DBAPPSecurity 安恒信息

WEB应用安全和数据库安全的领航者

政企安全之云化、大数据化和移动化

汇报人：范 渊

WHO AM I

- 范渊　CEO & CTO
  - 毕业于美国加州大学
  - 国际著名安全公司多年的研发和管理经验
  - 入选中组部“国家千人计划”
  - 第十届杭州市政协常委
  - 第十一届“杭州市十大杰出青年”
  - 第五届“科技新浙商”
  - 第一个登上黑帽子安全大会演讲的中国人
  - OWASP中国分会副会长
  - 2008北京奥组委安全组成员
  - 中国计算机学会计算机安全专委会常委
  - 浙江省海外高层次人才引进计划-浙江省特聘专家
  - 浙江省计算机信息系统安全协会副会长
  - 浙江省“新世纪151人才工程”
  - 《中国信息安全》杂志（特约）专栏作者

政企安全

1. 政企云化是大趋势
2. 政企的安全顾虑及现状
3. 政企云的云安全建设
4. 政企安全大数据化
5. 政企安全移动化

云计算是IT发展必然趋势

传统IT模式

单位机房

各单位独立购买硬件，自行建设政务系统。

独立管理

各自单位的管理人员进行IT规划建设和日常管理

目前到未来IT模式

虚拟化

通过更好地利用资源，产生更高的IT效率

云计算、大数据

公共云和私有云解决方案，推动更高的敏捷性。

数博会回顾—大数据需求的缩影

灵活响应实际需求

可灵活增减资源配备，
满足实际需求；

流程和大数据共享

民生大数据在各类政务
应用间可实现共享；
不同部门间的政务流程
可更简洁地整合。

政务系统集中监管

可进行统一的监管
全面提升政务应用能力
与安全水平

数博会 BIG DATA EXPO

大数据，超乎我们的想象，超越我们的梦想！
Big data has gone beyond our imagination and our dreams.

云计算、大数据受国务院高度重视

索 引 号：000014349/2015-00004　　主题分类：工业、交通\信息产业（
发文机关：国务院　　成文日期：2015年01月06日
标　　题：国务院关于促进云计算创新发展培育信息产业新业态的意见
发文字号：国发〔2015〕5号　　发布日期：2015年01月30日
主 题 词：

国务院关于促进云计算创新发展
培育信息产业新业态的意见

国发〔2015〕5号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

云计算是推动信息技术能力实现按需供给、促进信息技术和数据资源充分利用的
态，是信息化发展的重大变革和必然趋势。发展云计算，有利于分享信息知识和创新
降低全社会创业成本，培育形成新产业和新消费热点，对稳增长、调结构、惠民生和
新型国家具有重要意义。当前，全球云计算处于发展初期，我国面临难得的机遇，但
服务能力较薄弱、核心技术差距较大、信息资源开放共享不够、信息安全挑战突出等
重建设轻应用、数据中心无序发展苗头初步显现。为促进我国云计算创新发展，积极
息产业新业态，现提出以下意见。

一、指导思想、基本原则和发展目标

（一）指导思想。

适应推进新型工业化、信息化、城镇化、农业现代化和国家治理能力现代化的需

大数据支撑核心业务系统

索 引 号：000014349/2015-00109　　主题分类：工业、交通\信息产业（
发文机关：国务院办公厅　　成文日期：2015年06月24日
标　　题：国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见
发文字号：国办发〔2015〕51号　　发布日期：2015年07月01日
主 题 词：

国务院办公厅关于运用大数据
加强对市场主体服务和监管的若干意见

国办发〔2015〕51号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

为充分运用大数据先进理念、技术和资源，加强对市场主体的服务和监管，推进简政放权和政府职能转变，提高政府治理能力，经国务院同意，现提出以下意见。

一、充分认识运用大数据加强对市场主体服务和监管的重要性

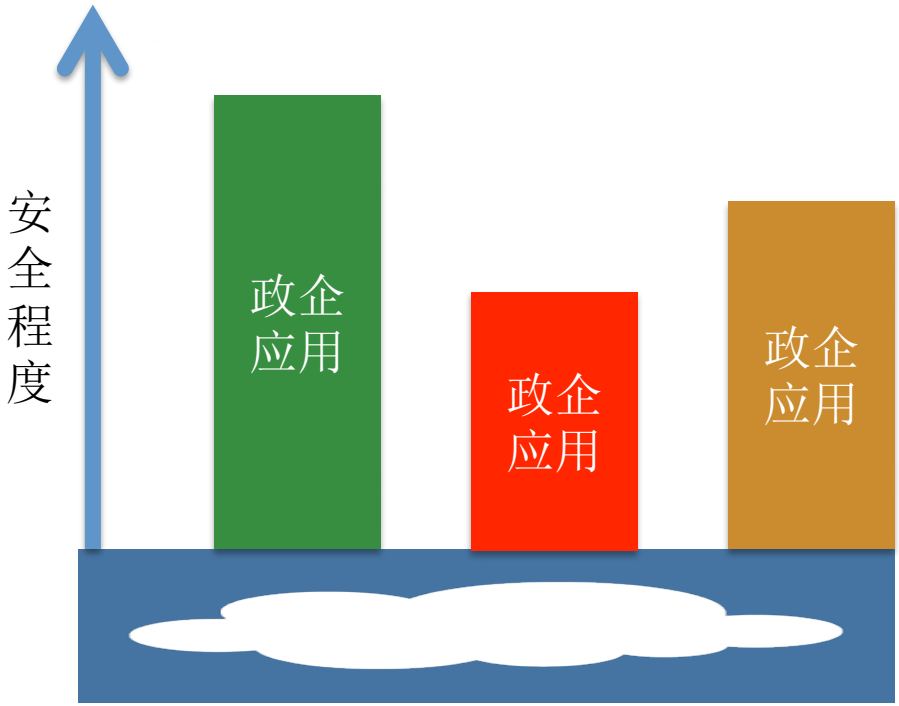
简政放权和工商登记制度改革措施的稳步推进，降低了市场准入门槛，简化了登记手续，激发了市场主体活力，有力带动和促进了就业。为确保改革措施顺利推进、取得实效，一方面要切实加强和改进政府服务，充分保护创业者的积极性，使其留得下、守得住、做得强；另一方面要切实加强和改进市场监管，在宽进的同时实行严管，维护市场正常秩序，促进市场公平竞争。

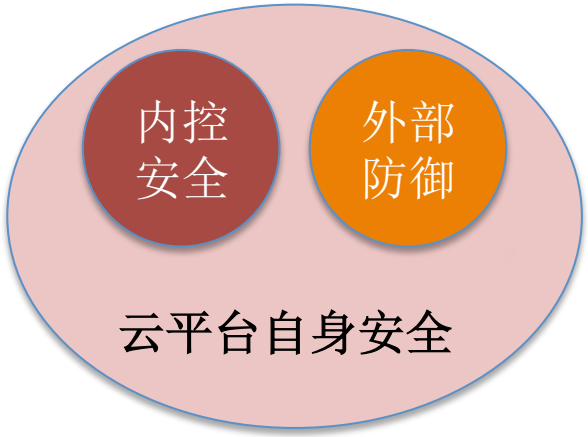
云计算保障基础运算能力

政企安全

1. 政企云化是大趋势
2. 政企的安全顾虑及现状
3. 政企云的云安全建设
4. 政企安全大数据化
5. 政企安全移动化

政企云的安全隐患





云基础设施安全程度一致，
但迁入的各类应用安全程度不一，
程度较低的应用有可能被入侵，
影响云内部其他应用安全。

新的业务安全问题层出不穷

Web业务和移动业务安全威胁贯穿整个过程

网站故障
木马
钓鱼网站
非法APP

漏洞扫描
DDOS攻击
用户注册欺诈
参数注入

口令破解
浏览器劫持
高风险访问

会话劫持
越权访问
逻辑漏洞利用

账户利用

暴力破解

批量注册

平行越权查询

垂直越权操作

验证码绕过

刷积分

身份伪造

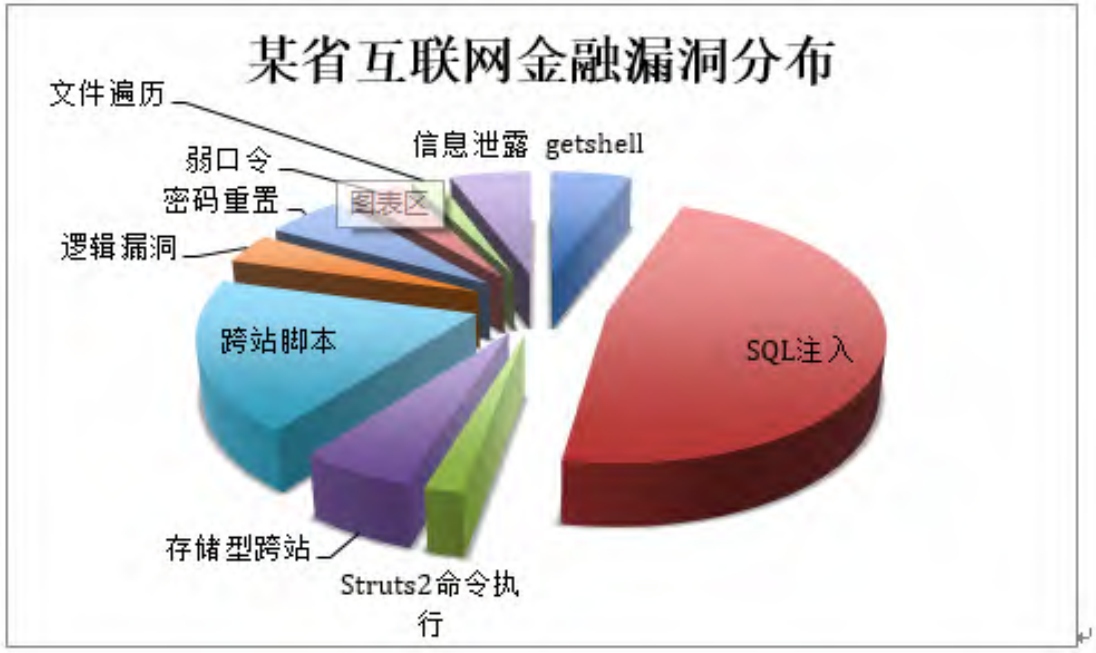
平行越权修改

敏感信息泄漏

平行越权下载

互联网金融行业应用安全风险

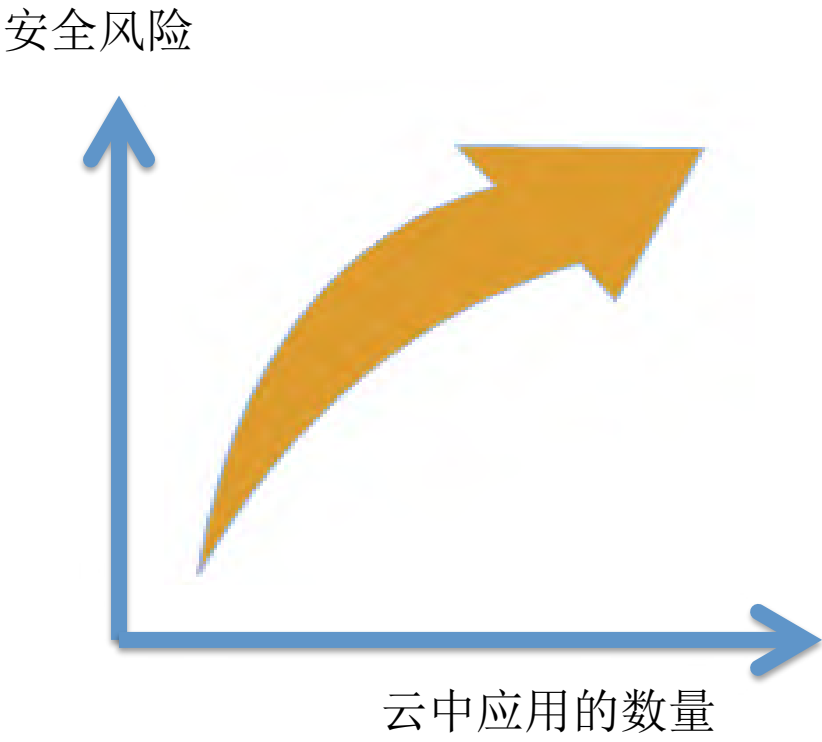
近期，安恒风暴中心受某部门委托，针对某省互联网金融网站抽样了100个进行了深入的检测，发现其中有53个网站存在高危漏洞，占总数的53%。其中，6%的网站可以getshell，47%的网站发现SQL注入漏洞，2%的网站发现Struts2命令执行漏洞，25%的网站发现跨站脚本漏洞，4%的网站发现逻辑漏洞，6%的网站发现密码重置漏洞，4%的网站存在弱口令，2%的网站发现目录遍历漏洞，6%的网站发现高危敏感信息泄露。



管理后台弱口令


首页
产品
新留言
新订单
运营状况
网站运营时长：733天
查看详情
域名：
续费
产品统计
排名
产品名称
浏览量
留言
20
15
10
5
0
2015-05-28
2015-06-07
2015-06-17

单一防护无法确保整体安全

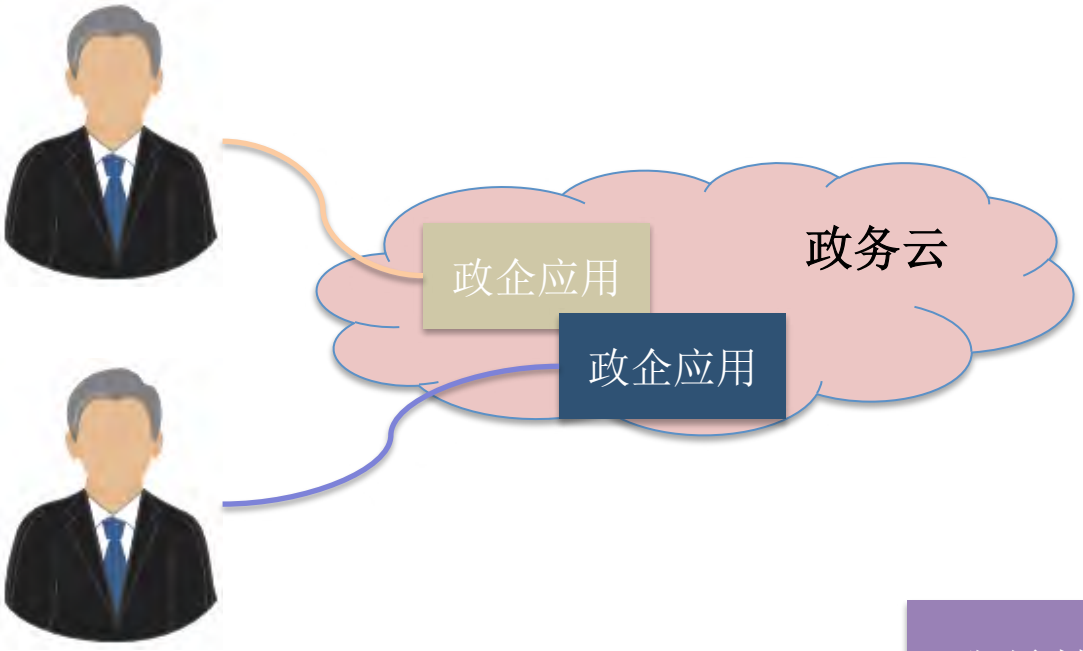


安全威胁的多样化

云中存在的大量应用

云安全风险呈几何级上升

内部安全威胁趋势未减



各单位管理员

第三方代维人员

账号越权使用

权限不规范

违规操作

数据泄露

政务通信安全

默克尔手机被美情报机关监听

非法伪造无线热点，交流信息泄露

2013年，美国“棱镜门"事件

苹果iPhone的“隐私门”

最近的苹果icloud账号被入侵。

政企云安全

1. 政企云化是大趋势
2. 政企的安全顾虑及现状
3. 政企云的云安全建设
4. 政企安全大数据化
5. 政企安全移动化

政企安全漏洞检测之变化

- 独立的漏洞检测工具
- 综合型安全检测工具箱
- 安全监测云

WEB应用弱点扫描器

数据库弱点扫描器

远程安全评估系统

安全监测云（风暴中心）

海量

快速

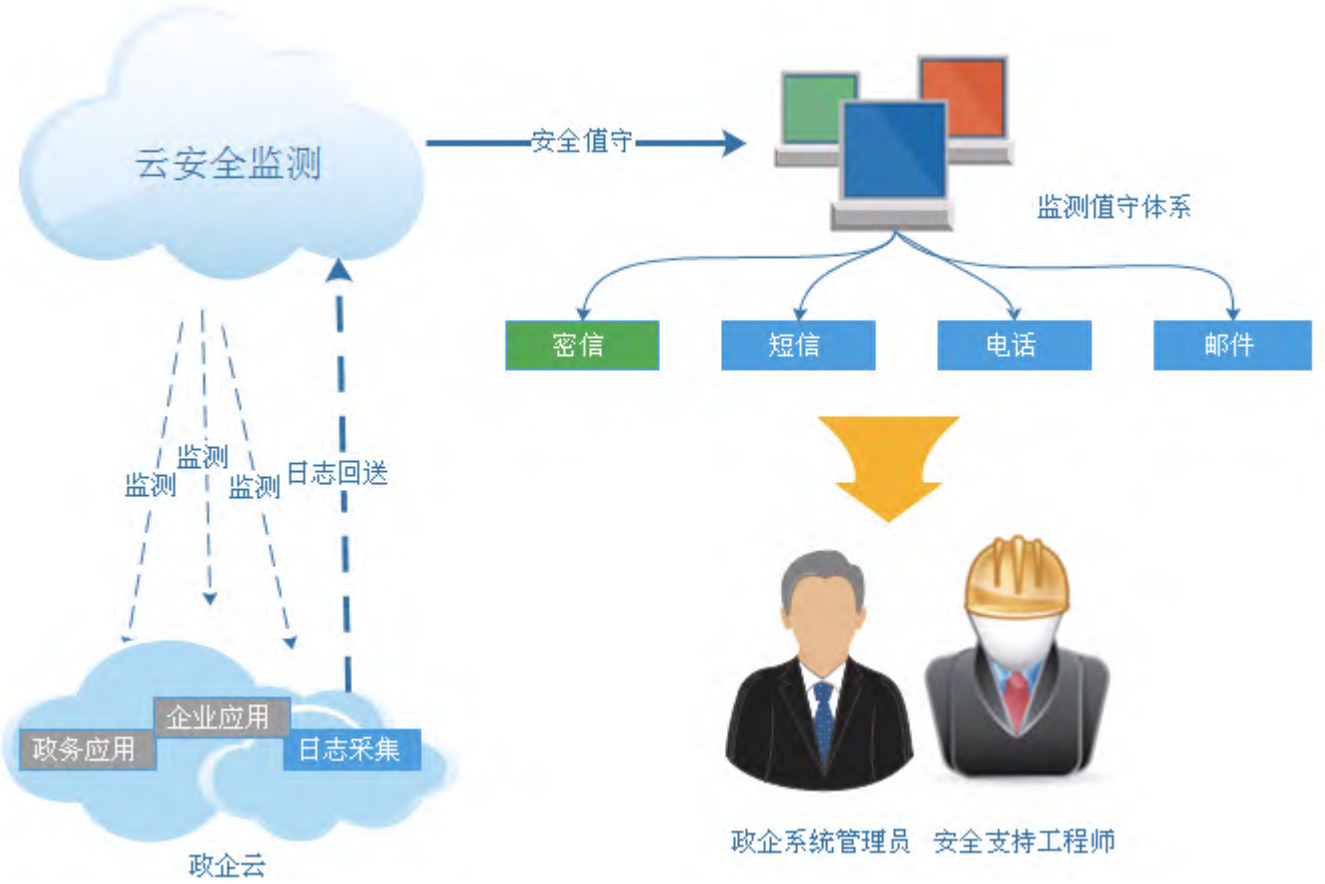
持久化

云安全监测

云端安全监测

安全值守

实时告警

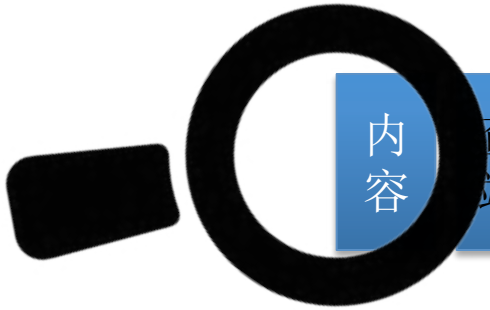


7*24小时监测与服务实践，政企用户，国家相关机构提供及时服务与大量数据支撑

网络空间安全搜索

风暴中心搜索引擎能够支持海量空间数据的毫秒级查询，精确定位要查找的各类信息，支持多维度、多关键字查询。

指纹	http、ssh、ftp、rdp、流媒体、CMS、工控系统等
内容	查找含有特定安全内容的站点



弱点	系统漏洞、应用层漏洞	事件	网马、篡改、敏感言论、暗链、黑页、域名劫持	区域	辖区安全数据

Openssl heartbleeding 漏洞

2014-4-9，openssl 爆出心脏出血漏洞（CVE-2014-0160）

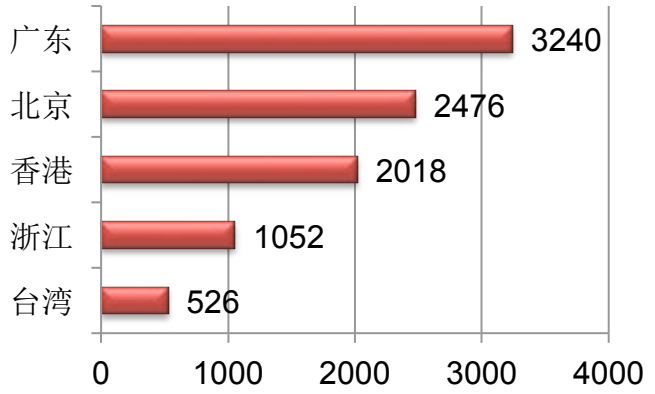
- 至今仍有23,512个站点未修复

2015-7-9，openssl又将披露一高危漏洞

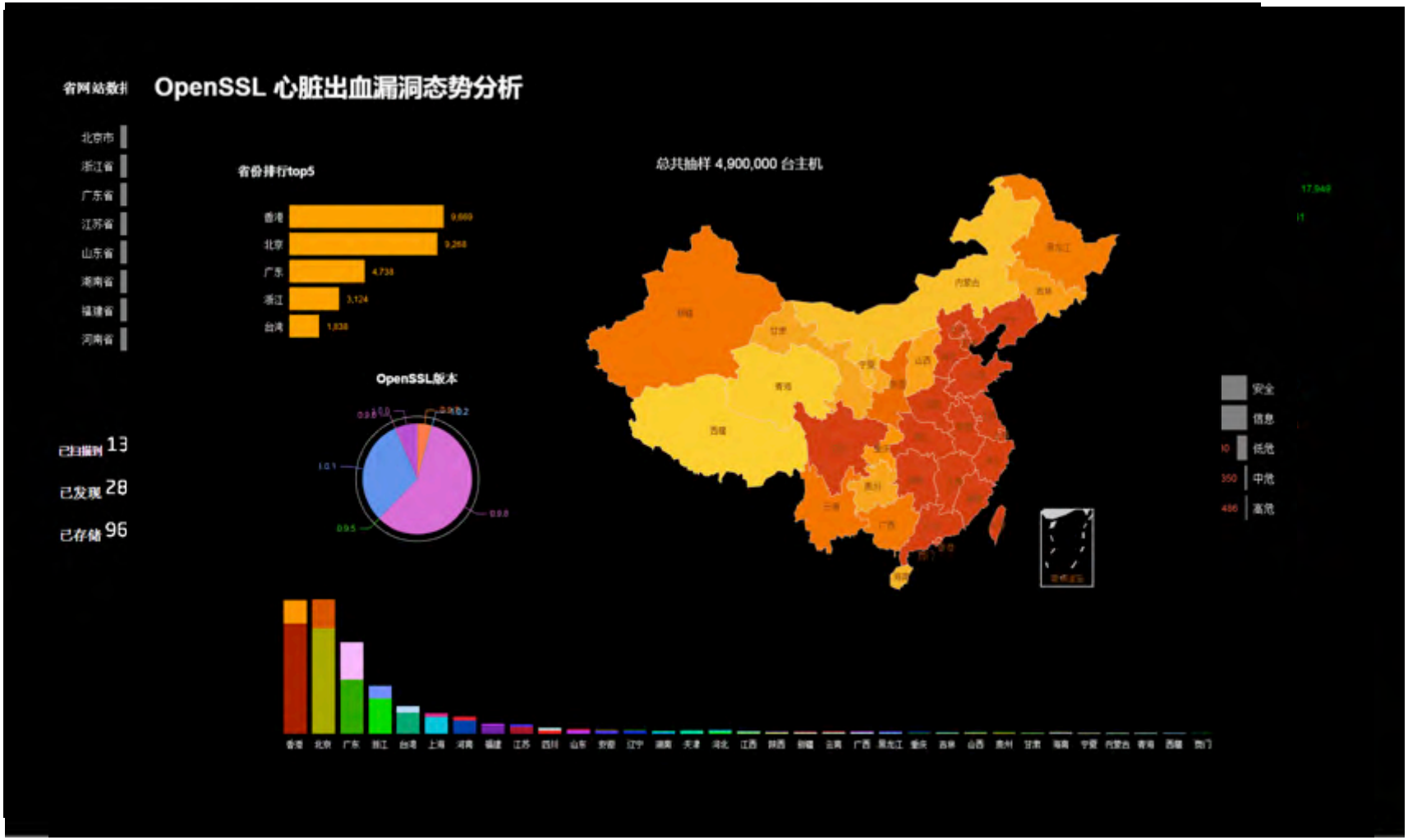
- 疑似受影响的有约31, 864 个网站

风暴中心对政府、金融、电子商务及重要在线系统进行抽样分析，通过对400余万的主机抽样分析发现问题非常严重。本次受影响openssl软件占比42%，影响最大的为广东、北京、香港、浙江和台湾。

本次漏洞受影响最严重区域TOP5



深度可视化

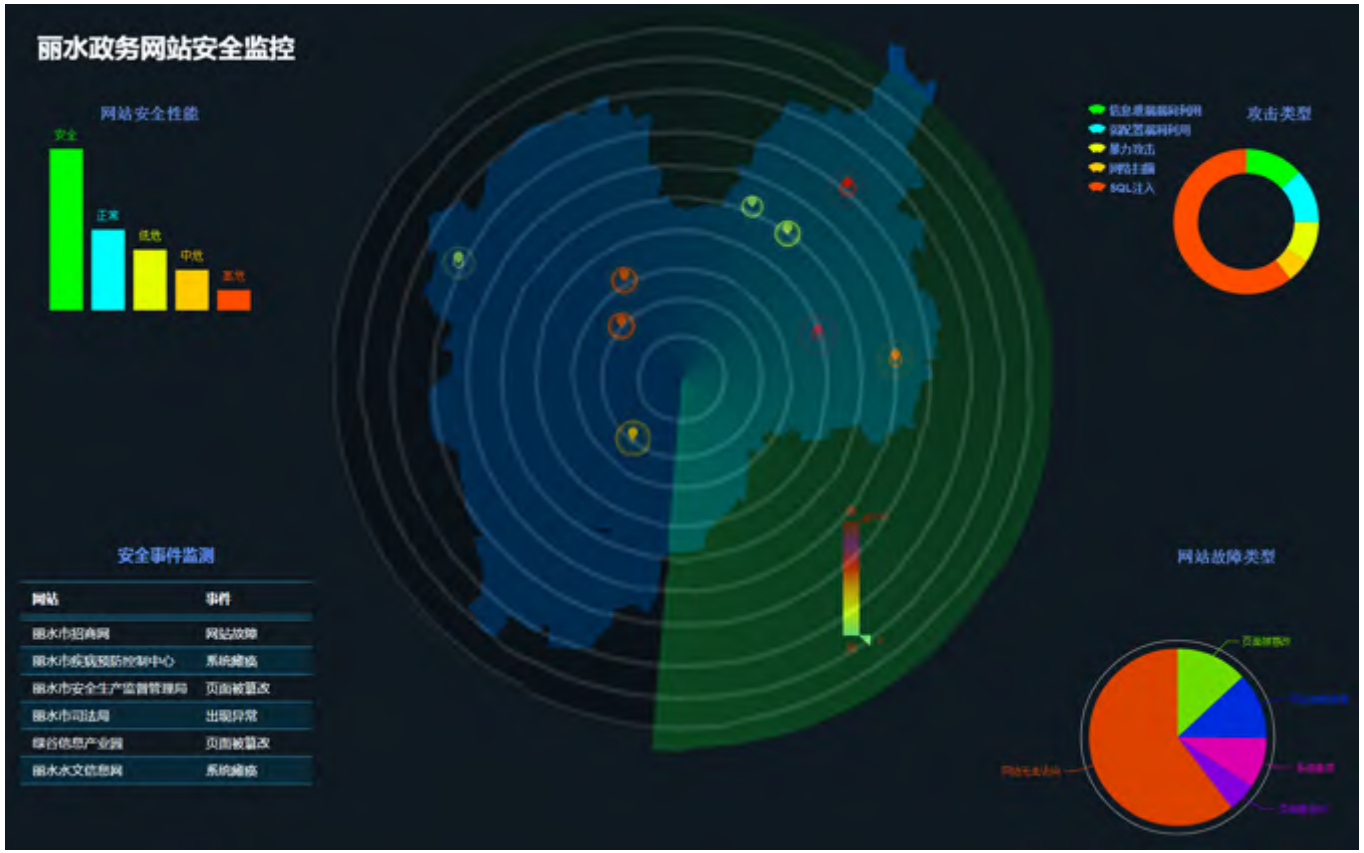

OpenSSL 心脏出血漏洞态势分析
省网站数排
北京市
浙江省
广东省
江苏省
山东省
湖南省
福建省
河南省
已扫描到 13
已发现 28
已存储 96
省份排行top5
香港
北京
广东
浙江
台湾
9,869
9,268
4,738
3,124
1,838
OpenSSL版本
总共抽样 4,900,000 台主机
安全
信息
低危
中危
高危

试点级云项目安全实践

政务云资产梳理

安全状态监测，攻击行为监控，安全走势预分析

政务云安全管理摆脱黑匣子困局



政府网站“跨境”事件发现

953个政府网站解析到国外地址

挖掘
分析

730起域名劫持事件

220多起伪造政务域名事件

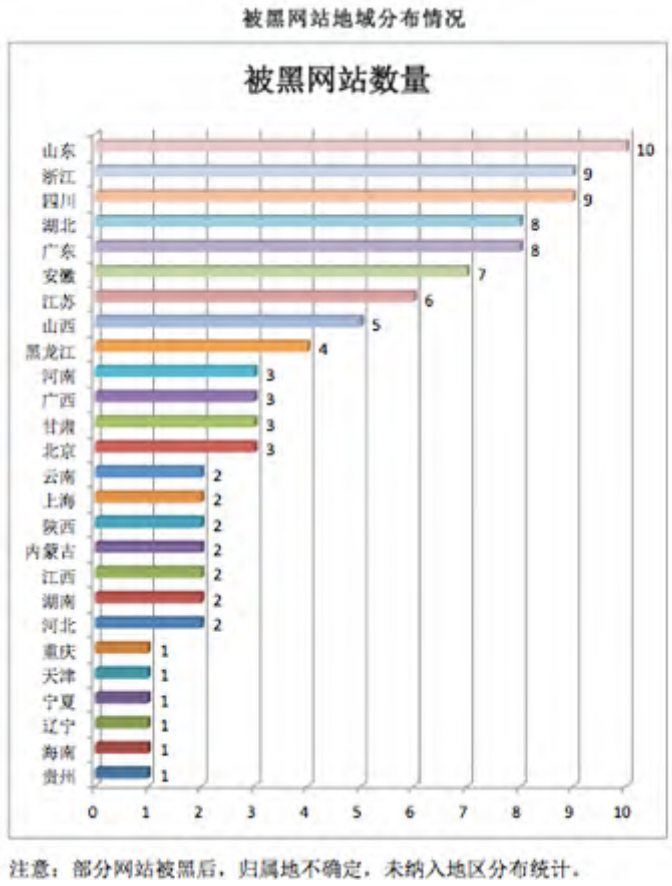
大多成为博彩类广告网站的入口

匿名者攻击事件

5-30　　风暴中心发现知名黑客组织匿名者发起对我国政府网站攻击

期间，监测发现158起被攻击事件

山东、浙江、四川等地受攻击严重



反共黑客事件监测

近两个月内，风暴中心共监测通报

22起反共黑客恶性攻击事件

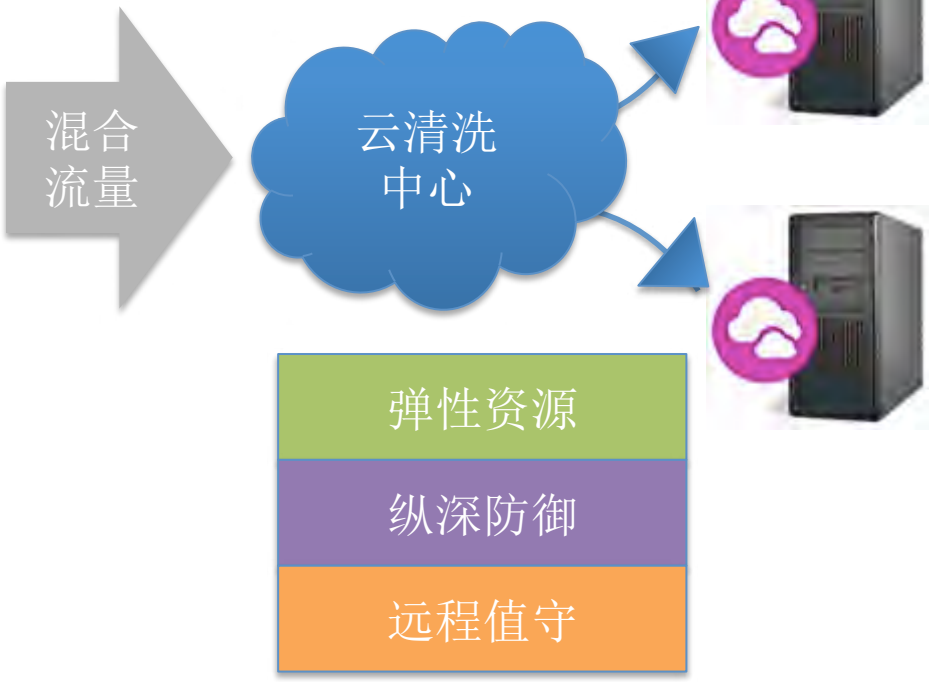
政企安全防护之变化

- 独立的硬件防护设备
- 云安全防护

下一代防火墙

WEB应用防火墙

DDos防护



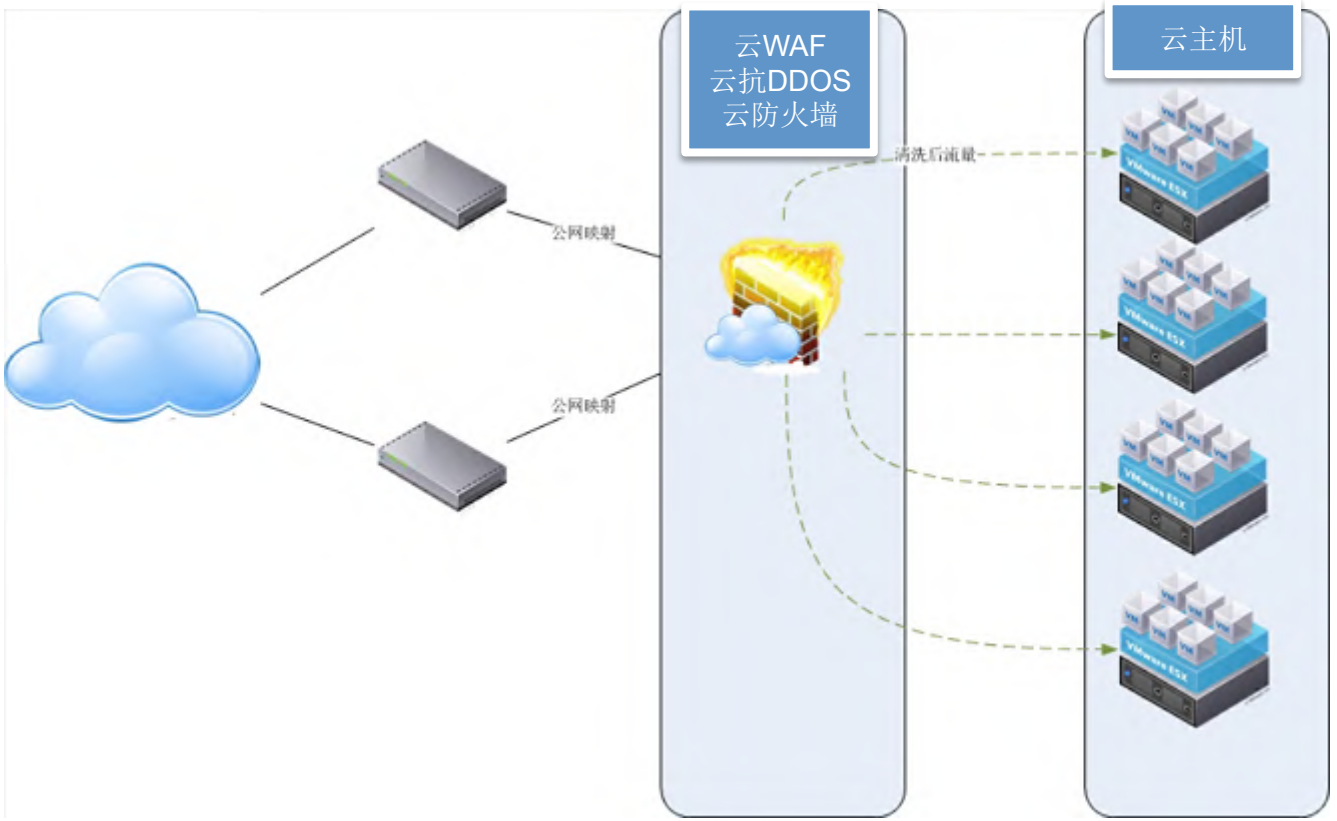
云安全防护

云端纵深安全防护

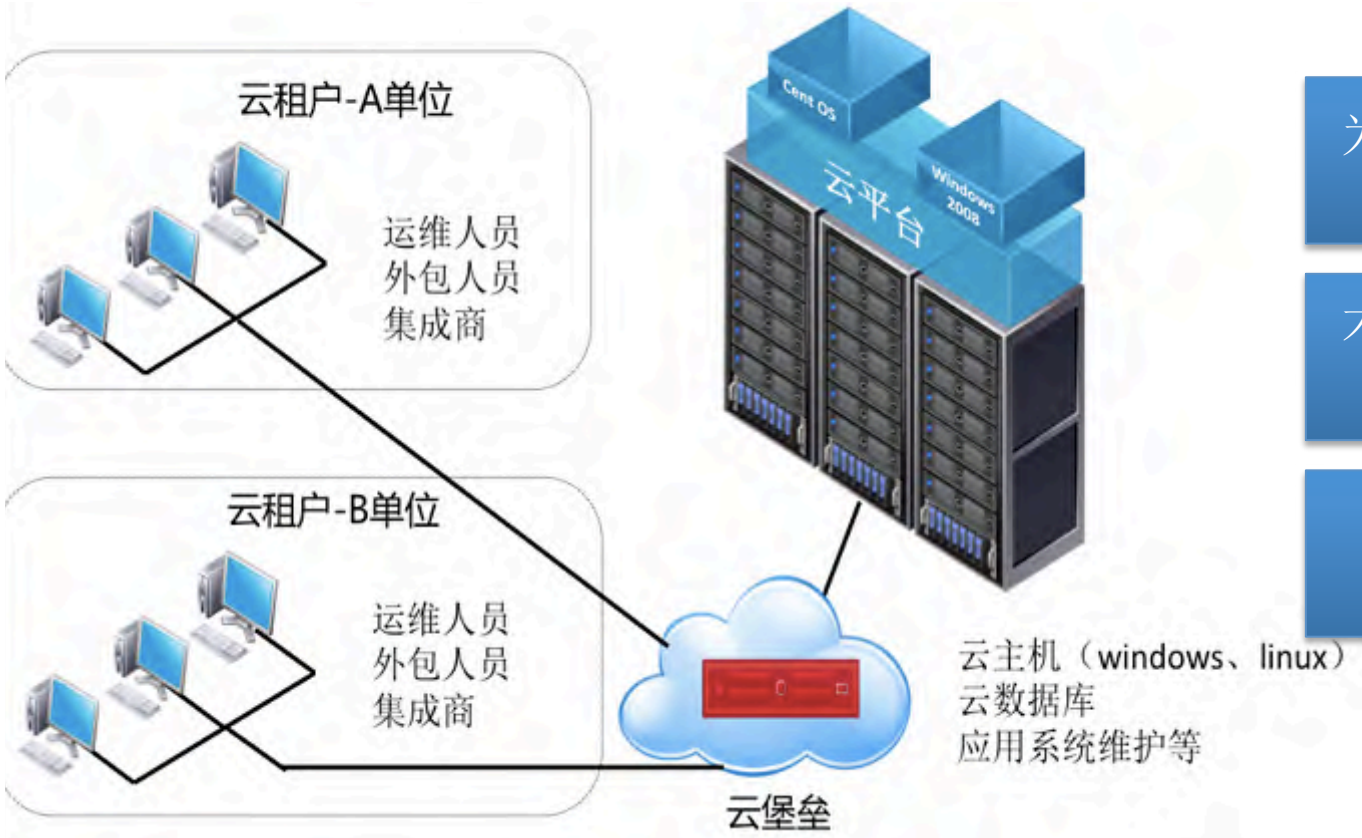
云DDOS流量清洗

应用层攻击防护

网络流量访问控制



云审计之运维审计 — 和云深度融合，极简的部署和管理



为各类租户应用进行运维管控和审计

不同的政务应用可定制不同管控策略

规范运维管理权限

政企安全

1. 政企云化是大趋势
2. 政企的安全顾虑及现状
3. 政企云的云安全建设
4. 政企安全大数据化
5. 政企安全的移动化

政企安全之大数据 — 简明但是诉求清晰

各类安全数据需要集中存储，关联分析，形成安全分析综合平台

网络设备日志

服务器日志

安全设备日志

……

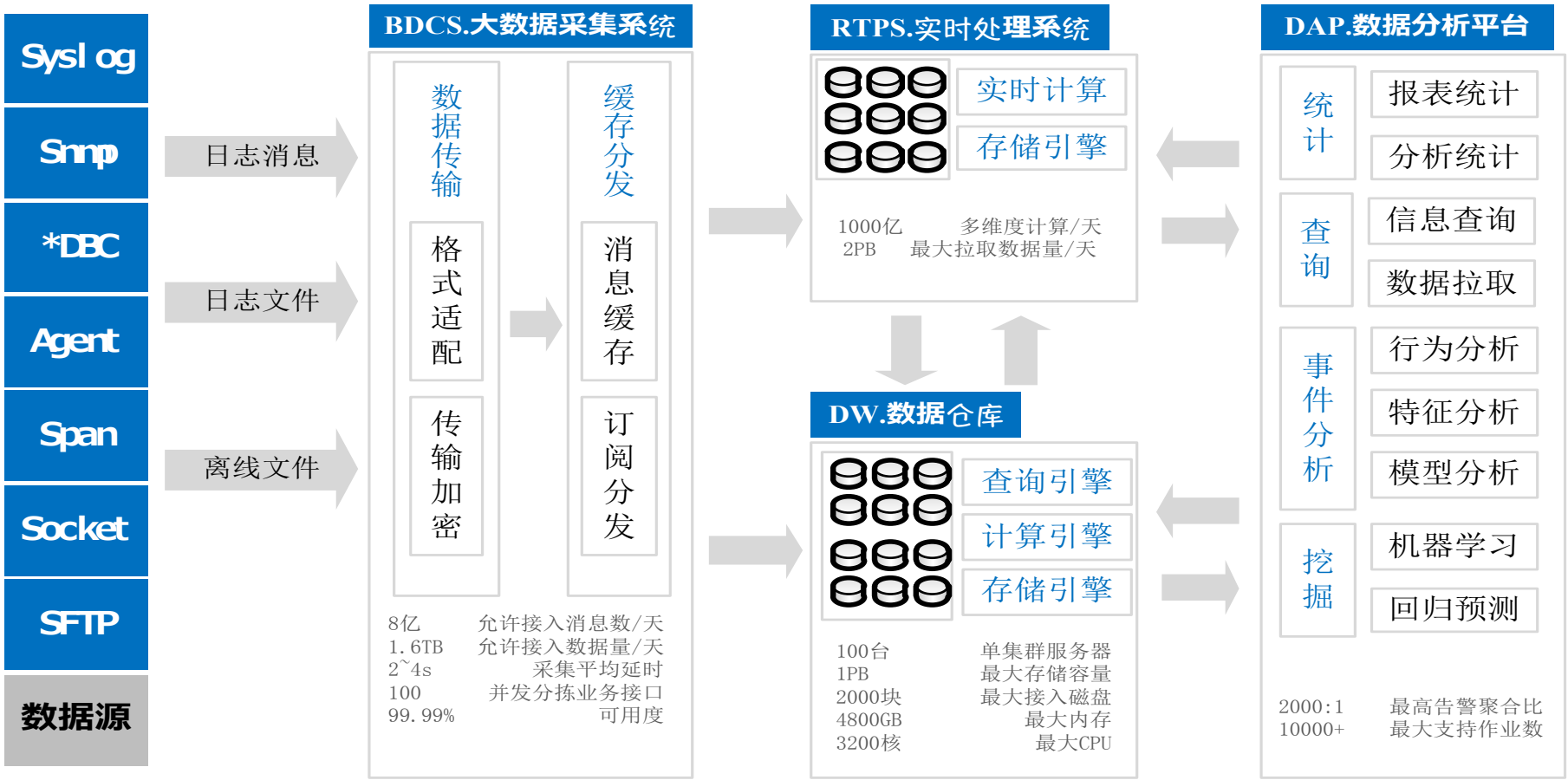
传统政企内网中的大量数据独立存放、独立分析

数据在线存储多为1-3个月

难于深入挖掘和关联分析

设备独立工作，无法协同联动

离线分析与实时分析双系统实践



日处理8亿tps,单集群能力超过100台服务器，最高聚合比2000:1

基于大数据的日志分析系统实践

虚拟设备　云安全设备　云主机　LINUX　云数据库　租户活动　虚拟化平台

LOG

海量存储，解决后顾之忧；
日志取证，确保有据可寻；

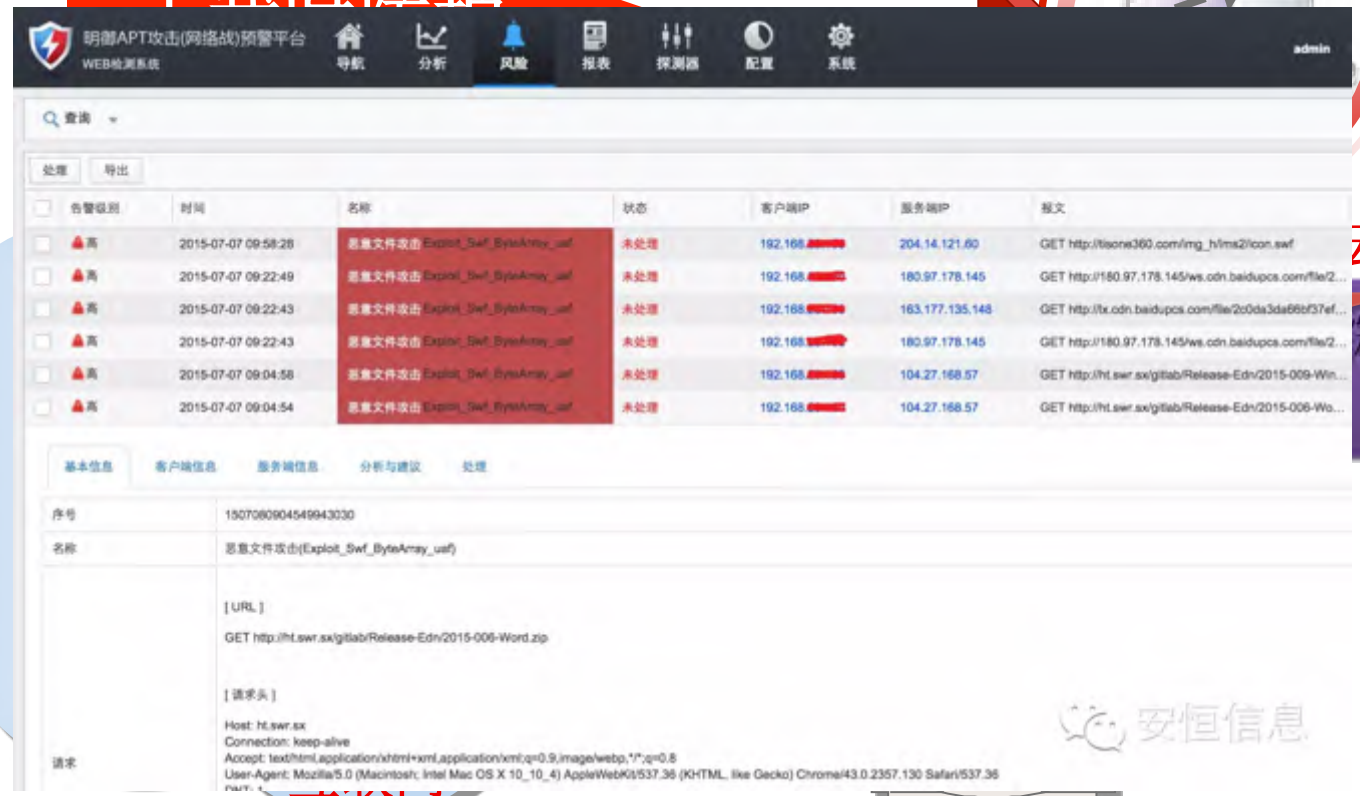
综合日志审计平台

多种日志，仅需一屏展现；
实时预警，让您未雨绸缪；

更广泛的日志源+深层次的智能=极为准确切实可行的洞查力

政企环境下的APT攻击预警

最近HackTeam被入侵，流传出来Flash的0day漏洞，安恒APT产品无需升级即可有效检出。



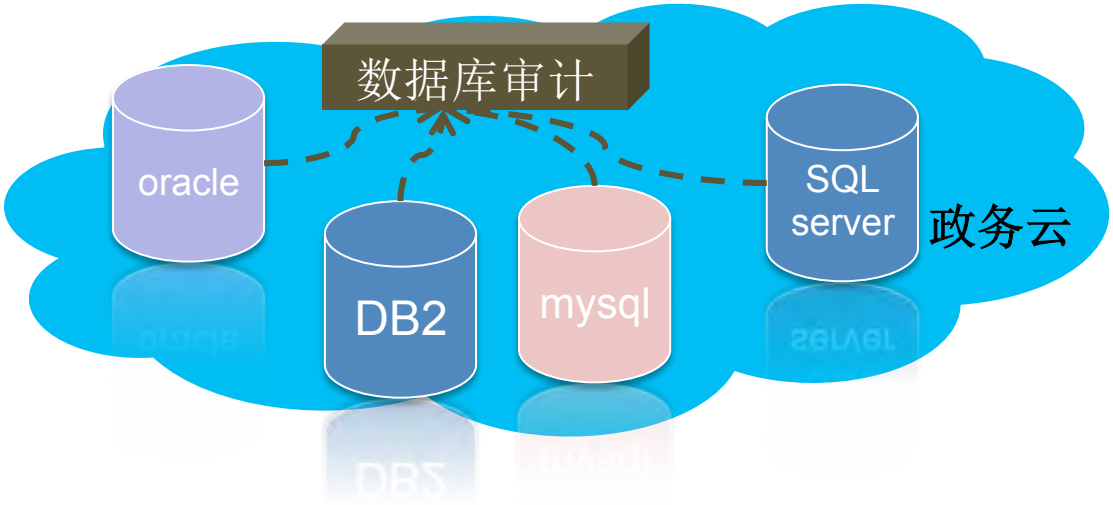
数据库审计 — 关心的是模型变化

全面审计、分析数据库操作行为

分析数据库操作现状

识别出现的异常行为

促进数据操作规范管理



用户或租户访问模型分析

服务器IP	帐号/应用帐号	源IP/应用源IP	客户端工具	表对象	操作类型	正常行为	可疑行为	异常行为
134.96.37.12(dbon...	14 / 0	31 / 0	9	447	12	23626	19234	28

第 1 页，共1页　　显示1 - 2, 共 2 条

服务器IP【134.96.37.12】帐号列表

帐号	源IP/应用源IP	客户端工具	表对象	操作类型	主机名	帐号类型
N/A	23 / 0	3	0	10	13	个人
c2migteam	1 / 0	1	2	4	1	个人
crmreport	1 / 0	1	1	3	1	个人
cwchen	1 / 0	1	4	4	1	个人
eaiprod	10 / 0	2	43	7	11	个人

帐号【cwchen】来源详细

源IP	客户端工具	主机名
134.98.104.146	plsqldev.exe	mshome\microsof-708f87

第 1 页，共1页　　显示1 - 1, 共 1 条

帐号【cwchen】权限详细

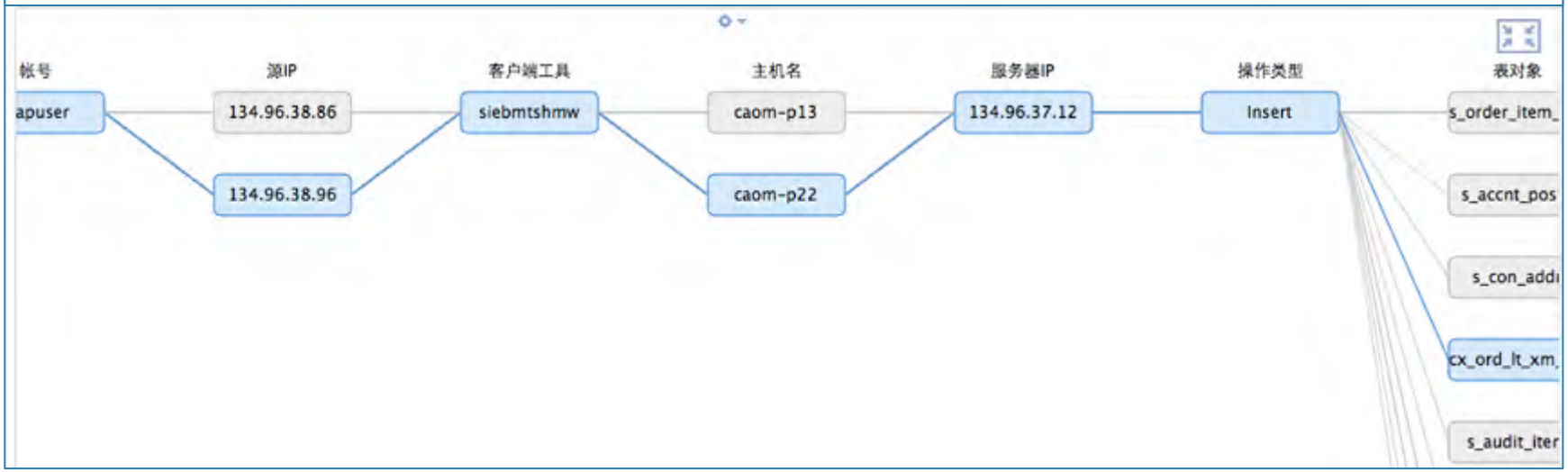
服务器IP	数据库名称	表对象	权限	业务主机群	探测器	敏感
134.96.37.12	sys	session_roles	Select	zjdx	dbone41	非敏感
134.96.37.12	sys	user_objects	Select	zjdx	dbone41	敏感
134.96.37.12	sys	plsqldev_authorization	Select	zjdx	dbone41	非敏感
134.96.37.12	cwchen	cwchen	Logout	zjdx	dbone41	非敏感

第 1 页，共1页　　显示1 - 4, 共 4 条

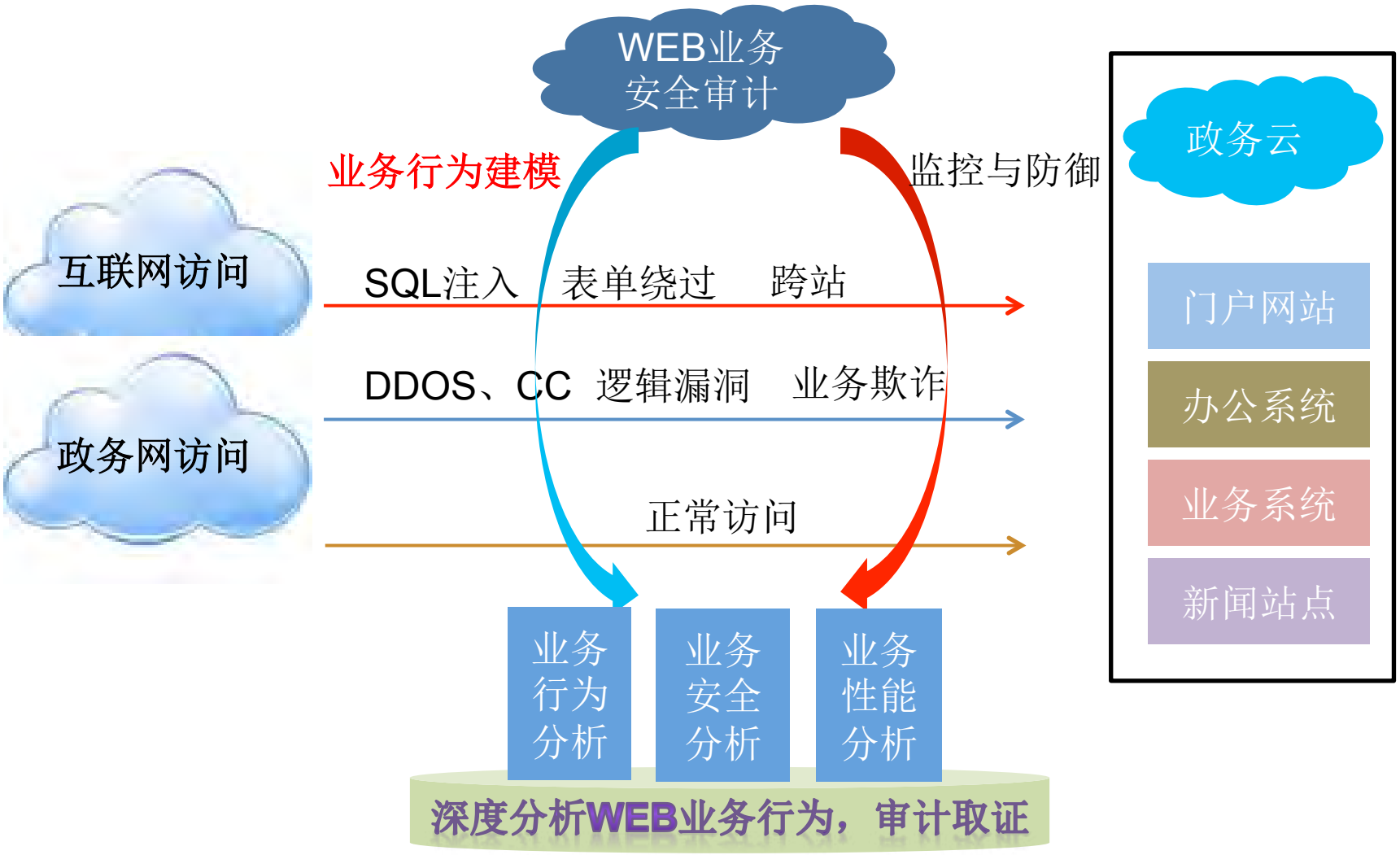
实现了用户或租户的访问轨迹分析

状态	帐号	源IP	客户端工具	主机名	服务器IP	操作类型+表对象	事件数
	ldapuser	134.96.38.86	siebmtshmw	caom-p13	134.96.37.12	Insert(s_order_item_xm)	790
	ldapuser	134.96.38.86	siebmtshmw	caom-p13	134.96.37.12	Insert(s_accnt_postn)	786
	ldapuser	134.96.38.86	siebmtshmw	caom-p13	134.96.37.12	Insert(s_order_item_xm)	790
	ldapuser	134.96.38.96	siebmtshmw	caom-p22	134.96.37.12	Insert(s_order_item_xm)	795
	ldapuser	134.96.38.86	siebmtshmw	caom-p13	134.96.37.12	Insert(s_order_item_xm)	802
	ldapuser	134.96.38.96	siebmtshmw	caom-p22	134.96.37.12	Insert(s_order_item_xm)	798
	ldapuser	134.96.38.86	siebmtshmw	caom-p13	134.96.37.12	Insert(s_con_addr)	786
	ldapuser	134.96.38.86	siebmtshmw	caom-p13	134.96.37.12	Insert(s_order_item_xm)	802
	ldapuser	134.96.38.96	siebmtshmw	caom-p22	134.96.37.12	Insert(s_order_item_xm)	795
	ldapuser	134.96.38.96	siebmtshmw	caom-p22	134.96.37.12	Insert(s_order_item_xm)	786

第 1 页，共2页 显示1 - 20, 共 36 条



业务安全分析与审计


WEB业务
安全审计
业务行为建模
监控与防御
互联网访问
政务网访问
SQL注入
表单绕过
跨站
DDOS、CC
逻辑漏洞
业务欺诈
正常访问
政务云
门户网站
办公系统
业务系统
新闻站点
业务
行为
分析
业务
安全
分析
业务
性能
分析
深度分析WEB业务行为，审计取证

业务安全分析与审计

业务分析

业务系统的访问行为分析

关键业务链分析；
访问用户建模分析；
基于业务统计分析
访问源分析：浏览器、操作系统
IP所在地进行分析；

安全分析

web攻击行为分析

业务逻辑漏洞分析；
越权行为分析
敏感数据泄漏分析；
网站商业爬虫、盗链、死链
新型攻击取证分析；

性能分析

web性能分析

网站访问并发、流量分析；
网站错误页面的分析；
网站延迟情况统计分析；

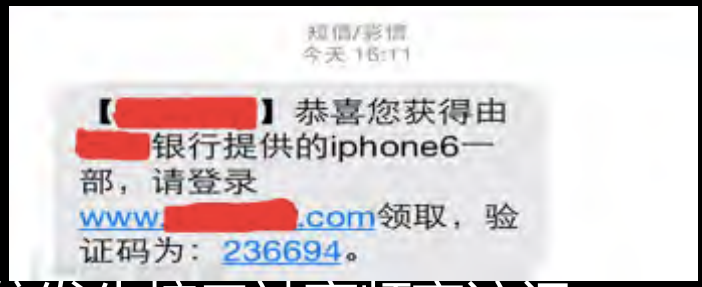
业务安全审计实践

案例一、高考志愿被篡改：

1、多名考试志愿信息被修改成别的学校；

2、在web业务审计中查询相关准考证号、找到修改记录，定位到具体IP地址；

案例二、某银行短信轰炸事件：



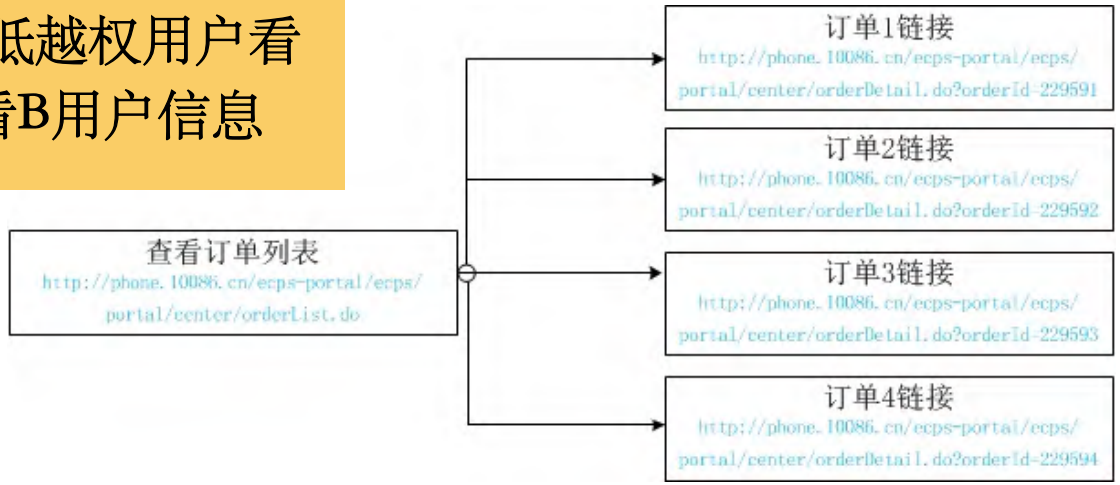
1、用户投诉某银行发生大量欺诈短信；

2、通过web审计访问频率统计，很快发现了短信发生接口被高频率访问；

3、进一步分析日志，发现是短信发送后台逻辑限制不合理导致；

业务安全审计实践

案例三、某业务存在低越权用户看高权限信息，A用户看B用户信息



Web业务审计分析：

1、基于用户访问行为模型分析，通过用户实际访问行为菜单和权限模型进行比较，识别低权限用户越权访问行为；

2、通过对业务系统关键参数字段的信息进行比较，识别A用户利用逻辑漏洞越权查看B用户信息的平行越权行为；

政企内网等保安全建设落地

技术安全
建设

安全管理
建设

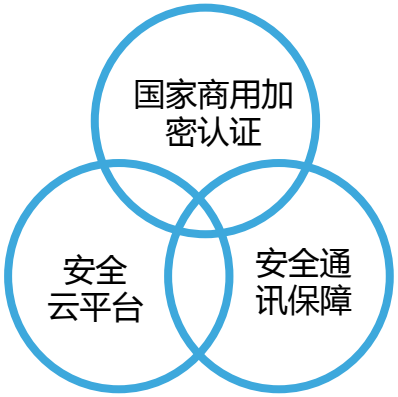
- 安全设计
- 安全开发
- 安全测试
- 安全实施
- 安全运维

等级保护 — 做虚还是做实？

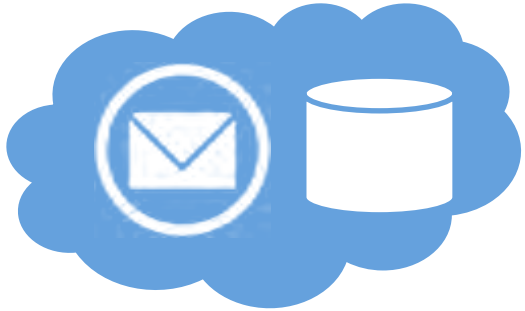
政企安全

1. 政企云化是大趋势
2. 政企的安全顾虑及现状
3. 政企云的云安全建设
4. 政企安全大数据化
5. 政企安全移动化

政务云安全——移动安全建设



全方位安全加密技术



通信过程加密

通信过程端到端全程加密。

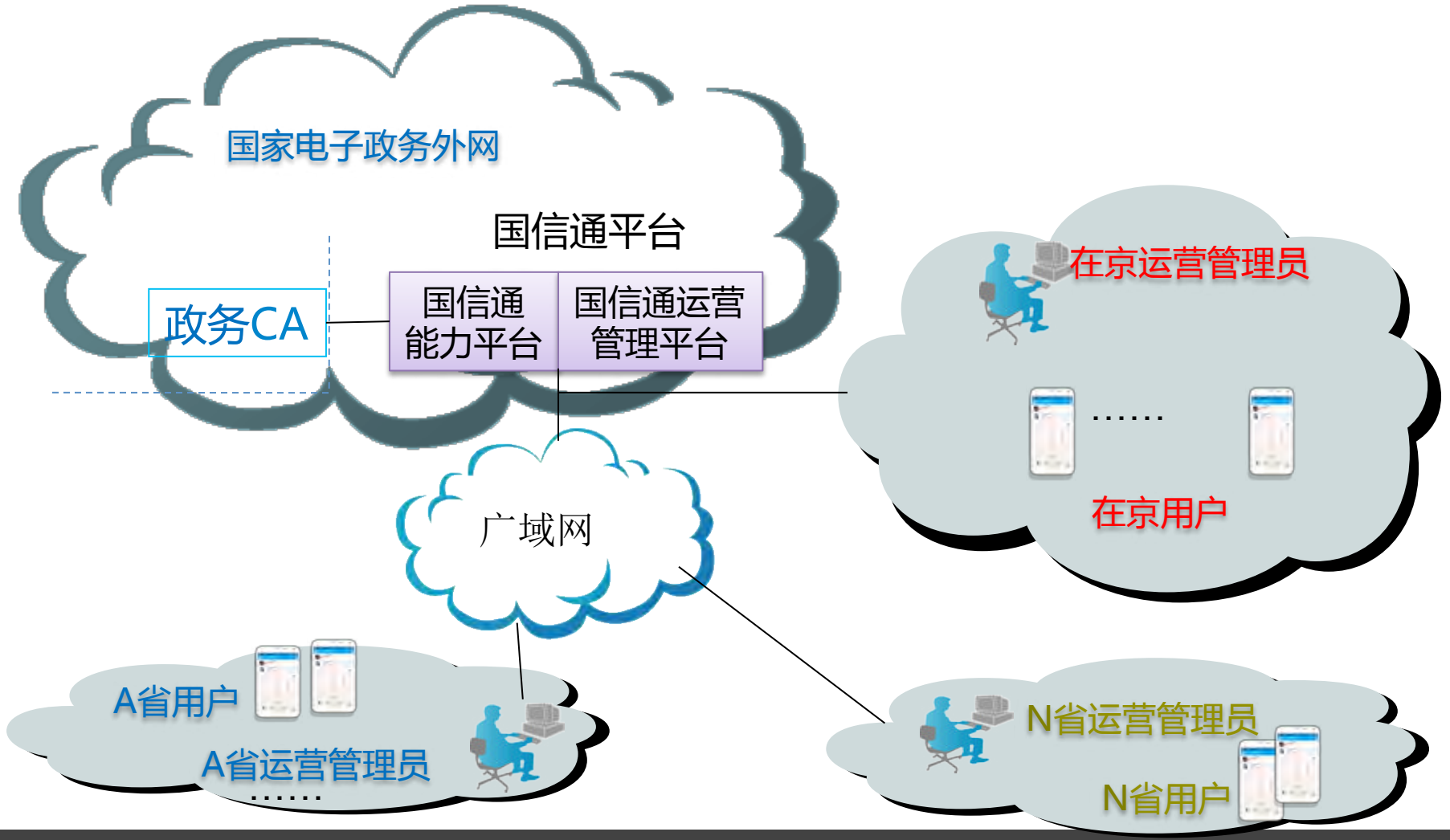
本地存储加密

本机数据存储加密。
密码登陆、保护消息、定时删除、阅后即焚、远程擦除

云端存储加密

提供重要数据云端加密存储功能，异地快速获取和同步，保障用户隐私

政务移动化办公--国信通系统



……

闭环云管端安全通道的建立

移动终端办公应用将成为一大重要方式
WIFI安全等威胁会加快安全通道和终端安全容器的需求。

未来将有云（云资源）——管（内网业务）——端（移动终端）办公趋势

DBAPPSecurity 安恒信息

WEB应用安全和数据库安全的领航者

THANK YOU

www.dbappsecurity.com.cn