金融科技安全架构演进

京东金融 刘明浩

京东金融
JD.Finance

2017携程信息安全沙龙

个人简介

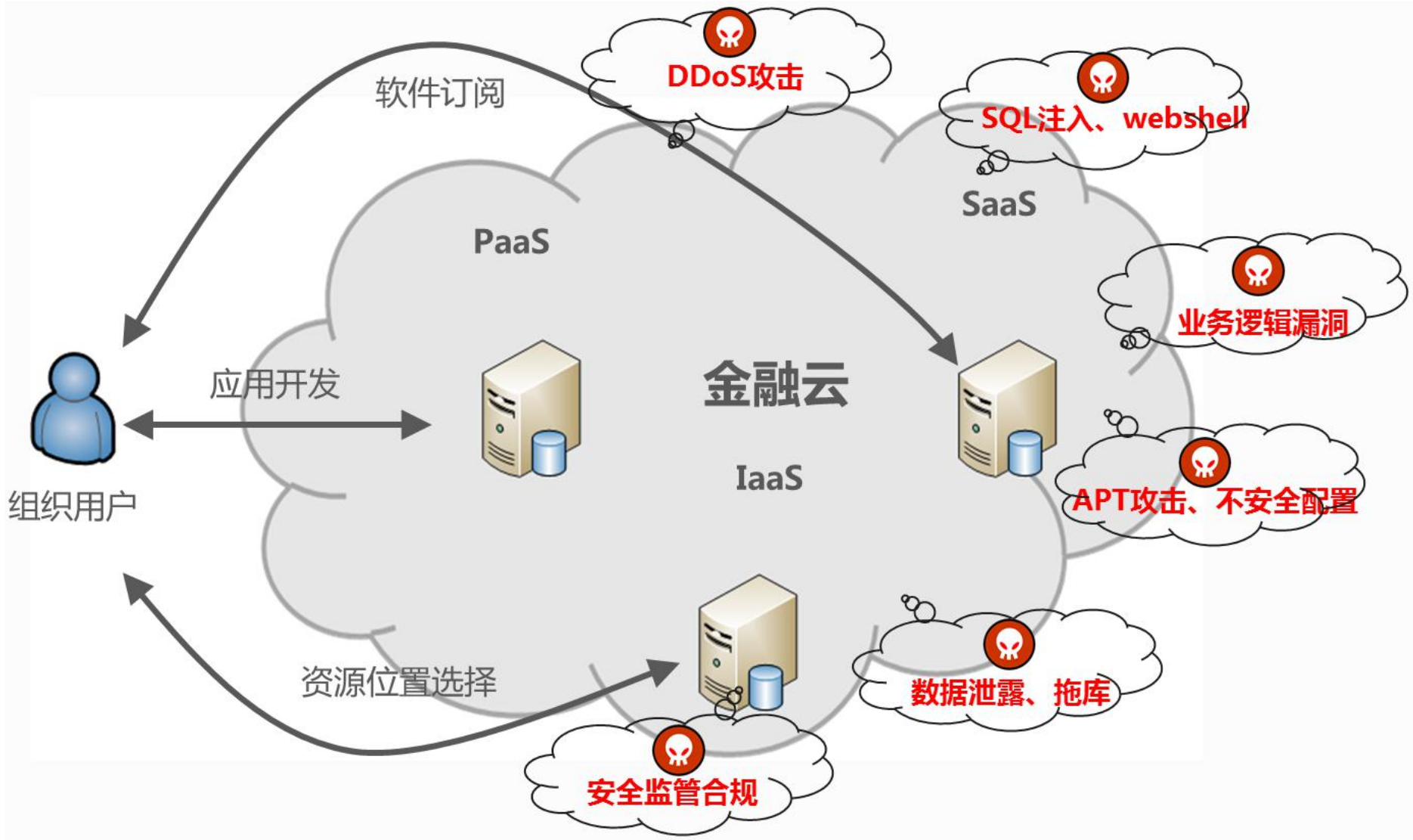
京东金融-安全负责人 **刘明浩**

十年信息安全从业经验，目前负责京东金融整体安全工作，主要包括自研安全产品开发与架构设计、业务安全、安全合规及安全运维等工作

目 录

目 录

金融科技所面临的安全挑战



金融科技所面临的安全挑战

互联网企业
安全挑战

- SQL注入
- XSS跨站脚本
- 文件上传
- DDoS攻击
- CC攻击
- 非授权操作
- 敏感数据保护
- 平行权限

金融科技
安全挑战

- 撞库扫号
- 活动作弊
- 垃圾账号注册
- 业务上云
- 快速迭代
- 安全合规

金融科技所面临的安全挑战

1. 业务安全

解决羊毛党活动被刷、撞库、垃圾账号注册等业务安全问题

5. 安全合规

符合等级保护、央行非金检测、PCI-DSS、ISO27001等安全监管合规要求

金融科技安全需求

2. 安全漏洞与安全运维

解决DDoS攻击、Web及系统安全漏洞、APT攻击、安全基线等安全问题

4. 数据安全

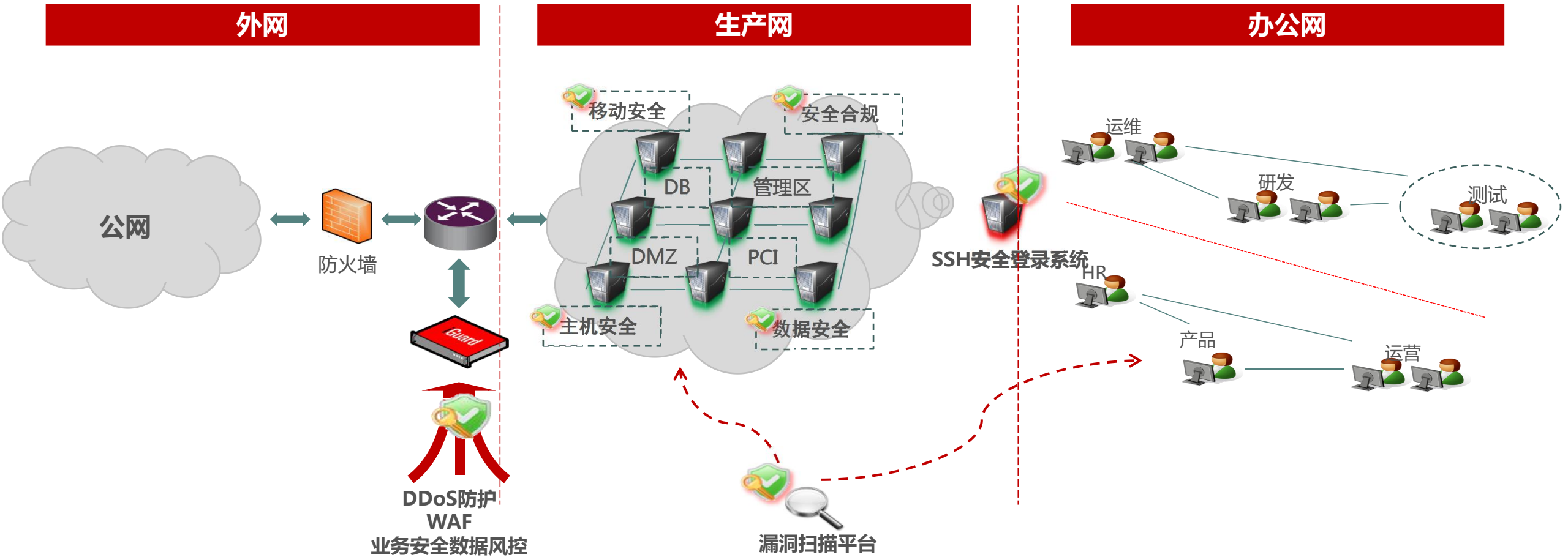
解决数据泄露风险

3. 移动安全

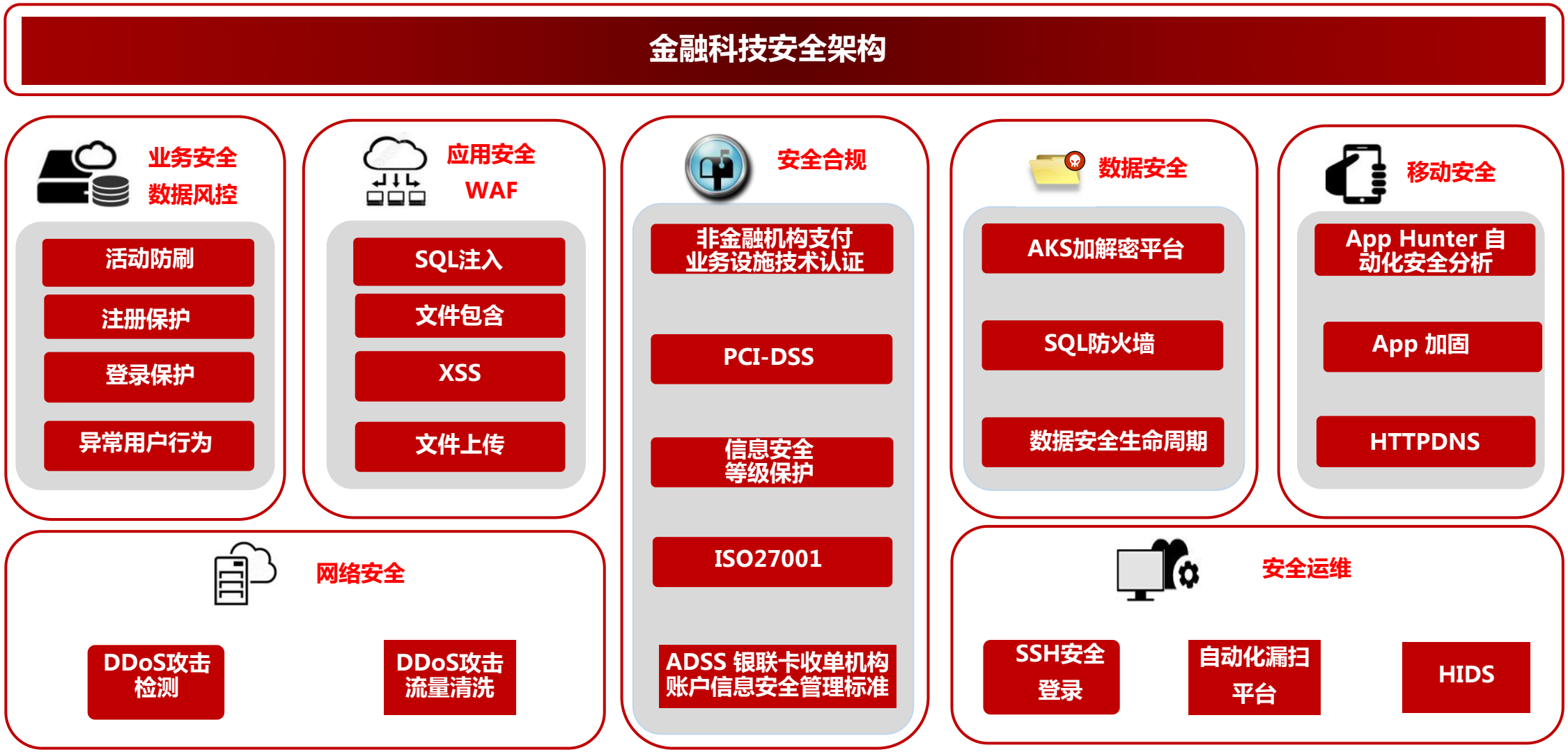
解决APP漏洞检测、APP加固等安全需求

目 录

金融科技安全架构


外网
生产网
办公网
公网
防火墙
Guard
DDoS防护
WAF
业务安全数据风控
移动安全
安全合规
DB
管理区
DMZ
PCI
主机安全
数据安全
SSH安全登录系统
漏洞扫描平台
运维
研发
测试
HR
产品
运营

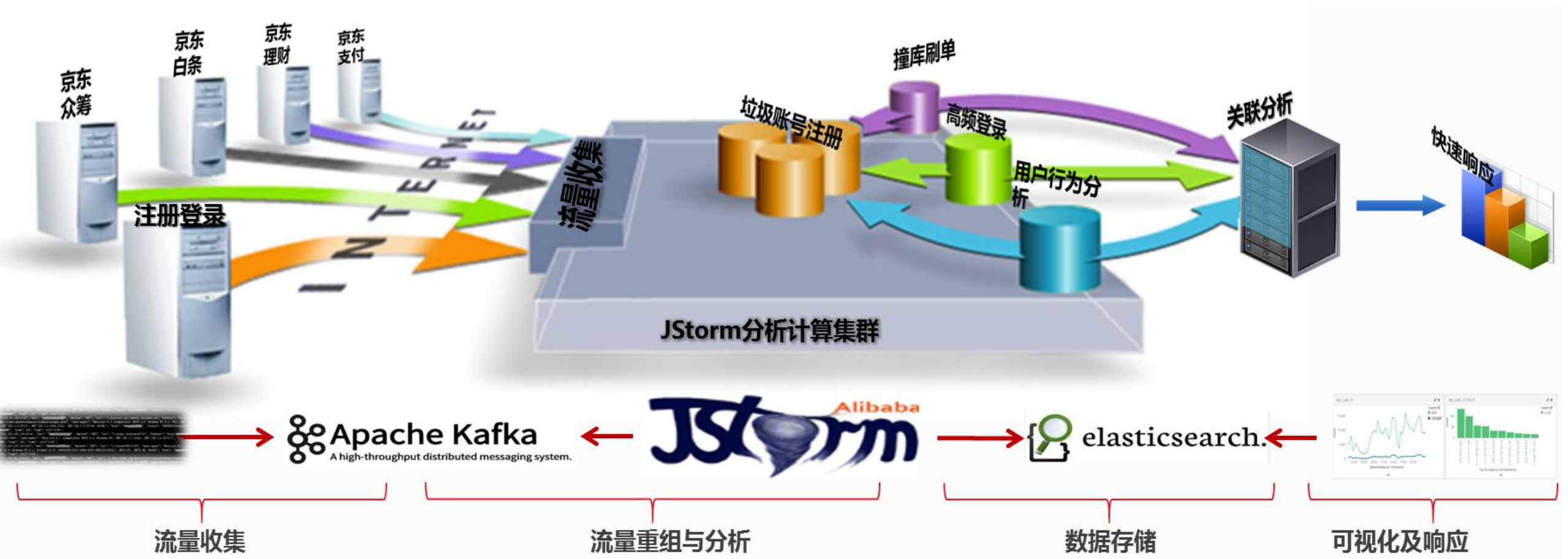
金融科技安全架构


金融科技安全架构
业务安全
数据风控
活动防刷
注册保护
登录保护
异常用户行为
应用安全
WAF
SQL注入
文件包含
XSS
文件上传
安全合规
非金融机构支付
业务设施技术认证
PCI-DSS
信息安全
等级保护
ISO27001
ADSS 银联卡收单机构
账户信息安全管理标准
数据安全
AKS加解密平台
SQL防火墙
数据安全生命周期
移动安全
App Hunter 自
动化安全分析
App 加固
HTTPDNS
网络安全
DDoS攻击
检测
DDoS攻击
流量清洗
安全运维
SSH安全
登录
自动化漏扫
平台
HIDS

目录

业务安全 – 业务安全数据风控

业务安全数据风控是基于大数据的计算能力，通过风险决策引擎，解决业务账号、活动、交易等关键业务环节存在的欺诈威胁



业务安全数据风控 – 功能模块

主要功能模块包括：流量收集、流量分析、数据存储与快速响应四部分组成

流量收集

- 全流量镜像
- 流量解析
- 流量重组

流量分析

- 业务安全风控模型
- 动态规则匹配
- 事件识别

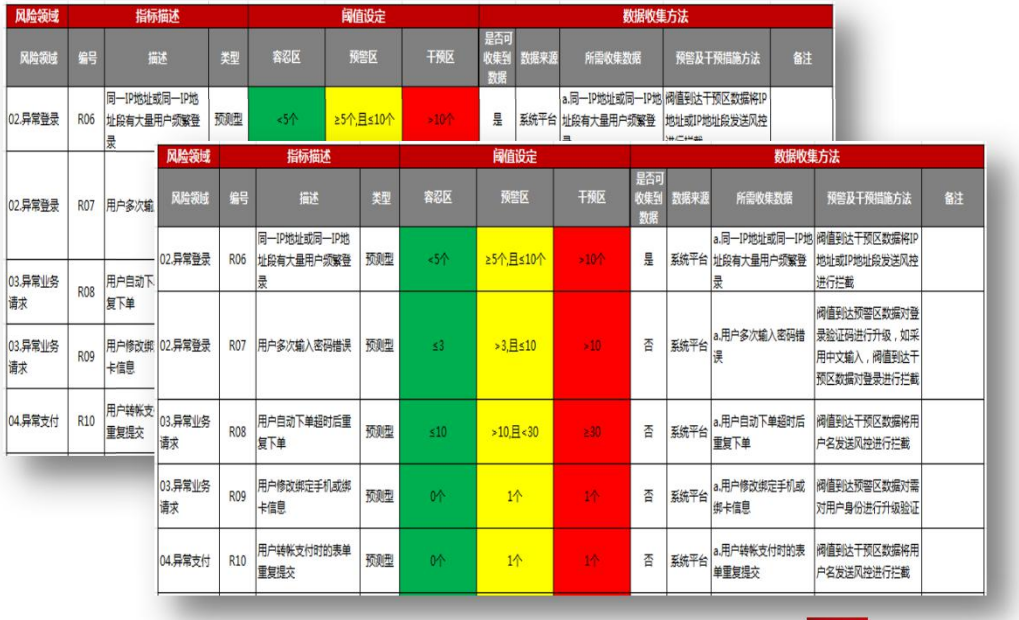
数据存储

- 数据存储
- 实时查询
- 威胁情报

快速响应

- 事件预警
- 系统接口
- 拦截阻断

业务安全数据风控–风控规则引擎



风险领域	指标描述			阈值设定			数据收集方法				
风险领域	编号	描述	类型	容忍区	预警区	干预区	是否可收集到数据	数据来源	所需收集数据	预警及干预措施方法	备注
02.异常登录	R06	同一IP地址或同一IP地址段有大量用户频繁登录	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登	阀值到达干预区数据将IP地址或IP地址段发送风控	
02.异常登录	R07	用户多次输									
03.异常业务请求	R08	用户自动下复下单									
03.异常业务请求	R09	用户修改绑卡信息									
04.异常支付	R10	用户转帐支重复提交									

风险领域	指标描述			阈值设定			数据收集方法				
风险领域	编号	描述	类型	容忍区	预警区	干预区	是否可收集到数据	数据来源	所需收集数据	预警及干预措施方法	备注
02.异常登录	R06	同一IP地址或同一IP地址段有大量用户频繁登录	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登录	阀值到达干预区数据将IP地址或IP地址段发送风控进行拦截	
02.异常登录	R07	用户多次输入密码错误	预测型	≤3	>3,且≤10	>10	否	系统平台	a.用户多次输入密码错误	阀值到达预警区数据对登录验证码进行升级，如采用中文输入，阀值到达干预区数据对登录进行拦截	
03.异常业务请求	R08	用户自动下单超时后重复下单	预测型	≤10	>10,且<30	≥30	否	系统平台	a.用户自动下单超时后重复下单	阀值到达干预区数据将用户名发送风控进行拦截	
03.异常业务请求	R09	用户修改绑定手机或绑卡信息	预测型	0个	1个	1个	否	系统平台	a.用户修改绑定手机或绑卡信息	阀值到达预警区数据对需对用户身份进行升级验证	
04.异常支付	R10	用户转帐支付时的表单重复提交	预测型	0个	1个	1个	否	系统平台	a.用户转帐支付时的表单重复提交	阀值到达干预区数据将用户名发送风控进行拦截	

1. 根据业务场景进行分析可能带来的业务安全风险
2. 根据风险容忍度设置监控预警阀值
3. 根据风险指标设计数据收集方法及干预\阻断措施

风险领域	指标描述			阈值设定			数据收集方法				
风险领域	编号	描述	类型	容忍区	预警区	干预区	是否可收集到数据	数据来源	所需收集数据	预警及干预措施方法	备注
02.异常登录	R06	同一IP地址或同一IP地址段有大量用户频繁登录	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登录	阀值到达干预区数据将IP地址或IP地址段发送风控进行拦截	

业务安全数据风控–风险行为监控

“暴力破解”行为监控

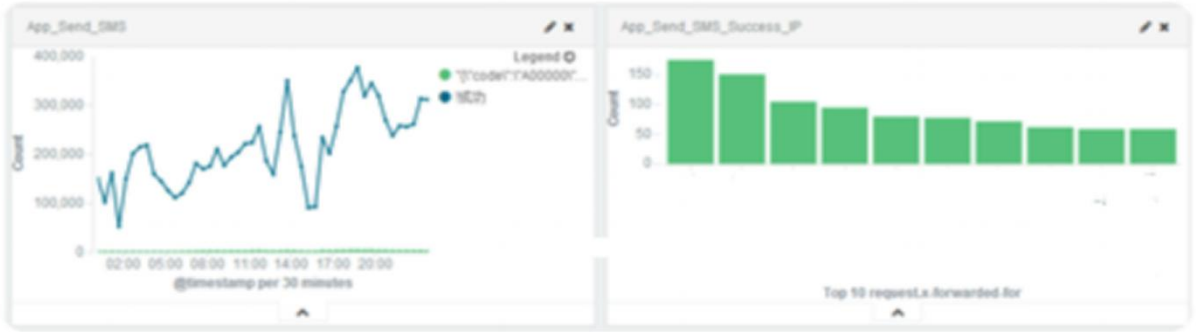
通过对线上业务登录成功及失败行为的实时监控

“撞库扫号”行为监控

通过对线上业务登录成功及失败行为的实时监控

“短信炸弹”行为监控

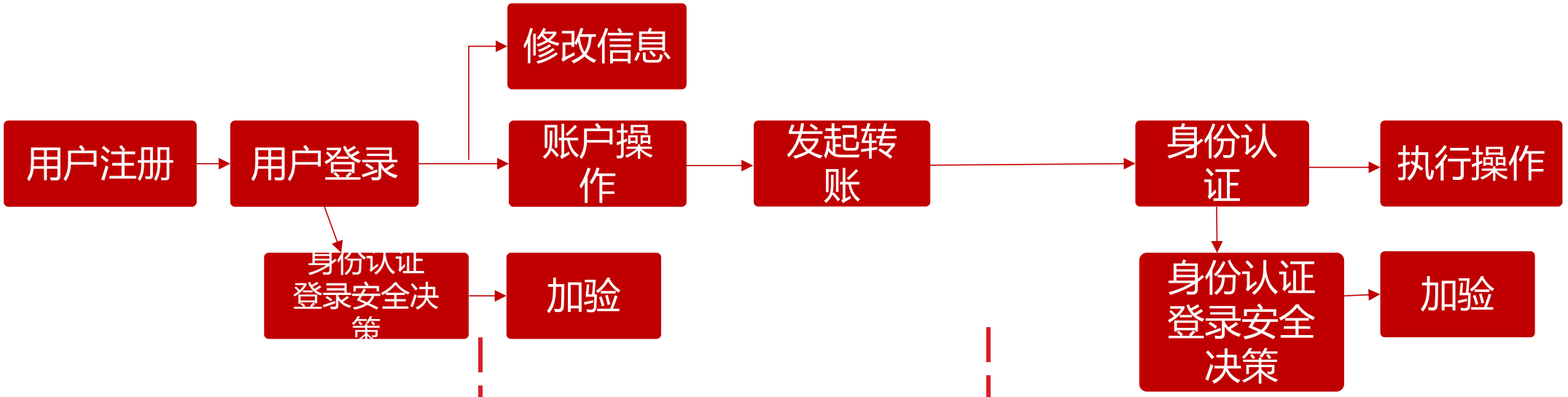
通过对线上所有短信验证接口进行实时监控



“垃圾帐号注册”行为监控

通过对线上所有业务的注册行为(频繁注册)进行实时监控

业务安全数据风控 – 应用场景



注册场景

反欺诈API服务-注册

- 机器注册风险
- 设备聚集风险等级
- ……

登录场景

身份认证产品

- 指纹、免密验证

账户风险识别产品

- 用户身份及登录安全识别
- 短信加验等风险处置手段

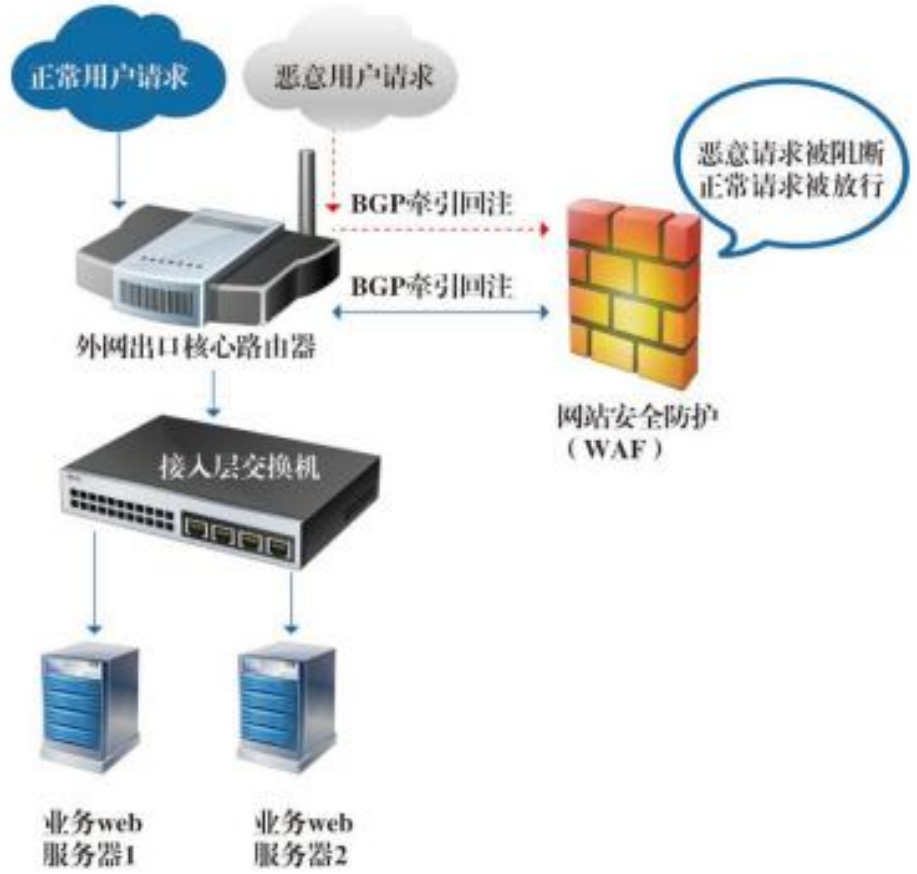
登录、交易及转账场景

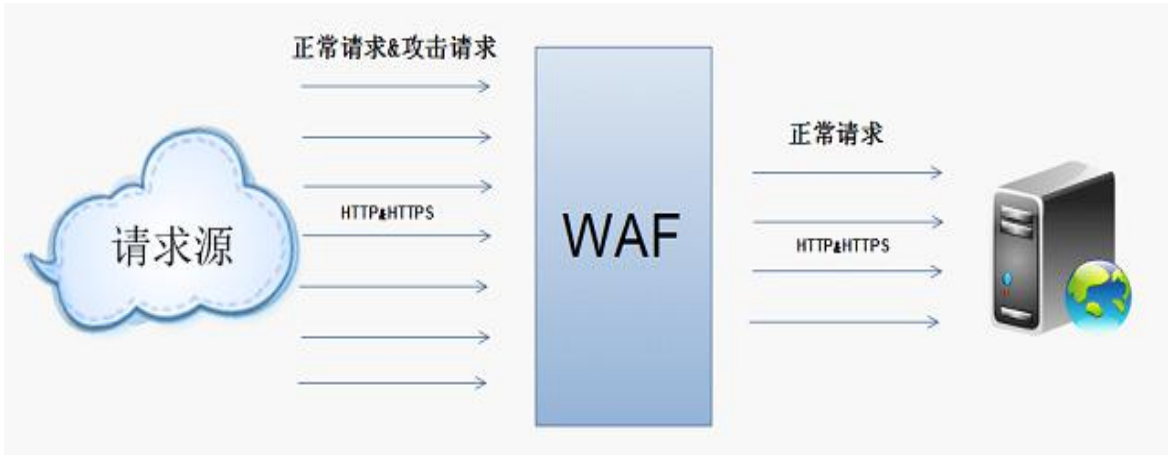
反欺诈API服务-登陆

- 用户安全风险等级
- 用户常用登录地
- 用户常用设备
- 用户安全设备
- 设备聚集性风险等级

应用安全 - WEB应用防火墙

Web应用防火墙目前根据对HTTP访问请求数据进行特征匹配，从而检测识别出相应的攻击类型





Web应用防火墙是向用户提供的网站安全防护产品，通过防御常见OWASP攻击、提供热补丁漏洞修复，网站业务的定制规则防护，从而成功保障网站Web应用的安全性与可用性

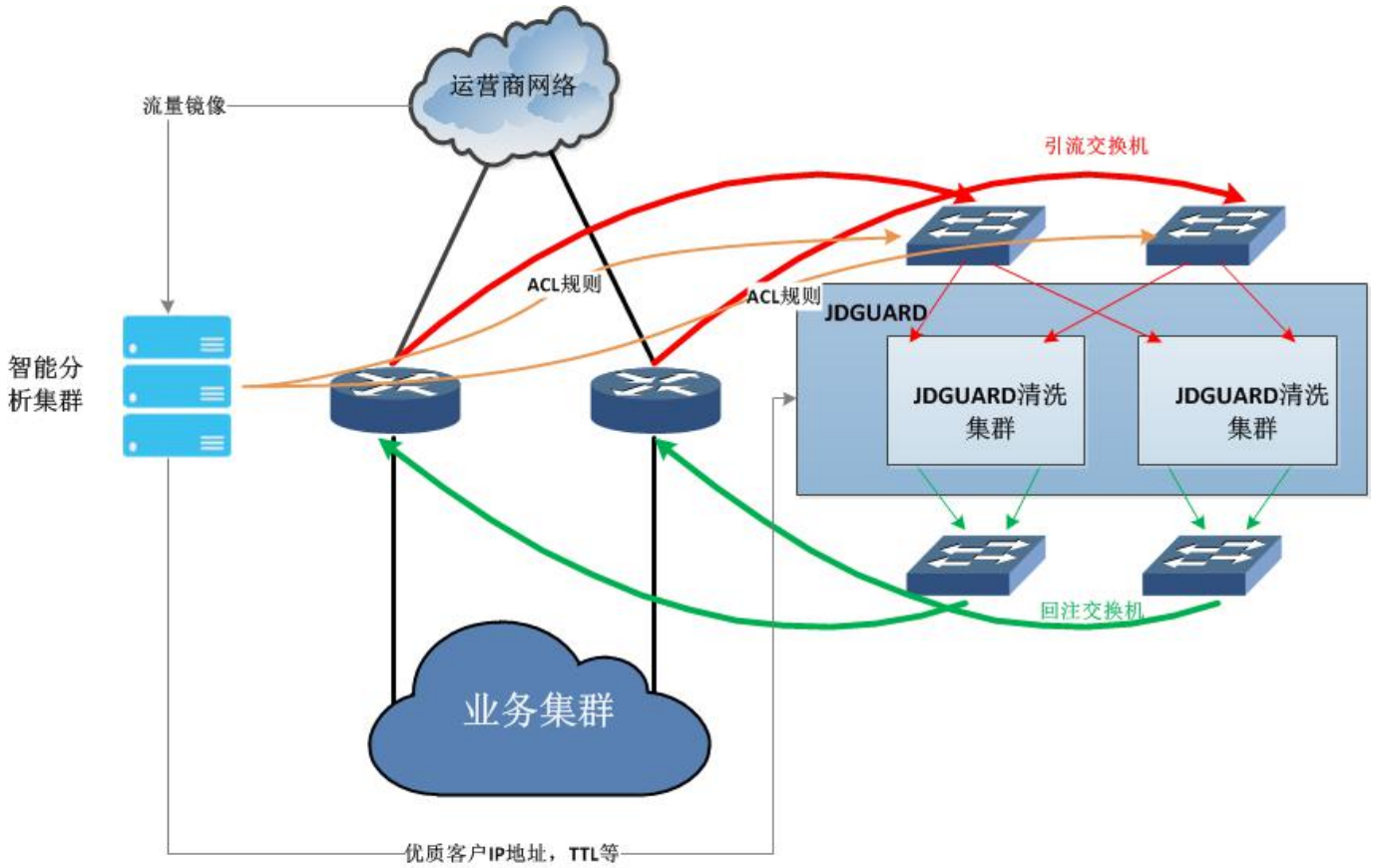
主要功能	功能描述
Web常见攻击防护	提供SQL注入、XSS跨站、Webshell上传、后门隔离保护、命令注入、非法HTTP协议请求、常见Web服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等安全防护
缓解CC攻击	对单一源IP的访问频率进行控制、重定向跳转验证、人机识别
精准访问控制	提供配置控制台界面，支持IP、URL、Referer、User-Agent等HTTP常见字段的条件组合，精准访问控制策略，可支持盗链防护、网站后台保护等防护场景

1. 云端清洗集群，单机40G流量清洗能力。可集群扩展

2. 有效检测并清洗SYN flood， ACK flood, UDP flood, ICMP flood，CC攻击等各类常见DDoS攻击

3. 部署灵活，流量智能牵引，攻击响应精准迅速

4. 支持TCP、UDP、HTTP、HTTPS等各种协议，适用于金融、游戏、电商、直播网站等各种业务场景



DDoS攻击检测&清洗回注 – 实现功能

畸形报文过滤

对报文的合法性进行检验，对畸形报文进行拦截，防止其穿透到后端系统

自定义黑白名单

可接入安全模块获得黑名单，同时将信任客户，合作伙伴等加入白名单

特征分析判定

对流量进行特征分析，动态维护可信任访问源集合

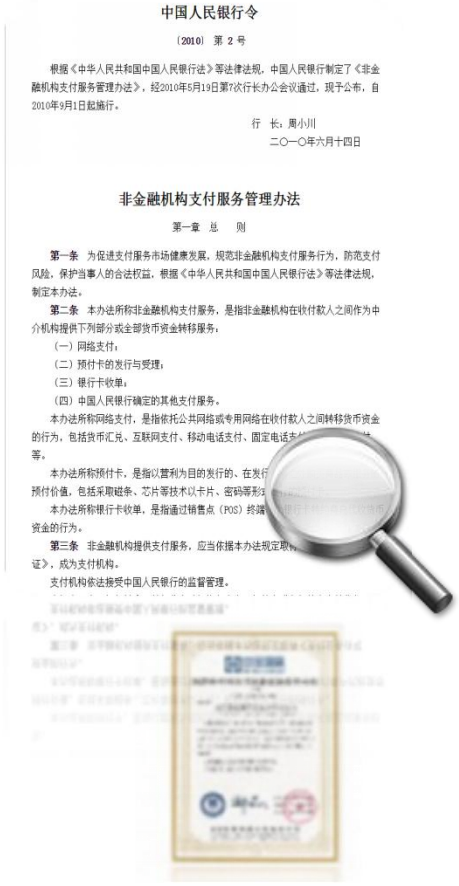
虚假源认证

对流量进行源认证，有效过滤sync flood, ack flood, icmp flood等

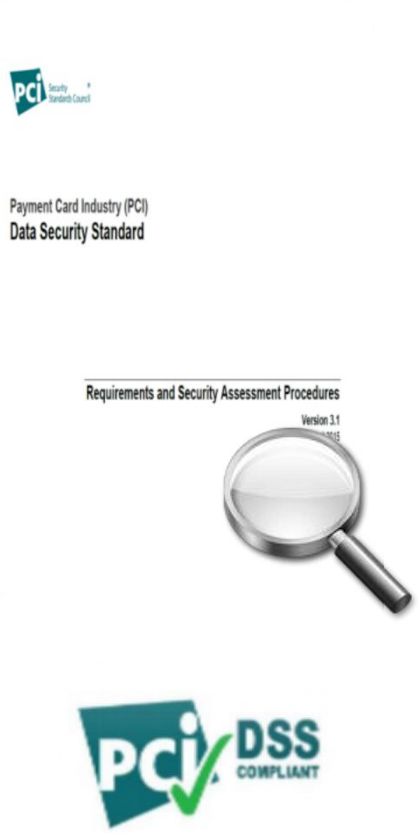
智能限速

对单个IP进行智能限速，有效防止突发异常流量

安全合规 - 安全标准与合规遵从



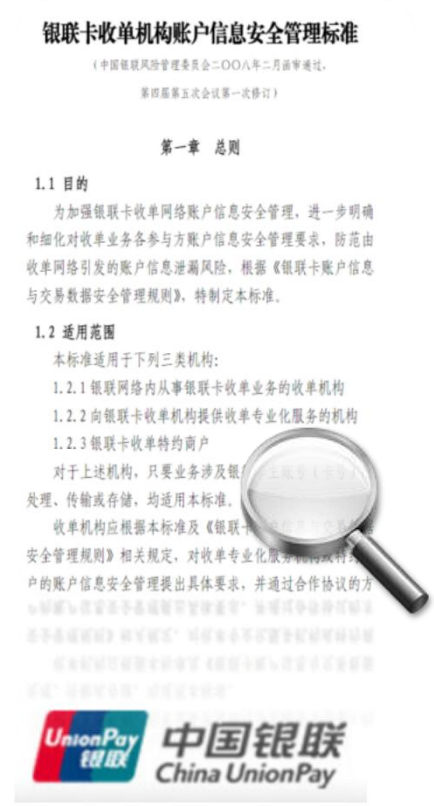
非金融机构
支付业务设施技术认证



PCI DSS
支付卡行业数据安全标准

信息安全等级保护

ISO 27001认证



ADSS 银联卡收单机构
账户信息安全管理标准

数据安全 – 数据安全生命周期

数据安全管理从数据全生命周期角度，从数据产生、数据存储、数据使用、数据展现、数据传输，到数据销毁，最终建立闭环数据安全管理机制

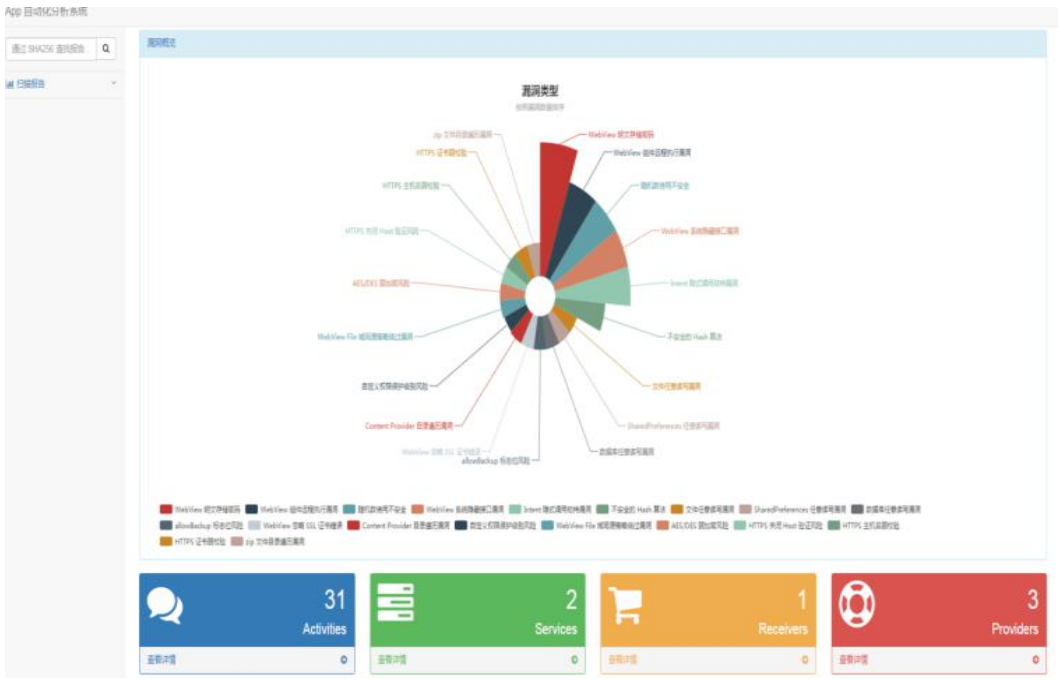
App Hunter 自动化安全分析平台提供全方位的移动App自动漏洞检测服务，能在App研发测试过程中发现App客户端存在的安全问题，并帮助App研发同学快速了解安全漏洞，定位问题及修复漏洞

漏洞检测（20 项）：

- WebView 远程代码执行漏洞
- 不安全的随机数使用
- 文件全局读写漏洞
- 数据库全局读写漏洞
- SharedPreferences 全局读写漏洞
- allowBackup 标志位配置不当
- debuggable 标志位配置不当
- WebView 明文存储密码
- WebView 忽略 SSL 证书错误
- WebView 系统隐藏接口漏洞
- Content Provider 目录遍历漏洞
- 自定义权限保护级别配置不当
- WebView File 域同源策略绕过漏洞
- Intent 隐式调用劫持漏洞
- AES/DES 弱加密缺陷
- 不安全的 Hash 算法
- HTTPS 关闭 Host 验证漏洞
- HTTPS 主机名弱校验
- HTTPS 证书弱校验
- ZIP 文件目录遍历漏洞

风险检测（4 项）：

- Activity 组件暴露风险
- Broadcast Receiver 组件暴露风险
- Service 组件暴露风险
- Content Provider 组件暴露风险



移动安全 - 域名解析HTTPDNS

HTTPDNS使用HTTP协议承载DNS服务，代替传统的基于UDP协议的DNS。绕开运营商LocalDNS，有效防止域名劫持，提高域名解析效率。智能解析，精准调度。域名修改实时生效，支持HTTP/HTTPS。

HTTPDNS-SERVER

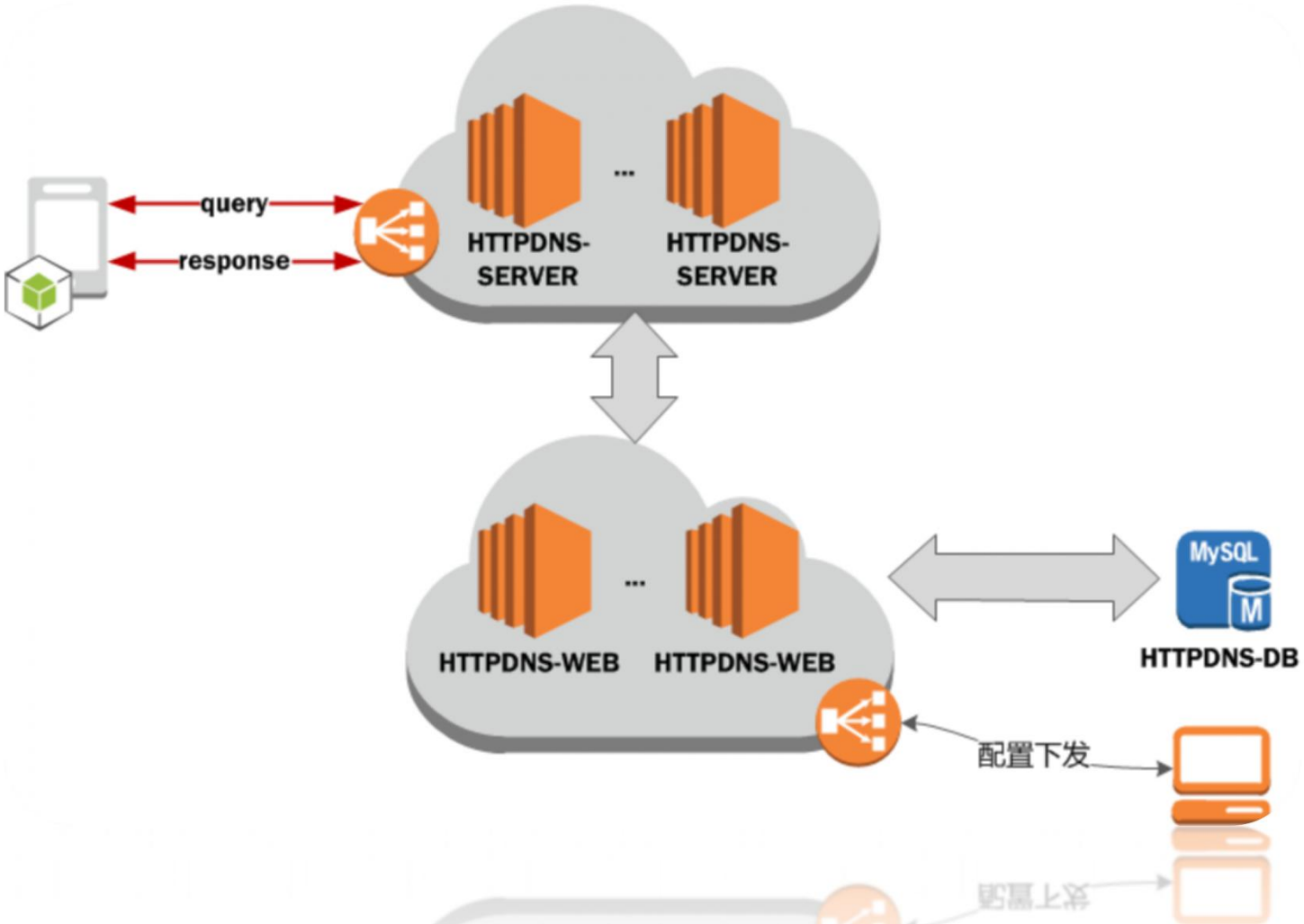
解析请求，生成HTTPDNS响应

HTTPDNS-WEB

下发指令，呈现服务信息

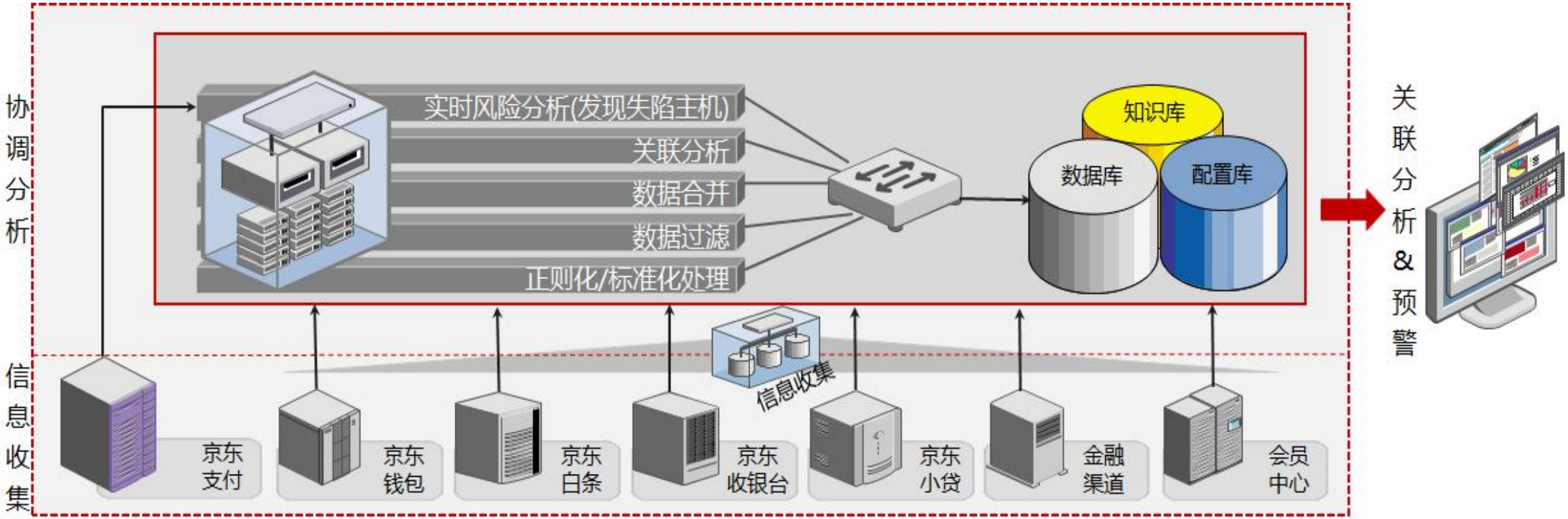
HTTPDNS-DB

存储所有相关数据



安全运维 - HIDS服务器安全

HIDS服务器安全由轻量级Agent和云端组成，集整体安全平台威胁情报于一体，通过Agent和云端大数据的联动，实现对文件变更监控、内网端口扫描、登录行为监控、Tomcat命令执行、webshell创建进程监控、命令执行监控等功能



HIDS服务器安全 – 功能介绍

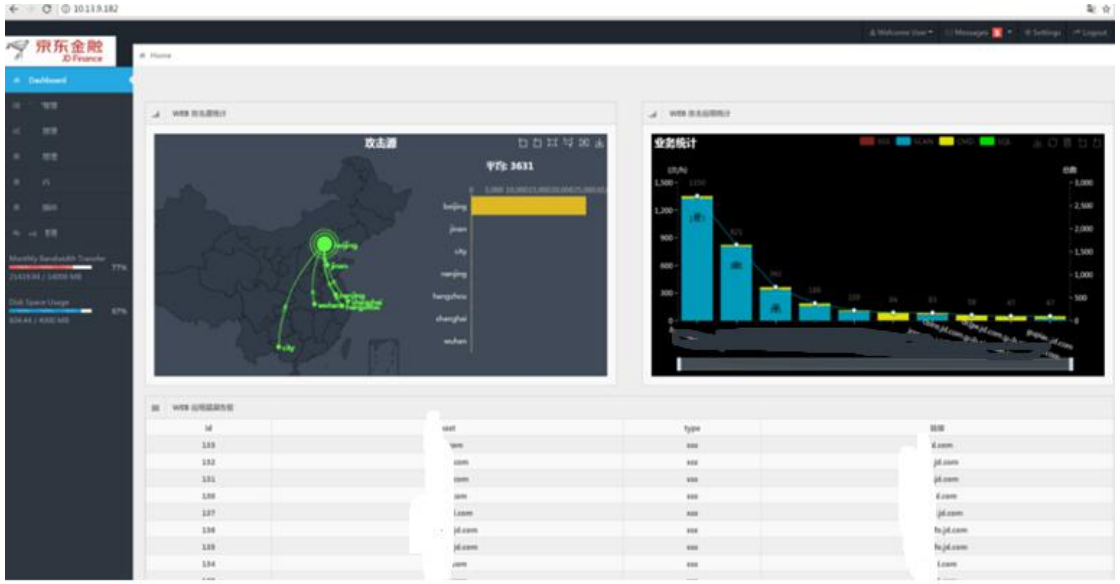
服务器安全是数据的最后一道防线，要建立纵深防御体系，服务器安全是必不可少的一环，服务器安全通过安装在服务器上的Agent和云端防护中心的联动，帮助用户守住最后一道防线

主要功能	功能描述
文件变更监控	通过Linux内核接口，实现对文件系统的增删查进行监控，对重要文件的修改进行记录
命令执行记录	通过Linux内核接口，记录所有系统命令执行，筛选提供服务的进程（Tomcat等）调用的系统命令
端口扫描识别	通过统计一分钟内同一源ip对主机连接端口数，超过上限50判断为端口扫描
服务爆破识别	服务爆破目前干扰信息比较多，部分应用连接次数较多导致和爆破相似

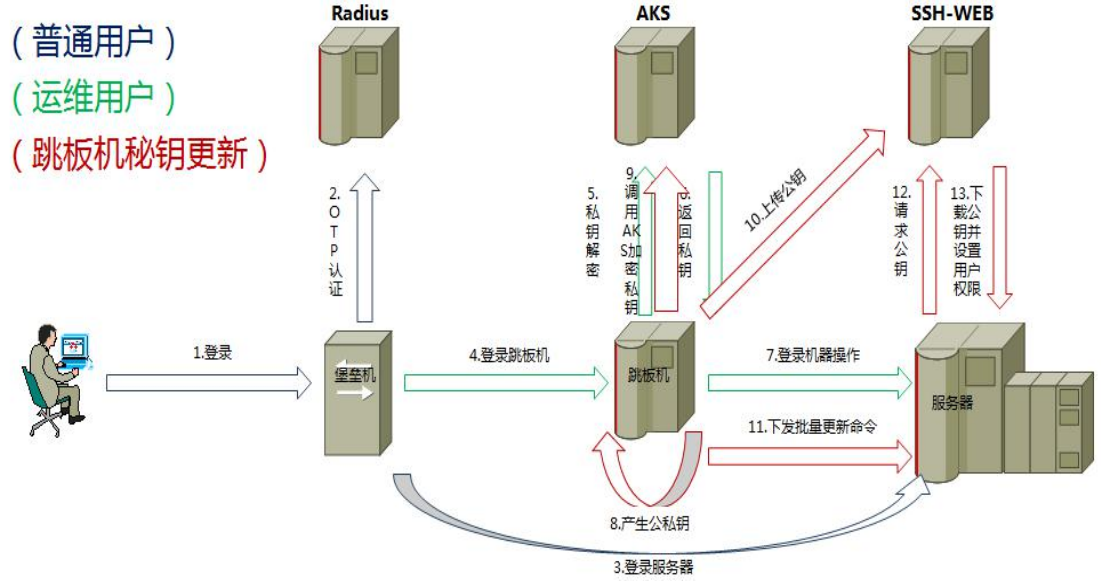
安全运维-生产/办公/测试网安全

自动化漏洞扫描平台实现全网7*24小时存活主机、高危端口、系统漏洞、web漏洞扫描。SSH安全登录系统，通过公私钥提供免密登录功能，解决密码泄露问题，通过跳板机将线上批量操作集中管理并监控，解决集中安全审计问题

自动化漏洞扫描平台



SSH安全登录系统



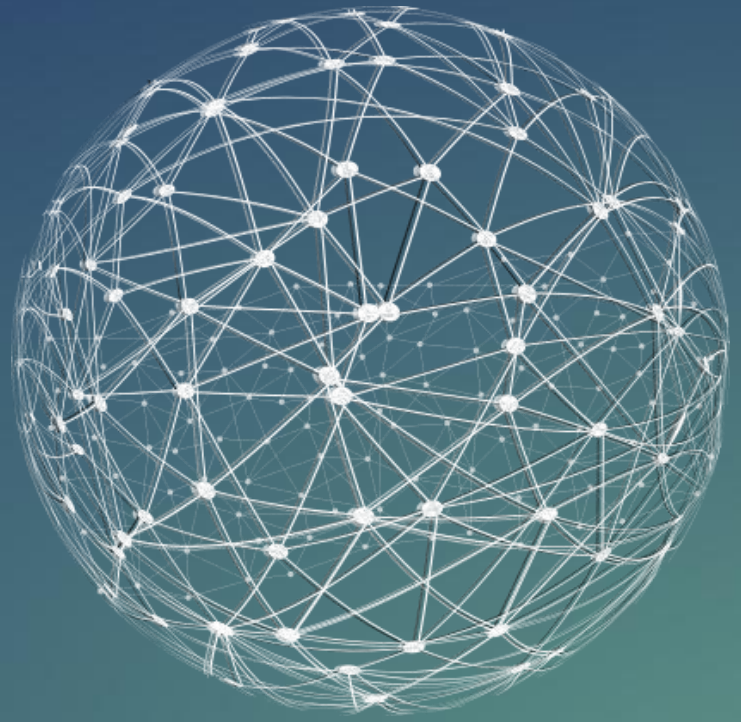
目 录

业务安全

软件定义安全

数据协作安全

态势感知



THANKS
Q&A