# 行为监管软件平台

# 白皮书

杭州融至兴科技有限公司

二〇二二年九月

目录

【第 1 部分】 概述 ..... 1
1.1 背景介绍 ..... 1
【第 2 部分】 行为监管软件平台 ..... 2
2.1 产品介绍 ..... 2
2.2 产品定位 ..... 2
2.3 技术原理 ..... 2
2.3.1 总体技术架构 ..... 3
2.3.2 应用平台技术架构 ..... 4
2.4 产品功能 ..... 5
2.4.1 操作行为审计 ..... 5
2.4.2 敏感信息截取 ..... 6
2.4.3 异常 IP 分析 ..... 7
2.4.4 时间节点管控 ..... 7
2.4.5 移动介质 USB 监测 ..... 7
2.4.6 特殊字段增量监控 ..... 8
2.4.7 恶意卸载插件预警 ..... 9
2.4.8 全屏水印保护 ..... 9
2.4.9 权限分立管理 ..... 10
2.4.10 动态短信告警 ..... 10
2.5 应用场景 ..... 11
2.5.1 终端日常操作审计 ..... 11
2.5.2 恶意搜索行为 ..... 11
2.5.3 自定义增量监控 ..... 11
2.6 运维实施 ..... 12

# 【第 1 部分】 概述

## 1.1 背景介绍

随着计算机技术和互联网的快速发展，信息化已经成为我们生活工作中必不可少的元素。网络信息化不仅拉近了人与人的距离，还为各企业提供更广阔信息平台，提高了企业的竞争力，在生产和办公效率方面作出了卓越的贡献。各企事业单位对信息系统依赖程度的日益增强，信息终端安全问题受到普遍关注。

由于信息化建设、业务不断扩展等因素，在各内网信息系统中的终端及各种网络设备的不断增加，相应也带来一系列的问题：安全事件频发、工作效率降低、企业机密泄露、带宽资源浪费等。

而行为监管软件平台目的是让管理员更加清楚地掌握企业内的信息、终端行为情况，并对行为情况进行科学的统计与分析，根据状况作出相应的调控，从而规范信息终端使用情况，提高工作使用效率，更大的发挥信息化带给企业的优势。

# 【第 2 部分】 行为监管软件平台

## 2.1 产品介绍

本产品让用户单位更加清楚地掌握自身企业内网终端的信息、企业自身员工使用电脑终端的行为记录情况，并对其行为情况进行科学的统计与分析，根据状况作出相应的调控，从而规范信息终端使用状态，提高工作使用效率，更大的发挥信息化带给企事业单位带来的优势。

该系统的实现将让企业对所有计算机的使用情况了如指掌，它将是企业对信息的安全防护和技术的广泛应用而应运而生的，其功能强大的计算机监视、控制与管理系统软件，是为现代网络管理人员量身定做的管理软件。不但可以对员工电脑的屏幕、上网、聊天、邮件和文件操作进行全面的监控、记录和管理，而且还可以防止员工盗窃公司机密资料，并对员工的工作进行一个客观的评价。它可以大幅度提高企业生产效率，减少不必要的资源浪费，帮助企事业管理人员培养企事业优良风气。

## 2.2 产品定位

【行为监管软件平台（以下简称：行为监管）】

1) 本产品由杭州融至兴科技有限公司自研产品，别名：行为监管软件/内网审计系统/内网智能监督管理平台
2) 集终端电脑操作行为监管、全屏水印保护、定时可用性、操作信息溯源、自定义监控项、外部插件识别、数字证书对接等功能为一体的行为审计及综合管理系统。
3) 适用对象：各地区公检法行业、政府机关单位、运营商、工业、医院、企事业单位，有内网机密条例规定的行业，信息较为重要且不可外泄的单位等。

## 2.3 技术原理

系统平台主要分为服务端与前端。服务端可部署在云上也可部署内网。前端部署在各个电脑的信息系统上。各前端主要完成数据采集工作，按照一定校验规则进行检查，并把符合条件的数据放到相应的表中，为服务端提供数据上传。服务端从若干个前端页面接收数据，并把接收来的数据按照一定的规则加以整理、

分析并储存，最终管理员通过分析结果对企业作出相应的调整和管控。同时，在服务端上运行管理程序，通过 B/S 方式提供管理功能，保证服务良好运行。

### 2.3.1 总体技术架构

系统设计遵循松耦合、高内聚原则，对于系统基础能力和数据统一抽象成服务，通过服务总线进行统一调用，减少系统间开发和部署的复杂性，同时对应用的业务逻辑进行模块化。

#### 1） 前端

该模块为在信息终端点提取数据的程序。

#### 2） 企业服务总线

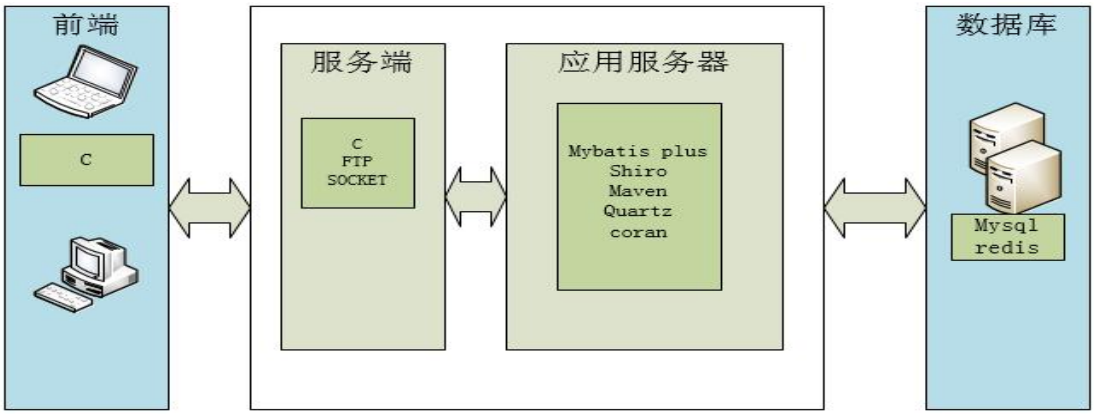
该模块为企业内的各个服务区域或者多个模块之间提供内部连接服务，针对相关项目建设管理业务，系统可以封装成服务，直接接入到企业服务总线。企业服务总线主要有以下功能：

a. 事件：通过“消息服务机制”提供以事件为驱动的服务；
b. 传递：提供通讯服务，实现同步、异步传递功能；
c. 仲裁：在传递过程中实现消息转换、动态路由以及绑定仲裁服务。

#### 3） 应用系统

该模块为用户定制的各类应用组件提供了一个基础架构和运行环境，针对相关需求管理业务，以后新的应用都可以利用以下已有的功能块进行快速开发部署。组件：提供一个运行环境或是一系列可以自动运行的程序容器，例如持续对象，关联对象，事务管理等；

a. 界面：提供一系列的服务，用来与数据库、消息系统、管理架构、其他企业级应用建立稳固的双向集成接口；
b. 核心逻辑：提供运行时服务，例如内存管理，对象实例，对象池，事件发布，目录及安全。必须是 Java、XML、消息和 Web 服务等常规编程模式的一部分。




## 2.3.2应用平台技术架构

1） 数据访问层

数据访问层包括硬件和软件。硬件部分主要包括主机系统、存储系统、安全系统及配套工程等；

软件部分主要包括数据库管理系统、应用中间件、数据集成中间件、消息中间件及其他接口等。

2） 数据存储层

主要包括基础数据库、决策分析数据库等内容。

3） 数据应用层

包括白名单管理、行为分析、文档查看、行为轨迹、监控管理。

4） 用户层

用户层是主要包括各级使用用户。

# 2.4 产品功能

## 2.4.1操作行为审计

能够有效监控用户上网操作行为、杀毒软件安装、违规软硬件安装、外部设备使用的主机安全监测与管控体系，包含基础安全、运行安全、安全检查、行为安全等功能。不但可以对员工电脑的屏幕、上网、聊天、邮件和文件操作进行全面的监控、记录和管理，而且还可以防止员工盗窃公司机密资料，并对员工的工作进行一个客观的评价。

企业网络管理员可对其企业内部成员进行管理。可自行创建菜单管理内容，分级化对用户进行管理，菜单内部可分为用户、角色、部门等各样管理分类，分类之后的菜单可以自行调整至适合自身企业规模的管理类型。可创建不同部门不同角色，将用户信息加入系统内部，可对其进行分类，便于企业管理员更好的对企业内部人员进行有效管理。

### 1） 文字录入识别

a. 聊天记录识别：用户使用终端电脑登陆聊天软件（例如：QQ、微信、邮箱等），系统将自动识别用户键盘所输入的文字信息，实时管控记录聊天内容。

b. 搜索引擎识别：用户使用终端进入任意浏览器，系统自动识别用户在浏览器内搜索的信息，记录用户所有历史操作文字内容。

用户在监控范围内的终端电脑上进行任意操作，系统自动识别用户输入的文字信息，获取文字上下文内容，形成日志保存至系统后台管理端。

### 2） 鼠标单击识别

用户在终端电脑操作时移动、单击鼠标，系统将会对鼠标的具体行动轨迹进行详细记录，并对鼠标单击瞬间图像获取，形成 JPG 格式的图像保存里系统后台管理端内部相应目录内。

如有出现操作违规行为等情况，可实现对用户操作行为完整还原，支持以图像形式查看。图像能够清晰还原，图像存储小于 5b 不会导致系统系统过多而软件瘫痪，图像保存时间默认为一年清除一次，支持弹性调整保存时间。

3） 网页端行为识别

透明地审计并管理用户的上网行为，屏蔽黄、赌、毒、邪教、黑客等不良网站，同时能够很好地满足来自信息安全市场的多种需求。提升教育形象、化解潜在的法律责任、提高企业的工作效率、营造绿色校园网络环境的目的，形成横跨多种行业的专业安全审计方案。

a. 记录终端 IP、访问网址等信息
b. 记录用户网页浏览的时间、URL 地址、标题等内容
c. 获取源目的 IP 地址、源 MAC 地址、源目的端口、网址分类信息
d. 匹配识别终端名称、使用者
e. 记录网页发帖和 BBS 发帖的内容
f. 支持常见的搜索引擎关键字抓取

4） 触发型行为审计

baidu、google 等常见搜索网站远程登录(TELNET 协议）审计文件传输(FTP 协议)审计除了记录用户文件传输的行为外，还能记录包括 BT 在内的文件传输行为。指定不允许搜索/触发的文字体系；限制用户上网行为搜索信息内容；限制用户网络聊天场景中的词汇触发。

## 2.4.2敏感信息截取

1） 敏感词监测

a. 场景一：在企事业单位日常工作中，部分用户在空闲时间，会对企业人员或其他方面产生好奇和兴趣。届时会通过网上搜索来获取自己想了解的信息。
b. 场景二：恶意员工在网络上抹黑自家企业。则会在网络上进行评论攻击，对企事业单位来说负面影响较大。

日常办公过程中，难免存在部分用户对企业好奇或不满，用户上网随意搜索关键词，管理人员无法及时发现和引导，稍有不慎会对企业造成影响或损失。本系统支持管理员设定敏感词汇（词汇数量不限），对企业用户进行敏感词监测，能够及时发现恶意员工行为，并对其进行思想沟通、诱导向善，加以及时防范。

2） 敏感网站监测

用户在日常办公时间内，搜索登陆与工作不相关网站（例如：娱乐网站、视频网站、赌博网站、病毒程序网站等），轻则会影响用户日常办公效率，工作积极性下降；重则会导致企业内部电脑被病毒攻击，大面积终端电脑瘫痪，对企业业务运行造成极大程度的影响。

3） 白名单设置

系统支持对部分用户进行白名单设置。启用白名单模式，列入白名单中用户无论搜索什么敏感词汇或敏感网站等信息，都将被系统自动过滤，不形成预警通知，处于完全信任的状态。建议对管理层用户、特殊用户使用白名单。

## 2.4.3异常 IP 分析

系统自动对监控范围内的 IP 进行实时监测，记录系统内异常 IP，并对其进行统计、查询等操作管理。防止企业部分员工使用监测范围内的终端电脑查询敏感词汇，便于企业网络管理员捕捉设备以及个人用户搜索信息，形成良好的工作环境，高效利用工作时间。

a. 异常 IP：通常指涉及敏感信息、无监控信息、信息频率过高等情况。

## 2.4.4时间节点管控

对于单位企事业管理者而言，针对不同用户的上网特殊性，可能需要对用户办公时间内的上网时间段进行限制。能够有效控制用户使用终端的时间范围，加强安全保障，实行严格管控制度。

系统支持对终端电脑的使用时间段进行管控（例如：用户在 8:00~16:00 范围内可以使用终端电脑）。支持设定时间段节点对用户使用终端进行限制，更高效管理企业内部终端设备使用情况。

## 2.4.5移动介质 USB 监测

USB 存储设备及数码设备使用的日益增多，管理员对网内用户使用 USB 设备的情况需要加强控制力度，防止未经授权的 USB 设备接入，导致内网终端重要数据泄漏。本系统实现自动识别任意移动存储介质的通过 USB 形式接入。并

通过策略分配对移动存储设备的使用进行禁用，防止了网内 USB 设备的滥用。

a. 移动端接入终端设备，平台自动识别 USB 接口信息；

b. 发现 USB 接入，终端自动禁停内网网卡，实现内外网隔离操作。

## 2.4.6特殊字段增量监控

在日常办公情况下，系统感知用户日常终端操作的情况。在某段时间内用户终端操作行为突然出现大幅度变动，系统自动认为该用户出现异常行为，立即对管理员做出预警。

### 1） 打印机使用增量

针对在职用户日常办公过程中，系统自动对所有用户每日使用打印机次数进行预估平均值（即用户 A，每日使用设备打印纸张数量≤10 张）。在任意一天内，该用户打印纸张数量超过 200 张，则系统监测到该用户行为有异常，则对管理员发出预警通知，平台记录用户预警信息。

### 2） 车辆查询增量

以公安行业为例，交管部门警员日常工作为每日大量查询车牌信息，同时有权力每日查询 200 条及以上的车牌信息。对于行政部门成员来说每日工作于此无关，如若出现行政部门成员某日查询车牌信息超过 200 条，系统自动对其行为进行预警告知。

出现此现象原因由 2 个：

a. 原行政部门成员调派到交管部门，工作职能和内容发生改变，导致该警员出现某日查询车牌信息超过 200 条。

b. 该行政部门成员个人原因或存有私心，违规查询大量车牌信息，系统自动预警。

### 3） 身份证查询增量

与上述情况相同，民政部门警员日常工作为每日大量查询身份证信息，同时有权力每日查询 200 条及以上的身份证信息。对于监察部门成员来说每日工作于此无关，如若出现监察部门成员某日查询身份证信息超过 200 条，系统自动对其行为进行预警告知。

出现此现象原因由 2 个：

a. 职位调遣，工作职能和内容发生改变。

b. 该监察部门成员个人原因或存有私心，进行违规操作。

## 2.4.7恶意卸载插件预警

系统部署完成后，需要在终端电脑设备下载一个软件插件，插件属于开机自启动，无感使用，完全不会对日常用户办公造成影响。插件存在意义：1、实时监控终端用户操作行为；2、记录录入文字信息；3、截取桌面图像信息；4、展现全屏水印等。

如若出现用户通过自身技术手段恶意卸载插件，则会导致终端电脑自动关机。并且系统会实时监测记录终端插件的存在与否，将尝试卸载插件的终端电脑进行记录预警，管理员加以制止防范，防止用户多次出现恶意行为。

a. 意外卸载：当客户端插件进程突然出现中断情况，导致终端电脑自动关机。重新开机即可正常使用。

b. 恶意卸载：当恶意人员通过技术手段想要将客户端插件卸载。终端电脑将会在 30s 后自动关机，以免造成不必要的损失。

## 2.4.8全屏水印保护

通过系统客户端插件，对接入企业内网的终端电脑屏幕进行水印展示，实现终端屏幕覆盖信息，起到防截屏、防拍照、追溯截图来源、实现版权保护的目的。

1） **水印展现方式：**

a. 设备默认展示用户终端的 IP 地址水印。

提醒员工谨慎对待机密信息，勿拍照、勿截屏，进而从根本上提升其信息安全保护意识，一旦企业组织发生数据泄露的情况，可以在短的时间内追溯数据泄露源，将损失降到最低；

b. 根据企业需求调整。

调整水印的可视度、覆盖范围、大小等，保护数据安全的同时，避免对日常办公造成干扰和影响；

### 2.4.9权限分立管理

一般情况下，企事业单位内部存在保密管理“三员”，以最小特权和权值分离为原则，将管理员分为系统管理员、安全管理员和安全审计管理员，各司其责，防止某一身份的管理员权限过大，引起安全威胁。

在此环境下，本系统支持自定义用户角色，支持权限可视范围，根据实际场景建立管理员、分配其权限。保障每个区域管理员使用不同权限互不干扰，不同管理员监管不同范围各司其职，有效保证权限合理分配。

### 2.4.10 动态短信告警

系统在触发预警的情况下，支持通过短信形式给管理员发送告警通知，实时监测终端电脑状态，及时报警。

# 2.5 应用场景

## 2.5.1终端日常操作审计

- 用户在终端的所有操作，都将被本系统监控。

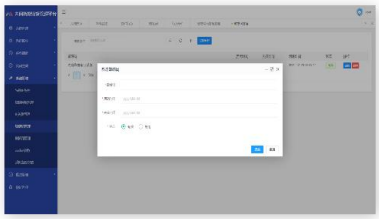
- 平台将用户操作鼠标形成的轨迹保留下来；
- 存放在本系统界面内留档。
- 平台将所获信息做分析处理；
- 系统将收集的信息以图像信息展示。
- 当某台终端出现问题时。平台可根据图像信息溯源；
- 防止业务数据泄漏。

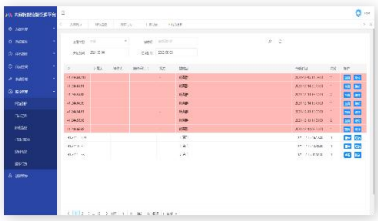
## 2.5.2恶意搜索行为

**预谋搜索**
用户通过学习时间，在终端电脑上搜索不正当词汇（例如：犯罪 等词汇）。

**系统自测**
系统通过已创建的敏感词库，对用户在终端所输入的文字进行匹配。

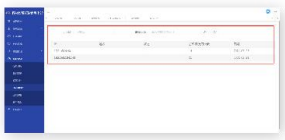
**日志报告**
若出现用户搜索敏感词，系统自动记录其输入内容的相关前后文，形成日志保存于控制端内。



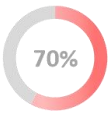


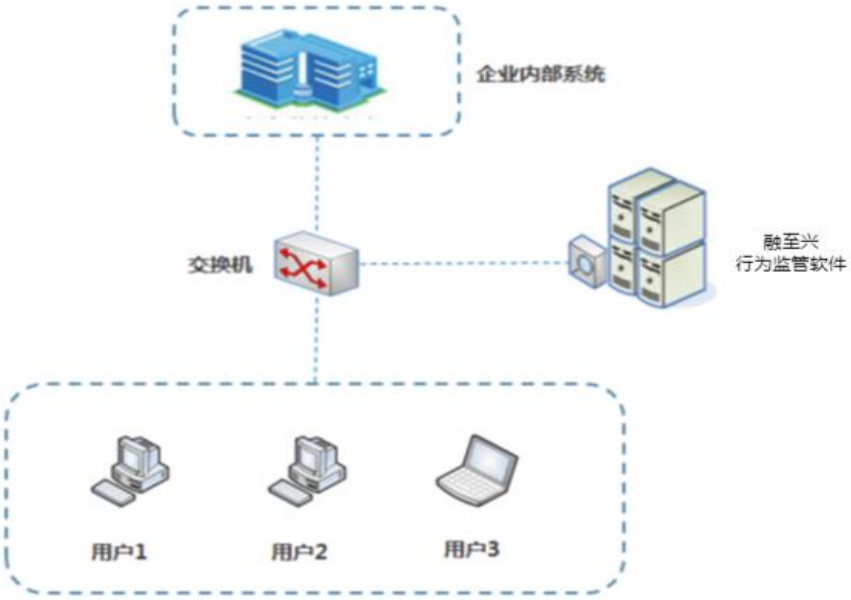
## 2.5.3自定义增量监控

**打印机队列监控**
- 记录正常情况下用户使用打印机次数、打印纸张
- 出现异常增量情况时，系统监测数据进行预警



**车辆牌照搜索监控**
- 日常办公中，特定用户工作职能为搜查车辆牌照
- 针对每日工作量进行平均记录，超出一定范围，视为情况有异常，系统出现预警
- 出现其他人搜查车辆牌照信息，则视为异常情况，系统预警




**身份证识别监控**
- 日常办公中，特定用户工作职能为搜查公民身份证信息
- 针对每日工作量进行平均记录，超出一定范围，视为情况有异常，系统出现预警
- 出现其他人搜查身份证信息，则视为异常情况，系统预警

## 2.6 运维实施