版本号：v5.0

**5.1迭代需求分析**

**北京爱普安信息技术有限公司**

**2018年9月**

# 目 录

[目 录 2](#_Toc526083304)

[1 需求列表 0](#_Toc526083305)

[2 集中部署、分级管控 1](#_Toc526083306)

[2.1 集中部署 1](#_Toc526083307)

[2.2 分级管控 1](#_Toc526083308)

[2.2.1 支持后台管理员分级 1](#_Toc526083309)

[2.2.2 用户可登录后台 2](#_Toc526083310)

[3 用户行为管理 2](#_Toc526083311)

[4 态势感知平台 3](#_Toc526083312)

[4.1 展示形式 3](#_Toc526083313)

[4.2 信息获取 3](#_Toc526083314)

[4.3 信息分析 5](#_Toc526083315)

[4.4 处置决策 6](#_Toc526083316)

# 需求列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **模块** | **功能点** | **编号** | **功能描述** | **优先级** |
| **集中部署、分级管控** | **服务器集群部署** | 1 | 对海军各部队单位分别部署一套安全管理系统，所有服务器集中部署在总部机房内 | **中** |
| **双机热备** | 2 | 对数据库和服务器进行双机热备，保证异常情况下数据安全 | **低** |
| **负载均衡** | 3 | 在服务器和外部网络之间部署负载均衡设备 | **中** |
| **三权分立** | 4 | 后台管理员分为系统管理员、审计管理员、安全管理员三个身份，分别执行不同的功能模块 | **高** |
| **分级授权** | 5 | 系统管理员可以创建下级三种管理员，但不能越级创建 | **高** |
| **用户行为管理** | **Url黑名单** | 6 | 可以对浏览器中的Url地址做黑名单过滤 | **高** |
| **Url审计** | 7 | 可以对用户访问过的Url地址做审计 | **中** |
| **敏感词过滤** | 8 | 可以对系统中出现的敏感词进行过滤 | **高** |
| **敏感词审计** | 9 | 可以对系统中出现的敏感词进行审计 | **中** |
| **IM审计** | 10 | 可以对IM软件中聊天记录进行审计 | **低** |
| **态势感知** | **数据收集与分析** | 11 | 收集终端数据和威胁信息 | **高** |
| **数据展示** | 12 | 对数据进行展示 | **中** |
| **其他** | **消息群发** | 13 | 支持管理员向用户群发消息，以客户端弹窗方式实现 | **高** |

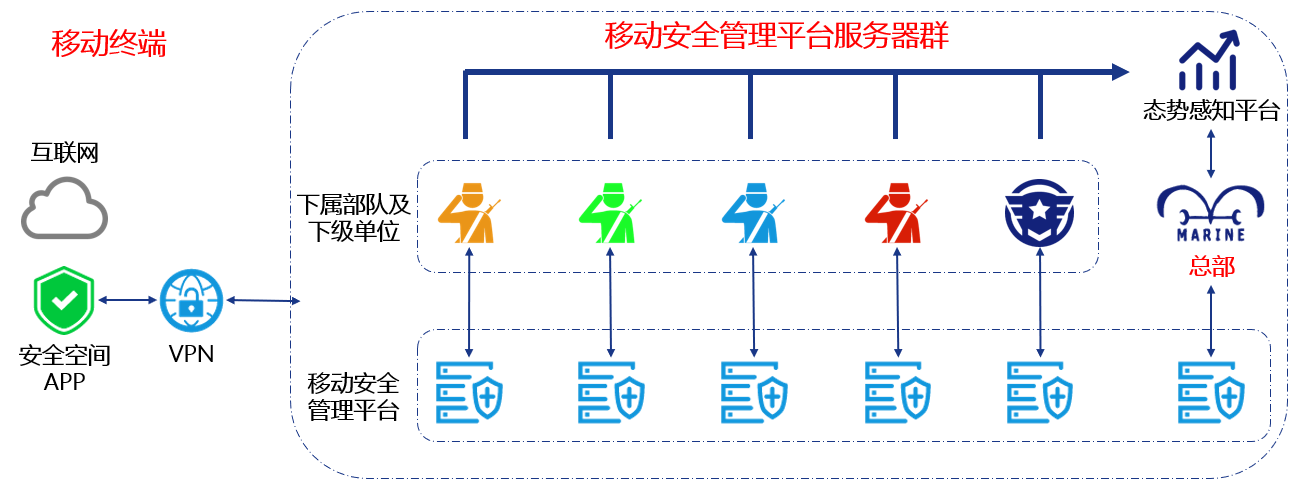
# 集中部署、分级管控

## 集中部署

为海军各部队分别用虚拟化的形式部署一套安全空间管理系统，在总部部署安全空间管理服务器和态势感知平台服务器，总部可以查看所有二级安全空间管理系统运行情况，同时态势感知平台收集所有下属部队和二级单位的客户端运行情况，并进行汇总分析。

服务器群统一部署在一个IDC机房内，并在服务器和外部网络之间安装负载均衡设备，实现智能化的流量管理。

双机热备，提供服务器和数据库的双机热备功能，防止数据丢失。



## 分级管控

### 支持后台管理员分级

三权分立：系统管理员 审计管理员 安全管理员

系统管理员：系统设置、用户管理、管理员管理

* 系统设置：后台管理系统配置
* 用户管理：对用户的增删改查管理，包括批量导入等
* 管理员管理：对下级管理员的管理，例如旅级管理员可以增删改团级管理员

审计管理员：管理员审计

* 审计日志：可以查看本级管理员操作的日志
* 下级审计日志：可以查看下级、下下级等管理员操作的日志

安全管理员：策略制定、下发、业务审计

* 策略制定：可以制定本级管理的设备、应用、合规等策略
* 策略下发：可以对本级及下级用户下发策略
* 业务审计：可以对客户端日志、策略日志、应用日志等业务日志进行审计

分级授权模型，系统管理员创建下级三种管理员身份，但不能越级创建。例如由军系统管理员创建多个旅的旅级三种管理员，但团级三种管理员由对应的上级旅系统管理员创建。

### 用户可登录后台

支持用户通过用户名+口令的方式登录后台管理系统，可以查看自己的设备信息、策略信息、应用授权情况、内容下发情况等，还可以对自己的设备推送响铃追踪、设备定位、擦除数据等功能。

# 用户行为管理

针对用户可能的不文明上网行为，如果需要管控，需要做到以下需求：

URL黑名单：禁止涉黄、涉赌等不健康网站，需要通过第三方数据库构建URL黑名单库；

URL审计：进入域名访问记录、访问时长、访问次数、域名IP地址、IP位置、访问设备、访问用户名、URL黑白名单，支持输出到后台管理日志；

敏感词黑名单：加入敏感词过滤功能，对高风险敏感词直接过滤，对低风险敏感词进行记录；

敏感词审计：记录词语、输入次数、使用场景、输入设备等；

IM消息审计：支持对QQ、微信等聊天工具聊天记录进行审计，**只适用于军警等特殊场景**。

# 态势感知平台

## 展示形式



总览界面：

总览界面最上方为首页总体信息展示，包括总用户数、在线用户数、注册设备总数、已激活设备数、在线设备数、自定义策略总数、已下发策略数、已上传应用总数、应用黑名单数等。

最下方为违规情况，如发现设备违规情况则在界面最下方列出。

中间为地图展示区，支持对地图进行缩放。在地图中用光点表明在线的设备，绿色光点为合规设备，红色为违规设备，点击可查看设备详细信息。

总览界面右侧为信息展示区，对当前鼠标点击的信息进行展示，包括设备详细信息、用户信息、生效策略信息、应用信息、设备日志等。未点击设备时显示当前展示区域的在线用户列表，支持筛选。

左侧为威胁探测区，包括风险评分、泄密对象风险排序、黄赌毒人员预测排序、TOP10热词、TOP10热门应用、TOP10网站等。

## 信息获取

监测收集终端的设备信息、设备标识、系统、网络、位置、用户、运营商、应用及应用列表等运行环境信息；监测收集设备可能发生的一些风险行为信息；监测收集应用异常堆栈信息。包括：

1. 国际移动用户识别码
2. 接入点的BSSID
3. SIM卡唯一标识
4. USB接口序列号
5. 生效策略
6. 违规情况
7. 内存大小
8. 分辨率
9. 设备型号
10. 设备品牌
11. 蓝牙地址
12. 主板
13. 显示屏参数
14. CPU指令集
15. 硬件制造商
16. 电池电量
17. RC设备标识
18. 国际移动设备辨识码
19. 手机序列号
20. 网卡地址
21. 安卓ID
22. 应用名称
23. 应用标识
24. 当前应用包名
25. 应用名称
26. 应用版本
27. 项目名称
28. 系统版本
29. 设备gps地址
30. 联网方式
31. 运营商信息
32. 手机号码
33. 提权检测
34. 非法攻击框架检测
35. 模拟器检测
36. 调试器检测
37. 危险软件检测
38. 设备信息修改检测
39. 代理抓包检测
40. 软件抓包检测
41. native hook检测
42. xposed劫持检测
43. substrate检测
44. 异常类型
45. 异常时间
46. 异常信息

## 信息分析

直观的描绘出所有应用及用户的活跃度、地理分布、受攻击情况、异常情况、风险设备、虚拟设备、伪造设备等；

从用户识别、用户总数、被攻击用户、可疑用户、用户地理分布、异常设备分析、异常系统分析等多维度精准全面的为企业描绘出用户画像；

从启动、应用区域分布、活跃设备、异常触发、攻击触发等多维度精准全面的为企业描绘出应用画像

## 处置决策

从可疑设备、攻击痕迹、异常回报等角度精准、全面分析定位威胁来源、目标、过程，助力企业快速、精准定位并解决安全问题：

* 快速精准识别风险设备、虚拟设备、伪造设备等可疑设备，分析可疑设备的地理分布，同时提供可疑设备名片，精准定位威胁来源
* 对攻击痕迹进行分类，展示不同类型攻击行为的精确地理位置、区域、累计次数、触发趋势及详细的攻击信息；
* 实时监控回传应用异常信息，与环境信息、风险信息深度关联分析，还原异常场景。