SecGator

数据治理与数据安全

演讲主题

- 数据安全与数据防泄漏的关系
- 企业数据治理为何需要数据防泄漏……

- 数据防泄漏项目需要涵盖的三个方面

- DLP数据防泄漏项目成功案例

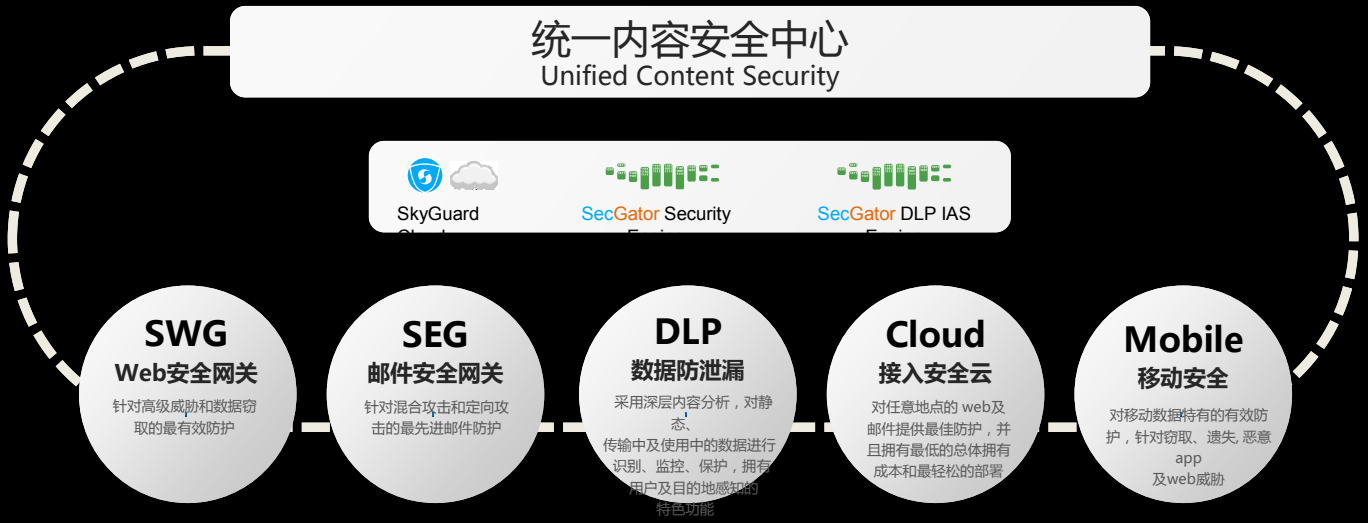
- 数据防泄漏项目成功要素
- 下一代技术

黑客窃取Verizon公司用户资料后在线出售

据 KrebsOnSecurity报道称，Verizon公司客户数据在地下网络市场被人出售。

但自己尚不知道。

传统的技术必须升级到能够智能感知内容的新信息安全技术！



DLP产品为何如此重要？

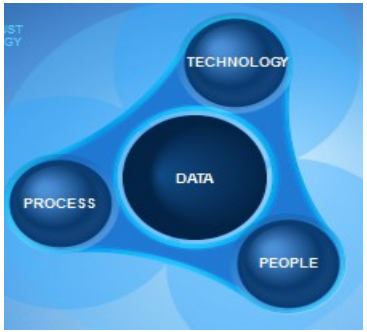
1 DLP是APT 攻击最后一道防线

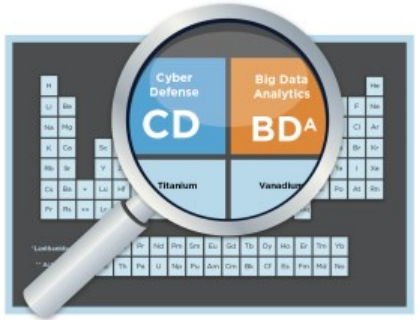
2 内部信息泄漏的最后一道防线

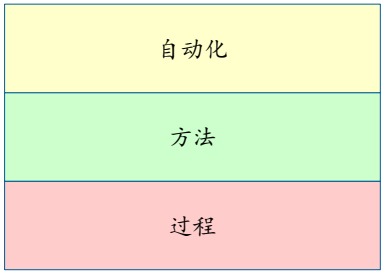
概述

对于企业信息安全，若想得到结构性的保障就需要有一个系统性信息安全支撑体系。无论这个体系采用什么样的参考框架，都需要考虑四个关键的构成要素，即人员People过程Process 、、技术Technology和数据Data （PPTD），其中：

- 人员是过程执行的资源；
- 过程是组织的系统性能力；
- 技术是过程有效性的支撑；
- 数据是过程执行的驱动。

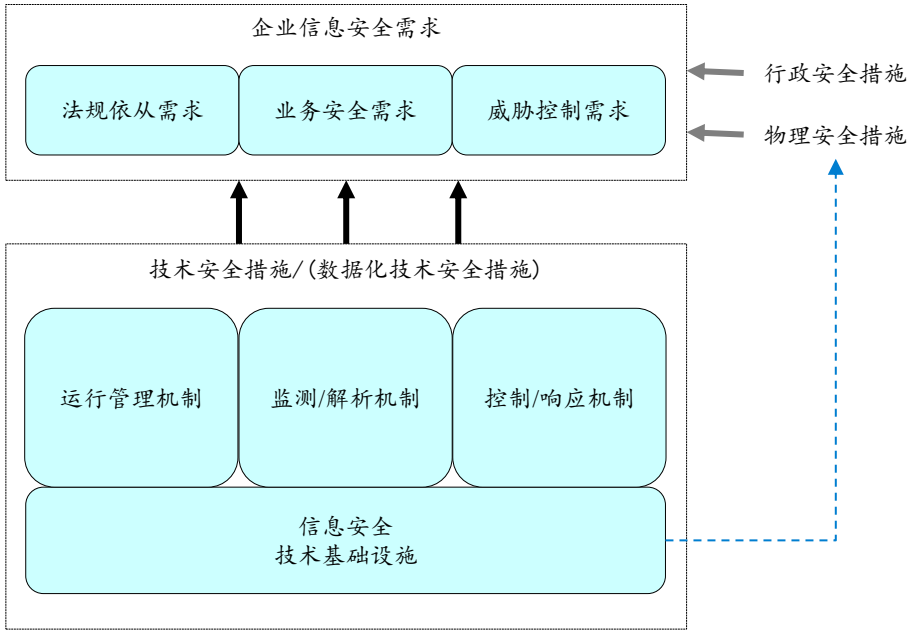






技术：企业信息安全技术控制框架

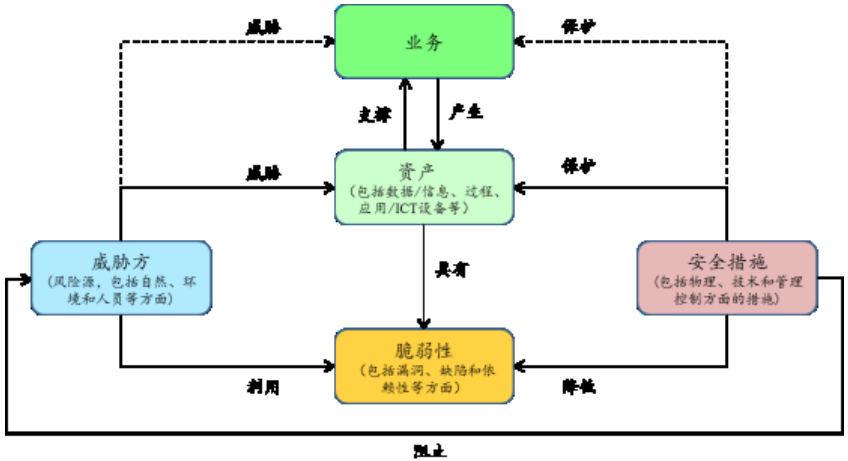
技术安全措施是满足企业信息安全需求的三类安全措施之一，也是其中最重要、最复杂的，因此需要通过架构的设计来保证技术控制之间的协同以及与其它安全控制的协同。



技术：有效性评估策略

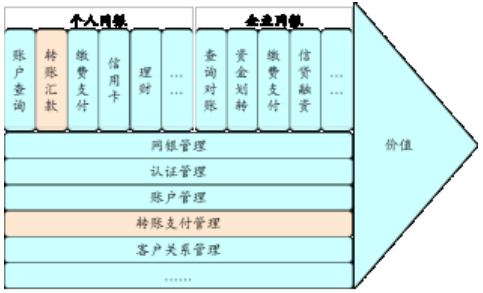
风险的核心是围绕着业务支撑或业务产生的资产，并取决于资产自身的脆弱性和已采取的安全措施，因此安全技术有效性评估策略包括：

- 面向业务/业务资产的有效性评估
- 面向威胁方的有效性评估
- 面向脆弱性的有效性评估
- 综合加权的有效性评估

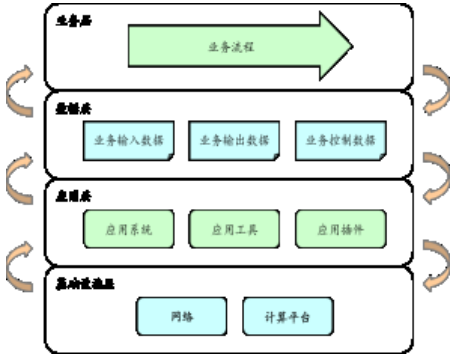


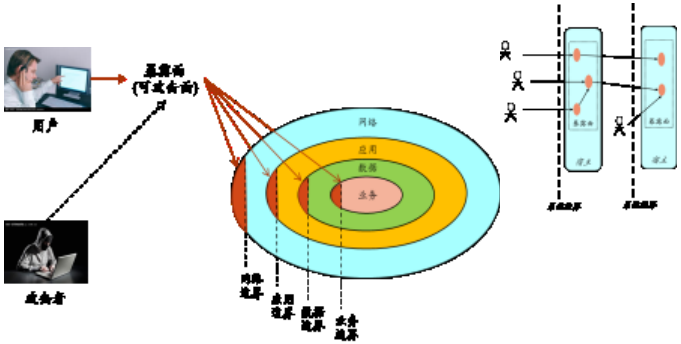
技术：面向有效性的规划与设计

基于价值链的范围确定

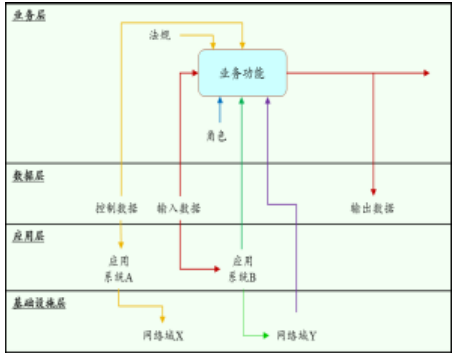


基于EA的安全需求分析





面向攻击语境的威胁评估



企业为何需要数据防泄漏…

企业面临数据安全风险的压力

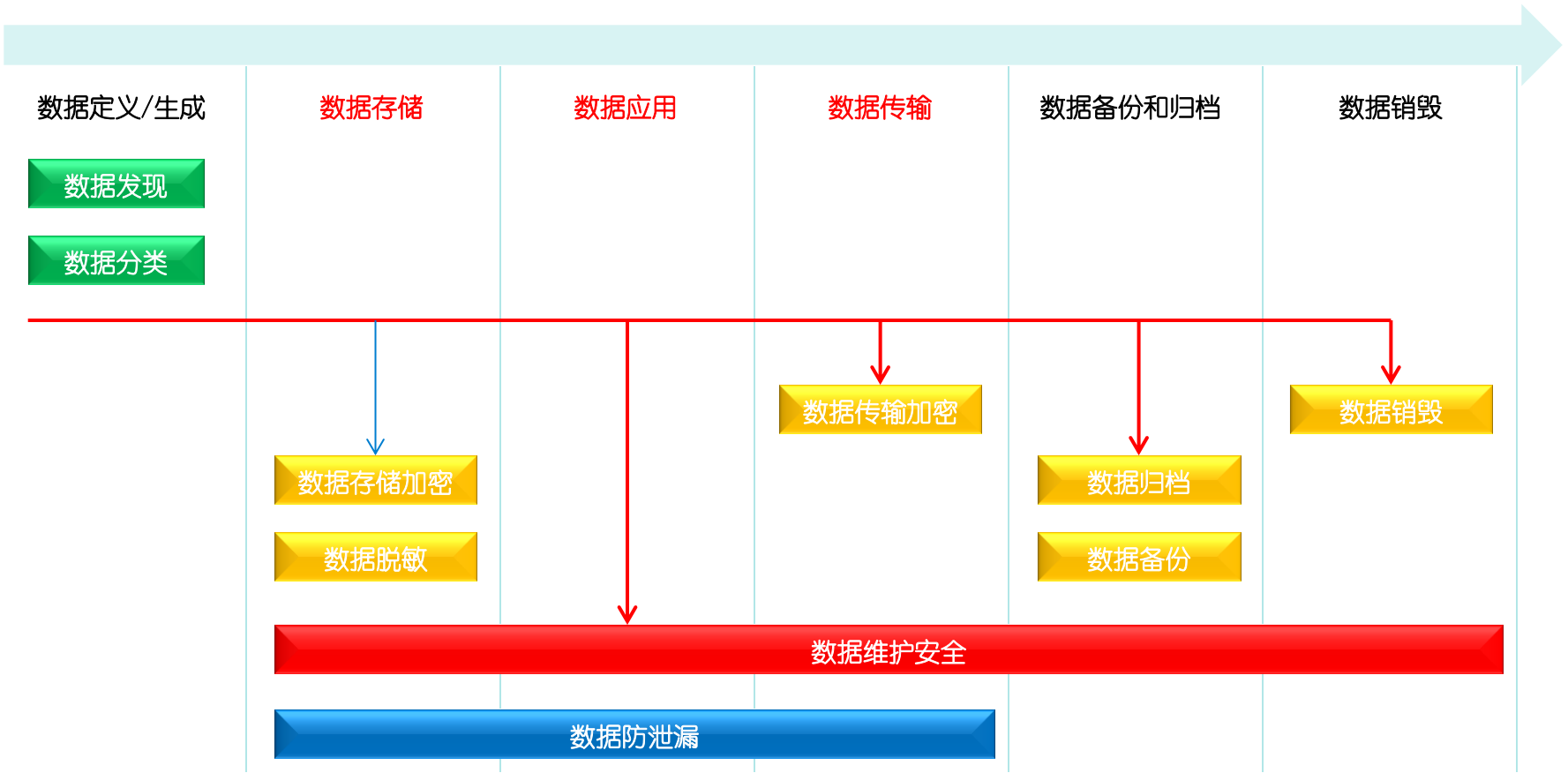
- **企业内部监管：**
  - 目前多数企业缺乏针对数据泄漏的有效管理/技术手段，增加了数据泄漏的风险；
  - 内部人员及第三方人员有意/无意的操作可能导致企业敏感数据的泄漏。
- **外部法律及合规要求：**
  - 银监会、保监会等监管机构日益提高对数据安全的重视程度，不断强调增强数据安全性且安全要求渐趋细化；
  - 其他法律法规，如PCI DSS、HIPAA法案等，均对敏感客户信息的保护提出要求。
- **数据泄漏风险：**
  - 随着IT技术的发展，数据传输渠道不断增加，造成数据泄漏的途径日益增多；
  - 大量数据泄漏给企业造成严重的负面影响，不能安全的提供客户服务，进而使企业声誉受损。

数据泄露防护准确定义

以集中策略为基础，采用深层内容分析，对静态数据，传输中的数据及使用中的数据进行识别，监控，保护的相关机制。

Rich Mogull – www.securosis.com

数据泄露防护覆盖重要的三个数据生命周期



全球数据防泄露防护的合规要求

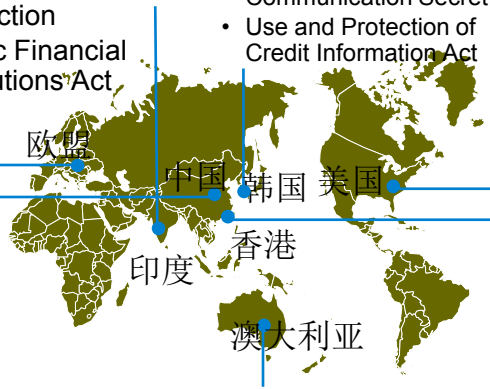
随着全球化的数据集中，合规问题将成为管理层重点关注领域

- The Act on Promotion of Information and Communications Network Utilisationand Information Protection
- Public Financial Institutions Act

- Protection of Personal Information Act
- The Act on Promotion of Information and Communications Network Utilisationand Information Protection
- Protection of Communication Secret Act
- Use and Protection of Credit Information Act

欧盟数据保护法

- 《信息安全等级保护管理办法(试行)》
- 《中华人民共和国保密法》
- 《商业银行信息科技风险管理指引》
- 信息安全技术个人信息保护指南



《隐私权法》

- 《个人资料（私隐）条例》及其监管指引
- 《银行营运守则》

- Model Data Protection Code for the Private Sector
- E-commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce

- Privacy Act 1988
- Privacy Amendment (Private Sector) Act

注：以上仅为部分国家或地区的部分主要信息保护及防泄露相关的法律法规示例

数据泄露风险与合规的挑战-案例分析

以香港为例：

法律法规名称	数据类型	覆盖领域	对于全球化数据传输是否有管理合规要求	针对银行全球化的影响	数据防泄露解决方案可以提供何种帮助
《个人资料（私隐）条例》	所有直接或者间接涉及用户个人信息	数据收集 数据保存 数据使用 数据准确 数据披露 数据传输	是 除特例以外，禁止个人数据从香港境内向任何缺乏足够数据保护体系的传输	如果需要按照全球化部署将香港客户个人数据做收集、保存、使用和传输，就需要金融企业建设完善数据防泄露保护体系，否则就会面临个人数据无法从香港传输至大陆，并且做集中存放和使用的风险；同时还需要在与其他国家的数据交换中避免香港客户数据外传。	1> 内容扫描：标识并过滤受到监管要求而不能传输的数据； 2> 策略定义：集中统一定义数据收集、保存、传输和披露策略，针对不同的法律法规要求设定数据收集、传输和保存的场景
《银行营运守则》	客户个人信息	数据收集 数据使用 数据披露 数据传输（第三方）	是 该守则要求遵循《个人资料（私隐）条例》	跨地区、跨国的传输增加了数据在传输环境泄露的风险，数据的泄露将直接违反法律法规的要求	NDLP(网络数据防泄露)的扫描和监控机制可以帮助数据在跨国、跨地区传输时大大降低数据在传播过程中泄露的风险
个人资料（私隐）条例监管政策手册（SA-2 外包）》	所有直接或者间接与外包相关数据	外包策略 数据外包	是 被监管者外包策略和安排需要遵从本规定；被监管者需要大致告知客户其数据被外包的可能…	如果金融企业在实际业务中采取了外包合作模式，需要使用数据防泄露保护机制加强管理，避免第三方泄露个人数据泄露情况的出现	结合数据防泄露产品对于敏感数据的扫描、标识、预警和拦截功能，帮助银行建立或完善数据防泄露保护机制，避免第三方泄露个人数据。

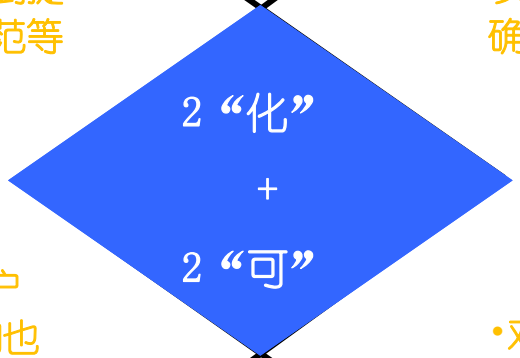
数据防泄漏对于客户的价值

1、员工行为可视化

•可以清晰了解员工日常工作中对于敏感数据操作行为；并结合企业对于数据安全的管理要求加以监督，从而达到提高员工安全意识，强化员工操作规范等目的

2、策略部署一体化

•可以通过完整的数据防泄漏技术手段将企业数据安全管理制度及流程加以实现，并可以覆盖到各种应用场景，确保建立完整的数据防泄漏体系；



3、行业规范可落地

•随着竞争压力的不断提高以及客户的法律意识不断加强，各监管机构也出台了与信息安全特别是敏感数据保护相关的各种合规要求，因此需要通过相应的技术手段来将合规落地

4、安全事件可追溯

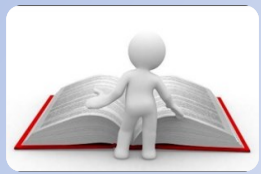
•对于出现的违规事件可以完整记录，并在必要时加以追溯，同时记录的事件可确保其完整性、防篡改性及不可抵赖性，以满足审计部门的要求

数据防泄漏项目涵盖的三个方面

数据防泄漏项目需要覆盖：组织、制度、技术

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

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。

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

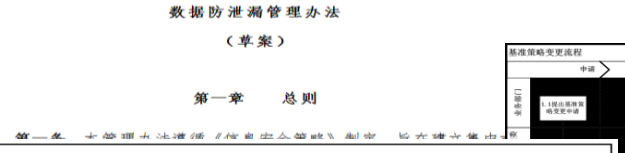
数据防泄漏整体解决方案 - 制度保障

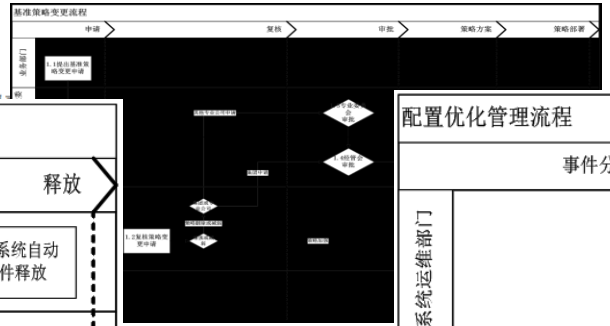
制度保障

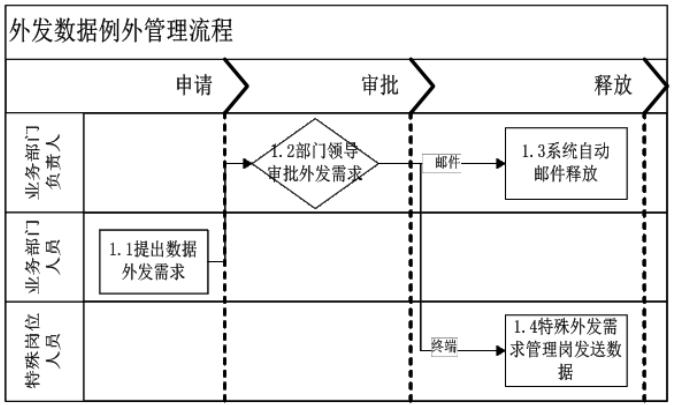
- 建立或完善数据防泄漏总体策略、数据防泄漏管理办法、数据防泄漏明细策略（面向数据）及具体的操作流程；
- 从制度体系上支撑数据防泄漏工作

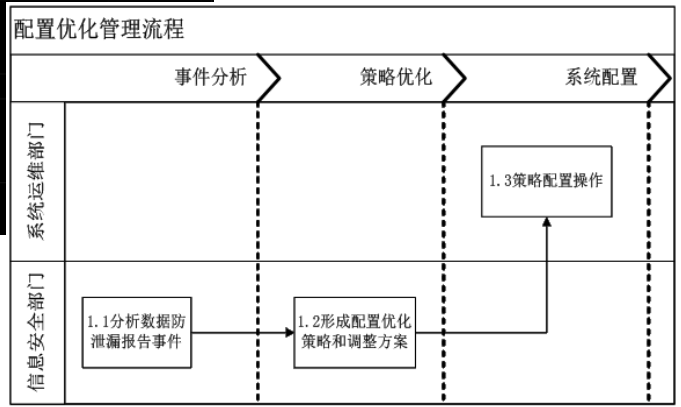
为支撑数据防泄漏管理机制，应建立结构化的制度体系，应包括：

- 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。





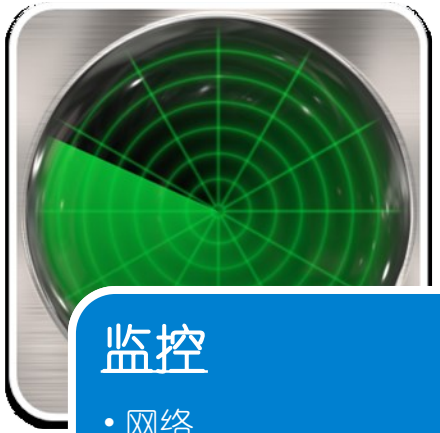




数据防泄漏整体解决方案 - 技术保障

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

数据防泄漏 – 整体机制

明确目标及高层策略

- 明确企业的敏感数据分类（机密/秘密/内部）
- 明确高层对数据防泄漏的期许并确立管控目标
- 梳理并明确数据防泄漏工作所涉及部门/岗位的职责

识别数据对象及外泄途径

- 基于业务部门的需求识别具体的敏感数据对象
- 针对需要保护的敏感数据识别需要管控的外泄途径

制定详细策略

- 结合数据类型、传输途径制定详细的数据防泄漏策略
- 制定与技术手段相配套的管理制度与流程

部署技术平台

- 选取具备完善、成熟功能的技术平台
- 将经由高层及业务部门认可的数据防泄漏策略部署在平台中并进行管控

企业数据防泄漏机制

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在数据防泄漏工作中职责。

制度保障

- 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。

技术保障

- 通过如网络/终端/邮件DLP平台落实管理层认可的详细策略，实现数据外泄行为的记录、告警及阻断。

通过职责的明确、制度流程的改善及平台的优化，持续改进并提升数据防泄漏工作的有效性，进而提高员工的安全意识

DLP数据防泄漏项目成功案例分析

– 某国有大型保险集团

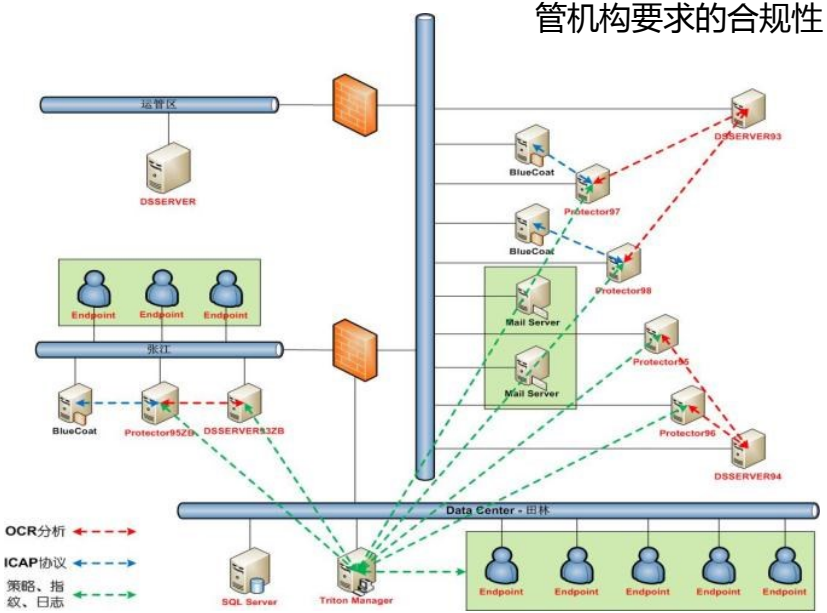
项目介绍

数据防泄漏（DLP）核心诉求

- 该保险公司在日常的运营中会使用海量的客户数据，考虑到源自外部监管机构的要求、同业竞争对手的压力，如何对公司的客户数据进行保护，防止客户信息外泄成为管理层的关注重点。

数据防泄漏（DLP）价值体现

- 该保险公司通过建立数据防泄漏的管理制度、完善技术管控手段，有效地对通过各种传输途径发送至公司外部的数据进行监控和管理，大大降低了公司客户数据泄漏的风险，既保障了公司的数据安全，又加强了对外部法律法规和监管机构要求的合规性



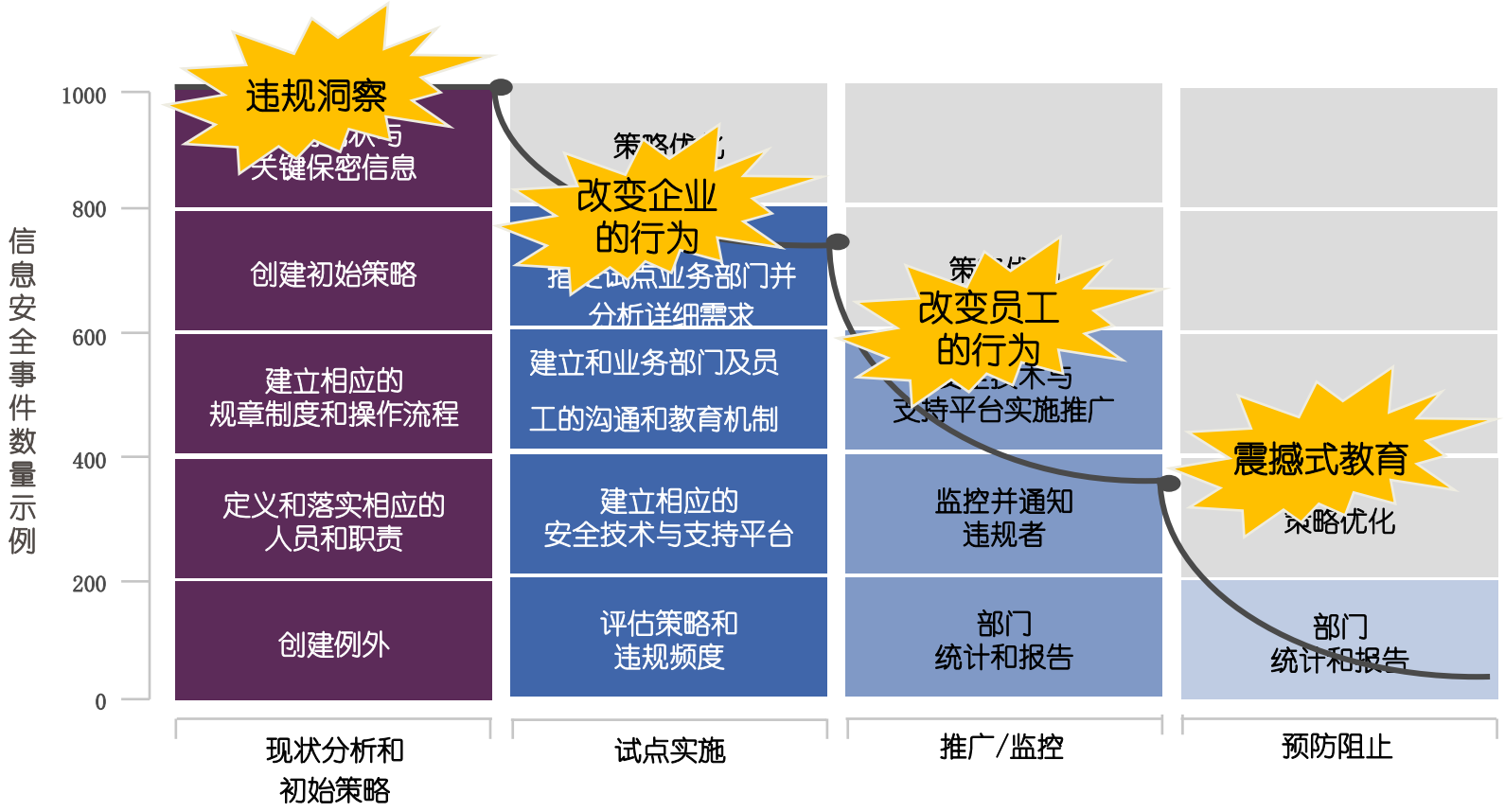
数据保护分类分阶段部署

1. 客户数据
2. 财务数据
3. 精算数据
4. 投资交易数据
5. 战略数据
6. 员工数据
7. IT数据
8. 合规与风险数据
9. 审计数据

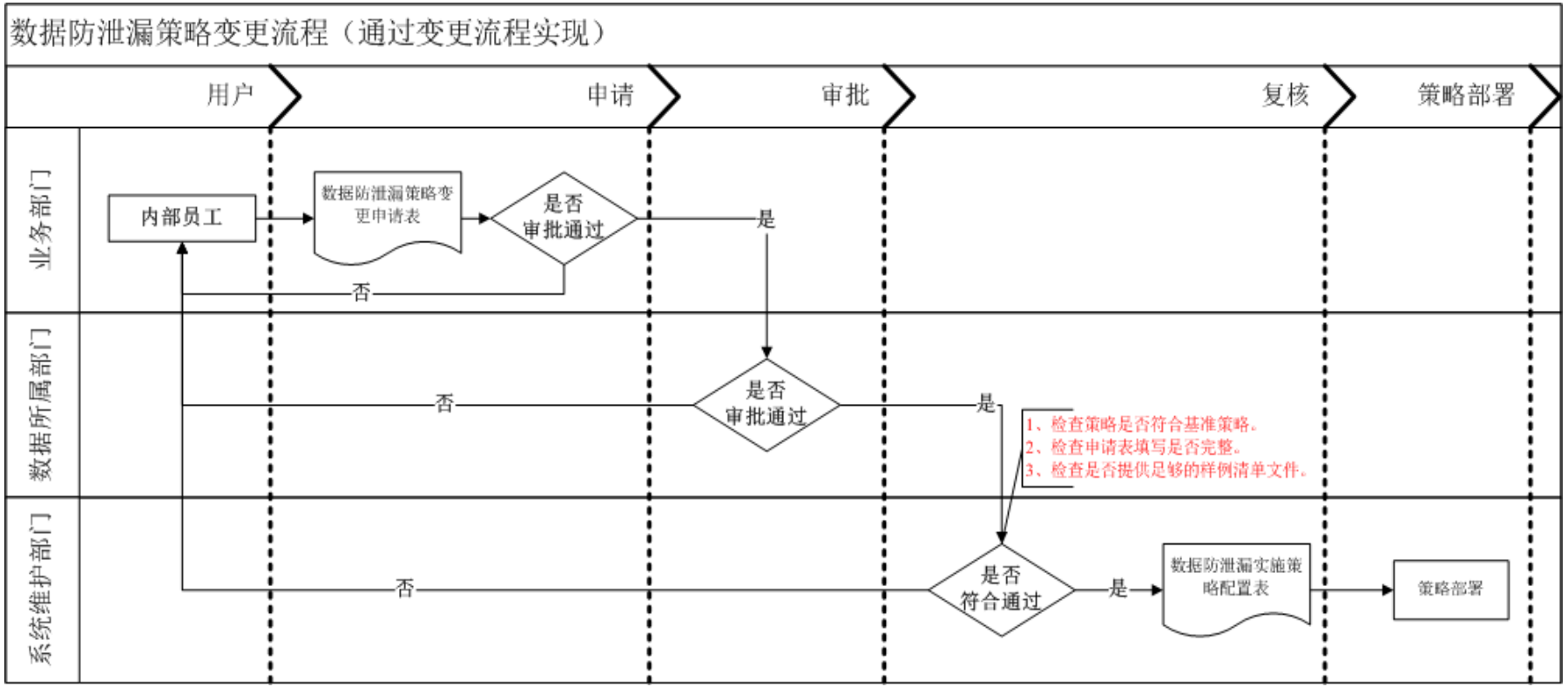
部署原则：循序渐进、按部就班

第一阶段 → 第二阶段 → 第三阶段

部署数据防泄漏策略的整体解决方案 - 分步实现、持续改进



管理流程制定

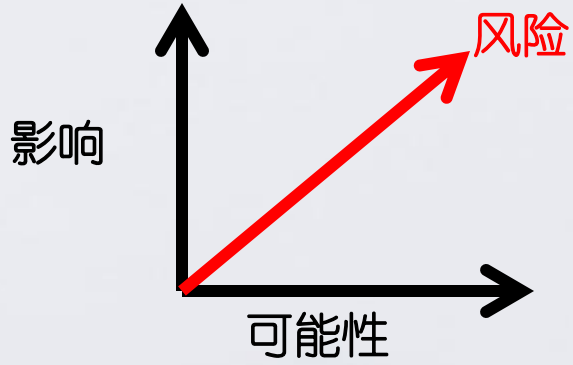

数据防泄漏策略变更流程（通过变更流程实现）
用户
申请
审批
复核
策略部署
业务部门
数据所属部门
系统维护部门
内部员工
数据防泄漏策略变更申请表
是否审批通过
是
否
否
是否审批通过
是
1、检查策略是否符合基准策略。
2、检查申请表填写是否完整。
3、检查是否提供足够的样例清单文件。
否
是否符合通过
是
数据防泄漏实施策略配置表
策略部署

数据防泄漏项目成功要素

以风险为导向找到亟需解决的问题

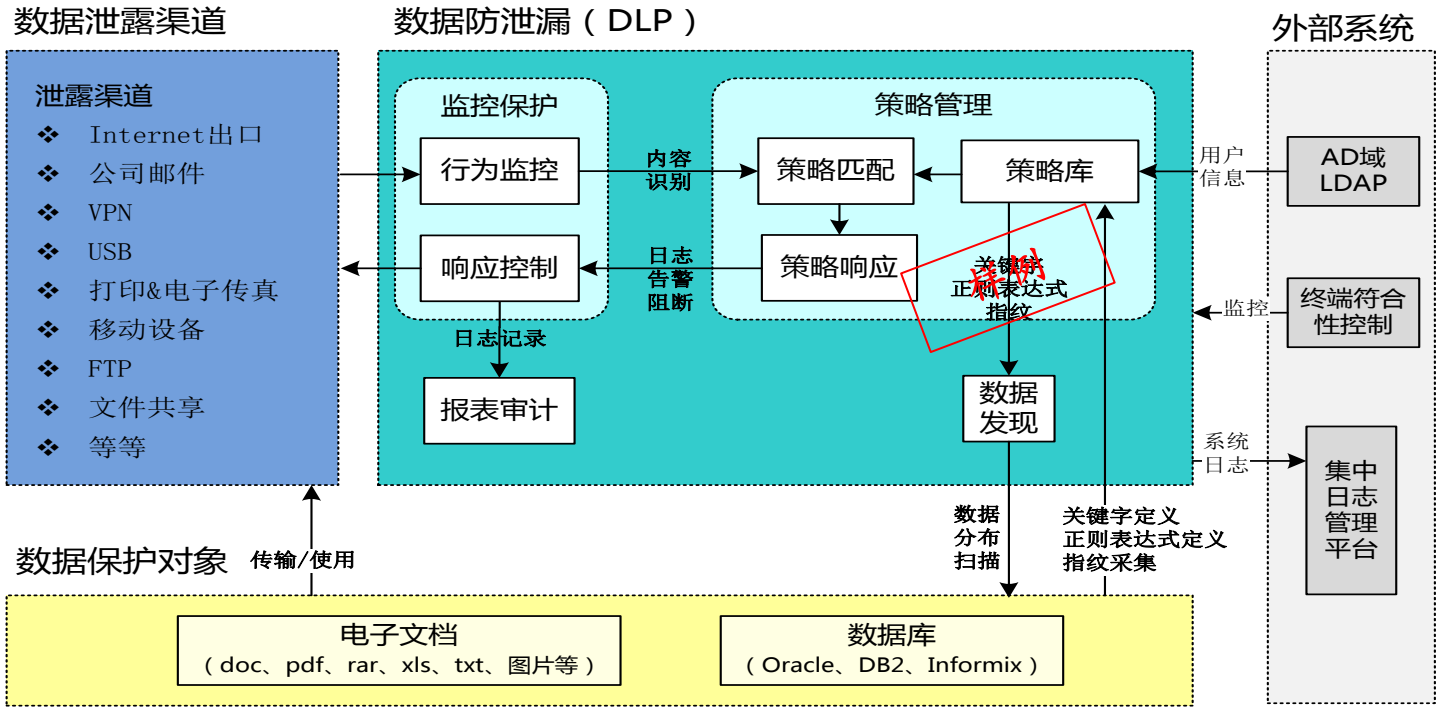
风险 = （影响 x % 可能性）

- 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*



制定完整的项目计划

需求与策略 → 方案设计 → 技术选型 → 实施和优化



数据防泄漏项目经验借鉴

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

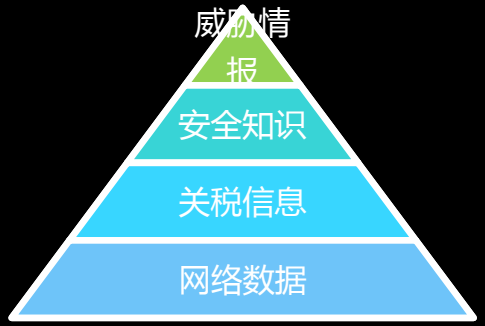
注重控制误报率

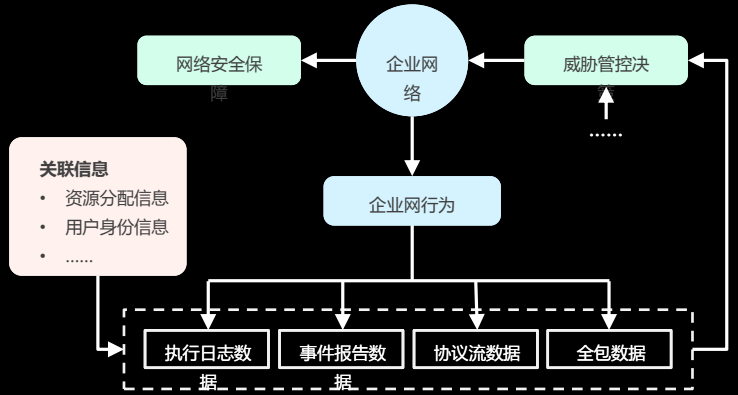
- 不断的调整策略精准度，减少误报和事件处理工作量
- 提供给相关部门和员工充分且有价值的信息，提升项目价值

大数据安全（BDSA）——需要智能内容安全技术支撑

数据：行为的映射 (安全的/不安全的)

数据用于安全是信息安全控制的一个新维度(BDSA：Big Data Security Analytics)，首先网络空间的数据能够真实地反映网络主体的行为以及行为后面的模式，其次，大数据技术的发展提供了可能。





BDSA不仅仅是大数据，而是以大数据为核心的数据全谱，其中包括解读大数据的关联信息，支撑大数据应用的安全知识和威胁情报。

数据：大数据安全解析(BDSA)

- 传统的攻击检测方法
  - 传统的攻击是基于“句法（Syntactic-based）”的，也称是“基于规则（Rule-based)”的。
  - 基于“句法”或“基于规则”的方法往往使用单一性指标（Atomic indicator）来检测攻击。这样的指标容易收集（如Hash值或IP），但与此同时攻击者也很容易通过改变这些指标来有效地逃避检测。
  - 现代的攻击已快速发展为3M方式（Multi-phased, Multi-asset, Multi-day），并导致受害者的巨大损失。
- 新一代的攻击检测方法
  - 新一代攻击检测需要在新的模型下（如Kill chain），运用大数据集合并基于语义（semantic-based)或模式(pattern-based）对攻击进行检测。
  - 新一代基于语义或模式对攻击检测方法是面向攻击者使用的工具、技战术和执行过程。识别这些内容并不容易，但对应攻击者而言也很难改变。
  - 将大数据、语义模型和KC模型结合到一起，提供了有效检测出现代地攻击的潜能。

数据：BDSA案例

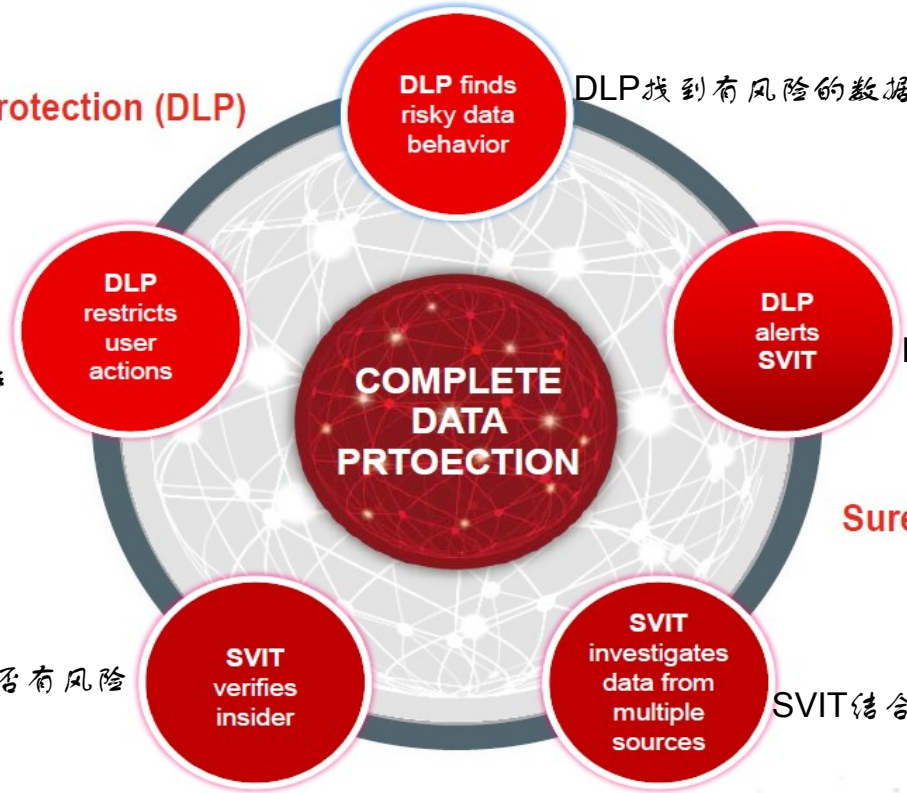
- 背景
  - 2013年，RSA、EMC和NEU以EMC企业网环境为基础，联合进行了大数据安全解析实验，据称该实验在当时是实际环境下大数据安全解析的首例应用。
  - 实验环境为EMC真实环境，数据量平均每天14亿条日志，约1TB数据，解析数据超过6T。
  - 监测对象包括EMC所有活跃主机，工作日规模为27,000～35,000台，周末规模为9,000~10,100台主机。
- 算法概要
  - 由于缺乏异常行为数据，项目采用了非监督学习的聚类算法。
  - 采用PCA(Principal Component Analysis)方法消除特征向的依赖关系、降低计算维度，采用了改进的K-means算法，进行聚类。
- 两周解析结果(2013/4/22~2013/5/5)：
  - 784个事件（平均每天56个）；
  - 仅有8个事件与企业先进的安全设备识别的事件相同；
  - 通过SOC对每个事件进行了复核：
  - 25.25%是恶意软件相关事件
  - 39.41%违规事件
  - 35.33%未能识别原因

下一代DLP的核心技术示意图

INSIDER THREAT + DLP

Data Loss Monitoring & Protection (DLP)

数据泄漏监控和保护



DLP找到有风险的数据

DLP限制用户的动作

DLP发送告警到SVIT

SureView® Insider Threat (SVIT)

SVIT验证内部的源是否有风险

SVIT结合更多信息来源进行数据分析

FORCEPOINT
POWERED BY Raytheon

UCS技术全貌 —— UCS技术不止是DLP

THANKS!