新型安全风险下的数据保护

Websense中国区技术总监
冯文豪

ISC 2014
中国互联网安全大会
360互联网安全中心

内容

websense

- 企业面临的数据安全问题
- 剖析高级安全威胁 --- APT
- 如何有效实现数据泄露防护

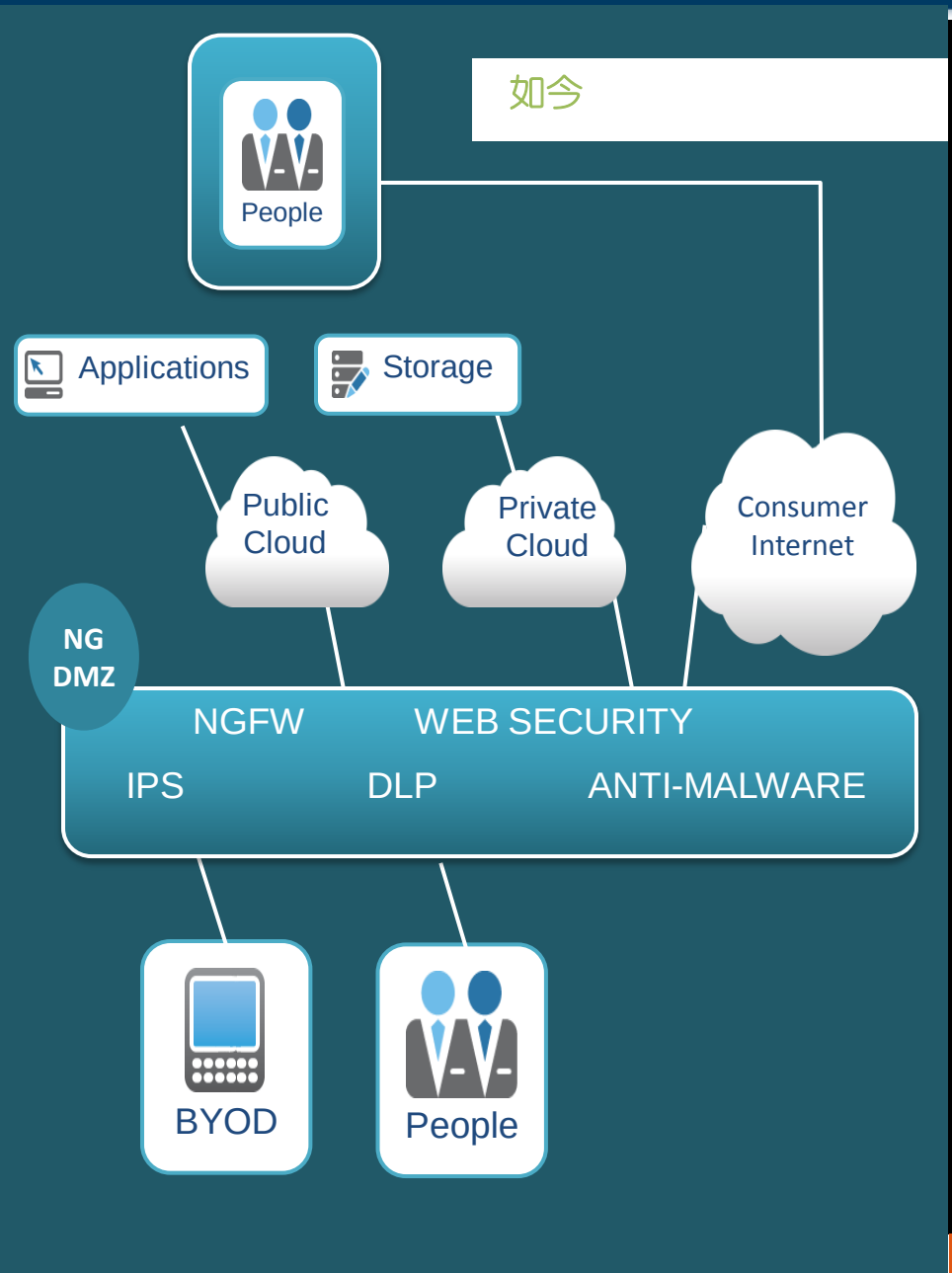
ISC 2014 中国互联网安全大会

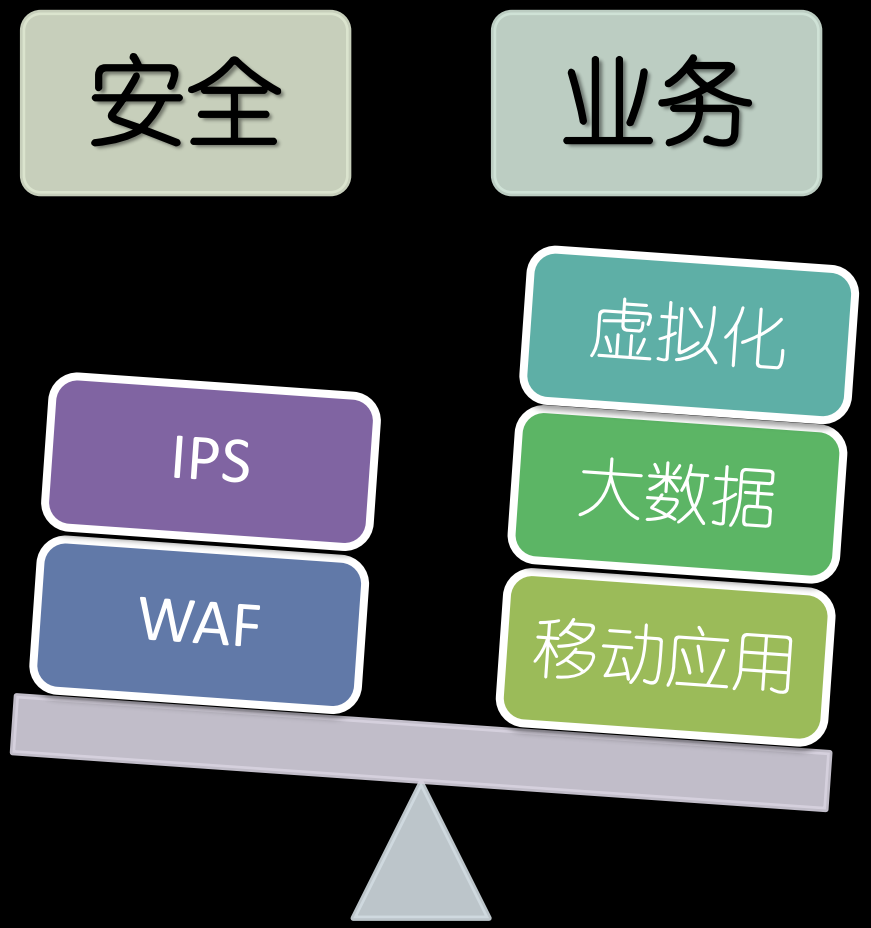
360互联网安全中心

金融行业面临的数据安全问题

业务模式的改变导致IT架构的变革

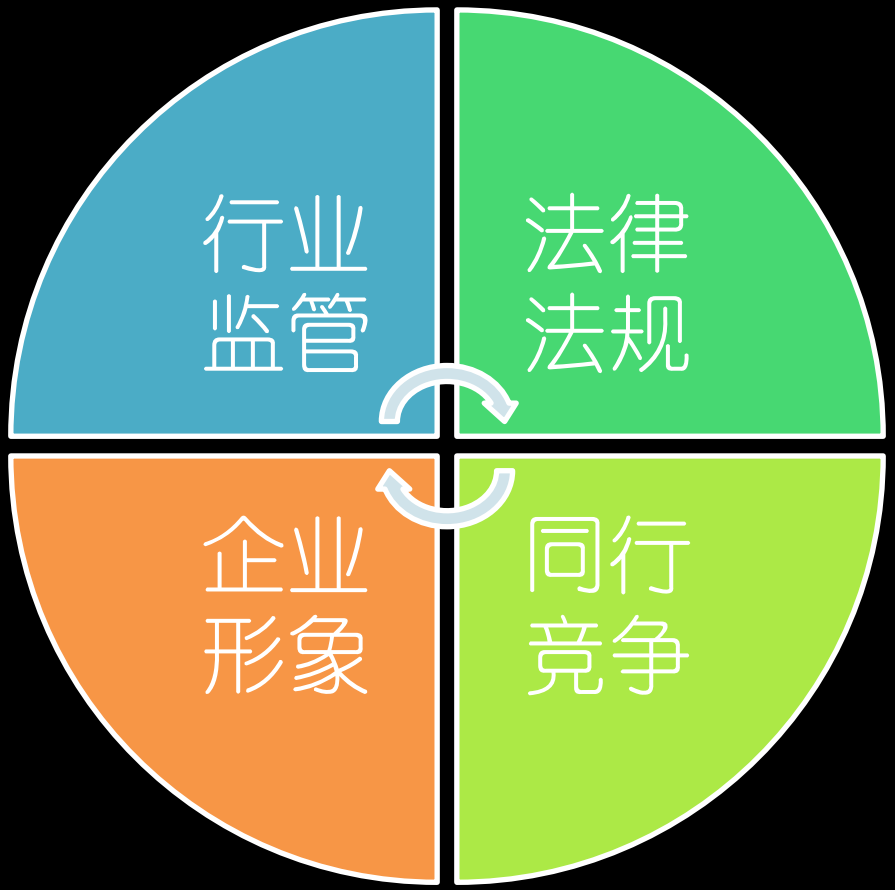
websense





不同行业面临来自各方面的压力

websense



ISC 2014 中国互联网安全大会

360互联网安全中心

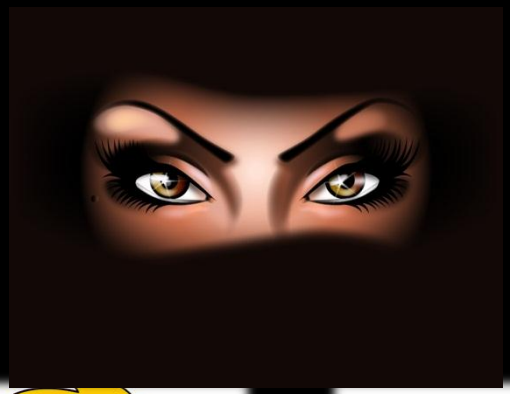
这些数据我们都保护到了吗？

websense

行业类别	涉及敏感数据	个人信息	知识产权
高科技制造业	专利文件、源代码、设计图纸、开发设计文档…		✓
金融服务	信用卡资料、客户身份信息、交易记录、合同文件…	✓	
政府单位	机密等级公文、人事档案、户籍资料、个人财产信息…	✓	
教育、医疗与服务	学籍信息、病患身份、病例、就医记录等、信用卡号码…	✓	
制药行业	研发计划、市场行销计划、配方、实验数据等…		✓
上市公司	未公布之财报、并购计划、重大信息、重大合约等…		✓

这些事件我们究竟发现了多少？

websense



偶发事件

有意泄露

内部恶意软件

恶意窃取

ISC 2014 中国互联网安全大会

360互联网安全中心

剖析高级安全威胁---APT

APT 威胁七部曲

websense

侦查

Recon

诱饵

Lure

重定向

Redirect

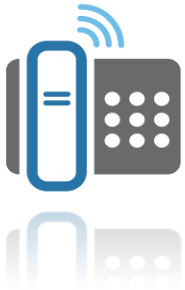
漏洞分析工具箱

Exploit Kit

播种

Dropper File

运程命令和控制



Call Home

窃取资料

Data Theft

攻击流程….

ISC 2014 中国互联网安全大会

360互联网安全中心

威胁七部曲

websense

侦查

Recon

诱饵

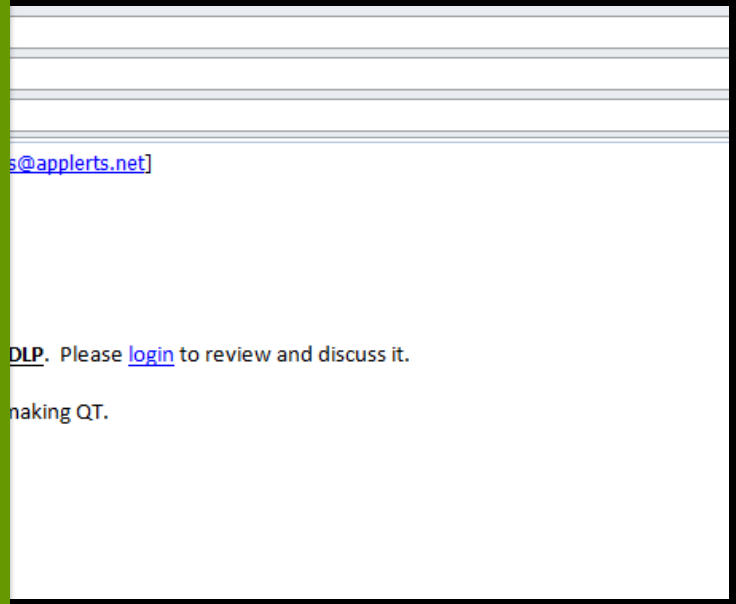
Lure

- Social Engineering
- 搜索引擎
- 丢在路边的U盘
- 鱼叉式/钓鱼
- …

客户需要的是:

- 用户意识
- 覆盖网页和邮件的保护
- 社交网络，微博控制
- 鱼叉式钓鱼攻击防护
- 信任认证
- 动态分析

当黑客使用你的名字登录，他的权限就是你的权限

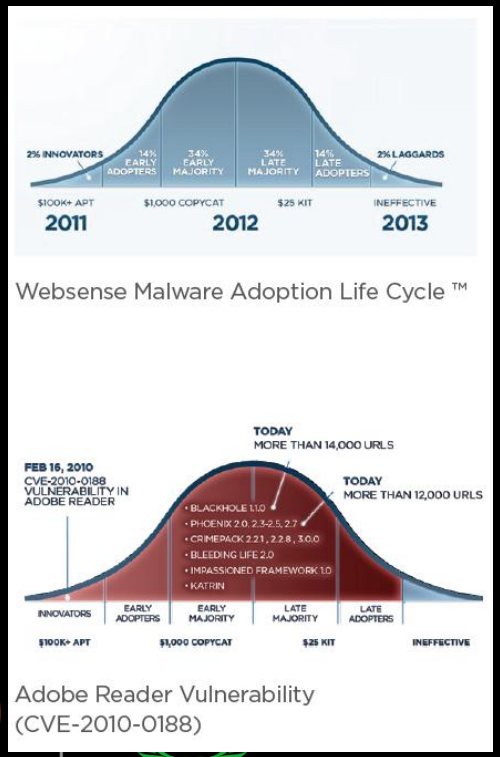


威胁七部曲

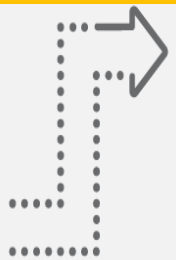
websense

单使用特征防卫导致效率低下的原因

- 形态特征多种多样
- 专用加密



重定向



Redirect

漏洞分析工具箱

Exploit Kit

客户需要的是：实时分析

- 浏览器编码和活动脚本
- 连接分析
- 漏洞分析
- 综合评估
- 预测级分析

威胁七部曲

websense

客户需要的是:
在线防卫

- 应用分析
- 恶意 PDF 文档
- 多重防病毒扫瞄
- 压缩档案处理
- 动态 DNS
- 僵尸网和运程命令和控制服务器通信

单使用特征防卫
- 动态播种包封

单使用网址过滤
- 缺乏对外发资

播种

Dropper File

运程命令和控制服务器通信

Call Home

威胁七部曲

websense

客户需要的是:

- 窃取资料防卫
- 内嵌式 DLP
- 资料抓取
- 地域控制
- 法证和报表
- 告警和工作流

窃取资料

Data Theft

使用传统UTM/DLP导致防卫效率低下的原因

- 欠缺针对高级资料泄漏技巧的防卫技术
- 缺乏完善和快速的通报机制
- 缺乏收集证据功能

当前防御技术四大失败理由

websense

1 单靠特征码和信誉

History is not a reliable indicator of future behavior.

Signature creation cannot keep up with the dynamic creation of threats

2 缺乏实时在线内容分析

Collect samples for lab analysis using background processes

Producing new signatures (network/file) and reputations (URL/file)

3 只检查请求，缺乏对外发资料的保护

Not data-aware, lack contextual analysis, minimal to no forensic visibility

4 忽略SSL死角

UTMs, NGFWs, IDSs, Network Threat Monitors

SSL severely impacts performance, or blind to it

ISC 2014 中国互联网安全大会

360互联网安全中心

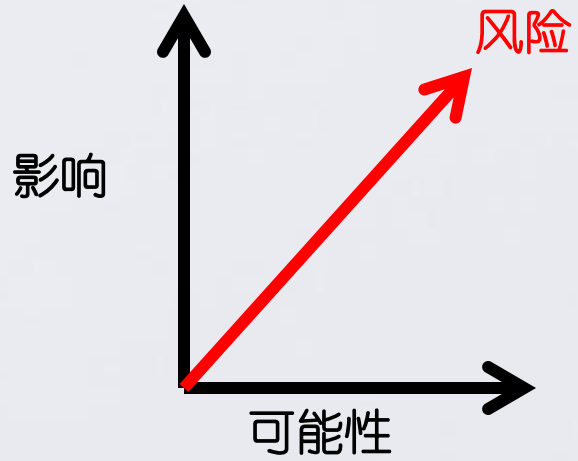
如何有效实现数据泄露防护

以风险为导向找到亟需解决的问题

websense

风险 = （影响 x % 可能性）

- 指导原则
  - 决定资产
  - 衡量影响
  - 确认相应威胁
  - *影响无法改变*
  - *关注降低可能性*
    - *降低发生率*
    - *缩短实现价值的时间*

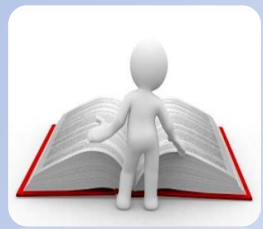


数据防泄漏项目需要覆盖：组织、制度、技术

websense

组织保障

- 自上而下梳理并定义管理层、业务部门、实施部门、合规监控及审计部门等的相关职责；
- 从组织上推动数据防泄漏管控的实施。



制度保障

- 建立或完善数据防泄漏总体策略、数据防泄漏管理办法、数据防泄漏明细策略（面向数据）及具体的操作流程；
- 从制度体系上支撑数据防泄漏工作

技术保障

- 采用成熟、专业的数据库防泄漏技术平台，落实管理层认可的详细策略，通过平台实现数据外泄行为的记录、告警及阻断；
- 从技术上实现数据防泄漏目标

形成体系化的、可持续优化的数据防泄漏管理机制

数据防泄漏整体解决方案 – 组织保障

websense

组织保障

- 自上而下梳理并定义管理层、业务部门、实施部门、合规监控及审计部门等的相关职责；
- 从组织上推动数据防泄漏管控的实施。

实施团队

信息安全管理岗

- 在总部，分支公司逐步设立
- 承担基本的违规事件检查、放行、报告、联系人职能

信息科技部

- 工程实施的项目管理牵头
- DLP 系统运维
- 提供技术支持培训
- 提供相应监控分析和违规报告

数据保密相关部门

- 组织细化策略制定
- 向各部室提出具体的工作要求

风险合规部门

- 对防泄漏工作落实后的数据安全情况进行评估

内审部门

- 负责检查评价各部门在各项信息安全管理过程中的进展情况

数据防泄漏整体解决方案 - 制度保障

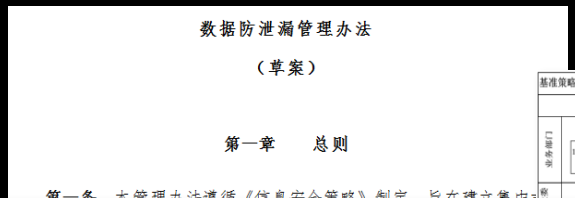
websense

制度保障

- 建立或完善数据防泄漏总体策略、数据防泄漏管理办法、数据防泄漏明细策略（面向数据）及具体的操作流程；
- 从制度体系上支撑数据防泄漏工作

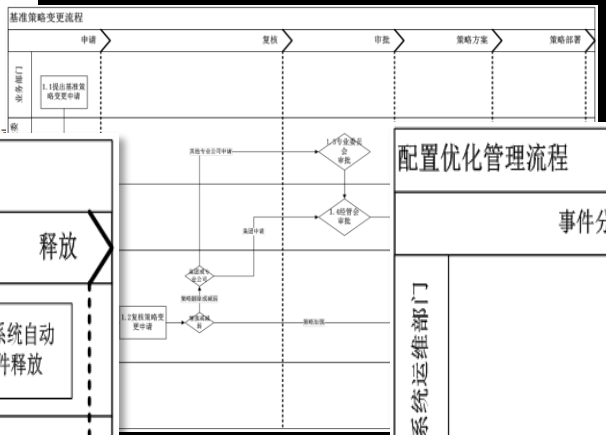
为支撑数据防泄漏管理机制，应建立结构化的制度体系，应包括：

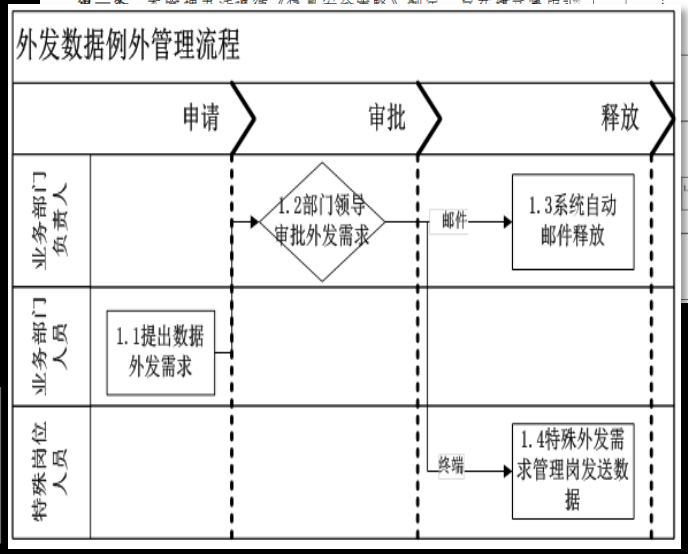
- 管理层确定的数据防泄漏**总体策略**；
- 数据防泄漏**管理办法**：明确管理目标并定义人员职责；
- 数据防泄漏相关的**操作流程**：可包括策略变更管理流程、例外策略管理流程及配置优化管理流程等。

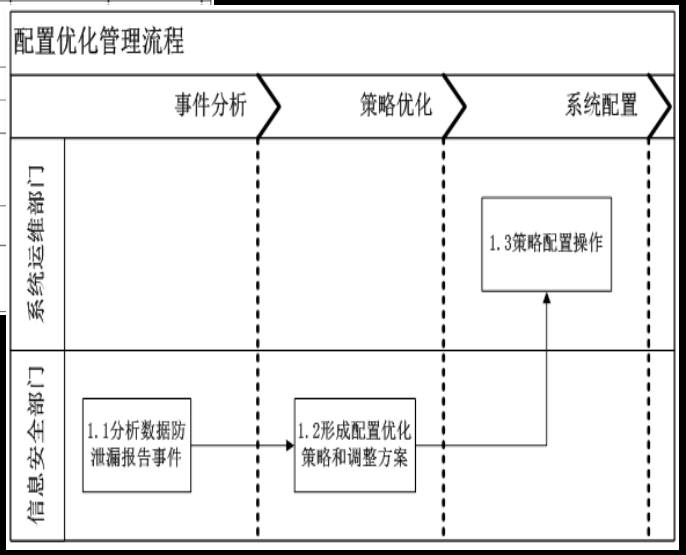

数据防泄漏管理办法

（草案）

第一章　总则







ISC 2014 中国互联网安全大会

数据防泄漏整体解决方案 - 技术保障

websense

识别

- PII
- 银联卡号
- PCI-DSS
- SOX
- 客户数据
- 员工资料
- 敏感文件

监控

- 网络
  - SMTP, HTTP, FTP
- 终端
  - Email, Web, USB, 应用程序, 打印
- 存储
  - 数据库, 邮件, 文件共, Sharepoint平台

保护

- 阻挡
- 隔离
- 加密
- 隔离 并加密
- 通知告警
- 确认并辩护
- 补救与整治

ISC 2014 中国互联网安全大会

360互联网安全中心

数据防泄漏项目经验借鉴

websense

部门之间的协作和高层领导的认同

- 定期生成数据泄漏统计分析报告和汇报制度，获得高层领导对执行策略的认同和支持
- 单一部门无法牵头协调信息泄露防护的各项管理工作

从最重要的数据保护开始

- 策略不贪多求全，先从最重要的客户数据保护开始
- 先从1-2个部门开始
- 初始阶段，优先选取3-5条监控策略，了解数据泄密的整体情况

注重控制误报率

- 不断的调整策略精准度，减少误报和事件处理工作量
- 提供给相关部门和员工充分且有价值的信息，提升项目价值

谢谢！

lfeng@websense.com