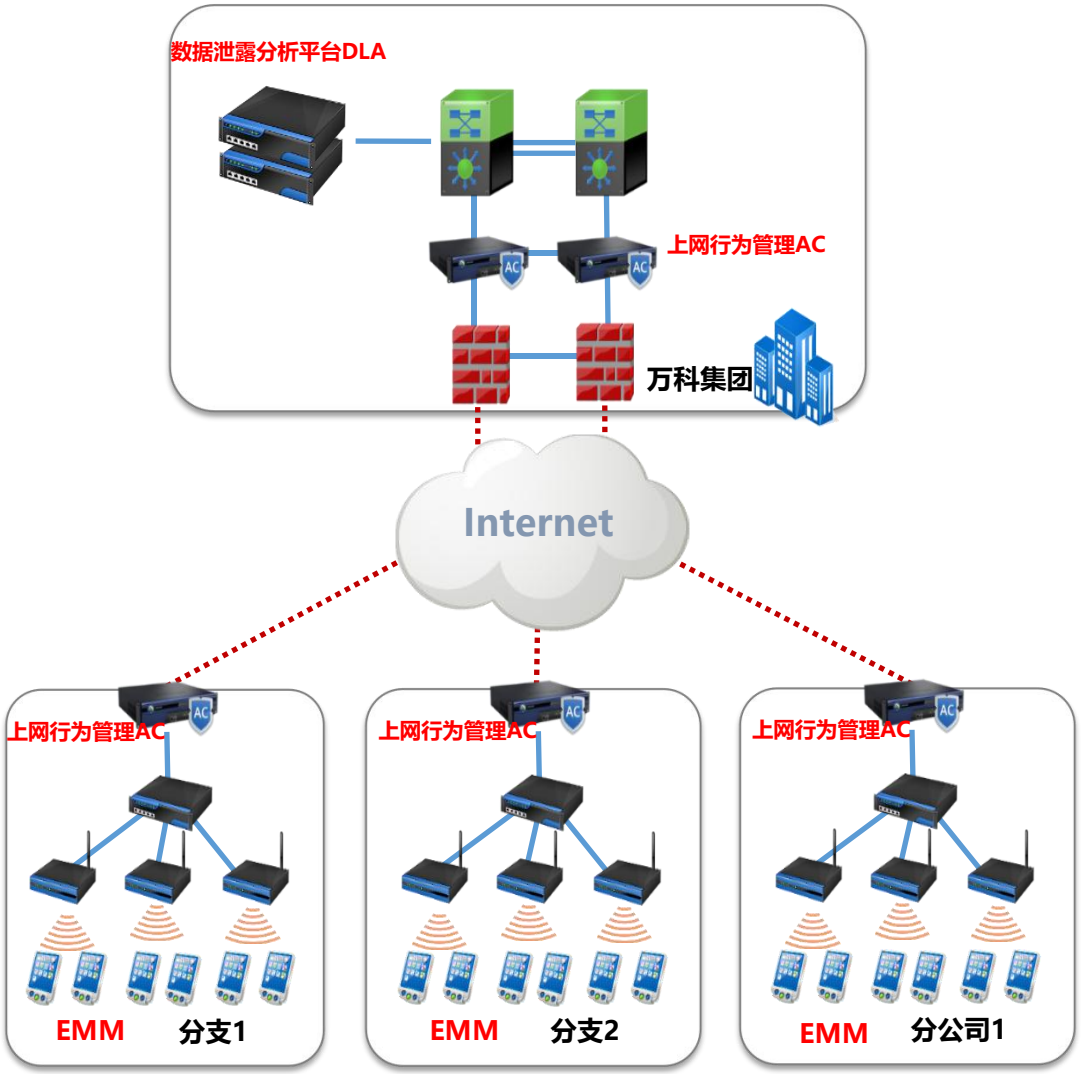
案例一：万科集团



需求背景

- 万科集团成立于1984年，在全国各地拥有多家分支机构，机密资料保护困难程度大幅上升，管理员难以发现泄密行为。
- 万科部署了McAfee的终端防泄密，但终端误判太多影响正常办公，所以退回至告警阶段，不做阻断。
- 2017年审计发现万科集团存在因QQ/微信、用户上网出口的邮件外发、网盘上传等途径数据传输的追踪分析缺失。
- 2018年发生严重泄密事件，但无法从终端层面追踪到泄密源。

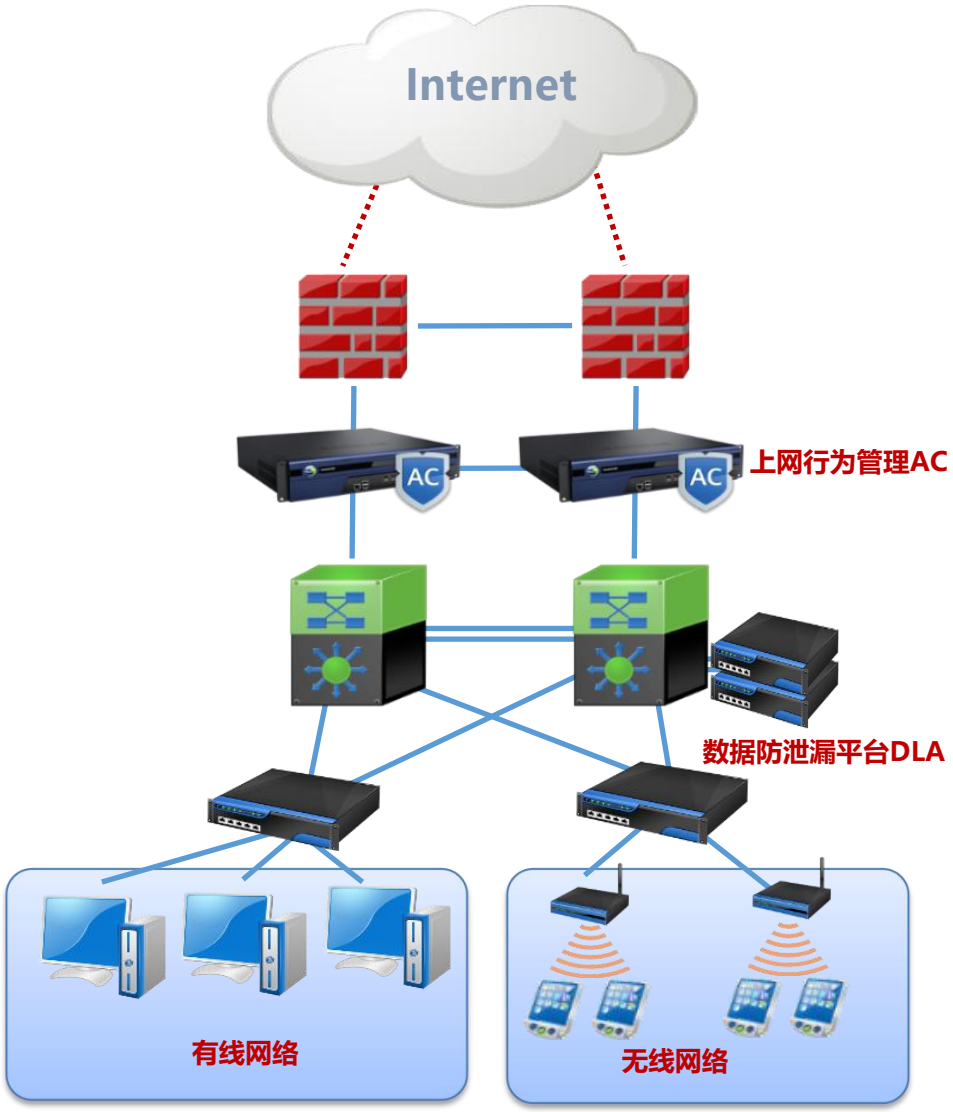
解决方案

- 在总部和各个分支机构的网络出口部署AC，移动端部署EMM，采集各个地区的上网数据并汇总到总部的DLA平台，通过DLA集群部署提高处理性能。
- DLA内置地产行业的泄密检测规则，对外发文件及信息进行泄密检测。
- 开启DLA内置各类场景及行为分析，帮助企业发现泄密风险行为，同时可以实现泄密追溯功能。针对非常重要的数据，开启阻断或者泄密邮件预警。

客户收益

- 完善防御：实现网关通道数据泄密的追踪分析，尤其是QQ/微信、邮件、网盘、云笔记的外发数据追踪分析。
- 数据审计：帮助安全管理人员掌握所有外发数据的概况
- 泄密分析：从行为及场景分析角度提高泄密分析准确性，实现AI泄密分析。
- 泄密追溯：根据关键字、段落或文件追溯到泄密员工，实现追溯压缩包内容和截屏抗抵赖。

案例二：科技部



- **需求背景**

中国科技部是是国务院的重要组成机构，有很多业务系统存储着重要的数据资产。业务人员因工作需要会接触到这些敏感数据，因此客户对互联网侧泄密有所顾虑，担心内网员工通过邮件、论坛微博、网盘等方式外发泄密。

- **解决方案**

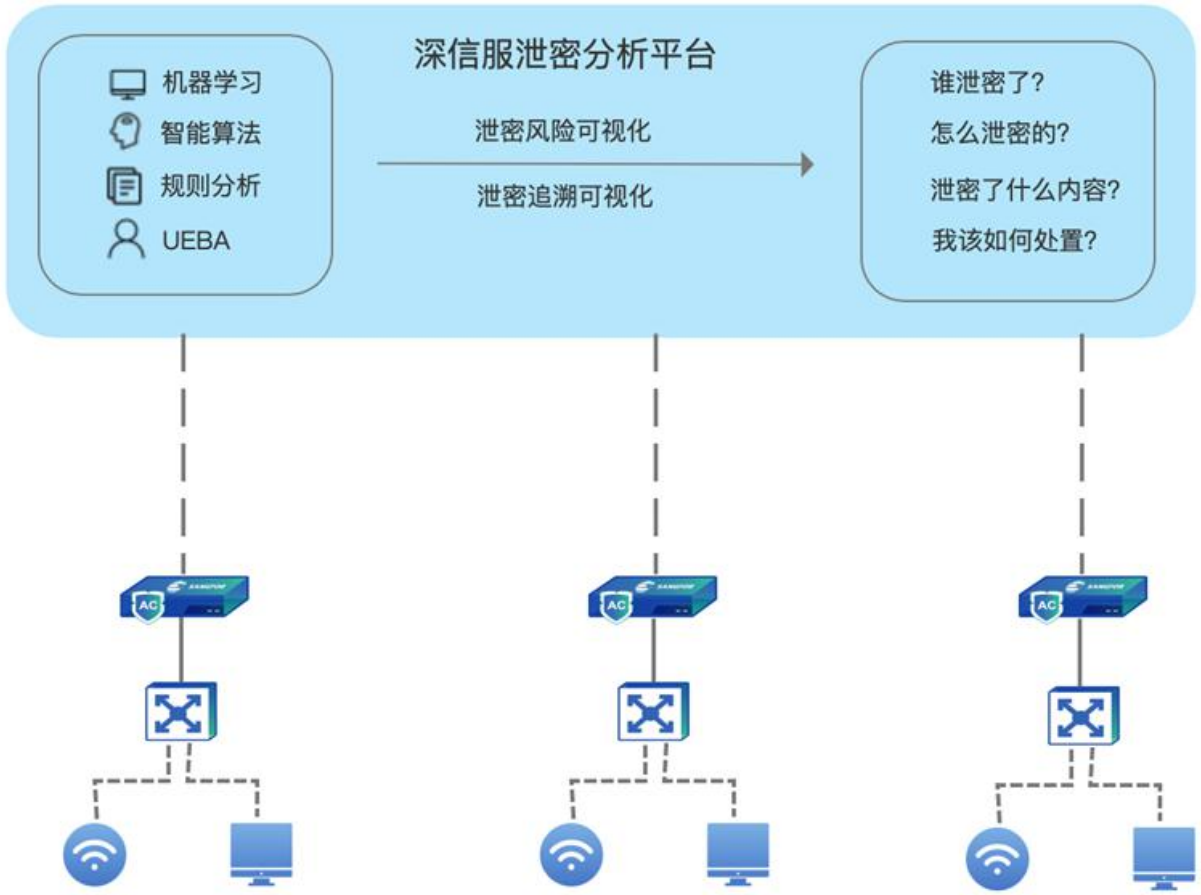
在互联网网络出口部署深信服AC，再通过深信服数据防泄漏分析平台DLA对泄密事件进行统计分析。

- **客户收益**

1.通过DLA，开启[泄密追溯分析]和应用。掌握所有外发行为，帮助科技部追溯泄密人员。

2.通过识别外发通路，对外发信息进行分类（合同资料、工程图纸等），然后通过指纹技术查找与泄密文件相似度最高的外发信息。实施测试过程中，客户将包含敏感信息的文件，通过doc、ppt、xlsx等格式的文件，采用zip压缩（多重压缩），通过webmail方式发送出去。然后取文件的一小段内容进行追溯，马上精准追溯到此外发行为。

案例三：中国太平保险集团有限责任公司



- **项目背景**

中国太平保险集团有限责任公司，简称“中国太平”。客户目前有10万用户，上网产生的数据巨大，对于这么大的数据量如果通过日志中心去做追溯和分析简直是天方夜谭，客户要求合规场景的前提下需要在发生安全泄密事件时快速定位人员，而不是大量的通过日志中心去查询，提高运维效率和质量，并且客户的分支数据也很庞大，在人员基数大，分支数量多的情况下，如何解决数据防泄密是客户建设的难题。

- **安全需求**

◆ 满足银保监的法律法规要求;

◆ 公司内部发现有员工通过IM聊天工具泄密内部资料，防泄密能力不足。

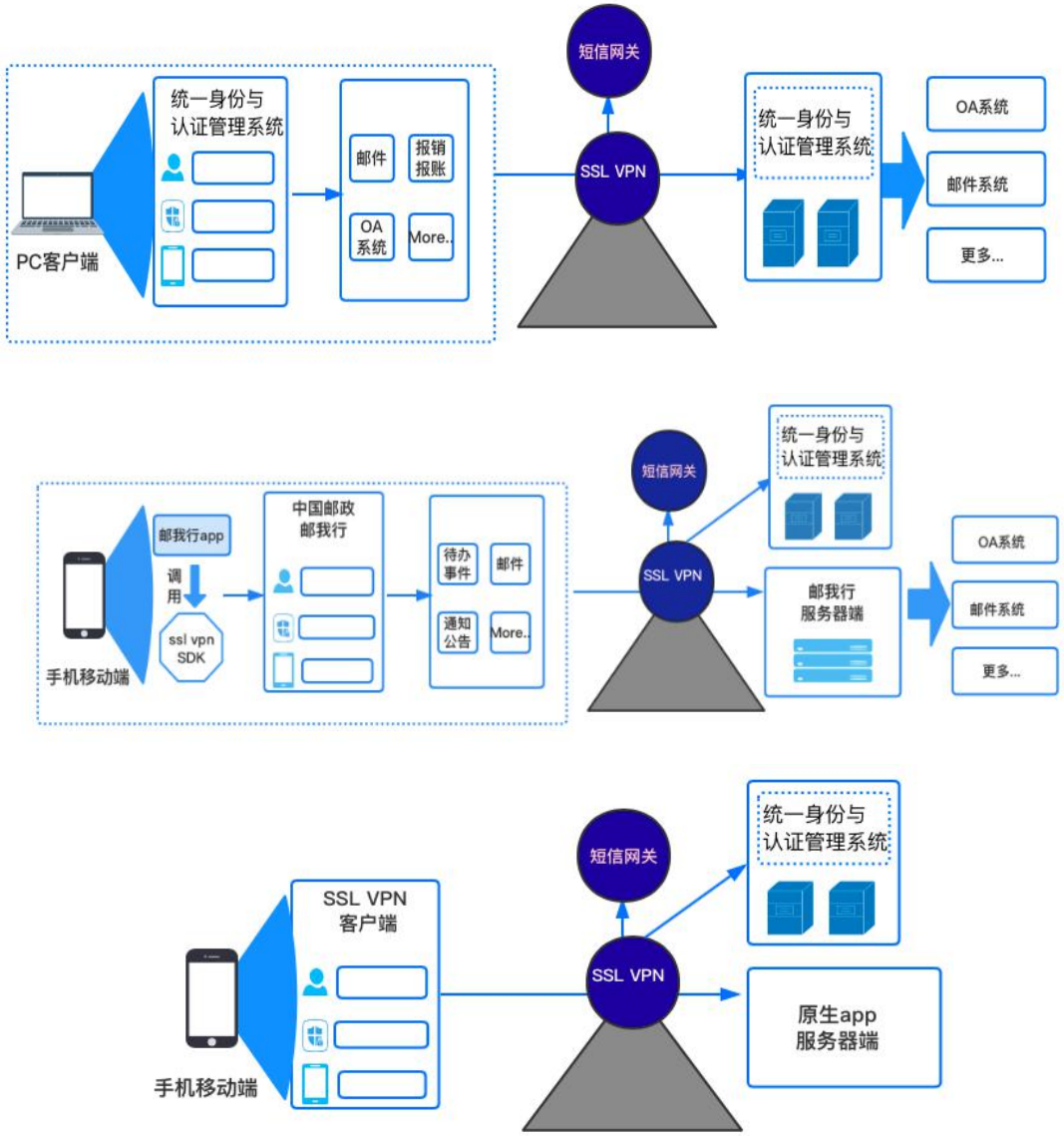
◆ 终端防泄密方案对事前的风险预警、事后的快速追溯支持不足。

◆ 在使用终端防泄密的过程中，有很多人都开放了解密的权限，导致加密解密的方案也没有用起来，方案管理难。

- **客户收益**

深信服DLA防泄密分析平台，在泄密侧的数据分析处理，支持AI智能涉密检测，提高泄密判断的准确率，符合国家网络安全法要求。

案例四：某大型国有银行全国移动办公统一接入门户项目



- **项目背景**

某大型国有银行OA系统以及其他互联网接入系统目前的安全防护措施需要提升。在技术调研与评估的基础上，借鉴其他大型央企的相关做法和先进经验，制定本方案，切实提升集团公司互联网生产管理、办公管理等系统的安全性。

- **解决方案**

◆ 系统入口从互联网接入移至SSL VPN接入。

◆ 统一接入门户：业务系统接入统一身份与权限管理。

◆ PC端外网办公接入 ：通过WEB面客户实现统一接入

◆ 手机端外网办公接入：通过SDK对接实现统一接入

◆ 原生app办公接入：通过移动客户端实现统一接入

- **客户收益**

增强系统安全性： 客户端必须统一登后才能访问业务管理系统，有效避免非法用户恶意入侵行为。

增强数据传输安全性： 用户终端与内部传输过程中的数据全部加密，避免数据在传输过程被监听。