企业信息安全：规划与实践

Planning And Practice On Information Security

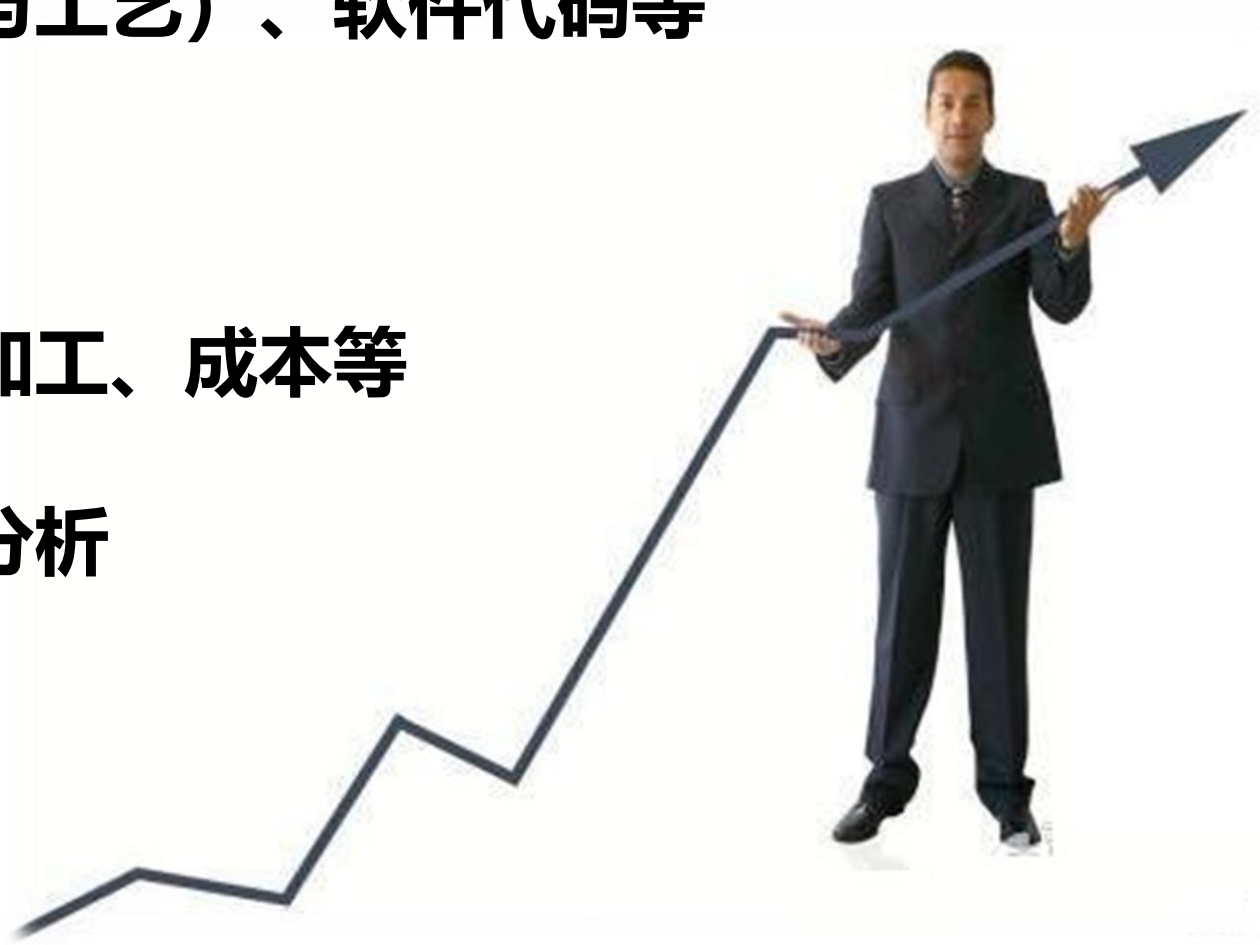
三花控股集团 叶根平

企业信息安全面临更复杂的挑战

数据等无形资产的比重快速增长

数据/信息类资产

- ✓ **创新：专利、产品（结构与工艺）、软件代码等**
- ✓ **市场：客户、需求、项目**
- ✓ **业务：管理平台、材料、加工、成本等**
- ✓ **环境：行业、政策、趋势分析**



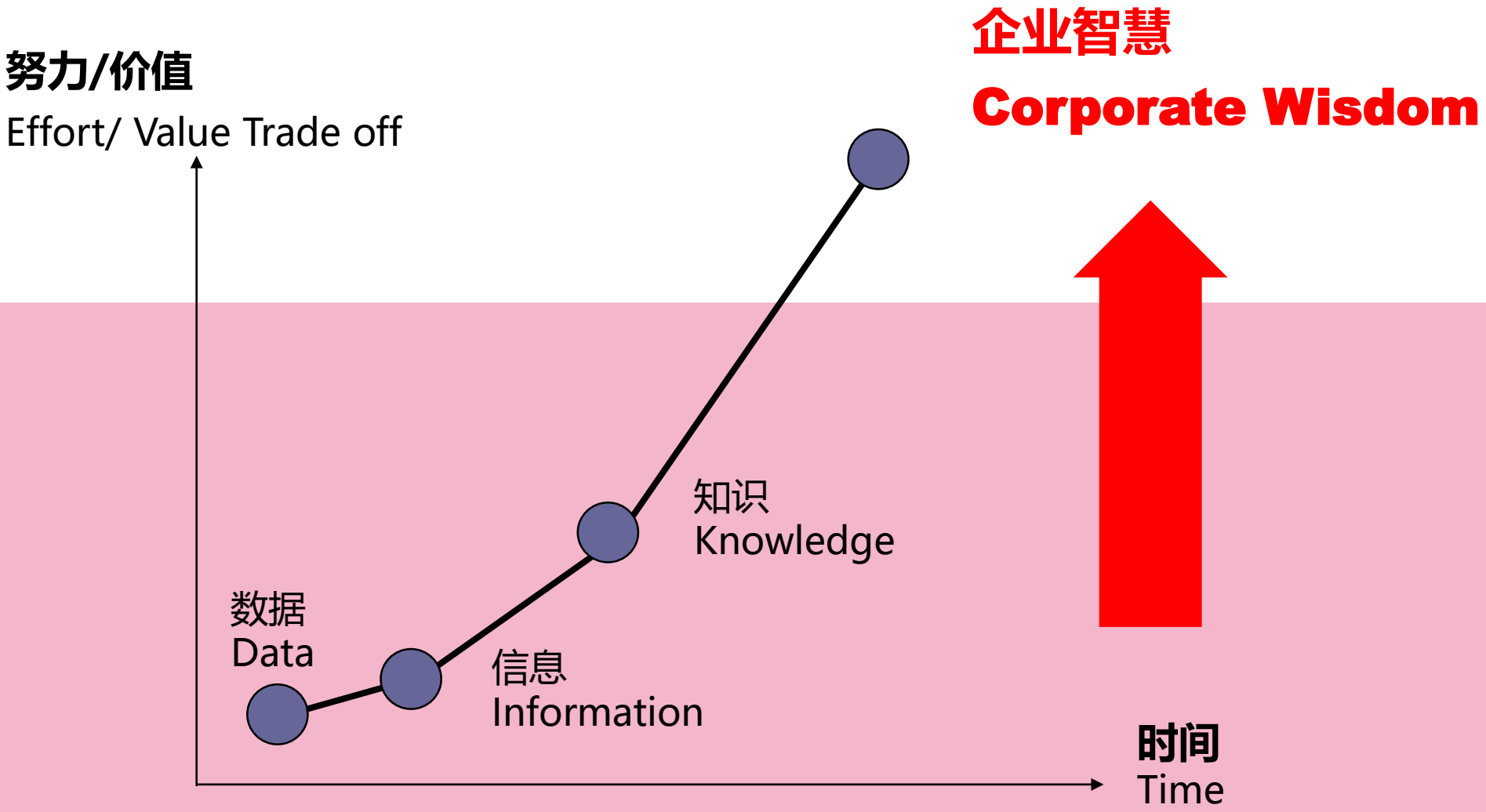
数据/信息类资产

“苹果” 公司的价值评估

2014年年报（资产负债表）里的全部“资产”为***261.9***亿美元。

2014年全球企业品牌价值排行榜上的品牌估值为***1188.63***亿美元。

数据/信息类资产


企业智慧
Corporate Wisdom
努力/价值
Effort/ Value Trade off
知识
Knowledge
数据
Data
信息
Information
时间
Time

企业信息安全：

数据/信息类资产面临各种内部和外部威胁！

数据/信息资产面临各种内部和外部威胁

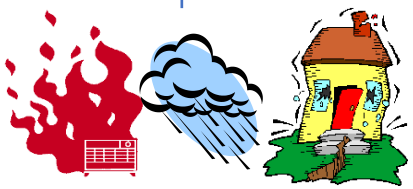
黑客攻击、拒绝服务

病毒、木马、恶意程序、

社会工程、APT

企业数据资产

通信、供电障、设备等故障



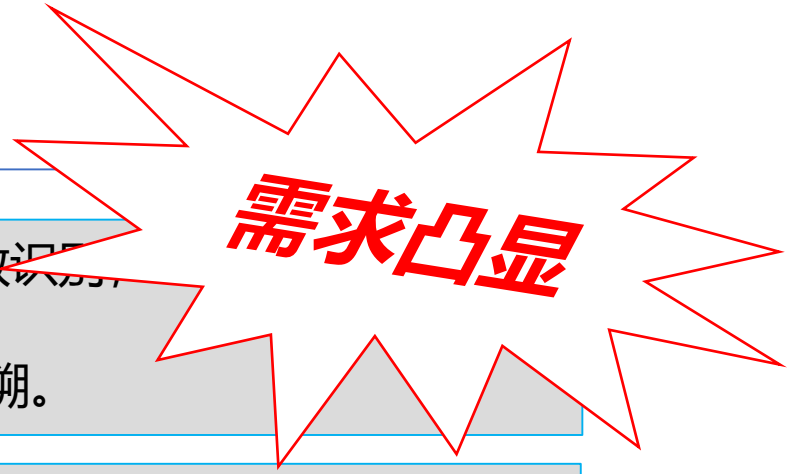
自然灾害

内部泄漏

据调查显示，互联网接入后内部重要机密通过网络泄密而造成重大损失的事件中，只有1%是被黑客窃取造成的，而**97%**都是由于内部员工有意或者无意之间泄露而造成的。

企业数据资产的内部防护是关键！

企业数据/信息管理面临的挑战



企业数据资产分布情况无法掌握

- 核心数据资产淹没在数据网络的汪洋中，无法有效识别；
- 对数据/信息资产的内部流转无法有效管理/控制；
- 对数据/信息资产的外泄情况一无所知、或无法追溯。

网络边界的界限不再分明

- 云计算、云应用打破传统企业的信息网络边界；
- 网络的互联性、共享性，导致企业缺乏有效的技术手段进行数据资产防护；
- 数据在公有云中难以得到有效保护（不被运营方和第三方人员获取？）；
- 公有云被入侵后，如何不殃及企业数据/信息资产？

信息泄露途径繁多

- 掌握核心数据的技术人员故意泄密；
- 离职人员电脑存有企业核心数据、存储企业核心数据设备丢失、被盗等；
- 核心设计文档、图纸被核心员工或高管通过U盘等方式泄露。
- 存储在云端的数据被泄漏、挖掘

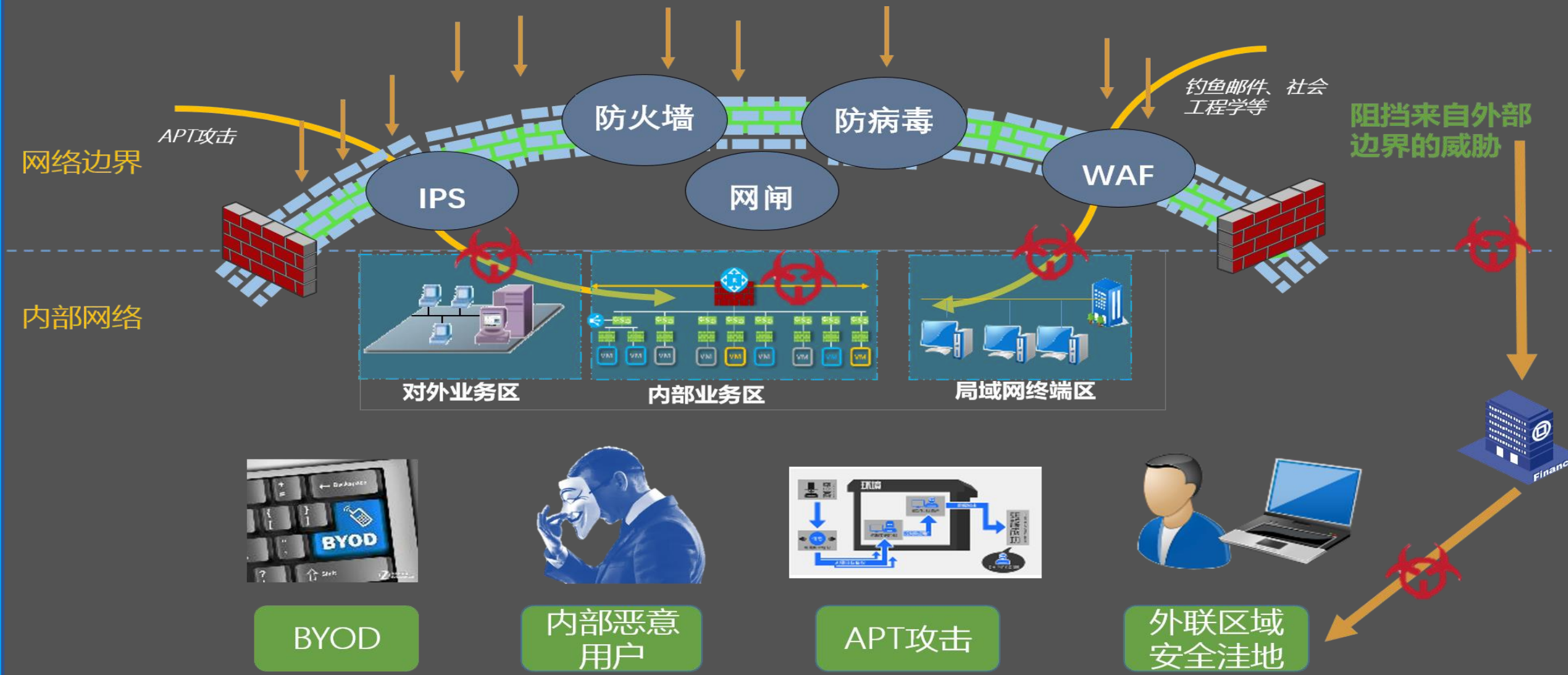
泄密无法追溯

- 如何提供泄密事件发生后的有效证据？
- 如何对企业数据资产的管理进行有效审计？

思考：GDPR时代的企业数据管理

传统“防御为主”策略有局限

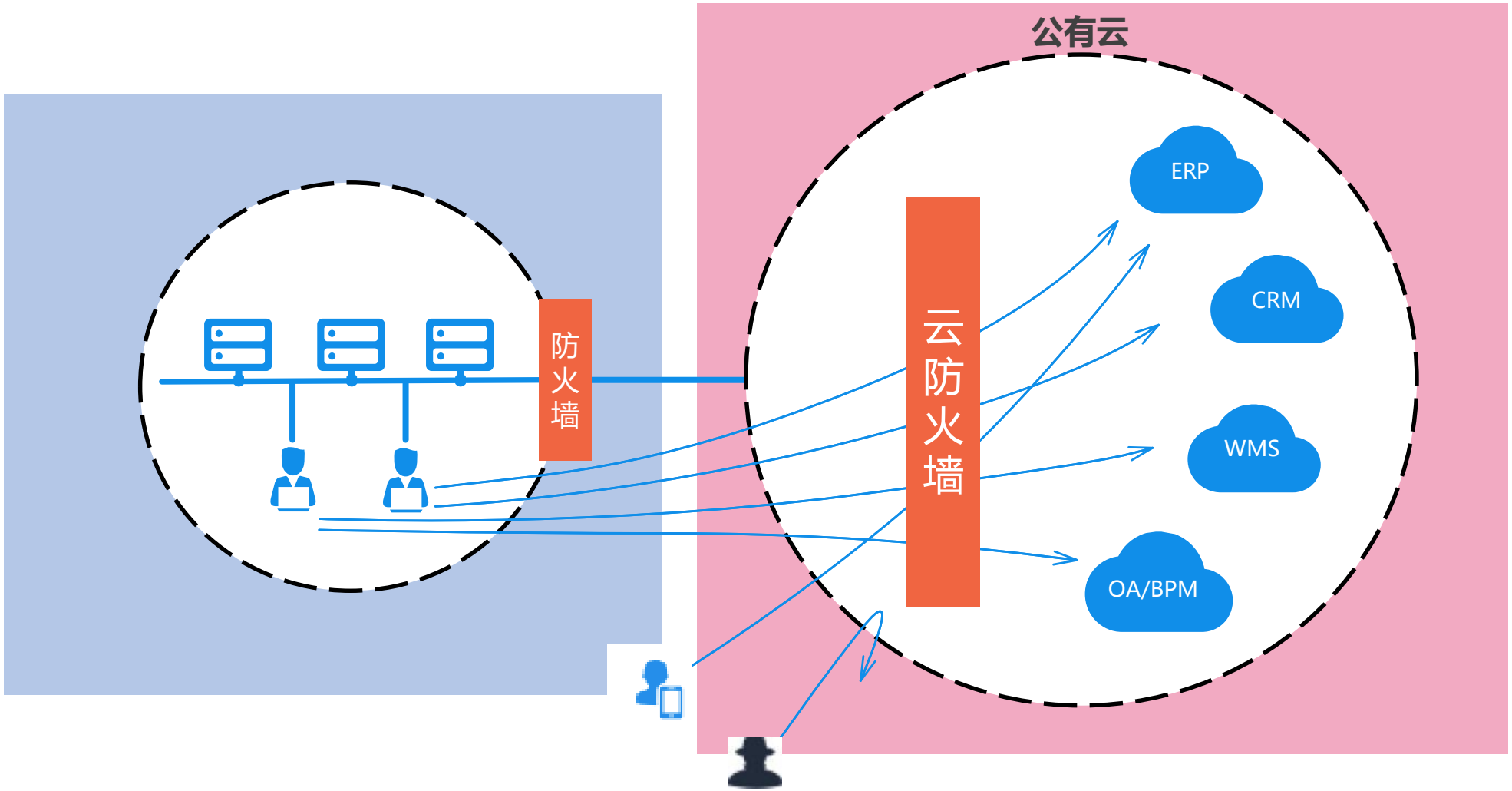
传统的“防御体系”


网络边界
APT攻击
防火墙
防病毒
IPS
网闸
WAF
钓鱼邮件、社会工程学等
阻挡来自外部边界的威胁
内部网络
对外业务区
内部业务区
局域网终端区
BYOD
BYOD
内部恶意用户
APT攻击
外联区域安全洼地

规划并实施全面数据安全管理!

1. 全部：所有信息资产及载体均有分级管理
2. 全程：重点信息资产的采/移/用轨迹可视化
3. 全员：高授权人士的涉密/泄密行为可追溯

规划：云环境下的“防火墙”



规划：数据/信息安全部署策略

事前防护

- 数据安全策略
- 文件标签和加密
- 用户访问权限设置
- 文件基因和数字资产库
- 安全分享控制
- 敏感数据脱敏

事中监控

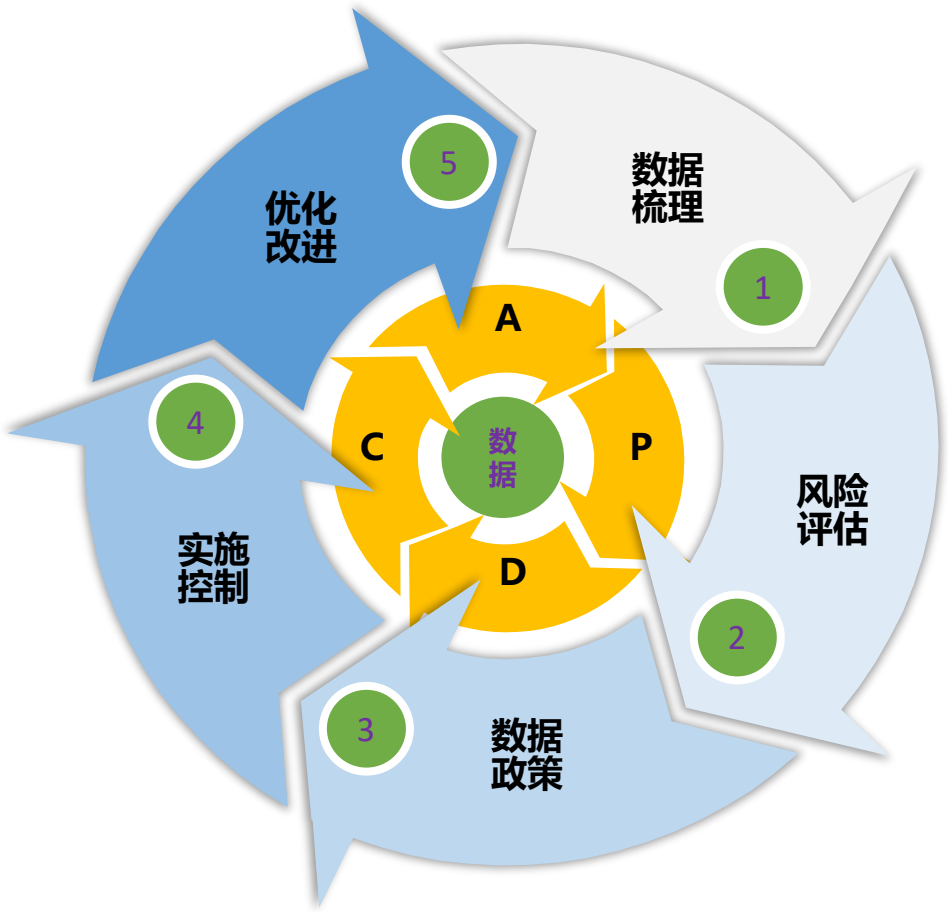
- 用户行为可视化
- 异常行为分析和监控
- 企业数字资产分布图谱
- 文件流转轨迹可视化

事后追溯

- 文件访问时序图
- 文件流转轨迹图
- 文件基因和关联识别
- 文件操作日志
- 文件泄露源头查询

解除各种数据泄露的痛点，寻求数据安全保护的**事前防护**、**事中监控**和**事后追溯**的方案，让数据自主、安全、可控

规划：数据/信息安全保护方法论



基于PDCA过程模型的数据安全保护方法论

- 数据识别和分级是安全保护的**首要环节**
- 风险评估是数据安全保护的**核心**
- 数据安全规章制度及执行是**基础**
- 系统建设和过程风险控制是**关键**
- 问题改进是防护能力不断提升的**保障**

规划：数据/信息安全建设步骤

STEP 01

构建关键边界

采用防火墙做ACL、NAT，实现把不合规IP、端口拦在外面；

STEP 02

边界安全加固

采用下一代防火墙进行IPS、勒索病毒防御、WEB防护，补充原Fw不足；

STEP 03

内部安全加固

通过安全态势感知分析内部流量、边界安全，掌握全网网络安全情况，从源头发现内鬼、潜伏者；

STEP 04

数据安全建设

数据外发分析，及时定位敏感数据，对违规行为进行拦截；

STEP 05

安全管理，运维可视化

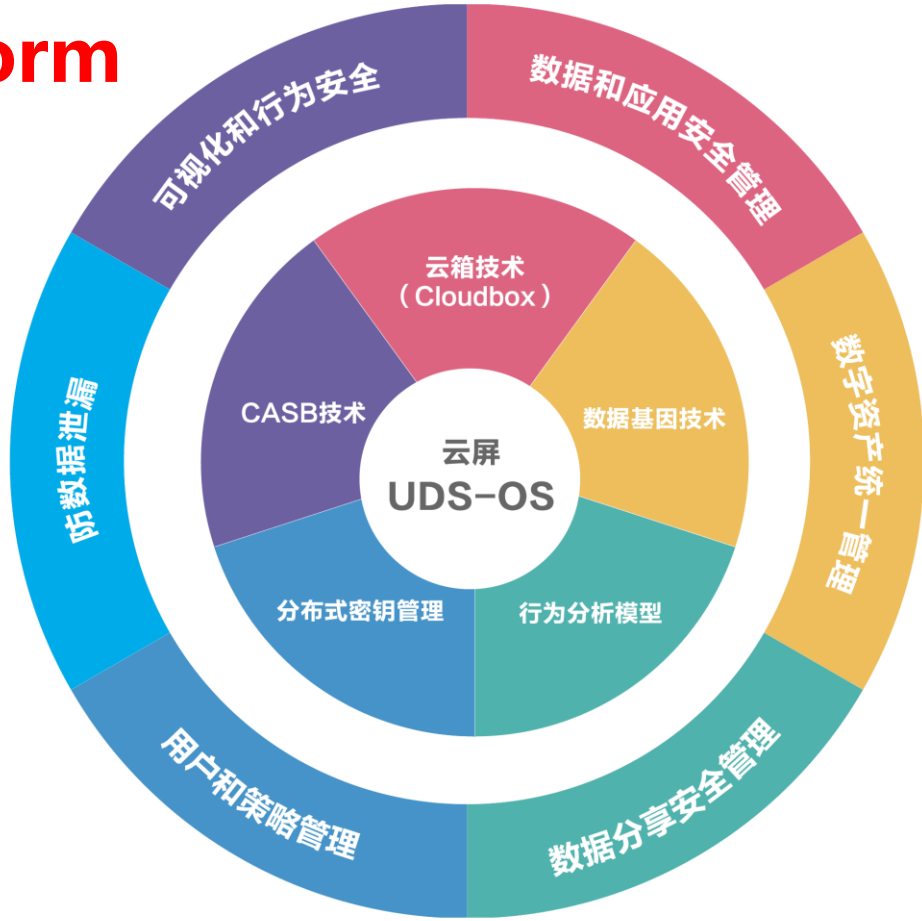
通过数据安全与网络安全建设平台联动，能够追溯，及时拦截违规行为，保障信息稳定安全

规划：数据/信息安全体系框架

构建企业数据综合防护平台 —

Unified Data Security (UDS) Platform

- 基于UDS平台建立用户行为分析模型、并采用云箱（Cloudbox）、文件基因（DNA)、分布式密钥管理加密等技术
- 从应用、数据和文件的存储、传输及使用等几个方面，为企业数据提供全方位无盲点的安全保护
- 确保在各种复杂业务场景下企业核心数字资产不被泄露和窃取
- 即便被泄露或窃取也可以有技术手段进行跟踪、追溯、取证

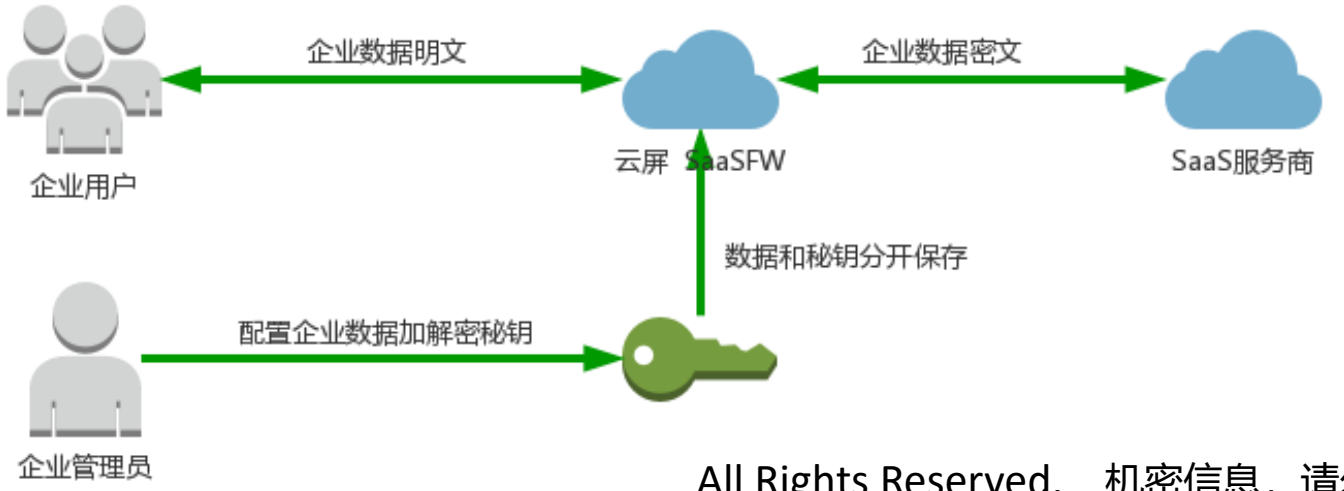


实施部署：数据/信息安全管理

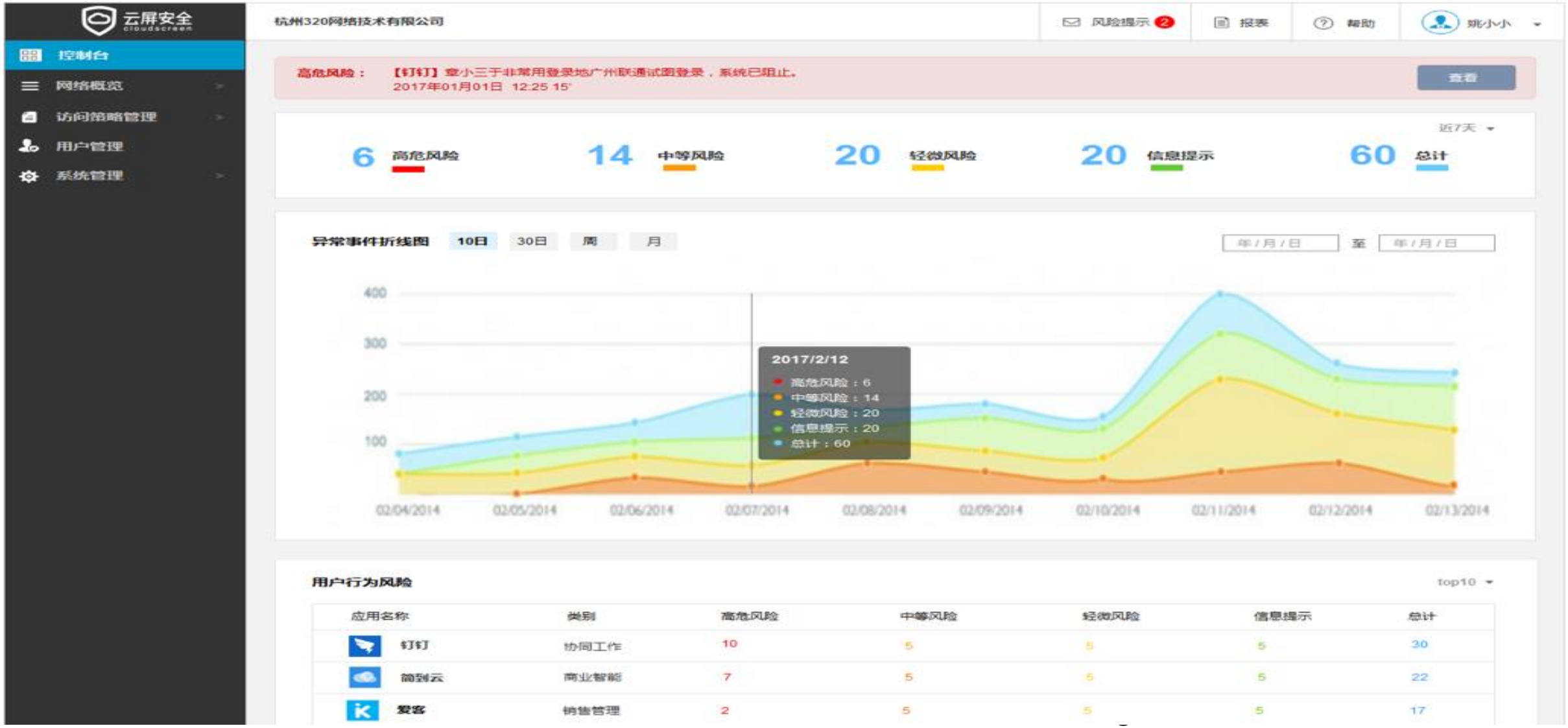
- 采用云箱(Cloudbox)、分布式密钥管理、文件基因等技术管理数据生命周期
- 追溯数据的传输轨迹，记录、归档、追踪、控制各种类型的涉密数据
- 追溯数据泄密的源头（包括人员和设备），记录各种越权或违规使用数据的行为
- 实时监控涉密数据在各种终端设备和用户帐号的分布和使用情况
- 对终端设备上的数据进行远程管控，防止在职或离职员工泄露或盗取涉密数据

实施部署：数据云端迁移及保护

- **利用某SaaSFW提供的第三方加密服务方案：**
  - 敏感信息将以密文形式存储在云端，即使被违规查看或泄漏也不会造成损失
  - 数据加密对SaaS应用透明，能正常通过SaaS应用的识别和校验
  - SH可以根据自身的安全需求，灵活指定需要加密的数据并设置秘钥
- **管理员能随时取消加密或更换秘钥，不会影响用户对数据的正常访问**



实施部署：数据/信息安全监控台



实施部署：企业数据风险可视化

企业数据安全状况

总体预览

实施部署：企业数据风险可视化

对数据的异常操作行为

进行可视化统计

实施部署：数字资产可视化

实施部署：用户异常行为监控和管理

- 实时监控和分析用户使用各种应用和数据的行为，覆盖企业的重点应用系统或SaaS服务
- 诊断、预报以及阻断各种异常行为，比如设备丢失或被盗，业务系统账号被滥，企业数据被转移到个人空间等等

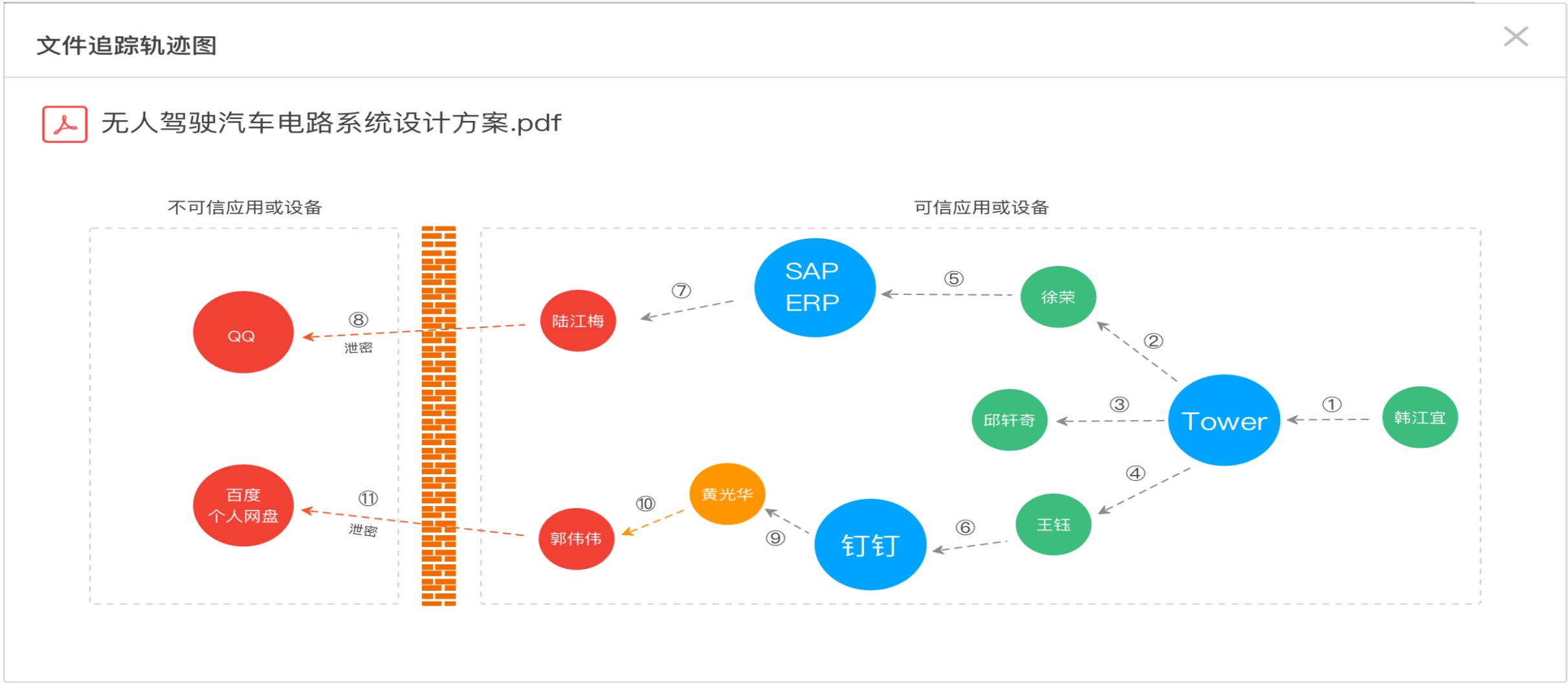
云屏高级威胁引擎

云屏安全所集成的高级分析引擎采用人工智能、大数据分析，以及态势感知和环境感知等先进技术，能够侦测用户的异常行为，并根据预设规则和动态威胁评估模型实时判断出各种用户行为的威胁，及时预警。

威胁日志

威胁名称	威胁类别	云屏账号	应用名称	用户行为	参数	时间
应用账号与云屏账号不匹配	账号异常	钟维	360企业云盘	登录	无	2017-11-09 15:24:07
应用账号在新设备登录	账号异常	钟维	360企业云盘	登录	无	2017-11-09 15:24:07
用户短时间内频繁下载数据	数据泄漏	陈晶	Tower	下载	频率： 10分...	2017-11-03 17:51:28
用户分享数据	数据泄漏	钟维	360企业云盘	分享	无	2017-11-03 17:01:17
用户短时间内频繁下载数据	数据泄漏	钟维	燕麦云	下载	频率： 10分...	2017-11-03 15:46:06
云屏账号短时间内异地登录	账号异常	姚晓峰	云屏安全	登录	30分钟内异使 ...	2017-11-03 15:39:42
用户短时间内频繁删除数据	恶意破坏	石旭	推事本	删除	频率：10分钟内	2017-11-03 15:31:55

实施部署：数据流转轨迹图



企业信息资产的保护需求凸显

内部防护是关键

规划实施全面信息安全管理

企业的资产和数据更安全