桌面管控系统

白皮书

杭州融至兴科技有限公司

二〇二二年八月

目录

【第 1 部分】 概述

1.1背景介绍

随着监狱行业信息化建设、业务规模不断地扩大，在监狱内网信息系统中的终端及各种网络设备的不断增加，随着新业务和新需求的发展，对于用户终端电脑的管理需求越来越重要。部分监狱的内网环境暂无部署保护管控措施，特别是罪犯网，建设桌面管控系统将是对内网信息安全的加固和整改，把各个终端的管理安全保护落实到点，实现信息系统的完整性、保密性和可用性。提高监狱行业的安全管理水平和安全保护能力，减少安全隐患和安全事件的发生。有效保障信息化健康发展。

1.2传统不足

常见的客户机维护和安全问题有：

1) 大量监狱机构分散，终端设备分布也非常分散，如何让少量的管理员能够完成大量、分散的设备，节省公司的管理成本是监狱部门非常关心的问题。
2) 为了保证监狱业务正常进行，当用户终端电脑发生故障时，如何快速响应问题，并分析和解决问题，能够为监狱避免因用户终端电脑故障而导致的业务损失。
3) 在用户终端电脑上，用户可以安装各种软件，为了安全，需要防范用户在终端电脑上安装病毒软件导致设备宕机情况，而做不到有效分析问题原因。
4) 用户终端电脑拥有较多的外部接口（如 USB 口、串并口等)，如何限制在智能客户端上随意接插使用外部设备，很多系统安全问题和泄密都是由于滥用外设导致的结果。

面对上述问题，由于大量监狱部门的管理人员对于计算机知识比较欠缺，很难让管理人员自行解决上述问题：公司必须要保持大量的设备/系统维护人员，在新业务上线、系统出现故障时，让维护人员到现场解决问题，不但浪费大量的人力成本，而且问题的解决效率还非常低。

【第 2 部分】 桌面管控系统

2.1产品介绍

桌面管控系统让监狱管理部门更加清楚地掌握监狱内网终端的信息、用户使用的行为记录情况，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状态，提高工作使用效率，更大的发挥信息化带给监狱带来的优势。实现监狱内网终端的主机登录统一管理、系统监控管理、行为日志审计等，保障了监狱信息系统安全稳定运行。

2.2产品定位

【桌面管控系统（以下简称：桌管系统）】

1) 本产品由杭州融至兴科技有限公司自研产品，行为监管软件/桌面管控系统/内网审计系统/内网智能监督管理平台
2) 集终端电脑一键控制、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桌面监控及综合管理系统。
3) 适用对象：各地区监狱行业、公安行业、政府机构、局域网，各行业重要监管部门，局域网/城域网/广域网等。

2.3产品功能

2.3.1终端解锁屏

1） 定时自动锁屏

在日常办公情况下，用户离开终端去其他办公区域忙于其他事情的时候，离开座位后一定时间电脑将会自动锁屏，有效防止电脑被他人误操作等等情况的出现，更加有效的保护系统内数据安全。

系统支持自定义锁屏间隔时间，用户未操作终端时，系统在该时间段内我发捕捉到用户使用终端的操作信息，即认为终端电脑处于无人使用的状态，并将终端进行锁屏操作，锁屏后需要以其他方式进行解锁使用。暴力破解会导致终端电脑自动关机，启动后仍处于锁屏状态。

2） 一键全选锁屏

对于非使用电脑的时间段内，用户离开桌面（例如：每日午休时间、午饭时间等），管理员可实现一键锁定终端电脑屏幕，实时管控电脑使用情况。

主要意义：

1、省电。终端电脑屏幕大且亮度高，是消耗电量的主要部分，一键锁屏可以及时让电脑处于待机状态；

2、安全。在用户离开桌面的情况下，一键锁屏可以阻止他人进入终端电脑窃取机密文件、操作违规行为、恶意破坏程序等行为。

3、方便。一键锁屏减少了不必要的操作，另外单位内存在恶意用户，一键锁屏可以有效防止用户在非使用电脑的时间段内对电脑程序造成破坏。

3） 一键全选解锁

所有用户均需要在规定时间内使用终端（例如：监狱内部，罪犯在规定时间内需要进行网上学习），系统支持管理员一对多方式管控用户终端电脑，后端选择用户实现一键解锁所有用户终端电脑，解锁后即可正常使用。

主要意义：

1、减少电源键使用频次。软件直接控制终端电脑锁屏，减少电源键使用频

次，避免电源键因频繁使用而损坏。

2、操作方便，软件插件开机自启，无需过多登陆操作，无感使用更方便快捷，随时在桌面上实现一键锁屏控制。

4） 批量选择锁屏

部分用户已完成学习进度、恶意操作电脑等状况时，系统支持管理员批量选择部分用户进行终端电脑锁屏操作。保障终端电脑安全，不受恶意用户违规操作；保障终端实用性，根据终端使用需求进行针对新解锁和锁屏。

5） 批量选择解锁

部分用户需要集中使用终端电脑时，系统支持批量选择部分用户进行屏幕解锁操作。合理利用资源，管控方式更为严谨。

6） 手机短信验证解锁

a. 场景一：管理员不启动统一解锁管理模式。系统支持用户根据终端使用需求进行短信验证，自行解锁。
b. 场景二：管理员由于特殊情况无法及时对电脑进行解锁。系统支持用户根据手机短信验证进行解锁使用。
c. 场景三：后台处于维护/更新期间内，无法对终端电脑进行统一管控。系统支持用户自定解锁使用终端。

手机短信验证实现姜终端操作行为溯源定位到“人”，有效保障终端电脑内部信息和资源安全。大大减少终端被恶意破坏、用户故意泄漏数据时，管理员束手无策找不到操作之人的困扰，更有利于单位内部对数据的合理管理和使用。

7） 特定密钥解锁

a. 场景一：管理员设定使用密钥解锁模式。支持用户使用统一的密钥进行所有管控范围内的屏幕解锁。
b. 场景二：由管理员统一进行解锁屏管理模式下。发现某台终端电脑处于掉线情况，无法被后台管控时，管理员可以通过密钥进行解锁。

如场景一情况，则密钥解锁后的终端可以被用户正常使用。如场景二情况，

则管理员通过密钥解锁之后，终端处于未被监控状态 30s 后自动关机。待终端重启之后，本产品插件自启动重新对终端进行控制。

2.3.2操作行为记录

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。

2.3.3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。

2.3.4异常 IP 分析

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。

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。

2.3.5时间节点管控

对于监狱管理者而言，针对不同角色用户的上网特殊性，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。

2.3.6外来设备监测

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。

2.3.7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。

2.3.8数字证书联动

针对政府单位所开设的此功能，由于公安、监狱等部门的特殊性，每位在职用户均有特定数字证书/UKey 等证明身份的认证标志。本平台支持对警员的数字证书与桌面管控系统做对接。

1） **实现效果：**

a. 终端插入警员数字证书，则屏幕自动解锁，正常使用。
b. 系统自动识别数字证书用户身份，记录用户使用本机操作时间段。
c. 针对用户在终端的一系列行为操作将会被保存记录。
d. 系统建立数字证书与终端数据关联，审计数据归纳到民警数字证书名下。

2.3.9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。

2.3.10 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。

2.3.11 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；

2.3.12 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。

2.4产品特点

1） 功能完善

实现大量电脑终端统一管理，由服务端统一解锁主机，监视、管理一切终端使用行为，帮助管理人员控制和管理对终端电脑的使用。具备相应终端行为监控和审计功能，功能齐全。

2） 两端搭配

前端、服务端两部分，前端在电脑安装插件，负责数据采集、上传；服务端负责数据归集、分析、预警和展示。

3） 自动运行

终端插件程序采用 C++语言开发，自动隐藏程序，对电脑运行无影响。

4） 可控性高

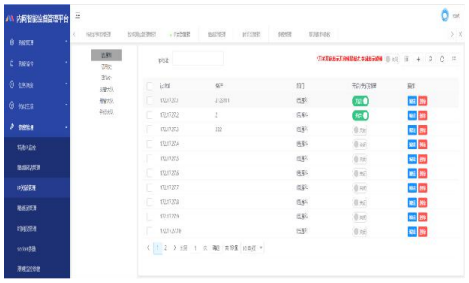
实时监测终端用户的行为操作，能够快速、全面的监控异常 IP 的情况，罗列、统计异常数据，提供直观的监测结果。

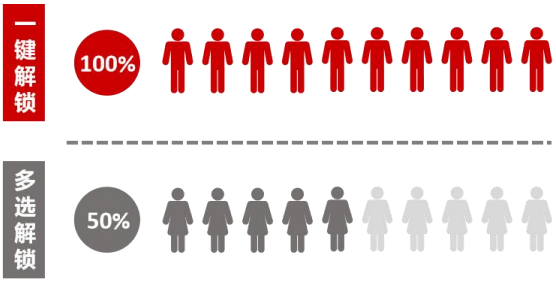
5） 维护方便

本产品全面由我司项目实施人员进行部署配置。警员日常操作使用过程中如遇问题，可以快速联系我司开发人员做定向调整。

2.5应用场景

2.5.1终端桌面解/锁屏控制





锁屏控制

在规定时间内，用户需要登陆终端电脑进行线上操作；
管理员通过控制台实现终端电脑一键解锁、或选中部分电脑实现批量解锁操作；
实现终端一对多进行实施操控、有效管控机房内设备情况。

2.5.2长期不使用,终端自动锁屏

用户正常使用

用户在正常情况下，使用终端电脑进行操作。
系统默认终端被使用，不对其进行定时锁屏。

用户停止使用

用户在正常情况下，不对终端电脑进行操作。
系统默认终端电脑处于未使用状态，在一定时间后自动锁屏。

2.5.3视频学习,终端不上锁

1 **用户使用终端进行视频学习**

- 用户在规定时间内，通过终端电脑在线观看教学视频；
- 终端电脑检测到用户未使用终端电脑。

2 **系统监测屏幕判断用户行为**

- 系统未检测到鼠标或键盘的使用；
- 系统自动对屏幕播放行为进行监测，若监测音频正在使用，则默认用户在使用终端，不对其进行锁屏；
- 反之，终端屏幕上锁。

总结

通过以上用户学习视频的场景分析，从桌管系统的监测方式切入点：

1、用户不使用终端：用户在不接触鼠标、电脑的情况下，系统在一定时间后将自动上锁；
2、监测方式：系统通过监测屏幕使用情况，对用户终端使用情况做出判断，判定是否在正常使用终端电脑；
3、实现效果：用户在进行网上视频学习时，系统不会出现锁屏现象；除视频学习外，长时间不操作电脑，系统自动锁屏。

2.5.4合理时间段管理

正常时间

1、用户在规定时间段内学习，终端电脑解锁后可直接使用；

2、使用过程中的行为操作将被系统自动记录下来。

非正常时间

1、非规定时间内，终端一直处于锁定状态，不能被解锁使用；

2、用户在非学习时间段内使用终端电脑时，电脑不能被解锁；

3、管理员可以自定义使用时间，支持设定多段时间节点。

2.5.5恶意搜索行为

预谋搜索

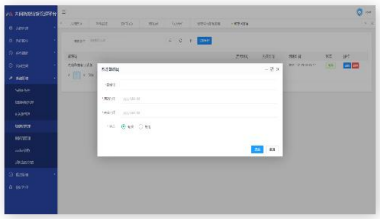
用户通过学习时间，在终端电脑上搜索不正当词汇（例如：犯罪 等词汇）。

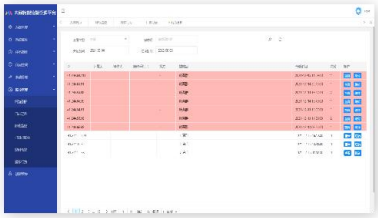
系统自测

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。





2.5.6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。

- 平台将所获信息做分析处理；
- 系统将收集的信息以图像信息展示。

- 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。

- 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。