美团点评 技术团队

IT大咖说 知识共享平台

数说真相：

取证技术概述
与信息防泄密系统建设方法

美亚柏科企业电子数据取证事业部
陆平

陆 平 (Ryan)

厦门市美亚柏科信息股份有限公司

企业电子数据取证事业部 副总

技术专家委员会秘书长 技术专家

2002年至今拥有15年计算机系统技术经验，其中11年电子数据取证技术经验

多次参与公安部取证技术论剑峰会嘉宾及主持人

全国取证技术年刊发表“加解密技术分析”论文

为数十个国内外世界500强企业提供个性化的专业咨询服务及解决方案，包括BAT、华为、中兴、平安、大众、顺丰、IBM、Dell等。

相关领域经验：

- 中华全国律协网络与高新技术委员会 特邀委员
- 中国企业反舞弊联盟调查委员会 技术专家
- 中国电子数据调查分析师（MCE）
- 美亚柏科技术专家委员会（MTEC）
- 戴尔领导人训练营（PLDP）
- 微软认证系统专家（MCSE）

美团点评 技术团队

IT大咖说 知识共享平台

Part ONE

电子数据取证技术简述

2 Part

电子数据取证技术与应用

电子数据取证的定义

电子数据取证是一门借助计算机技术对电子数据进行获取、分析及鉴定的学科，涉及了数据获取、数据恢复、密码恢复、数据分析等技术。

- 使用软件和设备，按照一些预先定义的程序和规范全面地检查计算机、手机及其他电子设备，以提取和保护有关的证据。

- 电子数据取证对象
  - 计算机、平板电脑、手机、CD/DVD、复印机、打印机、扫描仪、GPS导航仪、照相机、摄像机、各种存储卡...

古今中外

巡按御史

元芳，你怎么看？

狄仁杰

华生，没有你我怎么办？

夏洛克 福尔摩斯


美团点评
技术团队
IT大咖说
知识共享平台

2 Part

案例解析

电子数据取证技术的应用与价值

美团点评 技术团队

IT大咖说 知识共享平台

上网痕迹调查

- 马加爵案件

文件搜索、分析 & 远程调查

- 全球100强娱乐软件公司未发布游戏代码外泄
  - •两周内完成19个国家，91台服务器的调查，完成信息泄露途径说明
  - •服务费用大约100万美金
- 金融资产风险管理公司（代催不良贷款）员工外移业务
- 世界500强金融集团业务员违规放贷 ☆
  - •集团稽核部接到举报某市营业部存在业务员使用制作电子公章软件，伪造虚假公司进行贷款
- 阿里月饼门事件

2 Part

企业内部调查案例解析

远程调查的优势与价值

计算机可调查的常见应用

序号	图标	名称
1		PC版微信
2		360云盘
3		百度拼音
4		Cortana微软小冰
5		DreamMail
6		FileVault恢复密钥检索
7		iCloudDrive苹果云盘
8		金山快盘
9		Mac-通话记录
10		MicrosoftEdge浏览器
11		OneDrive云盘

序号	图标	名称
12		OneNote云笔记
13		营销QQ
14		QQ拼音
15		腾讯RTX
16		ShellBag资源管理器痕迹
17		搜狗五笔
18		腾讯微云
19		Thunderbird雷鸟
20		Win10邮件客户端
21		Windows-Apache日志
22		飞秋

总计约50多种常见应用可以进行解析

3 Part

电子数据司法鉴定资质

美亚柏科下属单位"福建中证司法鉴定中心"成立于2005年，是首批经审核
鉴定机构（许可证号：350205004），也是全国第一个通过CNAS实验室认可
鉴定机构（认可证书号：CNAS L4709）。

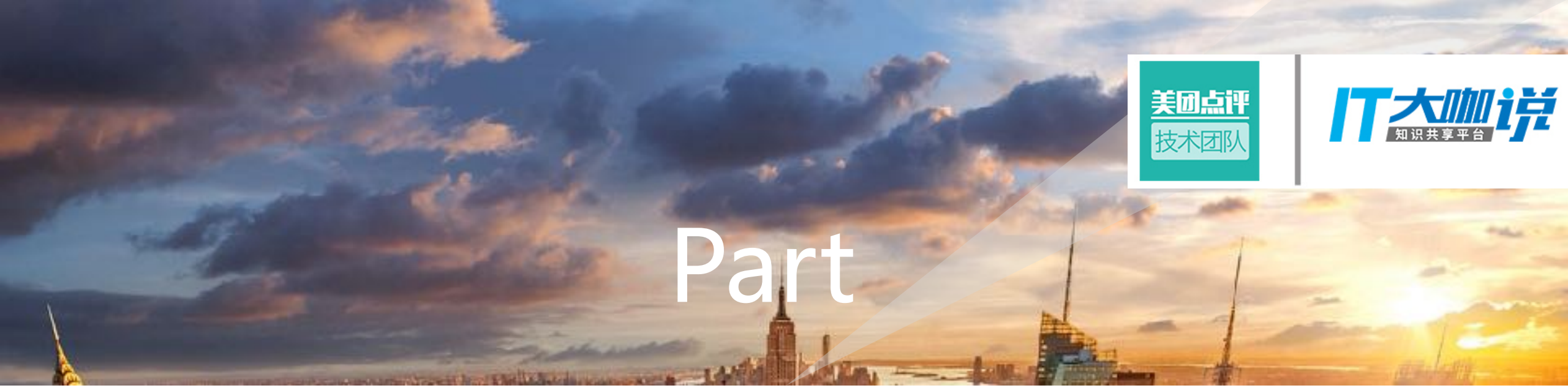
服务优势

- 鉴定效率高
- 鉴定结果采信率高
- 完善的鉴定设备
- 一流的鉴定技术
- 工作流程满足国际标准

3 Part

电子证据固定与保全的意义和方法

电子数据司法鉴定-经典案例



Part Two

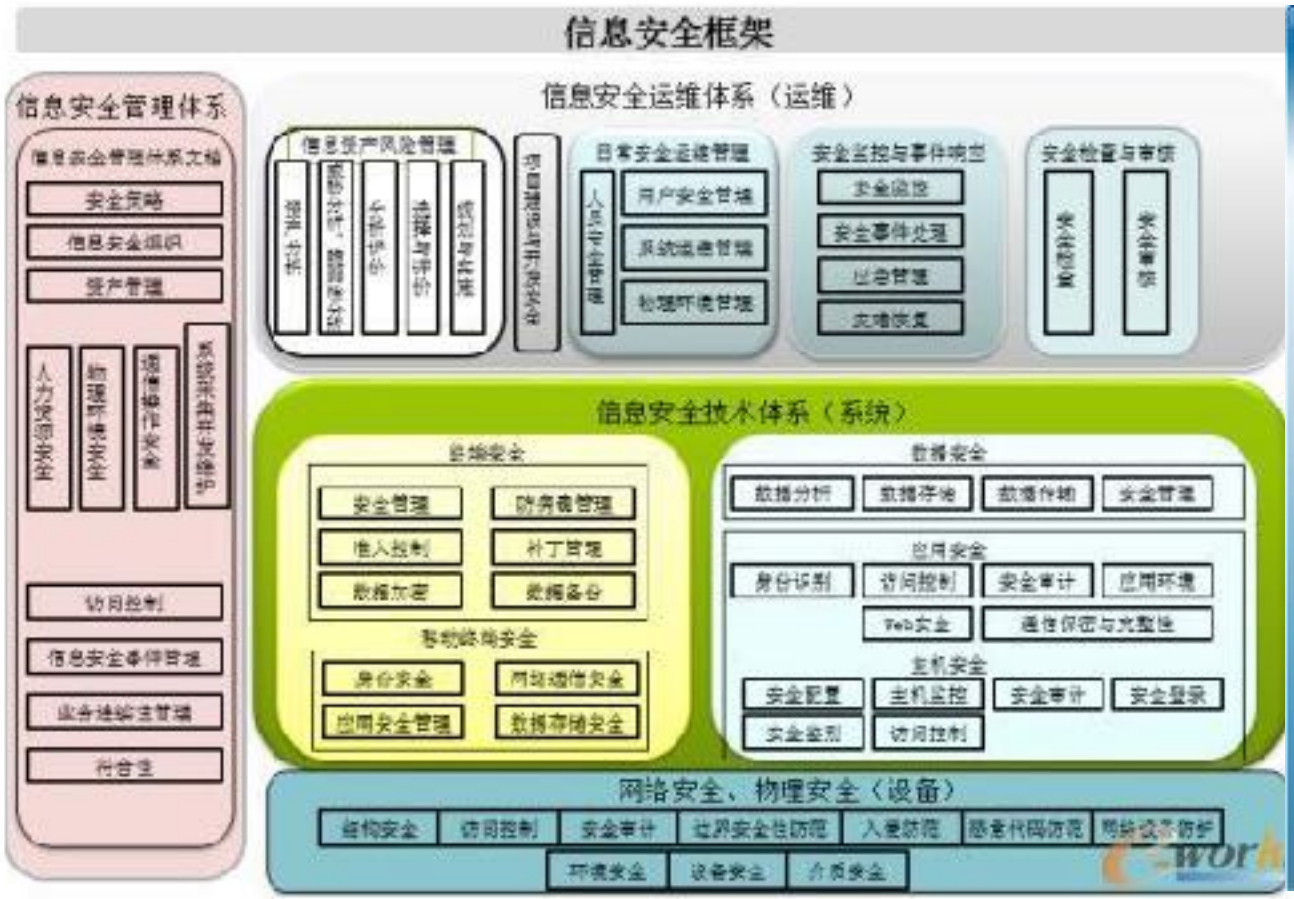
企业信息防泄密系统建设方法

3 Part

企业信息安全框架

美团点评 技术团队

IT大咖说 知识共享平台



物理安全　终端安全　主机安全　网络安全　数据安全　应用安全

3 Part

企业信息防泄密系统建设方法

McAfee常见参考产品

1	网络安全平台 (NSP/ISC)
2	终端安全保护套件 (Endpoint Security)
3	虚拟化防病毒 (MOVE)
4	应用程序白名单 (Application Control)
5	高级威胁防御设备 (ATD)
6	Web 安全网关 (Web Gateway)
7	数据防泄漏 (DLP)
8	安全信息和事件管理 (SIEM)
9	威胁情报交换系统 (TIE)

3 Part

企业信息防泄密系统建设方法

数据防泄漏的必要性

内部人员和合作伙伴造成大量的漏洞

- 内部人员错误的操作数据
- 不正确的业务流程添加了数据泄漏风险

泄漏中的
76%

合规强制要求数据保护

- 对于数据隐私越来越多的关注
- 需要数据安全控制的技术方法

数据泄漏公司中的
81%
没有PCI合规

数据泄漏越来越多的途径

- 针对有高级价值数据的外部泄漏
- 针对数据存放位置可视性的限制

$6.7M
平均每次数据泄漏
造成的损失

3 Part

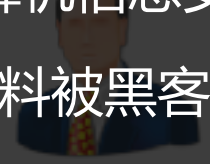
企业信息防泄密系统建设方法

国内企业安全的现状

调查报告

国家计算机信息安全测评中心数据显示:

- 重要资料被黑客窃取和被内部员工泄露比例为 1:99



管理者对信息安全不够重视

关注外网安全

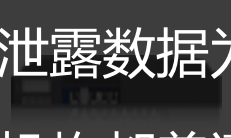
部署防火墙、IDS/IPS、漏洞扫描系统等，防范外部攻击

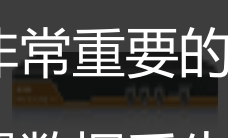
忽视内网安全

缺乏对内部各种行为进行有效、合规管理

《了解21世纪IT环境的安全复杂性》全球调研报告:

- 85%的泄密出自于内部泄密
- 83%的泄露数据为非常重要的文档及知识产权
- 77%的机构都曾遭遇数据丢失





员工安全意识普遍不高，水平参差不齐

内网信息安全 不容忽视

美团点评 技术团队

IT大咖说 知识共享平台

DLP系统建设

何为DLP
Data Lost Provent
Gartner 有专属分类及魔力象限

3 Part

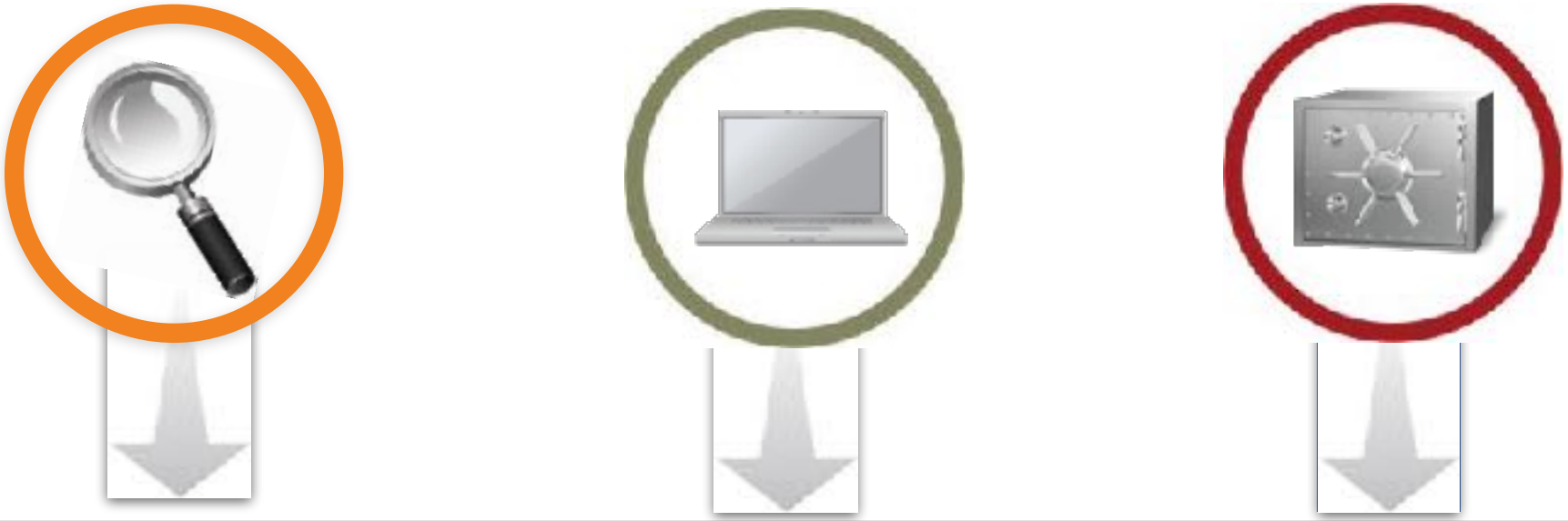
DLP系统建设

数据泄漏风险如何评估

机密数据位于何处

机密数据如何流转

机密数据如何被泄露



发现

监控

保护

数据防泄漏 (DLP)

3 Part

DLP系统建设

数据防泄漏的最佳实践

1. **发现和评估**

   发现保存在所有位置的敏感数据，对风险进行评估

2. **数据分类**

   确保安全的数据处理流程正常运转

3. **定义有效的策略**

   创建策略用于保护数据，并且确保策略的有效性

4. **实施控制**

   控制机密数据的授权访问和安全传输

5. **监控, 报告和审计**

   通过报警和事件管理来确保成功的数据安全防护

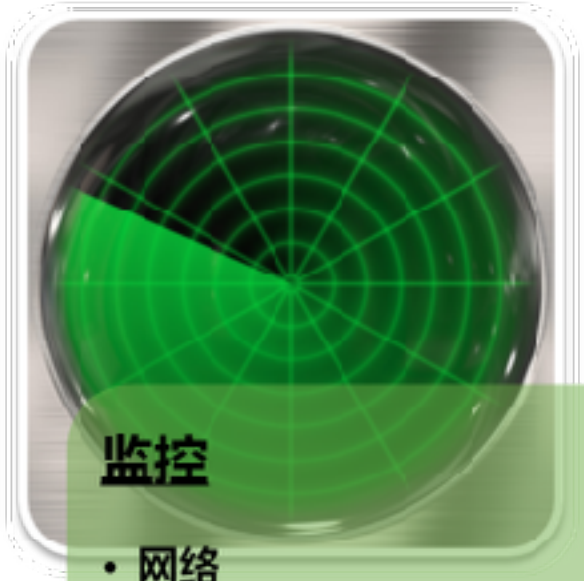
3 Part

DLP系统建设

数据防泄漏方案技术保障

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

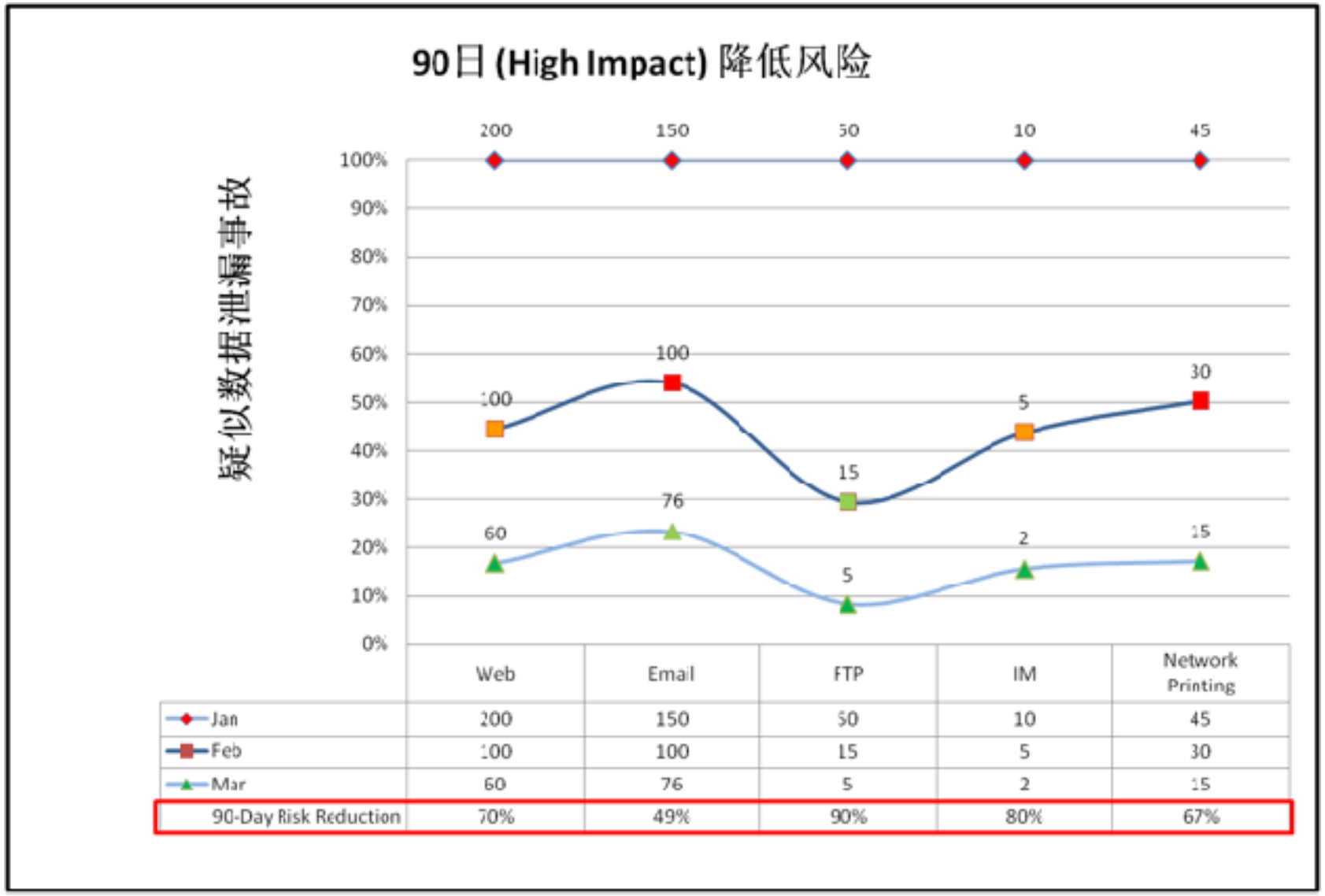
保护

- 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

3 Part

DLP系统建设

风险导向，快速体现投资回报



	Web	Email	FTP	IM	Network Printing
Jan	200	150	50	10	45
Feb	100	100	15	5	30
Mar	60	76	5	2	15
90-Day Risk Reduction	70%	49%	90%	80%	67%

GOALS	
30-days	Base Line
60-days	25%+ reduction
90-day	50%+ reduction

MARKER LEGEND
高
中
低
可接受

DLP 投资回报

3 Part

国外DLP系统的不完美

美团点评 技术团队 | IT大咖说 知识共享平台

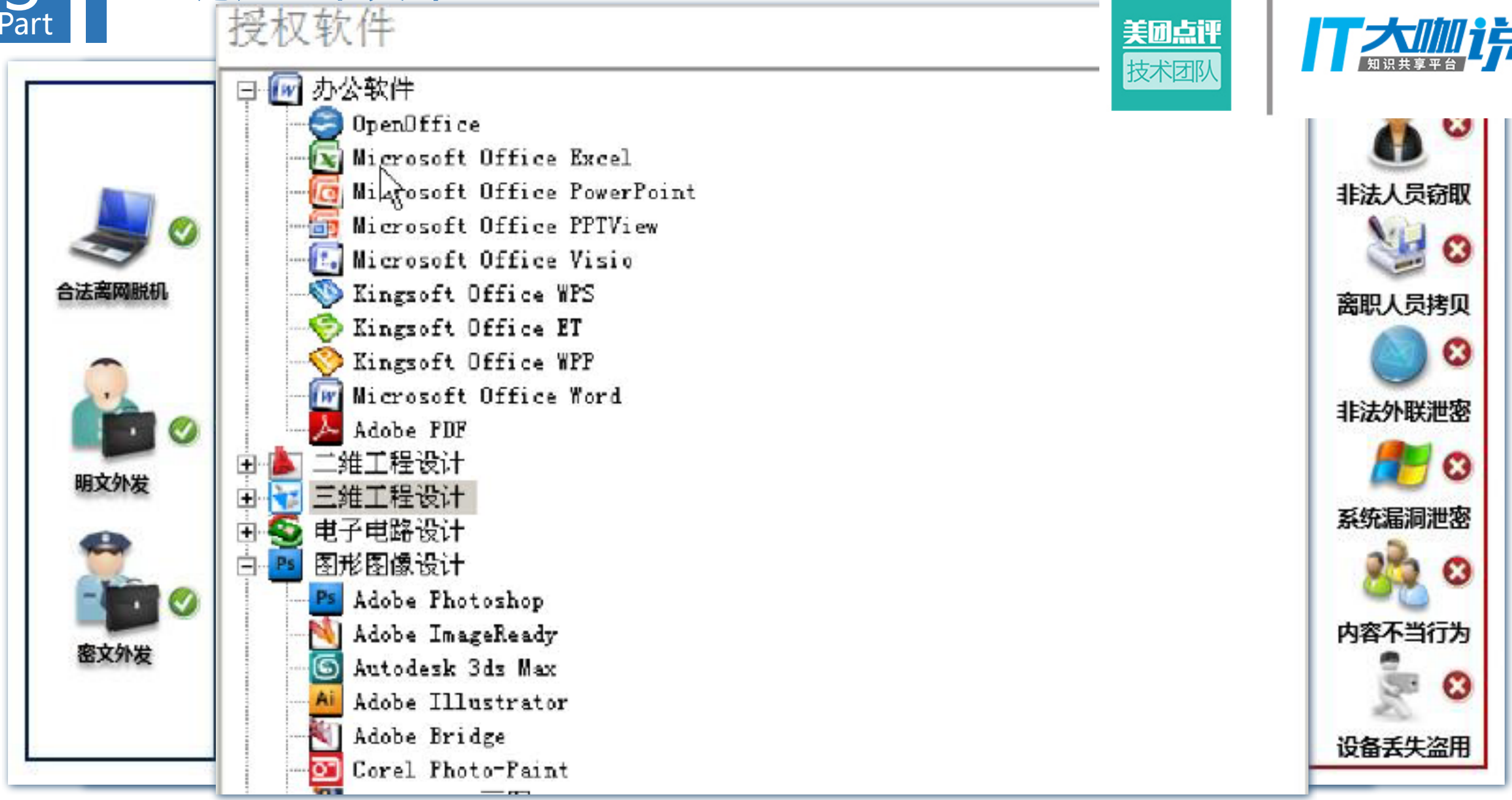
贵一点	功能精细但费用较高 • 精细到各个数据文件的内容，支持图片和语法 • 通常50-200万的建设预算
文雅了一点	缺乏终端行为管控 及 安全管理稍弱 • 不能全面记录用户的所有行为，必须提前设置策略 • 部分泄密途径没有精细的安全管理功能

美团点评 技术团队

IT大咖说 知识共享平台

透明加密技术

3 Part 透明加密技术



3 Part

国内数据防泄密系统建设

核心定位 → 数据

辅助定位 →

- 桌面管理
- 系统运维
- 行为管理

一款内网安全管理软件

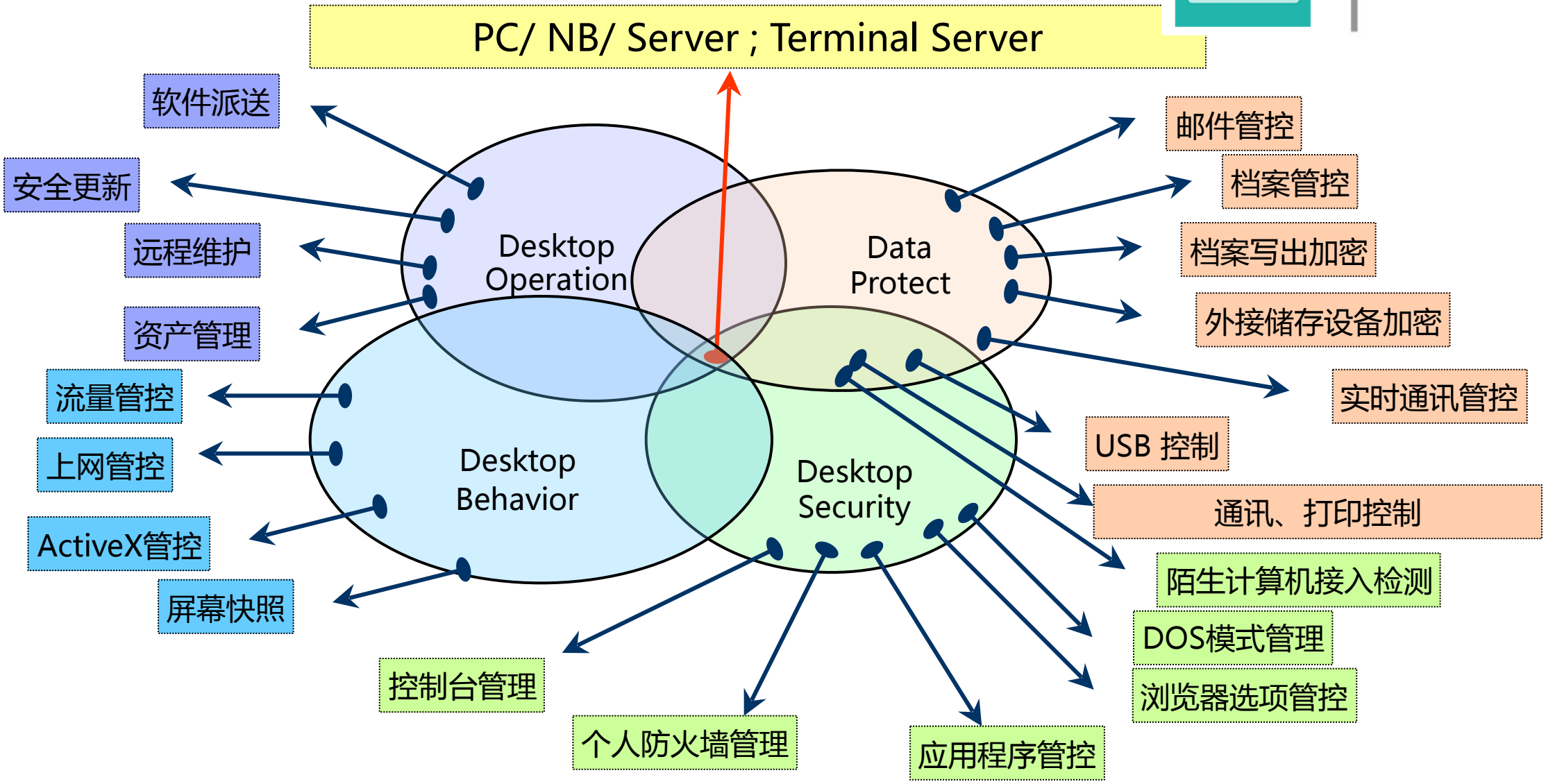
运用系统管理思想，充分利用操作审计、权限管控、文档加密等技术手段

全面解决信息安全、行为管理、系统运维等方面的内网安全难题

3 Part

国内数据防泄密系统建设

内网安全端点管理范围



3 Part

国内数据防泄密系统建设

常用功能

内网安全管理部分

基本模块
资产管理
设备管控
移动存储管控
打印管控
应用程序管控
文档操作管控
即时通讯管控
屏幕监视
远程控制
邮件管控
网络控制
网页浏览管控
流量管理
慧眼风险
审计报表

文档加密

透明加密
只读加密
智能加密
安全网关

美团点评 技术团队

IT大咖说 知识共享平台

存证的必要性

云图标

阿里云 aliyun.com	百度云	腾讯云	金山云
华为云服务 HUAWEI	亚马逊 aws	七牛云 QINIU	iCloud

存证云电子合同在P2P金融的应用

P2P金融的特点

•借款项目小额分散，借款方主要是小微企业和个人；

•在风控上的最大痛点是欺诈，停业、跑路、提现困难、诈骗等恶性事件时有发生。

！！既要求高效率的签约，又要尽量确保签约双方的履约能力。

存证云电子合同助力P2P金融

•实现短平快的在线签约；

•合同第三方存证，作为风控手段之一，降低欺诈风险，同时帮助提高其平台客户的信任度；

存证云的工作原理：以网页取证原理为例

① 用户输入网址

② 网址提交第三方保全机构

③ 第三方保全机构服务器进行本地环境清洁和网络环境检测

④ 第三方保全服务器抓取对应网页并存证

保存的网页内容

电子数据存证云应用场景

美团点评 技术团队 | IT大咖说 知识共享平台

电子数据存证应用场景

知识产权保护

网络侵权取证

电商平台/维权机构打假

货物查验

物流、运输、快递等领域

装货、运输情况存证

商务谈判/沟通

商务往来邮件存证

供应链监督管控

企业供应链、合作伙伴等

监督及资金对账、奖惩等

存证

电子合同+存证应用场景

互联网金融

双方或多方借贷合同

第三方支付合约

……

银行/证券

开户

服务协议

委托协议

……

企业管理

劳动合同

销售采购

订单处理

供应商管理

……

教育培训机构

教师合同

在线教育协议

各类申请书

……

存证云的应用价值

- 提升签约效率，优化合同管理流程，减少纸质合同、文件印刷仓储成本；
- 变普通电子数据为合法证据，降低维权门槛；
- 存证守护，帮助提升企业形象，提升其用户信任度。

什么是全流量？

----网络所有原始流量的存储、分析

全流量必须具备“三个全”

全流量鉴别

“4K全高清，鉴别身份”

全行为分析

“人脸识别+行为识别”

全数据回溯

“快速定位所需画面”

网络空间的“平安城市”、“雪亮工程”

美团点评 技术团队 | IT大咖说 知识共享平台

为什么要选全流量？

为什么要用全流量

1. 感知未知威胁：再高级的威胁都会产生流量
2. 满足合规要求：等级保护2.0要求部署全流量回溯
3. 事件调查取证：还原过程，责任界定

传统安全检测手段弊端

未知威胁难以感知

基于特征匹配

告警太多无法分析

最后也懒得看

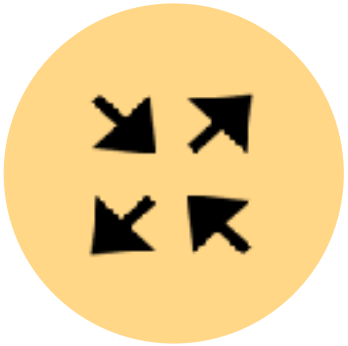
安全问题难以追溯

只有日志信息

44%的威胁，现有安全工具没有发现！

80%的泄密事件，依赖外部报告！

唯一万无一失的办法是网络全流量分析



全方向

网络出口

内网核心

安全域边界

+

全流量

协议鉴别

行为分析

全数据存储

网络全流量回溯分析VS传统安全检测手段

	防火墙	IPS/IDS	防病毒	网络审计	全流量回溯
已知威胁检测	无	支持	支持	无	支持
未知问题分析	无	无	无	无	支持
行为记录	简单	无	无	丰富	全面
追踪溯源	无	无	无	简答	完整