文档密级：公开

应用控制技术白皮书 V0.1

信锐网科技术有限公司
SUNDRAY TECHNOLOGIES CO.,LTD.

目录

1. 技术背景

随着互联网的普及，网络应用越来越丰富，尤其随着大量社交型网络应用的出现，用户将个人网络行为带入办公场所，由此引发各种管理和安全问题。

随着移动互联网的迅速发展，网络办公日益流行，互联网已经成为人们工作、生活、学习过程中不可或缺、便捷高效的工具。但是，在享受着电脑办公和互联网带来的便捷同时，员工非工作上网现象越来越突出，企业普遍存在着电脑和互联网络滥用的严重问题。网上购物、在线聊天、在线欣赏音乐和电影、P2P 工具下载等与工作无关的行为占用了有限的带宽，严重影响了正常的工作效率。

2. 应用识别

识别是管理的基础，全面的应用识别帮助管理员透彻了解网络应用现状和用户行为，保障管理效果。

信锐无线 AC 拥有多种应用识别技术，全面识别各种应用，进而有效管控和审计。主要包括：

a) URL 识别： 信锐 AC 内置千万级 URL 库、支持基于关键字管控、网页智能分析系统 IWAS 从容应对互联网上数以万亿的网页、SSL 内容识别技术。信锐 AC 除了内置的上百种 URL 类别以外，管理员还可以自定义 URL 分组。根据组织内部特殊需求，将一些指定的 URL 划分到一个 URL 分组下，此时，各种权限策略就可以引用这个 URL 分组来做控制，满足精细化的 URL 控制需求，让企业内网管理更加灵活高效，更加满足“权限最小化”的管理原则。

b) 应用规则识别库：信锐 AC 拥有国内最大的应用识别库，该库由深信服（信锐母公司）应用规则研发团队定期维护，保证库处于最新状态；该库支持 2100 种以上网络主流应用，4500 条以上规则，能识别 106 种以上 IM、66 种以上 P2P/P2P 流媒体、254 种以上游戏、39 种以上 OA、19 种以上网银、53 种以上金融行情软件、

45 种以上金融交易软件、13 种木马、37 种以上代理软件和 470 种以上移动 APP，涵盖主流的网络应用；

c) 文件类型识别：识别并过滤 HTTP、FTP、mail 方式上传下载的文件，即使删除文件扩展名、篡改扩展名、压缩、加密后再上传，信锐 AC 同样能识别和报警；

d) 深度内容检测：IM 聊天、在线炒股、网络游戏、在线流媒体、P2P 应用、Email、常用 TCP/IP 协议等，基于数据包特征精准识别，且支持管理员自行定义新规则，以及深信服科技及时更新和快速响应；

e) 智能识别：种类泛滥的 P2P 行为，静态“应用识别规则”已经捉襟见肘，通过 P2P 智能识别技术，识别出不常见、未来可能出现的 P2P 行为，进而封堵、流控和审计。

通过强大的应用识别技术，无论网页访问行为、文件传输行为、邮件行为、应用行为等信锐 AC 都能帮助组织实现对上网行为的封堵、流控、审计等管理。

图1 信锐AC应用识别库

3. 技术价值

使用信锐 AC，管理员能依据组织架构建立用户身份认证体系，并采用分时间段、分接入位置、基于用户、基于应用、基于行为内容的网络行为控制，从而实现员工职位职责与上网权限的匹配，如限制研发部门不得使用 webmail 外发邮件、上班时间不能使用 IM 聊天工具，限制财务人员不能访问不受信网站，等等。以此减少越权访问和权限滥用的现象，防止泄密和不良舆论风险。同时，限制员工上班时间的无关网络行为，减少员工因工作效率低下带来的加班、离职、薪金浪费、额外薪金支出等问题。

此外，信锐 AC 能帮助管理员过滤违法、违规、不良网页的网络信息，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，信锐 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，或者在特殊时期采用“允许看帖不允许发帖、允许收邮件不允许发邮件”的特殊管控手段，最大程度的减少舆论风险给组织形象声誉带来影响。

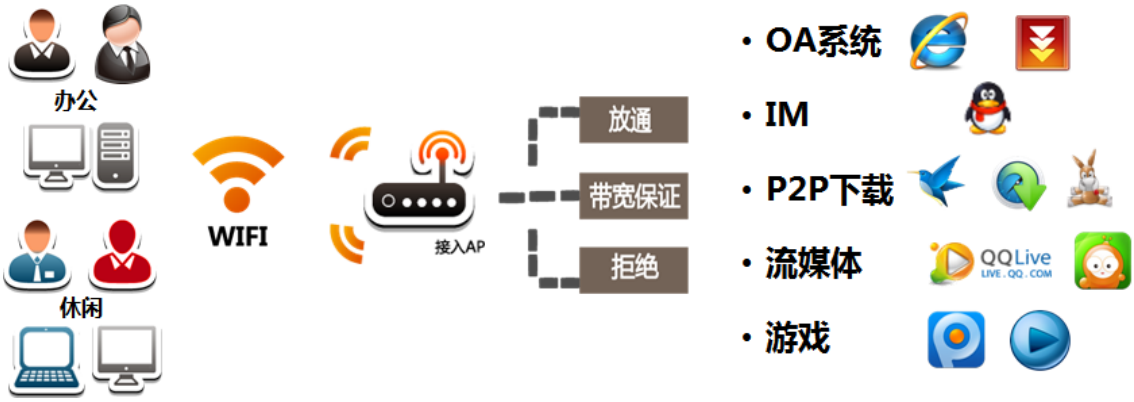

图2 精细的应用控制（缺乏时间段、接入位置、终端类型的展示）