# 终端违规外联审计平台
# OATD2.0
# 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
1.2 产生违规外联原因 ..... 1
【第 2 部分】 终端违规外联审计平台 ..... 3
2.1 产品介绍 ..... 3
2.2 产品定位 ..... 3
2.3 技术原理 ..... 4
2.3.1 系统架构 ..... 4
2.3.2 数据架构 ..... 4
2.3.3 网络架构 ..... 5
2.3.4 技术架构图 ..... 7
2.3.5 流程图 ..... 8
2.3.6 系统工具说明 ..... 9
2.4 产品功能 ..... 12
2.4.1 资产发现 ..... 12
2.4.2 设备准入 ..... 12
2.4.3 探针监测 ..... 13
2.4.4 操作行为审计 ..... 14
2.4.5 敏感信息截取 ..... 16
2.4.6 异常 IP 分析 ..... 16
2.4.7 移动介质 USB 监测 ..... 17
2.4.8 特殊字段增量监控 ..... 17
2.4.9 违规外联处置 ..... 18
2.4.10 恶意卸载插件预警 ..... 19
2.4.11 全屏水印保护 ..... 20
2.4.12 权限分立管理 ..... 20
2.4.13 动态短信告警 ..... 21
2.5 应用场景 ..... 22
2.5.1 终端准入控制 ..... 22

2.5.2 终端日常操作审计 ..... 22
2.5.3 恶意搜索行为 ..... 22
2.5.4 自定义增量监控 ..... 23
2.5.5 终端违规外联处置 ..... 23
2.6 界面展示 ..... 24
2.6.1 产品前端界面 ..... 24
2.7 运维实施 ..... 28

# 【第 1 部分】 概述

## 1.1 背景介绍

互联网技术的发展和广泛应用，关键信息基础设施单位的办公系统和业务系统已经实现了网络化、信息化，网络边界泛化及智能终端快速普及，给物理隔离或逻辑隔离的网络边界带来致命的挑战。各行业都颁布了相应的法律、法规对边界完整性和非法外联进行约束，对边界完整性和非法外联做出了明确要求。

在实际的工作中，部署重要信息系统的内部网络非法联接外部网络的网络安全事件时有发生，极易造成黑客入侵、数据泄露等安全事件。数据泄密是所有防护的基础和前提，风险点主要是“人”。内部人员将电脑违规外联，内部网络将面临病毒、木马、非授权访问、数据泄密、数据篡改等多种安全威胁；将工作资料、客户材料等敏感数据被非法获取，造成泄密等等。

## 1.2 产生违规外联原因

常见的企业终端电脑出现违规外联行为的原因有 4 点：

1） **一机两用。**

指终端电脑或者网络设备在未采取安全措施情况下连接企业内部信息网络或连接互联网（不同时连接）。主要有以下几种情况：

a. 曾经联入企业内网的计算机，断开内网网络连接后联入外网；
b. 曾经联入外网的计算机，断开外网后联入内网；
c. 在联入外网的计算机上处理涉密文件和资料。联入外网指的是使用一切手段和设备，包括使用手机、小灵通或红外线、蓝牙技术等与外网相联，不管是否浏览过网上信息，均为已联入外网。

2） **热点外联。**

指终端台式电脑或者网络设备在未采取安全措施情况下既连接企业内部信息网络又连接互联网（同时连接）。

a. 计算机同时联入外网和企业内网；
b. 计算机在网线连接内网状态下，通过手机热点联入外网。

3） 网线误接。

因网线及网口标识不清、机房搬迁工人操作不当，导致企业内网终端计算机网线误接入互联网，造成违规外联。

a. 原内网网线接口，接入互联网接口中；

b. 原在内网使用的终端，内部保存重要数据，联接互联网导致违规外联。

4） 移动端 USB 接口传输。

计算机 USB 接口接入手机数据线进行充电或数据传输。计算机共享了手机移动网络，联接互联网造成违规外联。

a. 移动存储介质交叉使用；

b. 手机端 USB 口连接终端电脑充电，导致终端安全环境出现缺口；

5） 保密意识淡薄。

违规外联行为就像我们人为在企业专网与互联网搭建了一个传输平台，严重影响企业内网的安全。

a. 导致病毒侵入，影响设备正常运行，导致企业网络瘫痪；

b. 导致企业内网被黑客攻击利用，造成严重后果；

c. 导致信息外泄，在内网计算机存有泄密文件的，外泄会造成严重损失；

# 【第 2 部分】 终端违规外联审计平台

## 2.1 产品介绍

终端违规外联审计平台（OATD），是融至兴科技根据多年的“安全区域边界”监测的经验，自主研发的一款以安全管控为核心，以实时监测为要求的全方位外联监测平台，主动处置网络终端安全状态的分析系统。从用户终端的资产出发，关注终端状态、违规行为等威胁信息，并且及时发现突破、绕过现有安全机制的违规行为，实时主动监测、审计终端操作行为、处置威胁信息与违规行为。

## 2.2 产品定位

【终端违规外联审计平台（以下简称：违规外联）】

1) 本产品由杭州融至兴科技有限公司自研产品，别名：外联处置平台/终端违规外联处置平台
2) 对专内违规外联行为（一机两网、一机多用、VPN 代理外联、VPN 代理接入等）进行监测发现与集中管控。全方位实现单位终端的入网认证、审计信息收集、违规外联探测、威胁处置、风险预警、终端行为追溯等，保障了信息系统安全稳定运行。
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

## 2.3.1系统架构

OATD 系统由三部分组成：客户端、控制服务器、存储，用户可根据管理的需要将客户端安装在需要进行违规外联审计的终端电脑上。

### 1） 客户端

执行来自服务器端管理员下发的安全管控策略，违规外联安全探测，同时将用户行为审计日志信息上传至服务器系统。客户端不影响用户终端正常操作，开机自启，无感适用。

### 2） 控制服务器

融至兴科技提供的软硬件一体化设备，用于入网认证审核、违规外联探针、威胁处置、预警提醒等。平台提供管理员和服务器的交互界面，方便灵活的审计数据追溯、审计数据分析、设定管理策略和进行实时维护，一般授权给相关管理人员。控制服务器旁路部署接入网络，于网络核心交换机处（具体位置根据网络拓扑灵活确定）。

### 3） 存储

存储终端审计数据，审计分析类数据，由客户提供或按实际需要配置。

## 2.3.2数据架构

### 1） 数据源 1

数据源指主要提取于企业信息终端使用、操作行为的数据。管理系统将整合来自于企业各个部门信息终端操作行为相关的数据信息，形成全局范围的统一的、一致的行为基础数据库，在统一视图的基础上形成管理应用。由于各种原因，不同的源系统的体系架构、开发平台、接口技术等存在很大差别，不同系统的数据定义、标准也存在很大的差异；另外由于业务的不断变化，历史数据与当前数据之间的含义也可能存在不同，因此数据整合必须充分考虑源系统在技术和数据方面存在的差异。

从数据需求总体看，管理系统的数据源包括大部分已经投入使用信息终端点的相关数据。

2） 数据源 2

数据提取、转换和发送是将数据从数据源整合到管理系统数据库的过程。提取是指识别用户行为，并从中获得所需的数据。它是将数据导入数据库的第一步。提取意味着截取并理解源数据，并复制到数据库所需要的部分。

转换泛指使数据库数据适合于前端使用的过程。这一过程包括那些将源数据格式变为目标数据库格式的模块。一般而言，转换主要是对截图、文字输入内容的识别。

3） 提取数据：

a. 图像数据：

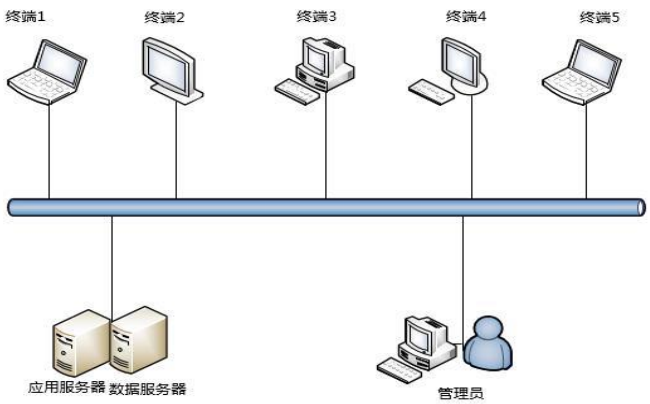
管理系统通过信息终端中的程序，对用户鼠标的操作区域进行截图，点击一次截图一次。并实时把截图数据发送到服务器进行存储。融合全部数据资源信息，进行整体的数据统计与分析，并在服务器的管理端进行展示。

b. 文字数据：

管理系统通过信息终端中的程序，对用户键盘输入内容进行截取，并实时把截取数据发送到服务器进行存储。融合数据资源信息，对键盘输入信息进行输入法识别与转换，并在服务器的管理端进行展示。

## 2.3.3网络架构

通过无线和有线网络系统的建设，实现企业内部的网络互连互通，串联所有信息终端点。



1） 数据层

基于数据资源中心一方面接收存储来自信息点的数据，为上层应用提供数据支撑，同时基于数据可以进行数据融合分析，进行数据的深度挖掘，反映实际状况，以及深层次的决策分析。

2） 支撑层

通过数据源的程序，对数据源的行为操作进行相应的数据提取，统一传送到后台数据管管理中心进行存储，数据层会对数据进行统计、分析等，使管理者通过分析结果对企业作出相应的调整和管控。

3） 应用管理层

基于数据层对数据进行数据处理能力的业务应用平台建设。

4） 统一标准规范体系

统一标准规范体系贯穿于管理系统建设全过程。统一标准规范体系确保系统的建设符合相关法规和指导方案，同时也必须符合相关的电子信息和行业数据标准。

项目编写依据：

1） 《网络安全法》
2） 中办[2003]27 号文件（关于转发《国家信息化领导小组关于加强信息安全保障工作的意见》的通知）
3） 公通字[2004]66 号文件（关于印发《信息安全等级保护工作的实施意见》的通知）
4） 公通字[2007]43 号文件（关于印发《信息安全等级保护管理办法》的通知）
5） 公信安[2009]1429《关于开展信息安全等级保护安全建设整改工作的指导意见》
6） 公信安[2014]2182 号《关于加强国家级重要信息系统安全保障工作有关事项的通知》（公信安[2014]2182 号）
7） GB17859-1999 计算机信息系统安全保护等级划分准则

8）GB/T25058-2010 信息系统安全等级保护实施指南

9）GB/T22240-2019 信息安全技术网络安全保护等级定级指南

10）GB/T25070-2019 网络安全等级保护安全设计技术要求

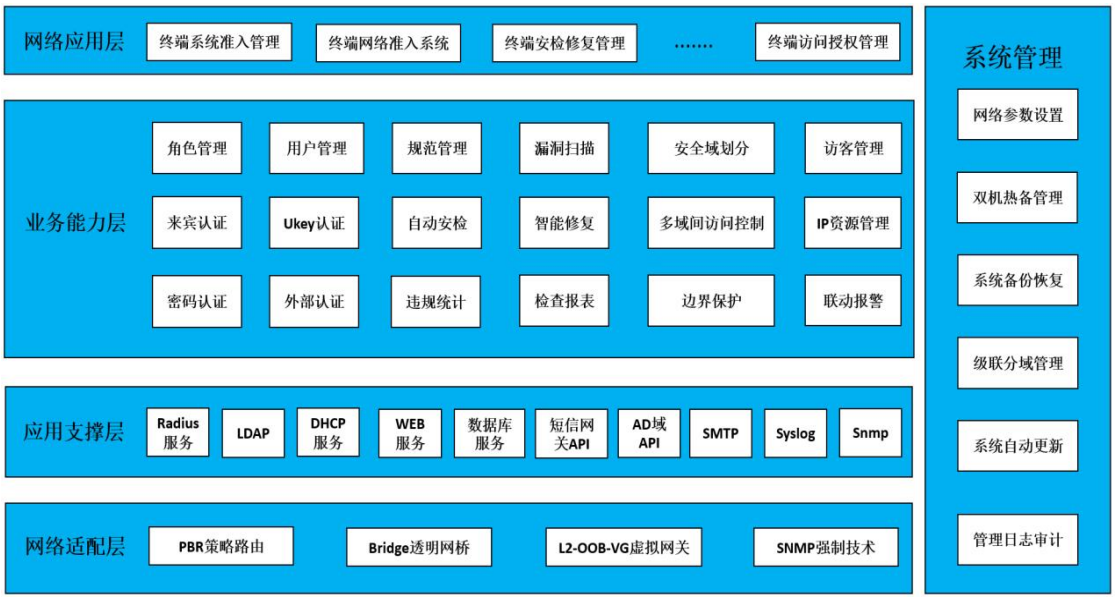
11）GB/T28448-2019 网络安全等级保护测评要求

12）GB/T28449-2019 网络安全等级保护测评过程指南

#### 5） 安全保障运维体系

安全保障运维体系确保管理系统安全运行采用必要的技术和管理手段，充分保证各系统应用系统信息安全；安全保障运维体系包括基于建设模式及运营模式上的保障体系，确保管理系统平台项目的建立稳定可靠的信息渠道，通过制定科学合理的建设管理体系以及长效运营机制，规范建设管理，保障管理系统持续长效运行。

### 2.3.4技术架构图




#### 1） 网络适配层

OATD 系统集成了 PBR 策略路由、Bridge 透明网桥、L2-OOB-VG 虚拟网关、SNMP 强制等多种网络准入强制技术，可以适应各种复杂的网络环境，兼容不同厂家的网络或安全设备，实现灵活的部署到实际网络中，具有良好的网络适应性。

2） 应用支撑层

OATD 基于广泛的第三方业务接口，结合 Radius、LDAP、AD 域、SNMP 等技术，建立准入技术和业务功能之间的衔接关系，成为网络适配层与业务功能层之间纽带。

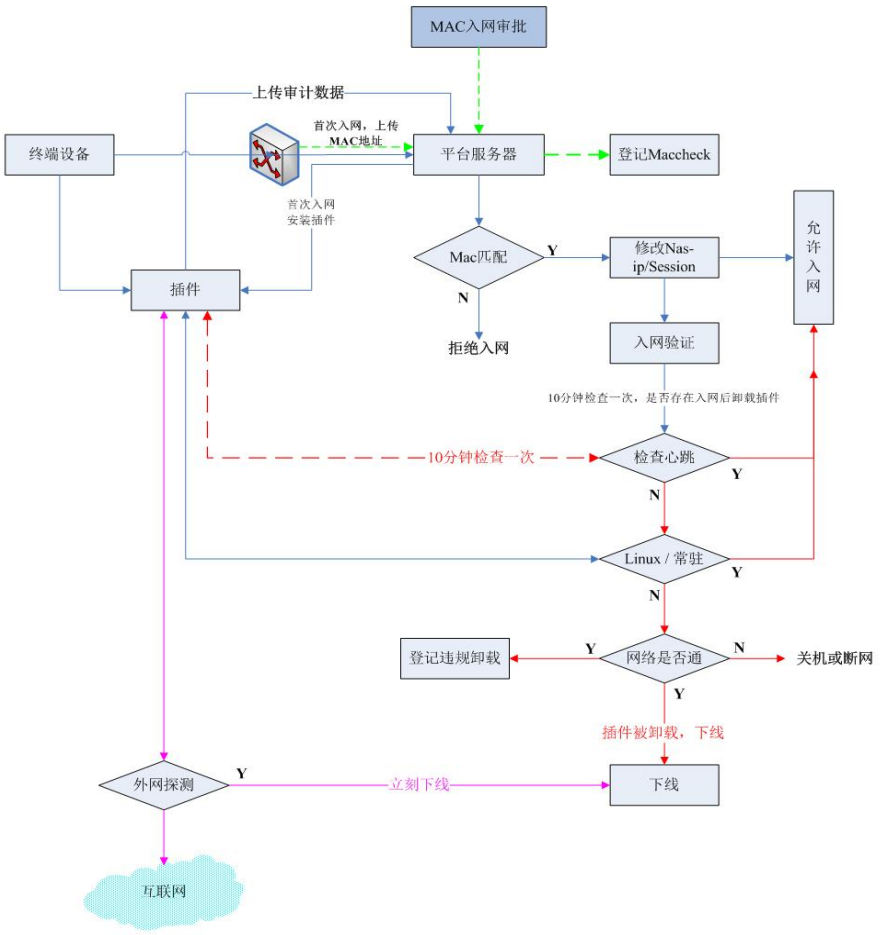
3） 业务功能层

OATD 通过对接入网络终端实现的一系列的管理功能，从身份识别管理、安全策略基线管理、安全策略修复管理、网络边界资源管理、访问授权管理等多个模块实现对终端准入控制的流程管理。

4） 网络应用层

终端违规外联审计平台针对现有终端违规外联需求，形成适应用户实际需求的解决方案。

## 2.3.5流程图



## 2.3.6 系统工具说明

1） 处置平台：

通过在接入交换机上配置端口安全，非法 MAC 接入网络时可通过处置平台的可视化界面将该端口关闭。同时配置非法 mac 接入日志通知功能，第一时间在管理界面显示非法接入事件的设备及接口信息表格。预配置未使用的交换机端口，将该接口关闭，可避免非法随意接入。经管理员授权后，确认需要使用时通过处置平台将该端口开启即可。

堡垒机将所有设备纳入统一管理，维护时通过堡垒机操作，可有效的降低外来终端接入导致违规的风险。

在互联网配置前置机，通过网闸开放互联网访问功能，可在维护时给维护人员提供互联网访问功能，同时也提供文件中转功能。为降低外来终端接入导致违规的风险，处置平台使用 linux 服务器，可以实现多用户。

2） 分析探针：

a. 资产安全监测

基于资产遥感技术，对专网中接入的资产进行识别，自动获取厂商品牌、设备类型、操作系统类型、协议、平台等信息。根据识别的资产建立设备指纹库，实现资产智能检索和资产统计，对资产非法接入、非法占用、非法替换等安全行为进行监测告警。

- 资产识别：提供设备类型、品牌型号、系统版本、固件版本、应用名称、品牌、版本、服务类型以及端口等信息。
- 资产大数据库：基于识别的资产信息建立资产大数据库。
- 资产统计：统计识别资产总数、在线数、类型、厂家以及位置等资产信息。
- 资产检索：对全网资产进行多维度检索以及关联分析。

b. 边界安全监测

基于多风险场景建模，对专网边界安全进行监测，主动监测专网内存在的违规和非授权网络边界，发现受控隐蔽的跨边界数据传输和网络访问通道，以及监测外部设备非授权入网和内部用户违规外联外部网络等高危风险行为。从而预防专网资源被不法人员利用，造成网内资源被破坏、数据被泄露以及非法入侵等安

全事件。

- 违规外联节点：对违规外联互联网、违规外联视频网以及其他专网等私自连接不受控网络的违规外联节点进行监控。
- 违规外界通道：对违规搭建的网闸设备、WIFI 路由设备、交换机串线、DHCP 服务、网络代理服务、可解析互联网域名的 DNS 服务等违规网络边界通道行为进行监控。
- 私网与专网连接：对私自搭建网中网、多网卡跨网、私网 IP 入网访问等行为进行监控。
- 不受控入网设备：定位网络中存在的非授权设备接入，包括非授权登记设备、移动设备等，掌握全网入网资源情况。
- 异常边界节点：对全网资产空间路径节点监测，及时发现专网中未知的第三方网络路由节点以及未知的第三方边界节点接入等安全行为。

c. 违规行为监测

探针依据国家、单位的管理条例和相关规定，基于违规行为特征建立模型，通过正则方式匹配网络行为，对专网内出现的各类违规行为进行监测并告警，并定位违规主机，减少安全隐患，提升安全考核。

- 违规入网：保护内部网络资源不被外部非授权用户使用，监测非合规终端入网、非授权终端入网以及移动设备入网等行为，提供入网设备的地址、所在位置等信息。
- 游戏行为：监测范围内的联网游戏行为，提取游戏主机、位置、游戏端口、游戏名和游戏版本等相关游戏特征信息。
- 违规站点：监测网络中未授权违规搭建的域名服务站点、FTP 站点、WEB 站点、论坛站点，提供服务器地址、访问方式、所在位置等信息。
- 违规通讯：监测网络中违规启用的非合规通讯系统和通讯工具，定位设备地址、位置和工具类型等相关信息。
- 违规传输：监测网络中存在的病毒文件传输、娱乐影音文件违规传输以及敏感信息文件传输行为，进一步避免数据信息被泄露、病毒传染源和木马扩散。

d. 安全隐患监测

探针对全网设备节点进行扫描，针对开放的端口进行识别，实时分析端口、

服务开放详情，及时发现国内自身存在脆弱性的资产设备、易被内外威胁利用或被当做攻击载体的设备。避免设备被恶意控制，引发各类安全事件。

- 异常端口开放：监测开放的敏感端口、全端口开放的设备，提供设备地址、信息等。
- 可匿名登录 FTP 服务器：监测网络中无需输入用户名密码即可登录匿名 FTP 服务器，提供 FTP 服务器地址、信息等信息。

# 2.4 产品功能

## 2.4.1资产发现

采用多种技术手段，发现网络内存活的资产，并自动获取资产的 IP、在线状态等信息。支持各类网络资产识别，包括：计算机设备、网络设备、安全设备、安防设备、办公设备、专用设备等。

1） 主动发现

区别于传统资产发现，具备主动探测发现未知(未管理)资产功能，并对资产进行全生命周期管理，并通过信息补全和深度扫描等方式完成资产属性的补全，最终实现全量资产的发现与生命周期的管理。

a. 提供部分 MAC 地址作为匹配项；

b. 设备接入平台，自动将设备 MAC 与设定 MAC 进行深度匹配；

c. 匹配成功，资产自动被发现且进入本平台审批范围内。

## 2.4.2设备准入

“终端违规外联审计平台”具备非常完善的终端接入管控方案，可以帮助企业对终端设备接入以及网络访问权限进行严格控制，防止内部机密信息外泄。准入平台能够自动发现管理域内的设备接入行为，自动上报接入设备的 IP/MAC 地址、操作系统、厂商信息等信息至处置审计平台，根据需要实现设备自动准入或经管理员审计通过后接入内网。企业可以提前设置检测条件，对每一台接入的客户端电脑进行合规性检查，不符合安全规定的终端电脑则禁止接入网络和访问受保护区域。当新的终端进入网络时，可通过 OATD 设备进行自动化审核入网。管理员可针对不同人员分类，对其进行终端入网审批。对于临时来访的计算机，通过准入平台进行身份认证，通过后方可接入网络。准入网关还可以防止内部计算机通过重装系统，安装多系统等方式脱离监管。

产品秉承不改变当前网络结构的特性，为用户解决终端入网的合规性要求。依据 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》，满足等保要求中的“安全区域边界”非授权设备私自接入内网的管控要求。采用多重网络接入控制技术，采用旁路部署方式，支持动态 IP 和静态 IP 入网，不改变原有的

网络环境。能够从源头对用户及终端进行管控，帮助用户将病毒、蠕虫、网络侦听、越权访问等各类攻击行为拒绝在网络之外。

其具体意义主要体现在以下四方面：

a. 建立设备和使用者身份的联系，解决实名入网问题，防止非法接入，为后续安全策略精准下发、安全问题追踪打下坚实基础；
b. 帮助企业执行统一的安全策略；
c. 根据系统评估结果将没有通过安全检查（如没有安装防病毒软件）的终端隔离，并引导其完成修复。
d. 帮助企业实现基于角色的访问控制，规范终端网络资源使用，解决越权访问等问题。

#### 1） 自动准入

通过资产主动发现，将多个 IP 段的自定义端口下资产进行扫描并且入库，自动发现可以对已扫描的设备进行审批入库选择。被发现的设备存放于“待分配”栏中，需等待管理员对其添加设备信息准许入库即可完成。

a. 通过资产发现，将未知设备调入平台分配界面；
b. 管理员有权对设备进行分配准入（包括网络设备、安全设备、摄像头等）；
c. 完善资产信息后，支持设备准入；
d. 已准入的设备由平台实时监测，动态信息通过大屏界面展示；

#### 2） 手动准入

针对特殊 IP 或少量设备，支持手动输入 IP 进行设备准入控制。手动准入设备数量少、网络结构较简单、设备种类较为复杂的场景，手动准入资产直接入库，进入检测范围内，无需管理员对设备进行审批和完善信息步骤。

a. 针对少量设备或新添设备，支持手动准入操作；
b. 手动准入，设备信息更完善，支持自定义项；

### 2.4.3 探针监测

将业务服务器流量镜像到系统即可完成部署，在非客户端模式下，提供镜像流量分析、主动扫描两种方式，对网内存在违规外联的行为进行检测。同时在互

联网提供外网取证平台，规避抵赖行为。违规外联监控系统根据企业对违规外联的管理要求，提供对内部网络主机监视网络用户的 Internet 接入行为，有效防范不安全因素对涉密网络的威胁，确保企业核心数据安全。

a. 内外网服务器构建双向通道，提供丰富的取证信息；
b. 纯旁路，不需要部署客户端，不需要再已有应用系统中部署插件、追溯代码；
c. 系统对正在访问互联网、曾经访问互联网进行全方位检测；
d. 实时扫描内部网络内所有在线主机情况，预防外部移动计算机设备非法连接到内部网络造成安全隐患，杜绝意外发生；
e. 实时监视网内受控计算机通过普通电话线、ISDN、ADSL 等方式的拨号上网；检测通过无线方式非法上网的行为；
f. 对拔掉内网网线或禁用本地网卡等进行非法外联的主机能报告其客户端 ID 号从而准确锁定非法外联主机，在单机环境下也能实现阻断并报警；

## 2.4.4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。

## 2.4.5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。

## 2.4.6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。

## 2.4.7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。

## 2.4.8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。

## 2.4.9违规外联处置

依据 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》，采用旁路部署方案，满足等保中“安全区域边界”监测防护要求，缓解当前网络设备、安全设备、服务器等非授权外联无法有限发现和防护的短板。

违规外联处置平台为了防范黑客攻击、内部信息泄露等安全事件而设计，它对内部人员的非法外联行为进行实时监控，对物理隔离措施或安全限制规定进行有效性检查，帮助用户进行安全审计并加强和落实相应的安全措施和规章制度。能够实时监测并发现内网用户的非法外连行为；发现外联行为，系统将会直接对外联设备做下线处理，保证内网环境安全，避免重要信息的泄露；以日志的形式详实地记录下每一次非法接入的具体信息。

该系统由处置审计平台和分析探针组合完成整个技术实现流程：探针向终端发送数据检测包是否可访问外网地址，若发现某个终端在接入内网的同时连接外网，将检测包返回发送给探针进行分析，同时违规告警事件推送给处置审计平台，由处置审计平台向接入交换机发送控制指令，关闭外联终端接入端口地址以阻断外网访问行为。

### 1） 违规外联监测机制

实时发现终端的违规外联行为并加以处理，一旦发生违规外联行为，应及时定位追溯，对相关责任人加以处理。通过机制、人员与管理的有机整合，可以更好地实现内网安全的动态管理及安全运营。

a. 终端内外网互联行为发现

自动发现管理域内同时连接内网和外网的终端，外联包括 WIFI 热点、内置

双网卡等途径，获取互联设备内网 IP 地址、外网出口 IP 地址、外联时间等。

b. 线路外联行为发现

支持依赖客户端或不依赖客户端两种模式，自动发现内网某个网络设备（如：交换机、路由器等）同时连接内部网路和互联网等其他网络，造成内网设备潜在外联的重大隐患。上报内网外联网络设备管理口 IP、MAC 及外网出口 IP 地址等信息。

c. 内外网交叉混用行为发现

通过日志记录违规终端 MAC 地址，自动发现管理域内脱离内网并连接过互联网等其他网络的设备，上报外联设备内网 IP 地址、外网出口 IP 地址等信息。

#### 2） 违规外联威胁处置机制

平台接收到违规外联告警，自动通知网络安全管理人员；平台还可以根据用户需求，实现对外联终端自动断网处理，大大减少了维护工程师的风险点排查时间。当违规外联处置平台检测到内网设备有外联行为，处置平台在推送告警信息的同时关闭外联终端接入端口地址，对非法外联设备进行下线处置，以阻断外网访问行为。

目前共分为 2 种类型的自动拒绝：

a. 如果安装客户端的用户，可在用户侧自动完成禁停网卡操作。

b. 非安装客户端用户，可通过 radius 认证自动下线对应 MAC 地址信息的交换机端口。

#### 3） 违规外联行为追溯

在内网的设备，被系统检测到终端有违规外联行为后，如若发生数据泄露状况，平台可对其历史行为进行历史行为追溯。本产品拥有行为日志审计平台，可以对违规外联设备泄漏的数据信息进行日志分析和回溯，在平台内追查历史操作记录信息，及时恢复设备被恶意篡改的行为，有效阻止外联带来的危害，不对正常工作业务造成影响。

### 2.4.10 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。

### 2.4.11 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；

### 2.4.12 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。

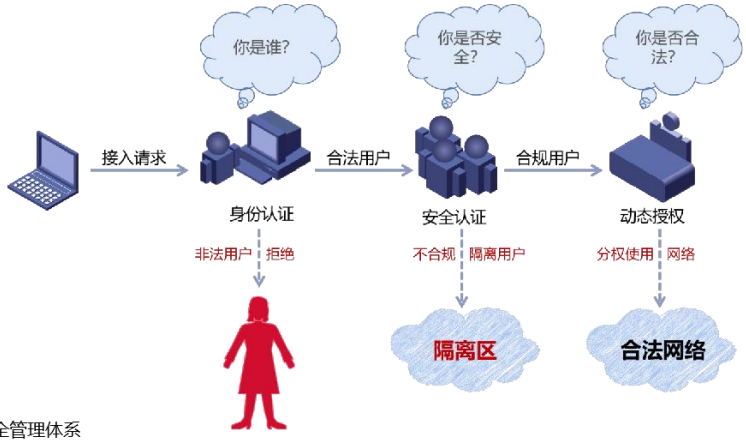
### 2.4.13 动态短信告警

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终端准入控制

- 手动添加
  - 规范入网流程，安全策略统一下发
  - 支持手动添加新增设备
  - 编辑设备详细信息，便于查找
- 自动发现
  - 自动发现网络设备、接入设备
  - 自动匹配入库规则
  - 核实信息后入库
- 统一管理
  - 统一身份认证，基于角色授权
  - 对于所有接入设备进行审计留痕
  - 提供安全可视化，实现系统化的安全管理体系




## 2.5.2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。

## 2.5.3恶意搜索行为

**预谋搜索**

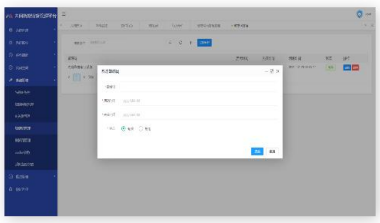
用户通过学习时间，在终端电脑上搜索不正当词汇（例如：犯罪 等词汇）。

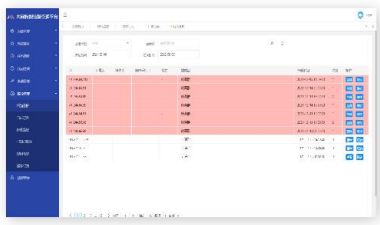
**系统自测**

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。





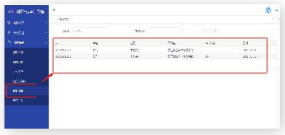
## 2.5.4自定义增量监控

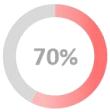

**打印机队列监控**

- 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**

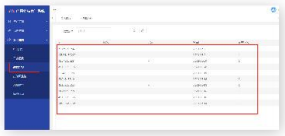
- 日常办公中，特定用户工作职能为搜查车辆牌照
- 针对每日工作量进行平均记录，超出一定范围，视为情况有异常，系统出现预警
- 出现其他人搜查车辆牌照信息，则视为异常情况，系统预警






**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



## 2.5.5终端违规外联处置

# 2.6 界面展示

## 2.6.1产品前端界面

1） 登录


2） 主界面


3） 准入审批


准入审批
资产信息
修改
待审批
待维护
MAC: 00-0C-29-19-35-C5
IP:
DATE: 2022-03-02 14:48:32

4） 资产信息


准入审批
资产信息
部门
类型
MAC: 00-0C-29-0E-DB-27
IP:
DATE: 2022-03-09 14:29:00

5） 行为审计


行为审计
行为日志
存放目录

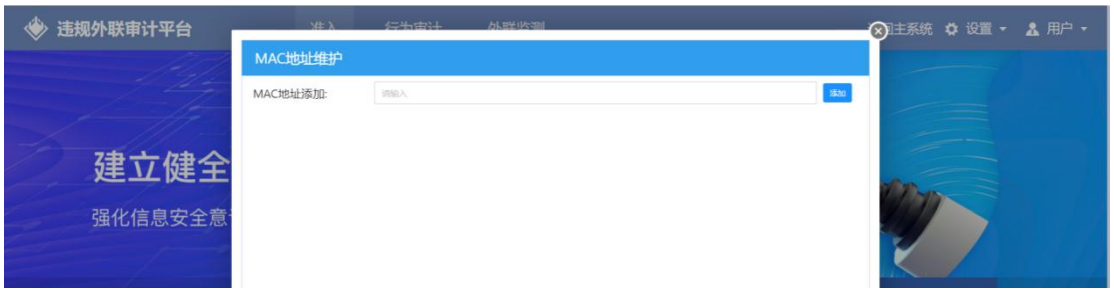
6） 行为日志


7） 敏感词汇


8） 外联监测告警

9） 设置界面


10）MAC 地址匹配




11）本地参数配置


12）用户界面

# 2.7 运维实施