上海艺赛旗软件有限公司
Shanghai i-Search Software Co.,Ltd

桌面行为分析（v2021.2.0）产品白皮书

Centralized Desktop Analysis

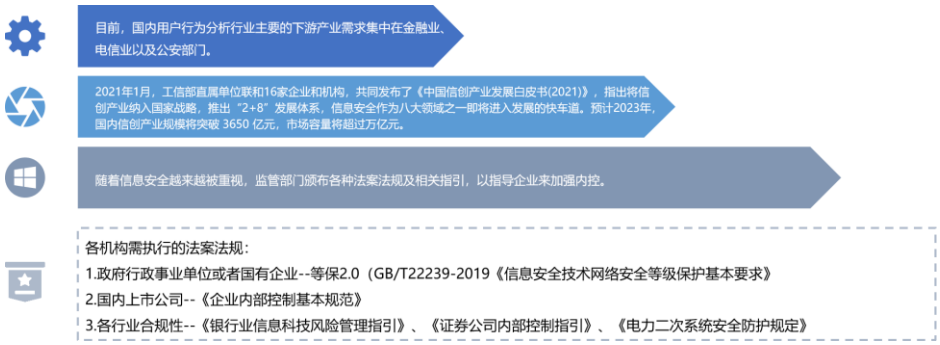
目录

1、了解 CDA

1.1 CDA 市场需求

随着信息技术的快速发展，越来越多的企业加入数字化转型大军，每个企业都在期待着数字化带来的业务创新及效益提升。一方面，企业在不断探索提高工作效率和协作的方式；另一方面，企业内部面临的数据泄密威胁也日益严重。

据统计，80%的信息泄露事件是由于内部或内外勾结造成的。如何防范业务纠纷，提升风控管理水平？如何提升业务操作效率和服务质量，节约成本？如何发现异常行为，有效防止和追溯敏感信息泄露及违规操作？这些都对企业的员工行为监测与管理工作提出了更高的要求。



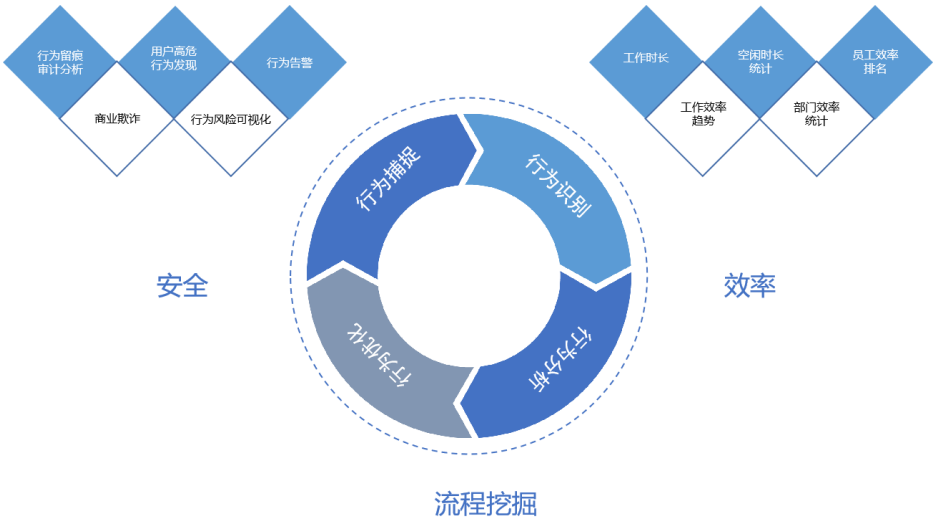
2021 年 1 月，工信部直属事业单位“中国电子学会”联合 16 家企业和机构，共同发布了《中国信创产业发展白皮书（2021）》。该白皮书首先分析了信创产业的发展背景，在全球产业从工业化向数字化升级的关键时期，中国明确提出“数字中国”建设战略，以抢占下一时期的技术优先权。但 2018 年以来，受“华为、中兴事件”影响，我国科技尤其是上游核心技术受制于人的现状对我国经济持续高质量发展提出了严峻考验，为了摆脱这一现状，国家将信创产业纳入国家战略，提出“2+8”发展体系，信息安全作为八大领域之一即将进入发展的快车道。预计 2023 年，国内信创产业规模将突破 3650 亿元，市场容量将超过万亿元。

此外，随着安全性和标准化越来越被重视，国家监管部门于 2019 年 5 月发布了《网络安全等级保护办法 2.0》，指导企业加强内部信息安全管控。在国际上，Gartner 在 2020 年发布的八大安全风险管理趋势上指出，组织对隐私风险的担心日益增加，无论是数据泄露导致的罚款、客户流失还是品牌名誉损失，说到底都是企业经济的损失。Gartner 预测，到 2022

年，核心行为审计分析技术将出现在 80%的威胁检测和安全事件响应解决方案中。因此，保障客户的敏感信息不被泄露，将成为企业不可忽视的重要工作。

1.2 什么是 CDA?

桌面行为分析（Centralized Desktop Analysis，简称 iS-CDA）是上海艺赛旗软件股份有限公司自主研发的用户行为分析管理产品。iS-CDA 通过可视化录屏、用户行为数据化和基于大数据的智能行为分析，真实全面的记录“人”的操作行为。用户的每一次点击，每一次按键，都不会错过。



- 安全

iS-CDA 在连续不间断录屏的同时，采集丰富的行为文本日志，并对日志进行自动化处理与分类，生成索引，便于快速检索。同时，通过 iS-CDA 的告警功能，可以进行危险行为的实时监控与告警通知，实时洞察员工异常行为。管理者和审计人员在 iS-CDA 系统中可输入指定内容快速检索终端桌面上的行为动作，并可定位跳转告警关联的录屏回放，对用户行为进行详细的安全审计与回溯。

- 效率

iS-CDA 也可以通过对用户的行为数据采集与统计分析，直观动态的展现员工的工作时长、空闲时长、出勤天数和应用/网页使用情况等信息，并可对不同员工、部门进行横向对比，从而帮助管理者实时了解团队的工作情况，发现员工技能瓶颈，有效的评估员工工作量，提升员工工作效率。

- 流程挖掘

iS-CDA 基于用户的行为录屏和日志，提取有价值的业务节点，通过事件分流与属性转

换，挖掘出最具重复性、价值性的业务流程序列并生成业务流程图，详细地分析业务操作流程，最终生成 RPA 工程。流程挖掘一方面帮助企业实现业务流程的发现、合规和改进；另一方面通过流程定义功能快速回溯企业真实业务环境，通过截取关键动作，灵活绘制完整的业务流程图，并支持导出流程定义说明书，帮助企业缩短业务流程调研时间，降低调研难度，加快企业自动化转型。

iS-CDA 系统是垂直领域的分析者，无论是从数据获取到数据分析，从数据梳理到数据模型构建，还是从得出结论到流程挖掘，都自成整套体系，全面真实的对用户桌面操作行为进行分析跟踪，从而帮助企业防范信息泄露，避免商业欺诈，提高客户服务质量和员工工作效率，加快企业自动化转型。

1.3 iS-CDA 的价值及优势

1.3.1 iS-CDA 的价值

iS-CDA 可以从人的行为层面捕获和分析，给安全团队带来独特的视角和能力，iS-CDA 的价值主要体现在发现未知、增强安全可见、提升能效、降低成本四个方面，具体内容如下：

- 发现未知

iS-CDA 可以帮助安全团队发现企业内部隐藏的威胁。通过行为录屏和日志记录终端用户的每一次桌面操作，实时监测用户危险行为，通过定量统计和分析全部危险事件，防范企业内部威胁。

- 增强安全可见

iS-CDA 可以监控所有账号，无论是特权管理员、内部员工、外包团队、合作伙伴等均可监控，应用角色广泛。同时，支持对终端进行离线录屏，无论是终端断网还是机器移动到公司网络外等情况，均能进行录屏和日志采集，保护性更强。CDA 将业务中不易被察觉的风险暴露出来，帮助管理员及时做出安全管控，从而避免企业遭受更严重的安全损失。

- 提升效能

录屏和日志关联播放，可以极大地缩短安全事件调查时间，提升审计效率。同时，iS-CDA 可以全面的记录业务人员操作活动，比如应用使用详情、打开的浏览器网页等，及时发现低效员工进行纠正，提升员工工作效率。

- 降低成本

基于专利录屏技术，可在 WEB 端进行录屏回放，实现员工操作行为快速回溯，简化事故调查和根因分析，缩短调查时间，降低安全事故耗费的调查工时，以及外部咨询开销。全新的流程定义功能，通过截取录屏中的关键动作，灵活绘制完整的业务流程图，并导出流程定义说明书，快速回溯企业真实业务环境，帮助企业缩短业务流程调研时间，降低调研难度，加快企业数字自动化转型。

1.3.2 iS-CDA 的优势

- **可视化录屏**

专利录屏技术，存储占用低至 10M 每小时。基于桌面变化进行完整和连贯的录屏，精确记录用户操作，同时录屏支持一键定位回放。会话录屏具有法律效力，可以为商业纠纷和回溯提供有效证据。支持用户的实时监控，实时掌握用户行为动向。

- **丰富的行为采集能力**

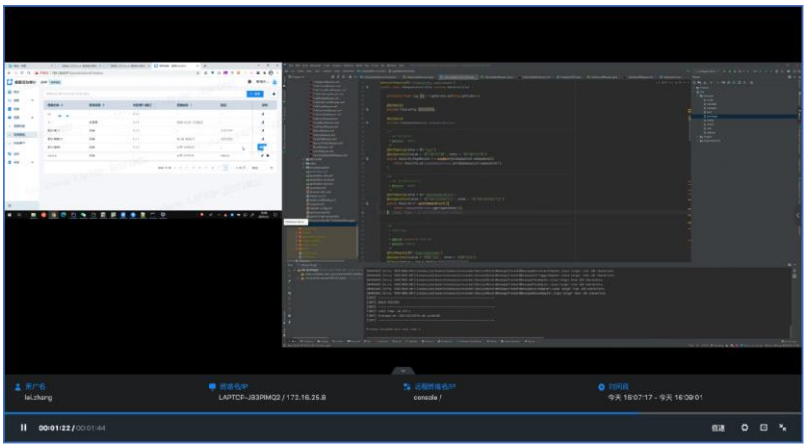
支持丰富的行为数据采集，包括键盘事件、鼠标事件、网页行为、文档操作、移动设备的插入和拔出、IP 地址修改、远程连接、运维工具操作行为等。采集的行为生成可视化的数据和文本，并进行自然语言化处理，可以快速检索和审计，可读性强，并且和录屏关联。

- **行为日志自然语言化**

由于 iS-CDA 采集的行为日志丰富，且生产环境产生的日志数量巨大，因此系统将日志进行归类和自然语言转化，直观显示了“用户在什么时间、哪台终端、做了什么动作以及关联的网址和窗口标题”，大大提升了日志可读性和检索便捷性，提高审计的细粒度，满足企业的业务部门、运维部门、客服部门等多种特定应用场景的需求。

- **多屏录屏审计**

支持多屏录屏审计，满足当前办公环境要求，帮助企业进行全面的安全审计。



- **风险行为告警与分析**

iS-CDA 根据事前定义的告警规则，实时监控、智能检测用户在浏览网站、发送电子邮件、复制文本信息等业务行为中存在的恶意活动，以及系统服务发生异常状态的现象，及时发出告警通知，以便通知相关人员采取措施，以免造成不必要的损失。

- **工作效率分析**

基于行为采集数据，提供强大的行为分析能力，帮助管理者掌握部门\员工工作效率，发现异常行为，并且可以统计部门员工工作量。通过行为数据的采集和分析，提供员工工作时长、空闲时长及占比统计，有效提升员工工作效率。

- **运维行为分析**

基于丰富的运维日志抓取能力，记录服务器工具、数据库工具和 FTP 工具操作的详细信息。通过全程的操作行为录屏和操作命令文本记录，实现全程定点审计，同时生成运维报表，分析服务器工具、数据库工具和 FTP 工具的登录、使用和执行命令情况。

- **流程挖掘能力**

iS-CDA 可以连续全面的记录每一次真实业务操作步骤，这完全满足了流程挖掘技术对数据的初始化要求。通过对数据的发现、合并、转换与提取，结合事件重复度的统计，iS-CDA 可生成简洁的业务流程图，便于用户理解。同时 iS-CDA 支持将其导出为 RPA 工程，方便用户的最终使用，加快企业自动化转型。

其中，作为流程挖掘能力的一个展现，流程定义功能基于录屏回放，快速回溯企业真实业务环境。用户可通过截取录屏中的关键动作，灵活绘制完整的业务流程图，并导出流程定

义说明书。从而帮助企业缩短业务流程调研时间，降低调研难度，实现流程自动化调研工作的降本增效。

- **国产化适配支持**

随着经济全球化的趋势不断深入，信息安全问题日益突出。自主研发操作系统，事关国家安全和市场利益，却一直是国内科技产业的短板。在国内市场，操作系统领域卡脖子的问题日益突出，拥有具有独立技术知识产权的 pc 终端、移动终端操作系统的呼声愈发强烈。针对以上问题，iS-CDA 率先进行国产化 UOS 操作系统适配的研发工作，且已完成了主流程适配，旨在扩大国产化操作系统的应用生态，让更多的企业共享降本增效红利。

- **低资源消耗**

被监控桌面上运行的 Agent 程度对资源的消耗保持在低水平，对 CPU 内存和带宽的占用都超小（约为 1-2%和 10M），且终端无感知安装与升级，完全不影响正常业务行为。Agent 具有防卸载功能，需要使用卸载口令才可卸载或停止。

- **智能搜索引擎**

将 ELK 搜索引擎技术应用到企业日志检索中，iS-CDA 会把采集/接收的所有源数据自动处理并提供统一搜索入口。用户可像使用普通搜索引擎一般，直接输入关键字、时间、业务信息等条件，对海量数据进行快速便捷的搜索。

录屏回放结合行为日志进行操作行为分析，提高的审计操作的可行性，使搜索更加快速和便捷，在此基础上可自定义报表、视图及搜索条件等，帮助审计人员高效完成审计工作。

- **多平台支持**

全面支持 Vmware、Citrix 等主流云桌面平台，支持 Windows Xp、Windows Server2003、Win7、Windows Server 2008、Win8、Windows Server 2012 等全系列的 Windows 操作系统。同时经过 Citrix、华为等云桌面厂商严格的融合测试，验证了 iS-CDA 良好的兼容性，获得测试厂商的官方认可，结成了战略合作关系。

- **桌面水印功能**

iS-CDA 通过屏幕动态水印，水印主体为当前账号信息，震慑手机拍照或截屏操作行为，防范、震慑手机拍照屏幕信息行为。当发生数据信息外泄时，结合水印账号和 iS-CDA 日志和录屏回放功能，迅速定位责任人并提供追责依据。

- **录屏和日志数据自动清理功能**

为了便于磁盘空间数据释放，新增数据维护功能，可根据需要自动清理保留天数以外录

屏和日志数据，减轻运维压力，降低因存储空间不足导致的录屏丢失风险。

- **应用场景众多**

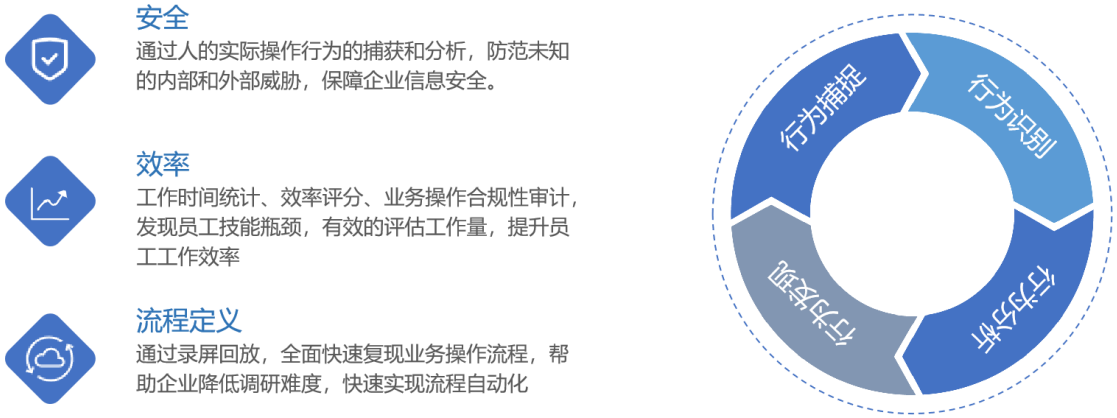
可满足众多应用场景的需要，为客户提供多方面核心价值的提升。通过 iS-CDA，可以对客服中心、营业网点、操作中心、运维开发、外包团队等人员的工作过程实现高效而详细的分析，检查工作流程是否符合业务规范，评估操作是否熟练，最终提升工作质量和效率。也可帮助 IT 系统进行安全防范，发现相关人员的高危敏感行为，防止数据泄露，尤其在保证第三方人员的行为安全可控方面，iS-CDA 可发挥良好作用。

- **满足安全规范要求**

满足 SOX、ISO 27001 等级保护标准和银监会相关规范等多种行业标准和安全规范，对信息系统中操作风险的监控上都做了明确要求，iS-CDA 将帮助企业在 IT 建设上更好地满足标准和规范要求。

2. 产品简介

iS-CDA（Centralized Desktop Analysis）即桌面行为分析。CDA 通过可视化录屏、用户行为数据化和基于大数据的智能行为分析，真实全面的记录“人”的行为，帮助企业防范信息泄露，避免商业欺诈，提高客户服务质量和员工工作效率。CDA 的主要有三个核心功能点：安全、效率以及流程挖掘。



- 安全

通过人的实际操作行为的捕获和分析，进行行为留痕审计、防范数据泄密、高危行为告警、防范商业欺诈和异常行为发现，从而防范未知的内部和外部威胁，保障企业信息安全。

- 效率

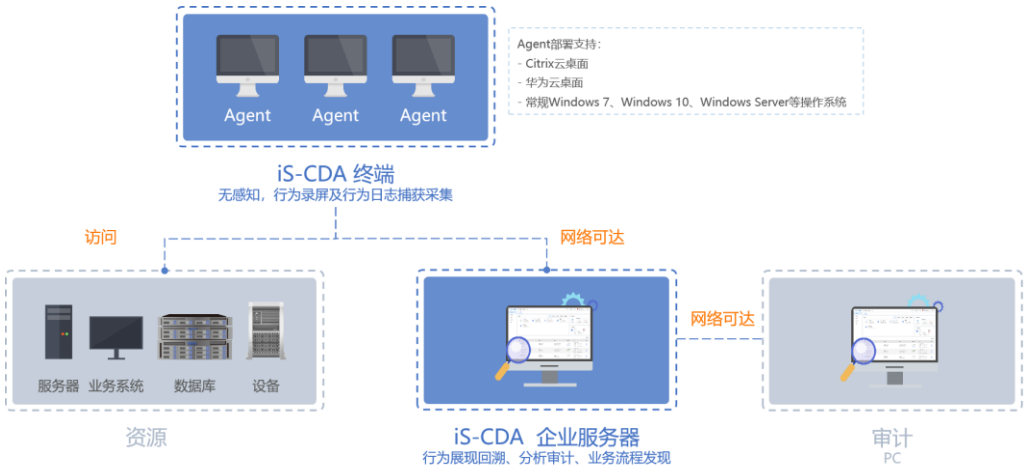
CDA 可对员工进行工作时间统计、效率评分、业务操作合规性审计，有效的评估工作量发现员工技能瓶颈，提升员工工作效率。

- 流程定义

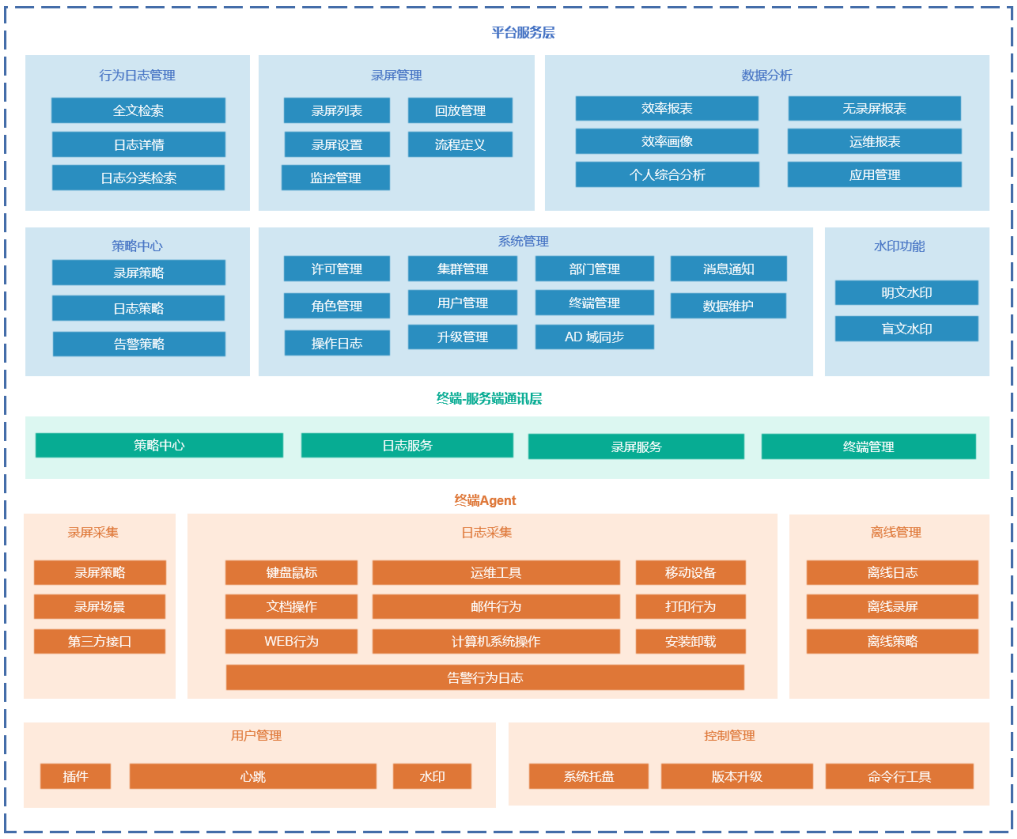
通过录屏回放，全面快速复现业务操作流程，帮助企业降低调研难度，快速实现流程自动化。

2.1 产品模块

产品由三部分组成，分别为终端、企业服务器和资源。iS-CDA 首先通过部署在桌面的代理程序（Agent）来完成用户操作行为的屏幕录制及采集，然后将生成的录屏和采集的日志在服务管理平台进行集成、关联匹配和统计分析。管理者可在服务平台直接查看这些数据，也可以将相关数据输出到大数据分析系统中进行分析，并且根据管理需要随时调取直观可信的录屏及日志进行回溯审计。

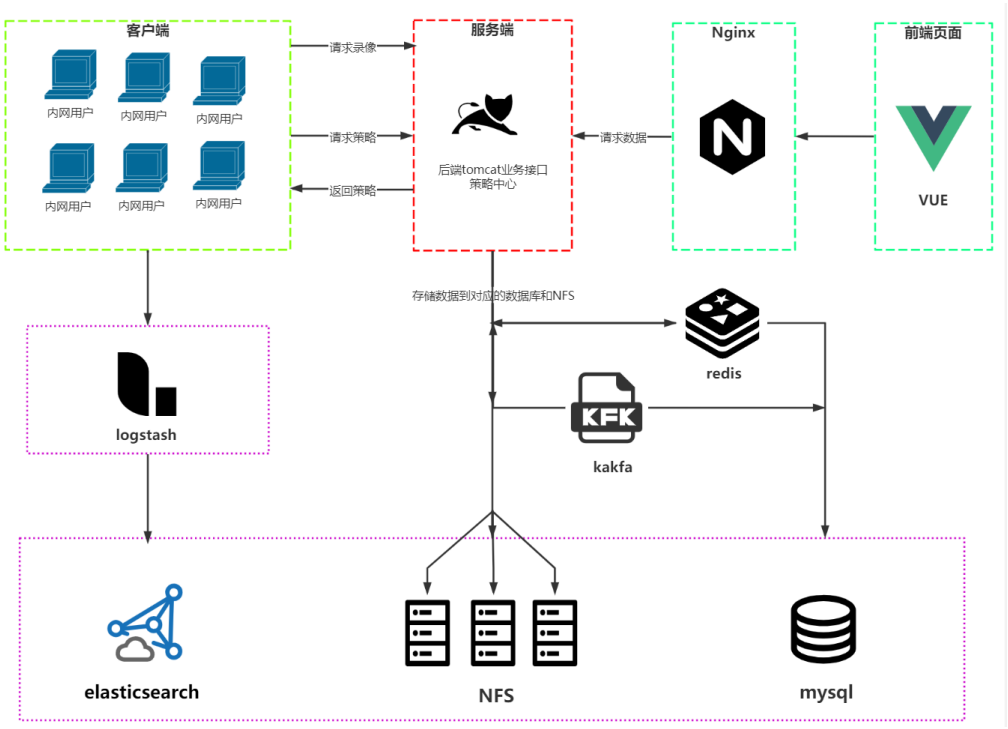


2.2 功能架构



- 平台服务层：提供强大的日志检索能力搜索、效率分析、告警分析、流程定义和报表功能，保证基础的大数据使用能力；提供完整的录屏－日志级别的展现，录屏和日志关联展现；提供专门的应用行为日志展现，直接展现经过针对性优化分析的、可读性较强录屏和自然语言化日志文件；提供流程定义功能，
- 终端－服务端通讯层：提供统一的数据接收、存储、分析、管理平台，提供全面数据接收发送能力，包括接收录屏、日志并进行数据集成，下发录屏策略、告警策略和录屏服务，提供完整的系统管理能力，包括分布式系统管理和终端管理等；
- 终端 Agent 功能层：基于下发的录屏策略，实现录屏和日志采集，支持黑白名单和细粒度的日志获取策略，支持 CPU 平缓化、网络平缓化、批量传送、断点续传、离线录屏和控制管理等能力。同时，根据服务端下发的告警策略对终端用户的行为进行实时监控，一旦触发告警规则，则会根据指定方式进行客户端通知、站内信通知和邮件通知。

2.3 技术架构



系统设计采用了支持分布式部署的 ELK 设计架构，ELK 是 Elasticsearch、Logstash、Kibana 的简称，这三者是核心套件。此架构搭建简单，易于上手，具备分布式部署的能力，具备强大的日志收集、分析、过滤、存储能力，以及亿级数据量的快速检索能力，高效地满足行为审计和回溯的需要。终端将采集的录屏和日志发送至 Logstash，由 Logstash 进行过滤、收集、处理等工作，Elasticsearch 进行日志存储和分析，最终 Kibana 提供可视化界面，进行相关日志及视图报表的数据展现。前端使用轻量级框架 VUE，实现了前后端分离的框架模式，提高系统整体页面响应的同时也提升了系统易用性和操作体验。通过 Nginx 以 Https 协议作为统一对外出口。同时，Kafka 和 Redis 的集成可以加强系统性能，提高系统并发速度。

2.4 环境要求

系统硬件配置要求

系统资源配置	服务器	终端
内存要求	32G	内存占用：180M
CPU 要求	16C	CPU 占用：0.45%
本地存储要求	500G	-

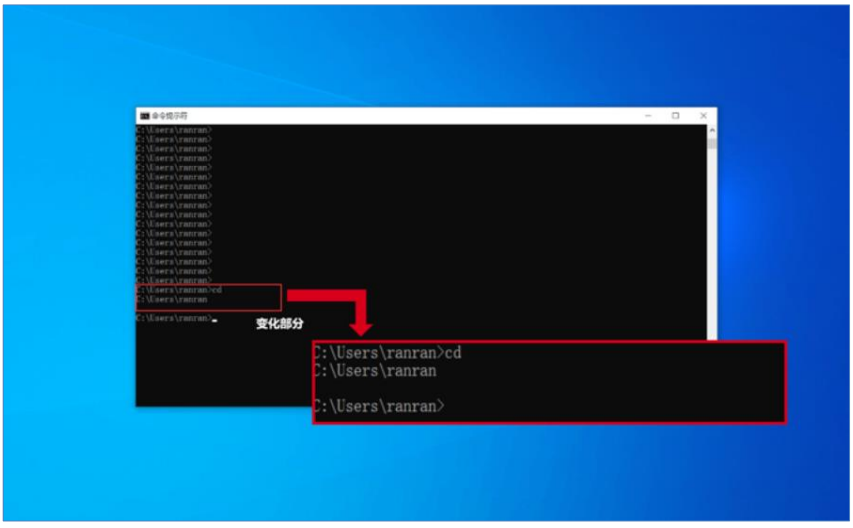
操作系统要求	Centos7 （64 位）	Citrix 云桌面、华为云桌面、Windows 7、Windows 10、Windows Server
浏览器	-	IE、Chrome、FireFox、Microsoft Edge

2.5 产品功能

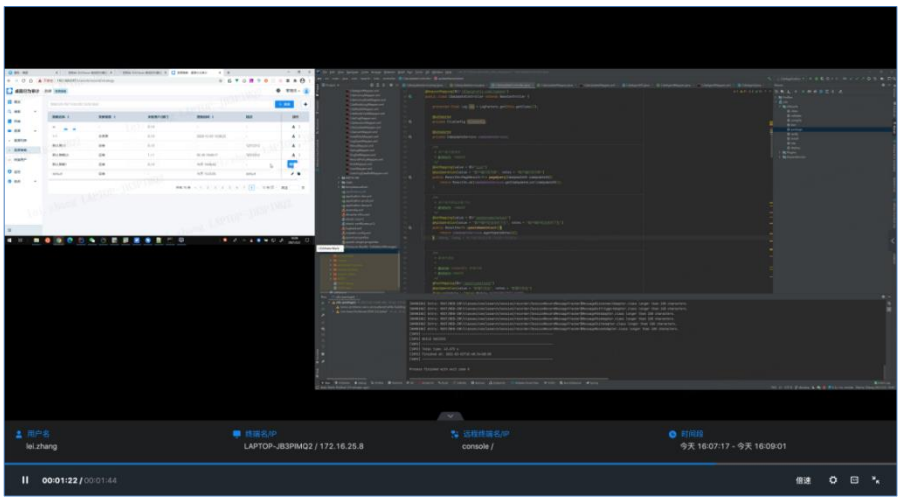
2.5.1 行为录屏及回放

2.5.1.1 专利录屏技术－完全满足合规审计要求

通过对用户桌面操作的完整录屏，全面真实的记录用户每一次操作，且录屏具有法律效力。iS-CDA 采用基于变化录屏原理，并且针对商业及字符应用特别优化了压缩算法，使用自有文件存储格式，并针对视频拖拉优化了索引。由于专利录屏技术的使用，比一般基于全屏截取的录屏软件，储存资源消耗可以减小 50-200 倍。基于变化的录屏示意图如下所示：



此外录屏时可以设置高低画质，在满足安全要求基础上，最大程度节省录屏存储占用。同时 iS-CDA 支持录屏记录，可满足当前办公习惯和环境要求。



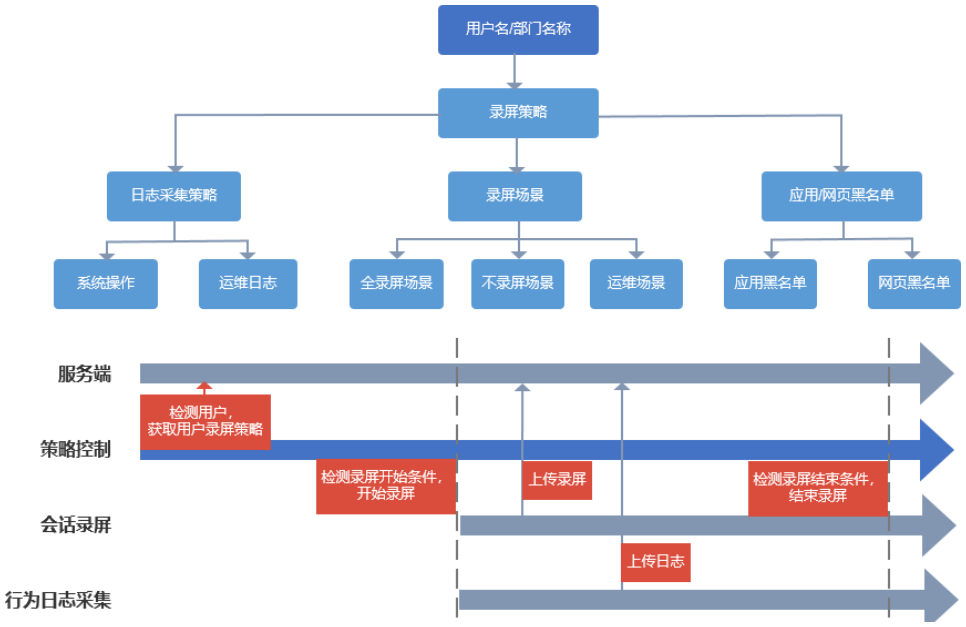
2.5.1.2 灵活的录屏策略配置

（1）根据场景设置录屏策略

通过灵活的录屏策略配置，完成对不同用户/部门的录屏设置。可以选择不同的录屏场景：运维场景、全录屏场景、不录屏场景，结合应用/网页黑名单的配置，可以满足针对指定的人员/部门、操作工具、应用和网页等进行单独的触发录屏或者不录屏。具体有：

- 运维场景：有操作动作时触发开始，无操作动作时即行停止；
- 全录屏场景：从登录到退出的全程录屏；
- 不录屏场景：从登录到退出的全程不录屏；
- 应用/网页黑名单：指定应用/网页不录屏。

如下图所示；



（2）根据用户和部门授权录屏策略

录屏策略配置完成后，可以按照用户和部门进行录屏策略授权，以满足管理员对不同用户和部门的录屏需要。

iS-CDA 根据配置的录屏策略，以会话录屏的形式整合所有采集的数据，并对每个会话录屏标识用户名、所属部门、终端名/IP 地址、远程终端名/IP 地址、录屏持续时间、日志数等摘要信息，便于搜索统计。

（3）离线录屏

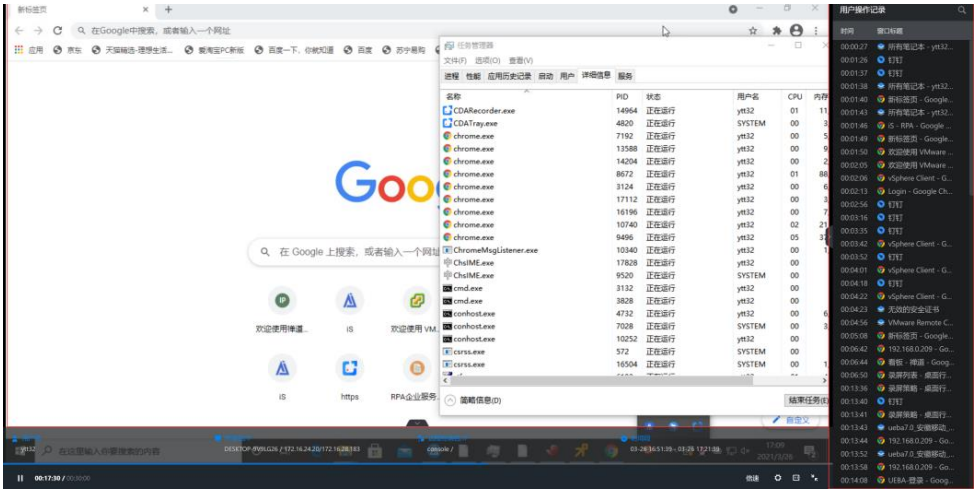
当终端与服务器通讯异常时，可正常对终端用户进行录屏并在通讯恢复后将本地录屏文件上传至服务器，同时也可以设置本地文件存储容量和上传方式，避免终端离线后无法录屏导致的数据丢失问题。同时，可设置离线文件上传的方式和时间，较少工作时间带宽占用，合理使用网络资源。

2.5.1.3 录屏回放

管理员或审计人员可直接在 iS-CDA 的 WEB 管理页面中在线观看录屏回放，无需另行

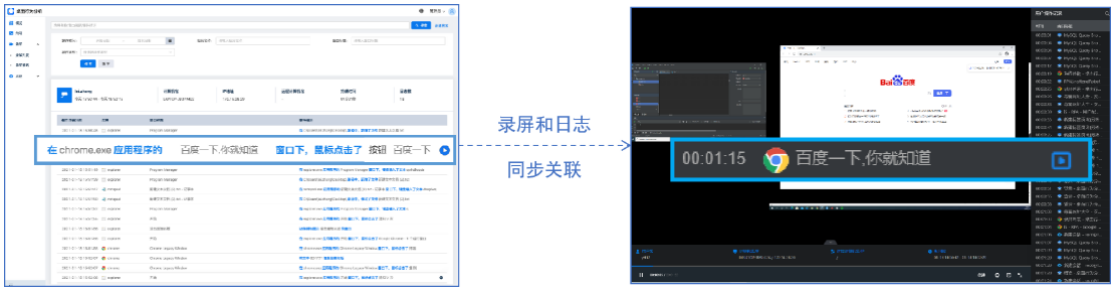
安装播放器，回放中鼠标点击事件会高亮标识，支持 HTML5 播放，简单方便。录屏播放操作栏具有滚动条、暂停、多倍速播放等常规录屏播放功能，支持相对时间、绝对时间的切换，支持一键截屏，也可以选择适应浏览器窗口大小的播放，或者 1：1 原始大小的播放。

录屏回放界面如下图所示：



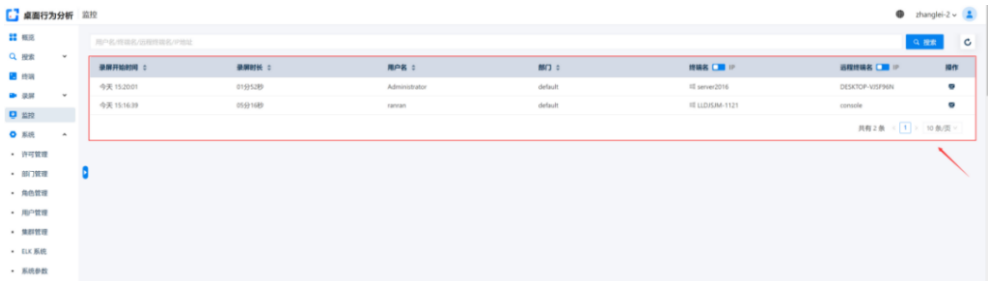
2.5.1.4 行为关联及高效审计

iS-CDA 系统把海量的录屏数据和丰富的行为文本日志进行同步关联，相当于为长时间的录屏配置了索引，在录屏回放窗口右侧栏显示录屏对应的行为文本日志，使用可视化的方式解决了录屏时间较长，无法快速检索日志的问题。同时在日志的查看窗口，可一键定位跳转至日志关联的录屏回放，直接定位播放日志显示的操作画面，较少审计时间，极大地提高了审计效率。



2.5.1.5 实时监控

可以对正在录屏的会话进行实时监控，实时查看正在录屏用户的实时操作画面，便于实时掌握员工工作情况。



2.5.2 行为日志采集

2.5.2.1 操作行为采集

iS-CDA 可采集丰富的行为文本日志，详细记录终端桌面上用户的每一次行为，例如打开的窗口标题、打开的文件名、键盘输入的内容、鼠标点击的内容、USB 的插入和拔出、文件的复制删除等操作。除了基础数据，iS-CDA 还可深入应用/网页中抓取更丰富的用户行为日志。

采集的行为日志主要有：

- 网页操作

iS-CDA 对网页上的操作行为进行采集和分析，使网页操作具备可见性，充分掌握用户的网页操作行为，防止公司信息泄露。iS-CDA 记录了用户的用户名、计算机名、IP 地址和浏览网页的时间、网站 URL、窗口标题等信息。

- 运维工具

记录运维工具、数据库工具和 FTP 工具的详细信息。通过全程的操作行为录屏和操作命令文本记录，实现全程定点审计。

a.运维工具：记录 cmd 的命令及回显，记录 putty、Securecrt 访问服务器的地址、访问协议、登录用户名和执行的命令内容及回显；

b.数据库工具：记录 plsql、sqlplus、Navicat 访问数据库的地址、实例名、数据库用户名、执行的 sql 命令内容及回显；

c.FTP 工具：记录 FlashFXP、filezilla 登录服务器的地址、用户名、文件的上传下载、删除、重命名等动作，记录 FTP\SFTP 协议下的文件传输。

- 文档操作

通过更改文档的名称或进行拷贝移动也是常见的文件泄密手段之一。iS-CDA 通过监控文档的重命名或新增、修改和删除行为，防止文档的泄密或丢失。

- 移动设备

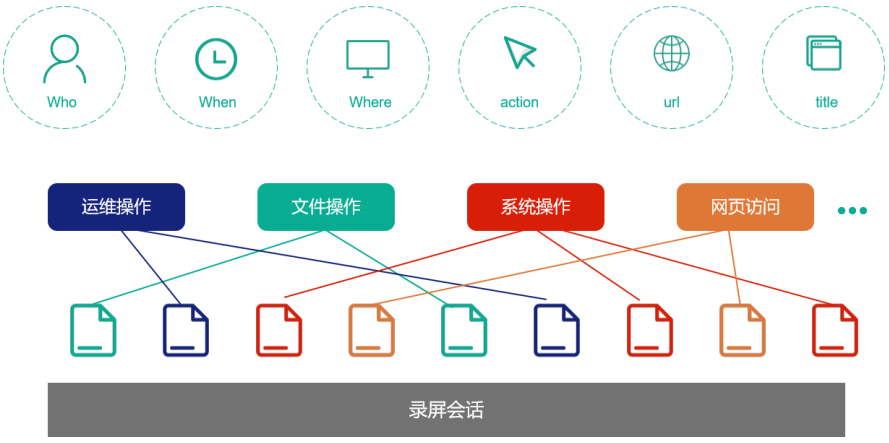
通过记录 USB 设备的插入、拔出和移动设备中的文件操作，监控文件泄密行为。

- 打印行为

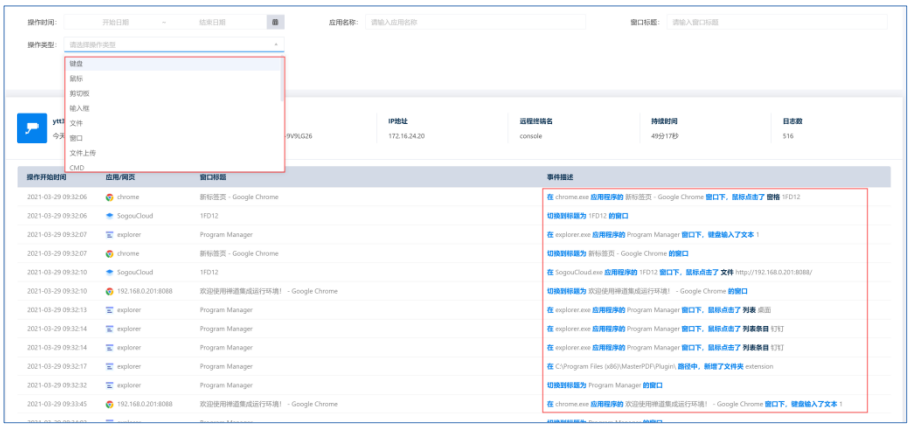
通过采集打印机的名称、IP、打印的文件名称，记录用户的打印行为。

2.5.2.2 自然语言化的行为文本日志

由于 iS-CDA 采集的行为日志丰富，且生产环境产生的日志数量巨大，因此系统将日志进行归类和自然语言转化，直观显示了“用户在什么时间、哪台终端、做了什么动作以及关联的网址和窗口标题”，大大提升了日志可读性和检索便捷性，提高审计的细粒度，满足企业的业务部门、运维部门、客服部门等多种特定应用场景的需求。



iS-CDA 的自然语言化处理后效果如下：



2.5.2.3 搜索引擎

iS-CDA 对终端的行为日志进行收集、过滤，提供了一个分布式的全文搜索引擎，支持亿级数据量的会话检索，可自定义视图，生成 dashboard，帮助用户高效地完成安全审计工作。

搜索界面如下图所示：

- 实时分析的分布式搜索引擎，支持亿级数量会话检索；
- 搜索结果自动分类，单条件、多条件联级检索；
- 支持基于索引字段进行汇总统计，并可以基于统计添加字段条件；
- 支持快速时间选择，默认统计最近 15 分钟，可选择多个自定义的时间段，支持相对时间和绝对时间，支持自动刷新搜索；
- 支持事件趋势柱状图，自动产生近期事件趋势图表；
- 支持事件详细信息的查看，支持从事件开始回放视频；
- 搜索条件和结果可以进行保存，便于下次使用，也可以用于创建新的视图和搜索；

- 支持自定义视图，生成 dashboard，数据展现方式直观丰富。

2.5.3 安全管控

作为一款终端桌面监控安全软件，实时保护企业信息安全，敏感信息不被泄露是 iS-CDA 的主要及重要职责。针对终端安全管控，iS-CDA 推出了告警、数据脱敏以及水印功能，多维度保护企业敏感信息，具体内容如下：

2.5.3.1 风险告警

在日常工作中，CDA 根据事前定义的告警规则，实时监控、智能检测出用户在浏览网站、发送电子邮件、复制文本信息等行为中存在的恶意活动，以及服务系统异常的情况。针对风险行为和服务异常发出告警通知，以便相关人员及时采取措施，以免造成不必要的损失。

（1）灵活的配置告警规则

iS-CDA 可以根据不同的工作场景，灵活的自定义告警触发条件，以规范员工的桌面操作行为。iS-CDA 支持的具体告警事件类型有：

告警类型	模块	具体内容
系统风险	主机运维监控	主机磁盘占用、主机 cpu 使用率、主机内容使用率
	集群运维监控	节点磁盘占用、负载情况、节点离线
	许可	许可数量、许可有效期
行为风险	操作系统行为	防火墙状态修改、IP 地址修改、系统时间修改、Mstsc 远程连接桌面
	键盘按键记录	支持记录用户对特殊键和组合键的使用

	复制文本内容	检测用户剪切板复制文本的内容，如：身份证、手机号或其他关键词
	文件操作行为	检测用户对文件的新增、修改、删除、重命名、复制操作
	移动设备挂载	检测用户插入或拔出 U 盘或移动硬盘的行为
	浏览器行为	检测用户访问网站的 url
	应用行为	检测用户安装、卸载或运行指定应用的行为
	邮件客户端行为	针对邮件主题、收件人、抄送、密送、附件、正文内容进行检测用户发送邮件行为
	打印行为监控	针对打印的文件名称进行检测用户是否打印违规文件
	DBA 运维工具使用	检测用户是否访问敏感服务器或数据库，或使用特殊账号访问，以及检测用户执行的命令内容是否违规
	主机执行 CMD 命令	主机执行 CMD 命令内容监控

- 系统风险：监控服务系统的主机内存、集群负载、许可不足等异常情况，防范服务系统运行异常。
- 行为风险：根据不同事件（剪切板复制、邮件发送、安装应用……），定义员工工作中的异常行为。如：复制身份证号、发送邮件包含客户资料，安装外挂程序等违规操作

（2）根据用户和部门分配告警规则的适用范围

告警规则配置完成后，可以按照用户和部门分配告警规则的适用范围，以满足管理员对不同用户和部门的异常行为监控需要。

- 适用于所有人：该告警规则对安装 iS-CDA 客户端的所有用户均生效。
- 适用于用户或部门：选择后，该告警规则适用于指定的人或部门。

（3）告警实时通知

当指定的用户在终端操作行为触发告警规则，或系统服务状态发生异常时，iS-CDA 会

根据规则通知中设定的通知频率和方式及时发送警报，通知管理员采取措施。

- 通知频率：通知频率指的是警报的发送频率，分为每次、每个会话一次、每个应用一次和按照“触发次数”通知，具体含义如下：

通知频率	含义
每次	每次检测到用户的操作满足定义的条件时发送警报
每个会话一次	同一段录屏中，第一次检测到用户的操作满足定义的条件时发送警报
每个应用一次	同一个应用从打开到退出的第一次操作满足定义的条件时发送警报
触发次数	自定义配置检测用户操作的频次，满足次数后发送一次警报

- 客户端通知：当客户端检测到用户的操作触发了告警规则条件时，在用户屏幕的右下角会弹出消息提示弹框，同时支持自定义告警的标题和内容。该客户端通知会在几秒后自动从屏幕上消失，因此不会影响工作效率。
- 服务端通知：当用户的操作触发告警时，系统会将该操作的详细内容通过规则指定的方式发送给通知相关人员。服务端支持邮件和站内信两种通知方式。

通知方式	含义
邮件	根据设置的通知频率将警报内容通过邮件的方式发送到指定邮箱。
站内信	根据设置的通知频率将警报内容通过站内消息通知发送给指定的 CDA 系统用户。

（4）系统风险行为记录与查看

当检测到系统主机、集群节点或者许可情况异常时，可以在记录中查看系统风险告警，便于管理员实时关注系统状态，保障系统服务正常。

（5）用户风险行为审计与追溯

针对用户风险行为，CDA 将用户的每一次风险行为操作进行记录，同时支持风险行为检索，支持一键定位录屏中的风险操作，快速取证，便于企业及时追溯异常情况，保障企业内部信息安全。

（6）用户风险行为分析

iS-CDA 从全局、用户和部门多维度进行风险行为统计分析，统计风险触发人数、频次、风险事件类型等指标，快速发现高风险用户和部门，便于管理人员有针对性地做出安全管控行动。

风险行为概览

用户风险分析

2.5.3.2 数据脱敏

iS-CDA 在自然语言化的日志中，将数据脱敏处理，保护敏感信息安全，降低运维人员泄露敏感信息的事故，支持日志脱敏的数据类型有银行卡、身份证和手机号。

2.5.3.3 支持明文、盲文水印

iS-CDA 客户端支持屏幕动态水印，水印主体为当前登录账号信息，防范、震慑手机拍照屏幕信息行为。当发生数据信息外泄时，结合水印账号和 iS-CDA 日志和录屏回放功能，迅速定位责任人并提供追责依据。

iS-CDA 支持明文和盲文两种水印方式，可选择水印内容，如用户名、计算机名和日期，也可以自定义内容，并设置水印颜色、字号、不透明度、水印范围和角度，最终将水印内容嵌入用户桌面，保护企业信息安全。

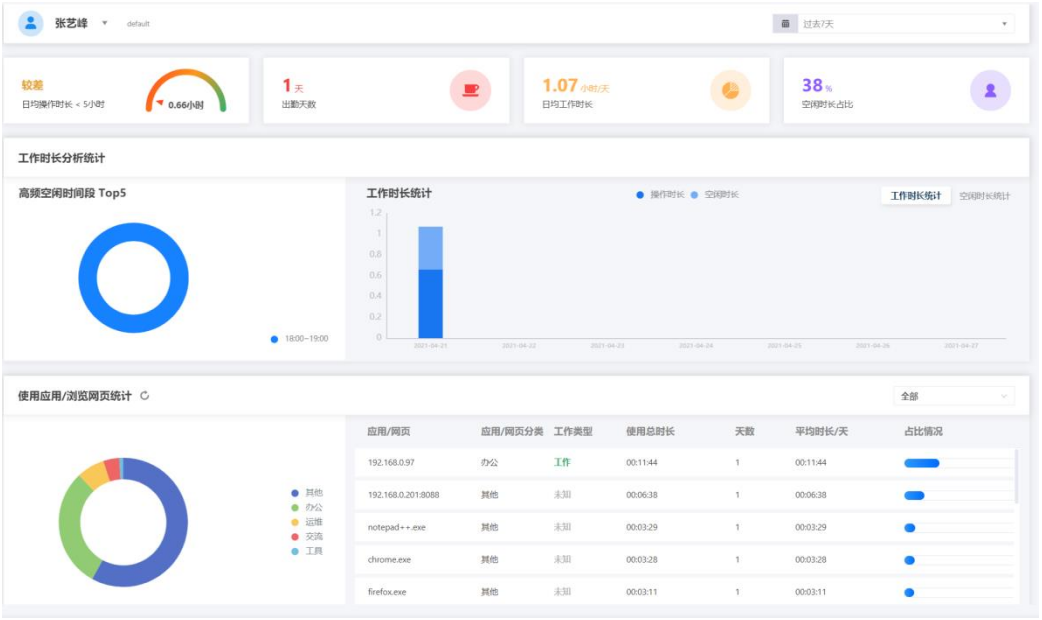

加明文水印后的桌面


加盲文水印后的桌面

2.5.4 工作效率分析

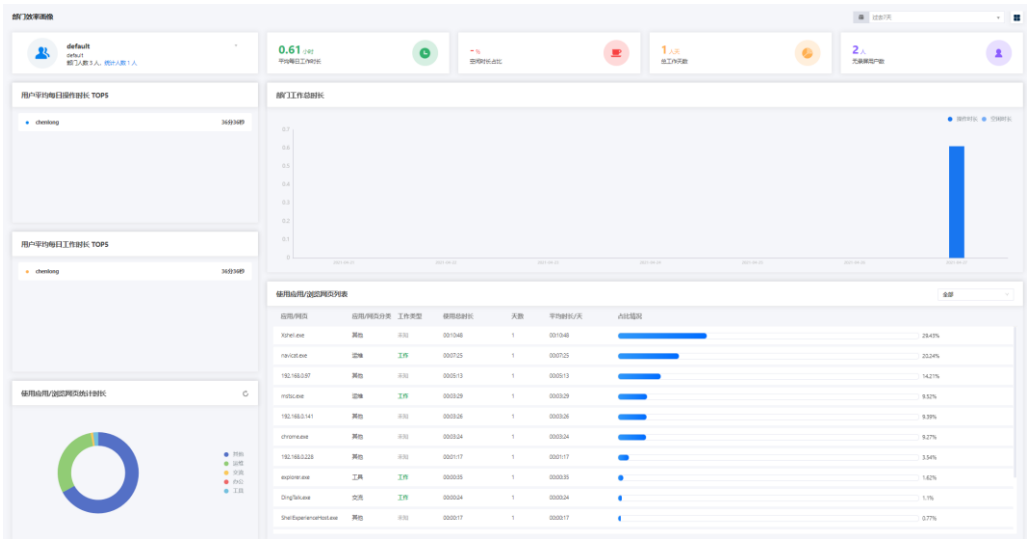
2.5.4.1 用户效率画像

基于用户的工作时长、空闲时长、高频空闲时间段以及对应用程序的使用进行统计和分析，以时间轴为序统计员工工作情况、空闲时长占比及高频的空闲时间段。分析用户每天的工作时长、空闲时长、什么时间段空闲最多？使用最多的应用/网页是什么？并且基于应用的分类，统计用户在某时间段内使用应用/网页的类型和时长。



2.5.4.2 部门效率画像

部门在选定周期内统计了多少员工？员工的平均工作时长是多少？员工每天有多少时间处于空闲状态？部门内员工的总工作天数是多少？哪些员工操作时长长？哪些员工工作时长长？在此时间范围没有产生过录屏的数量有多少？部门员工空闲时长占比高的原因是什么？是因为经常上网聊天做和工作无关的事情？在这里，我们可以通过图例和数据展现部门内员工的工作效率，并显示统计用户的平均工作时长、平均空闲时长占比、总工作天数和无录屏人数等数据。



- 统计指定时间的部门统计人数；
- 统计部门员工的平均工作时长、空闲时长占比、总工作天数

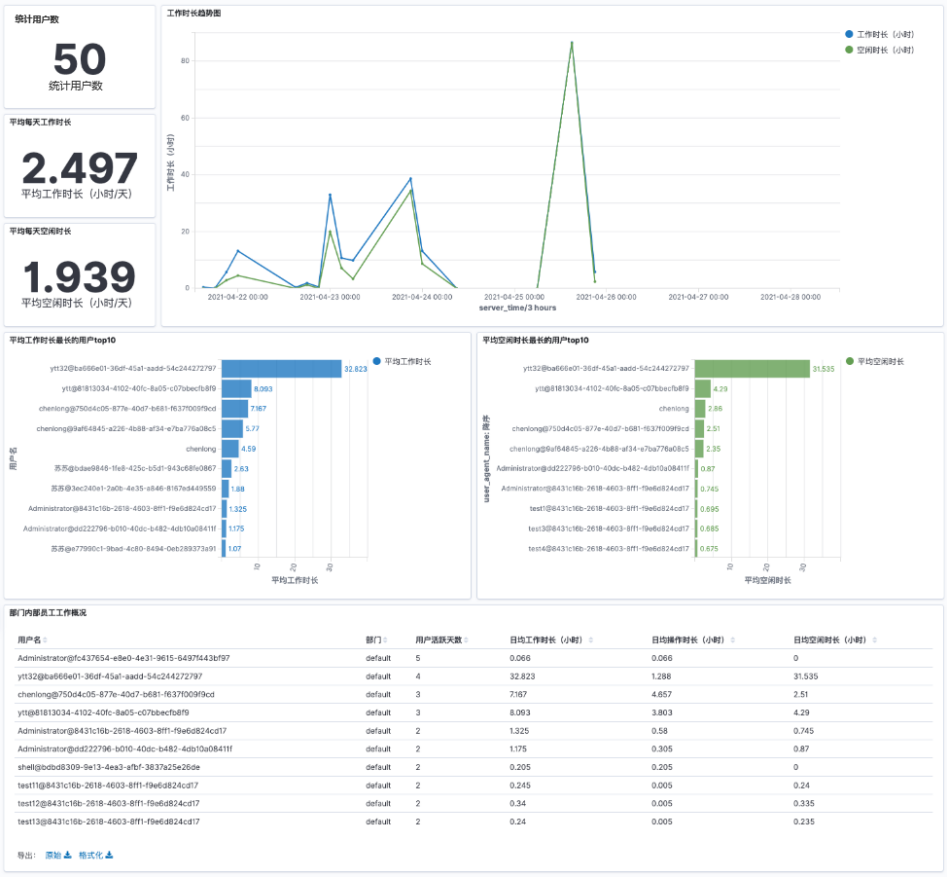
- 统计无录屏的总人数
- 统计部门内用户平均操作/工作时长排行 TOP5
- 统计部门常用应用/网页的使用时长情况
- 按时间的柱状堆叠，直观显示部门的工作时长趋势以及空闲时长

2.5.4.3 部门/用户效率报表

从部门和用户两个角度统计员工工作效率指标，如平均工作时长、平均空闲时长，对部门内员工或子部门的工作情况进行排名，了解员工/部门整体工作效率水平。

（1）员工效率报表

通过员工效率报表统计，了解部门平均工作时长最长的用户和空闲时长最长的用户，树立部门工作标杆，及时关注工作效率较低的员工，从而提升部门整体工作效率。



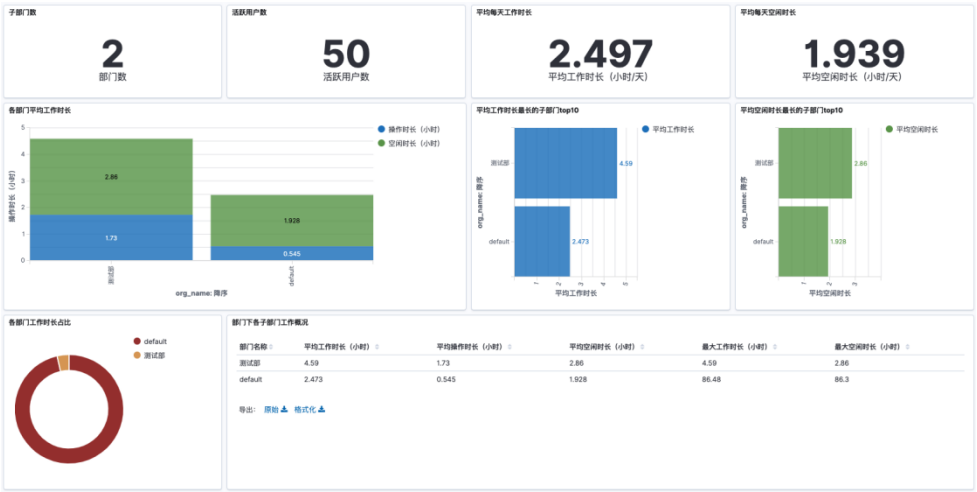
用户名	部门	用户活跃天数	日均工作时长（小时）	日均操作时长（小时）	日均空闲时长（小时）
Administrator@fc437654-e8e0-4e31-9615-6497f443bf97	default	5	0.066	0.066	0
ytt32@ba666e01-36df-45a1-aadd-54c244272797	default	4	32.823	1.288	31.535
chenlong@750d4c05-877e-40d7-b681-f637f009f9cd	default	3	7.167	4.657	2.51
ytt@81813034-4102-40fc-8a05-c07bbecfb8f9	default	3	8.093	3.803	4.29
Administrator@8431c16b-2618-4603-8ff1-f9e6d824cd17	default	2	1.325	0.58	0.745
Administrator@dd222796-b010-40dc-b482-4db10a08411f	default	2	1.175	0.305	0.87
shell@bdbd8309-9e13-4ea3-afbf-3837a25e26de	default	2	0.205	0.205	0
test11@8431c16b-2618-4603-8ff1-f9e6d824cd17	default	2	0.245	0.005	0.24
test12@8431c16b-2618-4603-8ff1-f9e6d824cd17	default	2	0.34	0.005	0.335
test13@8431c16b-2618-4603-8ff1-f9e6d824cd17	default	2	0.24	0.005	0.235

- 统计部门统计用户数；
- 统计部门员工的平均工作时长、平均空闲时长；
- 绘制员工工作总时长和空闲总时长的趋势；
- 统计平均工作时长最长的用户 TOP10；

- 统计平均空闲时长最长的用户 TOP10；
- 列出部门所有员工的工作概况。

（2）部门效率报表

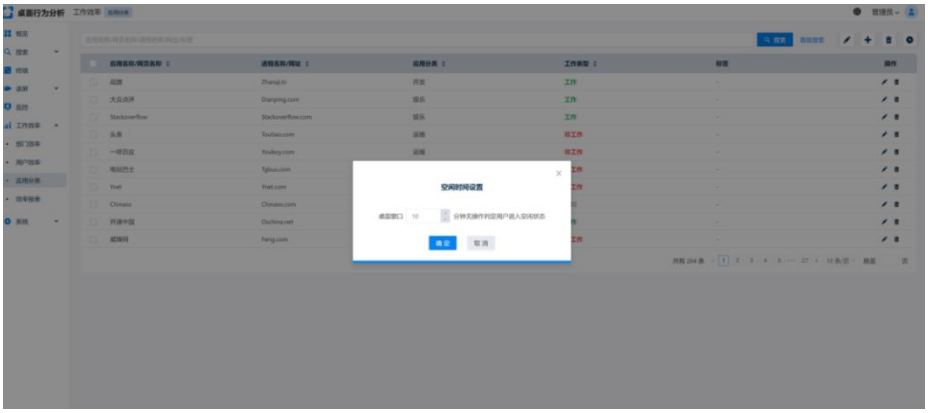
通过部门效率报表统计，了解部门平均工作时长最长的子部门和空闲时长最长的子部门，树立部门工作标杆，及时关注工作效率较低的子部门，从而提升部门整体工作效率。



- 统计部门统计用户数和部门数；
- 统计部门员工的平均工作时长、平均空闲时长；
- 统计各部门平均工作时长情况
- 统计平均工作时长最长的子部门 TOP10；
- 统计平均空闲时长最长的子部门 TOP10；
- 列出部门所有子部门的工作概况。

2.5.4.4 空闲状态设定

桌面窗口指定时间无操作则判定用户进入空闲状态，设置空闲时间判定参数，以便统计员工空闲时长。



2.5.4.5 应用分类

系统内置应用程序及网站的分类知识库，可对应用程序或常用网站进行灵活的分类和工作类型定义，以便用于分析员工的工作效率。如上班时间内操作了哪些类型的应用，有多少时间用在了非工作应用/网页上。

2.5.5 运维日志分析

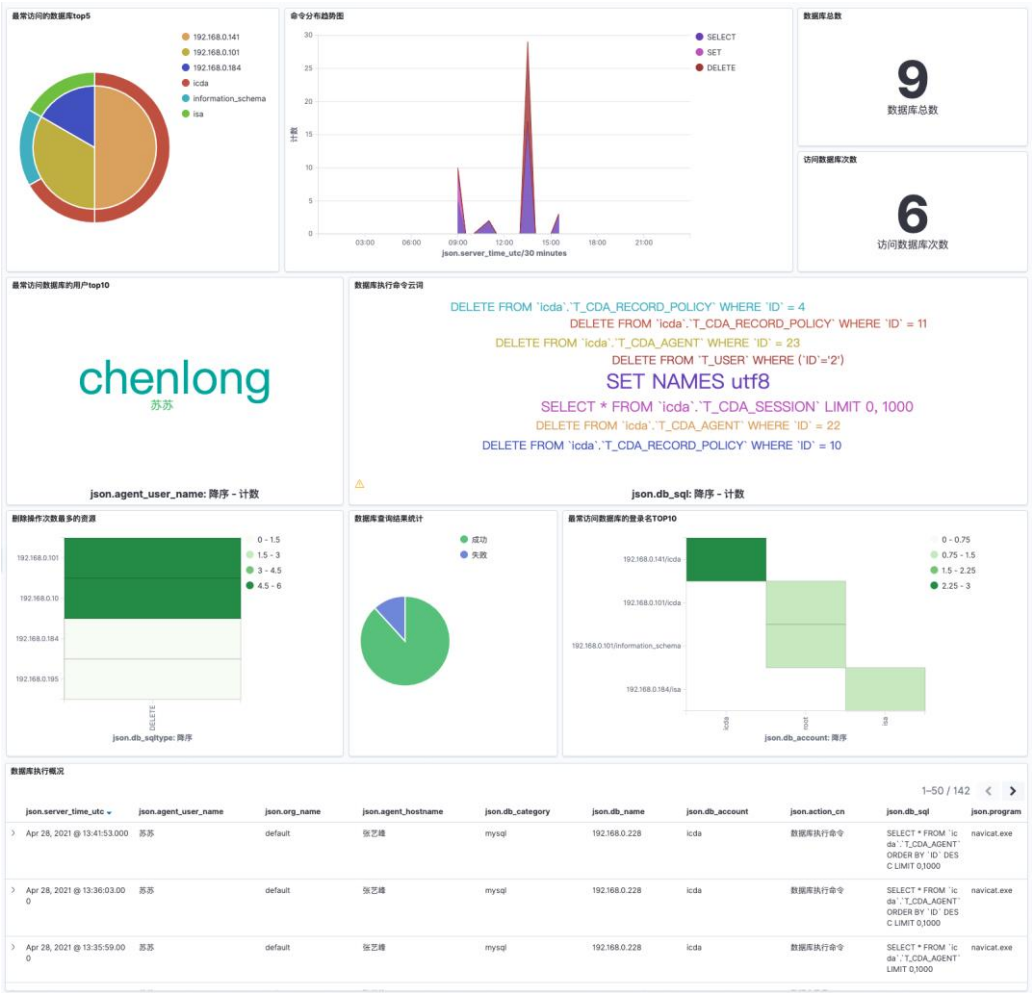
基于丰富的运维日志抓取能力，记录服务器、数据库和 FTP 工具操作的详细信息。通过全程的操作行为录屏和操作命令文本记录，实现全程定点审计，同时生成运维报表，分析服务器、数据库和 FTP 工具的登录、使用和执行命令情况。

2.5.5.1 服务器报表

基于采集到的相关服务器运维工具的日志数据集成单独的服务器运维报表。统计用户访问的服务器资源总数和访问次数、最常访问服务器的用户 top10、不同协议类型的服务器操作趋势、访问次数最多的 5 个服务器的 ip 以及访问的用户信息、服务器的常用命令以及不同操作类型的服务器访问热力图。最后，生成所有用户的服务器运维日志列表并可进行定位回放。

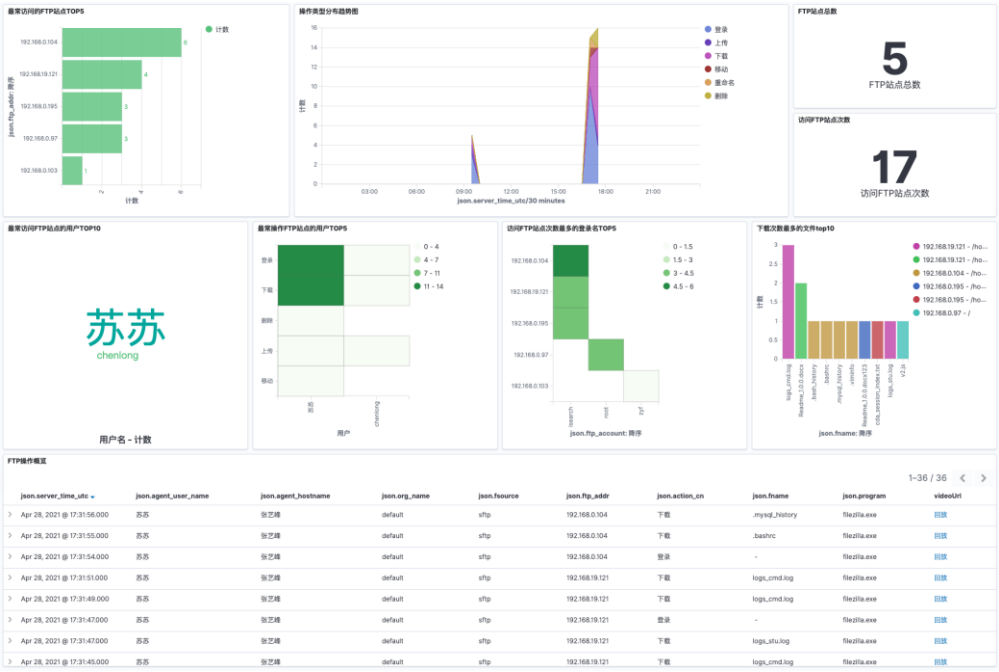
2.5.5.2 数据库报表

基于采集到的有关数据库运维工具的日志数据集成单独的数据库运维报表。统计分析最常访问的数据库资源和访问次数、最常访问数据库的用户、最常访问数据库的登录名、最常执行的命令、执行的命令类型趋势、哪些资源经常执行删除操作、数据库查询的成功率，最后生成数据库类日志列表。



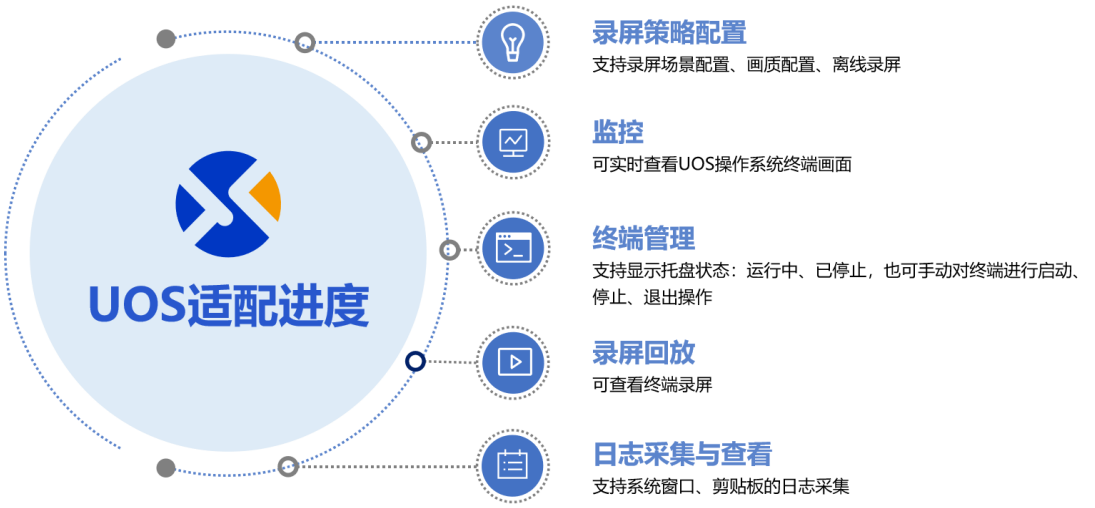
2.5.5.3 FTP 工具报表

基于采集到的有关 FTP 文件传输工具的日志数据集成单独的 FTP 运维报表。统计分析最常访问的 FTP 站点、FTP 站点总数以及访问次数、最常访问 FTP 站点的用户、最常访问 FTP 站点的登录名、下载次数最多的文件，最后生成 FTP 类日志列表，支持定位跳转，便于审计。



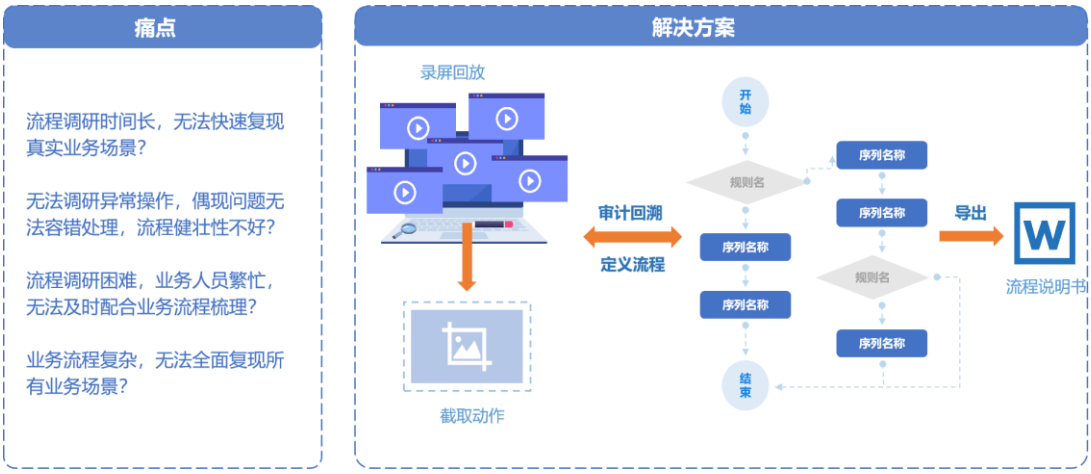
2.5.6 国产化操作系统适配

随着经济全球化的趋势不断深入，信息安全问题日益突出。自主研发操作系统，事关国家安全和市场利益，却一直是国内科技产业的短板。根据市场研究公司 IDC 的数据显示，2020 年微软、苹果、谷歌三家企业占据全球操作系统市场 98.8%份额。而在国内市场，三家公司的份额同样超过 95%，操作系统领域卡脖子的问题日益突出，拥有具有独立技术知识产权的 pc 终端、移动终端操作系统的呼声愈发强烈。针对以上问题，iS-CDA 率先进行国产化 UOS 操作系统适配的研发工作，且已完成了主流程适配，旨在扩大国产化操作系统的应用生态，让更多的企业共享降本增效红利。



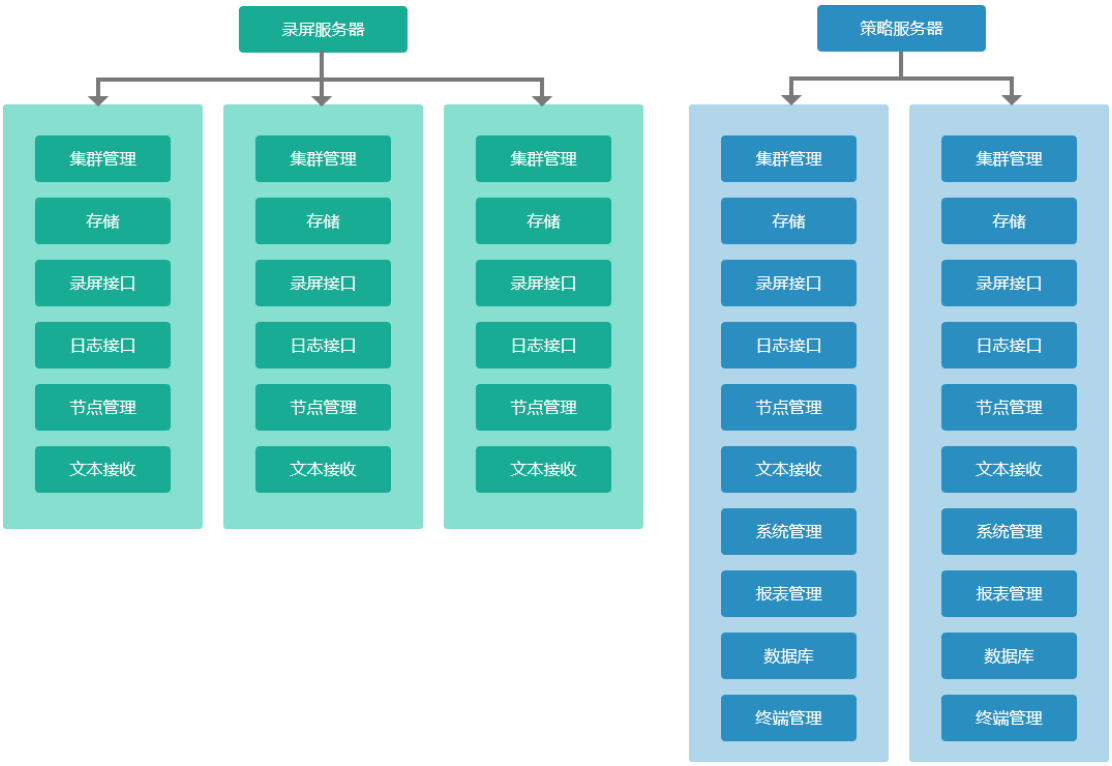
2.5.7 流程定义

在企业实现自动化的过程中，常常面临着流程调研时间长，无法快速复现真实业务场景？无法调研异常操作，偶现问题无法容错处理，流程健壮性不好？流程调研困难，业务人员繁忙，无法及时配合业务流程梳理？业务流程复杂，无法全面复现所有业务场景等困难。面对 RPA 自动化调研中存在的诸多问题，iS-CDA 基于录屏回放，快速回溯企业真实业务环境，通过截取录屏中的关键动作，灵活绘制完整的业务流程图，并导出流程定义说明书。从而帮助企业缩短业务流程调研时间，降低调研难度，加快企业数字自动化转型。



2.5.8 集群部署方案

在大规模多区域环境下，面对海量数据，可以采用集群化部署方案，部署示意图如下：



可以按照实际需要部署多台录屏服务器，每台服务器都可以接收视频和日志，并对数据进行处理，并将其及时同步到 elasticsearch 上面进行存储。这其中需要先开启门户网站，通过门户网站对录屏服务器的策略和规则进行设置，如配置集群，从而保证服务器高可用。

被连接终端上的 agent 程序会向服务器请求获取录屏策略，然后按照对应的策略配置获取到录屏服务器，最后所有的视频和日志都会上传至策略分配的对应录像服务器上。

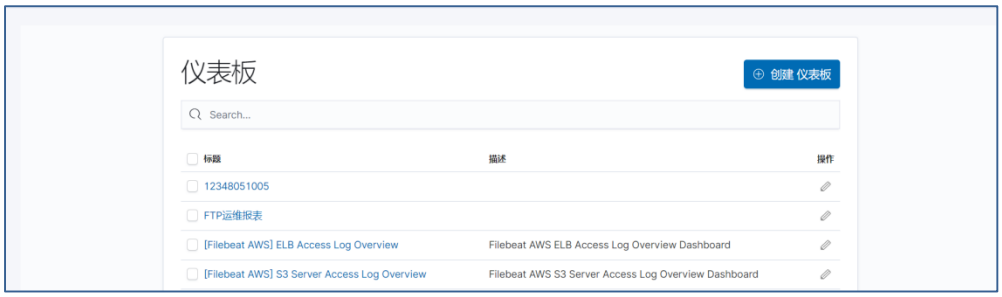
同样的，监控和审计人员访问审计数据时，可以直接通过服务器前端门户网站，播放录屏或者实时监控，并且可以同步查看对应的日志信息，也可以定时查看数据报表、效率报表、运维报表和无录像报表等数据。

录屏服务器可大规模扩展，随时按需增加。单台录屏服务器（8 核，32G 内存服务器）即可支持多达 500 单摄像头客户端的并发连接，多台叠加后，可完全支持大规模部署、海量数据的需要。

2.5.9 视图&报表

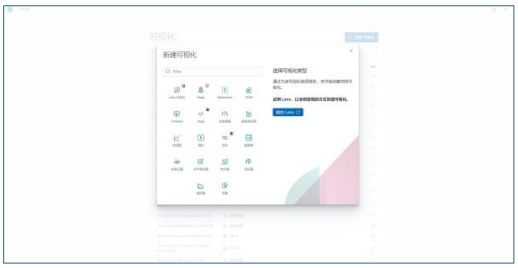
2.5.9.1 仪表盘面板

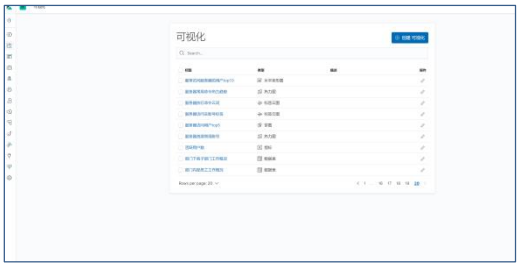
使用强大的 ELK 技术对接能力，可将所有的搜索结果转化为 KPI 指标，然后在 KPI 指标基础上，可以保存为视图，视图样式丰富，如仪表盘图、折线图、垂直条形图、饼图、热力图、标签云图和面积图。通过仪表盘面板页面中种类丰富的图表，能够以最直观的方式呈现管理者关心的数据，全面真实的展现企业各方面的业务运行状态。



2.5.9.2 视图及搜索管理

支持自定义视图，也可以根据搜索的结果或是已保存的搜索进行视图的创建，数据展示方式多样化，使用户关心的数据更直接更直观。





- 支持根据搜索条件创建视图；
- 支持搜索、视图的增、删、改、查操作；
- 支持量化仪表盘，支持指定搜索条件、数值可以是总数、最大值、最小值、平均值等、支持自定义字体大小和自定义描述；
- 支持数据表视图，支持指定搜索条件、支持自定义列、支持分表或分行；
- 支持仪表盘图、折线图、垂直条形图、饼图、热力图、标签云图和面积图等样式；
- 支持保存、加载和分享，支持指定搜索条件、支持自定义列、支持分表或分行；
- 支持定义后的实时预览。

2.5.10 系统管理

2.5.10.1 终端管理

在服务端的终端管理列表页面，可对客户端进行全面监控和实时控制管理，同时支持远程自动升级。

2.5.10.2 角色管理和部门授权

可从菜单控制和数据权限范围两个层面实现对审计人员的分权分级。通过建立角色并赋予菜单权限，指定用户可以访问的菜单。同时也可以给用户进行部门授权，授权后可查看被授权部门的数据。建立角色分配数据权限和部门授权示例图如下：

2.5.10.3 支持 AD 域同步用户和部门

支持 AD 域用户/部门的一键同步，无需繁复操作，即可简单高效地对账号进行集中式管理。 域用户既可被录屏，也可使用同一账号登录服务端平台管理数据。

2.5.10.4 支持许可管理，实时掌握许可使用情况

在许可管理页面，管理员可及时查看许可的有效期、使用情况和许可包含的服务，根据

许可状态有计划地进行扩容或续费，避免许可原因导致录屏丢失。

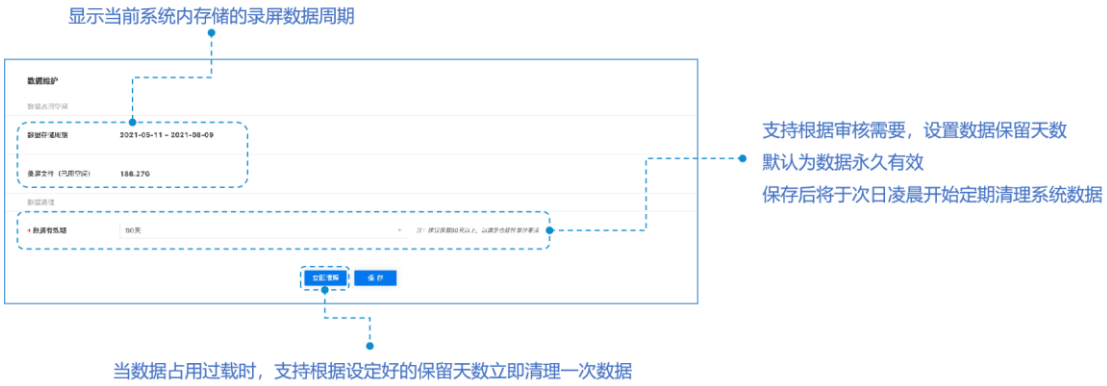
2.5.10.5 录屏集群管理与状态检测

可对集群和节点进行管理与状态监测，实时掌控集群的核心性能指标，支持以下功能：

- 支持集群的启停与删除；
- 支持节点的启停和移除；
- 支持根据 IP 范围和子网分配终端录屏集群；
- 支持无集群节点的临时归属；
- 支持待分配节点的重新分配和删除；
- 支持节点录屏磁盘的存储详情查看，及时掌握磁盘空间存储状态

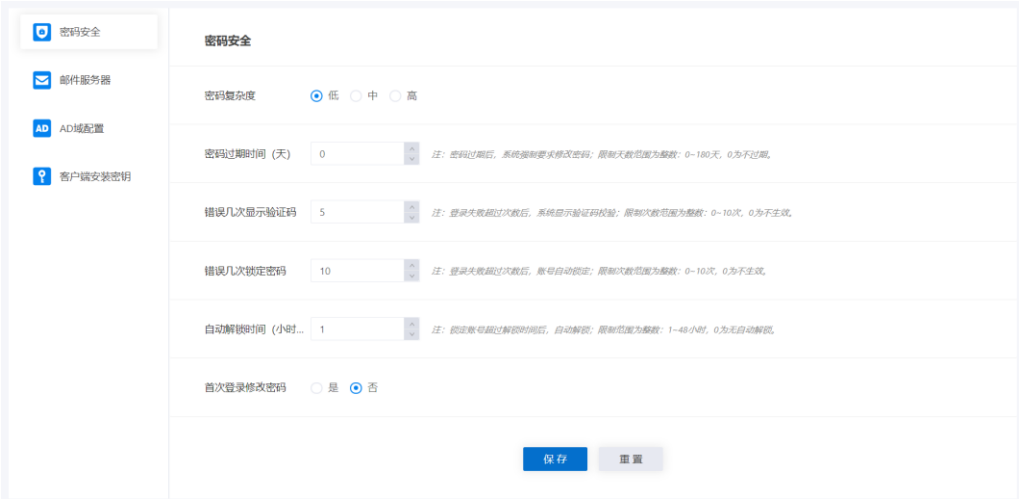
2.5.10.6 数据维护清理功能

iS-CDA 支持自定义设置录屏和日志等相关数据的保留时间，在满足合规性审计要求的同时，可自动定时清理系统内录屏、日志及其他数据，避免因系统存储空间不足造成录屏丢失等后果，降低了运维人员的系统维护难度，极大地提升了系统运维操作效率。



2.5.10.7 系统密码安全设定

为保障服务端各环节的安全，针对密码安全等级、过期时间和错误密码锁定等参数进行配置，大大提升了系统登录密码的安全性，为 iS-CDA 提供了全方位的安全防护保障。



2.5.10.8 操作日志

操作日志是指用户操作、配置服务端平台时所产生的日志，记录平台数据增删改的操作，保障平台内部安全。

3、场景&案例

3.1 应用场景

3.1.1 操作中心

针对企业内部员工及业务操作人员，iS-CDA 通过灵活的策略设置，为每笔业务操作生成录屏，完整记录员工操作过程，并采集丰富的行为日志，将用户行为分解成详细的日志记录保存下来。

员工上班是否在做与业务无关的事情？如何评价员工的操作速度和工作效率？通过对操作行为的分析，直观展现员工的工作时长及空闲时长详情，帮助企业提升业务操作效率。

- 为每笔业务操作生成操作过程录屏；
- 详细分析员工使用工作相关应用的时间；
- 分析业务人员工作时长和空闲时长；
- 通过可视化数据观察员工工作模式；
- 充分挖掘潜能，提高生产力。

3.1.2 研发及运维中心

针对开发、运维及外包团队的管理，要确保业务系统开发过程必须是保密严谨的，特别对于外包的开发团队，更需要对开发过程进行全程监控；而在测试阶段也需要记录测试的各个步骤，尤其是测试过程中的问题点、故障点，保证发生问题与故障的过程可追溯还原，帮助问题尽快解决；此外还需要针对终端应用性能，网页系统载入性能等进行一系列监控，帮

助开发人员随时掌握开发成果的表现状况，进行及时的改进；最后监控与记录的数据要能够帮助对人员工作情况进行绩效统计，为开发工作整体评估提供有用参考。

iS-CDA 可以很好地满足应用开发工作中这些方面的需求，具体可提供以下帮助：

- 实现运维行为分析，支持运维工具、数据库工作、FTP 工具等；
- 支持对命令及回显的抓取；
- 提升研发、运维及外包团队工作效率；
- 实现对外包团队的工作量的统计及风险审计。

通过应用开发环境中 iS-CDA 的部署，确保了对于开发、测试和试运行等过程的全程监控，提供了可视化开发的技术手段，即可以帮助杜绝潜在危害，发现异常行为，也可以帮助管理者统计工作量，提升开发效率。

3.1.3 客户联络中心

客户服务中心是直接面对客户要求、回应客户问题、满足客户需求的一线部门，它的工作质量直接影响客户对公司整体的满意度。这就需要不仅客服人员自身有较高的工作技巧，同时也更需要外界严格的监督，以促进其业务水平的不断提升，因此对客服工作的质检成了督促提升其工作质量，提升客户满意度非常重要内容。

iS-CDA 为质检部门增添一种必要的技术手段，填补质检工作的短板，采集缺失的操作数据。不仅对操作过程全程实时录屏，同时采集客服人员操作动作对应的文本化日志，并对日志进行可视化与自然语言化，从而使得质检工作更有目的性、方向性，提升了质检的命中率和时效性，提升了客户服务中心的整体工作质量。

- 客服人员服务过程可视化；
- 帮助实现快速质检，提升质检命中率；
- 结合培训体系提升员工服务质量；
- 提升风控管理水平，防止客户数据泄露；
- 为客户投诉提供了可回溯的证据；
- 解决在线客服的质检难题。

3.2 客户案例

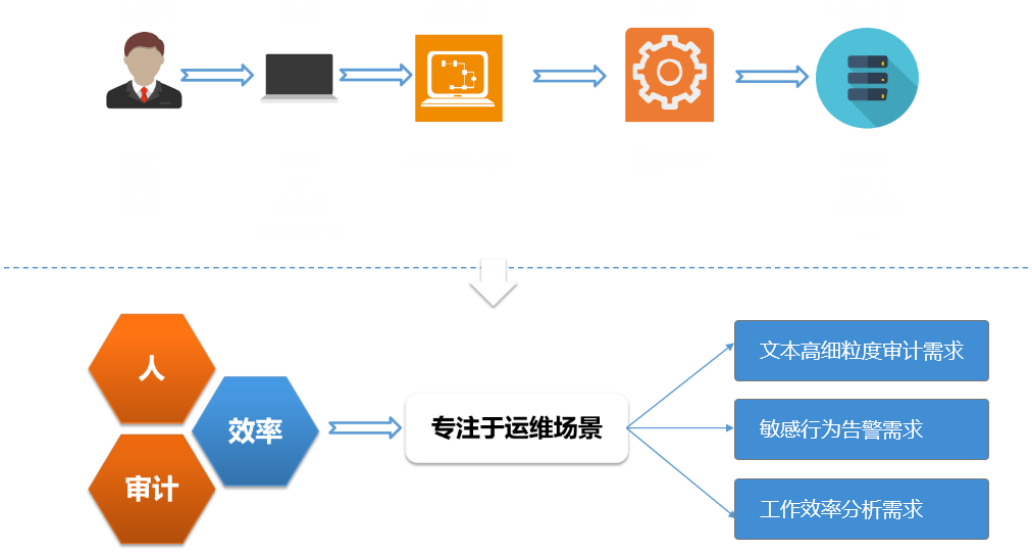
3.2.1 平安银行

3.2.1.1 外包开发

艺赛旗 iS-CDA 通过对研发人员的终端合规性监控和操作行为统计，如 USB、WIFI、绿色软件行为识别，分析研发人员的工作情况，回溯隐藏 BUG，提升代码质量，最终实现了 2 个管理人员对 1500 个外包人员的高效管理。

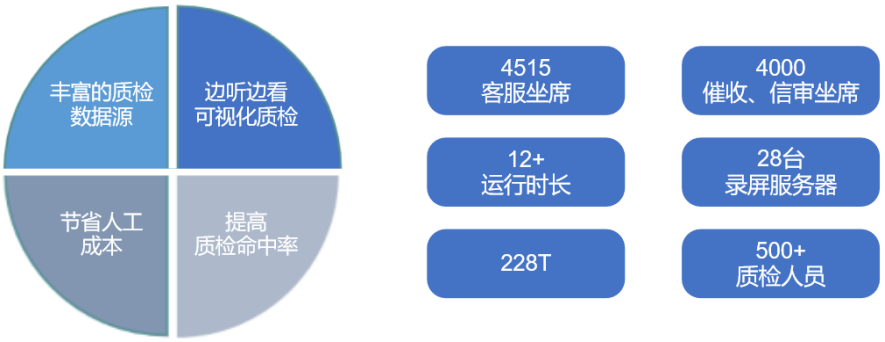
3.2.1.2 运维中心

通过对运维中心工单系统的对接，及时发现非授权行为和高危命令并告警，实现了对运维中心 600+运维人员操作审计。



3.2.2 交通银行太平洋卡中心

艺赛旗 iS-CDA 帮助交通银行太平洋卡中心成功实现了服务全过程的可视化，为客户投诉和客服人员的违规操作提供了确凿的证据。实现了对 8000+客服人员的自动化质检，解决在线客服的质检难题。通过操作行为和效率分析并结合培训体系，提升了员工服务效率，发现客服人员违规操作，提升风控管理水平，防止客户数据泄露。



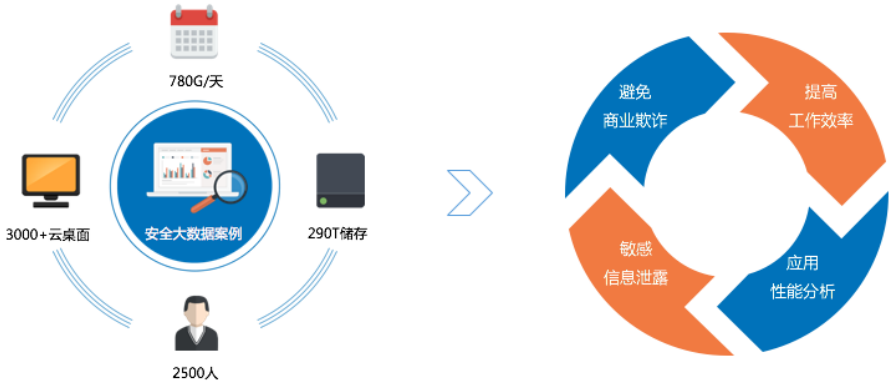
3.2.3 浦发银行

浦发银行通过使用艺赛旗 iS-CDA，对操作中心 10000+员工操作的每笔业务自动生成操作过程的全录屏，完整记录员工业务操作过程，通过可视化的数据，掌握员工工作情况。通过行为和效率分析，掌握业务人员的工作行为和工作效率，统计业务人员使用业务工具的时间，帮助员工提高了工作效率和生产力。

3.2.4 上海移动

艺赛旗 iS-CDA 帮助上海移动实现对运维及外包团队工作行为的可视化监控，并对其工

作行为分析，既可以杜绝潜在危害，及时发现异常行为，也可以帮助其提高开发效率。对运维过程中主机、数据库、网络设备的操作进行监控、记录和分析，主动实现对敏感数据访问的告警，降低了敏感信息泄露事故发生率。通过对企业内核心机密文档的传播途径的严密监控，发现潜在的商业欺诈行为。通过对研发人员的行为和效率分析，协助研发定位问题，统计研发人员工作效率和工作时间，提升研发效率，实现对外包团队的工作模式评价及风险控制。



3.2.5 上海电信云桌面行为监控

由于疫情原因，客服的工作人员需要居家远程办公，通过在客服人员的云桌面部署 iS-CDA 客户端，进行全量的操作数据的采集、生成文本日志和录像，并上传至服务端，实现了对 500+客服人员在云桌面操作行为的远程监控与记录，帮助审计人员或系统管理人员对居家客服人员的操作合规性进行审计和工作效率分析。

3.3 我们的客户


中国人民银行
ICBC (Asia)
中国农业银行
中国银行
交通银行
广发银行 CGB
UnionPay 银联
浦发银行 SPD BANK
南京银行
招商银行
太平洋保险 CPIC
海通证券
华夏银行
兴业银行
平安银行 PINGAN BANK
恒丰银行
兰州银行
张家港农村商业银行
海南银行
乌鲁木齐银行
红塔银行
中国太平 CHINA TAIPING
中国人寿 CHINA LIFE
中国光大银行
西藏银行
中信建投证券 CHINA SECURITIES
国泰君安证券
紫金农商银行
中国平安 PING AN
中国移动通信 CHINA MOBILE
China unicom 中国联通
中国电信 CHINA TELECOM
Telkom Indonesia
Sinopec
中国石油
国家电网 STATE GRID
中国南方电网
中国邮政 CHINA POST
中国东方航空 CHINA EASTERN
深圳公安
上海机场集团
中国疾病预防控制中心
中国烟草 CHINA TOBACCO
NIKE
一汽富维
Shell
立邦
SKF
ZARA
Electrolux 伊莱克斯
HUAWEI
ZTE中兴
pwc
Lenovo
Danfoss
KPMG
vanke
TRANSSION
链家
sojitz
龙田科技
荟才国际管理咨询 HUICAI INTERNATIONAL
上海心邑
驴妈妈
元年 YUANIAN
transcosmos
华谊集团
Mission
A.O.SMITH 史密斯
SAIC 上汽集团 SAIC MOTOR
中国建筑五局
.....


i-SEARCH