

**AuditSys桌面行为风险管理系统软件**

**产品白皮书**

北京华夏威科软件技术有限公司

2023年10月

目录

[1. 产品概述 3](#_Toc122077930)

[2. 系统架构 5](#_Toc122077931)

[3. 产品功能 8](#_Toc122077932)

[3.1. 行为数据采集 8](#_Toc122077933)

[3.2. 行为检索 8](#_Toc122077934)

[4. 系统管理 18](#_Toc122077935)

[5. 产品特点 22](#_Toc122077936)

[6. 产品部署 23](#_Toc122077937)

[6.1. 集中式部署 23](#_Toc122077938)

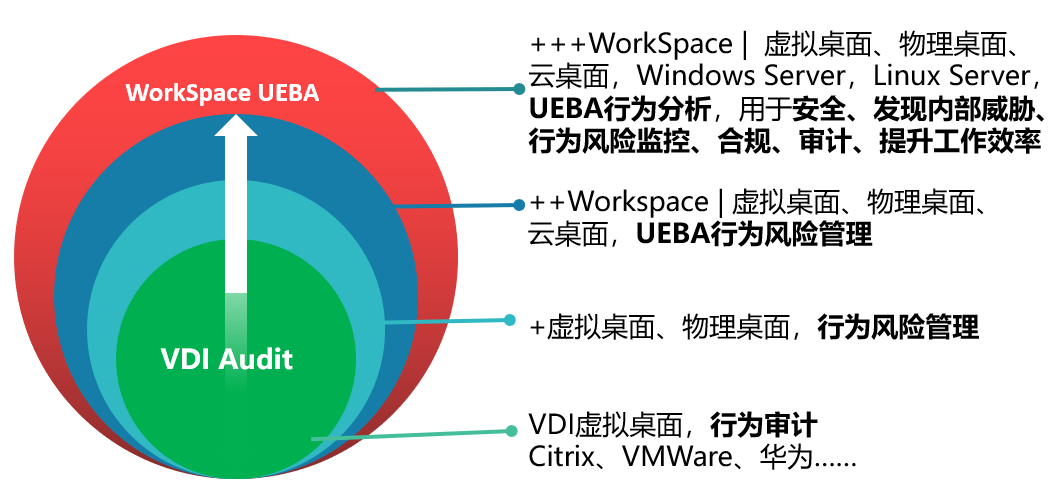
[6.2. 分布式部署 23](#_Toc122077939)

[6.3. 多中心部署 24](#_Toc122077940)

[6.4. 部署规模设计 25](#_Toc122077941)

# 产品概述

SinoUEBA（AuditSys）用户实体行为分析系统采用大数据引擎，对Windows和Linux虚拟桌面、物理桌面、云桌面和服务器实现无盲点UEBA行为分析，帮助用户实现内部人员的**行为风险监控、应用访问控制、行为审计与追溯、敏感数据保护**。从而助力用户保护信息安全、保障业务系统稳定运行、以及实现法规遵从（等保2.0的安全审计和审计管理）。



**功能模块介绍：**

|  |  |
| --- | --- |
| **模块名称** | **规格描述** |
| **行为审计系统** | 将用户的所有操作行为以录屏的方式保存下来，方便企业查看员工在什么时间做了什么操作；支持全文检索功能，可直接定位到某一个事件。 |

# 系统架构

SinoUEBA（AuditSys）主要通过部署的代理程序（Agent）来完成操作画面的捕获及用户的操作行为日志摘要，通过集中管理平台来完成录像和日志的集成、匹配和基础分析，管理人员在管理页面可以直接查看这些数据，也可以将相关数据输出到大数据分析系统中进行分析，而最终发现问题或者需要人工干预时，可以随时调取直观可信的录像及日志来进行观察。

**系统逻辑架构：**



**系统主要组件说明：**

|  |  |  |
| --- | --- | --- |
| **组件** | **功能** | **备注** |
| Center控制台 | 用来提供用户管理接口、配置策略与功能配置、为用户下发配置策略与应用服务器列表等基础配置信息 |  |
| MySQL数据库 | 用来存放系统配置信息，如记录策略，安全策略，风险规则，敏感词规则等基础配置策略 |  |
| ES大数据分析引擎 | 用来存放审计元数据以及平台的日志与性能监控数据 |  |
| Server应用服务器 | 用来接收用户的屏幕录像与元数据信息并存放至文件存储与数据库内 |  |
| Agent代理客户端 | 安装在用户端，根据审计策略用来收集用户的操作记录与行为并上传至应用服务器。 |  |
| S3对象存储 | 用来备份存储外发文件和录屏文件数据 | 可选 |

**① Center控制台**

提供前端可视化管理界面。可以用于数据检索，录屏回放，可疑分析展示，监控，报表，终端及应用服务器配置、升级，组织管理，平台管理等功能。管理控制器主要规划为几大功能块。

* **数据检索和回放：**包含会话检索、会话回放、行为检索及回放，支持全文检索。设计思路为方便客户快速查询、定位风险问题。
* **数据分析：**提供可疑行为分析、可疑行为查询，敏感词分析，报表等功能给客户。
* **平台配置：**包括二次认证用户、域配置、Agent策略、风险规则、记录策略、安全策略、网络配置、时间配置、告警通知、ES配置等
* **平台管理：**包括组织，管理员，角色，许可，终端管理，服务器管理，平台监控等。
* **数据备份策略：**在控制台界面提供数据库备份还原。可以在mysql上设置自动备份策略，定时自动备份数据库文件到指定的共享磁盘。

**② MySQL数据库**

MySQL是存储记录策略，安全策略，组织，用户组，用户管理，部门管理，风险规则，敏感词规则等基础策略配置规则。

**③ ElasticSearch大数据分析引擎**

Elasticsearch简称ES，是个实时全文搜索和分析引擎，提供搜集、分析、存储数据三大功能。它的特点有：分布式，简易配置，自动发现，索引自动分片，索引副本机制，restful风格接口，多数据源，自动搜索负载等。

SinoUEBA（AuditSys）采用ES作为元数据存储，充分利用其高可用，大数据分布式搜索引擎等特点，提供快速有效的数据查询分析服务。

**④ Server应用服务器**

应用服务器用来接受来自Agent客户端的审计记录，将视频数据保存到本地，根据管理员配置的规则进行判断分析后将日志数据发送给ElasticSearch服务，同时接收来自控制台服务器的录屏播放请求。

**⑤ S3对象存储**

备份外发文件和录屏文件数据。

**⑥ Agent代理客户端**

Agent提供用户的屏幕及行为的捕获。Agent的负载内存30M左右；CPU占用极低，约0-1%。

Windows和Linux系统支持：

* **Windows：**Win 7/10/11、Server2008/2012/2016/2019/2022 等32及64位系统；
* **Linux：**Centos、Redhat 6和7、统信UOS-20

信创终端兼容认证：

* 统信桌面操作系统（海光、兆芯、鲲鹏、飞腾）
* 麒麟软件桌面操作系统（鲲鹏、飞腾、海光、兆芯）
* 麒麟信安桌面操作系统

Agent代理客户端主要模块：

* **录屏模块**：根据用户的操作进行屏幕的录制，采用差额录制。
* **应用模块**：通过截获各个应用、窗口的信息获取用户行为数据。
* **数据发送**：Agent数据采用智能选路Server服务器，并且在线和离线数据均可合理的发送的Server端。

# 产品功能

SinoUEBA（AuditSys）通过对终端用户操作行为的抓取记录，可以做到分类展示细颗粒化全文检索。实时记录用户的各种人机操作，管理员可以实时查看。出现数据外泄或恶意操作的情况可以作为证据追溯；出现误操作造成故障可以快速定位原因，加快故障处理效率。

系统可以配置不同的审计策略，实现各种不同的审计规则。如只对重要业务系统进行录像。对于员工个人软件不进行录像，保护了员工的隐私的同时，也保证了业务系统的安全。

## 行为数据采集

SinoUEBA（AuditSys）系统可以对终端所有操作进行记录，包括日志记录和录屏记录。

录屏记录根据鼠标、键盘按键、屏幕变化量策略触发，系统默认添加了一部分按键，触发按键可以由管理员自定义配置，也可以通过黑白名单方式添加记录的用户和应用程序。

日志记录可以灵活的根据客户需要配置记录规则：是否录像、是否只记录远程操作、探针选择（选择记录那些内容，如：记录QQ、微信、钉钉、记录上网活动、usb、剪贴板、邮件、文档记录等等）、报文类型、以黑白名单的形式选择记录哪些用户或者应用的操作，都可以灵活定义。

可以在终端列表实时查看终端的详细信息（如cpu、内存、磁盘使用率、系统版本等）、关键事件（锁屏、解锁、登录等），终端日志和配置文件也可以直接从控制台查看，不用到客户端现场，可以更方便的管理终端。

## 行为检索

SinoUEBA（AuditSys）系统所有记录支持全文检索，检索分为会话数据、行为数据，支持全文检索，搜索任意关键字，快速找到自己想要的数据。

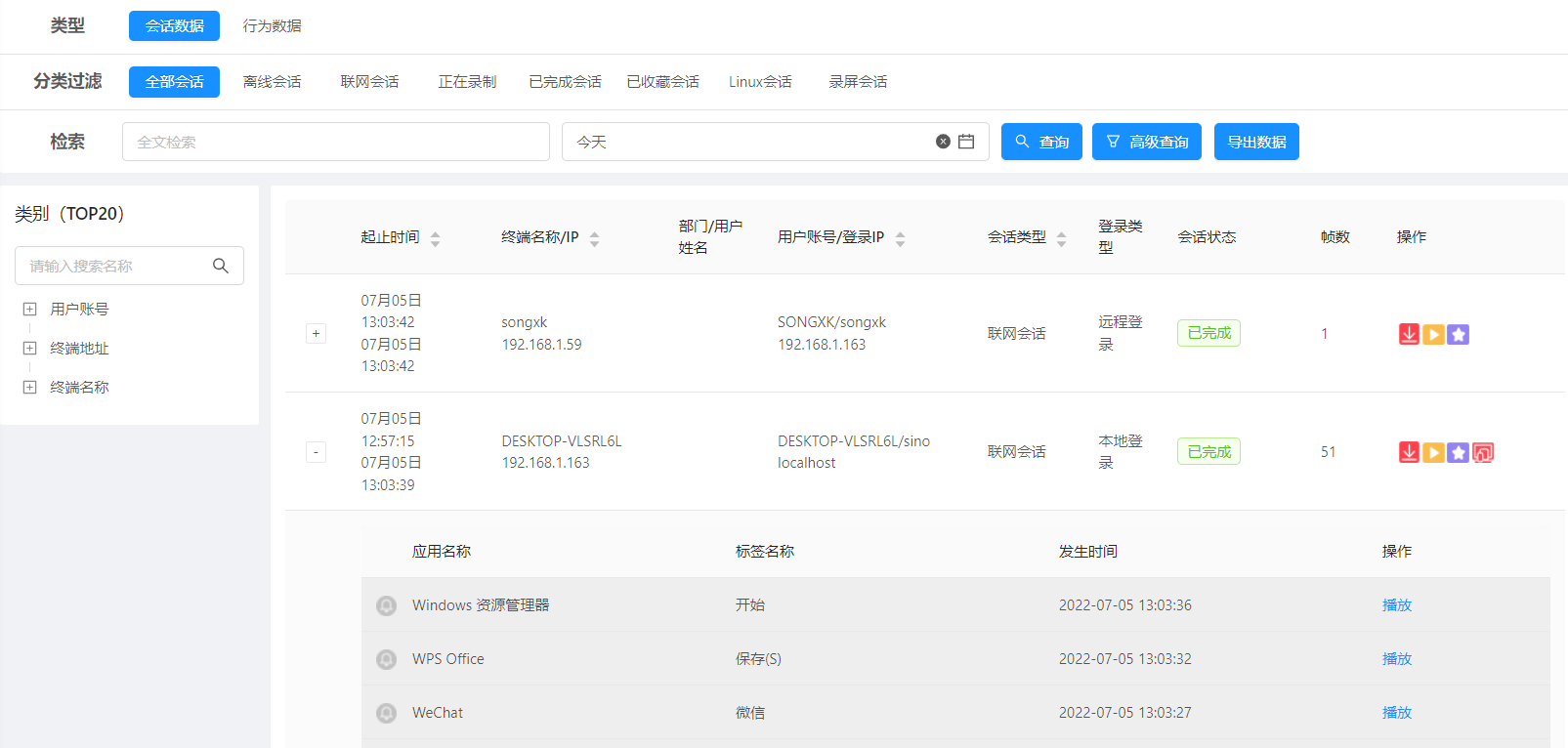
会话数据表示一段时间内的连续操作产生的视频数据。记录操作的时间范围、终端名称、终端IP、用户账号、用户登录的地址，打开会话详情可以查看该会话中包含的具体操作分类（以窗口标题、操作标签、URL、远程指令等分类展示），可以直接定位到录屏中某个操作的触发点，不需要再通过视频一段一段的播放查找。

行为数据将终端的操作数据根据操作类型分为了：应用记录、上网记录、剪贴板、文件操作、移动设备、远程运维、QQ、邮件、微信（企业微信）、钉钉、操作标签、POST报文、Linux记录。

* **会话数据**

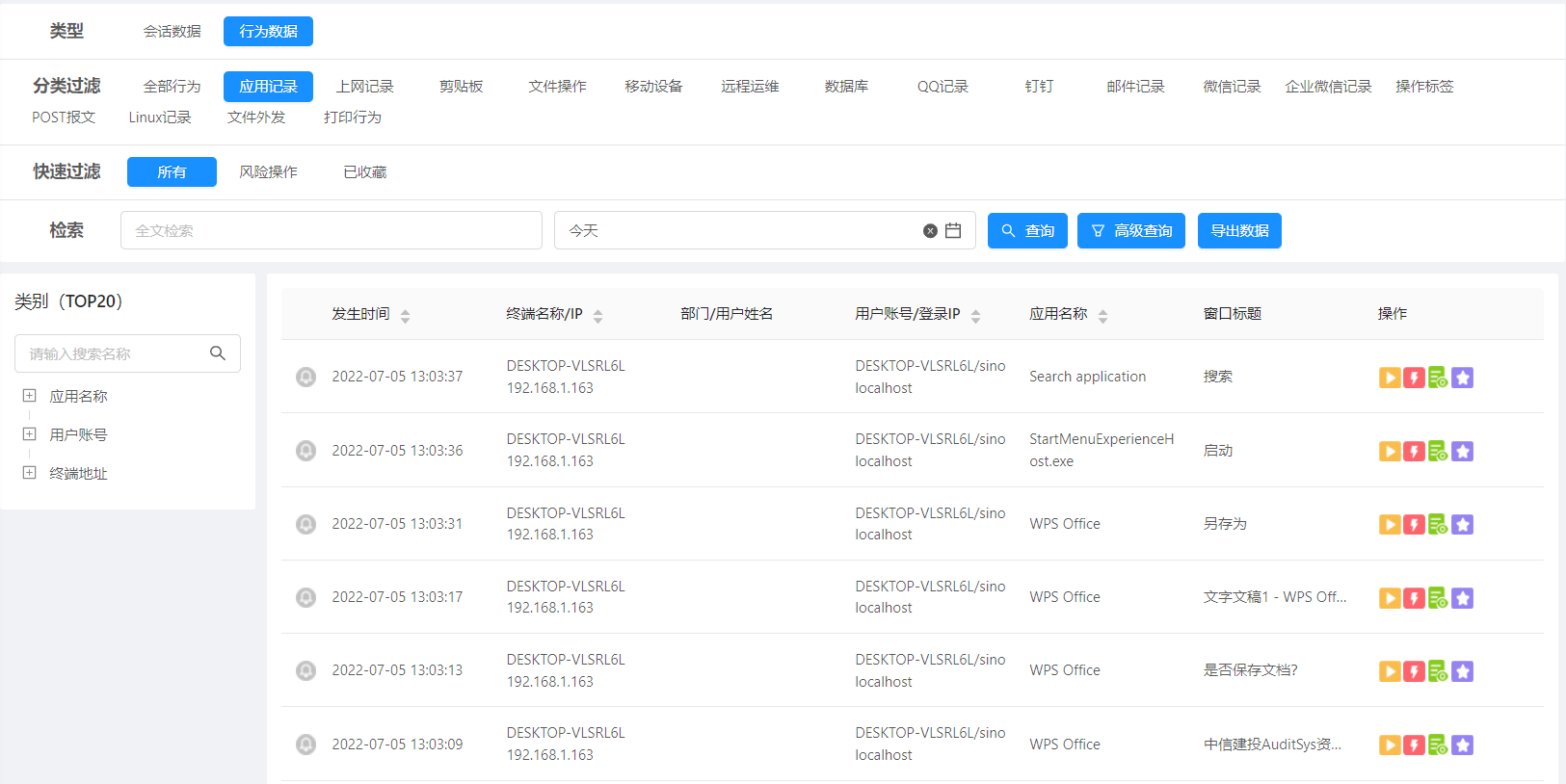
会话数据展示所有操作连续录屏，直接播放查看时间段内所有操作，详情中播放具体操作点可以直接定位到视频中该操作的位置，无需从头播放。

会话中**离线会话**指终端在连接不到服务器的情况下产生的操作数据会存放到本地，再次连接到服务器后自动上传的数据，可以有效地防止由于连接不到服务器而漏记漏录；**联网会话**指从终端抓取数据后正常上传到服务器的会话；**正在录制**指当前会话为连接状态的，视频没有满100帧并且没有超时未操作的会话；**已完成会话**指所有非增在录制的会话；**Linux会话**指客户端为Linux系统的会话。**已收藏会话**指管理员主动收藏的会话。

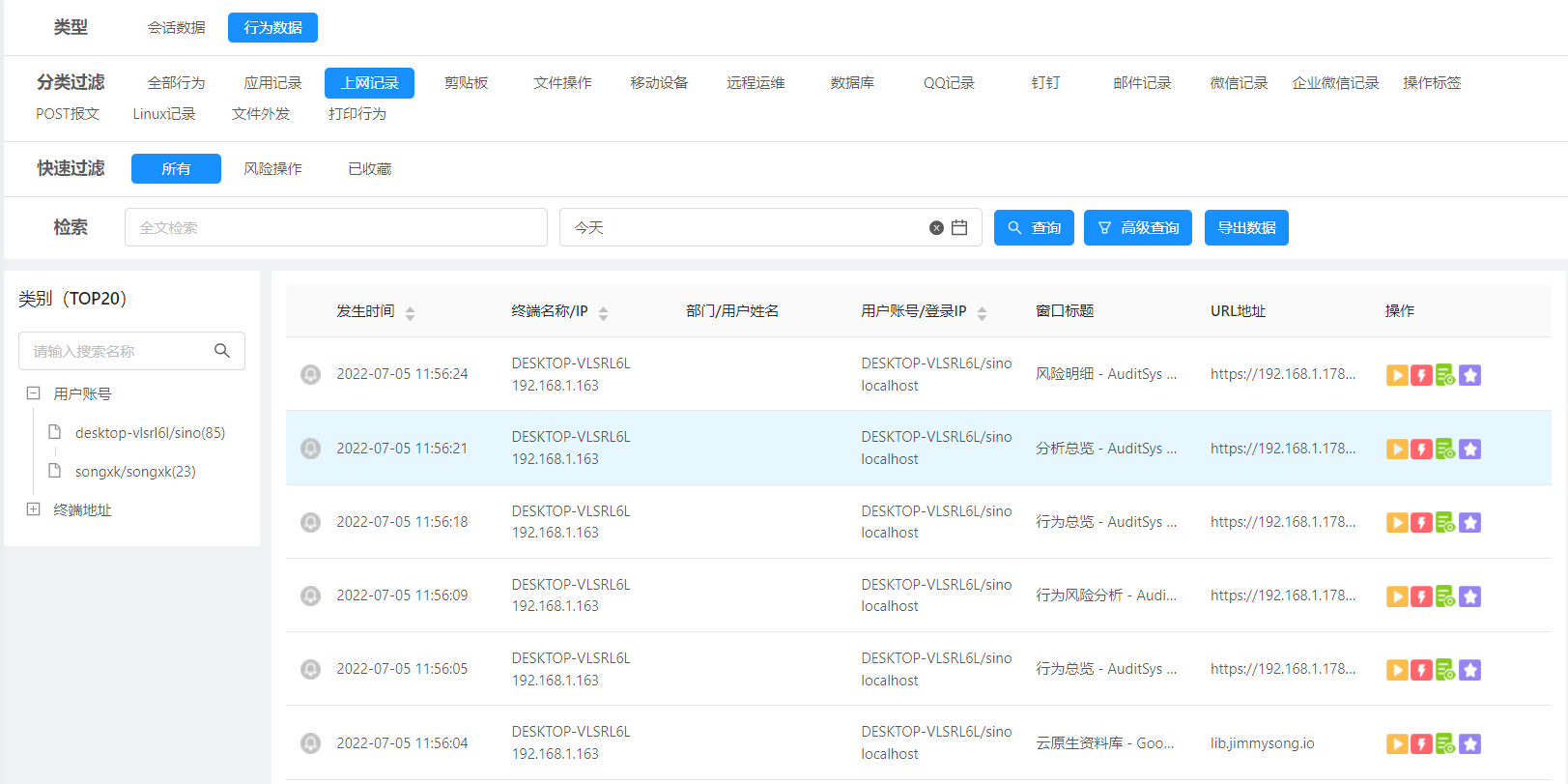


* **行为数据**

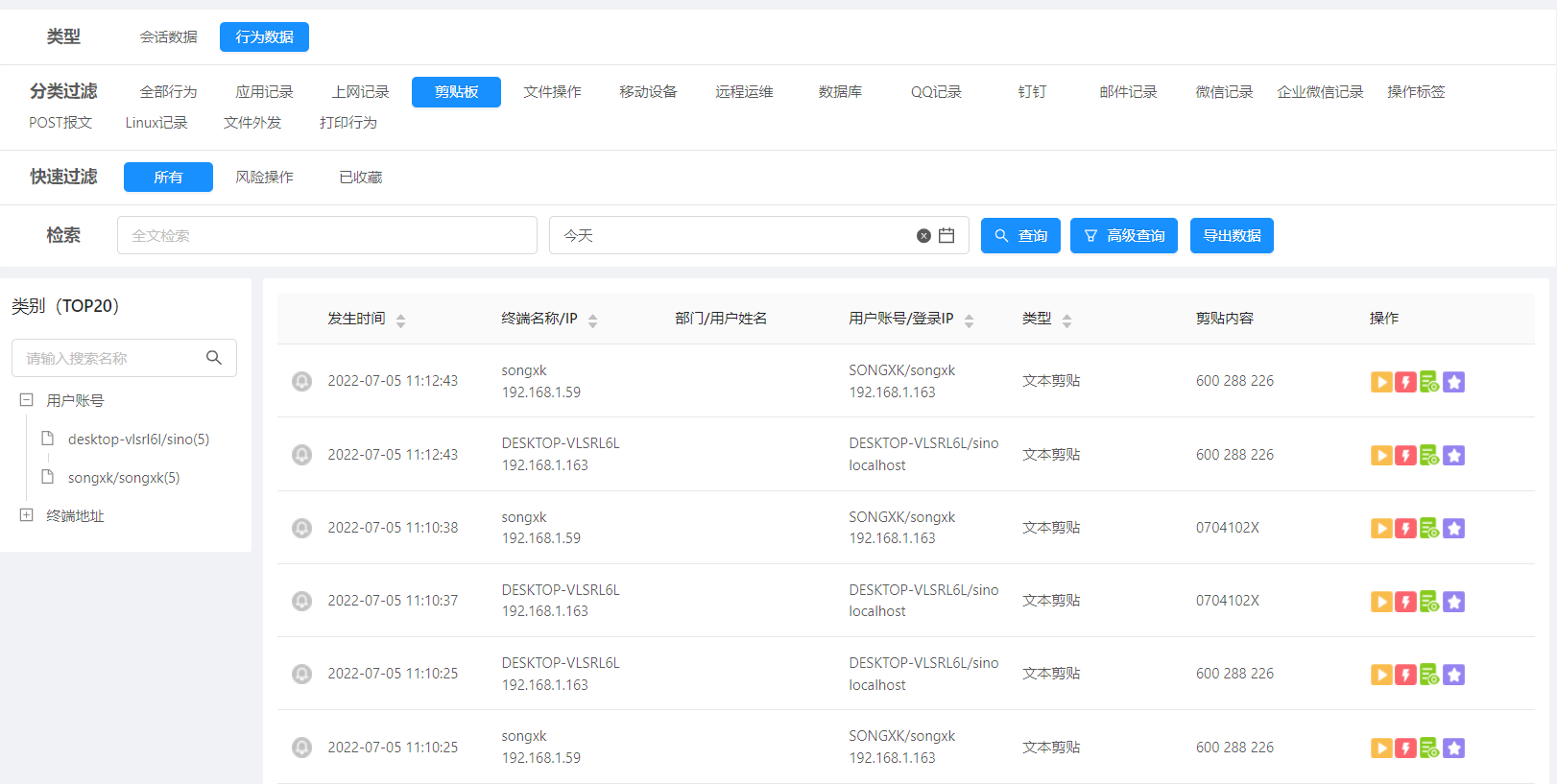
**应用记录：**将操作记录以应用程序的维度展示，包括应用名称、EXE名称、窗口标题的记录，可以通过左侧栏的应用名称、用户账号、终端地址进行快速组合查询。



**上网记录：**指的是所有使用浏览器访问的记录，详细记录了访问浏览器的窗口标题、站点地址、URL地址、应用名称（浏览器的名称），可以通过左侧栏筛选用户账号、终端地址，也可以直接搜索想要查询的地址或访问的窗口标题。（比如想查看是否有人访问过百度贴吧，可以直接搜索tieba.baidu.com）



**剪贴板：**这里汇总了所有终端在系统中复制或剪切的文字内容，可以查看剪贴板剪贴的详细内容，如果有开启敏感词功能，会展示剪贴内容中是否包含敏感词。

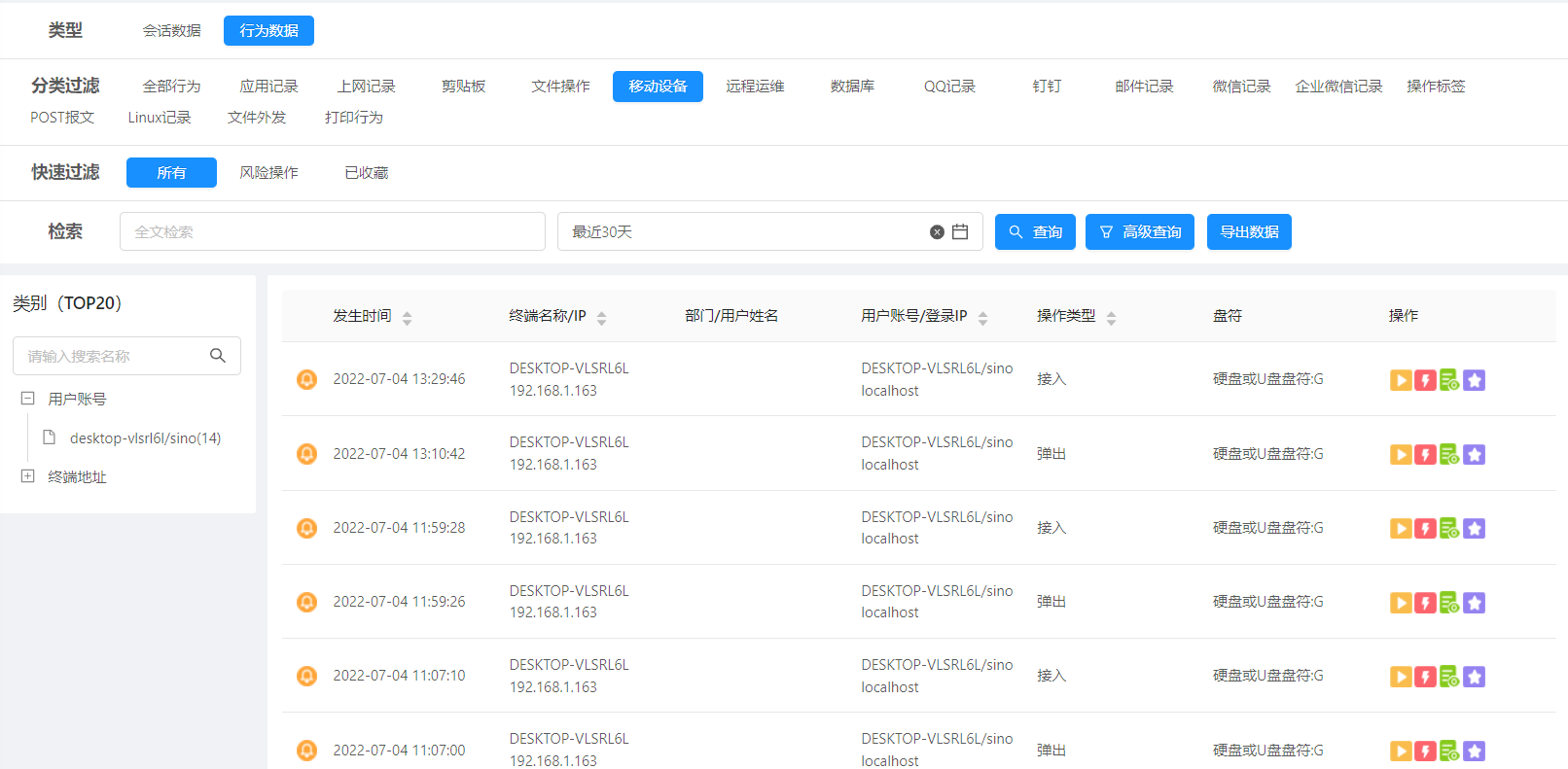


**文件操作：**针对文件的操作记录展示，用户对文件的移动、复制、删除、重命名操作，防止文件外传查看更方便，控制台展示文件存在的磁盘类型（本地磁盘、可移动设备），如果是移动或复制操作还会展示目标目录的磁盘类型，以及文件数量、大小、源目录和目标目录。

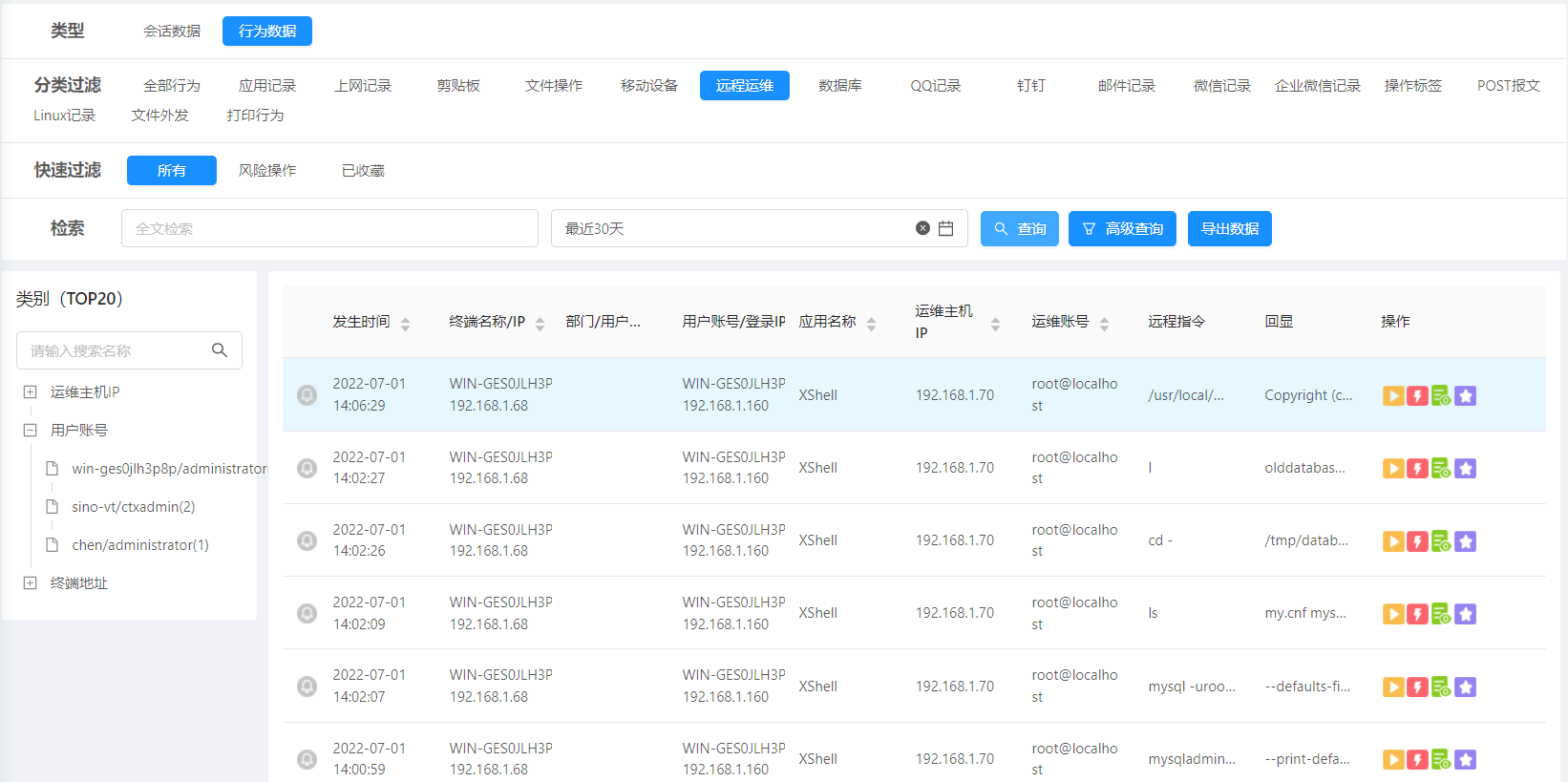




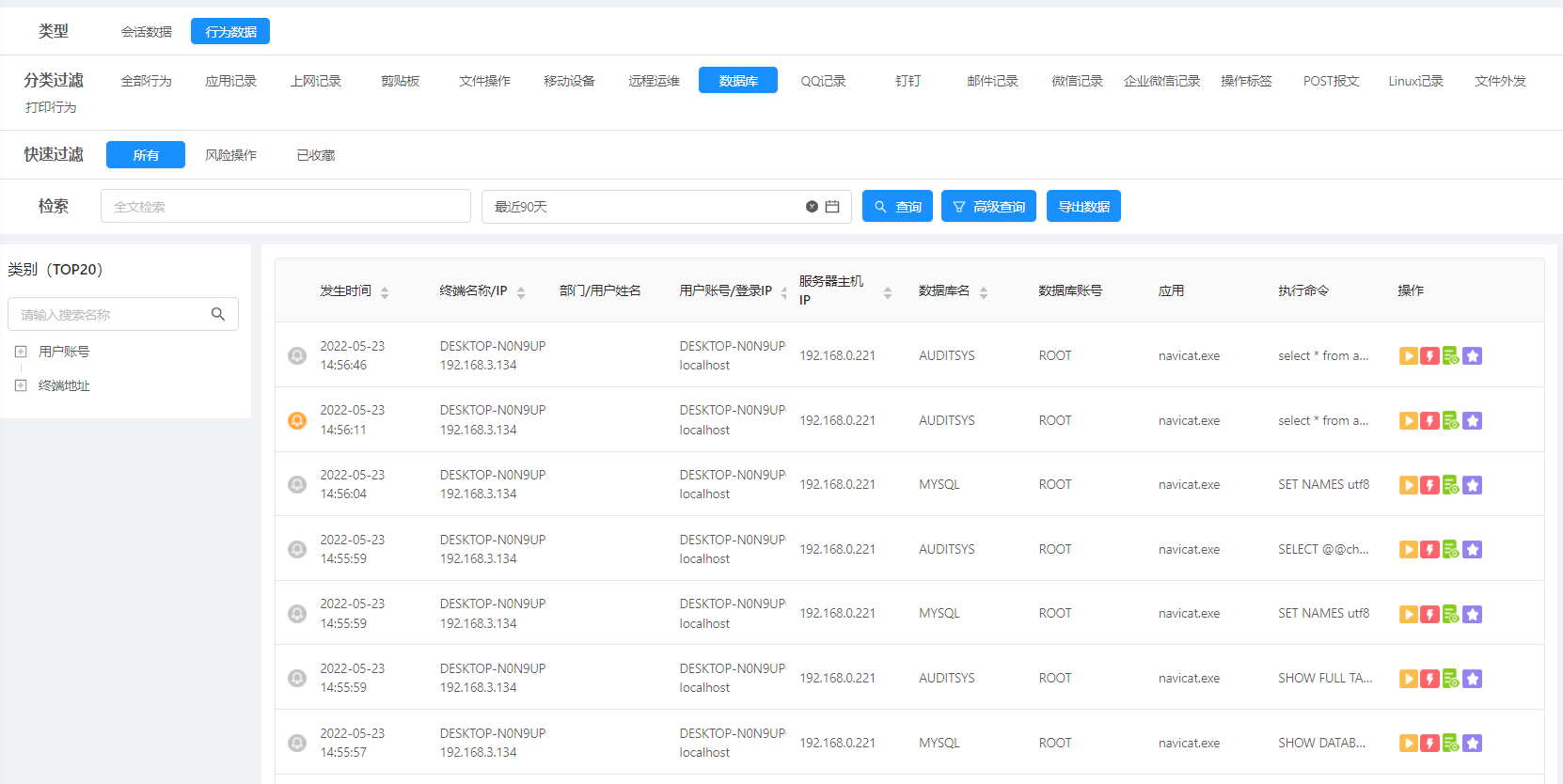
**移动设备：**指U盘、移动硬盘、手机等有存储功能的USB外部连接设备，接入、弹出时间、接入后使用的盘符，这种设备经常涉及到数据外传，一些场景下客户是不允许终端使用USB的，可以通过该功能来检查是否有终端违规使用USB痕迹。



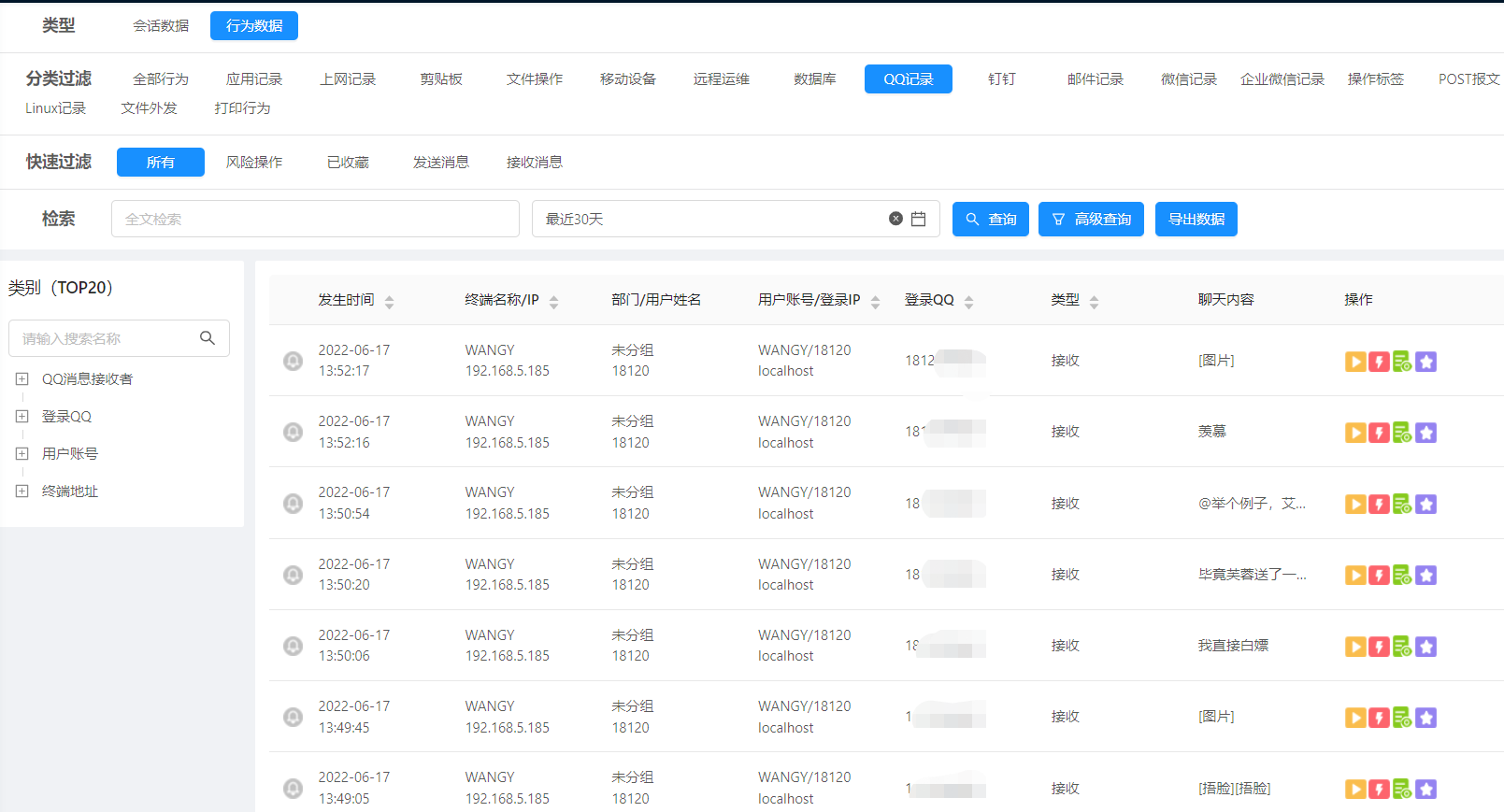
**远程运维：**指的是用户使用Xshell、SecureCRT、Putty这些远程工具去连接了Linux/unix的服务器远程对服务器进行的操作记录，SinoUEBA（AuditSys）会记录远程工具的应用名称、远程连接的服务器IP地址、登录远程系统的账户名、使用的运维命令以及命令执行后的回显内容。

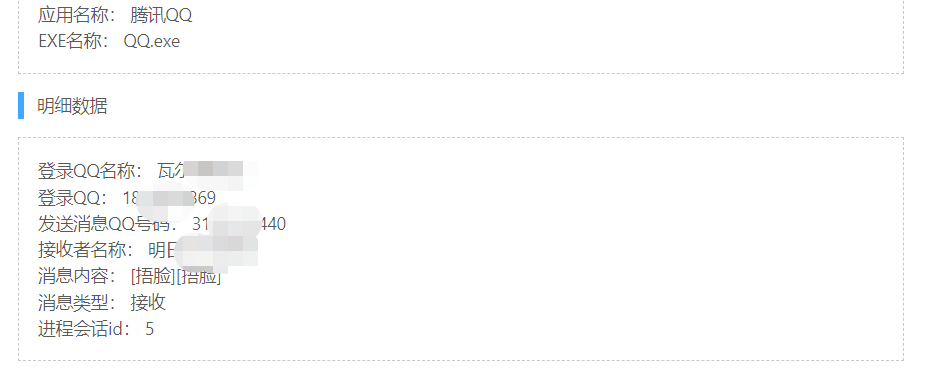


**数据库：**指通过数据库连接工具SSMS、PLSQL Developer、Navicat等工具连接到数据库执行的数据库命令，也会记录使用的工具名称、数据库名称、登录数据库使用的账号等信息。

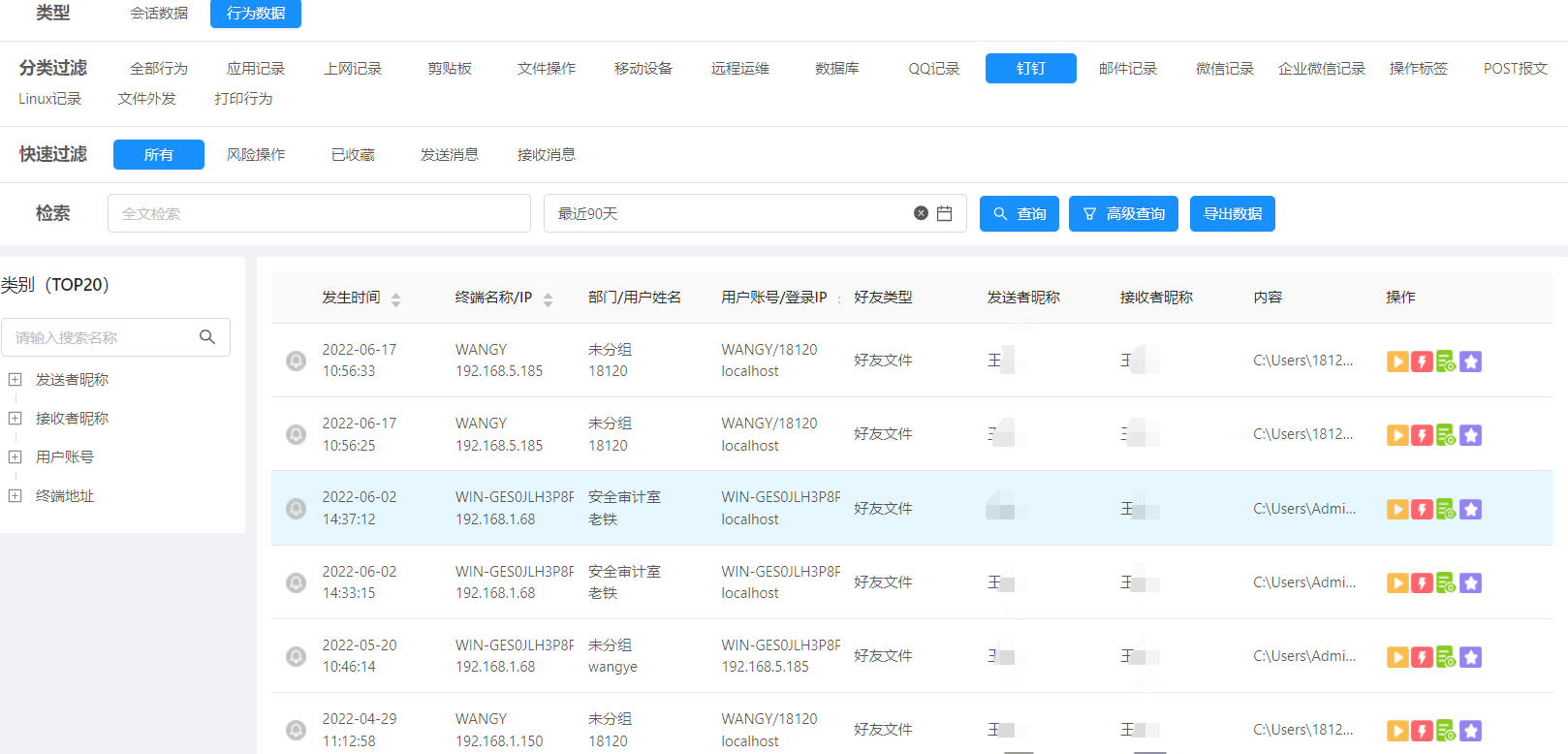


**QQ记录：**如果用户终端环境使用外网，聊天工具也是一种可以泄露数据的方式，SinoUEBA（AuditSys）可以将QQ聊天内容记录下来，包括收发人的昵称和网名，发送的文件也会记录，如果使用了SinoSDP功能模块，文件中有触发敏感词的内容还可以从控制台把相关文件的原件下载下来，QQ的消息记录会展示消息的收发类型、发送文件的名称、聊天记录，也会展示是否触发敏感词。

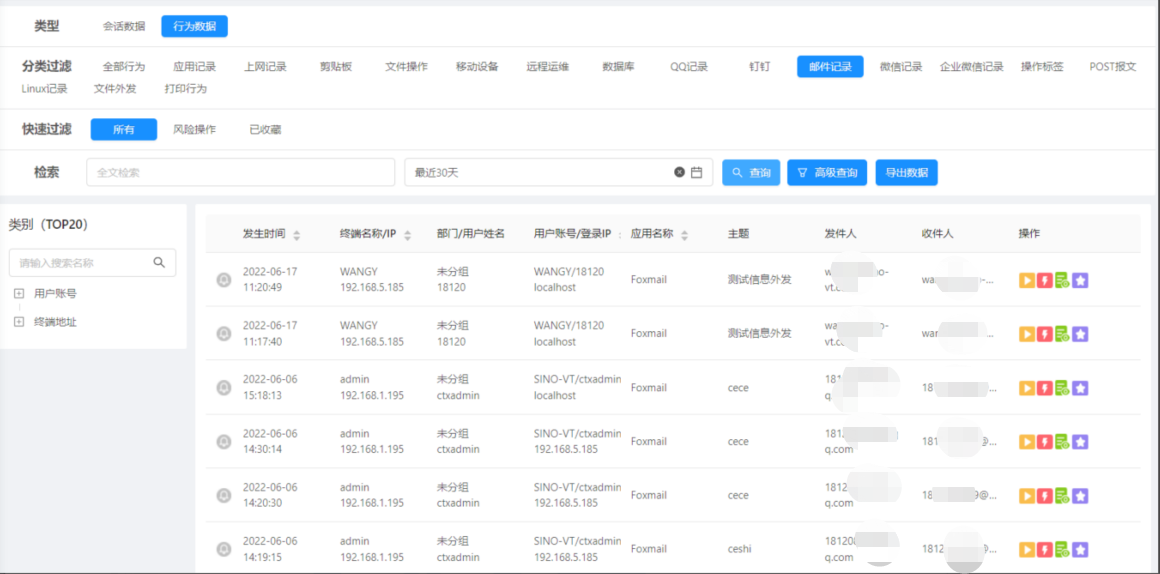


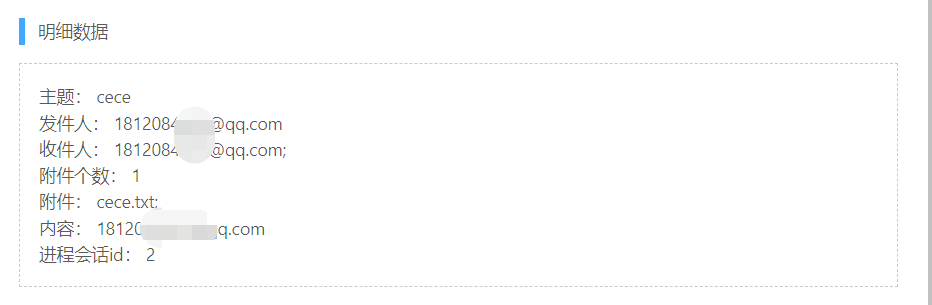


**钉钉：**和QQ记录类似，记录了钉钉聊天中收发的消息内容、文件、是否涉及敏感词，以及来往消息双方的钉钉号、昵称和备注。钉钉和QQ记录都可以通过收发类型来快速检索，更加有针对性。

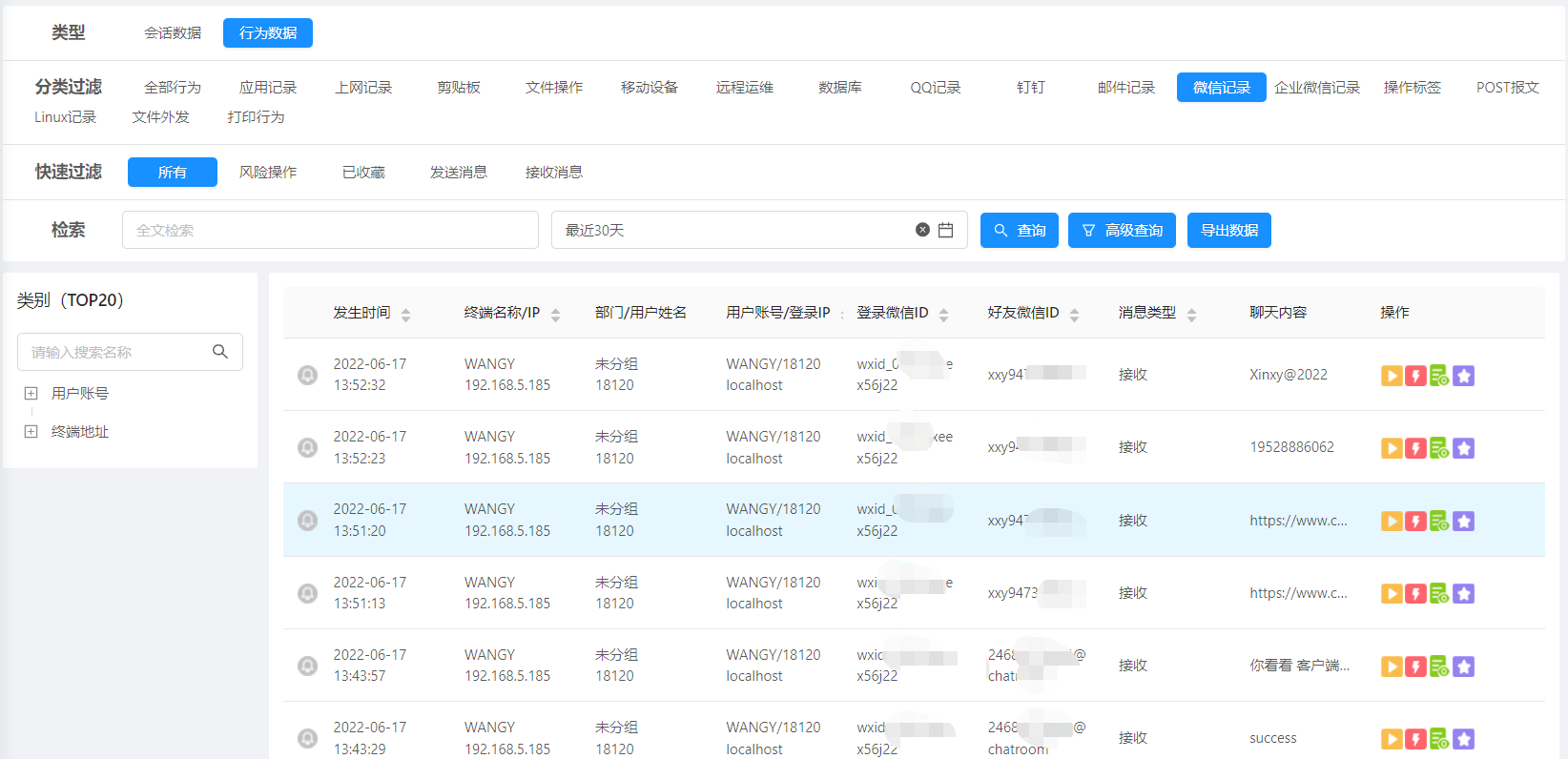


**邮件记录：**记录通过Foxmail、Outlook等应用执行的邮件发送操作，记录用户使用的工具名称、发件人、收件人、邮件的标题、是否触发敏感词。

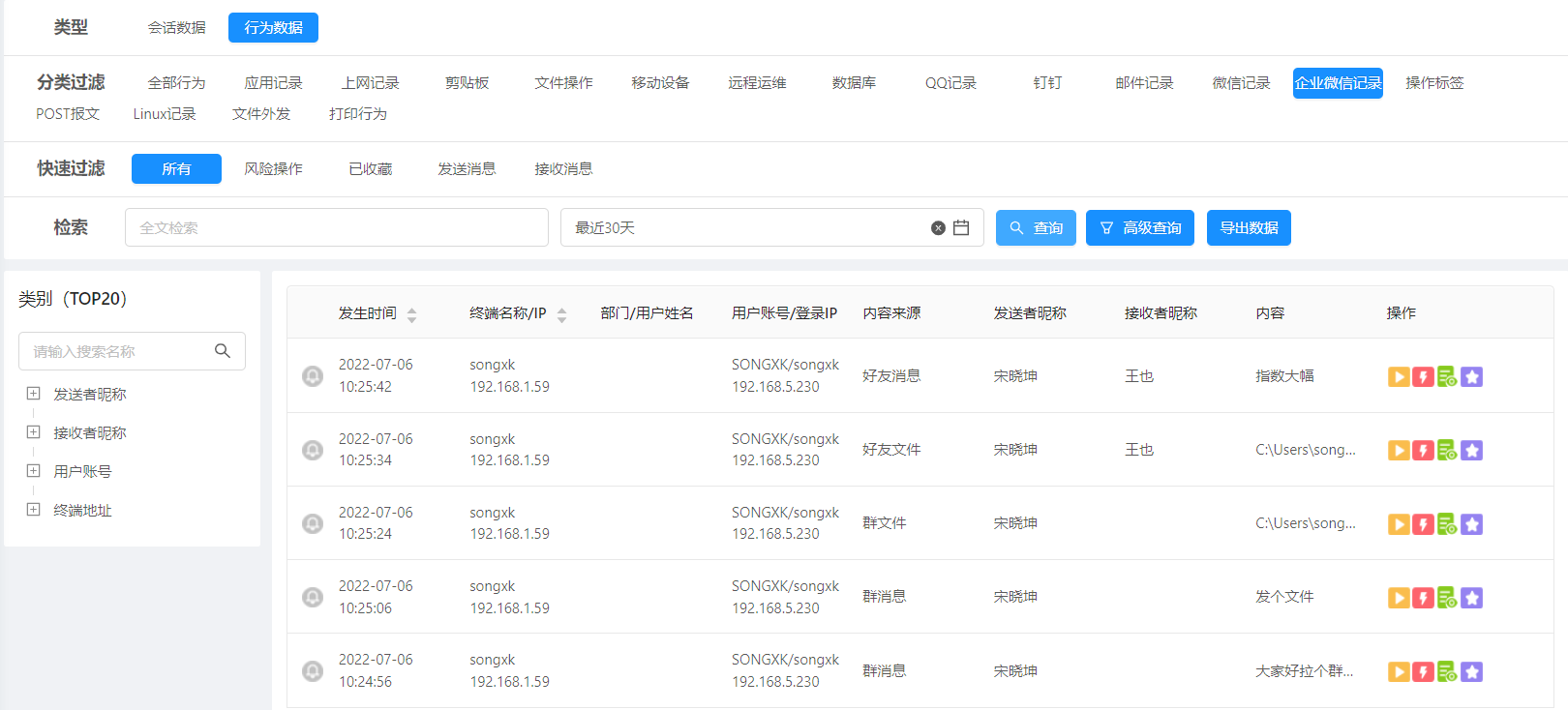




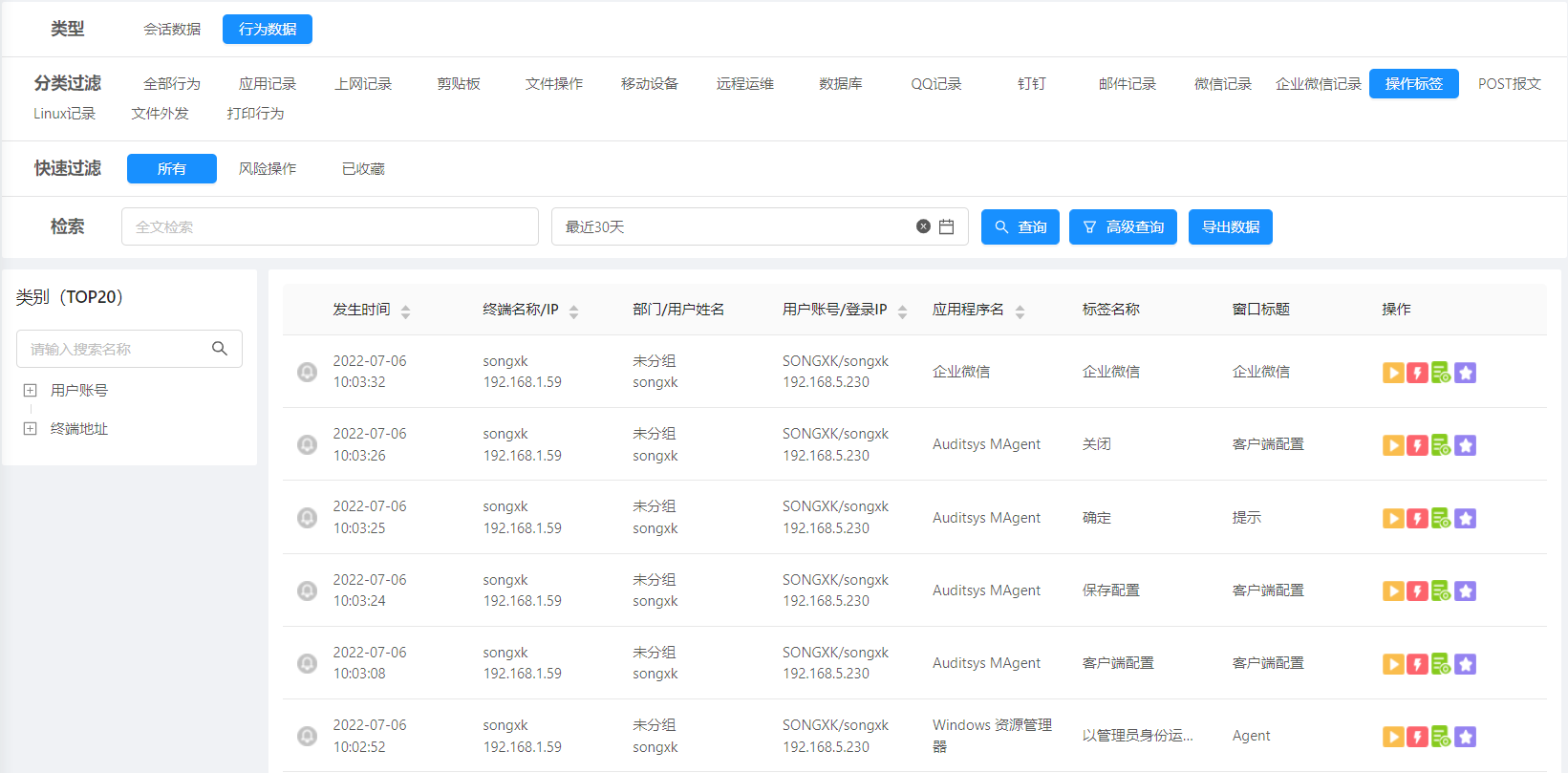
**微信记录：**和QQ记录类似，记录了微信聊天中收发的消息内容、文件、是否涉及敏感词，以及来往消息双方的微信号、昵称。微信、钉钉和QQ记录都可以通过收发类型来快速检索，更加有针对性。



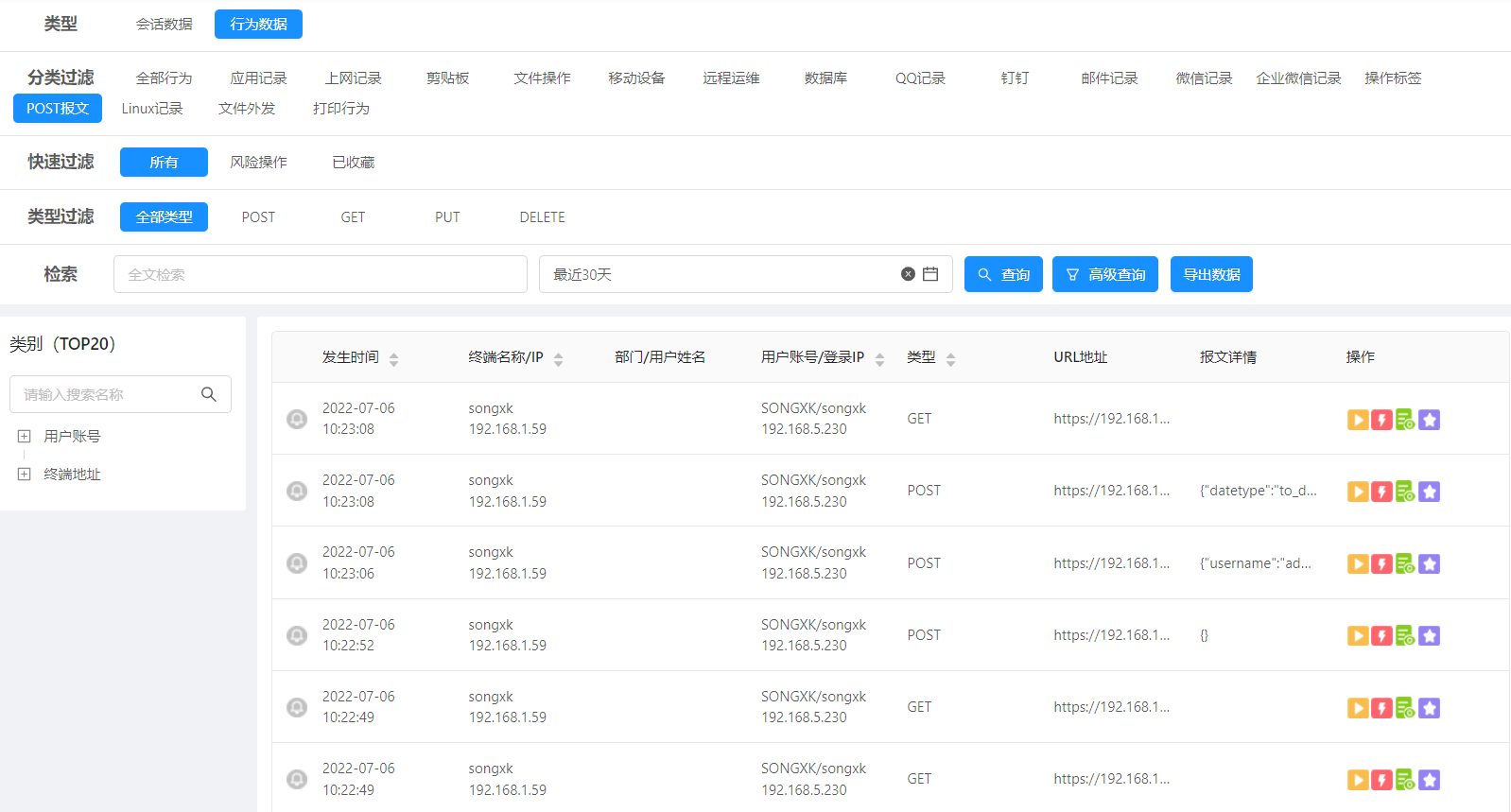
**企业微信记录：**和QQ记录类似，记录了企业微信聊天中收发的消息内容、文件，以及来往消息双方的名称。可以展示企业微信的消息来源。



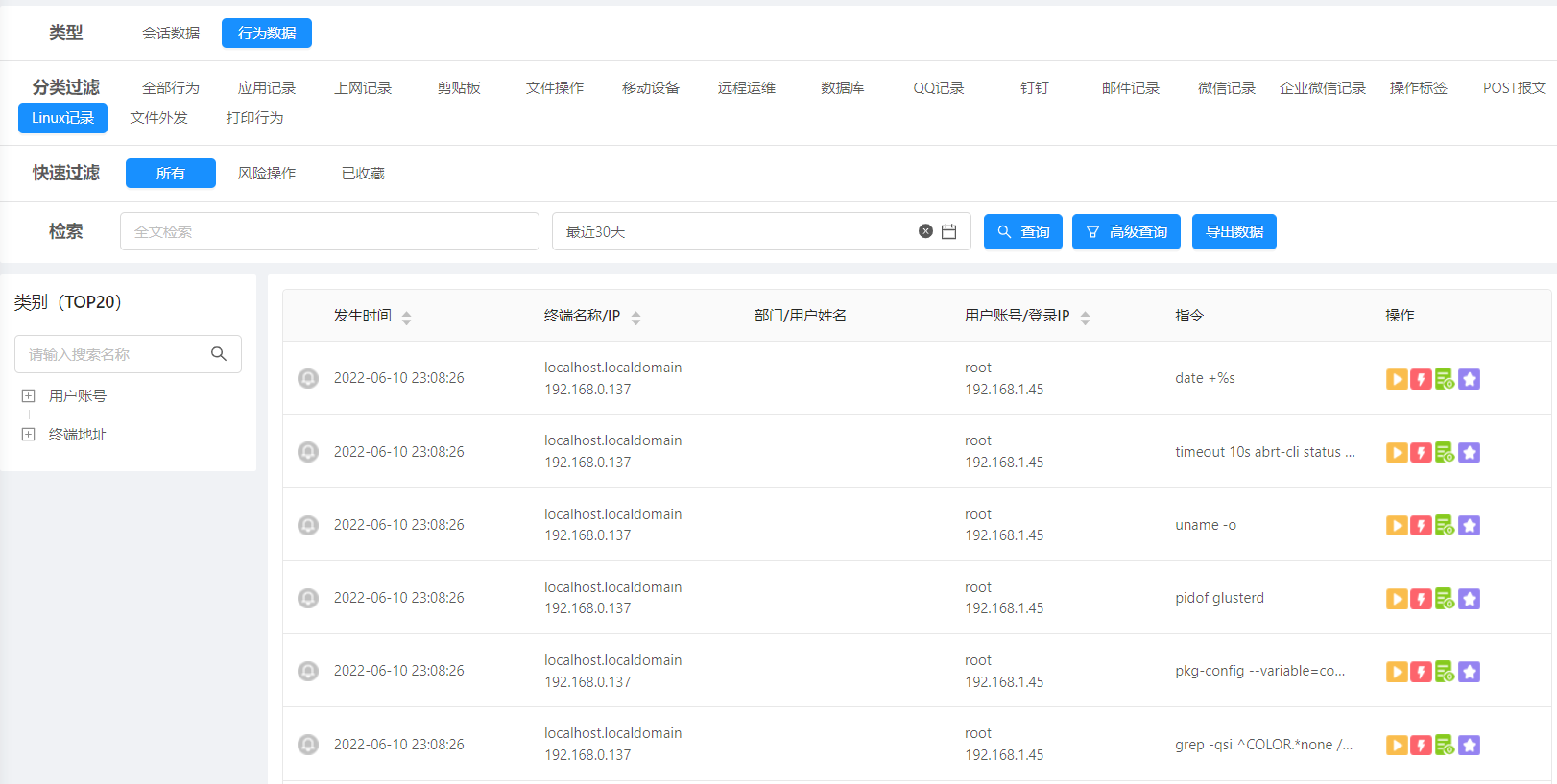
**操作标签：**指的是用户在使用应用时操作的一些按钮，可以通过这些按钮更准确的确定用户有没有进行一些具体的操作（比如导出、发送等动作）



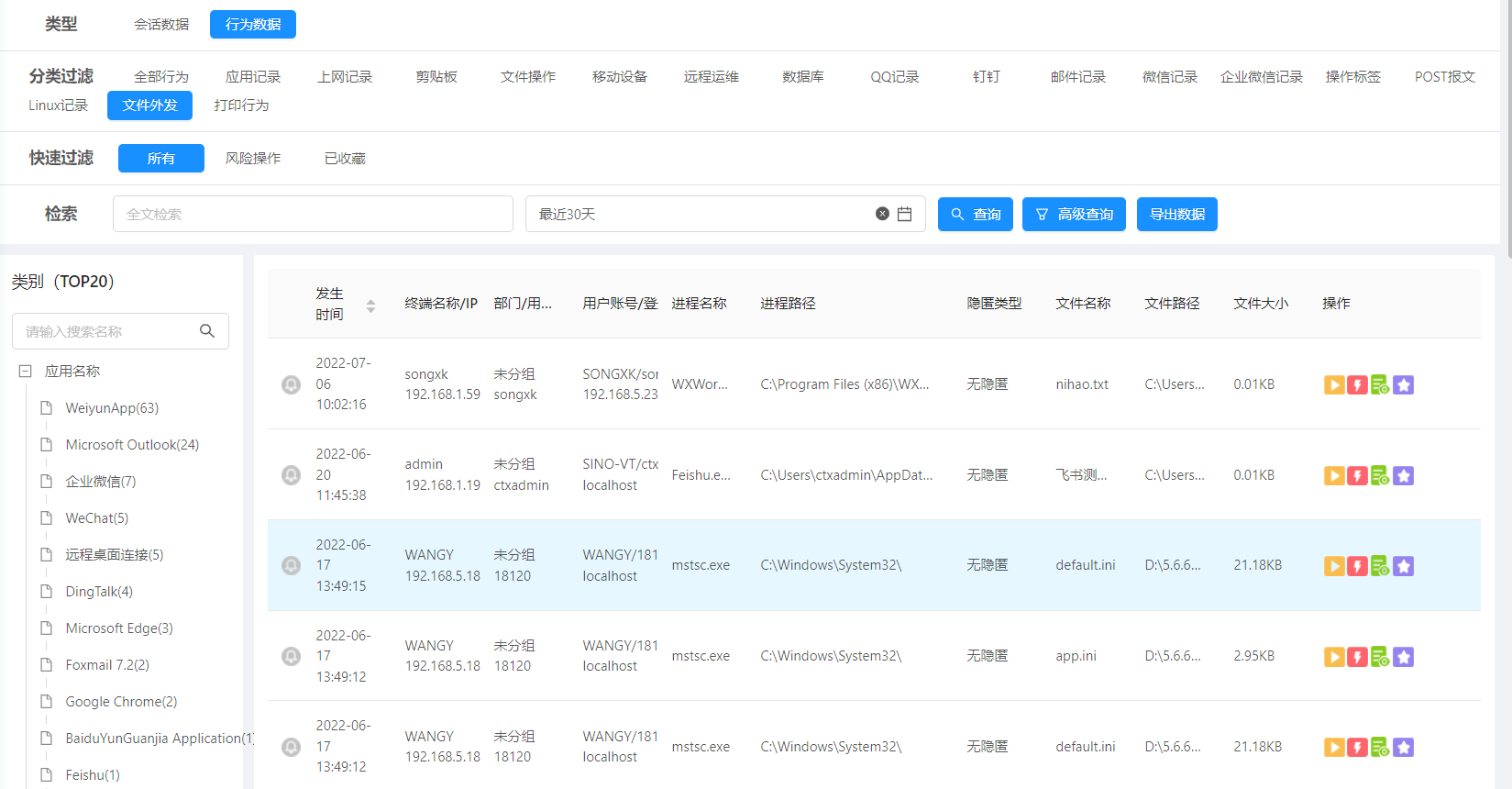
**POST报文：**可以获取未加密的报文信息，另外支持POST、GET、PUT、DELETE类型的报文，报文字段可以根据需求配置改写，方便查看报文内容。（支持主流IE、谷歌浏览器）



**Linux记录：**这里和远程运维中的效果不太一样，这里记录的是终端为Linux系统安装了我们的Agent获取到的数据，包括命令和回显。



**外发文件：**文件外发是用户在终端本地上传文件到外部应用的操作审计（百度云、360云盘、腾讯微云、QQ、微信、U盘、邮件等），可以通过左侧栏应用的名快速过滤。



**打印行为：**是用户在终端进行打印操作审计（支持网页、文档、应用等打印操作）



# 系统管理

* **管理员权限**

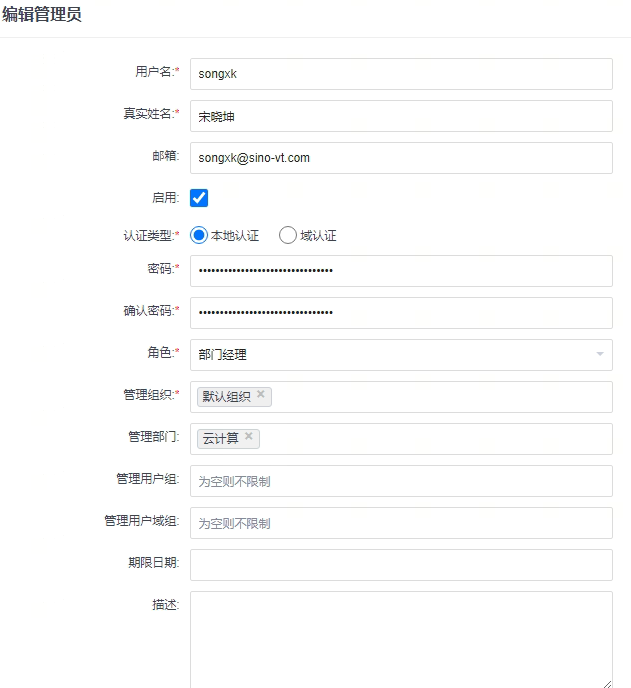
SinoUEBA（AuditSys）支持多个管理员同时登陆，超级管理员admin可以添加普通管理员，每个管理员的操作在平台都有日志记录。通过角色设置可以为管理员分配不同的权限，防止出现越权情况。

角色设置从菜单功能项维度以勾选的方式来控制管理员可以使用的功能，结合管理员绑定部门、组织、用户组等，来决定管理员可以访问的数据范围。

角色配置：



管理员配置：

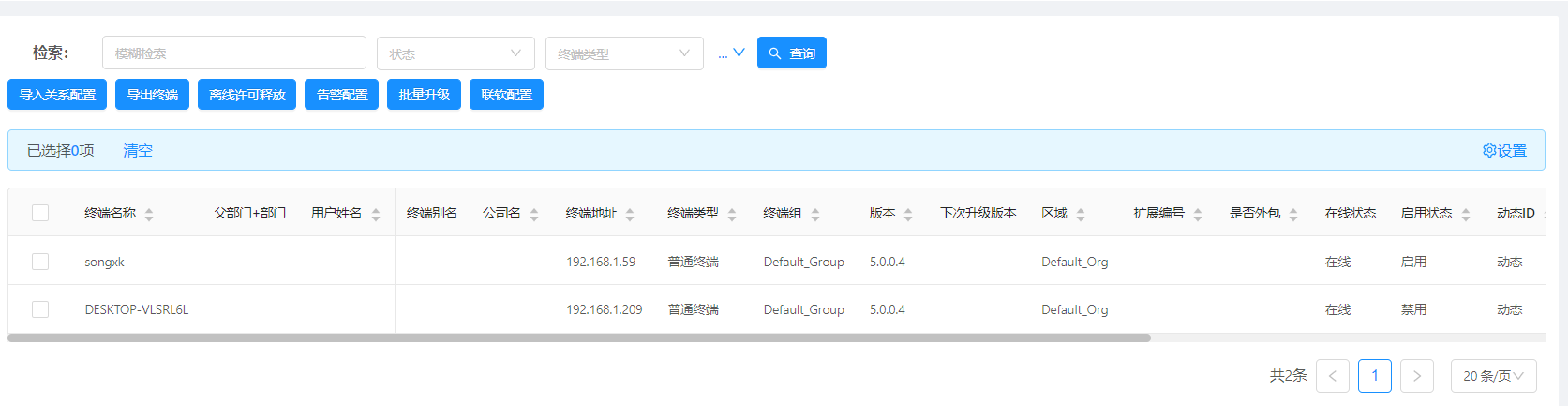


管理员登陆SinoUEBA（AuditSys）支持与Radius服务对接,对用户身份进行再次认证，更安全。



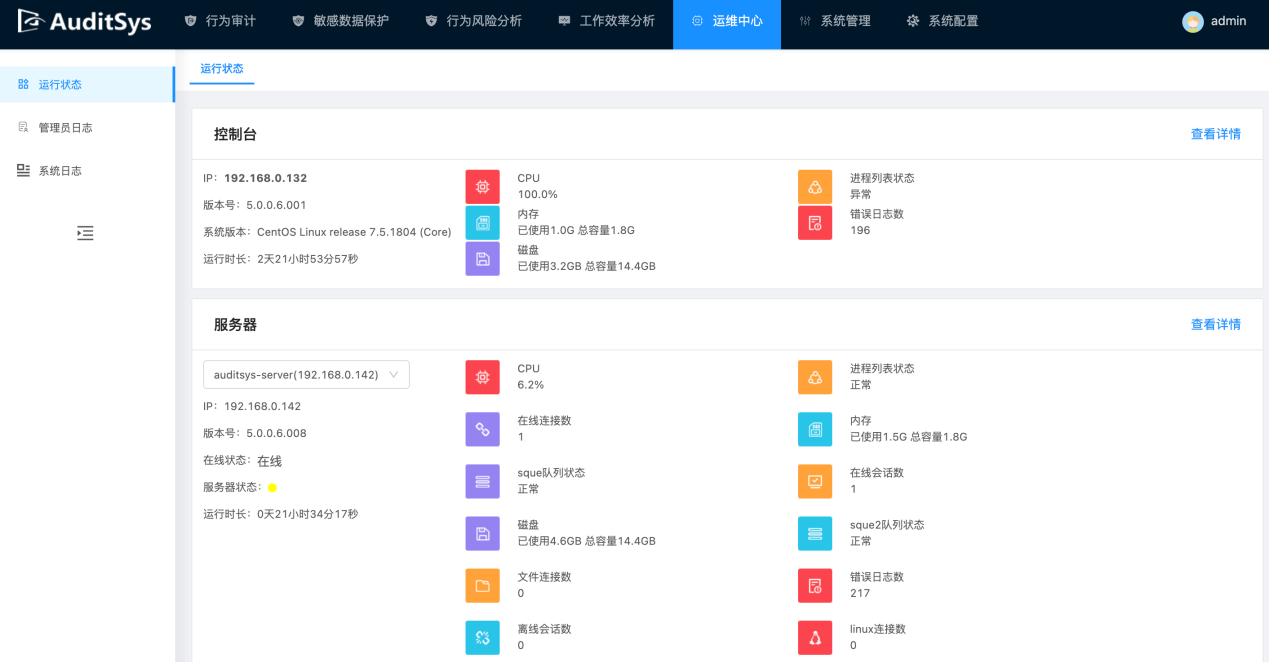
* **终端管理**

SinoUEBA（AuditSys）支持从控制台对终端管理，直接控制那些终端卸载、开启或禁用，在不需要记录某终端操作数据的时候直接禁用即可，无需终端用户卸载，需要记录时再次安装的反复操作，同时支持软禁用，当客户端有操作后自动开启减少管理员维护工作量。终端信息支持导入导出。展示字段可以通过列表右上角的设置按钮自定义。



* **服务管理**

SinoUEBA（AuditSys）提供服务概览页面。管理员可以从控制台查看服务器进程状态、资源消耗等信息，无需每台服务器登录检查。



# 产品特点

* **低消耗**

客户端Agent只在客户端活动时活动，客户端占用的CPU和内存资源和用户数量以及用户操作记录情况有关。一个活动用户会话大约会占用0%-1%的CPU和5-30M内存

客户操作时才会有记录，无操作不录屏，加上SinoUEBA（AuditSys）采用变量存储的方式,大大减少了服务端录像文件对磁盘的占用，一个用户以一天8小时的操作量计算，一天的视频数据大约120M-150M。

* **多屏录制**

支持多屏录制，一些终端用户使用扩展屏，在操作时SinoUEBA（AuditSys）会记录所有屏幕的变化，在播放时可以同时展示所有屏幕操作，也可以根据屏幕编号选择单独播放，屏幕排序与终端系统设置一致。

* **对接其他平台**

SinoUEBA（AuditSys）支持对接SIEM平台，通过syslog协议将SinoUEBA（AuditSys）的日志数据输出到SIEM平台,方便客户对数据进一步分析处理。

* **支持客户端通知**

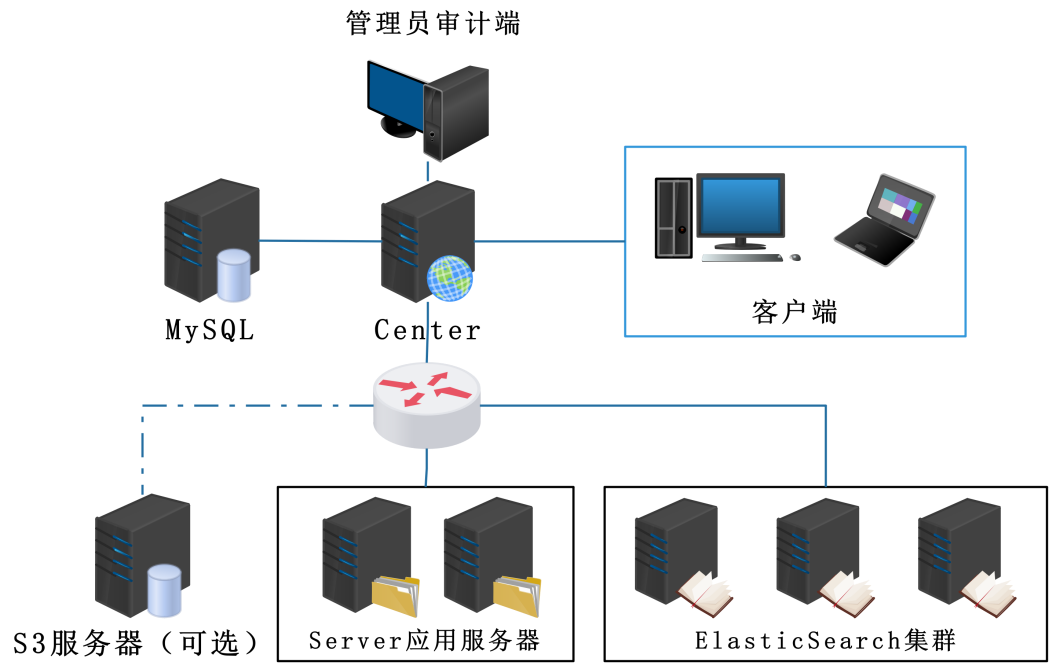
当客户端触发风险规则或操作中涉及敏感词，SinoUEBA（AuditSys）将通过弹窗的方式在客户端桌面提醒，管理员可以分别自定义触发风险规则和触发敏感词后的提示内容，并可以设置提示频率。督促和帮助用户规范自己的日常操作行为。

# 产品部署

SinoUEBA（AuditSys）部署需要把客户端Agent安装到每个需要被监控的终端（服务器、物理PC、虚拟桌面）上，通过Agent捕获所有终端用户的操作并把数据传到服务端。服务端我们将数据分为日志记录、录屏记录，分别存在ElasticSearch和Server应用服务器，外发敏感数据文件存储在S3对象存储中。Center服务和MySQL一般部署在同一台服务器，如果需要可以分开部署。

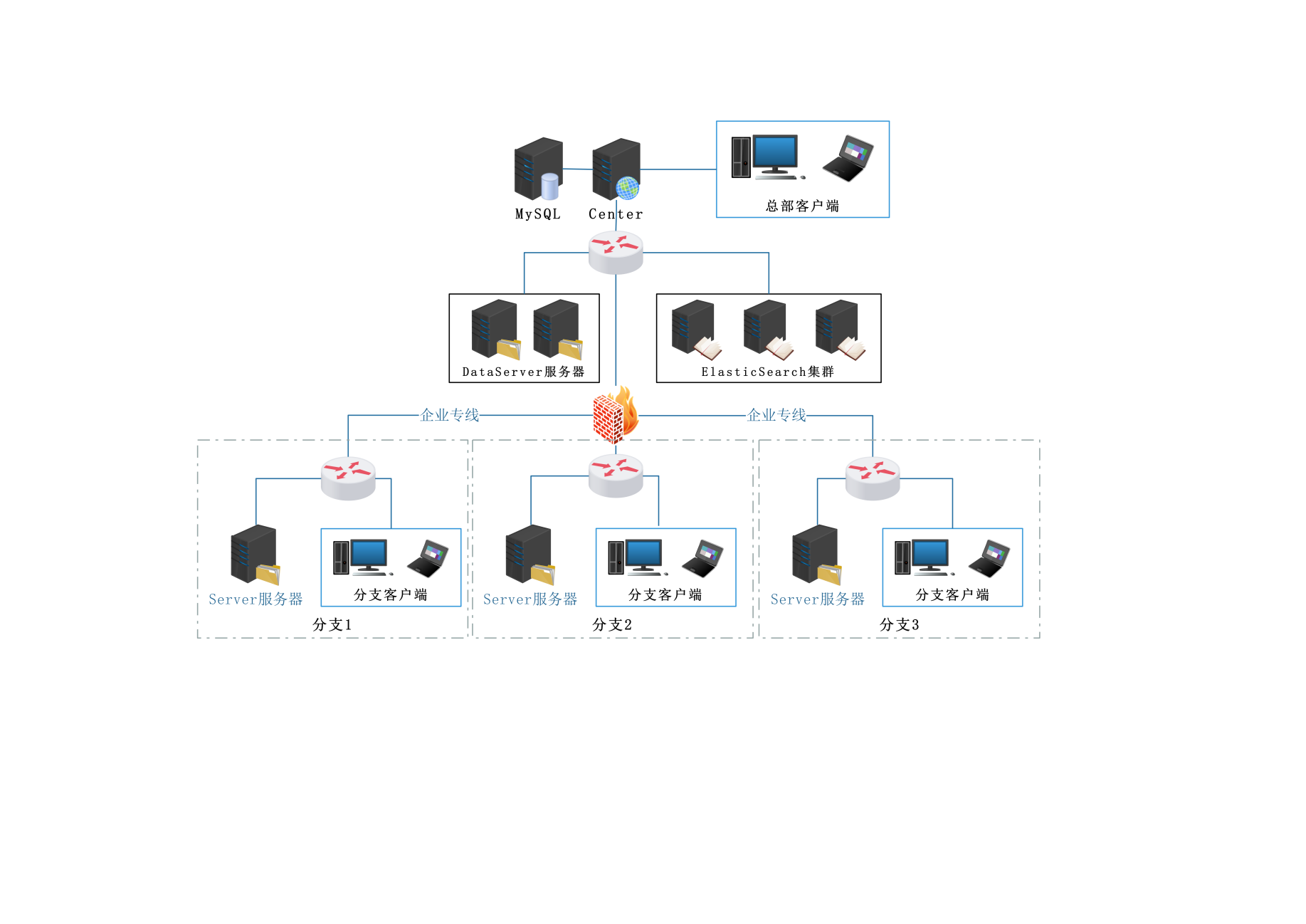
## 集中式部署

在终端用户集中的场景下，网络没有跨外网，不用考虑带宽占用问题，我们将SinoUEBA（AuditSys）服务端集中部署在局域网内，与客户端之间开放接口，客户端通过注册后有数据就可以直接实时的上传到Server服务器，S3服务器负责备份外发文件和录屏文件数据（可选）。



## 分布式部署

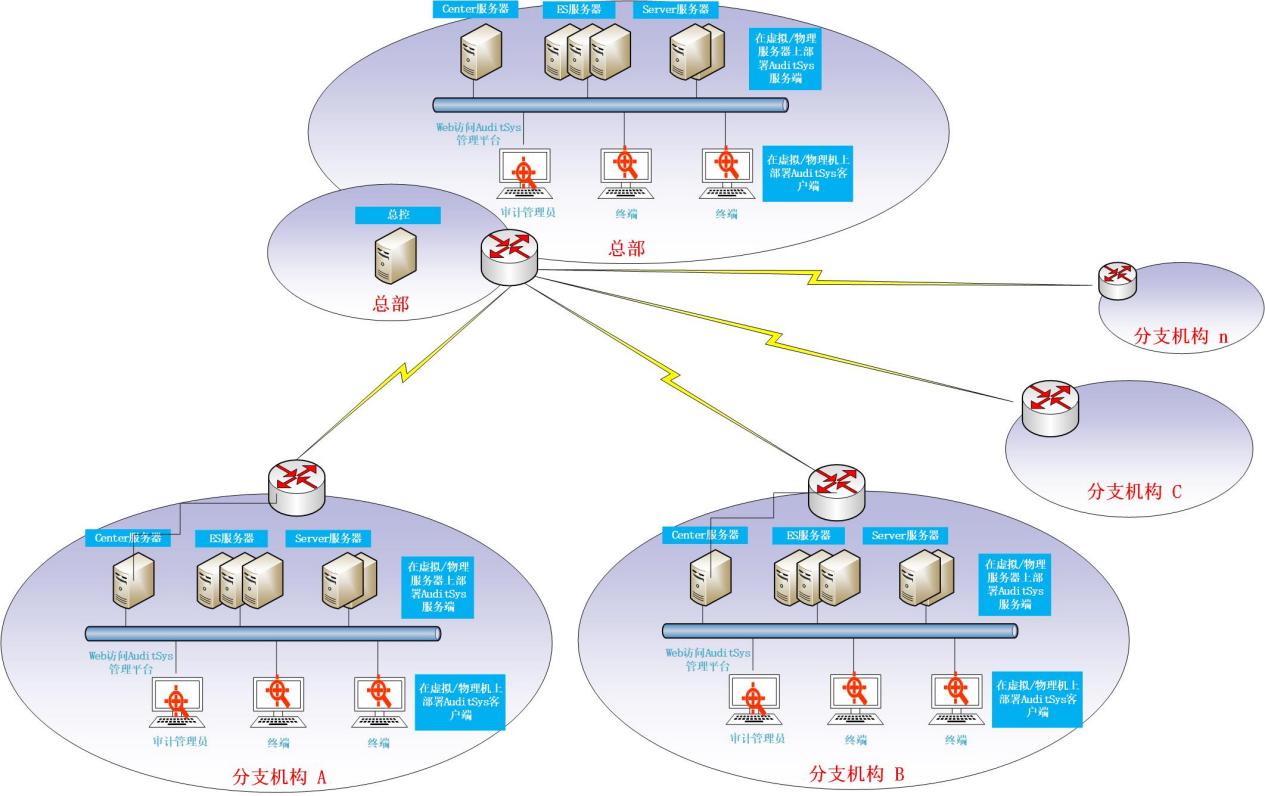
SinoUEBA（AuditSys）为了满足存在大量分支机构的客户，服务器部署困难，数据传输占用带宽高，维护成本高的问题，推出了分布式部署架构模式：在各个分支机构部署一套Server边缘计算服务器，接收从Agent端上传的数据并在非工作时间将数据传输至总部，减少带宽压力。



## 多中心部署

多中心架构场景下，主要体现在总部部署总控中心，在各个分支机构单独布置一套分管中心，实现总部统一管辖能力。主要优势可以降低带宽占用率，分管中心数据分析引擎分布在各中心，解决跨站点占用带宽难题。

其实现架构部署如下：



* 适用场景：多中心、分支机构
* 架构优势：总部可利用总控平台可直接调用各分支机构的独立系统

## 部署规模设计

1. **小规模部署**

在用户规模较小的部署模式下（如小于500个客户端），我们可以采用将Center、MySQL、Elasticsearch部署到一台服务器，Servre单独部署到一台服务器的方式来部署。如下图：

**应用服务器系统需求：**

* 物理 CPU 双核 2.4GHz
* 内存 16 GB
* 系统盘使用50G的高速磁盘，录像数据可放本地磁盘或NAS等共享存储，容量大小依据用户并发量而定。

**Center+MySQL+ES服务器系统要求：**

* 物理 CPU 双核 2.4GHz
* 内存 16 GB
* 系统盘使用50G的高速磁盘，es数据存储建议设置100G及以上容量依据用户并发量而定。

**S3服务器需求：**（**备份外发文件和录屏文件数据**）

* 物理 CPU 双核 2.4GHz
* 内存 8 GB
* 系统盘使用50G的高速磁盘，数据盘根据数据存储量而定。

1. **中等规模部署**

中等规模的部署时（500-1000个客户端），建议将Center，Server，与Es服务器单独安装 ，且Server建议采用负载均衡方式来部署。

**应用服务器建议配置：**（根据用户数量，确定服务器个数）

* 物理 CPU 八核 2.4GHz
* 内存 16GB
* 系统盘至少使用 100G的高速磁盘，存储根据用户并发量来定，建议采用nas等共享存储。

**Center服务器建议配置：**

* 物理 CPU 八核 2.4GHz
* 内存 16GB
* 系统盘至少使用 100G的高速磁盘

**Es集群服务器建议配置：**

* 物理 CPU 八核 2.4GHz
* 内存 16 GB
* 系统盘使用 100G（至少）的高速磁盘，元数据存储需要单独划分存储。

**S3服务器需求：**（**备份外发文件和录屏文件数据**）

* 物理 CPU 双核 2.4GHz
* 内存 8 GB
* 系统盘使用100G的高速磁盘，数据盘根据数据存储量而定。

1. **大规模部署**

在大规模部署时（超过1500），SinoUEBA（AuditSys） 应用服务器支持自动负载均衡跟故障转移，可以通过部署多台应用服务器，轻松地实现负载故障转移，Center可以采用冷备、Es可以使用集群部署方式技术实现。

**应用服务器建议配置：**（多台实现负载均衡，根据用户数量，确定服务器个数）

* 物理 CPU 八核 2.4GHz
* 内存1 6 GB
* 系统盘至少使用 100G的高速磁盘，录像存储建议采用NAS等共享存储。

**Center服务器建议配置：**

* 物理 CPU 八核 2.4GHz
* 内存 16GB
* 系统硬盘使用 100G的高速磁盘，

**Es服务器集群建议配置：**

* 物理 CPU 八核 2.4GHz
* 内存 16 GB
* 硬盘使用 800G（至少）的高速磁盘， 存储大小根据用户实际数量与保存时间进行计算。

**S3服务器需求：**（**备份外发文件和录屏文件数据**）

* 物理 CPU 双核 2.4GHz
* 内存 8 GB
* 系统盘使用100G的高速磁盘，数据盘根据数据存储量而定。