供毫秒级的关联关系查询能力（OLTP）， 并支持大规模分布式图分析（OLAP）。

HugeGraph优势

大规模

HugeGraph支持多种NoSQL后端存储，可以存储百亿级的海量数据



高效

HugeGraph在图存储和图计算方面做了深度优化，轻松完成百亿级快速导入，查询优化实现毫秒级响应

源数据	Twitter（2010），4200万顶点、14.7亿边、24.6GB					
图系统	HugeGraph	TigerGraph	Neo4j	Nebula	JanusGraph	ArangoDB
kout-1度查询（秒）	0.007	0.022	0.2	0.19	0.39	1.667
kout-2度查询（秒）	3.14	6.8	18.3	32	27.7	28.9
kout-3度查询（秒）	64.13	92.1	290	N/A	4300	3888
kout-6度查询（秒）	182.3	251.9	N/A	N/A	N/A	N/A

通用

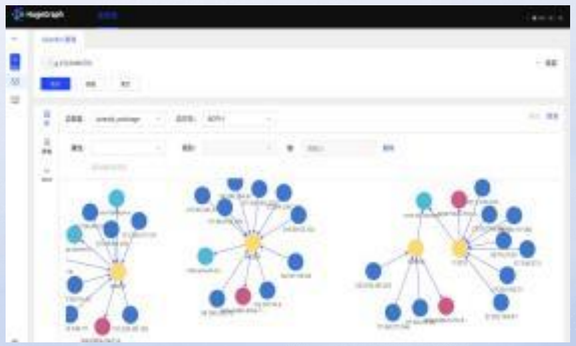
HugeGraph支持Apache TinkerPop Gremlin标准图查询语言、Cypher查询语言和Property Graph标准图建模方法，支持基于图的OLTP和OLAP

```
// Gremlin 2层好友查询
g.V()
  .has('name', 'Tom Hanks')
  .out('friend' ).out('friend' )
```


```
// 查询2点之间的最短路径
g.V(source_id)
  .repeat(out().simplePath())
  .until(hasId(target_id))
  .path().limit(1)
```

易用

HugeGraph拥有图管理、元数据建模、数据导入、数据分析全流程的可视化平台，简单易用，且具备功能齐全的周边工具，轻松实现基于图的查询分析运算



智能决策平台简介

智能决策平台(BD-KG)依托百度安全图技术能力，提供知识从生产、存储管理到智能决策应用一体化能力平台。支持结构化、半结构化、非结构化数据可视化接入并快速转化为属性图数据，并在高性能图数据库HugeGraph进行知识存储和管理，结合业务提供智能问答、知识检索等上层智能应用，支撑业务智能决策。

典型应用场景

典型行业应用

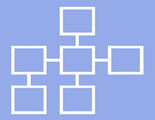
泛安全	金融	公安	医疗 & 制药	电商	交通 & 物流
社交 & 娱乐	物联网	司法	制造业	生命科学	互联网 & 通讯
……			……		

典型应用场景

实时推荐

网络安全

欺诈检测



路径追踪
(犯罪/黑产)

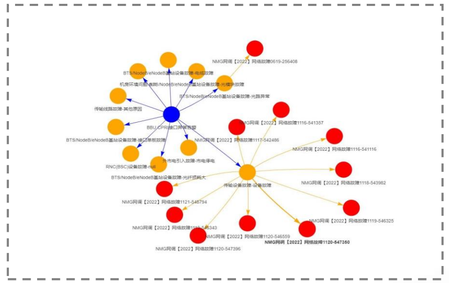
IT网络管理

知识图谱

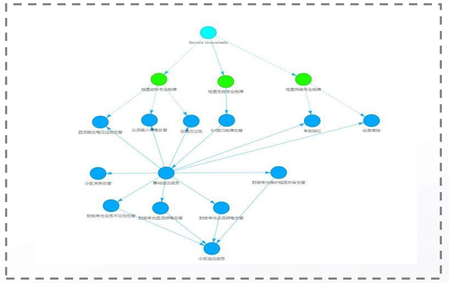
案例-智能安全运维大脑

业务应用

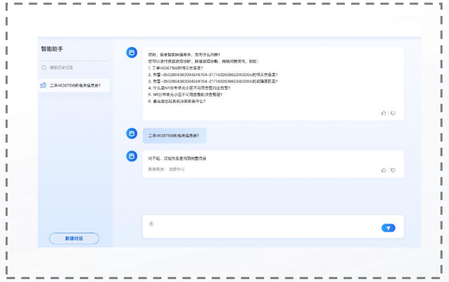
以知识图谱和机器学习技术为基础，综合应用大数据和NLP等技术和领域专家经验深度挖掘安全运维业务数据价值，沉淀运维知识，定位故障原因，辅助业务决策。



智能判障



故障根因分析



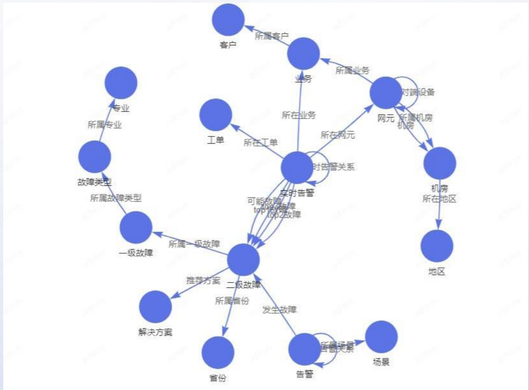
智能问答

数据管理

- 设备/运维手册
- 故障数据
- 告警数据
- 业务数据
- ……

业务建模

基于数据构建知识图谱

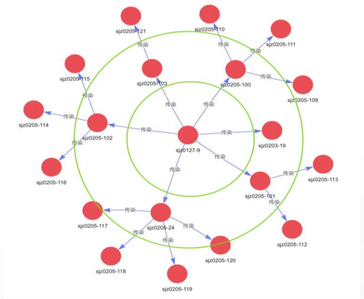


- 知识应用
- 知识管理
- 知识生产

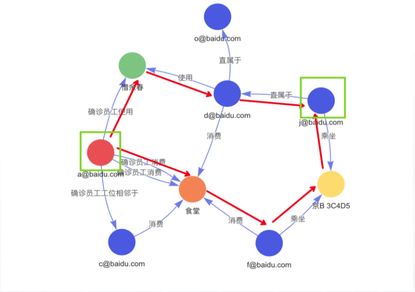
案例-公安研判

业务应用

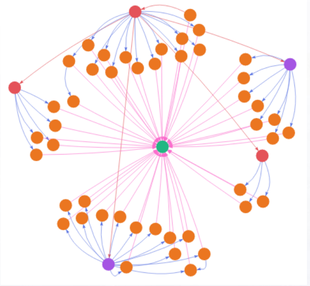
以时、地、人、事、物和组织等要素构建图谱，可对嫌疑人和事件进行深度挖掘，发现团伙、行踪和社会关系等，为研判提供数据支撑。



嫌疑人多度社会关系



嫌疑人路径追踪



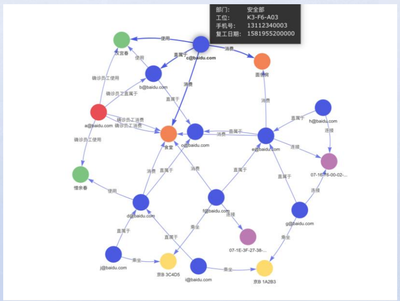
团伙分析

数据管理

基础信息	线上数据	线下数据
基本信息	社交数据	酒店数据
社保信息	网站登录	快递信息
社会关系	账号密码	运营商数据
	……	

业务建模

基于数据生成用户画像，并构建知识图谱



百度大模型安全解决方案

大模型应用面临的安全挑战

百度智能云

在构建大模型服务时，百度将大模型全生命周期划分为三个关键阶段：训练阶段、部署阶段、以及业务运营阶段，在各业务阶段面临的安全风险、以及挑战各有不同：

大模型训练阶段 .

企业自有数据如何在**保障数据安全与隐私**的前提下，实现大模型的精调、推理、共建?

大模型部署阶段.

大模型部署时如何防止**模型窃取与泄漏**?

大模型业务运营阶段.

大模型服务在运营阶段，如何保障接口安全、**投毒反馈**等**黑产攻击**？如保障**提问内容、输出内容安全**?

01 02 03

AIGC安全风控解决方案

百度智能云

围绕大模型全生命周期，针对三大业务阶段所面临的风险挑战，构建百度AIGC安全风控解决方案

AIGC安全风控解决方案

安全服务

- 数据隐私计算服务
- Prompt安全审核服务
- AIGC安全评测服务
- 业务风控服务
- 业务情报收集
- 安全专家服务

业务阶段

大模型训练阶段

客户业务风险

- **云上训练 / 精调**：敏感数据上云；数据隐私风险
- **私有化共建 / 精调**：数据不能出域；可用不可见

安全产品

大模型数据隐私保护

- 联邦大模型联合预训练
- 训练数据合规清洗
- 云上隐私大模型精调 / 推理
- 可信执行环境模型训练 / 推理

大模型部署阶段

客户业务风险

- **模型攻击**：模型窃取/泄露；模型文件攻击
- **控制与授权**：DDOS攻击 /代码注入、AK/SK滥用

安全产品

- **模型保护**：模型部署安全保护方案
- **网络/API安全**：WAF；API安全；云高防；安全认证

大模型业务运营阶段

客户业务风险

- **业务运营**：批量注册/薅羊毛/权益侵占/机器作弊等/
- **提问行为**：AIGC盗爬 / 垃圾提问 / 投毒反馈 / 接口攻击 / 频控突破 / 资源侵占
- **大模型 “输入” 与 “输出” 安全**：煽动 / 恶俗 / 暴力/色情 / 涉政 / 涉恐 / 虚假信息 反社会价值观 / 内容侵权 / 偏见 /歧视 / 隐私泄漏

安全产品

- **业务风控服务**：账号安全；流量反爬；接口防刷；营销风控；人机识别；行为检测；业务情报；风险设备；蓝军评测
- **Prompt审核**：违规内容审核；多轮指代改写；网址安全检测
- **回复干预**：红线知识库；红线大模型；Prompt改写
- **模型生成内容过滤**：违规内容检测；隐私信息识别；内容侵权识别；虚假信息防范

安全能力基础组件

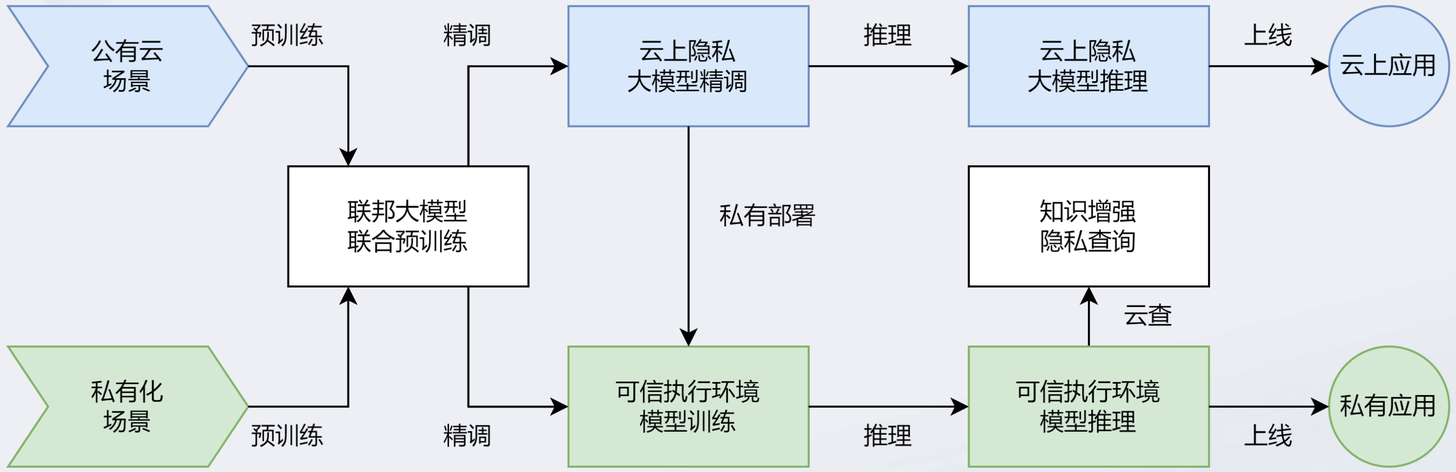
- **终端组件**：JS安全SDK；客户端安全SDK
- **网络安全**：DDoS防护；应用防火墙；安全检测
- **人机验证**：无感验证；行为验证
- **业务风控系统**：风控开放平台；设备指纹；专家策略；风险画像；智能决策引擎；安全因子；风控模型；风控情报
- **内容审核**：图文审核；音视频审核；内容安全蓝军
- **其他**：代码保护

核心技术

机器学习 · 模型引擎 · 决策引擎 · 设备指纹 · 攻防对抗 · 关联网络 · 隐私计算 · 图数据库 · NLP

大模型训练阶段-安全防护方案

百度智能云



基于百度点石构建以“联邦学习+可信执行环境”为核心的数据隐私保护方案，完全覆盖公有云和私有化场景，以及大模型预训练、精调、推理全生命周期。

01云上训练和预测

目的：预训练+精调+预测

客户诉求：无部署环境，希望付费即用，有较多敏感数据（但可以接受云端托管），需要百度提供训练（预训练+精调）数据，且数据量较大 。

02敏感数据云上精调

目的：精调

客户诉求： 无部署环境，希望付费即可使用，有少量敏感数据进行精调，当前方案可以支持客户使用浏览器参与：无需算力、无需上传原始数据

03私有化精调/预测

目的：精调/预测

客户需求： 接受私有化部署、用户数据不能以任何形式出域，如何与文心大模型进行精调/预测

04共建行业大模型

阶段：训练（预训练+精调）

客户需求： 需要私有化部署，客户有大量敏感数据+百度侧提供大量敏感数据，联合训练行业大模型，如何保障双方数据可用不可见

大模型部署阶段-安全防护方案

百度智能云

针对大模型在部署阶段所面临的风险，本方案从如下六个方向提供安全防护服务，全方位保障大模型部署安全。

访问控制与安全认证：

提供身份认证、权限管理、访问令牌等，确保只有合法用户或系统能够使用和操作模型。

网络与通信安全防护：

支持提供WAF、云高防、安全网关、以及API安全服务保障模型通信网络安全

模型水印：

支持模型中添加水印或标识信息，可以追踪和识别未经授权的模型副本，助于发现和追踪模型的盗用或泄漏

模型保护与防篡改：

提供模型加密、数字签名、模型完整性验证等安全服务，以确保部署的模型在传输和存储过程中不被篡改。

防止对抗性攻击：

支持提供鲁棒性增强技术、异常检测、入侵检测系统等，以提高模型对恶意攻击的鲁棒性。

安全更新和漏洞修复：

定期对部署的模型进行安全性评估，及时修复发现的漏洞或安全弱点。

大模型运营阶段-业务行为安全防护方案

百度智能云

以昊天镜业务安全风控为核心，构建大模型业务运营阶段安全风控防御体系，重点识别异常用户行为。

账号安全　行为检测　人机识别　流量反爬　营销风控　风险设备　接口防刷　业务情报

企业用户平台

用户注册/登录

用户申请环节

用户提问环节

结果反馈环节

其它业务环节

请求

风险

数据盗爬

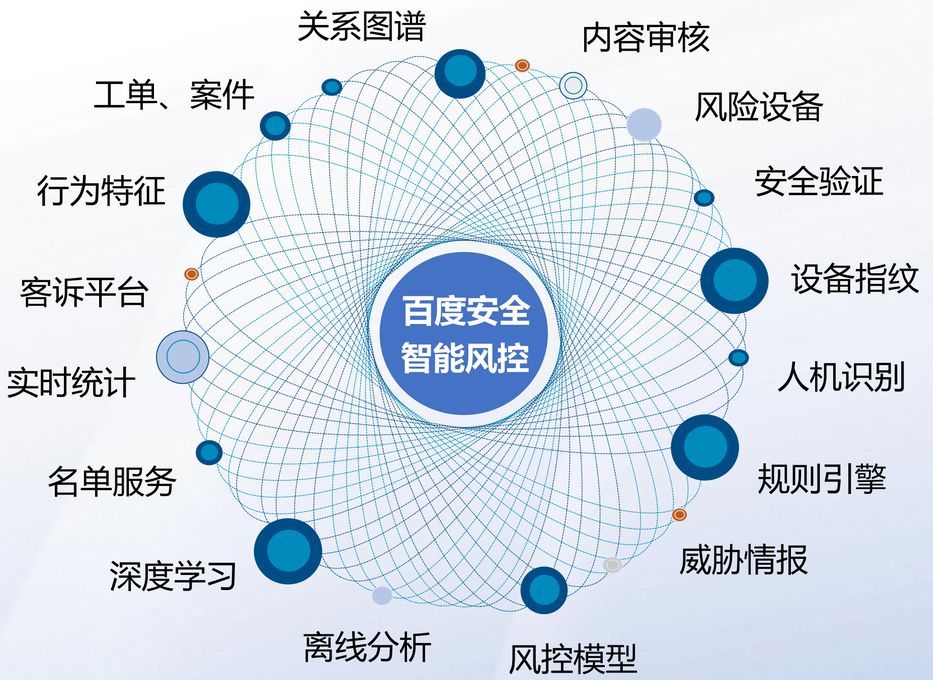
异常反馈

机器行为

等等

正常返回

百度业务安全风险防控体系



正常

返回内容

AIGC
大模型

多模态
内容生成

文本

图片

音频

视频

大模型运营阶段-提问内容过滤/AIGC输出内容安全

百度智能云

检测用户输入和生成内容，识别是否存在各类违规风险，结合人工审核、举报等机制，持续迭代模型，全面保障内容合规。

违规内容检测　网址安全检测　代码注入检测　Prompt风险提示　隐私信息过滤　内容侵权检测　虚假信息防范

百度业务安全风控系统

业务安全风控服务架构


业务数据
接入层
数据加工
风险识别与策略挖掘
采集与存储
设备指纹
业务数据
H5 js数据
实时在线接口
离线分析接口
数据衍生
设备指纹
安全因子
地域解析
数据补充
名单标签
实时累计
格式化处理
规则平台
决策引擎
模型平台
规则集
决策树
策略评估
关系图谱
设备关联
网络关联
账号关联
模型训练
模型评估
模型部署
风险特征挖掘
规则热部署
规则监控
团伙挖掘
特征工程
算法管理
模型组件
后聚类分析
有监督学习
无监督学习
大数据存储与分析平台
风险结果
硬件设备属性
设备画像
用户画像
网络环境数据
行为数据
安全因子
风险标签
地理位置数据
威胁情报

营销风控-产品能力

黑账号识别

- ✓ 黑卡账号识别
- ✓ 批量马甲号识别
- ✓ 团伙账号识别
- ✓ 接码平台账号

•••

脚本工具

- ✓ 脚本攻击识别
- ✓ 按键精灵
- ✓ 脚本精灵
- ✓ 触动精灵
- ✓ 一触即发
- ✓ auto.js

•••

设备篡改

- ✓ Xposed
- ✓ Magisk
- ✓ Root
- ✓ 越狱
- ✓ xx抹机神器

•••

设备模拟

- ✓ 分身、多开
- ✓ MuMu模拟器
- ✓ 夜神模拟器
- ✓ 雷电模拟器
- ✓ 逍遥模拟器
- ✓ 蓝叠模拟器
- ✓ 51模拟器
- ✓ 天天安卓模拟器

•••

线控\云控

- ✓ 群控设备
- ✓ 百度云手机
- ✓ 红手指云手机
- ✓ NBE云手机
- ✓ 夜神云手机
- ✓ 龙珠云手机
- ✓ 多多云手机
- ✓ 云控平板云手机

•••

异常IP识别

- ✓ 代理IP
- ✓ IDC IP
- ✓ 黑名单IP

•••

账号安全-产品能力

机器注册

- 结合机器学习等人工智能技术可有效识别各种账号注册机、脚本注册、以及各类异常设备注册。

盗号/养号

- 建立全链路的防御体系，可以有效识别账号被盗登录、批量注册账号养号行为

恶意注册

- 凭借各类专家策略，可以有效识别各类猫池小号、黑卡账号、解码平台黑号注册。

扫号/撞库

- 结合外部情报、登录场景化定制风控模型，可有效识别扫号、撞库等异常行为

智能可信设备指纹-产品能力

智能可信ID

结合设备多维度信息，通过专有加密模型算法，颁发全球唯一的设备标指纹ID

设备篡改识别

通过多维信息交叉验证、及关联百度海量设备库，有效识别篡改设备

风险环境识别

可以有效识别root、越狱、改机框架、应用多开、分身等众多设备风险环境

群控/云控识别

通过独特的设备对抗模型，可以有效识别手机农场、云手机等异常设备

虚拟设备识别

可精准识别市面上主流模拟器应用，输出安全因子

异常行为识别

专注设备使用过程中产生其它信息，感知设备使用中异常行为，

渠道推广反作弊-产品能力

设备新增刷量识别

- 模拟器刷量识别
- 设备篡改刷量识别
- 群控设备刷量识别
- 云手机刷量识别
- 双开分身刷量识别
- 低端机刷量识别

调起激活作弊识别

- 应用下载后，基于设备指纹SDK能力，实现对后续应用调起方式的有效性进行判断，识别脚本批量调起等作弊方式

推广渠道质量分级

- 结合渠道质量评估模型，对已经接入的推广渠道的效果、质量进行评估、分级别。

决策引擎-产品介绍

多场景事件接入

- 场景化事件接入，灵活管控。
- 自定义变量管理，自动解析。
- 多类型变量支持，扩展性强

复杂策略管理

- 可视化策略配置，操作简单
- 多状态策略管理，流程化策略上线
- 决策树挂载策略，清晰可控
- 多种决策组件，策略更灵活

多维度特征补充

- 自定义管理名单标签
- 实时累计特征，界面可视化管理
- 多维度特征在线补充

策略监控与分析

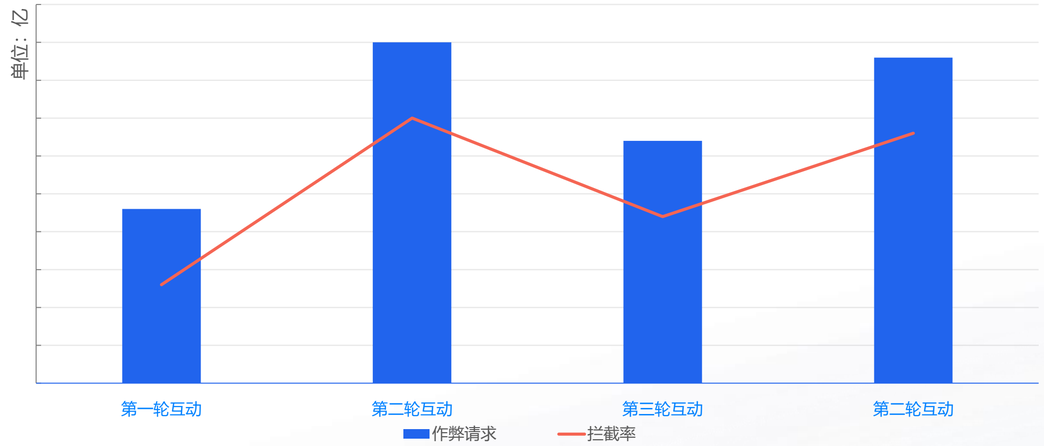
- 事件请求实时查询分析
- 策略命中监控，效果实时跟进
- 策略实验室评估分析

案例-营销风控

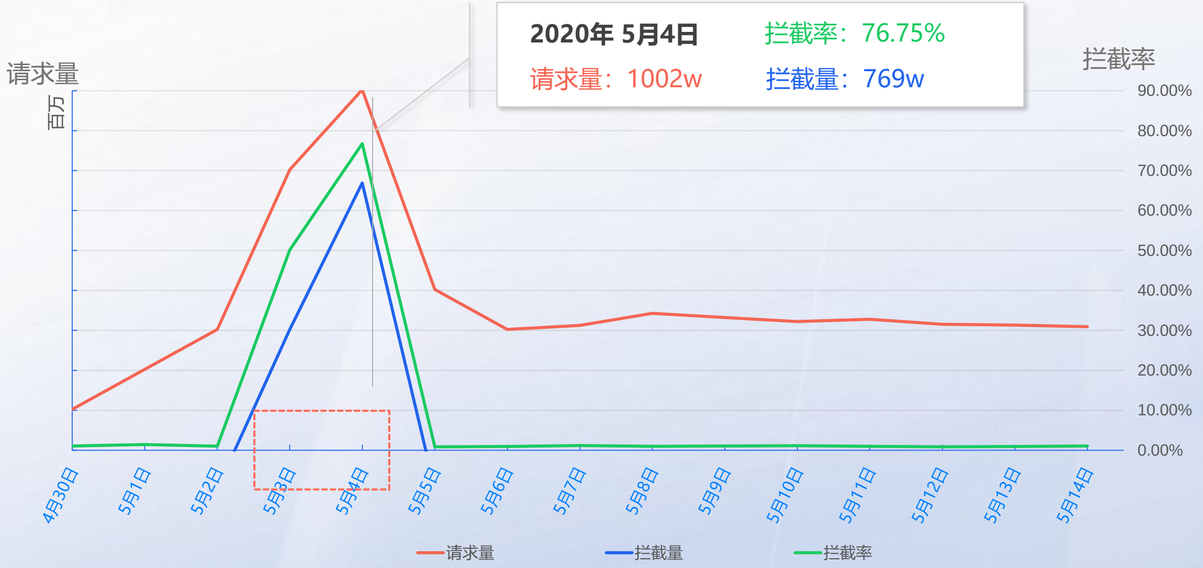
摇红包时请求风控

抽奖时请求风控

春晚4轮互动作弊趋势



作弊请求，随单个红包价值的增加而增加，其中第二轮互动、第四轮互动单个红包价分别高达88元、2019元，相应在二、四两轮互动的作弊情况也相对严重。



抽奖类活动，常见于脚本刷接口、篡改token等作弊形式，短时间内流量激增，拦截率快速上升。5月3日、4日作弊流量被识别，后续黑产放弃，流量回归正常

百度号码安全服务

应用场景

用户

用户寻找企业

用户有联系企业业务情况、投诉、建议等需求，但苦于无联系方式，导致企业与用户沟通的桥梁阻断

目标产品：企业客服卡片

企业

企业获得用户信赖

企业电话联系客户，不易获取信任，导致沟通失败

目标产品：来电名片

筑建深度信任桥梁

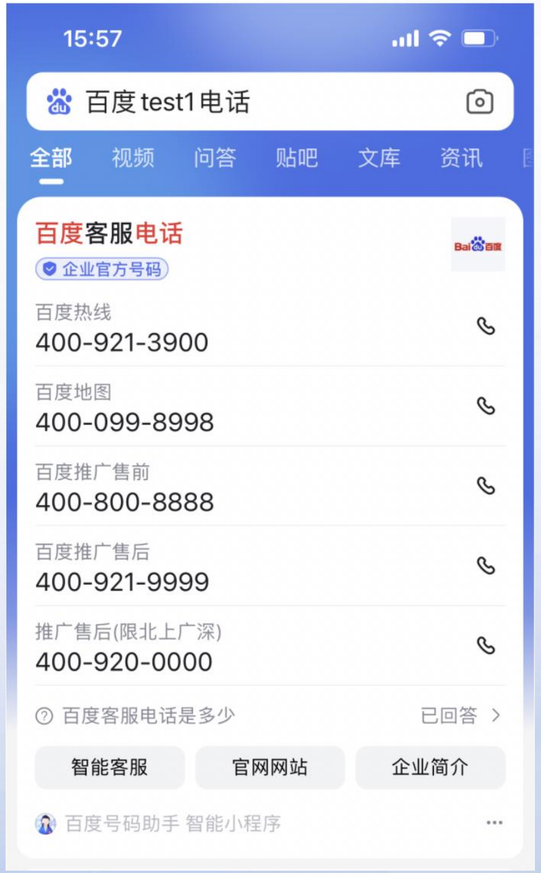
百度安全企业号码认证产品简介

百度安全企业号码认证是根据网民搜索以及企业品牌需求，当网民搜索企业号码相关关键词时展示企业号码认证相关信息的号码卡。

入口

百度客服/
百度售后

Xx电话/xx热线
Xx公司电话/
Xxxxxx电话是什么？



企业认证卡片

产品优势

杜绝恶意标记

官方号码标识，增强权威背书。严格的审核机制，从源头杜绝恶意标记信息。

提升号码曝光

亿级用户流量，更多潜客搜索。支持全称简称、商标以及全量号码相关词搜索，曝光率更高。

建立用户信任

屏蔽错误信息，提升服务质量。排名靠前，样式吸睛，百度官方背书，更能获取客户信任。

树立企业形象

全新升级卡片，实现品牌差异化。支持企业定制化需求，同时增加跳转按钮，满足客户多样个性化需求。

来电名片产品介绍

来电名片是根据企业品牌需求，在个人用户的手机端为企业客户提供品牌展示、号码关联和宣传服务的功能型产品

- 企业电话呼入呼出时，将企业信息呈现在用户手机端，包括**品牌名称、logo、号码**等。
- 助力企业打造移动端品牌商誉，提高外呼电话号码**可信度**、提升**接通率**、高频次展示企业**品牌形象。**

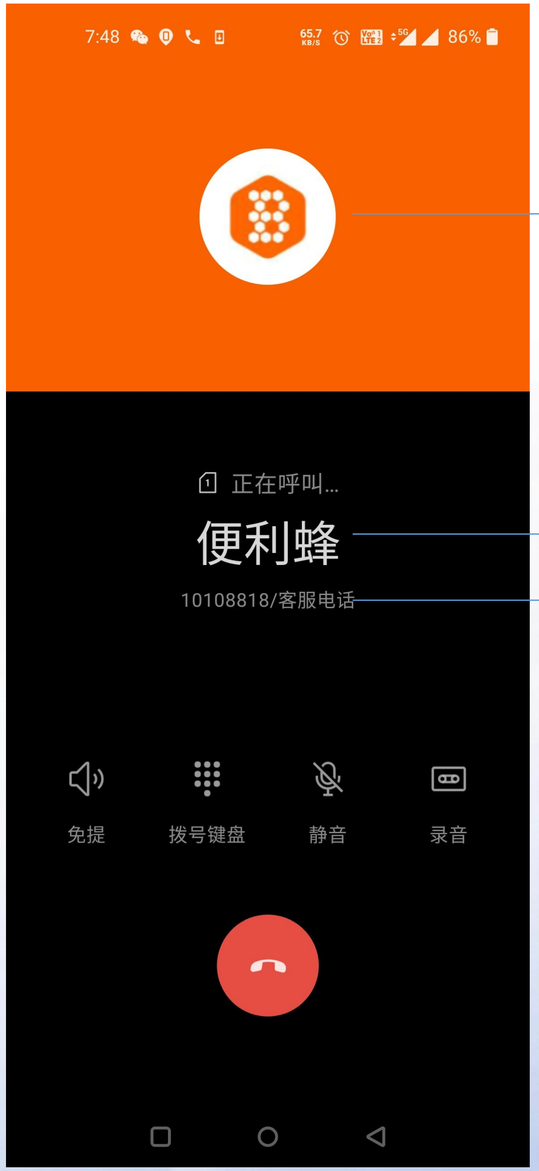
上线案例

客户需求

客户有大量的呼入和呼出需求，希望网民在接到客户的电话时候能够清楚的知道客户情况，提升接通率，同时方便网民进行回拨。

产品权益实现

- 企业电话呼入呼出时，将企业信息呈现在用户手机端，包括**品牌名称、logo、号码**等。
- 助力企业打造移动端品牌商誉，提高外呼电话号码**可信度**、提升**接通率**、高频次展示企业**品牌形象。**



显示logo

显示名称

显示电话

百度短网址

产品介绍

百度短网址（DWZ）

- ✓ 专业生产短网址
- ✓ 质优价低，提供服务质量保证
- ✓ 高级报表—专业用户统计分析
- ✓ 用户画像—细分用户人群，协助营销决策

- **长网址传播受限制?**
- **运营活动数据难以追踪?**

- **短网址缩短字符，易于传播**
- **缩短短网址的同时帮助用户科学分析数据，精准营销**

应用场景

APP分享

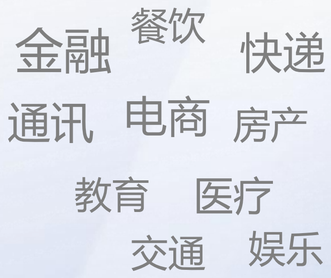
电商、社交、工具等各类app进行社会化分享时可使用短网址接，口，缩短链接便于分享传播。

二维码简化

降低二维码复杂程度,减少二维码像素，提升识别速度及成功率。

短信营销

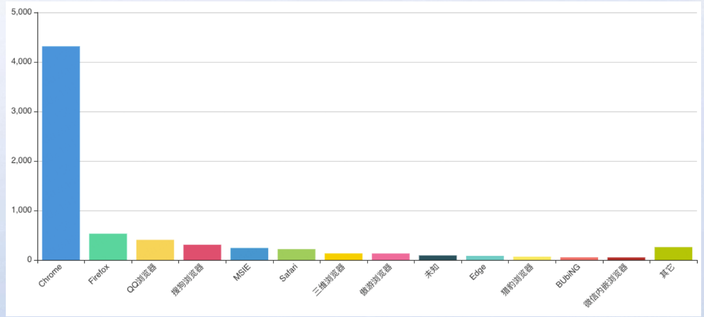
营销短信结合个性化短网址，让客户可以根据短网址点击情况了解短信推广效果。



渠道营销

营销渠道分析/AB测试

分析各大渠道，协助推广决策，优化成本及效率。



独特优势

独一无二性价比

- ✓ 质优价低
- ✓ 计费灵活易懂，多种可选套餐
- ✓ 智能过滤非预期流量，节约成本

专业数据分析

- ✓ 零成本接入，无需埋点
- ✓ 特色高级报表，全面展示网址点击数据
- ✓ 业界领先的大数据画像能力

API简单易用

- ✓ 稳定高并发
- ✓ 二次开发接入简便
- ✓ 提供多语言示例代码

安全 稳定 高可用

- ✓ 稳定性99.99%
- ✓ 安全管控、无恶意广告
- ✓ 1v1技术支持
- ✓ 可定制域名，降低安全风险

百度网址安全检测服务

互联网内容生态安全优势

内容生态恶意网址类型

- 据百度安全监测， 2020年全网日均新增检出恶 意网址2512.4万，同比增长72.48%。网络安全态 势依旧严峻，攻防对抗不断升级。
- 以博彩、色情为主的违法类恶意网址占比高达 98.18%，占比同比持续上升
- 新型电信网络诈骗层出不穷，利益链条更加复杂
- 网站被黑引发“蝴蝶效应”，攻击者逻辑和规则 正在改变

产品简介

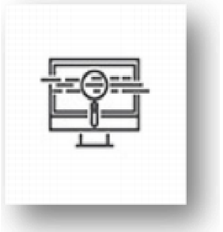
百度网址安全中心

百度网址安全中心是由百度基于安全网址检测库，结合百度大数据分析能力以及安全技术的沉淀，推出的恶意网址信息监测平台。百度网址安全平台为用户提供的服务包括但不限于：网页的恶意代码检测、欺诈信息检测、篡改页面检测。

- 海量恶意网页库
- 先进的智能算法DNN
- 庞大的检测系统计算集群
- 易用高效的开放平台

产品优势

- ✓ 服务稳定：百度的基础服务，稳定性99.99%
- ✓ 安全可靠：基于百度大数据和人工智能技术，研发针对恶意网页的检测算法
- ✓ 数据全面：依托于百度大数据高效的感知能力与集群强大的数据处理能力



API接入灵活

可通过API协议接入,让企业产品即刻拥有安全防护能力

查询结果分类多样化

覆盖欺诈,违法和风险类型,结合产品需求灵活定制防护能力

网站变化动态感知

对网站的新增网页进行动态感知,及时发现可能出现的威胁

多重预警

发现网页出现的威胁内容,多种途径及时反馈

安全态势感知

2512.4万个

全网日均新增恶意网页检出

公民权益维护

41.3万个

全年下线“涉嫌窃取公民个人隐私”网站

恶意网页拦截

777.9亿次

全年全网拦截恶意网页总量

应用场景

搜索

浏览器

社交APP

路由器

百度史宾格安全与隐私合规检测平台

史宾格安全与隐私合规检测平台简介

由百度安全团队打造，基于百度AI、文心一言大模型，围绕个人信息保护领域，根据《网络安全法》、《个人信息保护法》等信息安全的法律法规，建立全新的AI智能检测系统。我们致力于为监管、企业、开发者提供个人信息保护合规技术检测能力，助力移动互联网生态健康发展。

可选检测模式：自动化检测、静态检测、专家检测；

可下载报告：164号文报告、191号文报告、GBT35273检测报告、静态检测报告、google play上架检测、APP用户权益测评报告。

发布机构	依据标准
全国人大常委会	• 《中华人民共和国网络安全法》 • 《个人信息保护法》
全国信息安全标准化技术委员会	• 《GB/T 35273-2020-信息安全技术 个人信息安全规范》 • 《GB/T41391-2022-信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》 • 《移动互联网应用程序（App）收集使用个人信息自评估指南》 • 《网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南》 • 《移动互联网应用程序（APP）系统权限申请使用指南》
国家互联网信息办公室	• 《儿童个人信息网络保护规定》
App专项治理工作组	• 《App违法违规收集使用个人信息自评估指南》 • 《App申请安卓系统权限机制分析与建议》
四部委	• 《App违法违规收集使用个人信息行为认定方法》 • 《常见类型移动互联网应用程序必要个人信息范围规定》
工业和信息化部	• 《关于开展APP侵害用户权益专项整治工作的通知（工信部信管函〔2019〕337号）》 • 《关于开展纵深推进APP侵害用户权益专项整治行动的通知（工信部信管函〔2020〕164号） • 《关于开展信息通信服务感知提升行动的通知（工信部信管函〔2021〕292号）》 • 《关于进一步提升移动互联网应用服务能力的通知（工信部信管函〔2023〕26号）》
电信终端产业协会	• 《移动智能终端与应用软件用户个人信息保护实施指南》 • 《APP收集使用个人信息最小必要评估规范》 • 《APP用户权益保护测评规范》 • 《移动互联网应用程序（APP）用户权益保护测评规范》

产品价值-监管情况

监管部门-四部委

- 中央网信办、工信部、公安部、市场监管总局等四部门召开新闻发布会，在全国范围组织开展App违法违规收集使用个人信息专项治理

史宾格平台-产品优势

AI自动检测 AI辅助检测

- 智能分析识别隐私风险，检测过程**无需人工参与，**生成AI自动检测报告；
- **模拟真机检测，**深入挖掘APP隐私行为。包括隐私政策检测、个人信息收集和使用检测，用户权利保障检测等，生成AI辅助检测报告。

权限/SDK 分析

- 基于市面上最全的SDK特征库和权限API映射关系数据库，实现自动化检测最全的集成的第三方SDK，**解决第三方SDK的权限使用不可控的难题；**
- 快速检测敏感敏感权限，详细**划分权限使用场景，**精准**定位代码位置**并进行可视化展示
- 针对于申请权限和使用权限实现精准定位**过度申请权限、冗余权限。**

专家模式

- 将专业检测能力与经验封装为普适性工具，大大降低合规审核技术门槛；
- 将专业检测能力与经验封装为普适性工具，大大降低合规审核技术门槛；
- **数据统计总览。**检测结果一目了然。

检测报告 及堆栈

- 自动化检测报告和专家模式检测报告均包含问题描述、改进建议、截图存证等内容，相比于其他竞品报告清晰简洁；
- **堆栈信息丰富，**开发者通过堆栈即可找到问题代码。

史宾格平台-能力架构


史宾格安全及隐私合规管理
企业级
支持多角色
App
SDK
核心功能
AI自动/辅助检测
隐私专项检测
专家模式
权限及SDK分析
技术支撑
SDK数据库
应用类型库
最全API映射数据库
隐私行为合规分析库
法律法规库
专项合规性检测报告
《工信部信管函〔2020〕164号》
《APP违法违规收集使用个人信息行为认定方法》
《移动互联网应用程序（App）收集使用个人信息自评估指南》（2020）
权限及SDK自查报告
真机场景模拟自查报告
App隐私合规AI自动检测报告
App隐私合规AI辅助检测报告
合规指引
隐私专家APP隐私合规评估报告
App开发合规指引服务
病毒&漏洞检测报告
静态代码检测
完整的第三方SDK特征库
权限到API的映射关系数据库
详细展示嵌入第三方SDK
详细展示申请使用的权限
可视化敏感权限和代码位置
AI场景检测
基于深度学习的应用场景识别
智能识别隐私政策弹窗告知
输入型个人信息场景检测
隐私行为监控
典型应用运行场景模拟
隐私敏感行为溯源
合规性检测
基于NLP的隐私政策理解
对齐国家发布的法律法规
个人信息跨境传输风险
个人信息明文传输风险
内容违规风险检测
隐私专家合规辅导
APP隐私合规评估报告
专家人工解读报告
App开发合规指引服务
隐私合规产研培训
隐私合规技术沙龙

合作案例

监管机构

- **合作场景：**支撑监管进行APP违规风险检测、专项行动
- **服务类型：**私有化部署、人工检测

汽车厂商

- **合作场景**：车机自身APP合规检测及车机分发APP检测
- **服务类型：**SAAS平台、人工检测报告
- **代表客户：多家知名车企**

协助应用市场

- **合作场景：**工信部要求应用分发平台应加强上架审核责任
- **服务类型：**基于工信部164号文的API检测能力
- **代表客户：多家头部手机厂商**

游戏公司

- **合作场景**：满足监管的APP合规要求、通报下架整改、应用商店上架、日常版本发布前的自查自测
- **服务类型：** SAAS平台、私有化部署
- **代表客户：多家知名游戏公司**

互联网公司

- **合作场景**：满足监管的APP合规要求、通报下架整改、应用商店上架、日常版本发布前的自查自测
- **服务类型：**SAAS平台、人工检测报告、私有化部署
- **代表客户：知名头部互联网公司**

央国企、外企及其他

- **合作场景**：满足监管的APP合规要求、通报下架整改、应用商店上架、满足企业内部自查
- **服务类型：** SAAS平台
- **代表客户：知名媒体、银行、消费行业公司**

百度应用加固与安全检测

需求场景

应用安全 + 政策监管

通过应用加固与安全检测相关技术，保障应用安全

- 应用加固：程序防篡改、防盗版、反调试、文件加密、数据加密，代码和知识产权保护
- 安全检测：检测APP存在的漏洞风险，提供风险说明和修复建议
- 风险管理：对APP的风险进行收集统计，通过设置策略进行风险修复

满足国家法律、法规对应用的监管要求，保证应用合法、合规上线

- 工信部、公安部等不定期监管
- 各地通信管理局执行监管
- 等保2.0过检需求

产品简介

安卓应用加固　iOS应用加固　SDK加固　游戏加固　安全编译器

安全性更高　兼容性更强
性能更优越　服务更专业

百度应用加固，是百度安全旗下一款面向智能终端应用的安全加固产品和服务，依托百度公司20年的安全实践和技术积累，已拥有多项安全专利和行业资质。产品包括不限于代码保护、数据加密、运行时防护等数十项加固能力，可全面提高智能终端应用的安全指数，同时满足工信部及各地方监管部门的合规需求。

百度安全检测

为APK、IPA、SDK提供自动化应用检测及报告服务，报告提供风险说明及修复建议，帮助客户及时发现漏洞及风险，提高APP安全防护能力。

百度应用安全检测平台

Android应用检测

自我保护能力

应用自身安全

- 应用权限
- 应用行为
- 恶意代码
- SDK

应用源文件安全

- APK文件
- SO文件
- 资源文件
- Java代码

内容安全

- 敏感词
- 敏感图片

数据保护能力

本地数据存储安全

- WebView存储
- 数据加密/解密
- 数据读写漏洞
- 敏感信息残留

内部数据交互安全

- 组件数据交互
- Intent数据交互
- 敏感信息泄露漏洞

通信数据安全

- HTTP传输
- HTTPS弱校验

安全防护能力

身份认证安全

- 界面劫持/截屏风险
- 输入监听

恶意攻击防范能力

- WebView漏洞
- 第三方库漏洞
- 不安全的API调用
- ELF配置
- 开放端口
- Root、模拟器检验
- 动态注入
- 拒绝服务攻击

iOS应用检测

应用自身安全

- 第三方SDK漏洞

通信数据安全

- 不安全的网络连接
- ZipperDown漏洞
- AFNetworking SSL中间人漏洞

本地数据存储安全

- NSLOG未关闭
- malloc内存泄露风险

恶意攻击防范能力

- WebView漏洞
- 第三方库漏洞
- 不安全的API调用
- 弱加密算法
- 弱哈希算法
- 弱随机函数
- 调试风险
- PIE标志未开启
- SSP标志未开启
- ARC标志未开启

产品核心优势

安全性更高

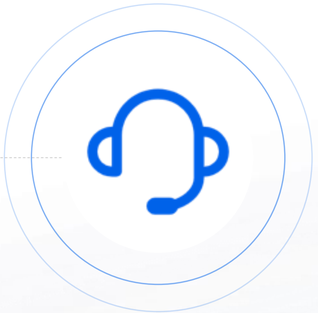
- 全数据加密保障。
- 累计服务千余家客户，拥有高稳定性，加固后零破解。
- 符合百度系产品高安全性标准规格，稳定应用于百度系各业务线。

兼容性更强

- 适配市面上TOP600机型。
- 兼容Android4.0至最新**Android14**，兼容AAB格式，兼容iOS最新版本和各类iOS设备。
- 加固技术能力支持Android/iOS/Linux/Windows/MacOS/等多种操作系统。

性能更优越

- 安卓加固后，APP体积增长不超过2M，CPU占用率增量不超过5%，内存占用率增量不超过10%，首次启动时间增量不超过2秒
- iOS加固后，内存影响不超过5%，体积影响不超过30%，性能影响不超过10%



服务更专业

- 自研自营，资深工程师及运营团队提供专业售前售后咨询服务，7*24，高质高效。
- 针对不同类型客户和使用场景，提供多种接入方式。
- 可提供APP安全解决方案（应用加固+漏洞扫描+隐私合规等）。

— 累计覆盖超3亿智能终端设备，服务6万余应用，超500万次加固 —

客户案例 | IoT

项目背景

- 客户为是全球知名电视品牌，4K电视系列和55-59英寸系列的出货量份额均位居全球前三。
- 该品牌电视预安装几十款APP，为用户提供影音娱乐、资讯、游戏等多场景服务。

需求分析

- 电视上预装的所有APP都需要进行加固，对APP中的所有文件和数据进行加密保护，防止APP被破解，保护自身的知识产权
- APP数量较多，需针对不同账号区分加固权限，加强对不同账号的加固内容管控

百度方案

- 提供线上标准公有云加固服务
- 公有云服务账号体系包含主子账号，管理员账号设定子用户可加固APP的数量和包名

客户收益

- 几十款APP通过加固后，实现对文件和数据的全加密保护，没有出现被破解情况。
- 百度的加固方案一方面保护了终端用户利益，一方面保护了客户口碑不受损
- 加固的主子账号体系满足海信对不同账号的加固权限管控

客户案例 | 金融

项目背景

- 客户为省级知名银行，对外提供服务有多种方式，通过APP提供线上服务是其中一种。

需求分析

- 客户APP分为安卓和iOS两个客户端，都需要加固，且金融行业对安全性要求极高。在加固服务基础上，需定制SDK满足APP运行环境检测的要求。
- 所有服务均以私有化部署形式提供，部署在客户自己的服务器上。

百度方案

- 基于百度应用加固的公有云服务和最高等级的加固保护能力，提供私有化部署方案
- 针对银行类APP，开发全方位的APP运行环境检测SDK，满足客户的定制化需求

客户收益

- 客户APP使用百度应用加固后可稳定运行，加固后APP性能不受影响
- 最高等级的加固保护能力和定制的SDK，使客户APP安全性得到全方位保障，满足需求
- 客户可在内部网络环境中使用加固服务，无需把APP上传到公有云环境

百度商用密码安全合规解决方案

商密合规检测重点行业

金融领域

使用金融 IC卡 、 动态令牌、 智能密码钥匙等实现对客户身份、 服务器等进行认证;

使用密码技术， 实现对系统存储的用户口令 、用户隐私信息、 重要交易数据等的加密保护 。

电力领域

发电环节， 基于商用密码的电子认证体系， 实现调控指令的可靠执行。 输电环节， 采用数据加密、 身份鉴别方法，包装输电环节安全。

变电环节， 通过部署纵向加密装置， 保证业务传输数据安全及身份认证 。

电子政务领域

利用密码技术增加安全防护， 确保网络数据的安全传输。

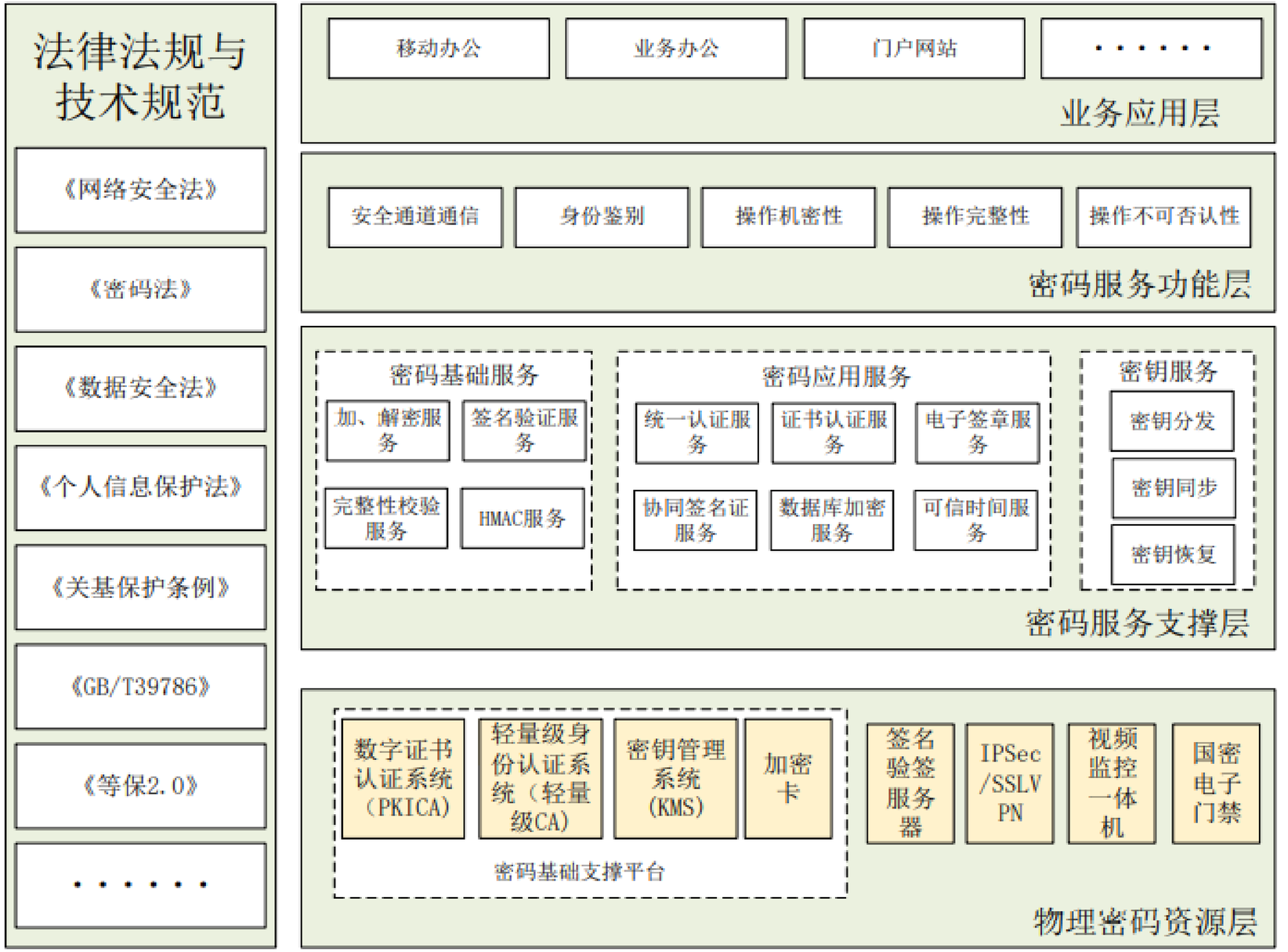
基于 PKI技术的电子认证， 对网络上传输的数据进行加密、 解密。

采用 SM9 算法和数字签名实现身份认证和邮件内容加密。

信息网络领域

密码安全协议包括： 优先局域网安全TLSec 技术、无线局域网安全WAPI技术、IP安全可信TISec技术、 射频识别RFID空中接口安全TRAIS技术等。

商密应用技术架构


法律法规与技术规范
《网络安全法》
《密码法》
《数据安全法》
《个人信息保护法》
《关基保护条例》
《GB/T39786》
《等保2.0》
· · · · · ·
移动办公
业务办公
门户网站
· · · · · ·
业务应用层
安全通道通信
身份鉴别
操作机密性
操作完整性
操作不可否认性
密码服务功能层
密码基础服务
加、解密服务
签名验证服务
完整性校验服务
HMAC服务
密码应用服务
统一认证服务
证书认证服务
电子签章服务
协同签名证服务
数据库加密服务
可信时间服务
密钥服务
密钥分发
密钥同步
密钥恢复
密码服务支撑层
数字证书认证系统（PKICA）
轻量级身份认证系统（轻量级CA）
密钥管理系统(KMS)
加密卡
密码基础支撑平台
签名验签服务器
IPSec/SSLVPN
视频监控一体机
国密电子门禁
物理密码资源层

商密安全合规解决方案价值

一站式交付

只需一套产品及服务，无需投入过多人力、过多对接联调、客户就能取得60分以上效果；以“物理和环境安全”改造为例：外装设备就能够实现满分效果，无需对原有系统进行工程化的改造，插电即用；

覆盖新型物联网业务场景

满足由物联网组成的数智化新型业务系统，密改指标要求的“物理和环境安全”、“网络和通信安全”、“设备和计算安全”、“应用和数据安全”密码应用合规；

全包式跟踪服务

专业咨询规划，综合解决方案，密码项目建设，后期运行维护全流程的服务，密评不迷茫；

安全合规

符合《网络安全法》、《密码法》、《网络安全审查办法》、《国家政务信息化项目建设管理办法》等系列法律法规，以及GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》等相关密码应用要求，信息安全等级保护2.0信息系统建设/整改需求。

产品介绍-PKI-CA

PKI CA证书管理系统

实现为人员颁发网络中的“身份证”，实现人员在网络中的可信身份认证，保障真实性、机密性、完整性和不可否认性。

符合国家规范，具备自主知识产权

支持双证书、双中心，即加密证书/签名证书和CA认证中心/密钥管理中心。

统计分析

提供证书的分发记录、统计、分析等功能，满足审核、监督和合规性要求。

技术先进性

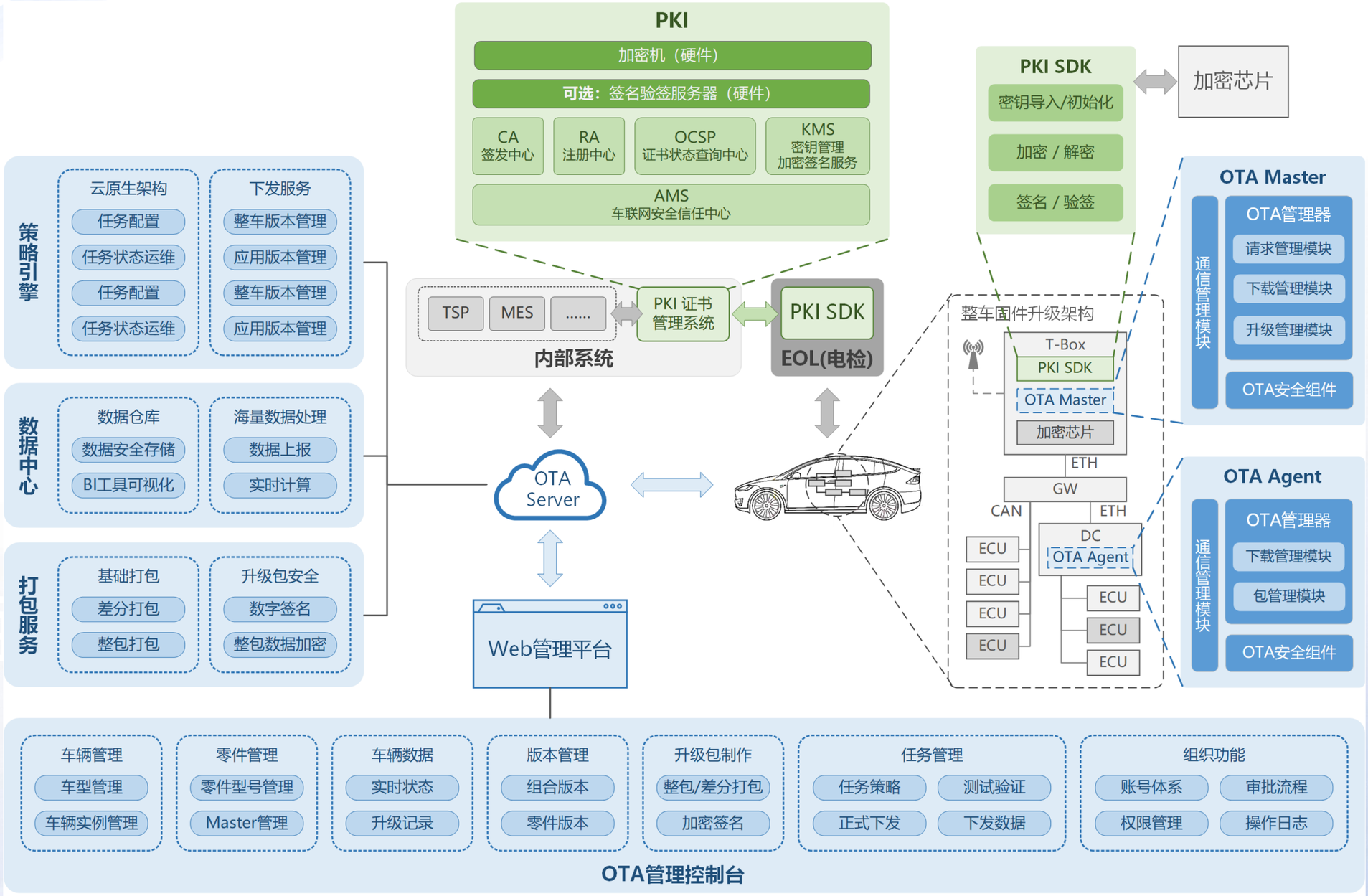
通过整合电子认证技术，实现认证服务中间件体系，构建异构集成环境，构建安全可信的认证环境

为云安全提供身份认证、数据安全传输及访问制管理等机制，可以较好的解决云平台所面临的安全问题

解决了网络中人员的身份认证、电子签名核心需求。

百度整车OTA解决方案

OTA技术方案 | 整体方案



OTA技术方案 | OTA管理平台-车辆及零件管理

车型管理

平台提供车型管理功能，支持管理配置字、动力总成、结构区别号、配置等信息，在车型下管理车辆、车组及零件

车辆管理

平台自动绑定上报的激活车辆，同时支持导入车辆信息；平台实时获取车辆状态、零件列表、升级历史、地域等信息

车组管理

平台支持通过自定义标签（如地区、批次）对车辆进行分组，同一台车支持多个标签，筛选标签可获得车辆列表

零件管理

平台支持维护零件图号、供应商、型号、批次等信息；可通过筛选零件图号查询实际安装车辆的VIN及其对应的软件版本

质量保障 | 全链路安全保障

平台安全

数据安全

网络安全

车端安全

身份验证
密码规范要求及身份认证限制

研发流程安全 自研 专利
百度自研“猫头鹰”“啄木鸟”等Web平台漏洞扫描平台，确保Web开发流程安全性

整包加密
全生命周期保障升级包机密性，防止升级包核心数据泄露

数据签名
阻止升级包恶意篡改攻击，保障设备仅信任平台签发的升级包

完整性校验
防止升级包传输过程出现篡改或损坏

HTTPS
基于HTTPS的安全网络访问协议

对接PKI
所有证书、密钥的生成和存储均基于PKI服务实现，确保密钥安全性

通信加密
基于AK/SK的安全授权访问方案，实现车型（产品线）间隔离，并支持基于HTTPS之上的二次数据加密

升级过程安全
充分考虑到车辆的内外部环境，确保只有在符合条件是才运行进行升级

车辆认证 自研
只有云端录入过的车辆才允许进行初始化，初始化后车辆必须通过AK/SK授权才能进行云端访问

百度优势 | 专业的汽车OTA & PKI供应商

1

二次开发支持

- 百度整车OTA系统可支持定制化的二次开发，车端基于状态机方式，提供了大量基础不变的底层接口，可实现超便捷的二次开发。

2

百度技术保障

- 基于百度先进的云端技术框架、安全技术及数据分析能力，确保OTA系统稳定性、高效性、安全性
- 百度具备大量行业顶尖的技术专家、行业专家以及安全专家

3

自研PKI

- 百度具备成熟的自研汽车PKI产品，符合国家认证体系要求
- 百度OTA原生支持自研PKI产品，可实现快速适配，降低交付风险

案例介绍 | 某知名品牌乘用车OTA

项目背景

某知名品牌需面向个人消费者的全新纯电SUV需要支持整车OTA升级，需要搭建云端OTA管理平台并实现车端整车升级功能。车型采用最新自研的以太网域控SOA架构，支持整车超过30个ECU的升级功能。

百度方案

百度提供了支持整车所有ECU FOTA升级的完整车云一体解决方案，云端OTA Server采用了最先进的车辆影子系统作为核心，支持百万级并行升级能力，为客户提供了安全、稳定、高效的OTA运营管理服务。车端采用了百度最新的全状态机车端OTA Master架构，极大的提高了客户后续二次开发便利性。

百度汽车VSOC&IDPS安全解决方案

汽车网络安全运营平台（VSOC）

为汽车场景客户提供安全态势感知和数据分析、安全运营、安全响应等一系列安全能力。

技术人员

公司领导

客服售后

运营人员

技术人员

云端 VSOC

态势感知 | 安全运营 | 安全响应

车端 IDPS

系统入侵检测 | 网络入侵检测 | 静态防御 | 动态防御

车端数据　应用数据

云端数据　风险管理

风险预警　安全工单

策略修复

态势感知和数据分析

- 车辆活跃统计
- 风险事件多维度展示
- 风险实时播报

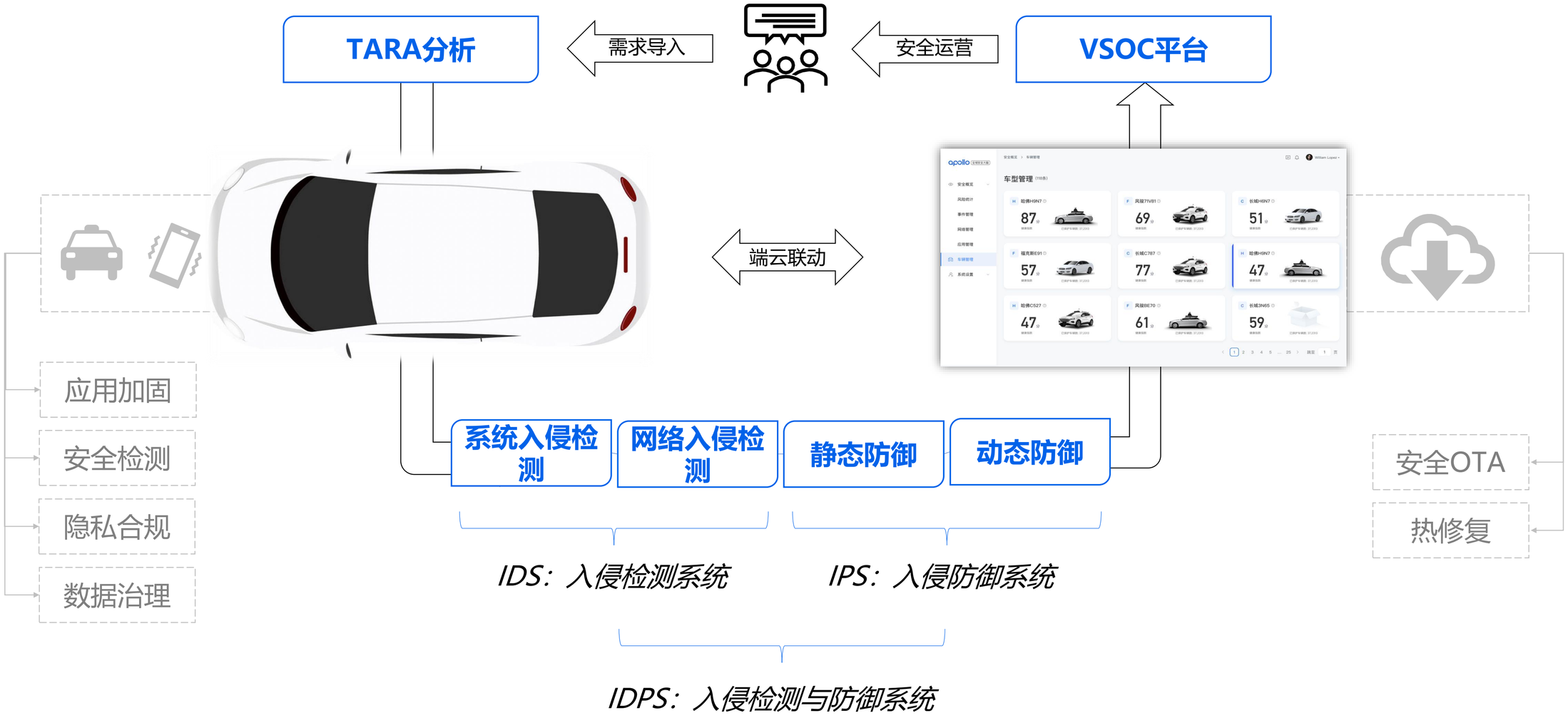
安全运营

- 车端、零件查询定位
- 车机端和手机端应用查询
- 云端服务器数据汇聚打通
- 针对车辆风险漏洞的管理

安全响应

- 发现车辆风险事件及时报警
- 风险通过工单处理、可追踪
- 多维度风险修复策略

汽车信息安全IDPS产品架构



成功案例-某知名品牌车厂

项目背景

- 某知名品牌车厂，某车型汽车出口海外，需要满足R155信息安全相关认证，同时完成咨询、测试、认证、VSOC上线等，需要有经验的供应商提供解决方案。

需求分析

- 合规性：出口海外的车型，要通过R155相关安全认证。
- 安全性：针对TBOX、IDC、IVI、车内车外通信等各零部件和整车系统，需要做入侵检测与防御，并通过统一平台进行管理。

百度方案

- 百度提供IDPS和VSOC解决方案，收集和处理车内外的网络安全相关信息；提供数据关联和分析能力；提供风险管理、事件和漏洞响应管理等工作流的集成能力等等。

客户价值

- 满足汽车海外车型的合规性、安全性
- 满足车型全生命周期对网络安全、数据安全和隐私保护的多重要求

THANKS

百度智能云官网：https://cloud.baidu.com

百度安全官网：https://anquan.baidu.com

百度安全公众号