深信服终端安全管理系统 EDR

用户手册

产品版本 3.5.26

文档版本 01

发布日期 2022-5-25

深信服科技股份有限公司

版权声明

特别提示

您购买的产品、服务或特性等应受深信服科技股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，深信服科技股份有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新，如有变更，恕不另行通知。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保，深信服科技股份有限公司不对本文档中的遗漏、变更及错误所导致的损失和损害承担任何责任。

联系我们

售前咨询热线：400-806-6868

售后服务热线：400-630-6430 （中国大陆）

深信服科技官方网站：www.sangfor.com.cn

7*24小时智能客服，排障咨询好帮手：

https://bbs.sangfor.com.cn/plugin.php?id=common_plug:online&ref=文档

打开微信扫一扫
可在手机端咨询

符号说明

在本文中可能出现下列标志，它们所代表的含义如下。

图形	文字	使用原则
 危险	危险	若用户忽略危险标志，可能会因误操作发生危害人身安全、环境安全等严重后果。
 警告	警告	该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。
 小心	小心	若用户忽略警告标志，可能会因误操作发生严重事故（如损坏设备）或人身伤害。
 注意	注意	提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。。
 说明	说明	对操作内容的描述进行必要的补充和说明。

在本文中会出现图形界面格式，它们所代表的含义如下。

文字描述	代替符号	举例
窗口名、菜单名等	方括号“[ ]”	弹出[新建用户]窗口。
		选择[系统设置/接口配置]。
按钮名、键名	尖括号“< >”	单击<确定>按钮。

目录

1. 产品简介

终端安全管理系统EDR（Endpoint Detection and Response）是深信服公司提供的一套终端安全解决方案，方案由轻量级端点安全软件Agent和管理端组成。管理端支持统一终端资产管理、终端病毒查杀、终端合规检查、微隔离访问控制策略统一管理、可对安全事件一键隔离处置以及热点事件IOC全网威胁定位。Agent支持防病毒功能、入侵防御功能、防火墙隔离功能、数据信息采集上报、一键处置等。

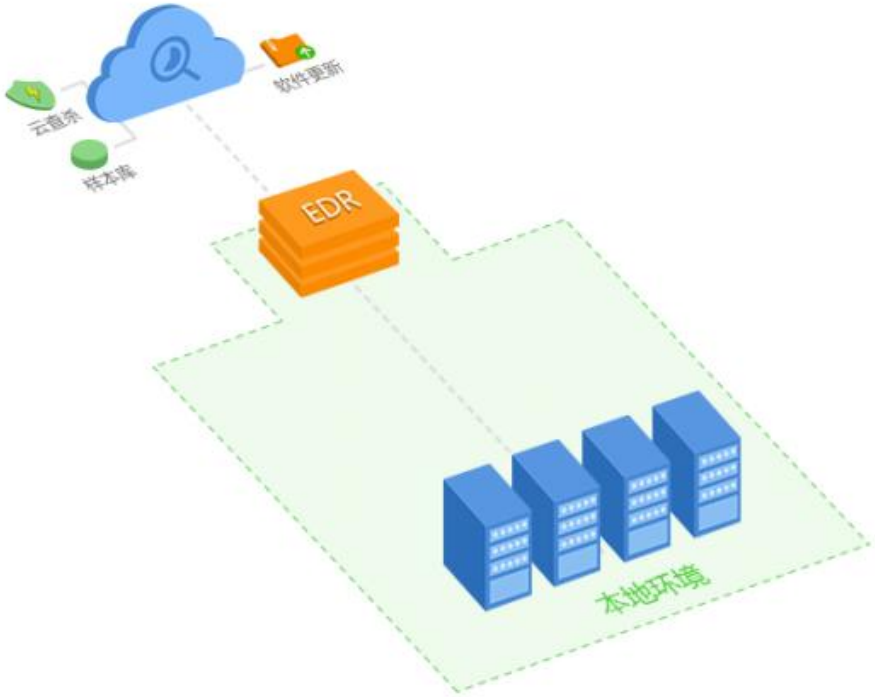
高级威胁检测功能针对热门威胁（勒索病毒、挖矿病毒等）以及采用的新型攻击手法（无文件攻击、白利用等）具备高效准确的检测能力，通过终端行为数据采集（进程操作、网络连接、模块加载、文件操作、注册表修改等），匹配基于ATT&CK框架定义的高级威胁攻击手法的规则，并通过进程链还原威胁攻击事件全貌。

同时也可基于安全攻防知识，使用威胁狩猎功能通过单条件（IP、域名、文件、哈希）或组合多种终端行为数据（网络连接、域名访问、文件操作、进程操作、加载模块、设备信息）检索进行潜伏的高级威胁攻击手法发现跟踪。

同时，终端安全管理系统EDR支持与AC、SIP、AF、SOC、X-central等产品的联动协同响应，形成新一代的安全防护体系。

1.1. 产品概述

终端安全管理系统EDR可部署在用户本地环境。EDR的管理端有软件和硬件两种形态，软件管理端部署在Linux服务器上，硬件管理端旁路接入网络核心，负责集中管理所有Agent；端点安全软件Agent安装在每台终端上。管理端通过公网与深信服安全云联动，内网每台终端Agent与终端安全管理系统联动，实现为本地终端用户提供准确的安全情报和解决方案，通信过程数据加密，部署效果图如下。



1.2. 关键特性

终端资产全面清点

全网终端资产的全面清点，包含业务服务器和用户PC终端资产清点。支持清点每台终端硬件信息、软件信息和资产管理信息等，帮助IT管理员实现对主机资产的“两清一减”：即看清全网主机资产全貌，理清全网主机风险暴露面，从而削减全网主机攻击面。

终端安全合规审查

每一个组织都有自己的终端安全合规要求，尤其是等级保护合规要求、对主机安全要求。终端安全合规审查依据等级保护的主机安全要求进行设计，对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等策略进行合规性审查，满足企业建设等级保护系统的主机安全要求。

勒索病毒实时防御

勒索病毒通过加密文件方式，要求中招者支持一定数额的赎金，这种攻击方式越来越流行，每天都有客户反馈中招。深信服EDR能够非常精准的识别不同的勒索软件家族，并通过专业分析识别出种种勒索病毒感染行为和加密特征，对最新的勒索软件进行有效的查杀，防止用户感染最新勒索软件。

系统漏洞检测与修复

系统存在不同风险等级的漏洞，如果没有及时识别和修复，攻击者很可能利用系统漏洞进入客户内网，对业务造成的影响和损失经常无法估计。EDR能够帮助管理员识别内网终端系统漏洞风险，并进行修复，加强系统安全性。

入侵攻击主动检测

终端主机被入侵攻击，导致感染勒索病毒或者挖矿病毒，其中大部分攻击是通过暴力破解的弱口令攻击产生的。深信服EDR可主动检测暴力破解行为，并对发现攻击行为IP进行封堵响应，同时，针对Web安全攻击行为，则主动检测Web后门的文件。

2. 首次上线

本章节介绍EDR首次上线部署工作，按顺序分别介绍部署准备工作、管理端部署、激活产品、分组管理、策略配置和终端部署。

2.1. 准备工作

2.1.1. 管理端安装环境

管理端有软件管理端和硬件管理端。其中软件管理端支持在真实物理环境及虚拟化环境进行部署，部署服务器需满足以下资源配置要求。

表1 主流场景部署管理端硬件资源要求

终端数	CPU	内存	磁盘
1-300	4 核	4G	200G
300-4500	8 核	16G	1T
4500-10000	12 核	16G	1T

表2 EDR与aTrust联动场景部署管理端硬件资源要求

终端数	CPU	内存	磁盘
1-150	6 核	8G	200G
150-2500	8 核	16G	1T
2500-5000	12 核	16G	1T

2.1.2. 客户端安装环境

EDR客户端Agent支持安装在Windows PC、Windows Server、Linux及MAC OS，操作系统支持详情如下。

表3 各系统及版本信息

系统类别	兼容版本信息
Windows PC	Win XPsp3/Win Vista/Win7/Win8/Win8.1/Win10/win11
Windows Server	WinServer 2003 SP2 WinServer 2008

	WinServer 2008R2 WinServer 2012 WinServer 2012R2 WinServer 2016 WinServer 2019
Linux	CentOS 5.x/6.x/7.x/8.x Ubuntu 10.x/11.x/12.x/13.x/14.x/16.x/17.x/18.x/20 Debian 6.x/7.x/8.x/9.x RHEL 5.x/6.x/7.x/8.x SUSE 11/12/15 Oracle Linux 5.x/6.x/7.x
MAC	Mac OS 12 Mac OS 11.x Mac OS 10.13 Mac OS 10.14 Mac OS 10.15

2.1.3. 网络连通性要求

为确保EDR各项功能正常使用，需要放行Agent客户端到管理端连通性、以及管理端到云端服务器的连通性，放行端口和服务器地址如下表。

表4 网络连通性要求

源设备	目的设备	协议/端口	端口作用
Agent	管理端	TCP 443	访问控制台端口
		TCP 4430	Agent 组件更新和病毒库更新
		TCP 8083	Agent 和管理端业务通信端口
		TCP 54120	紧急场景，管理端控制 Agent 禁用/启用
		ICMP	连通性探测
源设备	目的设备	需公网连通服务器地址	
管理端	云端服务器	漏洞补丁、ioa 升级	https://upd.sangfor.com.cn
		授权相关	https://auth.sangfor.com.cn
		云查服务器	https://analysis.sangfor.com.cn
		云安全计划	https://clt.sangfor.com.cn
		Ioc 规则升级	intelligence.sangfor.com.cn/
		漏洞补丁、规则、病毒库	http://download.sangfor.com.cn

2.1.4. 收集白名单文件

为了避免病毒查杀可能带来的误报影响，提前收集好信任文件并加入白名单。白名单文件包括确认无毒的业务软件、或者前期使用过其它杀毒产品时梳理的白名单文件。在部署完管理端并完成授权激活后，登录EDR管理端，在[响应中心/自定义IOC]或[响应中心/排除策略]中，添加白名单文件，信任名单中的文件不会进行病毒扫描查杀。

2.2. 管理端部署

EDR管理端有软件管理端和硬件管理端，当前软件管理端是交付主场景，此章节主要介绍软件管理端部署，硬件管理端部署指导参考第3章节安装部署。

软件管理端支持OVA镜像部署和ISO镜像部署，此章节主要以OVA镜像部署为例介绍管理端部署，ISO镜像部署指导参考第3章节安装部署。

OVA镜像部署：适用于VMware、HCI等虚拟化场景；

ISO镜像部署：适用于物理服务器及虚拟化场景。

步骤1：安装包下载

安装包从深信服社区下载，https://bbs.sangfor.com.cn/（路径：自助服务/软件下载/终端安全管理系统EDR）

📖 **说明：**

OVA 镜像部署：需下载“EDRXXX 正式版本 OVA 模板”；
ISO 镜像部署：需下载“EDRXXX 正式版本 ISO 模板”；
升级至新版本：需下载“EDRXXX 正式版本安装升级包”。

步骤2：导入OVA镜像

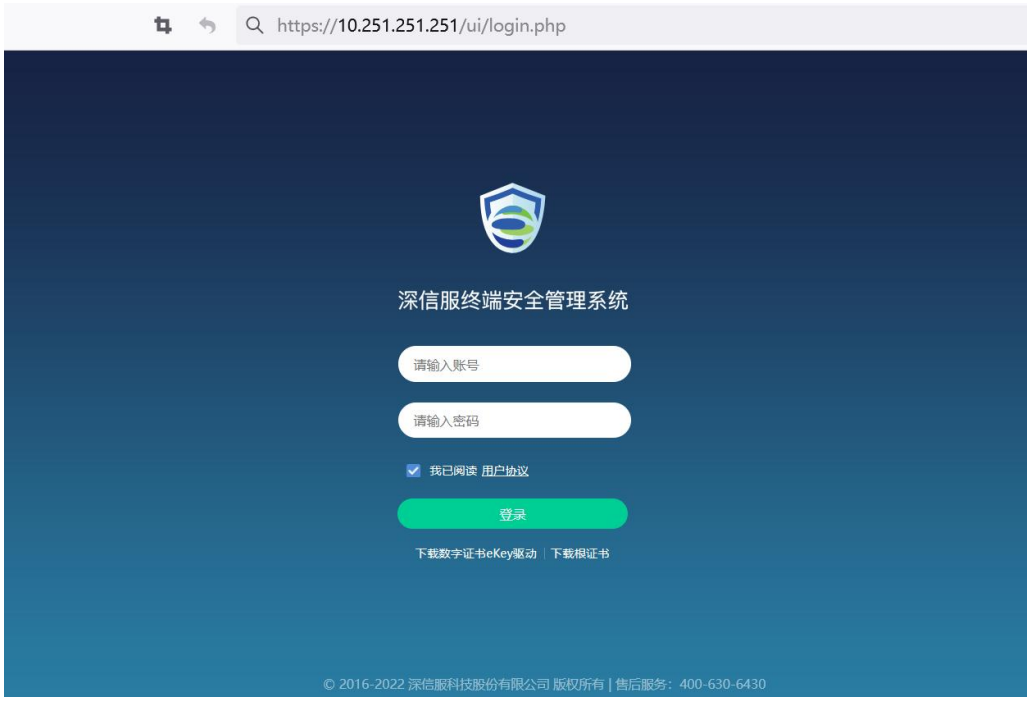
从虚拟化环境导入OVA镜像，如下图。

步骤3：网络配置

1.登录管理端

管理端第一块网卡默认地址为10.251.251.251/24。将电脑配置10.251.251.0/24同网段地址，使用浏览器通过默认地址登录。

浏览器打开https://10.251.251.251，默认用户名和密码为admin/admin。



📖 **说明：**

管理端管理口默认 IP 为 10.251.251.251/24；

浏览器支持 IE10 以上、FireFox、Chrome 等。

2.配置IP地址

登录管理平台后，打开[系统管理/系统设置/网络设置/接口设置]，配置管理端内网地址，如下图。

3.配置DNS

通过修改后的管理端IP地址重新登录管理端。打开[系统管理/系统设置/网络设置/高级设置]，配置主/备DNS地址，如下图。

📖 **说明：**

EDR 管理端更新病毒库等需要能解析域名，因此需配置相关 DNS。

4.配置路由

打开[系统管理/系统设置/网络设置/路由设置]，配置网关或路由，如下图。

📖 **说明：**

EDR 管理端需与终端通信及联网，因此需配置路由，保证可达。

2.3. 产品激活

完成EDR管理端部署后，需要进行产品激活，才能进行客户端组件安装及产品使用。此章节分别介绍EDR销售授权激活和EDR试用授权激活。

2.3.1. 销售授权激活

EDR销售授权激活包括软件EDR和硬件EDR销售授权激活，其中软件EDR销售授权激活为主场景，此章节主要介绍软件EDR销售授权激活，硬件EDR销售授权激活参考第3章安装部署。

步骤1. 获取产品授权ID

（1）访问深信服授权中心地址：https://license.sangfor.com.cn。

（2）全新注册或使用已有账号登录。

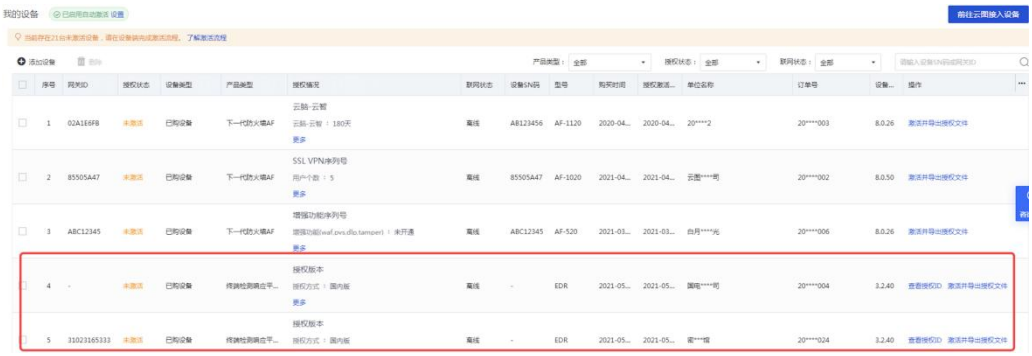
（3）登录授权中心，点击<现在激活>（初始状态下未添加任何设备），添加需授权设备。

（4）必须选择[通过订单号添加]方式，填入订单系统中的企业名称与订单号，并点击<确认>，进行设备导入。

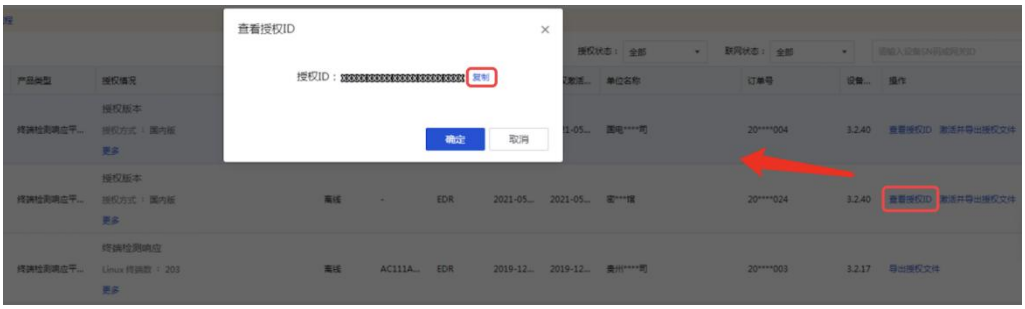
📖 **说明：**

EDR 授权激活导入需激活的设备信息只能选择[通过订单号添加]，不能选择通过[网关 ID 添加]。

（5）导入设备成功后，可显示本账号下所绑定的所有深信服设备、激活状态与授权过期时间等信息。



（6）找到需要激活的EDR设备，点击[查看授权ID]即可获取产品授权ID



步骤2. 激活产品授权

登录EDR管理端，打开[系统管理/授权管理]，在输入框中输入产品授权ID，如下图。

点击[激活授权]进行激活，管理端可以连接深信服授权中心，则进入在线授权激活；管理端不能连接深信服授权中心，则进入离线授权激活。

场景一：在线授权

如果管理端具备连接外网条件、能够和深信服授权中心正常通信，即可自动在线激活授权，激活成功效果如下图。

场景二：离线授权

如果管理端不能上网（即无法和深信服授权中心正常通信），在线激活授权失败，如下图，可以进行离线激活授权。

点击[前往离线授权]，进入离线激活授权页面，离线授权分为手机扫码授权和非扫码授权，手机扫码授权步骤如下图。

当手机无法使用微信扫码时，点击上图<无法扫码，请点这里>，进入非扫码激活，激码步骤参考第3章安装部署。

2.3.2. 试用授权激活

产品试用授权需要联系服务提供商激活。

步骤1.确认开通测试授权数量和时长

提前和客户确认PC和服务器（包括Windows Server和Linux）测试授权开通数量及开通时长（最长试用时间为3个月）。

步骤2.获取网关ID及测试设备硬件信息

打开[系统管理/授权管理]，如下图。

点击[申请试用]，获取网关ID和设备硬件信息。

步骤3.登录“测试设备授权”系统

登录企业门户，打开深信服“测试设备授权”系统。

步骤4.获取EDR测试授权文件

按下图填写申请测试授权信息。

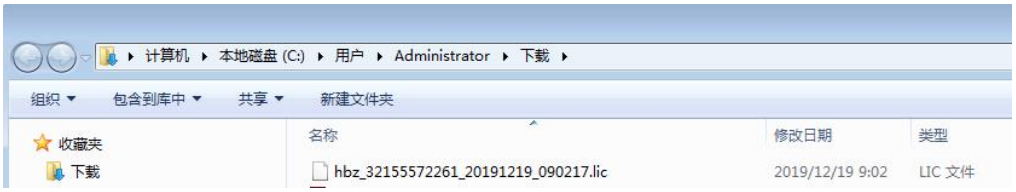
点击“立即获取”，如下图提示。

点击 

，如下图。设备信息栏中导入第2步导出的EDR管理平台硬件信息文件。

点击 激活 ，提示激活成功并下载授权文件，如下图所示。

点击 下载 ，下载授权文件，如下图。



步骤5.激活授权

再次回到EDR管理平台授权管理页面，将步骤4获取的授权文件按下图导入，激活成

功。

激活成功，如下图。

2. 4. 分组管理

EDR通过树形组织结构对内网终端进行管理，可实现终端从管理端上线时根据终端真实IP自动匹配归属分组。

提前梳理业务分组及IP地址规划，根据业务属性建好分组、启用根据IP自动分组，当终端Agent安装时根据终端地址自动上线至所属分组。

打开[终端管理/终端分组管理]，点击<新增>增加分组，并启用自动分组、配置自动分组IP地址段，如下图。

创建组织结构效果图如下。

当分组数量很多时，可以按照模板用excel表格制作好分组一次导入。打开[终端管理/终端分组管理]，点击<导入分组>下载示例模板，用excel编辑好分组后一次性导入。

2.5. 策略配置

安全策略涵盖基本策略、病毒查杀、实时防护、勒索防护、信任名单、漏洞防护、桌面管控等安全策略，不同终端支持功能如下。

表5 Windows PC、Windows Server、Linux对各安全策略支持情况

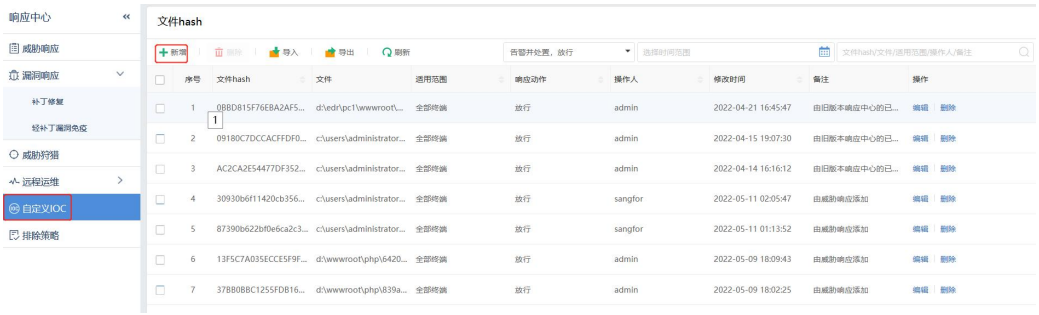
安全策略	Windows PC	Windows server	Linux
基本策略	√	√	×
病毒查杀	√	√	√
文件实时监控	√	√	√
webshell 检测	×	√	√
勒索病毒防护	√	√	×
暴力破解检测	√	√	√
高级威胁防护	√	√	×
服务器可信进程防护	×	√	×
信任名单	√	√	×
漏洞修复	√	√	×
违规外联	√	√	×
USB 外设管控	√	√	×
终端广告弹窗拦截	√	×	×
远程桌面二次认证	×	√	×

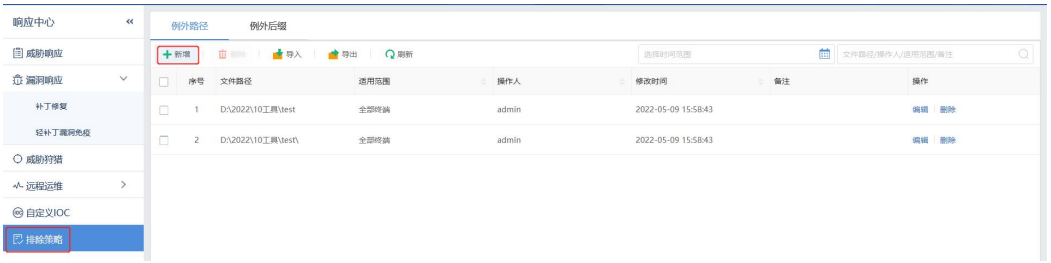
2.5.1. 白名单策略配置

为了避免病毒查杀可能带来的误报影响，提前收集好信任文件并加入白名单。白名单文件包括需要加白的业务软件、工具、powershell脚本参数（如果存在powershell编写的运维脚本，则将powershell参数加白）。

打开[终端管理/策略中心]，设置“本级中心”组的“信任名单”策略，添加powershell参数白名单，如下图。

打开[响应中心/自定义IOC]或[响应中心/排除策略]，根据md5添加白名单文件、或直直接添加排除文件或目录，如下图。





2.5.2. 安全策略配置

安全策略配置包括如下三部分。

以下安全策略在产品首次上线时按如下要求检查并开启

1.病毒查杀策略

打开[终端管理/策略中心/病毒查杀策略]，病毒查杀策略按如下配置。

定时查杀：建议开启。建议每周一次定时查杀、定时查杀时间选择中午等非上班时间，扫描类型设置快速扫描，扫描模式选择均衡。

文件类型：低风险文件类型不选（不选有利于提升查杀速度），其它类型全选。

发现威胁后处置动作：设置为自动处置-业务优先。

引擎配置：根据实际情况进行配置，默认配置是标准模式。

场景对比

模式类型	适用场景	内存占用	检出率	误报率
标准模式	通用的服务器和办公网场景均可适用	中低	高	低
低误报模式	通用办公场景和较为重要的服务器系统如财务、OA等	较低	高	极低
高检出模式	有严格保护要求且较为稳定的服务器场景	中低	极高	中低
资源低耗模式	适用于存在高负载和老旧系统等终端场景	极低	高	低

开

启资源优化模式：终端电脑配置比较低或Agent安装在桌面云环境，需启用资源优化模式。

2.远程桌面登录二次认证

Windows Server所在分组开启远程桌面登录二次认证，避免服务器被攻击者远程桌面登录爆破、拿到服务器权限。登录控制台时会提示开启远程桌面登录二次认证，如下图，按照提示启用远程桌面登录二次认证。

也可以打开[终端管理/策略中心]，选择Windows Server所在分组，通过[勒索防护/远程桌面登录认证]进行策略配置，如下图。

认证方式：选择[远程桌面登录二次认证]；

认证密钥：选择[验证码验证]，且正确配置EDR管理员的姓名和手机号，即密钥为EDR管理员手机号后6位，便于服务器管理员远程桌面登录服务器时能方便获取认证密钥。

2.webshell检测

打开[终端管理/策略中心]，选择Windows Server所在分组，通过[实时防护/webshell检测]进行策略配置，如下图。

检测方式：启用实时检测和定期检测。

发现WebShell：设置发现webshell后的处理动作，设置为自动处置

自定义Web目录：设置webshell检测目录。默认检测web服务器所在目录，也可以自定义目录。

以下安全策略默认启用并保留默认配置即可

暴力破解检测、勒索病毒防护、漏洞防护

以下安全策略根据需求选择性启用

微隔离、服务器可信进程防护、USB外设管控、终端广告软件弹窗拦截、非法外联等根据需求选择性启用，策略配置方法参考第4章节产品使用。

2.6. 终端部署

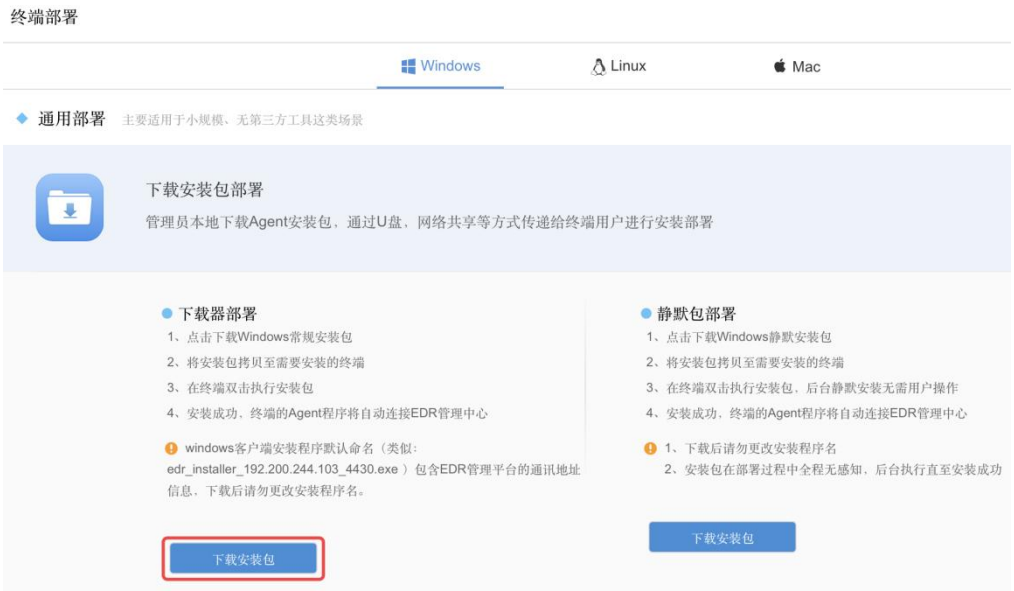
2.6.1. Windows 系统部署

Windows系统部署Agent支持通用部署和批量部署。 此章节介绍通用部署，批量部署参考第3章安装部署。

通用部署适用于小规模、无第三方工具场景，管理员在EDR管理端本地下载Agent安装包，并通过U盘等移动介质将其导入终端进行安装部署。

步骤1：下载安装程序

打开[系统管理/终端部署]，选中[Windows/下载器部署]下载Agent安装包，如下图。



📖 说明：

PC 客户端安装程序默认命名（类似 edr_installer_管理端 IP_4430.exe）包含 EDR 管理端通讯地址信息，下载后请勿更改安装程序名。

步骤2：将安装程序拷贝至需要安装的终端，双击执行安装。

阅读免责声明并勾选“同意免责声明”，点击<立即安装>，安装程序连接EDR管理端下载必要的安装组件进行安装，如下图。

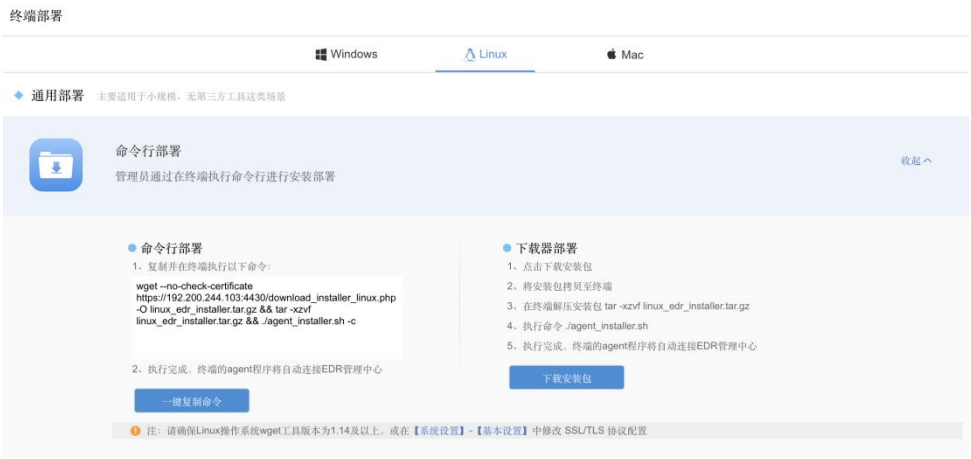
安装完成，点击<开启防护>完成资产信息上报登记，如下图。

安装成功后，终端 Agent 自动连接EDR管理端。在管理端[终端管理/终端分组管理]可以看到终端上线信息，如下图。

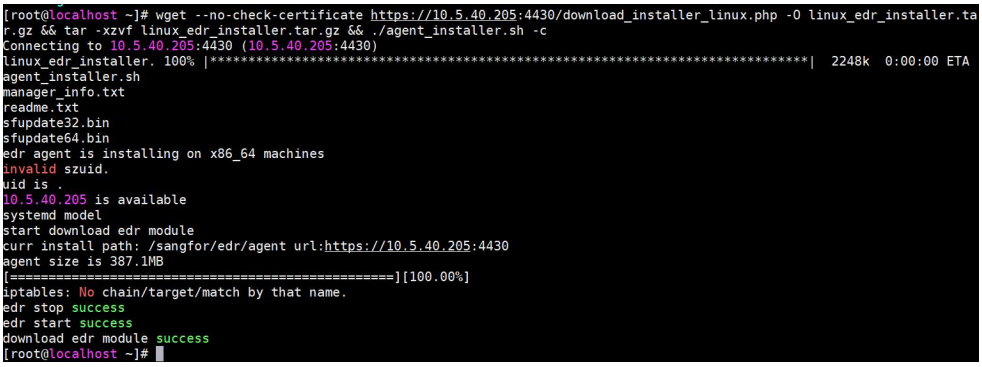
2.6.2. Linux 服务器部署

Linux系统部署Agent支持通用部署和批量部署。 此章节介绍通用部署，批量部署参考第3章安装部署。

通用部署适用于小规模部署场景，管理员获取安装命令并在终端命令行执行即可实现Agent安装。打开[系统管理/终端部署]，选中[Linux]，如下图。



点击<一键复制命令>，获取安装命令并在终端命令执行，完成安装，如下图。



2.6.3. MAC OS 部署

MAC OS部署Agent支持下载安装包部署和网页推广部署。

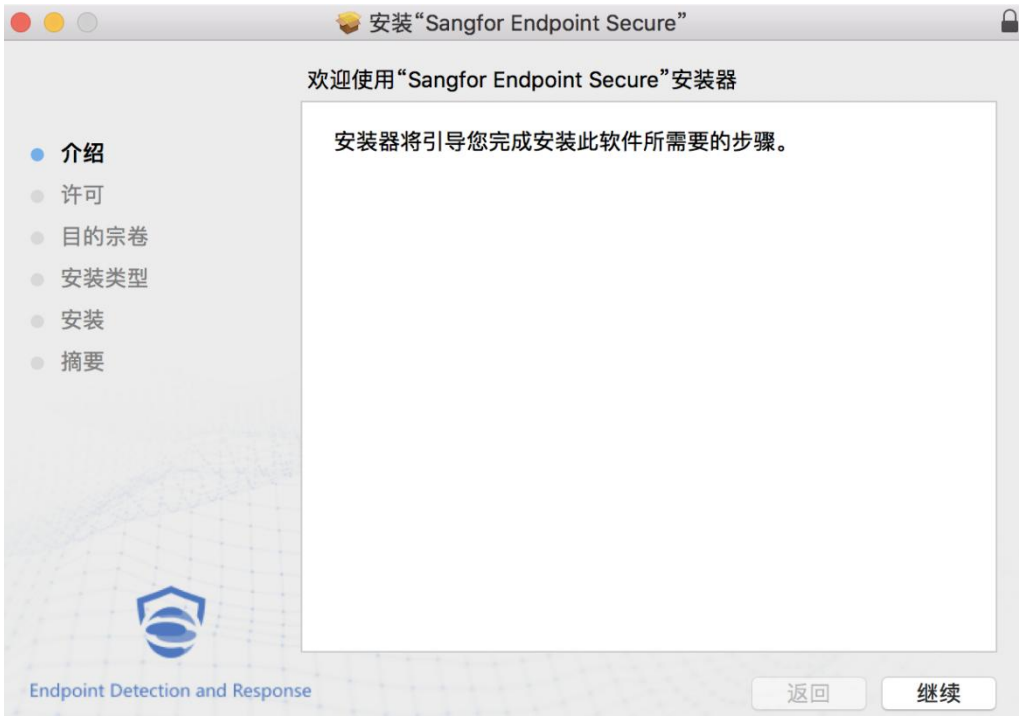
管理员本地下载Agent安装包，通过U盘，网络共享等方式传递给终端用户进行安装部署。

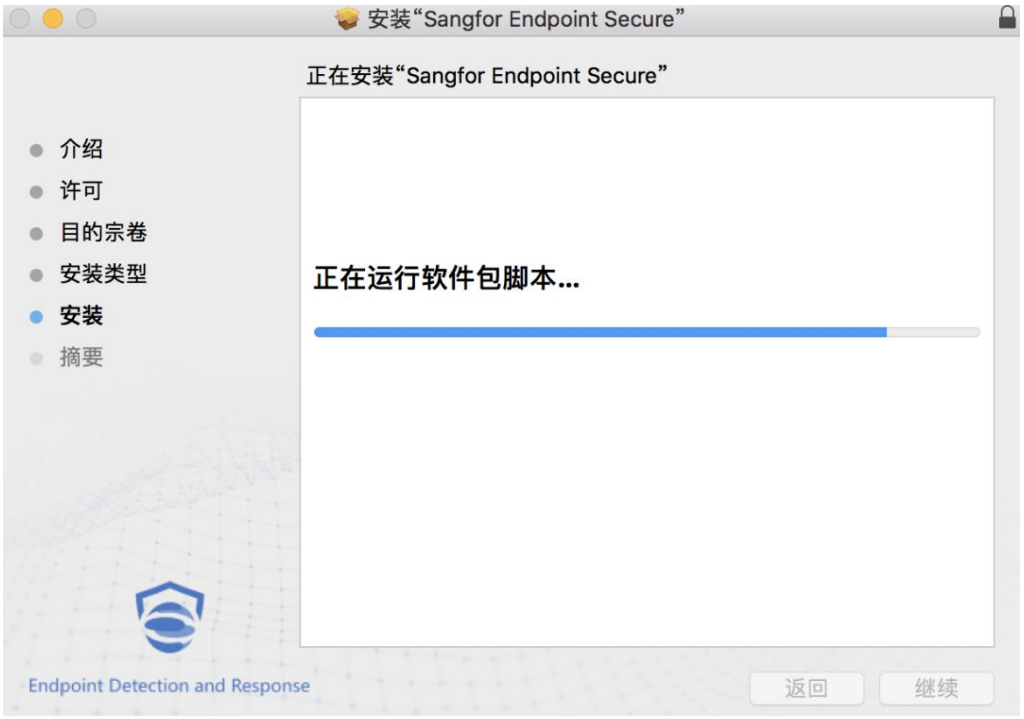
打开[系统管理/终端部署]，选中[MAC]并下载安装包，如下图。

📖 **说明：**

MAC 客户端安装程序默认命名（类似 edr_installer_管理端 IP_4430.exe）包含 EDR 管理端通讯地址和端口信息，下载后请勿更改安装程序名。

双击安装程序，如下图，按照向导进行安装。





安装完成，在MAC OS菜单栏生成EDR图标，说明已正常安装，如下图。

MAC OS 客户端Agent主页面如下。

2.6.4. 终端 Agent 部署成功确认

安装成功后，终端 Agent 程序将自动连接EDR管理端。在管理端[终端管理/终端分组管理]可以看到终端上线信息，如下图。

3. 安装部署

3.1. 准备工作

3.1.1. 管理端安装环境

管理端有软件管理端和硬件管理端。其中软件管理端支持在真实物理环境及虚拟化环境进行部署，部署服务器需满足以下资源配置要求。

表6 主流场景部署管理端硬件资源要求

终端数	CPU	内存	磁盘
1-300	4 核	4G	200G
300-4500	8 核	16G	1T
4500-10000	12 核	16G	1T

表7 EDR与aTrust联动场景部署管理端硬件资源要求

终端数	CPU	内存	磁盘
1-150	6 核	8G	200G
150-2500	8 核	16G	1T
2500-5000	12 核	16G	1T

3.1.2. 客户端安装环境

EDR客户端Agent支持安装在Windows PC、Windows Server、Linux及MAC OS，操作系统支持详情如下。

表8 各系统及版本信息

系统类别	兼容版本信息
Windows PC	Win XPsp3/Win Vista/Win7/Win8/Win8.1/Win10/Win11
Windows Server	WinServer 2003 SP2 WinServer 2008 WinServer 2008R2 WinServer 2012 WinServer 2012R2 WinServer 2016

	WinServer 2019
Linux	CentOS 5.x/6.x/7.x/8.x Ubuntu 10.x/11.x/12.x/13.x/14.x/16.x/17.x/18.x/20 Debian 6.x/7.x/8.x/9.x RHEL 5.x/6.x/7.x/8.x SUSE 11/12/15 Oracle Linux 5.x/6.x/7.x
MAC	Mac OS 12 Mac OS 11.x Mac OS 10.13 Mac OS 10.14 Mac OS 10.15

3.1.3. 网络连通性要求

为确保EDR各项功能正常使用，需要放行Agent客户端到管理端连通性、以及管理端到云端服务器的连通性，放行端口和服务器地址如下表。

表9 网络连通性要求

源设备	目的设备	协议/端口	端口作用
Agent	管理端	TCP 443	访问控制台端口
		TCP 4430	Agent 组件更新和病毒库更新
		TCP 8083	Agent 和管理端业务通信端口
		TCP 54120	紧急场景，管理端控制 Agent 禁用/启用
		ICMP	连通性探测
源设备	目的设备	需公网连通服务器地址	
管理端	云端服务器	漏洞补丁、ioa 升级	https://upd.sangfor.com.cn
		授权相关	https://auth.sangfor.com.cn
		云查服务器	https://analysis.sangfor.com.cn
		云安全计划	https://clt.sangfor.com.cn
		Ioc 规则升级	intelligence.sangfor.com.cn/
		漏洞补丁、规则、病毒库	http://download.sangfor.com.cn

3.1.4. 收集白名单文件

为了避免病毒查杀可能带来的误报影响，提前收集好信任文件并加入白名单。白名单文件包括确认无毒的业务软件、或者前期使用过其它杀毒产品时梳理的白名单文件。

在部署完管理端并完成授权激活后，登录EDR管理端，在[响应中心/自定义IOC]或[响应中心/排除策略]中，添加白名单文件，信任名单中的文件不会进行病毒扫描查杀。

3.2. 管理端部署

3.2.1. 软件管理端

软件管理端支持二种部署方式，包括OVA镜像部署和ISO镜像部署，适用场景如下：

1.OVA模板部署模式：适用于VMware、HCI等虚拟化场景；

2.ISO模板部署模式：适用于物理服务器及虚拟化场景。

3.2.1.1. 安装包下载

相关组件包下载链接如下：https://bbs.sangfor.com.cn/（路径：自助服务/软件下载/终端安全管理系统EDR）

📖 **说明：**

OVA 镜像部署：需下载“EDRXXX 正式版本 OVA 模板”；
ISO 镜像部署：需下载“EDRXXX 正式版本 ISO 模板”；
升级至新版本：需下载“EDRXXX 正式版本安装升级包”。

3.2.1.2. OVA 镜像部署

📖 **说明：**

以下操作步骤以 HCI 虚拟化平台为例，其他虚拟化平台可以此做参考。

步骤1：导入OVA模板

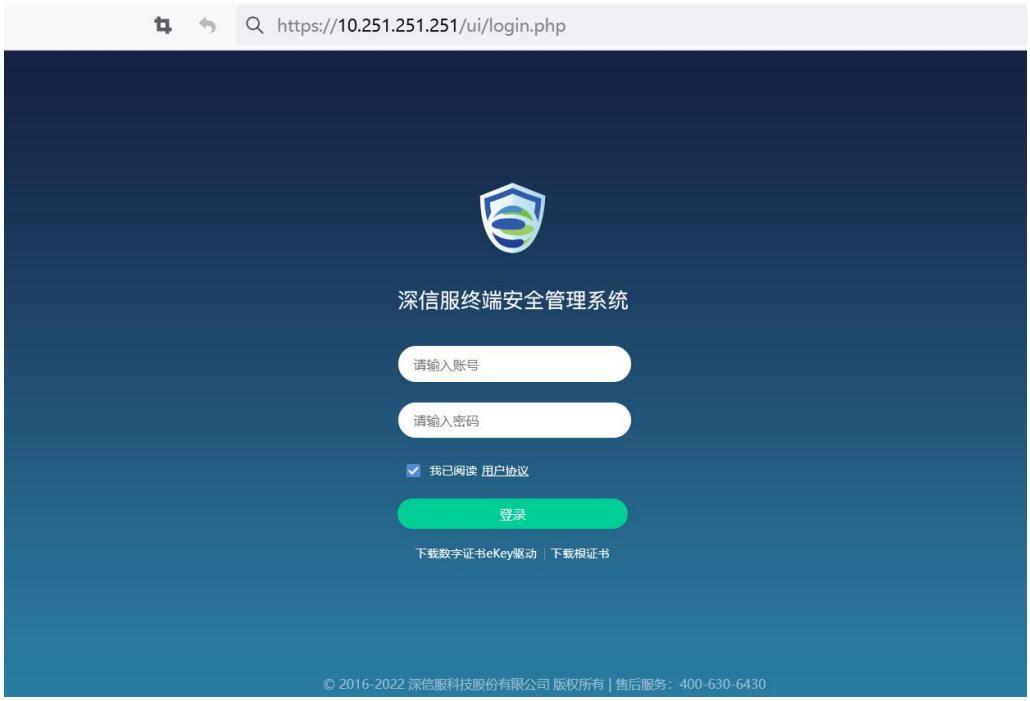
从虚拟化环境导入OVA模板，如下图。

步骤2：网络配置

1.登录管理端

管理端第一块网卡默认地址为10.251.251.251/24。将电脑配置10.251.251.0/24同网段地址，使用浏览器通过默认地址登录。

浏览器打开https://10.251.251.251，默认用户名和密码为admin/admin。



📖 **说明：**

管理端管理口默认 IP 为 10.251.251.251/24；

浏览器支持 IE10 以上、FireFox、Chrome 等。

2.配置IP地址

在[系统管理/系统设置/网络设置/接口设置]页签下，配置管理端地址，如下图。

3.配置DNS

在[系统管理/系统设置/网络设置/高级设置]一栏，可配置主/备DNS地址，如下图。

📖 **说明：**

EDR 管理端更新病毒库等需要能解析域名，因此需配置相关 DNS。

4.配置路由

在[系统管理/系统设置/网络设置/路由设置]页签下，可配置相关路由，如下图。

📖 **说明：**

EDR 管理端需与终端通信及联网，因此需配置路由，保证可达。

3.2.1.3. ISO 镜像部署

步骤1：安装准备

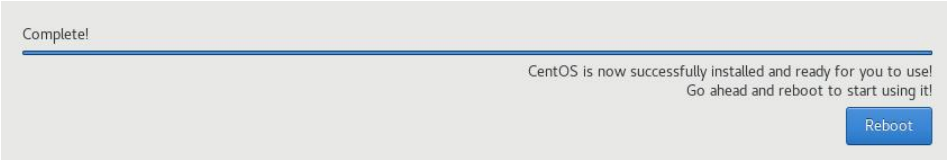
物理服务器安装，使用UltraISO刻录软件，将ISO模板刻录至空数据的U盘或DVD中。

虚拟机安装，可以直接导入ISO镜像安装，如下图。

步骤2：安装部署

设置服务器第一引导顺序从光驱或USB启动，启动页面如下图。

选择 [Install CentOS 7 by USB]，点击<Enter>键进入正式安装（自动进行，不需要进行手动操作），等待安装完成即可。



5.出现如上图页面说明安装完成，点击<reboot>重启进入服务器。

步骤3：网络配置

网络配置步骤请参考章节“OVA镜像部署”中的网络配置。

3.2.2. 硬件管理端

3.2.2.1. 硬件选型

EDR硬件管理端有4款型号，不同型号支持接入的终端数量如下。

表10 硬件选型

硬件型号	支持接入终端数
EDR-1000-B600	2000 台
EDR-1000-C600	4500 台

3.2.2.2. 产品外观

下图是EDR-1000-B600硬件型号的前面板，其中eth0口为默认通信网口。

3.2.2.3. 设备配置

1.登录管理端

将电脑配置与管理端eth0口同网段地址，使用浏览器访问管理端默认地址：https://10.251.251.251，默认用户名和密码为admin/admin。

📖 **说明：**

管理端 Eth0 口默认 IP 为 10.251.251.251/24；
浏览器支持 IE11 以上、FireFox、Chrome 等。

2.配置IP地址

在[系统管理/系统设置/网络设置/接口设置] 配置管理端地址，如下图。

3.配置DNS

在[系统管理/系统设置/网络设置/高级设置]一栏，可配置主/备DNS地址，如下图。

📖 **说明：**

EDR 管理端更新病毒库等需要能解析域名，因此需配置相关 DNS。

4.配置路由

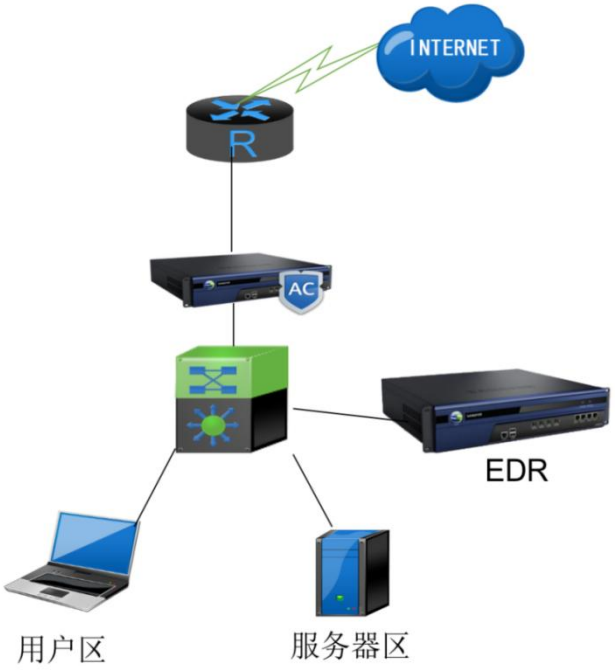
在[系统管理/系统设置/网络设置/路由设置]一栏，可配置相关路由，如下图。

📖 **说明：**

EDR 管理端需与终端通信及联网，因此需配置路由，保证可达。

3. 2. 2. 4. 接入网络

使用标准的RJ-45以太网线将设备ETH0口接入内网交换机（如下图），背板上连接电源线，打开电源开关，此时前面板的Power灯（绿色，电源指示灯）和Alarm灯（红色，告警灯）会点亮。大约1-2分钟后Alarm灯熄灭，说明网关正常工作。

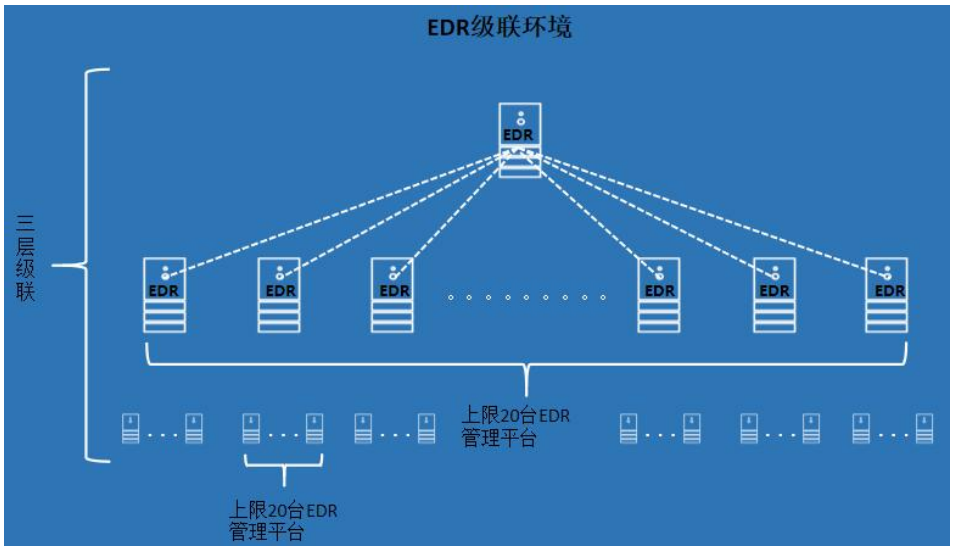


3.2.3. 级联部署

应用场景

集团公司(总部多分支场景)、终端数量总和超过1万点，在集团总部和分公司同时部署多个EDR分别管理终端，且实现集团总部对各分公司EDR授权动态调整（统一分配与回收）、从上级EDR查看下级EDR安全状态和接入的终端。

级联部署可支持三级级联，每台EDR可级联至多20台EDR管理端，EDR级联环境示意图如下所示。



部署条件

级联部署条件如下。

1.集团总部和分公司分别部署EDR管理端。

2.集团总部EDR激活所有授权，分公司EDR无需激活、由集团总部EDR向分公司EDR分配授权。

3.评估各分公司需要分配的授权数量（PC数量和服务器数量）。

级联配置

1.集团总部和分公司分别部署EDR管理端

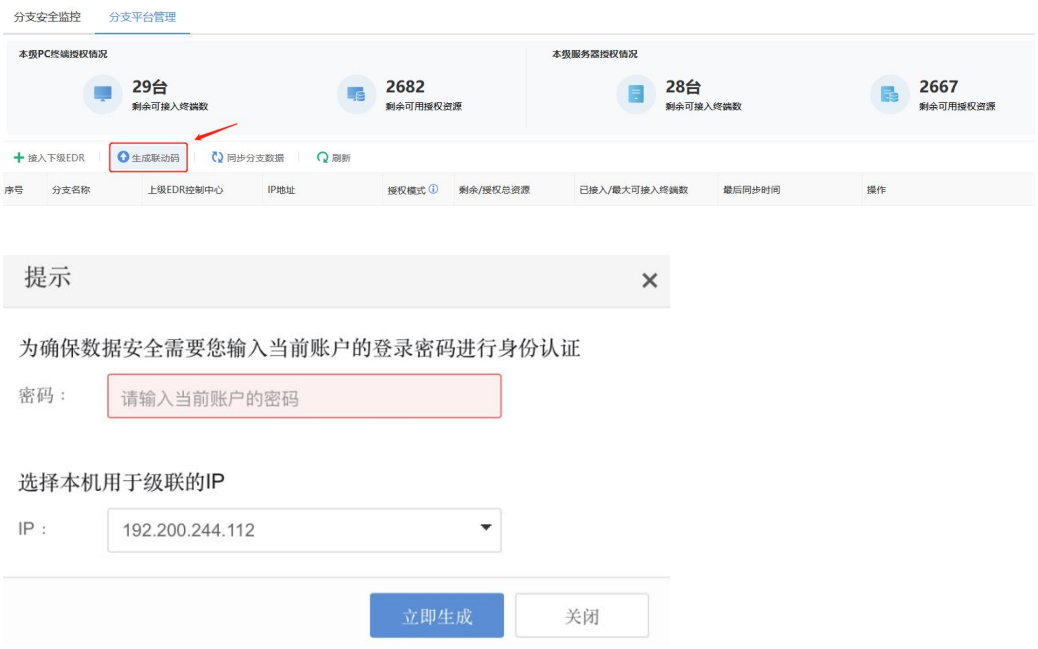
根据集团总部和分公司分别管理的终端数量进行EDR管理端服务器选型、并部署EDR管理端。

2.集团总部EDR产品激活

集团总部EDR激活所有授权，分公司EDR无需激活、由集团总部EDR向分公司EDR分配授权。

3.分支EDR管理端生成联动码

登录下级EDR管理端，打开[系统管理/分支管控/分支平台管理]，点击<生成联动码>，如下图。



输入当前控制台账号登录密码，点击<立即生成>，生成联动码，如下图。

点击<复制>，复制联动码到上级EDR平台完成级联对接。

4.分支EDR管理端开启SSH服务

登录下级EDR管理端，打开[系统管理/系统设置/网络设置/高级设置]，开启SSH服务设置，如下图。

5.集团EDR管理端完成级联对接

登录上级EDR管理端，打开[系统管理/分支管控/分支平台管理]，点击<接入下级EDR>，如下图。

依次填写分支名称、分支EDR平台IP、分支EDR控制台登录端口、分支SSH端口、分支SSH账号和密码（admin账号和密码）、以及下级联动码，点击<确定>，如下图。

输入当前管理端登录密码，点击<确定>，级联成功，如下图。

本级PC终端授权情况：显示本级平台PC剩余接入终端数和剩余可用授权数

本级服务器授权情况：显示本级平台服务器剩余接入终端数和剩余可用授权数

级联成功页面显示下级平台名称、IP地址、授权模式、剩余/授权总资源、已接入/最大可接入终端数、最后同步时间以及相关操作。

授权模式：级联部署场景下，下级管理端有独立授权和级联授权两种模式可以调整。独立授权，即下级管理端自己开通授权，上级管理端无法对下级管理端动态调整授权；级联授权，即下级管理端授权是由上级管理端分配的，上级管理端可以根据实际情况

动态调整下级管理端授权。

剩余/授权总资源：下级管理端剩余授权资源数和授权总资源数

已接入/最大可接入终端：下级管理端已接入的终端数量和支持最大接入的终端数量

6.集团总部EDR为各分公司EDR分配授权

评估各分公司EDR所需授权数量，由集团总部EDR为各分公司EDR分配授权。

打开[系统管理/分支管控/分支平台管理]，如下图。

选择分支，点击<授权调整>，进入授权调整页面，如下图。

可以设置下级平台的授权模式为[独立授权]或[级联授权]。独立授权，即下级管理端需要自己开通授权，上级管理端无法对下级管理端动态调整授权。这里我们选择[级联授权]，如下图，根据实际情况分配下级平台PC和服务器的接入数量和使用时长。

级联授权调整成功后，如下图

继续采用相同方法为其它分公司EDR分配授权。

7.集团总部EDR和各分公司EDR分别安装Agent

集团总部EDR和各分公司EDR分别安装Agent客户端。

级联效果

1.查看下级管理端安全状态

打开[系统管理/分支管控/分支安全监控]，鼠标移至下级管理端，显示下级管理端安全状态，点击<进入中心>可以跳转至下级管理端控制台登录页面，如下图。

2.查看下级管理端接入终端

打开[终端管理/终端分组管理]，可以查看下级管理端接入终端，如下图。

3.级联授权

当授权总数固定，各分支授权数需要动态调整时，可以采用级联授权。

上级管理端开通授权总资源，下级管理端不需要开通授权，上级管理端和下级管理端组成级联部署，即可通过上级管理端给下级管理端分配与回收授权。

打开[系统管理/分支管控/分支平台管理]，级联效果如下图。

点击<授权调整>，进入授权调整页面，如下图。

可以设置下级平台的授权模式为[独立授权]或[级联授权]。独立授权，即下级管理端需要自己开通授权，上级管理端无法对下级管理端动态调整授权。这里我们选择[级联授权]，如下图，根据实际情况分配下级平台PC和服务器的接入数量和使用时长。

级联授权调整成功后，如下图

说明：

1.如果调整的下级平台可授权 PC 终端、服务器数量低于下级平台当前已接入数量，则按下述顺序回收超出的终端授权：已禁用终端 > 离线终端 > 在线终端。

2.终端分组管理中终端状态为“已卸载”、“未授权”时，不占用授权数。

3.使用级联授权场景，只需要上级管理端开通授权、下级管理不需要激活授权，上级管理端和下级管理端组成级联部署，即可通过上级管理端将授权资源动态调整到下级管理端。

3.3. 产品激活

完成EDR管理端部署后，需要进行产品激活，才能进行客户端组件安装及产品使用。此章节分别介绍EDR销售授权激活和EDR试用授权激活。

3.3.1. 销售授权激活

3.3.1.1. 软件 EDR 销售授权激活

步骤1：获取产品授权ID

（1）访问深信服授权中心地址：https://license.sangfor.com.cn。

（2）全新注册或使用已有账号登录。

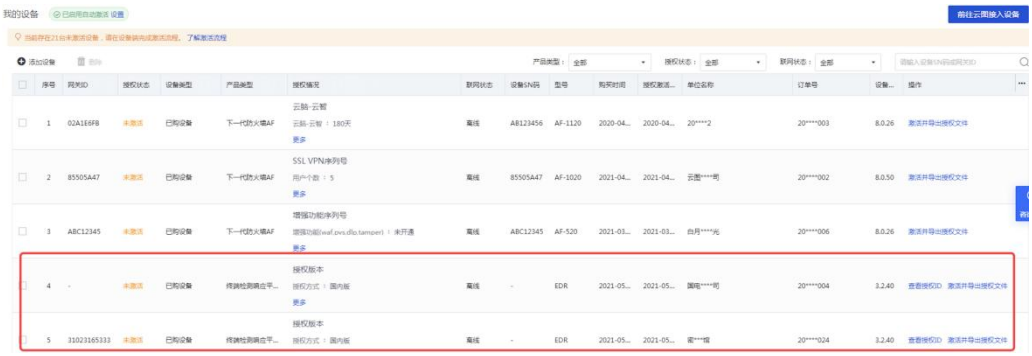
（3）登录授权中心，点击<现在激活>（初始状态下未添加任何设备），添加需授权设备。

（4）必须选择[通过订单号添加]方式，填入订单系统中的企业名称与订单号，并点击<确认>，进行设备导入。

📖 **说明：**

EDR 授权激活导入需激活的设备信息只能选择[通过订单号添加]，不能选择通过[网关 ID 添加]。

（5）导入设备成功后，可显示本账号下所绑定的所有深信服设备、激活状态与授权过期时间等信息。



（6）找到需要激活的EDR设备，点击[查看授权ID]即可获取产品授权ID

步骤2：激活产品授权

登录EDR管理端，打开[系统管理/授权管理]，在输入框中输入产品授权ID，如下图。

点击[激活授权]进行激活。管理端可以连接深信服授权中心，则进入在线授权；管理端不能连接深信服授权中心，则进入离线授权。

场景一：在线授权

如果管理端具备连接外网条件、能够和深信服授权中心正常通信，即可自动在线激活授权，激活成功效果如下图。

场景二：离线授权

如果管理端不能上网、无法和深信服授权中心正常通信，在线激活授权失败，可以进行离线激活授权，如下图。

点击[前往离线授权]，进入离线激活授权页面，如下图。

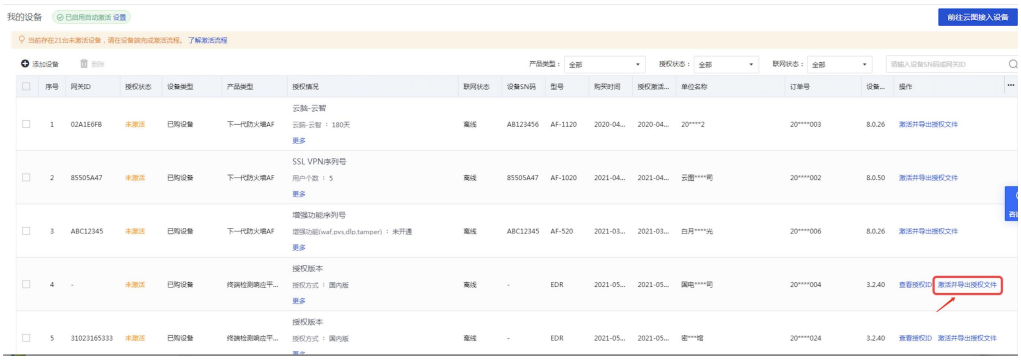
离线授权区分扫码授权和非扫码授权，优先选择手机扫码授权。

1.扫码授权

（1）用手机扫描上图二维码，自动提交设备硬件信息

（2）访问深信服授权中心，下载当前产品的授权文件。

点击[激活并导出授权文件]，如下图，下载当前产品授权文件。



（3）回到离线授权手机扫码授权页面，导入授权文件，如下图

导入授权文件，激活成功效果图如下：

3.非扫码授权

当手机无法扫码时，点击[无法扫码，请点这里]，如下图。

（1）访问深信服授权中心、添加设备。

具体方法参考[步骤1.获取产品授权ID]。

（2）获取EDR平台硬件信息

如上图，点击[导出设备硬件信息]导出硬件信息文件，或点击[复制设备硬件信息]直接复制到粘贴板。

（3）授权中心导出授权文件

在[授权中心/我的设备]列表中，匹配需激活的EDR设备，点击[激活并导出授权文件]。

选择[方式二:文件/文本上传]，选择[以文本形式提供(dev.info文件)]，上传EDR平台硬件信息文件，即可导出授权文件。

（4）EDR管理端导入授权激活

回到离线授权非手机扫码授权页面，导入授权文件，如下图

激活成功效果图如下：

3.3.1.2. 硬件 EDR 销售授权激活

硬件EDR只支持离线授权，不支持在线授权。硬件EDR销售授权激活方式如下。

打开[系统管理/授权管理]，如下图。

点击[硬件设备授权]，如下图。参考上述[软件EDR销售授权激活/离线授权场景/非扫码授权激活]方法激活硬件EDR授权。

3.3.2. 试用授权激活

产品试用授权需要联系服务提供商激活。

步骤1.确认开通测试授权数量和时长

提前和客户确认PC和服务器（包括Windows Server和Linux）测试授权开通数量及开通时长（最长试用时间为3个月）。

步骤2.获取网关ID及测试设备硬件信息

打开[系统管理/授权管理]，如下图。

点击[申请试用]，获取网关ID和设备硬件信息。

步骤3.登录“测试设备授权”系统

登录企业门户，打开“测试设备授权”系统。

步骤4.获取EDR测试授权文件

按下图填写申请测试授权信息。

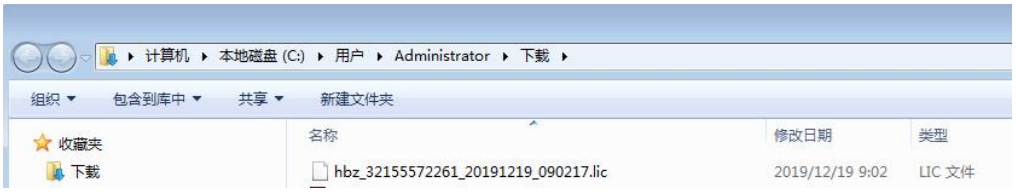
点击“立即获取”，如下图提示。

点击 

，如下图。设备信息栏中导入第2步导出的EDR管理平台硬件信息文件。

点击 激活 ，提示激活成功并下载授权文件，如下图所示。

点击 下载 ，下载授权文件，如下图。



步骤5.激活授权

再次回到EDR管理平台授权管理页面，将步骤4获取的授权文件按下图导入，激活成

功。

激活成功，如下图。

3.4. 终端部署

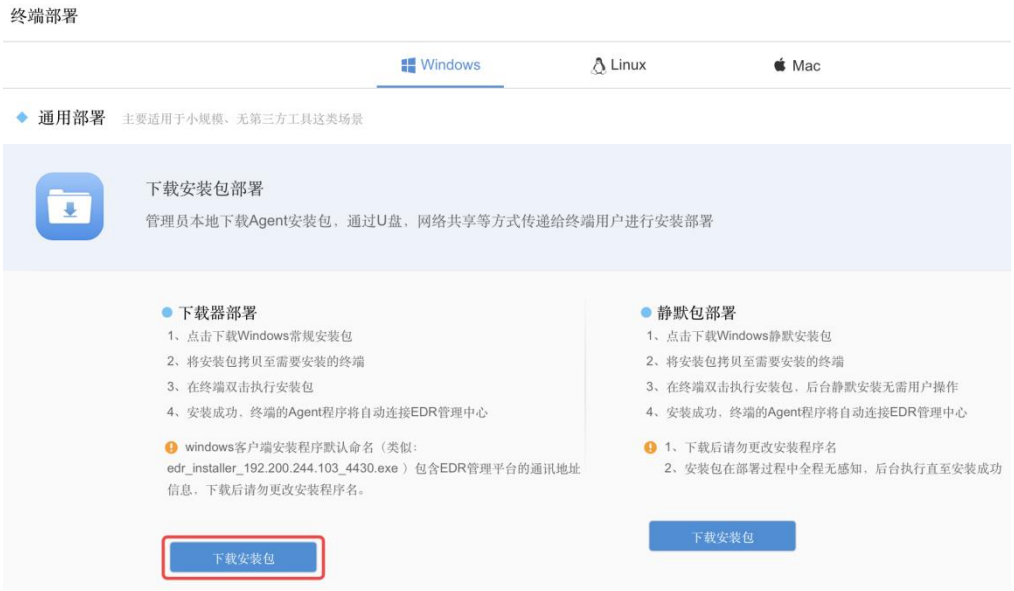
3.4.1. Windows 系统部署

Windows系统部署Agent支持小规模部署和大规模批量部署。 其中小规模部署包括下载器部署、静默包部署和网页推广部署，大规模批量部署包括AD域控批量部署、桌管批量部署、准入设备联动批量部署和虚拟机模板部署。

3.4.1.1. 下载器部署

下载器部署是小规模场景最常用的部署方式，管理员从EDR管理端下载Agent安装包，并通过U盘等移动介质将其导入终端进行安装部署，安装过程如下。

从EDR管理端下载安装程序。打开[系统管理/终端部署]，选中[Windows/下载器部署]下载Agent安装包，如下图。



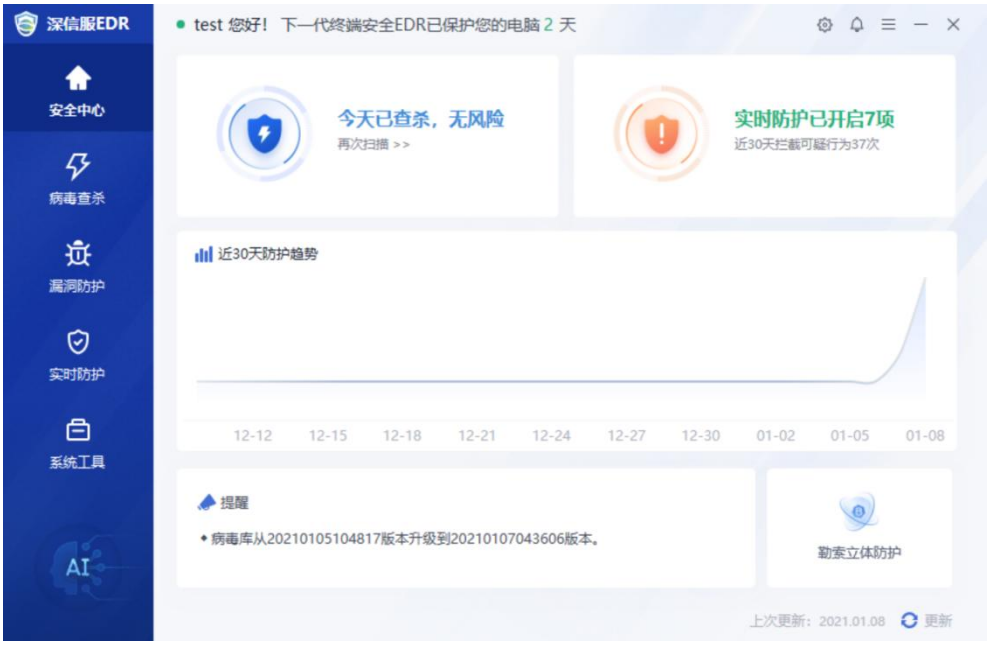
> 说明：
>
> PC 客户端安装程序默认命名（类似 edr_installer_管理端 IP_4430.exe）包含 EDR 管理端通讯地址信息，下载后请勿更改安装程序名。

将安装程序拷贝至需要安装的终端，并双击执行安装程序。

阅读免责声明并勾选“同意免责声明”，点击<立即安装>，安装程序连接EDR管理端

下载必要的安装组件进行安装，如下图。

安装完成，点击<开启防护>完成资产信息上报登记，如下图。

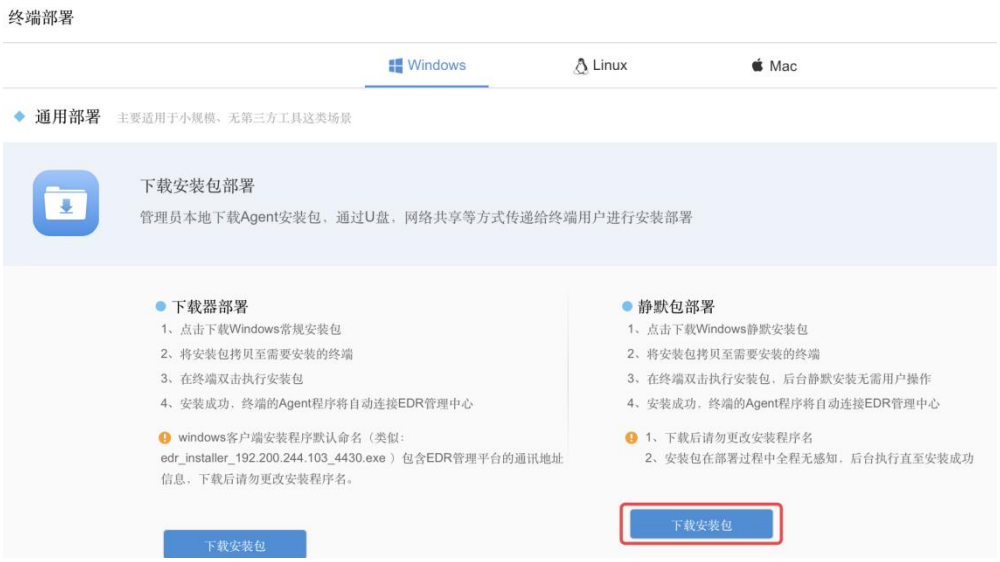


安装成功后，终端 Agent 自动连接EDR管理端。在管理端[终端管理/终端分组管理]可以看到终端上线信息，如下图。

3.4.1.2. 静默包部署

静默包安装全程无感知，适用于安装过程无感知、不需要人为干预场景。管理员从EDR管理端下载Agent安装包，并通过U盘等移动介质将其导入终端进行安装部署，安装过程如下。

从EDR管理端下载安装程序。下载路径[系统管理/终端部署]，选中[Windows/下载器部署]下载Agent安装包，如下图。



双击静默包自动安装、全程无感知，安装成功后，终端 Agent 自动连接EDR管理端，在管理端[终端管理/终端分组管理]可以看到终端上线信息。

3.4.1.3. 网页推广部署

管理员发布部署通知的web页面，将发布页链接通过邮件、OA等方式发送至终端，终

端用户自行下载Agent安装包进行安装部署。

打开[系统管理/终端部署]，选中[Windows]，打开[通用部署/网页推广部署]，如下图。

编辑推广通知页面标题和内容，点击<下一步>，生成推广链接，如下图。

管理员将推广链接通过邮件、OA等方式发送至终端，终端用户自行下载Agent安装包进行安装部署，如下图。

3.4.1.4. AD 域控推送批量部署

1.适用场景

客户内网已有微软AD域控，终端均接入域控统一管理。通过域控下发组策略，实现开机自动静默安装EDR客户端。

2.配置步骤

下载安装包和对应的操作文档，按照操作文档进行域控推送部署。打开[系统管理/终端部署]，选中[Windows]，打开[批量部署/AD域批量部署]，如下图。

> 说明：
> 安装程序默认命名（类似 edr_installer_管理端 IP_4430.exe）包含 EDR 管理端通讯地址信息，下载后请勿更改安装程序名。

3.4.1.5. 桌管推送批量部署

适用于客户有桌管软件且支持软件分发，可以通过桌管软件分发安装Agent，从而达到批量部署的目的。

场景一：桌管软件分发安装支持设置静默安装参数。

桌管软件分发安装支持设置静默安装参数场景，可以直接下载Agent常规安装包，并设置静默安装参数（-Silence=Y）分发安装。打开[系统管理/终端部署]，选中[Windows/批量部署/桌管批量部署]下载Agent常规安装包，如下图。

场景二：桌管软件分发安装不支持设置静默安装参数。

桌管软件分发安装不支持设置静默安装参数场景，需要下载Windows静默安装包分发安装。打开[系统管理/终端部署]，选中[Windows/批量部署/桌管批量部署]下载Agent静默安装包，如下图。

3.4.1.6. 准入设备联动批量部署

通过联动准入设备，检测到未安装Agent的终端则拦截终端上网流量，并引导至Agent下载页面进行安装部署，主要步骤如下：

1.准入设备启用准入策略，设置检测到终端未安装EDR Agent时，拦截终端上网页面并重定向至EDR客户端推广部署页面。

2.终端浏览网页，当准入检测到终端未安装EDR Agent时，拦截终端上网页面并重定向至EDR客户端推广部署页面。

3.终端下载EDR Agent安装后，符合准入规则，可以正常浏览网页。

如果同时有使用深信服行为管理（AC）产品，可以通过AC和EDR联动推广部署EDR Agent。打开[系统管理/终端部署]，选中[Windows/批量部署/准入设备部署]，参考AC

与EDR联动部署方案，如下图。

3.4.1.7. 虚拟机模板派生批量部署

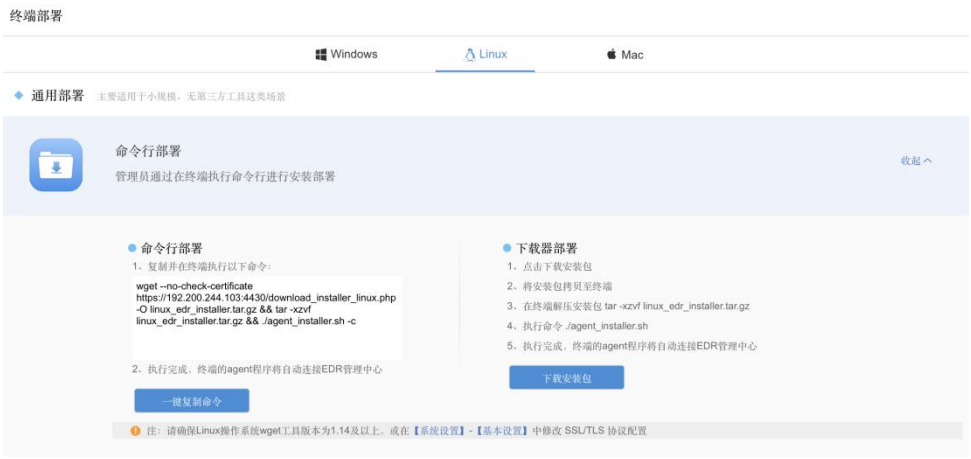
虚拟机模板部署适用于虚拟化环境，管理员将安装Agent的虚拟机制作成模板，通过模板批量派生成多个虚拟机。打开[系统管理/终端部署]，选中[Windows/批量部署/虚拟机模板部署]如下图。

3.4.2. Linux 服务器部署

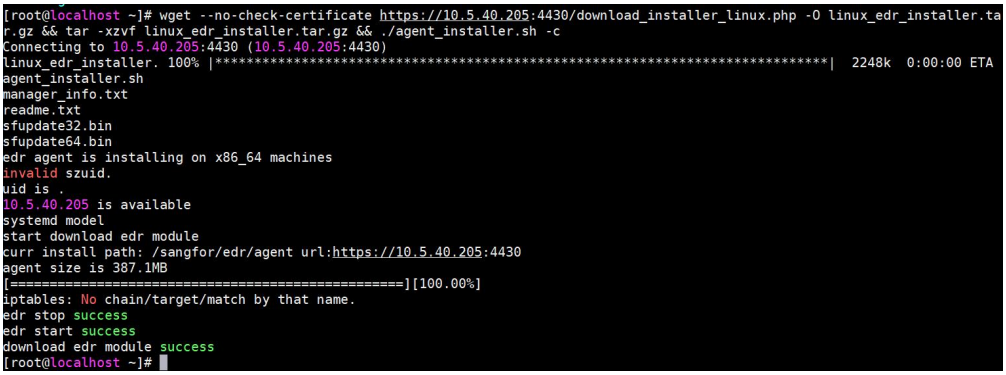
Linux服务器部署Agent支持支持小规模部署和大规模批量部署。 其中小规模部署包括命令行部署、下载器部署和网页推广部署，大规模批量部署包括Linux工具批量部署和虚拟机模板部署。

3.4.2.1. 命令行部署

命令行部署适用于小规模。获取安装命令并在终端执行即可实现自动部署，打开[系统管理/终端部署]，选中[Linux]，如下图。



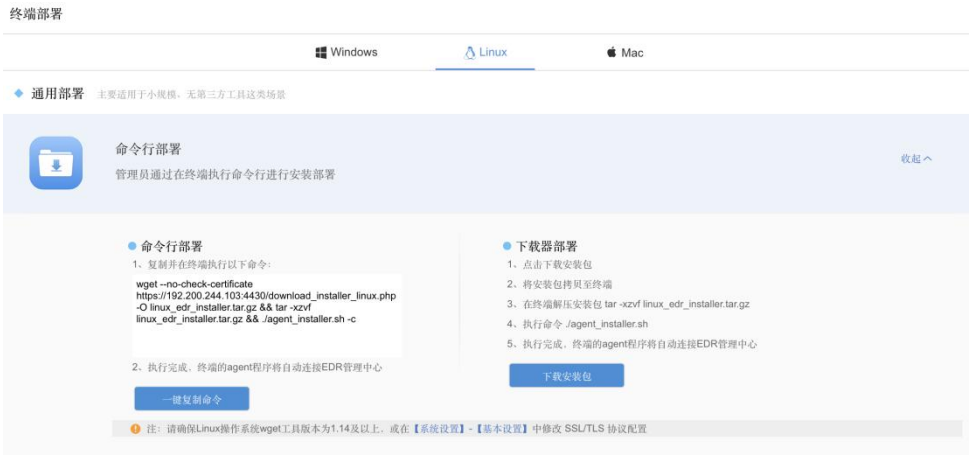
点击<一键复制命令>，获取安装命令并在终端执行，完成安装，如下图。



3. 4. 2. 2. 下载器部署

将Agent安装包下载至本地，并上传至终端，执行相关命令进行安装。

打开[系统管理/终端部署]，选中[Linux]，如下图。



1.点击下载安装包

2.将安装包拷贝至终端

3.在终端解压安装包 tar -xzvf linux_edr_installer.tar.gz

4.执行命令 ./agent_installer.sh

5.执行完成，终端的agent程序将自动连接EDR管理中心

3.4.2.3. 网页推广部署

管理员发布部署通知的web页面，将发布页链接通过邮件、OA等方式发送至终端，终端用户自行下载Agent安装包进行安装部署。

打开[系统管理/终端部署]，选中[Linux]，打开[通用部署/网页推广部署]，如下图。

编辑推广通知页面标题和内容，点击<下一步>，生成推广链接，如下图。

管理员将推广链接通过邮件、OA等方式发送至终端，终端用户自行下载Agent安装包进行安装部署，如下图。

3.4.2.4. Linux 工具批量部署

1.工具介绍

提供部署工具用于批量部署Linux客户端，该工具通过SSH协议批量连接Linux服务器并自动从管理端下载安装包安装，实现Linux环境批量部署EDR客户端。

2.工具运行环境

（1）Windows环境

3.工具使用条件

（1）提前收集需要安装EDR客户端的所有Linux服务器root账号和密码。

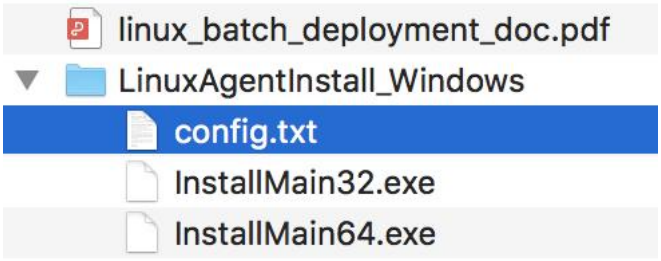
（2）运行工具的Windows PC可以通过SSH协议连接需要安装EDR客户端的Linux服务器。

4.工具使用说明

（1）下载工具包

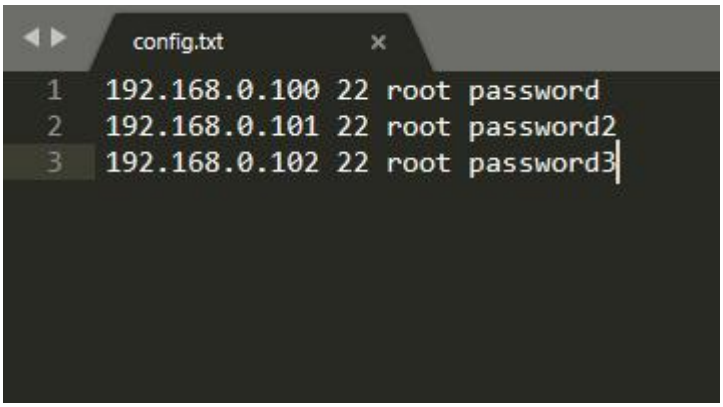
打开[系统管理/终端部署]，选中[Linux]批量部署，下载[Linux工具]和[操作文档]，如下图。

如下图。其中，config.txt为工具配置文件，InstallMain32.exe和InstallMain64.exe为工具主程序，分别运行在Windows 32位和windows 64位环境。



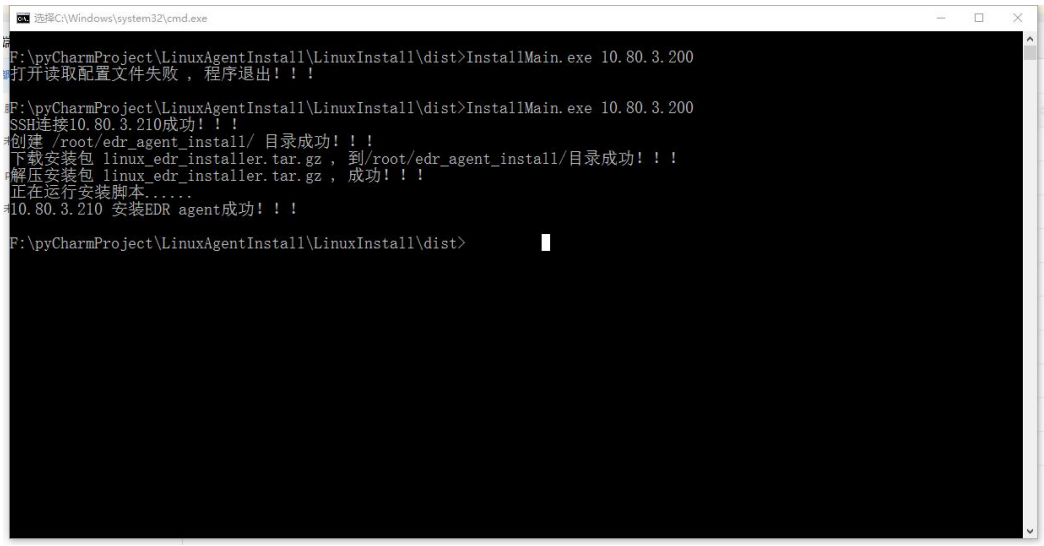
（2）编辑配置文件

提前收集需要安装EDR客户端的所有Linux服务器root账号和密码，并写入配置文件config.txt，格式为“Linux_IP SSH_port username password”，如下图所示(样例)：



（3）运行工具

运行InstallMain64.exe (或者InstallMain32.exe)，运行方式：InstallMain64.exe 管理端IP。如下图。



（4）安装成功确认

等待一段时间（安装时间和并发安装的数量有关，预计10分钟到30分钟左右），打开管理端[终端管理/终端分组管理]观察到Linux服务器已经上线，说明安装成功。

📖 **说明：**

1.配置文件需要与 InstallMain64.exe 处于同一目录下，并且配置文件名为 config.txt。
2.执行工具批量安装过程中，Linux 服务器会从 EDR 管理端下载安装包，为了避免大量终端同时下载而导致网络拥塞，建议限制单次批量部署最大终端数，保障安装稳定性。 如果 Linux 服务器到 EDR 管理端带宽是 100Mb ，建议一次批量部署最大终端数是 5 台终端；如果 Linux 服务器到 EDR 管理端带宽是 1000Mb ，建议一次批量部署最大终端数是 60 台终端。
3.终端安装完成后，请及时清空写有终端账户密码的配置文件 config.txt 的内容，并删除文件，防止密码意外泄漏。

3.4.2.5. 虚拟机模板派生批量部署

虚拟机模板部署适用于虚拟化环境，管理员将安装Agent的虚拟机制作成模板，通过模板批量派生成多个虚拟机。打开[系统管理/终端部署]，选中[Linux]虚拟机模板部署，如下图。

3.4.3. MAC OS 部署

MAC OS部署Agent支持下载安装包部署和网页推广部署。

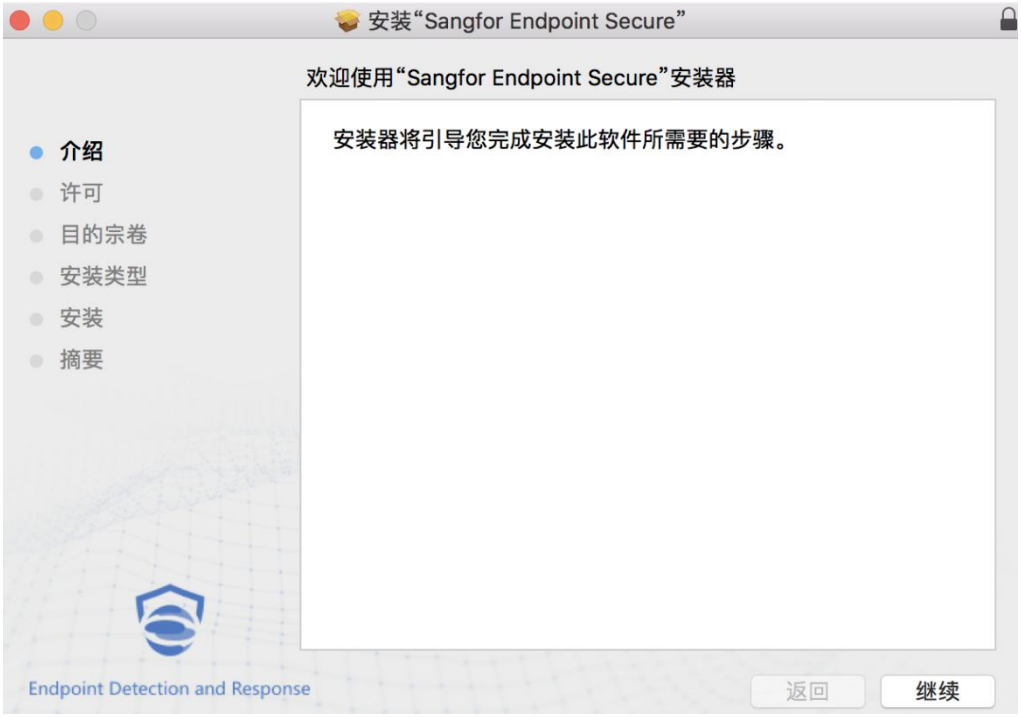
3.4.3.1. 下载安装包部署

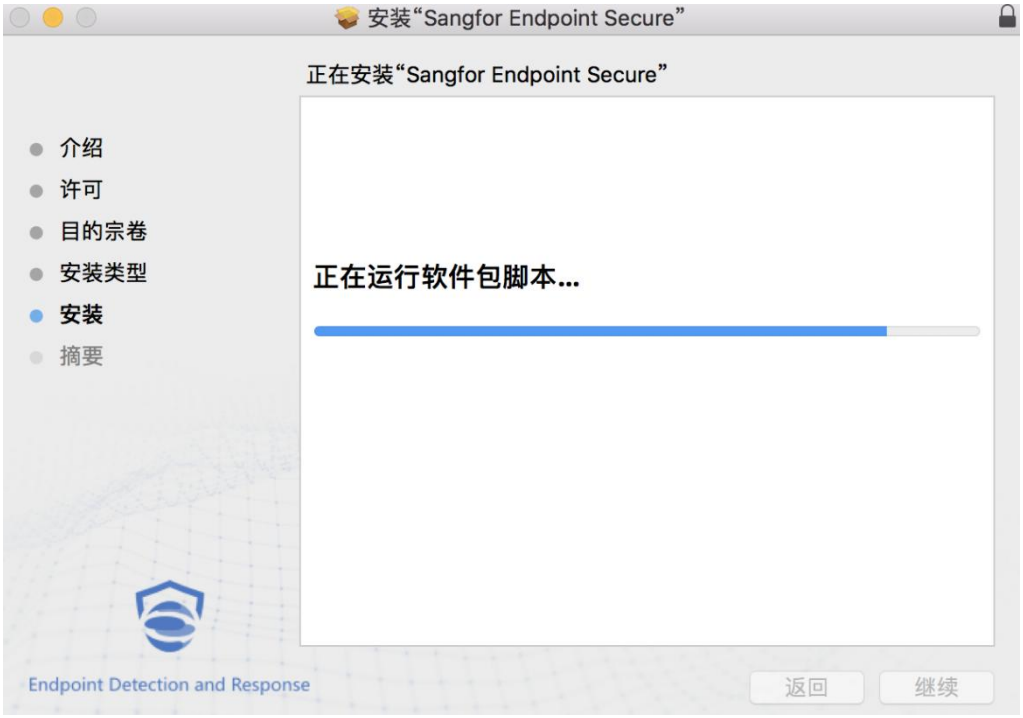
管理员本地下载Agent安装包，通过U盘，网络共享等方式传递给终端用户进行安装部署。

打开[系统管理/终端部署]，选中[MAC]并下载安装包，如下图。

> 说明：
>
> MAC 客户端安装程序默认命名（类似 edr_installer_管理端 IP_4430.exe）包含 EDR 管理端通讯地址和端口信息，下载后请勿更改安装程序名。

双击安装程序，如下图，按照向导进行安装。





安装完成，在MAC OS菜单栏生成EDR图标，说明已正常安装，如下图。

3.4.3.2. 网页推广部署

管理员发布部署通知的web页面，将发布页链接通过邮件、OA等方式发送至终端，终端用户自行下载Agent安装包进行安装部署。

打开[系统管理/终端部署]，选中[MAC]，打开[网页推广部署]，如下图。

编辑推广通知页面标题和内容，点击<下一步>，生成推广链接，如下图。

管理员将推广链接通过邮件、OA等方式发送至终端，终端用户自行下载Agent安装包

进行安装部署，如下图。

3.4.4. 终端 Agent 部署成功确认

安装成功后，终端 Agent 程序将自动连接EDR管理端。在管理端[终端管理/终端分组管理]可以看到终端上线信息，如下图。

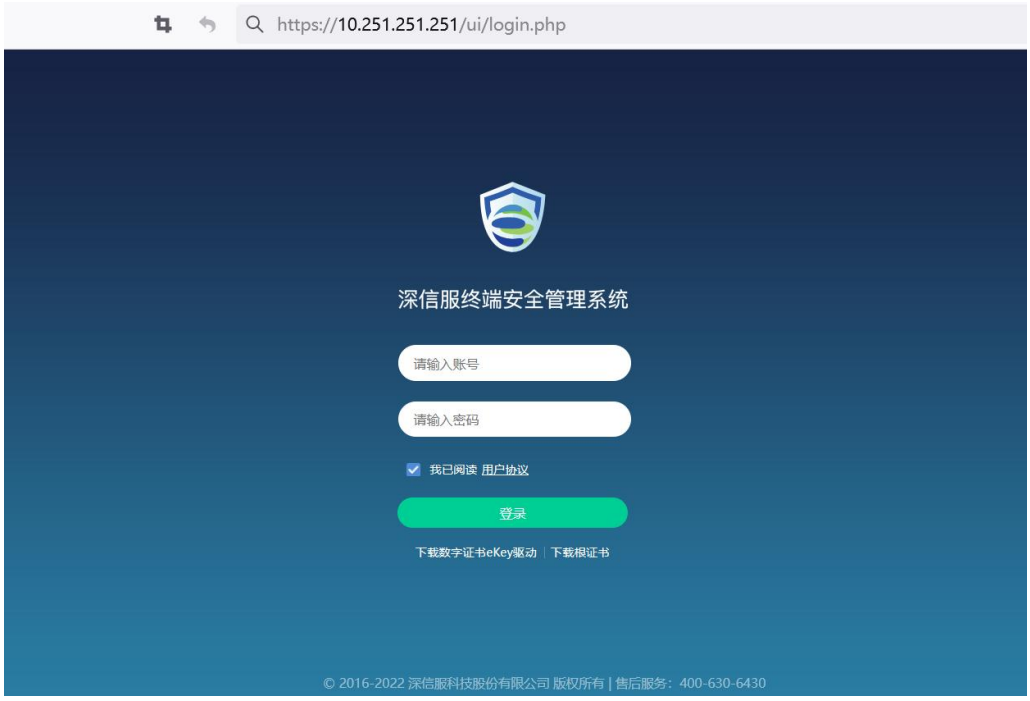
4. 产品使用

4.1. 登录管理端

为保障安全性，EDR管理端需使用HTTPS标准端口登录，登录流程如下：

1.打开浏览器，在地址栏输入https://EDR_IP，默认IP为10.251.251.251 ，并回车跳转。

> 说明：
> 如出现[无法验证此网站的标识或此连接的完整性]的安全提示，请点击<是>即可；
> 浏览器支持 IE11 以上/FireFox/Chrome 等。



2.在登录框输入用户名、密码及验证码，并点击<登录>按钮登录；

> 说明：
> 默认用户名与密码为：admin/admin。

3.首次登录系统会提示管理员修改初始密码，以保护平台安全性。

4.2. 终端管理

通过EDR终端管理页面，可实现对终端的发现、清点及分组管理，同时通过策略对终

端及分组进行管理，策略包括基本策略、病毒查杀、实施防护、安全加固、信任名单、漏洞防护、违规外联、管控防护等。

4.2.1. 终端分组管理

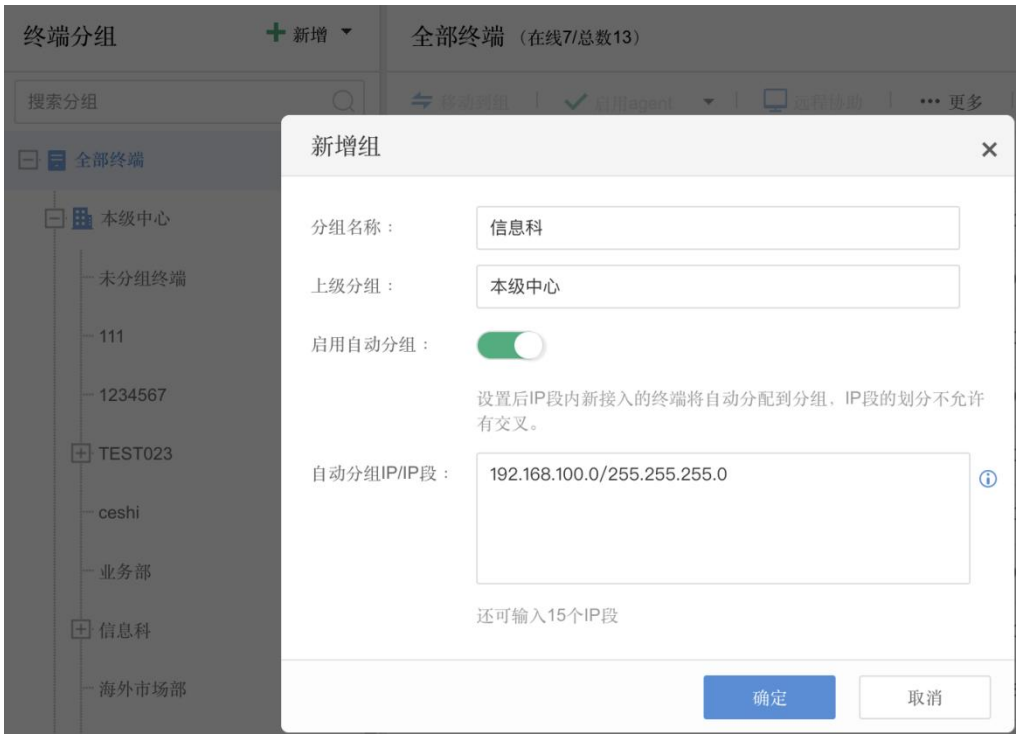
终端分组管理包括终端分组和终端管理，终端分组是通过树形分组形式对接入终端进行统一管理。终端管理可以集中显示终端名称、终端状态、所属组织、IP地址、MAC地址、操作系统、CPU利用率、内存利用率、资产责任人、资产编号和资产位置等信息，也可以对终端下发相关操作指令。

4.2.1.1. 终端分组

EDR支持建立树形组织结构对资产进行管理。需提前梳理业务分组及IP地址规划，根据业务属性建好分组并启用根据IP自动分组，当终端Agent安装时根据终端地址自动上线至所属分组。

分组管理

打开[终端管理/终端分组管理]，点击<新增>增加分组，如下图。



填写分组名称、上级分组、启用自动分组并配置自动分组IP段。当终端Agent安装时根据终端地址自动上线至所属分组。

📖 **说明：**

如果未启用自动分组，则终端默认上线至“未分组终端”，可通过移动终端到指定组实现终端分组。

导入分组

导入分组即通过编辑好的表格进行批量用户导入，具体操作步骤如下：

1.在[终端管理/终端分组管理]页面，点击<新增>导入分组；

2.下载示例文件并依文件内指导进行文件内容编辑；

3.在导入分组弹框中，选择已编辑好的xls、xlsx文件进行上传；

4.选择导入方式，并点击<确定>，导入方式包括：

- 保留原分组信息，信息冲突时，以原信息为主；
- 保留原分组信息，信息冲突时，以导入信息为主；
- 清除本级中心与未分组以外的所有分组，按照新的自动分组规则划分终端分组。

5.在弹出的[新增组]的页面，填写[分组名称]及[上级分组]字段，开启[应用自动分组]功能，并设置IP/IP段，然后点击<确定>；

6.分组生成后，可发现指定IP/IP段对应的终端已移入至该分组，同时管理员也可在[未分组终端]分组中选中需移入的终端进行移入。

📖 **说明：**

移动分组后，终端将继承新终端分组配置的安全策略。

导出分组

1.在[终端管理/终端分组管理]页面，点击<新增>导出分组；

2.在弹出界面，选择导出方式，包括按分组导出及按终端导出两种方式，按终端导出方式可跨分组进行终端选定；

3.选择对应分组及终端后，点击<确定>，系统会自动完成xlsx格式的用户信息导出结果。

4.2.1.2. 终端管理

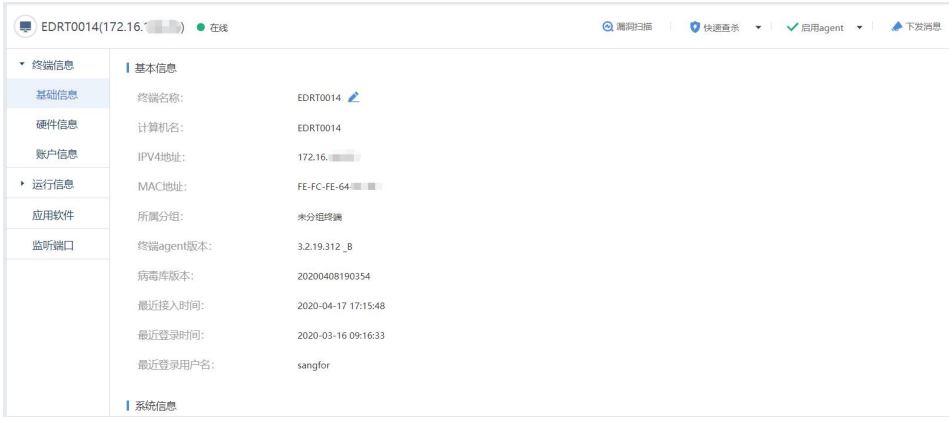
终端管理包括终端信息展示、移动到组、终端远程管理、远程协助、下发消息、导出终端。

终端信息展示

在终端分组管理界面，可展示全部终端的基础信息，如下图所示。

基本信息主要包括：终端状态、所属组织、IP地址、MAC地址、操作系统、CPU利用率、内存利用率、责任人、资产编号、资产位置等内容，管理员可在右侧[...]处进行显示项筛选与指定。

当点击具体终端名称后，会跳转至具体信息展示，如下图所示，可对该终端进行漏洞扫描、快速查杀、全盘查杀等指令下发操作，同时当发现客户端安装Agent存在异常时，可以从管理端对当前终端进行启用、禁用、卸载操作。



1.基础信息

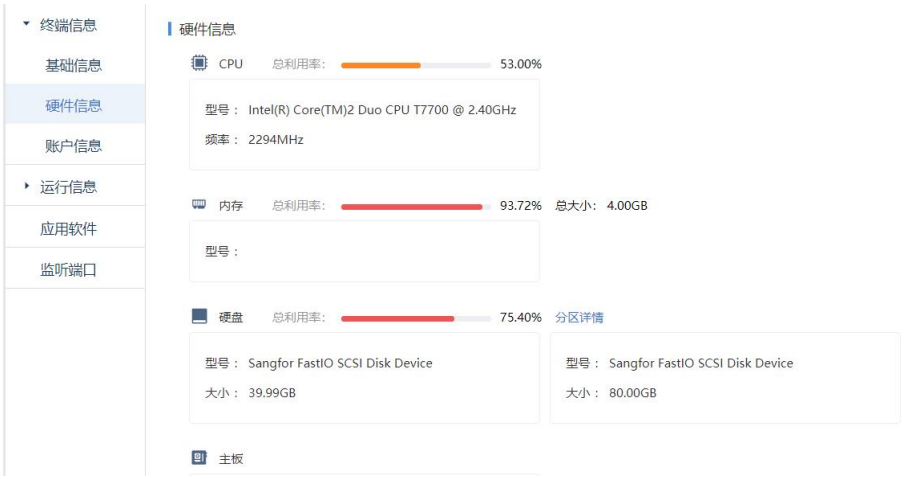
基本信息：终端名称（支持编辑）、计算机名、IPV4/MAC地址、所属分组、终端agent版本、病毒库版本、最近接入/登录时间、最近登录用户名等信息；

系统信息：包括操作系统、版本号、激活状态、安装时间等；

管理信息（支持编辑）：包括资产责任人、宿主机、资产编号、资产位置、工号、联系电话、联系邮箱等信息。

2.硬件信息

硬件信息：包括CPU、内存、硬盘、主板、网卡、声卡及显示器相关型号及使用率。



3.账户信息

账户信息：包括本终端已创建的账号名及对应的账户状态、类型、权限、风险（可点击叹号查看具体风险）、最近修改密码/登录时间，密码最长使用期限及登录历史查看。

说明：

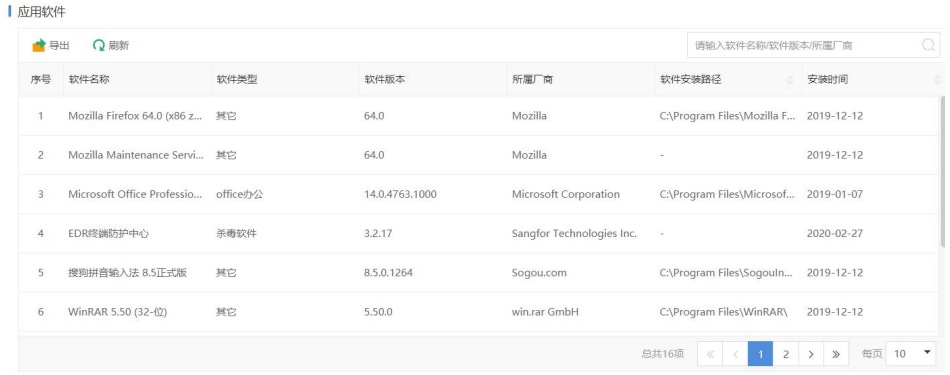
点击右侧[•••]可进行显示项筛选与指定。

4.运行信息

运行信息包括运行进程、运行服务、网络连接、启动项、计划任务、开放共享。

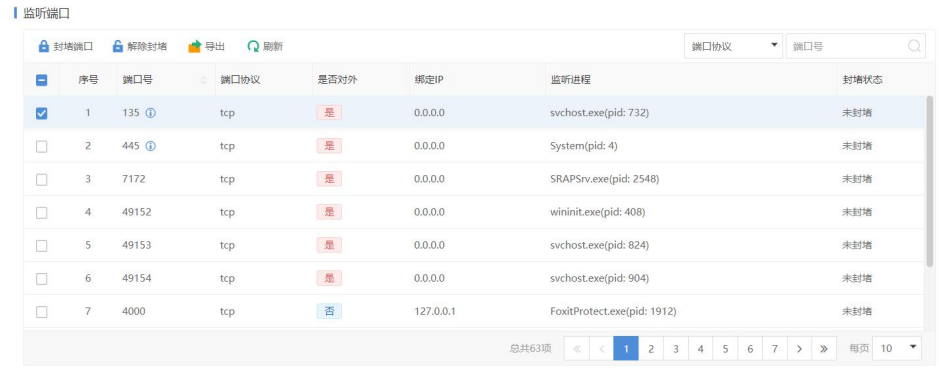
5.应用软件

应用软件包括本终端已安装的软件名称、类型、版本、所属厂商、安装路径及安装时间等信息，同时可实现一键导出及针对软件名称/版本/所属厂商进行筛选。



6.监听端口

可显示本终端监听端口的端口号、协议、绑定IP、监听进程、是否对外及封堵状态，可选中相应端口进行封堵/解封，以及实现导出与通过端口协议及端口号进行检索。

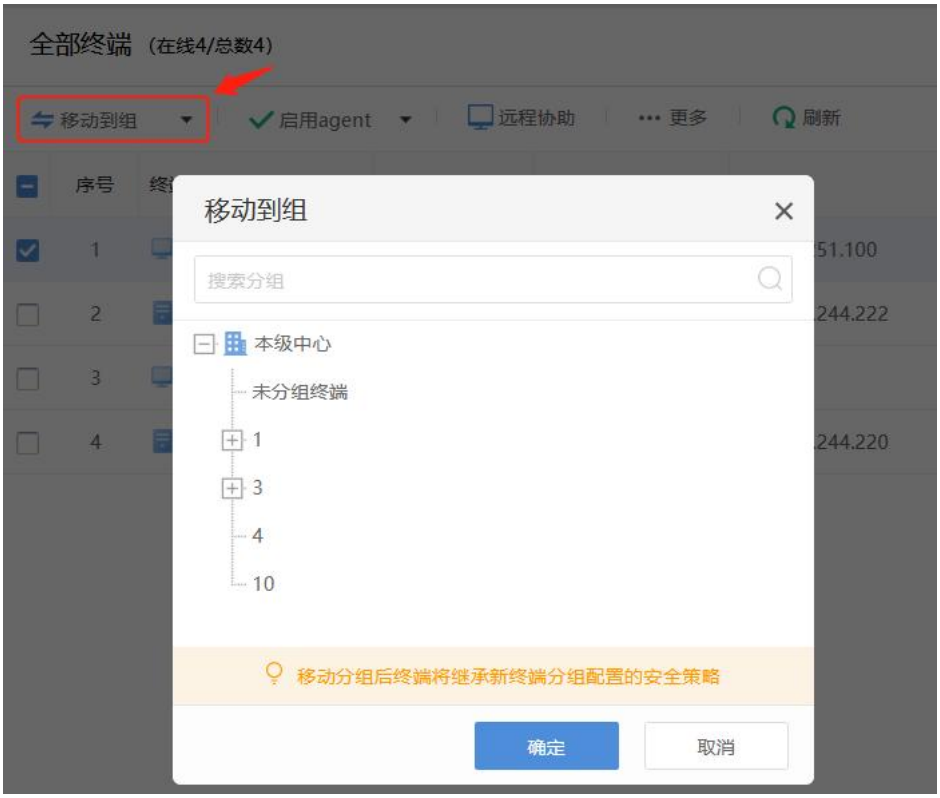


7.信任区

可以在管理端查看客户端自行添加的信任文件或信任目录，防止终端添加不合理、管理员也不知道，最终导致终端中毒。查看[终端详情/信任区]即为终端自行添加的信任文件，如下图。

移动到组

对于上线的终端，可以通过[移动到组]手动调整其分组，如下图。



当启用根据IP自动分组功能后，被手动移动调整分组的终端会自动加上 标记，说明该终端所属分组被锁定，不会再次根据IP自动分组，如下图。

当被锁定分组的终端需要恢复自动分组时，可以通过选中此终端并点击<允许自动分组>进行恢复，如下图。

说明：

1.低版本开启自动分组功能且已经对部分终端手动移动调整了分组，升级至 3.5.18 及以后版本，为避免升级前已经手动调整分组的终端重新根据 IP 自动分组。升级至此版本后自动分组功能会默认关闭，您可以通过[终端管理/终端分组管理/新增]选项卡下拉，点击<自

动分组管理>启用自动分组功能，同时批量选中升级前已经手动调整分组的终端设置为禁止自动分组。

2.打开[终端管理/终端分组管理]右上角[新特性]了解 IP 自动分组新特性介绍。

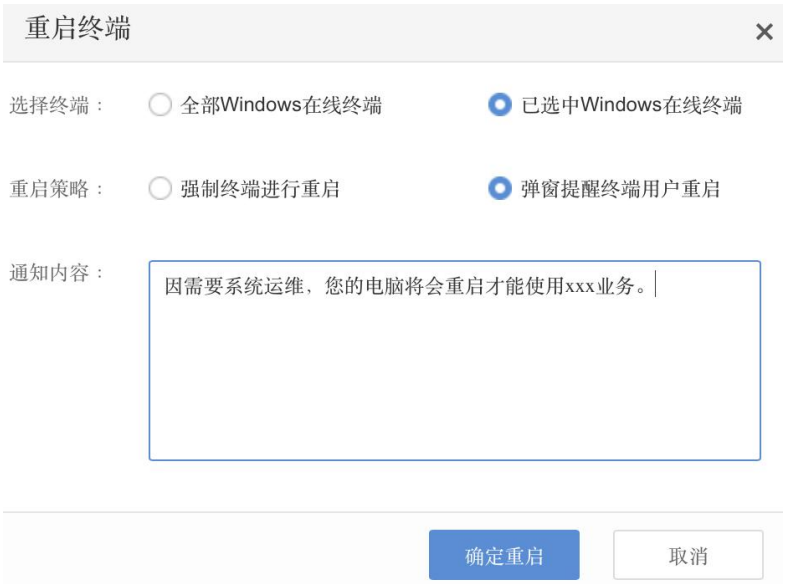
终端远程管理

终端管理能够对选中的终端进行启用、禁用、重启、卸载或移除操作，同时也可以对终端下发通知消息，如下图。

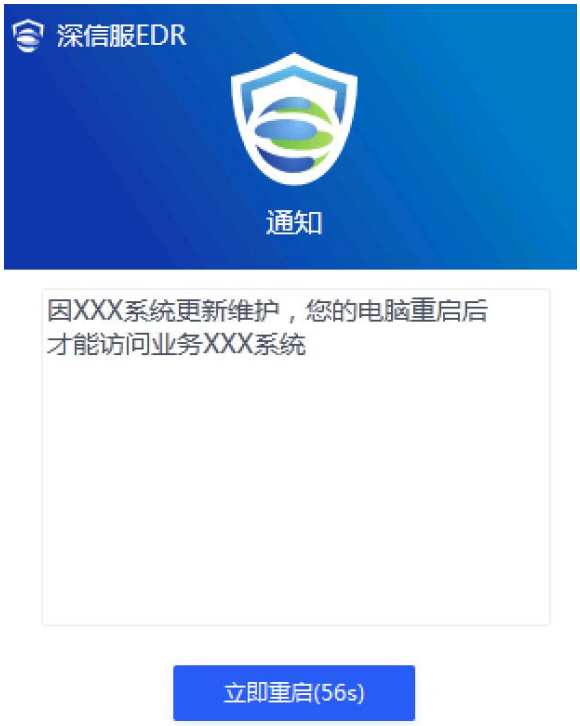
重启终端

在全部终端页面，选中单台或多台终端，可以控制重启终端，如下图。

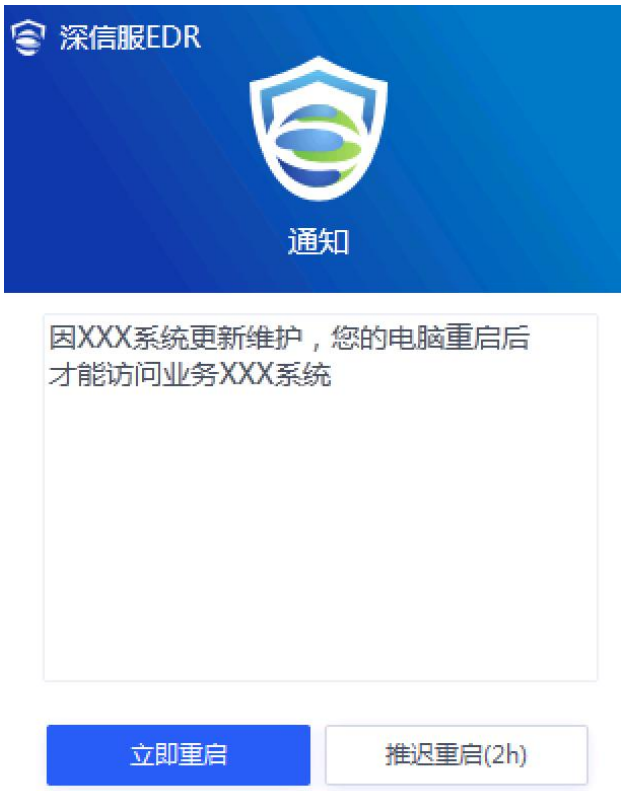
点击<重启终端>，设置终端重启策略。



当选中[强制终端进行重启]时，会倒计时1分钟重启，通知终端用户如下：



当选中[弹窗提醒终端用户重启]时，需要终端用户自己重启，通知如下：



> 说明：
>
> 此功能仅支持 windows 系统终端。

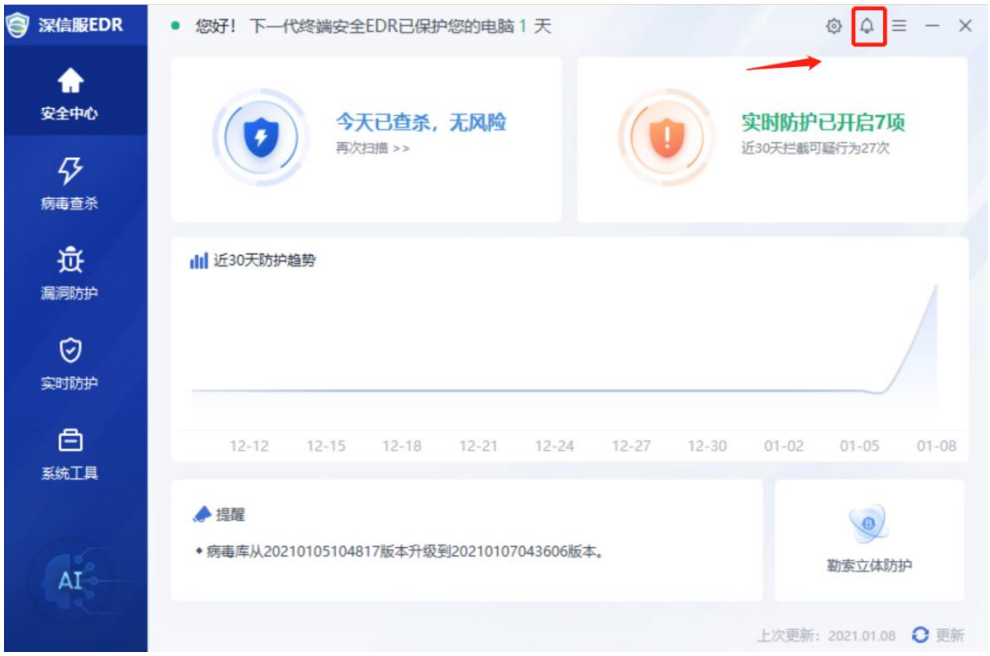
下发消息

在全部终端页面，选中单台或多台终端，可以对终端下发消息，操作步骤如下：

1.在平台的[终端管理/终端分组管理/全部终端]，勾选单台或多台终端，并点击横栏的[下发消息]按钮，进入编辑界面，如下图：

2.完成信息编辑后点击<确认>，选中终端将会接收到相应通知，如下图所示。

3.终端上可以点击<知道了>或点右上角的“X”关闭信息，可以通过下图位置查看历史消息。



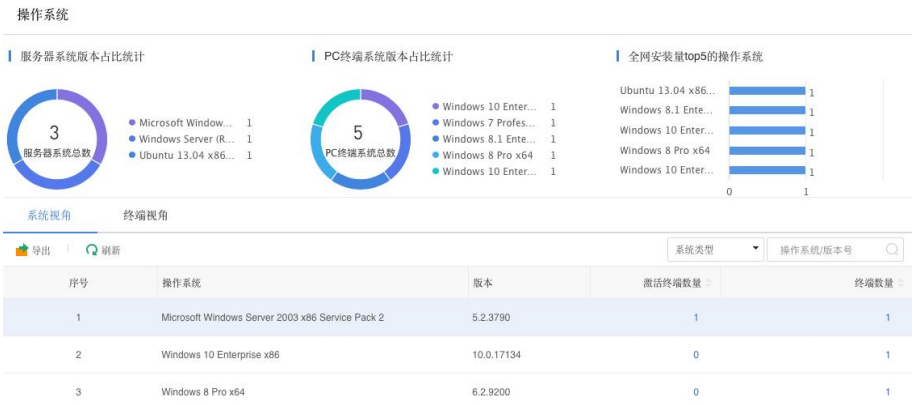
导出终端

打开管理端[终端管理/终端分组管理]，选中需要导出的终端，并点击横栏的[导出终端]按钮，如下图，将以excel表格形式导出终端及终端详情。

4.2.2. 终端清点

终端清点可针对全网终端进行清点并进行统计化显示，清单范围包括操作系统、应用软件、监听端口和终端账户。

操作系统清点

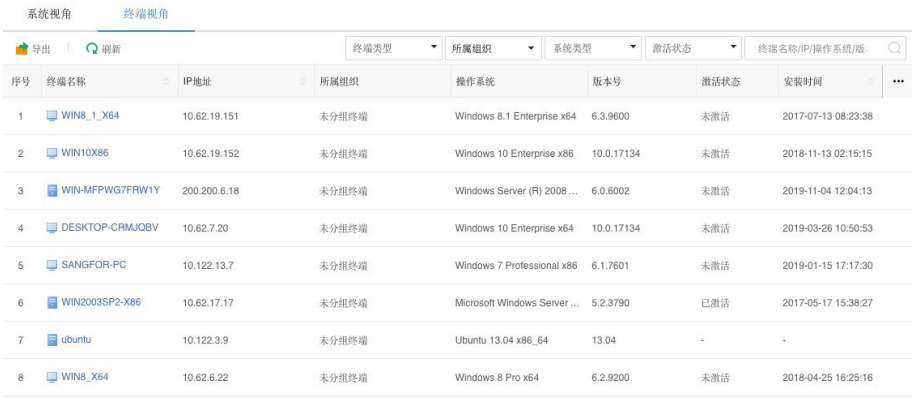


操作系统清点页面可展示全网主机整体的操作系统版本及分布，如上图所示，主要页面信息包括：

1.可展示服务器、PC终端的系统版本占比与全网安装量TOP5的操作系统信息。

2.可通过**系统视角**查看同一系统的安装及激活终端数量，点击[数量标签]，可跳转显示对应详情信息，也可点击[导出]进行表格形式导出，如下图。

3.可通过**终端视角**查看详细终端的IP地址、所属组织、系统类型、版本号、激活状态、安装时间及责任人等信息，如下图。



说明：

点击<导出>可直接以表格形式导出，方便管理员进一步统计分析；

可根据终端类型、所属组织、系统类型、激活状态等条件进一步筛选或直接在搜索栏进行检索。

应用软件清点

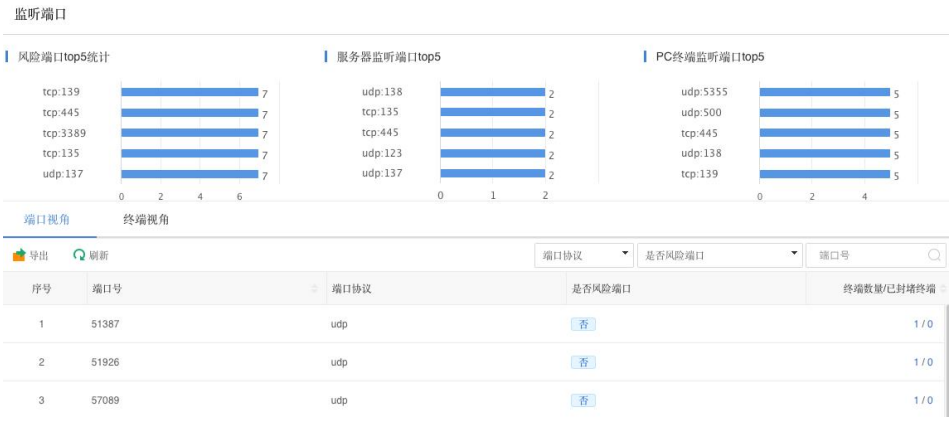
应用软件清点页面可展示全网主机安装软件汇总信息和详细信息，以便进一步对某些风险软件进行全网摸底和盘点，进而采取版本升级或应用加固等安全保障措施，如上图所示，主要页面信息包括：

1.可展示全网终端的软件类型分布、服务器/PC终端安装量TOP5的软件；

2.可根据**软件视角**查看软件类型、软件版本、所属厂商及安装此软件的终端数量等信息；

3.可根据**终端视角**查看各类型终端的所属组织及安装软件数量、详细信息（点击软件数量可跳转显示）等信息，支持通过终端类型、所属组织或搜索框进行指定终端检索。

监听端口清点



通过监听端口清点页面，可高效查看全网主机对外开放的端口信息，管理员可通过全局、服务器、终端等维度进行风险端口查看与处理，如上图所示，主要页面信息包括：

1.可展示风险端口TOP5、服务器/PC监听端口TOP5。

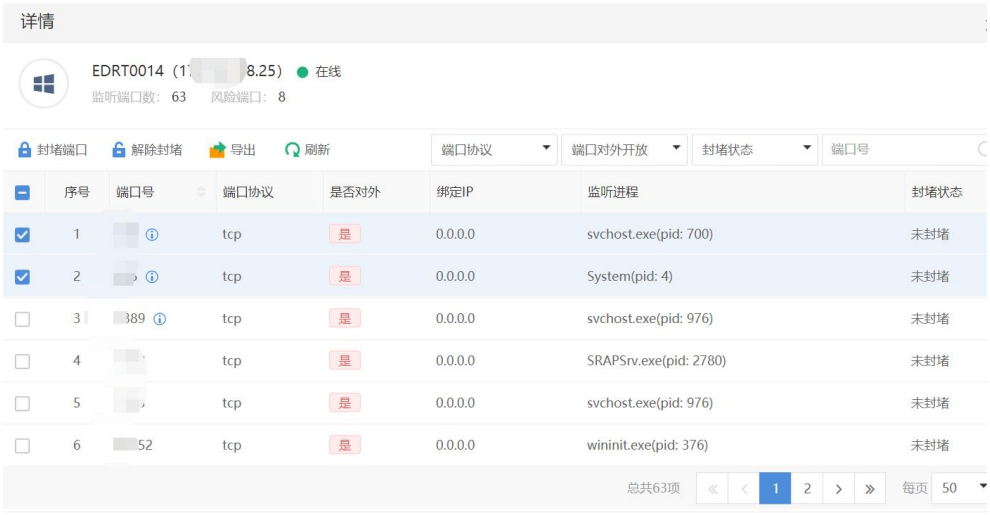
2.可通过**端口视角**查看开放某一端口的终端数量，点击[终端数量/已封堵终端]这列的数字，可跳转至开放该端口的终端详情页面进一步分析，如下图所示。

说明：

封堵端口：可选中需要封堵该端口的终端，点击[封堵端口]可对选中终端进行封堵，点击[解除封堵]可对已封堵的端口接触封堵；

数据导出：点击<导出>可直接以表格形式进行导出，方便管理员进一步统计分析。

3.在**终端视角**，可以查看每个终端的监听端口数、终端状态、终端名称、IP地址以及所属组织，点击<监听端口数>，可以查看该终端监听的端口详情，并可以根据实际使用情况进行封堵端口，如下图所示。

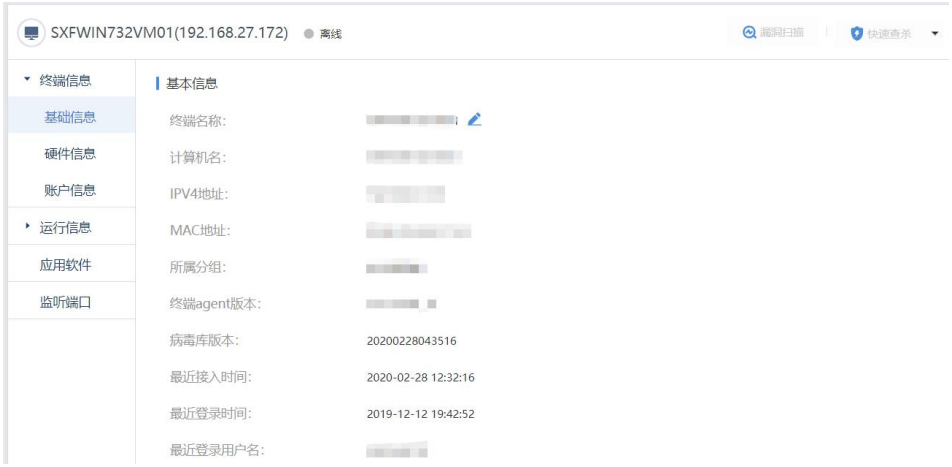


终端账户清点

通过终端账户清点页面，可查看全网主机的账号信息，包括账户状态、类型、权限、密码期限等信息，同时针对账户信息平台会进一步进行风险分析，提供账户风险信息提醒，如隐藏账号、弱密码账号、可疑root权限、长期未使用、夜间登录、多IP登录等，从而帮助管理员削减主机的风险暴露面，如上图所示，主要页面信息包括：

1.可展示账户权限、风险账户及长期未修改密码账户分布统计情况；

2.可通过账户状态、权限类型、账户风险类型、密码修改时间及登录时间等信息类型进行筛选，同时搜索栏也支持对终端名称/IP地址/账户进行检索，点击[具体终端]可跳转至详情页面，如下图。



4.2.3. 终端发现

终端发现功能可通过内网主动探测，识别企业内网中未管控终端（即未安装EDR客户端），实现高效的内网安全薄弱点与全网资产探测，及时防范，如下图所示。

1.点击[立即扫描]并完成扫描参数设置后，会进行内网扫描，扫描参数包括：

发起扫描设备：可设置由EDR管理端发起扫描，或由已安装EDR客户端的Linux终端发起扫描。

📖 **说明：**

如果扫描范围大，建议设置由多个已安装 EDR 客户端的 Linux 终端并发扫描，提升扫描速度。

扫描网端：设置扫描范围，支持填写主机地址或网段范围。

📖 **说明：**

[高级设置]可选择扫描协议及扫描端口，一般情况保持默认即可。

2.点击<确定>后，会弹出如下图所示的风险告警，在了解并认可相关风险后，可点击<确定>执行扫描操作。

📖 **说明：**

扫描过程中可以点击[取消扫描]结束当前扫描任务。

3.扫描完成后，可在页面查看未安装EDR的终端，可点击<导出>按钮，以表格形式导出，方便方便管理员进一步统计分析，如某终端不需要安装EDR客户端，可以点击<忽略>。

4.3. 策略配置

策略中心主要用于为分组制定对应的安全策略，安全策略涵盖基本策略、病毒查杀、实时防护、勒索防护、信任名单、漏洞防护、桌面管控等安全策略，不同终端支持功能如下。

表11 Windows PC、Windows Server、Linux对各安全策略支持情况

安全策略	Windows PC	Windows server	Linux
基本策略	√	√	×
病毒查杀	√	√	√
文件实时监控	√	√	√
webshell 检测	×	√	√
勒索病毒防护	√	√	×
暴力破解检测	√	√	√
高级威胁防护	√	√	×
服务器可信进程防护	×	√	×
信任名单	√	√	×
漏洞修复	√	√	×
违规外联	√	√	×
USB 外设管控	√	√	×
终端广告弹窗拦截	√	×	×
远程桌面二次认证	×	√	×

4.3.1. 基本策略

通过基本策略，可以设置Windows系统终端的资产信息登记、管理员联系方式、弹框提醒、密码保护以及终端行为与日志信息采集等策略，具体配置方式如下。

终端资产信息登记

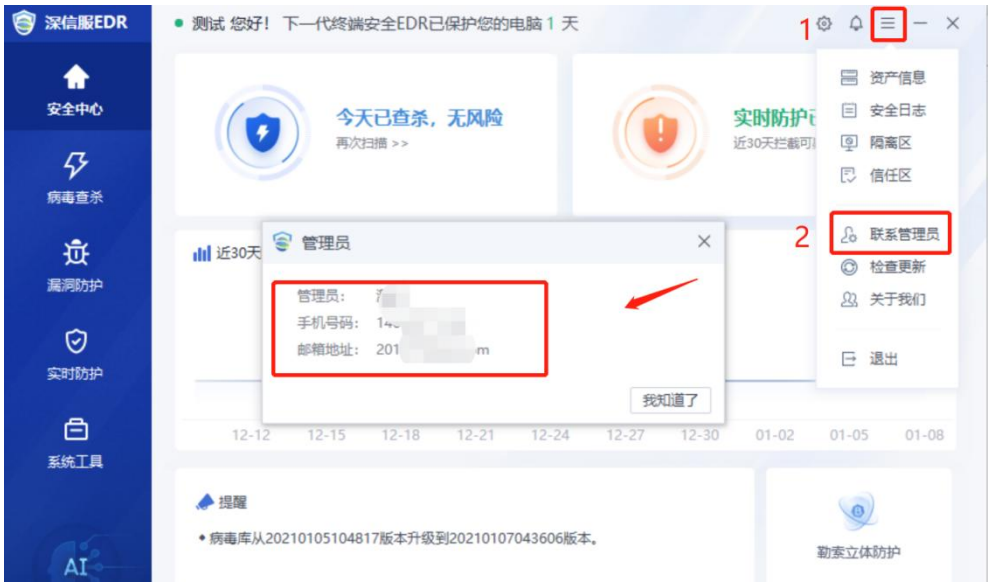
开启本选项后，受控终端需登记资产信息至平台，在策略中可对上报信息内容进行指定，内容包括责任人名称、资产名称、电话号码、邮箱地址、资产位置、资产编号及工号等信息，如下图所示。

配置完成后，终端可在系统消息中查看详情，并根据要求完成终端登记页面，如下图。

终端管理员联系方式

开启本选项后，终端用户可查看管理员联系方式，联系方式包括管理员名称、手机号及邮箱地址，如下图所示。

终端查看管理员信息，如下图所示。



终端弹框提醒（终端免打扰模式）

开启后终端发现各类异常安全问题后，将不再通过弹窗告知终端用户，配置界面如下图所示。

📖 **说明：**

当点亮图中锁定图标，则禁止客户端修改此配置，如解除锁定，则客户端可自行变更此配置。

终端防护中心密码保护

终端防护中心密码保护设置可以设置终端Agent退出、卸载、加白名单文件时需要密码保护，如下图。

当开启终端“防退出”密码保护，终端退出时需要授权密码才可以退出，如下图。

当开启终端“防卸载”密码保护，终端卸载时需要授权密码才可以卸载，如下图。

当开启终端“加白文件”密码保护，终端加入信任文件时需要授权密码才可以加信任，防止文件被恶意加白，导致终端得不到EDR安全保护，如下图。

> 说明：
>
> 此处终端“加白文件”密码保护只对 Windows PC 有效，Windows Server“加白文件”密码保护功能参考本手册[管理端使用/策略中心/勒索防护/远程桌面二次认证]章节。

终端行为与日志信息采集设置

EDR可以采集终端系统日志和终端行为日志，并传输给SIP或NGSOC进行集中分析。当管理员开启终端系统日志采集时，采集的日志包括windows和部分linux终端事件管理中的安全日志；当管理员开启终端行为数据采集的时间，采集的行为数据包含文件、进程、网络、注册表、DNS、计划任务、主机信息等。

当基本策略完成配置后，点击<保存>，可保存当前策略配置，如需恢复默认配置，可点击[恢复默认策略]，点击[应用到下级分组]，可将本组策略全部继承至下级子组。

4.3.2. 病毒查杀

病毒查杀策略支持对Windows和Linux终端的定时查杀、查杀扫描及终端病毒库升级等策略进行配置，具体配置方式如下。

📖 **说明：**

可点击 Windows/Linux 系统旁“倒三角”符号进行系统切换，同时支持将 Windows 系统策略同步至 Linux 系统。

定时查杀

通过定时查杀配置，可实现在指定时间内对内网终端进行查杀扫描，配置页面如下图所示。

定时查杀可以设置快速扫描和全盘扫描两种类型，每种扫描类型有极速、均衡、低耗三种扫描模式，主要区别在CPU占用率情况不同：

极速：全速扫描，不限制扫描软件自身的CPU占用率；

均衡：扫描速度和CPU占用率达到一定平衡，限制CPU占用率不超过30%；

低耗：扫描时尽量少占用CPU资源，限制CPU占用率不超过10%。

查杀扫描

通过查杀扫描，可定义扫描文件类型、扫描文件、恶意文件处置机制以、设置扫描引擎以及资源占用控制等，配置界面如下图所示。

📖 **说明：**

当点亮[查杀扫描]后锁定图标，则禁止客户端修改此配置，如解除锁定，则客户端可自行变更此配置。

文件类型：可选病毒查杀文件类型，包含文档文件、脚本文件、可执行文件、压缩文档、低风险文件。

📖 **说明：**

1.压缩文档，当前支持 7z、XZ、BZIP2、GZIP、TAR、ZIP、WIM 等 23 种类型，点击压缩文档旁的说明符号“ ⓘ ”，可以查看详细信息。

2.低风险文件，是经过分析筛选得出的风险极低的文件，建议不选中。病毒查杀时过滤 42 种低风险文件，提升扫描速度、降低 SAVE 引擎内存占用。低风险文件类型包括 .vmdk 、.iso、.lib、.a、.nsf、.pdb、.dmp、.db、.hdmp、.idb、.pch、.vdf、.pak、.evtx、.imd、.aac、.webm、.ntf、.cvd、.mof、.mdf、.mdb、.otf、.tlb、.jpg、.jfif、.jpeg、.jpe、.jp2、.png、.gif、.bmp 、.mp3、.mp4、.m4a、.mkv、.wmv、.wma、.tif、.tiff、.flv、.ogg

---

扫描文件：可配置扫描文件大小限制及扫描压缩包层级。

发现威胁：发现威胁文件的处置机制，包括自动处置-业务优先、自动处置-安全优先和仅上报不处置三种处理方法，默认配置是自动处置-业务优先。

- **自动处置-业务优先：**根据预置威胁判断机制，自动修复或隔离系统判断 100%为威胁的文件，系统判断为可疑威胁文件不自动修复或隔离、仅将可疑威胁文件上报至管理端，由用户分析处置；
- **自动处置-安全优先：**自动修复或隔离所有威胁文件，处置后的文件可在隔离区进行恢复，适用于严格保护场景；

- **仅上报不处置：**不自动修复或隔离病毒文件，仅将被感染文件的信息上报至管控平台。适用于有人值守且用户了解如何处置不同的病毒威胁的场景。

引擎配置：病毒查杀主要提供了四种引擎，包括深信服SAVE人工智能引擎、基因特征引擎、行为分析引擎和云查引擎。不同引擎组合形成四种模式，包括标准模式、低误报模式、高检出模式、资源低耗模式和自定义模式，根据业务场景选择适合模式，如下图。

模式类型	适用场景	内存占用	检出率	误报率
标准模式	通用的服务器和办公网场景均可适用	中低	高	低
低误报模式	通用办公场景和较为重要的服务器系统如财务、OA等	较低	高	极低
高检出模式	有严格保护要求且较为稳定的服务器场景	中低	极高	中低
资源低耗模式	适用于存在高负载和老旧系统等终端场景	极低	高	低

🕮 **说明：**

1.全新部署时，引擎默认配置为标准模式；
2.老版本升级时，引擎配置平滑转换为自定义模式；
3.高检出模式可能存在误报要高于其它模式，正常使用时不建议使用高检出模式，需要在工程师评估后确定是否使用高检出模式。

资源占用控制：当开启资源优化模式时，可以更大程度地限制EDR对CPU的资源占用，可能会相对延长病毒扫描时间，适用于老旧电脑场景、桌面云场景、高负载场景等。

🕮 **说明：**

开启资源优化模式时，EDR 对 CPU 的资源占用情况如下：
1.极速模式限制 CPU 占用率不超过 50%；
2.均衡模式限制 CPU 占用率不超过 20%；
3.低耗模式限制 CPU 占用率不超过 5%。

终端病毒库升级

通过终端病毒库升级配置，可定义终端病毒库的升级服务器，可选择为[从本控制中心升级]或从[启用多服务器升级]。如选择[启用多服务器升级]，可以配置多个升级服务器，如下图所示。

4.3.3. 实时防护

通过实时防护策略，包括文件实时防护、WebShell检测、暴力破解检测和无文件攻击防护配置。

📖 **说明：**

点击右侧 图标，则禁止客户端修改此配置，如解除锁定，则客户端可自行变更此配置。

文件实时防护

文件实时防护可实时监控终端文件读、写、执行，防止恶意文件影响终端运行。如下图分别为Windows终端和Linux主机文件实时防护策略配置。

其中：

防护级别：支持设置高、中、低三种防护级别，不同的防护级别对恶意文件的防护能力如下：

- 高：监控文件的所有操作方式，对电脑性能有一定影响；
- 中：监控文件的执行、写入，确保病毒无法入侵及运行，极少影响电脑性能；
- 低：监控文件的执行，确保病毒无法运行，不影响电脑性能。

文件类型：可选实时监控文件类型，包含文档文件、脚本文件、可执行文件、压缩文档、低风险文件。

📖 **说明：**

1.压缩文档，当前支持 7z、XZ、BZIP2、GZIP、TAR、ZIP、WIM 等 23 种类型，点击压缩文档旁的说明符号“ ⓘ ”，可以查看详细信息。
2.低风险文件，是经过分析筛选得出的风险极低的文件，建议不选中。病毒查杀时过滤 42 种低风险文件，提升扫描速度、降低 SAVE 引擎内存占用。低风险文件类型包括 .vmdk 、.iso、.lib、.a、.nsf、.pdb、.dmp、.db、.hdmp、.idb、.pch、.vdf、.pak、.evtx、.imd、.aac、.webm、.ntf、.cvd、.mof、.mdf、.mdb、.otf、.tlb、.jpg、.jfif、.jpeg、.jpe、.jp2、.png、.gif、.bmp 、.mp3、.mp4、.m4a、.mkv、.wmv、.wma、.tif、.tiff、.flv、.ogg

扫描文件：设置过大的或压缩层级较大的文件进行跳过不监控（绝大多数情况恶意文件都是较小的文件）；

引擎配置：主要提供了四种引擎，包括深信服SAVE人工智能引擎、基因特征引擎、行为分析引擎和云查引擎。不同引擎组合形成四种模式，包括资源低耗模式、低误报模式、严格保护模式和自定义模式，根据业务场景选择适合模式，如下图。

📖 **说明：**

1.全新部署时，引擎默认配置为资源低耗模式；
2 老版本升级时，引擎配置平滑转换为自定义模式；

发现威胁：发现威胁文件的处置机制，包括自动处置-业务优先、自动处置-安全优先和仅上报不处置三种处理方法，默认配置是自动处置-业务优先。

- **自动处置-业务优先：**根据预置威胁判断机制，自动修复或隔离系统判断 100%为威胁的文件，系统判断为可疑威胁文件不自动修复或隔离、仅将可疑威胁文件上报至管理端，由用户分析处置；

- **自动处置-安全优先：**自动修复或隔离所有威胁文件，处置后的文件可在隔离区进行恢复，适用于严格保护场景；
- **仅上报不处置：**不自动修复或隔离病毒文件，仅将被感染文件的信息上报至管控平台。适用于有人值守且用户了解如何处置不同的病毒威胁的场景。

WebShell检测

通过WebShell检测策略，可定义WebShell检测方式和发现WebShell后门的处理方法。WebShell检测对Windows Server和Linux生效。配置界面如下图所示。

其中：

检测方式：包括Agent首次安装后触发扫描、实时检测和定时检测三种检测方式。

- Agent 首次安装后触发扫描：在首次安装后对网站根目录及其子目录进行检测扫描；
- 实时检测：对网站根目录及其子目录新增文件进行检测；
- 定时检测：对网站根目录及其子目录所有文件进行定期检测。

发现WebShell：设置发现webshell后的处理动作，包括[自动处置]及[仅上报，不处置]两种方式。

自定义Web目录：设置webshell检测目录。默认检测web服务器所在目录，也可以检测自定义的Web目录。

暴力破解检测

暴力破解检测能够检测RDP、SMB、SSH暴力破解并拦截，其中Windows终端支持RDP和SMB暴力破解检测，Linux终端支持SSH暴力破解检测。

1.**Windows系统侧**，配置界面如下图所示。

其中：

- **快速暴破阈值：**可定义单分钟内联系爆破超过几次就定义为快速暴破，RDP 快速暴破阈值填写范围为 1-100，SMB 快速暴破阈值填写范围为 20-1000，而慢速暴破及分布式暴破类型会由系统按只能算法触发检测机制。
- **发现 RDP/SMB 暴力破解：**可选择[自动封堵]或[仅上报，不封堵]的后续处置策略。

2.**Linux系统侧**，配置界面如下图所示。

其中：

- **快速暴破阈值：**可定义单分钟内联系爆破超过几次就定义为快速暴破，SSH 快速暴破阈值填写范围为 1-100，而慢速暴破及分布式暴破类型会由系统按只能算法触发检测机制；
- **发现 SSH 暴力破解：**可选择[自动封堵]或[仅上报，不封堵]的后续处置策略。

无文件攻击防护（仅支持Windows）

无文件攻击主要利用存在缺陷的应用程序，将代码注入到正常的系统进程（内存、注册表、powershell脚本、Office文档），进而获得访问权，并在目标设备执行攻击命令的一种高级攻击手段。通过无文件攻击防护，可对可疑的powershell脚本进行加测并处置，配置界面如下图所示。

其中：

开启可疑powershell脚本执行检测：需要同时开启文件实时防护策略，防护功能才可生效；

发现可疑powershell脚本执行：可设置为[自动阻断脚本执行]或[仅告警，不阻断]。建议默认设置为[仅告警，不阻断]，当发现可疑powershell脚本执行时：

- 针对 PC：对 powershell 脚本执行进行报警并挂起，由用户选择是否放行或阻断；
- 针对服务器：对 powershell 脚本执行进行报警但不挂起，由用户选择是否阻断或忽略。

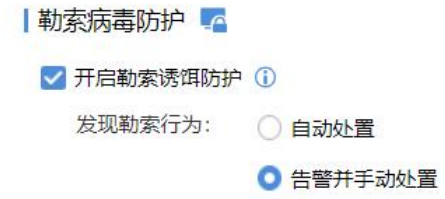
弹出如下告警。

4.3.4. 勒索防护

勒索防护策略可以设置勒索诱饵防护策略、远程桌面二次认证和服务器可信进程防护。

勒索病毒防护（仅支持Windows）

通过勒索病毒防护，可在终端操作系统关键目录下投放诱饵文件，当终端感染勒索病毒时，会先加密诱饵文件，EDR客户端及时进行报警拦截，从而更早更及时地发现和清除未知勒索病毒，避免终端业务文件或业务文件被加密，配置页面如下图所示。



其中：

- **开启勒索诱饵防护：**需要同时开启文件实时防护策略，防护功能才可生效。
- **发现勒索行为：**设置发现勒索病毒后的处置动作，建议设置[告警并人工处置]，当终端发现勒索病毒时，电脑右下解会弹出如下图告警提示。

远程桌面二次认证（仅支持windows server）

RDP远程暴破登录是目前黑客攻击的常用手段之一，黑客可利用远程登陆控制服务器，进而进行勒索攻击等。为了保障您的业务安全，建议您开启此功能。

📖 **说明：**

此功能仅支持 windows Server 操作系统主机。

认证方式

1.远程桌面登录二次认证

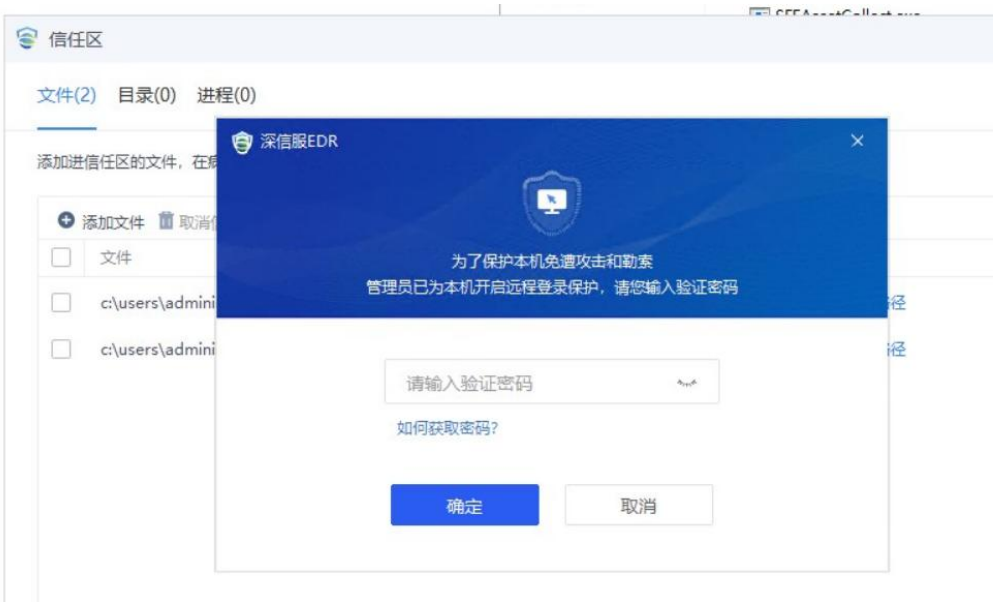
防止黑客成功通过远程桌面登录服务器、轻松拿到服务器权限，可以设置认证方式为远程桌面登录二次认证。

设置认证方式为远程桌面登录二次认证后，当黑客成功通过远程桌面登录服务器时，EDR对服务器进行锁屏保护，如下图，需要通过EDR二次认证才能拿到服务器权限，从而保护服务器安全，建议认证方式选择此项。

2.远程桌面文件信任二次认证

防止黑客将病毒文件加入EDR信任名单、并植入勒索病毒进行勒索，可以设置认证方式为远程桌面文件信任二次认证。

黑客成功登录服务器并尝试植入勒索病毒，由于服务器安装了EDR进行保护，勒索病毒默认无法运行。如果黑客将勒索病毒加入信任名单，则可以成功植入勒索病毒并进行勒索。当认证方式设置为远程桌面文件信任二次认证后，黑客对文件加信任时，需要通过EDR二次认证才可以加信任，避免了病毒文件植入，如下图。



认证密钥

1.验证码验证

验证码为管理员手机号码后6位，如15258227998，设置验证码为227998。打开[终端管理/策略中心/基本策略]，配置终端管理员联系方式，如下图。

📖 **说明：**

建议认证密钥设置为验证码验证、且正确配置管理员手机号，服务器运维管理员可以通过公司通讯录或 EDR 托盘获取管理员手机号，从而获得远程桌面二次认证验证码。

2.自定义密码验证

设置自定义密码验证后，服务器管理员是不知道该密码的，避免敏感时间段无法远程访问服务器，需尽快将自定义的密码通知到服务器管理员。

策略生效时间段

策略生效时间段设置远程桌面二次认证生效时间，默认是所有时间段生效。

免二次认证白名单

白名单内的IP在敏感时间段通过远程桌面登录服务器不需要远程桌面二次认证。访问服务器可信的电脑可以加入白名单。

服务器可信进程防护（仅支持windows server）

服务器可信进程防护对服务器系统或服务器特定目录进行安全防护，只允许可信进程运行、读写操作，同时支持开启远程登录保护功能。

> 📖 **说明：**
>
> 此功能只适用 Windows Server，不适用 Windows PC 和 Linux 系统。

场景一：服务器系统防护

适用场景：

适用于保护运行稳定的服务器系统，阻止不可信进程（如未知勒索病毒等恶意病毒）在服务器运行，从而达到保护服务器安全的目的。

配置步骤：

步骤1. 服务器病毒查杀

先对服务器进行病毒查杀，确认服务器当前环境安全。

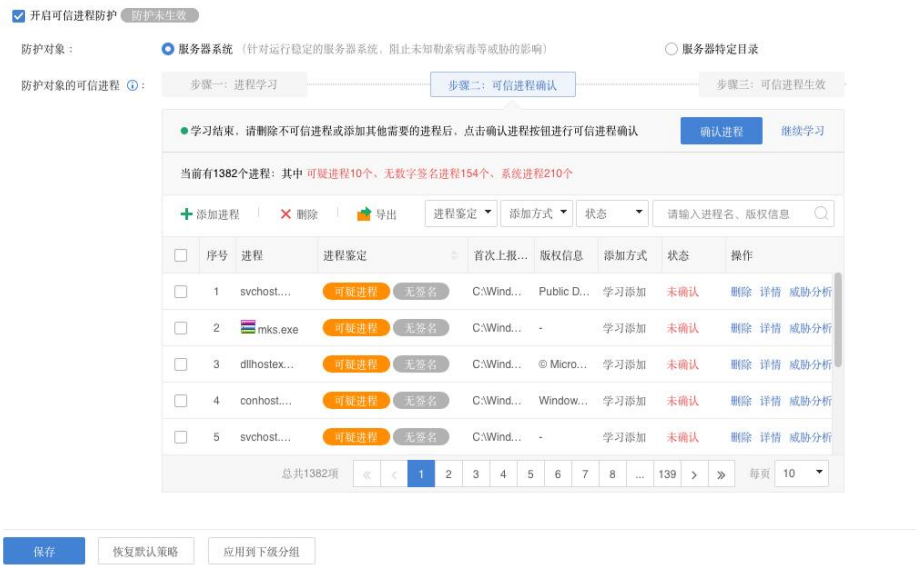
步骤2. 进程学习

启用[可信进程防护]，防护对象选择[服务器系统]，设置进程学习，学习时间范围从1天到30天可配，点击<保存>，如下图所示。

当学习完后可在页面查看已学习到的进程，并可查看进程鉴定情况，例如是否为可疑进程、该进程是否无签名等，为下一步可信进程确认提供参考。

步骤3. 可信进程确认

进程学习结束，需要进行可信进程确认，可通过对进程学习结果进行分析，删除不可信的进程，对没有学习到的可信进程进行添加，配置界面如下图所示。



其中：

- **进程鉴定**：EDR 对进程鉴定为可疑进程或者系统进程；
- **首次上报进程路径**：即进程文件首次上报的路径；
- **添加方式**：显示进程添加方式，有学习添加、手动添加和模板添加三种方式；
- **状态**：进程当前状态，[未确认]指当前未进行可信进行确认；
- **操作**：可以对进程进行删除、查看进程详情或进行进程分析操作。

其他说明：

1.如果发现需要添加的可信进程不在学习结果中，可点击<添加进程>进行添加，添加配置界面，如下图。

其中：

添加方式：进程人工添加方式有按模板导入、上传进程文件及手动输入进程文件信息3种添加方式。

- **按模板导入：**适用于客户需要加固的服务器是模板中提供的 web 服务器或数据库服务器；
- **上传进程文件：**上传服务器中可信的进程文件实现添加；
- **手动输入进程文件信息：**收集可信进程的进程名、原始文件名、版权信息手动录入。

可信进程核对完成后，点击<确认进程>并完成可信进程确认。

步骤4. 可信进程生效

点击<保存>后，可在页面查看到服务器防护生效中。

场景二：服务器特定目录防护

适用场景：

适用于针对服务器的重要目录防护，避免重要目录及其文件被勒索病毒等进行非法篡改/获取。

配置步骤：

步骤1. 服务器病毒查杀

先对服务器进行病毒查杀，确认服务器当前环境安全。

步骤2. 添加服务器防护目录

启用[可信进程防护]，防护对象选择[服务器特定目录]，手动添加需要防护的服务器重要目录，目录添加格式支持*号通配符路径或系统环境变量。

步骤3. 可信进程学习与确认

进程学习和可信进程确认与服务器系统防护场景一致，请参考“场景一：服务器系统防护”进行配置即可。

当发现不可信进程时，可按如下方式进行处理。

其中：

- **禁止不可信进程对防护目录的操作：**不可信进程无法对防护目录进行增删改，可以设置是否允许访问防护目录；
- **发现不可信进程对防护目录的操作：**发现不可信进程操作防护目录时，可以设置阻止操作或阻止操作并结束进程运行。

4.3.5. 信任名单

包含暴力破解IP信任名单和Powershell运行参数白名单两部分。

暴力破解源IP加入信任名单

支持 Windows 终端或 Linux 终端暴力破解源 IP 加入信任名单。当发生暴力破解误报时，可以将源地址加入白名单，白名单中的 IP 地址会被放行、不告警不封堵。

Windows终端信任名单配置：

Linux终端信任名单配置：

其中：

- **防暴力破解 IP 白名单**：支持填写 IP/IP 段/子网。当发生暴力破解误报时，可以将源地址加入防暴力破解 IP 白名单，白名单中的 IP 地址会被放行、不告警不封堵。

Powershell运行参数白名单

当有用到powershell命令编写的正常运维脚本时，需要将powershell运行参数加白，防止误报影响业务，如下图。

Powershell参数加白操作：检测到包含白名单运行参数的Powershell运行时，系统自动放行。Powershell运行参数支持部分字符串的匹配，如Powershell运行参数：powershell -ExecutionPolicy Restricted -Command Write-Host ‘Final result:1’可完整填写，也可以填写部分关键字段，如Command Write-Host ‘Final result:1’进行匹配。不少于10个字符。

4.3.6. 隔离区设置

支持设置Windows终端或Linux终端的备份策略和隔离区大小，配置界面如下图。

Windows隔离区配置：

Linux隔离区配置：

📖 说明：

不支持 mac 终端

Windows 终端支持在端上设置隔离区管理

4.3.7. 漏洞防护

在漏洞防护页面，包含“零”干扰漏洞免疫（即轻补丁漏洞免疫）和实体漏洞补丁修复两部分。两部分同时启用共同防御漏洞攻击，配置页面如下图。

📖 **说明：**

此功能仅支持 windows 终端。

“零”干扰漏洞免疫

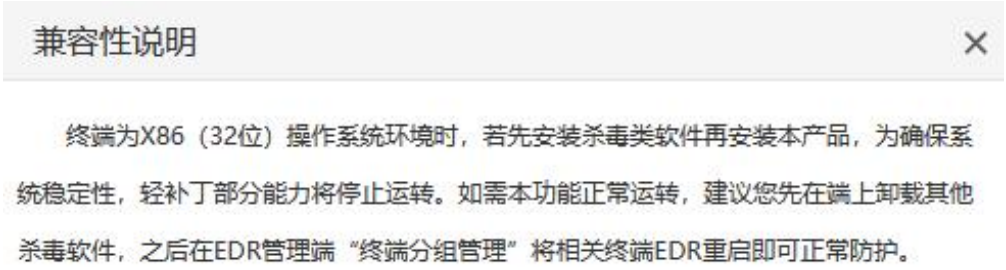
1.轻补丁漏洞免疫介绍

“零”干扰漏洞免疫，也可称为“轻补丁漏洞免疫”，具备对业务系统“零侵害、无干扰”的优点，可在业务或终端正常运行的情况下进行免疫，防御流行的高危和0day漏洞利用攻击，无需重启或中断业务，不存在兼容性问题，过程轻量化，同时具备修复速度快、防御效果好等特性。

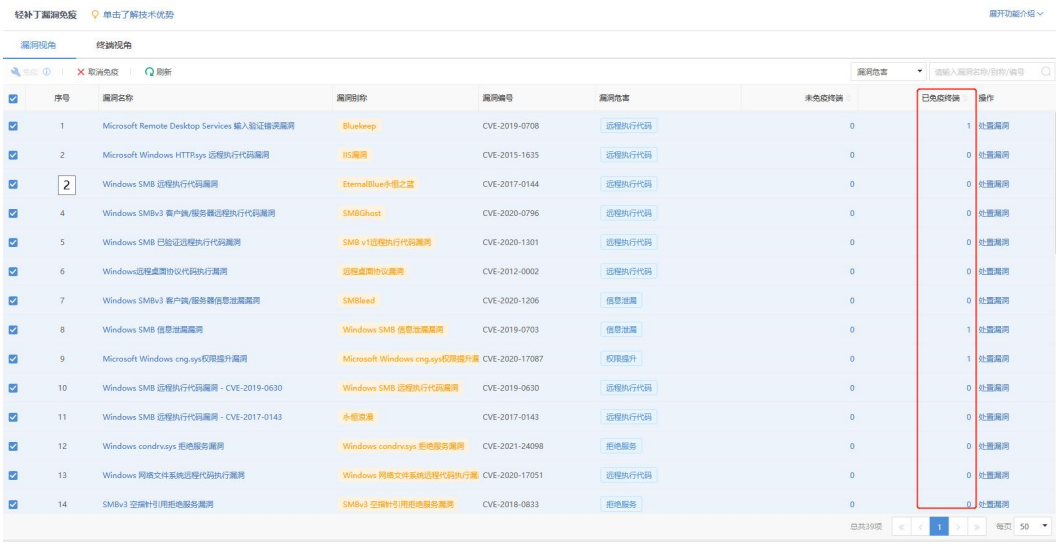
勾选“开启轻补丁漏洞免疫”，开启该功能。

“🔒”表示禁止客户端设置；点击该图标，“🔓”则表示允许客户端设置。

点击上图“兼容性说明”，兼容性说明如下图



当开启轻补丁漏洞免疫功能时，存在对应漏洞的电脑将会自动免疫。打开[响应中心/漏洞响应/轻补丁漏洞免疫]，如下图。

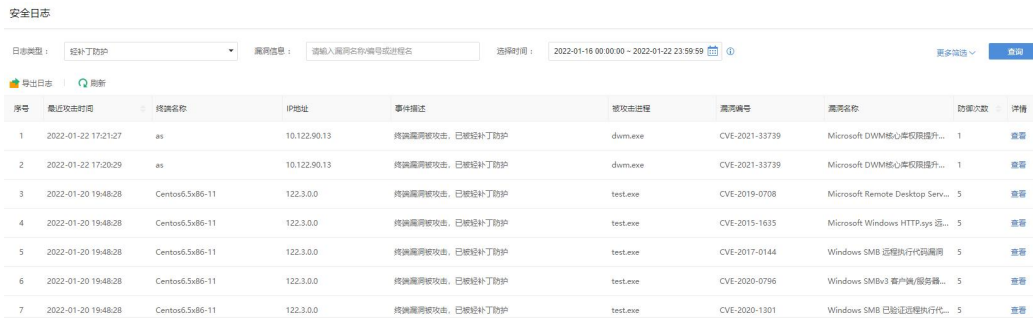


当终端不需要对某漏洞进行免疫时，如上图，选中漏洞，点击<取消免疫>。

2.轻补丁漏洞免疫效果

当终端检测到漏洞攻击时，成功拦截攻击并弹窗提醒如下图。

登录管理端，打开[日志报表/安全日志]，选择轻补丁防护日志，如下图。查询最近一段时间轻补丁功能拦截漏洞攻击日志记录。



实体漏洞补丁修复

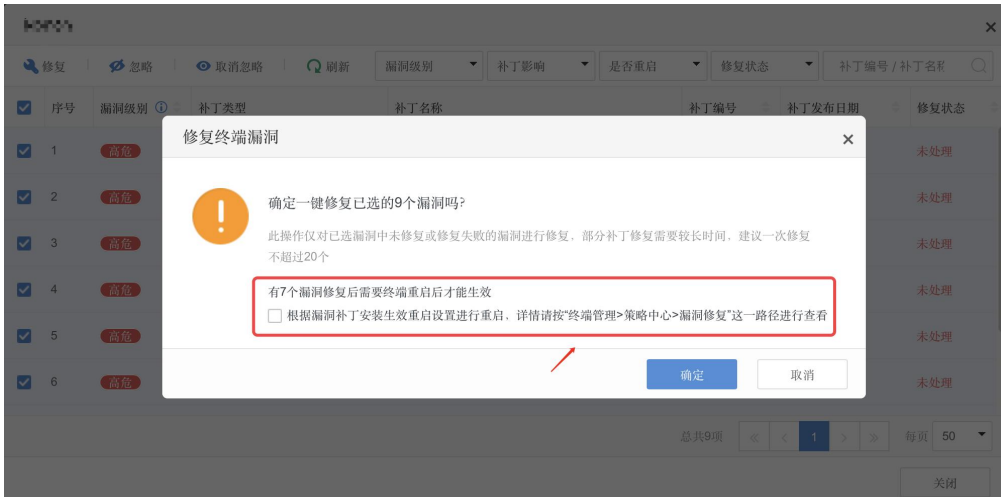
实体补丁修复指通过EDR检测Windows终端存在的漏洞，并通过EDR下发修复策略，终端无感知安装补丁进行漏洞修复。

1.漏洞补丁安装生效重启设置

部分实体补丁安装完成，需要终端重启才生效。这里定义补丁安装后终端重启策略及

通知内容，可以设置[强制终端安装补丁后立即重启]或[弹窗提醒终端用户重启]

打开[威胁检测/终端漏洞查补]进行漏洞检测与修复。检测到有补丁安装需要重启时，提示如下，管理员可选是否[根据漏洞补丁安装生效重启设置进行重启]，如下图。



当管理员可选中[根据漏洞补丁安装生效重启设置进行重启]，且重启策略设置为[弹窗提醒终端用户重启]，则终端收到弹窗提醒如下图。

当管理员可选中[根据漏洞补丁安装生效重启设置进行重启]，且重启策略设置为[强制终端安装补丁后立即重启]，则终端收到弹窗提醒如下图。

2.漏洞扫描与补丁修复

勾选“开启定期自动扫描”，可以开启该功能，实现在指定时间段进行扫描。

其中：

- **定期漏洞扫描**：定义漏洞定时检测的时间段。
- **漏洞扫描结果**：定义发现系统漏洞后的处置方法，处置方法包括[扫描完自动修复]和[仅上报，不修复]（推荐）。
- **终端补丁包获取服务器地址设置**：定义终端下载漏洞补丁的服务器，默认是深信服 CDN 服务器、微软漏洞补丁服务器及本管理端。

终端无法连接互联网、EDR管理端可以连接互联网场景，此时终端无法从互联网服务器下载漏洞补丁包。点击图中<去设置>，跳转至[系统管理/系统设置/基本设置]，如下图，选中“当终端无法从内置服务器下载补丁包时，允许管理端主动下载补丁包文件”，即可实现由管理端代理终端下载补丁包完成补丁修复。

📖 **说明：**

当终端和管理端都没有互联网权限时，参考[系统管理/系统设置/系统工具]章节，通过离线工具下载漏洞补丁完成漏洞修复。

4.3.8. 桌面管控

桌面管控当前只针对windows系统生效。桌面管控主要包含USB存储设备管控防护、终端违规外联防护和终端广告弹窗拦截。

USB设备管控防护

未经授权的移动存储介质的接入可能会导致终端面临病毒、木马、数据泄密、数据篡改等多种安全威胁。通过EDR管理端的USB存储设备管控防护功能，支持对包括U盘、移动硬盘、手机等移动设备在内进行禁用或白名单放行，并可设置终端弹窗告警提示终端用户，减轻终端用户因移动设备管控不足带来的风险。

在[策略中心/管控防护]的页签下，勾选“开启USB存储设备管控”，则开启该功能。

1.定义禁止使用设备

禁止使用设备：仅禁止带有存储功能的USB接口设备，不会禁用鼠标键盘等设备，常见的USB设备如“U盘”、“移动硬盘”、“便携设备（手机、数码相机等）”等。

- 可以根据实际情况勾选禁止使用的设备。
- 当部分 USB 设备被允许使用时，可以通过外设白名单进行添加和配置，按需求填写设备信息，如下图所示。

2.设置弹窗提醒

当勾选“发现终端使用禁止的设备，弹窗提醒用户”选项，在服务器或终端上使用禁止类设备时，会收到弹窗提醒，如下图。

终端违规外联

违规外联当前只针对windows系统生效，linux终端不受限制。当内网计算机、专网设备直接或间接通过其他网络访问互联网时，均为违规外联，这使得黑客能够绕过防火墙、网关等防护屏障，侵入违规外联的计算机从而进一步渗透重要服务器，导致内网面临重大的安全风险。

通过EDR管理端配置安全策略，基于网络侧探测，支持域名解析、PING探测地址两种违规探测方式，对存在违规外联的行为进行断网、关机、邮件告警等多种处置，实现违规终端的实时管控。

违规外联策略配置探测间隔、探测地址、处置方式，如下图。

其中：

1.探测间隔：终端检测违规外联的时间间隔，最小值为60秒，最大值3600秒。

2.探测地址：定义违规外联的探测地址，默认是www.baidu.com，管理员可以自己添加IP或者域名。

3.发现违规外联终端：定义发现违规外联的处理方法。

- 不处理：仅弹窗告警。
- 断开网络：终端倒计时 30s 断开网络，vista 及以上系统的断开网络效果与终端隔离类似，终端除了与管理端通信之外，其他访问都不能访问，管理员可以在终端管理中重启 agent 恢复网络；server2003 跟 xp 是禁用网卡，需要用户手动启用网卡或者重启。
- 关机：终端倒计时 60s 关机。

4.违规外联提醒：如果终端发生违规，桌面右下角会出现弹窗提示用户违规，此处可设置提醒的内容。

5.邮件告警：当终端发生违规时，邮件告警通知管理员。

终端广告弹窗拦截

终端的大量软件为盈利自带广告弹窗功能，给用户的办公带来很大的干扰，尤其是教育、政府行业。通过EDR管理端，能够对终端进行一键弹窗拦截，减少垃圾信息的干扰，为用户提供一个纯净的工作环境。

1.智能拦截

管理员登陆EDR控制台，在[终端管理/策略中心]的页面下，点击[桌面管控]，勾选“开启终端广告弹窗拦截”，即开启该功能，能够让终端拦截已安装软件的恶意广告弹窗，点击<应用到下级分组>，实现一键设置。

📖 **说明：**

当点亮图中锁定图标，则禁止客户端修改此配置，如解除锁定，则客户端可自行变更此配置。

2.效果可视

终端用户可在客户端的[系统工具/广告弹窗拦截]，开启该功能，在[拦截历史]查看详细的拦截效果，如拦截次数、内容等。

📖 **说明：**

终端广告弹窗拦截功能对 win7 和 win10 系统有效，且依赖规则库更新。发现软件广告弹窗无法拦截的场景，请联系服务提供商处理。

远程协助

当被管控的终端出现故障时，管理员可以通过远程协助功能对终端进行远程控制，快速、安全的响应解决终端问题。

前提条件：

管理员能够远程管理终端的前提条件是终端Agent开启了[授权管理员远程]，右键Agent客户端托盘图标，如下图。该功能默认打开，如果终端关闭了[授权管理员远程]，则管理员无法通过EDR远程协助管理终端。

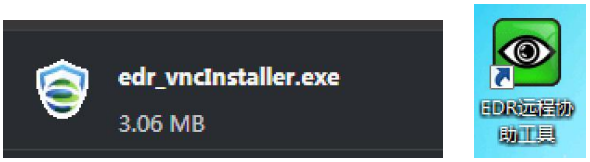
场景一：不需要终端确认、直接远程终端电脑。

不需要终端确认、管理员可以直接远程终端电脑，适用于终端无人值守场景。

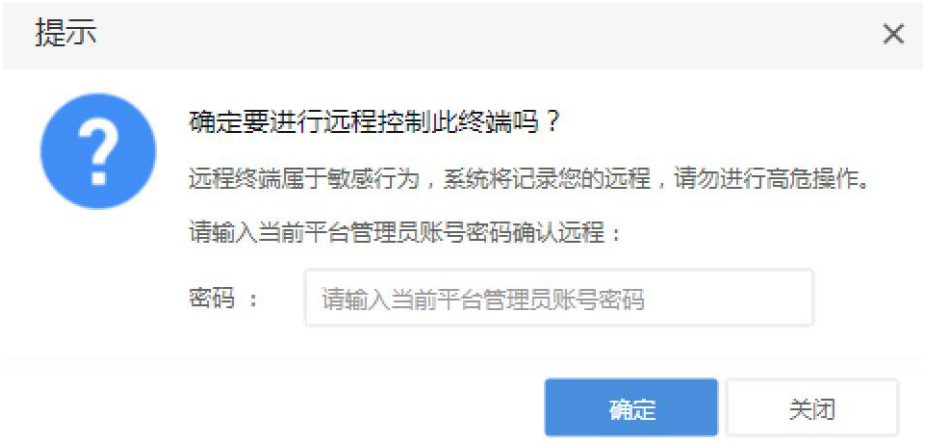
打开[终端管理/策略中心]，设置需要远程控制的终端所在分组的桌面管控策略，如下图。[是否需要终端用户同意]选择[不需要]。

打开[终端管理/终端分组管理]，选中需要远程的终端，发起远程协助，如下图。

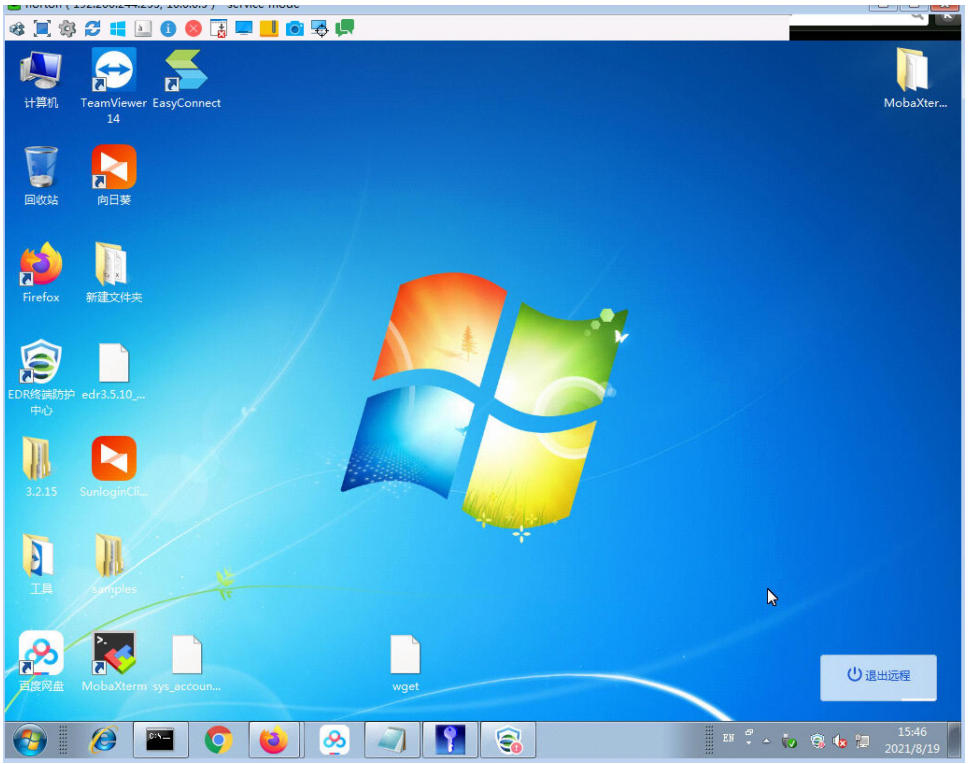
首次使用远程协助时，需要下载VNC客户端远程工具 ，点击<立即下载>下载并安装VNC客户端远程工具，如下图。



安装VNC客户端远程工具后，再次对终端发起远程，如下图。



为了确认是管理员操作，需要输入当前管理员账号密码，输入管理员密码后点击<确定>，建立远程连接并成功远程被控制端电脑，如下图。



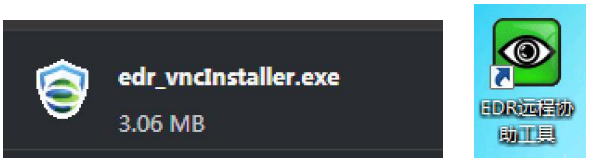
场景二：需要终端确认、才可以远程终端电脑。

需要终端确认、管理员才可以远程终端电脑，适用于有人值守、对远程操作敏感场景。

打开[终端管理/策略中心]，设置需要远程控制的终端所在分组的桌面管控策略，如下图。[是否需要终端用户同意]选择[需要]。

打开[终端管理/终端分组管理]，选中需要远程的终端，发起远程协助，如下图。

首次使用远程协助时，需要下载VNC客户端远程工具 ，点击<立即下载>下载并安装VNC客户端远程工具，如下图。

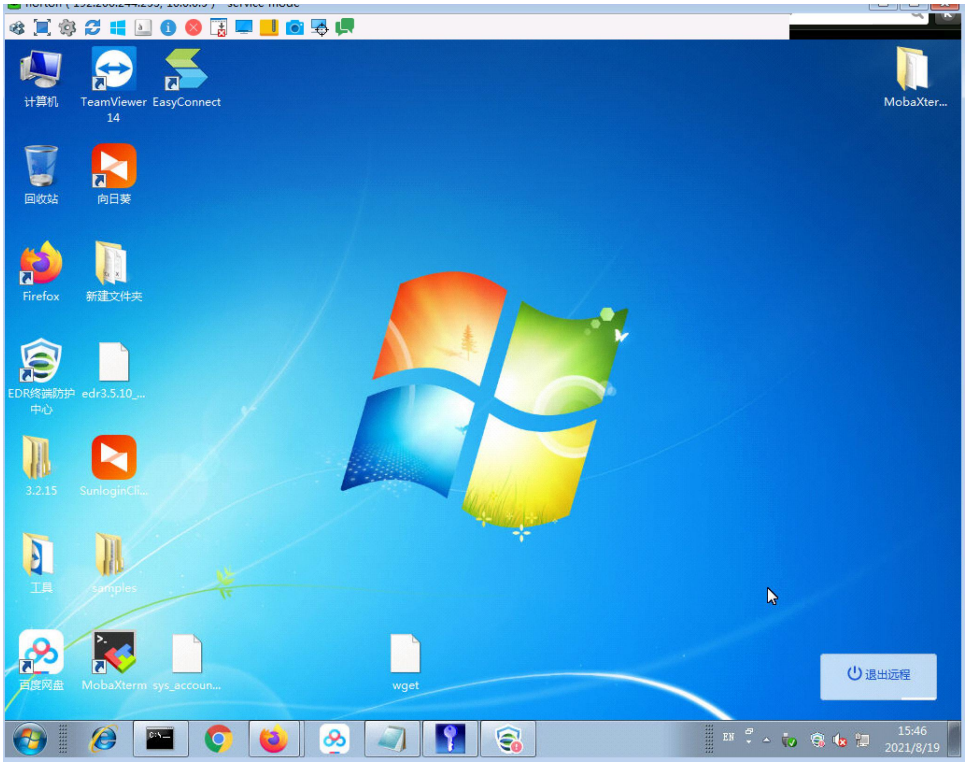


安装VNC客户端远程工具后，再次对终端发起远程，如下图。

终端电脑EDR客户托盘弹出提示。

终端用户点击<允许>，管理员即可远程控制终端电脑。

为了确认是管理员操作，需要输入当前管理员账号密码，输入管理员密码后点击<确定>，建立远程连接并成功远程被控制端电脑，如下图。



📖 说明：

1.只有 admin 管理员和安全管理员具有远程控制权限，整个通信过程加密。

2.远程协助默认使用随机端口远程被控制电脑，可以通过[系统管理/系统设置/基本设置]中的『远程协助端口设置』提前设置好固定端口，通过固定端口远程被控制电脑。

3.远程协助功能被远程终端支持 win7/win10/xp /win8/win8.1 系统。

4.3.9. 微隔离

通过微隔离策略，可针对服务器/终端必要的业务端口进行放通、非必要的端口进行禁止，同时支持流量状态可视化，高效提升客户业务安全性。

4.3.9.1. 业务梳理

梳理客户业务系统及业务系统间的访问关系，为后续的微隔离策略做准备，如下表。

对象	业务系统	数据库（Server1） 财务系统（Server2） OA 系统（Server3） 人事系统（Server4、Server5）
	IP 组	办公终端(x.x.x.x)

		办公服务器(y.y.y.y)
	服务	SMB（135\136\137\139\445）
		HTTP（80）
访问关系	访问关系	1、SMB 服务拒绝 源：办公终端 目的：业务系统服务器 服务：SMB 动作：拒绝 2、HTTP 服务允许 源：办公终端 目的：业务系统服务器 服务：HTTP 动作：允许

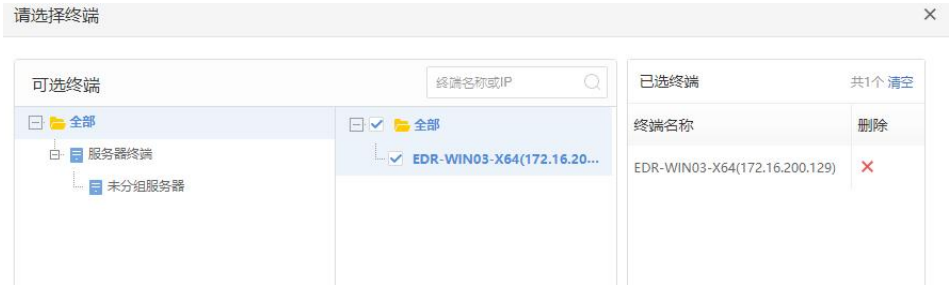
4.3.9.2. 创建对象

根据第上述梳理的业务系统，定义业务系统/IP组/服务等对象，为微隔离策略调用。

业务系统创建

通过定义业务系统分类，可将多个服务器终端纳归到统一的业务系统分类中，便于微隔离策略源调用及流量状态展示，配置流程如下：

1.在[微隔离/业务系统]页面，点击<新增>，进行业务系统名称及服务器终端选择，配置界面如下图所示。



说明：

一台服务器终端只能加入一个业务系统；

终端仅支持选择服务器终端。

2.创建完成后，可在业务系统页面，查看已创建的业务系统分类及对应分类下的服务

器终端信息，可进行角色关联、状态查看等操作。

角色创建

通过角色属性，可定义服务器终端在业务系统分组中的角色，可理解为该服务器终端所提供的服务类型，平台内置了WEB、数据库、FTP、SLB、邮件、消息队列、WebSphere、WebLogic等角色以及对应的角色特征，角色新增配置流程如下：

1.在[微隔离/角色]页面，点击<新增>，在弹出的页面中进行角色名、描述和角色特征编辑，如下图所示。

其中角色特征支持进程名称或端口信息，要求一行一个特征。

2.完成信息编辑后，点击<确定>即完成新角色创建，可在业务系统页面对服务器终端角色进行指定，方便微隔离策略的调用与流量状态显示。

IP组创建

通过IP组可划分内网或互联网的IP到对应的IP组中，平台内置了默认内网IP组包括10.0.0.0/8 、 172.16.0.0/12 、 192.168.0.0/16 ， 默 认 互 联 网 IP 组 包 括0.0.0.0-255.255.255.255，策略通过从上到下进行匹配，方便微隔离策略的调用，IP组创建流程如下：

1.在[微隔离/IP组]页面，点击<新增>，在弹出页面进行IP组添加操作，配置页面如下图所示。

其中地址范围支持单IP、IP范围和子网。

2.点击<确定>进行提交，即完成IP组创建，在IP组页面可对已创建的IP组进行上移、

下移等操作，实现策略的从上到下匹配。

服务创建

通过服务属性可定义服务端口，用于微隔离策略调用，内置服务包括35种，可自定义添加，配置流程如下：

> 📖 **说明：**
> 自定义服务端口不能与已有所使用端口不能重复。

1.在[微隔离/服务]页面，点击<新增>进行服务添加，如下图所示。

其中流量类型包括其他流量、业务流量及运维流量，用于流量状态的展示。

2.配置完成后，点击<确定>进行提交即可。

4.3.9.3. 策略配置

1.配置微隔离访问控制策略

在微隔离策略页面，点击<新增>，进行微隔离策略配置，配置界面如下图所示。

其中：

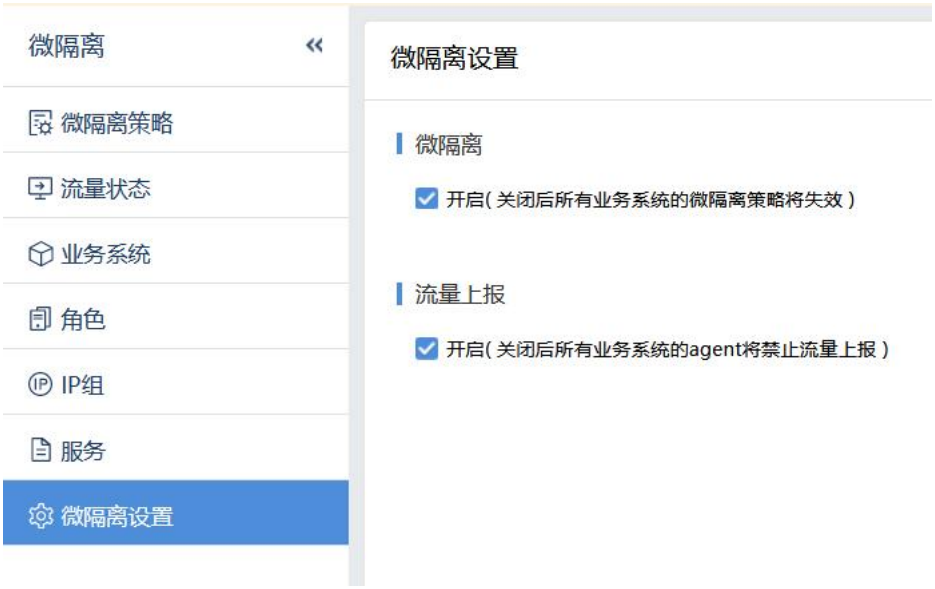
- **源：**访问目标服务的源，可以选择业务系统、角色、服务器、IP 组；
- **目的：**被访问的目标终端；
- **服务：**目标终端的服务端口；
- **动作：**微隔离策略的动作可选择允许或拒绝。

📖 **说明：**

源和目的可以点击 进行互换。

2.启用微隔离并开启流量上报。

打开[微隔离设置]，如下图。启用微隔离和流量上报。



其中：

- **微隔离**：勾选即开启微隔离功能，关闭后所有业务系统的微隔离策略将失效；
- **流量上报**：开启后可在[流量隔离状态]中展示流量访问情况，关闭后客户端将禁止流量上报，影响[流量隔离状态]的展示。

4.3.9.4. 流量查看

微隔离支持流量状态可视化，支持查看终端系统的流量访问情况，可以显示互联网出口、内网互访及已放通和未放通的流量访问情况，同时支持通过过滤策略进行筛选查看，界面如下图所示。

在[过滤流量]中过滤选项说明如下：

- **红色流量线**：表示未放通的流量；
- **绿色流量线**：表示已放通的流量；
- **业务之间流量**：业务系统之间的流量访问情况；
- **业务内部流量**：业务系统内部的流量访问情况。

4.4. 威胁检测

4.4.1. 终端病毒查杀

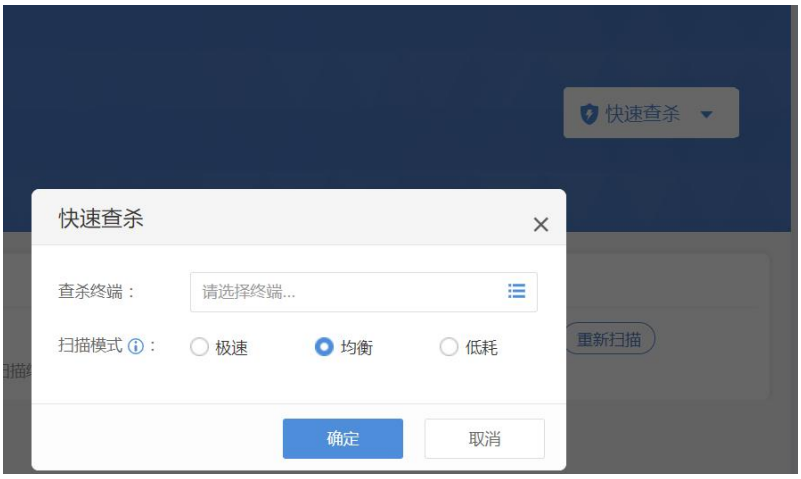
终端病毒查杀可从管理端对终端下发病毒查杀任务。通过结合本地信誉库、自研SAVE引擎、行为检测引擎、基因特征检测引擎、云查等多引擎对终端进行威胁文件扫描查杀。

病毒查杀方式包括“快速查杀”和“全盘查杀”，点击[快速查杀]右侧的三角可以选择查杀方式。快速查杀和全盘查杀区别如下表所示。

全盘查杀	扫描终端所有硬盘文件

快速查杀	扫描系统盘中重要文件目录，重要文件目录包括： Windows： /Windows 和/Windows/system32 本级目录 /Windows/system32/drivers 目录和其子目录 Linux: /bin、/sbin、/usr/sbin、/usr/bin、/lib、/lib64、 /usr/lib/usr/lib64、/usr/local/lib、/usr/local/lib64、 /tmp、/var/tmp、/dev、/proc MacOS ： /private/tmp、/Users/“当前账户名”/Downloads、/Users/“当前账户名”/Desktop、/Users/“当前账户名”/Documents

点击<快速查杀/全盘查杀>，进入查杀配置界面，如下图所示。



其中：

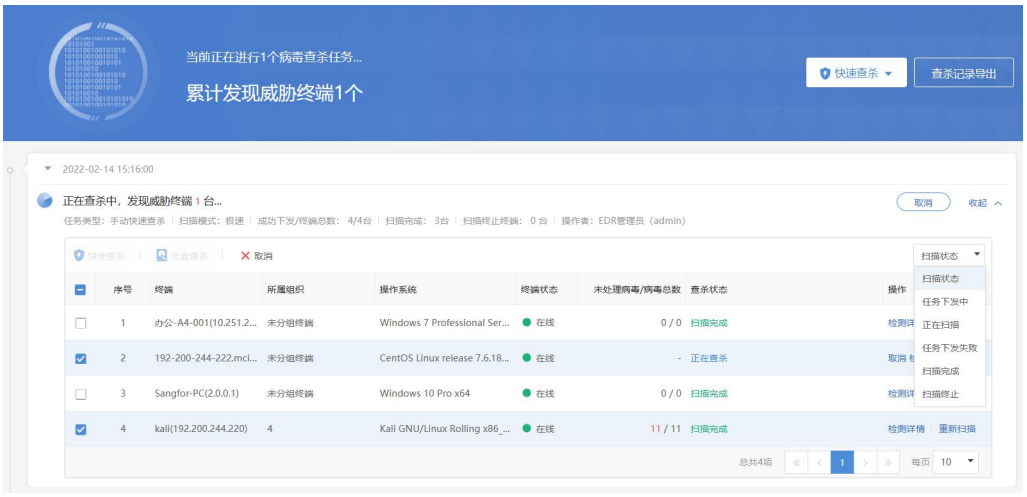
查杀终端：在可选终端页面管理员可查看近七天风险主机、最近一周/一个月/三个月未查杀终端及终端上次查杀时间，便于筛选需查杀终端，同时也支持针对终端名称或IP进行特定检索。

扫描模式：包括极速、均衡及低耗模式，差异如下：

- **极速：**全速扫描，不限制扫描软件自身的 CPU 占用率（资源优化模式下则不超过 50%）；

- **均衡：**扫描速度和 CPU 占用率达到一定平衡，限制 CPU 占用率不超过 30%（资源优化模式下则不超过 20%）；
- **低耗：**扫描时尽量少占用 CPU 资源，限制 CPU 占用率不超过 10%（资源优化模式下则不超过 5%）。

选中待查杀终端，下发查杀任务。根据扫描状态过滤，查看不同查杀状态的终端，如下图。



点击具体终端右侧的<检测详情>可查看该终端查杀进度，如下图。

病毒查杀完成后，可查看此次查杀结果，主要展示信息包括任务类型、扫描模式、成功下发终端台数、扫描完成情况、终端终止终端，终端名称IP地址、所属组织、操作系统、终端状态、未处理病毒和病毒总数的情况、查杀状态等信息，如下图所示。

对查杀发现的威胁文件进行处置（隔离）、信任处理。如果威胁文件为可疑文件，可以点击[威胁分析]进入情报网站进行分析、通过情报分析结果作出进一步处理，如下图所示。

点击[查杀记录导出]，支持导出一段时间内病毒查杀记录，如下图。

以表格形式导出病毒查杀记录，如下图。

终端病毒查杀任务记录

汇总信息	符合查询条件的记录总数为6条，当前共导出6条

查询条件

时间	2021-06-09 00:00:00 - 2021-06-15 23:59:59
时间排序	降序
查杀记录范围	根据时间导出，时间范围：2021-06-09 00:00:00-2021-06-15 23:59:59（注：仅支持导出10万条以内的查杀记录）

查询结果

序号	任务下发时间	终端	所属组织	操作系统	终端状	未处理病毒/病毒总数	查杀状态	任务类型	扫描模式
1	2021-06-15 19:03:49	WIN-6UVL58LI3DM(192	未分组终端	Windows Server 2008 R	在线	2/52	扫描完成	手动快速查杀	极速
2	2021-06-15 19:03:49	localhost.localdomain(19	未分组终端	Red Hat Enterprise Linux	在线	0/0	扫描完成	手动快速查杀	极速
3	2021-06-15 19:03:49	hbz.com(192.200.244.10	未分组终端	Red Hat Enterprise Linux	在线	0/0	扫描完成	手动快速查杀	极速
4	2021-06-15 19:03:49	kali(192.200.244.166)	未分组终端	Kali GNU/Linux 2.0	在线	3/3	扫描完成	手动快速查杀	极速
5	2021-06-15 19:03:49	Norton(192.200.244.253	未分组终端	Windows 7 Professional	在线	0/0	扫描完成	手动快速查杀	极速
6	2021-06-15 19:03:49	hbz-PC(192.200.244.24(	未分组终端	Windows 7 Professional	在线	0/0	扫描完成	手动快速查杀	极速

4.4.2. 终端漏洞查补

终端漏洞查补模块可检测windows终端系统漏洞并修复，当前支持远程执行代码、拒绝服务、特权提升、安全功能绕过、信息泄漏等五种影响类型漏洞检测与修复。漏洞查补操作流程如下图所示：

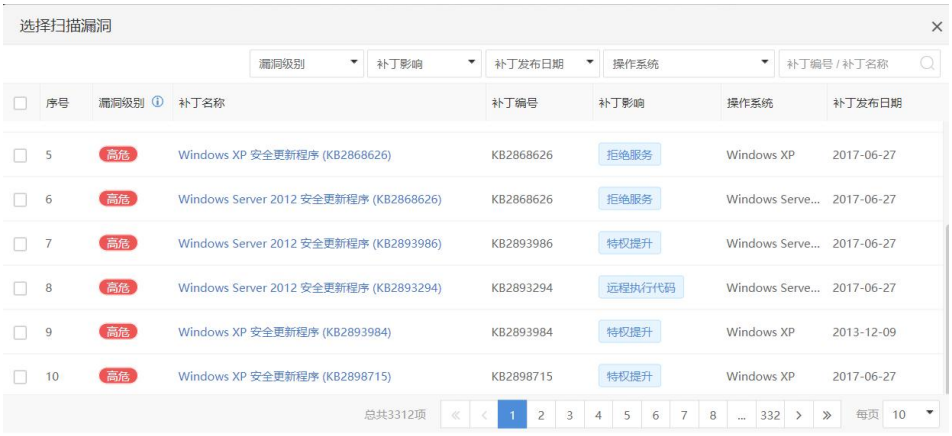
1.在[威胁检测/终端漏洞查补]页面下，点击[添加漏洞扫描任务]，创建漏洞扫描任务，配置页面如下图所示。

其中：

选择终端：在可选终端页面管理员可查看最近一周/一个月/三个月未扫描及终端上次扫描时间，便于筛选需扫描终端，同时也支持针对终端名称或IP进行特定检索；

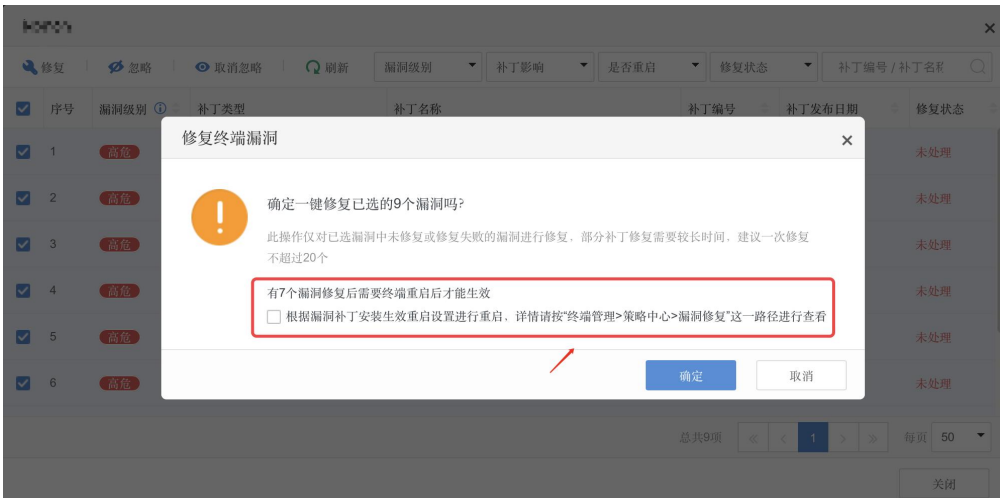
选择漏洞：包括全部漏洞、高危漏洞和自动以选择：

- **全部漏洞：**会针对远程执行代码、拒绝服务、特权提升、安全功能绕过、信息泄漏等五种影响类型漏洞进行扫描与修复；
- **高危漏洞：**会针对高危等级漏洞进行扫描与修复，高危漏洞信息可在[自定义选择]中进行过滤筛选；
- **自定义选择：**管理员可自定义需扫描漏洞，在自定义选择页面可基于漏洞级别、补丁影响、补丁发布日期、操作系统等标签进行分类筛选，并支持补丁编号/补丁名称查询，管理员可在筛选结果中选中需扫描漏洞进行自定义，如下图所示。



2.点击<确定>后，会自动执行漏洞扫描任务，可在页面左侧对任务类型及任务状态进行筛选，并点击具体任务进行查看，针对具有未修复漏洞的终端可点击<处置漏洞>进行需修复漏洞选择与下发修复任务，如下图所示。

点击<修复>，检测到有补丁安装需要重启时，提示如下，管理员可选是否[根据漏洞补丁安装生效重启设置进行重启]，如下图。



当管理员可选中[根据漏洞补丁安装生效重启设置进行重启]，且重启策略设置为[弹窗

提醒终端用户重启]，终端收到下图弹窗提醒。

当管理员可选中[根据漏洞补丁安装生效重启设置进行重启]，且重启策略设置为[强制终端安装补丁后立即重启]，则终端收到下图弹窗提醒。

4.4.3. 终端基线检查

基线检查是根据等保三级系统安全基线要求对终端操作系统进行合规检查，可对终端Windows操作系统和Linux操作系统进行合规性检查，不同终端系统检查的内容有所差异：

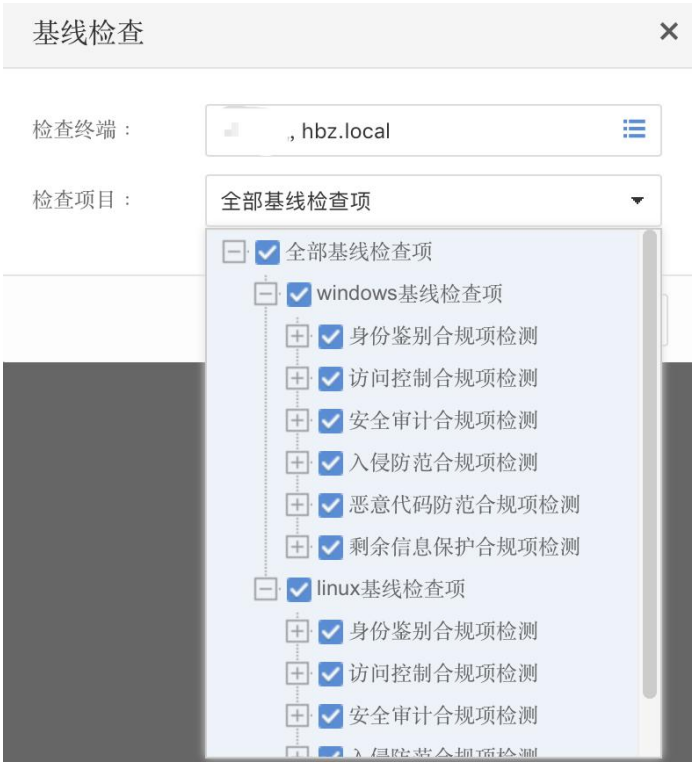
Windows终端：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范；

Linux终端：身份鉴别、访问控制、安全审计、SSH策略检测、入侵防范、恶意代码

防范。

打开[威胁检测/终端基线检查]，如下图所示。

点击[立即检查]，对需要检查的终端下发基线检查任务，如下图。



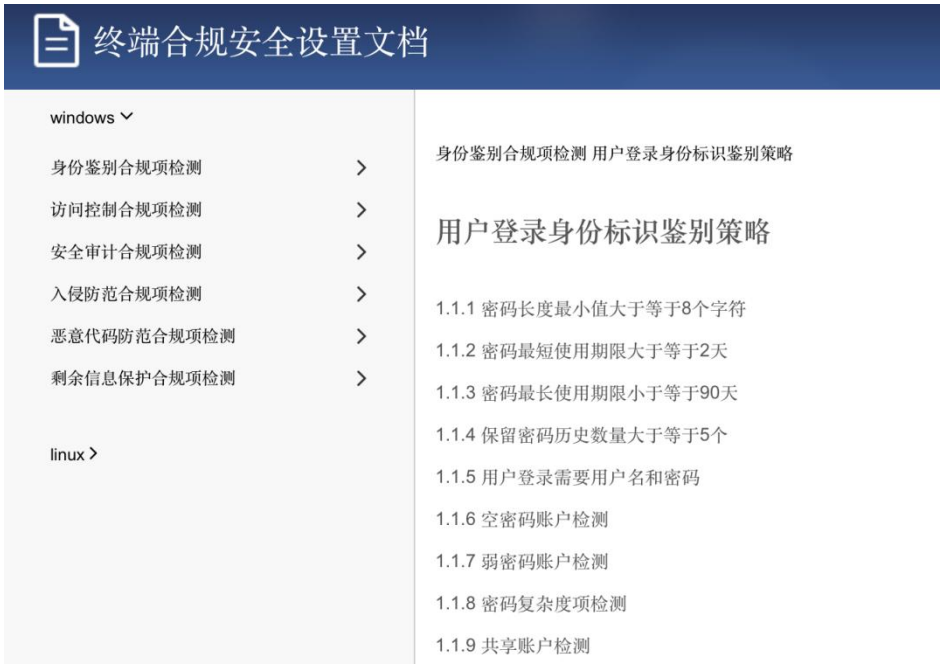
[检查项目]可以选择下发全部基线检查项，如果关注某个类别的检查，也可以自定义基线检查项。

完成检测后，检查效果如下图。

查看合规检测的结果，点击[查看详情]，红色显示为基线检查不合规项。

如果需要将检查结果下发至终端或其它管理员处理，可以点击[导出]，以表格形式导出检查结果下发到终端处理。

针对基线检查不合规的项目，可以参考加固指导文档进行修复加固。打开[威胁检测/终端基线检查]，点击[查看完整配置文档]



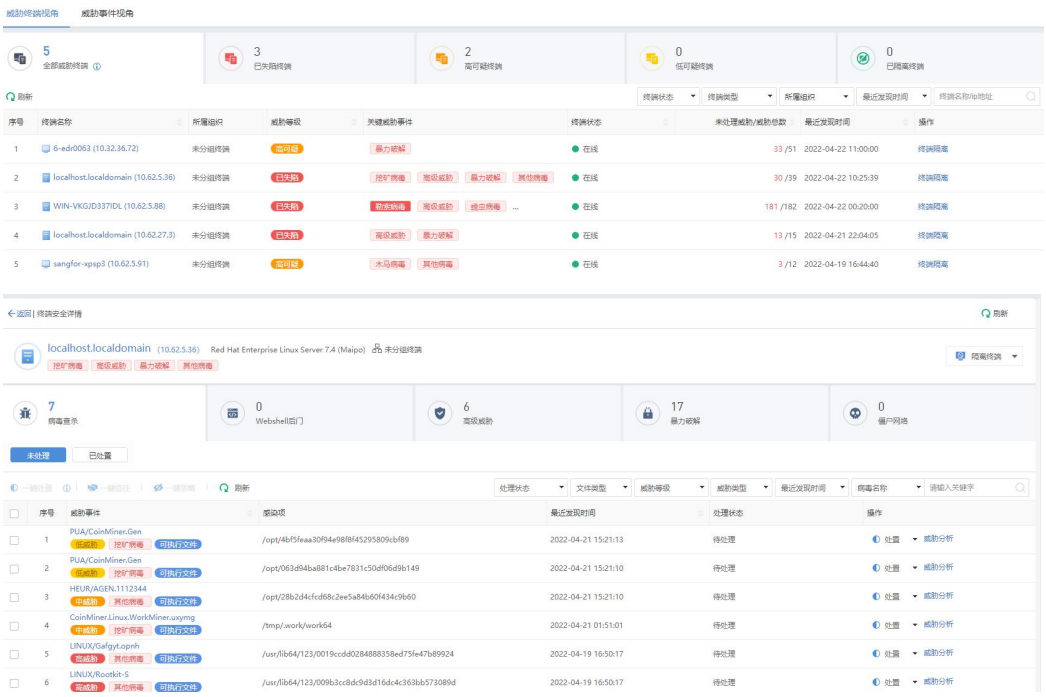
4.5. 响应中心

4.5.1. 威胁响应

威胁响应可通过威胁终端/事件视角对全部威胁终端、已失陷终端、高可疑终端、低可疑终端、已隔离终端进行分析展示。

4.5.1.1. 威胁终端视角

在威胁终端视角页面，可点击终端名称，跳转到该终端的<终端安全详情页面>，对威胁进行处置操作，并且可以对终端进行隔离操作，<威胁终端视角>和<终端安全详情>如下图所示。



根据威胁程度将威胁终端分为已失陷、高可疑、低可疑三级，各等级说明如下：

- 已失陷终端：发生了高危病毒、严重和高危行为威胁、高危 Webshell 后门、高危僵尸网络等威胁事件的终端；
- 高可疑终端：发生了中危病毒、中危行为威胁、中危僵尸网络、暴力破解这些威胁事件的终端；
- 低可疑终端：发生了低危病毒、低危 Webshell 后门、可疑 powershell 执行、低危僵尸网络等威胁事件的终端。

根据终端状态、终端类型、所属组织、最近发现时间、终端名称或IP地址进行筛选，帮助管理员运维。例如只处理在线的威胁终端事件，可以将终端状态作为筛选条件过滤在线的终端。

当发现威胁终端，可以对终端隔离处理，隔离后该终端将无法访问任何网络，请确保不会对业务系统产生影响，隔离后可在已隔离终端恢复，如下图。

4.5.1.2. 威胁事件视角

在威胁事件视角页面，展示病毒查杀、勒索病毒、Webshell、高级威胁、暴力破解、powershell执行、僵尸网络等威胁事件说情，如下图。

根据终端状态、处理状态、文件类型、威胁等级、威胁类型、最近发生时间、终端名称/IP地址/病毒名称/文件路径进行筛选，帮助管理员运维。例如只处理在线的威胁事件，可以将终端状态作为筛选条件过滤在线的威胁事件。

点击威胁事件名称，了解威胁事件详情，如下图。

未处理标签：

未处理标签展示检测到所有未处理的威胁事件。针对具体威胁事件可在右侧选择处置、信任、忽略等处置操作，如不确定文件是否为恶意，可点击<威胁分析>由情报中心进一步判断或点击具体威胁事件查看详情信息，同时查看对应处置建议。

选中需要隔离的威胁文件，点击<一键处置>，如下图。

选中[同时隔离其他终端上有相同MD5值的文件]，实现针对其它终端存在相同威胁文件批量处理；

选中[若终端隔离区空间不足时，自动清理隔离区后继续处置]，隔离文件时，检测到终端隔离区满会自动清理隔离区文件再进行隔离。

> 说明：
> 选中[若终端隔离区空间不足时，自动清理隔离区后继续处置]时，会按已隔离文件的先后顺序自动清理终端隔离区 50%的文件。

已处置标签：

已处置标签展示所有加入隔离区的威胁文件，可以对已处置文件彻底清除或恢复操作，如下图。

选中威胁文件，点击<一键处置>，批量删除终端隔离区文件；点击<一键恢复>，批量恢复隔离区文件，如下图。

支持一次支持处置1W个威胁文件，选中威胁文件，点击<一键处置>，点击<勾选所有项>，批量处置威胁文件，如下图。

4.5.1.3. 高级威胁展示

适用场景

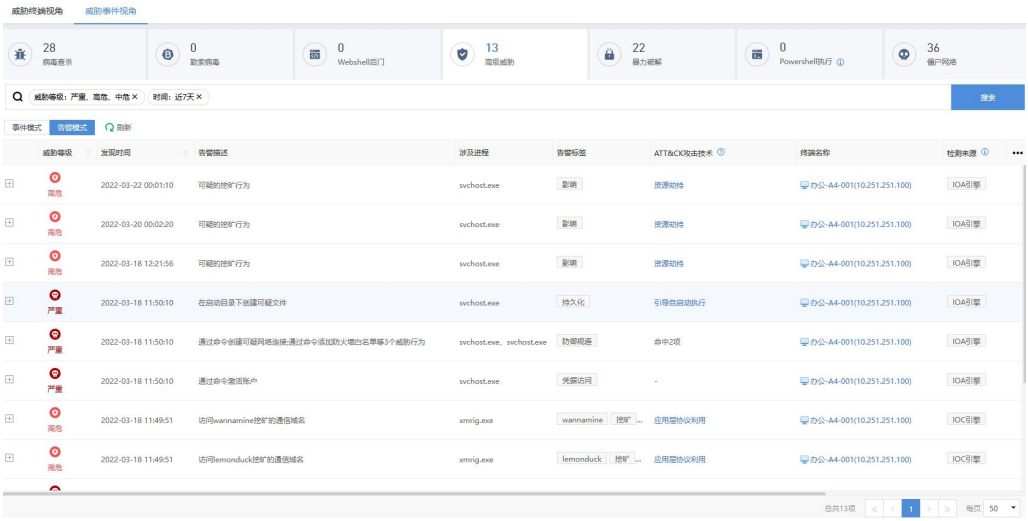
针对新威胁场景、攻防对抗场景，如勒索攻击、钓鱼邮件等借助办公网突破内网的情况，可通过IOA规则匹配到勒索、钓鱼等相关攻击的异常行为（参考att&ck，如异常注入、窃取凭证、提权行为等），及时告警威胁信息并对高危动作进行拦截 ，同时

追溯发起攻击威胁程序的所在进程链，聚合所有异常行为形成准确的安全事件，协助定位攻击源头，并提供可闭环到启动项的能力，确保清理干净。

高级威胁使用案例

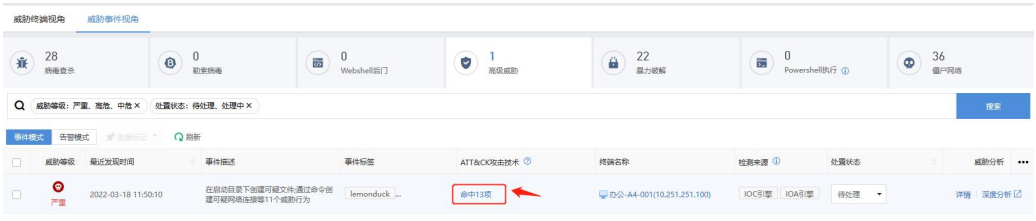
下面以挖矿事件案例讲述高级威胁使用。

在例行运维过程中，安全管理员发现EDR高级威胁检测到多条挖矿行为、帐户激活、创建可疑文件等可疑行为告警，如下图。



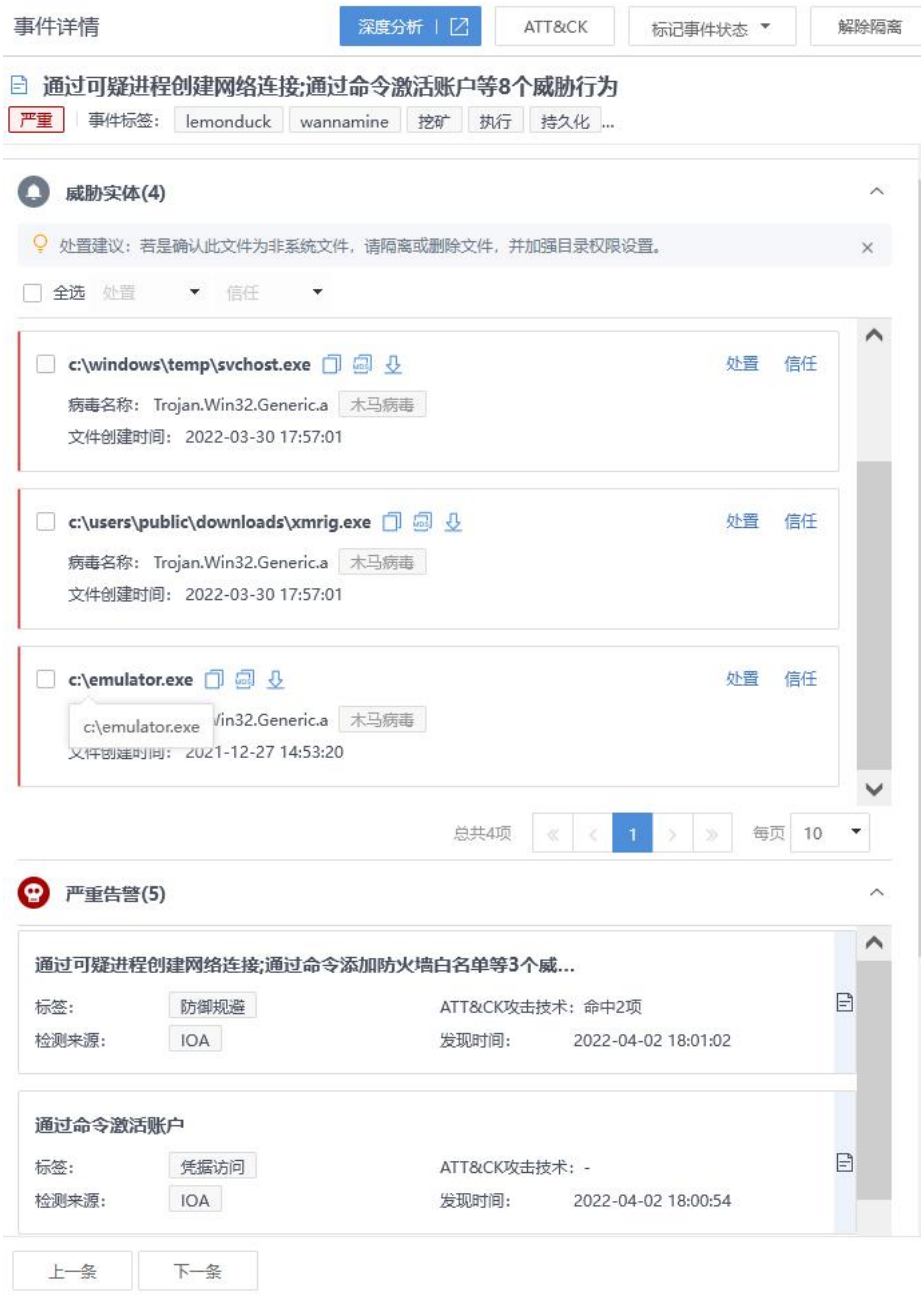
查看安全事件，EDR检测出一起威胁等级“严重”的安全事件，如下图。EDR将终端多个可疑行为聚合成一个完整的攻击事件进行展示。

查看安全事件，已经多项匹配ATT&CK威胁矩阵模型，如下图。



攻击行为多次命中ATT&CK威胁模型中的执行、持久化、防御规避、凭据访问、探测、命令与控制、影响等战术。

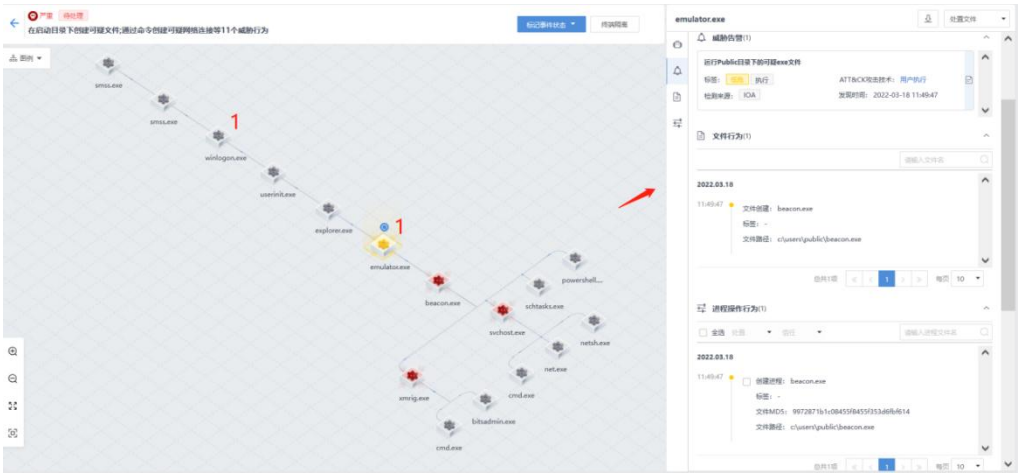
点击安全事件<详情>，查看该安全事件威胁实体及异常行为告警。



点击安全事件<深度分析>进行进程攻击链可视化溯源分析。

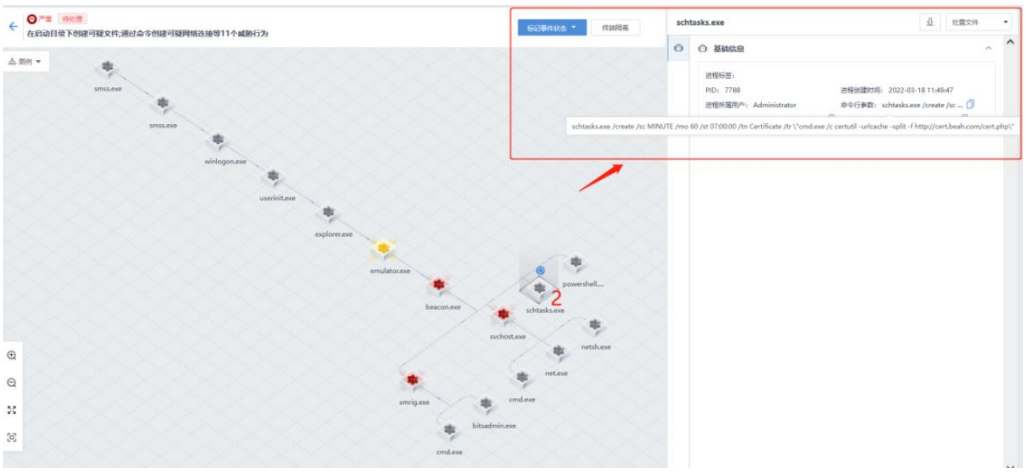
（1）攻击入口

攻击者通过远程桌面登录拿到测试机权限，投放攻击样本emulator.exe。执行样本后自动创建beacon.exe文件和进程。



（2）创建可疑任务计划实现持久化攻击

beacon.exe创建schtasts.exe进程，通过schtasts.exe进程创建可疑任务计划实现持久化攻击。

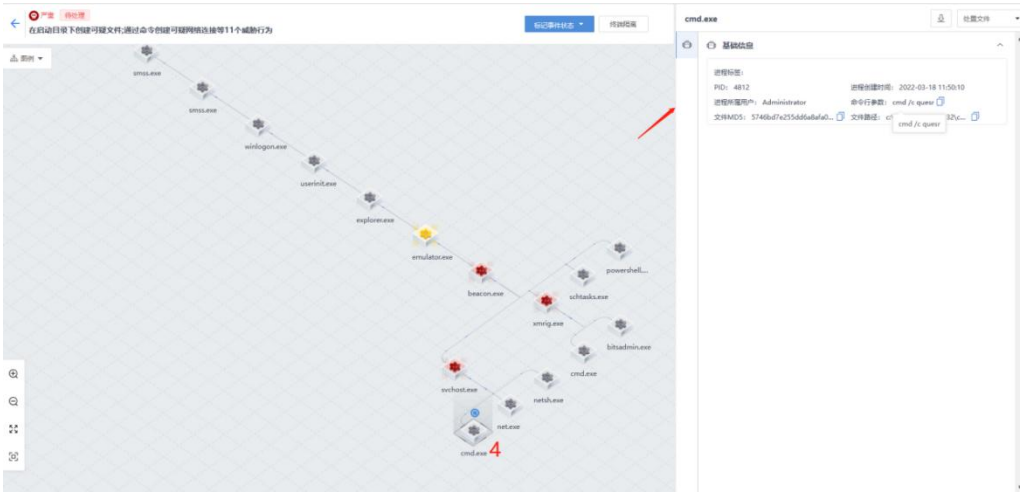


（3）执行混淆powershell命令绕过安全防护、实现攻击

beacon.exe创建powershell.exe进程，通过执行混淆powershell命令绕过安全防护、实现攻击。

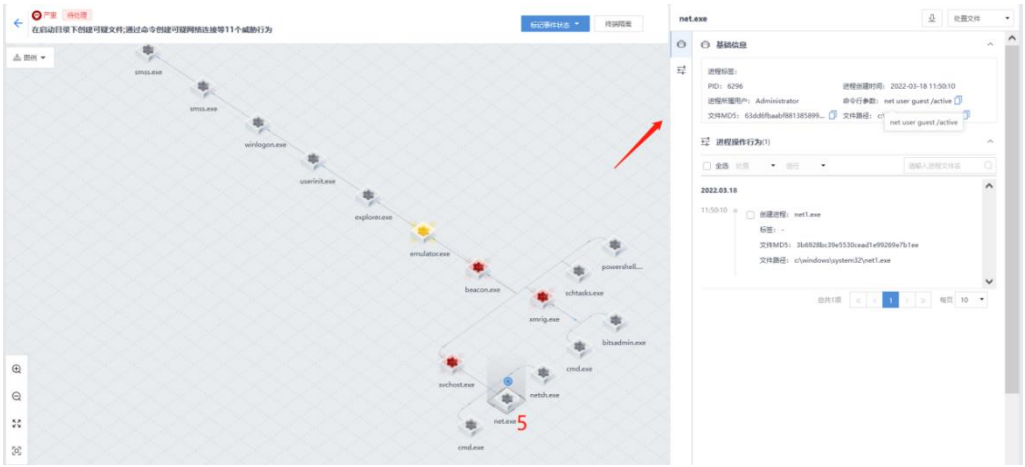
（4）探测主机用户实现信息收集

beacon.exe创建svchost.exe进程，调用命令cmd /c quser探测主机用户信息实现信息收集。



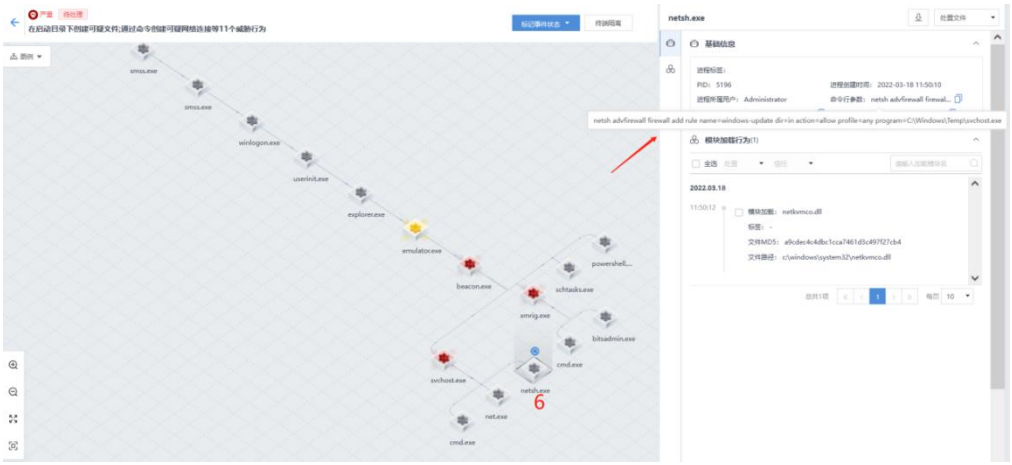
（5）激活主机guest用户实现持久化攻击

beacon.exe创建svchost.exe进程，调用命令net user guest /active激活主机guest用户实现持久化攻击。



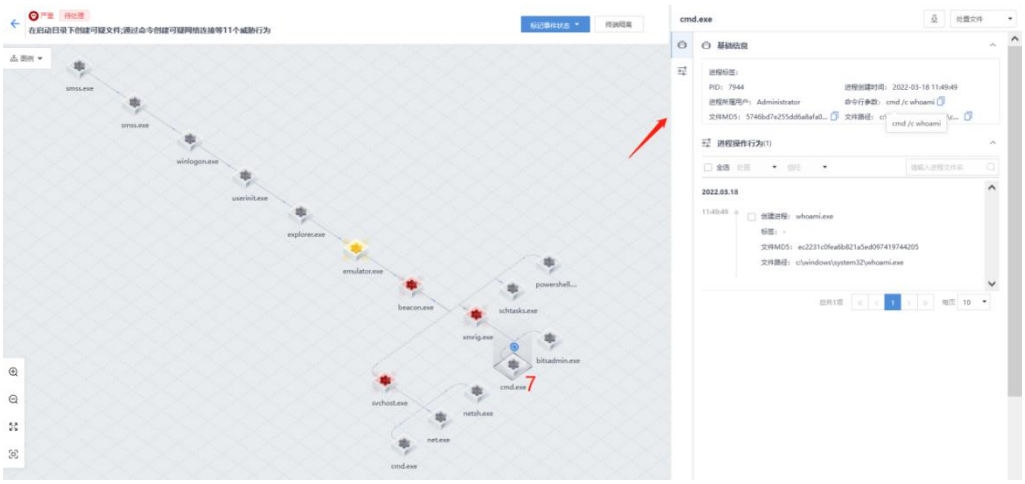
（6）通过netsh创建可疑防火墙绕过名单

beacon.exe创建svchost.exe进程，调用命令netsh添加防火墙白名单规则、建立可疑连接，企图绕过防火墙安全防护。



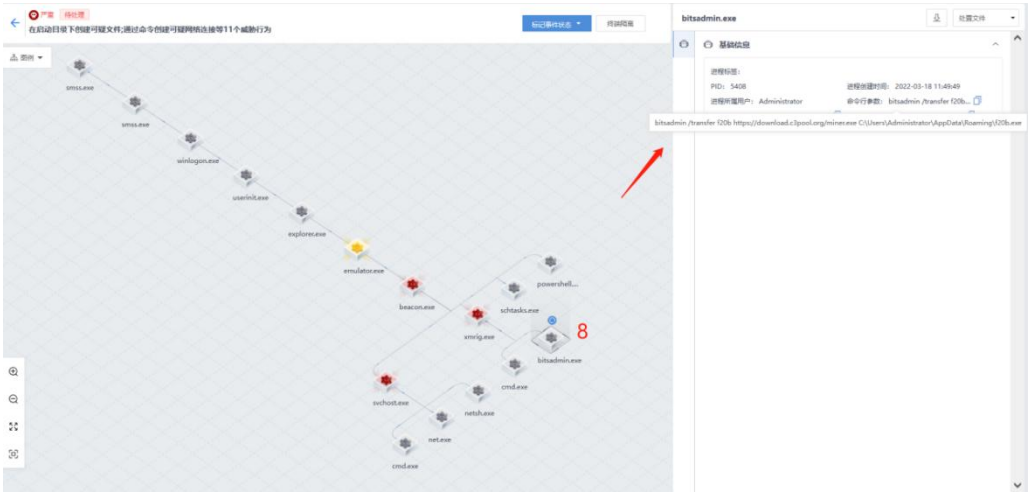
（7）查看当前用户权限，收集敏感信息

beacon.exe创建xmrig.exe文件和进程，调用命令cmd /c whoami查看当前用户权限，收集敏感信息。



（8）下载挖矿病毒进行挖矿

beacon.exe创建xmrig.exe文件和进程，调用bitsadmin.exe下载病毒进行挖矿。



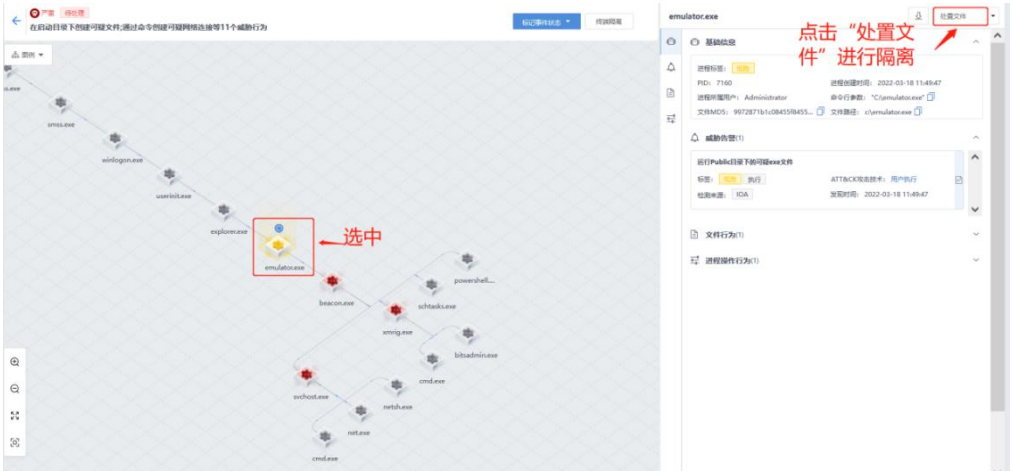
攻击事件处置：

1、溯源总结：

测试机感染了挖矿病毒。攻击样本emulator.exe创建了恶意文件beacon.exe和xmrig.exe，拉起了多个进程完成了执行、持久化、防御规避、凭据访问、探测、命令与控制等攻击行为。

2、处置方法如下：

（1）隔离恶意文件emulator.exe、beacon.exe、xmrig.exe。



（2）隔离终端，在不影响业务的情况下隔离终端、避免威胁横向扩散。

（3）威胁终端进行全盘查杀，清除残留项。

2、攻击者通过远程桌面登录/爆破获得权限、植入病毒，建议采用以下加固措施。

（1）关闭非必要的远程端口

（2）EDR开启远程桌面登录二次认证和暴力破解检测

（3）及时更新系统安全补丁

4.5.2. 漏洞响应

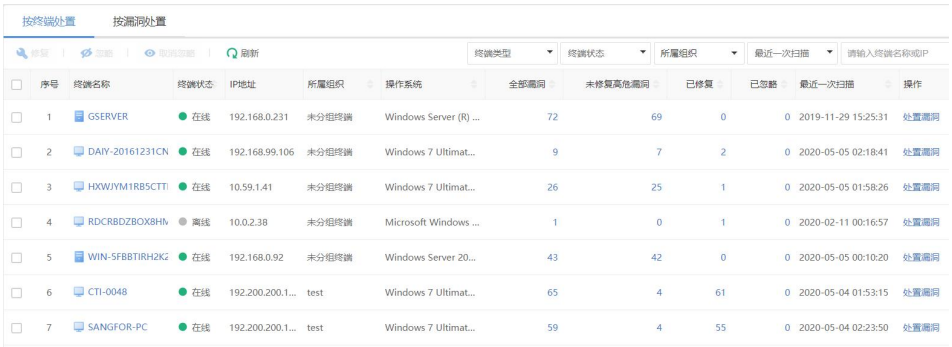
漏洞响应包含补丁修复和轻补丁漏洞免疫两部分，轻补丁漏洞免疫展示当前所有漏洞已经免疫的终端，补丁修复包含按终端处置和按漏洞处置两种方式进行漏洞修复。

> 说明：
> 本功能需先完成对内网终端完成漏洞检测，再进行漏洞修复。

4.5.2.1. 补丁修复

按终端处置

在[按终端处置]页签下，EDR可针对具体终端进行漏洞响应，可在处置页面查看待处置终端的全部漏洞、未修复高危漏洞、已修复/已忽略漏洞数等信息，可针对单一/多个终端进行处置，处置页面如下图所示。



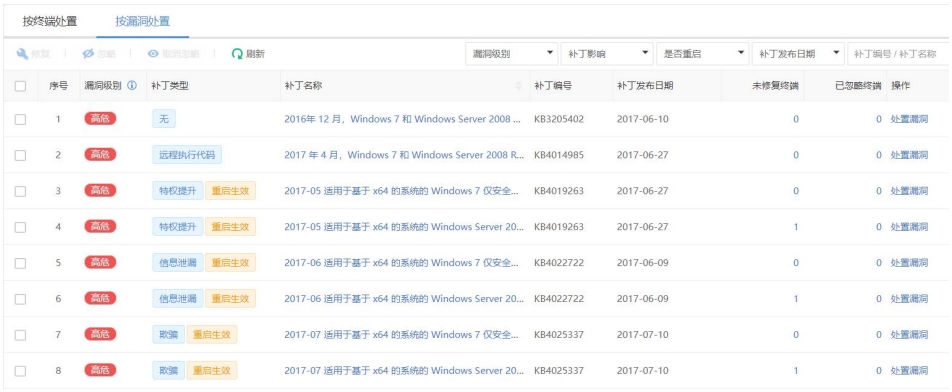
在[**处置漏洞**]页签下，可以：

1.查看具体终端相应的漏洞级别、补丁相关信息及修复状态，并可通过漏洞级别、补丁影响、是否重启及修复状态等类型进行筛选；

2.勾选多个补丁信息，进行一键修复或忽略。

按漏洞处置

在[按漏洞处置]页签下，EDR可针对具体漏洞进行漏洞响应，可在处置页面查看待处置的漏洞及补丁信息，可针对单一/多个漏洞进行处置，处置页面如下图所示。



在**[处置漏洞]**页签下，可以：

1.查看与此漏洞相关的具体终端相关信息，包括终端名称、终端状态、IP地址、所属组织、操作系统等信息，同时可针对终端状态、终端组织及修复状态等标签进行筛选，也可通过终端名称或IP进行检索；

2.勾选多个终端进行意见修复或忽略。

4.5.2.2. 轻补丁漏洞免疫

深信服EDR下一代轻补丁漏洞免疫，直接在内存里对有漏洞的代码进行修复，避免遭受漏洞攻击。通过EDR终端安全管理系统提供的高危漏洞免疫模块，提供业务无感知的轻补丁修复能力。

点击<单击了解技术优势>按钮，可以了解轻补丁漏洞免疫的功能详情和价值。

主要从漏洞视角和终端视角来展示当前所有漏洞已经免疫的终端。

漏洞视角

1.查看与管理

在[响应中心/轻补丁漏洞免疫/漏洞视角]页签下，可以查看漏洞的名称、漏洞的编号、漏洞的危害、未免疫终端、已免疫终端等详细信息。

支持根据漏洞危害/远程执行代码进行筛选，同时也支持“输入漏洞名称/别称/编号”进行关键字搜索，便于精准定位漏洞详情，方便运维管理。

2.免疫或取消免疫的配置

在[操作]栏下，点击<处置漏洞>，可以对当前漏洞进行免疫或取消免疫的操作，支持批量配置免疫或取消免疫。

📖 **说明：**

轻补丁漏洞免疫能在业务不中断、终端不重启的情况下阻止漏洞被功击利用，当某项高危漏洞免疫取消时，防护将失效；若要永久性阻止漏洞被攻击利用，建议使用补丁修复该漏洞，修复后的漏洞将无需免疫。

终端视角

1.查看与管理

在[响应中心/轻补丁漏洞免疫/终端视角]页签下，可以查看终端的名称、终端状态、IP地址、所属组织、操作系统、未免疫高危漏洞及已免疫高危漏洞等详细信息。

支持根据“终端类型”、“终端状态”、“所属组织”进行筛选，同时也支持“输入终端名称/IP”进行关键字搜索，便于精准定位终端详情，方便运维管理。

2.免疫或取消免疫的配置

在[操作]栏下，点击<处置漏洞>，可以对当前漏洞进行免疫或取消免疫的操作，支持批量配置免疫或取消免疫。

📖 **说明：**

系统未检测到需要免疫高危漏洞的终端，可能是功能未开启或者管控终端不存在高危漏洞。

4.5.3. 威胁狩猎

当客户已知或从外部获取新威胁情报时，可通过简易的条件组合检索相关情报信息（如IP、域名、行为等），即可在全网发起所有终端的威胁狩猎，定位潜在威胁的主机、进程等相关信息，助力客户发现新威胁或排查全网潜在风险。

4.5.3.1. 单条件检索

单条件检测包括域名访问检索、网络连接检索、可执行文件hash检索和文件名检索。

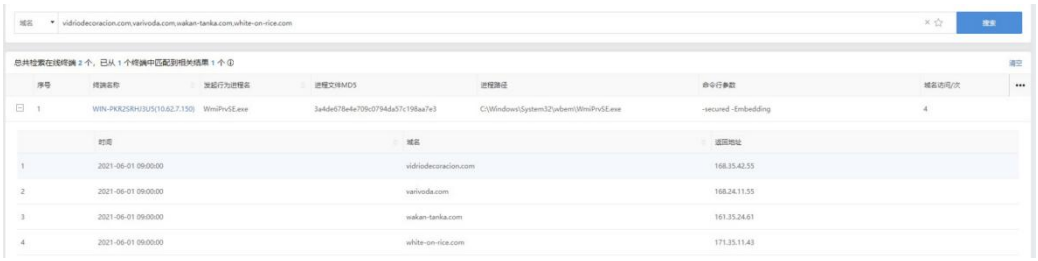
域名访问检索

输入单个或多个域名，通过","（英文逗号）区分，将检索与相关域名通信的设备和行为信息。域名支持使用"*"通配符进行模糊查询。

示例：已知Emotet病毒相关域名情报，查询可能感染Emotet病毒的终端和与Emotet病毒域名通信的对应进程信息

写法：vidriodecoracion.com,varivoda.com,wakan-tanka.com,white-on-rice.com

查询结果如下图。



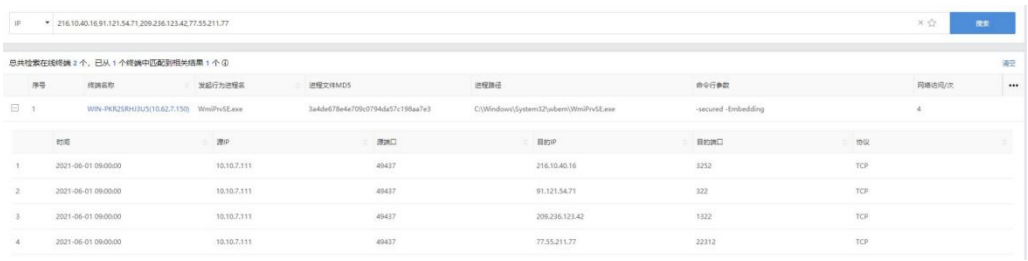
网络连接检索

输入单个或多个IP地址，通过","（英文逗号）区分，检索源IP或目的IP中包含所检索地址的网络连接行为的终端和对应进程信息。

示例：已知Emotet病毒相关IP情报，查询可能感染Emotet病毒的终端，以及与Emotet病毒IP地址通信的进程信息

写法：216.10.40.16,91.121.54.71,209.236.123.42,77.55.211.77

查询结果如下图。



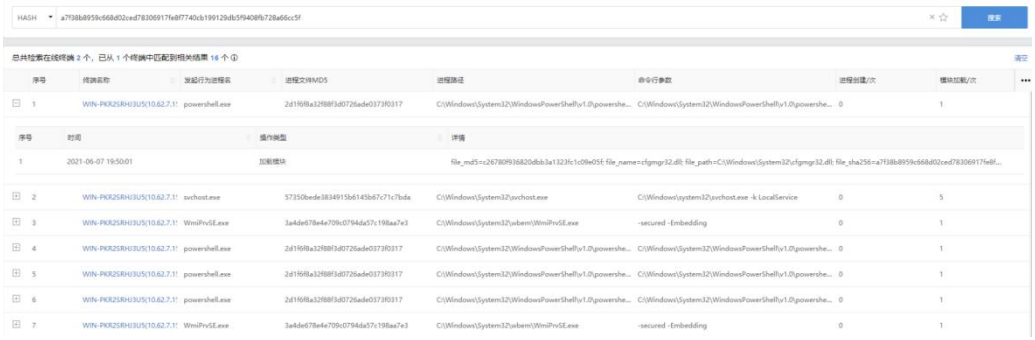
可执行文件Hash检索

输入单个或多个待查询的可疑程序文件的MD5或SHA256值，通过","（英文逗号）区分，可检索进程操作事件和模块加载事件中，与输入的文件Hash匹配的终端和对应的进程信息。

示例：已知Emotet病毒相关文件SHA256情报，查询可能感染Emotet病毒的终端

写法：a7f38b8959c668d02ced78306917fe8f7740cb199129db5f9408fb728a66cc5f

查询结果如下图。



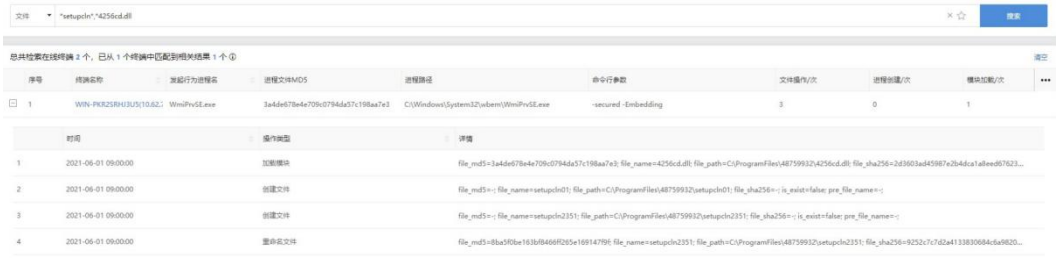
文件名检索

输入单个或多个待查询的可疑文件的文件名，通过","（英文逗号）区分，检索与所输入文件名相关的终端和事件。文件名支持"*"通配符进行模糊查询。

示例：获取到Emotet恶意文件的名称，查询可能感染Emotet病毒的终端

写法：setupcln*,4256cd.dll

查询结果如下图。



4.5.3.2. 组合条件检索

多行为组合搜索语句构成

搜索语句由“搜索对象”、“字段名”、“值”、“比较运算符”、“逻辑运算符”组成，如下图所示。

对象1.字段1 比较运算符 值1 逻辑运算符 对象2.字段2 比较运算符 值2

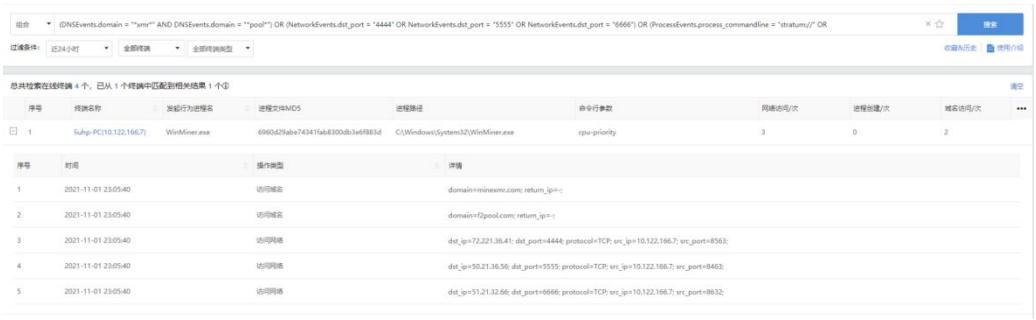
Network.src_ip	=	"1.1.1.1"	OR	Process.process_name	=	"Powershell*"

示例：挖矿病毒检测

写 法 ： (DNSEvents.domain = "*xmr*" AND DNSEvents.domain = "*pool*") OR (NetworkEvents.dst_port = "4444" OR NetworkEvents.dst_port = "5555" OR NetworkEvents.dst_port = "6666") OR (ProcessEvents.process_commandline = "stratum://" OR ProcessEvents.process_commandline = "cpu-priority")

备注：整个搜索语句的元素不区分大小写。

查询结果如下图。



对象和字段说明

可检索对象包含域名访问、网络连接、进程操作、文件操作、模块加载、设备信息。具体对象和对应的字段如下。

域名访问表检测字段：

字段名	字段说明	举例
timestamp	事件发生时间	2021-06-14 12:12
device_name	终端名称	edr0043(10.32.36.52)
action_type	操作类型	访问域名
domain	查询的域名	baidu.com
return_ip	返回的地址	39.156.69.79,220.181.38.148
process_id	进程ID	4305
process_name	进程名	PING.EXE
process_md5	进程文件MD5	f926bedd777fa0f4f71dd2d28155862a
process_SHA256	进程文件SHA256	1d35014d937e02ee090a0cfc903ee6e6b1b65...
process_path	进程路径	C:\WINDOWS\system32\PING.EXE
process_commandline	进程执行命令	C:\WINDOWS\system32\PING.EXE
process_user	进程所属用户	NT AUTHORITY\SYSTEM

网络连接表检测字段：

字段名	字段说明	举例
timestamp	事件发生时间	2021-06-14 12:12
device_name	终端名称	edr0043(10.32.36.52)
action_type	操作类型	访问网络
src_ip	源IP	1.1.1.1
src_port	源端口	22345
dst_ip	目的IP	192.168.1.1
dst_port	目的端口	80
protocol	协议（tcp/udp）	tcp
process_id	进程ID	4305
process_name	进程名	PING.EXE
process_md5	进程文件MD5	f926bedd777fa0f4f71dd2d28155862a
process_SHA256	进程文件SHA256	1d35014d937e02ee090a0cfc903ee6e6b1b65...
process_path	进程路径	C:\WINDOWS\system32\PING.EXE
process_commandline	进程执行命令	C:\WINDOWS\system32\PING.EXE
process_user	进程所属用户	NT AUTHORITY\SYSTEM

文件操作表检测字段：

字段名	字段说明	举例
timestamp	事件发生时间	2021-06-14 12:12
device_name	终端名称	edr0043(10.32.36.52)
action_type	操作类型	创建文件
file_name	文件名	sss.php
file_md5	文件的MD5值	f926bedd777fa0f4f71dd2d28155862a
file_sha256	文件的SHA256值	93d48bf194d87b190dc1fb9b8837011a58dc1...
file_path	文件路径	E:\www\sss.php
prev_file_name	修改前文件路径	E:\www\shell.php
is_exist	文件是否存在	是/否
process_id	进程ID	4305
process_name	进程名	PING.EXE
process_md5	进程文件MD5	f926bedd777fa0f4f71dd2d28155862a
process_SHA256	进程文件SHA256	1d35014d937e02ee090a0cfc903ee6e6b1b65...
process_path	进程路径	C:\WINDOWS\system32\PING.EXE
process_commandline	进程执行命令	C:\WINDOWS\system32\PING.EXE
process_user	进程所属用户	NT AUTHORITY\SYSTEM

进程操作表检测字段：

字段名	字段说明	举例
timestamp	事件发生时间	2021-06-14 12:12
device_name	终端名称	edr0043(10.32.36.52)
action_type	操作类型	创建进程
child_id	子进程ID	4305
child_name	子进程文件名	SearchFilterHost.exe
child_md5	子进程文件MD5值	f926bedd777fa0f4f71dd2d28155862a
child_sha256	子进程文件的SHA256值	0ba37d0db6d5d74e9b1d8ebc540c1acd4a47...
child_path	子进程路径	C:\WINDOWS\system32\SearchFilterHost.exe
child_commandline	子进程执行命令	0 812 816 824 8192 820
child_user	子进程所属用户	NT AUTHORITYSYSTEM
process_id	进程ID	29733
process_path	进程路径	C:\Windows\system32\services.exe
process_md5	进程文件MD5值	f926bedd777fa0f4f71dd2d28155862a
process_name	进程名	services.exe
process_SHA256	进程文件SHA256	1d35014d937e02ee090a0cfc903ee6e6b1b65...
process_commandline	命令行参数	C:\Windows\system32\services.exe
process_user	进程所属用户	NT AUTHORITY\SYSTEM

模块加载检测字段：

字段名	字段说明	举例
timestamp	事件发生时间	2021-06-14 12:12
device_name	终端名称	edr0043(10.32.36.52)
action_type	操作类型	加载模块
file_name	加载文件名	kernel32.dll
file_path	文件路径	C:\Windows\System32\kernel32.dll
file_md5	被加载文件的MD5值	e1ff9d65e6b86f7ebb531ae36c5af635
file_sha256	被加载文件的SHA256值	92981d598dc950c191b0320955dd777fbac7b...
process_id	进程ID	4305
process_name	进程名	PING.EXE
process_md5	进程文件MD5	f926bedd777fa0f4f71dd2d28155862a
process_SHA256	进程文件SHA256	1d35014d937e02ee090a0cfc903ee6e6b1b65...
process_path	进程路径	C:\WINDOWS\system32\PING.EXE
process_commandline	进程执行命令	C:\WINDOWS\system32\PING.EXE
process_user	进程所属用户	NT AUTHORITY\SYSTEM

设备信息表检测字段：

字段名	字段说明	举例
device_name	终端名称	edr0043(10.32.36.52)
host_name	主机名	sangfor
os_name	系统名称	Microsoft Windows 7 专业版
os_version	系统版本	6.1.7601 Service Pack 1 Build 7601
mac_address	mac地址列表	FE:FC:FE:11:98:F2
ipv4_addresses	ipv4地址列表	10.62.7.150
ipv6_addresses	ipv6地址列表	fe80::b0eb:5d89:f3c1:63d2
cpu_total	cpu总Hz	2.4GHz
cpu_used	cpu使用大小	1GHz
mem_total	内存总大小	4096MB
mem_used	内存使用大小	1024MB
disk_total	磁盘总大小	50GB
disk_used	磁盘使用大小	20GB
user_name	系统账户名	Administrator
group_name	所属分组	Administrators
last_login_time	上次登录时间	2020-03-16T07:41:16.730Z

值说明

值输入时需加双引号。支持通配符搜索，支持在一个值内的单个和多个字符的通配符搜索，使用"*"号表示多个字符的通配符搜索，匹配零个或多个字符。通配符"*"只支持与比较符"="（等于）、"!="（不等于）配合使用。

示例：搜索单词 mongodb 或 mondodb，可使用写法为： mon*

比较运算符

运算符	说明
=	等于
>	大于
>=	大于或等于
<	小于
<=	小于或等于
!=	不等于

逻辑运算符说明

日志检索系统支持AND、OR、NOT三种运算符

1、AND 运算符

AND 运算符关联两字段内容，代表两字段内容必须同时满足。

2、OR 运算符

OR 运算符关联两个字段对应的值，满足任意一项即可。

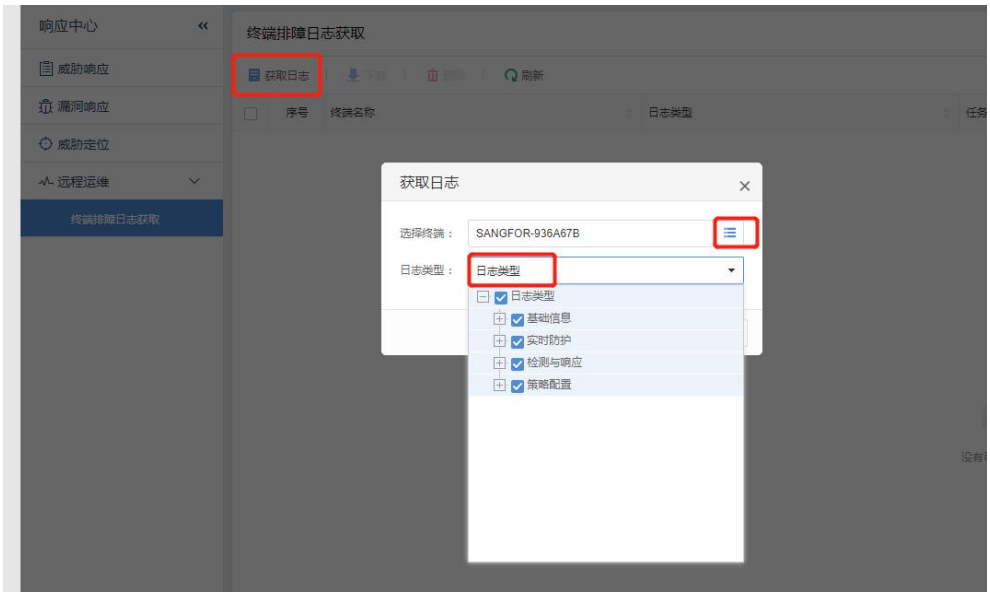
3、NOT 运算符

NOT 运算符排除含有 NOT 运算符后面的单独项或短语的记录。相当于非运算符。

4.5.4. 远程运维

远程运维可支持远程获取终端排障日志，便于运维管理。

1.在[响应中心/运维管理/终端排障日志获取]的页签下，点击[获取日志]，选择对应的终端以及日志类型，如下图所示。

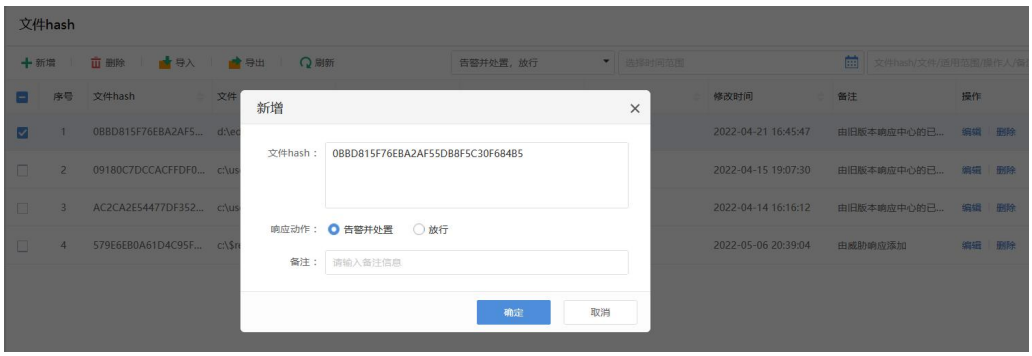


2.点击<确定>，等待日志获取完成，点击<下载>，可以下载该终端的排障日志。

4.5.5. 自定义 IOC

为了在误报漏报场景可快速响应、提升运维效率。支持根据文件hash设置黑白名单

打开[响应中心/自定义IOC]，如下图。当发现恶意文件漏报或误报时，可以根据文件hash设置黑白名单。



响应动作包括告警并处置、放行。

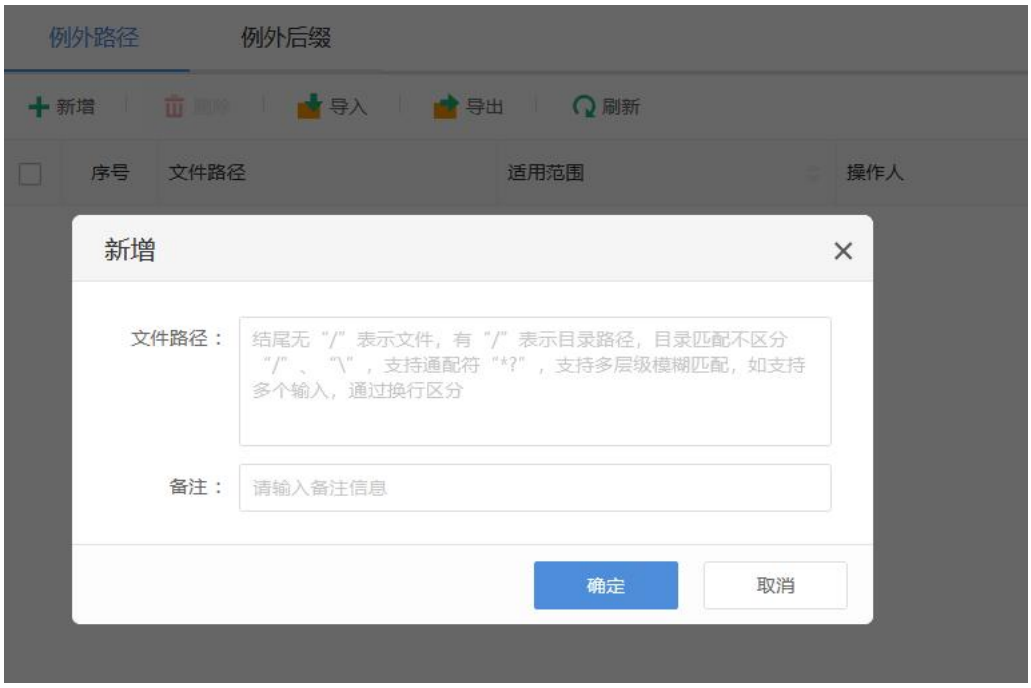
告警并处置：当发现漏报时，将响应动作设置为告警并处置。

放行：当发现误报时，将响应动作设置为放行。

4.5.6. 排除策略

支持按文件、目录、后缀加白，支持模糊匹配、批量导入功能。

打开[响应中心/排除策略]，如下图。当发现误报时，可以根据文件、文件目录、后缀进行排除，排除的文件、目录不会进行病毒查杀、实时监控、webshell检测等。



排除文件：结尾无“/”表示文件，如 D:\2022\10工具\test

排除目录：结尾有“/”表示目录，如 D:\2022\10工具\test\

根据后缀排除，后缀格式为.xxx，如下图。

4. 6. 联动响应

联动管理可实现EDR与深信服AC、AF、SIP、aTrust、合规自检平台、X-Central及MSS的联动对接与管理，为客户提供从发现威胁到查杀闭环处理方案。打开[系统管理/联动管理]，如下图所示。点击页面上的<如何接入>的按钮，可以查看不同产品的联动配置。

联动可以实现的功能

各产品与EDR联动功能支持情况如下表所示。

表12 联动功能

联动产品	部署Agent	联动隔离终端	日志上报	访问控制	联动下发查杀扫描	联动处置威胁文件	IOC取证	终端AIO	环境感知
AC	√	×	×	×	√	√	×	√	×
AF	×	×	×	×	√	√	√	×	×
SIP	×	√	√	√	√	√	√	×	×
X-Central	×	×	×	×	×	√	√	×	×
aTrust	×	×	×	×	×	×	×	√	√

📖 说明：

深信服终端All in one（以下简称AIO）针对深信服各安全产品，提供统一客户端安装卸载、统一系统托盘、产品功能联动等特性，结合零信任安全办公，在终端与接入建立控制点，为客户提供内网办公、远程办公、混合办公一体化的整体解决方案。

联动全局配置

EDR和任何产品联动，需要先启用“联动设备准入设置”和“SSL/TLS协议设置”。打开[系统管理/系统设置/基本设置]，如下图，启用联动设备准入设置，并设置联动设备接入时间，联动设备需要在设置的指定时间内接入；同时“SSL/TLS协议设置”启用TLS1.0和TLS1.1。

4.6.1. EDR 与 AC 联动

AC与EDR 联动可实现客户端统一安装和使用、统一AC和EDR客户端托盘、AC联动EDR下发病毒查杀、AC联动EDR从终端封堵防代理软件。

联动条件

AC与EDR联动需要满足以下版本要求和服务端口开放要求，防火墙需要终端与设备之间、设备与设备之间以下通信端口。

设备类型	版本	服务端口	备注
AC	13.0.26	TCP80：客户端 portal 认证端口； TCP88：准入客户端上报合规检查结果； TCP886：客户端上报审计日志； TCP817：客户端自动升级及安装； TCP61111：终端代理解密上报 SSL 密钥； UDP667：客户端发送保活心跳； UDP61182：UDP 自动找网关端口；	

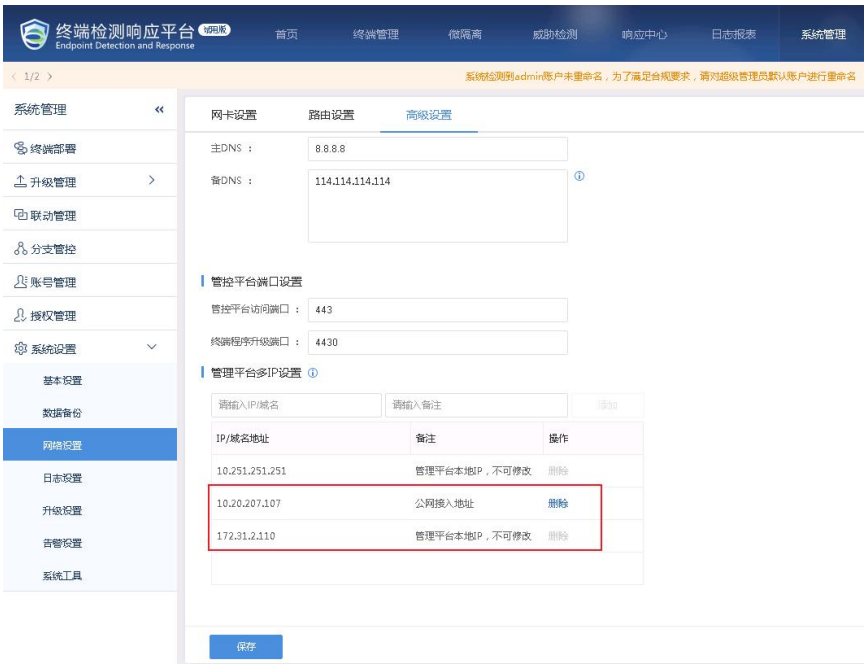
		TCP61182：TCP 自动找网关端口 TCP9998：AC 联动通信端口	
EDR 管理端	3.5.15	TCP 443：控制台访问端口（可修改） TCP 4430：Agent 组件更新和病毒库更新（可修改） TCP 8083：Agent 和管理端业务通信端口 TCP 54120：管理端控制 Agent 禁用/启用/卸载 ICMP：Agent 安装时，到管理端连通性探测	

联动配置

1.EDR管理端接入配置

在[系统管理/系统设置/网络设置/高级配置/管理端端口设置]页面，可以修改 EDR 管理端控制台端口和终端程序升级安装端口，建议保持默认配置端口。

EDR 管理端接口如果存在多个 IP 地址，需要在[管理端多 IP 设置]页面配置 EDR 管理端所有 IP 地址。



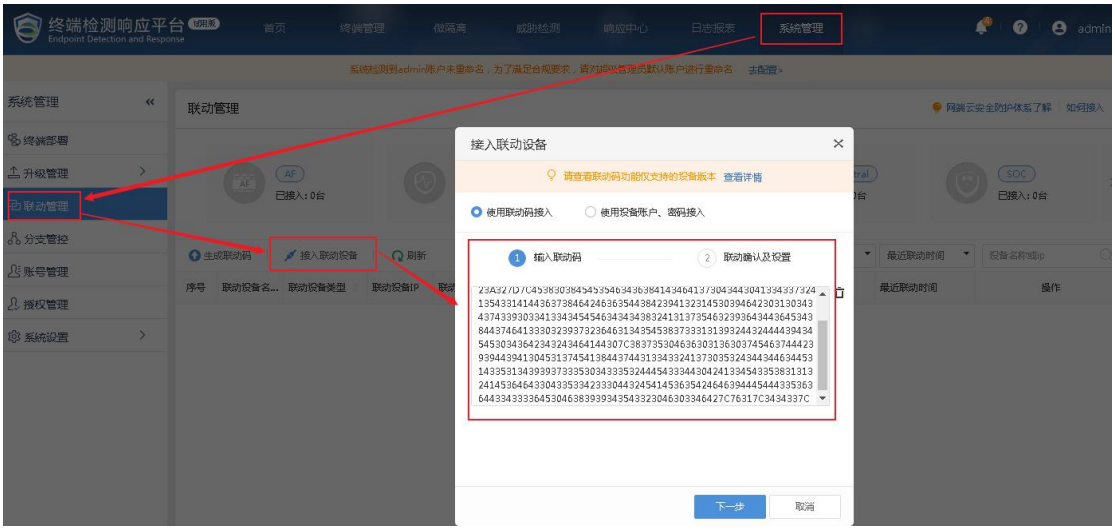
2.设备对接配置

（1）AC生成联动码

登陆AC管理端，在[终端行为安全/终端安全联动]页面，选择联动设备通信的IP地址后，点击生成联动授权码。

（2）EDR接入联动设备

登录EDR管理端，在[系统管理/]联动管理]页面，点击接入联动设备，选择[使用联动码接入]，粘贴AC上生成的联动码。



点击<下一步>后可以读取到AC的连接信息，选择与AC通信的IP地址后点击确定即

可。

配置完成后，点击<连通性测试>测试联动配置是否成功。

通过AC也可以看到EDR联动状态已经成功。

说明：

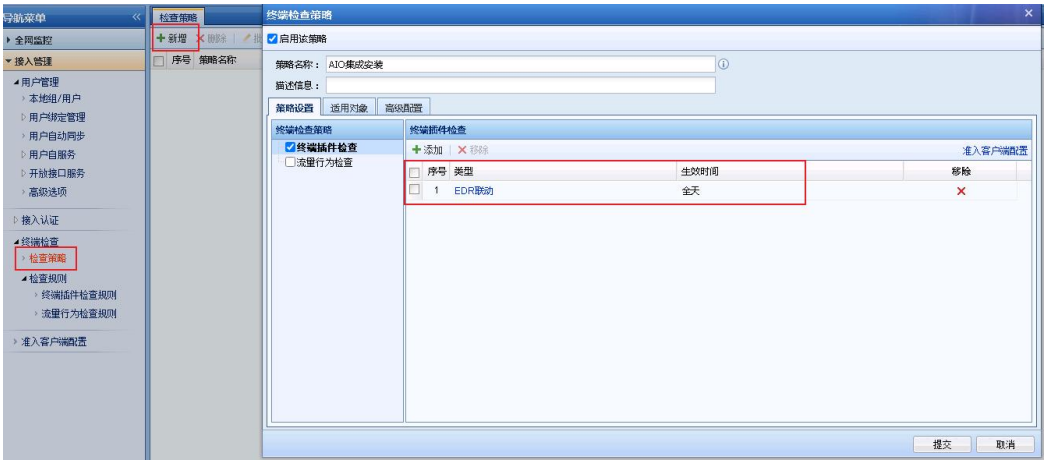
也可以在 EDR 生成联动码，在 AC 识别联动码生成关联关系。

3.启用集成策略

（1）AC集成策略配置

在AC管理端[接入管理/终端检查/检测规则/终端插件检查规则]页面，新增[客户端集成规则]，输入规则名称、规则类型、规则描述，客户端需要集成的设备选择配置的联动的EDR设备。

新增检查策略，将创建的集成策略关联给需要安装AIO客户端的用户。



说明：

准入策略启用后，目标终端会显示准入安装页面，上网过程会中断直至准入安装完毕，建议开启策略前提前通知用户。

（2）EDR集成策略配置

用户如果需要通过先安装EDR再联动安装AC客户端，还需在EDR管理端[系统管理/系统设置/基本设置]页面勾选[客户端集成并下载AC零信任客户端]选项。

说明：

如果所有用户均通过先安装 AC 准入客户端再联动下载 EDR 客户端，也可不开启该选项。

联动效果

1.客户端AIO

（1）客户端安装

全新安装场景(客户当前无AC准入和EDR)

该场景面向用户新上AC准入和EDR场景。

AC开启准入策略后，用户上网流量经过AC，AC会重定向用户至安装准入客户端页面。

下载安装完成后，如果未开启准入认证客户端，可在任务管理器看到准入进程。

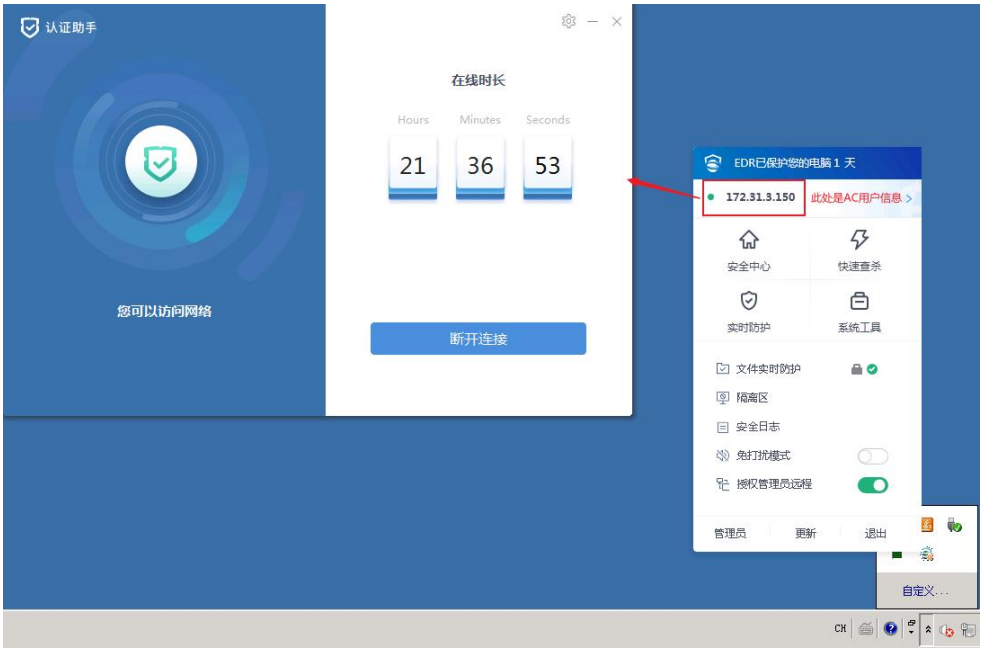
用户关联了集成安装策略，EDR客户端会在后台静默下载安装（由于EDR安装包比较大，内网环境需要等待5-10分钟）。

说明：

当前版本 EDR 后台安装暂时没有下载和安装进度可以展示。

等待EDR客户端安装完成后，如果用户未开启AC准入认证，系统托盘只有EDR客户端。

如果用户开启了AC准入认证客户端，系统托盘会展示AIO融合后的图标。



说明：

AC+EDR 场景下，AIO 系统托盘主界面为 EDR 客户端。

加装场景(客户当前有AC，但是没有EDR)

该场景面向已经部署AC准入客户端，新增部署EDR客户端的用户。

1.用户如果部署的AC为非AIO版本，需要先完成AC设备升级，并完成EDR设备部署和联动配置，具体各项配置与前述基本一致。

2.客户端AC准入找到网关后，客户端会静默升级，升级完成后会在后台静默安装EDR客户端，EDR静默安装过程需要耐心等待。

3.客户端升级安装全部完成后，客户端系统托盘会融合成一个，具体过程与新装和升级场景基本一致。

加装场景(客户当前有EDR，但是没有AC)

该场景面向已经部署EDR客户端，新增部署AC准入客户端的用户。

1.用户如果部署的EDR为非AIO本，需要先完成EDR管理端升级，并完成AC设备部署和联动配置，各项配置与前述基本一致。

2.EDR平台升级完成以后，客户端会自动静默升级，升级过程需要耐心等待。

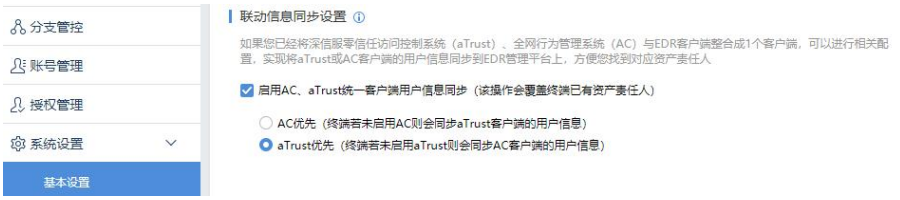
3.EDR管理端如果同步开启了【客户端集成并下载AC准入客户端】选项，客户端更新成功后会自动在后台静默安装AC准入客户端。

4.客户端升级安装全部完成后，客户端系统托盘会融合成一个，具体过程与新装和升级场景基本一致。

（2）用户信息同步功能

EDR平台可配置是否开启信息同步功能，且可配置接受AC/aTrust用户信息的优先级，优先接受AC还是aTrust传来的信息。

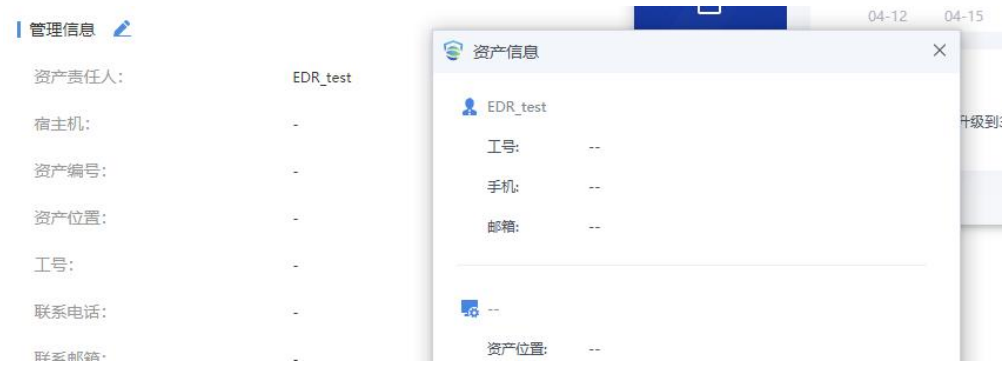
EDR页面配置：



触发方式：

AIO场景下，在终端管理平台登录AC，AC会将登陆的用户名发送给EDR，EDR上报到平台。AC登录用户名变化时，EDR会收到新登录用户名消息，并上报给平台。如果aTrust优先级高，且aTrust此时上报了用户名消息，则会用aTrust的用户名信息。

在EDR Agent界面填写后，会上报到平台，查看配置中心会发现信息来源为EDR。



登录AC后，AC将用户名发送给EDR，EDR终端和平台的用户名显示均为AC上报的用户名，且配置中心显示消息来源为AC产品线，分组路径作为附加信息也保存在配置中心。

（3）客户端使用

当EDR与AC集成时，当AC开启准入认证策略，并且终端用户未认证前，托盘上方显示“上网认证”的按钮。

用户如果已经认证在线，则看到的是用户认证信息。

（4）客户端退出

AC和EDR无法一次性整体退出，右键点击系统托盘，点击退出选项，输入EDR退出密码，退出的是EDR的单独客户端。

EDR客户端退出后，系统托盘将变为独立的AC认证客户端托盘，如需整体退出，还需要单独再次退出AC的认证客户端，AC认证客户端退出后，用户会注销下线。

说明：

AC 认证客户端退出仅关闭认证客户端，准入运行进程依然会常驻运行。

（5）客户端卸载

当前版本各产品线卸载相互独立，互不干扰。

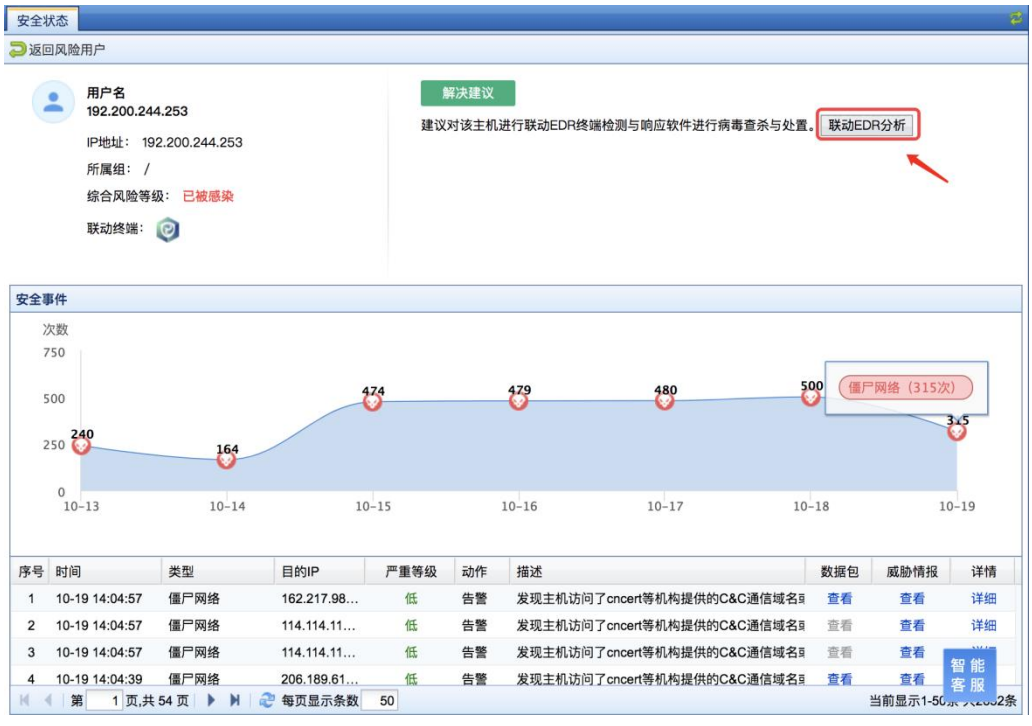
说明：

AC 与 EDR 终端 AIO 功能当前仅支持 win xp、win 7、win 8、win8.1、win10 和 win11 系统，不支持 MAC OS、Linux 和 Windows Server 操作系统。

2.联动下发病毒查杀

当AC开启“僵尸主机检测”，并识别到风险终端时，可以联动EDR进行查杀。打开AC设备[终端行为安全/终端上网安全/安全状态/风险用户]，如下图。

点击<查看明细>，如下图。



点击<联动EDR分析>，下发对风险终端病毒查杀操作，并返回查杀结果，如下图。从

AC设备可以对联动查杀发现的威胁文件可以进行“隔离”、“信任”、“忽略”等操作。

3.联动封锁防代理软件

当AC检测到终端存在防代理软件时，可以联动EDR对终端防代理软件进行封堵，解决防代理软件通过网络侧设备封堵效果不佳的问题。

打开AC[终端行为安全/终端防翻墙]，启用『代理工具检测』，如下图。

点击<配置选项>，启用『EDR联动阻断违规代理』，如下图。

当EDR检测到终端存在代理软件在运行，立即进行封堵，并弹窗告警，如下图。

打开AC[终端行为安全/终端防翻墙]，如下图，显示终端的代理软件已经被EDR阻断。

4.推广部署Agent

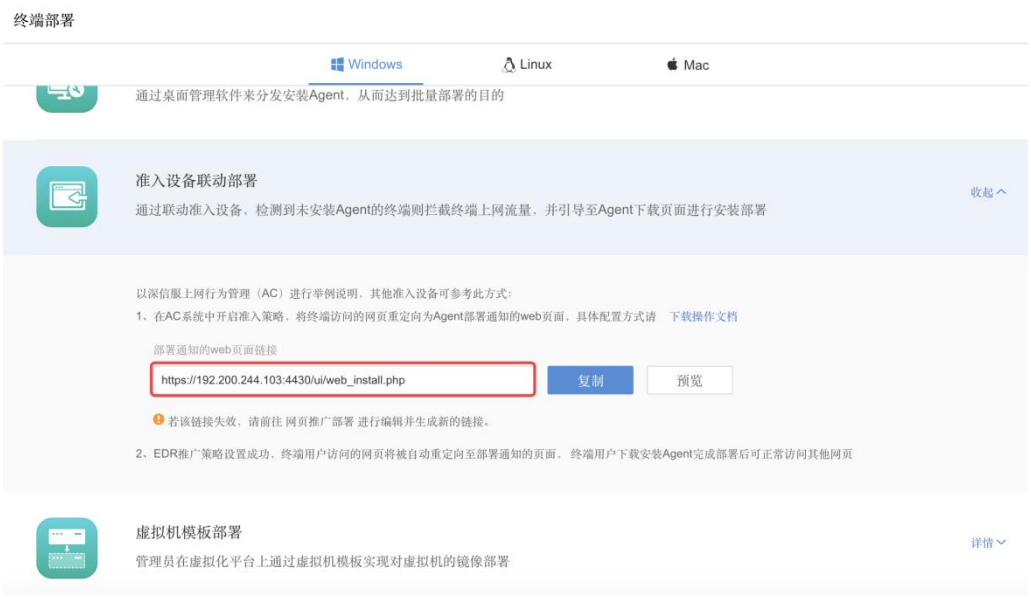
推广部署Agent是早期AC与EDR联动安装EDR客户端方案，此版本推出了AC与EDR联动终端AIO方案，可优先采用AIO方案。

此方案适用于在不安装AC准入客户端的情况下安装EDR客户端。

打开[终端行为安全/终端上网安全/安全能力/健全配置/终端检测与响应（EDR）]，点击<推送配置>配置推广安装Agent客户端的地址范围及重定向下载Agent客户端的地址，如下图。

策略适用范围：填写需要安装Agent客户端的内网电脑IP范围。

重定向地址：终端电脑上网被重定向到下载Agent客户端的地址，填写管理端[系统管理/终端部署]，上网行为管理系统联动部署中的地址，如下图。



配置完成，用户打开网页被重定向到通知部署Agent页面，此页面定时弹出，直到用户安装了Agent为止，如下图所示。

4.6.2. EDR 与 aTrust 联动

aTrust与EDR 联动可实现客户端统一安装和使用、统一aTrust和EDR客户端托盘、aTust联动EDR对终端环境进行检测，当终端存在风险时，禁止用户通过不安全终端访问业务，隔离来自终端的风险。

联动条件

aTrust与EDR联动需要满足以下版本要求和服务端口开放要求，防火墙需要终端与设备之间、设备与设备之间以下通信端口。

设备类型	版本	服务端口	备注
SDPC （控制器）	2.1.11	TCP4488：终端接入端口（缺省 443，可修改）	
Proxy （代理网关）	3.5.15	TCP443：WEB 服务代理端口（可修改） TCP441：隧道应用接入端口（可修改）	
EDR 管理端	172.31.2.110	TCP 443：控制台访问端口（可修改） TCP 4430：Agent 组件更新和病毒库更新（可修改） TCP 8083：Agent 和管理端业务通信端口	

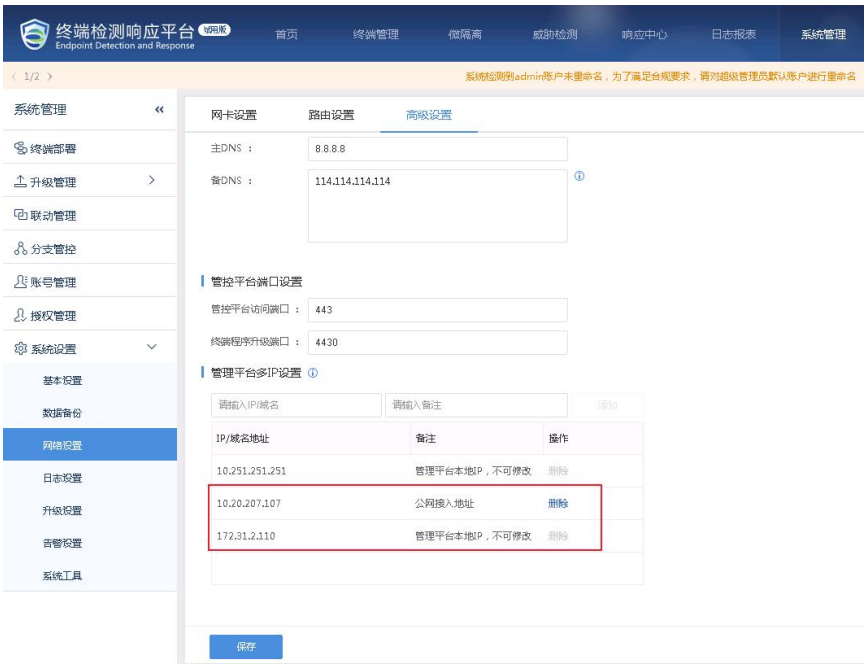
		TCP 54120：管理端控制 Agent 禁用/启用/卸载 ICMP：Agent 安装时，到管理端连通性探测	

联动配置

1.EDR管理端接入配置

在[系统管理/系统设置/网络设置/高级配置/管理端端口设置]页面，可以修改 EDR 管理端控制台端口和终端程序升级安装端口，建议保持默认配置端口。

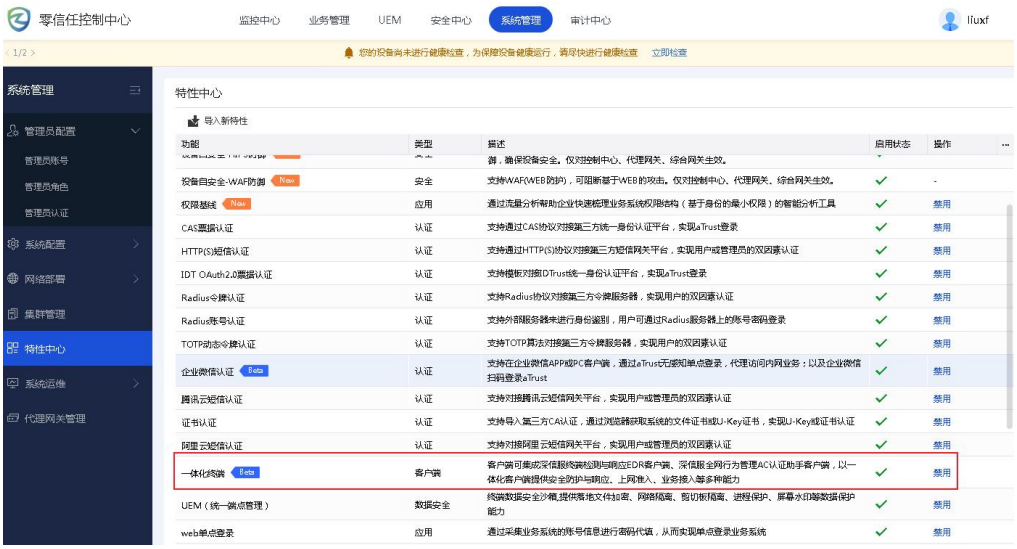
EDR 管理端接口如果存在多个 IP 地址，需要在[管理端多 IP 设置]页面配置 EDR 管理端所有 IP 地址。



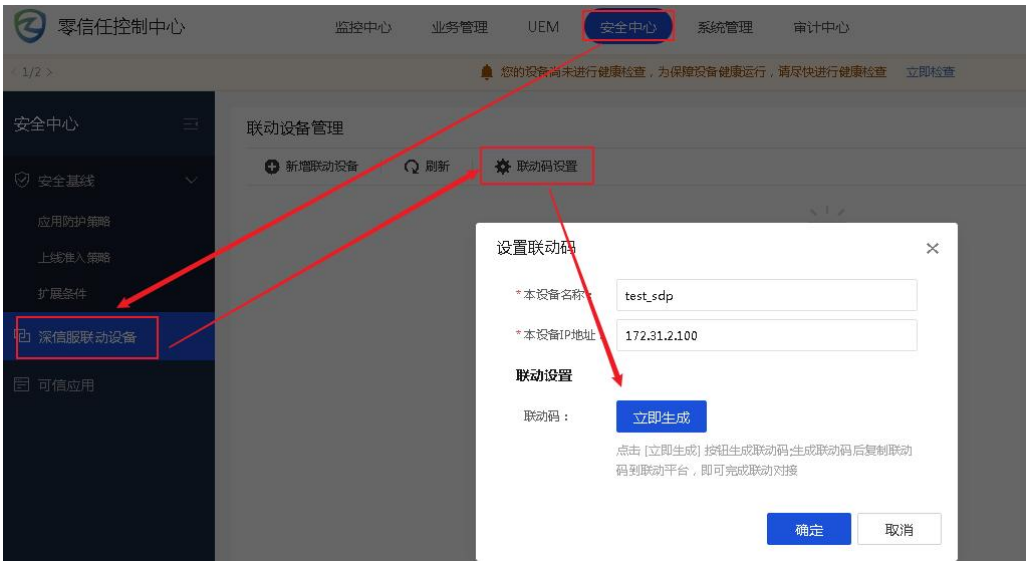
2.设备对接配置

（1）aTrust生成联动码

登陆aTrust管理端，打开[系统管理/特性中心]，开启<一体化终端>特性。

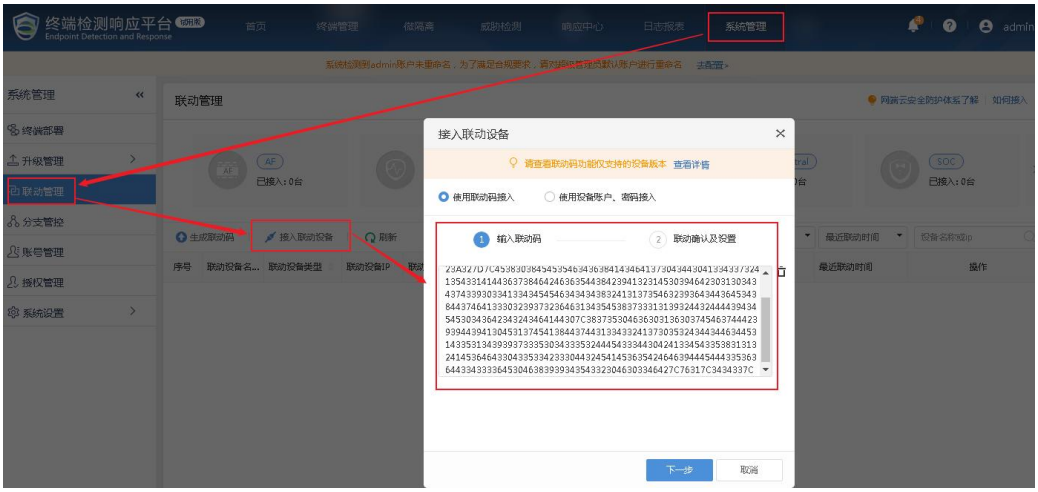


打开aTrust管理端[安全中心/深信服联动设备]页面，点击<联动码设置>，生成联动码。



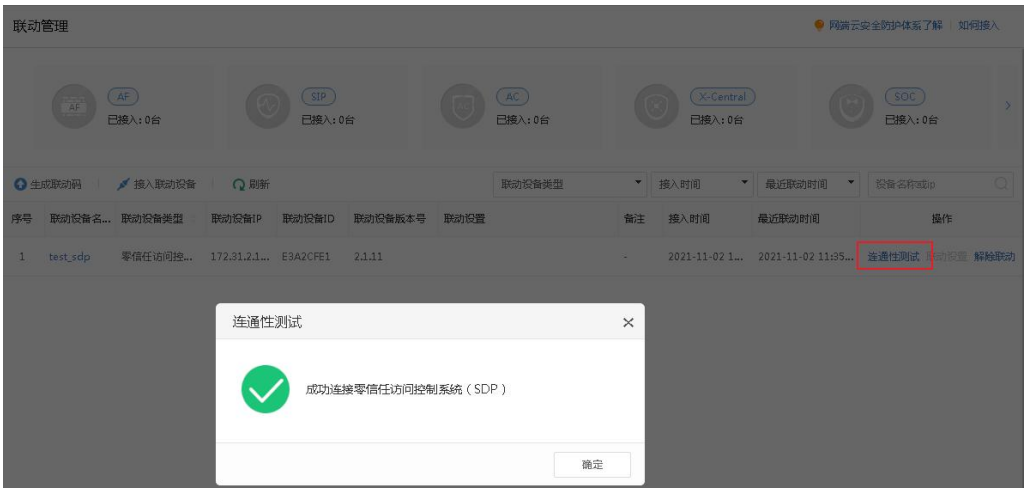
（2）EDR接入联动设备

登录EDR管理端，打开[系统管理/联动管理]页面，点击<接入联动设备>，选择[使用联动码接入]，粘贴aTrust上生成的联动码。



点击<下一步>后可以读取到aTrust的连接信息，选择与aTrust控制器通信的IP地址后点击确定即可。

配置完成后，点击<连通性测试>测试联动配置是否成功。



通过SDP也可以看到EDR联动状态已经成功。

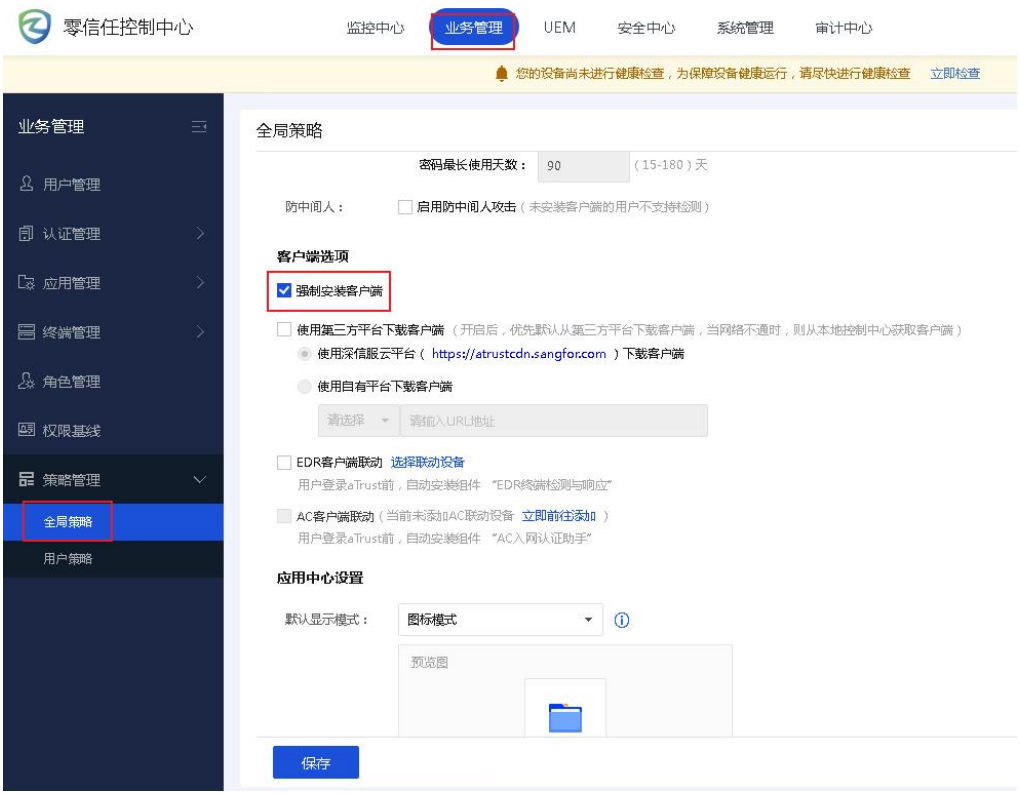
说明：

也可以在 EDR 生成联动码，在 aTrust 控制器识别联动码生成关联关系。

3.启用集成策略

（1）aTrust集成策略配置

登录aTrust管理端，打开[业务管理/策略管理/全局策略]页面，勾选【强制安装客户端】开启终端强制安装。



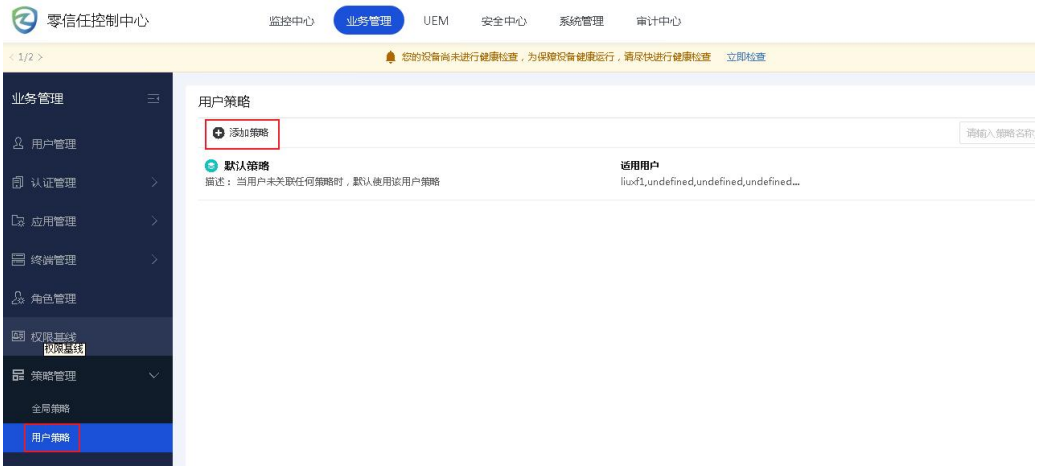
说明：

如果不开启强制安装客户端，纯 WEB 资源环境下不会主动推送 aTrust 客户端。

集成安装策略aTrust可以设置全局推送或者针对指定用户定向推送。

如果针对全部用户推广，可在全局策略同步勾选[EDR客户端联动]选项，并选择联动的EDR设备。

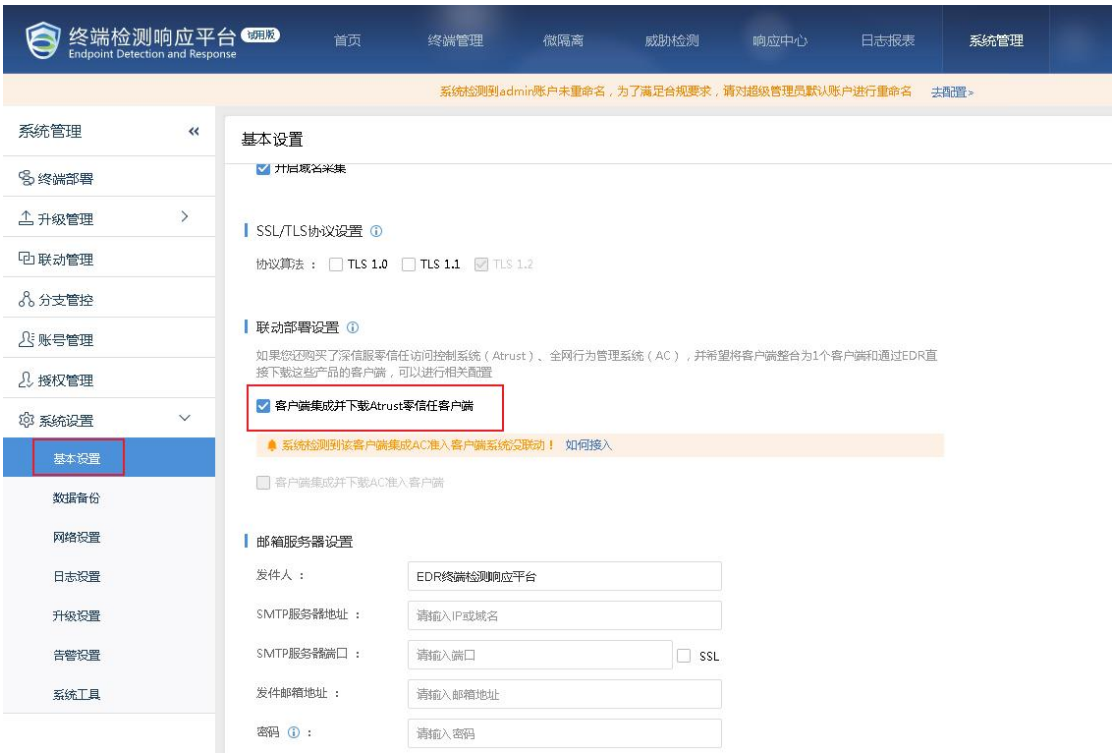
如果只针对部分用户推广，可以在aTrust管理端[业务管理/策略管理/用户策略]页面添加策略。



选择适用用户，勾选<EDR客户端联动>，并选择联动的EDR设备。

（2）EDR集成策略配置

用户如果需要通过先安装EDR再联动安装aTrust客户端，还需在EDR管理端[系统管理/系统设置/基本设置]页面勾选<客户端集成并下载aTrust零信任客户端>选项。



说明：

如果所有用户均通过 aTrust 登录客户端并联动下载 EDR 客户端，也可不开启该选项。

联动效果

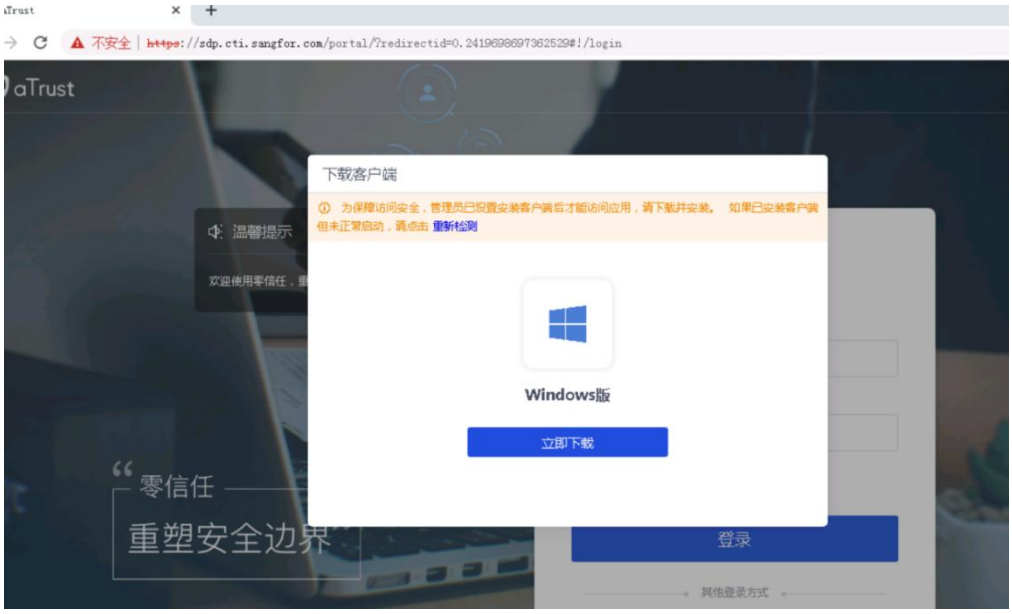
1.客户端AIO

（1）客户端安装

全新安装场景(客户当前无AC准入和EDR)

该场景面向用户新上aTrust和EDR场景。

当用户需要远程访问aturst代理的业务系统，提示用户需要安装aTrust客户端。



下载安装完成后，可在客户端看到aTrust系统托盘。

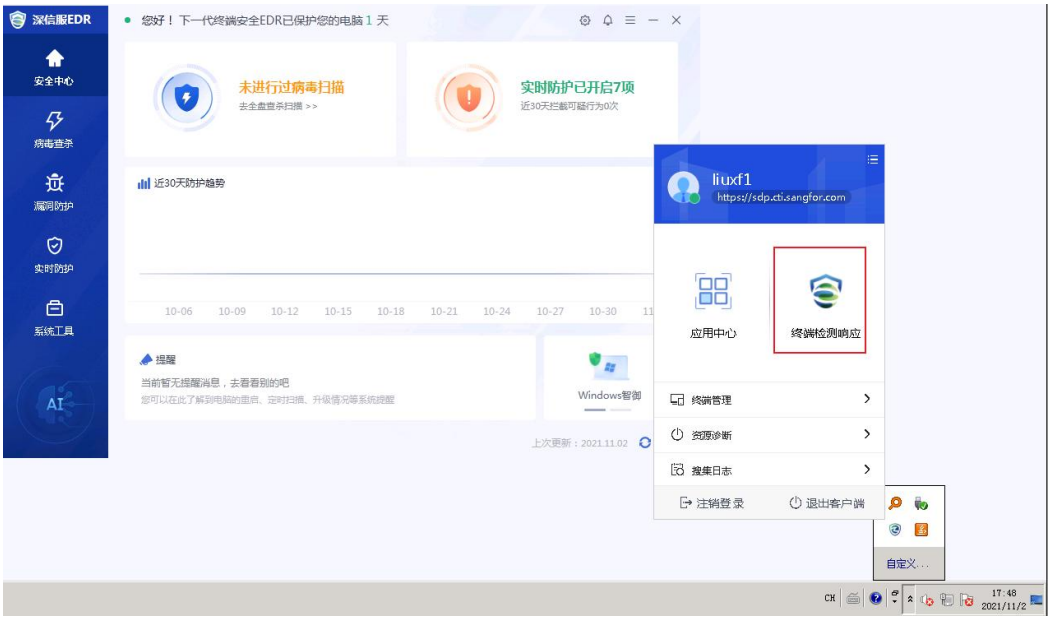
如果是开启的全局策略，aTrust客户端安装完成后，EDR客户端会在后台静默下载安装（由于EDR安装包比较大，内网环境需要等待5-10分钟，公网环境根据实际的带宽

情况可能会比较久）。

说明：

1. 如果没有开启全局策略，只开启了用户策略的话，需要对应用户认证登录成功以后才会联动下载 EDR。
2. 当前版本 EDR 后台安装暂时没有下载和安装进度可以展示。

等待EDR客户端安装完成后，用户可以看到All in one客户端，即aTrust托盘上有“终端检测响应”的图标，认证后可访问业务系统。



说明：

aTrust+EDR 场景下，AIO 系统托盘主界面为 aTrust 客户端。

加装场景(客户当前有aTrust，但是没有EDR)

该场景面向已经部署aTrust客户端，新增部署EDR客户端的用户。

1.用户如果部署的aTrust为非AIO版本，需要先完成aTrust设备升级，并完成EDR设备部署和联动配置，具体各项配置与前述基本一致。

2.客户端登录aTrust后，aTrust会提示升级并在后台静默安装EDR客户端，EDR静默

安装过程需要耐心等待。

3.客户端升级安装全部完成后，客户端系统托盘会融合成一个，具体过程与新装和升级场景基本一致。

加装场景(客户当前有EDR，但是没有aTrust)

该场景面向已经部署EDR客户端，新增部署aTrust客户端的用户。

1.用户如果部署的EDR为非AIO本，需要先完成EDR管理端升级，并完成aTrust设备部署和联动配置，各项配置与前述基本一致。

2.EDR平台升级完成以后，客户端会自动静默升级，升级过程需要耐心等待。

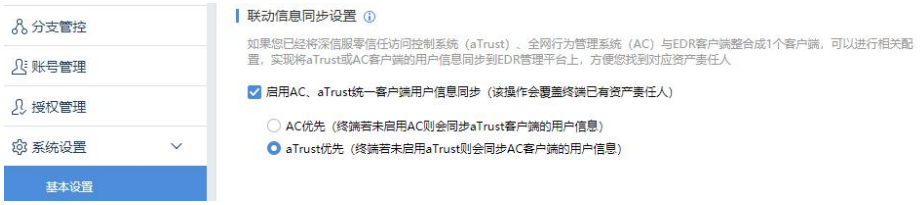
3.EDR管理端如果同步开启了[客户端集成并下载aTrust零信任客户端]选项，客户端更新成功后会自动在后台静默安装aTrust客户端。

4.客户端升级安装全部完成后，客户端系统托盘会融合成一个，具体过程与新装和升级场景基本一致。

（2）用户信息同步功能

EDR平台可配置是否开启信息同步功能，且可配置接受AC/aTrust用户信息的优先级，优先接受AC还是aTrust传来的信息。

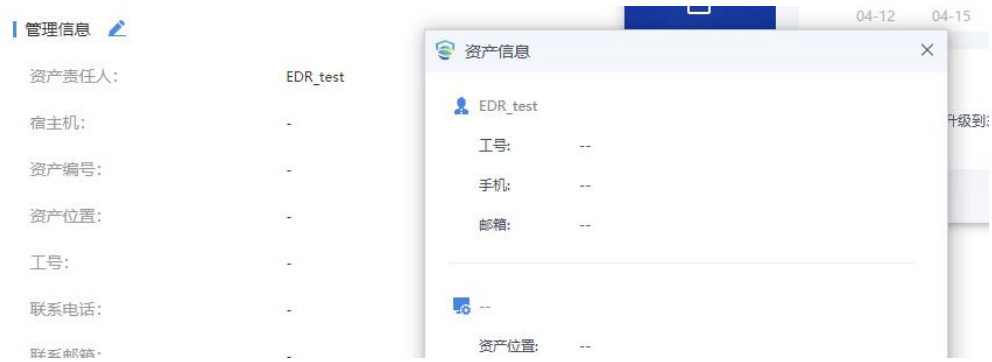
EDR页面配置项：



触发方式：

AIO场景下，在终端管理平台登录aTrust，aTrust会将登陆的用户名发送给EDR，EDR上报到平台。AC登录用户名变化时，EDR会收到新登录用户名消息，并上报给平台。如果aTrust优先级高，且aTrust此时上报了用户名消息，则会用aTrust的用户名信息。

在EDR Agent界面填写后，会上报到平台，查看配置中心会发现信息来源为EDR。



登录aTrust后，aTrust将用户名发送给EDR，EDR终端和平台的用户名显示均为aTrust上报的用户名，且配置中心显示消息来源为aTrust产品线，分组路径作为附加信息也保存在配置中心。

（3）客户端使用

在aTrust未认证前，如果用户需要进入EDR界面进行终端安全相关问题的发现和处置，点击右上角图标进入对应的EDR产品界面。

在aTrust认证后，用户可点击<终端检测响应>图标，进入EDR产品界面。

（4）客户端退出

整体退出

右键点击系统托盘，点击退出客户端选项。

在对话中选择同时退出“EDR终端检测响应”，可以同时退出aTrust和EDR客户端。

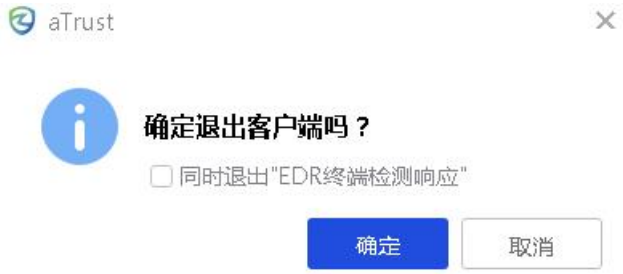
EDR客户端退出需要输入防护密码，需要由管理员提供，输入密码后即可整体退出客户端。

说明：

客户端完整退出后，重新登录 aTrust，此时只会拉起独立的 aTrust 客户端。同理，如果只单独打开 EDR 客户端，也只会开启 EDR 独立客户端。

分开退出

右键点击系统托盘，点击退出客户端选项，在对话中缺省不选择同时退出“EDR终端检测响应”选项，可单独退出aTrust客户端。



退出aTrust客户端后，系统托盘将变更为EDR独立客户端托盘。

如需单独退出EDR，可点击进入EDR托盘图标以后，再点击退出选项，即可单独退出EDR客户端。

（5）客户端卸载

当前版本各产品线卸载相互独立，互不干扰。

说明：

aTrust 与 EDR 终端 AIO 功能当前仅支持 win 7、win10 和 win11 系统，不支持其它操作系统。

2.环境感知

aTrust通过与EDR联动，对终端环境进行检测并给出评分，当终端环境存在风险，不满足aTrust安全要求时，可以禁止用户访问业务，隔离来自终端的风险。

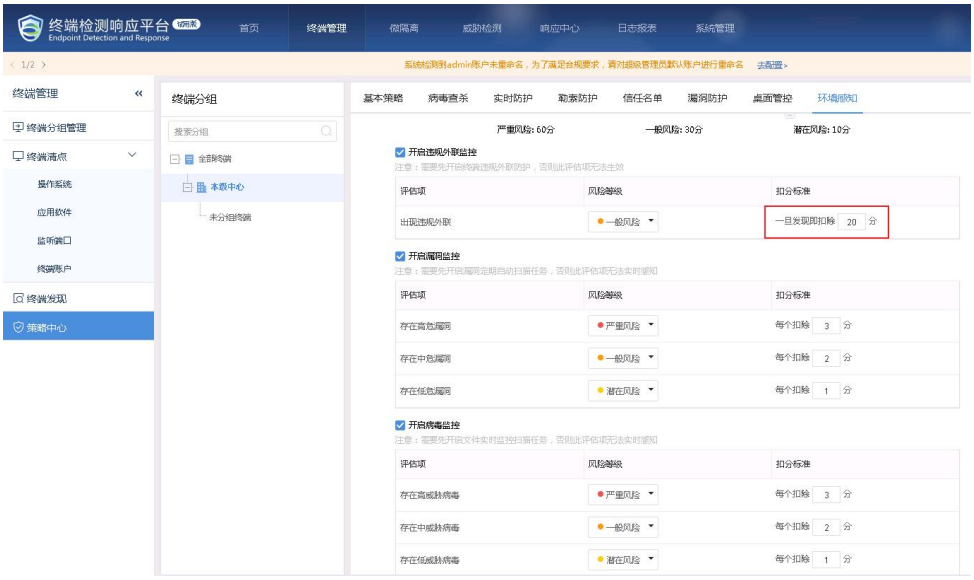
aTrust与EDR联动实现此功能，除了上述基础联动配置，还需要按如下进行配置。

（1）EDR配置

说明：

配置前，我们需要提前跟了解客户的业务场景和安全策略，沟通清楚对各项安全风险的容忍度，以便合理设计扣分值。例如，在电子政务外网中，客户严格要求不允许终端接入业务系统的时候有外接互联网的行为，我们可以将违规外联监控的扣分设置一个相对较高的值，以便发生这种行为 aTrust 能感知并禁止用户接入，保障客户业务安全，以下配置以该需求为例。

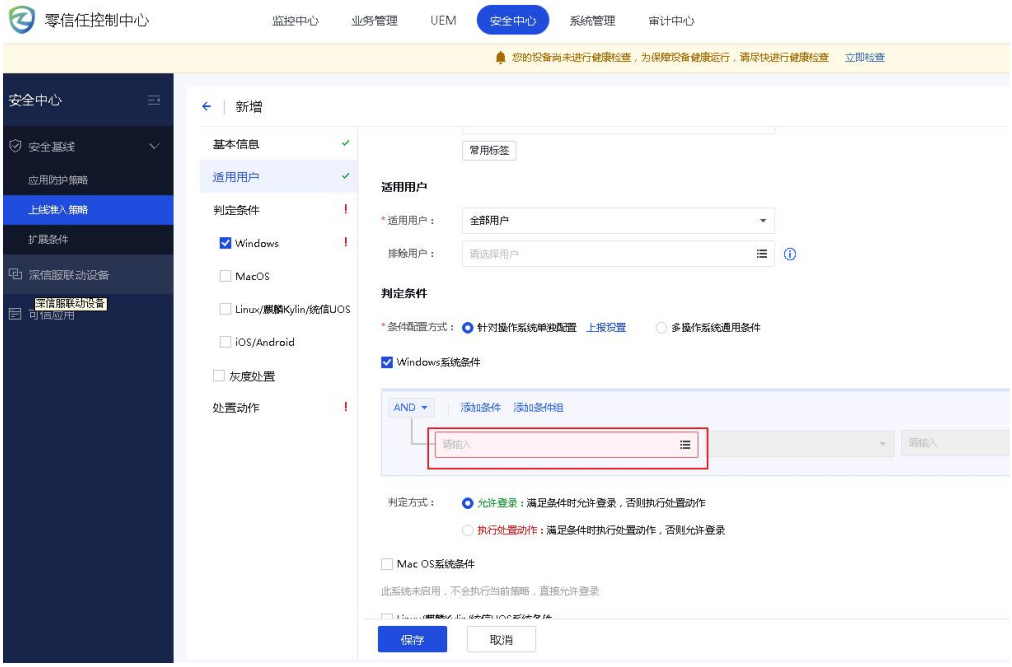
登录EDR管理端，打开[终端管理/策略中心/环境感知]页面，勾选[开启环境感知]选项，勾选需要关注的环境感知项目如违规外联监控、漏洞监控、病毒监控、Windows防火墙监控等，并根据实际的业务场景和客户安全需求设置扣除的分数。



打开[终端管理/策略中心/桌面管控]页面，开启终端违规外联防护策略，并设置探测间隔、探测域名以及发生外联行为以后的处置策略。例如，如果探测终端有连接www.baidu.com的行为，就认为终端有违规外联的行为，由于检测外联行为的目的是联动aTrust，因此发现外联行为设置的策略是不处理，仅提醒。

（2）aTrust配置

登录aTrust管理端，打开[安全中心/安全基线/上线准入策略]页面新增一条策略，设置Windows系统条件。



使用外部变量中的[EDR终端检测评分]。

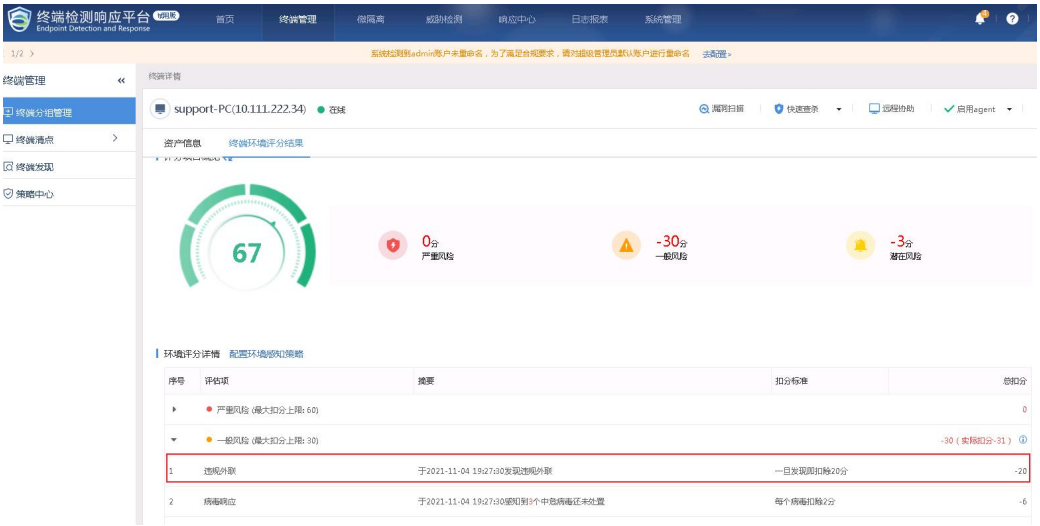
根据实际用户需求选择判断条件，例如此处设置>=90分才允许登录。

（3）环境感知联动效果

当终端环境不满足上线准入策略要求时，用户登录aTrust被准入策略拒绝登录。

如果用户aTrust当前处于在线状态，被检测到不符合准入策略要求，用户会被强制注销下线。

通过EDR管理端查看终端详情，在终端环境评分结果中可以看到当前终端的评分结果以及具体扣分项。



说明：

由于 EDR 各项策略的检查周期不是实时的，例如外联检测缺省时间为 300s，最小可以设置为 60s，同时 aTrust 向 EDR 管理端获取评分的周期是 5 分钟，并且下发策略存在 1 分钟左右的延时，因此配置完策略后，客户端可能需要等待一段时间才会被强制注销下线。

4.6.3. EDR 与 SIP 联动

SIP与EDR联动可实现SIP检测到风险资产，联动EDR对主机进行联动隔离、访问控制、一键查杀、IOC取证。同时，EDR安全日志和资产可上报至SIP平台，由SIP进行集中分析。

联动条件

网络连通性：SIP需与EDR的TCP443端口通信，EDR管理端可与SIP的TCP7443端口通信；

版本要求：SIP需使用3.0.59及以上版本。

联动配置

SIP平台联动配置：

1.配置SIP接入EDR

登录SIP平台，打开[系统设置/设备管理]，点击<新增>，如下图所示。

其中：

接入设备IP：请填写EDR管理端的IP地址；

设备名称：可自定义易识别的设备名称；

设备类型：请选择“终端安全管理系统”

联动通信端口：请填写EDR管理端控制台登录端口。

2.添加EDR应用实例

登录SIP平台，打开[系统设置/联动响应]，点击<深信服终端检测与响应平台>，如下图。

点击<新增>，添加EDR应用实例，如下图。

其中：

请求地址：请填写EDR管理端的IP地址；

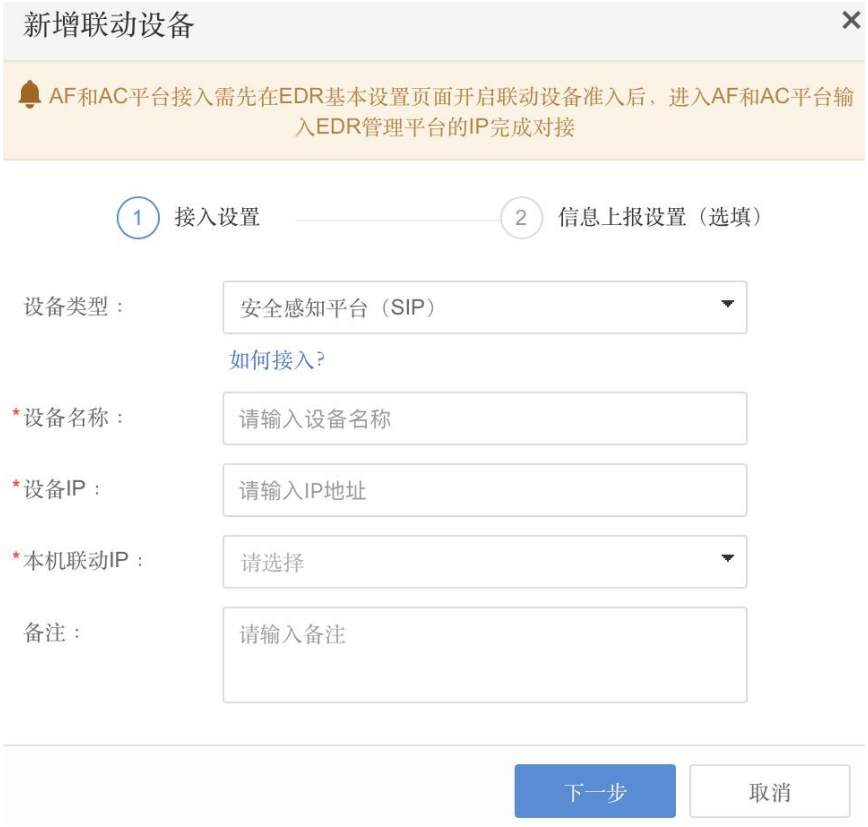
请求端口号：请填写EDR管理端控制台的端口号；

用户名：请填写EDR管理端admin帐号；

密码：请填写EDR管理端admin帐号的密码。

EDR平台联动配置:

登录EDR管理端，打开[系统管理/联动管理]，点击<接入联动设备>，选择[使用设备账户、密码接入]，填写设备类型、名称、IP及本机联动IP等信息，如下图。



其中：

设备类型：请选择[安全感知平台（SIP）]

设备名称：可自定义易识别的设备名称；

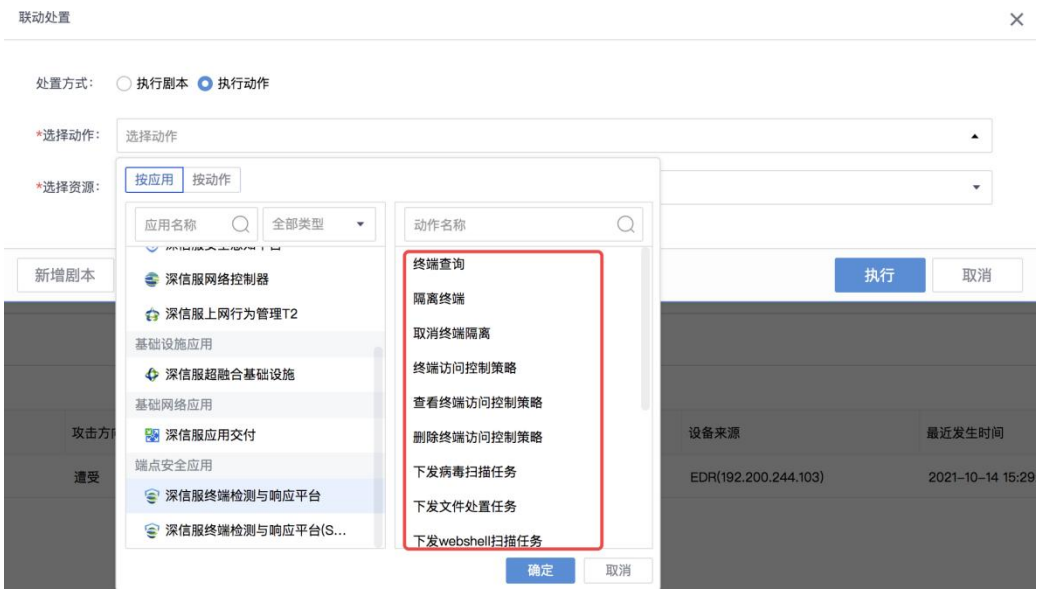
设备IP：请填写SIP平台的IP地址；

本机联动IP：填写EDR管理端可以和SIP通信的IP地址；

点击<下一步>，跳转至[信息上报]页，如下图，启用终端资产信息上报和安全日志上报至SIP平台。

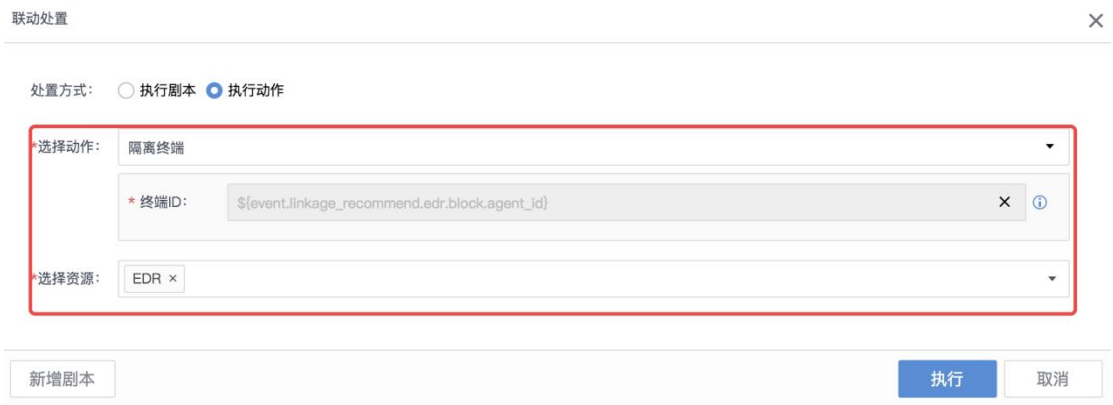
联动效果

当SIP检测到已失陷主机时，可以联动EDR对主机进行联动隔离、访问控制、一键查杀、IOC取证。打开SIP[处置中心/风险资产视角]，打开具体风险资产，点击<联动处置>，可以进行具体联动处置操作，如下图。



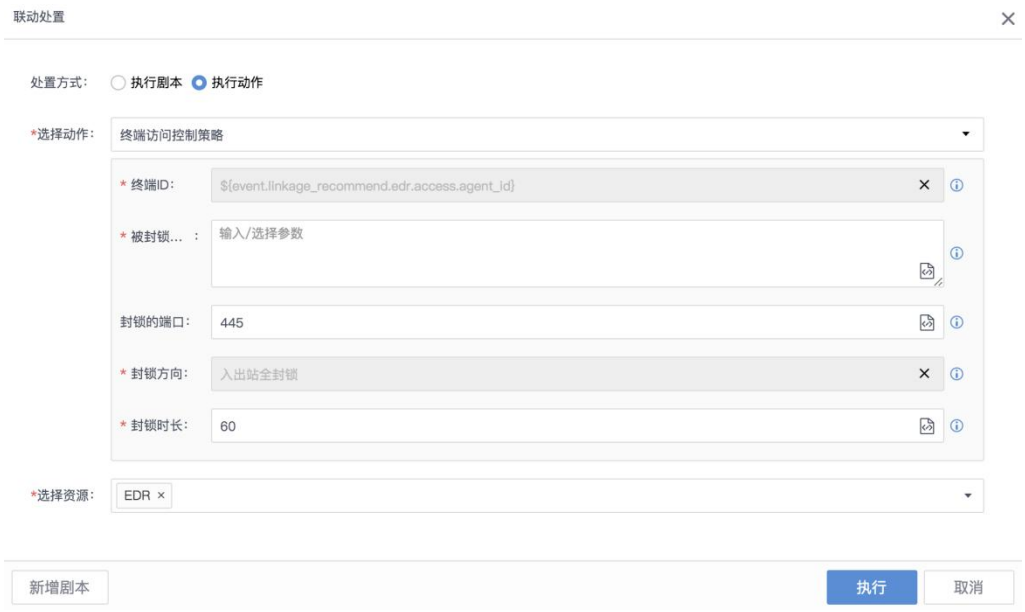
1.联动下发封锁

联动封锁可以在SIP上联动EDR下发对风险资产隔离，如下图配置。



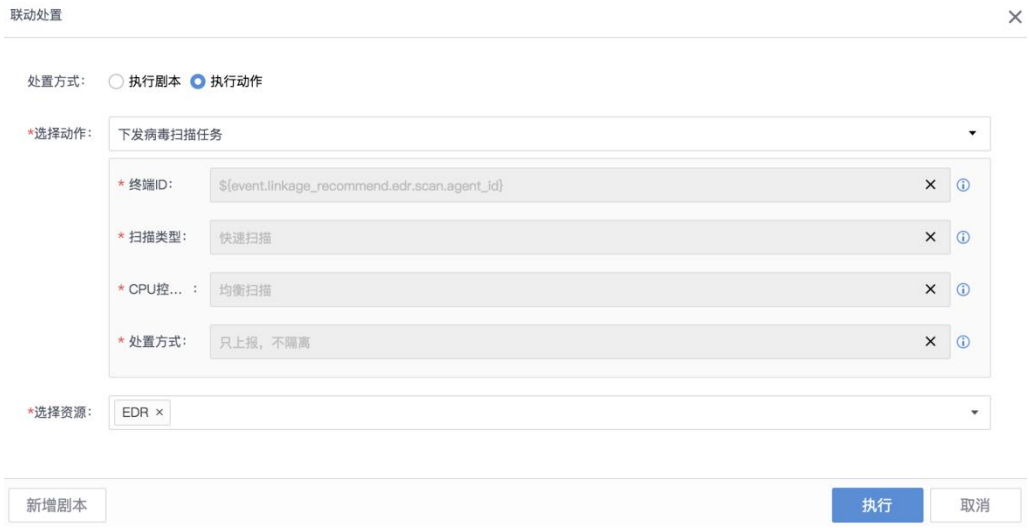
2.联动下发访问控制

访问控制可以在SIP上联动EDR下发对风险主机出站、入站流量进行控制，基于IP、端口进行控制，如下图配置。



3.联动下发病毒查杀

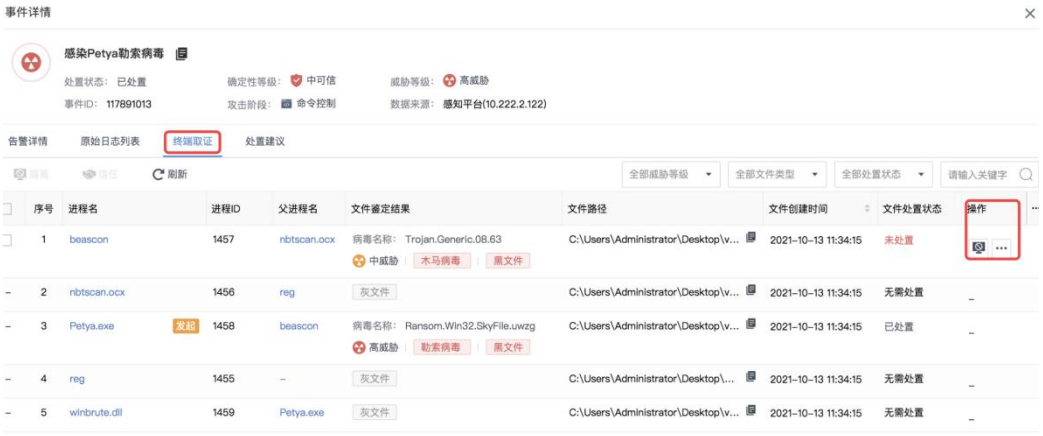
联动下发病毒查杀可以在SIP上联动EDR对风险主机下发病毒查杀操作，可以下发快速查杀或全盘查杀，如下图配置。



当查杀发现威胁文件时，可从SIP联动EDR对威胁文件进行隔离操作，如下图。

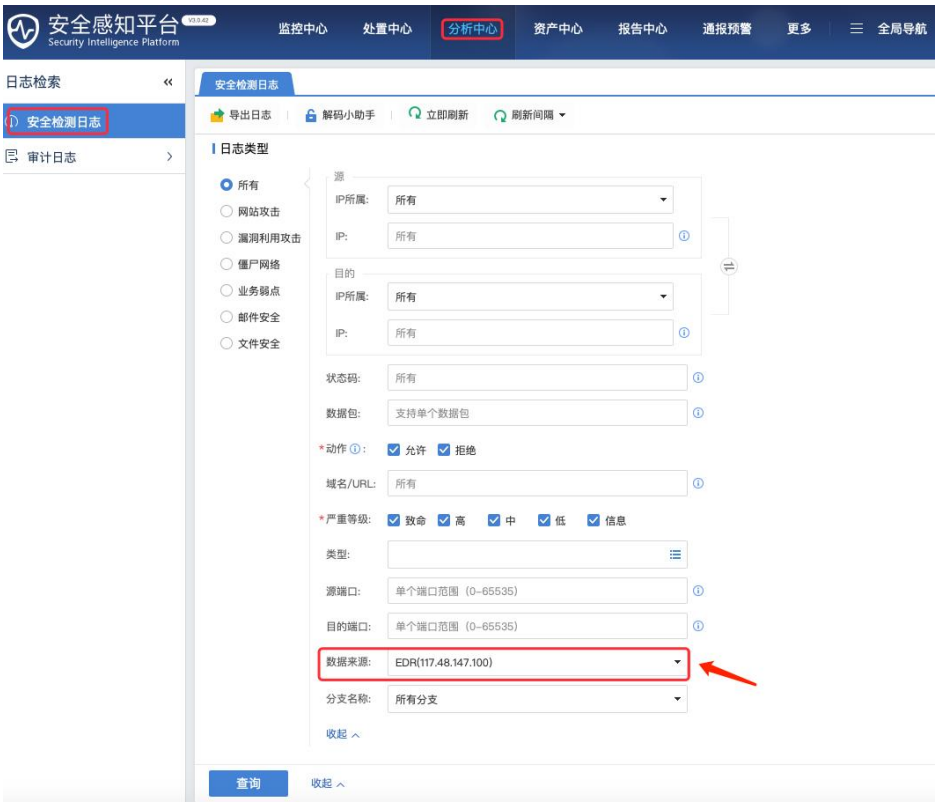
4.IOA取证

当SIP检测到风险主机有恶意外联行为，可以根据外联的恶意域名或五元组信息自动联动EDR进行IOC取证，如下图。



5.安全日志上报

联动成功后，EDR将安全日志上报至SIP平台，实现集中分析与运营。可在SIP平台的[日志中心/日志检索/安全日志检索]页签下，通过选择对应EDR作为数据来源，实现EDR上报的安全日志查询与分析，如下图所示。



6.资产上报

联动成功后，EDR将终端信息上报至SIP，帮助用户进行资产管理。如下图，SIP资产中心中的资产来源为EDR上报。

点击资产主机名，能看到EDR上报的该资产的硬件、软件、开放端口等所有信息，如下图。

4.6.4. EDR 与 AF 联动

AF与EDR联动可实现联动下发病毒查杀及僵尸网络域名访问进程取证。

联动条件

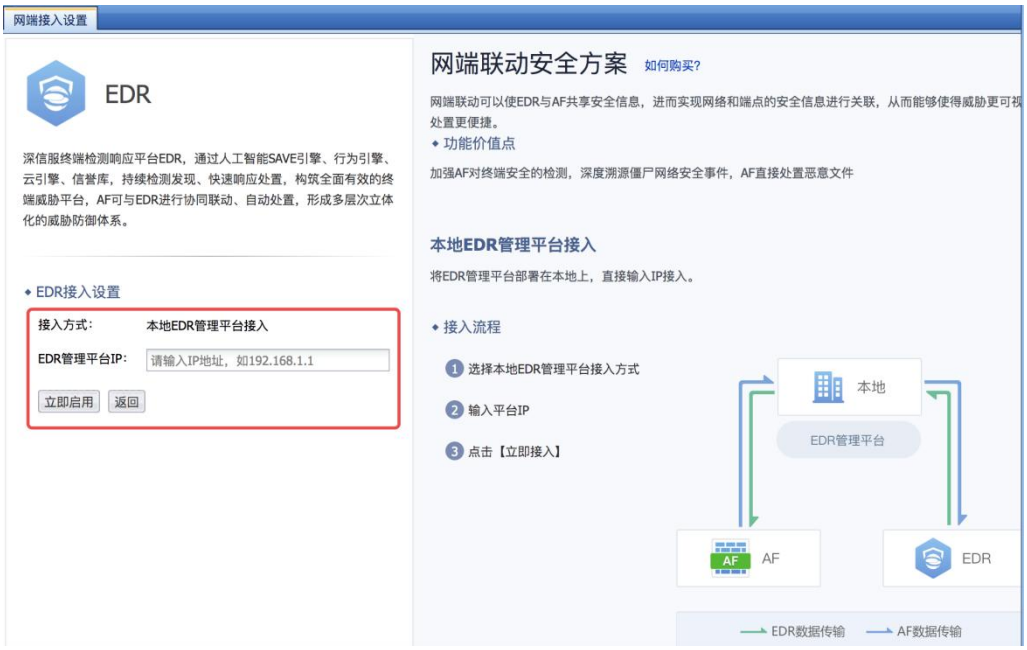
网络连通性：AF与EDR的TCP443端口可以正常通信；

版本要求：AF使用8.0.12及以上版本。

联动配置

1.登录AF平台，在[下一代安全防护体系/网端联动/网端联动接入设置]页签下，输入

EDR管理端IP，编辑完成后点击<立即启用>，配置页面如下图所示。



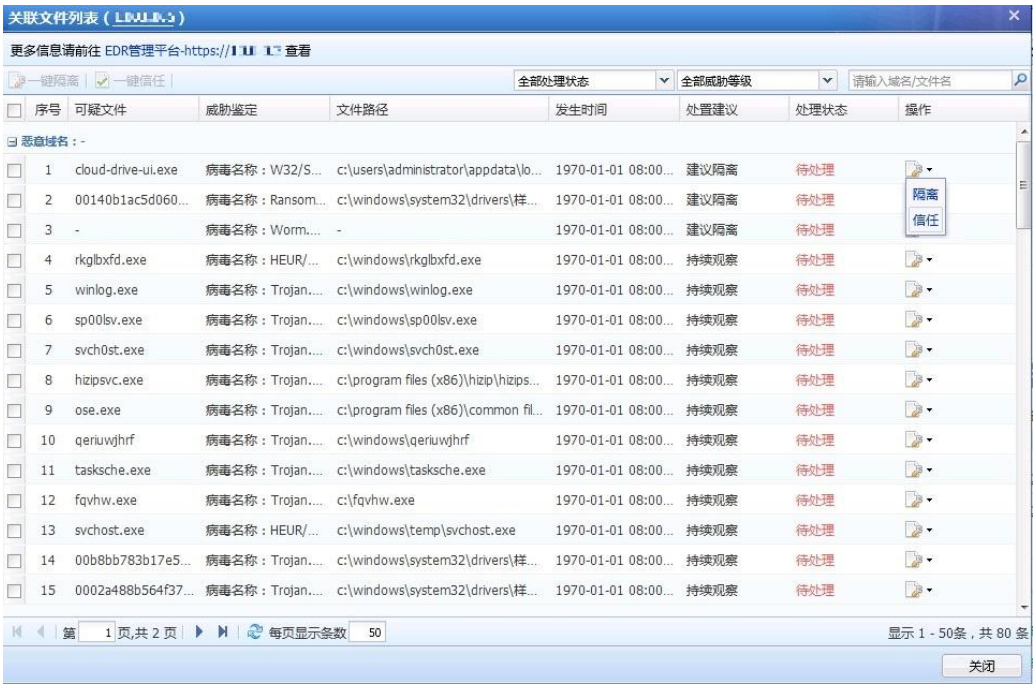
2.联动成功后，在上页面可看到服务状态为在线标识，如下图所示。

联动效果

联动成功后，可实现AF与EDR联动下发病毒查杀及访问僵尸网络进程举证等操作。

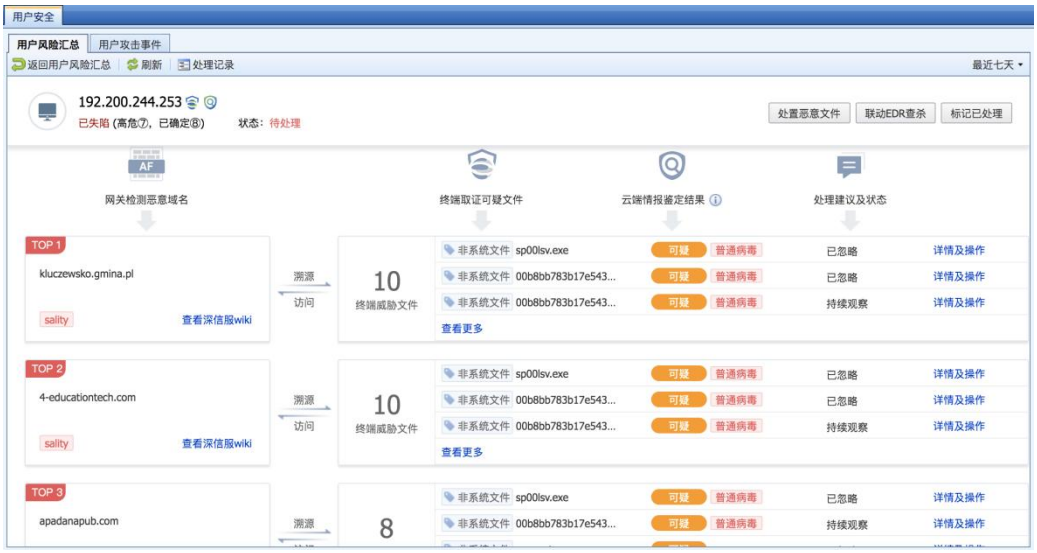
1.联动下发病毒查杀

当AF识别到风险终端时，可联动EDR进行查杀。在AF平台的[运行状态/用户安全]页签下，可实现针对发现的风险终端联动EDR进行病毒查杀、对识别到的威胁文件进行隔离、信任等操作，联动页面如下图所示。



2.联动举证访问僵尸网络进程

EDR能够记录终端访问的域名及访问域名的进程，当AF上发现僵尸网络日志时，可联动EDR进行举证、溯源，帮助用户有效举证终端访问僵尸网络域名的具体进程及进程关联文件。在AF平台的[运行状态/用户安全]页签下，可查看具体风险终端对应的[终端取证可疑文件]，即是AF联动EDR进行僵尸网络举证的结果，如下图所示。



同时可点击<详情及操作>查看EDR举证的恶意域名访问溯源结果，并对威胁文件进行相关处置，如下图所示。

4.6.5. EDR 与合规自检平台联动

合规自检平台是部署SIP、云镜、云图、X-SEC上的等保合规检测工具。合规自检平台与EDR联动可实现对终端联动下发等保基线检查，并对检查结果进行分析，给出整改建议。

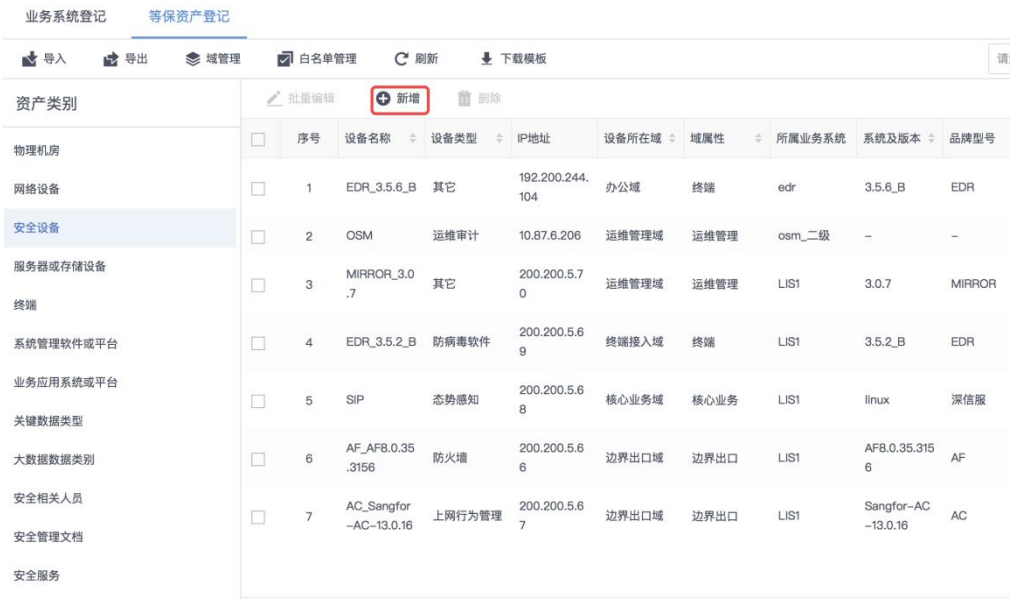
联动条件

网络连通性：EDR与合规自检平台的TCP443端口可以正常通信。

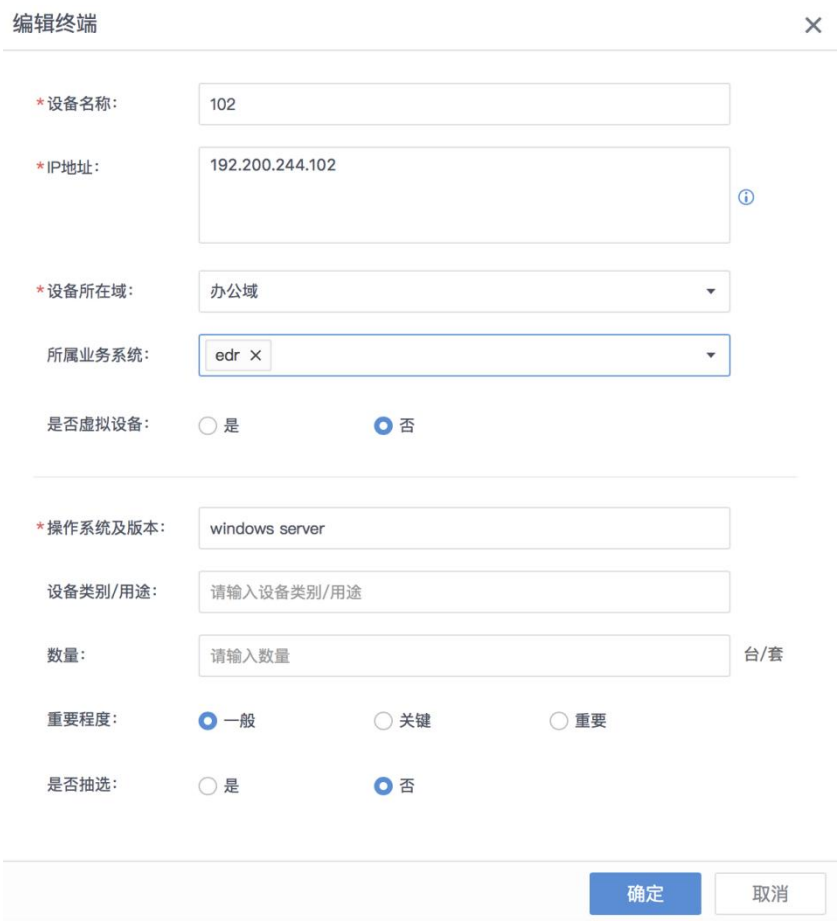
联动配置

1.合规自检平台登记资产

登录合规自检平台，打开[等保资产中心/等保资产登记]，点击<安全设备>，登记EDR管理端，如下图。



点击<终端>，登记需要评估的终端，如下图。



2.配置EDR与合规自检平台联动

登录EDR管理端，打开[系统管理/联动管理]，点击<接入联动设备>，选择[使用设备账户、密码接入]，填写设备类型、名称、IP及本机联动IP等信息，如下图。

设备类型：选择 合规自检平台

接入方式：选择 IP/端口

设备IP：配置合规自检平台访问地址

设备端口：配置合规自检平台控制台访问端口，默认配置443

本机联动IP：选择 与合规自检平台通信的IP地址。

联动成功，如下图所示。

联动效果

从合规自检平台下发检测。登录合规自检平台，打开[等保监测中心]，点击<新建检测>，如下图。

点击<开始检测>，下发检测中，如下图

等待检测完成，返回检测结果如下图。

4.6.6. EDR 与 MSS 联动

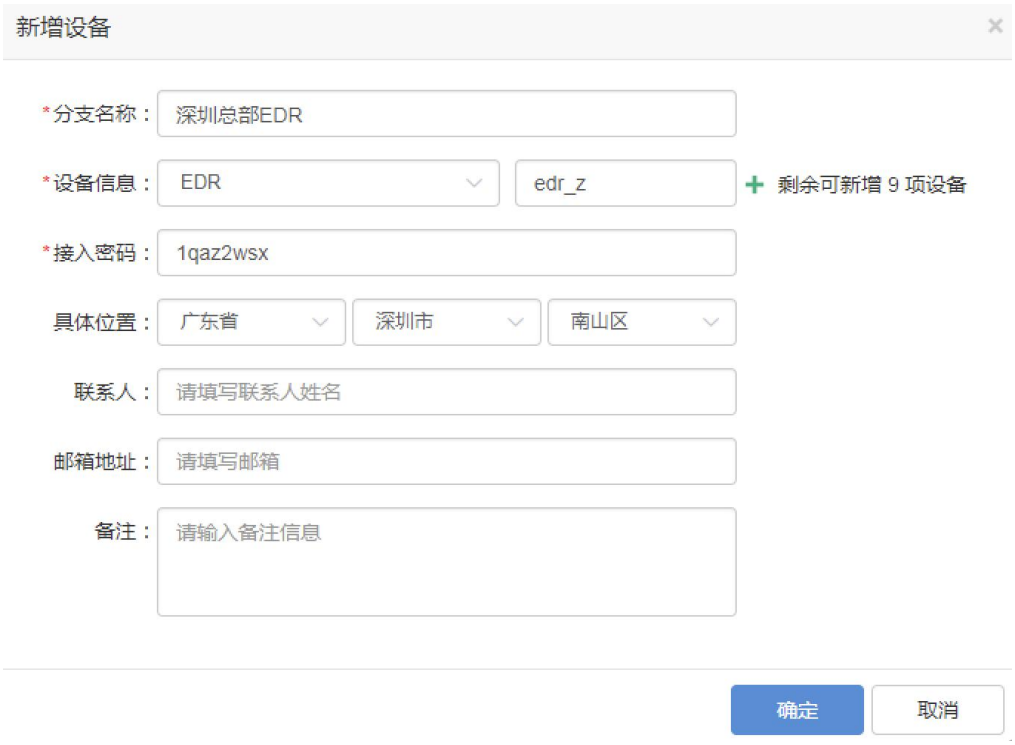
安全运营服务（MSS）是深信服公司提供的一套基于安全运营服务平台（MSS）和安全服务平台（SSP）两大平台，为客户提供的一套系统化、标准化、持续化的安全风险管理和安全运营管理方案。EDR与MSS联动，能够将EDR安全日志上报至MSS平台集中分析，并支持从MSS对终端下发病毒查杀、webshell查杀、下发命令等操作，方便通过MSS对终端运维。EDR与MSS联动配置如下：

MSS平台配置

EDR接入MSS需要提前获取MSS企业ID、接入MSS帐号和密码。

打开MSS客户管理页面，新增或者选择现有客户的设备管理『进入设备管理页面』，点击<新增>按钮，如下图。

在下图弹窗页面填写必填项“设备信息”和“接入密码”，即可完成MSS平台的联动信息输入。创建的账号和密码即为EDR平台接入MSS的认证账号和密码。



完成上述步骤后，返回客户管理页面，获取上述新增EDR设备的客户ID信息（用于在EDR平台对接MSS时填写企业ID）

EDR平台配置

登录EDR管理端，打开[系统管理/联动管理]，点击<接入联动设备>，选择[使用设备账户、密码接入]，填写企业ID、接入帐号和密码，如下图。点击<下一步>启用日志上报，即完成EDR接入MSS配置。

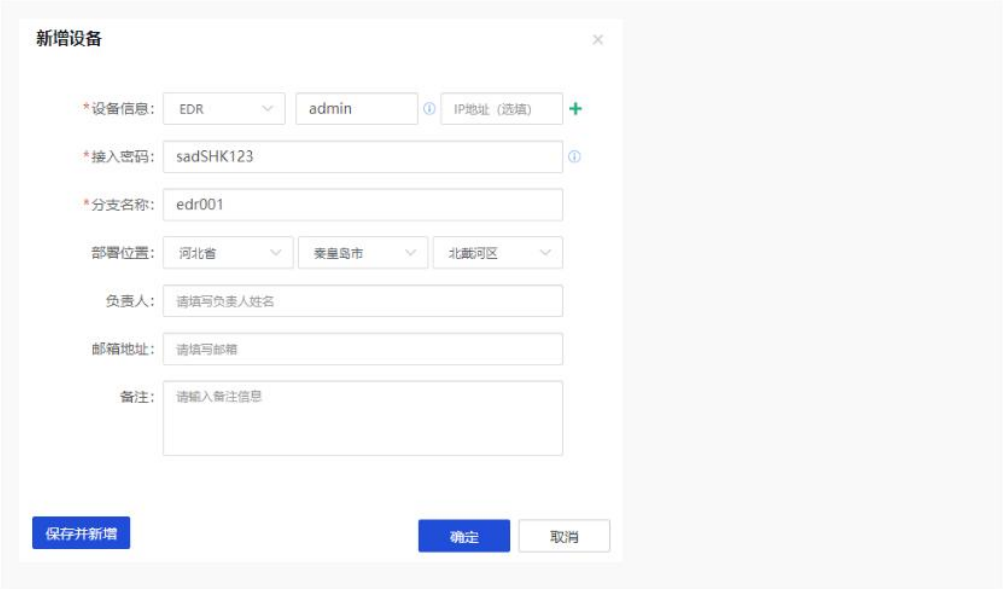
4.6.7. EDR 与 XDR 联动

安全检测与响应管理（XDR）是深信服公司提供的一套基于安全检测与响应管理的平台，为客户提供的一套系统化、标准化、持续化的安全风险管理和安全运营管理方案。EDR与XDR联动，支持从XDR对终端下发联动主机隔离、联动威胁处置、联动脚本下发等操作，方便通过XDR对终端运维。EDR与XDR联动配置如下。

XDR平台配置

在XDR的设备管理页面，点击新增按钮

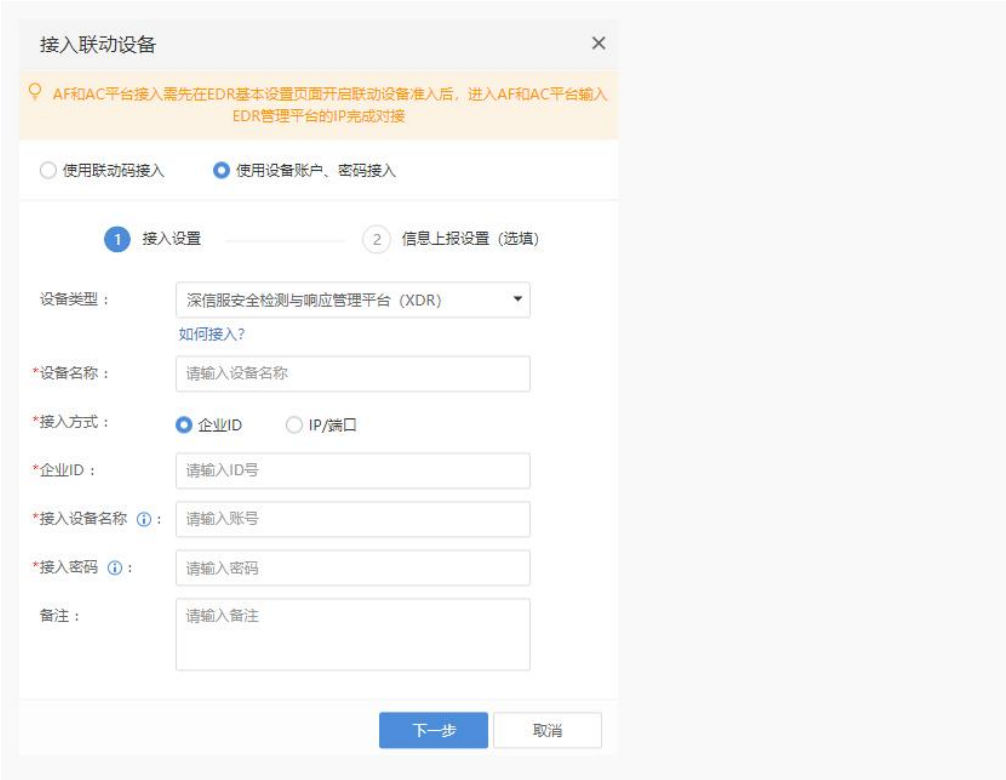
在新增弹窗填写必填项“设备信息”和“接入密码”即可完成XDR平台的联动信息输入，此步骤创建的账号和密码即为EDR平台填写需要输入的认证账号和密码。



EDR平台配置

在EDR的“系统管理>联动管理”页面，点击“接入联动设备”按钮

在EDR的“系统管理>联动管理”页面，点击“接入联动设备”按钮

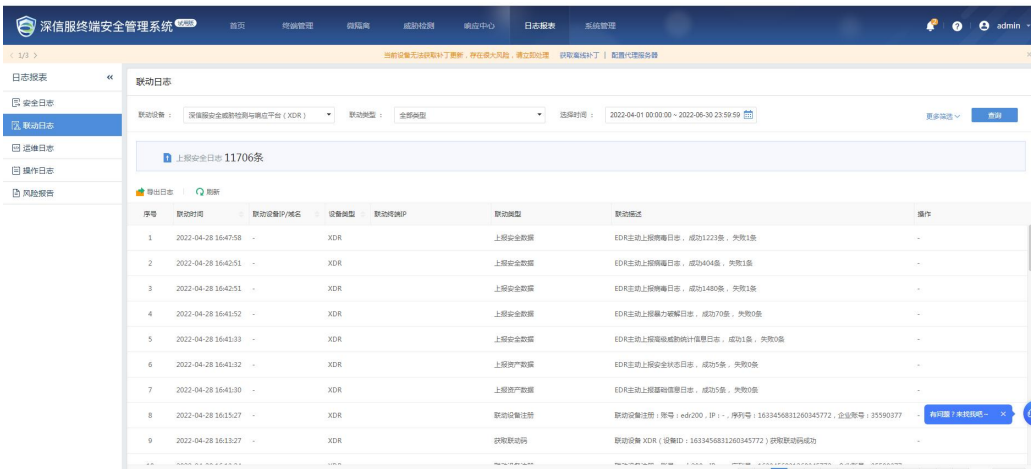


完成上述步骤后，获取上述新增EDR设备设备信息”和“接入密码”的客户ID信息（用于在EDR平台对接XDR时填写企业ID）

序号	客户ID	客户名称	服务渠道	负责人	手机号	客户类型
1	54165351	EDR-兼容性测试	测试渠道	林诗超	18588211815	测试客户
2	68312322	测试123	湖南	陈旭	18254145144	正式客户
3	91312314	MSS邮件测试	湖南	王MSS	18920114414	正式客户
4	38396423	客户公司1	湖南	刘客户	18520843536	正式客户
5	18515957	B类客户	湖南	陈旭	18520846541	正式客户

联动效果

EDR将安全日志、行为日志上报至XDR进行展示分析。



说明：

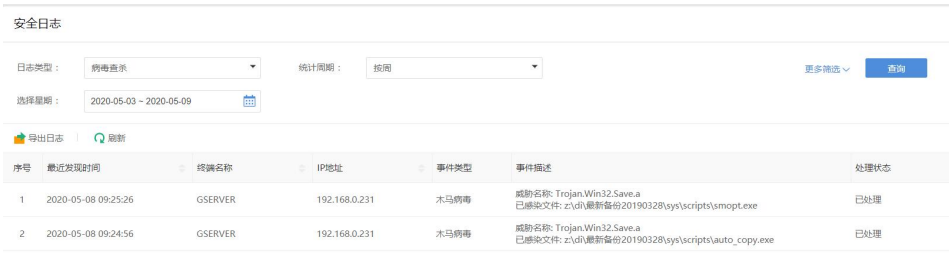
企业 ID 需要在 XDR 平台获取；认证账号和密码需与 XDR 创建的设备账号和密码保持一致； 确保 EDR 管控平台网络要能联通 XDR 平台

4.7. 日志报表

在[日志报表]页签下，EDR可提供安全日志、联动日志、运维日志及操作日志查看，并可针对风险进行手动报告导出和报表订阅配置。

4.7.1. 安全日志

安全日志主要展示EDR记录的安全相关信息，包括病毒查杀、漏洞扫描、基线检查、入侵检测、微隔离、安全加固及外设管控等类型，日志页面如下图所示。



可通过日志类型、统计周期及指定星期进行初步筛选，同时点击<更多筛选>可进一步依据终端名称、IP地址进一步查询，检索结果支持导出日志操作。

4.7.2. 联动日志

联动日志主要展示EDR与其他产品联动相关信息，包括总体联动情况概览、联动时间、联动设备/终端IP、设备类型、联动类型及联动描述等信息，可联动设备包括AF、SIP、AC、X-Central及MSS，日志界面如下图所示。

可通过日志类型、统计周期及指定星期进行初步筛选，同时点击<更多筛选>可进一步依据终端名称、IP地址及联动类型进一步查询，检索结果支持导出日志操作。

4.7.3. 运维日志

运维日志主要展示远程运维相关操作记录，包括操作时间、终端名称、IP地址、操作系统、类型及执行状态等，日志页面如下图所示。

可通过脚本文件名称、统计周期及指定星期进行初步筛选，同时点击<更多筛选>可进一步依据终端名称、IP地址及执行状态进一步查询，检索结果支持导出日志操作。

4.7.4. 操作日志

操作日志主要展示管理员针对EDR管理端的操作记录，包括操作时间、操作用户、操

作IP地址、操作类型、操作对象、操作描述及操作结果等，日志页面如下图所示。

可通过统计周期及指定星期进行初步筛选，同时点击<更多筛选>可进一步依据操作用户、操作IP地址及执行状态进一步查询，检索结果支持导出日志操作。

4.7.5. 风险报告

报告导出

EDR支持对全网终端风险报告进行导出，报告可整体分析全网安全状况，便于管理员快速了解业务和网络的安全风险，在导出时可对报告名称、报告时间范围进行自定义，如下图所示。

报告订阅

可针对报告进行自动订阅，在[报表订阅]页签下，可对报告名称、报告类型、发送时间及收件人进行配置，配置界面如下图所示。

其中：

- **报告类型**：包括日报、周报及月报，分别按自然日（00:00-24:00）、自然周（每周一到周日）、自然月（每月 1 日到月底）生成的报表内容；
- **发送时间**：指在该时间发送上个自然日、上个自然周或上个自然月的报表到收件人邮箱。

4.8. 系统管理

在**[系统管理]**页签下，可进行终端部署、升级管理、联动管理、分支管控、账号管理、授权管理及系统的相关配置。

📖 **说明：**

终端部署请查看章节“安装部署”，升级管理请查看章节“产品升级”。

4.8.1. 账号管理

4.8.1.1. 管理员权限分离

根据需求，可以新建不同权限的管理员角色，登录EDR控制台，在[系统管理/账号管理]页面，点击<新增>创建管理员账号，如下图。

在角色选项可以根据需求分配不同的角色。

系统管理员：只能在平台首页查看、在系统管理页面操作。

安全管理员：不能对平台微隔离模块、联动管理、报表订阅、账号管理、升级、授权、分支管控、系统设置模块进行操作，其他权限不限。

审计管理员：只能查看平台上的内容，不能在平台上进行修改、增加、删除操作。

不同管理员的操作权限不同，从而实现管理端账号的三权分立。

4.8.1.2. 密码安全策略

登录管理端的安全策略可以根据用户安装需求进行设置，登录EDR控制台，在[系统管理/账号管理]页面，点击<设置>，打开[密码安全策略]，如下图。

密码安全策略共有4种配置：

密码使用天数设置：可以开启密码有效期功能(默认关闭)，超期(默认 90 天，取证范围：[1-365])后登陆时强制用户修改，不修改退出当前登陆。

图像验证码设置：可以开启图形验证码功能（默认开启），连续输入错误超过 n 次(默认 0 次，取证范围：[0-5])时，才显示验证码。

登录锁定设置：登陆连续失败 n 次(默认 5 次，取值范围：[0-4])锁定 m 分钟(默认 1 分钟，取值范围：[1-30])。

登录退出设置：登陆超过 n 分钟(默认 10 分钟，取值范围：[1-120])未操作退出当前登陆。

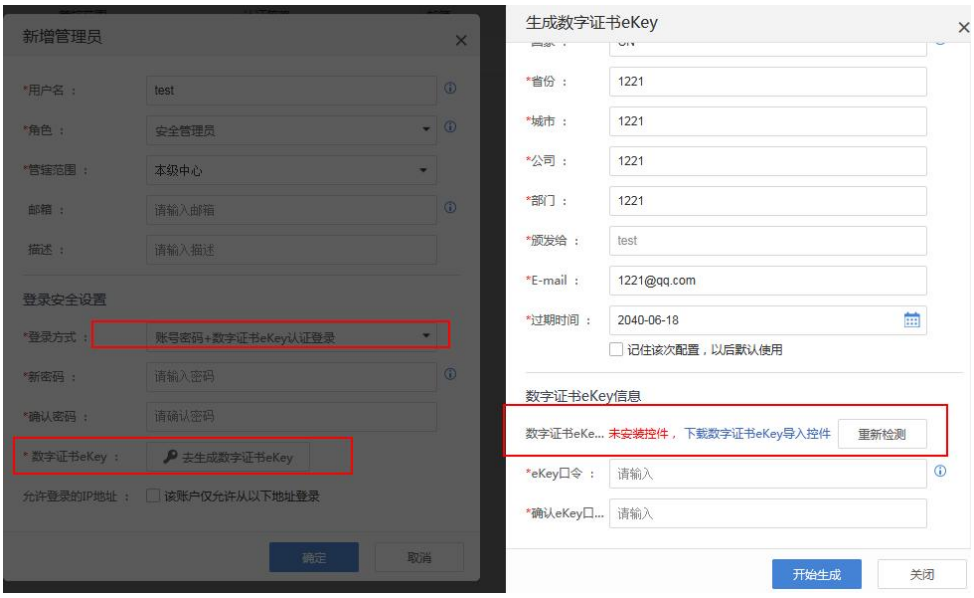
4.8.1.3. 管理端账号登录认证

登录管理端提供了两种认证方式，账号密码认证登录和账号密码+USB-KEY认证登录。在[系统管理/账号管理]页面下，点击<新增>创建管理员账号，如下图。

其中账号密码+USB-KEY认证登录是需要先进行KEY认证通过后再进行的账号密码认证，USB-KEY认证的操作步骤如下：

1.生成管理端的根证书。在[系统管理/账号管理]页面下，点击<设置>，打开证书管理页面输入根证书信息后，点击<确定>即可生成，如下图。

2.生成USB-KEY数字证书。以管理员身份打开IE11及以上浏览器登录管理端，新增管理员账号，生成USB-KEY证书。在生成USB-KEY页面输入证书的信息，同时插入USB-KEY并按照页面提示安装控件，输入证书认证时需要输入的校验ekey口令，点击<开始生成>生成USB-KEY证书，如下图。



📖 **说明：**

生成 USB-KEY 只能使用 IE11 及以上浏览器，同时需要以管理员身份运行 IE 浏览器。

3.登录控制台。生成USB-KEY证书后，插到电脑USB接口，打开浏览器登录EDR管理端，输入对应的账号密码验证码后点击登录，此时浏览器就会弹出需要输入ekey口令的提示框，如下图，输入KEY口令验证成功后即可登录控制台。

📖 说明：

证书认证不支持火狐、Edge、safari 浏览器。

4.8.1.4. IP 地址限制登录

管理端的账号支持只允许在授权的电脑登录，打开新增管理员账号页面，启用[允许登录的IP地址]，设置允许登录EDR管理端的电脑IP地址，如下图。

4.8.2. 授权管理

EDR授权区分PC终端授权和服务器授权，其中PC终端授权可选基础版或高级版、服务器授权为主机旗舰版，不同类型授权具备的功能模块和安全防护能力不一样，如下图。

功能模块		PC终端		服务器
		基础版	高级版	主机旗舰版
周密预防	系统漏洞扫描	✓	✓	✓
	补丁修复管理	✓	✓	✓
	终端基线检查	✓	✓	✓
	资产盘点	✓	✓	✓
	资产主动发现	✓	✓	✓
	微隔离		✓	✓
	轻补丁漏洞免疫		✓	✓
全面防护	文件实时监控	✓	✓	✓
	勒索诱饵防护	✓	✓	✓
	勒索病毒立体防护	✓	✓	✓
	勒索攻击对抗	✓	✓	✓
	无文件攻击防护		✓	✓
	停更系统智诊	✓	✓	✓
	远程桌面登录认证（强力防勒索）			✓
	可信进程防护（强力防勒索）			✓
	关键目录防篡改（强力防勒索）			✓
灵敏检测	恶意文件检测	✓	✓	✓
	僵尸网络检测	✓	✓	✓
	暴力破解检测	✓	✓	✓
	网黑联动杀毒		✓	✓
	WebShell检测			✓
快速响应	文件急速隔离	✓	✓	✓
	终端一键隔离	✓	✓	✓
	感染文件修复	✓	✓	✓
	病毒处置响应	✓	✓	✓
	网黑深度联动（XDR）		✓	✓
	全网威胁定位		✓	✓
简便运维	外设管控	✓	✓	✓
	违规外联检测	✓	✓	✓
	远程协助	✓	✓	
	广告弹窗拦截	✓	✓	

授权采用积分计算方式，每个点使用1天消耗1个积分，如下图：

举例说明如下：

客户购买200点PC授权、总时长1年，已安装使用100点、已用时长6个月；同时购买50点服务器授权、总时长1年，已安装使用30点、已用时长6个月。则积分计算如下：

PC授权总积分：200*365=73000积分

服务器授权总积分：50*365=18250积分

PC已用授权积分：100*180=18000积分

服务器已用授权积分：30*180=5400积分

PC剩余可用授权积分：

73000-18000=55000积分，PC可用1到200点、对应可用275到55000天。

服务器剩余可用授权积分：

18250-5400=12850积分，服务器可用1到50点、对应可用257到12850天。

全新部署场景

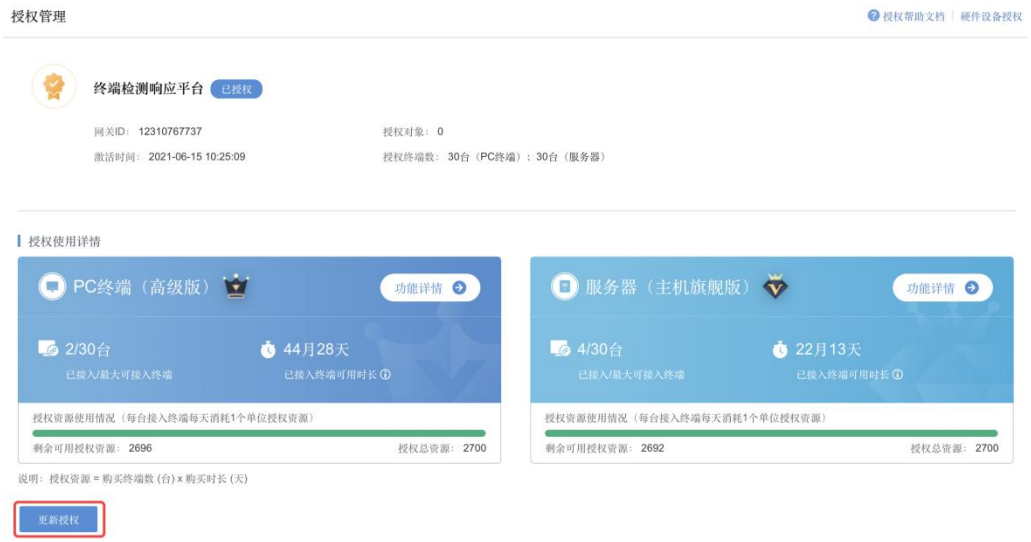
产品销售授权通过深信服授权中心进行激活，产品试用授权通过测试授权申请系统或深信服助手app激活，销售授权和试用授权激活方法参考此手册[安装部署/产品激活]章节。

老版本升级场景

此版本授权采用积分计算，相比之前版本计算方式不同，之前版本升级至此版本，授权会平滑转换。

加点续费场景

授权过期续费或加点场景，会生成新的授权ID或新的授权文件，打开[系统管理/授权管理]，点击<更新授权>，输入新的授权ID在线激活或导入授权文件离线激活即可，如下图。

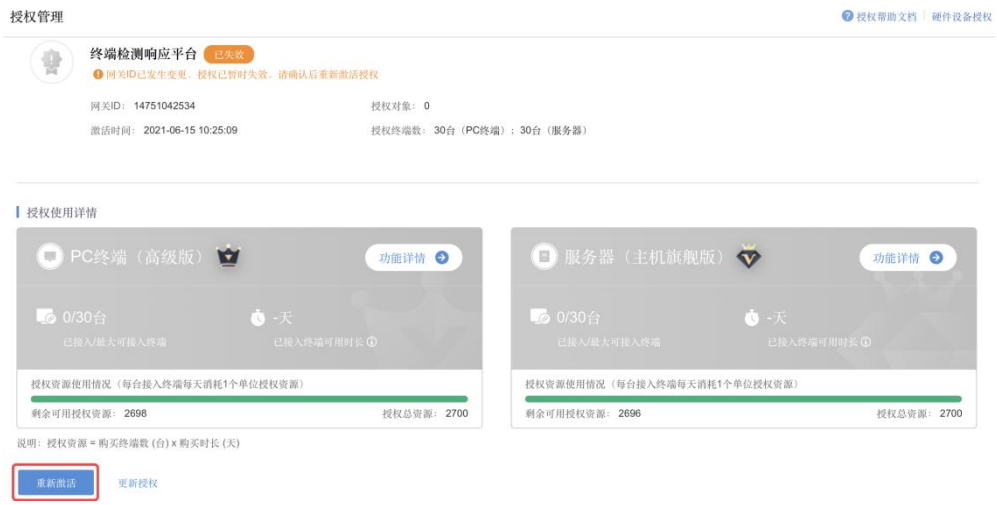


重新授权场景

授权允许激活两次，即首次激活和授权失效后激活。授权信息和管理端硬件有关，如果硬件信息发生变化，则原有授权失效。重新授权有以下两种情况。

1.原有管理端硬件信息发生变化，需要重新授权

打开[系统管理/授权管理]，点击<重新激活>即可，如下图。



2.原有管理端故障，迁移到新的服务器安装，需要重新授权

打开[系统管理/授权管理]，在输入框中输入产品授权ID，重新激活授权即可，如下图。

4.8.3. 系统设置

系统设置主要涵盖基本设置、数据备份、网络设置、日志设置、升级设置、告警设置及系统工具模块。

4.8.3.1. 基本设置

在[基本设置]页签下，可对管理端日期/时间、终端连接策略、终端数据采集间隔、管理端补丁包下载、联动设备准入设置、域名采集、邮箱服务器及云安全计划进行相关配置，配置页面如下图所示。

其中：

1.日期与时间：用于设置EDR管理端的时间。点击<获取本地时间>，则EDR管理端时间和当前登录控制台的电脑时间同步；点击<获取系统时间>，则获取EDR管理端服务器主板时间；EDR管理端能够联网的场景下，也可以启用[自动与NTP服务器同步]，则管理端的时间和NTP服务器保持在线同步。

2.终端连接策略：用于设置自动删除管理端上长期不在线的终端信息，自动释放闲置授权。

3.远程协助端口设置：设置固定端口，EDR远程协助功能可以通过设置的固定端口远程被控制电脑。

4.终端数据采集设置：用于设置终端清点功能采集终端数据时间间隔，设置范围为4小时到168小时。

5.管理端补丁包下载设置：终端无法上网的环境，无法下载漏洞补丁，此时可以通过管理端代理下载漏洞补丁，终端从管理端下载漏洞补丁修复漏洞。

6.联动设备准入设置：用于设置和EDR联动的设备允许联动接入的时间范围。为了联

动接入安全，只有在管理端上勾选该复选框，且在有效时间内才允许AC、AF、SIP等设备主动接入。

7.域名采集设置：开启后，EDR能够记录恶意域名访问的进程，此功能和联动实现僵尸网络恶意域名举证、全网威胁域名定位配合使用。

8.SSL/TLS协议设置：协议算法包括TLS1.0\TLS1.1\TLS1.2，默认开启TLS1.2（安全性更高）若需要和其他设备进行联动，需要同时勾选TLS1.0/TLS1.1。

9.联动部署设置：用于AC、aTrust与EDR联动场景，先安装了EDR客户端，再自动安装AC准入客户端或aTrust客户端场景，详情参考[系统管理/联动管理/EDR与AC联动或EDR与aTrust联动]。

10.邮箱服务器设置：用于配置发送订阅邮件和告警邮件的邮件服务器信息。点击<发送测试邮件>验证邮箱服务器配置是否成功，如果配置成功，则会收到测试邮件，如下图所示。

10.云安全计划：加入云安全计划，EDR将自动把可疑文件上传到云安全中心进行分析，以便提供更有力，更全面的安全服务，需要EDR中心端能连接到https://clt.sangfor.com.cn。

4.8.3.2. 数据备份

数据备份包括外部Syslog备份和策略配置备份与恢复两部分。

外部Syslog备份

适用将EDR管理端的日志通过SYSLOG协议上传至SYSLOG服务器，在SYSLOG服务器进行安全日志统一分析，如下图所示。

[通信协议]选择Syslog服务器支持的通信协议，大多数Syslog服务器支持UDP协议。

IP地址和端口输入Syslog服务器的IP地址和端口。

[通信协议]选择需要备份至Syslog服务器的日志类型。

策略配置备份与恢复

策略备份分为策略中心的配置和微隔离策略配置两部分，选择需要备份的配置，点击<导出配置文件>的按钮，可以导出当前的备份数据。

恢复配置有两种方式，可以从自动备份中恢复，也支持从本地文件恢复。

- 选择自动备份文件，点击<恢复>按钮，等待恢复完成即可；
- 点击<打开本地文件>按钮，选择对应的本地备份文件，等待恢复完成。

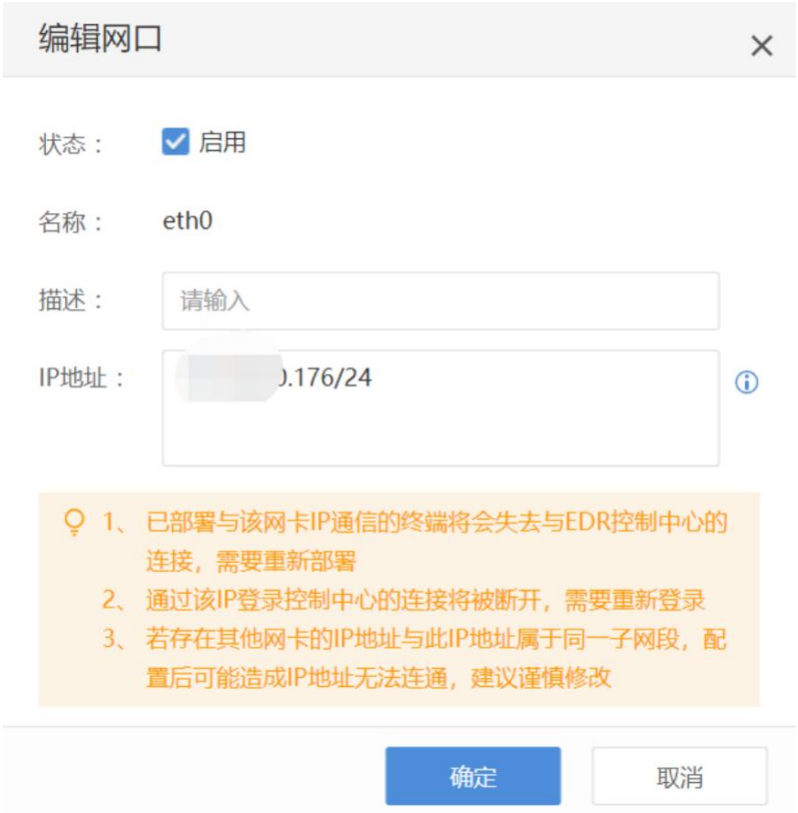
4.8.3.3. 网络设置

网络设置里面包含了网口设置、路由设置、DNS设置、SSH设置及管控平台端口设置。

1.网口设置

网口设置配置管理端与内网终端可以通信的IP地址，此地址即用于管理端和终端通信，同时用于接入管理端。在[系统管理/系统设置/网络设置/网口设置]页面下，如下图所示。

点击网口名称配置该网口的地址，如下图。

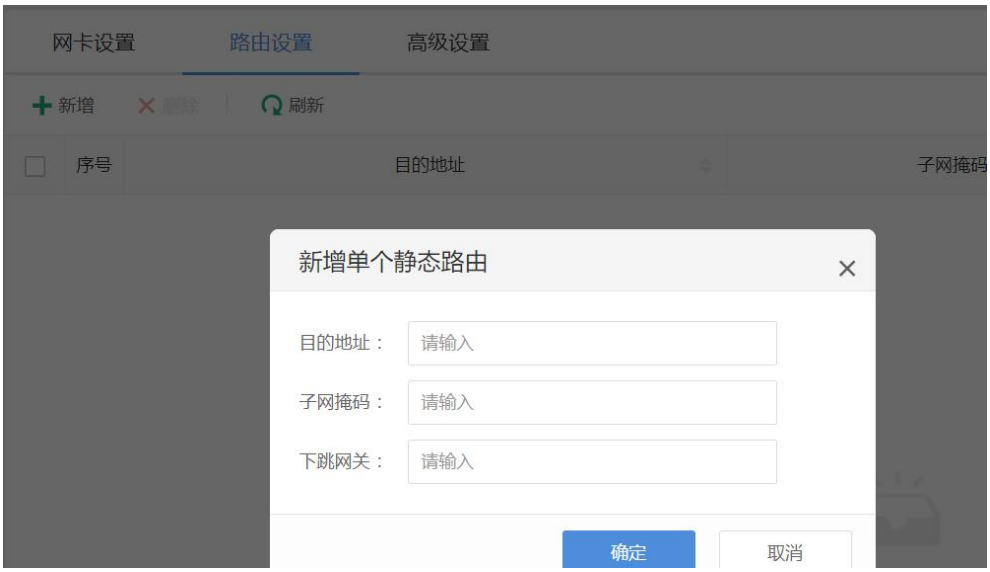


警告：

IP 修改后，已部署的终端将会失去与 EDR 控制中心的连接，需要重新部署，请谨慎操作；通过 ISO 安装及 OVA 模板安装的方式则会显示本选项，如使用脚本方式安装则不显示。

2.路由设置

EDR管理端需要联网及和终端通信，所以需要配置路由可达。打开[系统管理/系统设置/网络设置/路由设置]配置路由或网关，如下图。



点击<新增>配置路由或网关。

3.高级设置

高级设置包括SSH端口设置和DNS设置以及管理端端口设置，打开[系统管理/系统设置/网络设置/高级设置]，如下图。


网卡设置
路由设置
高级设置
SSH服务设置
开启
端口：
22345
DNS设置
主DNS：
8.8.8.8
备DNS：
114.114.114.114
管控平台端口设置
管控平台访问端口：
443
终端程序升级端口：
4430
网络代理设置
启用服务器代理
当设备自身不能连接互联网时，可通过配置代理服务器来访问互联网
地址：
请输入IP或域名
端口：
输入端口，如：8080
用户名：
代理服务器的登录用户名
密码：
代理服务器的登录密码
连通性测试
管理平台多IP设置
请输入IP/域名
请输入备注
添加
IP/域名地址
备注
操作
192.200.244.103
管理平台本地IP，不可修改
删除

其中：

SSH 端口设置：可对 SSH 端口进行开启或关闭，用于修改 EDR 管理端后台的 SSH 端口，默认为 22345 端口。如果没有使用级联，建议关闭 SSH 接入服务，默认开启 8 小时后自动关闭，

DNS 设置：设置 EDR 管理端的 DNS 服务器地址，平台联网更新病毒库需要能解析域名。

管控平台端口设置：管理员可以设置访问平台的端口以及终端程序升级的端口。

网络代理设置：当管理端不能直接连接互联网、且内网有代理服务器时，可以配置通过代理服务器联网更新规则库、使用云查等功能。支持 http 或 https 代理。

管理端多 IP 设置：支持配置多个管理端的 IP 地址或域名，终端 Agent 从上到下探测地址连通性、并接入第一个可以连通的管理端，此功能主要解决以下场景问题。

1.解决远程办公和出差场景的终端通信问题

终端用户在公司时Agent通过内网地址连接EDR管理端，终端用户出差或远程办公时需要通过外网地址连接EDR管理端，保障终端在内外网切换时的通信连续性。

此场景需要在[管理端多IP设置]同时配置EDR的内网地址和外网地址。

2.解决迁移场景客户端Agent平滑接入迁移后管理端问题

用户已经部署了 EDR 管理端及大量的终端 Agent，由于网络改造，管理端需要迁移至新的网段，迁移后的管理端 IP 地址发生了变化，导致已经部署了 Agent 的终端不能连接迁移后的管理端。为了避免已经安装 Agent 的终端重新安装 Agent，使用此功能配置迁移后管理端地址，实现迁移场景客户端 Agent 平滑接入迁移后管理端。

此场景需要在[管理端多IP设置]先配置迁移前后两个管理端的IP地址、再关闭迁移前的EDR管理端。

4.8.3.4. 日志设置

日志设置用于设置日志自动清除机制，可以自动删除的日志包括安全日志、联动日志、运维日志和操作日志，可设置自动删除天数为7-1095天，默认开关开启。日志预警设置，可以设置日志期望保留天数以及日志预警占用率。

在[系统管理/系统设置/日志设置]页面下，如下图。

其中：

1.当日志存储超过70%会进行横幅提醒。

2.超过存储空间清除阈值，会自动删除日志。安全日志包含病毒查杀日志、漏洞扫描日志、基线检查日志、入侵检测日志（webshell检测日志、暴力破解检测日志、无文件攻击日志）、安全加固日志、违规外连日志及异常登录日志。

4.8.3.5. 升级设置

EDR平台支持针对平台和特征库升级的灰度升级和错峰升级：

1.灰度升级：是一种升级时候的平滑切换，当有些服务器的客户端要进行升级，只对其中一个客户端升级，确保程序无误后再全局升级，也就是说所有服务器不同步更新升级；

2.错峰升级：为避免大量终端程序同时更新造成网络拥堵，设置同时下载更新的终端上线，减少升级对网络的影响。

在[系统管理/系统设置/升级设置]页面下，如下图。

终端程序和规则库升级：用于设置终端升级方式及并发升级的数量。

- 更新方式设置：即灰度升级，选择需要升级的终端，进行策略。
- 更新数量限制：即错峰升级，控制同时更新的终端数量，减少升级对网络带宽的影响。

平台漏洞库升级：用于设置管理端漏洞库自动更新时间，启用后，管理端在指定时间范围自动更新漏洞。

4.8.3.6. 告警设置

EDR平台支持对平台CPU、内存、磁盘使用率进行检测，当在指定时间段内超过阈值则会以邮件形式通知管理员，让管理员及时掌握EDR运行情况及全网安全情况。

在[系统管理/系统设置/告警设置]页签下，配置告警事件，如下图所示。

在[系统管理/系统设置/告警设置]页签下，配置告警通知，如下图所示。

当有告警事件触发时，管理员邮箱会收到如下图所示的告警邮件。

> 说明：
>
> 使用邮件告警，需先在[基本设置]页签下，配置邮箱服务器。

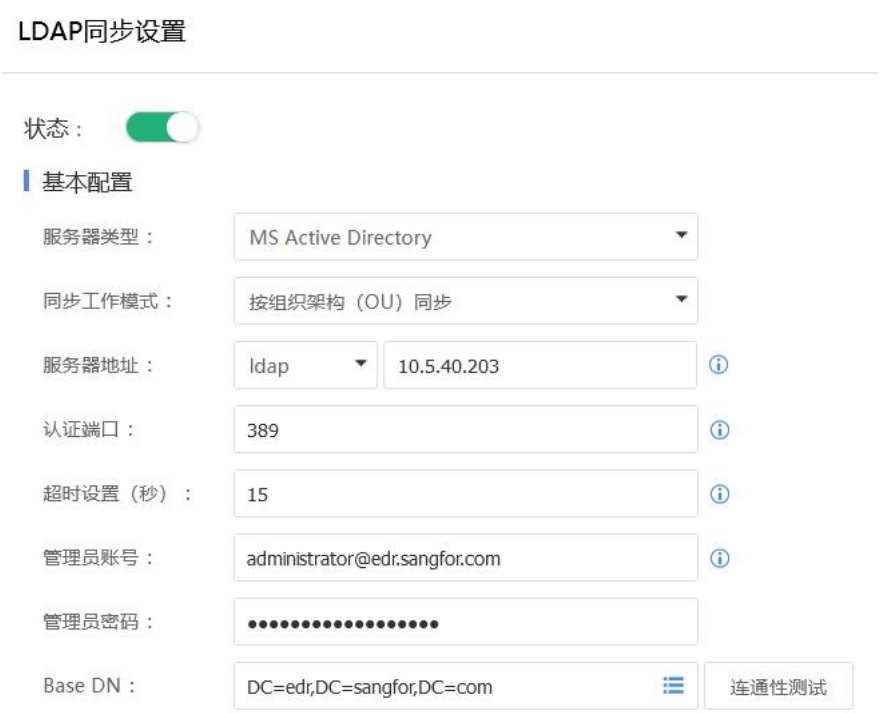
4.8.3.7. LDAP 同步设置

适用场景

管理员需要一种方式，能够自动同步AD域服务器指定范围的组织结构到EDR的分组列表中，不用重复在EDR上创建分组，使EDR分组和AD域控服务器OU保持同步。

LDAP同步配置

打开[系统管理/系统设置/LDAP同步设置]，如下图。



基本配置：配置AD域控服务器地址、端口、管理员帐号和密码及Base DN。其中，管理员帐号需要用以下格式，如administrator@domain.com

同步配置：配置组织架构路径和本地组织架构创建模式，其它保持默认即可。其中，组织架构路径需要填写具体OU、不能直接填写Base DN，如OU=test,DC=edr,DC=com

更新周期配置：启用定时同步，并配置定时同步时间。

触发LDAP同步

可以通过手动同步或定时同步触发LDAP同步。

（1）手动同步

打开[终端管理/终端分组管理]，点击<更多>下拉菜单，如下图。点击<LDAP同步>手动触发立即同步。

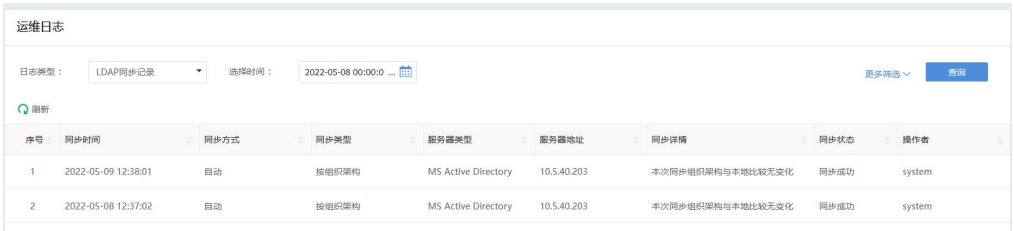
（2）定时同步

参考LDAP同步配置章节，启用定时同步，同步时间范围为1到1000小时，如下图。

LDAP同步效果

域OU同步至终端分组管理页面，如下图。设置根据IP自动分组策略，终端自动上线至所属分组。

查看[日志报表/运维日志]查看LDAP同步详情，如下图。



4.8.3.8. 系统工具

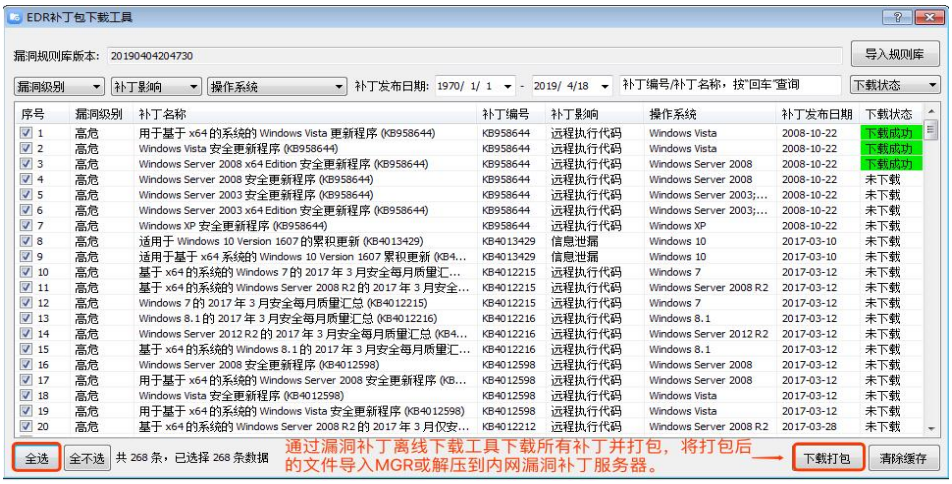
系统工具为漏洞补丁包离线下载工具，此工具和EDR系统漏洞检测与修复功能配合使用。当客户的EDR管理端以及其所管理的所有终端都无法访问外网时，可以使用此工具下载系统漏洞补丁后导入平台进行终端系统漏洞修复。

在[系统管理/系统设置/系统工具]页签下，如下图所示。

工具使用步骤

步骤1. 在上图位置下载工具，并将本工具拷贝到可上网的电脑终端。

步骤2. 打开此工具，并下载系统漏洞补丁包，如下图所示。



步骤3. 将下载的漏洞补丁包导入管理端即可，如下图所示。

步骤4. 进行终端漏洞检测与修复操作。

4.9. Agent 使用

终端用户通过终端组件Agent可进行病毒查杀、文件隔离与信任、部分功能设置及日志查看等操作。

4.9.1. Windows 系统 Agent 使用

Windows系统客户端Agent支持安装在简体中文及其它语言操作系统，并自适应终端系统环境。简体中文操作操作系统EDR客户端展示中文；其它语言操作系统EDR客户端展示英文。

4.9.1.1. 首页展示

当完成终端组件Agent部署后，在首页可查看终端保护时长、上次查杀时间、实时防护趋势等，首页如下图所示。

4.9.1.2. 安全中心

安全中心顶端显示当前终端受保护时长及客户端和管理端连接状态。

- 左上角“ • ”图标为绿色表示客户端和管理端连接正常，
- 图标为灰色表示客户端和管理端连接异常。

安全中心提供了病毒查杀、实时防护的快速入口，以及近30天的防护趋势。

提醒版块列出最近消息提示，如病毒库版本更新、软件版本更新、管理员下发的通知等消息。

安全中心右下角“ ”版块显示EDR从预防、防护、检测和响应每个阶段对勒索病毒的立体防护机制，如下图。

4.9.1.3. 病毒查杀

病毒查杀页面可以对终端进行快速扫描、全盘扫描、自定义扫描，以及查看查杀日志。

快速扫描：对windows系统关键位置查杀，例如对/windows和/windows/system32本级目录，/windows/system32/drivers本级目录和其子目录进行查杀。

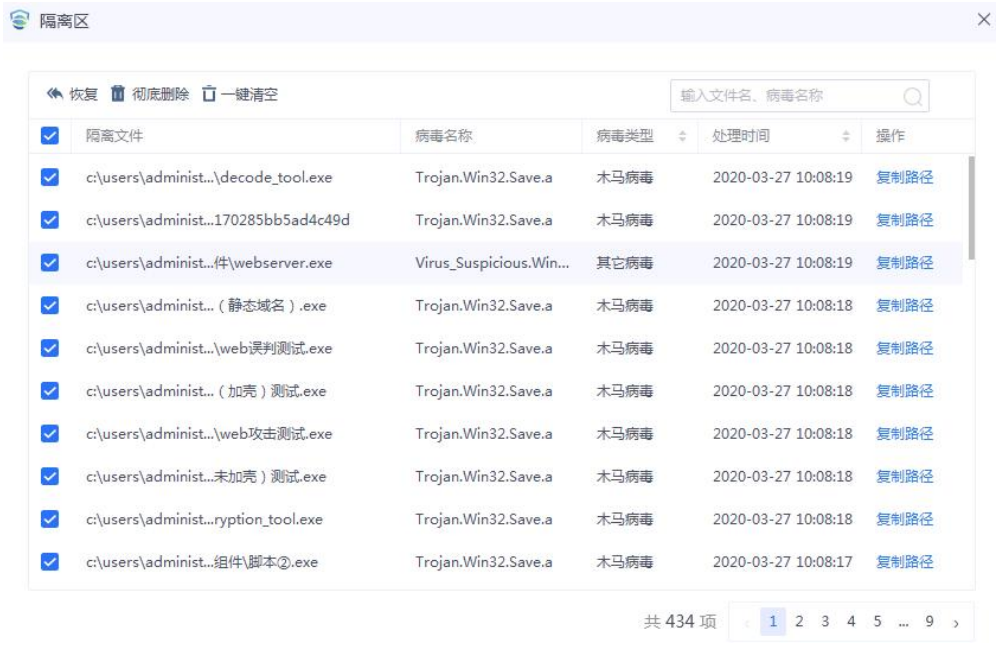
全盘扫描：对windows系统所有位置进行查杀。

自定义扫描：对指定文件或目录进行查杀。

病毒查杀页面左下角可以查看查杀引擎，蓝色图标表示引擎开启，灰色表示引擎关闭，鼠标移动到引擎图标，会有引擎详细说明。

图标	名称	功能
	深信服 SAVE 人工智能引擎	提升未知病毒的检测能力。深信服自主研发的人工智能引擎，精通勒索病毒查杀，机器自学识别各种变种病毒。
	基因特征引擎	通过对热点事件的病毒家族进行基因特征的深度提取，使之能有更精准的检测效果。
	行为分析引擎	通过虚拟执行的方式发现病毒，擅长识别未知新变种病毒。
	云查引擎	拥有海量的病毒库，云端多引擎联动查杀，具备强大的病毒识别能力。

病毒查页面右下角可以查看隔离区、信任区的文件，以及病毒查杀日志，点击<隔离区>，对隔离区的文件可以进行恢复、彻底删除或一键清空，如下图。



例如，点击<快速扫描>触发对系统关键位置进行扫描，如下图。

选中扫描页面右下角[扫描完成后自动关机]适用于下班前开启病毒扫描，查杀后自动关机的场景。

对查杀发现的威胁文件可以进行处置、信任、忽略、查看详情操作，如下图。

处置：将发现的病毒文件进行隔离，如果是宏病毒或感染性病毒文件先尝试修复，隔离后的文件可以在“隔离区”查看。

信任：人为分析为正常文件后定义为信任。信任后的文件可以在“信任区”查看。

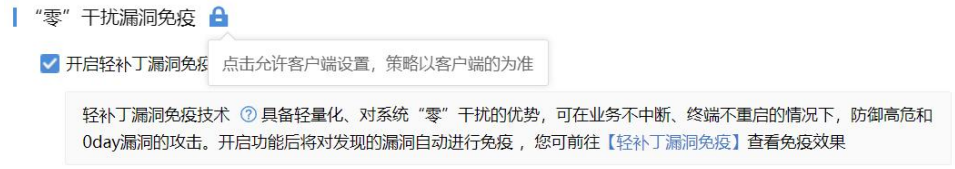
忽略：忽略此次文件的检查。

详情：打开威胁文件详细信息，如下图。

4.9.1.4. 漏洞防护

管理员在EDR管理端设置允许在终端组件开启漏洞防护，若管理员在EDR的管理端设置开启轻补丁漏洞免疫，且不允许客户端修改，则终端组件默认开启轻补丁漏洞免疫，如下图所示。

EDR管理端



终端组件显示

4.9.1.5. 实时防护

实时防护包括系统防护、高级威胁防护、网络防护和其它防护四类，实时防护首页向用户整体展示防护开启起情况，如下图。

点击<系统防护>，打开系统防护详情，系统防护包括文件实时防护。管理员可以回收终端用户的配置权限，如果管理员不允许终端修改配置，则终端会提示“管理员设置不允许修改”，如下图。

点击<高级威胁防护>，打开高级威胁防护详情，包括勒索诱饵防护、powershell无文

件攻击防护、顽固病毒免疫防护，如下图。

点击<网络防护>，打开网络防护详情，包括RDP远程爆破登录防护和SMB远程爆破登录防护，如下图。

点击<其它防护>，打开其它防护详情，包括自保护和终端外设管控，如下图。

终端外设管控默认开启，当终端接入U盘时会在右下角弹出提示，可打开U盘、弹出U盘或对U盘进行病毒查杀，如下图。

点击<弹出>，插入的U盘自动弹出，如下图。

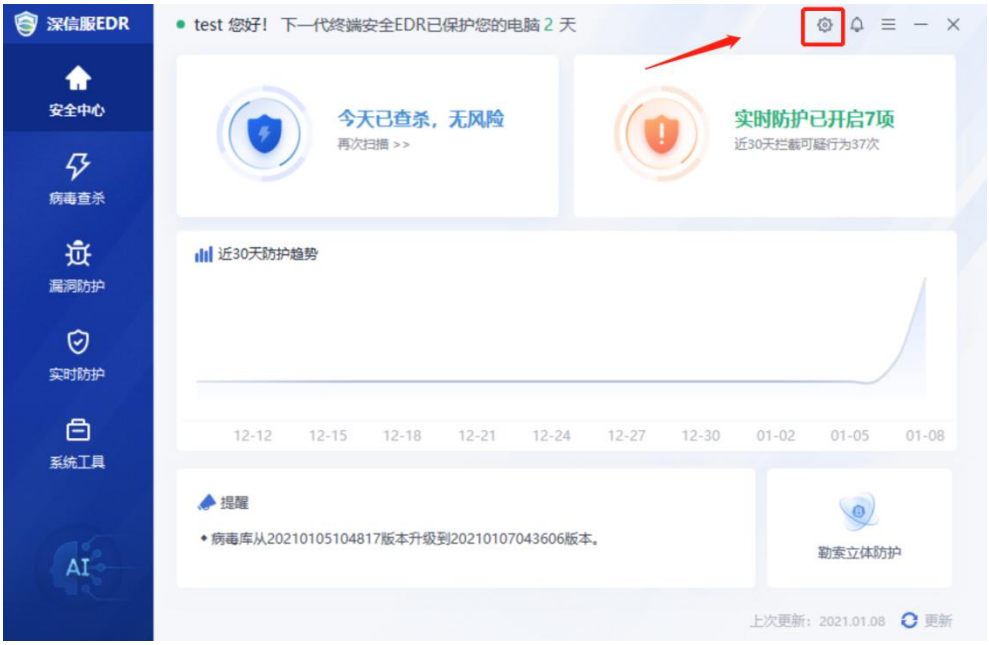
4.9.1.6. 系统工具

系统工具包括勒索病毒解密、挖矿病毒巡检工具、误报反馈和问题反馈。

勒索病毒解密：当服务器被加密勒索时，可以根据勒索特征，如加密文件后缀、勒索信息等通过勒索病毒解密工具查询勒索信息及是否有解密工作。

4.9.1.7. 设置中心

点击客户端右上角“ ”图标，进入设置中心，如下图。



进入设置中心，设置中心包括病毒查杀、系统防护、高级威胁防护、网络防护和提醒设置各项功能参数设置。每个功能在管理端有相同的配置项，管理员可以回收客户端的配置权限。在管理端策略中心每个策略右边有锁图标，锁图标点亮，则管理员不允许客户端单独配置，此时客户端会给出提示“管理员设置不允许修改”。

病毒查杀：病毒查杀设置包括扫描模式、引擎配置、文件类型和处置方式设置。各参数设置与管理端文件实时监控设置方法一致，具体参考“管理端使用/终端管理/策略中心/病毒查杀”章节。

系统防护：系统防护设置文件实时防护的防护级别、引擎配置、文件类型、扫描文件和处置方式。各参数设置与管理端文件实时监控设置方法一致，具体参考“管理端使用/终端管理/策略中心/实时防护”章节。

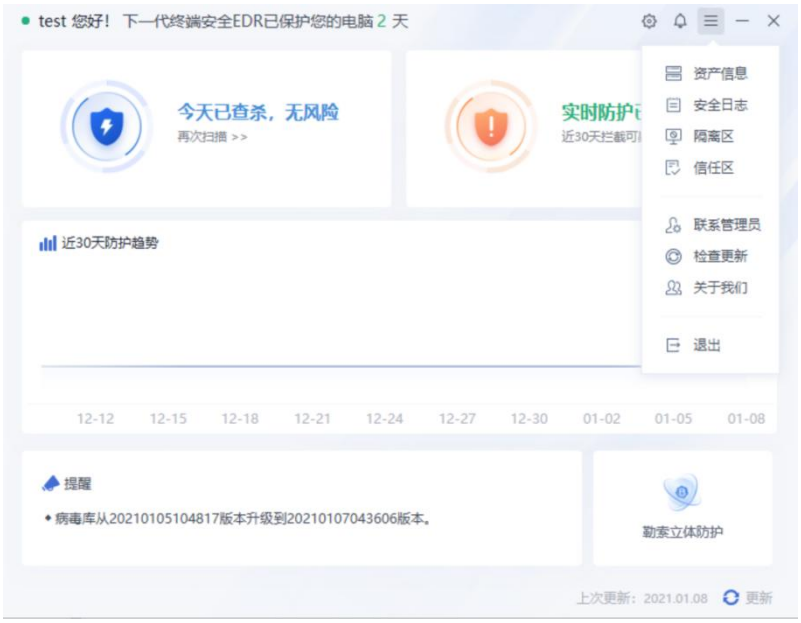
高级威胁防护：高级威胁防护设置包括勒索诱饵防护设置和无文件攻击防护设置。各参数设置与管理端勒索诱饵防护设置和无文件攻击防护设置方法一致，具体参考“管理端使用/终端管理/策略中心/实时防护”章节。

网络防护：网络防护设置包括RDP暴力破解检测和SMB暴力破解检测设置。各参数设置与管理端暴力破解检测设置方法一致，具体参考“管理端使用/终端管理/策略中心/实时防护”章节。

提醒设置：提醒设置包括病毒查杀提醒设置、文件实时防护告警弹框设置、勒索诱饵防护告警弹窗设置、Powershell无文件攻击防护告警弹窗、暴力破解防护告擎弹窗和轻补丁漏洞免疫弹窗设置。用户可以根据实际需求，个性化设置是否允许弹窗提示。如果管理员从管理端统一设置禁止弹窗提醒或终端启用了免打扰模式，则此处为灰色，不允许修改。

4.9.1.8. 安全日志

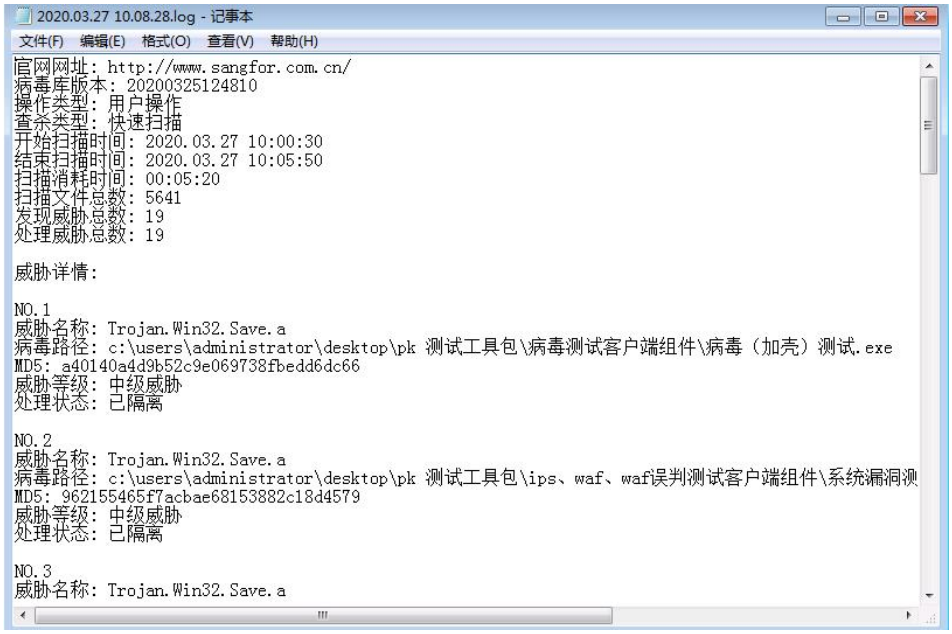
点击客户端页面右上角“ ”图标，打开安全日志，如下图。



安全日志包括病毒查杀日志和实时防护日志。

实时防护日志是开启文件实时监控后检测到威胁文件产生的安全日志。

病毒查杀日志指触发病毒查杀的操作日志，点击详情查看当时病毒查杀的详细信息，如下图。

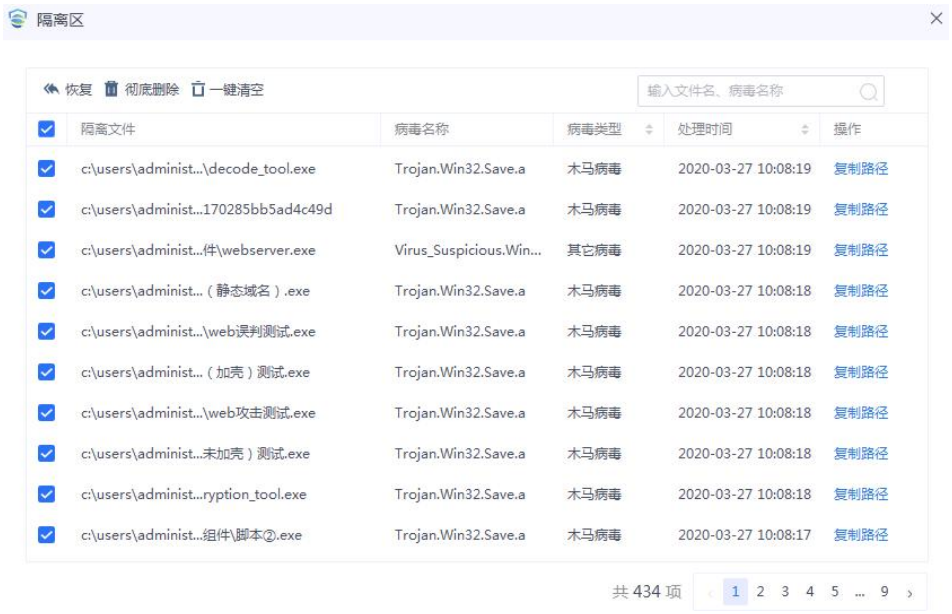


4.9.1.9. 隔离区/信任区

EDR检测到威胁文件进行处置时会进行隔离，文件移至隔离区；被误报的文件或进程加入信任区，信任区的文件，病毒查杀及文件实时监控会自动跳过。

点击客户端页面右上角“☰”图标，打开隔离区/信任区，如下图。

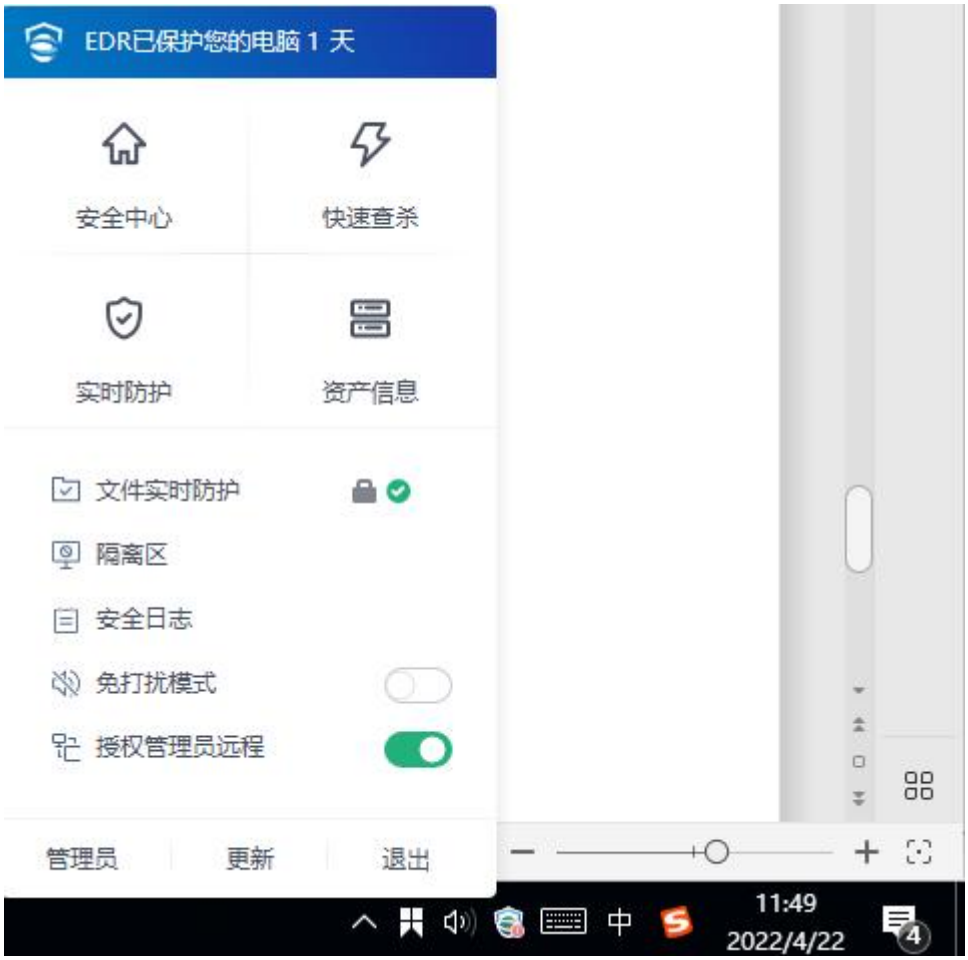
进入隔离区，对隔离区的文件可以进行恢复、彻底删除或一键清空，如下图。



进入信任区，可以对文件、目录、进程添加信任，如下图。

4.9.1.10. 托盘

EDR客户端在系统右下角的托盘可以实现一些快捷操作，在图标上单击右键如下图所示。

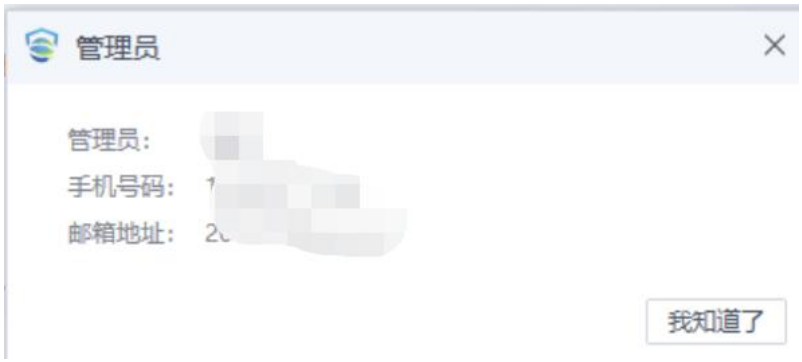


安全中心、快速查杀、实时防护、系统工具、文件实时防护、隔离区、安全日志都是托盘提供的功能快捷入口。

免打扰模式：开启免打扰模式，则EDR检测到威胁文件不会进行弹窗告警提示。此功能可以由客户单独配置或管理员在管理端统下发。

授权管理员远程：此功能默认开启，管理员可以通过远程协助功能远程管理终端。

管理员：点击<管理员>弹出如下管理员信息，当用户使用EDR需要协助时，可以方便的找到管理员。



4.9.2. MAC OS Agent 使用

4.9.2.1. 病毒查杀

病毒查杀页面可以对终端进行快速扫描、全盘扫描、自定义扫描，以及查看查杀日志。

快速扫描：对MAC系统关键位置查杀，例如对/private/tmp、/Users/“当前账户名”/Downloads、/Users/“当前账户名”/Desktop、/Users/“当前账户名”/Documents目录进行查杀。

全盘扫描：对MAC系统所有位置进行查杀。

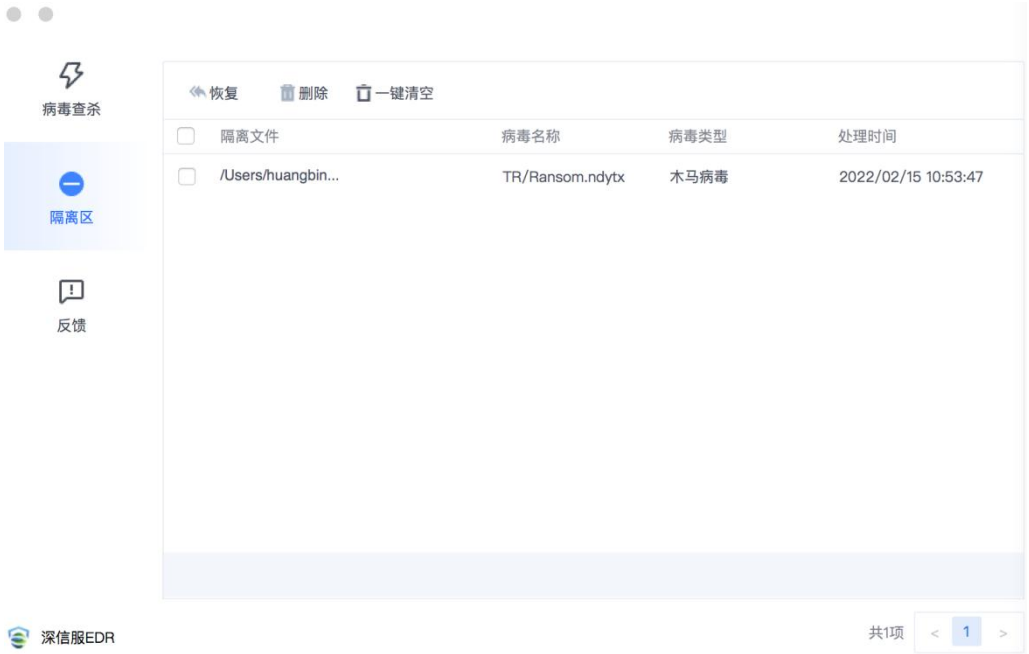
自定义扫描：对指定文件或目录进行查杀。

点击图中右上角<导出日志>导出病毒查杀日志；点击图中右上角可以在英文及简体中文之间切换Agent显示语言。

病毒查杀效果图如下，选中威胁文件点击<处置>将隔离威胁文件，点击<忽略>将忽略此次查杀文件不处理。

4.9.2.2. 隔离区

EDR检测到威胁文件进行处置时会进行隔离，文件移至隔离区。进入隔离区，对隔离区的文件可以进行恢复、彻底删除或一键清空，如下图。



5. 产品升级

EDR产品升级包括新版本升级、安全补丁升级、病毒库升级以及漏洞规则库升级。

5.1. 新版本升级

升级前检查

1.检查产品授权

打开[系统管理/授权管理] ，查看授权是否有效期内，授权过期不能升级，如下图。

2.检查产品是否存在定制

升级前查看是否有定制，如有定制，需联系服务提供商确认后升级。定制确认方法如下，打开管理端[系统管理/升级管理/平台和终端升级]，查看是否有安装定制或补丁。

升级注意事项

管理端升级后，客户端会自动从管理端下载组件进行升级，为保障Agent稳定与高效升级，建议采取灰度升级与错峰升级相结合的策略。

1.灰度升级

在管理端可设置当管理端升级时，只允许部分终端进行自动更新，当部分终端升级成功没问题后，再选择[全部终端自动更新程序]，以实现全网更新的平滑过渡的一种升级方式，保证整体系统的稳定。

配置路径：[系统管理/系统设置/升级设置]终端程序和规则库升级，如下图。

2.错峰升级

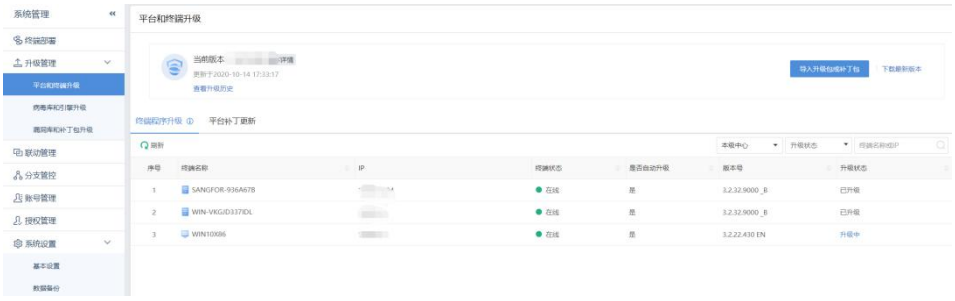
为避免大量终端程序同时更新造成网络拥堵，在管理端可对同时间段自动更新的Agent数量做限制，建议百兆带宽设置不超过5台终端同时更新，千兆带宽设置不超过30台终端同时更新。

配置路径：在[系统管理/系统设置/升级设置]页面下，更新数量限制，如下图。

升级步骤

1.在深信服社区下载对应版本升级包并验证MD5值，升级包下载链接：https://bbs.sangfor.com.cn/（路径：自助服务/软件下载/终端安全管理系统EDR/EDR升级包）

2.登录EDR管理端，在[系统管理/升级管理/平台和终端升级]页面，点击<导入升级包>，如下图。



3.升级过程不需要重启服务器，等待五分钟左右升级完成，需要重新登录控制台，查看当前版本为升级后版本，说明升级成功。

5.2. 安全补丁更新

当发布EDR安全补丁时，管理端可以联网更新或离线手动导入平台安全补丁。通过[系

统管理/升级管理/平台和终端升级/平台补丁更新]可以查看安全补丁更新详情。

平台补丁检测

检查适用当前平台的安全补丁。

打开[系统管理/升级管理/平台和终端升级/平台补丁更新]，点击<补丁检测>，可以检查适用当前平台的安全补丁。

补丁更新设置

设置平台补丁更新方式

打开[系统管理/升级管理/平台和终端升级/平台补丁更新]，点击[更新设置]，配置更新方式、升级服务器，如下图所示。

当管理端不能直接连接互联网，但登录管理端的电脑可以联网，可以启用浏览器代理、管理端通过电脑代理获取补丁更新，如下图。

当平台有紧急补丁发布，且客户没有开启自动更新，我们可以通过紧急联系人联系用户侧，避免影响客户的业务使用，所以需要提前配置紧急联系人，如下图。

当管理端和PC都无法访问互联网时，可以用手机扫描二维码获取补丁包列表，手动下载并导入到管理端更新。

打开[系统管理/升级管理/平台和终端升级/平台补丁更新]，点击[获取离线包]，如下图。

5.3. 规则库升级

5.3.1. 病毒库升级

病毒库升级模式分为在线升级与离线升级两种：

在线升级

默认开启，管理端能够上网，即可实现规则库在线自动更新。

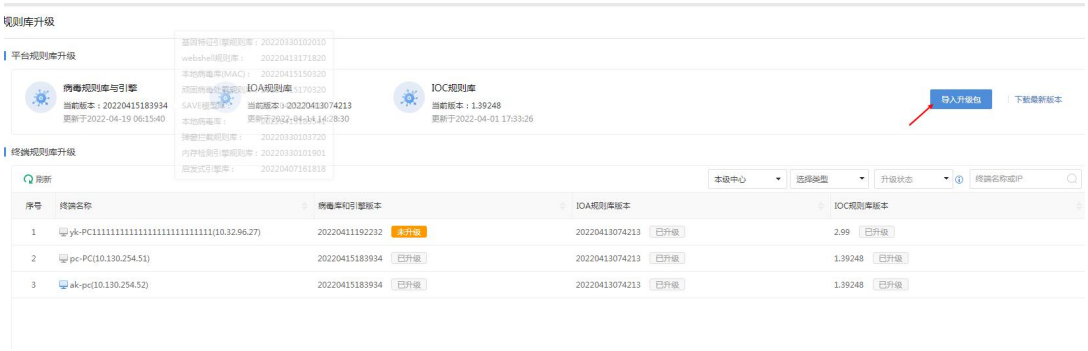
离线升级

如果管理端处于隔离网环境，即无法上网。则需要使用离手动升级方式，升级步骤如下：

1.下载离线病毒库或引擎组件并验证MD5值。

病毒库下载地址：https://bbs.sangfor.com.cn/（路径：自助服务/软件下载/终端安全管理系统EDR/病毒库）

2.登录控制平台，进入[系统管理/升级管理/病毒库和引擎升级]页面，点击<导入更新包>，选择步骤1中下载的规则库，平台病毒库和引擎组件导入成功后，Agent会自动升级病毒库和引擎组件，如下图。



5.3.2. IOA 规则库、IOC 规则库升级

IOA规则库或者IOC规则库升级模式分为在线升级与离线升级两种：

Ps：IOA-IOC规则库同时包含IOA规则库和IOC规则库

在线升级

默认开启，管理端能够上网，即可实现规则库在线自动更新。

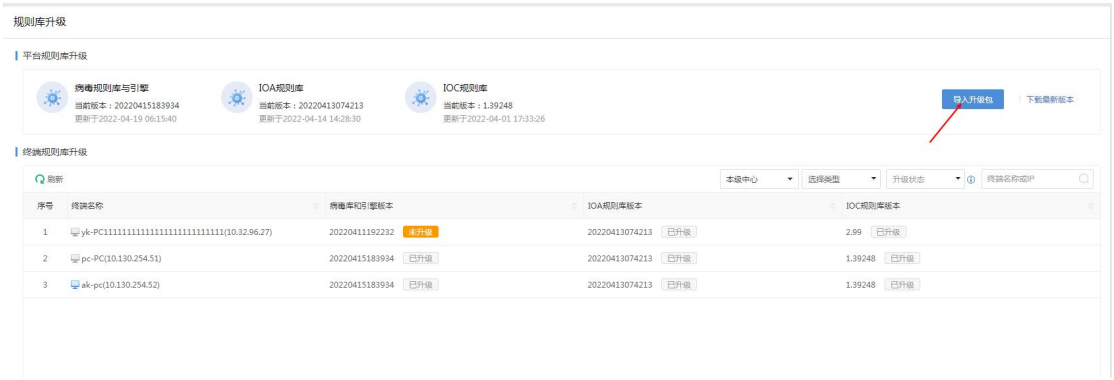
离线升级

如果管理端处于隔离网环境，即无法上网。则需要使用离手动升级方式，升级步骤如下：

1.下载IOA-IOC规则库并验证MD5值。

IOA-IOC规则库下载地址：https://bbs.sangfor.com.cn/（路径：自助服务/软件下载/终端安全管理系统EDR/规则库）

2.登录控制平台，进入[系统管理/升级管理/规则库升级]页面，点击<导入更新包>，选择步骤1中下载的规则库，平台IOA-IOC规则库导入成功后，Agent会自动升级IOA规则库和IOC规则库，如下图。



5.4. 漏洞规则库升级

漏洞库规则库升级分为在线升级与离线升级两种。

在线升级

默认开启，管理端能够上网，即可实现漏洞库和补丁包在线自动更新。

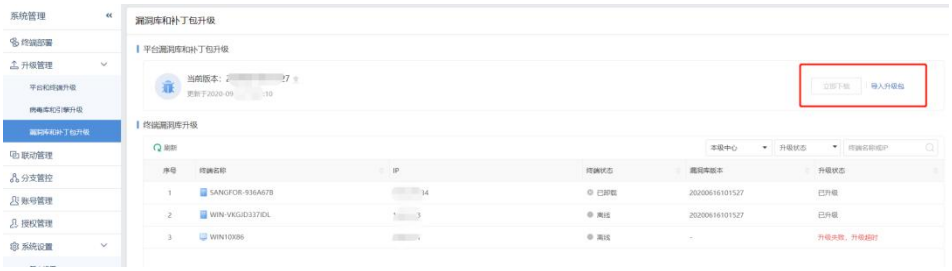
离线升级

如果管理端处于隔离网环境，即无法上网。则需要使用离手动升级方式，升级步骤如下：

1.下载漏洞库或补丁包并验证MD5值。

漏洞规则库下载地址：https://bbs.sangfor.com.cn/（路径：自助服务/软件下载/终端安全管理系统EDR/漏洞规则库）

2.登录控制平台，进入[系统管理/升级管理/漏洞库和补丁包升级]页面，点击<导入升级包>，选择步骤1中下载的规则库，平台漏洞库和补丁包导入成功后，Agent会自动升级漏洞库，如下图。



6. 高危操作

在日常使用EDR时，请先了解下表中的高危操作并避免这些操作。如果使用不当，会对业务产生影响，严重时会造成业务中断。

表13 高危操作

主模块	一级目录	二级目录	风险操作	风险说明	风险级别	风险应对
终端管理	策略中心	病毒查杀	发现威胁文件后的处置动作设置为“自动处置-安全优先”	可能存在误判，将客户的业务文件隔离，导致业务系统异常	高风险	将发现威胁文件后的处置动作设置为“自动处置-业务优先”
终端管理	策略中心	病毒查杀	日常使用时，引擎配置启用了“高检出模式”	高检出模式能够提高病毒检出率，但也会增加误判，一般在测试病毒检出率时使用，所以正常使用时不启用	高风险	正常使用时引擎配置不启用“高检出模式”
终端管理	策略中心	实时防护	文件实时监控中，当发现威胁文件后的处置动作设置为“自动处置-安全优先”	可能存在误判，将客户的业务文件隔离，导致业务系统异常	高风险	将发现威胁文件后的处置动作设置为“自动处置-业务优先”
威胁检测	终端病毒查杀	扫描模式	当服务器性能不足时，使用了极速扫描模式下载扫描	极速扫描将会消耗更多的终端 CPU 资源，如果服务器性能不足，则会影响业务正常使用。默认建议使用均横模式扫描	高风险	服务器性能不足时，使用“低耗”或“均衡”扫描模式
响应中心	威胁响应	威胁终端视角	终端隔离	隔离后终端无法访问任何其它网络。如果是服务器被隔离，会影响业务正常使用	高风险	在[响应中心/威胁响应/已隔离终端]进行移除
响应中心	漏洞响应	漏洞修复	某些漏洞需要重启系统才能	服务器重启，导致业	高风险	修复漏洞时建议不要选

			完成修复，如果选择了修复后自动重启服务器，是业务会中断	务中断		择重启服务器，而是在统一时间（不影响业务时间）人为重启
终端管理	策略中心	勒索防护	启用了服务器可信进程防护，但服务器业务进程没有加入可信进程	导致服务器关键业务运行不起来，导致业务中断	高风险	将服务器业务进程加入可信进程

7. 常见问题

7.1. 智能机器人

产品支持智能在线客服，能够全天候在线提供便捷性产品配置问题、产品功能疑问等相关产品问题解决方案。摆脱繁琐的电话客服流程，只需点击智能客服图标就可以直接快速跟深信服的智能机器人、人工客服进行一对一在线交流。

7.2. 安装部署

1.安装过程中出现下图提示。

解决方法：

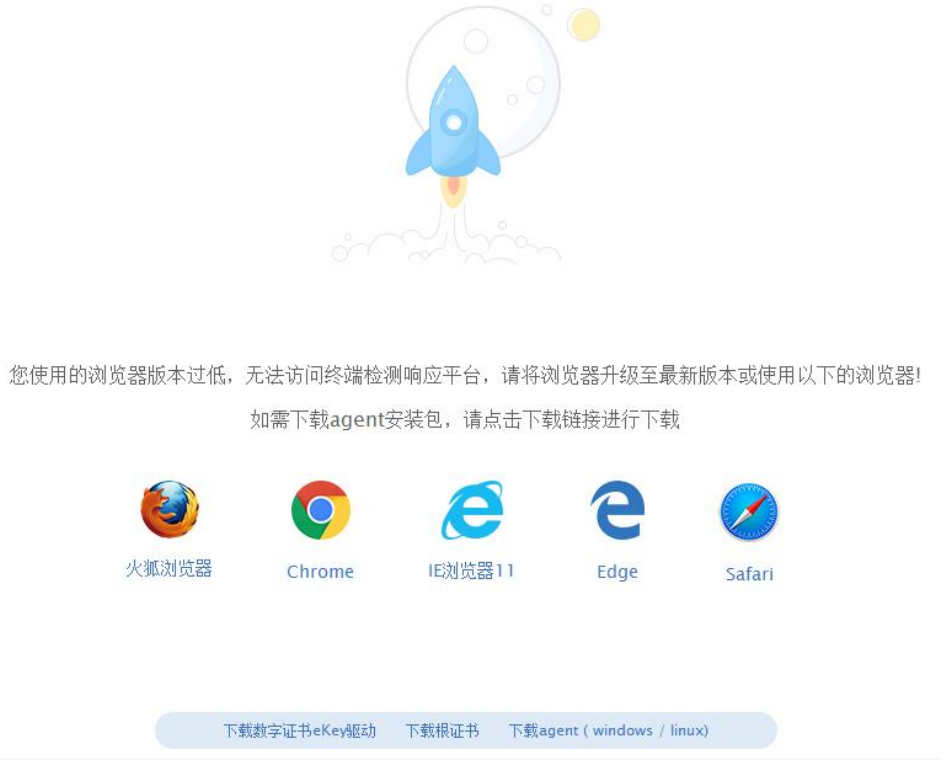
出现上图提示，说明安装程序文件名被改。在上图填写EDR管理端地址及443端口即可完成安装，或者也可以重新下载安装程序（不能修改安装程序文件名）进行安装。

2.安装过程中弹出提示“检测到您安装了其它安全软件，可能与EDR终端防护中心存在冲突”。

解决方法：

卸载电脑上其它的安全软件后继续安装EDR终端防护软件。

3.使用IE浏览器打开EDR管理端控制台，无法登录控制台，提示如下图。



解决方法：

出现上图提示，说明IE浏览器版本太低。请使用IE11或其它浏览器登录。

4.病毒库无法自动升级。

解决方法：

请确保EDR管理端IP地址、网关、DNS配置正确，所在环境可以联网访问download.sangfor.com.cn

5.电脑安装EDR后出现异常情况。

解决方法：

通过EDR管理端[终端管理/终端分组管理]，禁用问题电脑的agent，如下图，如果禁用后故障恢复，则联系服务提供商进一步处理。

7. 3. 病毒查杀

1.EDR是否可以支持U盘文件、网络共享路径下的文件进行查杀？

解决方法：

EDR支持对U盘文件扫描查杀，不支持对网络共享路径下的文件进行查杀。

2.电脑性能不足，EDR下发病毒扫描时，CPU使用率高？

解决方法：

打开EDR管理端[终端管理/策略中心/病毒查杀]，启用“资源优化模式”，如下图。

3.隔离病毒文件时，提示隔离区满，病毒文件无法隔离。

解决方法：

windows端隔离区默认大小为4G，路径在

C:\ProgramData\Sangfor\EDR\SAV，当该路径下的文件超过4G时，将无法再继续隔离，可以通过管理端或终端agent删除隔离区文件。

7. 4. 微隔离

1.微隔离策略不生效。

解决方法：

请按如下检查，如果仍然不生效，请联系服务提供商处理。

- 微隔离功能不支持终端操作系统为 Windows XP 或 Windows Server 2003，如果终端操作系统是上述版本，则微隔离不生效。
- 打开 EDR 管理端[微隔离/微隔离策略]，检查“微隔离生效开关”是否启用状态，如下图。

2.微隔离流量状态无法显示。

解决方法：

请按如下检查，如果无法解决，请联系服务提供商处理。

- 打开 EDR 管理端[微隔离/微隔离设置]，检查“流量上报”开关是否启用状态，如下图。

- 打开 EDR 管理端[微隔离/流量状态]，检查“过滤流量”条件是否启用，如下图。

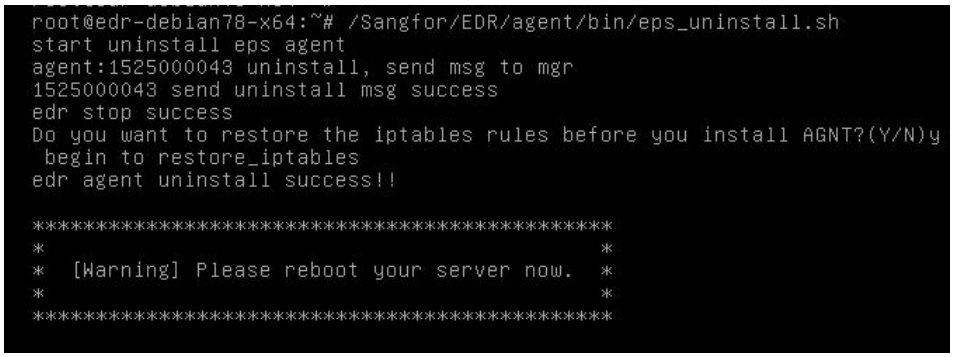
7.5. 终端 Agent 卸载

7.5.1. Windows 系统卸载 Agent

打开Windows开始菜单栏，定位“EDR终端防护中心”，点击[卸载EDR终端防护中心]，按提示进行卸载，如下图所示。

7.5.2. Linux 服务器卸载 Agent

在 Linux 终端命令行，定位 EDR 文件目录：/Sangfor/EDR/agent/bin，运行“eps_uninstall.sh”文件进行卸载操作，如下图所示。



7.5.3. 管理端卸载 Agent

1.在管理端上，[终端管理/终端分组管理]，勾选需卸载Agent组件的终端设备；

2.在横栏中，点击[卸载agent]按钮，如下图，进行终端Agent组件卸载。

> 说明：
> 仅支持对终端状态为在线/已禁用进行卸载 Agent 的操作。

8. 缩略语

	英文全称	中文全称
A		
AC	Access Control	上网行为管理
AF	Application Firewall	深信服下一代防火墙
C		
CVE	Common Vulnerabilities & Exposures	公共漏洞和暴露
E		
EDR	Endpoint Detection and Response	终端安全管理系统
H		
HCI	Hyper-Converged Infrastructure	超融合基础设施
S		
SIP	Security Intelligence Platform	安全感知平台
SOC	Security Operation Center	安全运营中心