**面临的挑战**

**1.规范员工上网行为**

■如何规范员工的上网行为？

■如何防止员工IM、邮件、论坛形式主动泄密？

■如何过滤不良网站、防范资金风险及法律风险？

■如何满足银监、公安部等监管要求？

**2.防止病毒、木马造成文档被动泄密**

■如何防止员工电脑中毒或被黑客入侵，窃取资料？

**深信服解决方案**

在有独立互联网出口的总行和分支机构分别部署深信服AC设备，再通过总行部署的SC集中管理设备进行统一管理，从而实现对银行至上而下的互联网风险管理。



**管控上网权限**

实现员工职位职责与上网权限的匹配，减少越权访问和权限滥用的现象。AC强大的内容识别能力能实现基于内容的外发信息过滤，管控文件、邮件发送行为，防止泄密事件；

**过滤不良信息**

帮助管理员过滤违法、违规不良网页、含有不良关键字的网络信息，防止用户不慎访问不受信的网站带来法律风险。对于内网用户的外发信息行为，AC基于内容的外发信息过滤能帮助管理员及时拦截不良言论，最大程度的减少舆论风险给组织形象声誉带来影响；

**行为管控及审计**

实现基于内容的相关管控，对网络中的异常流量、用户异常行为及时发起告警，更有数据中心保留相关日志，风险智能报表发现潜在的泄密用户，实现“事前预防、事发拦截、事后追查”。

**客户价值**

■管控网络行为，防范泄密，保障组织信息安全；

■过滤不良信息，规避管理与法律风险；

■审计及日志留痕，满足监管要求。