360政企安全

360 企业安全云
产品操作手册

2022.3

【版权声明】

版本信息

文档名称	更改内容	文档版本	密级	创建日期
360 安全卫士团队版使用手册	官网大幅度改版	V3.0	公开	2020/11/03
360 安全卫士团队版使用手册	官网大幅度改版	V4.0	公开	2020/12/18
360 安全卫士团队版帮助手册	部分样式更新	V4.1	公开	2021/02/02
360 安全卫士团队版帮助说明	新增部分功能	V4.2	公开	2021/03/17
360 安全卫士团队版使用手册	新增部分功能及问题修复	V4.3	公开	2021/05/10
360 安全卫士团队版产品操作手册	新增部分功能及问题修复	V4.5	公开	2021/07/09
360 安全卫士团队版产品操作手册	新增部分功能及问题修复	V4.6	公开	2021/10/20
360 安全卫士团队版产品操作手册	新增部分功能及问题修复	V4.7	公开	2021/12/31
360 企业安全云产品操作手册	全面升级改版	V5.0	公开	2022/03

目录

1、安装部署指南 7
1.1 客户端配置环境要求 7
1.2 企业注册 7
1.3 客户端部署 9
1.3.1 windows 系统提供五种部署方式 9
1.3.2 Linux 系统部署 20
1.3.3 macOS 系统部署 22
1.4 退出企业 26
2、管理后台功能简介 27
2.1 总览 27
2.2 终端 27
2.2.1 终端部署 27
2.2.2 终端管理 28
2.2.3 终端状态 31
2.2.3.1 运行状态 31
2.2.3.2 安全状态 32
2.2.3.3 版本状态 33
2.2.4 终端定制 33
2.2.5 外设管理 35
2.2.6 设备安全 37
2.2.6.1 安全体检 37

2.2.6.2 木马查杀.....37
2.2.6.3 杀毒管理.....37
2.2.6.4 漏洞修复.....38
2.2.6.5 系统修复.....38
2.6.6 分组策略（部分专业安全管理运维服务）.....39
2.3 资产.....57
2.3.1 资产管理.....57
2.4 软件.....57
2.4.1 软件管理.....57
2.4.2 软件分发.....59
2.4.3 文件分发（专业安全管理运维服务）.....60
2.4.4 软件优化.....60
2.4.4.1 弹窗过滤（专业安全管理运维服务）.....60
2.4.4.2 启动项优化.....61
2.5 上网.....62
2.5.1 上网限制.....62
2.6 数据.....63
2.6.1 屏幕水印（专业安全管理运维服务）.....63
2.6.2 安全设置（专业安全管理运维服务）.....64
2.7 防勒索.....64
2.7.1 勒索防护（专业安全管理运维服务）.....64
2.7.2 安全基线（专业安全管理运维服务）.....65

2.8 服务 66
2.9 页眉功能导航 67
2.9.1 关键字搜索 67
2.9.2 设置 67
2.9.2.1 团队管理 67
2.9.2.2 全局设置 68
2.9.2.3 身份认证 70
2.9.3 站内信 70
2.9.3.1 站内消息 70
2.9.3.2 历史推送 71
2.9.4 工单系统 71
2.9.4.1 提交工单 71
2.9.4.2 历史工单 72
2.9.5 账号设置 73
2.9.5.1 积分中心 73
2.9.5.2 切换团队 73
2.9.5.3 账号中心 74
2.9.5.4 退出登录 75
3、客户端主要功能简介 76
3.1 首页体检 76
3.2 木马查杀 77
3.3 系统安全 78

3.4 网络安全.....79
3.5 数据安全.....80
3.6 优化加速.....81
3.7 安全大脑.....81
3.8 软件管家.....82
4、客户端退出、卸载.....84
4.1 退出.....84
4.2 卸载.....85

1、安装部署指南

1.1 客户端配置环境要求

类型	操作系统	CPU	内存	硬盘	备注
Windows 终端	Windows XP Windows Vista Windows 7 Windows 8 Windows 10 Windows 11	双核 2.0GHZ	1G	>20G	最低配置

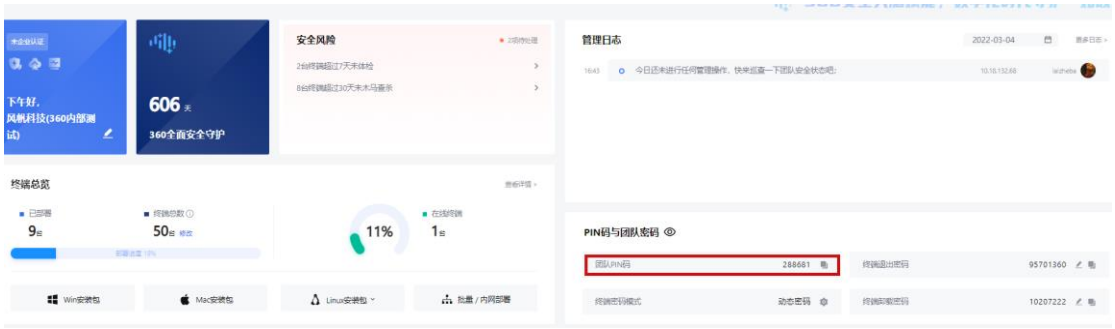
1.2 企业注册

通过官方网址 https://ent.online.360.cn/ 管理员可以为企业注册账号，注册非常简单，只需要填写注册手机号、验证码和设置密码即可。

注册成功，补充填写企业的真实信息后，就可以进入管理后台了。

登录管理后台会有企业专属的 PIN 码，这是客户端（员工）将本地的 360 安全卫士连接到

企业组网的识别编码，每个企业都有唯一的 PIN 码。



1.3 客户端部署

1.3.1 windows 系统提供五种部署方式

方式一，未安装个人版 360 安全卫士，管理员登录管理后台后直接下载企业专属安装包分发给企业成员进行安装；即可自动加入企业组织完成部署。

方式二，已安装个人版 360 安全卫士的成员，可与 360 企业安全云客户端无缝转换，只需要通过安全卫士界面右上角设置菜单中的“加入团队”选项，输入正确的 PIN 码即可自动升级为 360 企业安全云客户端并加入相应企业组织。

加入企业组织后，可在客户端输入或修改终端登记信息，用于标识设备的归属人。

方式三：已部署 360 网管版的终端，可通过网管版控制中心推送 360 企业安全云的新版安装包，请先从管理后台 -->【终端】-->【终端部署】-->【外网场景部署】下载需要的安装包，如下图:

然后打开 360 网管版控制中心-->【其他工具】-->【软件分发】浏览上传下载的 360 企业安全云安装包，选择弹窗告知接收，接收后运行，完成批量版本切换。

方式四：代理终端部署，对于有防火墙或代理出口方式控制互联网访问的企业，360 企业安全云提供了简单便捷的部署方法：

首先确保内网终端和联网终端可以连接，联网终端可以按需连接互联网，然后在管理后台的【终端】→【终端部署】→【内网场景部署】页面，下方【内网代理安装包定制】输入代理 IP 和端口，点击【生成安装包】按钮

即可下载代理专用安装包。

该安装包既用于代理服务端，也用于代理终端的安装，注意：该 IP 是联网机器的本机 IP，如果内网终端访问该机器 IP 是经过映射的，部署内网终端时需要更改一下安装包文件名对应的 IP 和端口，例如：服务端安装包文件名是 T1nGtrFf[192.168.28.131-80].exe，其内网映射 IP 是 192.168.86.144，那客户端安装包就改成 T1nGtrFf [192.168.86.144-80]Update.exe 后再执行安装。

代理服务端安装后只提供 360 安全卫士功能相关的域名和 IP 代理，如病毒库升级、补丁包

下载等，不可用户其他网站访问。(注意：请勿修改此安装包的文件名，以免安装部署失败)

目前 360 企业安全云暂不支持第三方代理软件，如果代理出口 IP 有变化，请下载新安装包覆盖安装，或者手动修改代理地址。

客户端代理设置入口：鼠标右键点击电脑任务栏 360 安全卫士图标，选择【升级-360 下载管理】页面右上角的设置即可打开设置。

如果代理服务端测试未成功，请检查网络防火墙设置，确保放行下列域名和 IP 的 80、443 端口：请访问管理后台→终端→终端部署→内网场景部署→复制域名。

方式五：域控方式部署

- 管理员通过管理后台获取域控安装包

- 将安装包放入共享目录下，并记录当前路径（格式一般为\\:IP 地址\目录名）（请务必测试目标机器确实可以直接访问此共享文件夹）
- 创建脚本，新建一个文本文件，修改文件名及后缀名为 start.bat（文件名可自定义，后缀名必须为.bat），start.bat 内的文本内容分两种情况：

（1） 目标机器有管理员权限，直接/S 参数运行 exe 即可，示例：

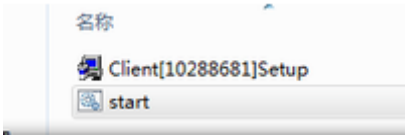
\\192.168.28.132\x\Setup[T0HLWK].exe /S

（2） 目标机器无管理员权限，需要在域控服务器里创建管理器权限的账户，并以命令行方式将账号密码传入安装包（部署完毕后可以删除此临时提权用的账号），

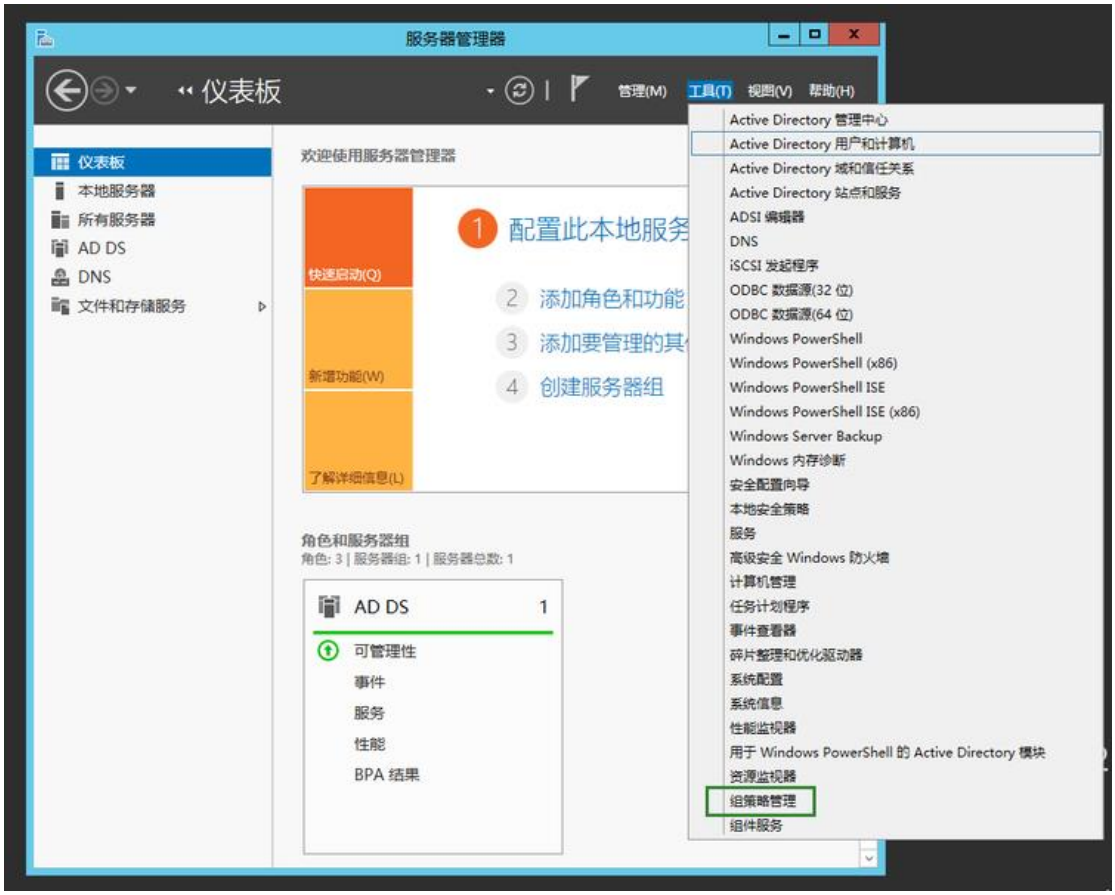
示　例　:\\192.168.28.132\x\Setup[T0HLWK].exe　/USER=admin /PASSWORD=pass-** /DOMAIN=test001.com /runas /S

【说明：admin 请使用您创建的账号替换，pass-**请使用您设置的密码替换，test001.com 替换为您的域】

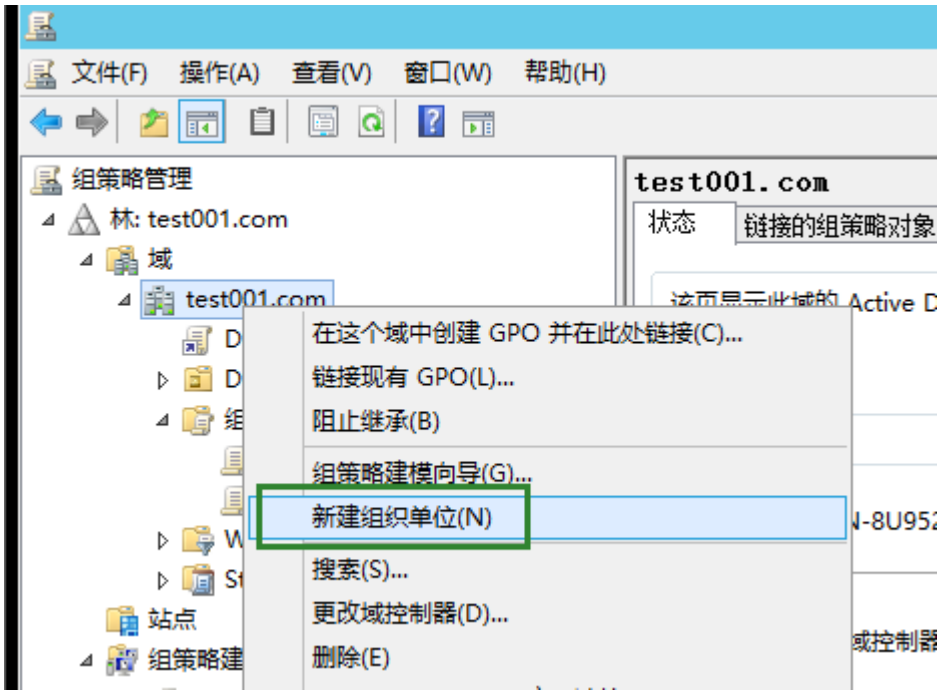
- 将脚本与安装包放到同一个共享目录下



- 进行域控下发：进入组策略管理页面

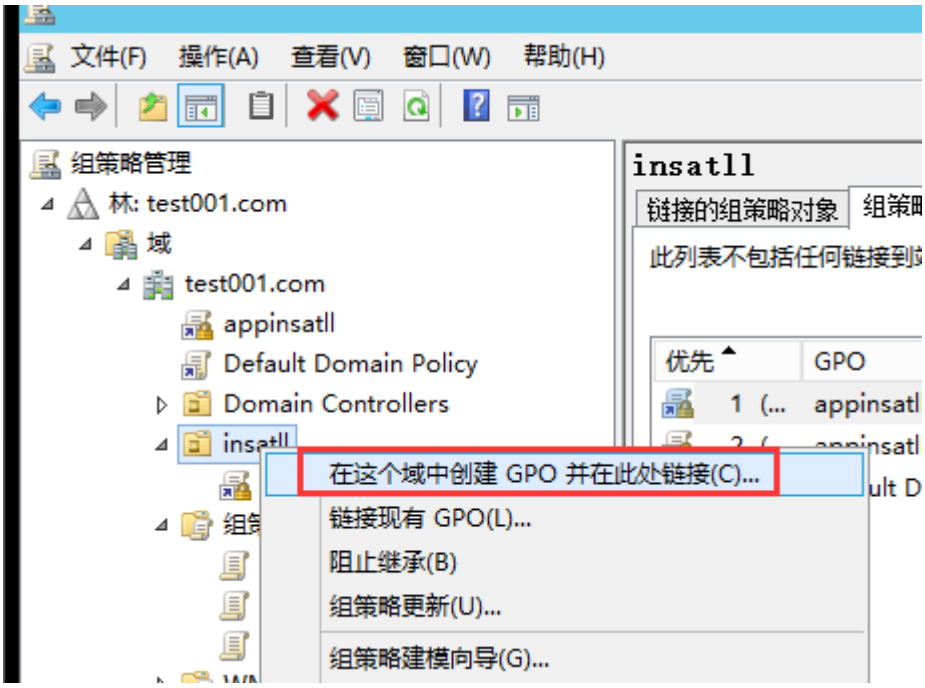


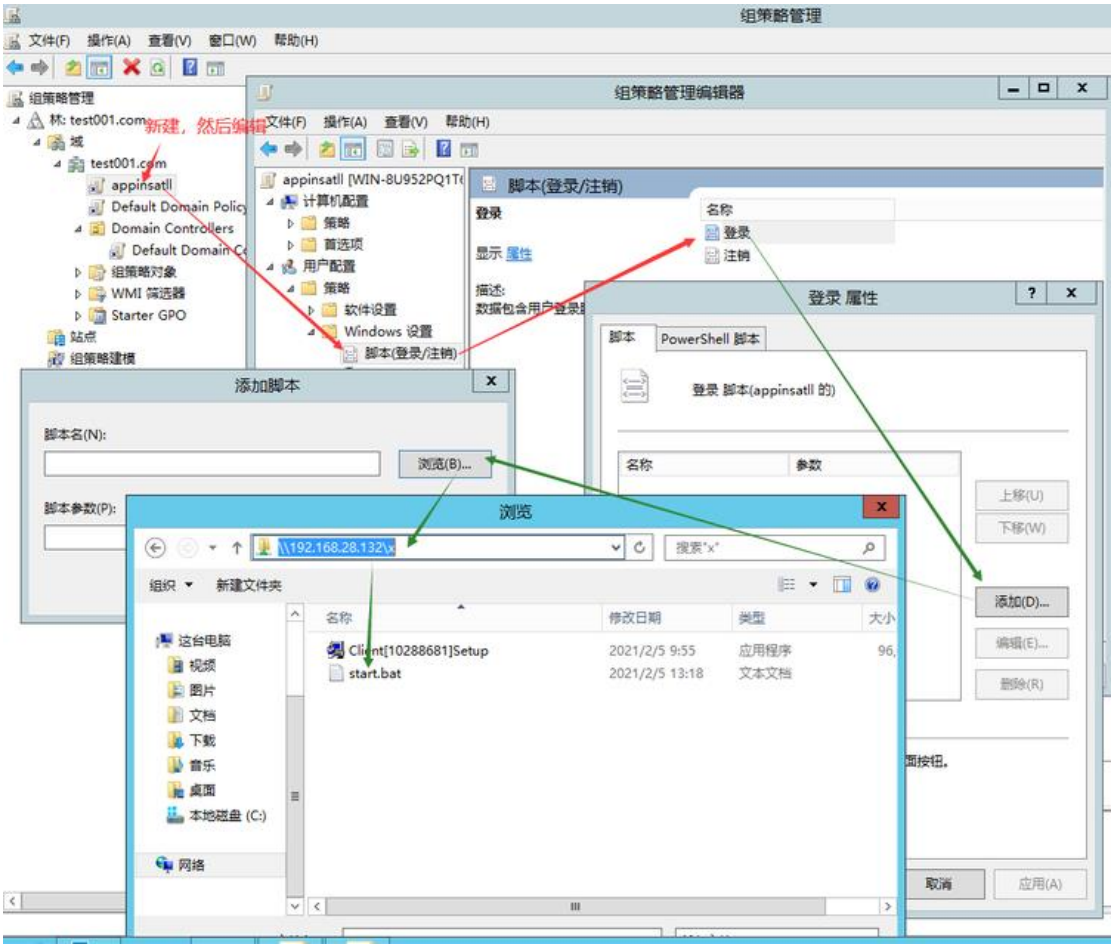
- 然后使用已有组织单元或者新建组织单元(请注意查看里面涉及的机器是否是目标机器)



- 创建 GPO 并连接，然后编辑，如下图示，选择用户配置→策略→Windows 设置→脚本→登录，将编辑好的在共享目录里的 start.bat 文件选入，(只能选入网络路径，切记

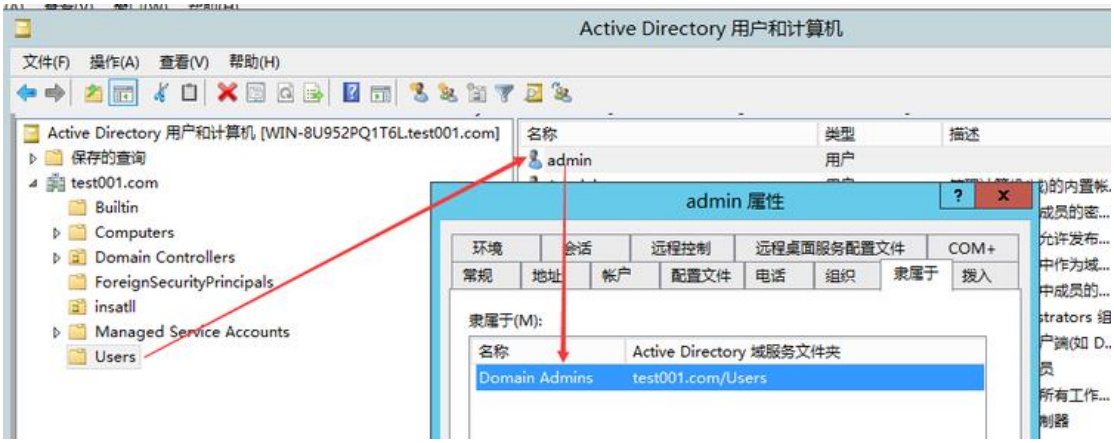
不要选本地的!)



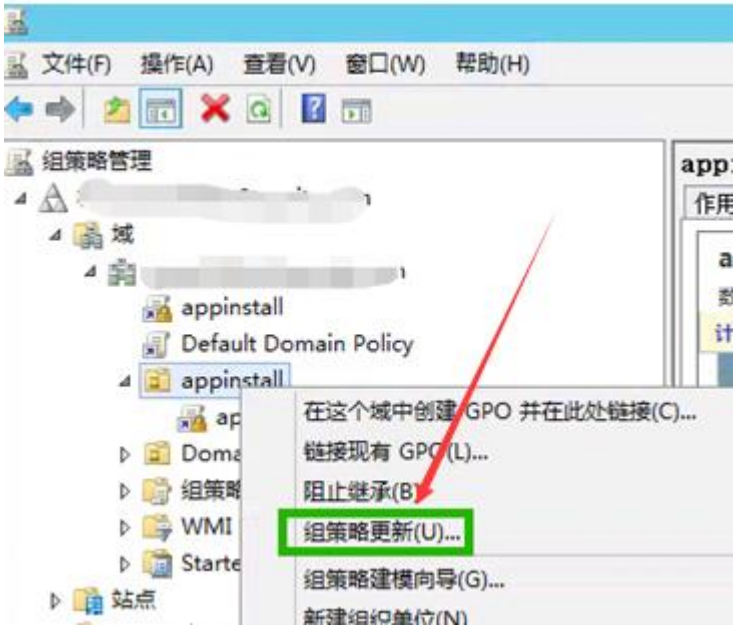


- 若是目标机器没有管理员权限的情况，请确保存在管理员权限的域账户 (且在 start.bat

里编辑的此账号密码是无误的）



- 执行组策略更新，也可以通过 cmd 下执行 gpupdate /force 来操作。



- 目标机器重启后，会执行静默安装，安装完成后会自动加入企业组织并启动主界面，需要企业成员填写登记信息，用于识别设备的归属人。

1.3.2 Linux 系统部署

目前支持 Ubuntu18、Ubuntu16、Centos7、Centos6、Deepin 20。

请先在控制台下载最新的 linux 部署安装包。

下载完成后，执行./Team{10590864}.run 即可安装。(./后是您文件名的全称）请勿修改安装包名称。

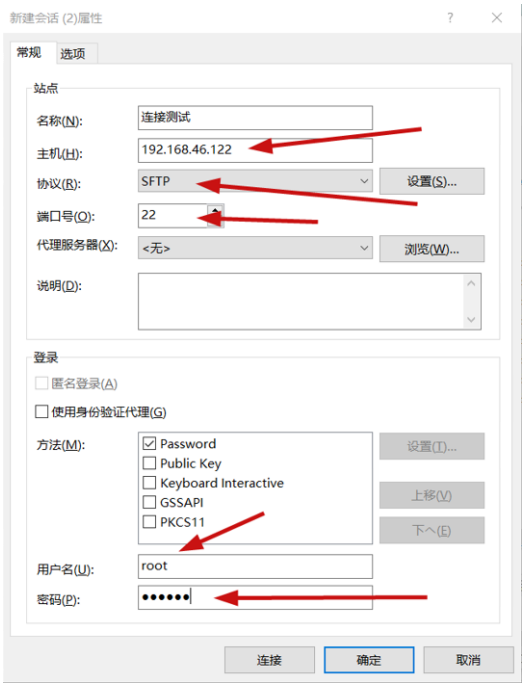
- 安装完成后即可在管理后台查看终端信息并对终端下发管理策略。

温馨提示：

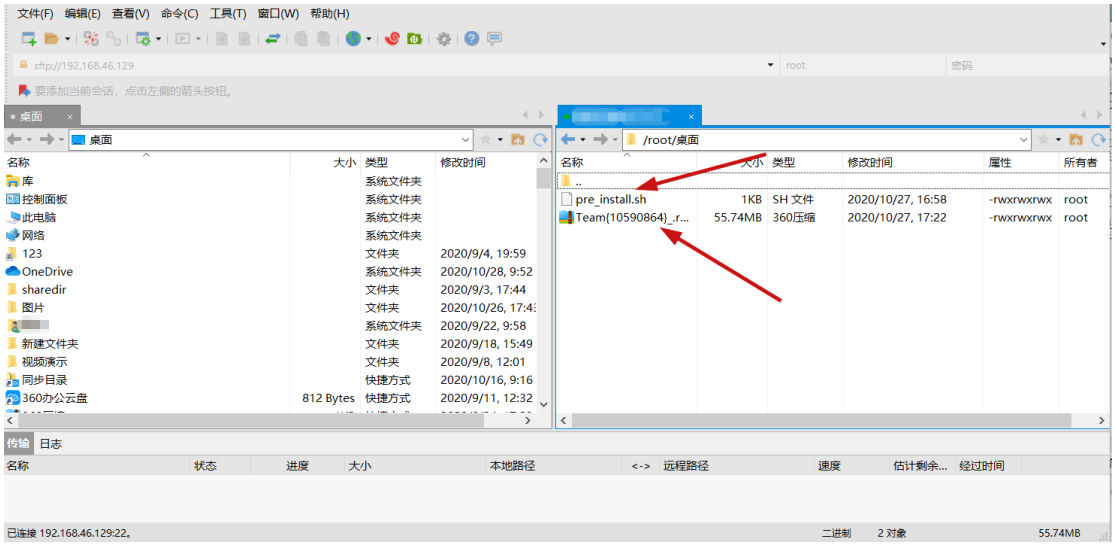
FTP 上传文件举例：

1、以 xFTP 为列，下载并安装 xFTP，选择【文件】-【新建】

2、根据终端具体情况，填入正确 IP、端口及登录用户名和密码



3、将 Team{数字 PIN 码}.EL7.x86_64.rpm 安装包文件上传到 Linux 终端上，此处以放在桌面举例：

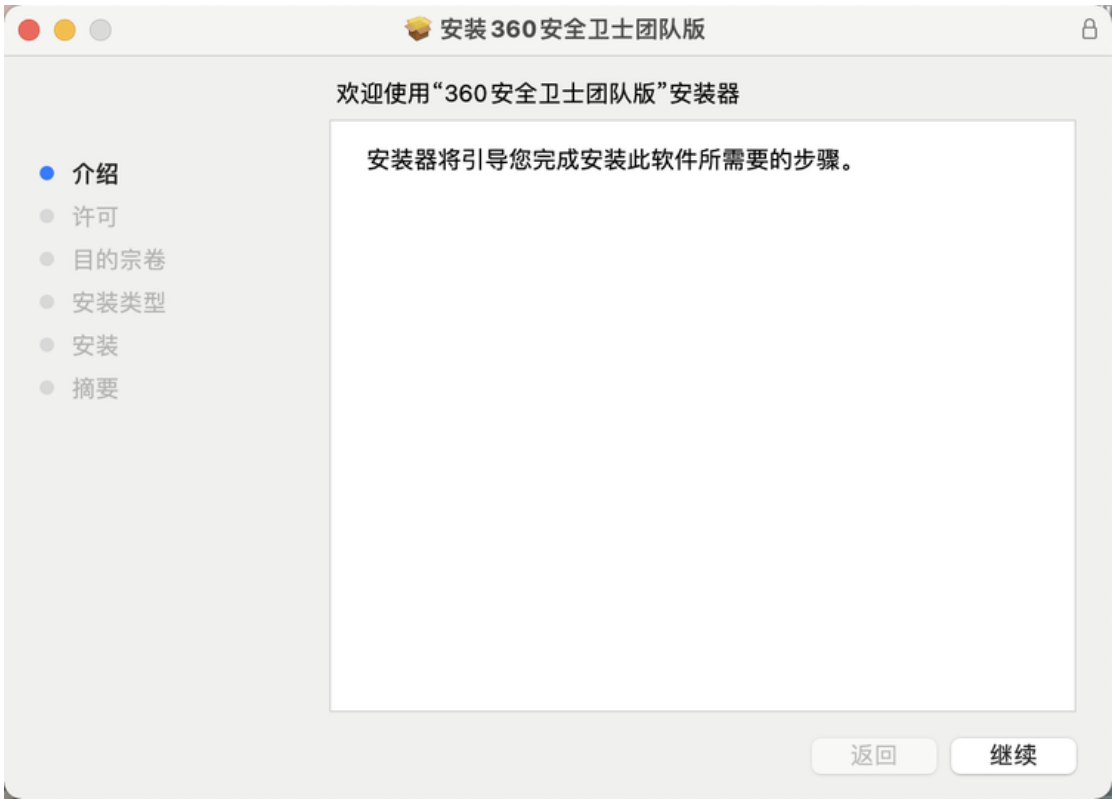


1.3.3 macOS 系统部署

➢ 360 企业安全云在 macOS 系统上的部署：

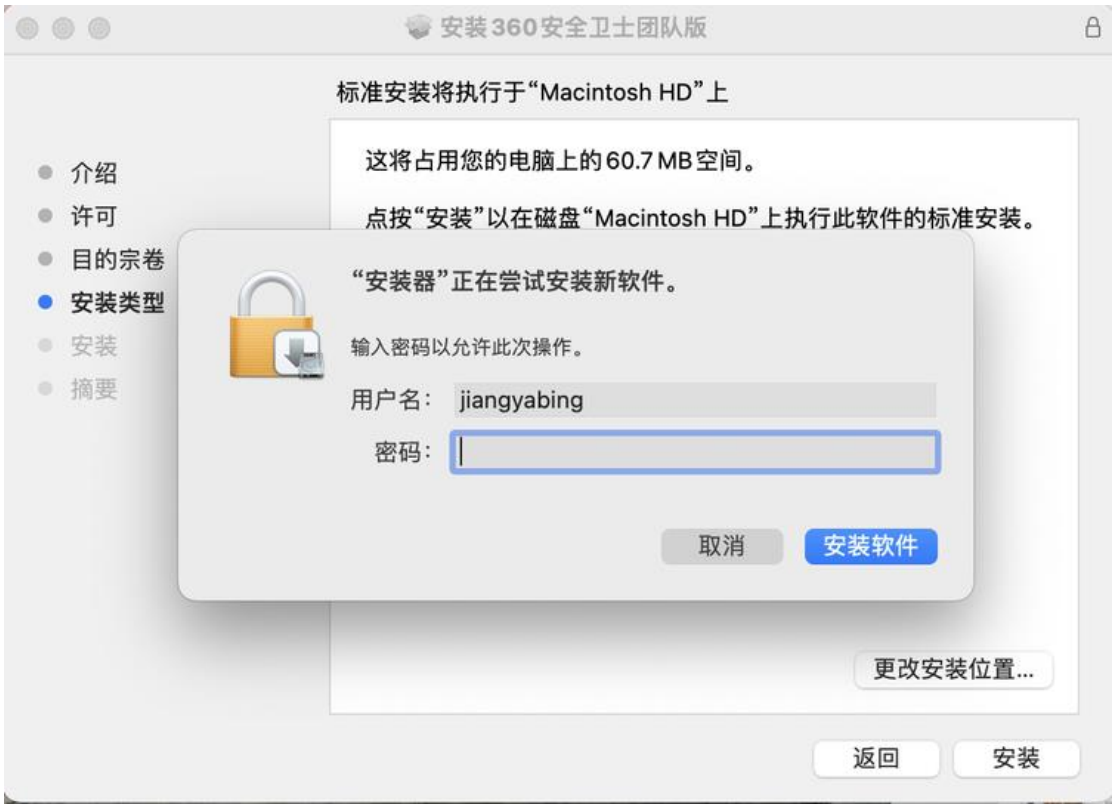
请先在管控后台下载适配 macOS 系统的安装包，

将下载下来的 pkg 安装包放到可读写的文件夹内，切勿修改文件名。然后双击 pkg 文件，根据安装向导点击“继续”。



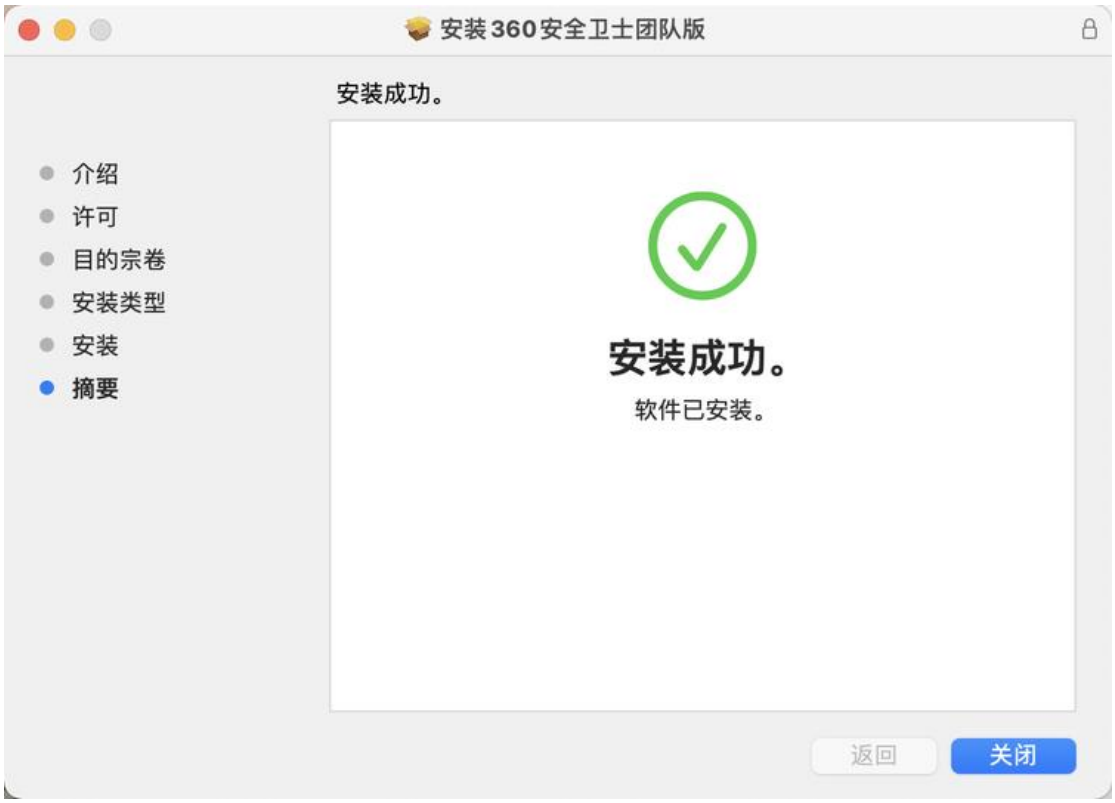
点击“安装”“继续”按钮

点击“安装”，弹出用户密码框，输入密码，点击“安装软件”按钮



安装过程中，会出现系统弹出的文件夹访问的确认框，请点击 “好”

剩余安装过程，请耐心等待



如果提示安装失败，请重启系统，重新执行安装过程。

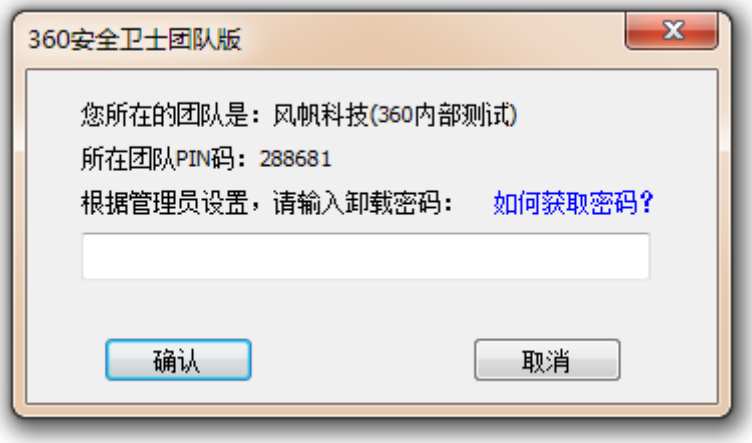
安装完成后即可启动界面

➢ 即可在控制台【设备管理】-【终端管理】中查看终端信息，并对终端下发管理策略

1.4 退出企业

退出企业组织的方式有两种：

方式一，卸载客户端，会提示用户输入卸载密码，用户填写正确的卸载密码后会退出企业



方式二，联系管理员，在管理后台【终端】-【终端管理】中进行删除，(需要注意的是，这种方式删除终端之后，该终端的数据将不能恢复，请谨慎操作)。

2、管理后台功能简介

2.1 总览

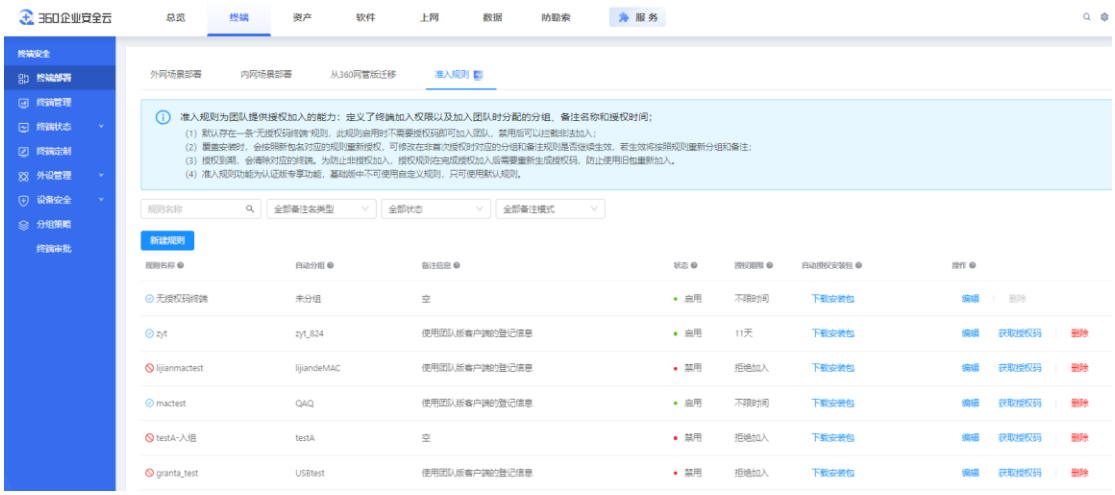
首页总览直观展示了企业全网终端的状态，包括：终端数量和状态统计、风险处理情况、安全状态、管理日志、PIN 码与团队密码、系统安全、防勒索信息等，便于管理员全面了解当前终端的整体情况。

2.2 终端

2.2.1 终端部署

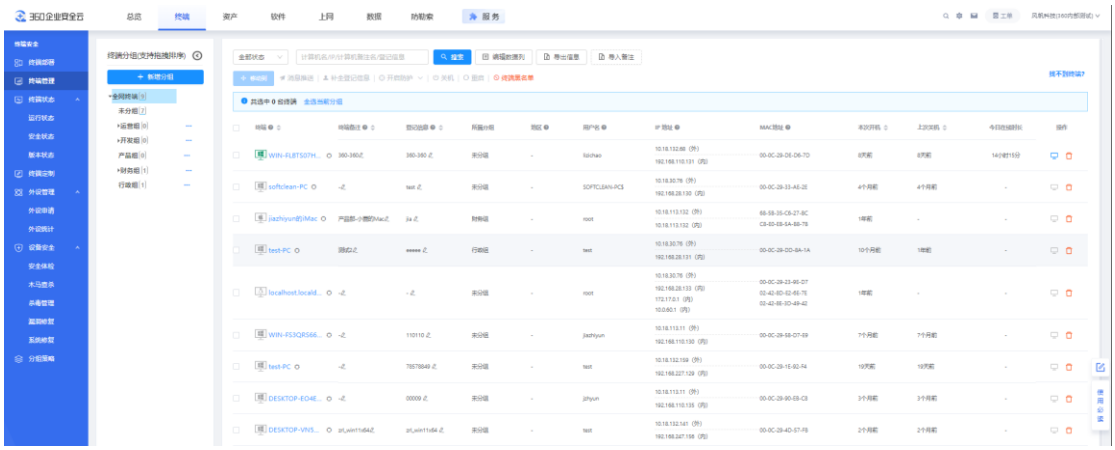
用户可根据各自企业内部网络情况选择不同部署方式，包括外网场景部署，内网场景部署，从 360 网管版迁移部署，亦可设置准入规则，此页面给予用户明确的部署方案。

准入规则设置（专业安全管理运维服务），可以下载相应规则的安装包，获取授权码，分发给终端用户安装部署即可，可有效避免非团队终端误加入团队。



2.2.2 终端管理

展示了企业内所有终端的基本情况，包括计算机基本信息：在线状态、计算机名、终端策略、备注名、登记信息、所属分组、IP、用户名、操作系统、开关机时间等，管理员可根据计算机名、IP、备注名等信息进行搜索，也可自定义列表展示信息，并且可以进行消息推送和一键关机重启的操作。



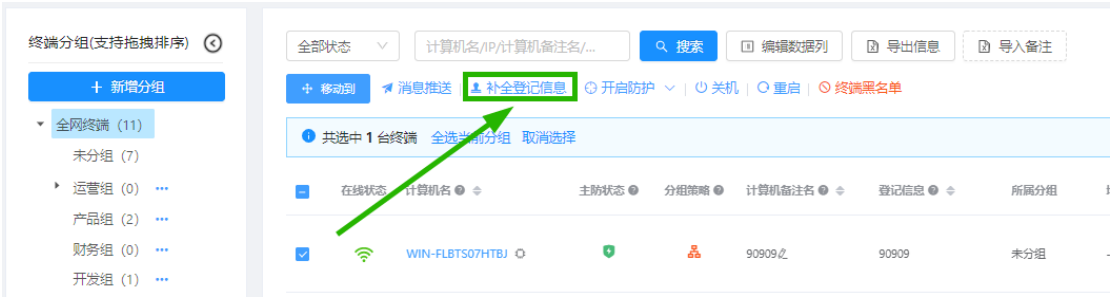
如果管理员想对某个终端进行远程协助，也可以在终端管理里操作

点击远程桌面-开始

等终端弹出 360 远程助手的提示框，点击确定

控制台会提示启动 360 远程助手，点击开启远程即可

在此页面也可以给终端发送补全登记信息的通知，以便管理员统计与管理。



2.2.3 终端状态

2.2.3.1 运行状态

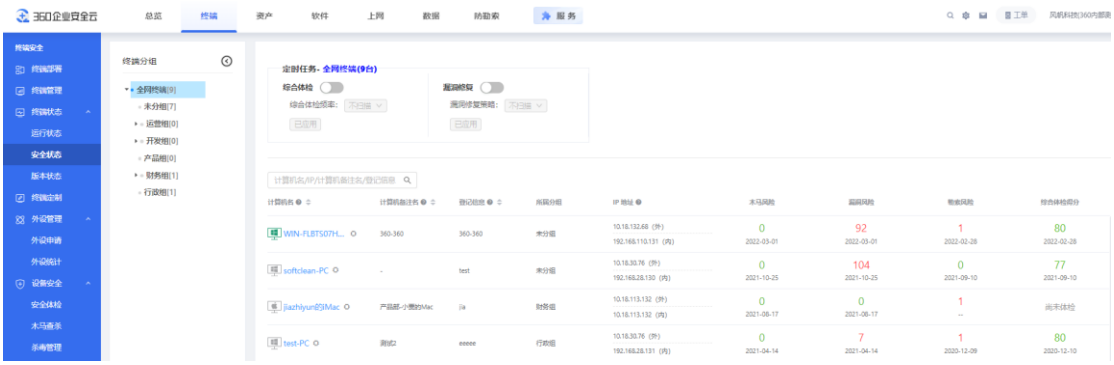
可以查看每台终端的运行状态，CPU（占用百分比和温度），内存（占用百分比和具体数据），系统盘（占用百分比和具体数据），硬盘（占用百分比和具体数据），实时速度，今日累计流量（包括上传下载）。

当然也可以对分组进行限速设置，还有分组定时关机和定时重启设置

2.2.3.2 安全状态

主要展示各终端的木马风险，漏洞风险和勒索风险，以及综合体检得分，帮助管理员快速发现风险，并修复存在的各种风险。

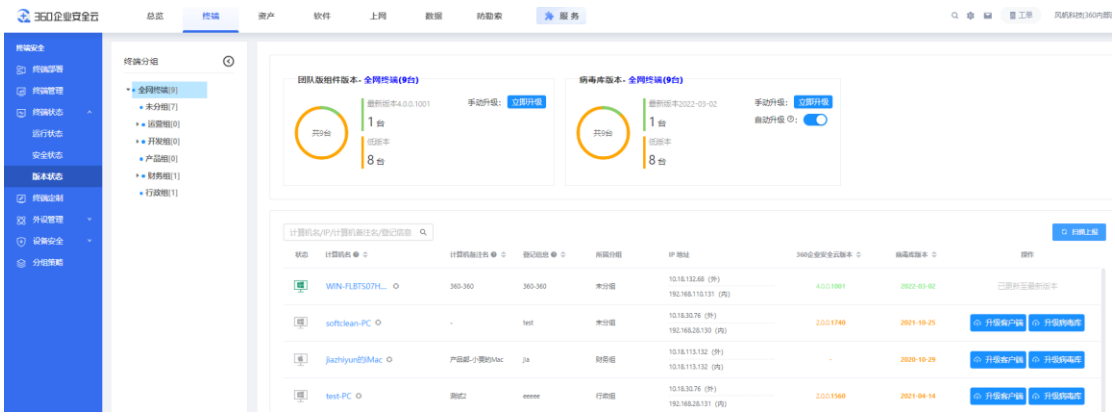
展示内容有计算机名，备注名，登记信息，所属分组，IP 地址，木马风险，漏洞风险，勒索风险，综合体检得分



同时可对分组进行定时体检和定时漏洞修复的设置

2.2.3.3 版本状态

可通过终端分组的维度，查看 360 企业安全云的版本，病毒库版本等，管理员可对分组或全局终端一键升级 360 企业安全云的版本，一键升级病毒库，亦可以对单台终端进行升级，如果您觉得此页面显示的版本号未更新，可以点击【扫描上报】更新控制台的数据。



2.2.4 终端定制

- **安全卫士主界面**

  默认样式：

  客户端默认界面，展示默认 logo

定制样式：

可在客户端主界面展示您企业组织的品牌 logo，企业信息卡片上可以显示管理员的联系方式及常用网址快捷入口，需要注意的是企业 logo 请按规定格式上传。

➢ **桌面壁纸（专业安全管理运维服务）**

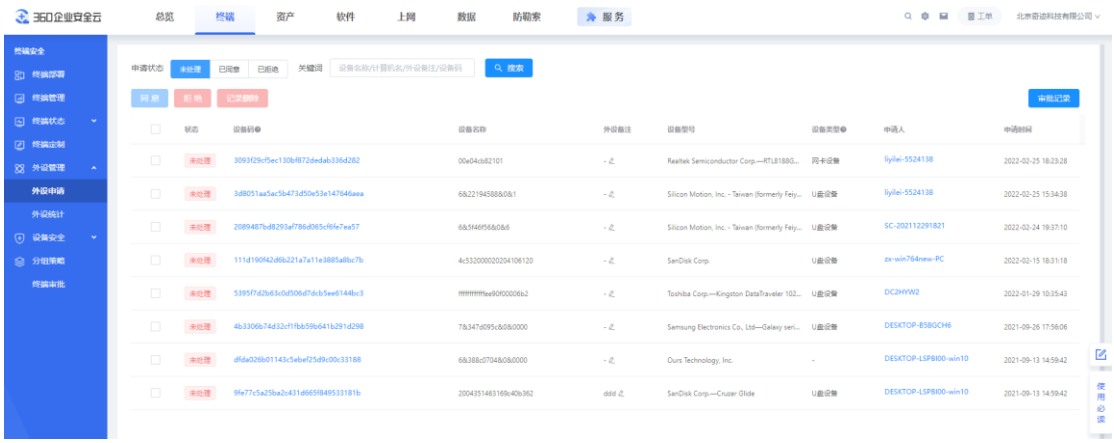
管理员可不限制桌面壁纸，终端用户可全权自行设置桌面壁纸样式；也可设置终端统一桌面壁纸。目前桌面壁纸功能只支持 windows 系统，每日上传壁纸次数为 3 次，壁纸库数

量不得大于 10 张（包括审核+未审核）； 壁纸文件格式为 JPG、PNG，且大小不能超过 20M。

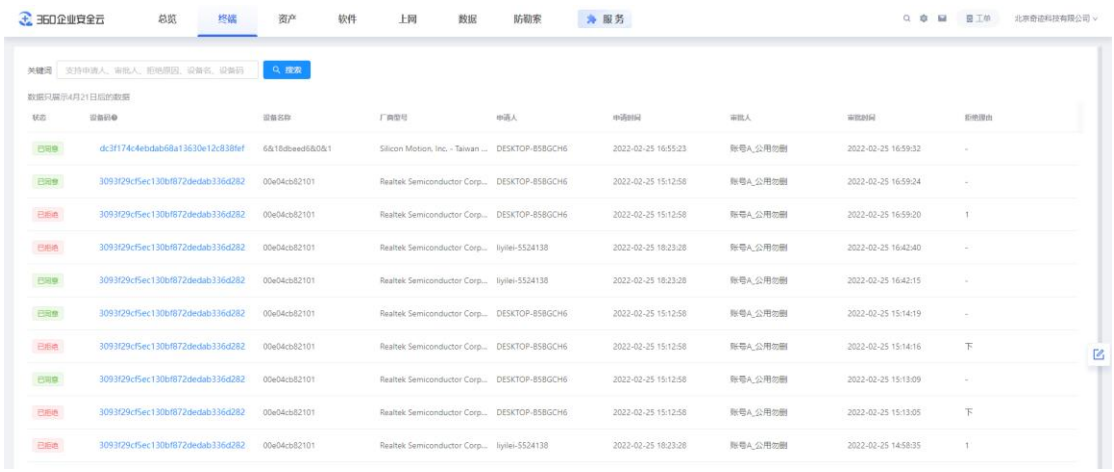
2.2.5 外设管理

在【外设申请】中，可以处理终端上提交使用 U 盘和网卡的申请。可以放行或者拒绝。设置成功后还可以再进行更改。

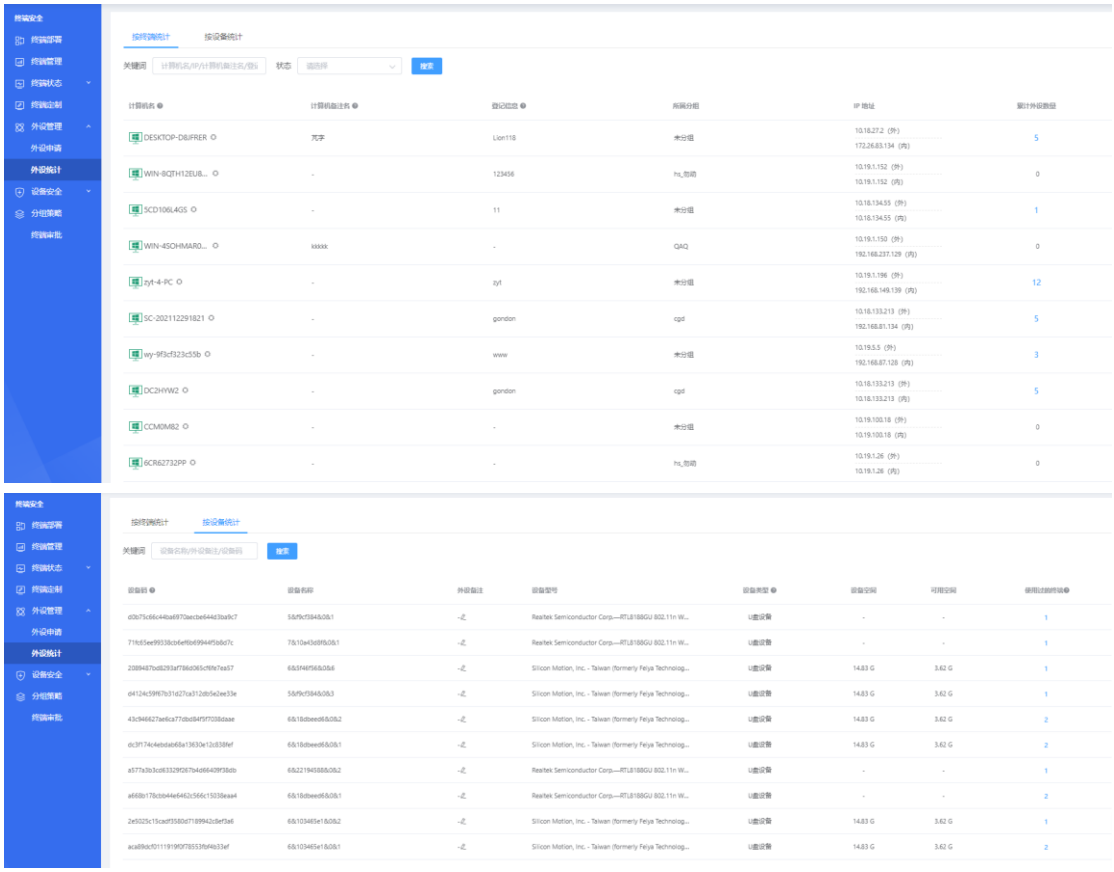
具体的外设限制策略，见【分组策略】中的【外设禁用】和【网卡禁用】



审批记录中可查看处理外设申请的记录，支持申请人、审批人、设备名、设备码、拒绝原因搜索。



外设管控是一个很常用的功能，【外设统计】中可按终端和设备两个维度统计，亦可查看使用外设记录。



2.2.6 设备安全

2.2.6.1 安全体检

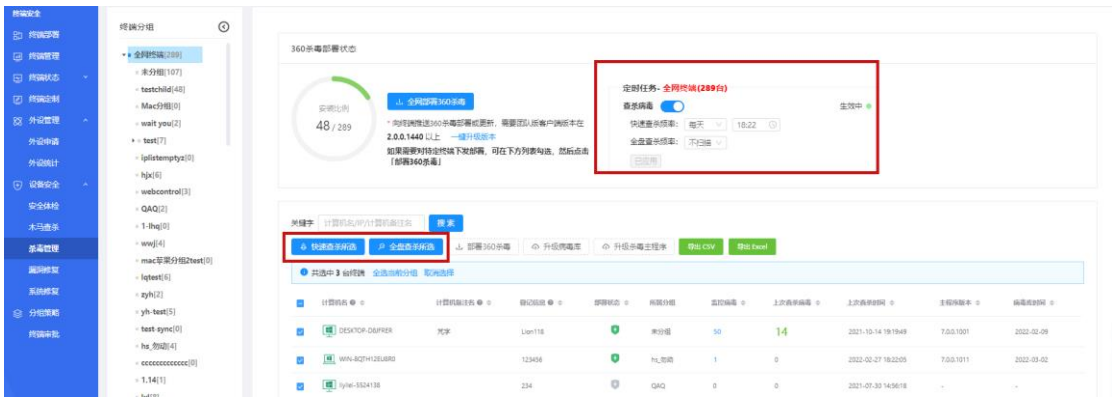
在安全体检页面中，可以查看全网终端的在线离线状态、IP 地址、MAC 地址以及体检状态等，可以对特别的终端进行修复，或者对多个终端进行一键扫描和一键修复。

2.2.6.2 木马查杀

支持选择终端进行【快递查杀】和【全盘查杀】，并展示查杀进度、查杀时间等。

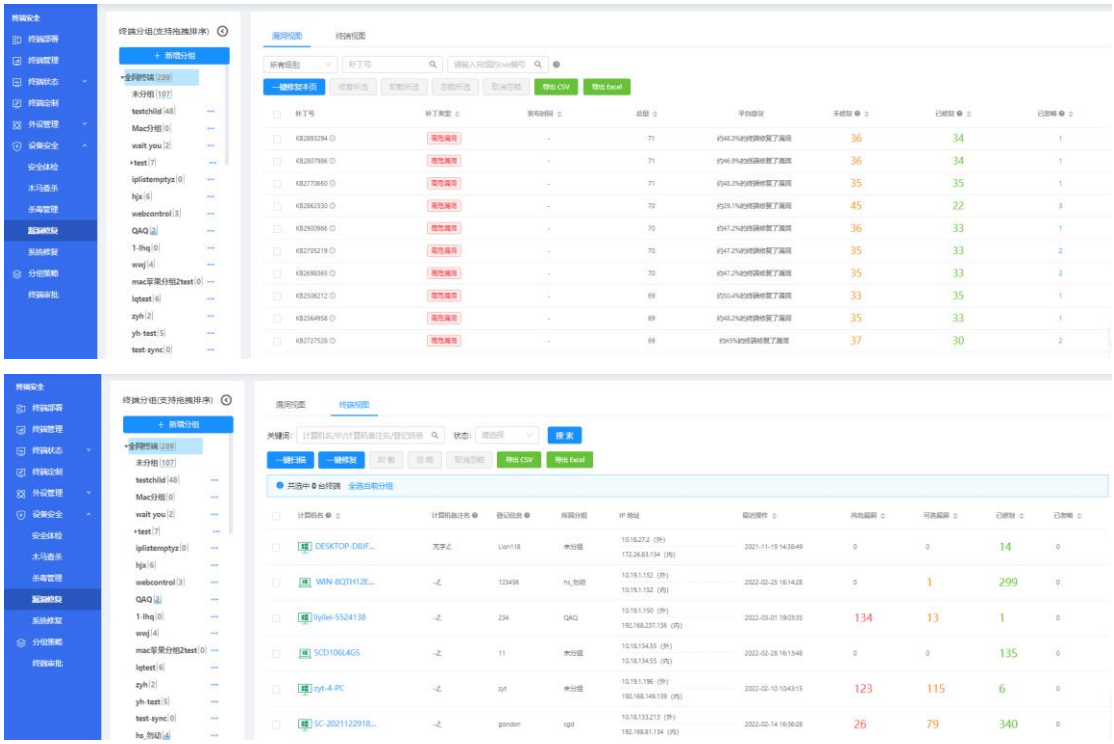
2.2.6.3 杀毒管理

360 企业安全云可以轻松的批量部署 360 杀毒，该功能是为了满足对 360 杀毒有需求的用户提供的。在该页面中，可以进行【快速扫描】、【全盘扫描】。也可以一键全网部署 360 杀毒，并升级病毒库。同时，在此也可进行分组定时杀毒设置。



2.2.6.4 漏洞修复

可以从漏洞统计和终端统计的不同维度展现目前整个企业内终端的漏洞情况，管理员可以针对不同程度的漏洞和特定的终端下发扫描、修复、卸载、忽略、取消忽略的命令。

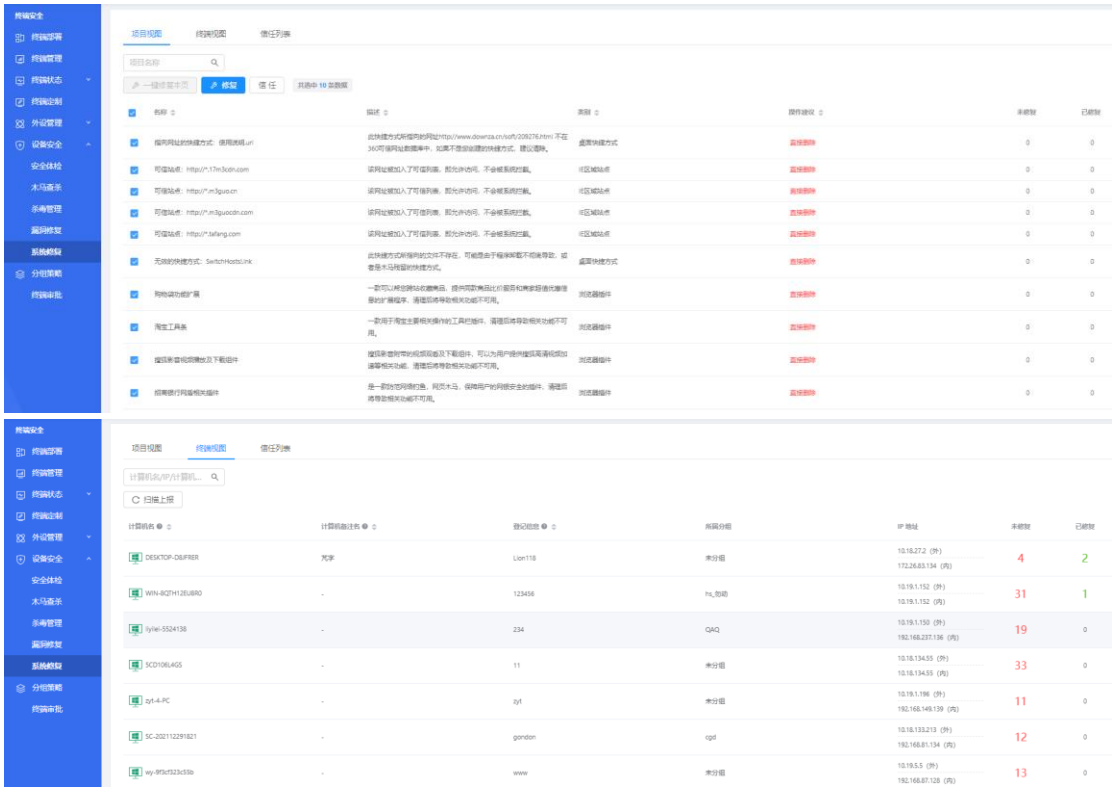


2.2.6.5 系统修复

可以从项目统计和终端统计的维度展现修复项的数量。

按项目统计页面可以查看修复项的名称、描述、类别、操作建议及未修复和已修复数量，

管理员可以下发批量修复和信任的命令，也可选择对特定项目进行修复和信任操作。



并且管理员还可以设置全局信任列表，或者对某个项目移除信任。

2.6.6 分组策略（部分专业安全管理运维服务）

目前支持对 windows、Linux、macOS 系统进行全网终端和分组终端的策略设置。

可对全网终端和分组终端进行基本设置、防护设置、消息推送、浏览器设置、文件白名单设置、漏洞管理、软件管家、外设禁用、USB 网卡禁用、预警设置、上网限制、安全基线、勒索防护等策略设置。

提示：面向分组设置不同的安全策略，设置过的分组和策略，会标记为 • XXX，设置过的子分组**不继承**上级分组的策略。

- **基本设置：**
  - 客户端设置

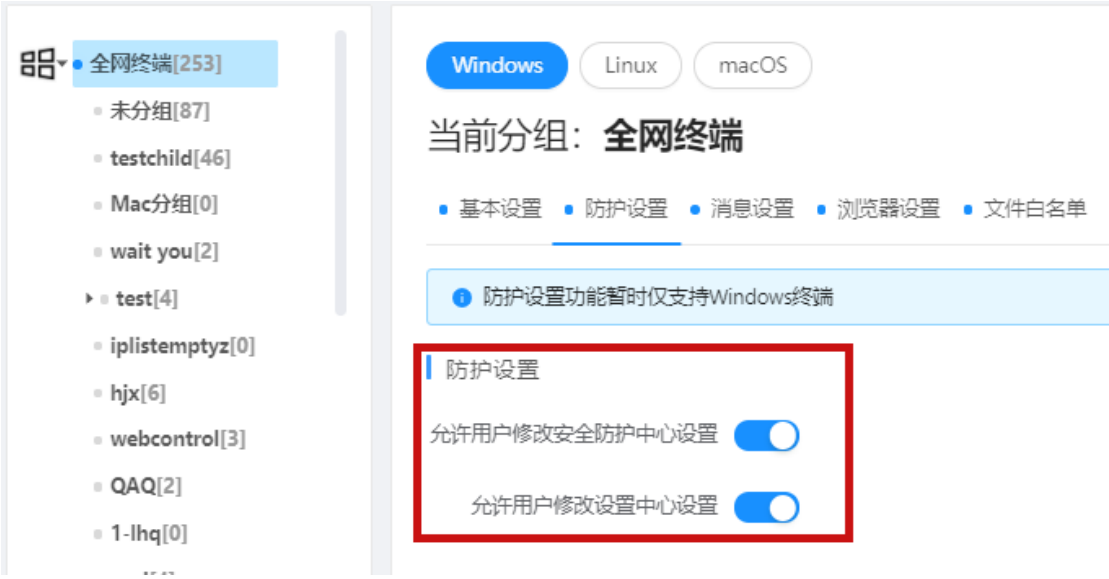
    卸载密码：设置防止终端卸载客户端的密码

    退出密码：设置防止终端退出客户端的密码

  可设置密码策略为动态密码或者静态密码

- **防护设置：**

  防护设置功能，可以批量设置是否允许用户修改客户端安全防护中心和设置中心的设置，暂时仅支持 windows 终端。



可以对终端客户端的设置中心和安全防护中心进行统一设置之后进行策略下发，以避免单台客户端进行重复设置。

➢ **消息设置：**

用于创建全局或者分组下发给终端的定时和周期性通知，管理员可根据通知需求进行内容编辑和时间设置，有效期过后，终端将不再接受消息。

➢ **浏览器设置（专业安全管理运维服务）：**

可设置全局或者分组终端的默认浏览器和浏览器主页。

➢ **文件白名单：**

对木马查杀任务的自定义设置，可以添加目录白名单、文件白名单、MD5 白名单，添加信任之后，木马查杀任务将不再扫描这些位置和文件。

➢ **漏洞管理：**

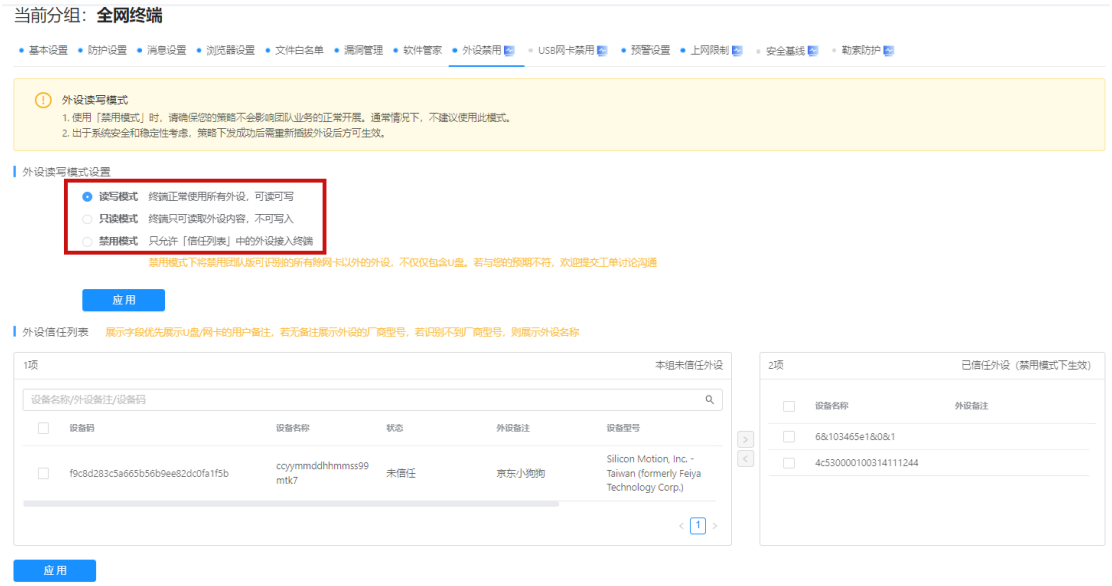
管理员对终端下发漏洞修复策略的设置，包括修复漏洞时间、漏洞类型、漏洞级别、修复完是否重启等设置。

➢ **软件管家：**

这里可以设置是否屏蔽软件管家入口，是否禁用软件管家的下载功能，可以防止终端通过软件管家下载不必要的软件。

➢ **外设禁用（专业安全管理运维服务）：**

管理员可设置全局终端或分组终端的外设读写模式，并可添加外设的信任列表。



➢ **USB 网卡禁用（专业安全管理运维服务）：**

管理员可设置全局终端或分组终端的网卡启用/禁用模式，并可添加网卡的信任列表。

➢ **预警设置：**

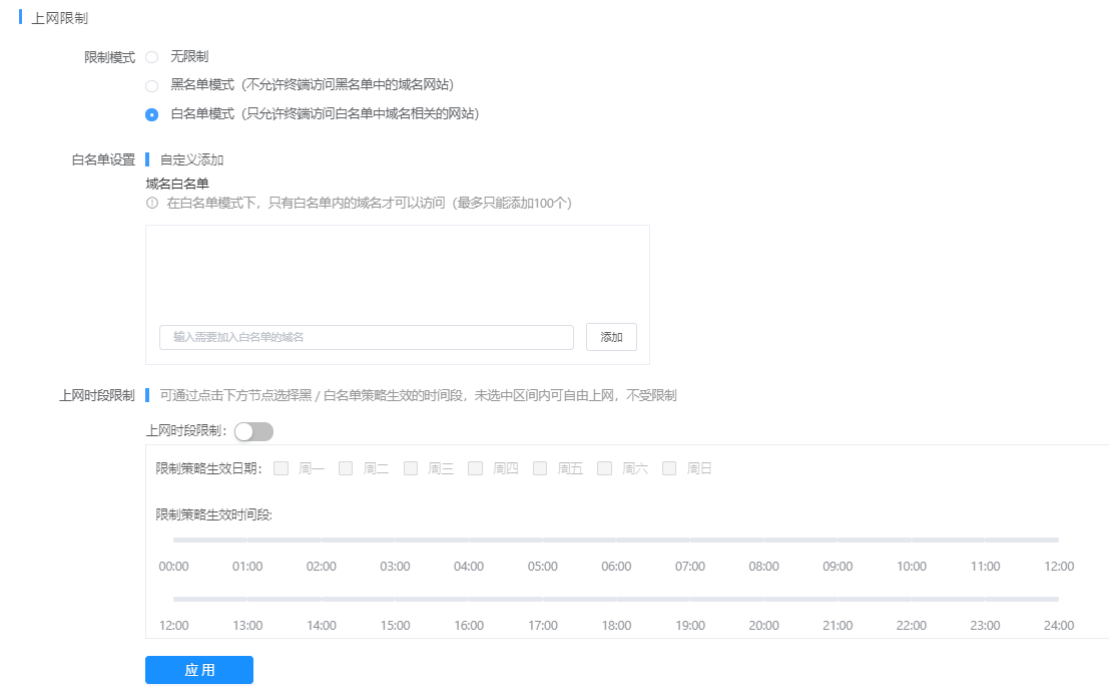
可以设置全局终端和分组终端的预警时间和预警类型。预警时间可以设置预警频率和预警时间段；预警类型可以选择哪些关注的项目进行预警提示，设置预警阈值并邮件告警。

➢ **上网限制（专业安全管理运维服务）：**

上网限制分为无限制、黑名单和白名单三种模式，默认为无限制模式。

黑名单模式即不允许终端访问黑名单中的域名网站；可设置上网时段限制。

白名单模式即只允许访问白名单中域名相关的网站，可设置上网时段限制



➢ **安全基线（专业安全管理运维服务）：**

检查有助于用户一键获知全网主机安全基线配置详情，找出不符合安全管理规范的终端，节省大量人工检查时间，并能持续进行监控。此功能设置后，可以在【防勒索】-【安全基线】页面中查看对应的防护效果。

➢ **勒索防护（专业安全管理运维服务）：**

对于终端的勒索防护设置可以选择允许远程桌面连接的时间段。

Linux 系统：

目前 Linux 系统支持的分组策略有基本设置、消息设置、文件白名单和预警设置，并且在持续更新中，策略下发与 windows 系统一致。

- **基本设置：**

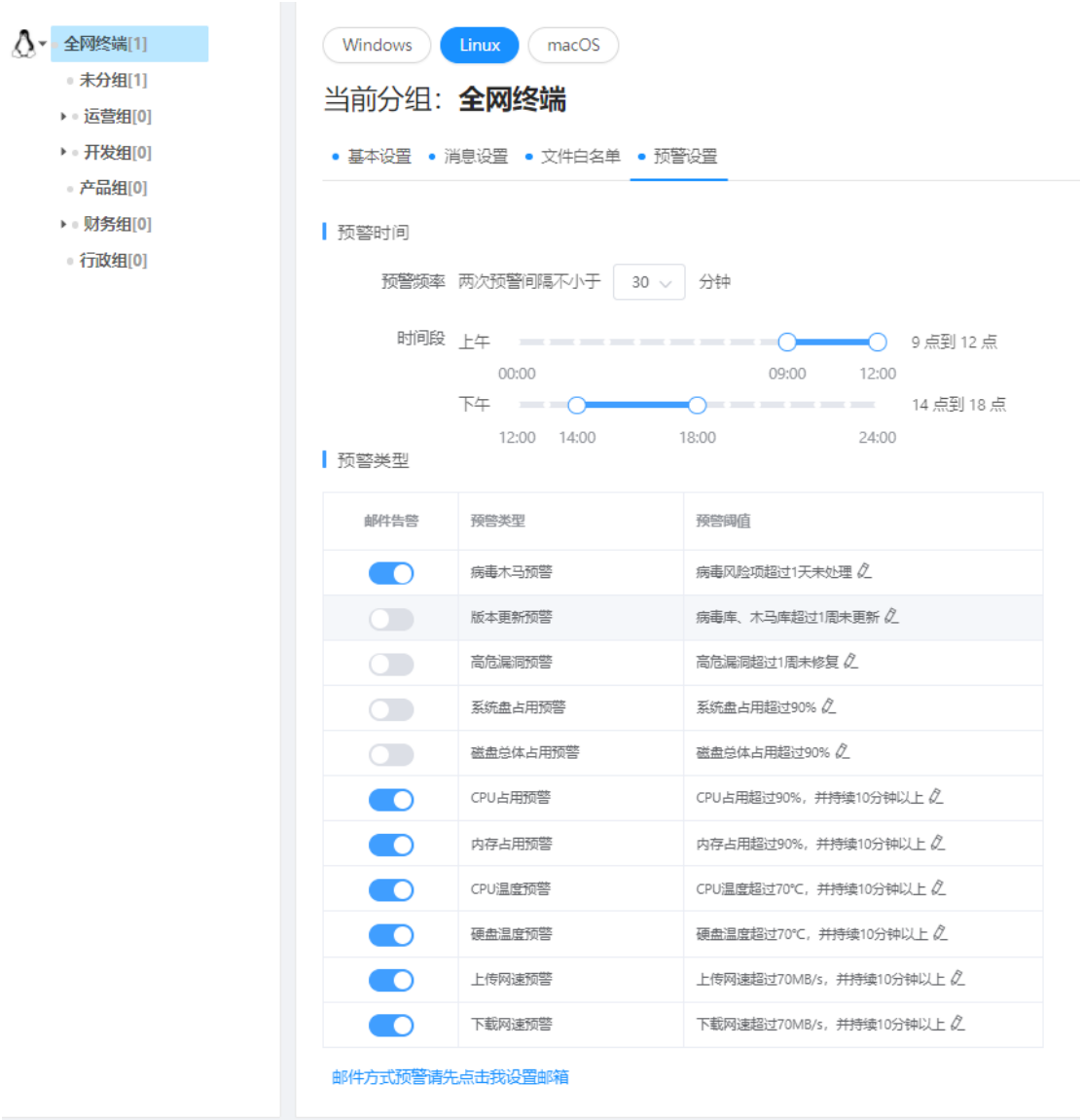
- **消息设置：**


全网终端[1]
未分组[1]
运营组[0]
开发组[0]
产品组[0]
财务组[0]
行政组[0]
Windows
Linux
macOS
当前分组：全网终端
基本设置
消息设置
文件白名单
预警设置
向终端推送定时和周期性的消息。有效期过后，终端将不再接收消息。
消息设置
消息设置开启
* 消息标题
消息标题
* 消息内容
请输入消息内容，不能超过500个字符
推送URL
URL地址，例如: https://www.360.cn
* 有效期至
选择时间
发布时间
开机显示
周期显示
每周一
08:00
应用

- **文件白名单：**


全网终端[1]
Windows
Linux
macOS
当前分组：全网终端
基本设置
消息设置
文件白名单
预警设置
自定义设置
目录白名单
文件白名单
MD5白名单
如何查询文件MD5?
未添加
添加
应用

- **预警设置：**



macOS 系统：

目前 macOS 系统支持的分组策略有基本设置、消息设置、文件白名单、外设禁用和预警设置，并且在持续更新中，策略下发与 windows 系统一致。

- **基本设置：**


Windows
Linux
macOS
当前分组：全网终端
基本设置
消息设置
文件白名单
外设禁用
预警设置
设置「卸载密码」和「退出密码」可以防止终端用户随意卸载/退出客户端。
客户端设置
当前应用策略为动态密码，此处并未生效 【查看动态密码】 【修改密码策略】
卸载密码
卸载密码
应用
退出密码
退出密码
应用

- **消息设置**

➢ **文件白名单**

➢ **外设禁用（专业安全管理运维服务）：**


全网终端[1]
未分组[0]
运营组[0]
开发组[0]
产品组[0]
财务组[1]
行政组[0]
Windows
Linux
macOS
当前分组：全网终端
基本设置
消息设置
文件白名单
外设禁用
预警设置
macOS网卡禁用
macOS不支持网卡的禁用管控
外设读写模式
1. 使用「禁用模式」时，请确保您的策略不会影响团队业务的正常开展。通常情况下，不建议使用此模式。
2. 出于系统安全和稳定性考虑，策略下发成功后需重新插拔外设后方可生效。
外设读写模式设置
读写模式 终端正常使用所有外设，可读可写
禁用模式 只允许「信任列表」中的外设接入终端
应用
外设信任列表
展示字段优先展示U盘/网卡的用户备注，若无备注展示外设的厂商型号，若识别不到厂商型号，则展示外设名称
本组未信任外设 0/7
已信任外设（禁用模式下生效） 0/0
京东小狗狗
Initio Corporation—INIC-3619PN SATA B...
VMware, Inc.
SanDisk Corp.—Ultra
[鼠标]Logitech, Inc.—M105 Optical Mouse
Parallel Dice Co., Ltd
无数据
应用

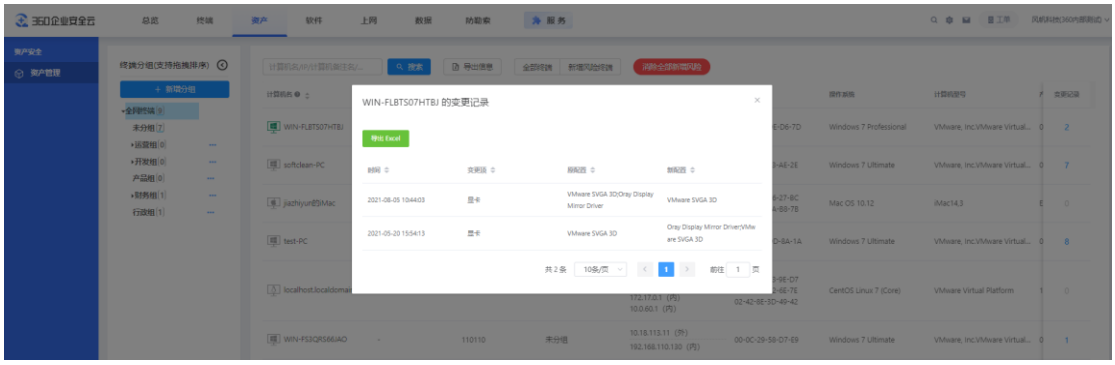
- **预警设置：**


Windows
Linux
macOS
当前分组：全网终端
基本设置
消息设置
文件白名单
外设禁用
预警设置
预警时间
预警频率 两次预警间隔不小于 30 分钟
时间段 上午 9 点到 12 点
00:00 09:00 12:00
下午 14 点到 18 点
12:00 14:00 18:00 24:00
预警类型
邮件告警 预警类型 预警阈值
病毒木马预警 病毒风险项超过1天未处理
版本更新预警 病毒库、木马库超过1周未更新
高危漏洞预警 高危漏洞超过1周未修复
系统盘占用预警 系统盘占用超过90%
磁盘总体占用预警 磁盘总体占用超过90%
CPU占用预警 CPU占用超过90%，并持续10分钟以上
内存占用预警 内存占用超过90%，并持续10分钟以上
CPU温度预警 CPU温度超过70℃，并持续10分钟以上
硬盘温度预警 硬盘温度超过70℃，并持续10分钟以上
上传网速预警 上传网速超过70MB/s，并持续10分钟以上
下载网速预警 下载网速超过70MB/s，并持续10分钟以上
邮件方式预警请先点击我设置邮箱

2.3 资产

2.3.1 资产管理

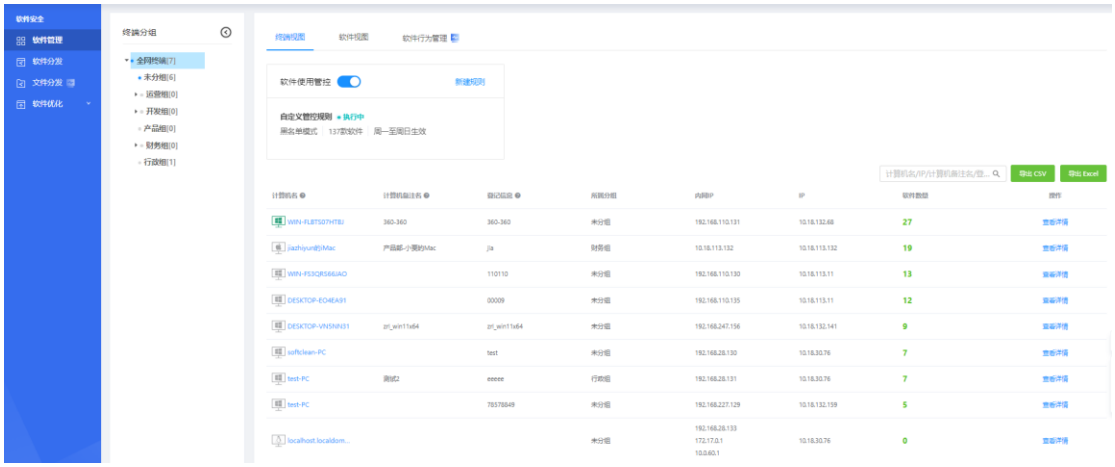
方便管理员针对终端的系统（操作系统版本，产品 ID)、硬件信息（计算机型号，CPU,内存容量，内存信息，硬盘，主板，显卡，网卡，声卡，显示器，SN 码等)、变更记录进行查看，导出分析。

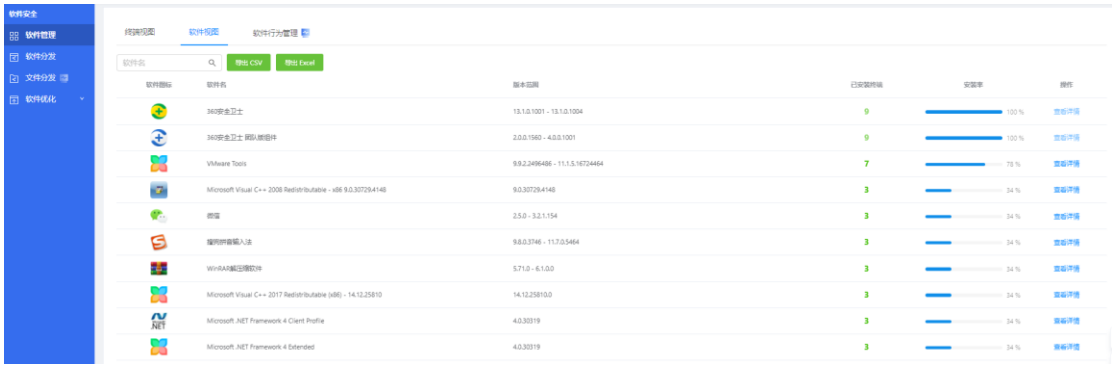


2.4 软件

2.4.1 软件管理

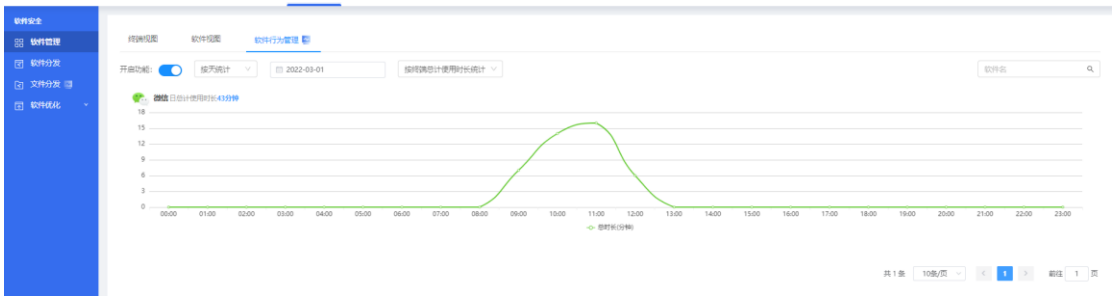
软件管理可以对终端已安装的软件情况进行查看以及相应的操作：卸载、数据导出、软件升级。具体的操作请点击该终端对应“查看详情”。





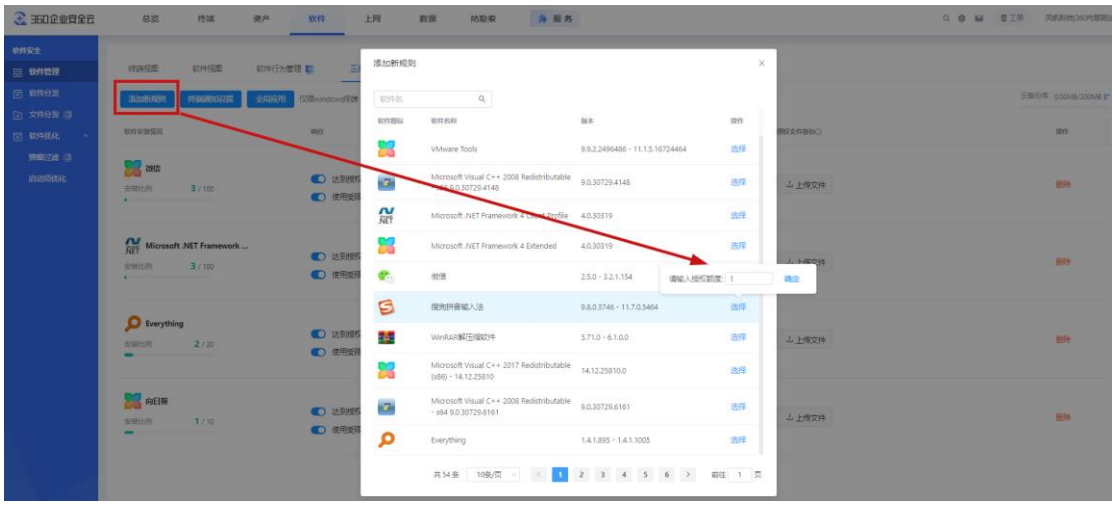
- **软件行为管理**（专业安全管理运维服务）

软件行为管理，可以按天，周针对终端进行软件使用总时长，软件使用平均时长统计。也可以统计软件使用的终端数和时间段。

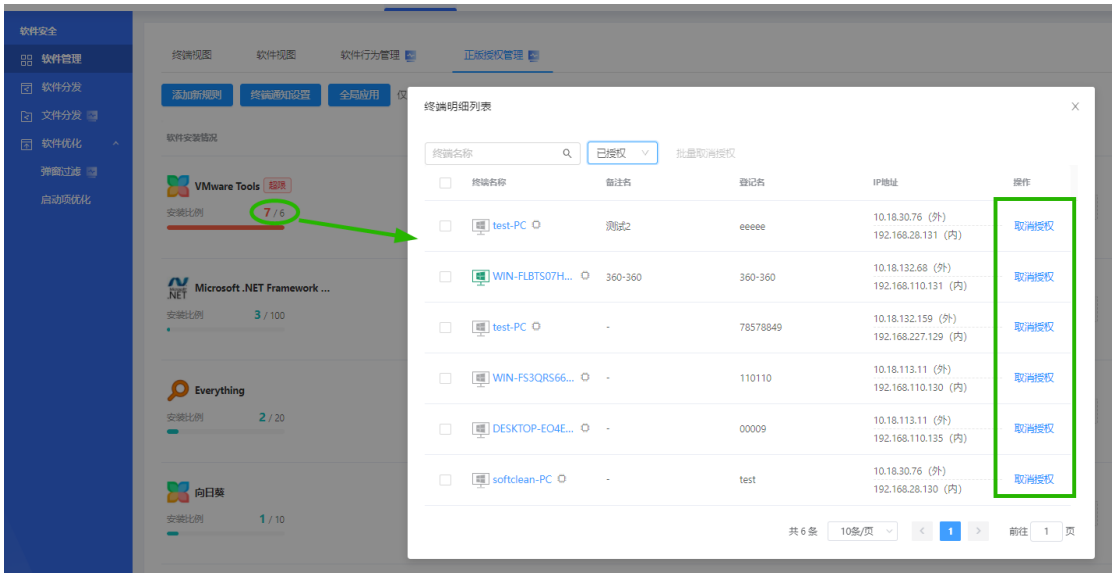


- **正版授权管理**（专业安全管理运维服务）

此功能可以设置在终端上运行的软件，达到软件授权的数量后，剩余的终端将不能使用此软件，有效的提高正版软件的使用率。软件使用受限时，会提醒终端用户。

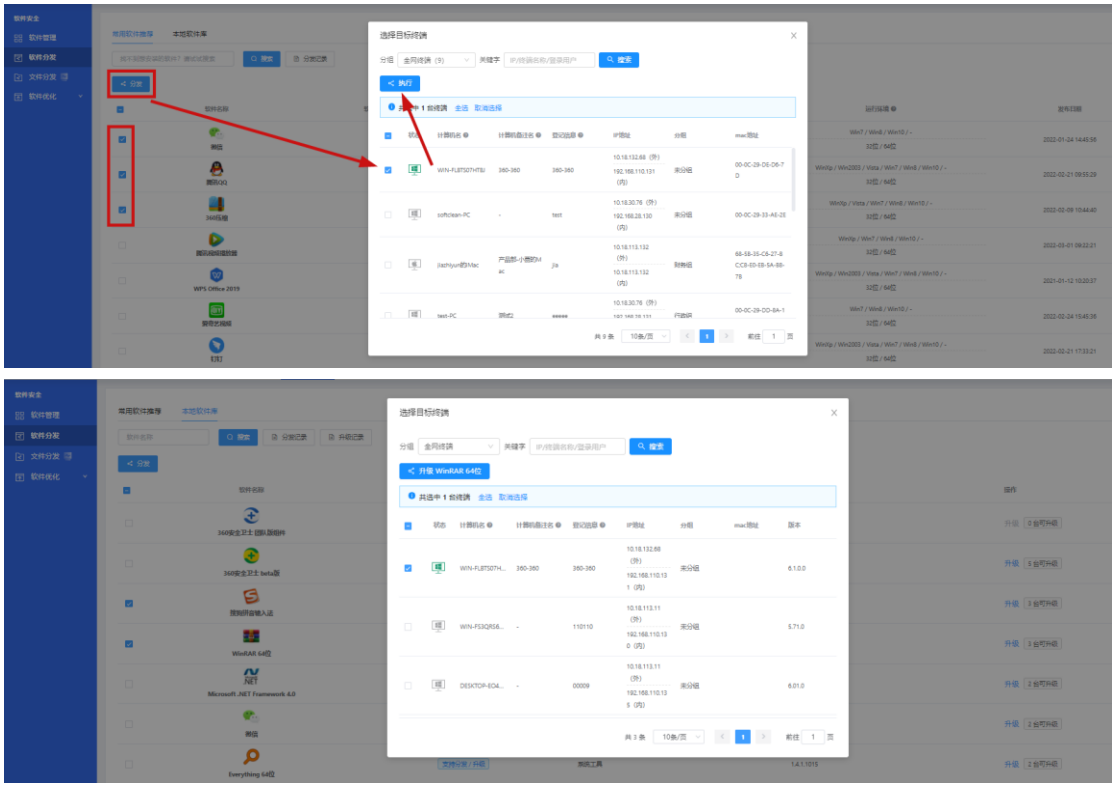


点击安装比例的数字，可以查看终端明细，进行授权和取消授权的操作。



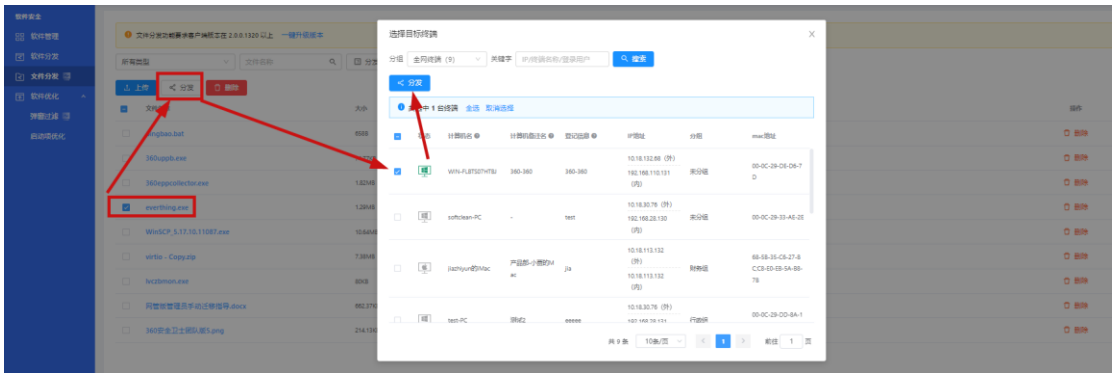
2.4.2 软件分发

软件分发顾名思义是对软件的一种分发策略。在【常用软件推荐】中，提供了部分用户常用的软件，可以直接进行分发。【本地软件库】中的软件识别是来自全网终端上安装的软件。可以对版本较低的终端进行升级。



2.4.3 文件分发（专业安全管理运维服务）

文件分发是可以分发文件、或者一些软件安装包。操作流程是先将文件上传到云服务器，然后通过云服务器进行分发，如果是安装包可以设置在终端执行。

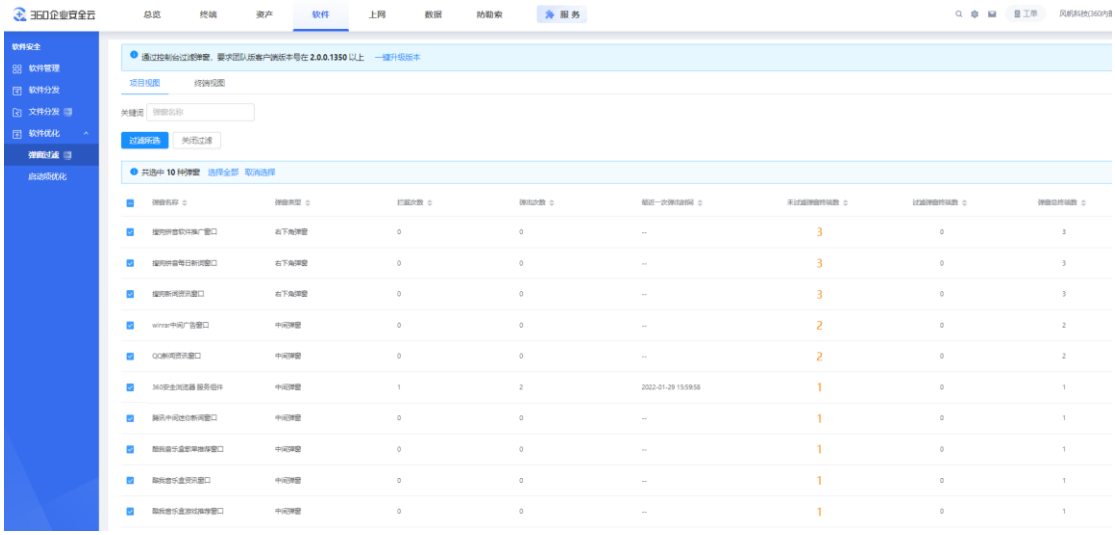


2.4.4 软件优化

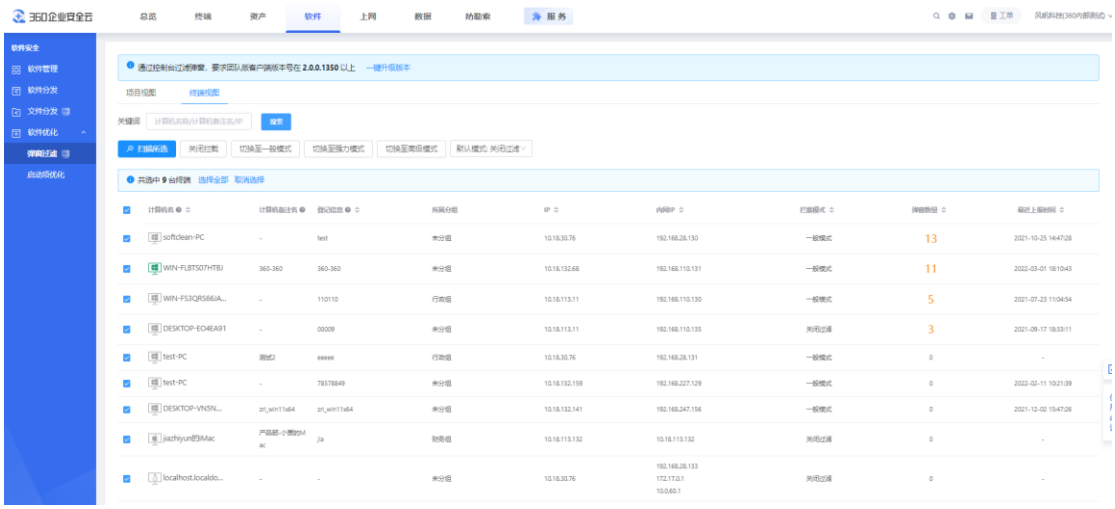
2.4.4.1 弹窗过滤（专业安全管理运维服务）

项目视图，显示目前全网终端所有弹窗的信息，可选择对某个项目开启或者关闭过滤策

略。

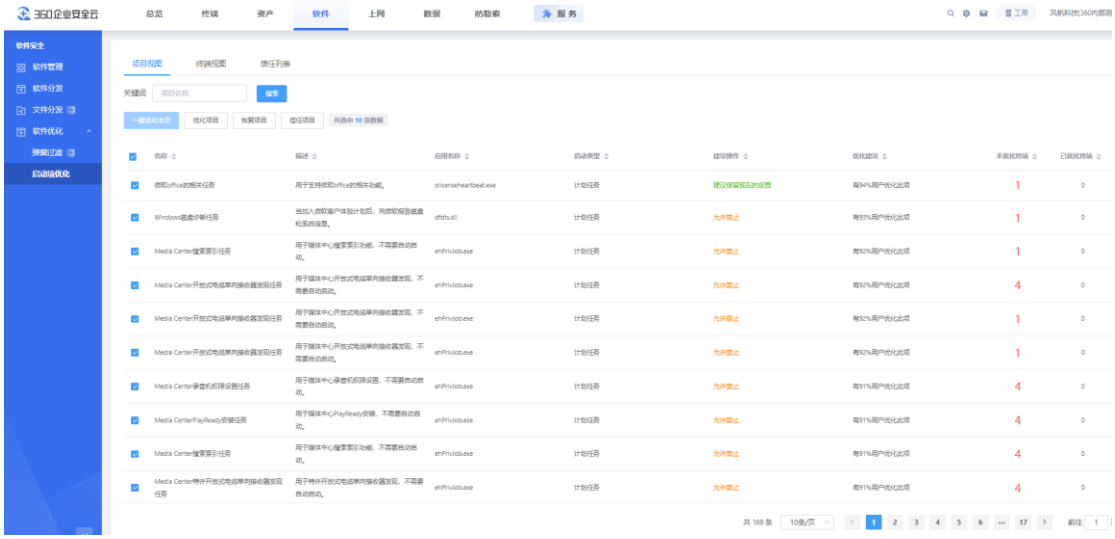


终端视图，可以设置全网终端的弹窗拦截策略，拦截模式分为一般模式、强力模式和高级模式，可根据不同终端实行不同拦截模式。

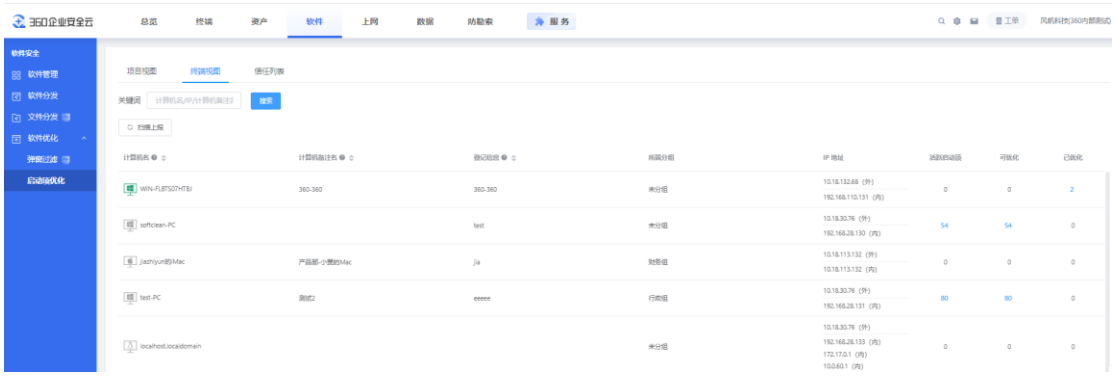


2.4.4.2 启动项优化

从启动项目维度具体可以查看启动项的名称、描述、类型、优化建议等，点击对应数字均可查看每个项目未优化终端和已优化终端，管理员可以按需下发优化、恢复和信任项目的指令。



从终端统计维度展现各个终端活跃启动项、可优化启动项、已优化启动的数量。点击数字可以查看具体启动项目。如需即时更新，可点击【扫描上报】按钮。



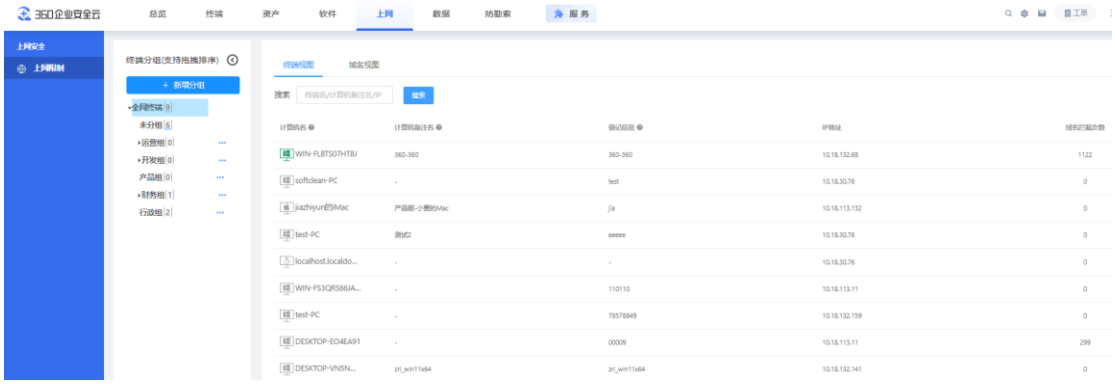
管理员也可添加和移除全局信任项目。

2.5 上网

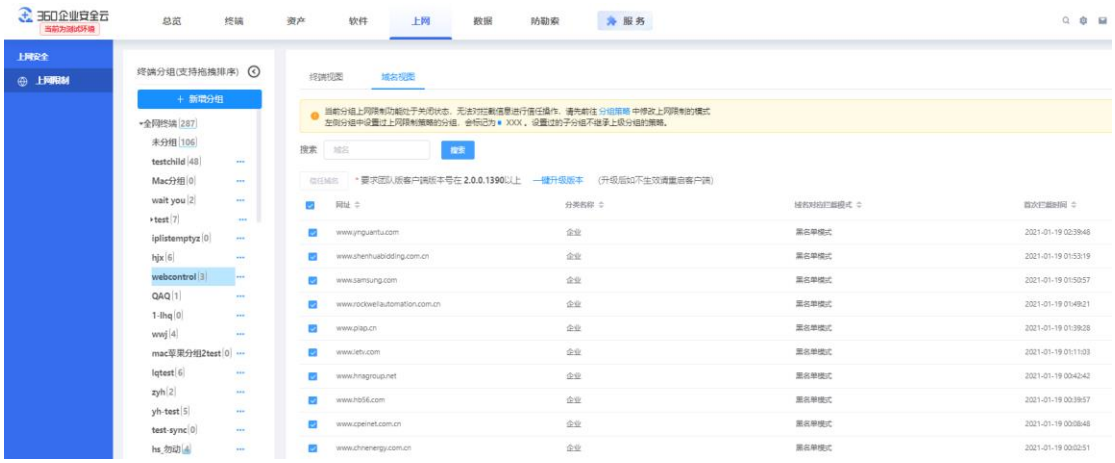
2.5.1 上网限制

上网限制功能主要有黑名单和白名单两种策略，在此页面中，可以查看到具体终端受到域

名拦截的次数。



也可按域名展示，查看已设置域名的规则和具体域名是什么。



2.6 数据

2.6.1 屏幕水印（专业安全管理运维服务）

开启屏幕水印，将在终端屏幕顶层覆盖自定义信息，可以追溯截图来源，实现版权保护。

2.6.2 安全设置（专业安全管理运维服务）

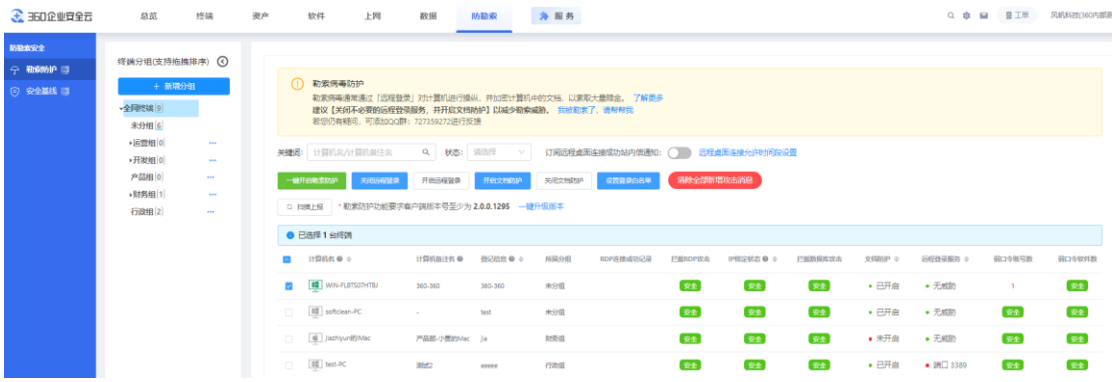
开启屏幕锁屏，所选分组终端将在无人使用时定时自动锁屏，可节省电费、延迟设备使用寿命，保护企业电脑隐私安全，防止他人偷偷获取或修改企业重要数据。

2.7 防勒索

2.7.1 勒索防护（专业安全管理运维服务）

管理员可查看电脑的防护状态：文档防护状态，远程登录服务端口的状态，拦截 RDP 攻击

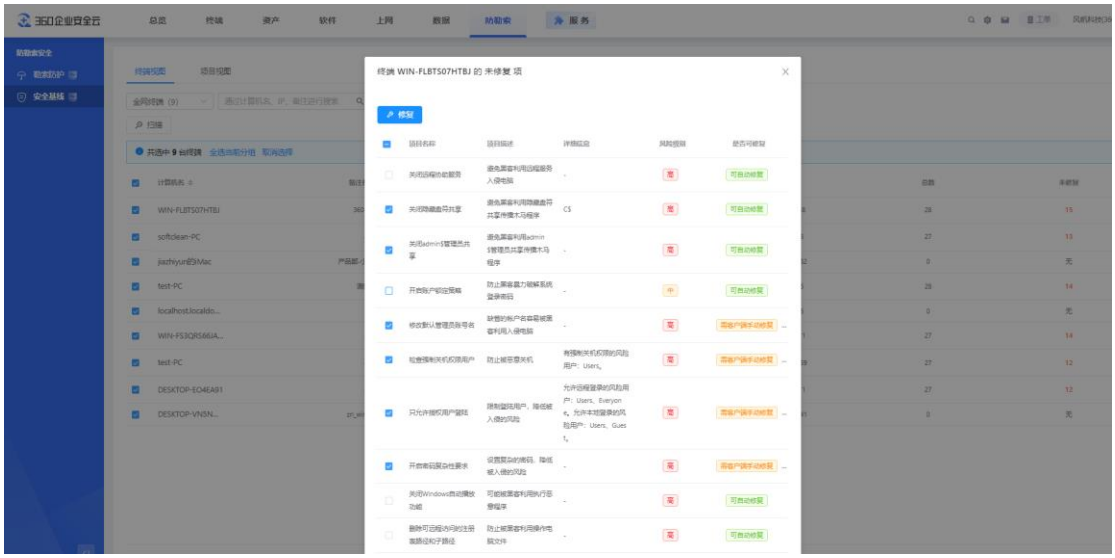
次数，IP 锁定状态，拦截数据库攻击次数，弱口令账号数，弱口令账号软件等。情动一键批量开启或关闭远程登录，文档防护功能，以避免勒索病毒加密电脑中的重要文档。也可在【终端】-【分组策略】-【勒索防护】对允许远程桌面连接的时间进行设置。



2.7.2 安全基线（专业安全管理运维服务）

安全基线检查有助于用户一键获知全网终端安全基线配置详情，找出不符合安全管理规范的主机，节省大量人工检查时间，并能持续进行监控。

此功能需要在【终端】-【分组策略】-【安全基线】中进行功能开启和配置。



2.8 服务

服务模块将展示您已订阅的服务和服务市场，您可以在此页面看到订阅详情和服务内容。

为助力产业数字化，【全面安全守护服务】和【通用云存储服务】可永久免费使用，不限制终端数量，【专业安全管理运维服务】可选择购买。

点击相应服务即可查看具体服务内容。

2.9 页眉功能导航

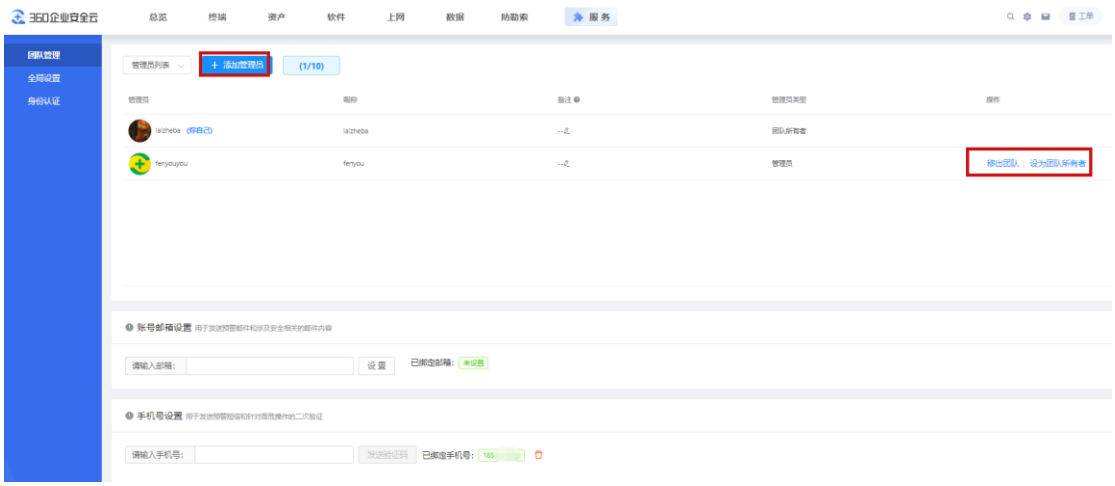
2.9.1 关键字搜索

根据您需要的具体功能，可以查询跳转到对应的功能页面，比如搜索：“木马查杀”、“体检”、“软件分发”、“弹窗过滤”等关键字进行页面跳转。

2.9.2 设置

2.9.2.1 团队管理

支持添加管理员，转移权限，设置新的账号所有者，绑定和设置用于接收预警邮件及安全相关邮件内容的邮箱和手机号码。



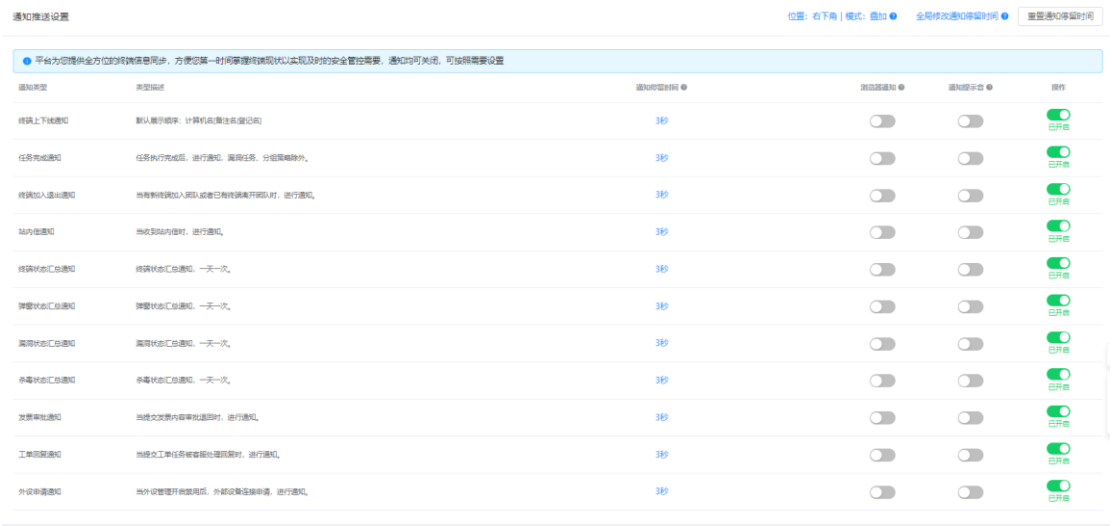
2.9.2.2 全局设置

➢ 全局列筛选

该设置用于选择需要展示的终端名称，隐藏不需要的项，请至少选择一项展示，该设置将应用于平台中需要展示终端名称的所有页面

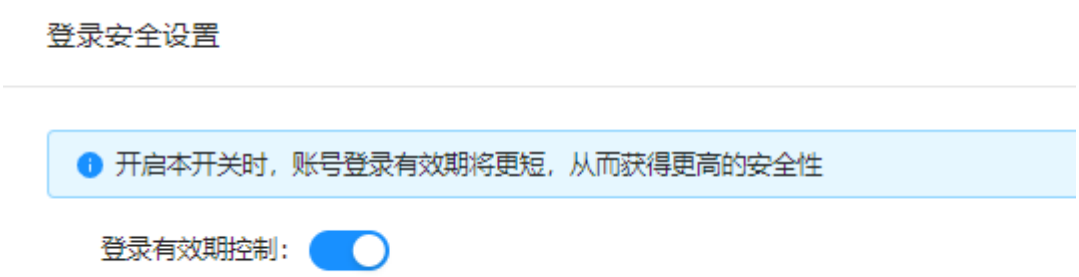
➢ 通知推送设置

平台为您提供全方位的终端信息同步，方便您第一时间掌握终端现状以实现及时的安全管控需要，通知均可关闭，可按照需要设置



- **登录安全设置**

开启登录有效期控制开关，当管理员离开一定时间后，再打开控制台需要重新输入登录账号和密码才可以查看控制台信息，可有效保护控制台的安全。



- **终端密码策略设置**

在此可以设置终端电脑客户端退出和卸载时的密码形态，静态密码或者动态密码。设置动态密码的变更周期范围为 60 秒-3600 秒之间。卸载和退出时必须在有网络的环境下进行。

2.9.2.3 身份认证

购买付费服务、开具产品授权申明需要进行身份认证，个人、企业认证后均可获得产品授权声明，未进行企业认证时购买的订单，不能开具增值税专用发票。

2.9.3 站内信

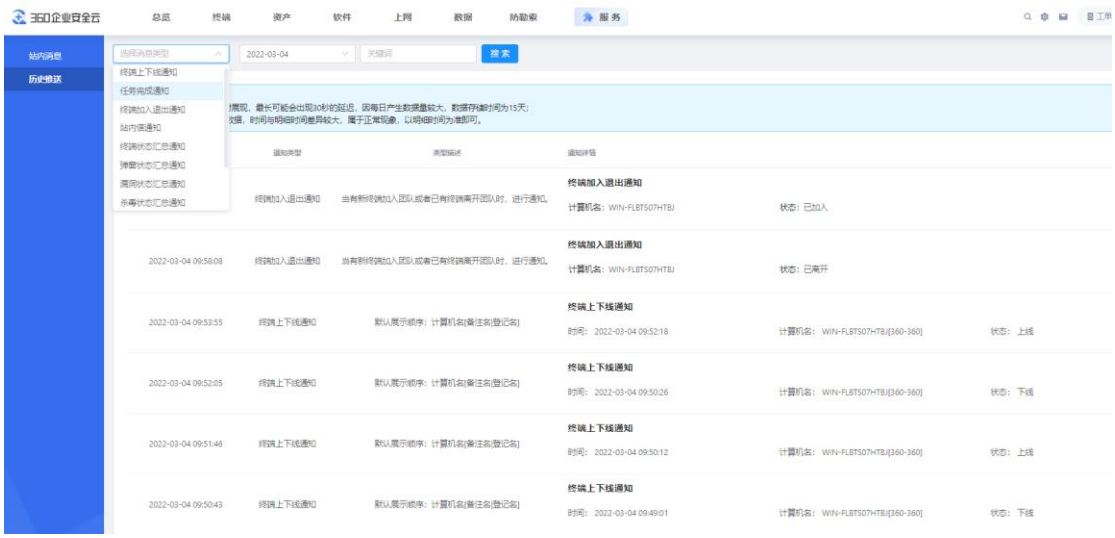
2.9.3.1 站内消息

360 企业安全云的公告、通知、预警信息、壁纸和 logo 审核结果等都会通过站内消息发送给管理员，记录在此。

2.9.3.2 历史推送

管理员可查看终端上下线通知，任务完成通知，终端加入退出等通知，

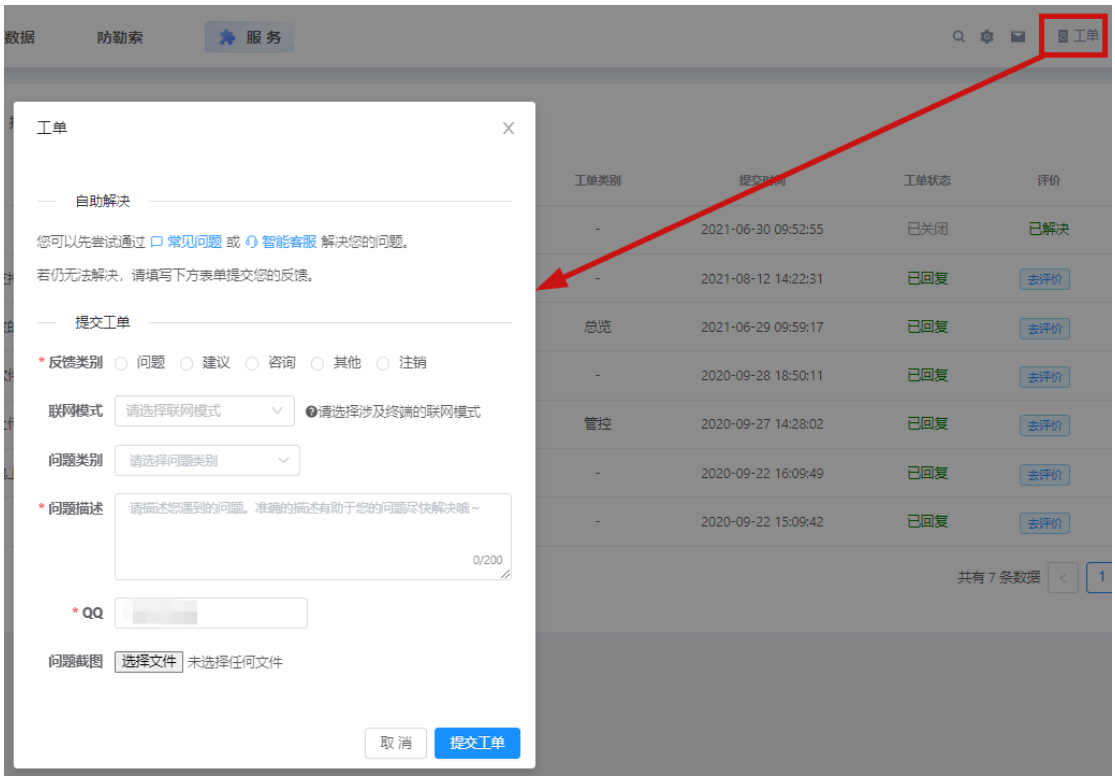
需注意的是：历史推送数据非实时展现，最长可能会出现 30 秒的延迟，因每日产生数据量较大，数据存储时间为 15 天。



2.9.4 工单系统

2.9.4.1 提交工单

如果您在安装和使用 360 企业安全云的过程中有什么问题或者建议，欢迎通过【提交工单】反馈给我们，点击“提交工单”即可选择相应的问题分类，客服人员收到您的反馈会第一时间回复或与您取得联系核实问题。



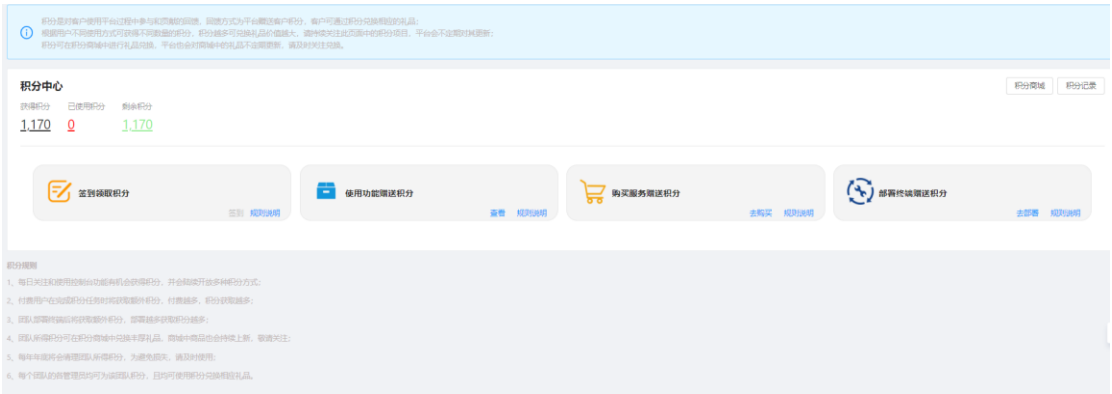
2.9.4.2 历史工单

工单列表展示的是您曾经提交过的工单，可以在次查看客服人员给您的回复或者继续追问。

2.9.5 账号设置

2.9.5.1 积分中心

积分是对用户使用平台过程中参与和贡献的回馈，回馈方式为平台赠送用户积分，根据用户不同使用方式可获得不同数量的积分，用户可通过积分兑换相应的礼品。



2.9.5.2 切换团队

同一个账号下可以创建多个企业团队，比如既有收费版本，又有免费版本的企业；一个集团下面多个子公司的企业，更方便管理。

2.9.5.3 账号中心

可以对账号的绑定手机号码、邮箱、登录密码进行修改。

2.9.5.4 退出登录

退出登录即可回到 360 企业安全云管理后台的登录页面。

3、客户端主要功能简介

3.1 首页体检

体检为电脑进行从病毒木马、高危漏洞、系统异常、电脑垃圾、电脑速度等方面的安全性快速检测，解读安全性能，指引快速修复，帮助用户保持电脑健康。

打开 360 企业安全云，会直接展现体检主界面，点击“立即体检”开始体检。

扫描完成，会展现电脑健康得分与电脑当前存在的问题，并提供解决方案，点击“一键修复”即可。

3.2 木马查杀

全球领先的云查杀技术，加上立体的主动防御系统和人工智能查杀引擎，第一时间拦截查杀

最新木马。

查杀方式分为快速查杀，全盘查杀和按位置查杀，用户可以自由选择查杀类型。

3.3 系统安全

修补电脑漏洞，修复系统故障，及时更新补丁和驱动，确保电脑安全。修复方式分为全面修复和单项修复，用户可按需选择。

扫描完成，会将可修复项分类展现，点击“一键修复”即可修复完成。

3.4 网络安全

保护网络安全，杜绝网络隐患，解决网络信号差。

3.5 数据安全

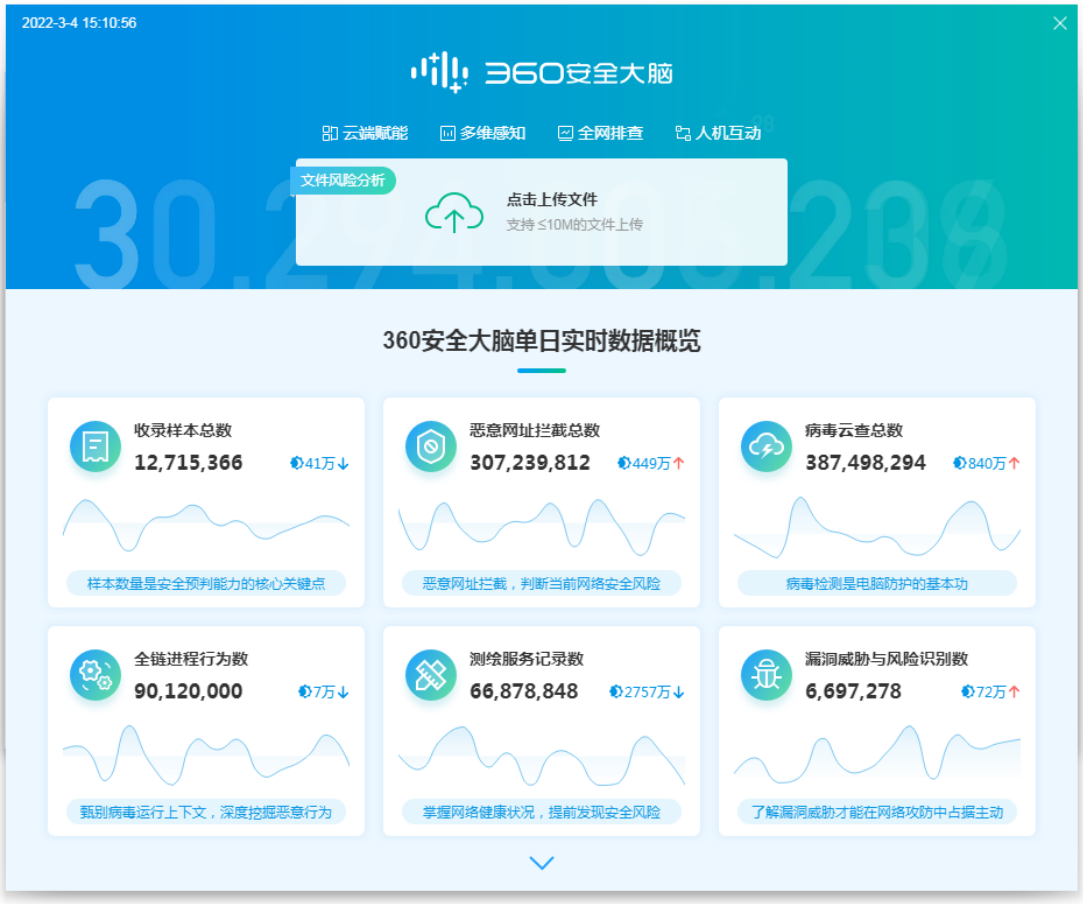
保障数据安全，解决文档被勒索、篡改的问题。

3.6 优化加速

清理电脑垃圾，全面优化电脑性能，轻装运行。

3.7 安全大脑

直观感受 360 安全大脑单日实时数据概览，也可将本地风险文件上传进行分析

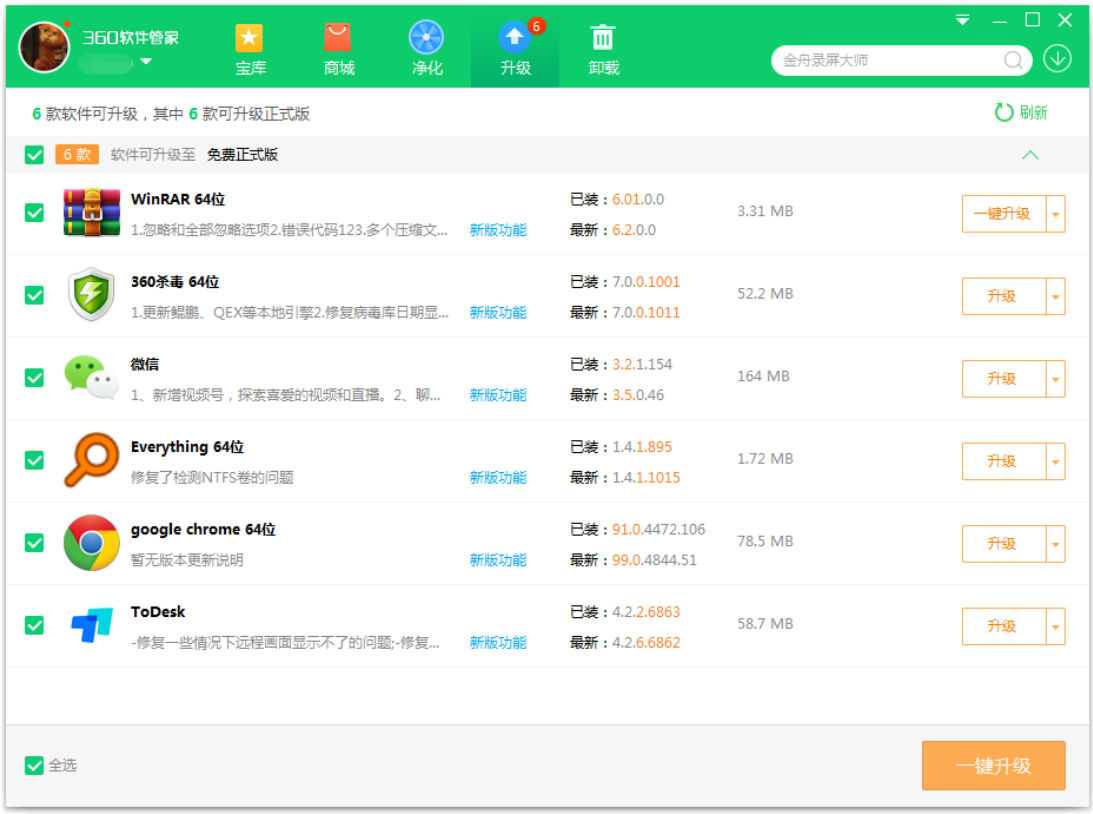


3.8 软件管家

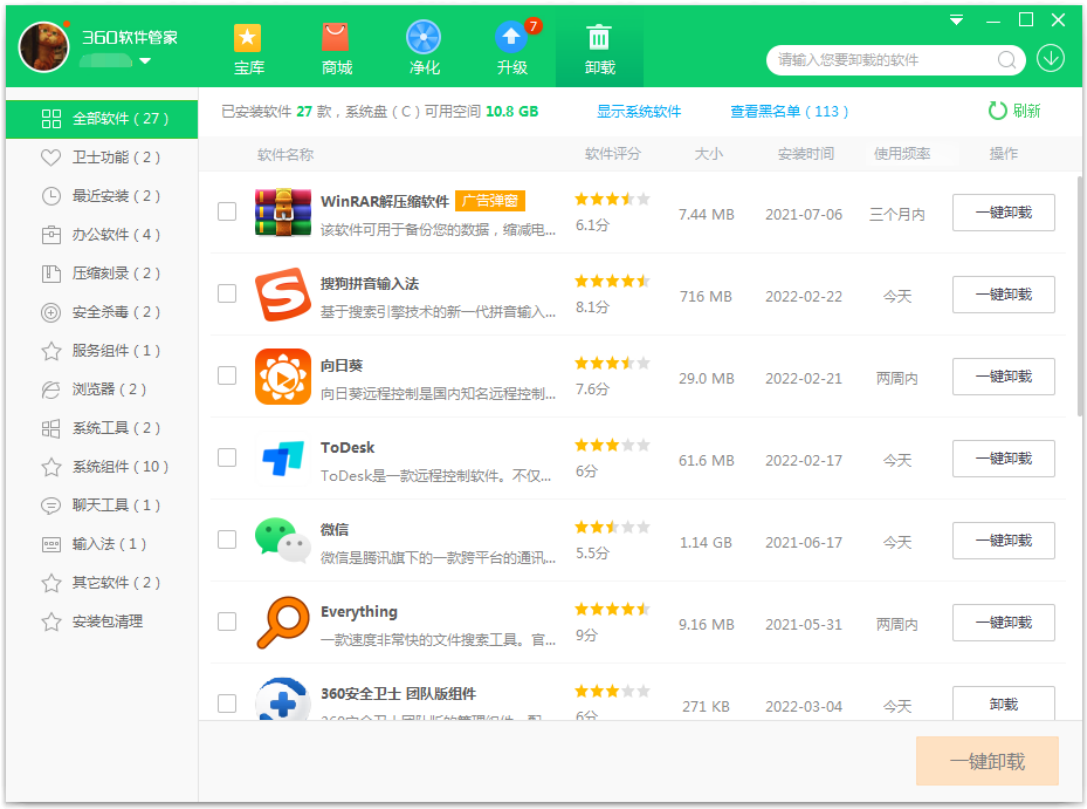
软件管家为用户提供海量的正版软件的高速安全下载服务。

用户可以通过左侧分类导航或者搜索功能快速定位到所需软件，点击“一键安装”即可。

点击软件管家主界面上的“升级”界面，可为用户提供可升级软件的详细更新信息，用户可点击“一键升级”对软件进行升级。



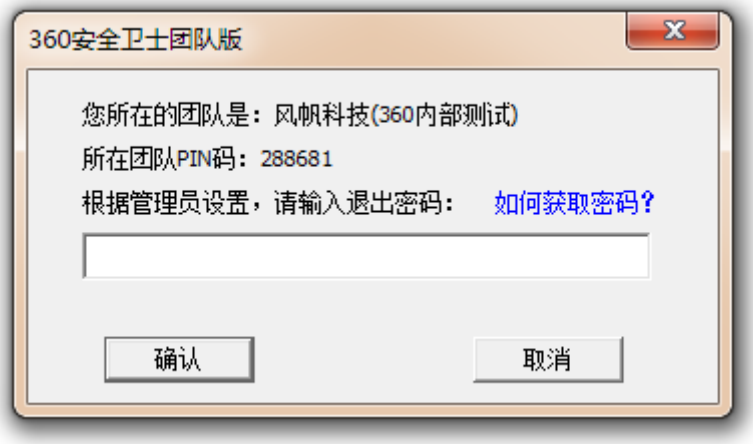
点击软件管家主界面上的“卸载”界面，用户可以通过左侧分类导航或者搜索功能快速定位到需要卸载的软件，点击“一键卸载”即可卸载。



4、客户端退出、卸载

4.1 退出

已加入企业组织的终端，如果想在本地退出，需要输入退出密码，密码需要联系管理员获取。



输入正确的退出密码后，可进入正常退出的流程。

4.2 卸载

已加入企业组织的终端，如果想在本地卸载，需要输入卸载密码，密码需要联系管理员获取。

输入正确的卸载密码后，可进入正常的卸载流程。