H.4、360企业安全云[适合钓鱼]

2023年10月1日 14:22

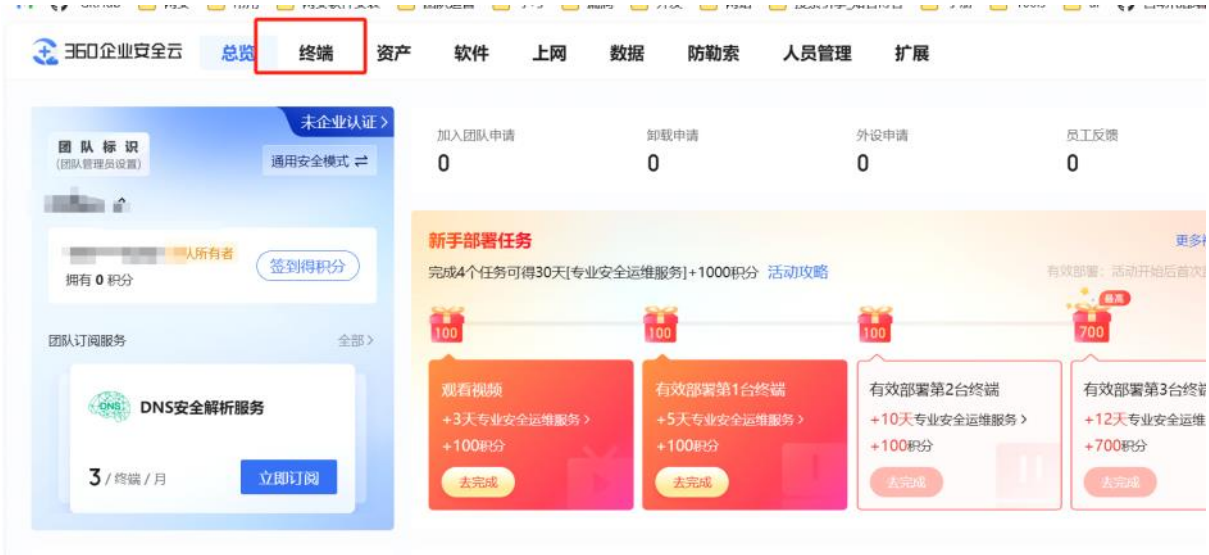
By:弱鸡
笔者微信：vivo50KFCKFC
项目地址：https://github.com/RuoJi6/Deskbypass
博客：https://vlog.taoyuan.cool/
工具链接：
链接：https://pan.baidu.com/s/1XdVkAJU_Q9rD0PMiSDZFKQ?pwd=zdpm
提取码：zdpm
--来自百度网盘超级会员V4的分享

360企业安全云作为新一代数字安全与管理SaaS服务，基于360安全大脑安全能力，依托全面SaaS架构，实现硬件、软件、数据、资产、上网、防勒索等全方位数字安全与管理服务。从管人员、管资产、管数据三大价值层面助力企业数字化管理提效，对人员身份及行为管理、软、硬资产兼管、数据全链路守护等实现了一体化综合统效，全面赋能企业数字化转型。

地址：https://saas.360.cn/

步骤一：选择部署方式

1. 选择部署方式，创建部署连接



这里提供三种安装方式：

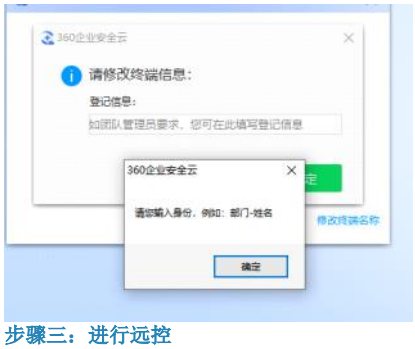
- 手动下载安装：该方式需管理员自己下载好客户端安装包，并在需要安装客户端的主机上运行。
- 员工自主下载：该方式需要客户端用户自行下载客户端，并安装，需管理员提供下载链接，通过沟通软件或者邮件发送给所需用户。
- 域控分发：管理员通过AD域环境将安装包分发到终端并执行。在指引中提供了分发方案。
  在攻防场景中，如果去钓鱼的话，建议使用方式一和方式二（而且该平台还贴心提供了邮件信息模版），如果在内网已经有了一定的权限，可使用方式一和方式三进行远控。

该链接是企业专属的下载链接。即按照我创建的链接下载客户端，安装后会加入到我的企业管理后台，被我远控。（hvv钓鱼那个事就是这个方式）

或者12.0及以上版本卫士主界面右上角三条横杠菜单 > 加入团队 > 输入pin码

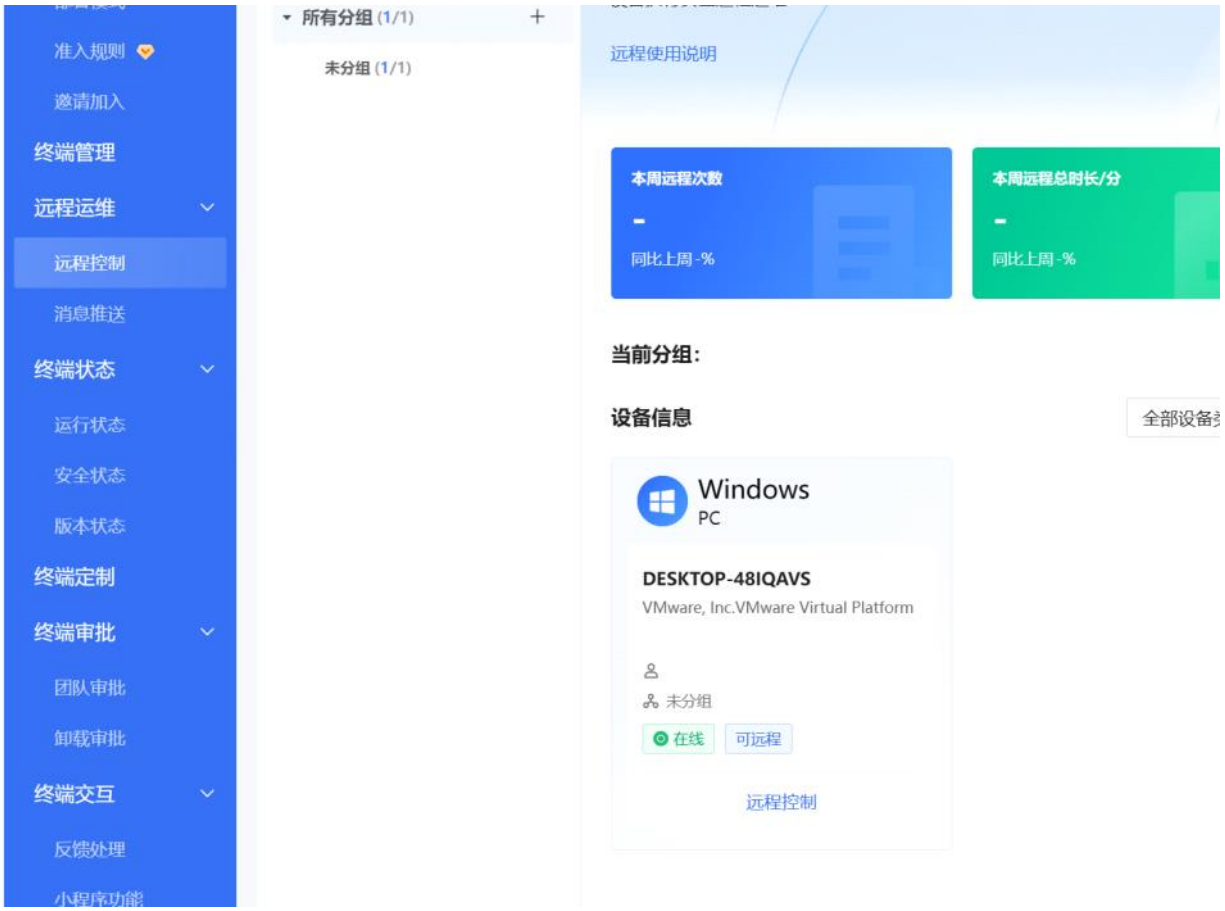
邮件模板【这个下载之后，需要手动安装才行】

而且按照之后，需要输入这个



步骤三：进行远控

安装完成后，在远程运维-远程控制，可进行远控，如下图



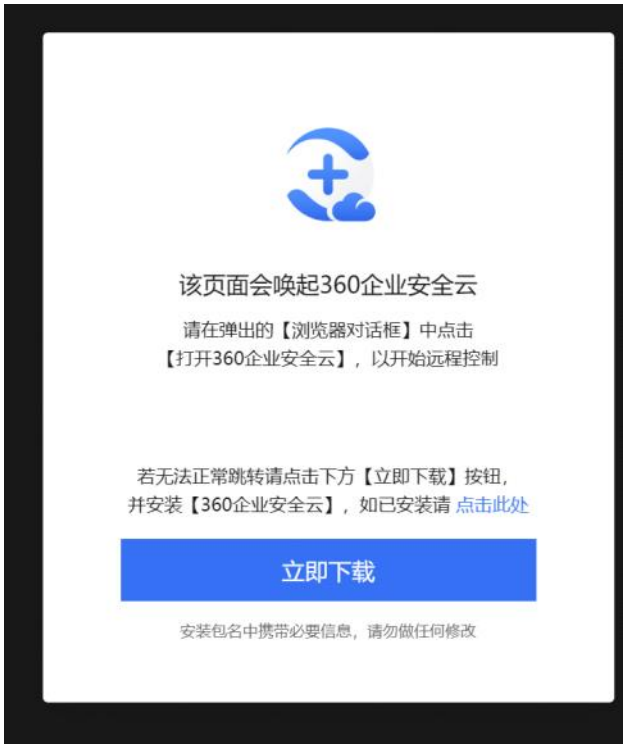
而且需要对方同意

这几个需要80一年[在实战的适合，可以买一个]

而且这个三个都需要授权[因为我付了80大元子]

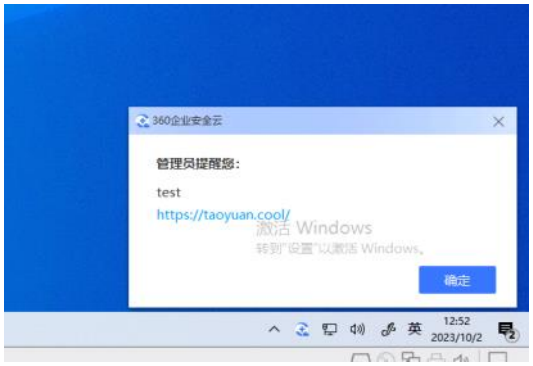
同意之后

而且本机需要安装360企业云



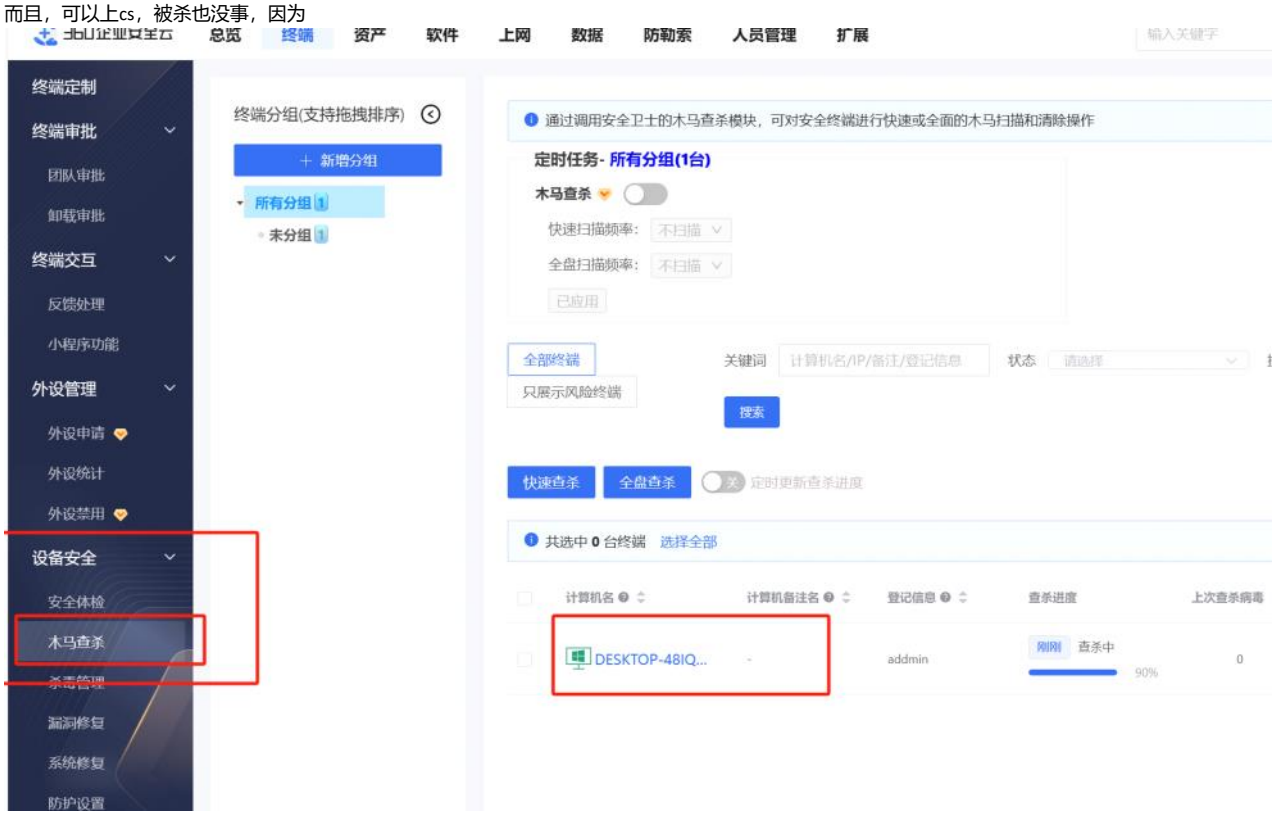
但是可以进行消息推送

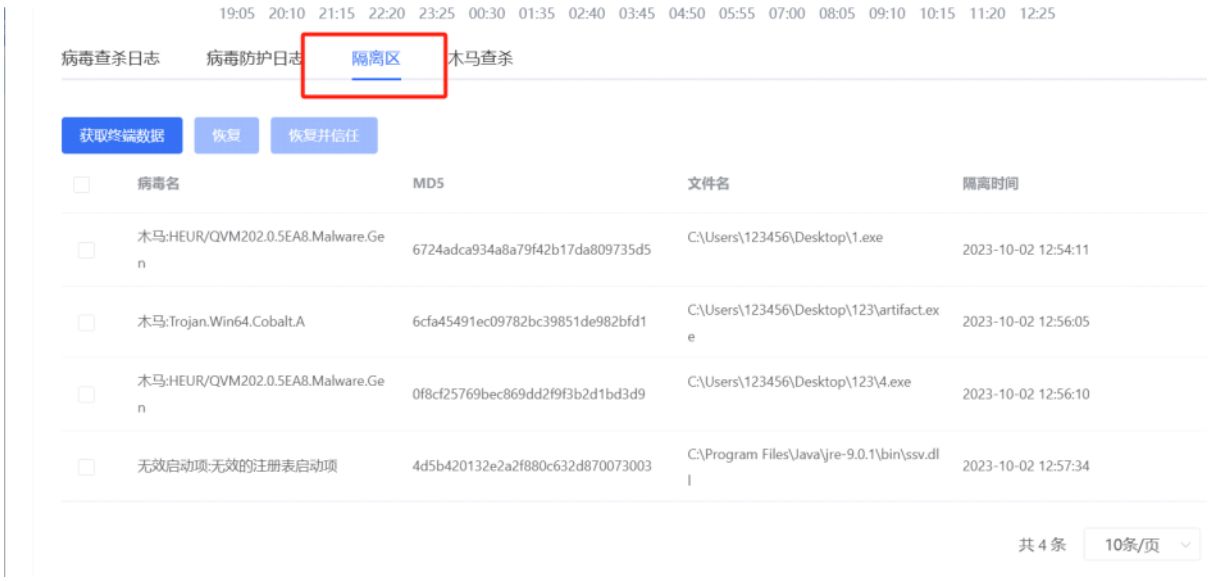
就会出现



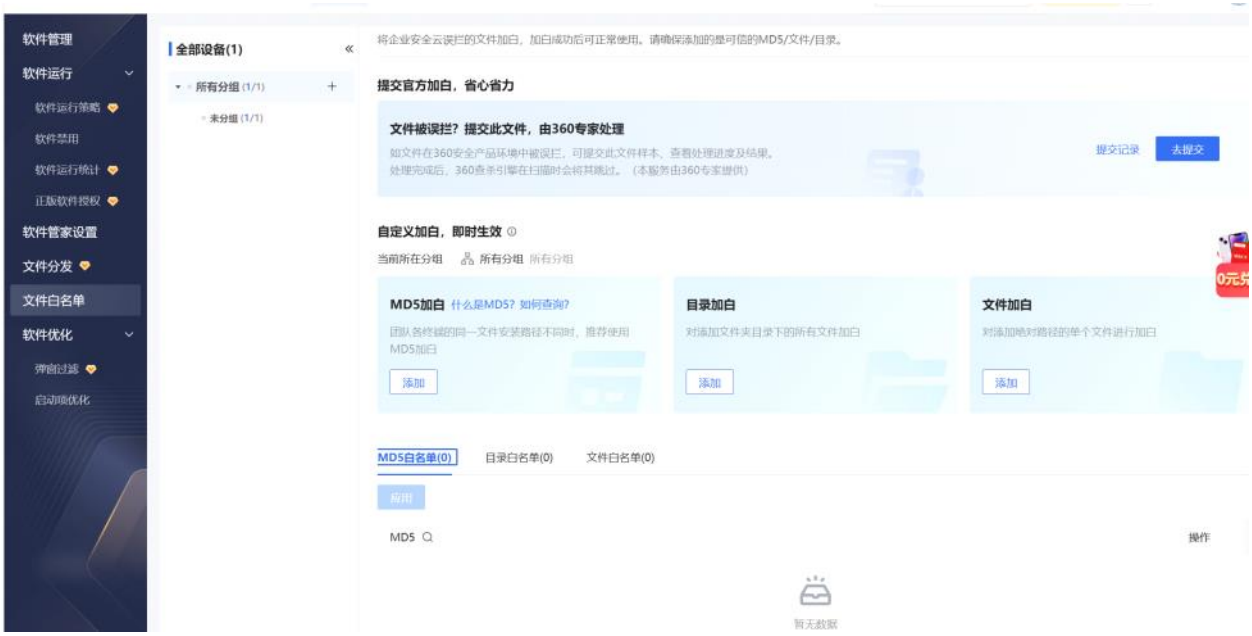
其实我这边建议[可以在自己电脑安装一共，相比卡巴，这个杀毒没有广告和捆绑，而且80一年，功能多，实时更新漏洞防护]

而且，可以上cs，被杀也没事，因为





但是恢复并信任不了{不知道为什么，但是可以使用下面这个}，但是可以恢复配合下面使用



而且上传一个木马，点击分发

[但是这个需要你的企业认证才行]


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)
ccc.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
有效时间
一周
指定时间
分发
取消