



360企业安全云

360企业安全云

产品操作手册



©2020-2025 360 公司 保留所有权利

本文档所有内容均为 360 公司独立完成，未经 360 公司作出明确书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形状）对本文档的任何部分进行复制、修改、存储、引入检索系统或者传播。

版本信息

文档名称	更改内容	文档版本	密级	维护人
360 企业安全云产品操作手册	新增部分功能及管理后台页面改版	V5.7	公开	贾志云

目录

1、安装部署指南	11
1.1 客户端配置环境要求	11
1.2 企业注册	12
1.3 客户端部署	14
1.3.1 windows 系统部署	14
1.3.2 Linux 系统部署	26
1.3.3 macOS 系统部署	29
1.4 退出企业	33
2、管理后台功能简介	35
2.1 总览	35
2.2 终端	36
2.2.1 终端部署	36
2.2.2 终端管理	41
2.2.3 远程运维（专业安全管理运维服务）	42
2.2.3.1 远程控制	42
2.2.3.2 消息推送	44
2.2.3.3 文件分发	46
2.2.4 终端状态	47
2.2.4.1 运行状态	47
2.2.4.2 安全状态	48

2.2.4.3 版本状态	49
2.2.4.4 文件白名单.....	49
2.2.5 终端定制	50
2.2.5.1 终端界面定制.....	50
2.2.5.2 桌面壁纸定制（专业安全管理运维服务）	51
2.2.5.3 软件管家设置（专业安全管理运维服务）	51
2.2.6 终端审批	52
2.2.6.1 团队审批	52
2.2.6.2 卸载审批	53
2.2.7 终端交互	53
2.2.7.1 反馈处理	53
2.2.7.2 小程序功能.....	54
2.2.8 外设管理	57
2.2.8.1 外设申请（专业安全管理运维服务）	57
2.2.8.2 外设统计	57
2.2.8.3 外设禁用（专业安全管理运维服务）	58
2.2.9 设备安全	59
2.2.9.1 安全体检	59
2.2.9.2 木马查杀	60
2.2.9.3 杀毒管理	60
2.2.9.4 漏洞修复	61
2.2.9.5 系统修复	62

2.2.9.6 防护设置	63
2.2.10 分组策略（部分专业安全管理运维服务）	64
2.3 资产	72
2.3.1 资产管理	72
2.3.1.1 资产体检	72
2.3.1.2 资产信息（专业安全管理运维服务）	73
2.3.2 风险预警	74
2.3.2.1 预警管理	74
2.3.2.2 预警日志	75
2.4 行为	75
2.4.1 软件管控	75
2.4.1.1 软件管理	75
2.4.1.2 软件运行拦截（专业安全管理运维服务）	78
2.4.1.3 正版软件授权管理（专业安全管理运维服务）	79
2.4.1.4 安装与启动禁用.....	80
2.4.1.4 软件运行统计（专业安全管理运维服务）	81
2.4.2 软件优化	82
2.4.2.1 弹窗过滤（专业安全管理运维服务）	82
2.4.2.2 启动项优化.....	83
2.4.3 上网管控（专业安全管理运维服务）	84
2.4.3.1 上网拦截	84
2.4.3.2 IP 地址拦截	86

2.4.3.3 端口拦截	86
2.4.3.4 拦截统计	87
2.4.4 人员行为审计（需单独付费）	88
2.4.4.1 桌面动态可视	89
2.4.4.2 软件行为审计	92
2.4.4.3 上网行为审计	93
2.4.4.4 防挖矿	95
2.4.5 应用流量管控（需单独付费）	96
2.4.6 浏览器访问管理	98
2.4.6.1 部署和锁定（专业安全管理运维服务）	98
2.4.6.2 首页管理	98
2.4.6.3 应用管理	99
2.4.6.4 兼容管理	99
2.4.6.5 策略管理	100
2.4.6.6 消息管理	101
2.4.6.7 使用统计（专业安全管理运维服务）	102
2.4.7 零信任访问（需单独付费）	102
2.4.8 DNS 安全解析（需单独付费）	105
2.5 数据	106
2.5.1 数据云盘（需单独付费）	106
2.5.2 水印管理（专业安全管理运维服务）	111
2.5.3 安全设置（专业安全管理运维服务）	114

2.5.4 数据统计	114
2.5.4.1 数据概览（需单独付费）	114
2.5.4.2 数据报表（需单独付费）	116
2.5.5 数据防泄漏（需单独付费）	118
2.5.5.1 关键数据发现	118
2.5.5.2 数据管控审计	119
2.5.5.3 风险行为审批	123
2.5.6 数字可视化大屏（需单独付费）	124
2.6 防勒索（专业安全管理运维服务）	125
2.6.1 勒索防护	125
2.6.2 远程接入策略	125
2.6.3 勒索风险及日志	126
2.6.4 安全基线	127
2.6.5 勒索病毒解密	128
2.7 人员管理	129
2.7.1 组织机构	129
2.7.2 企业登录配置	129
2.7.3 应用访问控制	129
2.8 扩展（需单独付费）	130
2.8.1 苏打办公账号管理	130
2.8.2 Web 应用防火墙	131
2.8.3 安全运营托管服务	132

2.9 服务市场	133
2.10 页眉功能导航	134
2.10.1 关键字搜索.....	134
2.10.2 福利中心	134
2.10.3 SaaS 商店.....	135
2.10.4 站内信.....	136
2.10.4.1 站内消息	136
2.10.4.2 历史推送	136
2.10.5 设置	137
2.10.5.1 账户中心.....	137
2.10.5.2 切换团队.....	138
2.10.5.3 团队管理（部分专业安全管理运维服务）	139
2.10.5.4 工单管理.....	142
2.10.5.5 左导航偏好设置	143
2.10.5.6 退出登录.....	144
3、客户端主要功能简介	144
3.1 首页体检	144
3.2 木马查杀	146
3.3 系统安全	147
3.4 优化加速	148
3.5 数据安全	149
3.6 软件管家	150

3.7 功能面板	152
4、客户端退出、卸载.....	153
4.1 退出	153
4.2 卸载	154

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 系统	Windows XP sp3 及以上 Windows Server 2003 R2 及以上	2 核	4G	>50G	最低配置
Linux 系统	Centos6/7/8 Deepin 20 Ubuntu16/18/20/22/24 Ubuntu20-aarch64-无桌面刻录版				
信创系统	银河麒麟 V10(sp1)桌面版 Loongarch64/amd64/arm64 银河麒麟 V10 桌面版 mips64/arm64 银河麒麟服务器版 amd64/arm64 统信 UOSV20 桌面版 amd64/arm64/loongarch64/mips64 中科方德 5 桌面版-amd64				
MacOS	macOS 10.11 以上				

1.2 企业注册

通过官方网址 <https://saas.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。

完善团队信息 开启管控

 请填写真实的组织/公司名称

组织规模：☒ 几台电脑 ☐ 200台以下
☐ 200-1000台 ☐ 1000台以上

进入控制台

☐ 我同意 [许可协议](#) 和 [隐私协议](#)

登录管理后台会有企业专属的 PIN 码，这是客户端（员工）将终端电脑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

注：无论您使用的是 360 企业安全云哪个版本，客户端部署方式均相同。

1.3.1 windows 系统部署

模式一：外网部署模式

🚦 联网环境未安装个人版 360 安全卫士，管理员在【终端】-【终端部署】-【部署模式】-【外网部署（直连模式）】可通过 3 种方式进行部署：1、管理员可通过手动下载安装包在终端上安装；2、管理员将部署链接发送给员工自助安装部署，代理模式下该链接指向代理服务器，请确保员工可以访问；3、域控方式分发/安装，由管理员通过配置 AD 域环境的组策略或其他具有分发能力的方式将安装包分发到终端并执行自动静默安装。

(无论以哪种方式进行安装, 请勿修改安装包名称)



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。



模式二：内网部署（代理模式），

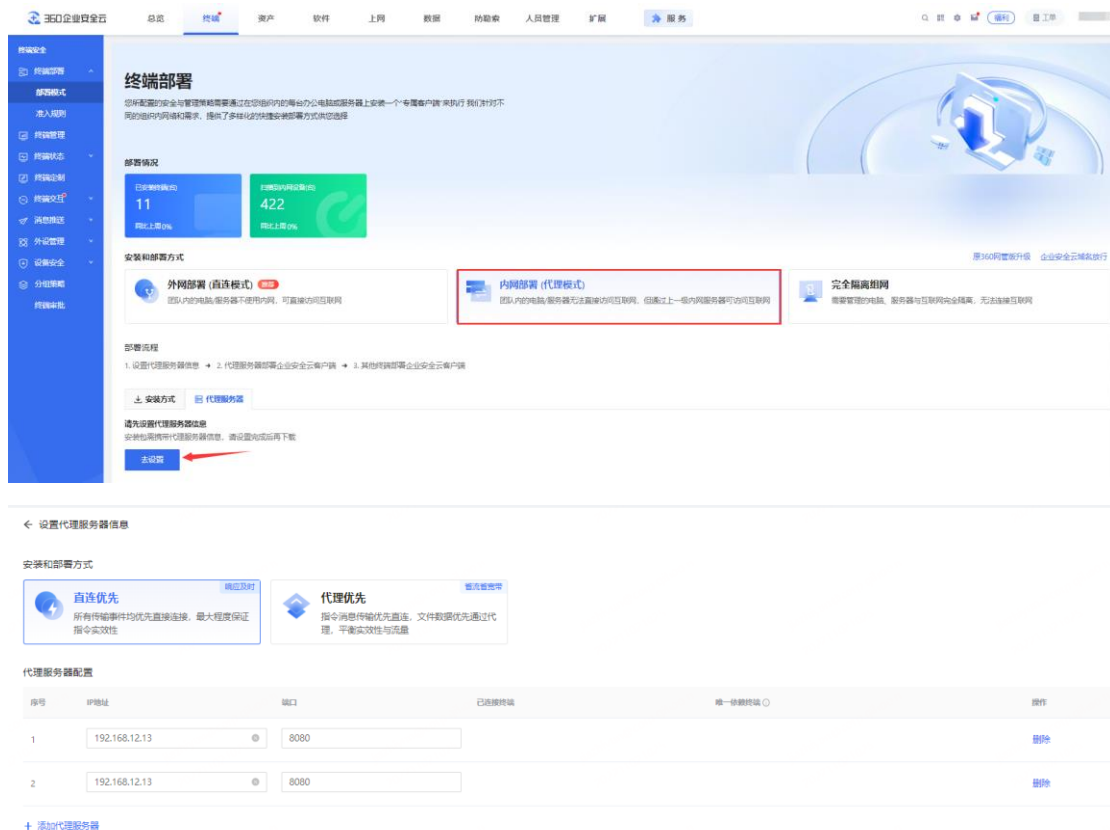
对于有防火墙或代理出口方式控制互联网访问的企业，360 企业安全云提供了简单便捷的

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】→【部署模式】-【内网部署（代理模式）】，设置内网代理服

务器



保存设置后，配置安装包信息，管理员需要先将安装包在代理服务器上安装，然后进行安装

包下发，1、管理员可通过手动下载安装包在终端上安装；2、管理员将部署链接发送给

员工自助安装部署，代理模式下该链接指向以上代理服务器，请确保员工可以访问；3、

域控方式分发/安装，由管理员通过配置 AD 域环境的组策略或其他具有分发能力的方式

将安装包分发到终端并执行自动静默安装。（无论以哪种方式进行安装，请勿修改安

装包名称）



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].exe 后再执行安装。

代理服务端安装后只提供 360 企业安全云功能相关的域名和 IP 代理，如病毒库升级、补丁包下载等，不可用于其他网站访问（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 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→部署模式→复制域名。



将企业安全云域名加白名单放行

X

如果您的网络出口支持针对特定域名加白放行，可以将企业安全云域名添加到您的网络出口白名单中，之后按照外网场景部署即可。

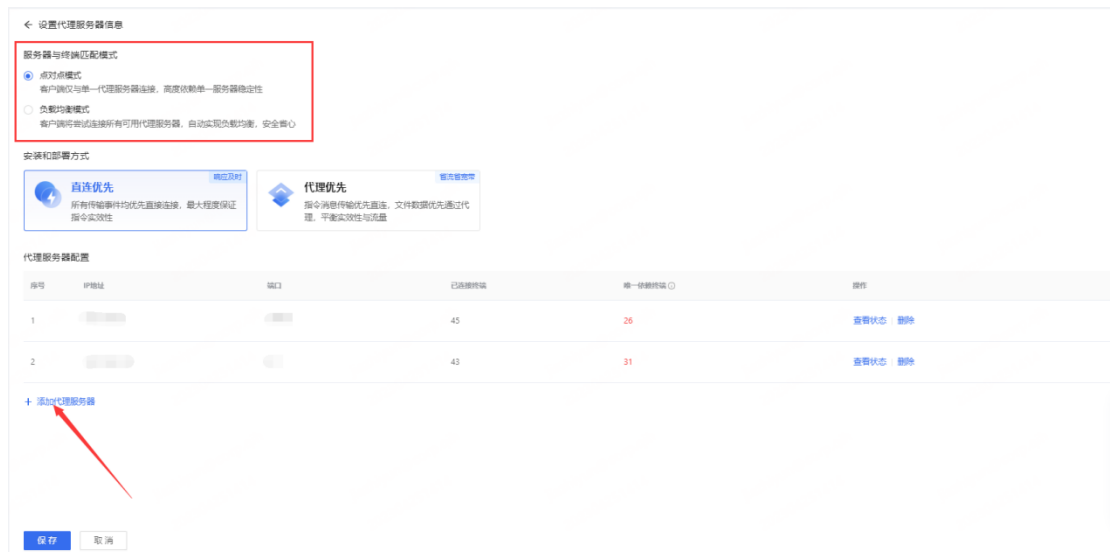
www.360.cn; admin.online.360.cn; api.online.360.cn; s.360.c...

请确保放行这些域名/IP的 80 和 443 端口，否则可能影响使用

取消

复制

同时需要说明的是，代理部署方式支持负载均衡模式，客户端可尝试连接所有可用代理服务器，自动实现负载均衡，安全省心。



温馨提示：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 /corp=1

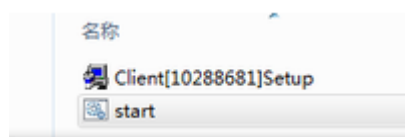
(2) 目标机器无管理员权限，需要在域控服务器里创建管理器权限的账户，并以命令行方式将账号密码传入安装包(部署完毕后可以删除此临时提权用的账号)，
示例：

\\192.168.28.132\X\Setup[T0HLWK].exe /USER=admin /PASSWORD=pass-**
/DOMAIN=test001.com /runas /S /corp=1

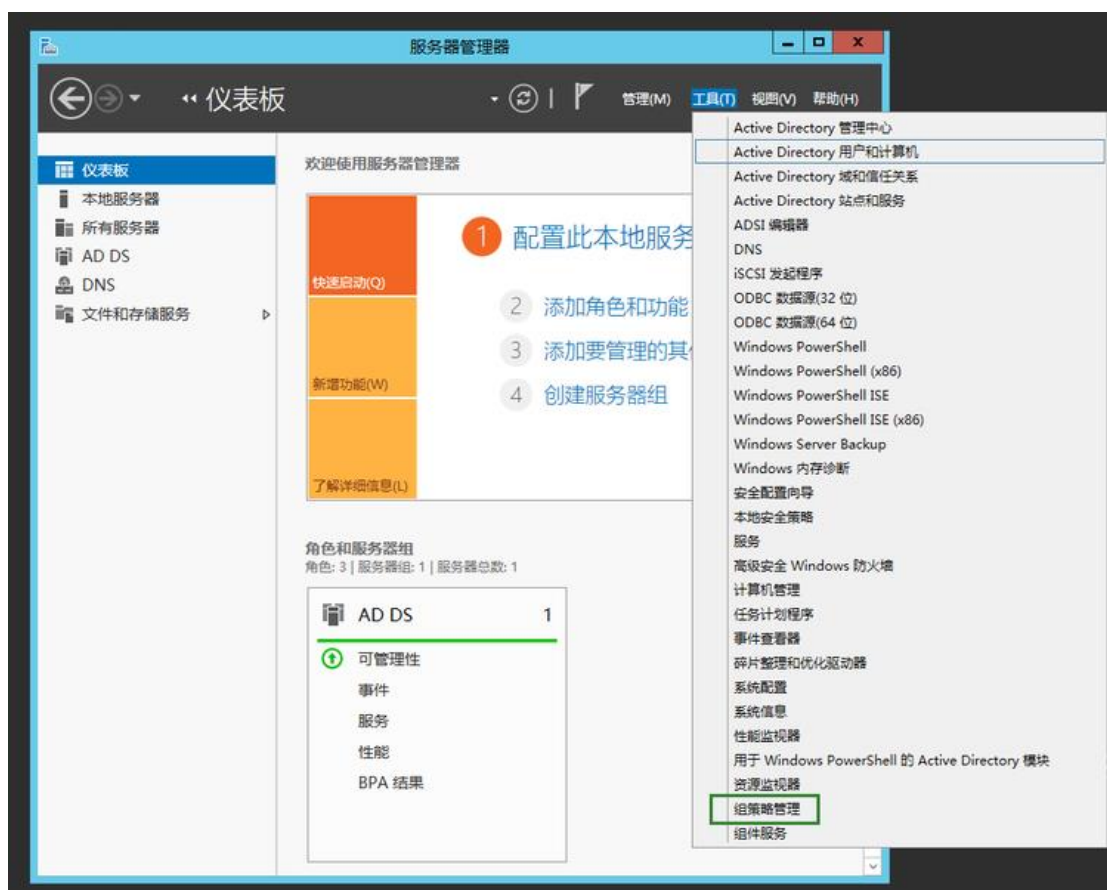
【说明：admin 请使用您创建的账号替换，pass-**请使用您设置的密码替换，
test001.com 替换为您的域】



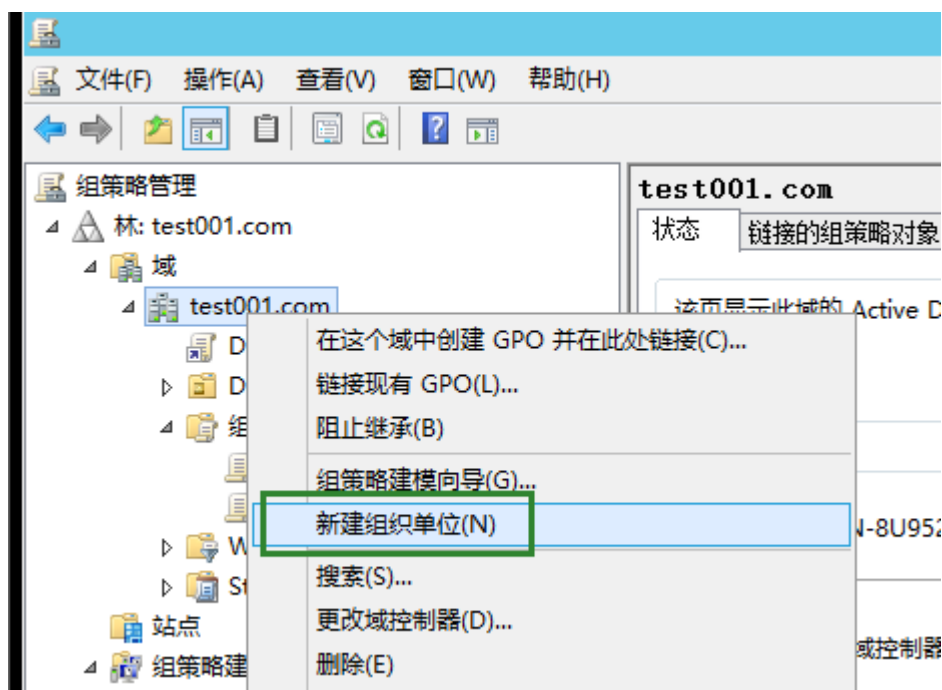
➤ 将脚本与安装包放到同一个共享目录下



➤ 进行域控下发：进入组策略管理页面

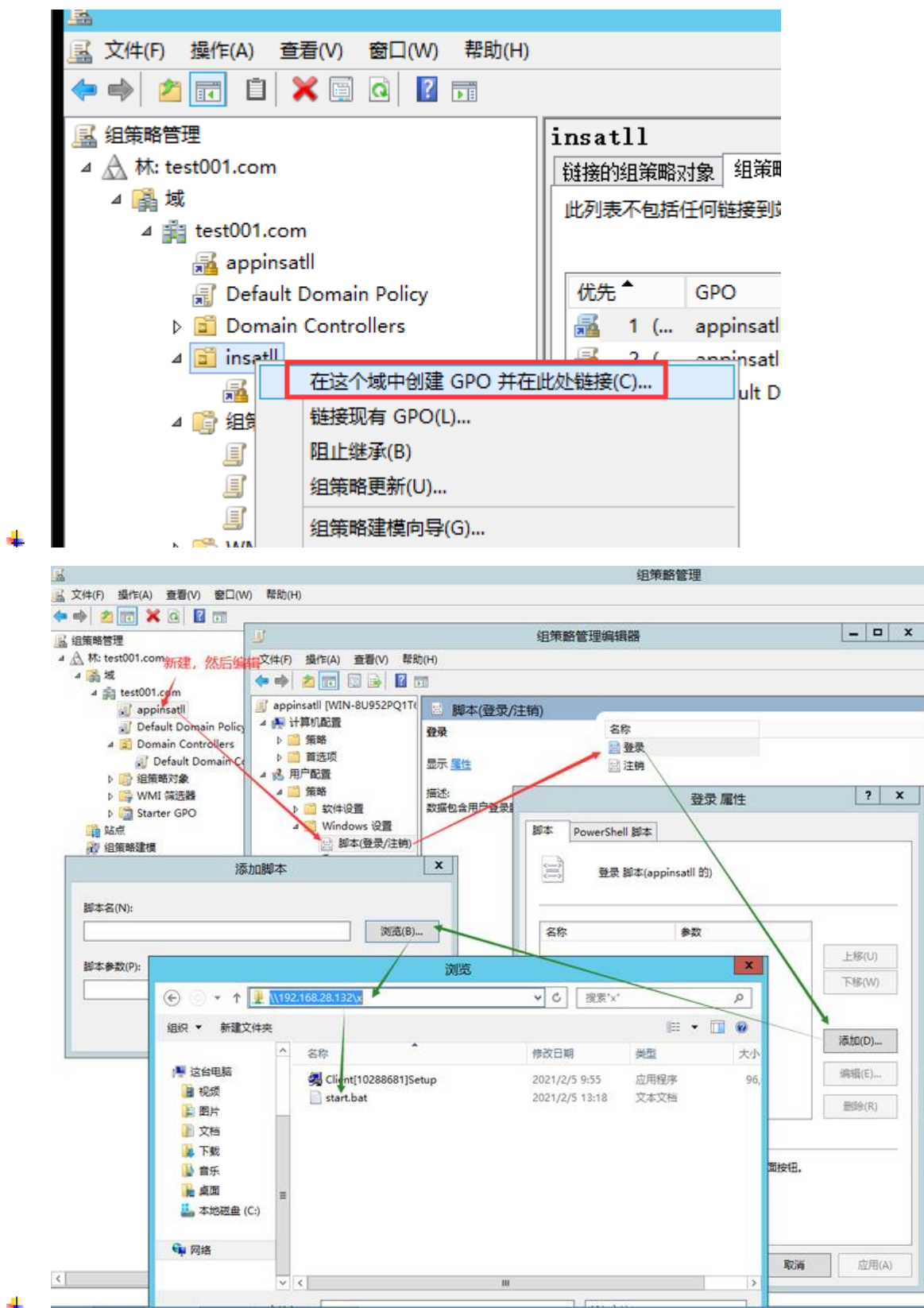


- 然后使用已有组织单元或者新建组织单元 (请注意查看里面涉及的机器是否是目标机器)

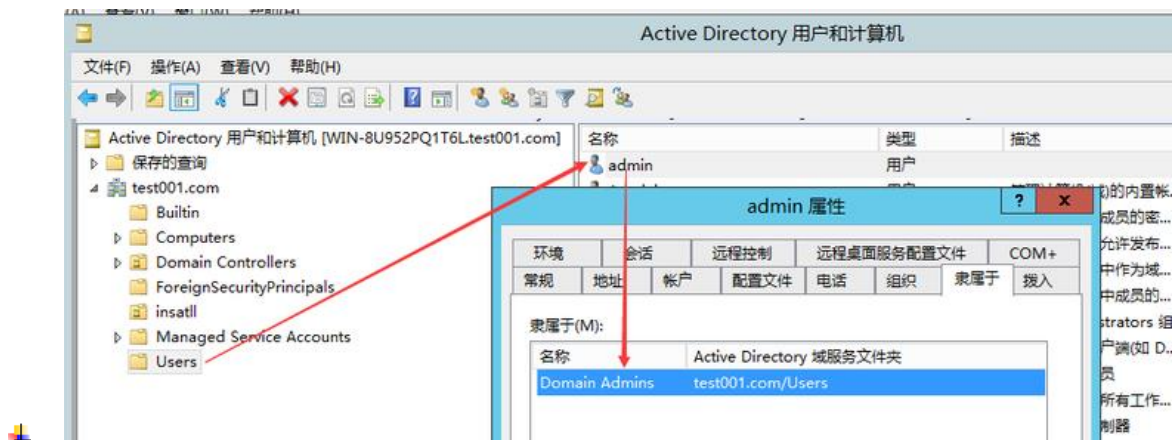


- 创建 GPO 并连接，然后编辑，如下图示，选择用户配置→策略→Windows 设置→脚

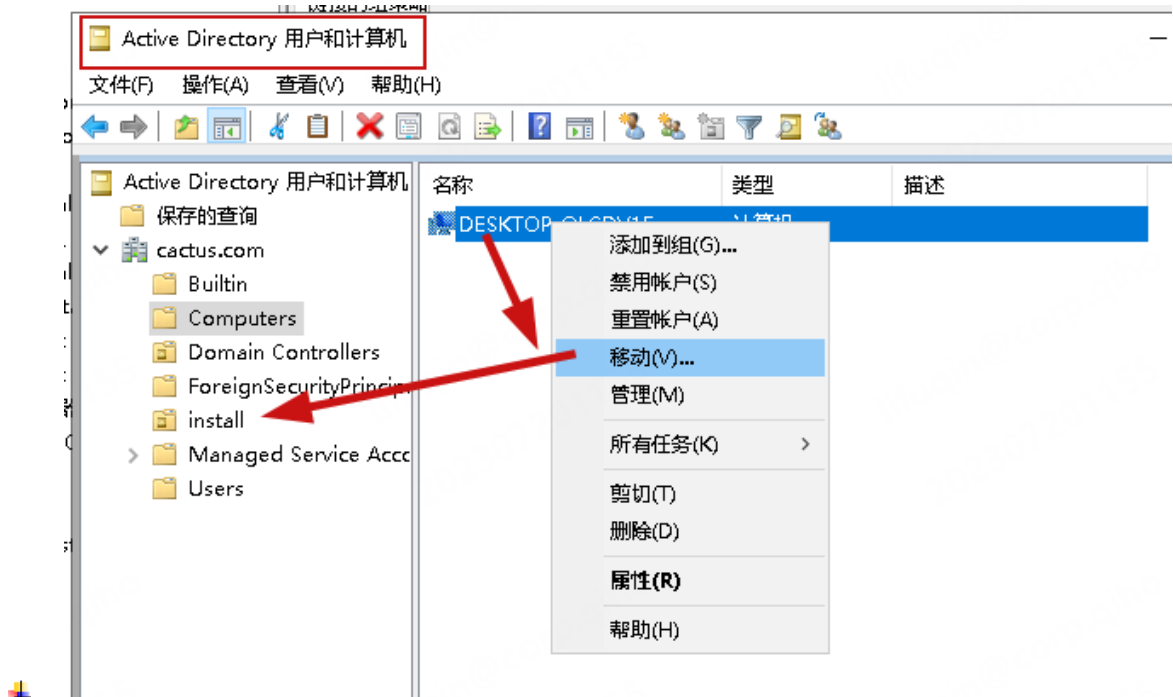
本→登录，将编辑好的在共享目录里的 start.bat 文件选入，（只能选入网络路径，切记不要选本地的！）



- 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)

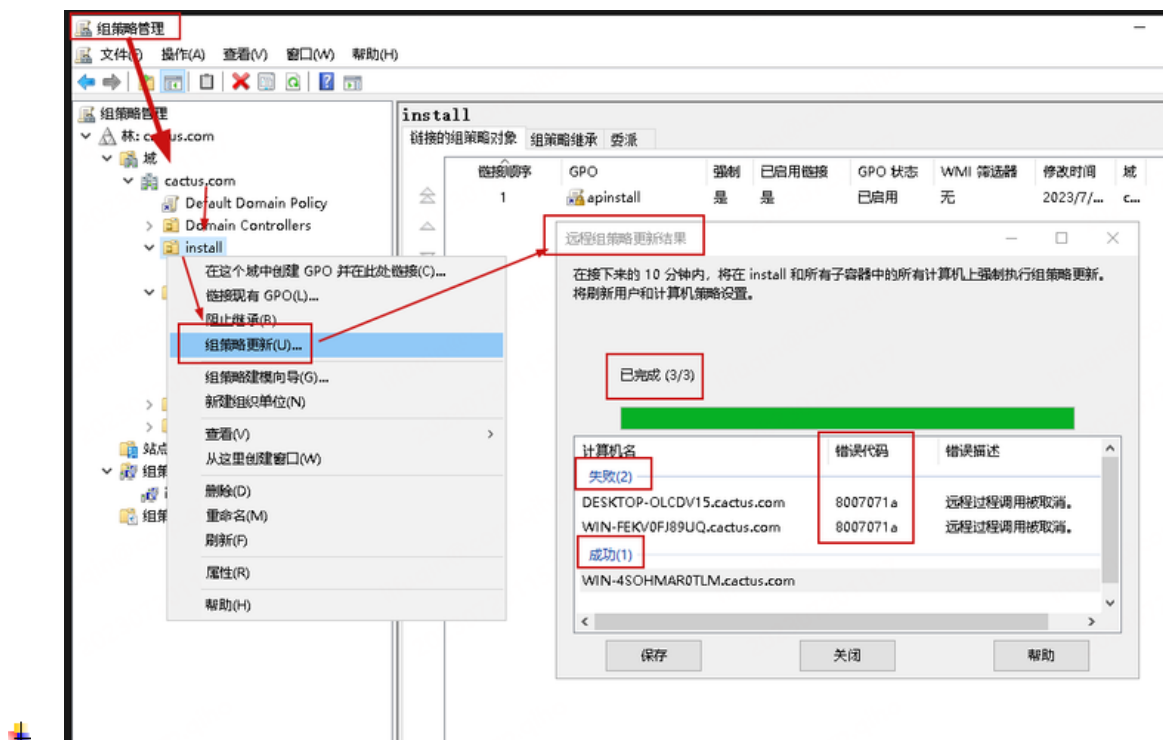


- 将要执行此策略的计算机及用户移动至组织单元

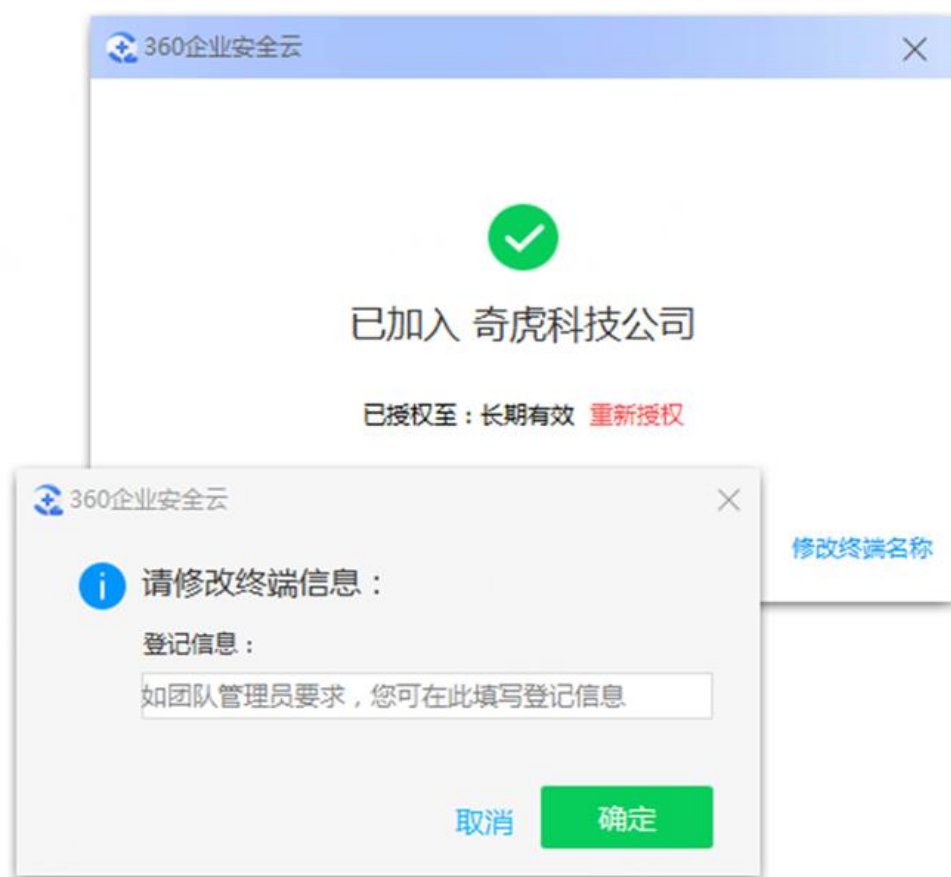


- 回到组策略管理执行组策略更新, 也可通过 cmd 下执行 `gpupdate /force` 来操作。
- 策略更新完提示组策略更新结果, 如图: 如果提示更新失败, 错误代码为 "8007071a" 则表示是终端上防火墙拦截了组策略更新, 管理员可设置组策略统一关闭防火墙, 也可

手动关闭防火墙；显示成功则表示组策略更新成功。



- 策略更新成功，目标机器重启后会执行企业安全云的静默安装，安装完会提示已加入企业组织并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

➤ 请先在控制台下载对应系统最新版的安装包。

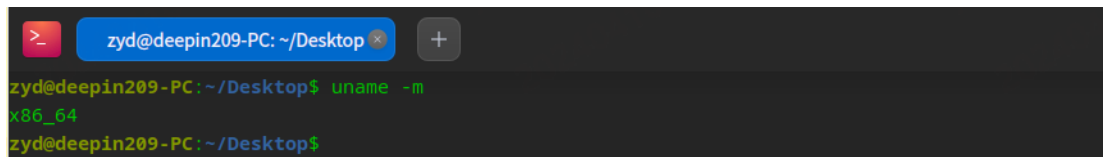


注：终端系统架构判断：

国产/信创系统，在桌面任意位置点击鼠标右键，选择在终端中打开，输入命令 `uname -m`

可查看系统架构。

如下图以统信 UOS 系统为例，结果显示 x86_64 即是 amd64 架构，则对应下载 UOSV20 桌面版-amd64 安装包。



```
zyd@deepin209-PC: ~/Desktop
zyd@deepin209-PC: ~/Desktop$ uname -m
x86_64
zyd@deepin209-PC: ~/Desktop$
```

如下图若结果显示 loongarch64 即是 loongarch64 架构，则对应下载 UOSV20 桌面版-loongarch64 安装包。



```
test@uos-loongarch-test: ~/Desktop
test@uos-loongarch-test: ~/Desktop$ uname -m
loongarch64
test@uos-loongarch-test: ~/Desktop$
```

- 下载完成后，可以看到安装包名称和您团队 PIN 码相关，请勿修改安装包名称，将安装包分发给终端用户安装即可。

注意：

1. 下载的 安装包 名称 格式 是 Team{*****}.deb(或 Team{*****}.run 或 Team{*****}.rpm)，切勿修改安装包名称，否则会导致加入团队失败。
2. Linux 及信创版本暂不支持代理部署模式。

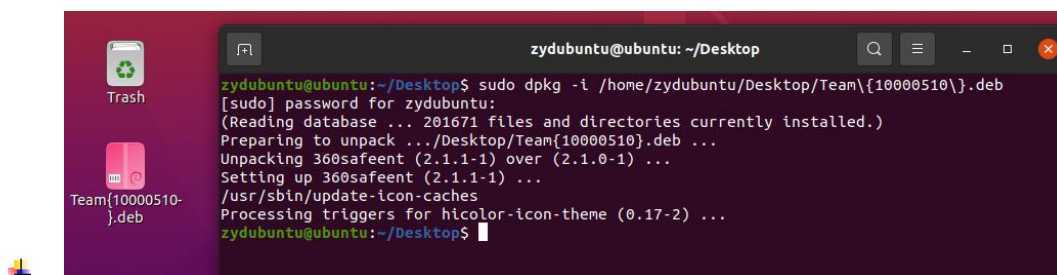
- deb 格式包安装

🌈 安装方式：

统信 UOS 桌面版、银河麒麟桌面版、中科方德 5、deepin20 支持界面双击安装包进行安装。

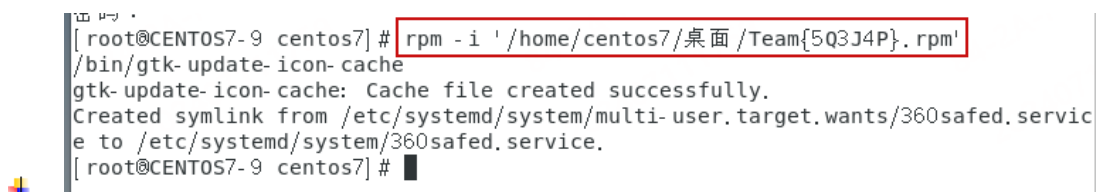
🌈 命令安装：

🌈 所有系统均支持通过命令安装：sudo dpkg -i 文件完整路径



➤ rpm 格式包安装

可通过命令安装：`sudo rpm -i 文件完整路径`

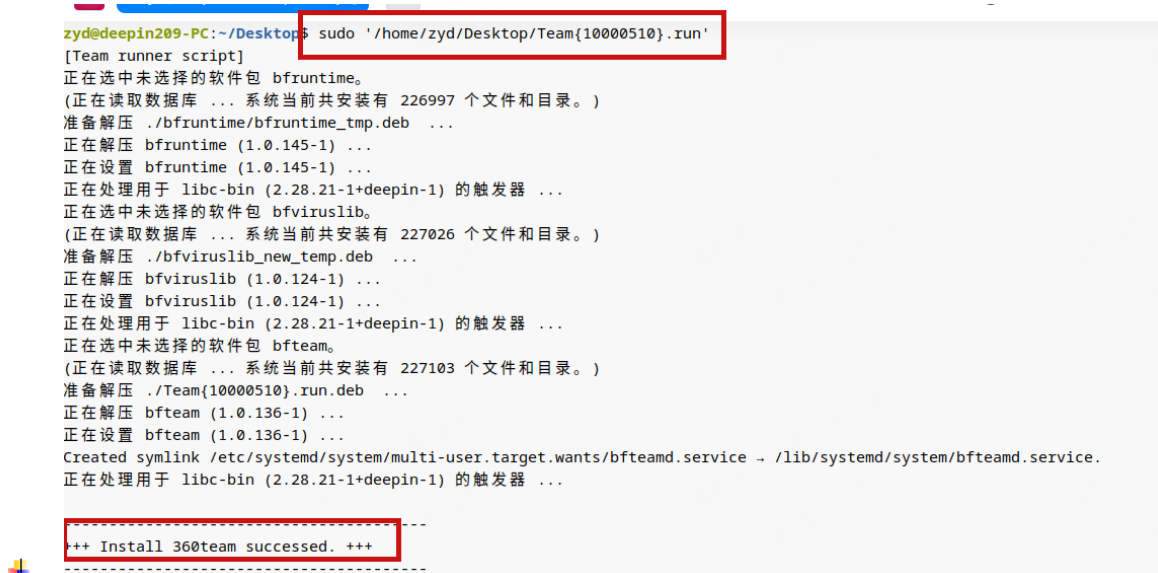


安装后可以通过命令 `ps -ef | grep 360safeent` 查看是否有 360 相关进程，有进程则表示

软件正常运行中。

➤ run 格式包安装

执行命令 `sudo chmod +x 安装包完整路径`，安装成功如下图所示



安装后可通过命令 `ps -ef | grep bfteam` 查看是否有 360 相关进程，有 bfteamd 进

程则表示件正常运行中。

➤ 安装成功后即可在管理后台查看终端信息并对终端下发管理策略。



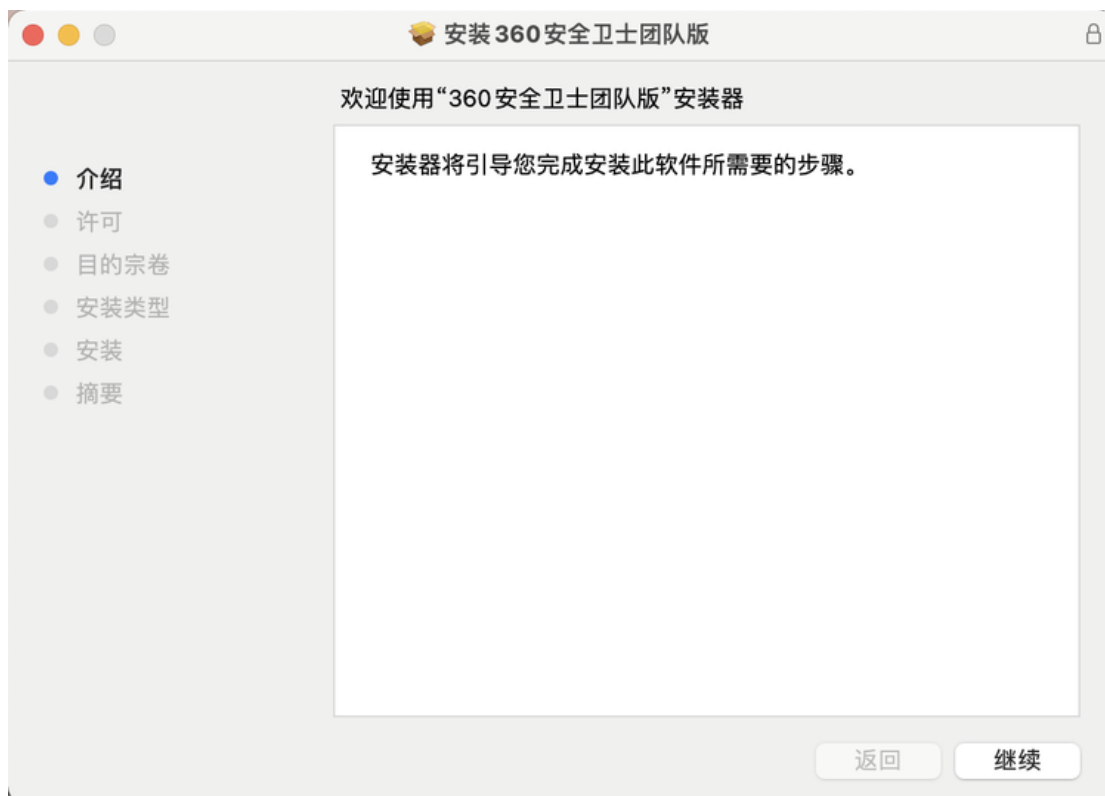
1.3.3 macOS 系统部署

- 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

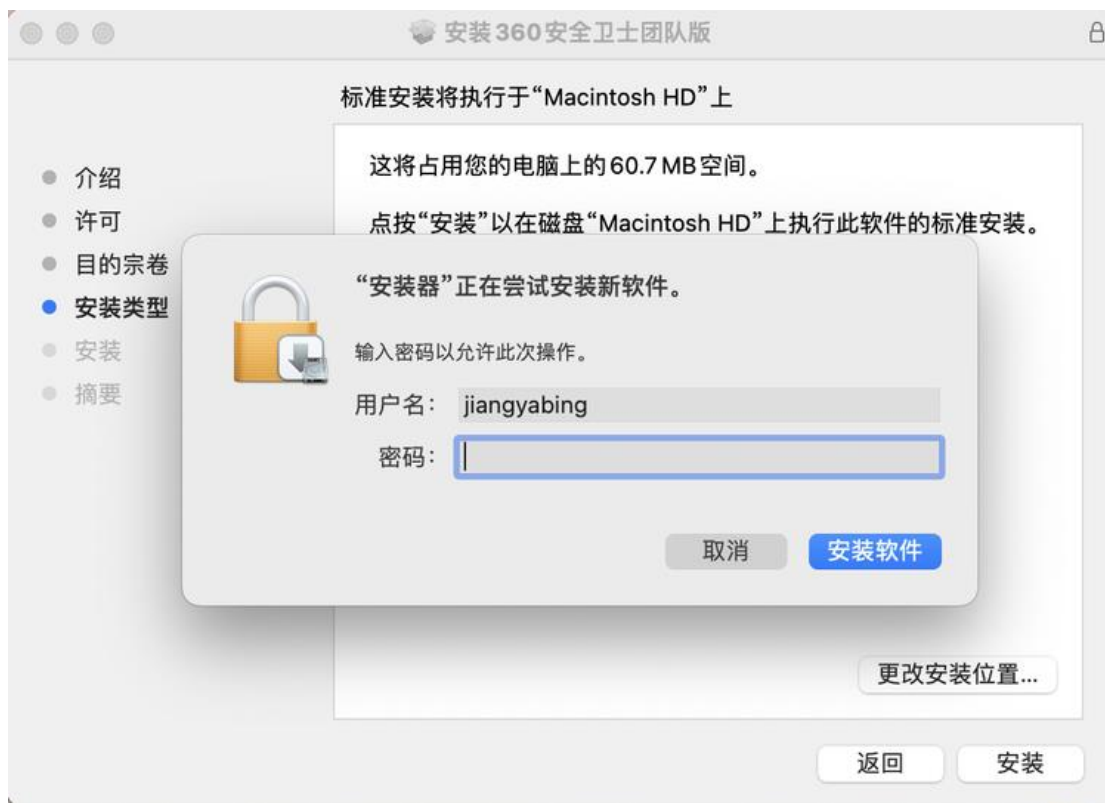
安装向导点击“继续”。



点击“安装”“继续”按钮



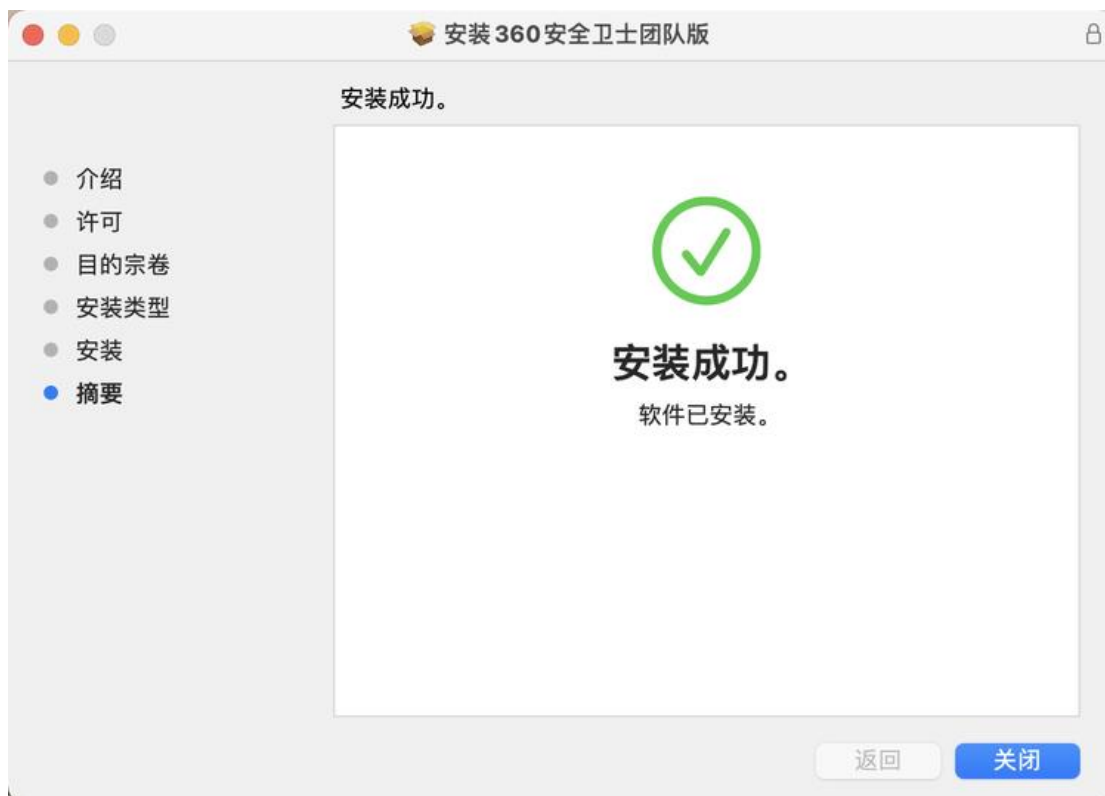
点击“安装”，弹出用户密码框，输入密码，点击“安装软件”按钮



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【终端】-【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

临时退出企业组织

已加入企业组织的终端，如果想在本地退出客户端，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。

想工作免打扰或玩游戏，可尝试以下模式

- ☒ **暂时退出** 1小时 ▾
在此期间内您的电脑将不受保护
- ☐ **游戏模式**
玩游戏时，自动处理风险，不再弹窗（仅本次有效）
- ☐ **免打扰模式**
处理风险，减少弹窗打扰，兼顾安全和娱乐（仅本次有效）
- ☐ **退出企业安全云**
退出企业安全云，停止对电脑保护

[添加误报软件](#)

取消

确定



完全退出企业组织

完全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组织



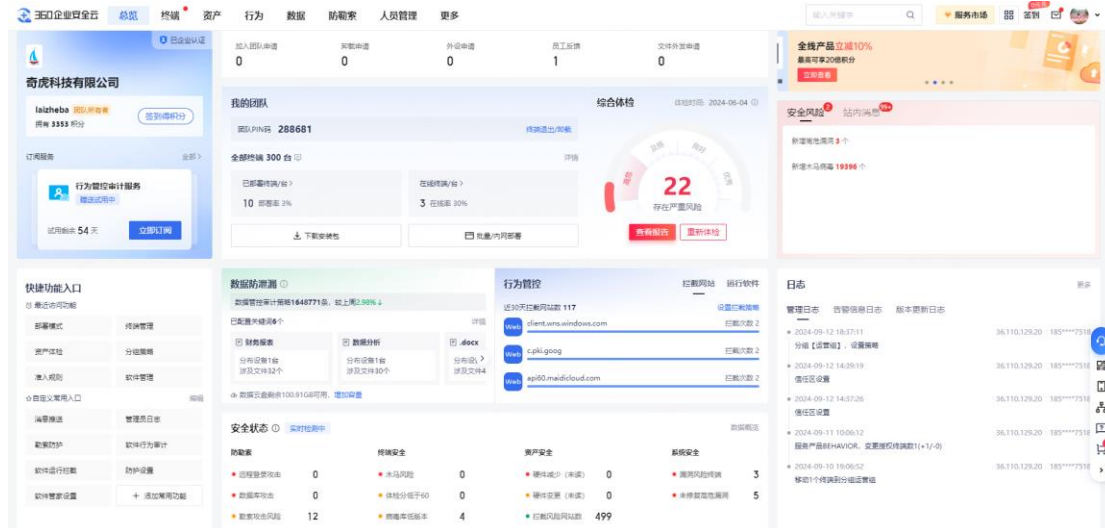
方式二，联系管理员，在管理后台【终端】-【终端管理】中进行删除，（需要注意的是，这种方式删除终端之后，该终端的数据将不能恢复，请谨慎操作）。



2、管理后台功能简介

2.1 总览

一站式、全方位的安全管理运维服务。直观展示了企业团队全网终端的状态，包括：终端数量和状态统计、安全状态、管理日志、PIN 码与团队密码、常用功能等，便于管理员全面了解当前企业团队内终端的整体情况。



2.2 终端

2.2.1 终端部署

2.2.1.1 部署模式

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，此页面给予用户明确的部署方案。

模式一：外网部署（直连模式）

管理员在【终端】-【终端部署】-【部署模式】-【外网部署（直连模式）】可通过 3 种方式进行部署：1、管理员可通过手动下载安装包在终端上安装；2、管理员将部署链接发送给员工自助安装部署，代理模式下该链接指向代理服务器，请确保员工可以访问；3、域控方式分发/安装，由管理员通过配置 AD 域环境的组策略或其他具有分发能力的方式将安装包分发到终端并执行自动静默安装。（无论以哪种方式进行安装，请勿修改安装包名称）



模式二：内网部署（代理模式），

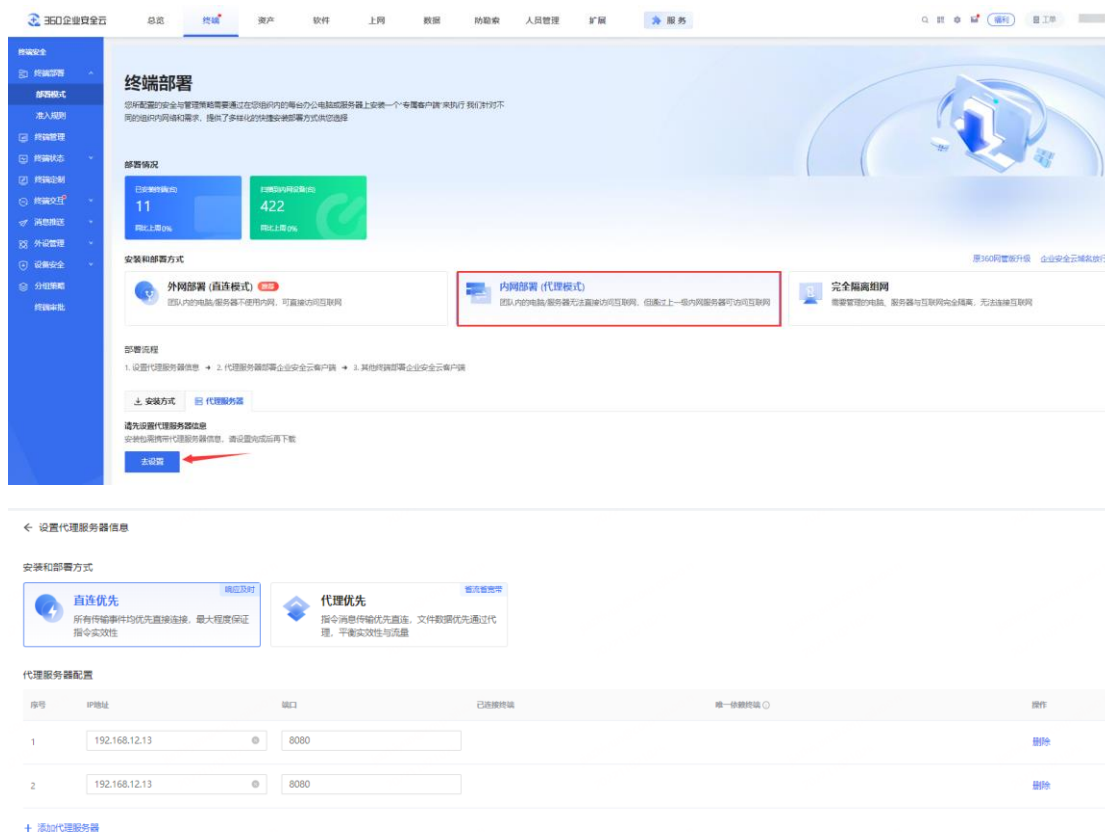
对于有防火墙或代理出口方式控制互联网访问的企业，360 企业安全云提供了简单便捷的

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】→【部署模式】-【内网部署（代理模式）】，设置内网代理服

务器



保存设置后，配置安装包信息，管理员需要先将安装包在代理服务器上安装，然后进行安装

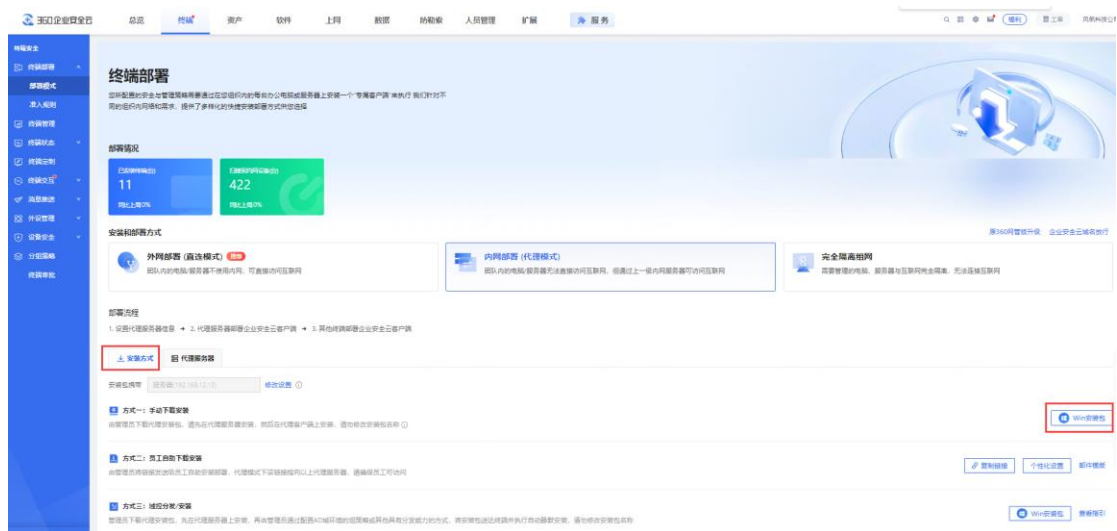
包下发，1、管理员可通过手动下载安装包在终端上安装；2、管理员将部署链接发送给

员工自助安装部署，代理模式下该链接指向以上代理服务器，请确保员工可以访问；3、

域控方式分发/安装，由管理员通过配置 AD 域环境的组策略或其他具有分发能力的方式

将安装包分发到终端并执行自动静默安装。（无论以哪种方式进行安装，请勿修改安

装包名称）



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 企业安全云功能相关的域名和 IP 代理，如病毒库升级、补丁包下载等，不可用于其他网站访问（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 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→部署模式→复制域名。



将企业安全云域名加白名单放行



如果您的网络出口支持针对特定域名加白放行，可以将企业安全云域名添加到您的网络出口白名单中，之后按照外网场景部署即可。

www.360.cn; admin.online.360.cn; api.online.360.cn; s.360.c...

请确保放行这些域名/IP的 80 和 443 端口，否则可能影响使用

取消

复制

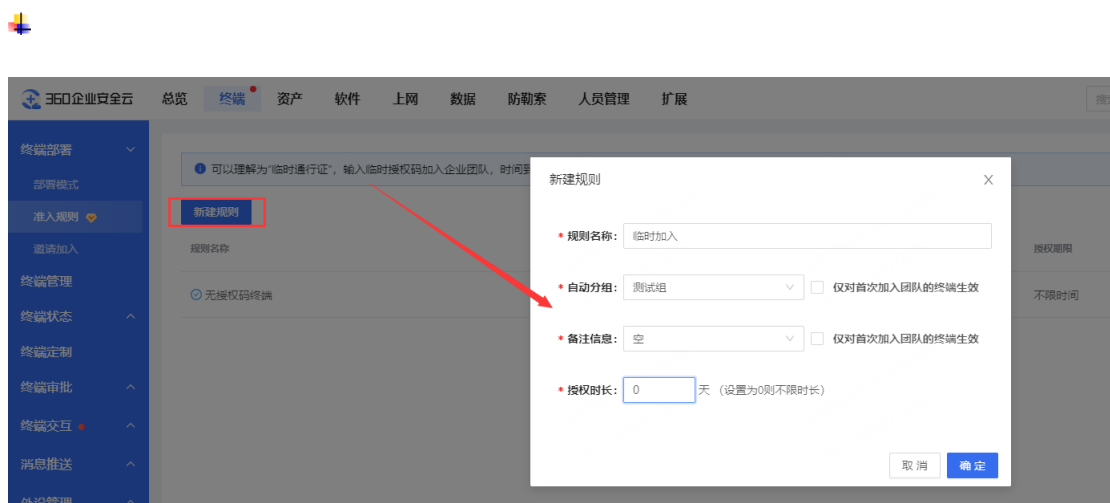
2.2.1.2 准入规则（专业安全管理运维服务）

准入规则设置，可以理解为“临时通行证”，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。

无授权码规则，关闭后，已经安装个人版安全卫士的终端用户将不能通过输入 PIN 码的方式加入团队，开启则可以通过输入 PIN 码的方式加入团队内，可有效防止非团队内的终端误加入占用名额。



新建规则，可以自定义加入团队的规则，比如设置加入团队后分配到某个分组，也可以设置加入团队的时间，授权时间到期会自动退出团队，方便管理临时加入团队的成员。



2.2.1.3 邀请加入

可以邀请网内其他终端用户加入团队，发送邀请即可。



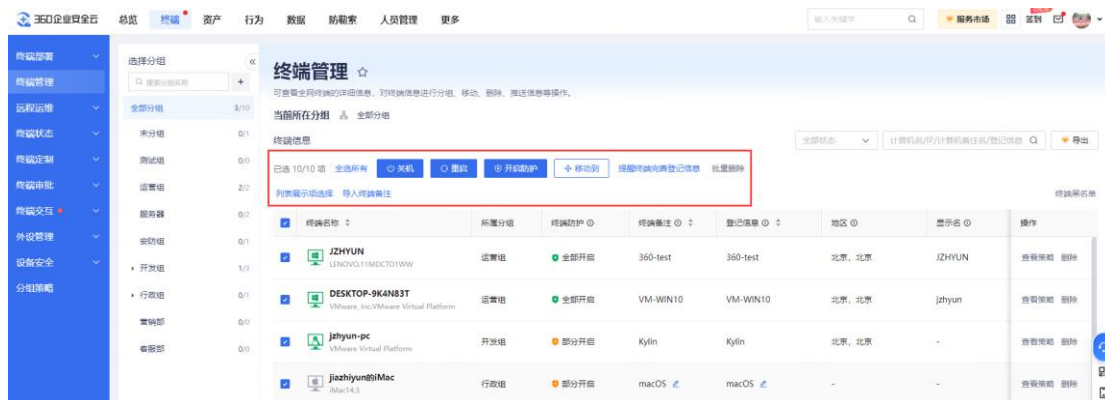
2.2.2 终端管理

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。



如果某台终端需要临时退出团队，管理员可以直接在这里操作删除，终端即可退出团队，回

到个人版安全卫士。



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。

终端信息

已选 1/10 项 全选所有 🔌 关机 🔄 重启 🛡️ 开启防护 ➕ 移动到 提醒终端完善登记信息 批量删除

列表展示项选择 导入终端备注

☐	终端名称	所属分组	终端防护	终端备注	登记信息
☒	JZHYUN LENOVO.11MDCT01WW	运营组	全部开启	360-test	360-test

提醒终端完善登记信息

① 点击发送后对应终端会收到右下方的推送消息，点击消息的确认按钮后，即可在后续的弹窗中修改/添加对应终端的登记信息

格式要求 BJ-部门-姓名

有效时间 7 天 有效时间过后将停止推送

完善登录信息

您的设备登记信息还不完整，请及时补充完善
登记信息格式为：BJ-部门-姓名

确定

取消 发送

2.2.3 远程运维（专业安全管理运维服务）

2.2.3.1 远程控制

🔧 远程控制（需进行管理员实名认证和企业认证）

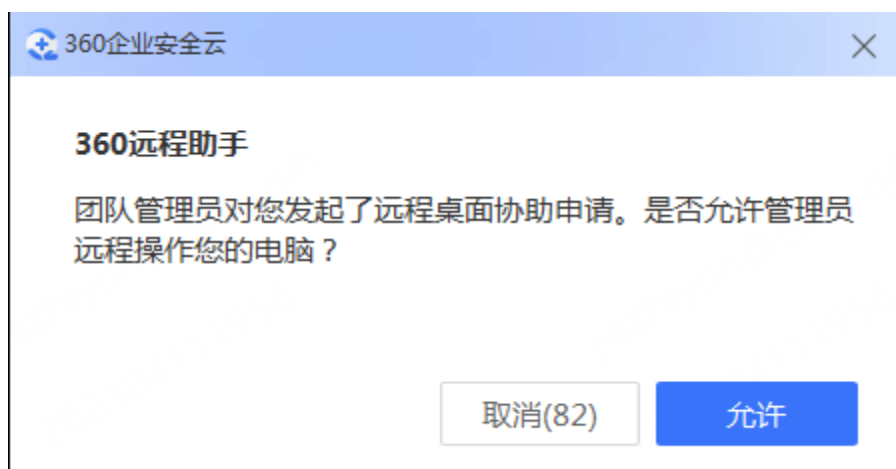
通过管理后台【远程控制】页面发起远程请求，主控端需要安装 360 企业安全云客户端。



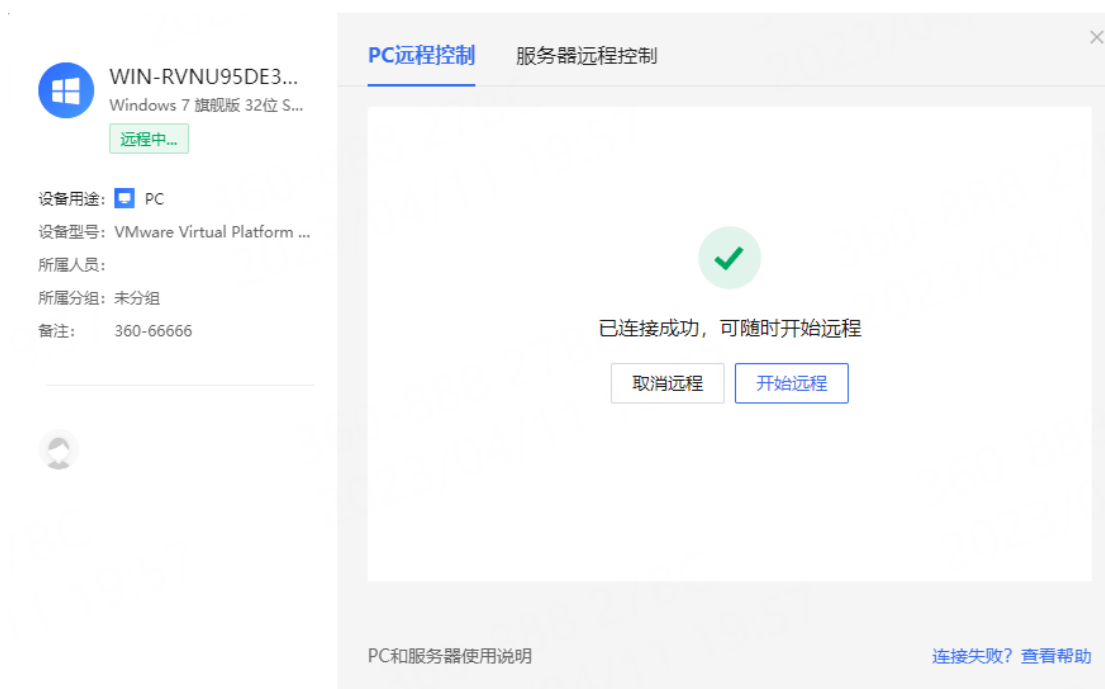
远程控制分为普通 PC 远程控制和无人值守远程控制



普通 PC 远程控制的两个通道发起远程后均需要终端用户点击【允许】，管理员才可以远程连接成功。



无人值守远程控制发起后无需终端用户允许，连通后即可开始远程。



无人值守远程控制支持文件传输、远程 CMD、观看模式，可满足不同管理需求。



服务器远程控制

服务器远程控制使用方法与 PC 远程控制相同，目前只支持 windows server 系统。

2.2.3.2 消息推送

设置向终端推送定时和即时消息的策略，有效期过后终端将不再接收消息。



定时消息策略

用于创建全组或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。支持创建多条定时推送策略。

360企业安全云 总览 终端 资产 软件 上网 数据 防勒索 人员管理 更多

终端部署 终端管理 远程运维 远程控制 消息推送 终端状态 终端定制 终端审批 终端交互 外设管理 设备安全 分组策略

定时消息推送策略

*消息推送对象
全部分组 x

*消息标题
管理员提醒您: 7/50

*消息内容
请各位同事下班记得关机。 12/200

推送URL 终端用户可直接从推送弹窗打开该链接
请输入推送URL, 不超过50个汉字 0/50

*策略有效期至 仅在该时段内执行推送策略
2024-02-29 19:00:00 日

*策略执行时间
☐ 开机推送
☒ 周期推送 推送有效时间默认1小时, 仅该时段在线终端可收到推送
每天
17:30 发布后 - 1 + 小时内推送

保存策略 取消

定时消息-推送效果预览
360企业安全云
管理员提醒您:
请各位同事下班记得关机。
确定

即时消息策略

可创建全组或分组或单台终端的即时推送通知,管理员可根据通知需求进行内容编辑和时间设置。

360企业安全云 总览 终端 资产 软件 上网 数据 防勒索 人员管理 更多

终端部署 终端管理 远程运维 远程控制 消息推送 终端状态 终端定制 终端审批 终端交互 外设管理 设备安全 分组策略

即时消息推送策略

*消息推送对象
DESKTOP-2F1A1UG x yunyun-PC x WIN-RR19T9SN85D x localhost.localdomain x

*消息标题
管理员提醒您: 7/50

*消息内容
请各位同事下班记得关机。 12/200

推送URL 终端用户可直接从推送弹窗打开该链接
请输入推送URL, 不超过50个汉字 0/50

*推送持续时间 该时间内在线终端才会收到消息
发布后 - 1 + 小时内推送

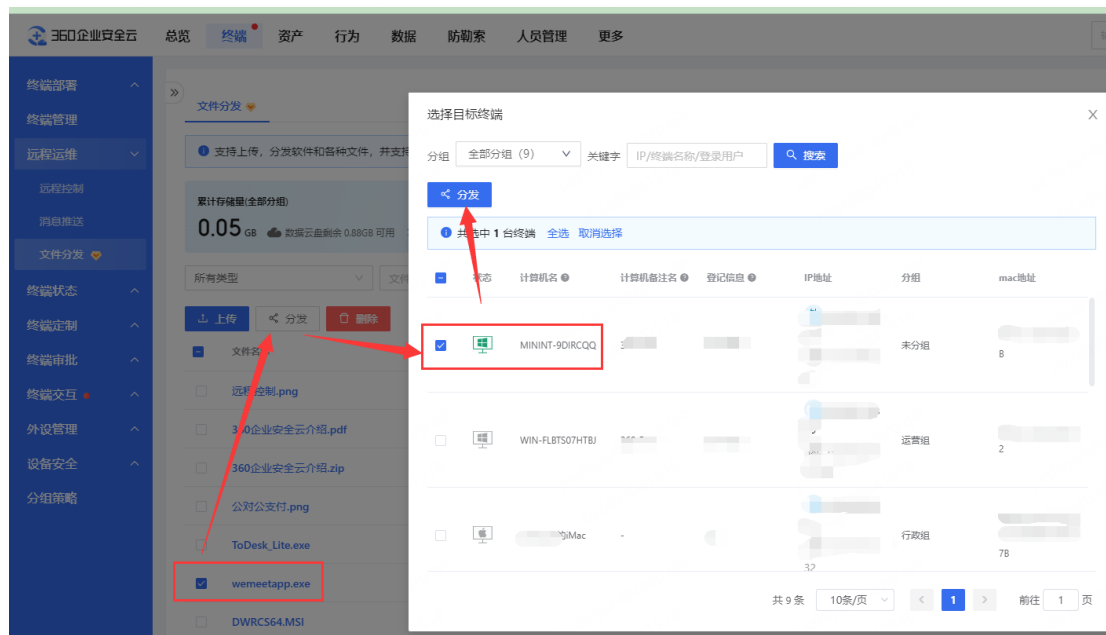
立即推送 取消

定时消息-推送效果预览
360企业安全云
管理员提醒您:
请各位同事下班记得关机。
确定

2.2.3.3 文件分发

(需进行管理员实名认证和企业认证)

文件分发是先将文件上传到云服务器，然后通过云服务器进行分发，可以分发文件或者一些软件安装包（单个文件均不超过 350M）。



如果下发的是程序安装包，可以设置在终端执行

分发对象

时间 ☒ 立即 ☐ 指定时间存放位置 桌面 ☐ 替换同名文件执行方式 ☒ 接收后运行 ☐ 只接收☐ 分发失败 20 分钟后再次执行分发☐ 终端资源占用率不高于70%时执行☐ 终端重启时安装

运行参数 (配置软件运行参数, 可以使软件有各种不同的展现形式, 如使软件静默运行)

360uppb.exe

运行参数

添加

文件名称

运行参数

操作

暂无数据

终端提示 ☒ 运行时需要终端确认 ☐ 提示后自动运行 ☐ 不提示直接运行

亲爱的用户, 管理员正在进行分发任务, 请配合管理员完成相关文件阅读或者软件下载安装操作

0/50

有效时间 ☒ 一周 ☐ 指定时间

分发

取消

2.2.4 终端状态

2.2.4.1 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（专业安全管理运维服务），还有分组定时关机和定时重启

设置



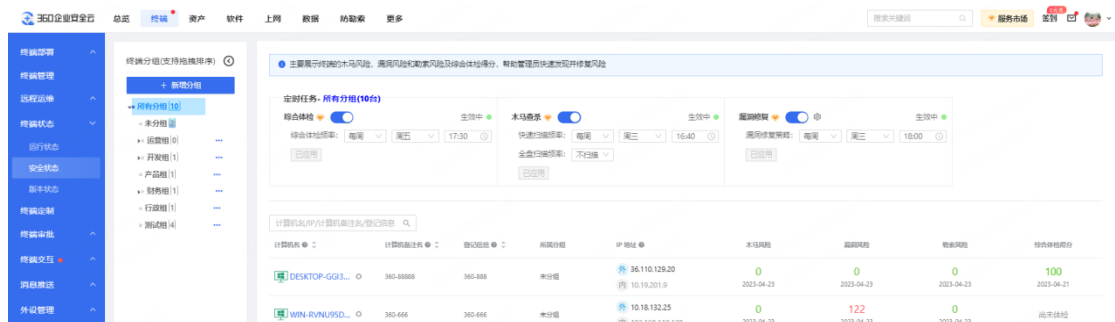
2.2.4.2 安全状态

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、定时木马查杀和定时漏洞修复的设置（专业安全管理运维服务）



2.2.4.3 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。



2.2.4.4 文件白名单

如文件在 360 企业安全云环境中被误拦可将误拦的文件加白，加白成功后可以正常使用。

加白方式有两种：

提交官方加白，省心省力

可提交误拦的文件样本到官方检测平台，处理完成后，360 查杀引擎在扫描时会将其跳过。支持查看提交记录及处理进度和结果。（本服务由 360 专家提供）



自定义加白，即时生效

对查杀文件的自定义设置，可以添加 MD5 白名单、目录白名单、文件白名单，请确保添加的是可信的 MD5/文件/目录，添加信任之后，查杀任务将不再扫描这些位置和文件。



2.2.5 终端定制

2.2.5.1 终端界面定制

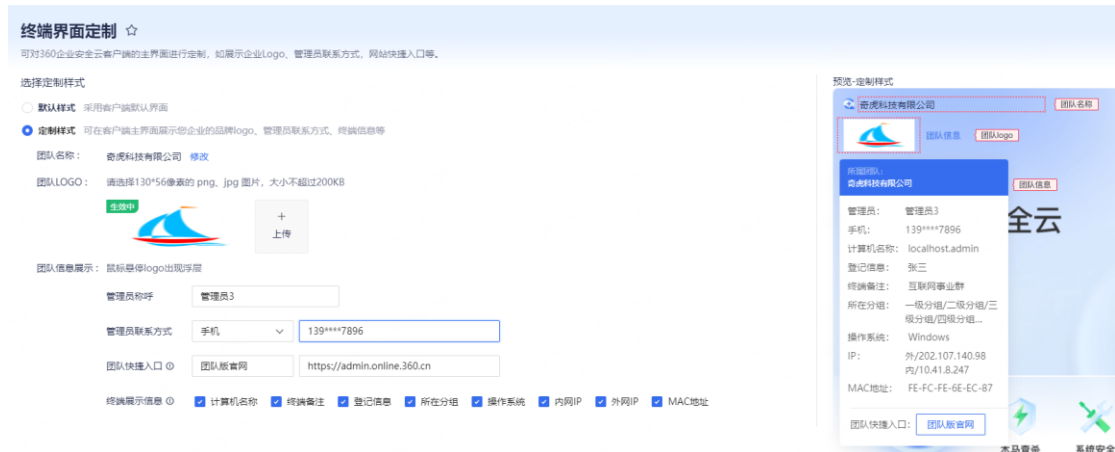
可对 360 企业安全云客户端的主界面进行定制，如展示企业 Logo、管理员联系方式，网站快捷入口等。

客户端默认界面，展示默认 logo



客户端定制界面

可在客户端主界面展示企业团队的品牌 logo、管理员联系方式、终端信息等。需要注意的是企业 logo 请按规定格式上传（请选择 130*56 像素的 png、jpg 图片，大小不超过 200KB）。



2.2.5.2 桌面壁纸定制（专业安全管理运维服务）

管理员可根据企业需求设置终端统一桌面壁纸，宣扬企业文化。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。



2.2.5.3 软件管家设置（专业安全管理运维服务）

可设置是否隐藏客户端上软件管家的入口及软件管家的桌面图标

策略设置



可设置软件管家界面左侧栏显示和隐藏的内容

软件管家栏目编辑

可编辑软件管家左侧栏目的显示情况，除软件分类、卸载、个人中心三个栏目不可编辑外，其余栏目均可设置显示或隐藏。

宝库

推荐 ☒ 含热门、游戏、必备、工具箱等软件分类 ☒ 默认开启

功能

升级 ☒卸载 ☒ 默认开启净化 ☒个人中心 ☐ 默认关闭

可设置开启捆绑软件拦截功能，防止自动安装捆绑软件占用电脑资源。

捆绑软件拦截 ☒ 已开启

开启后，自动强力阻止捆绑软件的安装，避免占用电脑资源。（捆绑软件是指安装一款软件时，会附带静默安装的软件。）

2.2.6 终端审批

2.2.6.1 团队审批

团队管理员可以对申请加入团队的终端进行审批，可通过、可拒绝。



2.2.6.2 卸载审批

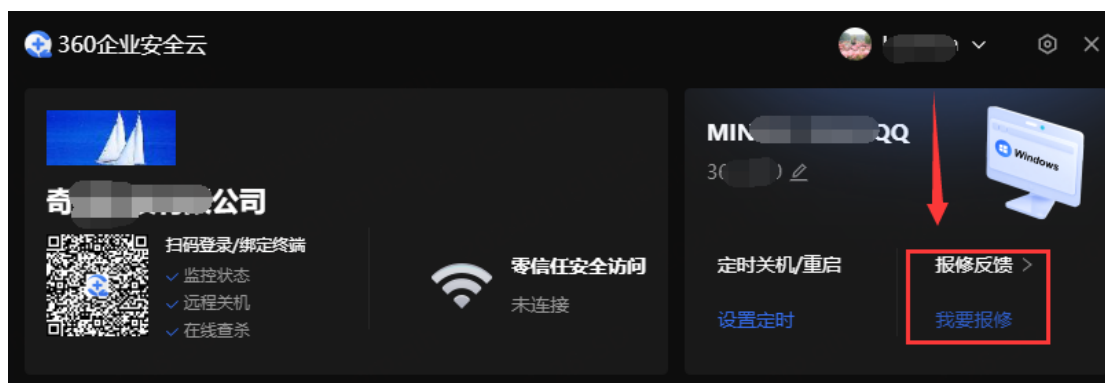
团队管理员可以对申请卸载的终端进行审批，可通过、可拒绝。



2.2.7 终端交互

2.2.7.1 反馈处理

终端用户可以通过客户端功能面板提交报修或者其他问题，管理员可以集中化处理终端用户的反馈，远程排查故障，也可选用专业工程师上门服务。



团队成员反馈处理

管理类可以集中化处理跨系统中的故障、处理部署故障，亦可选择专业工程师上门服务

导出工单信息

工单信息总结

今日工单数量
76
同比上周: 10%

工单分类统计

工单
24 / 24
待处理: 累计

行类型
5 / 5
待处理: 累计

人数量
17 / 17
待处理: 累计

非处理出数量
26
待处理: 累计

专业运维上门服务 360与生态伙伴旗下的专业安全与运维专家，为您提供运维支持或上门服务

选择专业服务 我的服务记录

工单详情

全部工单状态	全部优先级	全部优先级	搜索人员/内部工单号	进行中			
工单 W30220190530180000010	进行中	工单 W3022019430420000010	进行中	人事类 W3022019553018000010	进行中	人事类 W30220192512170000010	进行中

2.2.7.2 小程序功能

管理员可在此设置终端功能面板上的功能是否可以开启使用，终端用户如果绑定了微信小程序

序，小程序上的功能是否可用也会受此管控。



同时管理员绑定小程序之后，可以在手机上进行部分管控操作，如报修反馈管理、定时消息推送、小程序功能管控等。



2.2.8 外设管理

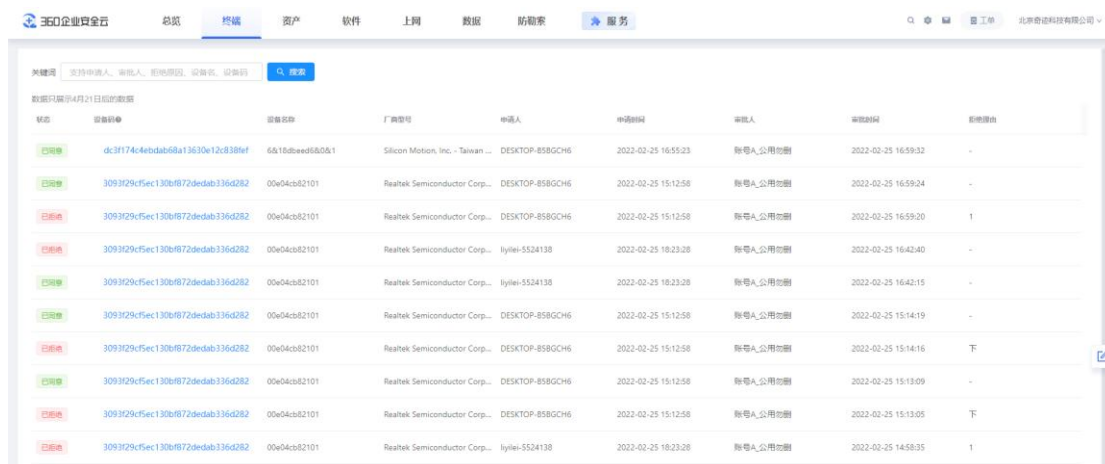
2.2.8.1 外设申请（专业安全管理运维服务）

在【外设申请】中，可以处理终端用户提交使用 U 盘和网卡的申请（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【外设管理】-【外设禁用】和【USB 网卡禁用】

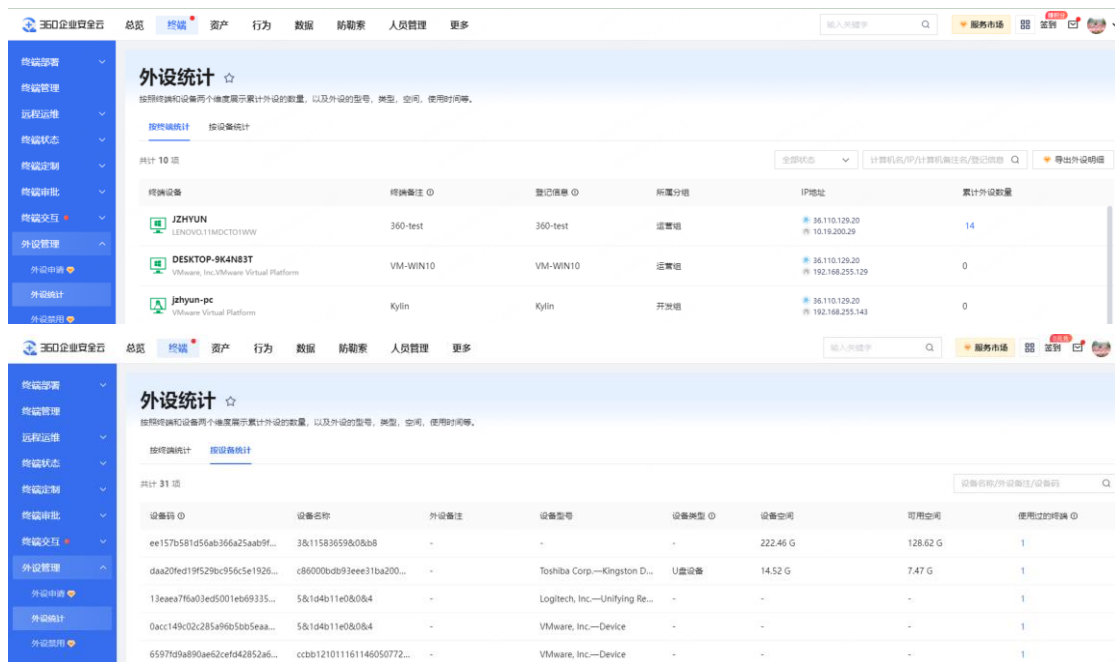


审批记录中可查看处理外设申请的记录，支持申请人、审批人、设备名、设备码、拒绝原因搜索。



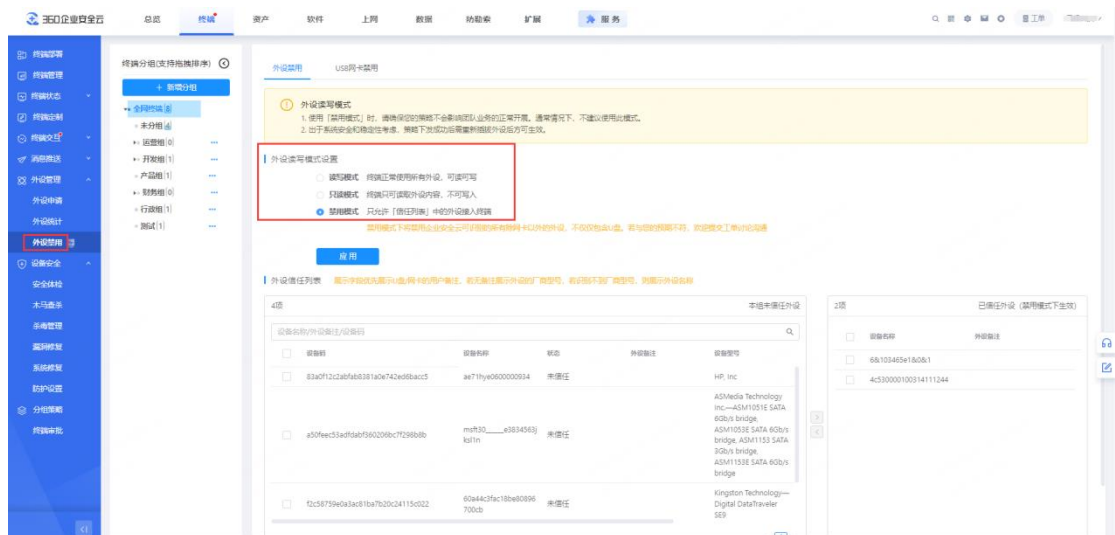
2.2.8.2 外设统计

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。支持导出外设明细（专业安全管理运维服务）。



2.2.8.3 外设禁用（专业安全管理运维服务）

管理员可设置全网终端或分组终端外设的读写模式，和 USB 网卡的启用/禁用模式，并可添加外设的信任列表。

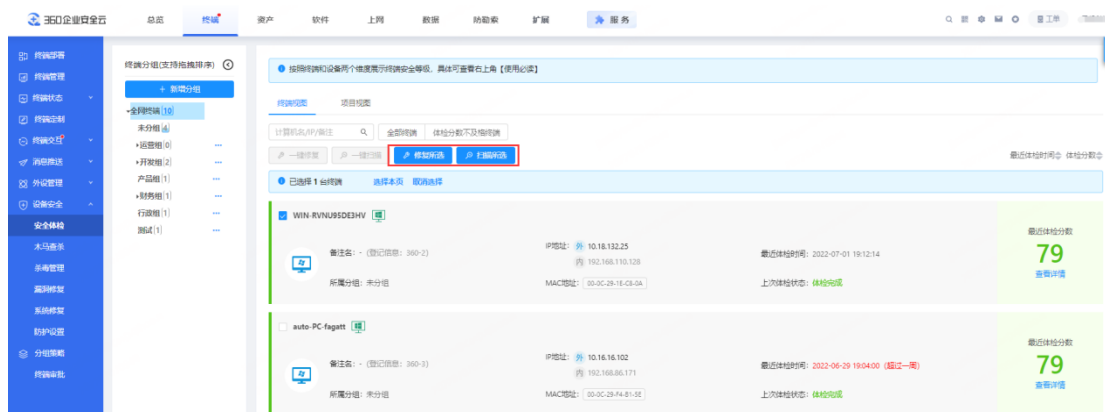




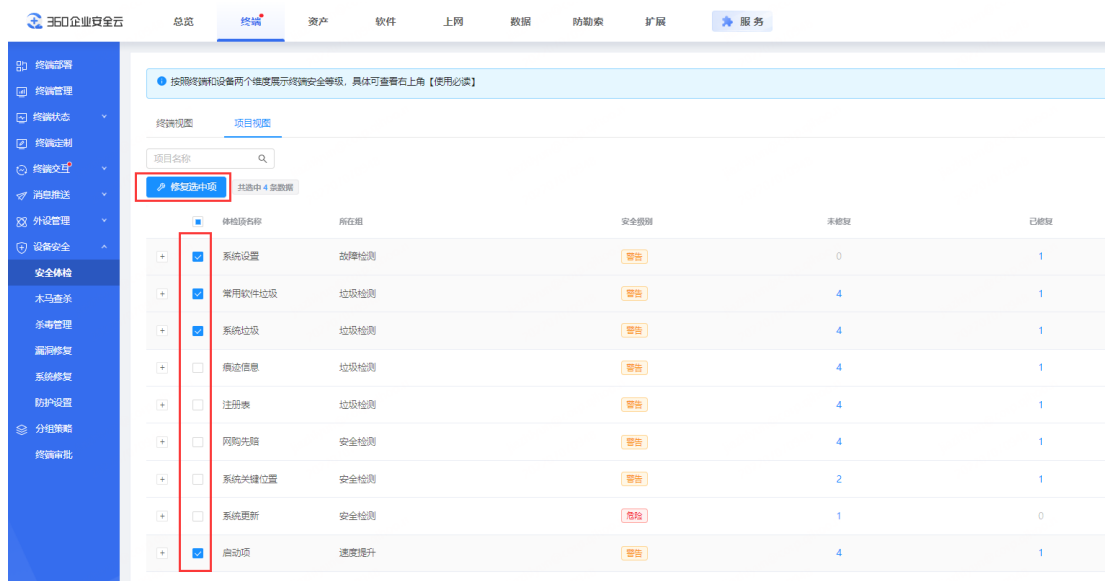
2.2.9 设备安全

2.2.9.1 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。

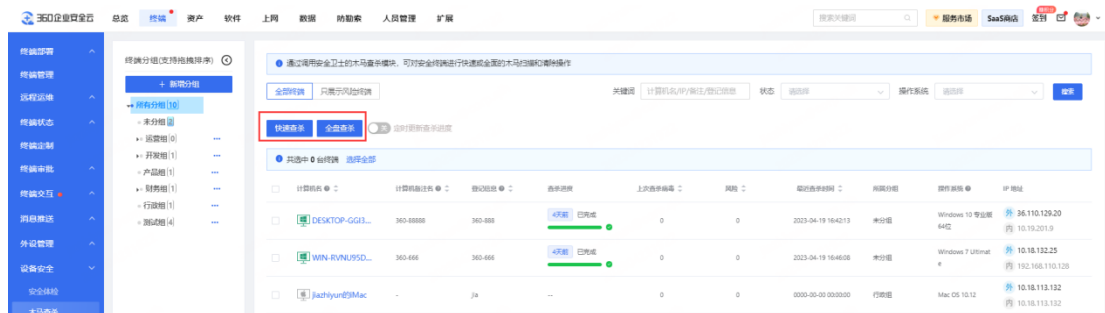


也可根据各企业需要的项目分类进行选择修复



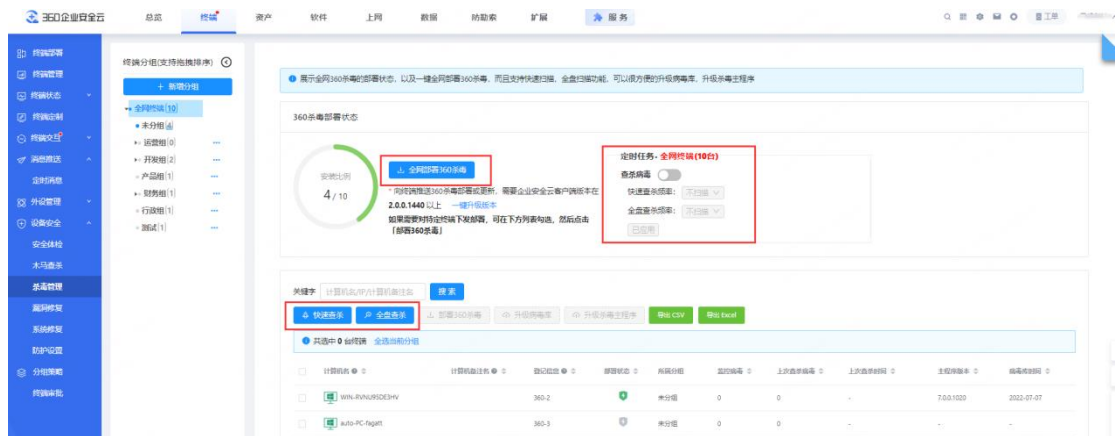
2.2.9.2 木马查杀

支持选择终端进行【快速查杀】和【全盘查杀】，并展示查杀进度、查杀时间等。



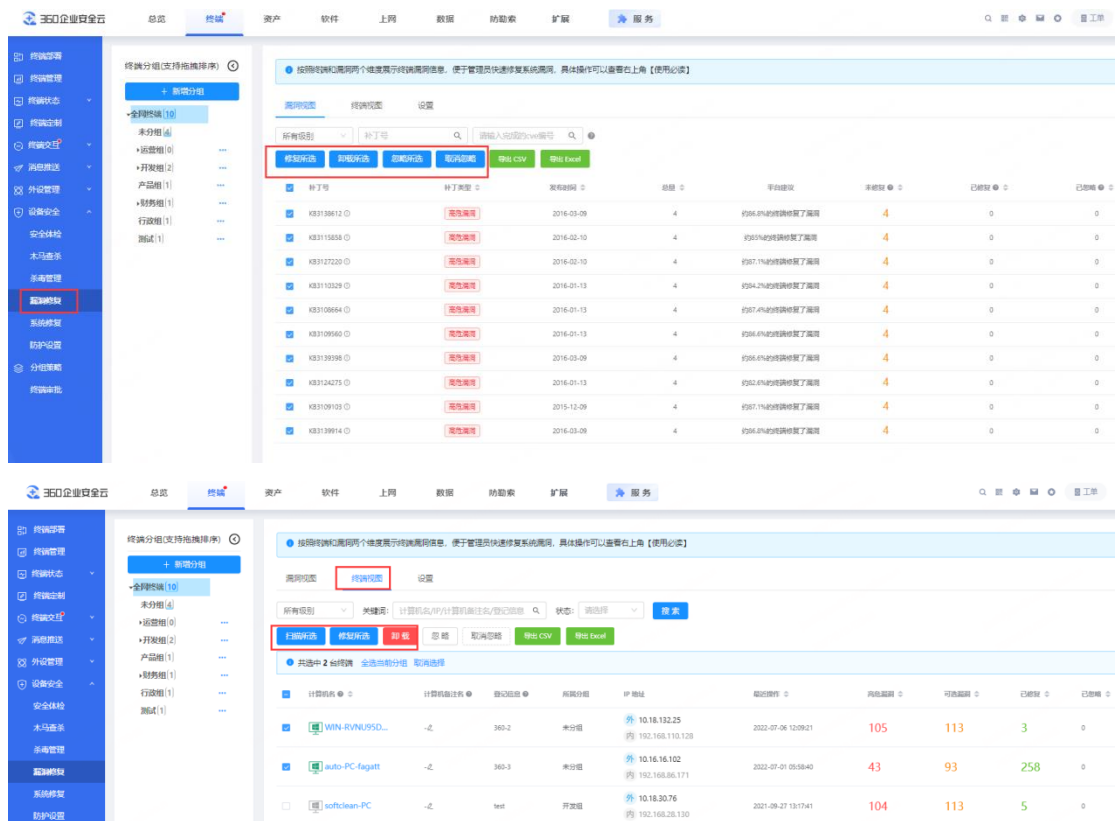
2.2.9.3 杀毒管理

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。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（专业安全管理运维服务）。

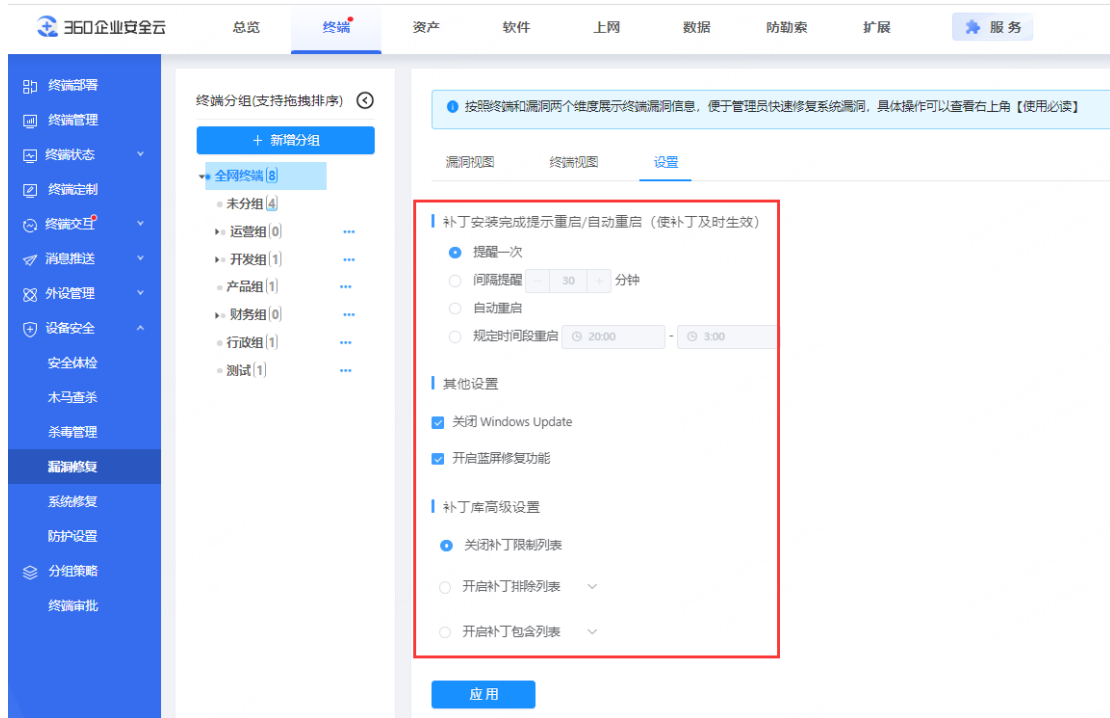


2.2.9.4 漏洞修复

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。



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

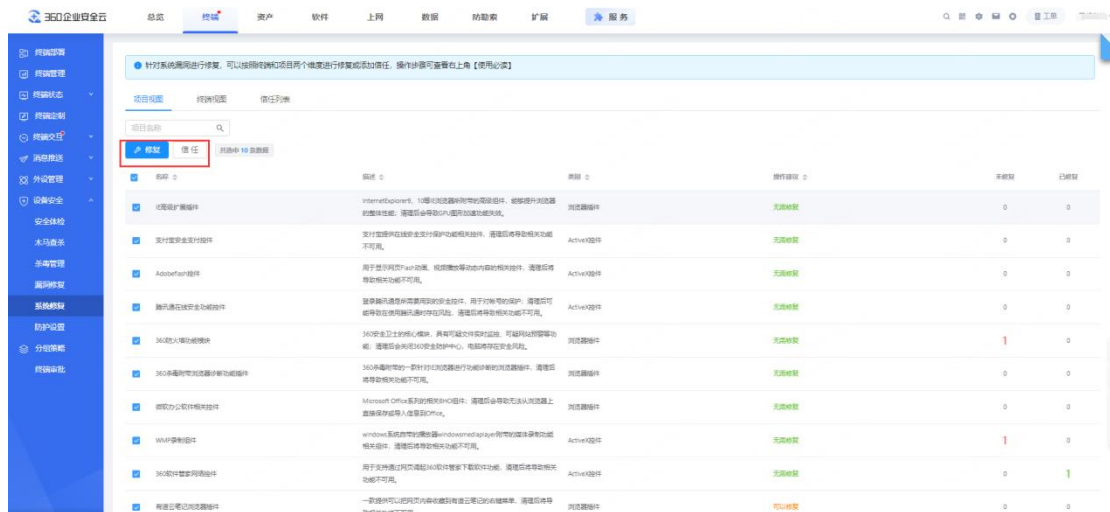


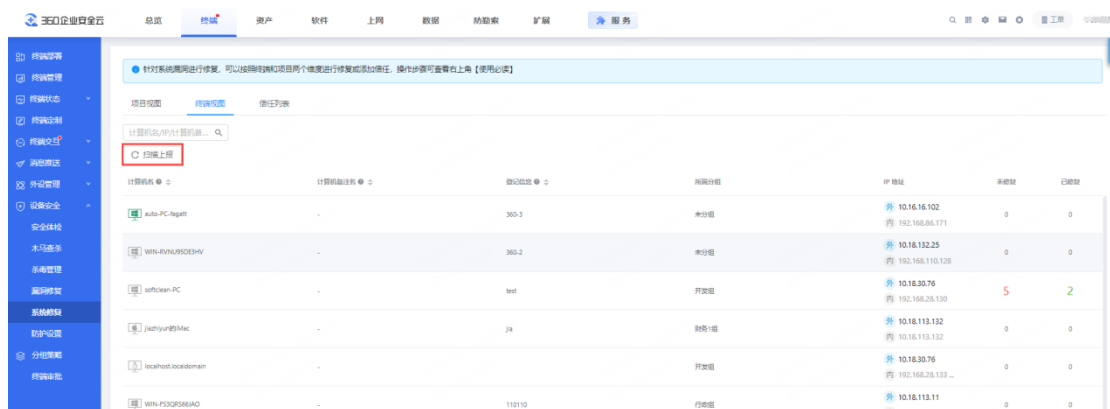
2.2.9.5 系统修复

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。



2.2.9.6 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。



2.2.10 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**全组终端**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

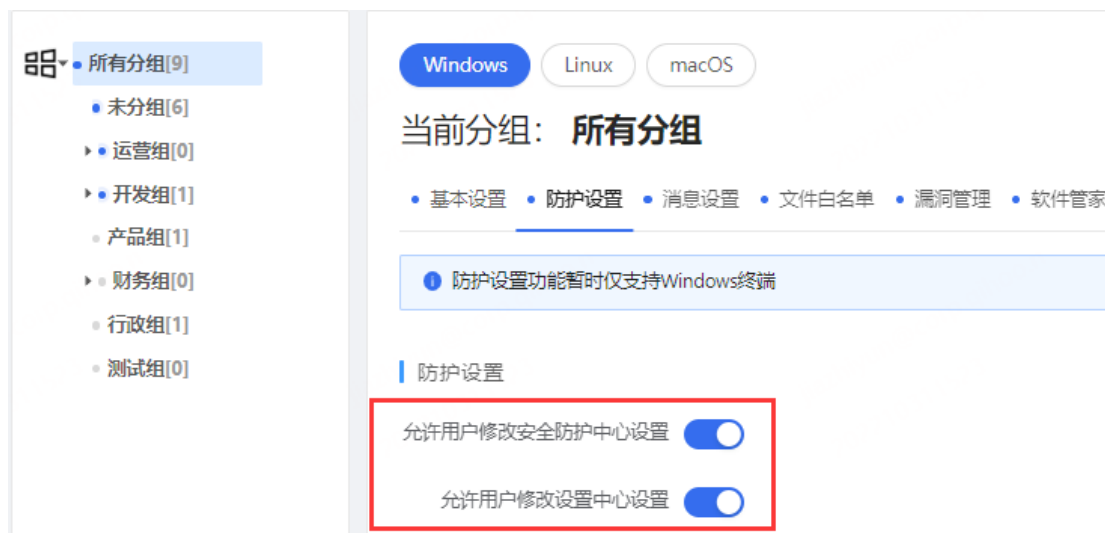
🔧 退出密码：设置防止终端退出客户端的密码

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。



➤ 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。



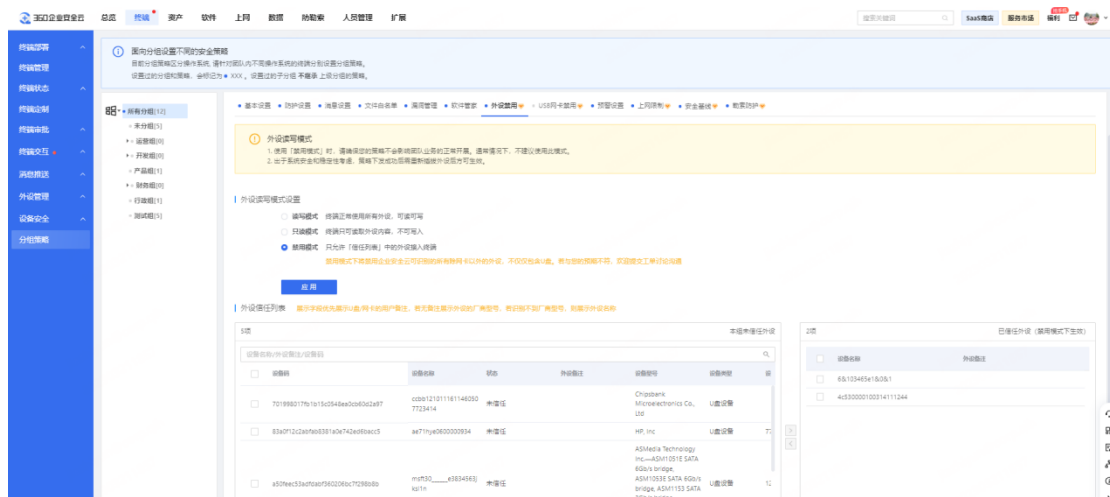
➤ 软件管家：

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。

具体设置请移步【软件-软件运行策略-软件管家设置】

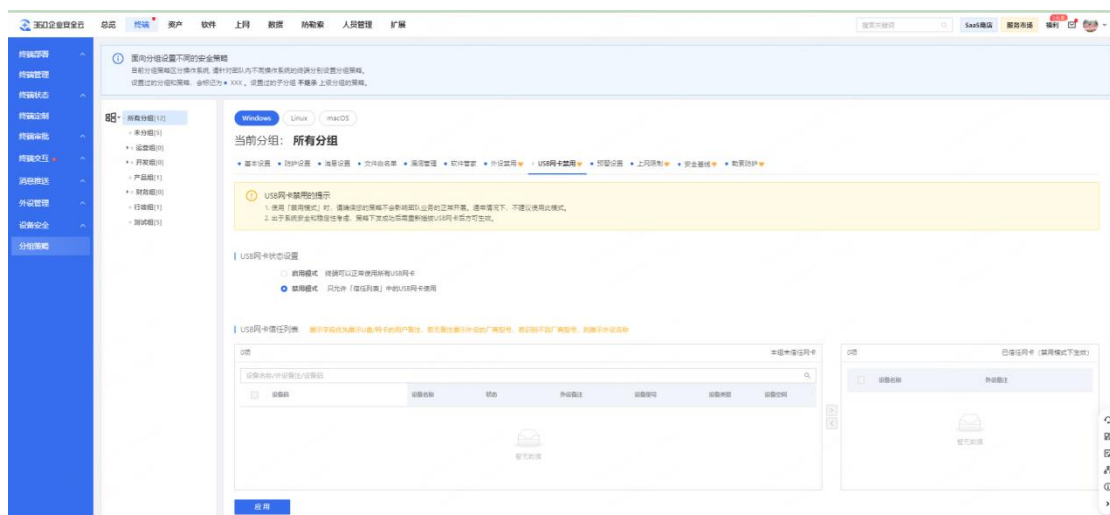
➤ 外设禁用（专业安全管理运维服务）：

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（专业安全管理运维服务）：

管理员通过对预警时间、类型的设置，能及时准确的从邮箱获取预警信息，具体设置请移步

【资产-风险预警-预警管理】

➤ 上网限制（专业安全管理运维服务）：

管理员可以设置终端用户访问网络的策略黑白名单，具体设置请移步【上网-行为限制-上网

拦截】

- 安全基线（专业安全管理运维服务）：

安全基线检查有助于管理员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，具体设置请移步【防勒索-安全基线】

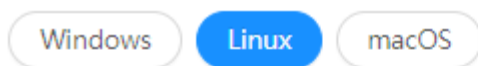
- 勒索防护（专业安全管理运维服务）：

对于终端的勒索防护设置请移步【防勒索-勒索防护】

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：



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

① 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

- 文件白名单：



➤ 预警设置：

该功能具体设置请移步【资产-风险预警-预警管理】

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。

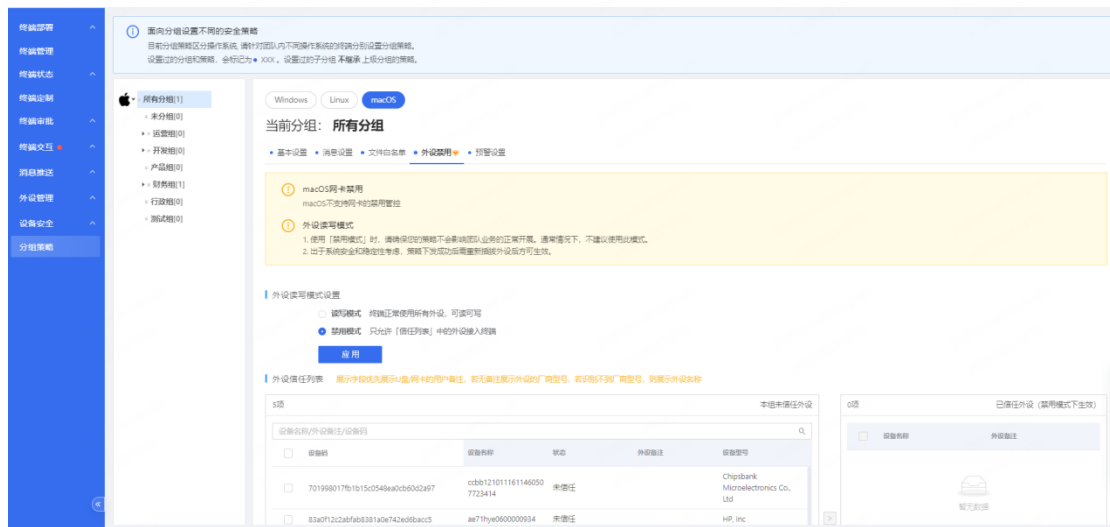
➤ 基本设置：



➤ 文件白名单



➤ 外设禁用（专业安全管理运维服务）：



➤ 预警设置：

管理员通过对预警时间、类型的设置，能及时准确的从邮箱获取预警信息，具体设置请移步【资产-风险预警-预警管理】

2.3 资产

2.3.1 资产管理

2.3.1.1 资产体检

通过资产体检的形式,增加资产全景视图,方便管理同时可及时了解企业整体资产使用情况,解决企业管理资产的痛点。



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。



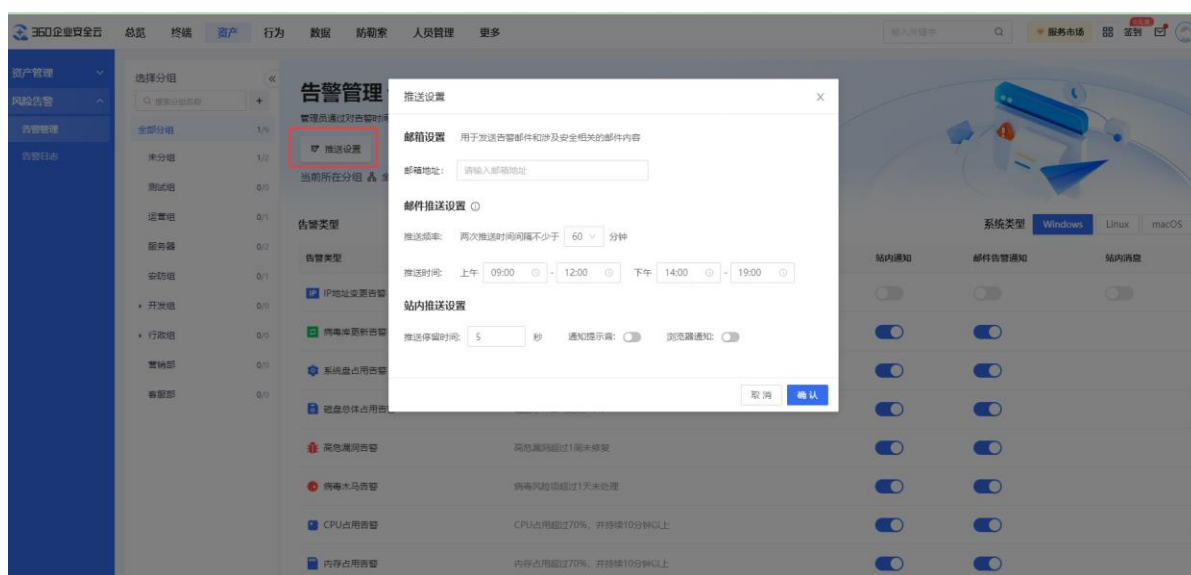


2.3.2 风险告警

2.3.2.1 告警管理

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

告警邮箱请在【推送设置】进行设置和修改



2.3.2.2 告警日志

可以查看全网终端的告警日志，可根据设备名称和登记信息查询



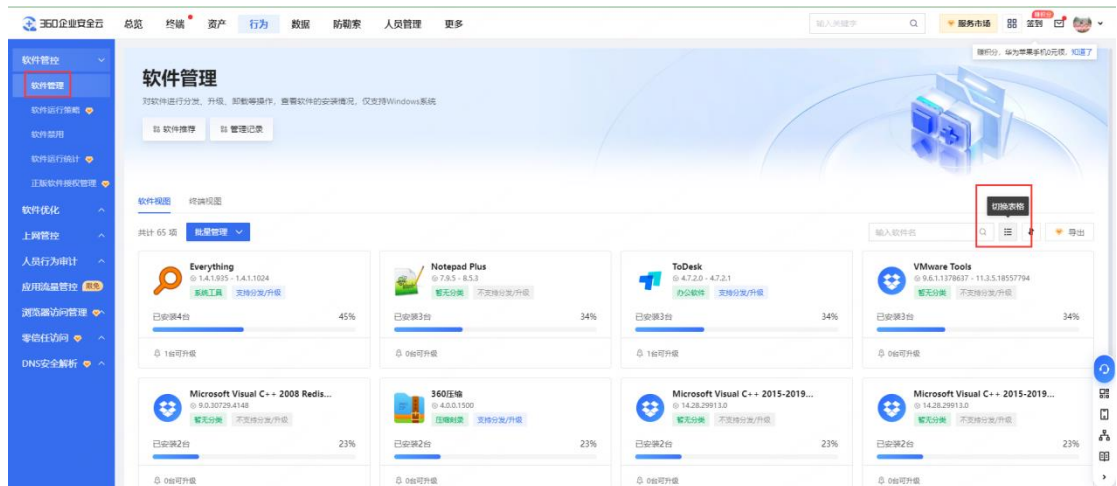
2.4 行为

2.4.1 软件管控

2.4.1.1 软件管理

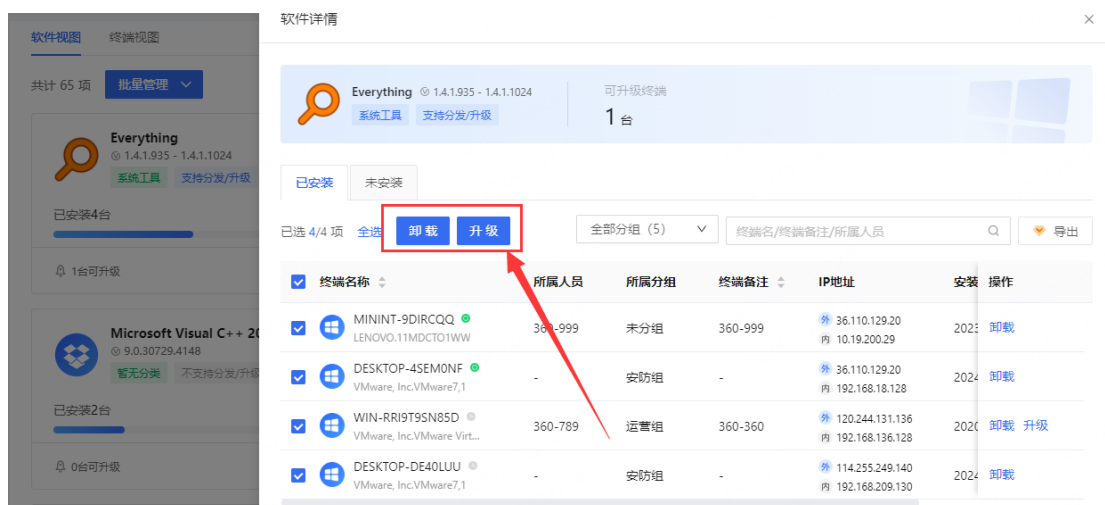
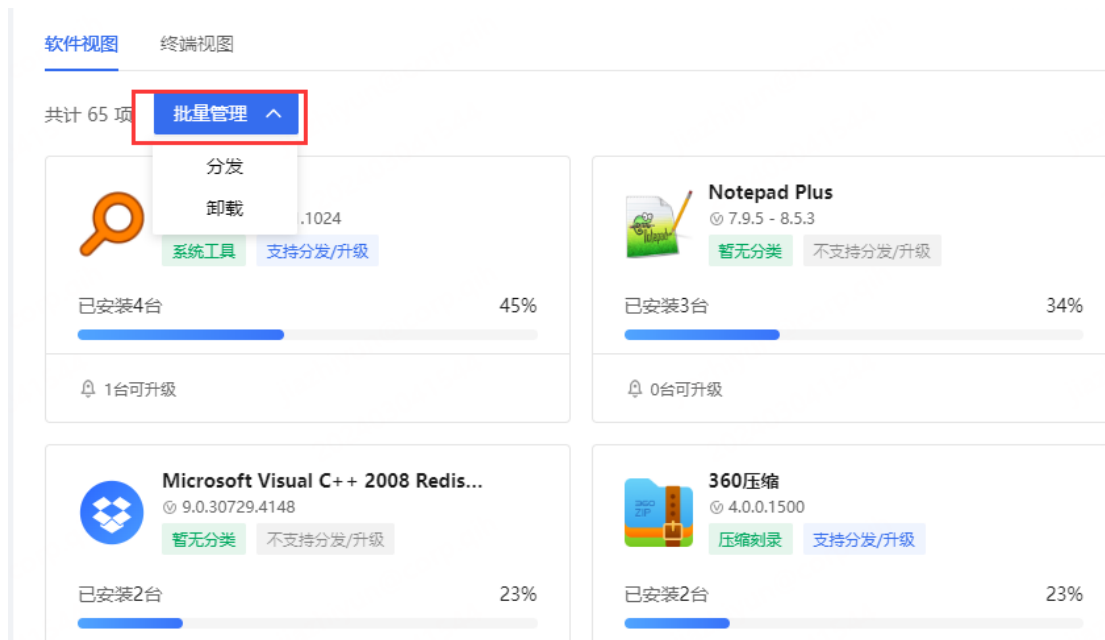
软件管理可以终端视图和软件视图对已安装的软件情况进行查看以及相应的操作：卸载、升级、数据导出等。

软件视图默认为“卡片模式”展现，可以切换为“列表模式”。

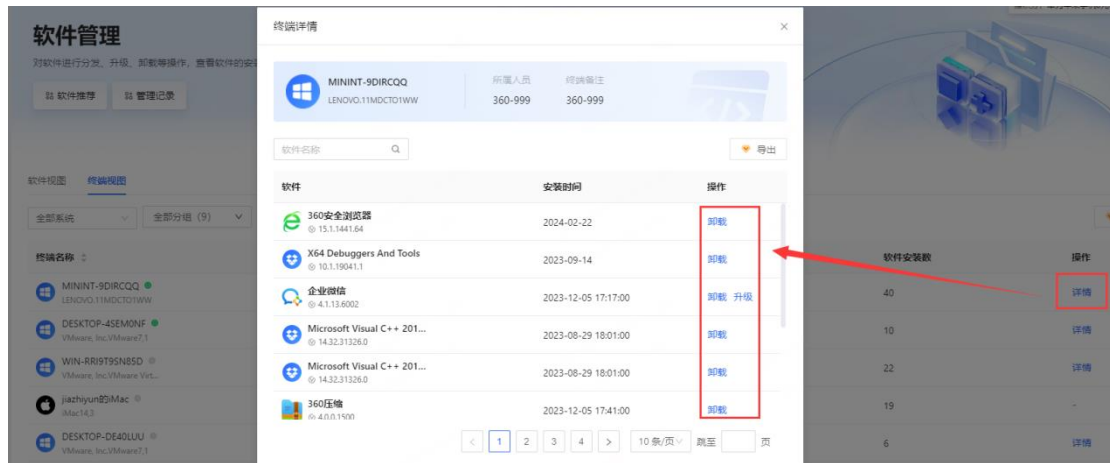




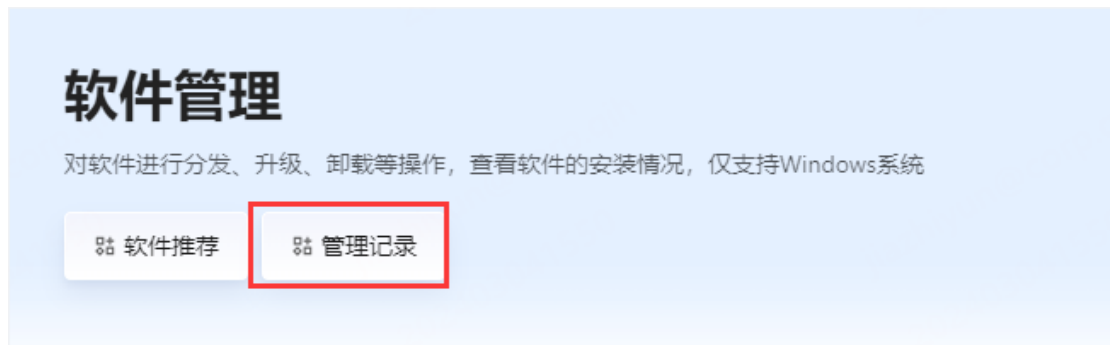
可以对所有软件进行批量管理（分发、卸载、升级）



终端视图，可以对单台终端上安装的软件进行操作（卸载、升级）

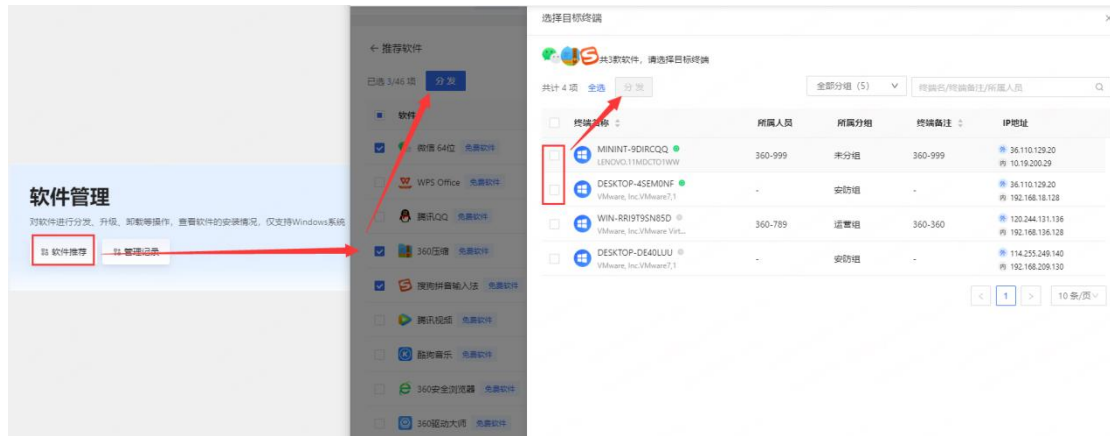


管理记录也可以在这里查看（分发任务、升级任务、卸载任务）



分发任务 升级任务 卸载任务					
软件名称	操作人	任务进度	发布日期	操作	
腾讯电脑管家		1/1	2024-02-06 11:46:22	详情	
腾讯电脑管家		1/1	2024-02-06 11:44:16	详情	
360压缩		2/2	2023-12-29 15:06:09	详情	
360杀毒 64位		1/1	2023-12-11 14:23:22	详情	
360杀毒 64位		1/1	2023-12-11 14:15:56	详情	
360杀毒 64位		1/1	2023-12-07 17:23:05	详情	
WPS Office		1/1	2023-11-03 10:33:43	详情	

在【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。



2.4.1.2 软件运行拦截（专业安全管理运维服务）

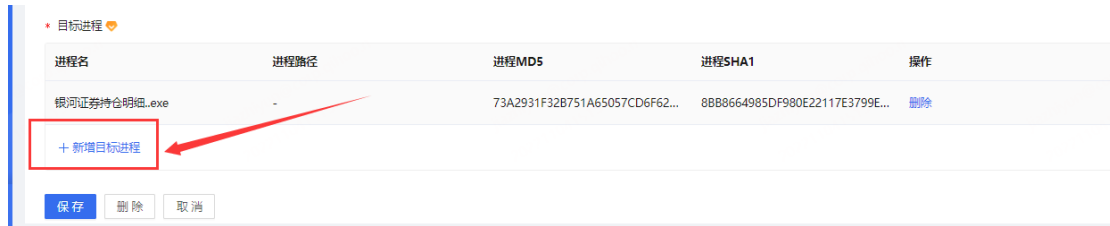
开启软件运行策略的开关，【创建运行策略】可以根据企业需要创建软件黑名单或者软件白名单，应用于所有分组或者某个子分组。



策略执行时间段可以根据需要进行设置

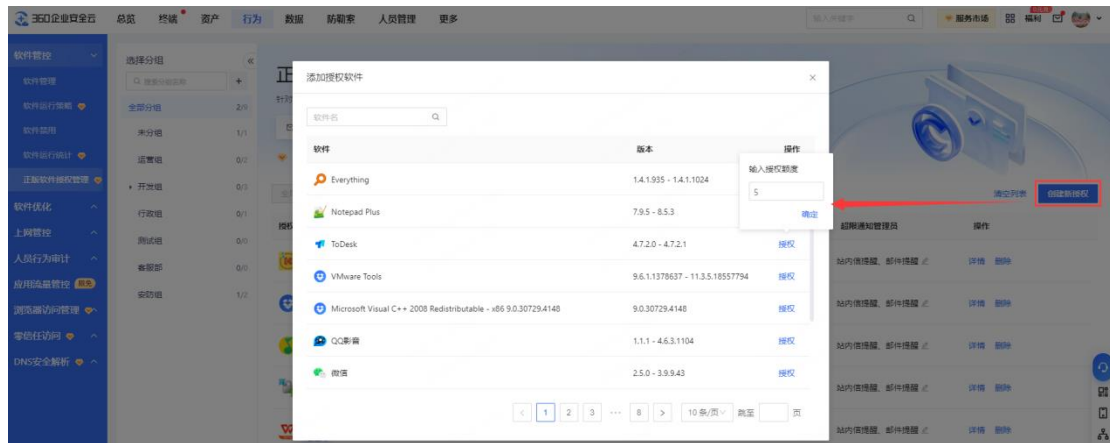


软件列表中搜索不到的软件，可以通过添加软件进程达到禁用或者启用的目的

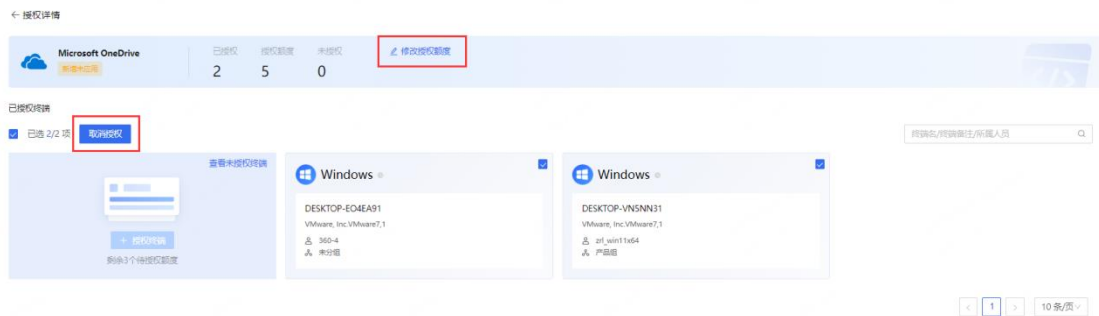


2.4.1.3 正版软件授权管理（专业安全管理运维服务）

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。



点击某款软件的详情，可以查看授权终端明细，进行授权额度修改和取消授权的操作。



超出授权数额的终端使用软件时，会进行使用受限提醒



超限通知模板设置：

设置超限通知模板

* 通知标题

正版授权管理

* 通知内容

抱歉，您所在的团队不允许此终端使用【#softname#】，详情请咨询您的团队管理员

注：使用'#'包裹的字符串为动态内容。目前仅支持展示软件名：#softname#

推送URL

输入URL

取消

确定

2.4.1.4 安装与启动禁用

一键禁止安装或启动有风险或对企业安全云管控有威胁的软件。



➤ 软件安装拦截：

开启后将针对存在破坏和攻击能力的软件进行安装拦截，防止因为损毁客户端程序导致的管控失效（建议添加有恶意行为、禁止安装的软件）

← 软件安装拦截

已订阅「专业安全管理运维服务」，此功能正常使用中

执行对象 全部分组

软件安装拦截

开启后，针对存在破坏和攻击能力的软件进行安装拦截，防止因为损毁客户端程序导致的管控失效。(建议添加有恶意行为、禁止安装的软件)

目标软件

金山毒霸 x

腾讯电脑管家 x

火绒安全软件 x

瑞星杀毒软件 x

2345安全卫士 x

应用

➤ 软件禁止启动：

可设置禁用软件名单，设置后会自动拦截名单内软件运行并弹窗提示终端卸载，部分软件会尝试自动卸载。

← 软件禁止启动设置执行对象 全部分组

区别于软件运行黑名单设置，开启后会尝试卸载已添加的软件，执行优先级高于软件运行黑名单策略。(建议添加一些流氓软件或禁止运行的软件)

目标软件

2345游戏大厅,1900062322 x

2345王牌输入法,0 x

桔子浏览器 x

腾讯手游助手 x

速浪极速浏览器 x

驱动总裁,0 x

qq游戏 x

腾讯游戏平台 x

37游戏盒子 x

植物大战僵尸 Plants Vs. Zombies x

浏览器 >

37游戏盒子

压缩刻录 >

Steam

其它软件 >

qq游戏

系统工具 >

中国游戏中心客户端

网络应用 >

奇妙加速器

视频软件 >

植物大战僵尸 Plants Vs. Zombies

2.4.1.4 软件运行统计（专业安全管理运维服务）

软件运行统计开启后，第二天即可查看数据，可按天、按周对终端上使用的软件进行使用总时长、软件使用平均时长、终端使用数量统计，可帮管理员分析软件使用的高峰时间段。

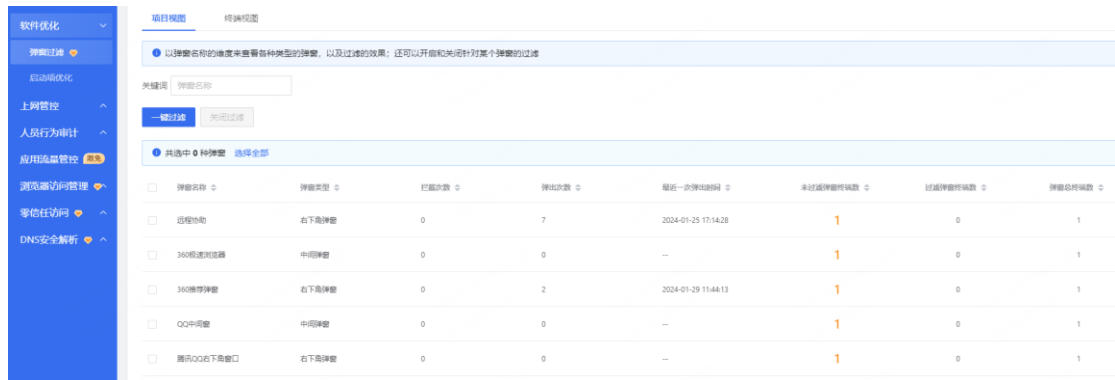
81



2.4.2 软件优化

2.4.2.1 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，可选择对某个弹窗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。



2.4.2.2 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，点击对应数字即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。

项目视图								
管理已部署计算机可进行优化的启动项								
关键词		项目名称		搜索				
优化项目		信任项目		共选中 50 条数据				
名称	描述	应用程序	启动类型	建议操作	系统建议	未优化终端	已优化终端	
金山WPS启动任务	用于定时启动金山WPS办公软件，有广告弹窗，无需开机启动。	koolaunch.exe	计划任务	允许禁止	每94%用户优化此项	1	0	
App清理相关任务	用于执行相关的清理功能。	AppDeploymentClient.dll	计划任务	建议保留现在的设置	每90%用户优化此项	1	0	
系统的键盘鼠标任务	用于在系统空闲时关闭键盘鼠标设备，提高设备使用效率。（Windows 8/7以上系统启动后默认55秒后关闭）	defrag.exe	计划任务	允许禁止	每94%用户优化此项	2	0	
系统备份还原任务	用于创建系统还原点。	rtss.exe	计划任务	允许禁止	每94%用户优化此项	1	0	
磁盘清理任务	用于清理磁盘空间，不需要开机启动。	cleanmgr.exe	计划任务	允许禁止	每94%用户优化此项	1	0	
远程协助任务	用于远程协助桌面查看与远程协助相关的更改。	RAServer.exe	计划任务	允许禁止	每94%用户优化此项	2	0	
网络信息收集器	用于收集网络信息。	gatherNetworkInfo.exe	计划任务	允许禁止	每94%用户优化此项	2	0	
媒体库缓存文件权限更新任务	用于更新用户共享媒体库中缓存的文件权限和所有新文件的安全权限。	wmpnetcfg.exe	计划任务	允许禁止	每94%用户优化此项	2	0	

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。

360企业安全云

总览终端资产行为数据防勒索人员管理更多

软件管控

软件优化

策略设置

启动项优化

上网管控

人员行为审计

应用流量管控

浏览记录管理

零信任访问

DNS安全解析

项目视图终端视图信任列表

管理已部署计算机启动项优化情况

关键词计算机名/APP/计算机备注名搜索

扫描上报

计算机名	计算机备注名	登记设备	所属分组	IP地址	活跃启动项	可优化	已优化
MININT-90RCQJ	360-999	360-999	未分组		106	102	1
DESKTOP-4E6MNF			安全组		32	28	0
WIN-FLRT507HJ	360-777	360-258	运营组		0	0	0

360企业安全云

总览终端资产行为数据防勒索人员管理更多

软件管控

软件优化

策略设置

启动项优化

上网管控

人员行为审计

应用流量管控

浏览记录管理

零信任访问

DNS安全解析

项目视图终端视图信任列表

管理已部署计算机启动项优化情况

关键词计算机名/APP/计算机备注名搜索

扫描上报

计算机名	计算机备注名	登记设备	所属分组	IP地址	活跃启动项	可优化	已优化
MININT-90RCQJ	360-999	360-999	未分组		106	102	1
DESKTOP-4E6MNF			安全组		32	28	0
WIN-FLRT507HJ	360-777	360-258	运营组		0	0	0

管理员也可添加和移除全局信任项目。

软件管控

软件优化

弹窗过滤

启动项优化

上网管控

人员行为审计

应用流量管控

浏览器访问管理

项目视图

终端视图

信任列表

文件或目录添加白信任后，在进行启动项优化时不会展示此启动项，后续针对一键优化会自动跳过

关键词

项目名称

搜索

信任

移除信任

共选中 1 条数据

☒	名称	文件路径	启动类型
☒	微软office的相关任务	c:\program files\common files\microsoft shared\office15\olicenseheartbeat.exe	计划任务

2.4.3 上网管控（专业安全管理运维服务）

2.4.3.1 上网拦截

上网拦截策略分为无限制、黑名单和白名单三种策略模式，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。

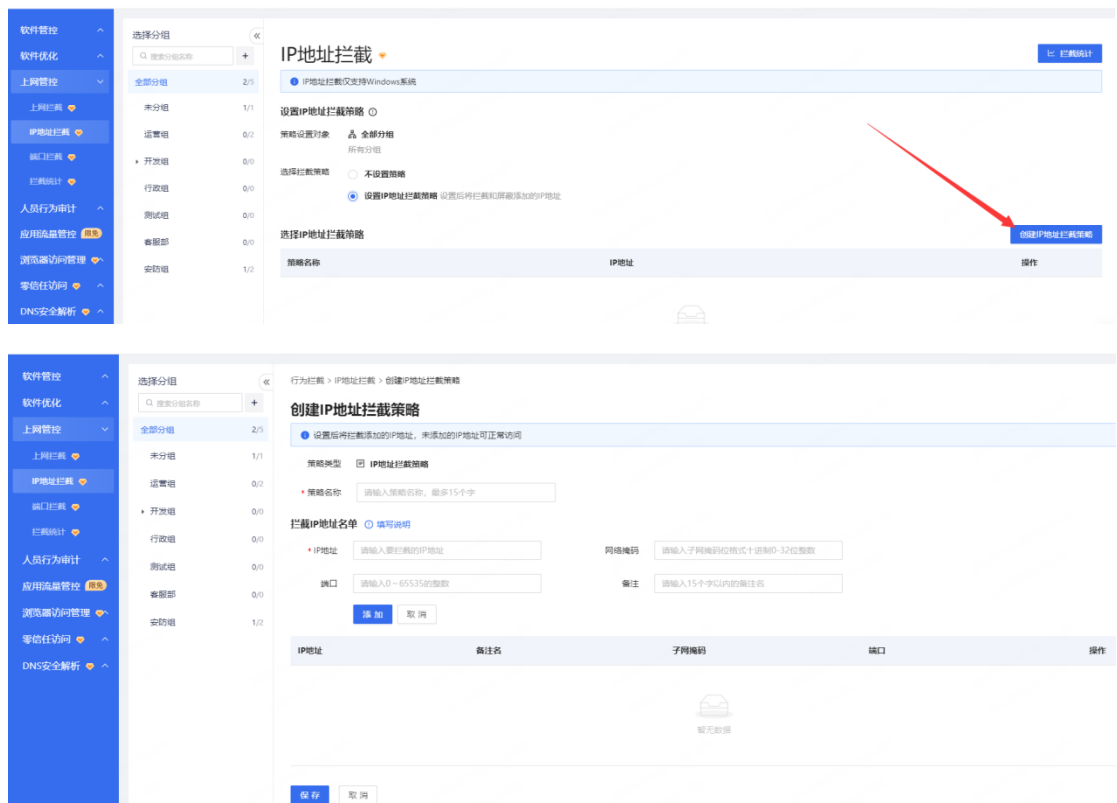


白名单模式即在指定的时间段内，只能访问白名单中的域名网站；



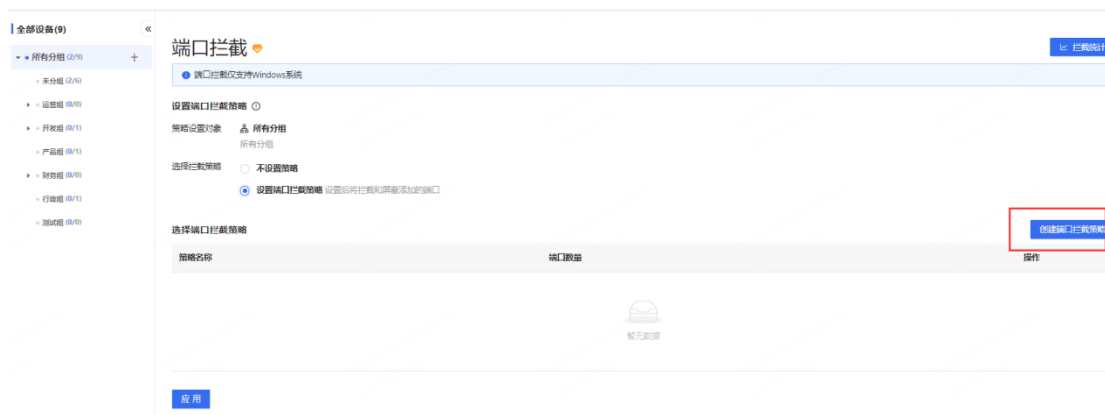
2.4.3.2 IP 地址拦截

可设置分组或者全网 ip 拦截策略



2.4.3.3 端口拦截

支持常用端口和自定义端口拦截



行为拦截 > 端口拦截 > 创建端口拦截策略

创建端口拦截策略

设置后将拦截添加的端口，未添加的端口可正常访问

策略类型 端口拦截策略

* 策略名称

本地禁用端口列表

请选择要禁用的端口(共包含3个分类30个端口)

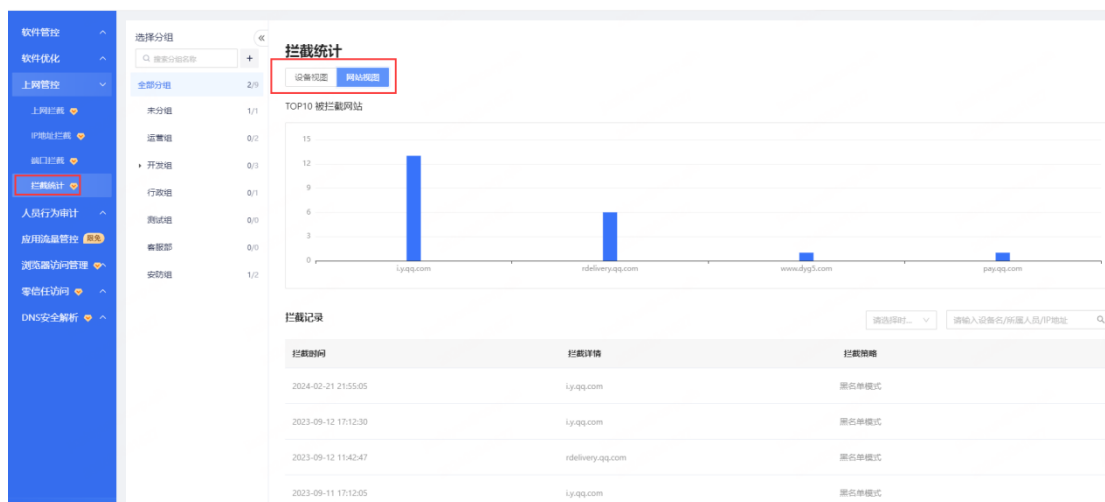
☐ 全部端口	☐ TCP	备注信息
☐ 常用TCP	☐ 135	分布式链接跟踪客户端、分布式传输协调服务、传真服务
☐ 常用UDP	☐ 139	入站 TCP 文件和打印机共享服务、计算机列表服务、TCP/IP NetB
☐ 自定义端口	☐ 445	域登录服务、文件和打印机共享服务、传真服务
	☐ 53	因特网联机共享和防火墙服务
	☐ 3389	远程桌面共享服务
	☐ 1723	路由服务
	☐ 2869	SSDP发现服务
	☐ 5000	SSDP发现服务

保存

取消

2.4.3.4 拦截统计

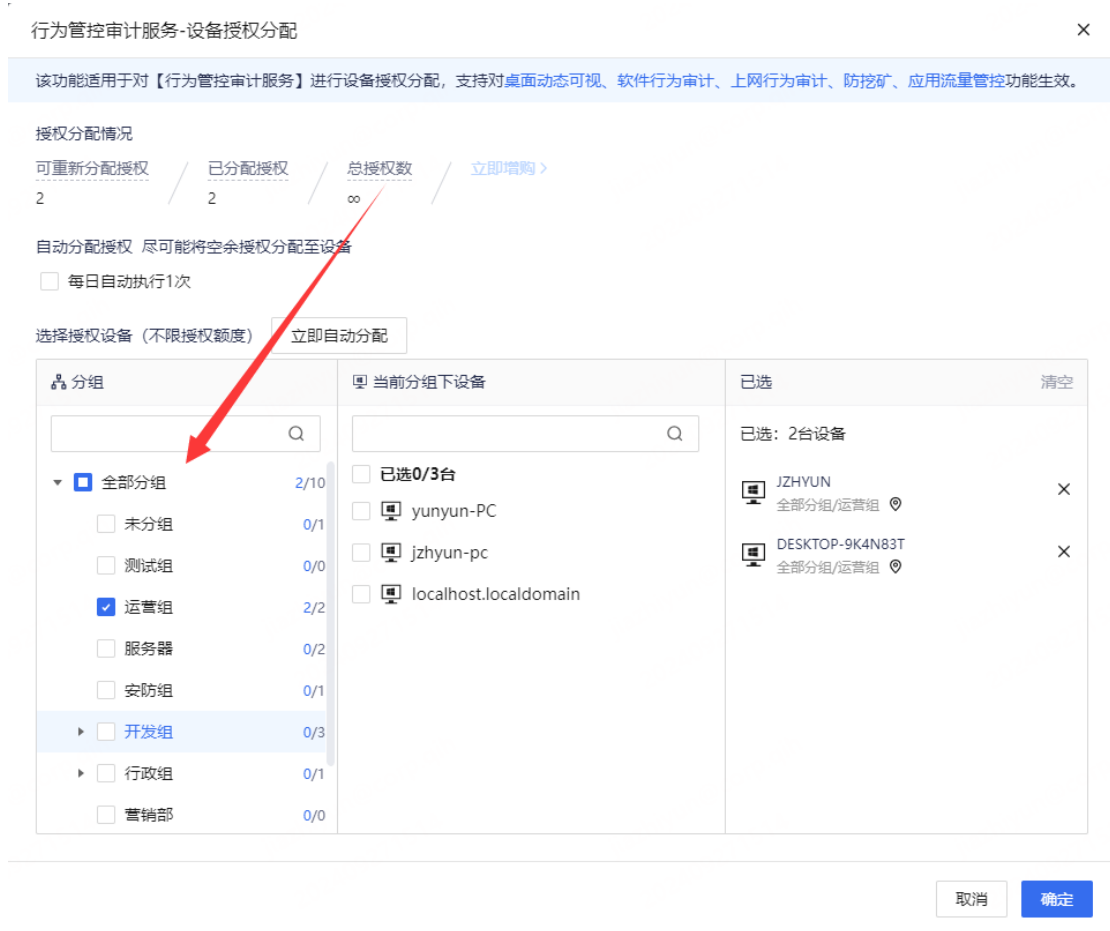
可以根据设备视图和网站视图查看拦截统计数据



2.4.4 人员行为审计（需单独付费）

该功能需要对终端进行授权分配后，策略才可生效。





2.4.4.1 桌面动态可视

对终端设备画面进行实时监控，并对终端桌面操作进行不间断缩时录像以供后续审计。

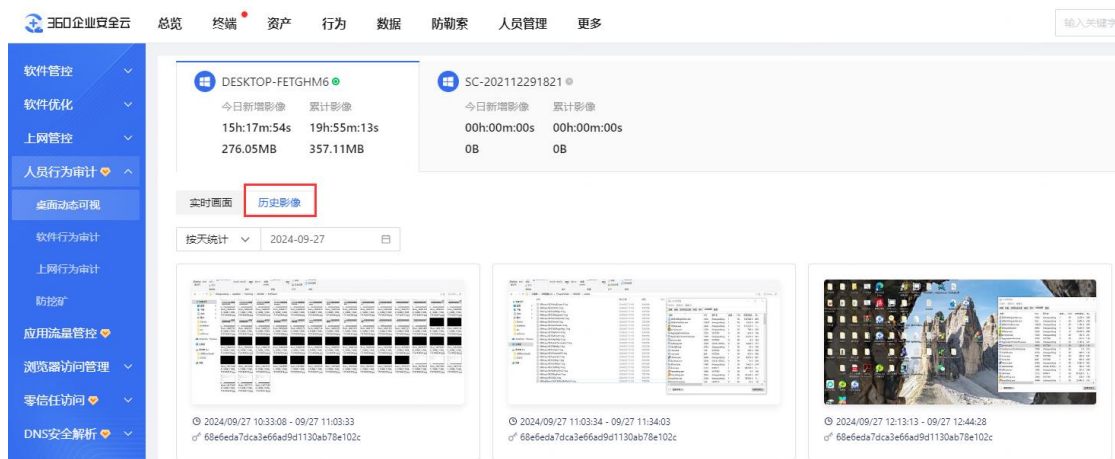
点击查看影像即可查看实时画面及历史影像。



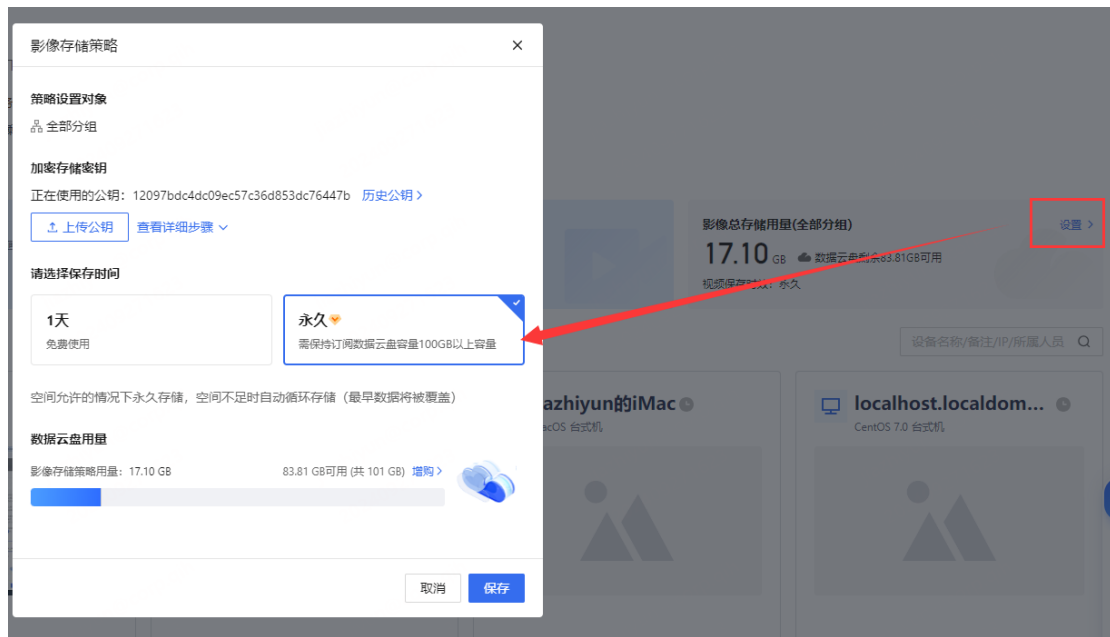
➤ 开启实时画面，会实时采集并上报终端设备的画面



➤ 开启缩时录像存储，会对终端设备进行短暂采集并存储



(视频保存时效为 7 天，如需保存更长时间需另外订阅数据云盘容量 100G 及以上)



开启缩时录像功能后, 所有影像文件均会在本地用公钥加密后上传存储在云盘, 通过控制台下载后仍是加密状态, 可通过解密工具和私钥进行解密后查看。

影像存储策略



策略设置对象

品 全部分组

加密存储密钥

● 步骤一：下载离线加解密独立工具

[↓ 下载工具](#)

V1.0 MD5: 7e2ff89b041a23385f2fe38e509bce55

● 步骤二：在安全可信的设备(推荐离线环境)上安装并使用独立工具，生成密钥对

● 步骤三：上传密钥对中用于加密的公钥

正在使用的公钥：12097bdc4dc09ec57c36d853dc76447b [历史公钥 >](#)[↑ 上传公钥](#)[收起详细步骤 ^](#)

请注意：

1. 配置密钥并开启“缩时录像”功能后，所有影像文件均会在本地用公钥加密后上传存储在云端，您通过控制台下载后仍是加密状态，您可在安全环境下通过独立工具使用您持有的私钥进行解密后查看，如您遗失“私钥”，则加密存储的数据永久无法进行解密；
2. 我们采用RSA+AES方案，生成密钥对后，请您妥善保存“私钥”，并将“公钥”上传；只有“私钥”才可解密数据，“公钥”仅能用于加密，无法解密数据也无法转换为“私钥”；
3. 您可以多次更换用于加密的公钥，但已经通过离线加密并上传至云端的数据，无法在线解密，无法切换密钥，只能使用加密时公钥对应的私钥解密，如您需要，独立工具可在完全隔离离线环境下生成密钥或解密数据，因此“私钥”可全生命周期离线保存使用；
4. 您在本处设置的密钥，仅用于当前功能(桌面动态可视)的桌面画面缩时录像数据存储所用，密钥与其他功能(包括数据云盘在内)不通用，分别设置互不干涉；

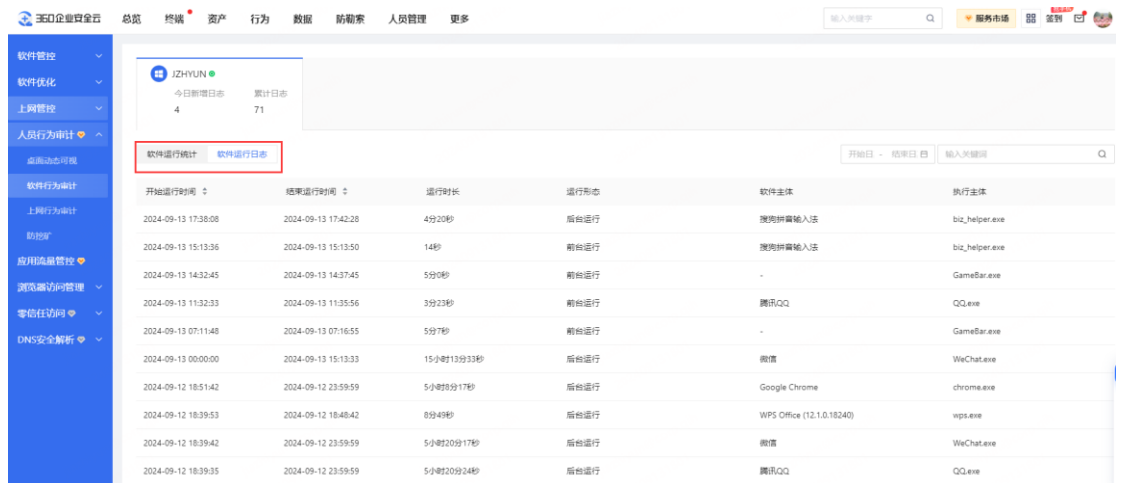
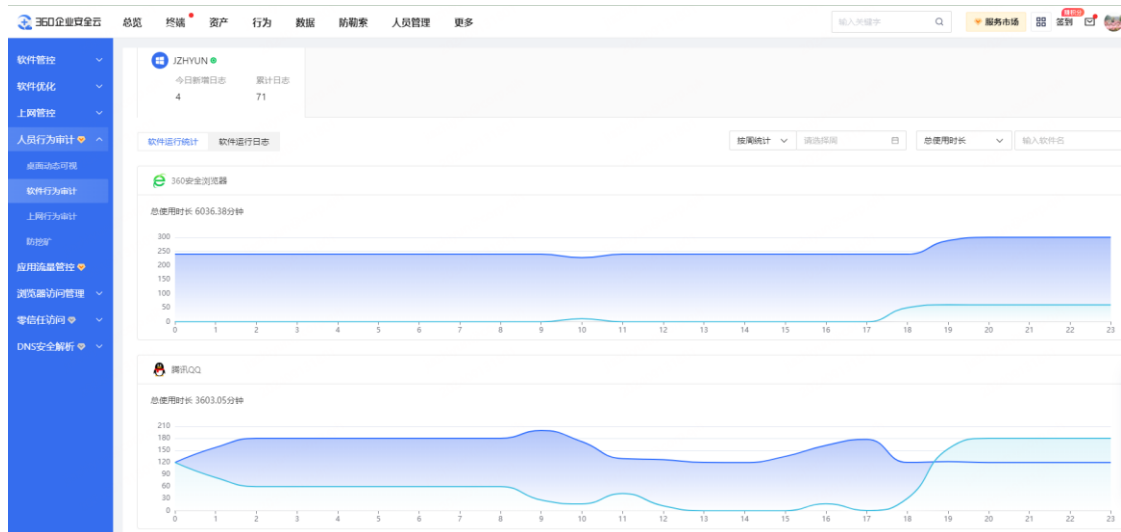
2.4.4.2 软件行为审计

对企业团队内终端上软件使用行为进行上报审计与存档备份。

- 开启软件使用审计策略后，终端上的软件使用行为会上报



➤ 点击终端名称即可查看终端上的软件运行时长统计及软件运行日志



开始运行时间	结束运行时间	运行时长	运行形态	软件主体	执行主体
2024-09-13 17:38:08	2024-09-13 17:42:28	4分20秒	后台运行	搜狗拼音输入法	biz_helper.exe
2024-09-13 15:13:36	2024-09-13 15:13:50	14秒	前台运行	搜狗拼音输入法	biz_helper.exe
2024-09-13 14:52:45	2024-09-13 14:57:45	5分0秒	前台运行	-	GameBar.exe
2024-09-13 11:32:33	2024-09-13 11:35:56	3分23秒	前台运行	腾讯QQ	QQ.exe
2024-09-13 07:11:48	2024-09-13 07:16:55	5分7秒	前台运行	-	GameBar.exe
2024-09-13 00:00:00	2024-09-13 15:13:33	15小时13分33秒	后台运行	微信	WeChat.exe
2024-09-12 18:51:42	2024-09-12 23:59:59	5小时8分17秒	后台运行	Google Chrome	chrome.exe
2024-09-12 18:39:53	2024-09-12 18:48:42	8分49秒	后台运行	WPS Office (12.1.0.18240)	wps.exe
2024-09-12 18:39:42	2024-09-12 23:59:59	5小时20分17秒	后台运行	微信	WeChat.exe
2024-09-12 18:39:35	2024-09-12 23:59:59	5小时20分24秒	后台运行	腾讯QQ	QQ.exe

2.4.4.3 上网行为审计

对企业团队内终端用户上网行为进行上报审计与存档备份

➤ 开启上网行为审计策略后，终端上的上网行为会上报



➤ 点击终端名称即可查看终端的上网行为日志及上网时长统计



上网行为日志

开始访问时间	结束访问时间	目标域名/IP	访问时长(s)	执行主体
2024-09-13 17:42:31	2024-09-13 17:55:47	dl.360safe.com	13分16秒	chrome.exe
2024-09-13 17:41:42	2024-09-13 17:42:25	weibo.com	43秒	chrome.exe
2024-09-13 17:41:24	2024-09-13 17:41:38	weibo.com	14秒	chrome.exe
2024-09-13 17:41:00	2024-09-13 17:41:20	weibo.com	20秒	chrome.exe
2024-09-13 17:40:38	2024-09-13 17:40:59	s.weibo.com	21秒	chrome.exe
2024-09-13 17:40:27	2024-09-13 17:40:37	weibo.com	10秒	chrome.exe
2024-09-13 17:39:53	2024-09-13 17:40:26	s.weibo.com	33秒	chrome.exe
2024-09-13 17:39:39	2024-09-13 17:39:49	s.weibo.com	10秒	chrome.exe
2024-09-13 17:39:22	2024-09-13 17:39:38	weibo.com	16秒	chrome.exe
2024-09-13 17:38:58	2024-09-13 17:39:21	s.weibo.com	23秒	chrome.exe

2.4.4.4 防挖矿

监测并拦截挖矿病毒，防止挖矿行为消耗公司电力与计算资源。管理员可给全组或子分组配置

“挖矿程序拦截”和“浏览器网页挖矿拦截”的策略。



拦截功能开启后，该分组下的终端将会对挖矿程序的运行和浏览器网页中的挖矿行为进行拦

截，并上报相关日志。

分组终端						
设备名称	使用人员	终端备注	ip地址	Mac地址	挖矿程序拦截	网页挖矿拦截
WIN-LMJS8E7CIGK VMware Virtual Platform 其他	-	np01	...	...	3	13

点击拦截数量即可查看此终端所有相关日志内容

挖矿程序拦截日志 设备: WIN-LMJS8E7CIGK			
时间	进程名	进程路径	进程MD5
2024-02-23 19:40:32	sockettestdlg(1).exe	c:\users\administra...	8be546653090bfc1ed29d4ca5fbf4d11
2024-02-23 19:32:47	sockettestdlg(1).exe	c:\users\administra...	8be546653090bfc1ed29d4ca5fbf4d11
2024-02-23 19:23:55	sockettestdlg(1).exe	c:\users\administra...	8be546653090bfc1ed29d4ca5fbf4d11

浏览器网页挖矿拦截日志 设备: WIN-LMJS8E7CIGK

✕

时间	浏览器	网页URL
2024-03-02 17:01:28	360Chrome64	http://www.fengsung.com/
2024-02-27 17:25:39	360Chrome64	http://www.fengsung.com/
2024-02-27 17:25:39	360Chrome64	http://www.fengsung.com/
2024-02-27 17:25:25	360Chrome64	http://www.fengsung.com/
2024-02-27 17:25:22	360Chrome64	http://www.fengsung.com/
2024-02-27 17:24:59	360Chrome64	http://www.fengsung.com/
2024-02-27 17:24:41	360Chrome64	http://www.fengsung.com/
2024-02-27 17:23:02	360Chrome64	http://www.fengsung.com/
2024-02-27 17:22:25	360Chrome64	http://www.fengsung.com/n-2...
2024-02-27 17:20:09	360Chrome64	http://www.fengsung.com/

< 1 2 > 10条/页 前往

2.4.5 应用流量管控（需单独付费）

该功能需要对终端进行授权分配后，策略才可生效。

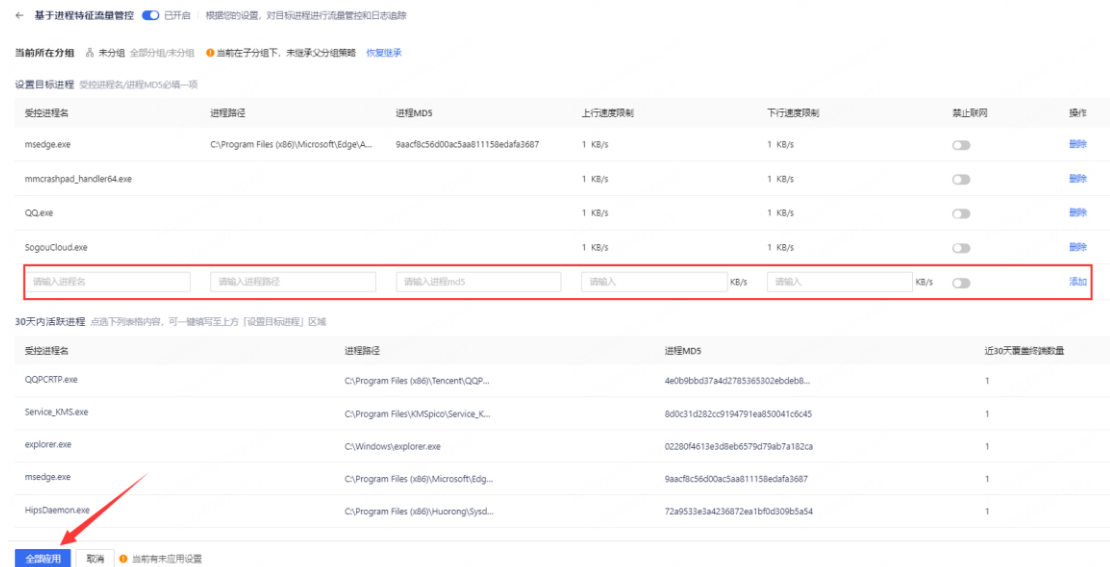


对终端设备上运行的软件、进程的上下行流量进行管控，避免带宽资源非合理性消耗。

如下所示，管理员可以给全组或子分组开启/关闭“基于进程特征流量管控”策略，



并根据不同性质分组设置不同进程的限制策略。



策略设置完成后，在终端列表中即可显示终端的流量信息。



点击流量管控日志即可查看终端流量实时状态和历史日志。



MININT-9DIRCQQ

实时监控

今日统计

管控流量

↑ 0KB/s

↑ 0KB

↑ 0KB/s

↑ 0KB

昨日统计

2

实时状态

历史日志

开始日期

结束日期

输入关键词

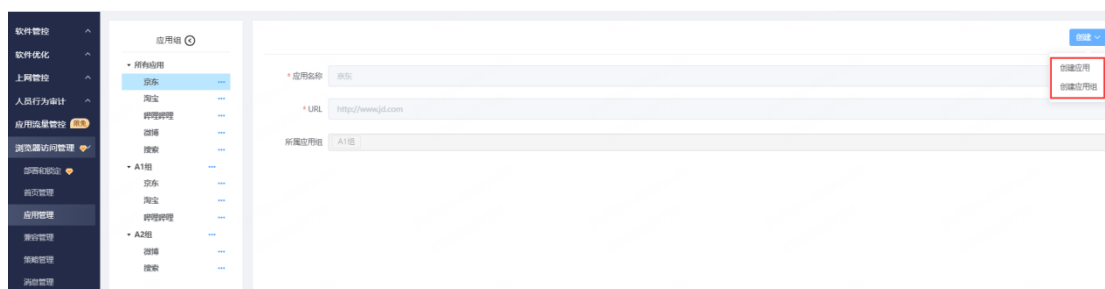
Q

开始时间日期	受控进程名	进程路径	进程MD5	软件主体	当日累计上行流量	当日累计下行流量
2024-03-06	SogouCloud.exe	C:\Program Files (x86)\sogoupinyin\13...	65266a0a1f109d53223f...	搜狗拼音输入法	47KB	68KB
2024-03-06	QQ.exe	C:\Program Files (x86)\Tencent\QQ\Bin\...	d7bc69f7c6c8e47f5703d...	腾讯/QQ	10.2MB	8.05MB



2.4.6.3 应用管理

可以创建应用和应用组，不同分组分配不同的应用和应用组。

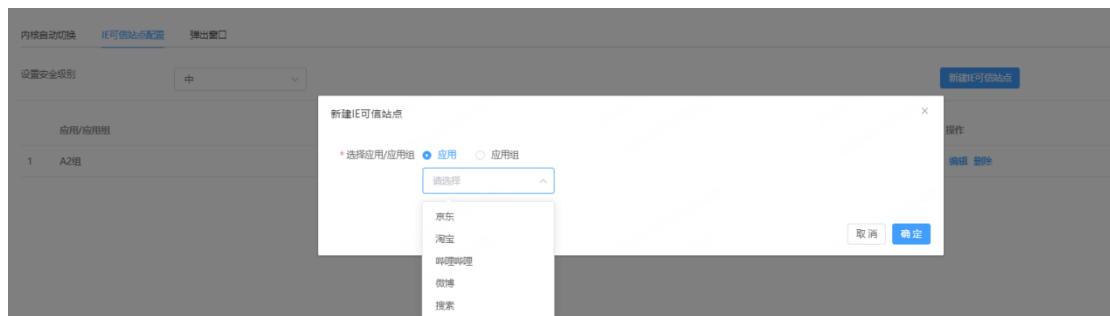


2.4.6.4 兼容管理

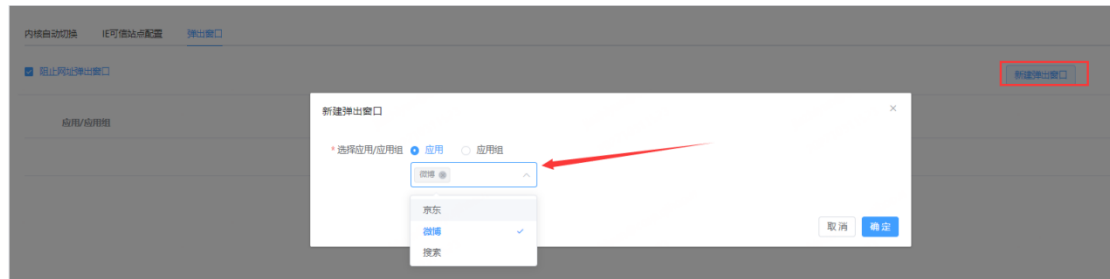
➤ 内核自动切换，可设置不同应用或应用组使用不同的浏览器内核。



➤ IE 可信站点配置

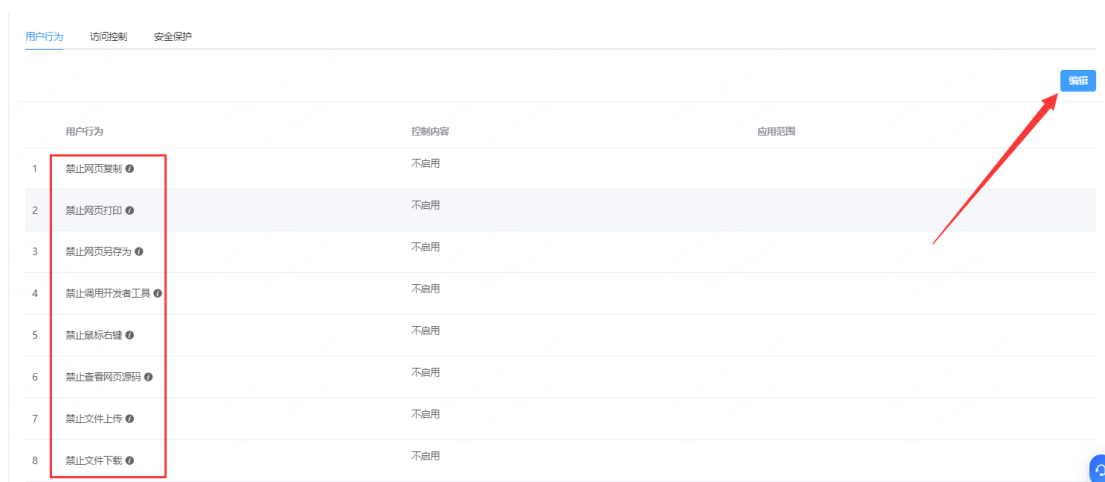


➤ 弹窗窗口配置



2.4.6.5 策略管理

👤 用户行为管理，可以对浏览网页的浏览设置行为限制



访问控制，可以设置终端用户使用浏览器访问网站时的一些权限控制



安全保护，可以设置终端用户使用浏览器时是否可以对网页截图，是否可以清除上网痕迹、下载文件时是否进行安全检测



2.4.6.6 消息管理

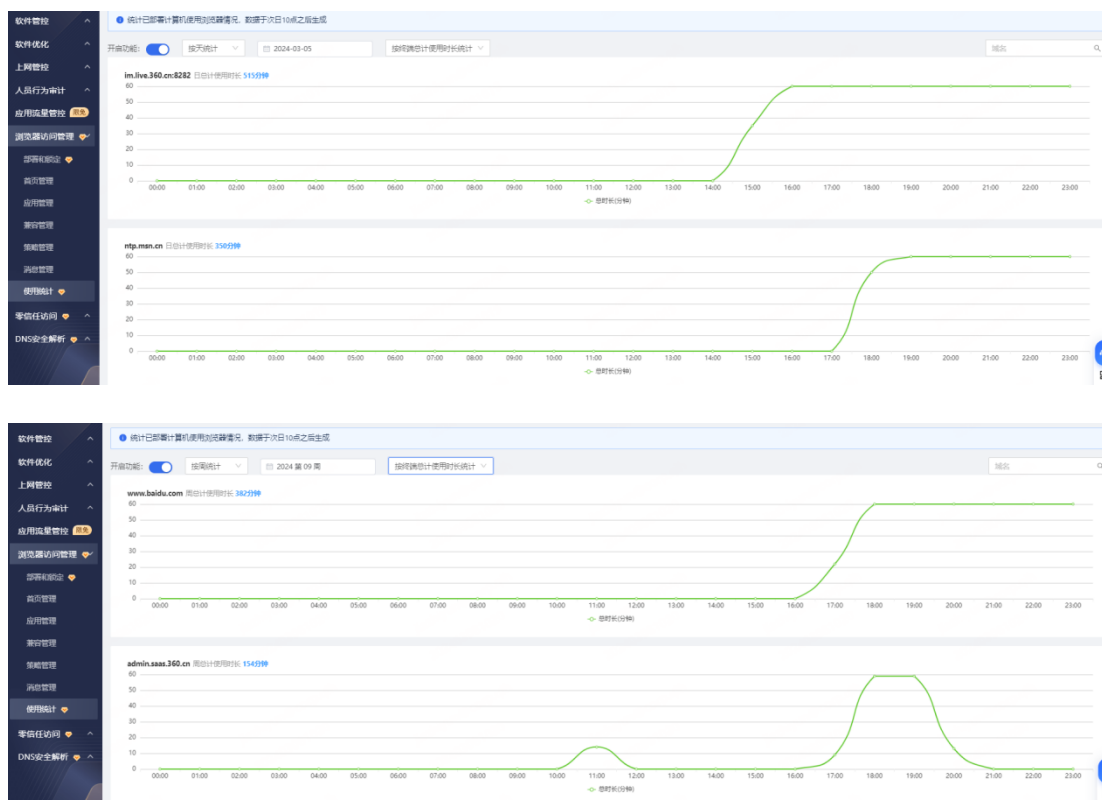
可配置首页【消息中心】的信息，如通知信息、快捷访问链接等



2.4.6.7 使用统计（专业安全管理运维服务）

可以统计全网终端使用浏览器访问网址的情况，可按天和按周查看统计时长。

统计功能开启后，数据于次日 10 点之后更新。



2.4.7 零信任访问（需单独付费）

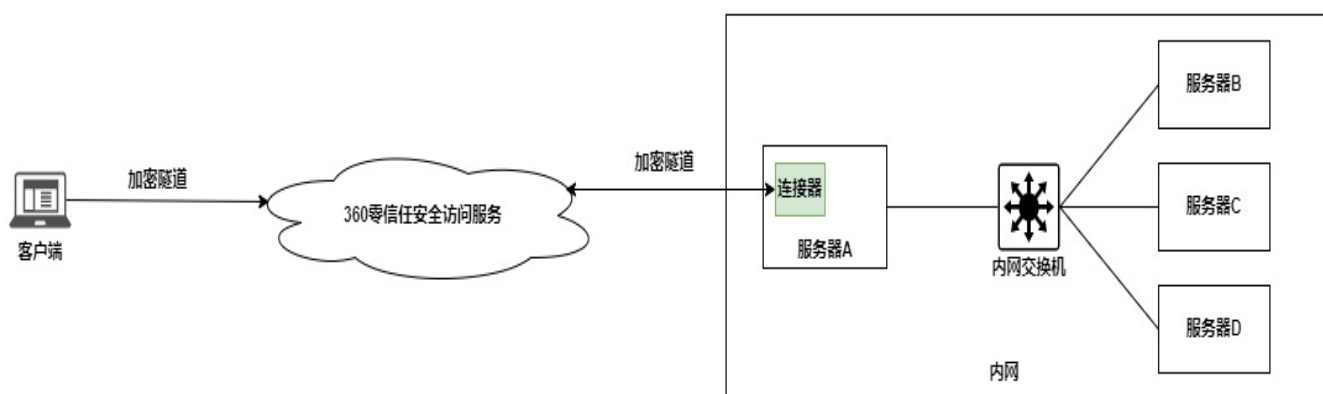
360 零信任安全访问服务通过从端到资源的全链路安全防护，为客户提供安全可靠的远程接入体验。通过精细的访问控制和丰富的动态决策能力，使合法用户可以快速便捷的访

问被授权的资源，同时有效防范各种网络攻击和数据泄露风险。（具体操作手册可联系
官方客服人员获取）

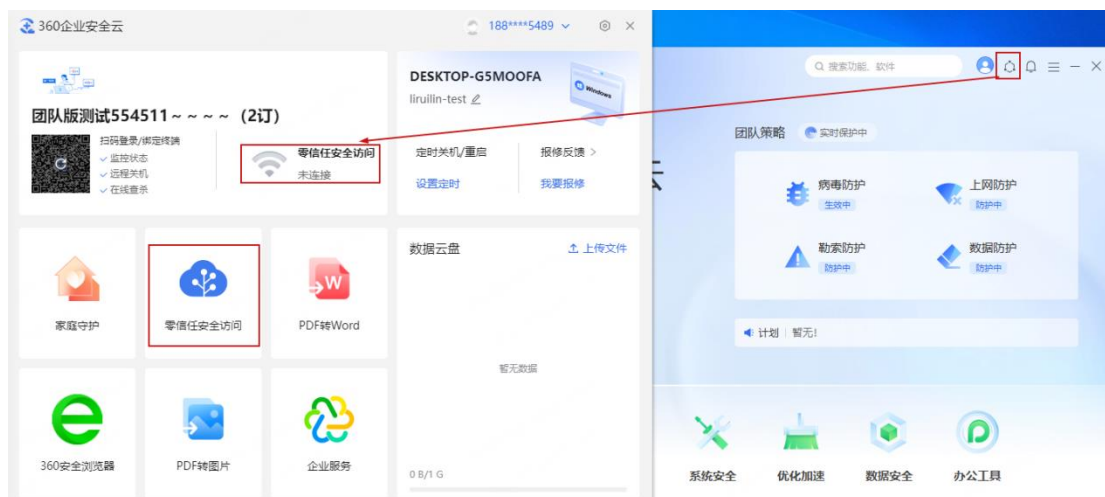
- 下图为企业团队开通零信任访问服务的入口



- 如下图所示，企业开通 360 零信任安全访问服务后，无需将公司内网资源暴露在互联网上，通过在组织内网部署连接器，一键运行连接器，建立从企业内网到 360 安全平台的加密隧道，即可实现让分布各地的企业员工安全的远程访问企业内网资源。



- 资源和权限配置完成后，终端用户通过企业安全云客户端一键接入访问资源



➤ 用户点击一键接入后即可接入到零信任网络中





- 控制台概览页面即可查看企业零信任接入情况的数据大盘，包括账号总数、在线情况、策略配置情况、连接器情况、接入用户统计等信息

首页



2.4.8 DNS 安全解析（需单独付费）

- ✚ 360DNS 安全解析服务作为 360 云端安全大脑的组成部分，集 DNS 稳定解析、威胁检测和防御、上网行为管理等功能于一体。为企业用户提供稳定、智能的 DNS 解析服

务，同时基于 360 积累的海量云端威胁情报和威胁检测模型 AI 分析系统评估内网的安全状况，实时拦截企业与恶意域名的通信行为。全年稳定解析时间超 99.99%，轻松解决僵木蠕、挖矿、可视、钓鱼等上网安全问题。（[具体操作手册可联系官方客服人员获取](#)）



如下图为企业团队开通 DNS 安全解析服务的入口



2.5 数据

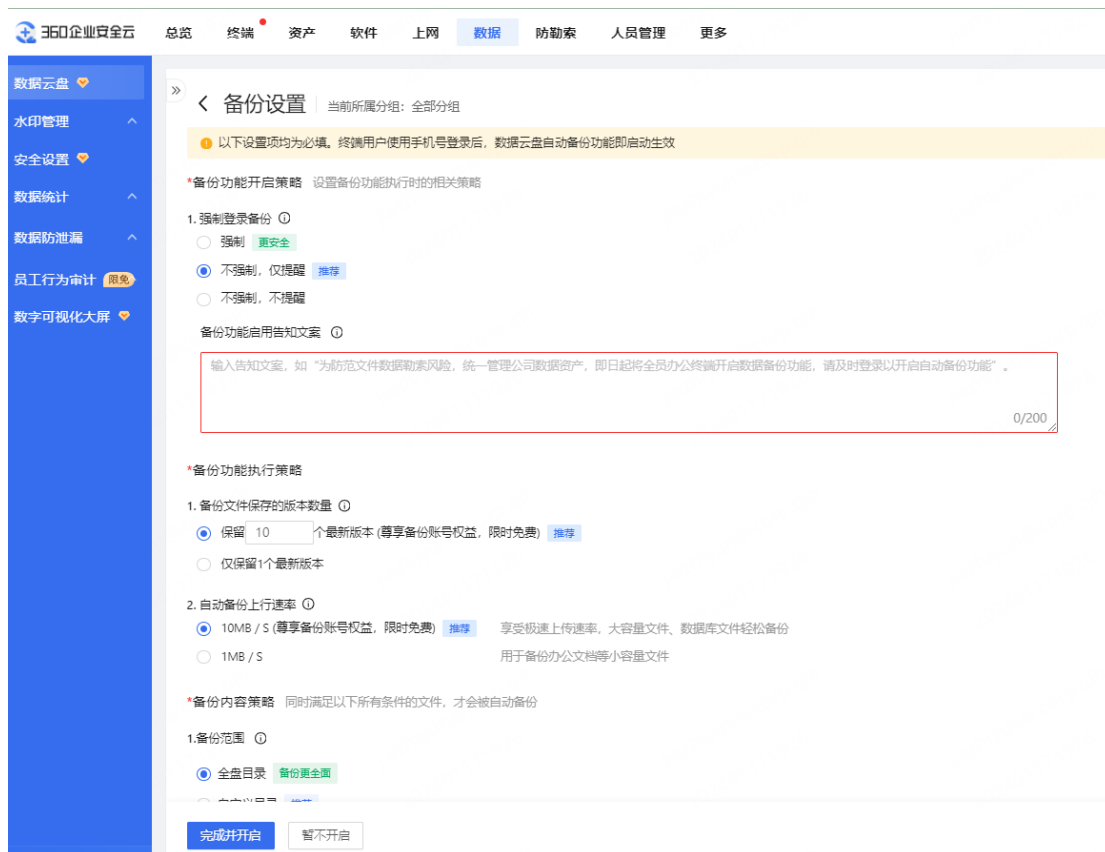
2.5.1 数据云盘（需单独付费）

对组织文档与数据资产进行备份集中管理，避免数据遭勒索攻击或意外损失，提高办公协作效率。

➤ 首次使用，需到控制台【数据】-【数据云盘】开启数据备份服务



➤ 点击“开启并去设置自动备份策略”按钮会自动跳转至策略配置页面。



➤ 策略配置分为备份功能开启策略、备份功能执行策略、备份内容策略、备份数据解冻取回四部分，前三项为必填项。

- a. 备份功能开启策略，可设置备份功能开启时是否强制通知终端用户进行账号登录以便进行数据备份。自动备份是静默将终端文件备份至云端，管理员可以自定义对终端用户

的知情通知。

*备份功能开启策略 设置备份功能执行时的相关策略

1. 强制登录备份 ①

- ☐ 强制 **更安全** 对于自动备份策略覆盖的终端，每次开机后或每个自然日提醒登录并开启自动备份功能，可跳过登录3次
- ☒ 不强制，仅提醒 **推荐** 对于自动备份策略覆盖的终端，每次开机后提醒登录并开启自动备份功能，可跳过
- ☐ 不强制，不提醒 对于自动备份策略覆盖的终端，仅在终端主动登录后开启自动备份功能，不提醒

备份功能启用告知文案 ①

输入告知文案，如“为防范文件数据勒索风险，统一管理公司数据资产，即日起将全员办公终端开启数据备份功能，请及时登录以开启自动备份功能”。

0/200

- b. 备份功能执行策略，可设置需要保留“相同完整路径的文件”多少个最新版本，最多可支持 10 个；也可设置每个账号自动备份时的上传速率上限，同账号登录多个设备时，设备之间平分上行速率。

*备份功能执行策略

1. 备份文件保存的版本数量 ①

- ☒ 保留 个最新版本 (尊享备份账号权益，限时免费) **推荐**
- ☐ 仅保留1个最新版本

2. 自动备份上行速率 ①

- ☒ 10MB / S (尊享备份账号权益，限时免费) **推荐**
- ☐ 1MB / S

- c. 备份内容策略，可以设置备份文件目录（全盘或自定义目录）、备份文件格式、备份文件大小、是否开启离线加密存储，同时满足这四个条件的文件，才会被自动备份。

*备份内容策略 同时满足以下所有条件的文件，才会被自动备份

1. 备份范围 ①

- ☒ 全盘目录 **备份更全面**
- ☐ 自定义目录 **推荐**

2. 备份文件格式

.docx	.doc	.xlsx	.xls	.csv	.pptx	.ppt	.pdf	.zip	.rar	.7z	.png	.jpg	.bmp	.tif	.gif	.tiff
.jpeg	.mp3	.mp4	.mkv	.avi	.amv	.rmvb	.mpeg	.flv	.dts	.fvt	.fxx	.fxt	.mxf	.mxb	.fmx	.abd
.dtx	.ppt	.mox	.mmt	.qpx	.cdx	.jdx	.qpx	.qpx	.db	.avb						

返回与随Enter也建要添加的扩展名 还可以添加9个扩展名

添加推荐:

3. 备份文件大小 不设置表示不限大小

KB KB

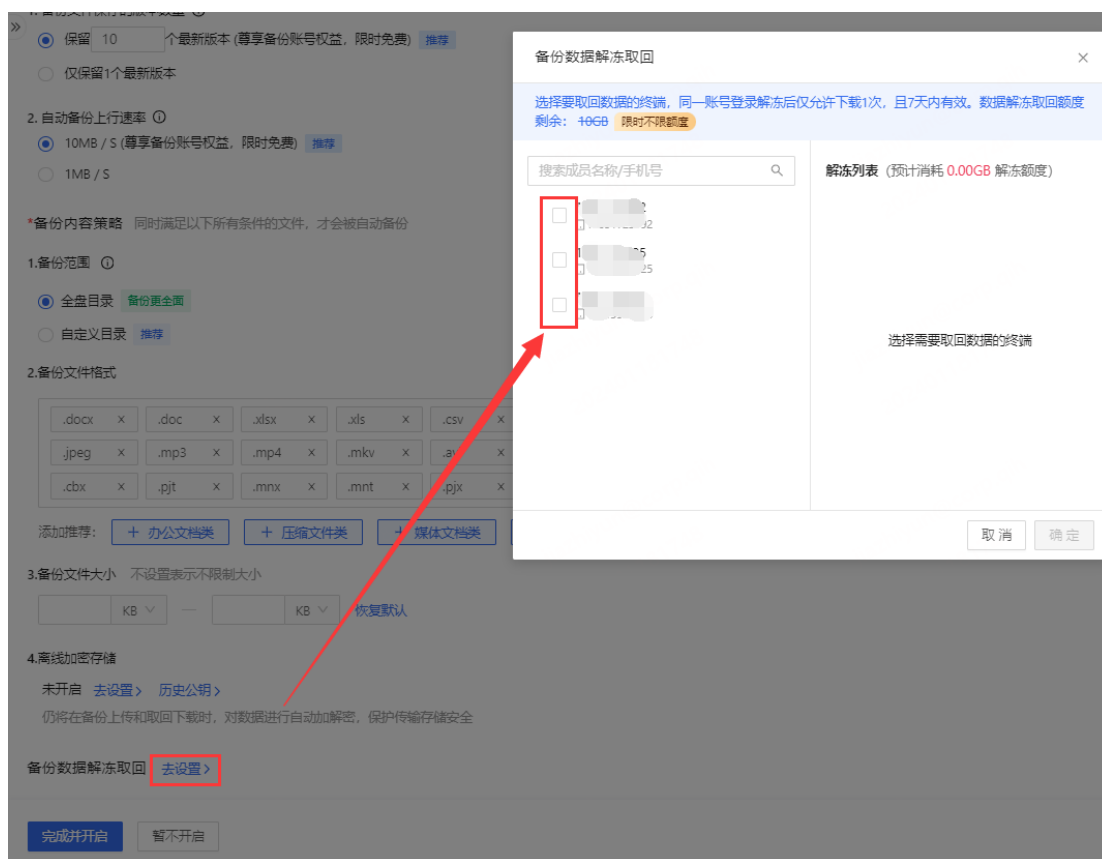
4. 离线加密存储

未开启

仍然在备份上传和回传时，对数据进行自动加密，保障存储数据安全

友情提示： 离线加密存储，开启并配置密钥对后，设备数据将会在本本地，经过配置的公钥加密后上传备份，取回下载后的数据将仍是加密状态，您可在离线环境下通过独立工具使用您持有的私钥进行解密。仅供数据高度敏感场景使用。

- d. 备份数据解冻取回，如需要取回终端自动备份的数据，管理员可在控制台设置取回的权限，允许终端取回备份文件后，终端用户即可下载已自动备份的文件。



- 以上四部分全部设置完成后，点击【完成并保存】按钮，即启动了自动备份策略。

备份设置

✕



备份设置成功

[继续编辑](#)[返回首页](#)**备份功能开启策略**

强制登录 不强制，仅提醒
告知文案 数据备份

备份功能执行策略

保存的版本数量 3
自动备份上行速率 10MB / S

备份内容策略

备份范围 全盘目录
备份文件格式 .docx .doc .xlsx .xls .csv .pptx .ppt .pdf .zip .rar .7z .png .jpg .bmp .tif .gif .tiff .jpeg .mp3 .mp4 .mkv
 .avi .wmv .rmvb .mpeg .flv .dbf .fpt .frx .frit .mdf .mdb .frm .ibd .cbx .pjt .mnx .mnt .pjt .cdx .idx .qpr
 .qpx .db .wdb
备份文件大小 不限制
离线加密存储 已开启
 正在使用的公钥: 586275738f3dc43051b3c0e899d4a3e4

- 客户端数据云盘入口如下图，在面板上登录手机账号后即可备份文件。



2.5.2 水印管理（专业安全管理运维服务）

➤ 水印设置

屏幕水印：可以选择开启全局模式或指定某些软件窗口覆盖水印，开启后将在终端屏幕或软

件顶层覆盖自定义信息，可以追溯截图来源，实现版权保护。



打印水印：开启后打印的文件上将覆盖自定义的水印信息，可根据具体需求选择只在指定的软件/进程的打印内容显示水印，或指定某些软件/进程打印内容不显示水印，或全部打印内容都显示水印。



➤ 水印显形

开启屏幕水印后，如公司内部信息被截图外传，可查看图片中【不清晰】或【隐形】的水印信息



2.5.3 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。



2.5.4 数据统计

2.5.4.1 数据概览（需单独付费）

以日、周和月为维度对企业团队整体安全与管控数据效果汇总并进行可视化展示。

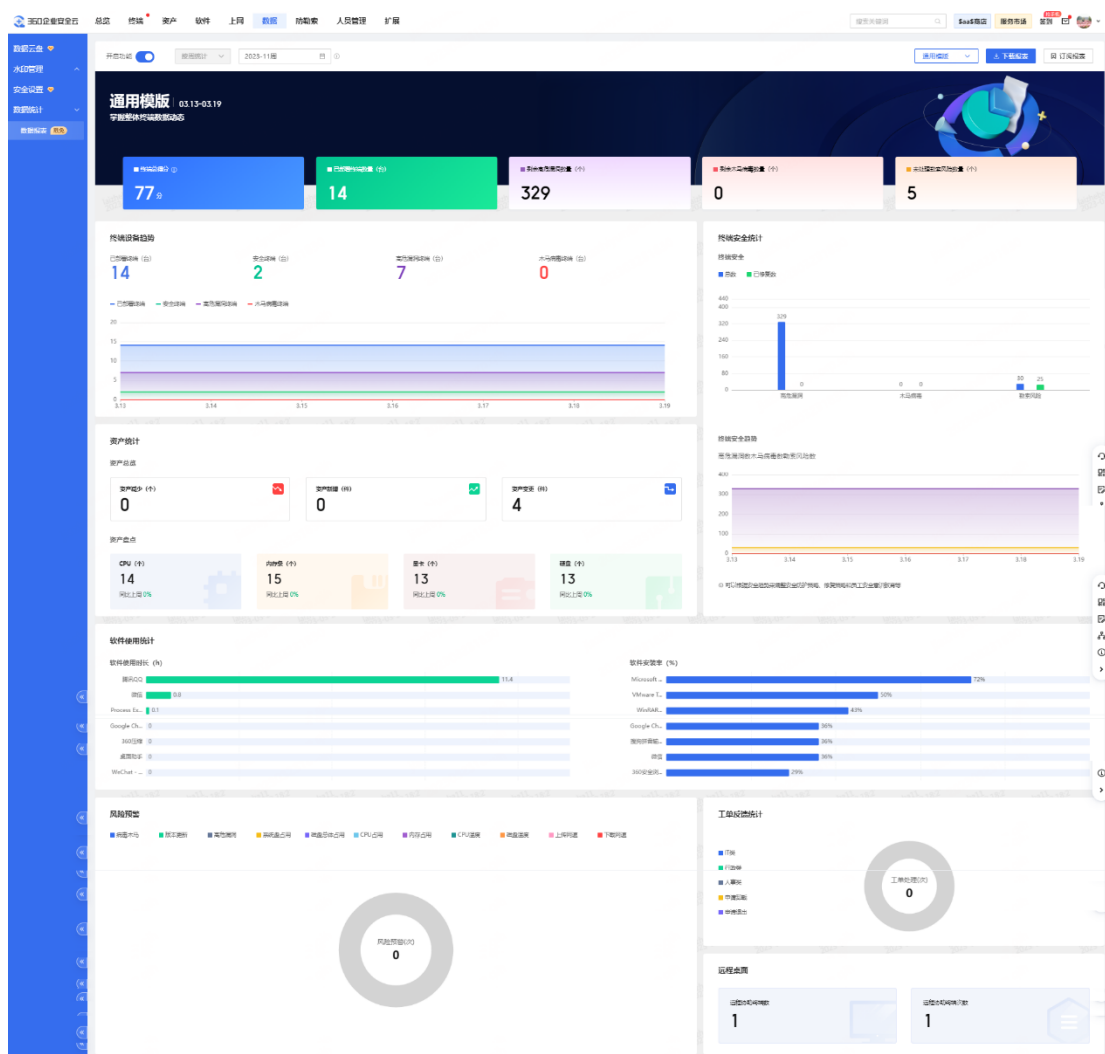


2.5.4.2 数据报表（需单独付费）

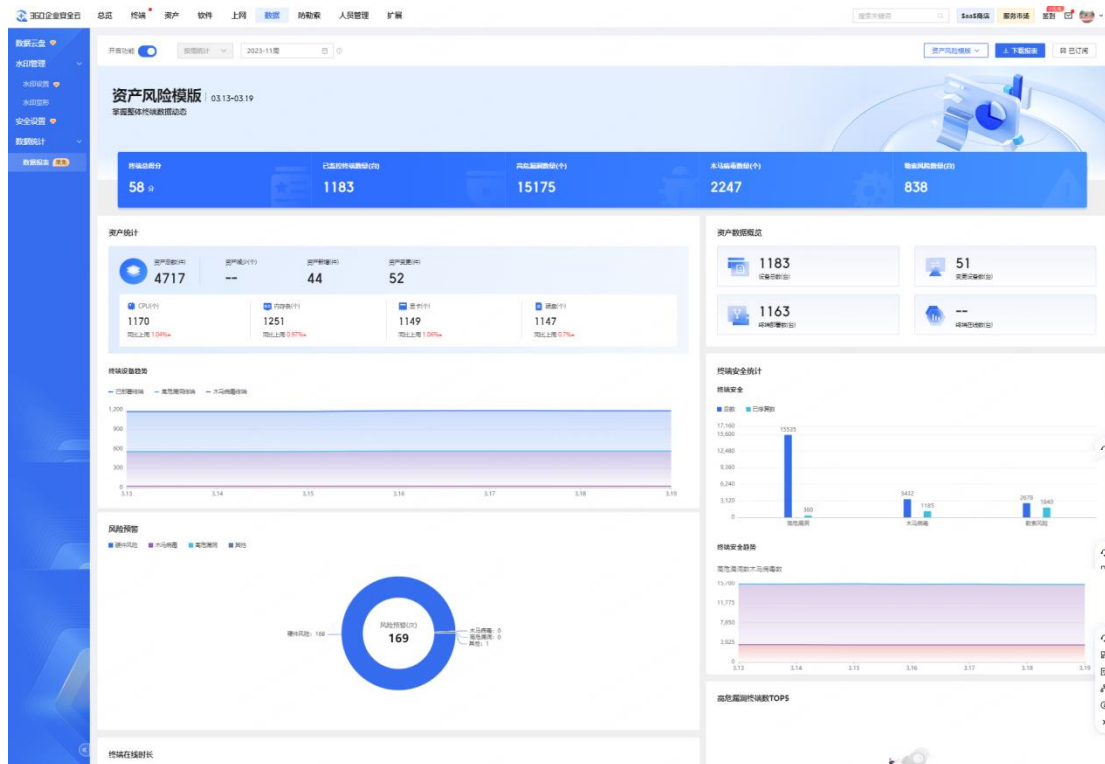
开启数据报表功能后，可选择三种模板样式查看近一个月内每周终端管理数据报表（首次开启将于次周产生数据），可下载数据报表，并且支持订阅报表定时发送至邮箱。



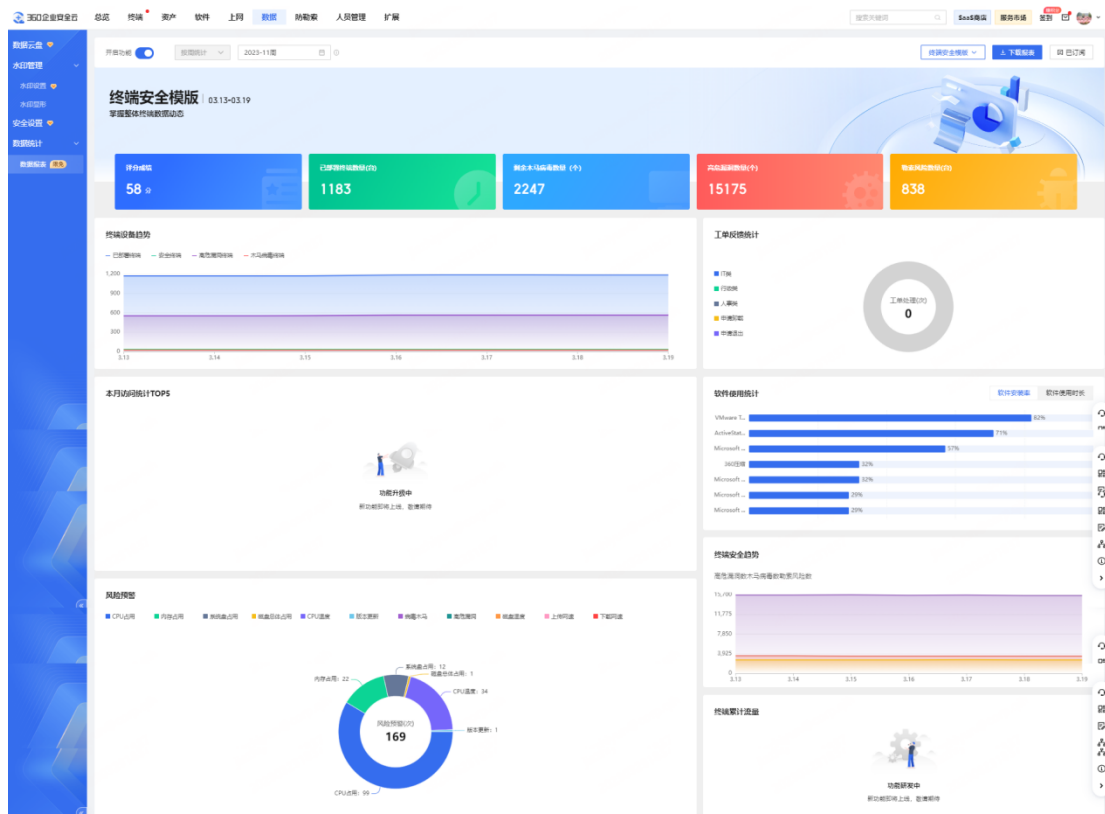
➤ 通用模板，各方面数据均衡展示，掌握整体终端数据动态



➤ 资产风险模板，展示全局终端软件、硬件资产数据动态



➤ 终端安全模板，侧重终端风险监控数据统计



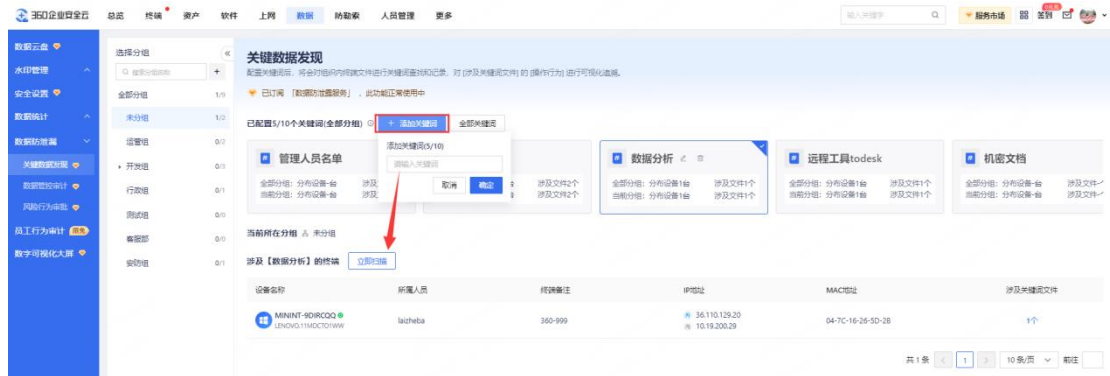
2.5.5 数据防泄漏（需单独付费）

该功能需要对终端进行授权分配后，策略才可生效。



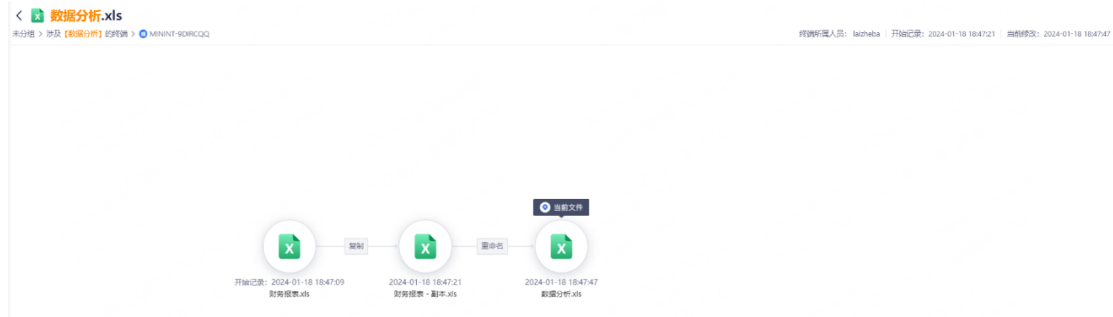
2.5.5.1 关键数据发现

- 管理员可配置需要关注的关键词，配置后，点击【立即扫描】可对企业团队内终端上的文件进行关键词查找和记录。



- 扫描完成后，对【涉及关键词文件】的【操作行为】可进行可视化追溯。





2.5.5.2 数据管控审计

- 可对全组或子分组设置终端数据管控审计策略（日志追踪策略、行为管控策略）



- a. 日志追踪策略开启后，需选择追踪的本地目录范围，全盘目录或自定义目录；追踪是否排除 PE 文件类型如.exe、.dll、.sys；选择需要追踪的操作行为，勾选后将会对选中的操作行为进行管控和记录。

当前所在分组 品 全部分组

日志追踪策略 ① ☒ 已开启

1.选择需要追踪的本地目录范围

- ☒ 全盘目录 更全面
- ☐ 自定义目录 推荐

2.是否排除PE文件类型

☐ 排除PE文件(.exe .dll .sys等) ①

3.选择需追踪的操作行为 ① 需选中全部【管控必需】项，才能开启下面【行为管控策略】

- | | |
|--|---|
| ☒ 文件创建 管控必需 | ☒ 文件重命名 管控必需 |
| ☒ 文件编辑 管控必需 | ☒ 文件恢复 管控必需 |
| ☒ 文件删除 管控必需 | ☐ Web脚本写入(全盘目录) |
| ☒ 文件复制 管控必需 | ☐ 快捷方式写入(全盘目录) |
| ☒ 文件移动 管控必需 | ☐ 关键启动项文件更改(全盘目录) |
| ☒ 文件读取 | |

- b. 行为管理策略开启，即可设置关键词管控策略，配置好需要关注的关键词后，选择需要记录的文件外发行为，如通过即时通信软件外发、通过网络协议外发、外部设备外发或其他风险行为外发。

行为管控策略 ① ☒ 已开启

1.关键词管控策略 ①

关键词分类 ①	关键词 ①	告警提醒	行为阻断
核心文件	数据分析 × +	☒	☒ ☒ 需审批 ☐ 操作者自行确认
机密	财务报表 × +	☒	☒ ☒ 需审批 ☐ 操作者自行确认
重要	远程工具toodesk × +	☒	☒ ☒ 需审批 ☐ 操作者自行确认
其他文件			

2. 请选择需记录的外发行为 ①

① 通过即时通信软件外发

- ☒ 将文件通过QQ外发
- ☒ 将文件通过微信外发
- ☐ 将文件通过钉钉外发
- ☐ 将文件通过飞书外发
- ☐ 将文件通过百度网盘外发
- ☐ 将文件通过腾讯微云外发
- ☐ 将文件通过天翼云盘外发
- ☐ 将文件通过阿里云盘外发
- ☐ 将文件通过移动云盘外发

② 通过网络协议外发文件

- ☐ HTTP ☐ SMTP
- ☐ HTTPS ☐ SMTPS
- ☐ FTP

③ 通过外部设备外发文件

- ☒ 将文件拷贝至移动存储设备
- ☒ 将文件进行打印
- ☒ 将文件通过蓝牙外发

④ 通过其他风险行为外发文件

- ☒ 将文件通过网络共享
- ☐ 将文件通过拖拽外发
- ☒ 将文件通过剪贴板外发

全部应用

取消

⚠ 当前有未应用设置

- c. 以上策略设置完毕后点击【全部应用】按钮，策略即可生效，终端设备再操作含有关键词的文件时会有如下图提示，如是必要操作，可提交申请解除限制。

⚠ 该文件为受控文件，如需外发请提交申请**财务报表.xls**

文件路径: C:\Users\Administrator\Downloads

MD5: 1d9c66df97467dd63cf5f7a7c0131e65

**通过拖拽外发**

需要发送领导查阅，请解除限制

取消操作

提交申请

- 支持搜索查看某台终端设备上的文件审计详情, 点击设备名称即可跳转查看文件操作审计。

The screenshot displays the '文件操作审计详情' (File Operation Audit Details) page. At the top, there's a search bar with filters for '全部状态', '全部系统', '全部类型', and a search input '360-999'. Below this is a table listing devices. The first device, 'MININT-90RCQQ', is highlighted with a red arrow. The main content area shows the audit details for this device, including a summary of file operations and a detailed log table. The log table has columns for '时间', '文件名', '文件类型', '涉及关联文件', '文件大小', 'MD5', '原文件路径', '文件操作', '执行进程', '执行主体', and '操作'. A red arrow points to the '涉及关联文件' column, and another points to the '操作' column. The '操作' column contains links like '详情' (Details) for each entry.

时间	文件名	文件类型	涉及关联文件	文件大小	MD5	原文件路径	文件操作	执行进程	执行主体	操作
2024-01-19 11:42:45.588	进程工具.exe	.exe	全部文件	5.60MB	0db448c797b8b96fe13a8...	C:\Users\Administrator\Downloa...	删除操作 (已取消)	explorer.exe	-	详情
2024-01-19 11:42:43.668	进程工具.exe	.exe	涉及关联文件	5.60MB	0db448c797b8b96fe13a8...	C:\Users\Administrator\Downloa...	删除	explorer.exe	-	详情
2024-01-19 11:42:43.667	进程工具.exe	.exe	普通文件	5.60MB	0db448c797b8b96fe13a8...	C:\Users\Administrator\Downloa...	删除	explorer.exe	-	详情
2024-01-19 19:41:16.128	数据报告.xls	.xls	涉及关联文件	4.27KB	1d9c66df7467d563c5f7a...	C:\Users\Administrator\Downloa...	删除操作 (已取消)	explorer.exe	-	详情
2024-01-19 19:32:04.393	数据报告.xls	.xls	涉及关联文件	4.27KB	1d9c66df7467d563c5f7a...	C:\Users\Administrator\Downloa...	删除操作 (已取消)	explorer.exe	-	详情
2024-01-19 19:31:02.075	数据报告.xls	.xls	涉及关联文件	4.27KB	1d9c66df7467d563c5f7a...	C:\Users\Administrator\Downloa...	删除操作 (已取消)	explorer.exe	-	详情
2024-01-19 18:47:49.344	数据报告.xls	.xls	涉及关联文件	4.27KB	1d9c66df7467d563c5f7a...	C:\Users\Administrator\Downloa...	删除	cgcontrol.exe	DLP	详情
2024-01-19 18:47:49.339	数据报告.xls	.xls	涉及关联文件	4.27KB	1d9c66df7467d563c5f7a...	C:\Users\Administrator\Downloa...	删除	cgcontrol.exe	DLP	详情
2024-01-19 18:47:49.337	数据报告.xls	.xls	涉及关联文件	4.27KB	1d9c66df7467d563c5f7a...	C:\Users\Administrator\Downloa...	删除	cgcontrol.exe	DLP	详情

- 团队通用云存储空间为 1G, 用于产品各项功能数据存储, 如文件分发、日志保存等。

文件操作审计日志数据量比较大, 可免费查看或下载最近 7 天的日志, 如需长时间保存或永久保存, 可订阅数据云盘服务, 保证审计日志存储无忧。

The screenshot displays the '数据管控审计' (Data Management Audit) page. It shows a summary of data management audit results, including a bar chart and a table. A red arrow points to the '数据管控审计结果' (Data Management Audit Results) section, which shows a total of 1875.23 MB and 9.08 GB. Another red arrow points to the '数据云盘' (Data Cloud) section, which shows a total of 0 GB. The page also includes a table listing devices, with the first device, 'MININT-90RCQQ', highlighted. The table has columns for '设备名称', '所属人员', '设备状态', '设备类型', '设备IP', 'Mac地址', '备注', '登记信息', and '今日新增日志'.

设备名称	所属人员	设备状态	设备类型	设备IP	Mac地址	备注	登记信息	今日新增日志
MININT-90RCQQ	laizheba	在线	台式机	36.110.129.20	04-7C-16-26-5D-28	360-999	360-999	2280216

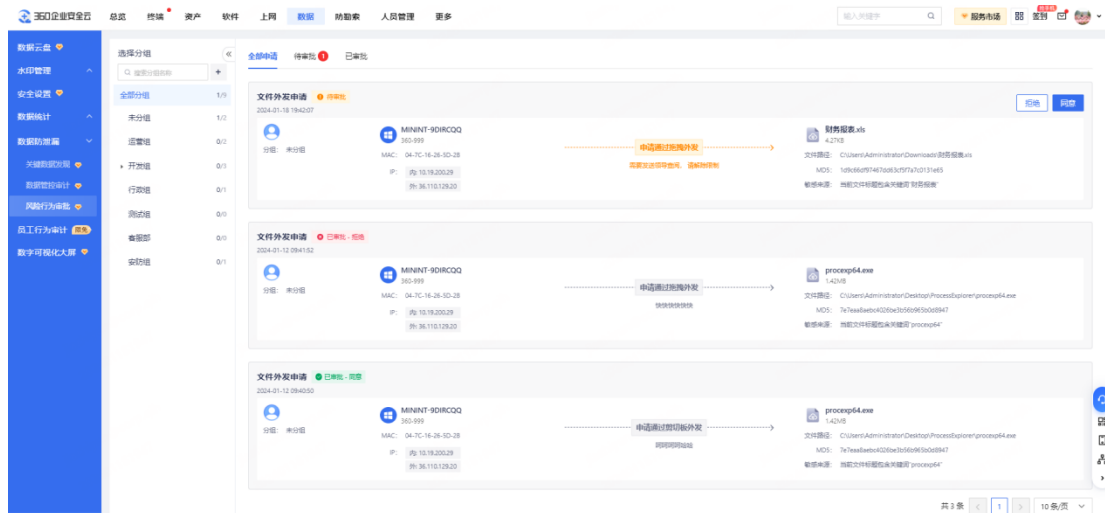


2.5.5.3 风险行为审批

- 如上所述，终端用户提交外发申请后，管理员可在控制台查看和审批，如果同意外发，可选择外发有效期限和可外发次数。



- 同时可以查看所有的审批记录。



2.5.6 数字可视化大屏（需单独付费）

360 数字可视化大屏，是使用图表、二维、三维动效等形象可视化方式，将企业庞杂的安全数据生动的呈现出来，旨在将企业终端安全数据通过直观、炫酷、震撼的视觉画面展现，满足企业安全状况监控、安全风险预警、数据安全成果展示等多种业务需求。

可以在控制台【数据】-【数字可视化大屏】功能页面预览可视化大屏风格样式，或联系官方客服了解更多产品详细信息。



2.6 防勒索（专业安全管理运维服务）

2.6.1 勒索防护

管理员可查看终端的远程登录服务端口状态,文档防护状态,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。



2.6.2 远程接入策略

可设置远程拦截 IP 的类型,支持拦截风险 ip 访问、境外 ip、FTP 风险 IP、FTP 境外 IP 访问,以及允许远程的时间段,如果特殊远程登录需求也可以设置登录白名单(支持 IP 段)。



设置白名单



① 支持IP段，例如 172.12.34.1 ~ 172.12.34.126 可以用IP段 172.12.34.0/25 表示。

终端 casbrain-worker-19 将放行以下IP的远程链接

添加白名单

选择协议



输入IP，多个用英文“;”分隔，如192.168.2.1;192.168.2.1

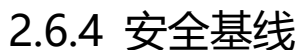


取消

确定

2.6.3 勒索风险及日志

针对团队内终端的攻击拦截信息、弱口令的账号和软件进行显示

[illegible]

可针对敏感项目多维度开启防护，避免远程操纵代理的信息泄露等损失。



2.6.5 勒索病毒解密

基于勒索病毒搜索引擎，支持检索超过 800 种常见勒索病毒，如果您遇到了勒索，可以先行到这里查询是否已经支持解密。



2.7 人员管理

2.7.1 组织机构

管理您组织的人员分组结构，可以手动配置也可从第三方平台同步（仅支持钉钉）



2.7.2 企业登录配置

通过企业身份源的配置，公司员工可以使用企业身份源（钉钉）登录系统



2.7.3 应用访问控制

企业对组织和人员进行应用访问权限管理，用户通过统一身份验证可直接登录各个应用

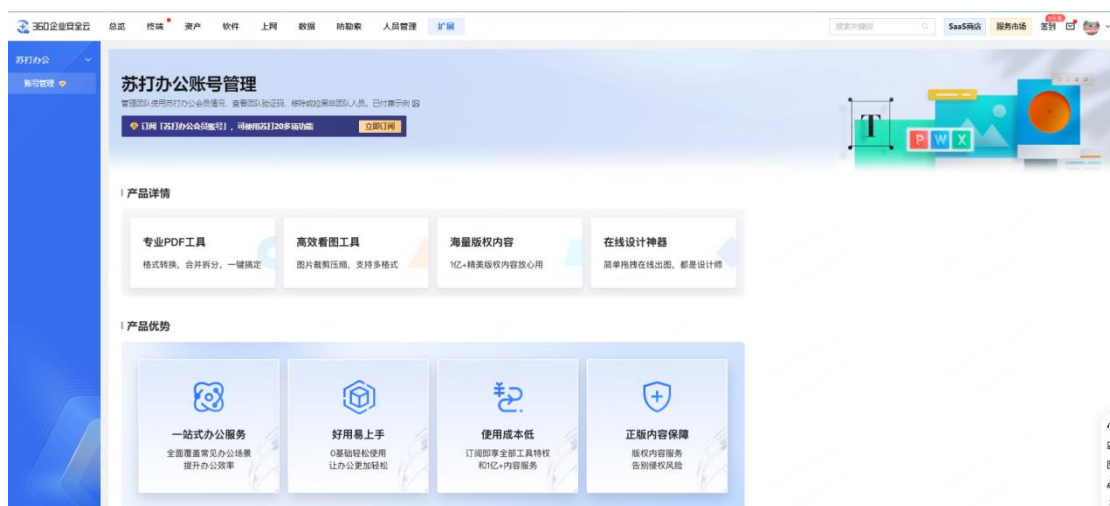


2.8 扩展（需单独付费）

2.8.1 苏打办公账号管理

苏打办公是一款主打简约、高效的办公平台，含 1 亿+ 版权内容服务、PDF 工具集，看图

功能。（具体购买事宜请联系官网在线客服）



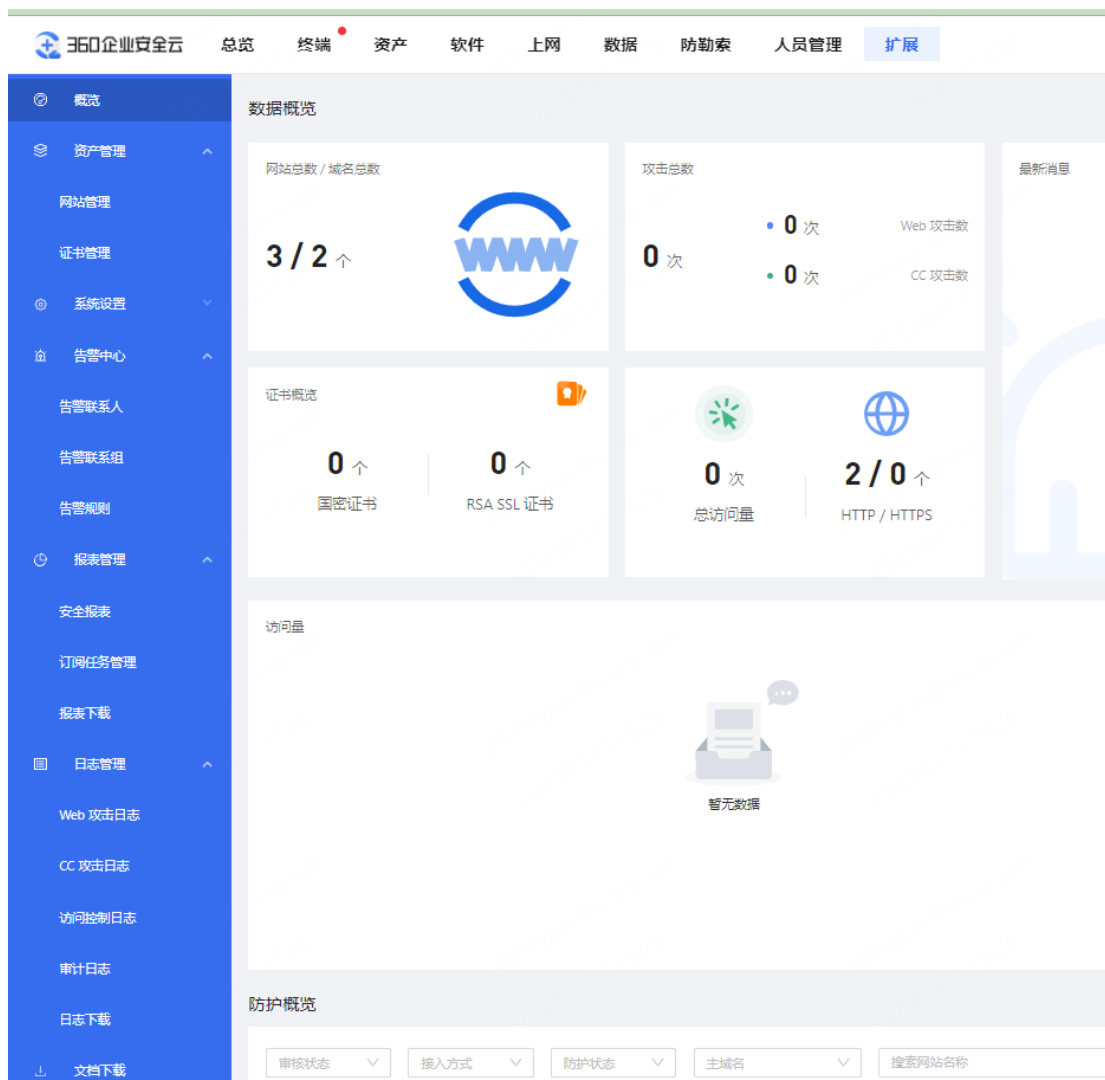
购买此服务后，管理员可以在管理后台管理团队使用苏打办公的会员情况，查看团队验证码，

移除或拉黑非团队人员。



2.8.2 Web 应用防火墙

Web 应用防火墙安全防护系统旨在解决用户网站安全问题，为用户提供一套集合 Web 应用防护、DDoS 攻击防护、CC 攻击防护、访问控制、日志管理、报表管理等功能以及统一管理配置的多合一的网站安全解决方案。（具体购买事宜请联系官网在线客服）



2.8.3 安全运营托管服务

继探针、管理工具平台 SaaS 化后，360 将世界领先的安全大数据、威胁情报，与安全专家服务能力云化，为广大客户提供即点即用的安全托管运营服务，可与企业内 IT 运维人员紧密合作，形成“云地一体”的技术小组，打造最优守护屏障。[更多产品详细信息请联系官方客服人员了解](#)



360安全运营托管服务

继探针、管理工具平台SaaS化后，360将世界领先的安全大数据、威胁情报，与安全专家服务能力云化。为广大客户提供即点即用的安全托管运营服务，可与企业内IT运维人员紧密合作，形成云地一体的技术小组。



探针即服务

功能全面强大的安全探针能力，采集各场景基础安全数据

平台、工具即服务

管控能力云化部署，无需本地硬件，即装即用

数据、情报、知识即服务

海量安全大数据与威胁情报，动态防御未雨绸缪

专家、能力即服务

超3000名安全专家，赋能企业组成云地一体专业运维小组

产品优势



服务模式创新

SaaS化软件工具与专家服务紧密结合



客户体验突破

形成云地一体运维小组，体验专业IT团队支持



能力边界升级

360矩阵化产品+原生研发专家包围性支持



商业模式颠覆

按能力场景交付，不再担心工具买了不会用，用不好

2.9 服务市场

服务市场页面将展示目前支持企业可订阅的功能与服务

总览 终端 资产 行为 数据 威胁情报 人员管理 更多

服务市场

安全运营服务 云存储与网络服务 数据可视化服务 其它服务

安全运营服务

专业安全管理运维服务(免费版)

包含专业专用的运维管理和安全防护服务，满足企业日常需求，支持公共网络付款，可开展企业网络运营，专业发展。

¥80 原价:¥99/月/年 (优惠价)

立即订购

专业安全管理运维服务(免费版)

可任意：功能服务自由组合订阅，满足企业个性化需求，降低订阅成本，支持公共。

¥40 原价:¥99/月/年 (优惠价)

立即订购

360安全运营托管服务

将专业安全运营能力和领先的企业安全管理能力服务化，形成“云地一体”专家小组。

限时免费

查看详情

零信任安全访问服务

通过精细访问控制和丰富的动态决策能力，为客户提供安全可靠的网络运营流程。

¥15.9 原价:¥99/月/年 (优惠价)

立即订购

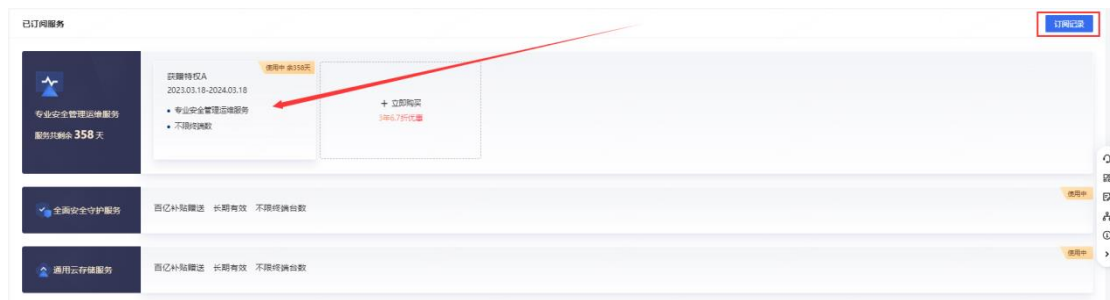
行为管控审计服务

对设备操作、软件使用、网络访问行为进行日志审计与规范性稽核，全面提升设备。

¥160 原价/年 (优惠价)

立即订购

在此页面可查看订阅记录及订单详情。



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功能列表。

2.10 页眉功能导航

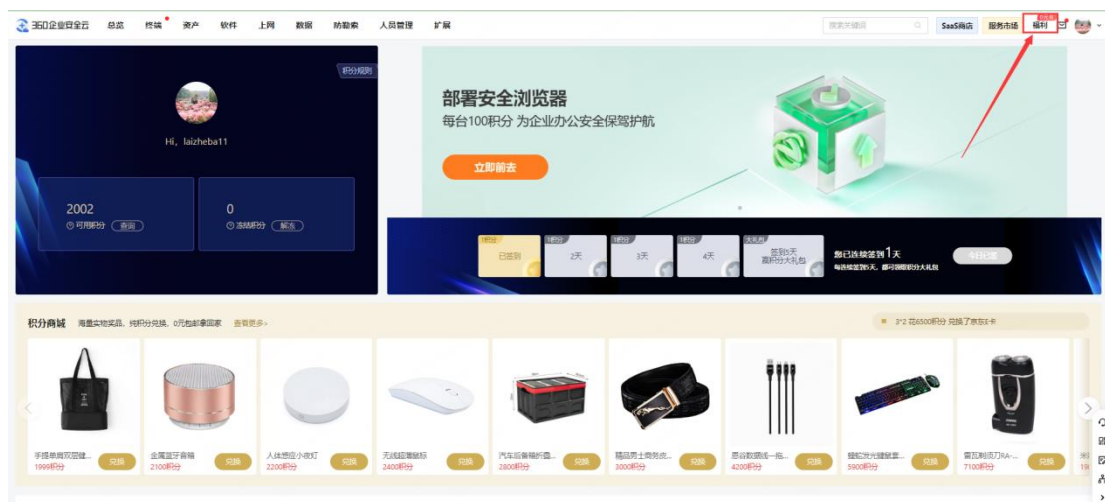
2.10.1 关键字搜索

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。

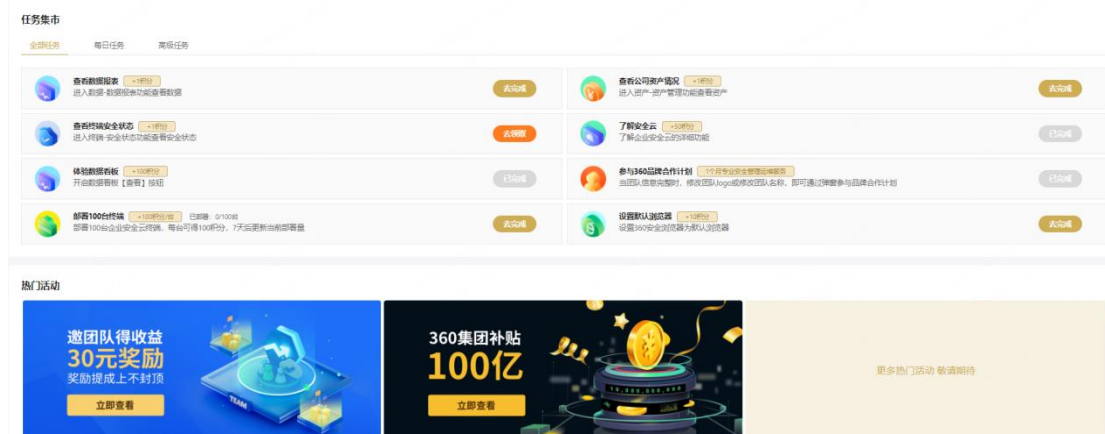


2.10.2 福利中心

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。



参与任务集市和热门活动可以领取积分



2.10.3 SaaS 商店

360SaaS 商店 (<https://store.saas.360.cn/>) 作为企业用户与 SaaS 服务的高效连接器,

帮助企业全面实现数字化, 共建 SaaS 生态。



2.10.4 站内信

2.10.4.1 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。



2.10.4.2 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，数据存储空间为 15 天。



2.10.5 设置

2.10.5.1 账户中心

可对当前登录的团队管理员账号进行设置，支持修改昵称、修改登录密码、修改手机号码、注销账号。





2.10.5.2 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。

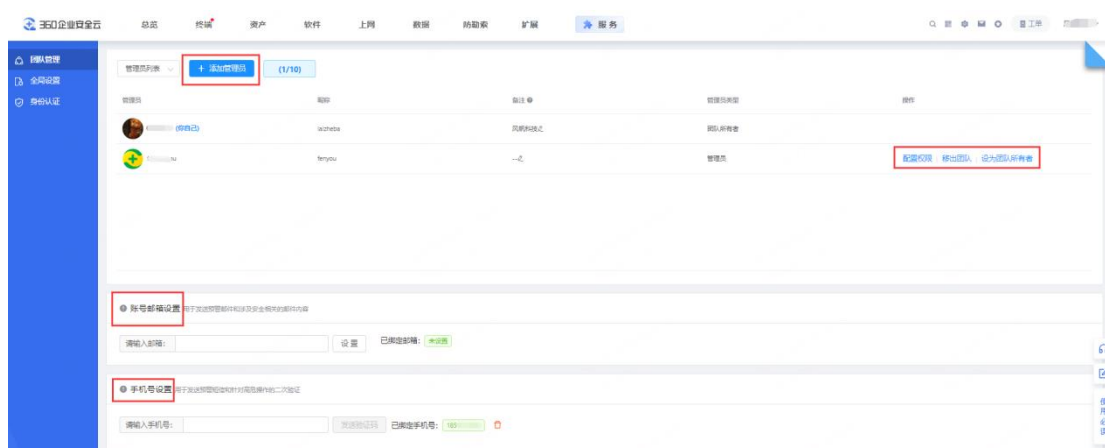


2.10.5.3 团队管理（部分专业安全管理运维服务）

➤ 团队账号管理

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。

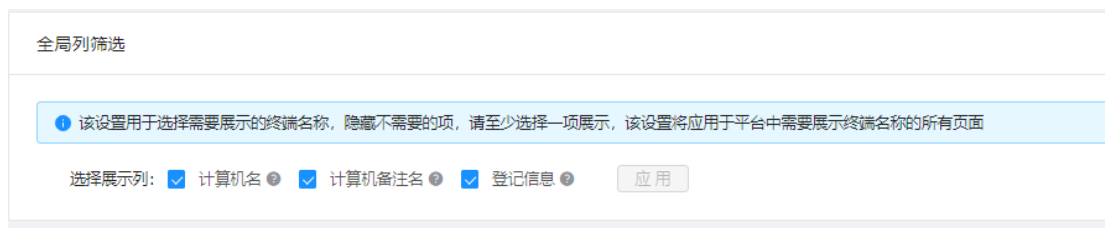
➤ 支持团队所有者给管理员分配不同的管理权限（专业安全管理运维服务）



➤ 全局设置

1) 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



2) 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。

通知推送设置

位置: 右下角 | 模式: 默认 | 全局修改通知停留时间 | 重置通知停留时间

平台为您提供全方位的终端信息推送, 方便您第一时间掌握终端现状以及时的安全管理需要。通知均可关闭, 可按需设置。

通知类型	类型描述	通知停留时间	消息推送通知	通知显示	操作
终端上下线通知	默认显示结束, 计算机由(未)注册/注销	30秒	☐	☐	☒ 已开启
任务完成通知	任务执行完成后, 进行通知, 漏洞任务、分信策略除外。	30秒	☐	☐	☒ 已开启
终端加入通知	当前新增终端加入网络或已有终端离开网络时, 进行通知。	30秒	☐	☐	☒ 已开启
站内信通知	当收到站内信时, 进行通知。	30秒	☐	☐	☒ 已开启
终端状态汇总通知	终端状态汇总通知, 一天一次。	30秒	☐	☐	☒ 已开启
策略状态汇总通知	策略状态汇总通知, 一天一次。	30秒	☐	☐	☒ 已开启
漏洞状态汇总通知	漏洞状态汇总通知, 一天一次。	30秒	☐	☐	☒ 已开启
杀毒状态汇总通知	杀毒状态汇总通知, 一天一次。	30秒	☐	☐	☒ 已开启
发票策略通知	当提交发票内容审核通过时, 进行通知。	30秒	☐	☐	☒ 已开启
工单提醒通知	当提交工单任务被审核处理时, 进行通知。	30秒	☐	☐	☒ 已开启
外设策略通知	当外设策略审核通过后, 外部设备策略审核, 进行通知。	30秒	☐	☐	☒ 已开启

3) 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。

登录安全设置

开启本开关时, 账号登录有效期将更短, 从而获得更高的安全性

登录有效期控制: ☒

4) 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。

终端密码策略设置

切换为动态密码后, 卸载和退出时, 变更周期, 设置范围为60秒~3600秒

☐ 静态密码 ☒ 动态密码 变更周期 1200秒

5) 终端时间同步（专业安全管理运维服务）

可自定义设置终端电脑的系统时间同步频率，避免终端系统时间错误。



➤ 身份认证

购买付费服务需进行个人身份认证，开具产品授权声明、付费后开具增值税专用发票需要通过企业认证。

购买付费服务、开具产品授权声明需要进行身份认证

① 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，仅能开具个人抬头发票。



2.10.5.4 工单管理

➤ 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“工单管理-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。

工单

— 自助解决 —

您可以先尝试通过 [常见问题](#) 或 [智能客服](#) 解决您的问题。

若仍无法解决, 请填写下方表单提交您的反馈。

— 提交工单 —

* 反馈类别 ☐ 问题 ☐ 建议 ☐ 咨询 ☐ 其他 ☐ 注销

联网模式 ☒ 请选择涉及终端的联网模式

问题类别

终端名称

* 问题描述 0/200

* 手机号

问题截图 未选择任何文件

➤ 历史工单

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

来源路径	工单编号	工单内容	工单类型	工单状态	提交时间	工单状态	评价	操作
-	210630005235960053	虚拟机分情况情况下	咨询	-	2021-06-30 09:52:55	已关闭	已解决	查看
-	21061214231487424	请问什么时候可以支持病毒扫描过防火墙?	咨询	-	2021-06-12 14:22:31	已回复	未评价	回复
-	210620005917162076	病毒分类里漏掉失败的不能查杀病毒查杀病毒都失败了	问题	处理	2021-06-29 09:59:17	已回复	未评价	回复
-	200920185011668a66	建议增加一键刷机软件, 和软件白名单功能	建议	-	2020-09-28 18:50:11	已回复	未评价	回复
-	2009271438027fba06	建议支持本地文件上传分享到网盘	问题	管理	2020-09-27 14:28:02	已回复	未评价	回复
-	2009221609490a1b2e	建议支持本地安装软件上传分享	建议	-	2020-09-22 16:09:49	已回复	未评价	回复
-	20092215094274b134	官网这里坏了	问题	-	2020-09-22 15:09:42	已回复	未评价	回复

共有 7 条数据 < 1 > 10 条/页

2.10.5.5 左导航偏好设置

左侧导航栏颜色偏好设置，支持深色模式、浅色模式，默认为蓝色模式。





2.10.5.6 退出登录

退出登录即退出 360 企业安全云管理后台的登录状态，退出后回到登录页面，需再次登录查看团队情况。

3、客户端主要功能简介

3.1 首页体检

体检为电脑进行病毒木马、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。



首页左上角显示企业团队名称与 logo，鼠标停留在 logo 上即可显示信息卡片，包括企业管理员信息及电脑基本信息。



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 优化加速

清理电脑垃圾，全面优化电脑性能，轻装运行。



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 软件管家

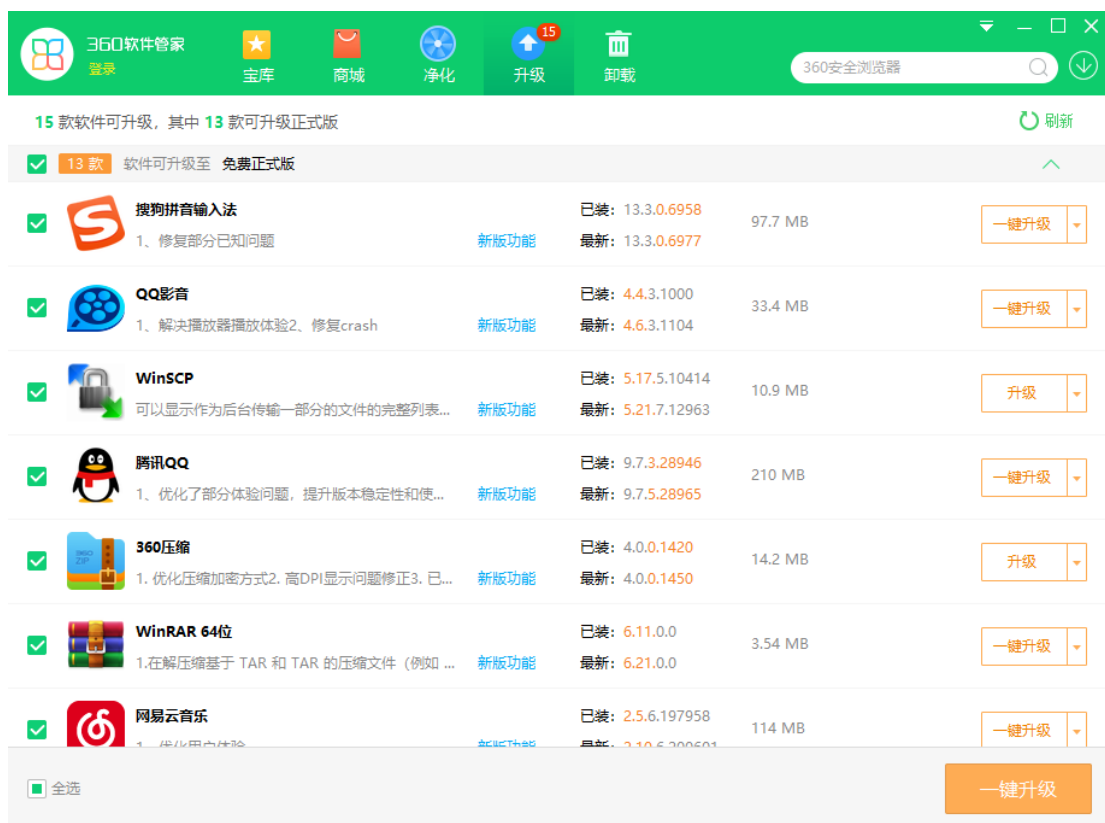
软件管家为用户提供海量的正版软件的高速安全下载服务。

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。

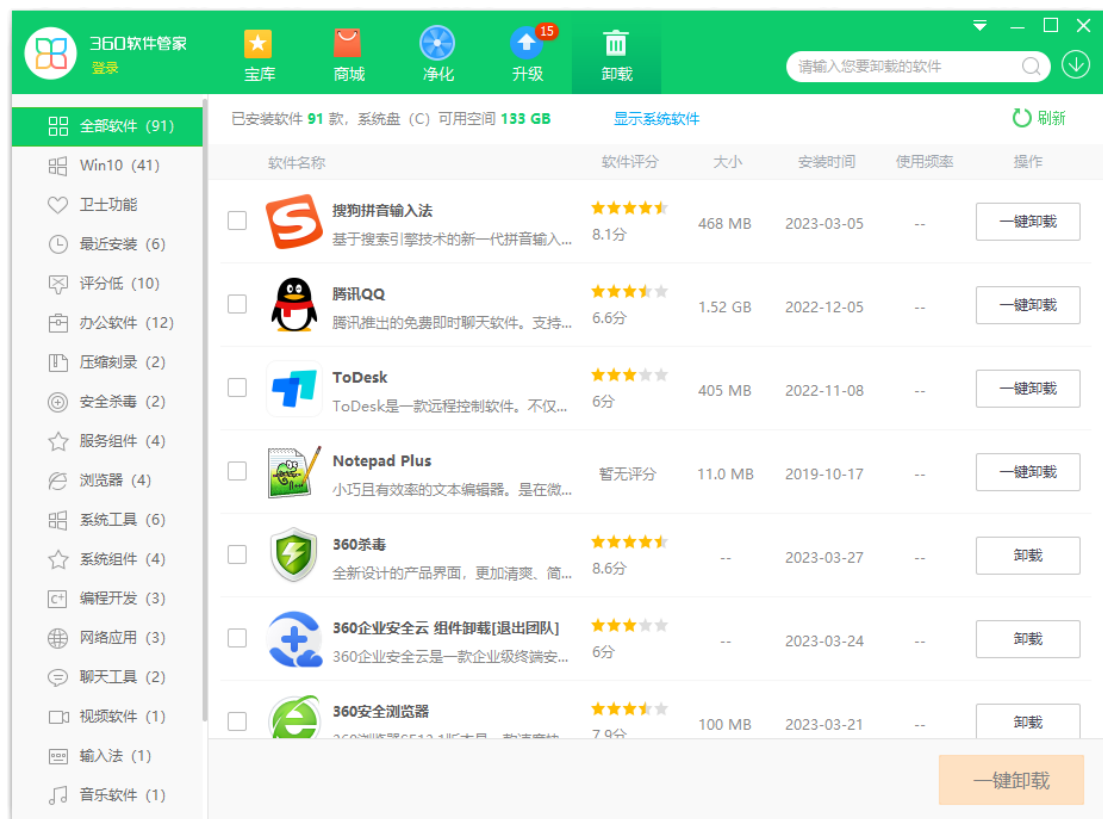


点击软件管家主界面上的“升级”界面，可为用户提供可升级软件的详细更新信息，用户可

点击“一键升级”对软件进行升级。

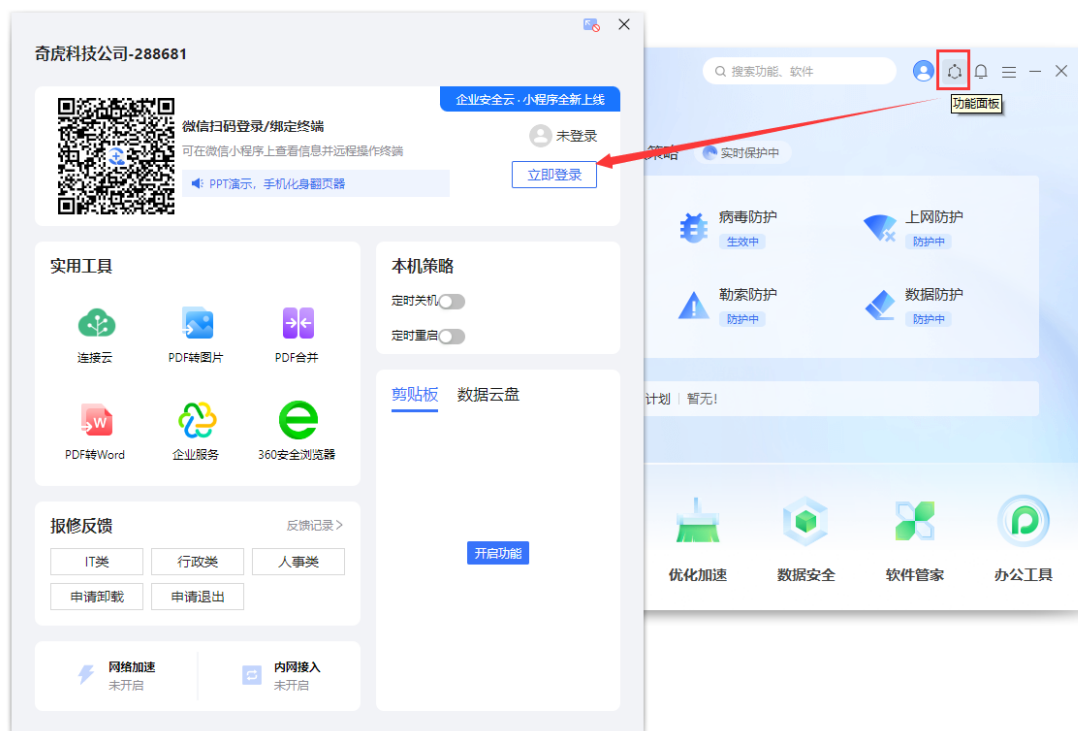


点击软件管家主界面上的“卸载”界面,用户可以通过左侧分类导航或者搜索功能快速定位到需要卸载的软件,点击“一键卸载”即可卸载。



3.7 功能面板

终端用户可以扫描二维码绑定小程序,通过手机小程序对终端进行报修反馈、关机、重启等操作。管理员可在管理后台【小程序功能】页面对终端用户是否可以使用面板功能进行管控。



4、客户端退出、卸载

4.1 退出

已加入企业组织的终端，如果想临时退出，需要输入退出密码，密码请联系管理员获取。



输入正确的退出密码后，可进入正常退出的流程。

 360企业安全云 反馈 ×

想工作免打扰或玩游戏，可尝试以下模式

☒ 暂时退出 1小时 ▾
在此期间内您的电脑将不受保护

☐ 游戏模式
玩游戏时，自动处理风险，不再弹窗（仅本次有效）

☐ 免打扰模式
处理风险，减少弹窗打扰，兼顾安全和娱乐（仅本次有效）

☐ 退出企业安全云
退出企业安全云，停止对电脑保护

[添加误报软件](#) 取消 确定

4.2 卸载

- 已加入企业团队的终端，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



- 或者点击去申请，提交申请卸载的理由



- 管理员在控制台审批通过后，即可进入正常的卸载流程。

