云计算、大数据等新技术在医院信息安全领域的应用

东软集团股份有限公司

网络安全事业部

目录

1

云计算、大数据介绍及医疗云化情况


移动医疗
移动护理
医嘱管理
电子病历
病区信息
综合查询
医嘱执行单
护理评估
护理记录
生命体征
压疮管理
检查检验手术
健康宣教
病区信息

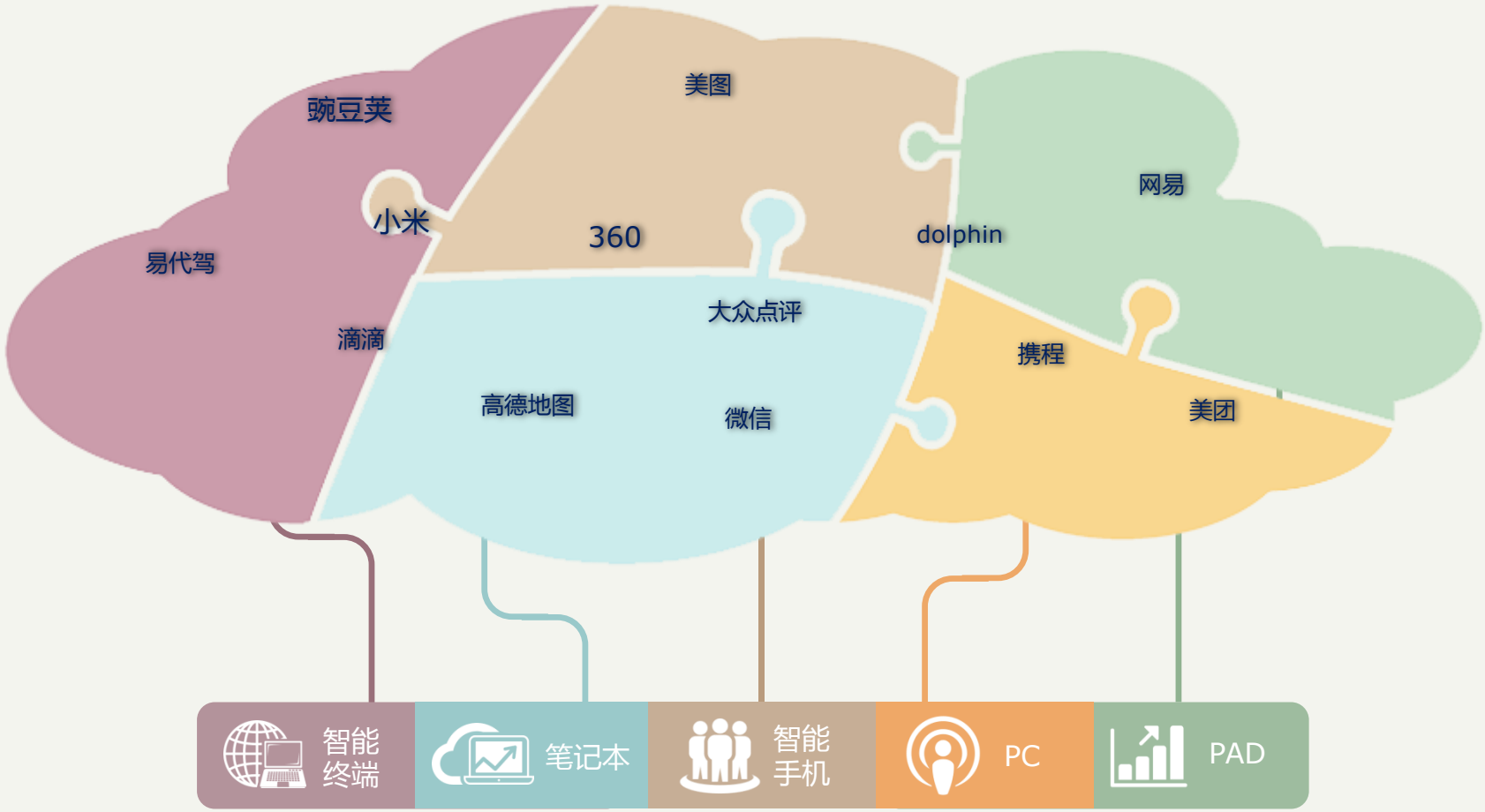
何为云计算?


齐齐哈尔市
挂号
医院
齐齐哈尔第一医院
科室
儿科门诊
儿科门诊 普通号
诊费 3.0元
王志刚 主任医师号
诊费 21.0元
全顺玉 副主任医师号
诊费 6.0元
导诊
发烧 眩晕
头疼 头 失眠
哮喘 眼 耳 皮肤瘙痒
感冒 鼻炎 恶心呕吐
咳嗽 咽喉肿痛 冠心病 颈椎病
贫血 肺炎 胸 心 高血压
湿疹 手 肠胃炎 心悸
反酸 胃 腰椎病 风湿
腹痛腹泻 腹 糖尿病 尿频尿急
骨质疏松 腿 关节疼
脚
北京市
科室


远程医疗
医学专家，为期待中的您找到方向

云计算概念

- 云计算是一种资源交付和使用模式，指通过网络获得应用所需的资源（硬件、平台、软件）。
- 提供资源的网络被称为**“云”**。
- “云”中资源在使用者看来**可以无限扩展的**，并且可以随时获取。这种特性精彩被比喻为**像水电一样使用**硬件资源，按需购买和使用。



Neusoft

云计算特点

- 数据在云端：不怕丢失,不必备份,可以任意点的恢复 ；
- 软件在云端：不必下载自动升级 ；
- 无所不在的计算：在任何时间，任意地点，任何设备登录后就可以进行计算服务；
- 无限强大的计算：具有无限空间的，无限速度。

PC	C/S	云计算
		
硬件为中心	软件为中心	服务为中心

Neusoft

云计算服务方式

SaaS 软件即服务

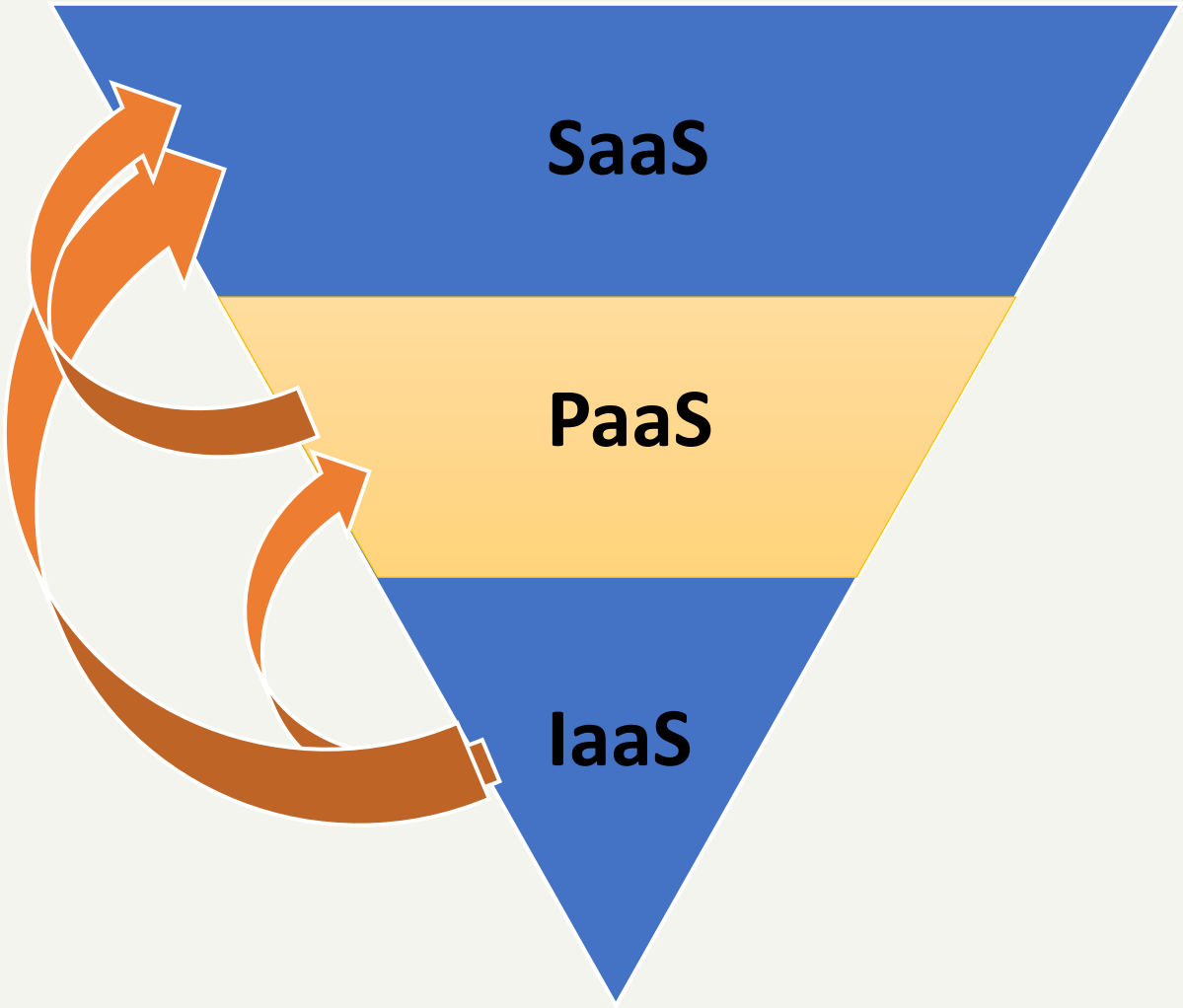
- 是基于互联网提供软件服务的软件应用模式。
- 特性：互联网特性、多租户特性、服务特性

PaaS 平台即服务

- 是一种分布式平台服务，厂商提供开发环境、服务器平台、硬件资源等服务给客户。
- 用户在其平台基础上定制开发自己的应用程序并通过其服务器和互联网传递给其他客户。

IaaS 基础设施即服务

- 把厂商的由多台服务器组成的“云端”基础设施，作为计量服务提供给客户。
- 将内存、I/O设备、存储和计算能力整合成一个虚拟的资源池为整个业界提供所需要的存储资源和虚拟化服务器等服务。



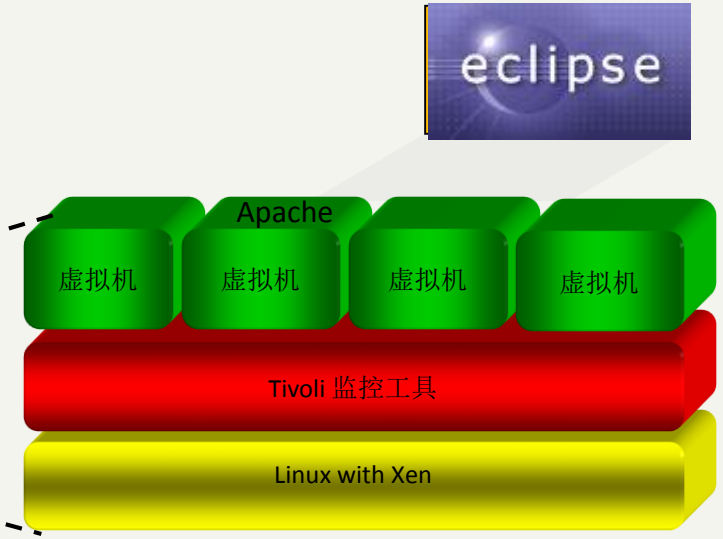
Neusoft

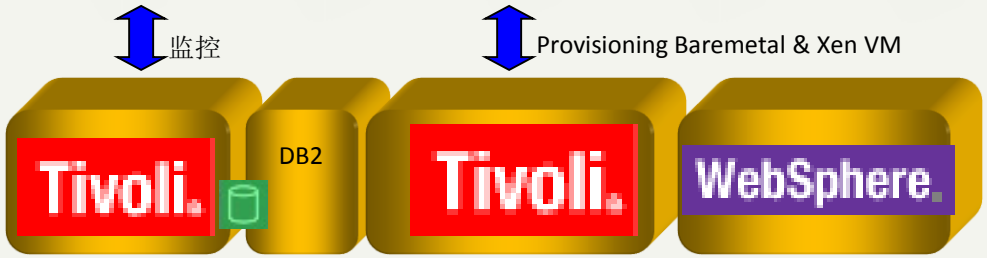
云计算为什么受关注？

Neusoft

云计算体系物理结构

数据中心 – System x





资源管理栈

云计算基础设施，可提供托管或现场解决方案。

Neusoft

云计算的应用-IaaS

- 当你想运行成批的程序组，但是没有合适的软硬件环境，可使用Amazon的EC2。
- 当你想在网络上发布一个短期（几天到几个月）的网站，可使用Flexiscale。

云计算的应用--PaaS

- 当你想把一个大容量的文件上传到网络上，允许35000个用户使用2个月的时间，可使用Amazon的Cloud Front。
- 当你想在网络上存储大量的文档，但是你没有足够的存储空间，可使用Amazon的S3。

云计算的应用--SaaS

- CRM
- 财务计划
- HR
- 文字处理
- Email

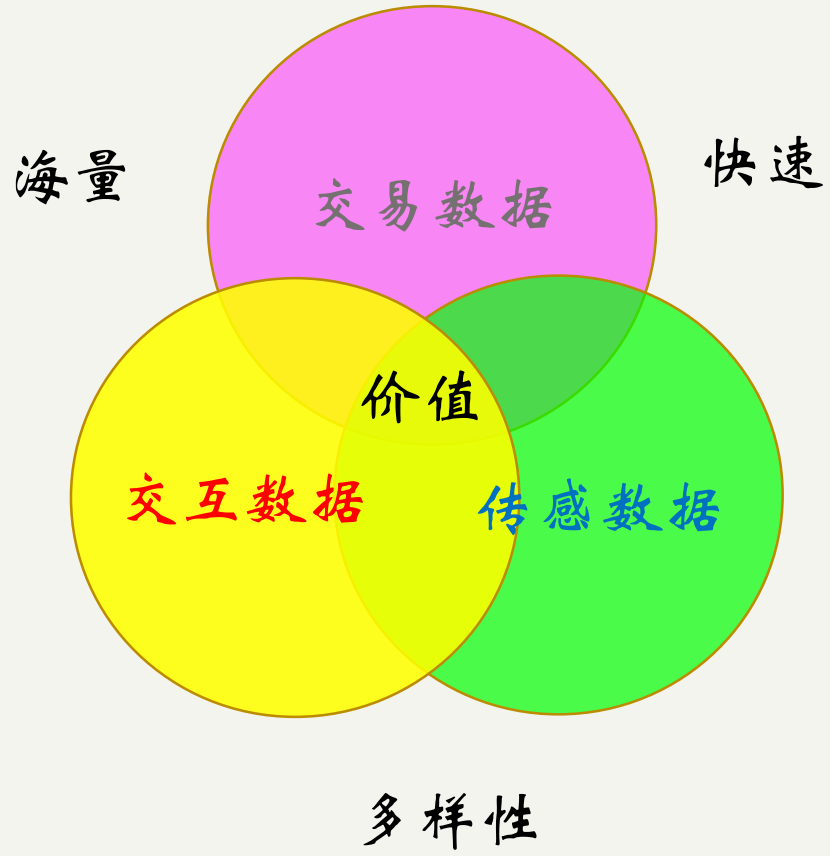
何为大数据？

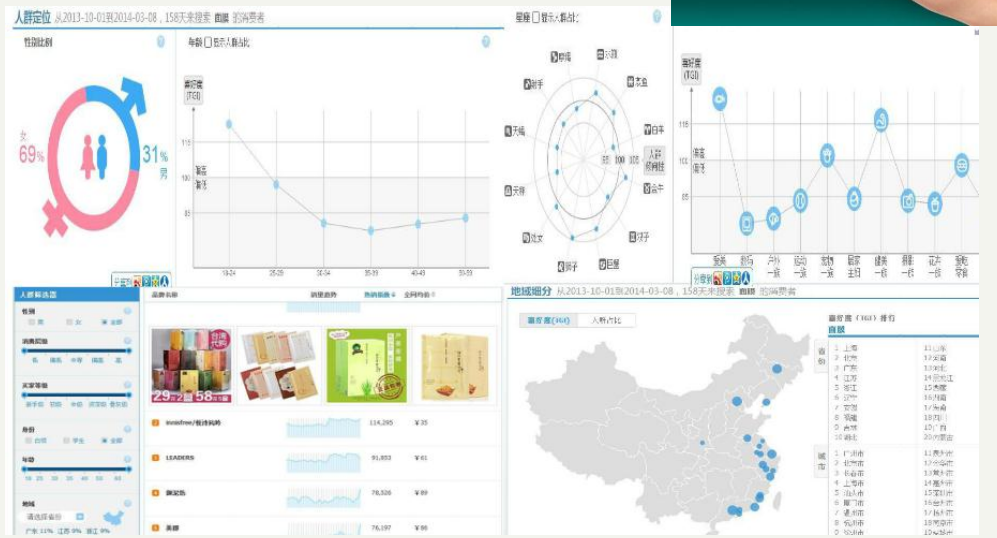
Neusoft

何为大数据？

何为大数据

大数据是指需要通过快速获取、处理、分析以从中提取价值的海量、多样化的交易数据、交互数据与传感数据。





Neusoft

大数据究竟有多“大”

各大公司的业务量

Google 公司通过大规模集群和MapReduce 软件，每个月处理的数据量超过400PB

百度每天大约要处理几十PB数据，大多要实时处理，如微博、团购、秒杀

Facebook 注册用户超过8.5亿，每月上传10亿照片，每天生成300TB日志数据

Yahoo! Hadoop云计算平台有34个集群，超过3万台机器，总存储容量超过100PB

淘宝网 有3.7亿会员，在线商品8.8亿，每天交易数千万，产生约20TB数据

Neusoft

大数据特点

Volume
（数据体量巨大）

- 数据量大 目前一般认为PB级以上数据看成是大数据

Variety
（数据类型繁多）

- 种类多 包括文档、视频、图片、音频、数据库数据等

Velocity
（处理速度快）

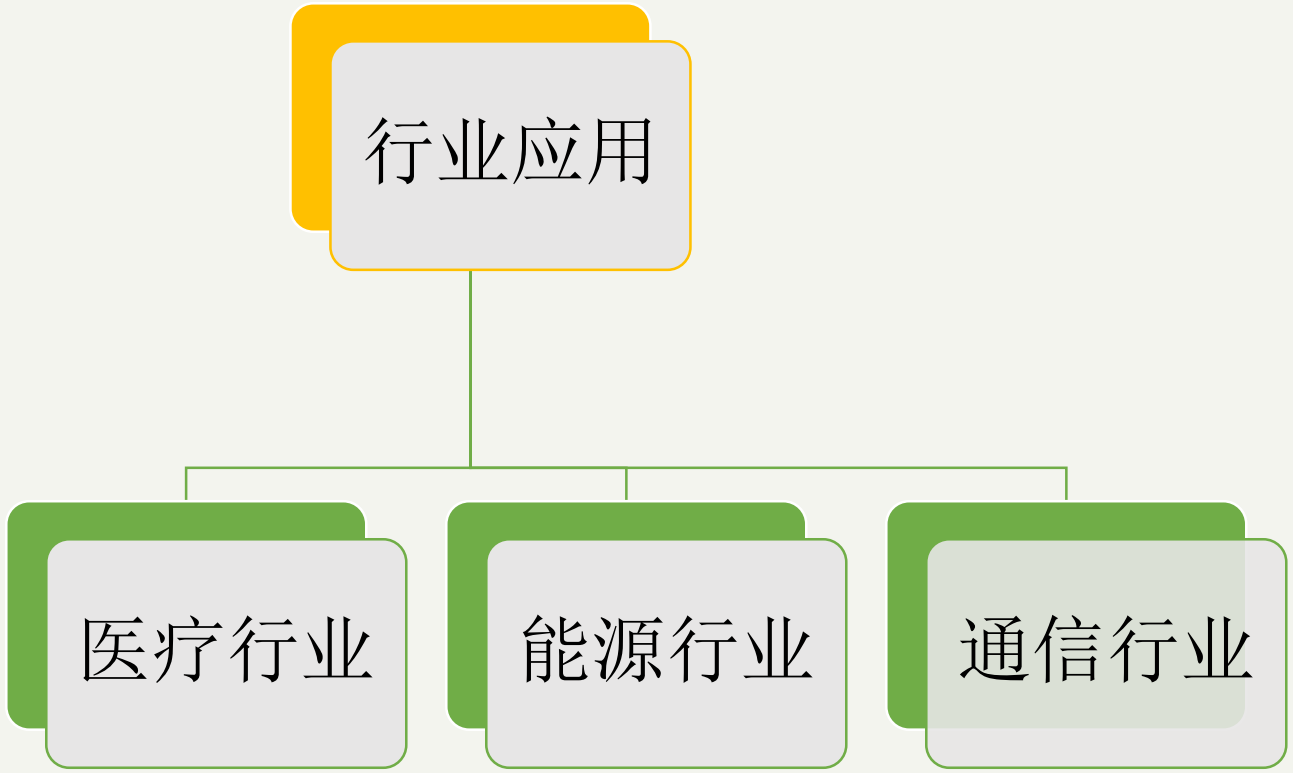
- 速度快 数据生产速度很快，要求数据处理和I/O 速度很快

Value
（价值密度）

- 存在大量的不相关信息，价值密度的高低与数据总量的大小成反比。

Neusoft

大数据行业应用



Neusoft

大数据为什么重要

	没有大数据	有了大数据
实时性	分析和应用间有长时间延迟，例如需求预测、市场营销活动等等	实时分析
混合数据	分析基于数量有限的企业实时数据	基于不同来源的数据，公共数据和私人数据
无限制访问	访问受到物理位置或设备限制	无限制访问
数据驱动做出决策	数据管理以实现监管或存档为目的	大规模的数据分析杠杆式开发客户洞察能力和驱动策略
数据的货币化	数据作为一种管理最小风险的分产品，价值低	数据作为一种资产被货币化

云计算与大数据

大数据不仅仅是“大”

多大？TB级PB级ZB级

比大更重要的是数据的复杂性，有时甚至大数据中的小数据如一条微博就具有颠覆性的价值

云计算本身也是大数据的一种业务模式

为大数据提供了无线延展的计算资源

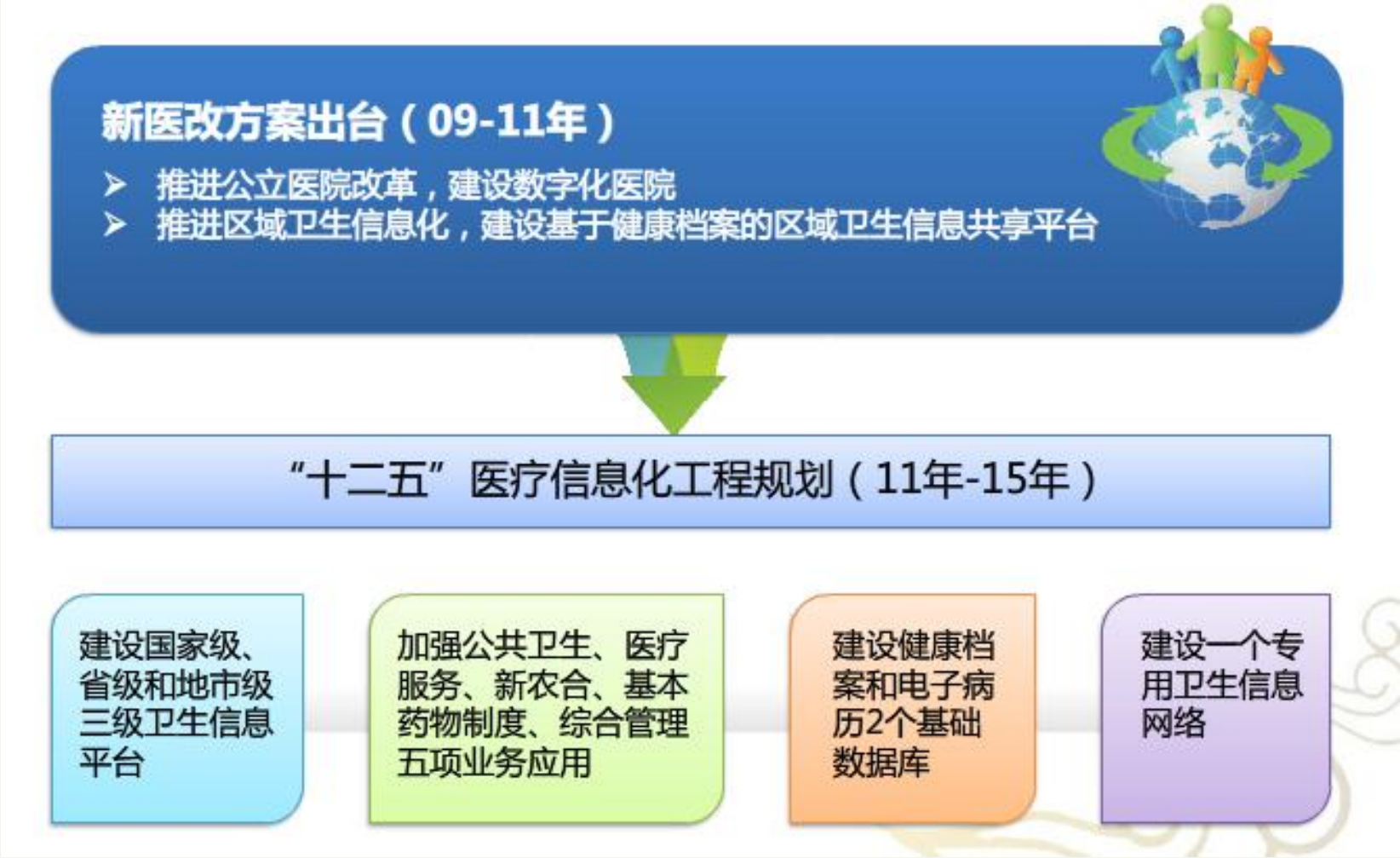
商业模式驱动

应用需求驱动

云计算本身也是大数据的一种业务模式

Neusoft

医疗信息“云”化背景——中国医疗改革



Neusoft

云医疗模式

- 云医疗是云计算技术在医疗领域的先进应用，
- 缓解了海量数据难于存储、信息数据孤岛这两大就医难题。

Neusoft

云医疗模式的优益性

Neusoft

云医疗——宁波云医院

什么是云医院

- 在**线上**是一个虚拟医院，**线下**则是一家混合所有制医院
- 通过线上线下的**联动**，实现网上门诊、转诊和远程医疗服务

云医院的作用

- 个人健康档案管理服务
- 健康知识指导与咨询
- 健康生活方式服务
- 慢性病追踪管理服务

为什么选择云医院

- 足不出户看医生，**节约看病成本**
- 享受网上远程会诊服务，**专家就在身边**
- 随时随地与医生互动，**健康干预与康复管理更贴心、更及时。**

Neusoft

2

云计算、大数据面临的信息安全风险

云计算时代的安全威胁

云的7大安全威胁

- 共享技术的漏洞
- 数据损失/数据泄露
- 恶意的内部用户
- 审计服务以及通讯骑劫
- 不安全的应用接口
- 恶意使用服务
- 未知的风险

云的新安全挑战

- 如何在不安全的环境中构造安全服务
- 如何强制远程第三方实施安全策略
- 如何应对动态的安全边界
- 如何应对虚拟化环境的安全挑战
- 如何对云中数据泄漏进行检测
- 如何防止利用云来进行安全攻击

舒马赫医疗数据外泄事件的引发

数据泄露方式可能会出现在医疗机构信息化流程中的各个环节，

都使得医疗机构面临的数据泄露威胁日趋严峻，具体表现在以下三方面

一、联通信息孤岛，种下安全祸根。

- 近年来，消除信息孤岛是医疗信息化建设的重中之重。
- 政策推动医疗机构上传数据，方便医疗主管部门监管医院运营；
- 区域平台、医联体每个终端都可能成为数据泄露的出口。
- 与各级主管部门以及定点药店对接，在数据与业务共享的前提下为参保人提供服务。安全威胁的来源也更加广泛，远远不局限于医疗机构内部。

二、BYOD浪潮引发新漏洞

- Android系统缺乏合法验证机制，没有安全机制，缺乏有效的防护手段，一旦医生使用Android系统时从不安全的移动应用商店中下载APP就可能被植入木马，再将木马带入医院系统，进而威胁医院数据安全。

三、云应用埋下隐患

- 数据从数据中心机房通过云传到用户终端，然而中间的云安全保护机制是否完善呢？
- 据调查医疗机构云服务安全保障还有待完善，医疗机构在构建云应用时一定要注意安全保护工作。

Neusoft

一则几乎刚刚发生在昨天—携程事件思考

通过携程事件反思我们自己的信息安全状况

- 我们的安全管理者是否对信息系统中的IT防护措施做到可见、可控、可追溯？
- 防火墙、ips、WAF等安全控制策略是否有效、完整，上一次更新时间是多少？
- 应用和系统漏洞上一次修复时间点是？
- 有哪些业务系统和人可以调用访问数据库？其访问权限是否合理、最小化？
- 有多少内部人员、第三方人员可以接触核心系统？他们的开发、运维过程是否可视？
- 服务器的批量操作、高危命令执行是否可靠、经过不少于两方的确认？
- 关键服务器、网络设备的密码什么时候修改过？
- 数据备份的机制什么，上一次数据恢复演练是什么时间？

相信有很多人是没法完整答复的，因为我们的管理者没有这样去想过，更没有定期去系统性的梳理过。

Neusoft

云计算、大数据面临的信息安全风险分析

用户端

- 病毒攻击
- 欺诈邮件
- 欺诈短信
- 假冒链接
- 僵尸终端

- 一次性密码
- 强身份认证
- 硬件网银设备
- 交易签名
- 授权短信
- 安全插件
- 强制安全软件

网络通讯

- 钓鱼网站
- 账号截获
- 线上监听
- 诈骗信息
- 钓鱼基站
- DNS污染

- 传输加密
- 钓鱼信息监控
- 钓鱼网站强制关闭
- 钓鱼Wi-Fi基站监控
- DNS修改监控

网页应用

- 黑客窃密
- 网站挂马
- 应用弱点
- 网页篡改
- 跨站请求伪造
- 越权指令
- 密码试错

- 防火墙
- 网关加固
- 安装UTM, IDS
- 服务器加固
- 应用防火墙
- SSL证书
- 安全审计
- 运维安全管理

后台服务

- 监守自盗
- 内外共谋
- 审计跟踪
- 数据泄漏
- 命令行注入
- SQL注入

- 存储加密
- 数据库加密
- 数据库保护
- 加强日志及审计
- 异常交易监控

前端客户环节

- 用户端、传输层

中间应用环节

- 应用、门户、云环境防护、安全综合分析、审计

后端服务环节

- 防止数据泄露

Neusoft

风险隐患——前端客户环节

客户端

- 客户端、APP本身极具开放性
- 开发厂商、人员技术层出不清
- 普遍存在安全意识淡薄
- 更甚者 缺少基本的安全验证或验证代码明文传输

风险隐患——中间应用环节

云化

环境因素

- 目前多数租用公有云或政府私有云（属半私有云，因为大量其他政府行业在公用当地政府云环境）
- 投资有限，难以建立医疗完全自有私有云环境
- 将原有封闭的医疗内网信息、数据暴露在公有/半共有云环境中

价值因素

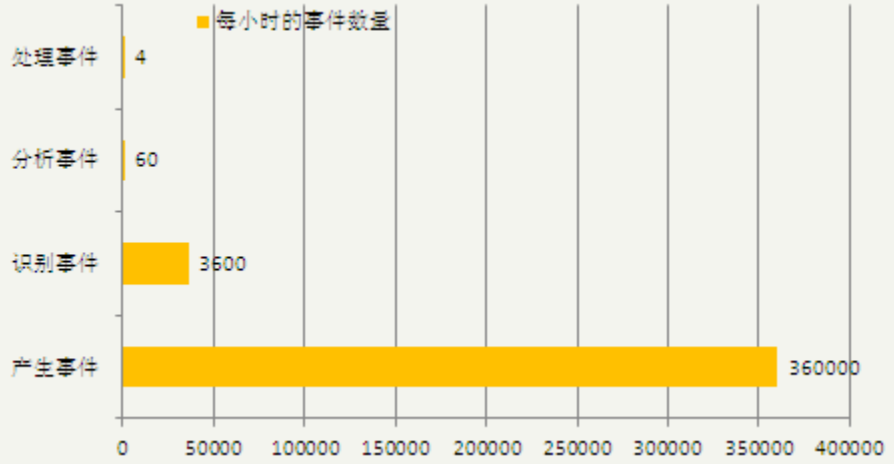
- 使得更多的社会、不相关人员可以通过网络窥探医疗信息数据

针对虚拟化、云环境中

- 缺少针对弹性运算的跟踪防护
- 缺少多租户隔离措施

综合安全分析整合

- 云环境中多种设备，不同的报警，如何整合？
- 海量的事件，海量的日志，如何分析、存储、归敛
- 人员操作如何审计、控制

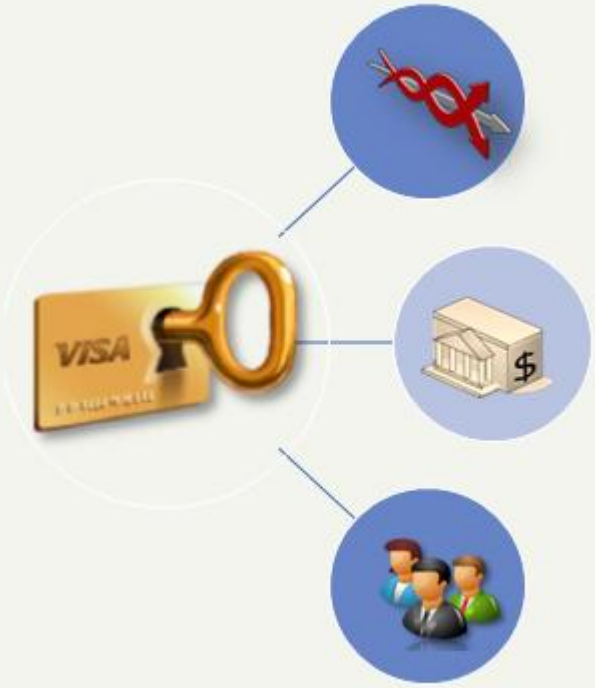


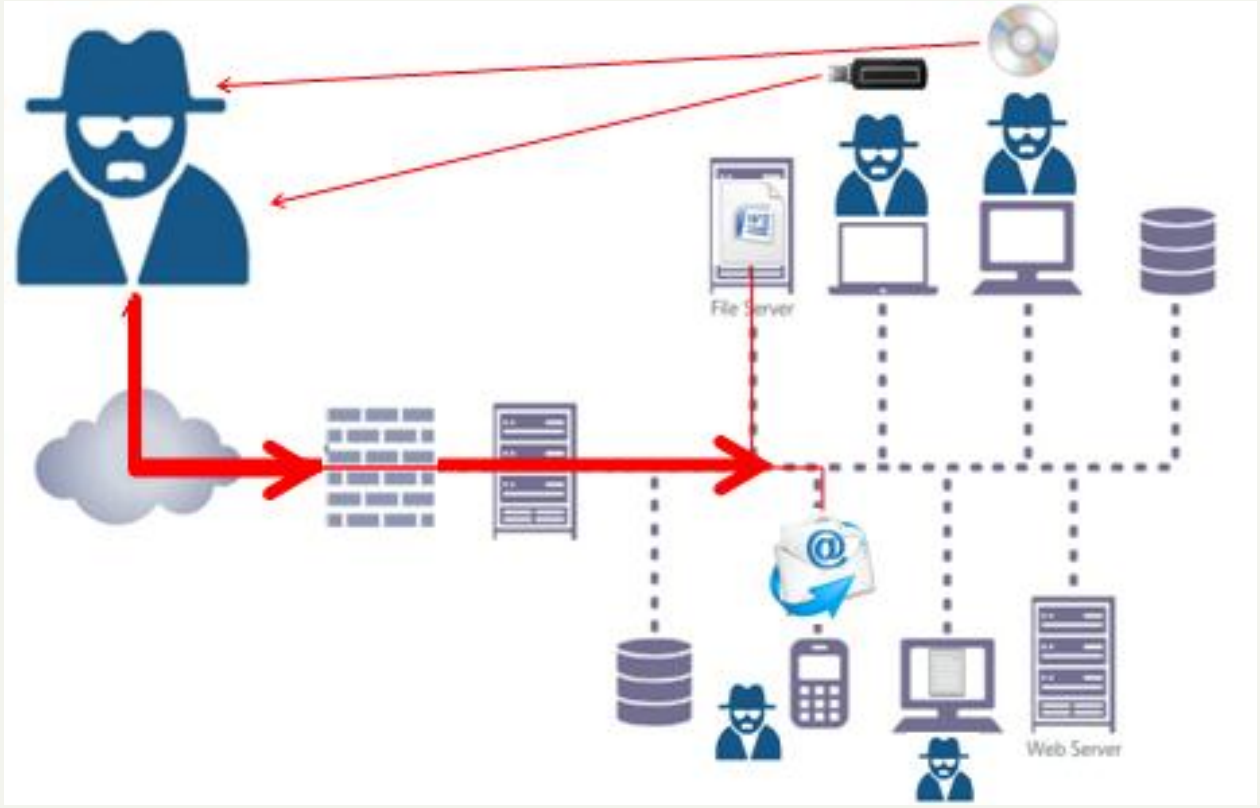
Neusoft

风险隐患——后台服务环节

后端服务

- 防止数据泄露
- 泄露事件回溯
- 泄露事件审计
- ……



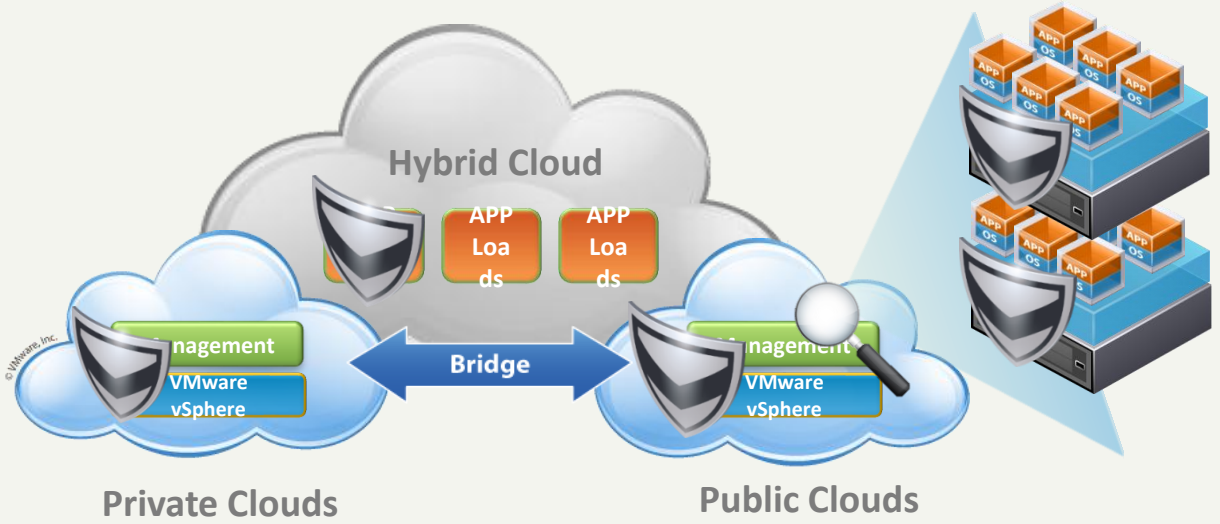


Neusoft

3 云计算、大数据综合防护解决方案

3.1 前端安全：边界&应用恶意代码防护

面向云计算的虚拟化下一代防火墙



NISG-A

vmware READY

CITRIX ready

openstack

amazon web services

阿里云 aliyun.com

虚拟化与物理环境的混合部署

对于该系统虚拟化后带来的网络变化及其网络安全挑戒，目前在业界存在两个方向上的解决方案

NISG-A

虚拟化防火墙

- 在服务器内增加软件防火墙/AV/IPS虚拟机
- 提供物理世界中的防火墙相同的功能

物理防火墙

- 强制将虚拟机的流量转发到外部
- 通过物理安全设备的检查后，再转发回该物理服务器

	虚拟化防火墙	物理防火墙
性能	能够随着资源的动态分配而调节性能	受硬件固定配置限制，有确定的性能上限
可扩展性	能够按需弹性伸缩	靠硬件扩容或升级，扩展性和及时性差
通用性	依赖虚拟化平台	无依赖
可靠性	防火墙本身是虚拟机，由虚拟化平台保证可靠性	需要考虑硬件的灾备和故障等可靠性问题
资源占用	占用主机部分资源	不占用主机资源

安全联动和集中管理

SMC SecurityManagement Center

安全管理平台

- 设备集中管理
- 全网日志集中审计
- 规则库统一更新
- 策略集中下发
- 统一备份和恢复
- 全网流量实时监控

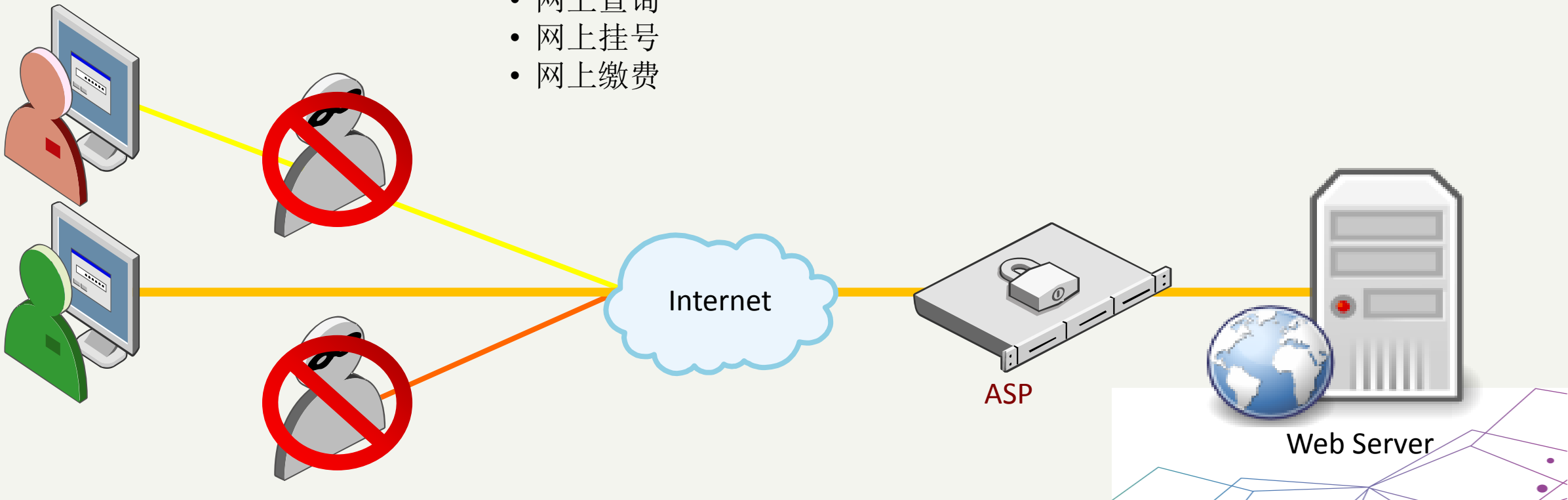
应用恶意代码防护——基于网页的应用

- 保护基于网页（HTTP，HTML5，JS）应用:

自动化攻击，SQL / 指令注入，跨站脚本，跨站请求伪造，各种中间人攻击，撞库，权限提升，恶意插件，应用层DDoS，等

应用场景:

- 网上查询
- 网上挂号
- 网上缴费



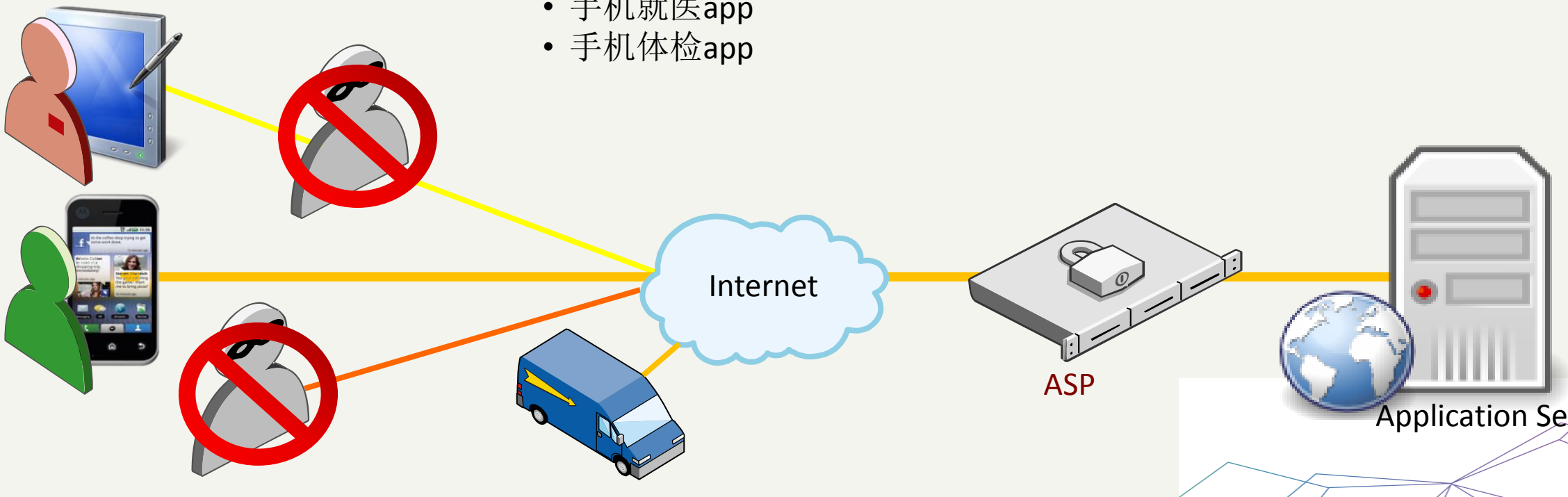
应用恶意代码防护——基于手机的应用

- 保护基于移动的应用:

自动化攻击，各种中间人攻击，账户假冒，权限提升，逆向工程，应用层DDoS，木马，数据泄漏，应用假冒或替换，等

应用场景:

- 手机挂号app
- 手机就医app
- 手机体检app



核心技术：动态加密&一次性令牌

之前

```
POST /bank/login.aspx HTTP/1.1
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9;
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Language: zh-tw,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://demo.testfire.net/bank/login.aspx
Cookie: ASP.NET_SessionId=4fk4bi55kbg0pl34rjpjh23h; amSe
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 38

uid=admin&passw=123456&btnSubmit=Login
```

一次性令牌

之后

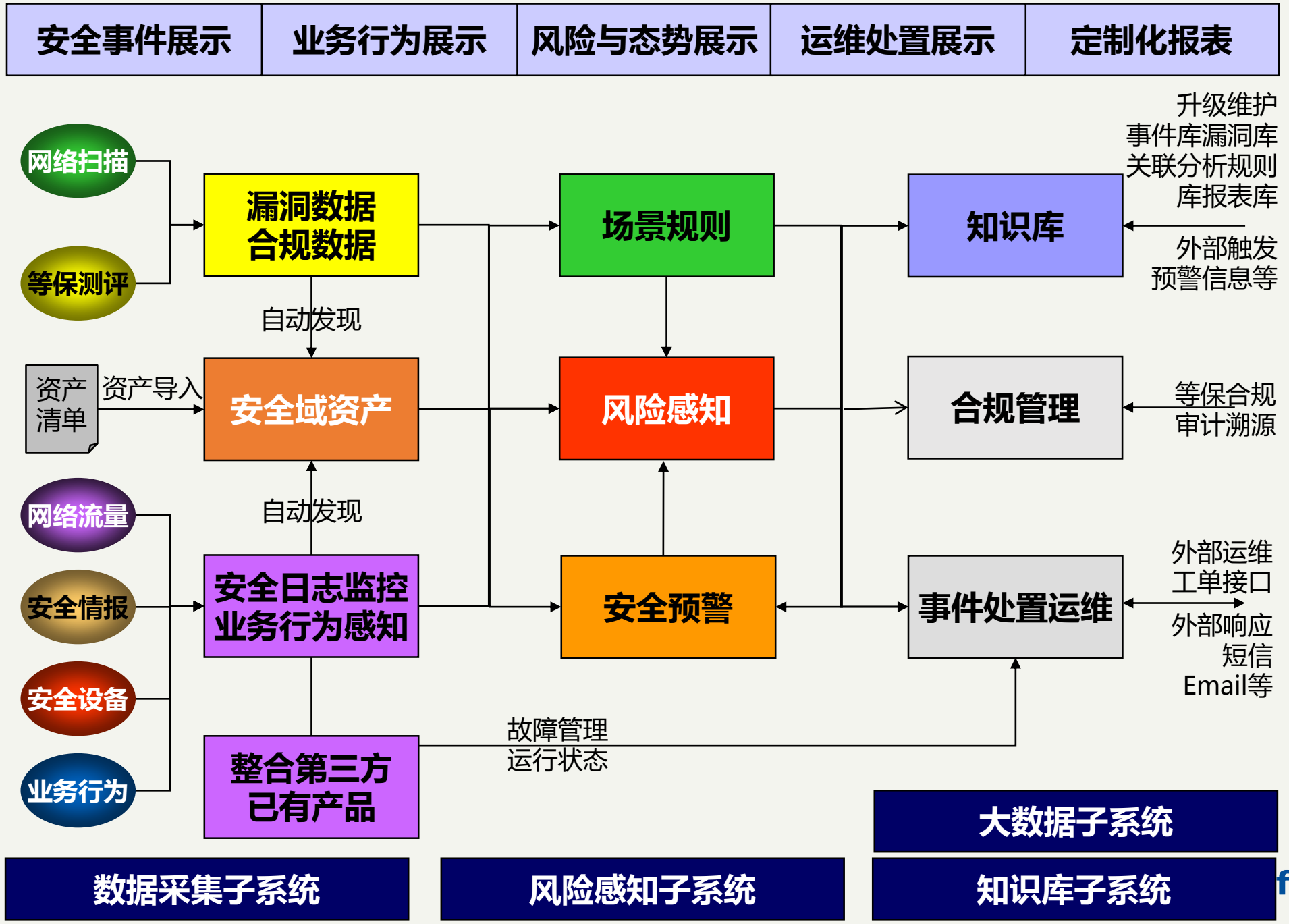
```
POST /bank/login.aspx?y7bRbP=k~RV24ZKg4vfeNwEAjUkm1J-5tq
Host: txdemo.blueangles.info
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9;
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Language: zh-tw,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://txdemo.blueangles.info/bank/login.aspx?y
Cookie: csrftoken=jAJQWho5MZe93i4gDNuznRSCxWdDZO3q; sess
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 139

c1K5tw0w6_=WA3Ax0XAIIkU6-ZQ0GpHYSoE0qs_DBg-KR5TPJ7AX_n6u
```

动态加密

3 云计算、大数据综合防护解决方案

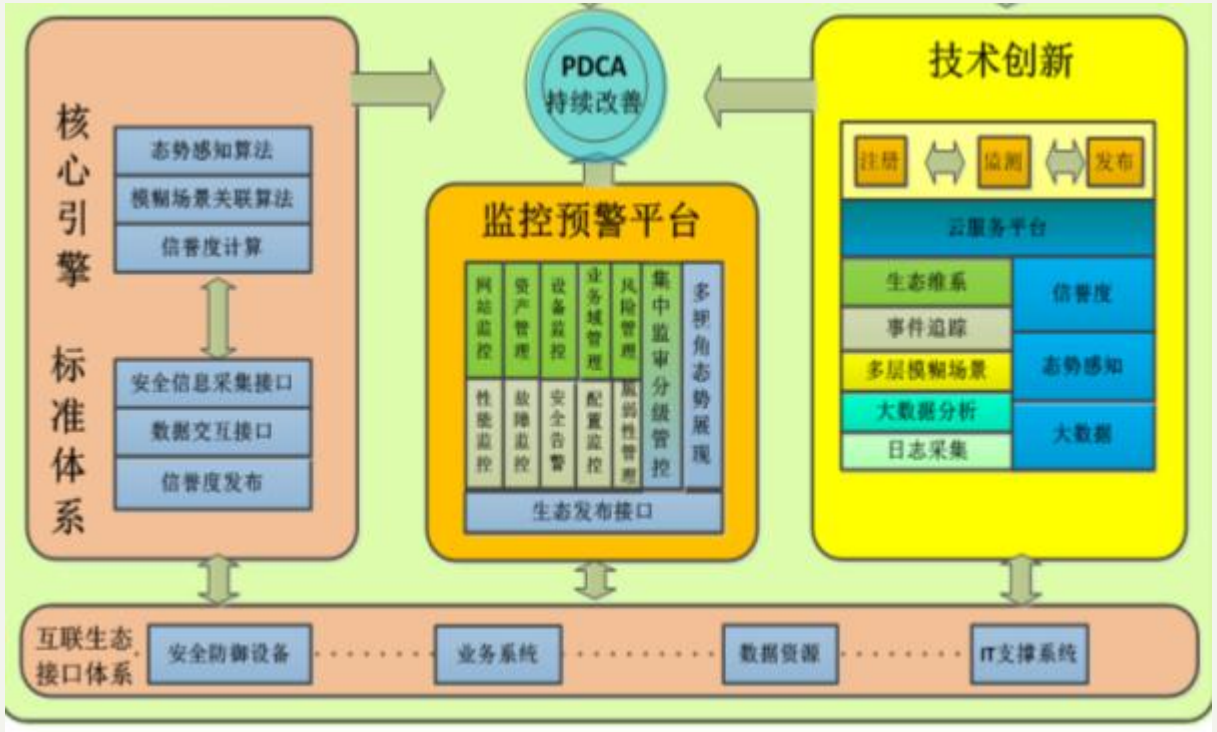
3.2 中间安全：综合安全审计&分析

综合安全审计&分析平台架构



构建自下而上构建开放的安全防御生态

- 基于虚拟化和多源数据结构支撑，底层数据采集和顶层业务管理支持双向互联接口和SaaS云服务管理模式。通过模糊关联场景的风险感知算法将平台内部打通。



1. 传统的企业化管理和SaaS模式结合的安全服务；

2. 系统框架支撑
   - 系统功能完善可以支撑云服务模式和大数据的分析预警处置；

3. 模糊关联场景的态势感知
   - 实现模糊多层关联分析算法，结合基线学习与神经感知；

4. 虚拟化与大数据平台支撑
   - 提供海量日志数据高效分析的支撑平台，采集引擎升级为分布式计算引擎；

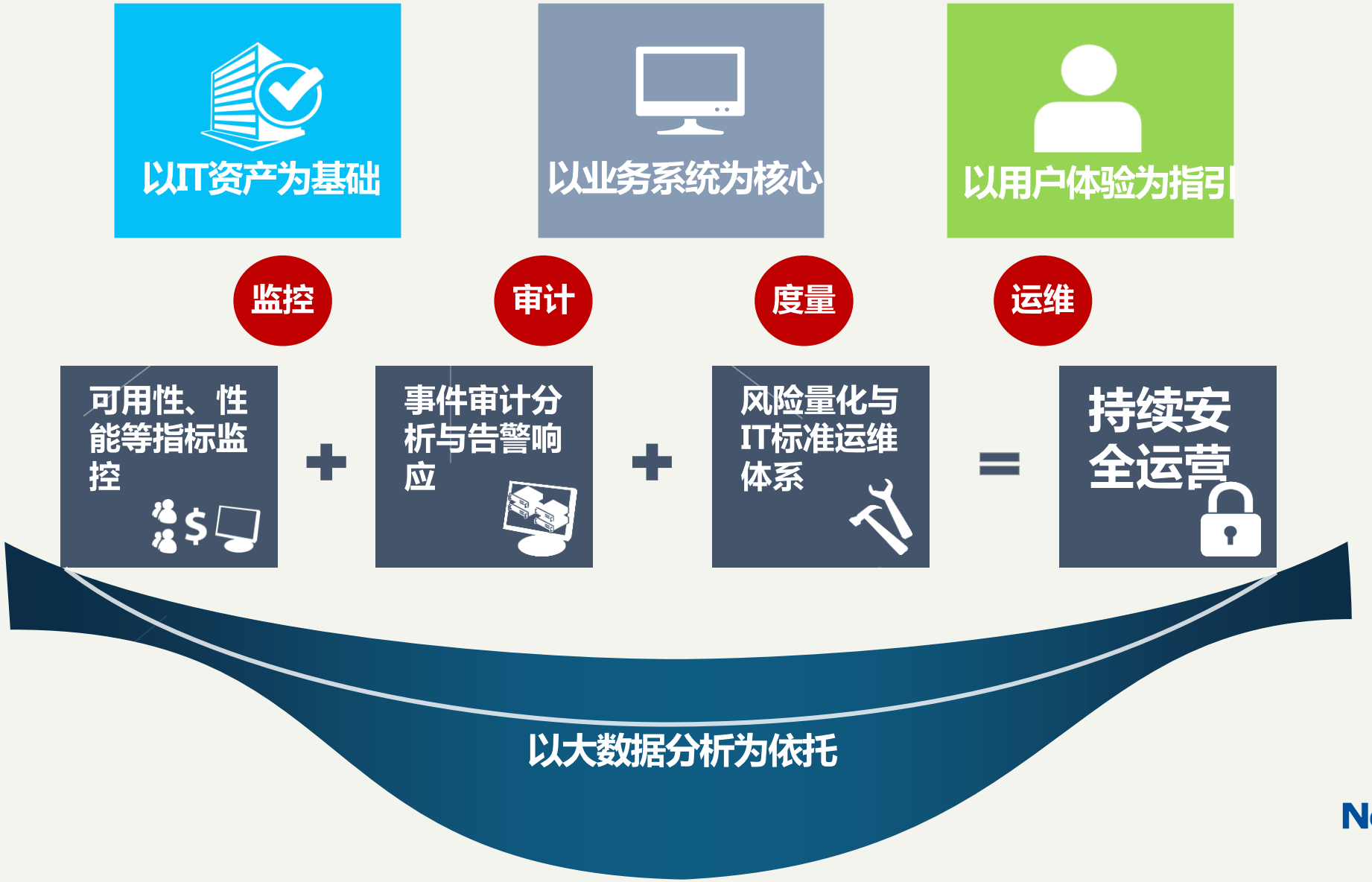
5. 支持与防御设备开放互联
   - 提供开放的双向管理接口，构建防御生态信息共享。

Neusoft

基于大数据分析的系统架构

Neusoft

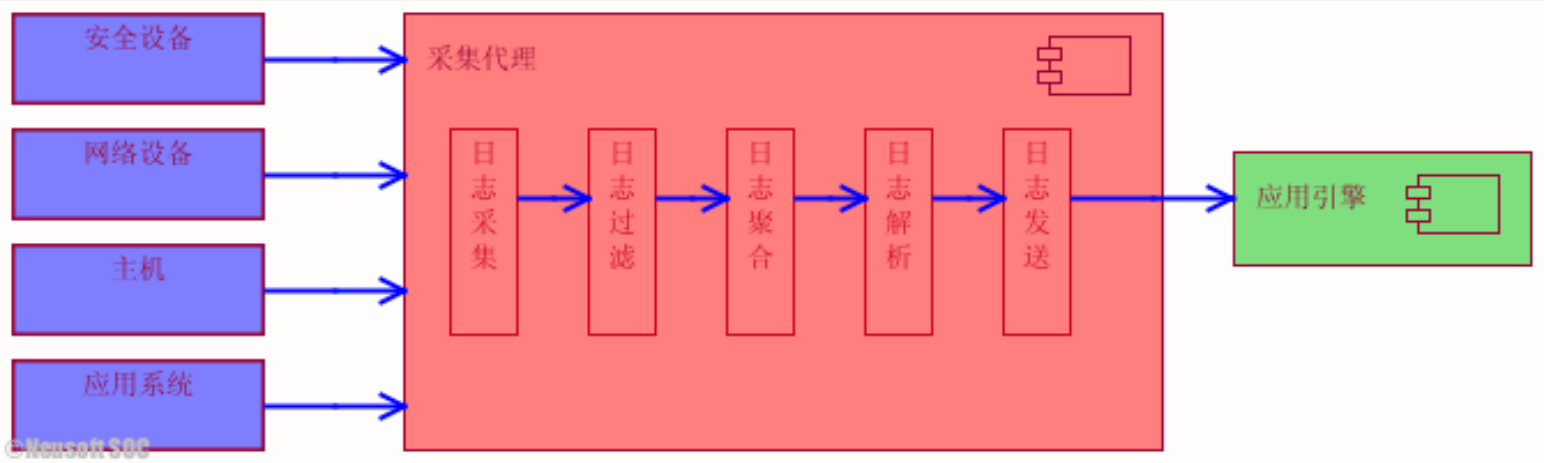
大数据综合安全分析平台

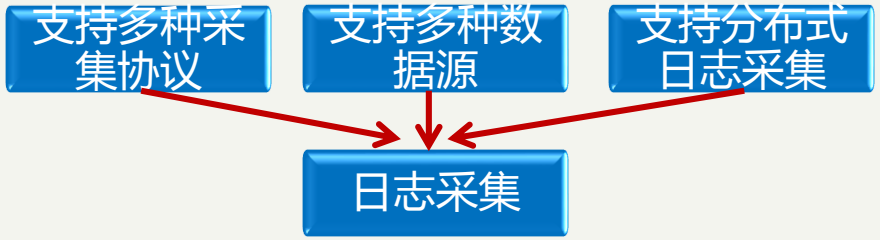


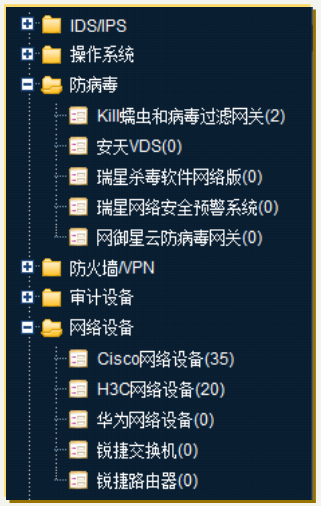
Neusoft

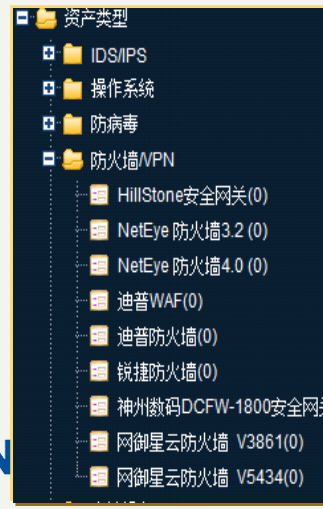
以大数据分析为依托——海量日志采集

日志采集主要完成各类安全日志收集，收集后的日志分别经过日志过滤、日志聚合、日志解析，最终将日志发送给上层的应用引擎进行处理。

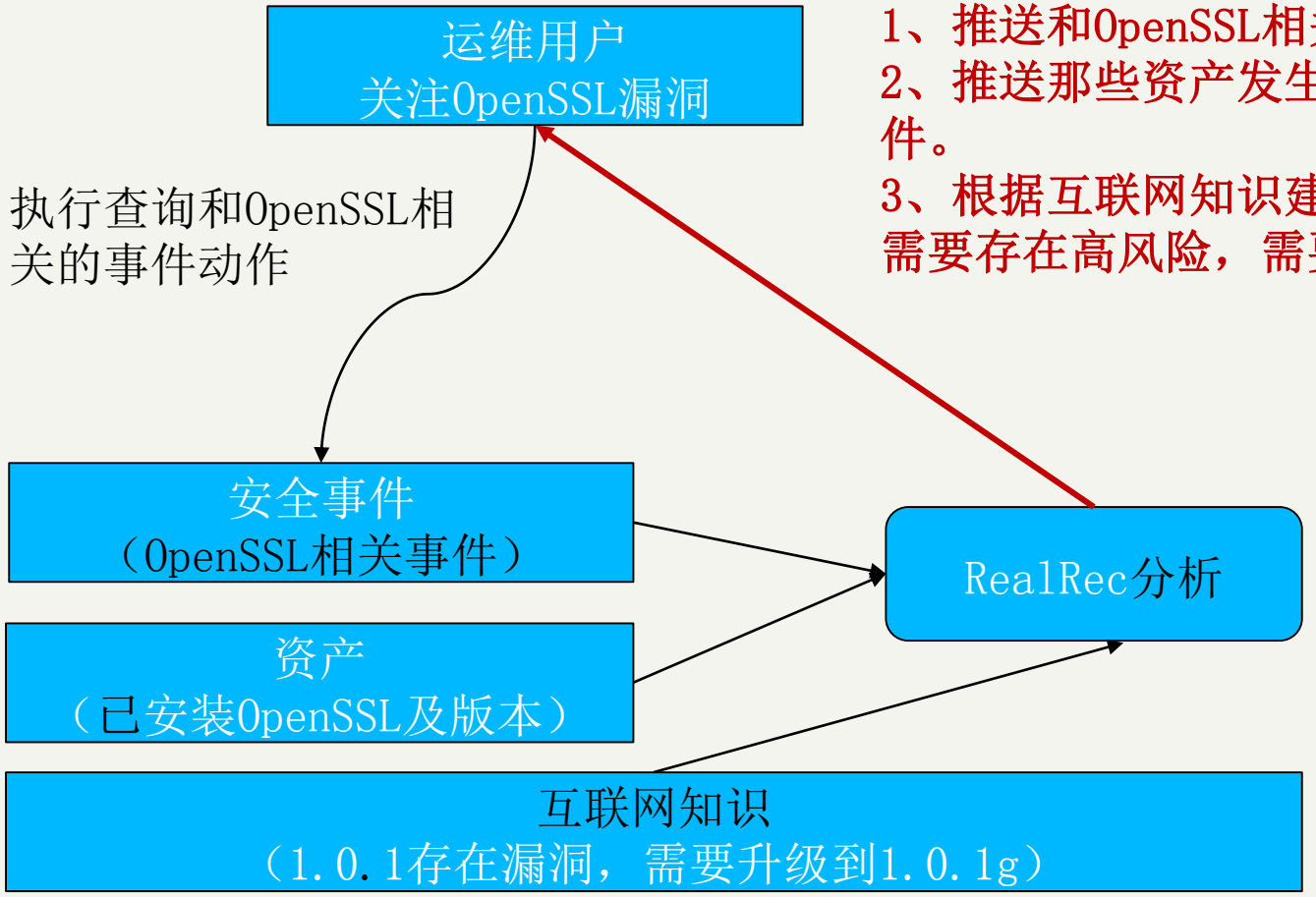








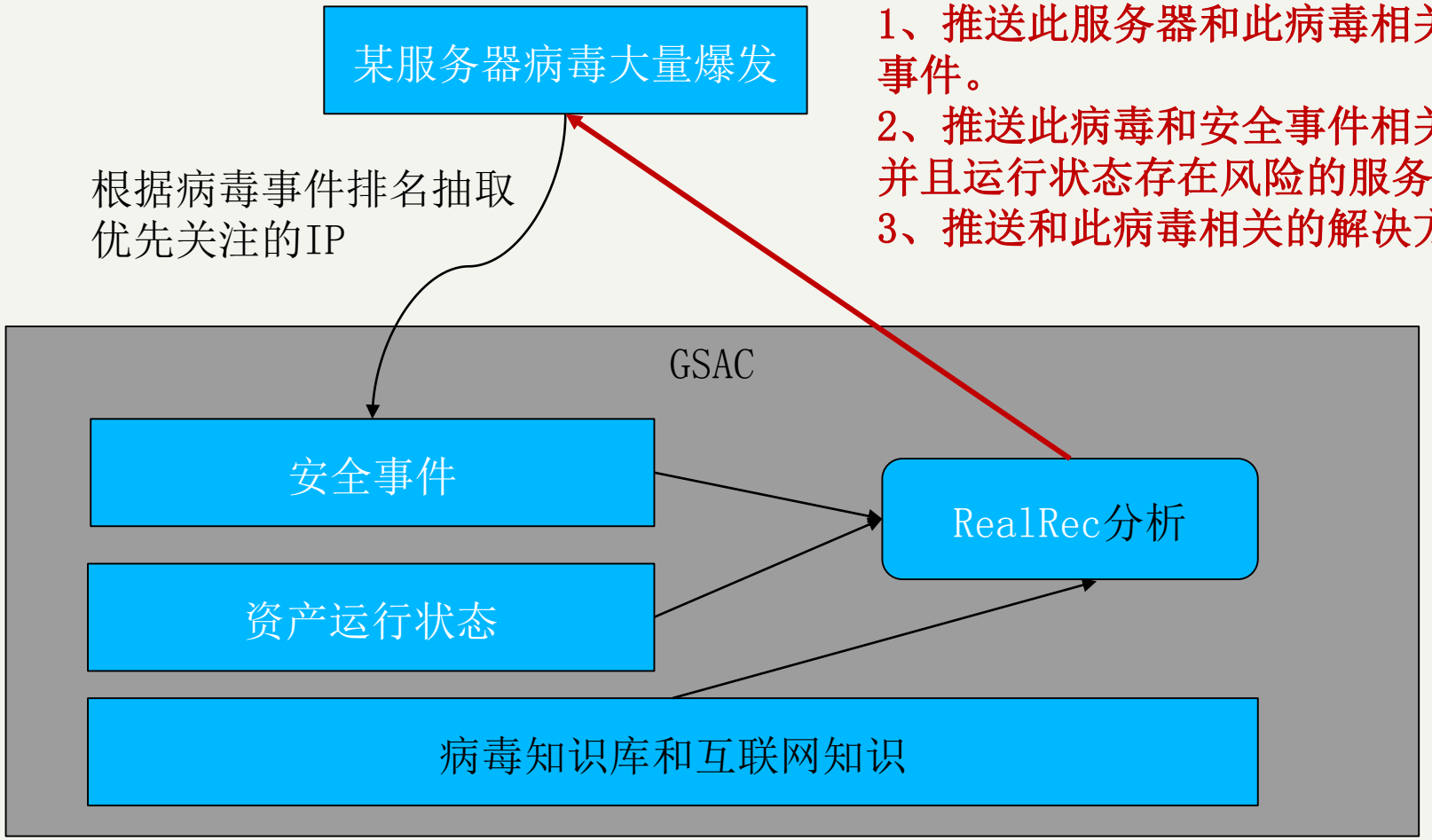
大数据分析举例——
根据运维用户使用进行个性化智能关联分析推荐



1、推送和OpenSSL相关的高频事件。
2、推送那些资产发生了OpenSSL事件。
3、根据互联网知识建议那些资产需要存在高风险，需要打补丁。

Neusoft

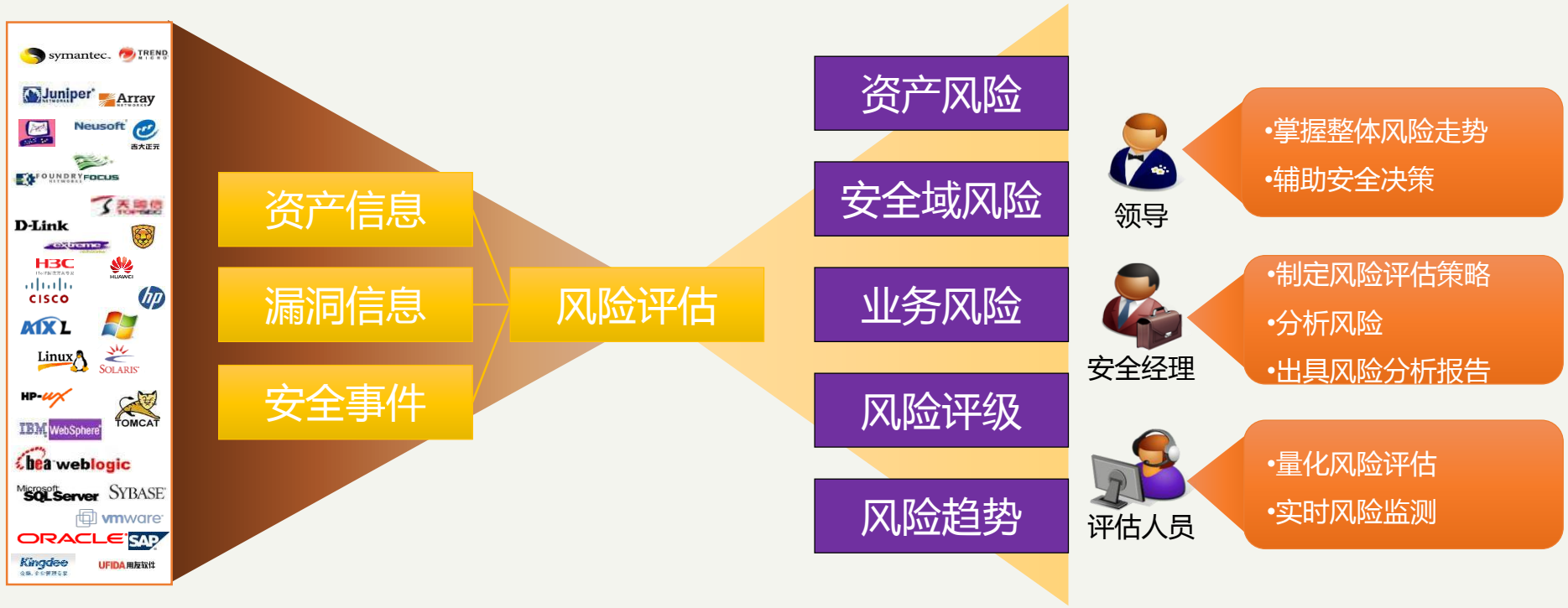
大数据分析举例——
根据漏洞、阈值指标、病毒等进行智能关联分析推荐



1、推送此服务器和此病毒相关的事件。
2、推送此病毒和安全事件相关的，并且运行状态存在风险的服务器。
3、推送和此病毒相关的解决方案。

Neusoft

大数据分析——安全风险评估



Neusoft

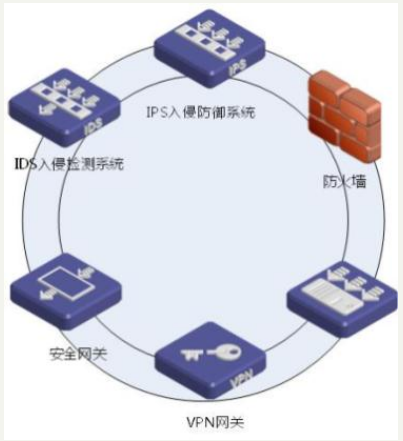
大数据分析——风险展示

- 整体告警统计分析
- 安全事件
- 故障事件
- 性能事件
- 脆弱性事件
- 基线检查事件
- 配置事件
- 原始日志统计

Neusoft

基于云的SaaS服务—云安全检测

检测系统是一站式全新的SaaS服务模式，能够为客户的**网站、服务器及网络安全设备**提供的在线安全监测服务。



网络安全设备及服务

安全运维管理中心

行业及互联网用户

Neusoft

基于云的SaaS服务--云安全检测

实时在线服务与客户互动，及时的告警信息让客户随时掌握您网站、服务器以及安全设备的运行情况。

门户网站　　数据中心

多种服务配合，全面服务于大型网络用户及互联网用户，现场应急响应让服务更贴心。

云平台 ＋ **服务**

管理员通过智能终端随时查看企业WEB及应用系统安全状况

Neusoft

3 云计算、大数据综合防护解决方案

3.3 后端安全：数据防泄漏

数据泄露问题分析

- 来自外部的病毒、木马、网络攻击等种种网络安全威胁。
- 来自内部有意或无意的数据泄露

- 机构的安全、公信力、财产、隐私、声誉等方面都会遭受到严重的威胁。

- e-mail、IM软件、WEB、云环境存储、物理介质

Neusoft

解决办法

解决办法：

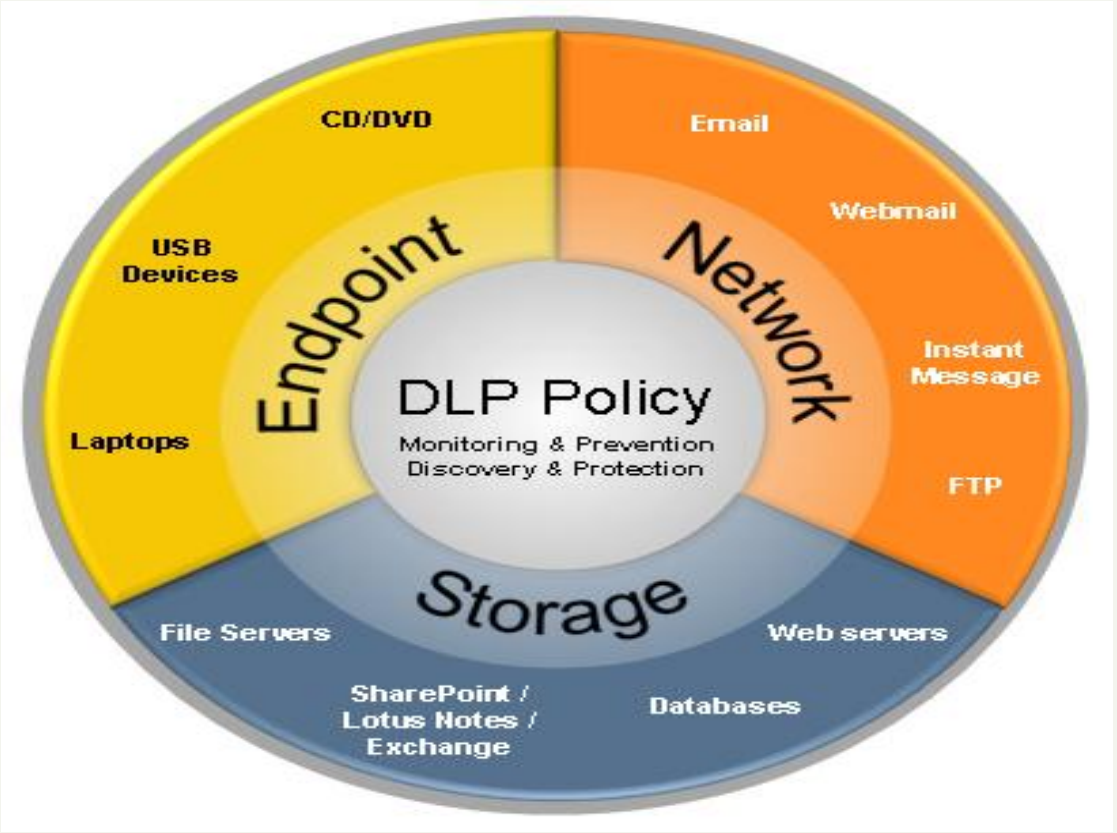
全面的多层次防护

- IT基础架构安全防护
- 数据防泄密
- 信息安全管理流程化

数据的生命周期：

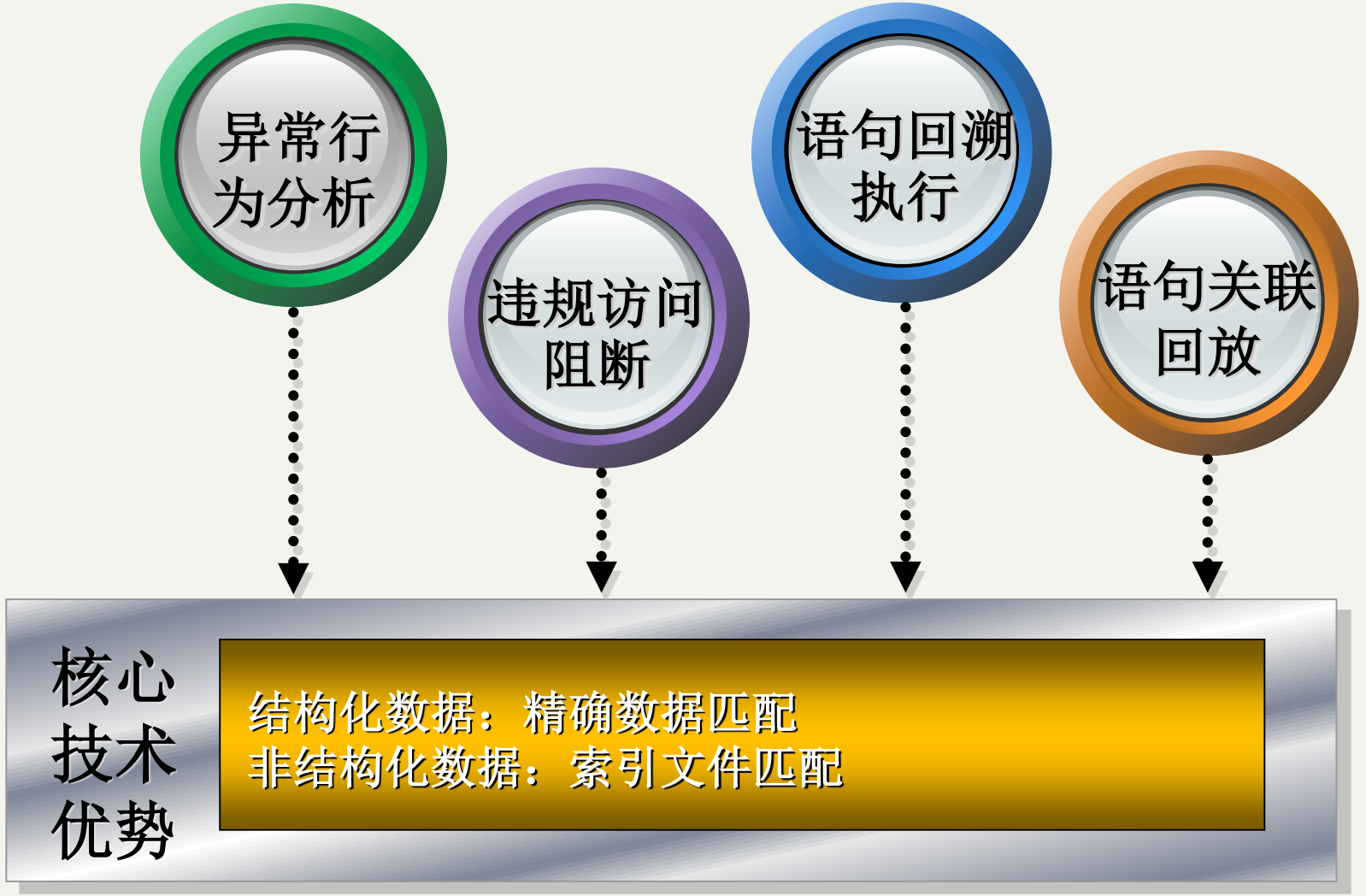
- 存储（服务器）
- 使用（终端）
- 传输（网络）

为机密数据的存储和使用或是传输提供保护



Neusoft

核心技术



Neusoft


THANKS
Neusoft
Beyond Technology