第四届全国网络与信息安全防护峰会

云中利剑——百度云查杀

冯侦探

fengzhentan@baidu.com

百度安全实验室

大纲

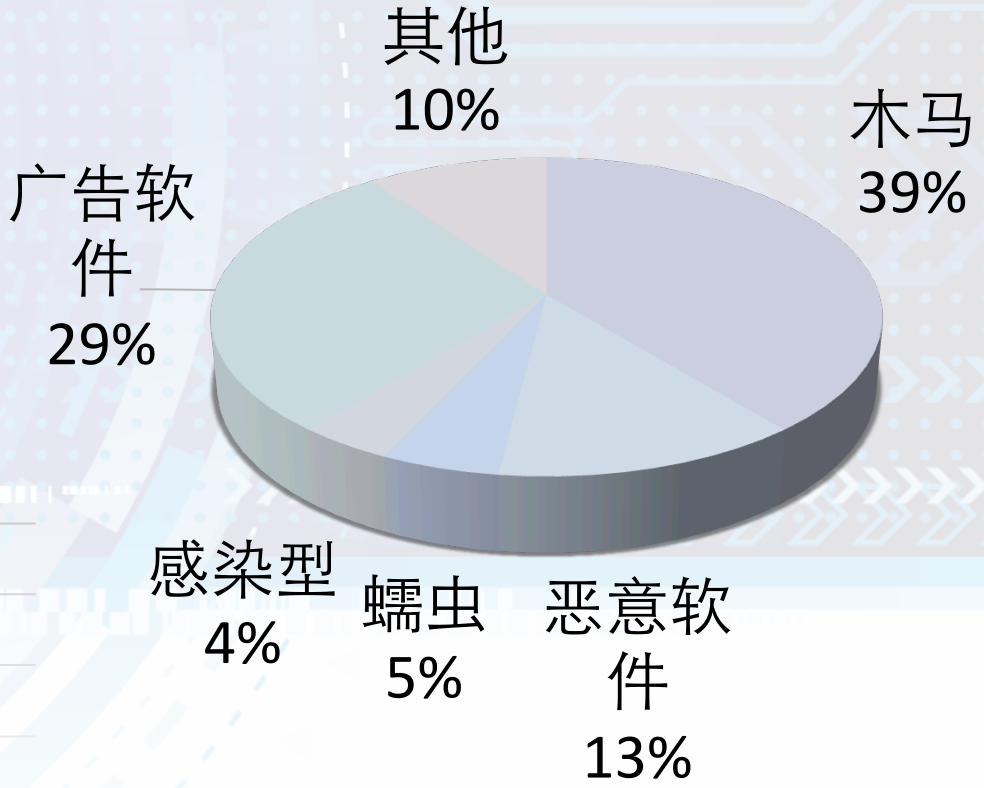
- 安全现状

- 云端安全体系概述
  - ✓ 文件云
  - ✓ 特征云
  - ✓ URL云

- 大数据时代的安全
  - ✓ 云端智能启发式引擎
  - ✓ 威胁情报数据平台

现状

- 恶意风险类型
  - ✓ 木马、广告为主
  - ✓ 欺诈、漏洞、挂马网站
  - ✓ 灰色化、隐蔽、复杂

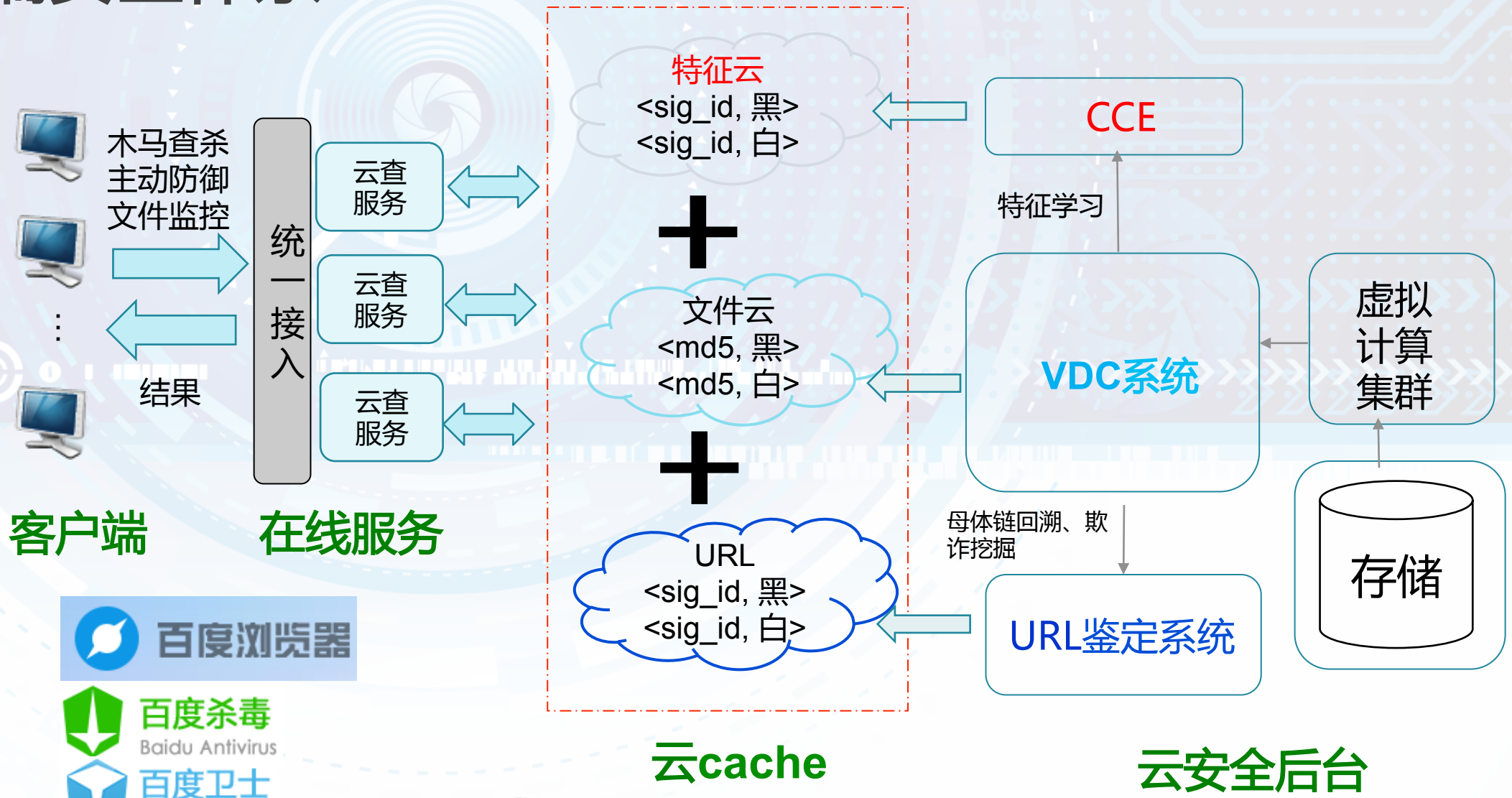


样本类型分布

大纲

- 安全现状
- 云端安全体系概述
  - ✓ 文件云
  - ✓ 特征云
  - ✓ URL云
- 大数据时代的安全
  - ✓ 云端智能启发式引擎
  - ✓ 威胁情报数据平台

云端安全体系

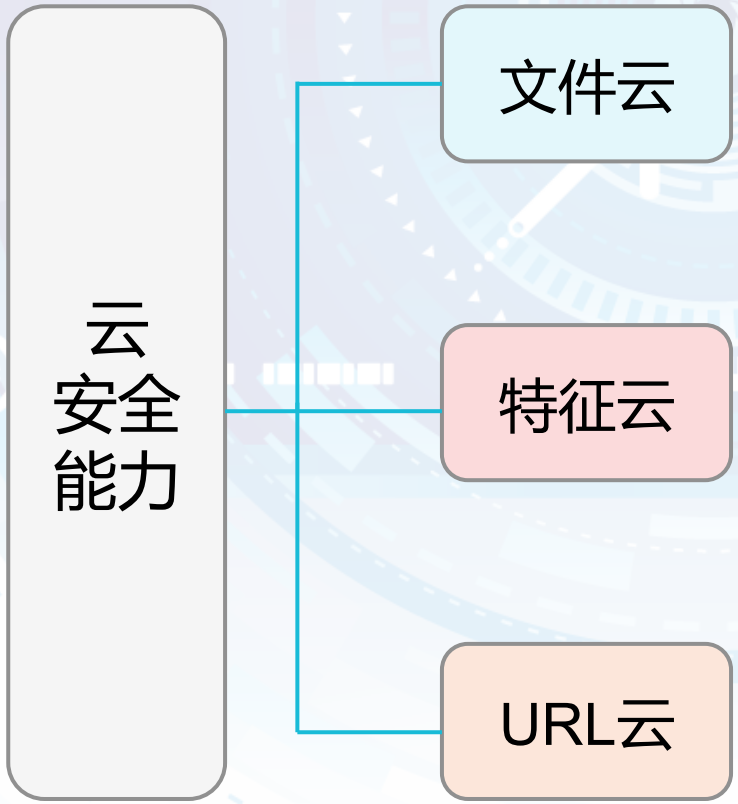


百度浏览器

百度杀毒 Baidu Antivirus

百度卫士 Baidu Guard

云端安全能力



云安全的核心
16亿样本文件，存储6+PB。
覆盖全网用户98.2%的查询请求

常规云查杀

文件云的强力补充
检出率：85%
误报率：0.001%
扫描速度：249个/秒

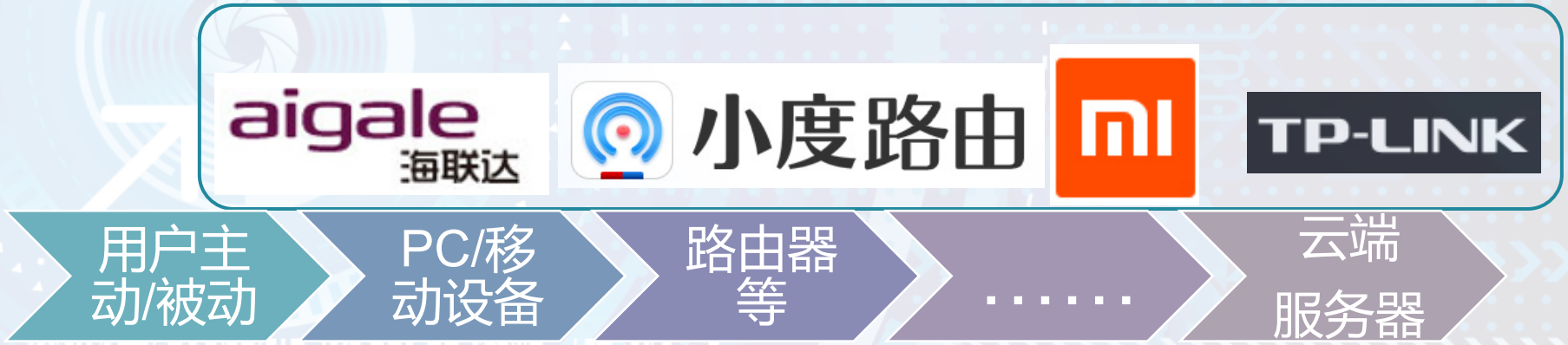
专注未知文件

欺诈、挂马、漏洞的克星
自研DB条目：20亿条
单URL检测响应时间：<10s

虚假欺诈网站
链路层检测

全链条立体防御

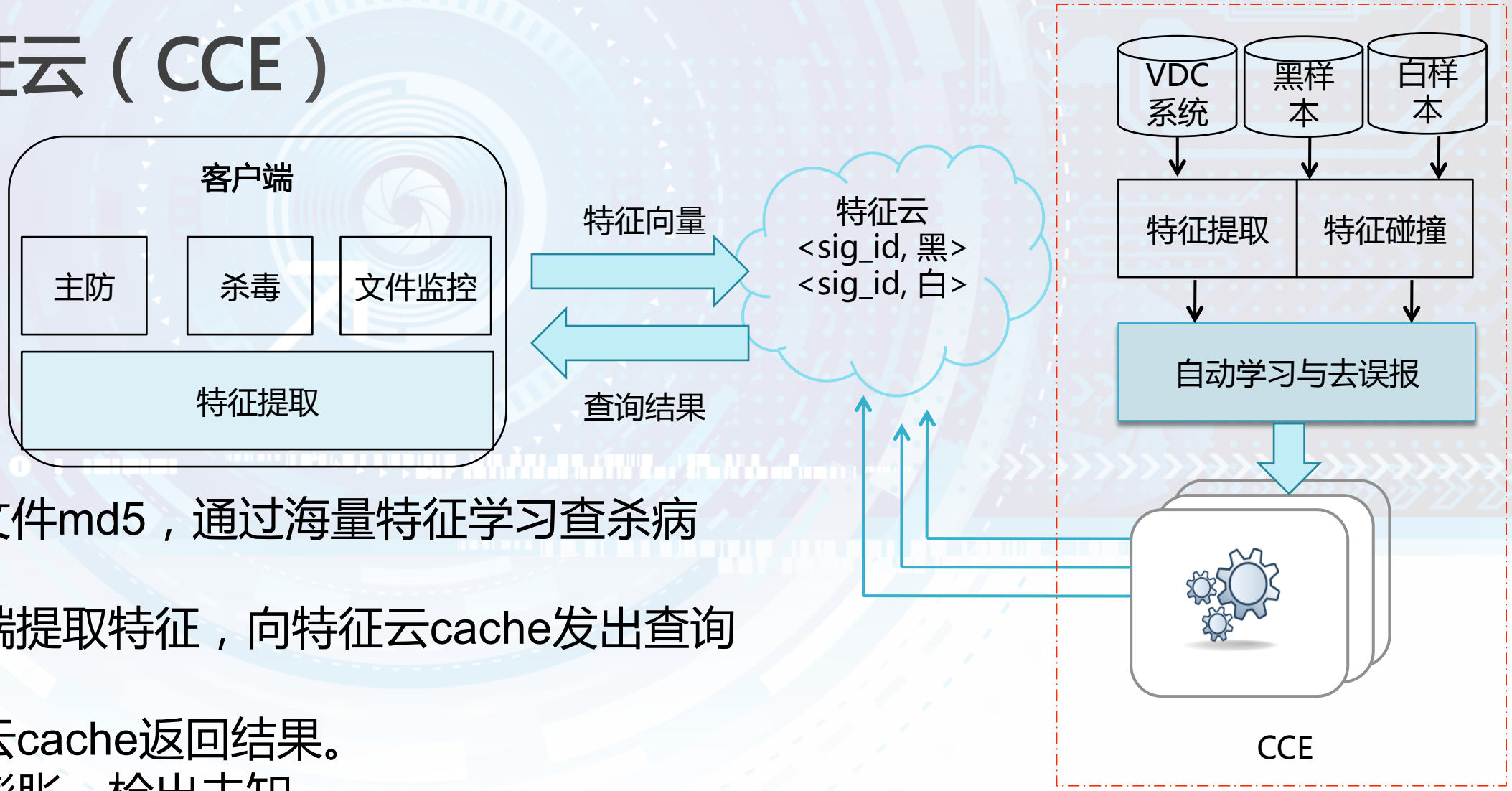
用户上网环节



文件云——VDC系统

- 云安全平台

特征云（CCE）

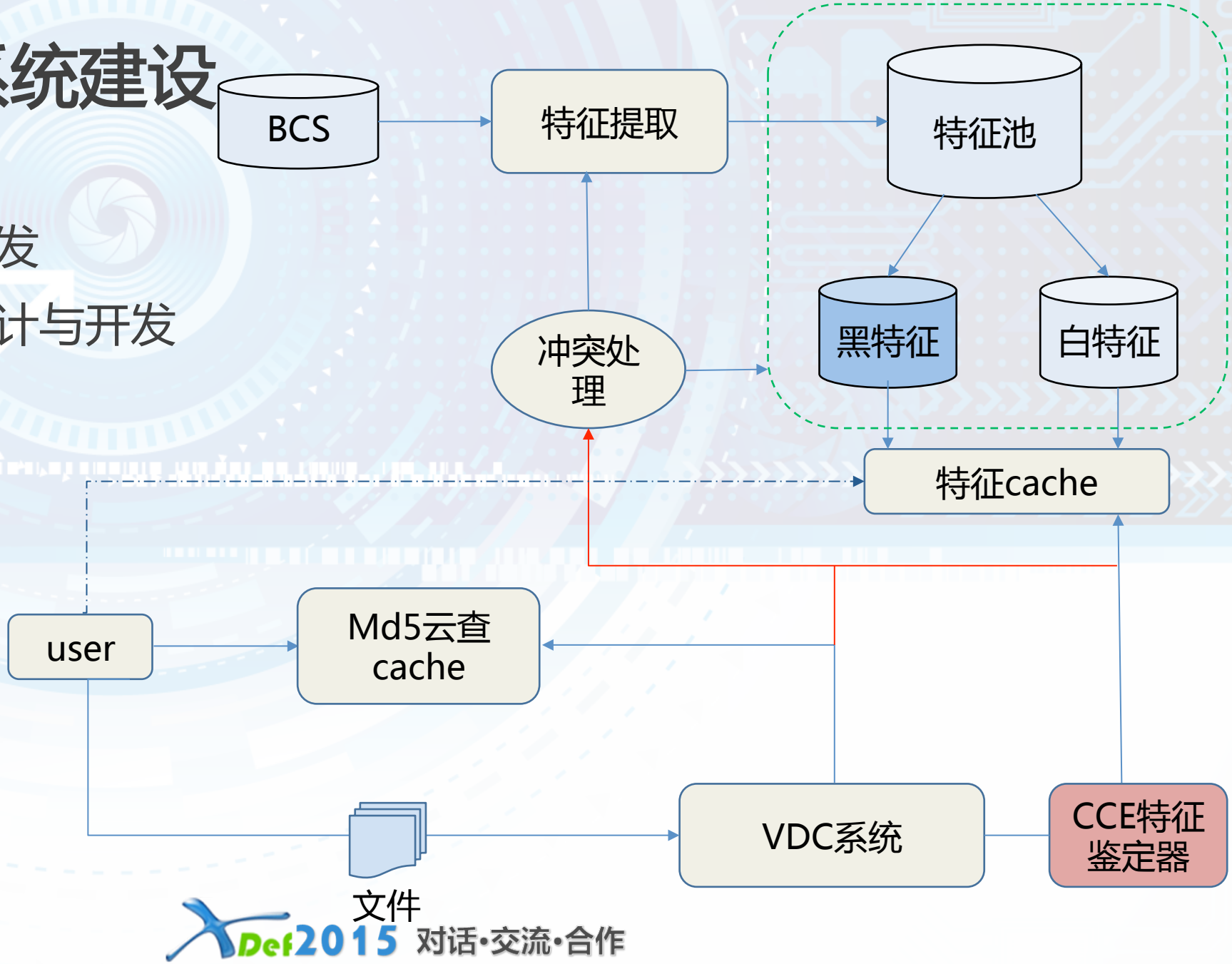


不依赖文件md5，通过海量特征学习查杀病毒变种：

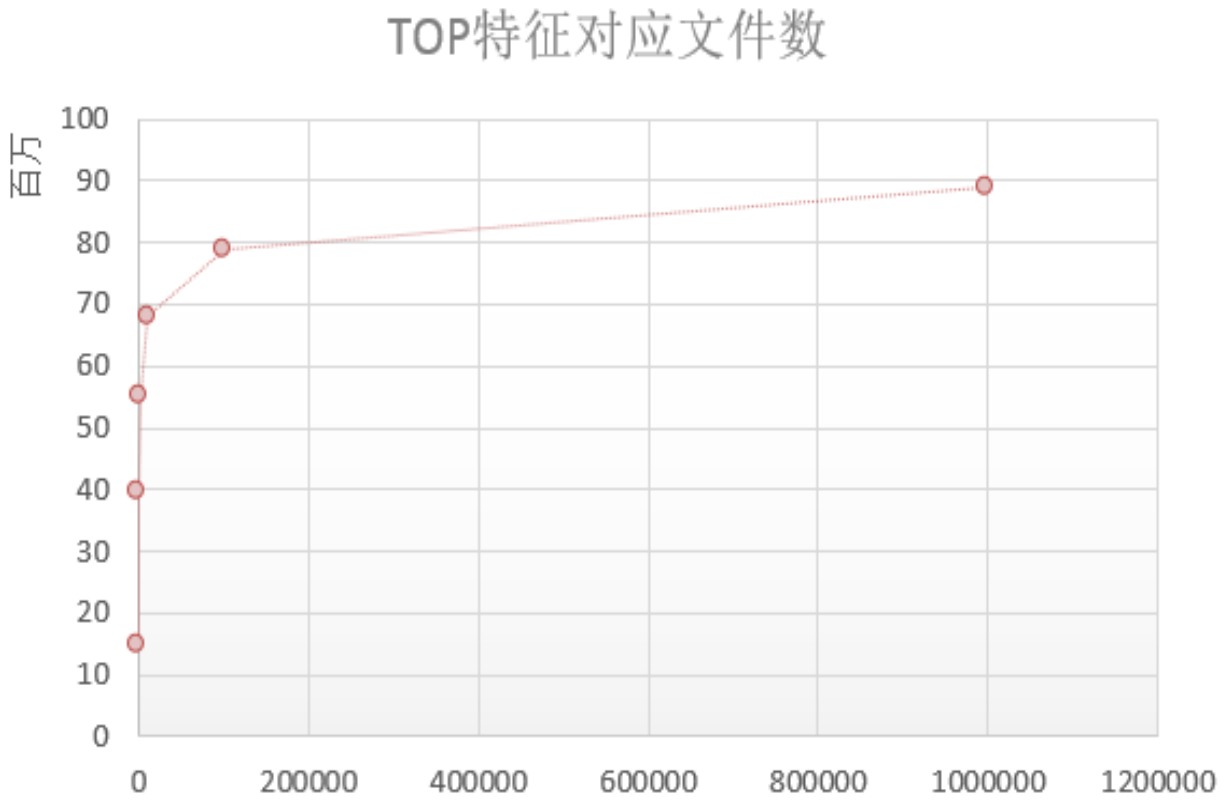
1. 客户端提取特征，向特征云cache发出查询请求。
2. 特征云cache返回结果。
3. 控制膨胀，检出未知

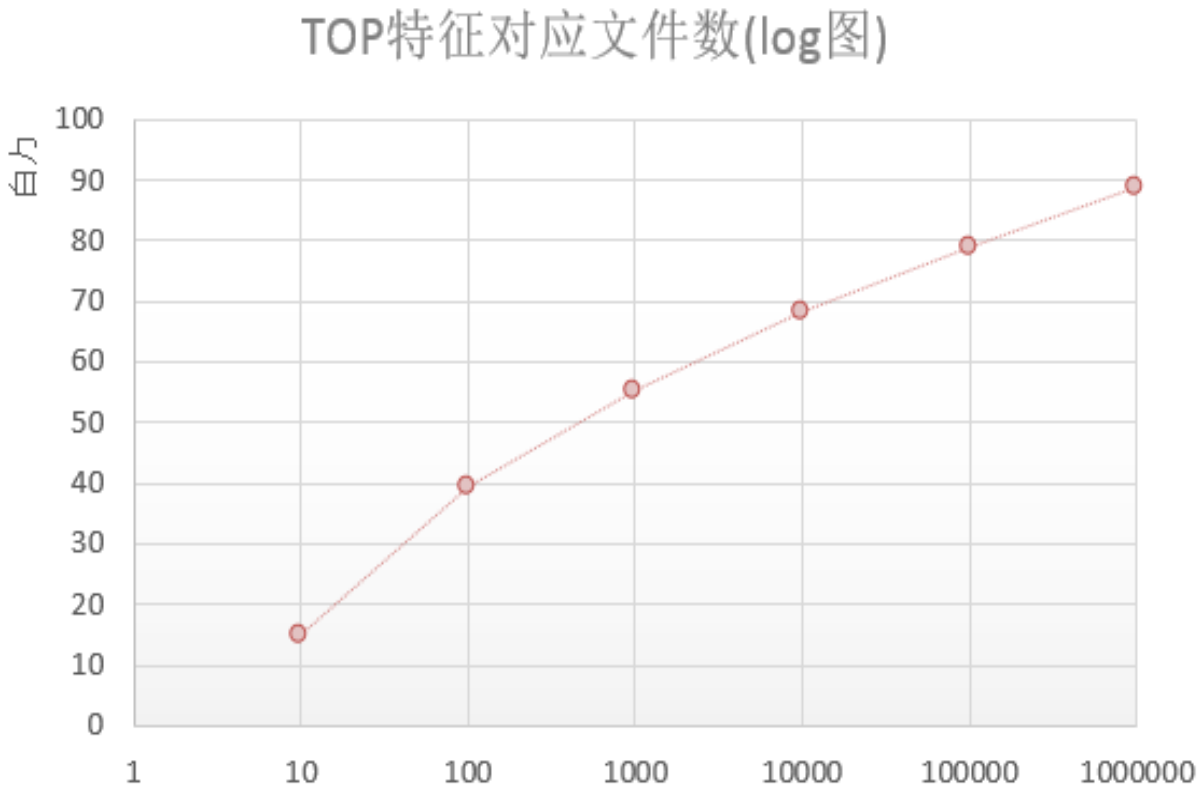
特征云——系统建设

- 特征提取
  - ✓ 特征提取程序开发
  - ✓ 特征池的库表设计与开发
  - ✓ 特征提取的监控
- CCE特征鉴定器
  - ✓ 用于冲突检测
  - ✓ 校准特征库
- 冲突处理
  - ✓ 人工+自动流程
- 特征cache
  - ✓ 自动更新



特征云


TOP特征对应文件数
百万
100
90
80
70
60
50
40
30
20
10
0
0
200000
400000
600000
800000
1000000
1200000

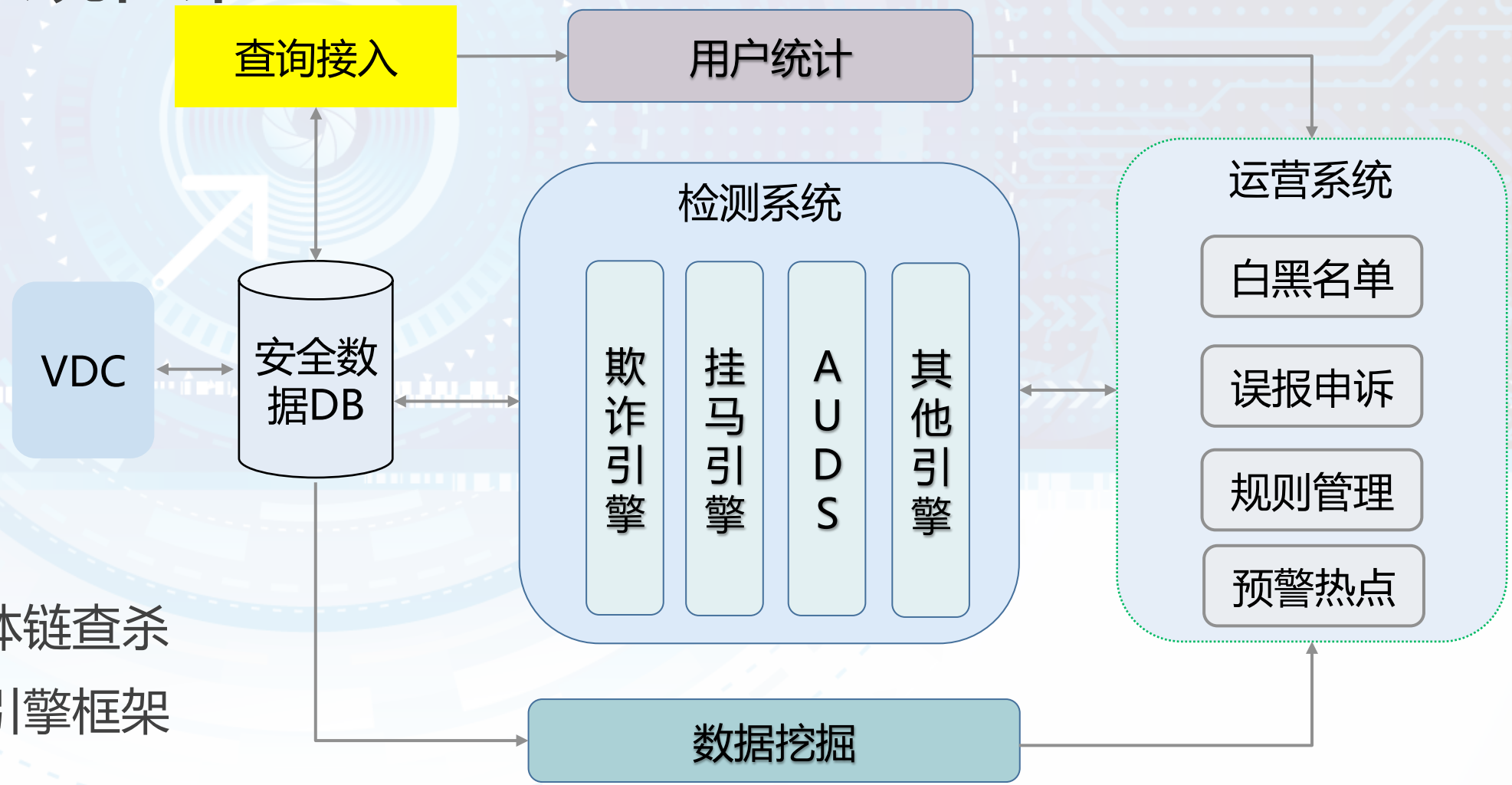

TOP特征对应文件数(log图)
百万
100
90
80
70
60
50
40
30
20
10
0
1
10
100
1000
10000
100000
1000000

URL云

- 威胁形式


欺诈
金融证券
虚假中奖
虚假购物
虚假招聘
仿冒银行
虚假票务
模仿登陆
虚假药品
挂马
下载恶意程序
网页内嵌恶意代码
漏洞
挖掘
参透
扫描
违法
违法色情
违法博彩
违法政治

URL云系统框架



- ✓ 溯源母体链查杀
- ✓ 插件式引擎框架

大纲

- 安全现状
- 云端安全体系概述
  - ✓ 文件云
  - ✓ 特征云
  - ✓ URL云
- 大数据时代的安全
  - ✓ 云端智能启发式引擎
  - ✓ 威胁情报数据平台

引擎发展趋势

- 智能启发式云安全引擎（3.0）
  - ✓ 依托大数据、方兴未艾

1.0时代
（2009年前）

- Signature-based
- 传统的人工运营分析特征
- 定时更新特征库

本地化

2.0时代
（2009~2012）

- Cloud-based
- 云端海量样本存储
- 云端丰富的样本+运营体系
- 本地传统引擎更轻快
- 响应更加迅速
- 依托海量用户基础更有效

一体化

3.0时代
（2012~今）

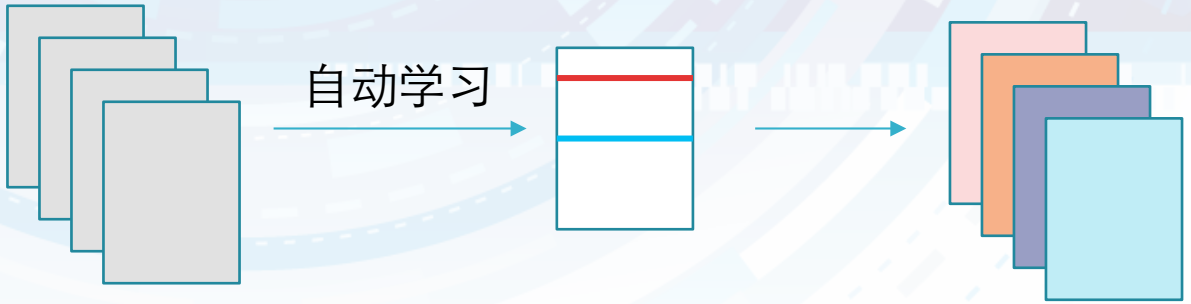
- SVM, DTree, ANN, Deep Learning 等数据挖掘技术
- 传统引擎弱化，启发引擎变强
- 技术更灵活，云端训练，客户端检测；亦可直接云端部署。
- 云端根据客户端反馈调整学习训练策略
- 云端能力第一时间可达客户端
- 云端本地多种引擎技术互相结合，更难“免杀”
- 技术“立体化”，“智能化”

智能化

智能启发式云安全引擎

- 解决问题
  - ✓ 传统特征技术易“免杀”
  - ✓ 传统特征引擎启发能力较弱
  - ✓ 对未知恶意文件快速检出

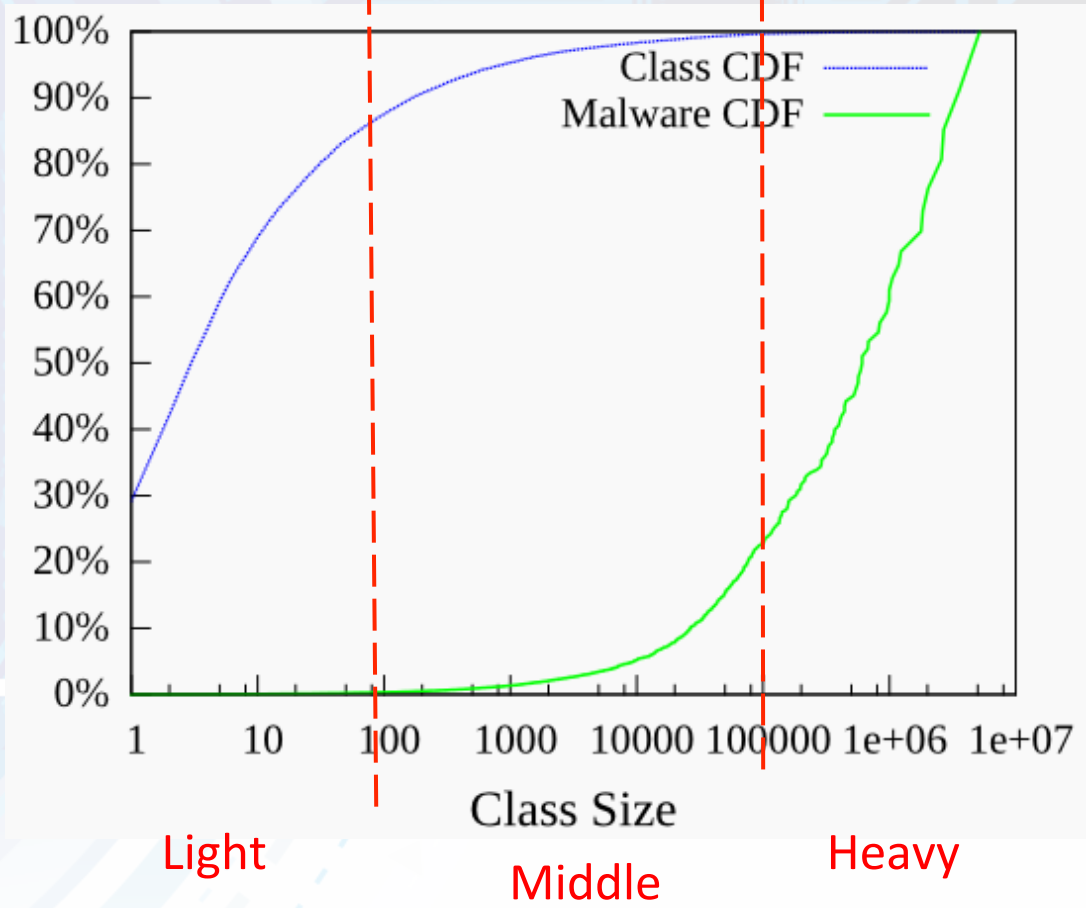
- 特点
  - ✓ 基于海量数据挖掘训练模型
  - ✓ 自动化、智能学习，减少人工干预
  - ✓ 特征点不固定，不易“免杀”
  - ✓ 分析流行趋势，实时自动学习修正



黑样本文件　　特征点（不固定）　　各种未知文件

智能启发式云安全引擎(HRS)

- 面临问题
  - 样本分布不均匀
    - Power-Law distribution
  - “单一”模型算法具有局限性
    - SVM，决策树，ANN等
  - 时间上波动
    - Time-based model
  - 如何有效控制误报
    - 组合拳



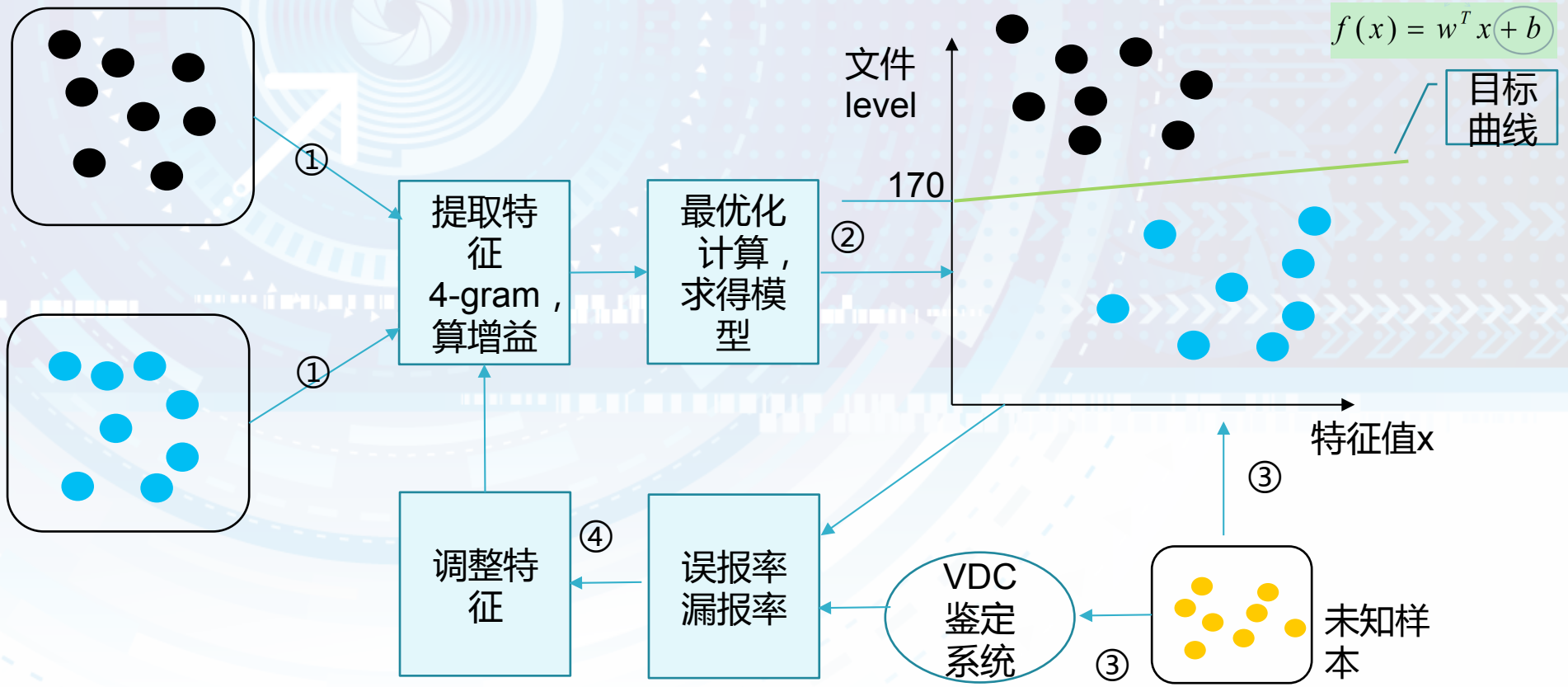
Heavy-weight： 5%的家族10,000以上 (75%文件) （ SVM ）

Middle-weight： 10%的家族100-10,000 （ Rule-based ）

Light-weight： 85%的家族样本少于100 （ 特征,md5 ）

智能启发式云安全引擎(HRS)

- 基本原理（基于二进制文件4-gram，1w维，线性核）



1. 从训练文件的不同位置提取特征x，每个特征对应一个分数值x_n。<x_1,x_2, … x_n>。

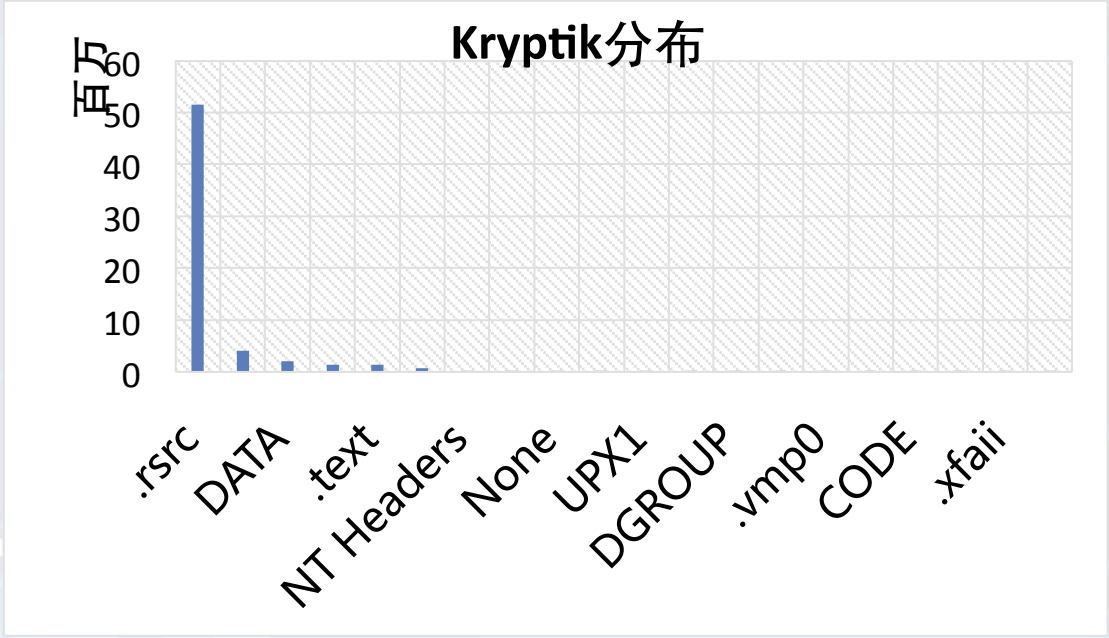
2. 采用线性分类器模型求得分类模型对不同特征的权重，得出具体的分类模型。

3. 对未知文件应用该模型得出结果，并用VDC系统进行验证。

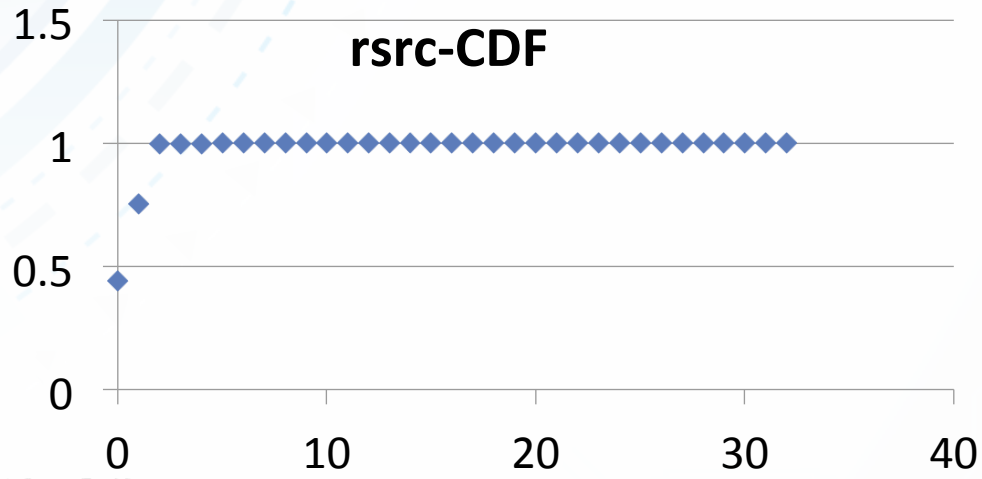
4. 预测结果与VDC结果对比，分析未知文件与训练文件特征差异，调整特征项。

智能启发式云安全引擎HRS（性能优化）

- 提升扫描速度
  - ✓ 4-gram全文太慢
  - ✓ 统计模型来修正
- 敏感区段
  - ✓ 全文n-gram提取太耗时
  - ✓ 统计数据支持区段位置，区段位置不固定



特征提取范围	全文	关键点附近10k	关键点附近3k	关键点附近1k
检出(%)	99.1%	98.6%	98%	97.8%
误报(%)	0.55%	1.4%	1.5%	2.3%
速度(个/s)	15	183	354	553



智能启发式云安全引擎HRS（误报控制）

- 灵活多种
  - ✓ 1）模型反馈训练
    - 万分之几
  - ✓ 2）分数阈值
    - 万分之几
  - ✓ 3) CCE白特征
    - 趋近于0误报
  - ✓ 4) 白名单人工运营
    - 紧急处理高热度误报

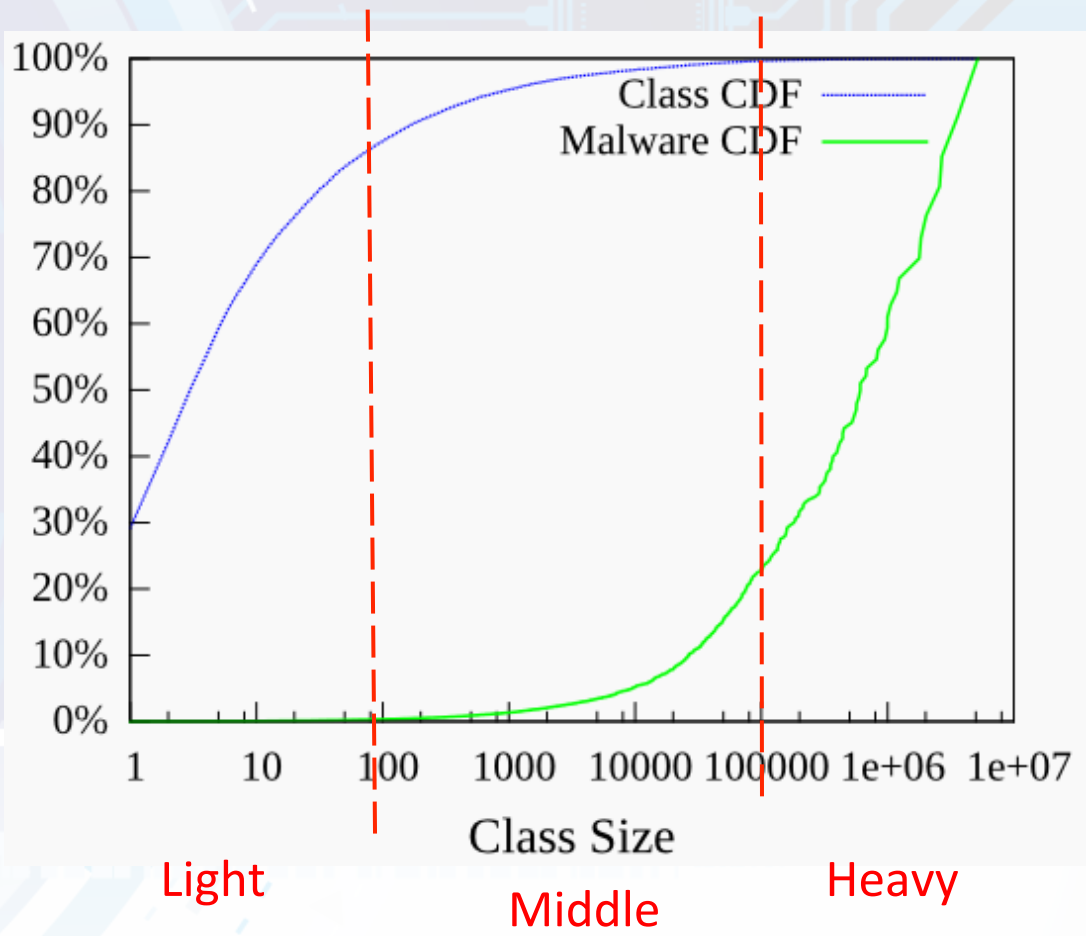
指标\分数	BASE	反馈1轮	反馈2轮
检出(%)	99.48%	99.54%	97.8%
误报(%)	2.33%	0.1%	0.05%

分数阈值	>=0	>=2	>=5	>=10
检出	92%	86.60%	56.30%	33%
误报	0.700%	0.05%	0.025%	0.0028%

智能启发式云安全引擎 (rule-based module)

- Middle weight：不适用于SVM，误报高
  - 逻辑表达式： (0xAA & 0xBB) | (0xCC & 0xDD)
  - 特征来自于自动学习

- 优点
  - 极大减少特征数量
  - 低误报率
  - 检出逻辑可解释，使用和维护方便

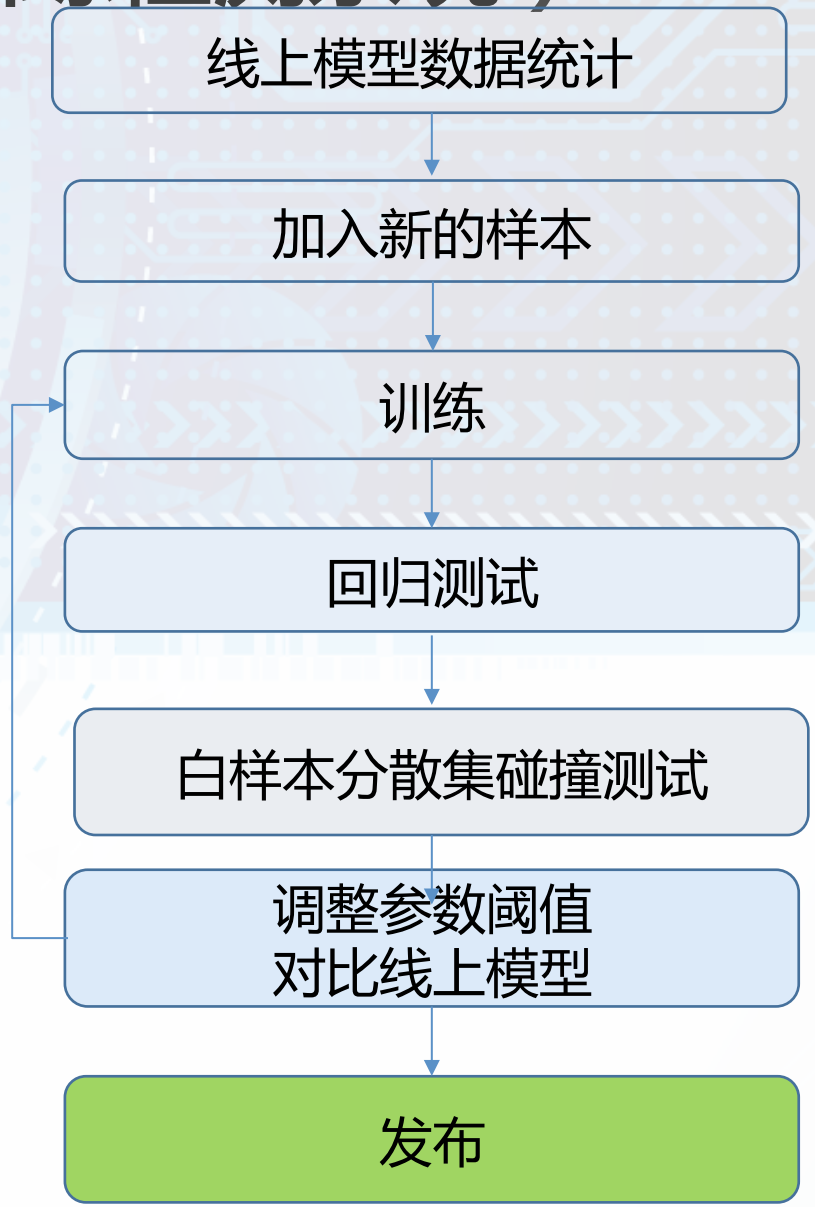


Approaches	TP Rate	FP Rate	Storage Cost	Unknown Files
Hash	1	0	1.8MB	0
Rule	0.761	0.0001	0.4KB	1826
SVM	0.9993	0.0417	46.9KB	1960
HRS	0.9984	0.0017	17.9KB	2329

Adware.Hao123
规则： (0xE70A03F1 & 0x8583052F)
仅占用8字节，对4500黑样本的检出率100%
对10000白样本的误报率0%

智能启发式云安全引擎HRS（实时训练检测系统）

- 样本统计模块
  - ✓ 线上最新样本的时间分布（精确到小时）
  - ✓ 鉴定器对新样本的检出数据
  - ✓ 触发条件设定（防止震荡重复训练）
- 训练样本选择
  - ✓ 新旧样本的时间系数比例
  - ✓ 新旧样本的类型筛选
- 测试回归系统
  - ✓ 对模型进行自动上下线管理
  - ✓ 分散度足够的白样本
  - ✓ 高热度白样本误报对比
  - ✓ 层级式追加 VS 循环替换



大纲

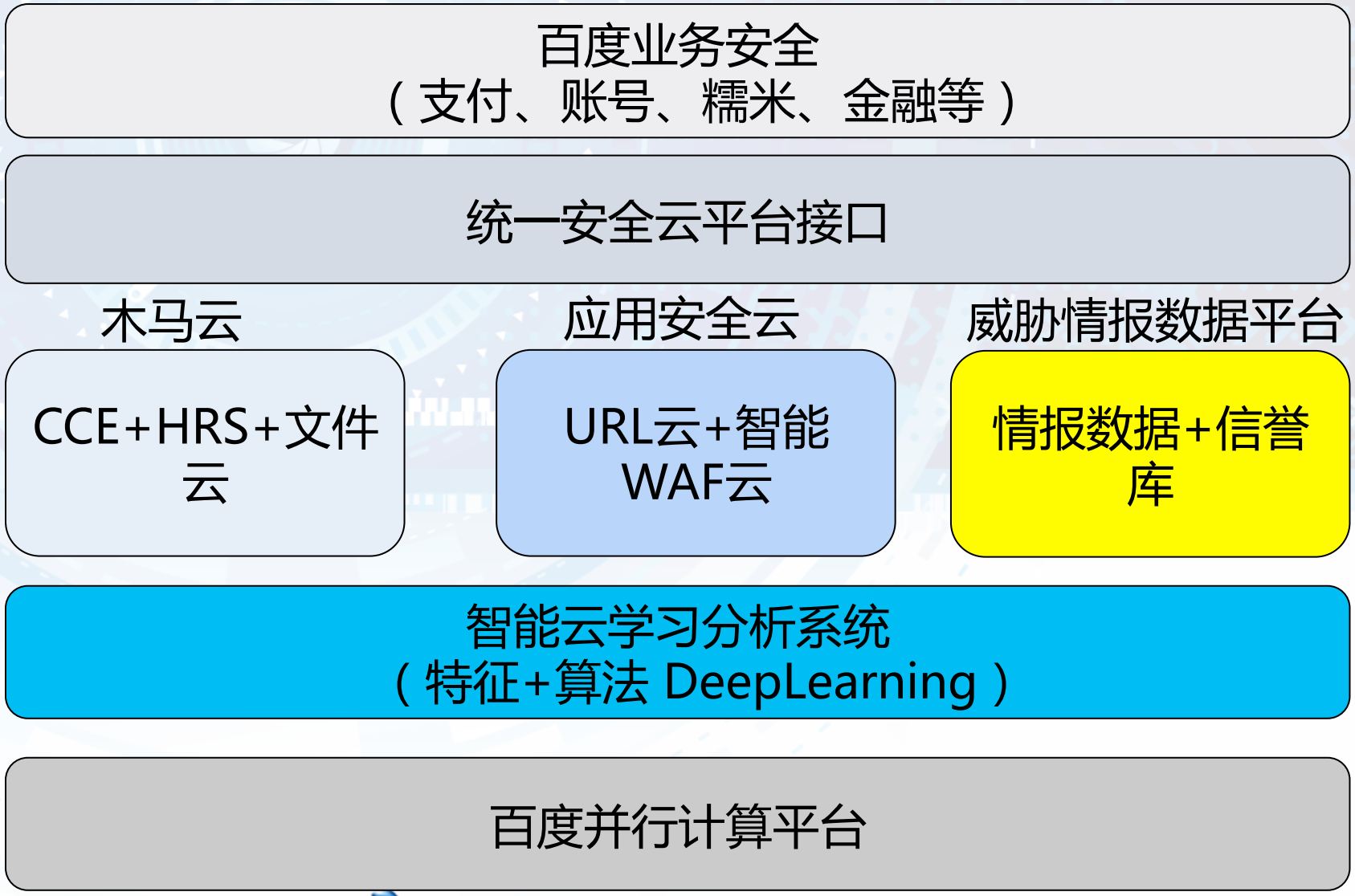
- 安全现状
- 云端安全体系概述
  - ✓ 文件云
  - ✓ 特征云
  - ✓ URL云
- 大数据时代的安全
  - ✓ 云端智能启发式引擎
  - ✓ 威胁情报数据平台

背景

- 单点攻击行为从分析到拦截、到规则生效具有延时性
  - ✓ 云端需要实时感知，自动添加
  - ✓ 客户端需要辅助梳理链条信息
  - ✓ 海量数据基础下预警是关键

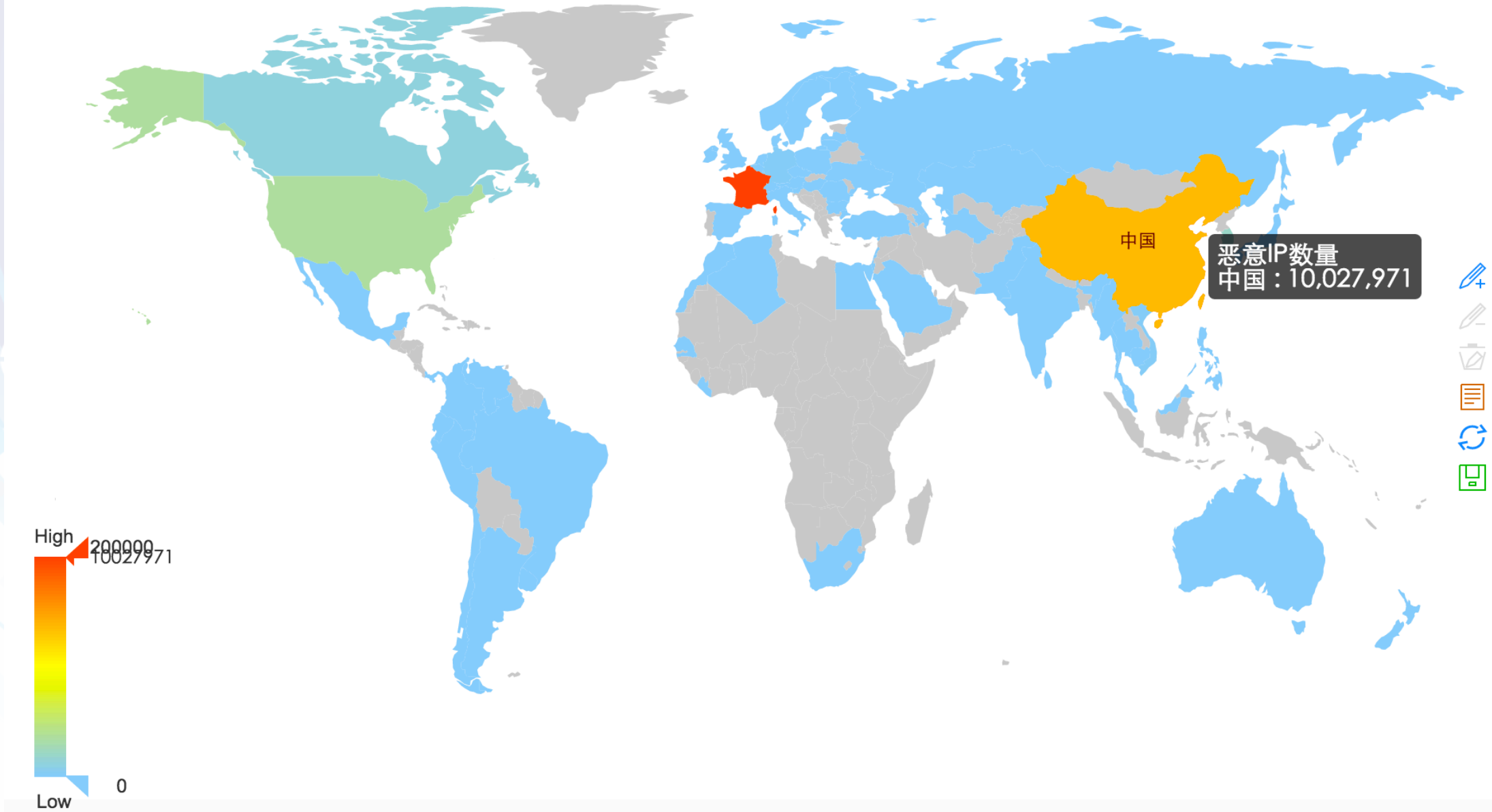
- 连通百度的“端”和“云”
  - ✓ 百度杀毒与手机卫士→“端”+“云”
  - ✓ 充分整合百度强大的爬虫搜索数据
  - ✓ 基础安全平台为业务侧具体形式服务，可追溯，高危预警及时处理。

百度统一安全云平台


百度业务安全
（支付、账号、糯米、金融等）
统一安全云平台接口
木马云
应用安全云
威胁情报数据平台
CCE+HRS+文件云
URL云+智能WAF云
情报数据+信誉库
智能云学习分析系统
（特征+算法 DeepLearning）
百度并行计算平台

恶意全球IP分布(今天)

数据来源：IP基础数据平台



DNS 、 IP 变化关联分析

domain	详情
www.[redacted]av1080.com	2015-11-15 210.[redacted].17
www.[redacted].av1080.com	2015-11-15 210.[redacted].17
www.[redacted]v1080.com	2015-11-16 210.[redacted].17
www.[redacted]av1080.com	2015-10-28 210.[redacted].17 2015-10-30 110.[redacted].67 210.[redacted].17 2015-10-31 210.[redacted].17
www.[redacted]av1080.com	2015-10-28 210.[redacted].17 2015-10-30 110.[redacted].67 210.[redacted].17 2015-10-31 210.[redacted].17

恶意攻击源监测

恶意IP列表

IP	热度
218.[redacted]	842982
195.[redacted]59	756126
195.[redacted]86	740088
195.[redacted]94	724642
195.[redacted]63	718844
195.[redacted]38	717563

恶意攻击目标监测

攻击目标

目标	次数
<PUBLIC>www.s[redacted]se.com	27811
<PUBLIC>www.s[redacted].cc	23302
<PUBLIC>www.s[redacted]n.com	22050
<PUBLIC>www.sh[redacted].la	19641
<PUBLIC>www.zh[redacted]l.com	17344
<PUBLIC>www.sh[redacted]enhu.cn	16310
<PUBLIC>www.sh[redacted]51.com	15004
<PUBLIC>www.sf[redacted]0.com	15001
<PUBLIC>www.se[redacted]d.cn	13590
<PUBLIC>www.sg[redacted]s.com	13521

总结与展望

- 总结
  - ✓ 安全系统没有“一招鲜“
  - ✓ 不断对抗，演变，智能化
  - ✓ 系统稳定，规则明确，结论可靠是基础
- 展望
  - ✓ 不单单立足与引擎技术，增强链条安全能力，形成立体化防御
  - ✓ 运营与自动化系统的“无缝”结合与反馈，打造“泛安全”体系
  - ✓ 立足海量数据，深度发掘“云”与“端”的数据，溯源、互通、关联；从引擎到威胁情报信息的转换

期待与同行更多的合作交流

谢谢