天翼云 • 安全专区•终端安全 EDR

用户使用指南

中国电信股份有限公司云计算分公司

目 录

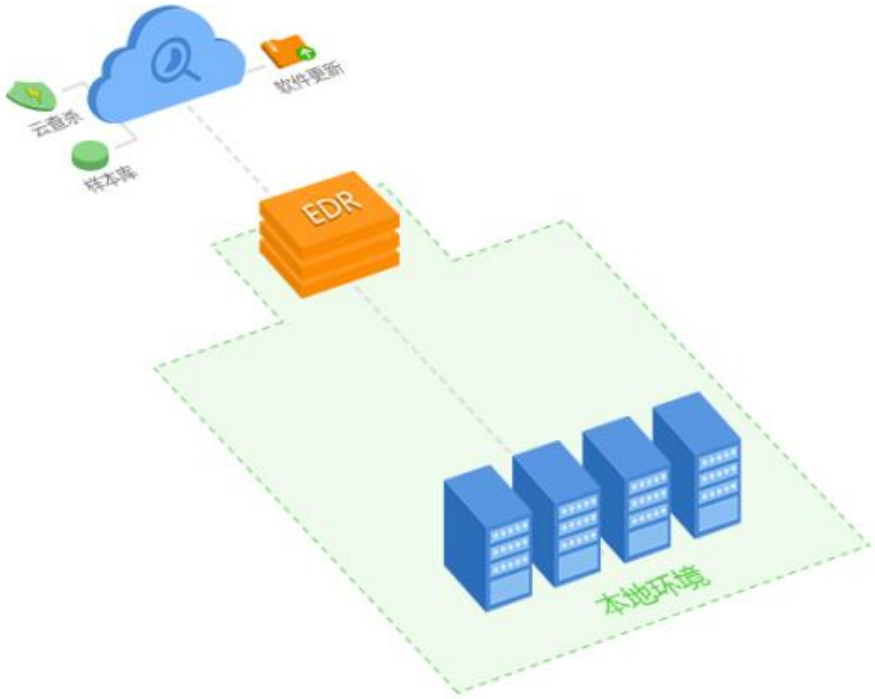
1. 产品概述

终端检测响应平台EDR（Endpoint Detection and Response）是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和管理平台组成。管理平台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。

同时，终端检测响应平台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. 产品简介

终端检测响应平台EDR可部署在用户本地环境。EDR的管理平台有软件和硬件两种形态，软件管理平台部署在Linux服务器上，硬件管理平台旁路接入网络核心，负责集中管理所有Agent；端点安全软件Agent安装在每台终端上。管理平台通过公网与安全云联动，内网每台终端Agent与终端检测响应平台联动，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。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。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。

热点事件快速响应

安全云脑可通过全球大数据安全分析，提供热点事件IOC情报，及时推送情报数据至EDR产品。EDR产品能根据IOC情报数据快速完成全网威胁定位分析，及时发现和响应最新热点事件，并且根据历史行为数据进行溯源分析，避免组织受到安全事件的通报。

2. 安装部署

EDR是由云端服务中心、管理平台及客户端Agent三部分组成的终端安全解决方案，本章节主要对整体平台的安装部署进行指导。

2.1. 部署计划

产品安装部署按照先部署管理平台、然后激活产品、最后安装客户端Agent的顺序进行部署。为确保客户业务稳定性和连续性，安装客户端Agent前，需要提前做好安装计划，避免突发无法提前预知的情况影响到客户业务，安装计划遵从以下要求：

1. 先部署在测试环境，测试环境运行无问题再逐步上线到正式环境；
2. 正式环境应按计划分期逐步部署，避免一次性部署出现意外突出情况影响客户业务。

2.2. 准备工作

2.2.1. 管理平台安装环境

具体安装环境设置，请登录天翼云控制平台进行查看。

2.2.2. 客户端 Agent 安装环境

客户端Agent具备广泛兼容性，支持windows、Linux多版本系统，目前已明确支持系统如下表所示。

表1 各系统及版本信息

系统类别	兼容版本信息
Windows	WinXP/Win7/Win8/Win8.1/Win10（32/64）
Windows Server	WinServer2003 SP2 WinServer2008/2008R2 WinServer2012/2012R2 WinServer2016
Linux	CentOS 5.7x86/6/7 Ubuntu 10.04/11.04/12.04/13.04/14.04/16.04 Debian 6/7

	RHEL 5/6/7 SUSE 11/12/15 Oracle Linux

2.2.3. 网络连通性要求

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

表2 网络连通性要求

源设备	目的设备	端口	端口作用
Agent	管理平台	443	Agent 下载端口
		8083	业务端口
		54120	管理端口

2.2.4. 收集需放行的白名单文件

为了避免病毒查杀可能带来的误报影响，提前收集好需放行的白名单文件。白名单文件包括客户自己开发的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。在部署完管理平台并完成授权激活后，登录EDR管理平台，在[终端管理/策略中心/信任名单]页签下，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。

2.3. 终端组件 Agent 部署

2.3.1. Windows 系统部署

针对Windows 系统（PC或Server），EDR可实现下载安装包部署、网页推广部署、联动AC推广部署、虚拟机模板部署、域推脚本部署及桌管软件分发部署等多种部署方式，可依客户侧部署场景不同，针对性使用推荐的部署模式，常见场景与部署模式推荐如下。

表3 场景与部署方式

场景	推荐部署模式
PC 数量小	下载安装包部署、网页推广部署
PC 数量大（有域控）	域推脚本部署
PC 数量大（无域控）	联动 AC 推广部署
虚拟化环境（云桌面等）	虚拟机模板部署
具备桌管软件场景	桌管软件分发部署

2. 3. 1. 1. 下载安装包部署

下载安装包部署模式，需管理员在EDR管理平台本地下载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。部署步骤如下：

1. 下载安装程序：下载路径[系统管理/终端部署/下载安装包部署]。

> 说明：
> PC 客户端安装程序默认命名（类似 edr_installer_117.48.147.100_443.exe）包含 EDR 管理平台通讯地址信息，下载后请勿更改安装程序名。

也可以从控制台首页下载安装程序，如下图。

2. 将安装程序拷贝至需要安装的终端。

3. 在终端双击执行安装程序。

勾选“同意免责声明”，点击<立即安装>，安装程序连接EDR管理平台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，终端的 Agent 程序将自动连接EDR管理平台。在管理平台[终端管理/终端分组管理]可以看到终端上线信息，如下图。

2.3.1.2. 网页推广部署

网页推广部署支持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，终端用户依部署通知自行下载Agent安装包进行安装部署。部署步骤如下：

1. 编辑部署通知

在[系统管理/终端部署/网页推广部署]，编辑部署通知的页面标题和内容，可进行预览，预览无问题后可点击<保存并生成链接>。

2. 复制链接，发送至终端

可将定稿链接，通过全网邮件、OA等方式发送给终端用户，终端用户通过链接指引进行自行安装，打开指引链接如下图所示。

2.3.1.3. 联动 AC 推广部署

联动AC推广部署，可实现EDR和AC设备联动，当终端用户打开网页时，未安装Agent的PC将被AC重定向至安装Agent页面，直至终端成功安装Agent，从而实现Agent部署批量安装，部署步骤如下：

> 说明：
> EDR 要求 3.2.8 及以上版本， AC 要求 12.0.14 及以上版本，且终端用户系统在产品兼容范畴。

1. 该部署模式仅需在AC界面配置即可，登录AC控制台，在[上网安全/安全能力/安全配置/终端检测与响应（EDR）]页签下，在EDR接入设置界面填入EDR平台IP并点击<接入>。
2. 接入成功后，页面会显示服务状态为[在线]，且EDR平台IP正常显示，同时点击页面[查看联动详情]，可查看EDR上已有的联动终端。
3. 在[终端检测与响应（EDR）]页面右上角，点击[推送配置]，在弹出页面配置策略使用的网段范围、重定向地址及推送时间间隔。

> 说明：
> 重定向地址为 EDR 控制台，[系统管理/终端部署/上网行为管理系统（AC）联动部署]一栏内的重定向地址。

4. 配置成功后，用户打开网页会被重定向到通知部署Agent页面，此页面定时弹出，直至用户下载并完成Agent安装为止。

2.3.1.4. 域推脚本部署

域推脚本部署，可通过域控配置响应策略下发相应策略，实现终端用户登录后会自动执行安装脚本，静默安装Agent组件，达到批量部署Agent目的。

📖 **说明：**

域推脚本安装需要域用户有安装软件权限（需将域用户添加到管理员组，如下图），且终端用户系统在产品兼容范畴。

部署步骤如下：

1. 按下图编写“edr.bat”脚本，需修改Route对应的IP及EDR_EXE对应的文件名，如下图所示，其中：

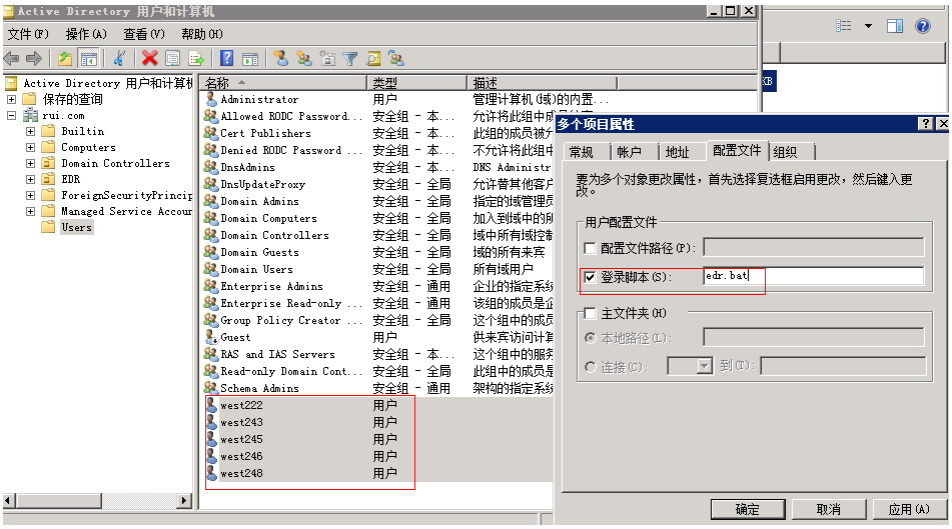
   ROUTE对应的IP为域控服务器的IP；

   EDR_EXE对应的文件名为平台EDR平台下载的安装文件名。

```
@echo off

rem 设置共享路径名和执行文件名
set "Route=\\10.12_ _ _1\netlogon"
set "EDR_EXE=edr_installer_10.122.__.__3.exe"


rem  不可修改
set "ProcessFlag=edr_monitor.exe"
tasklist | findstr /IM %ProcessFlag%
if %errorlevel% == 0 (
    exit /b 0
)

rem copy  /Y "%Route%\%EDR_EXE%"  %windir%\Temp\

start /MIN "" %Route%\%EDR_EXE% -Silence=Y
if %errorlevel% == 0 (
    echo >%windir%\Temp\flag.log
    exit /b 0
)

exit /b 0
```

2. 将“edr.bat”脚本与安装包放到域共享目录下，共享目录为 “\\域控制器IP\netlogon”。（安装包命名格式为edr_installer_EDR管理平台IP_443.exe，安装文件是从管理平台下载的安装包，只需要将安装包命名中的IP改为客户的EDR管理平台IP即可）

3. 选中需要推送安装Agent的域控账户，[右键属性/配置文件/登录脚本处填写“edr.bat”]，点击<确定>，如下图。



⚠ 注意

如域用户本身已有一个登录脚本，只需在基础登录脚本文件最末尾加以下语句即可:\\域控制器 IP\netlogon\edr.bat，其中域控制器 IP 填写客户真实的 IP。

4. 当域用户重启电脑后，会执行安装脚本，静默安装Agent。

2.3.1.5. 虚拟机模板部署

虚拟机模板部署适用于客户桌面办公环境为虚拟化环境的场景，管理员在虚拟化平台上通过模板更新等功能，可快速将Agent组件批量部署到终端。部署流程如下（以aDesk平台为例）：

1. 将下载完成的Agent组件导入虚拟机模板；
2. 在虚拟机中完成Agent组件安装；
3. 配置模板更新策略进行立即/定时更新，实现Agent组件批量部署。

2.3.1.6. 桌管软件分发部署

桌管软件分发部署适用于客户桌面办公环境具有桌管或类似软件场景，可以通过桌管软件统一对终端进行Agent组件分发与安装，实现批量部署。具体操作步骤请咨询桌管软件厂商进行协助。

2.3.2. Linux 服务器系统部署

针对Linux服务器系统，EDR可实现下载安装包部署及shell脚本部署2种部署方式，可依客户侧部署场景不同，可针对性使用推荐的部署模式，场景与部署模式推荐如下。

表4 场景与部署模式推荐

场景	推荐部署模式
Linux 服务器数量小	下载安装包部署
Linux 服务器数量大	脚本部署

2.3.2.1. 下载安装包部署

下载安装包部署，支持管理员在EDR管理平台本地下载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；或直接在终端通过wget方式进行远程下载与安装。wget部署流程如下：

1. 在Linux主机上执行如下命令，直接下载安装脚本：“wget --no-check-certificate https://Manager_IP/html/linux_edr_installer.tar.gz”，其中Manager_IP为管理平台的实际IP地址，如下图。

2. 执行命令："tar -xzvf linux_edr_installer.tar.gz"，进行文件解压。

3. 定位至解压目录，执行如下命令进行安装："./agent_installer.sh"，默认安装路径为/tmp/EDR/agent。

> 说明：
>
> 1../agent_installer.sh 管理平台 IP 安装路径，可以指定 Agent 客户端安装路径。
>
> 2.安装过程中如果出现询问是否安装 ipset，可以选择 y 或 n，推荐选择 y 安装 ipset 再安装 Agent 客户端。

2.3.2.2. 脚本部署

方案介绍

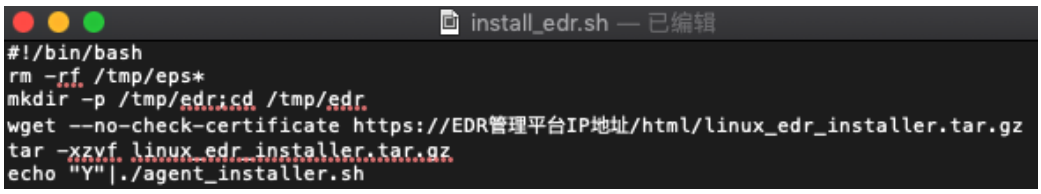
通过下发执行shell脚本自动下载安装包安装。

前置条件

Linux操作系统在支持的范围，参考"准备工作"章节。

配置步骤

1. 按下图编写shell脚本"stall_edr.sh"。



2. 将修改后的脚本上传至linux服务器，执行脚本开始自动下载并安装agent（如果客户有linux服务器集中管理软件，可由管理软件统一上传安装脚本，并执行）。

2.3.3. 终端组件（Agent）卸载

2.3.3.1. 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]，卸载程序或在控制面板进行卸载。

📖 说明：

也支持安装目录下，直接运行 uninstall.bat 卸载。

2.3.3.2. Linux 系统卸载 Agent

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

```
root@edr-debian78-x64:~# /Sangfor/EDR/agent/bin/eps_uninstall.sh
start uninstall eps agent
agent:1525000043 uninstall, send msg to mgr
1525000043 send uninstall msg success
edr stop success
Do you want to restore the iptables rules before you install AGNT?(Y/N)y
 begin to restore_iptables
edr agent uninstall success!!

**************************************************
*                                                *
*  [Warning] Please reboot your server now.      *
*                                                *
**************************************************
```

2.3.3.3. 管理平台卸载 Agent

1. 在管理平台上，[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。

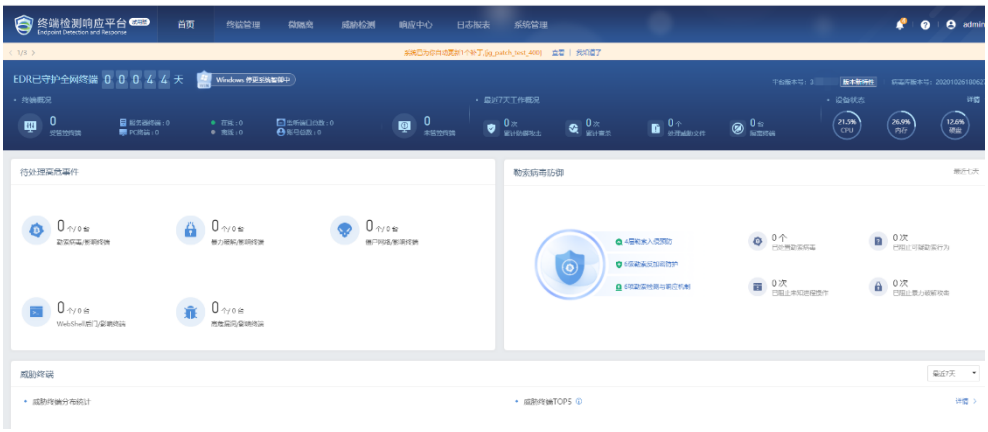
3. 管理平台使用

3.1. 管理平台登录

为保障安全性，EDR管理平台登录请参考“天翼云安全专区安全管理中心使用手册”

3.2. 首页展示

EDR首页可为管理员展示平台及终端整体运行状态，包括终端概况、待处理高危事件、勒索病毒防护、威胁终端、风险事件、全球热点威胁、联动响应等模块，如下图所示。



终端概况

在终端概况模块，可查看受控终端（涵盖PC终端与服务器终端）总数、在线状态、账号总数、监听端口总数以及未管控终端总数。

同时，针对平台探测到的为管控终端数量也会进行显示。管理员点击<受控制终端或数量>，可跳转至“终端分组管理”页签下，查看终端名称、终端状态、IP地址、操作系统等详细信息，如下图所示。

点击<监听端口总数>，可跳转至“监听端口”页签下，查看端口号、端口协议等详细信息；

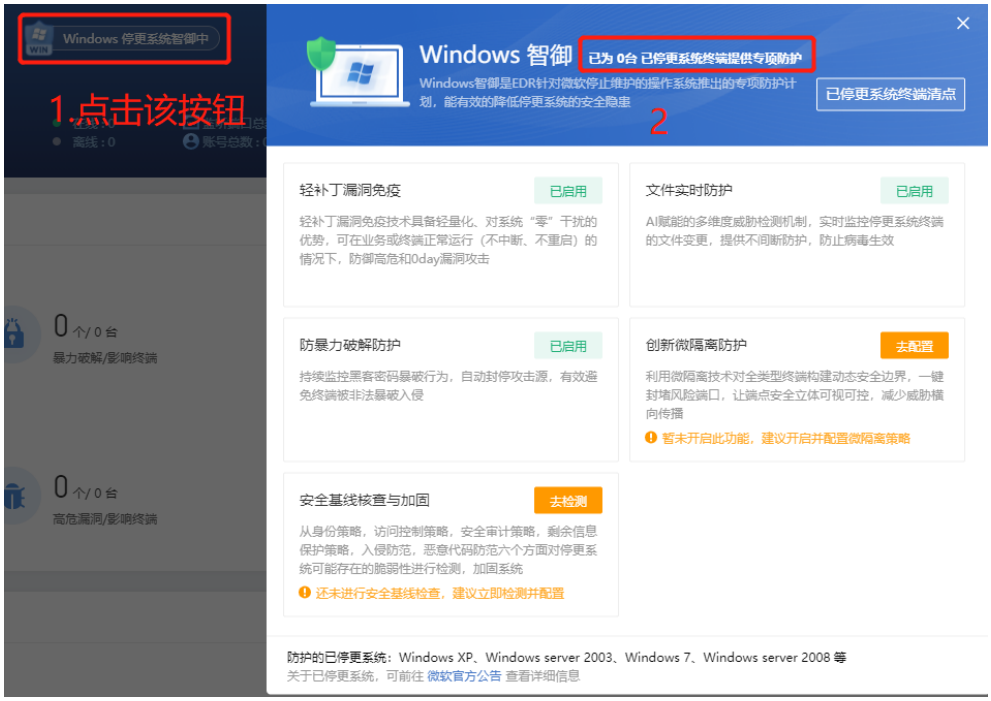
点击<账号总数>，可跳转“终端账户”页签下，可查看账户名称、终端名称、IP地址、账户风险等详细信息，如下图所示；

点击<未管控终端/数量>，可跳转至“终端发现”页签下，可查看终端IP地址、操作系统、发现时间等详细信息，如下图所示。

Windows智御

Windows智御是EDR针对微软停止维护的操作系统推出的专项防护计划，通过构建0day漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能，并结合人工智能引擎发现潜伏的未知威胁，为Windows已停更的系统提供专项防护和加固。

1. 在首页点击<windows停更系统智御中>按钮，可以查看当前已经停止维护的终端数及对应终端的防护情况，如下图所示。



2. 点击<已停更系统终端清点>按钮跳转到“终端清点”页面，支持通过系统类型（windows/linux系统）对微软已停更系统进行过滤筛选，同时也支持按“操作系统或版本号”进行搜索，查看该系统中终端数量等详情，方便运维人员明确当前终端情况并作出对应的处理，如操作系统升级或更换，终端迭代等。

3. 可以查看当前防护措施的状态（开启或需要配置），如轻补丁漏洞免疫、文件实时防护、防暴力破解防护、创新微隔离防护及安全基线核查与加固。

- 轻补丁漏洞免疫：轻补丁漏洞免疫技术具备轻量化、对系统“零”干扰的优势，可在业务或终端正常运行（不中断、不重启）的情况下，防御高危和 0day 漏洞攻击，点击<已启用>按钮，可跳转至“漏洞防护”页面查看详情以及关闭该功能。
- 文件实时防护：AI 赋能的多维度威胁检测机制，实时监控停更系统终端的文件变更，提供不间断防护，防止病毒生效。点击<已启用>按钮，可跳转至“实时防护”页面查看详情以及关闭该功能。

- 防暴力破解防护：持续监控黑客密码爆破行为，自动封停攻击源，有效避免终端被非法暴破入侵。点击<已启用>按钮，可跳转至“实时防护”页面查看详情以及关闭该功能。
- 创新微隔离防护：利用微隔离技术对全类型终端构建动态安全边界，一键封堵风险端口，让端点安全立体可视可控，减少威胁横向传播。点击<去配置>，可跳转至“微隔离策略”页面，打开“策略生效开关”，新增微隔离策略等操作。
- 安全基线核查与加固：从身份策略，访问控制策略，安全审计策略，剩余信息保护策略，入侵防范，恶意代码防范六个方面对停更系统可能存在的脆弱性进行检测，加固系统。点击<去检测>按钮，可跳转至“终端基线检查”页面，点击<立即检测>的按钮，可以开始终端基线的检查。

版本新特性

版本新特性主要是对版本新增特性的描述，在[首页]的页面下，点击<版本新特性>按钮，可以查看详细信息。

横幅提醒

1. 等保提醒

当不符合等保的需求时，如admin账户没有禁用或者重命名的时候，会有对应的横幅提醒，如下图所示。

点击<去配置>的按钮，可以跳转至“帐号管理”页面，使用安全管理员账户对admin默

认账户进行重命名或禁用，同时也支持编辑账号权限等操作，合理分配权限，避免因权限问题导致的信息泄漏问题。

2. 补丁更新提醒

登录控制台，当系统检测到有补丁需要更新，或系统已完成补丁的自动更新，会有横幅提醒，如下图所示。

点击<查看>的按钮，可跳转“平台补丁更新”页面，查看该补丁的详细信息，如补丁描述、重要级别、是否重启服务以及更新时间等。

3. 端口修改提醒

当检测到系统中有容易被暴力破解或攻击的端口，系统会提醒修改端口，如下图所示。

点击<前往修改>的按钮，可跳转至“高级设置”，修改相应的端口号，避免因暴力破解导致病毒感染等情况，保障系统安全。

最近7天工作概况

在最近7天工作概况模块，可展示最近7天内的累计防御攻击总数、累计查杀总数、处置威胁问价总数以及隔离终端总数，如下图所示。

其中：

- **累计防御攻击**：所有处理的威胁事件数；
- **累计查杀**：页面下发的杀毒任务次数；
- **处理威胁文件**：总处理威胁文件量，包括病毒查杀、webshell 及僵尸网络；
- **隔离终端**：通过响应中心隔离的终端数量。

设备状态

在设备状态模块中，可以查看管理平台的CPU、内存以及硬盘的使用情况，点击<详情>，可查看实时、最近24小时以及最近30天的CPU及内存的使用详情，如下图所示。

待处理高危事件

在待处理高危事件模块，可展示勒索病毒、暴力破解、僵尸网络、WebShell后门、高危漏洞等未处理的安全事件数量以及对应受影响的终端数量，点击[安全事件或数量]，可跳转至[响应中心/威胁响应]页签下，查看对应安全事件的详细信息及处置状况，以“暴力破解/影响终端”为例，如下图所示。

勒索病毒防御

在勒索病毒防御模块下，可展示已处置勒索病毒和已阻止的可疑勒索行为、未知进程操作以及暴力破解攻击的数量，如下图所示。

其中：

- **已处置勒索病毒数量**：管理员或平台处置勒索病毒数量；
- **已阻止可疑勒索行为**：平台通过勒索诱饵实时防护监测并阻止的可疑勒索行为次数；
- **已阻止未知进程操作**：平台监测并阻止的非白名单进程对防护目录的操作行为或者运行行为次数；
- **已阻止暴力破解攻击**：平台阻止的暴力破解攻击行为次数。

勒索病毒防御主要由4层勒索入侵防御、5级勒索反加密防护和6项勒索检测与响应机制组成。

1. **4层勒索入侵防护**，如下图所示。

- **漏洞检测及补丁修复：**一键检测和修复勒索病毒常利用的系统漏洞，如永恒之蓝漏洞，避免勒索病毒利用漏洞传播或发起攻击；点击<去修复>，可跳转至[威胁检测/终端漏洞查补]，查看扫描状态、漏洞数量等详细信息与处置状态。
- **安全基线检查：**通过身份鉴别策略、访问控制策略、安全审计策略、剩余信息保护策略、入侵防范、恶意代码防范六方面进行安全合规性检测，提前识别终端脆弱点；点击[去查看]，可跳转至[威胁检测/终端基线检查]，查看终端基线检查详情。
- **SAVE 人工智能引擎：**基于人工智能技术的 SAVE 引擎，具有强泛化能力，能预测变种攻击，及时分析并设计解决方案，防范未知的勒索病毒。
- **微隔离：**应用创新微隔离技术的动态防护体系，动态构筑安全边界，有效应对勒索病毒的横向传播，将病毒遏制在指定范围之内。

2. **5级勒索反加密防护，**如下图所示。

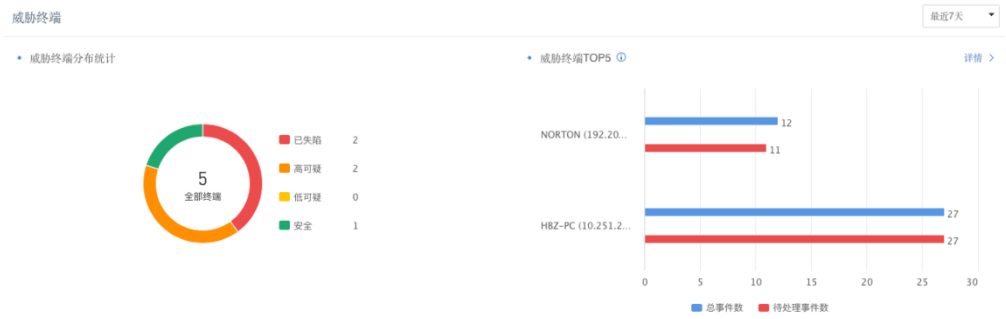
- **文件实时防护（主动防御）：**通过对终端上新增或变更文件/进程进行实时检测，预防诱导如钓鱼攻击、鱼叉攻击等传播的勒索病毒进入本地。
- **勒索诱饵防护（主动防御）：**针对勒索病毒的加密特点，在终端关键目录放置诱饵文件，通过加密诱饵文件的进程回溯病毒文件并进行查杀，阻止勒索病毒的进一步加密和扩散。
- **防暴力破解防护（主动防御）：**持续监控密码暴破行为，如发现非法人员进行密码暴破，自动封停攻击源 IP，有效避免终端被非法暴破成功。
- **系统的可信进程防护（服务器加固）：**在相对稳定、固定业务的服务器中，通过配置允许运行的白名单进程，使勒索病毒进程在执行前就被阻止，阻止未知勒索病毒等威胁对重要资产的影响。
- **目录的可信进程防护（服务器加固）：**对重要目录进行权限控制，仅允许配置的白名单进程操作目录，避免重要文件或目录被勒索病毒等进行非法篡改/获取。

3. **6项勒索检测与响应机制，**如下图所示。

- **勒索病毒检测与查杀：**多维度、轻量级漏斗型检测框架，包含基因特征检测引擎、AI 技术 SAVE 引擎、云查引擎等 5 大引擎。通过层层过滤，检测更准确、更高效。
- **一键终端隔离：**当一台终端发生勒索威胁时，可通过便捷的一键终端隔离，阻止感染终端持续向外扩散。
- **网端云联动：**与云、网端设备联动，形成涵盖云、边界、端点上中下立体防御架构，内外部威胁情报可实时共享，在第一时间发现潜在勒索威胁，并协同响应。
- **全网威胁定位：**根据 IOC 情报数据快速进行全网威胁定位分析，及时发现和响应最新的热点事件，可实现快速定位网内威胁终端、同步处理、快速清除威胁等效果。
- **已知解密工具：**除勒索病毒家族的分析报告和处置建议外，还提供 GandCrab、CryptON、Planetary 等勒索病毒解密工具或方法，解密勒索病毒数量将持续增加。
- **威胁分析百科：**威胁情报中心提供病毒详细的静态、动态行为分析和威胁报告，以及病毒的影响范围、针对性的攻击事件等相关威胁内容。

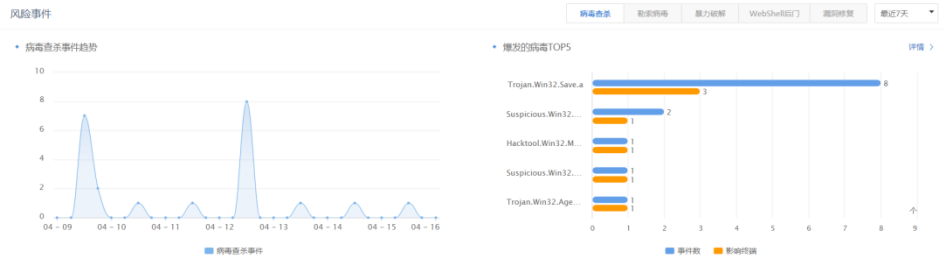
威胁终端

在威胁终端版块，主要包括威胁终端分布统计与威胁终端TOP5两大图表。**威胁终端分布统计**中可查看风险终端已失陷、高可疑、低可疑和安全的终端数量情况，点击后可以自动跳转到[响应中心]中的[威胁响应]并完成了筛选；**威胁终端TOP5**列出终端发现的问题总数与待处理事件数最多的top5，可点击<详情>跳转到[响应中心]中的[威胁响应]中，如下图所示。



风险事件

在风险事件版块，主要包括病毒查杀事件趋势及爆发的病毒TOP5两大图表，如下图所示。



- **病毒查杀事件趋势：**可统计最近 7 天、最近 30 天、最近 90 天内发现的病毒事件数量，包括勒索病毒事件、木马病毒事件和其他病毒事件等。
- **爆发的病毒 TOP5：**列出终端上出现最多的 5 种病毒，可点击右上角<详情>进行查看，同时在右上角可选查[**病毒查杀**]、[**勒索病毒**]、[**暴力破解**]、[**webshell 后门**]、[**漏洞修复**]对应的情况，并可以选择数据统计天数。

全球热点威胁

在全球热点威胁模块，可显示全球最热点、威胁最大的安全事件及其在网内终端的爆发情况，如下图所示。

联动响应

EDR可以与的安全感知平台（SIP）、下一代防火墙（AF）、上网行为管理（AC）、云图（X-Central）、运营中心（SOC）进行联动，在本联动响应模块，可展示最近7天、最近30天及最近3个月的EDR与各产品联动状态，以及联动下发的策略，如下图所示。

3.3. 终端管理

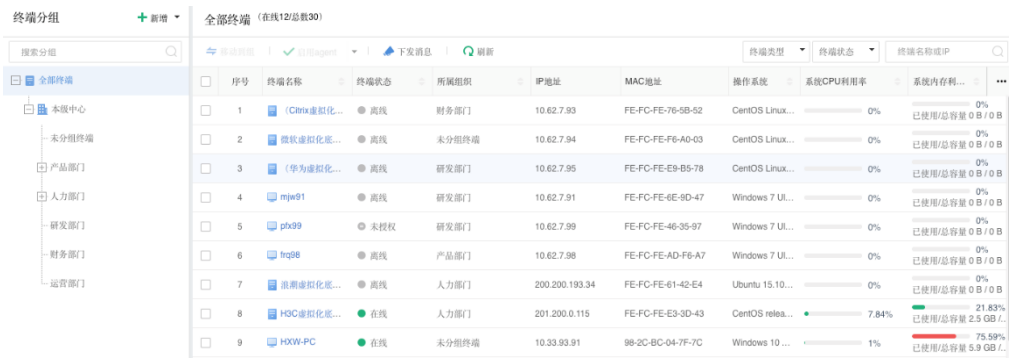
通过EDR终端管理页面，可实现对终端的发现、清点及分组管理，同时可对终端分组进行基本策略、病毒查杀、实施防护、安全加固、信任名单及漏洞修复等内容进行策略配置。

3.3.1. 终端分组管理

终端分组管理模块通过树形分组形式对接入终端进行统一管理。

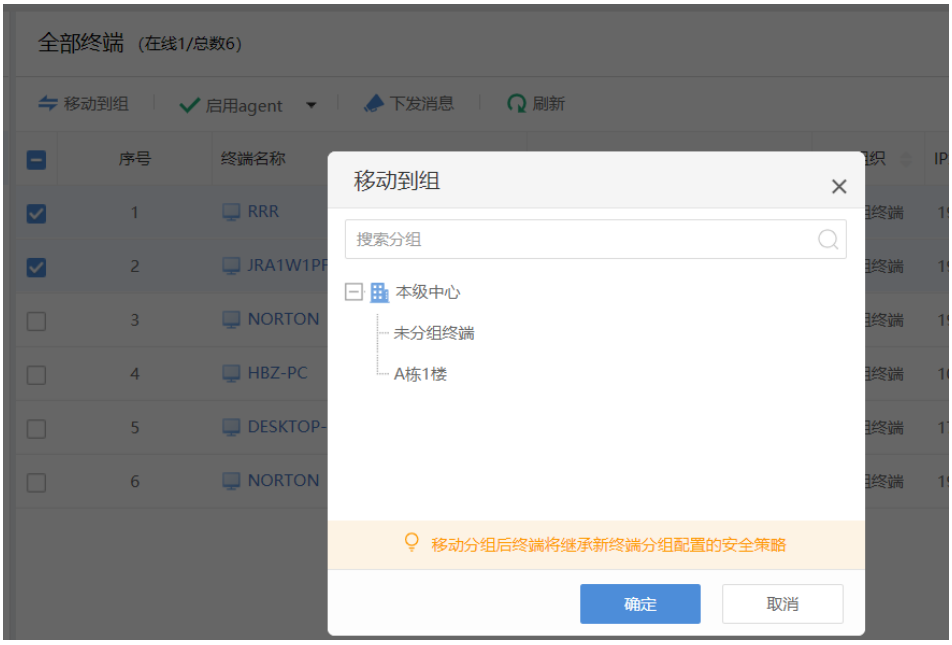
1. 终端信息展示

终端信息展示集中显示终端名称、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。管理员可在右侧[...]处进行显示项筛选与指定。



2. 终端管理

终端管理对选中的终端，可以移动不同的分组，如下图所示。



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。

3.3.1.1. 终端分组新建

当终端Agent安装完成后，终端会自动上线至[终端分组管理]的[未分组终端]一栏，管理员可依业务情况对未分组终端进行分组管理。终端分组支持手动分组、自动分组及通过xls/xlsx导入导出分组等方式进行分组创建操作。

手动分组

手动分组即新建分组后，通过人工筛选相应终端进行移入，具体操作步骤如下：

1. 在[终端管理/端分组管理]页面，点击<新增>；
2. 在弹出的[新增组]的页面，填写[分组名称]及[上级分组]字段，[应用自动分组]功能不开启，点击<确定>；
3. 在[未分组终端]分组中选中需移入的终端，并选择[移动到组]，在弹出页面中选中需要移入的分组名称，并点击<确定>即可。

> 说明：
> 移动分组后，终端将继承新终端分组配置的安全策略。

自动分组

自动分组即新增分组时，可指定IP/IP段，在分组创建成功后，系统会自动将指定IP/IP段对应的终端移入至该分组，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>新增；
2. 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>；
3. 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。

导入与导出分组

导入导出分组即通过编辑好的xls、xlsx进行批量用户导入并可对已有分组进行xlsx格

式的分组导出，具体操作步骤如下：

导入分组

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/终端；
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。

自动分组管理

自动分组管理模块可对自动分组策略进行统一的新建与管理，具体操作如下：

新增与删除自动分组策略

1. 在[终端管理/终端分组管理]页面，点击<新增>自动分组管理；

2. 在弹出页面点击<新增>，并对[选择分组/启用自动分组/自动分组IP/IP段]进行编辑，然后点击<确定>即可；

3. 在自动分组管理界面，选中对应分组策略，在[操作]一栏，点击<删除>，即可完成自动分组策略的删除。

📖 **说明：**

删除后，该分组下的终端自动分组功能将关闭。

编辑自动分组

1. 在[终端管理/终端分组管理]页面，点击<新增>自动分组管理；

2. 在弹出页面选中对应分组策略，在[操作]一栏，点击<编辑>，即可针对该自动分组策略进行编辑。

📖 **说明：**

自动分组策略编辑需在分组策略状态为[启用]时才支持对 IP/IP 段进行编辑。

启用与禁用自动分组

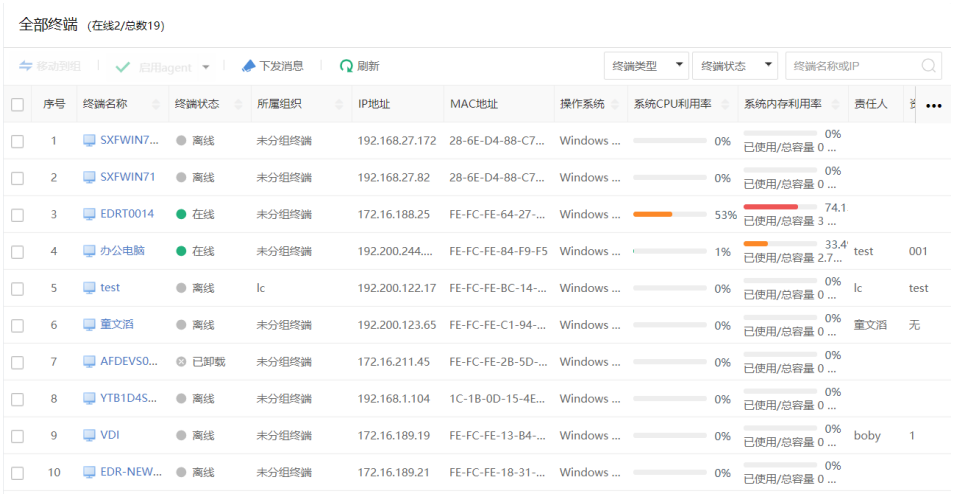
自动分组策略可依业务情况进行启用/禁用的灵活调整，具体操作步骤如下：

1. 在[终端管理/终端分组管理]页面，点击<新增>自动分组管理；

2. 在弹出页面选中对应分组策略，在[状态]一栏，点击<启用/禁用>图标，即可进行切换，或在编辑界面进行切换。

3.3.1.2. 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。

详细信息分类如下：

终端信息

1. 基础信息

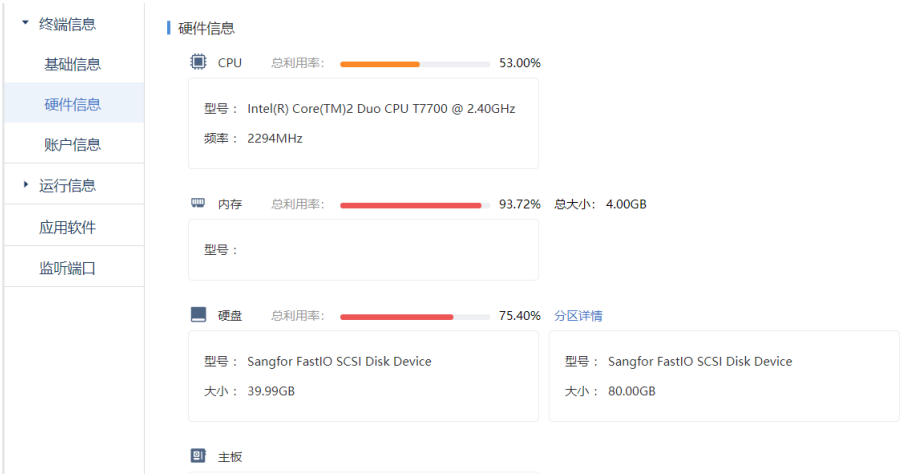
基本信息：终端名称（支持编辑）、计算机名、IPV4/MAC地址、所属分组、终端agent版本、病毒库版本、最近接入/登录时间、最近登录用户名等信息；

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：

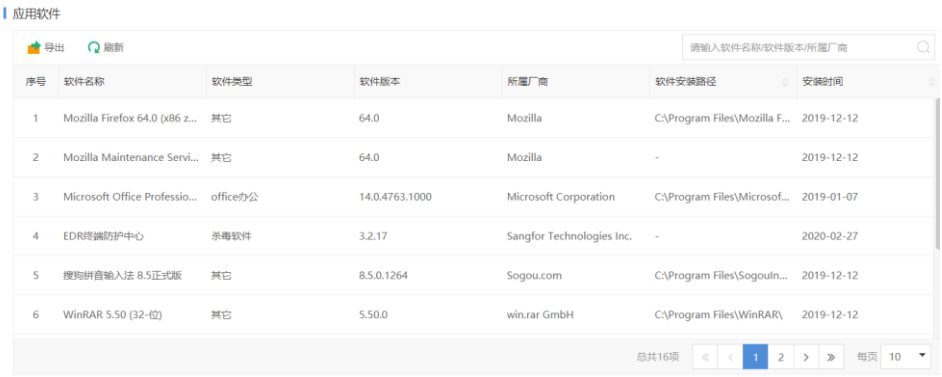
点击右侧[…]可进行显示项筛选与指定。

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。

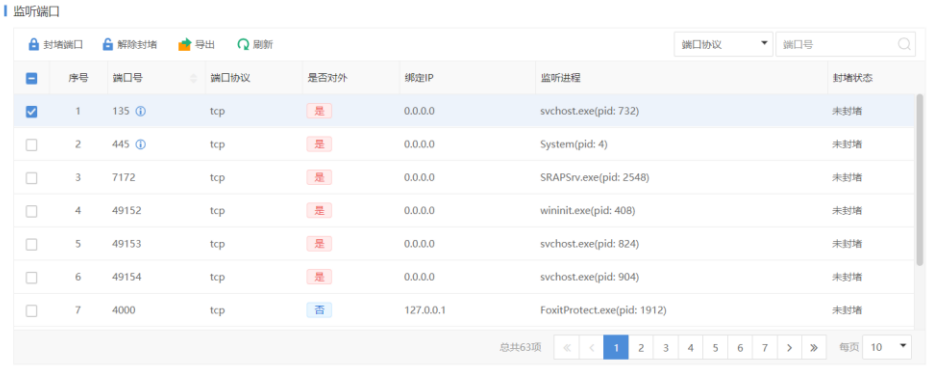
应用软件

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。



监听端口

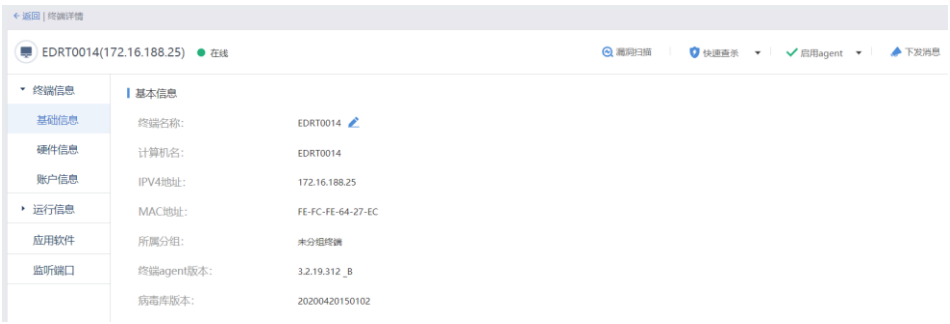
可显示本终端监听端口的端口号、协议、绑定IP、监听进程、是否对外及封堵状态，可选中相应端口进行封堵/解封，以及实现导出与通过端口协议及端口号进行检索。



3.3.1.3. 终端远程管理

指令下发

当点击在线状态的终端名称进入详情界面后，可通过平台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，如下图所示。



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。

> 说明：
>
> 在全部终端页面也可选中多终端设备，进行 agent 启用、禁用等操作；
>
> 当需要释放授权数量，需要先将终端 agent 卸载，同时从管理端移除已卸载的终端。

消息下发

在全部终端页面，可以勾选单台或多台终端，对安装了客户端的windows终端进行消息提示，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。

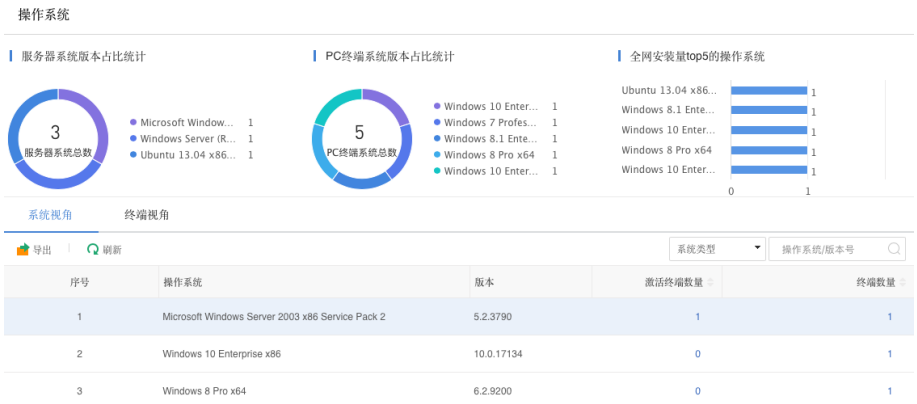
2. 完成信息编辑后点击<确认>，选中终端将会接收到相应通知，如下图所示。

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。

3.3.2. 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。

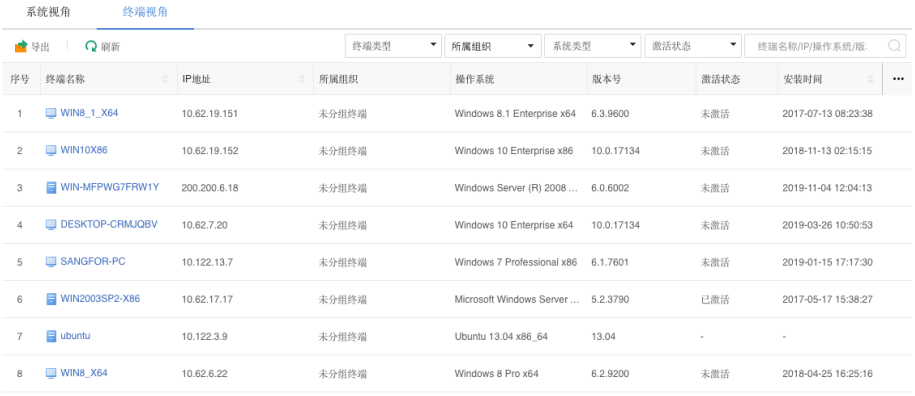
操作系统清点



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。

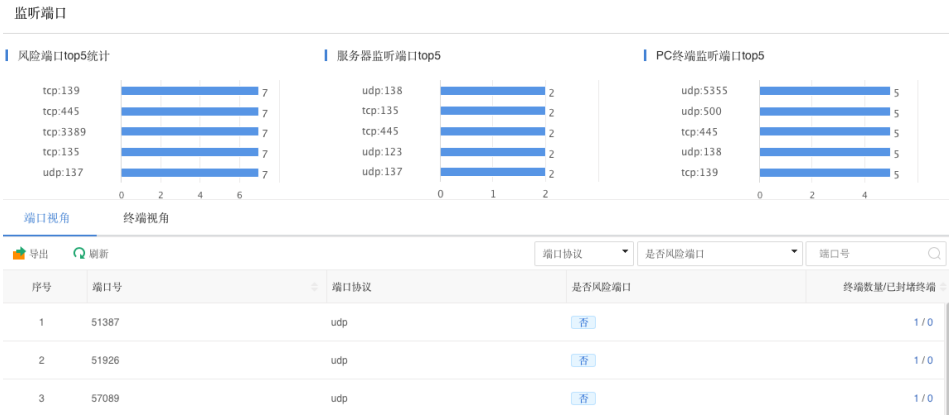
应用软件清点

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. 可根据终端识别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：

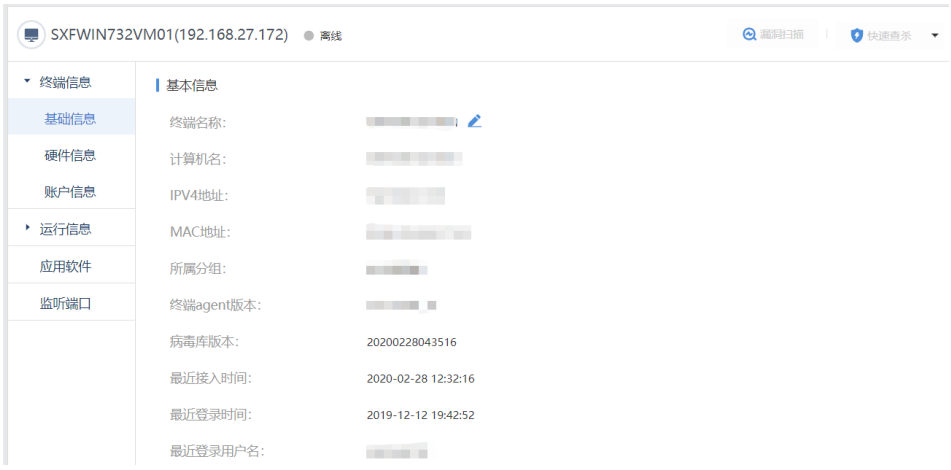
1. 可展示风险端口TOP5、服务器/PC监听端口TOP5。
2. 可通过端口视角查看开放某一端口的终端数量，点击[终端数量/已封堵终端]这列的数字，可跳转至开放该端口的终端详情页面进一步分析，如下图所示。

> 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。

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。



3.3.3. 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管理平台发起扫描，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>。

3.3.4. 策略中心

策略中心功能，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、安全加固、信任名单和漏洞修复六种安全策略。

3.3.4.1. 基本策略

通过基本策略，可对Windows系统终端的资产信息登记、管理员联系方式、弹出提醒、密码保护等策略进行配置，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。

终端登记页面如下图所示。

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，策略以管理平台为准，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

防护中心密码保护设置后，终端Agent退出或卸载时需要输入密码，可针对[防退出]及[防卸载]密码保护分别配置，如下图所示。

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。

3.3.4.2. 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，可定义扫描文件条件、恶意文件处置机制以及设置扫描引擎，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，策略以管理平台为准，如解除锁定，则客户端可自行变更此配置。

扫描文件：可配置扫描文件大小限制及扫描压缩包层级。

发现恶意文件：当发现恶意文件的处置机制，包括标准处置、严格处理和仅上报不处

置三种处理方法，默认配置是标准处置。

- **标准处置：**针对恶意文件，归属在黑名单库的恶意文件进行隔离处理，不在黑名单库中的威胁文件不隔离，仅上报检测日志；
- **严格处理：**EDR 检测的所有威胁文件均隔离处理；
- **仅上报，不处置：**所有威胁文件仅上报安全日志，不进行隔离，适用于有人值守且用户了解如何处置病毒场景。

扫描引擎：病毒查杀共用到四种引擎，包括SAVE人工智能引擎、云查引擎、基因特征引擎和行为分析引擎。其中：

- SAVE 人工智能引擎和云查引擎默认开启，且不能关闭；
- 基因特征引擎和行为分析引擎可选开启；
- 启用更多引擎，可提高病毒检出率，但同时会加大对系统性能的影响。

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。

高级设置（仅支持windows系统终端）

在高级设置中，可开启“高启发式扫描”，此扫描模式调高了对病毒威胁检测的AI计算敏感度和引擎分析的启发式级别，可大幅度提高整体威胁检出率，但也会引入轻微误判，需要在服务提供商分析后再决定是否启用。

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。

3.3.4.3. 实时防护

通过实时防护策略，可针对Windows终端进行文件实时防护、勒索病毒防护、WebShell检测、暴力破解检测和高级威胁防护策略配置，针对Linux终端进行WebShell检测和

暴力破解检测策略配置。

> 说明：
>
> 点击右侧 图标可以点亮小锁，终端文件实时监控策略从管理端统一下发、终端无法单独配置，默认是允许终端配置文件实时监控策略。

文件实时防护（仅支持Windows）

开启文件实时防护可对终端文件系统实现实时性防护，策略配置如下。

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：可多选指定需要监控的文件类型；

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）；

扫描引擎：扫描引擎设置文件实时监控引擎，文件实时监控共用到3种引擎。其中云查引擎默认开启，且不能关闭，SAVE人工智能引擎和基因特征引擎可选开启，需要注

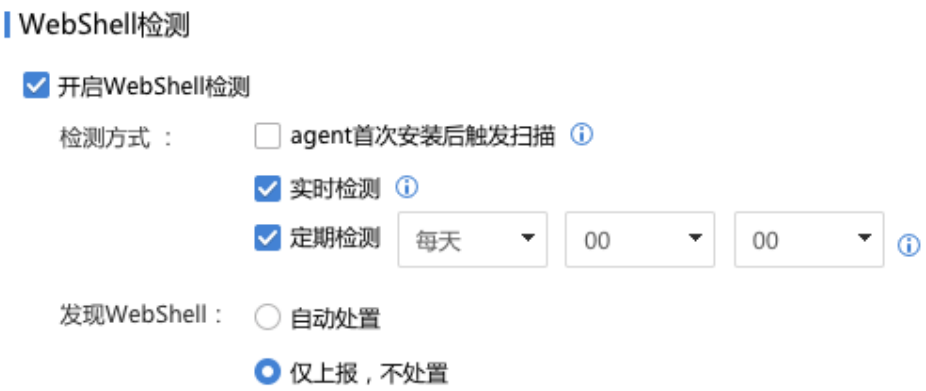
意启用更多引擎，可提高病毒检出率，但同时会加大对系统性能的影响;

发现恶意文件：当发现恶意文件的处置机制，包括标准处置、严格处理和仅上报不处置三种处理方法，默认配置是标准处置。

- 标准处置：针对恶意文件，归属在黑名单库的恶意文件进行隔离处理，不在黑名单库中的威胁文件不隔离，仅上报检测日志；
- 严格处理：EDR 检测的所有威胁文件均隔离处理；
- 仅上报，不处置：所有威胁文件仅上报安全日志，不进行隔离，适用于有人值守且用户了解如何处置病毒场景。

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，可检测Web服务器根目录及其子目录下的WebShell后门。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。

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。

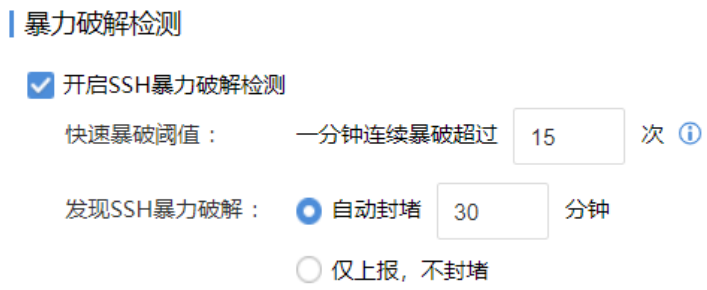
Windows系统侧配置界面如下图所示。

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。

Linux系统侧配置界面如下图所示。



其中：

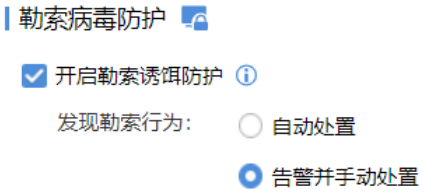
快速暴破阈值：可定义单分钟内联系爆破超过几次就定义为快速暴破，SSH快速暴破

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。

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。



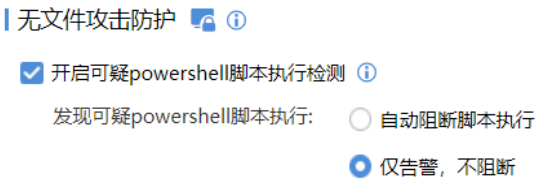
其中：

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。

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。

3.3.4.4. 安全加固

安全加固可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。

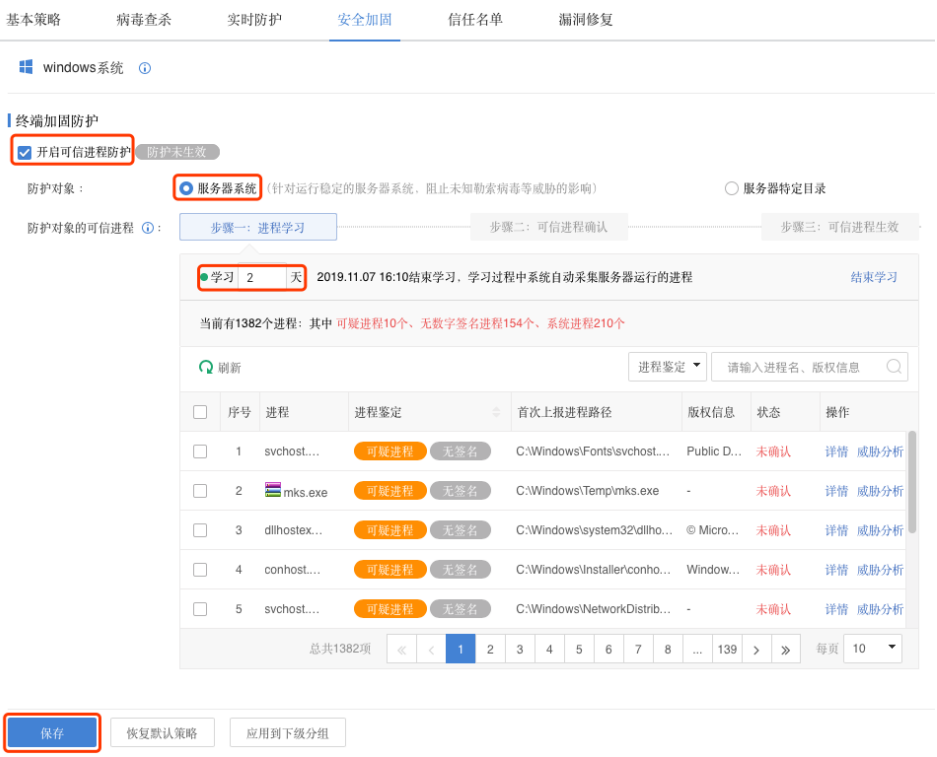
配置步骤：

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

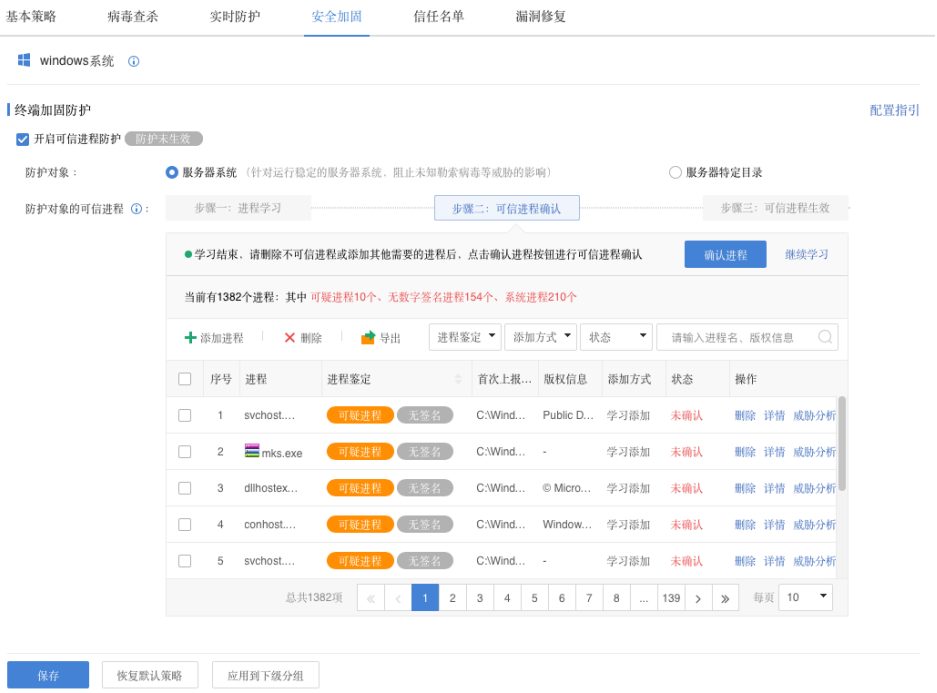
启用[可信进程防护]，防护对象选择[服务器系统]，设置进程学习，学习时间范围从1天到30天可配，点击<保存>，如下图所示。



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. 如果无法确认当前进程是否可信进程，可以点击[威胁分析]，借助威胁情报对当前进程进一步分析后再确认；
2. 如果发现需要添加为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，如下图所示。

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。

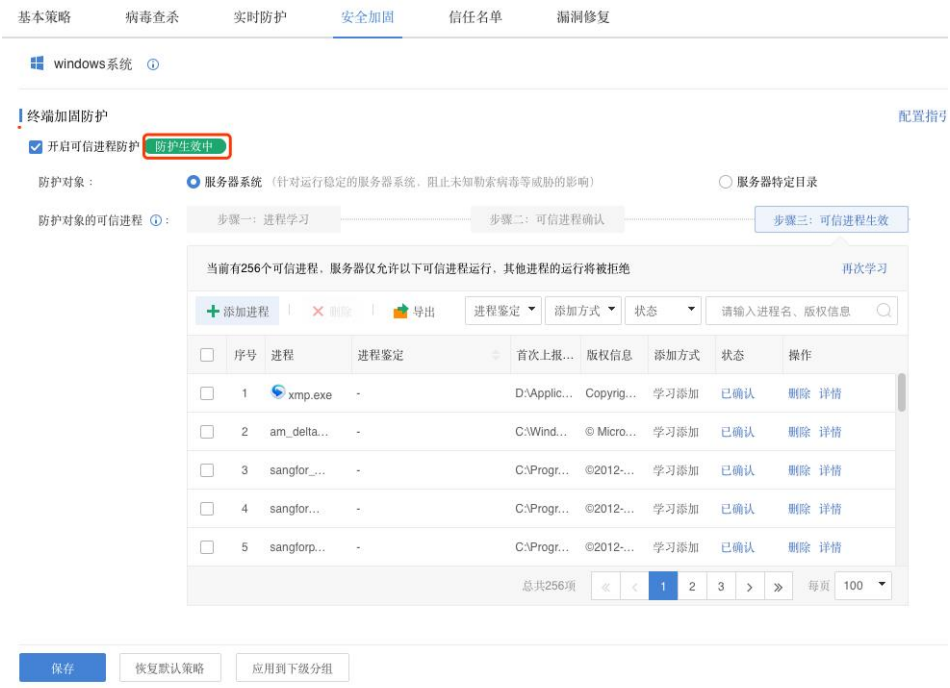
- **按模板导入：**适用于客户需要加固的服务器是模板中提供的 web 服务器或数据库服务器；
- **上传进程文件：**上传服务器中可信的进程文件实现添加；

- **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。

开启远程登录保护

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。

勾选“开启远程登录保护”，EDR将默认对敏感时间内的RDP远程登录要求用户进行二次密码验证。

> 说明：
>
> 本功能仅支持 windows Server 操作系统主机。

1. 自定义远程敏感时间段

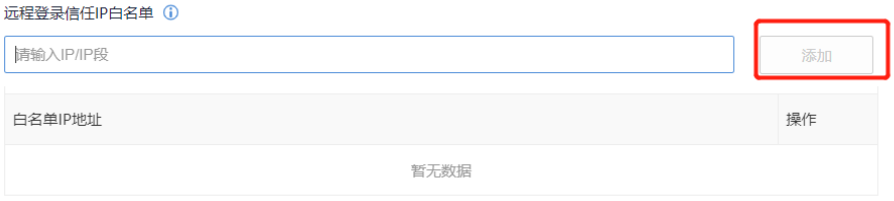
   点击<添加>按钮，可以自定义添加远程敏感时间段；点击<删除>按钮，可以对时间段进行删除。

2. 修改远程登录的二次验证密码

   针对非信任名单的IP，输入二次验证密码成功后，才能进行访问。当修改密码时，建议尽快告知企业内相关人员二次验证的密码，避免敏感时间段无法远程访问服务器。

3. 设置远程登录信息IP白名单

   白名单内的IP在敏感时间段进行RDP远程登录时不需要输入二次验证密码。



3.3.4.5. 信任名单

信任名单支持配置文件/目录白名单（仅支持windows系统）及防暴力破解IP白名单配置，加入信任名单中的文件或目录，病毒查杀或实时文件监控不处理，加入防暴力破解IP白名单中的IP发起暴力破解攻击时会被放行，不告警不封堵，配置界面如下图。

其中：

- **文件/目录信任名单：**信任名单可以添加文件或目录，结尾无[\]表示文件，结尾有[\]表示目录；
- **防暴力破解 IP 白名单：**支持填写 IP/IP 段/子网，加入防暴力破解 IP 白名单中的地址发起暴力破解攻击时会被放行，不告警不封堵。

3.3.4.6. 漏洞修复

通过漏洞修复策略，可针对漏洞检测与修复进行定时执行、漏洞补丁下载服务器地址的指定以及轻补丁漏洞免疫的开启和关闭，配置界面如下图所示。

> **说明：**
>
> 本功能仅支持 windows 系统终端可以上网的场景。

“零”干扰漏洞免疫

“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，如实体补丁一样，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。

通过勾选“开启轻补丁漏洞免疫”，可开启或关闭该功能。

“ ”表示禁止客户端设置，策略以管理平台为准；点击该图标，“ ”则表示“允许客户端设置，策略以客户端为准”。

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 CDN 服务器、微软漏洞补丁服务器及本管理平台。

📖 **说明：**

可以通过上移或者下移调整服务器地址的顺序，终端补丁包获取依据服务器地址的顺序进行；当终端无法从内置服务器获取补丁包时，允许管理平台主动下载补丁包缓存文件。

3.3.4.7. 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，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，终端除了与管理平台通信之外，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

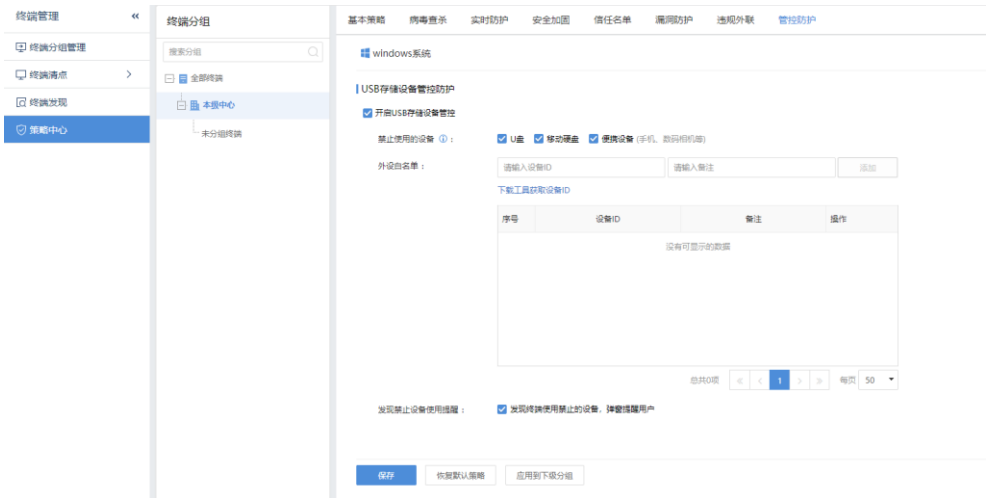
设置提醒的内容。

5. 邮件告警：当终端发生违规时，邮件告警通知管理员。

3.3.4.8. 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。USB管控可以对接入终端的移动存储设备进行有效的管控，以保障全网终端的安全。

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。

3.3.4.9. 各系统对安全策略支持情况一览表

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	√	√	×
安全加固	×	√	×
信任名单	√	√	×
漏洞修复	√	√	×
违规外联	√	√	×

管控防护	√	√	×

3.4. 微隔离

通过微隔离功能，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。

3.4.1. 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。

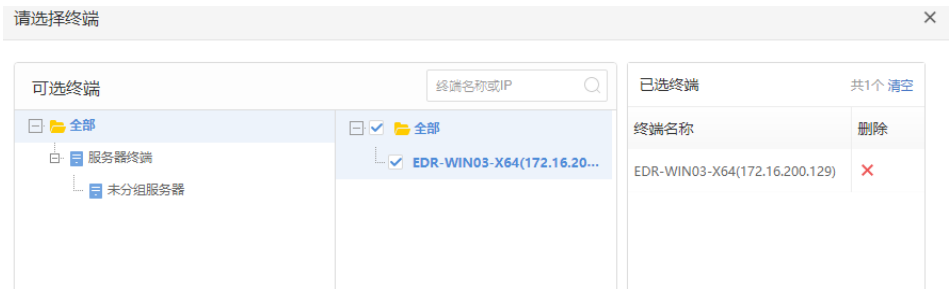
对象	业务系统	业务系统名称	终端组	包括的终端	
		所有终端-ALL	用户区1、用户区2、用户区3、服务器区1、服务器区2	pc1、pc2。。。server1、server2。。。	
	IP组	IP组名称	IP地址范围	IP组类型	
		办公终端	172.16.200.1-172.16.200.254	内网	
	服务（只需要梳理自定义策略）	服务名称	协议类型	端口	流量类型
		smb	TCP	135、136、137、139、445	业务流量
		rtp	tcp	3389	运维流量
对象间访问关系	访问关系	源	目标	服务	动作
		IP组：默认互联网	业务系统：所有终端-ALL	smb、rtp	拒绝

3.4.2. 业务系统/角色/IP 组/服务/创建

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。

3.4.3. 微隔离策略配置

微隔离策略主要通过五元组匹配数据进行放通或拒绝访问，可点击右上角[策略生效开关]进行功能全局开启或禁用，具体配置流程如下：

1. 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. 配置完成后，点击<确定>进行提交即完成策略新增，在[微隔离策略]页面可查看已有策略的详细状态信息，并可进行上移/下移、启用/禁用等操作。

3.4.4. 流量状态查看

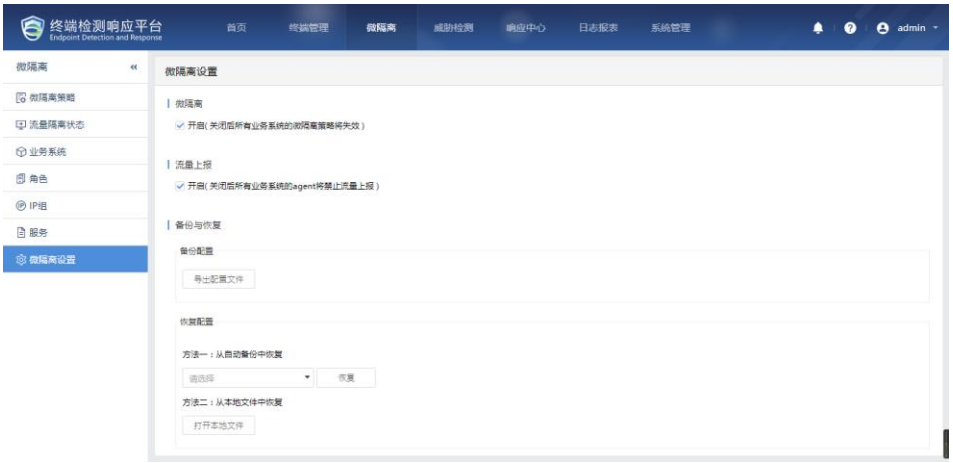
微隔离支持流量状态可视化，支持查看终端系统的流量访问情况，可以显示互联网出口、内网互访及已放通和未放通的流量访问情况，同时支持通过过滤策略进行筛选查看，界面如下图所示。

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。

3.4.5. 微隔离全局配置

微隔离全局设置包括隔离功能启用、流量上报启用以及微隔离策略的备份与恢复，配置界面如下图所示。



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；
- **备份与恢复**：可导出微隔离的配置文件，以及从导出的配置文件中进行恢复。系统每天 0 点自动进行配置备份。

3.5. 威胁检测

3.5.1. 终端病毒查杀

终端病毒查杀模块可对接入EDR管理平台的终端进行体检任务下发，通过结合本地信誉库、自研SAVE引擎、行为检测引擎、特征检测引擎、云查等多引擎对终端进行威胁文件扫描并展示查杀结果。

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

1. 点击<快速查杀/全局查杀>，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；
- **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%。

2. 配置完成后，会执行查杀任务，点击具体终端右侧的<检测详情>可查看该终端查杀进入，如下图所示。

3. 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。

4. 进行隔离等处置措施，点击威胁终端检测详情查看该终端详细的扫描结果，可点击[处置]，对病毒进行隔离等处置措施，如下图所示。

3.5.2. 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:

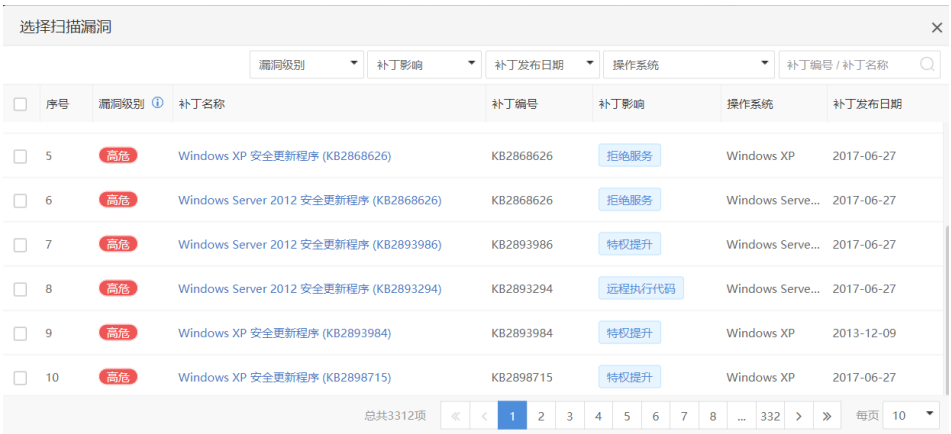
1. 在[威胁检测/终端漏洞查补]页面下，点击[添加漏洞扫描任务]，创建漏洞扫描任务，配置页面如下图所示。

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;

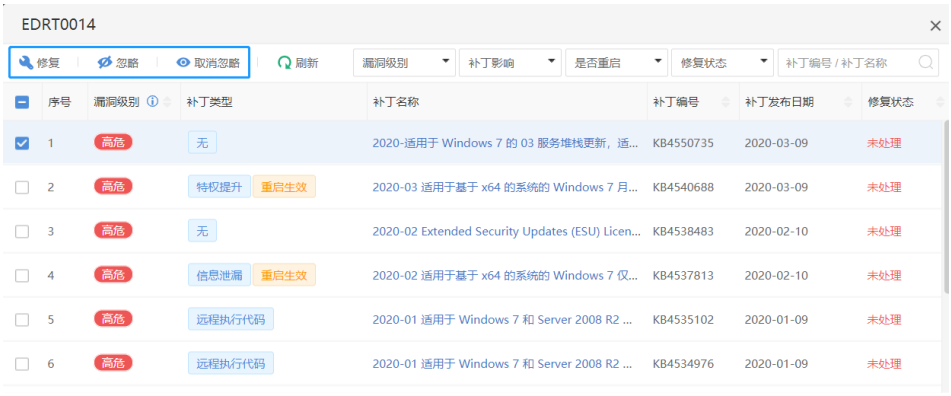
选择漏洞：包括全部漏洞、高危漏洞和自动以选择:

- **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>，如果存在需要重启才能修复生效的补丁，启动修复时会给出下图提示。在管理员允许的情况下，才可勾选[强制终端修复后立即重启生效]，避免导致终端用户数据丢失风险。一般不建议勾选此项，修复补丁后等待下班时间再重启。

📖 **说明：**

此章节提到的漏洞修复需要终端电脑可以上网，如果终端电脑无法上网，请参考："漏洞响应"章节进行漏洞修复。

3.5.3. 终端基线检查

终端合规检查模块可对终端进行合规性检查，但不同终端系统检查的内容有所差异：

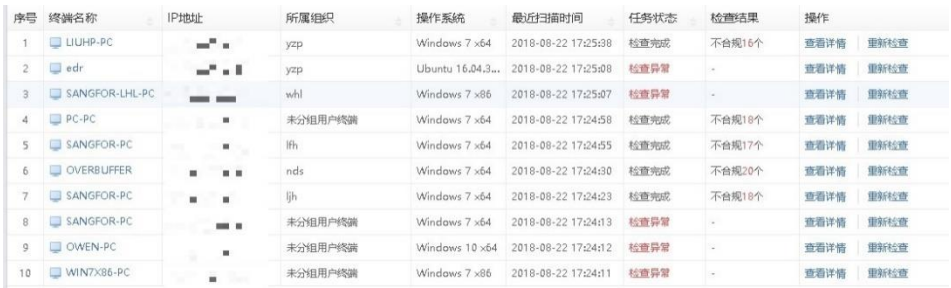
Windows终端：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范；

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。

如下图所示。

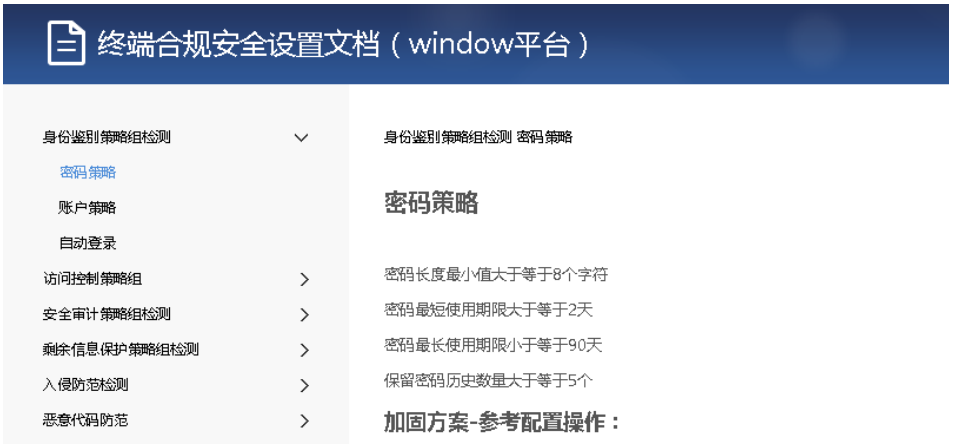
点击[立即检查]，可选择需要进行合规检查的终端下发检测命令，如下图。

完成检测后，可以查看检测的结果。



查看合规检测的结果，点击[查看详情]。

查看设置文档：可查看合规检查定义的配置要求。



按照**终端合规安全设置文档**完成配置修改后，可点击<重新检查>选择重新进行检查。

点击“”可以下载合规检查报告。

警告

合规检查中需要关注字体为橙色的项。

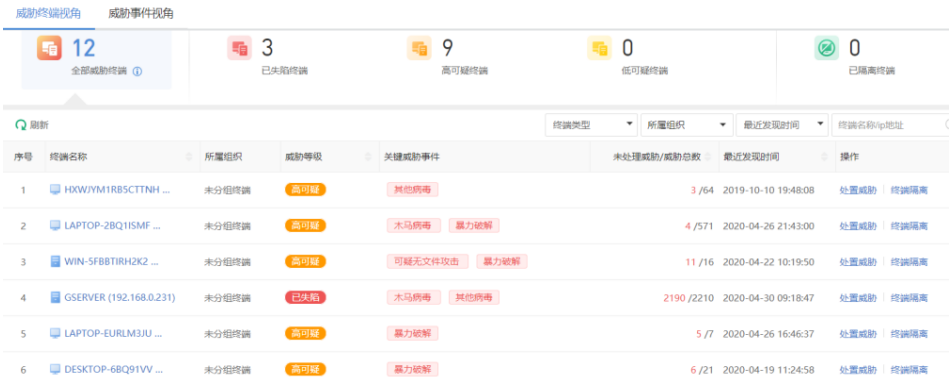
3.6. 响应中心

3.6.1. 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。同时，支持通过“终端类型”、“所属组织”、“最近发现时间”进行筛选，也可直接依据终端名称/ip地址进行检索。

3.6.1.1. 威胁终端视角

在威胁终端视角页面，可点击对应威胁终端类型，查看相应的终端名称、所属组织、威胁等级、关键威胁事件、未处理威胁/威胁总数、最近发现时间等信息并支持筛选，同时可针对威胁终端进行处置威胁/终端隔离操作，威胁终端视角页面如下图所示。



威胁等级分为已失陷、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、高威胁 Webshell 后门、高危僵尸网络这些威胁事件的终端；
- 高可疑终端：发生了高危病毒、低威胁 Webshell 后门、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、低危僵尸网络等低威胁事件的终端。

最近发现时间：最新一次发现威胁的时间。

威胁处置包括处置威胁及终端隔离两种方式。

- 终端隔离

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。

- 处置威胁

点击处置威胁，在弹出页面可勾选对应感染文件/进程进行[一键处置]、[一键信任]及[一键忽略]等操作，支持针对[威胁等级]、[威胁类型]及[发现时间]进行筛选。

一键处置可针对：

木马等恶意程序，将对文件进行删除；

感染性病毒，将进行修复来清除感染；

Powershell无文件攻击将进行阻断。

处置完成后可在各时间的已处置区域查看处置记录。

一键信任可针对：

文件加入信任区；

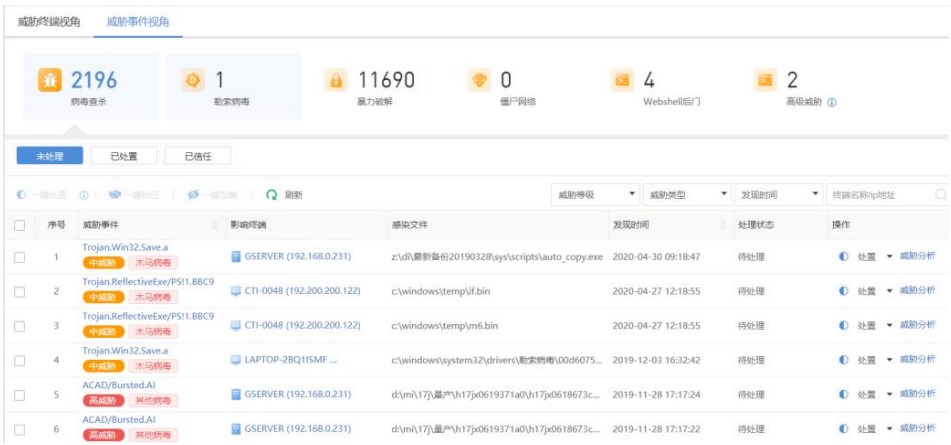
一键忽略可针对已经检测出来的文件/进程或攻击源IP进行忽略操作。

📖 **说明：**

为降低风险，针对暴力破解威胁，不开放一键处置，且黑名单需逐一添加。

3.6.1.2. 威胁事件视角

在威胁事件视角页面，可点击对应威胁事件类型（包括病毒查杀、勒索病毒、暴力破解、僵尸网络、Webshell后门及高级威胁等），查看相应的威胁事件名称、影响终端、感染文件、发现时间及处理状态等信息，并支持通过处置状态、威胁等级等类型筛选，同时可针对多个威胁事件进行批量一键处置操作，威胁事件视角页面如下图所示。



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，如不确定也可点击<

威胁分析>进一步确认或点击具体威胁事件可查看病毒名称、感染文件、病毒类型、检测引擎等详情信息，同时可查看对应处置建议。

📖 说明：

针对处置及信任操作，可选择[同时隔离其他终端上有相同 MD5 值的文件]，实现针对其它终端相同文件的批量处理。

3.6.2. 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。

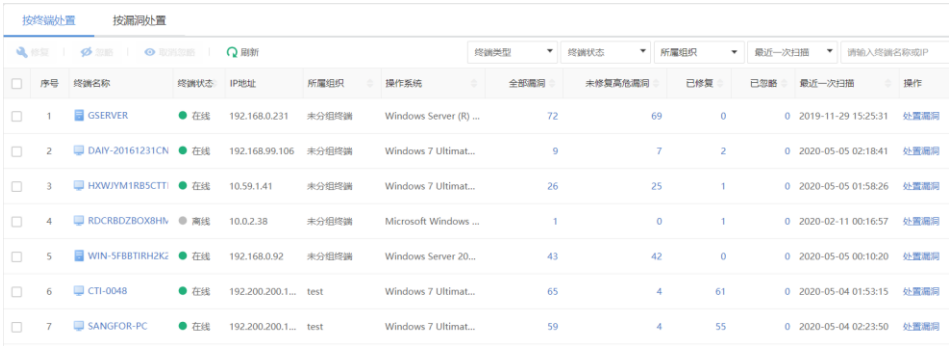
📖 说明：

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。

3.6.2.1. 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。

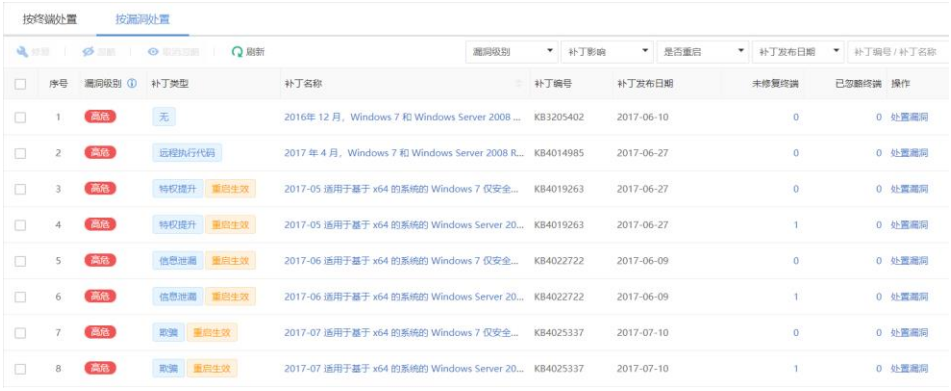


在[**处置漏洞**]页签下，可以：

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。

3.6.2.2. 轻补丁漏洞免疫

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终端检测响应平台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

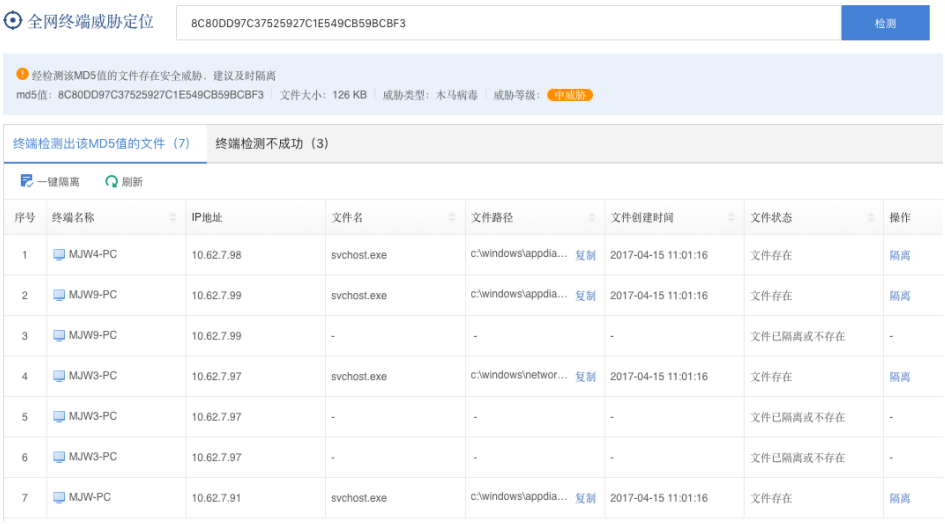
在[操作]栏下，点击<处置漏洞>，可以对当前漏洞进行免疫或取消免疫的操作，支持批量配置免疫或取消免疫。

> 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。

3.6.3. 威胁定位

威胁定位可基于威胁文件的md5值/域名实现快速精准地定位出全网感染相同威胁文件的终端或访问相同威胁域名的终端，管理可根据定位结果进行相应威胁处置。

在**[威胁定位]**页签下，将威胁文件的md5值/域名输入搜索框中，并点击搜索按钮进行威胁定位，定位结果如下图所示。



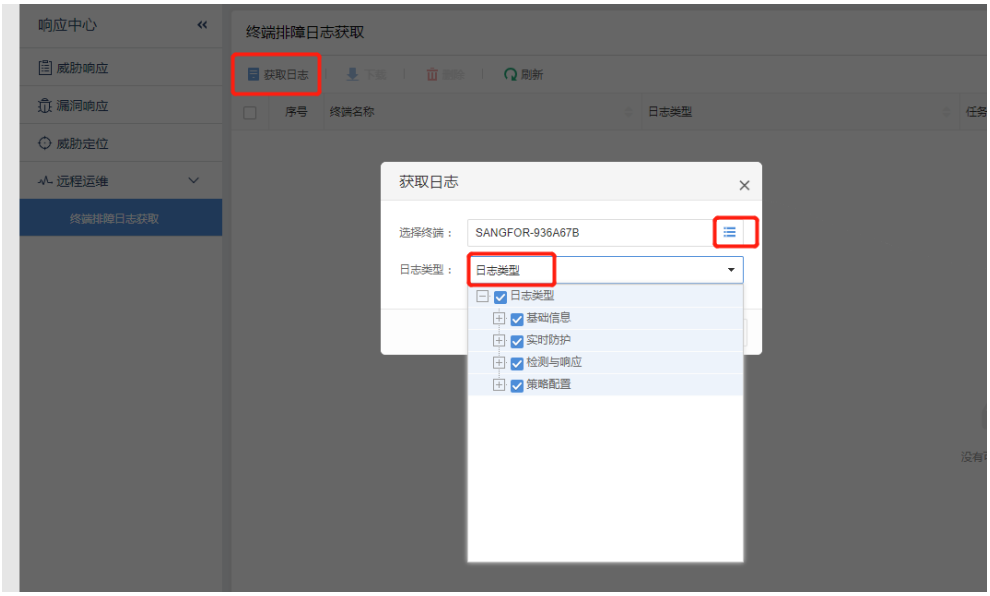
在结果页面可针对性查看访问域名的终端、访问域名的进程及进程对应的文件路径，同时可统计访问次数及进程关联文件总数等信息，针对威胁终端可在[操作]一栏，对多个终端存在的病毒进行处置，包括威胁详情查看、威胁进程/关联文件处置、信任、忽略等操作项。

3.6.4. 远程运维

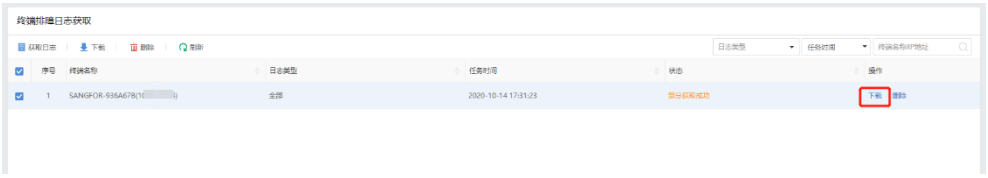
远程运维功能可支持终端排障日志获取，便于运维管理。

终端排障日志获取

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。



终端排障日志管理

1. 在[响应中心/远程运维/终端排障日志获取]的页签下，可以查看当前日志的终端名称、日志类型以及状态等详细信息，支持按日志类型、任务时间筛选对应终端，同时右上角的搜索栏也支持通过终端名称、IP地址进行精准搜索。

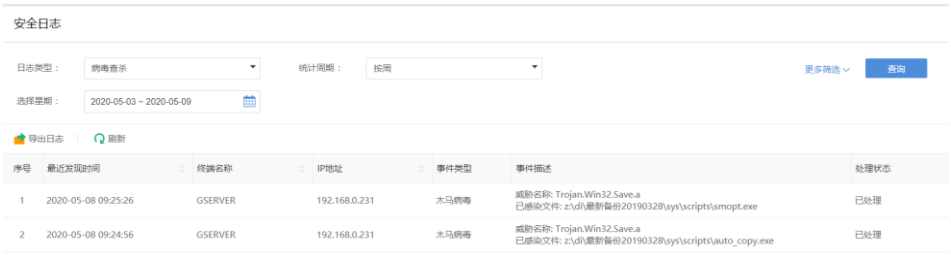
2. 勾选单个/多个日志，点击<下载>/<删除>，可以下载和删除单个/批量日志。也可点击操作栏目下的<下载>、<删除>进行单个日志的管理，如下图所示。

3.7. 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。

3.7.1. 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、微隔离及安全加固，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。

3.7.2. 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SOC，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。

3.7.3. 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。

3.7.4. 操作日志

操作日志主要展示管理员针对EDR管理平台的操作记录，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。

3.7.5. 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，在导出时可对报告导出名称、报告数据时间范围和报告格式进行指定，配置界面如下图所示。

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。

3.8. 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”。

3.8.1. 联动管理

联动管理可实现EDR与AC、AF、SIP、X-Central及SOC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，联动管理界面如下图所示。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。

在[联动管理]页签下，可查看设备整体联动情况和各联动设备的相关信息，信息包括联动设备名称、类型、IP、版本号、接入时间及最近联动时间，同时可通过类型、接入时间及最近联动时间进行筛选或通过设备名称或IP进行查找。

同时，针对联动设备可在[操作]一栏进行连通性测试或解除联动操作。

各产品与EDR联动功能支持情况如下表所示。

表6 联动功能

联动产品	推广部署Agent	联动封锁	日志上报	访问控制	联动下发查杀扫描	联动处置威胁文件	进程举证
AC	√	×	×	×	√	√	×
AF	×	×	×	×	√	√	√
SIP	×	√	√	√	√	√	√
X-Central	×	×	×	×	×	√	√
SOC	×	×	√	×	√	√	×

EDR和任何产品联动，需要先启用“联动设备准入设置”。打开[系统管理/系统设置/基本设置]，启用联动设备准入设置，并设置联动设备接入时间，如下图，联动设备需要设置的指定时间内接入。

3.8.1.1. 联动 AC 配置

EDR与AC联动可实现EDR客户端推广部署、联动查杀病毒处置等方案。如需进行联动需满足以下条件:

网络连通性：AC需与EDR的TCP443端口通信;

版本要求：AC需使用12.0.16及以上版本。

联动操作步骤

EDR与AC实现联动仅需在AC上配置即可。配置步骤如下:

步骤1. 登录AC控制台，在[上网安全/安全能力/终端检测与响应（EDR）]页签下的[EDR平台IP]位置，填写EDR管理平台的IP地址，并点击<接入>，配置页面如下图所示。

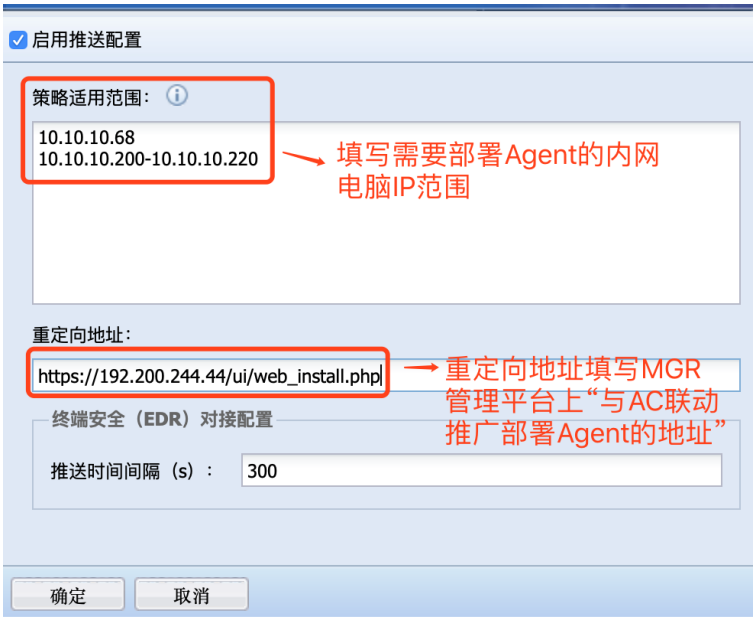
步骤1. 联动成功后，在AC设备[EDR服务信息]下会显示服务状态为[在线]，点击<查看联动详情>可以查看EDR上的联动终端信息。

序号	联动终端	联动终端IP	状态	联动操作数	最近更新时间
1	ubuntu14.novalocal	192.168.3.12	在线	0	2019-03-27 09:46:27
2	WIN-JO60TMANJPR	192.168.3.9	在线	0	2019-03-27 09:46:27
3	centos7.2.novalocal	192.168.3.11	在线	0	2019-03-27 09:46:27
4	DESKTOP-10F75VA	192.200.202.51,2.3.1.160	在线	0	2019-03-27 09:46:27
5	VINCENT_WIN10	172.16.110.218	禁用	0	2019-03-27 09:46:27
6	DESKTOP-4P2L4UI	192.168.43.40	在线	0	2019-03-27 09:46:27
7	WIN-RERJ941FPU6	172.16.28.152	离线	0	2019-03-27 09:46:27
8	HXWJYM1RB5CTTNH	192.168.100.100	在线	0	2019-03-27 09:46:27
9	DESKTOP-GASEFVC	192.168.100.7	在线	0	2019-03-27 09:46:27
10	tomcat-2	192.168.1.8	在线	0	2019-03-27 09:46:27
11	mysql-m1	192.168.1.20,172.17.42.1	在线	0	2019-03-27 09:46:27
12	mysql-m3	192.168.1.19,172.17.0.1	在线	0	2019-03-27 09:46:27
13	dev	192.168.1.17,172.17.0.1	在线	0	2019-03-27 09:46:27
14	tomcat-1	192.168.1.7	在线	0	2019-03-27 09:46:27
15	nginx-2	192.168.1.5,192.168.1.21	在线	0	2019-03-27 09:46:27
16	nginx-1	192.168.1.4	在线	0	2019-03-27 09:46:27
17	WEIXINYU	192.168.8.100	离线	0	2019-03-27 09:46:27
18	HYSCOFIELD-C4CD	10.211.55.3	离线	0	2019-03-27 09:46:2
19	WIN-A1TTV0QTO5H	10.20.20.42	在线	0	2019-03-27 09:46:2

联动效果

1. 推广部署Agent

打开[上网安全/安全能力/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。

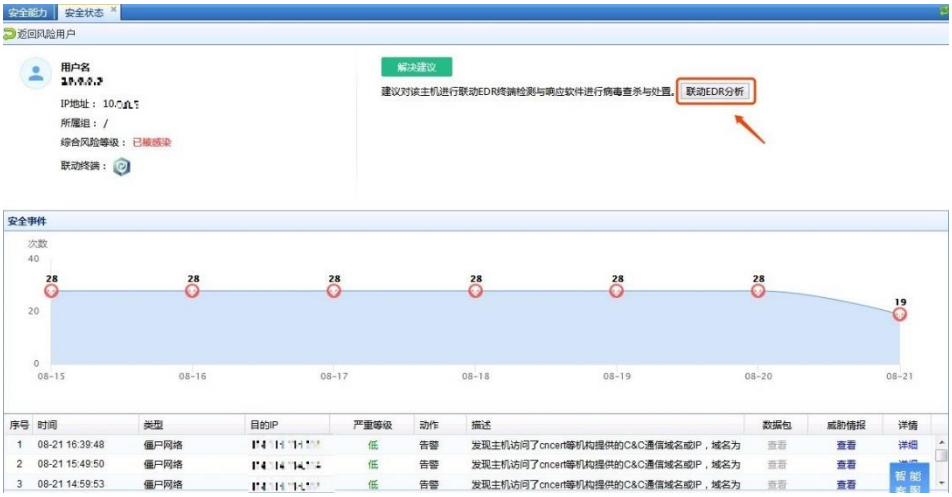
重定向地址：终端电脑上网被重定向到下载Agent客户端的地址，填写管理平台[系统管理/终端部署]，上网行为管理系统联动部署中的地址，如下图。

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。

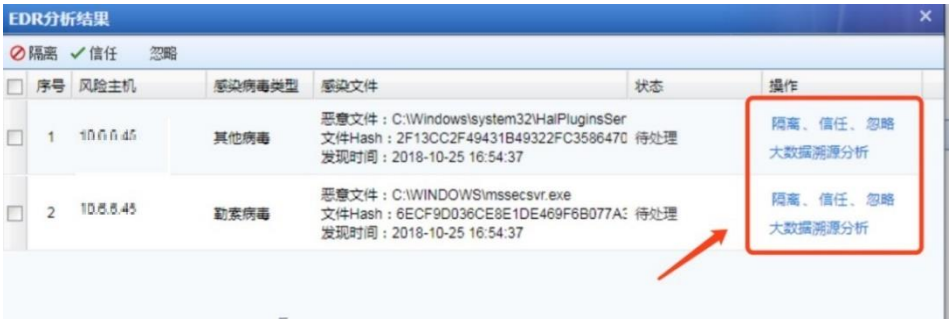
2. 联动杀毒

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[实时状态/安全状态/风险用户]，如下图。

点击<查看明细>，如下图。



点击<联动分析>，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。



3.8.1.2. 联动SIP配置

EDR与SIP联动可实现SIP发现威胁文件/威胁终端后，可联动EDR进行病毒查杀或进行威胁终端出入站流量隔离。同时，EDR安全日志可上报至SIP平台，由SIP进行集中运营分析，如需进行联动需满足以下条件：

网络连通性：SIP需与EDR的TCP443端口通信，EDR管理平台可与SIP的TCP7443端口通信；

版本要求：SIP需使用3.0.49及以上版本。

EDR与SIP实现联动可在EDR平台或SIP平台进行配置，选取其中任意平台完成单次配置即可。

SIP平台联动操作步骤

步骤1. 登录SIP平台，在[系统设置/设备管理]页签下，点击<新增>，并在弹出的[新增]页面进行接入设备IP、设备名称、设备类型等信息的编辑，编辑完成后点

击<确定>，配置页面如下图所示。

其中：

接入设备IP：请填写EDR管理端的IP地址；

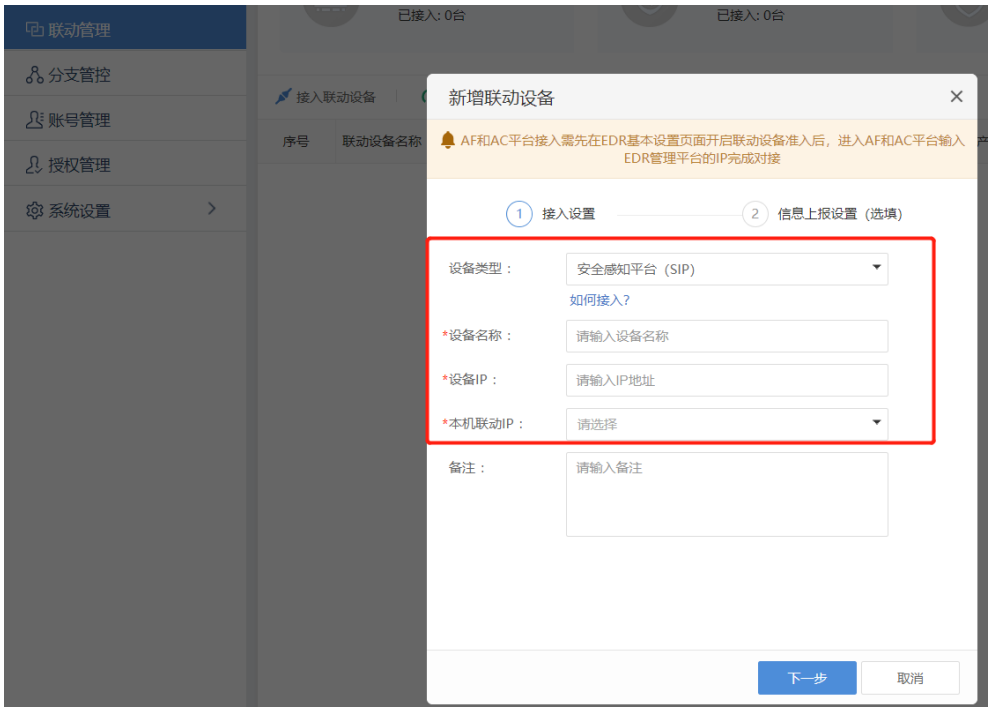
设备名称：可自定义易识别的设备名称；

设备类型：请选择“终端检测响应平台”。

步骤2. 联动成功后，在EDR平台的[系统管理/联动管理]页签下可查看该SIP设备已与EDR完成联动，并可查看该SIP设备的相关信息并通过连通性测试。

EDR平台联动操作步骤

1. EDR平台的[系统管理/联动管理]页签下，点击<接入联动设备>，并在弹出的[新增联动设备]页面进行设备类型、名称、IP及本机联动IP等信息的编辑，编辑完成后点击<下一步>，配置页面如下图所示，也可以点击“如何接入”查看具体操作。



其中：

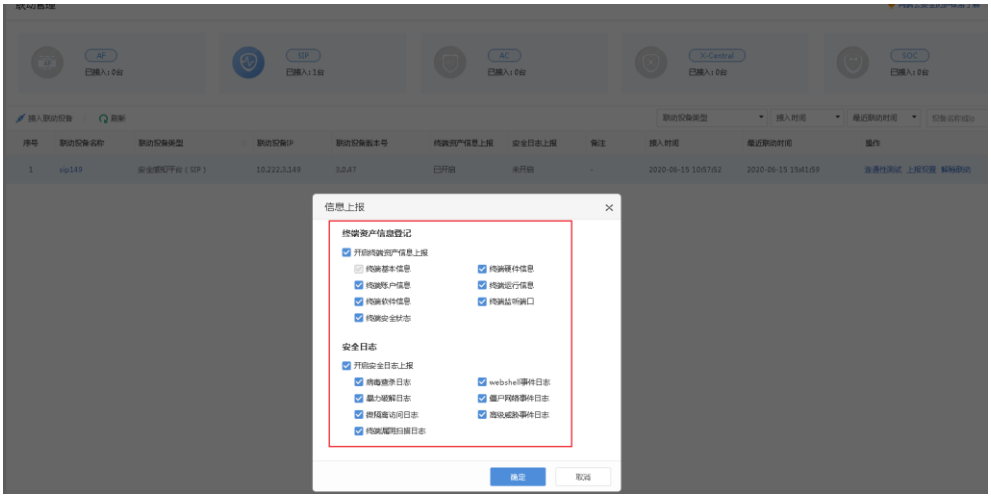
设备类型：请选择[安全感知平台（SIP）]；

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；

2. 信息上报设置，支持上报的日志类型开关设置。若过程中想要对上报日志类型或开关做修改时，也可以通过<上报设置>按钮进行重新设置，如下图所示。

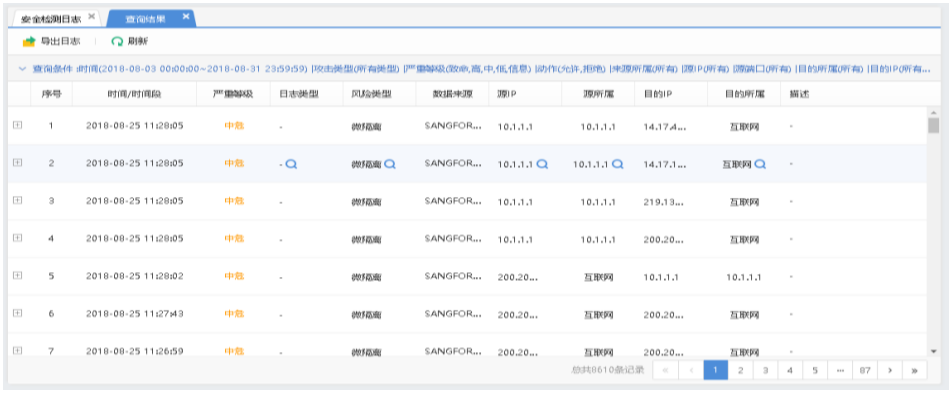


信息上报：勾选后，EDR会把勾选的信息上报至SIP平台进行集中分析。

联动效果

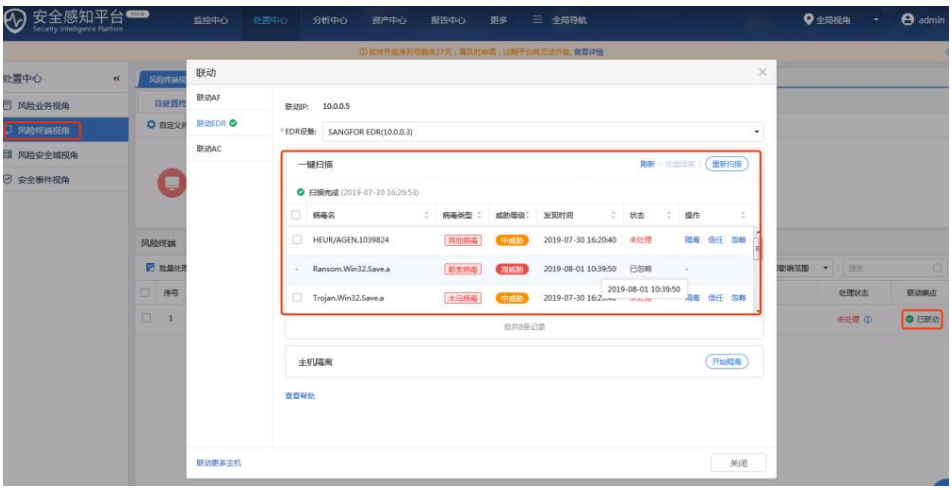
1. EDR安全日志上报

当EDR产生安全日志后，可以自动上报至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。



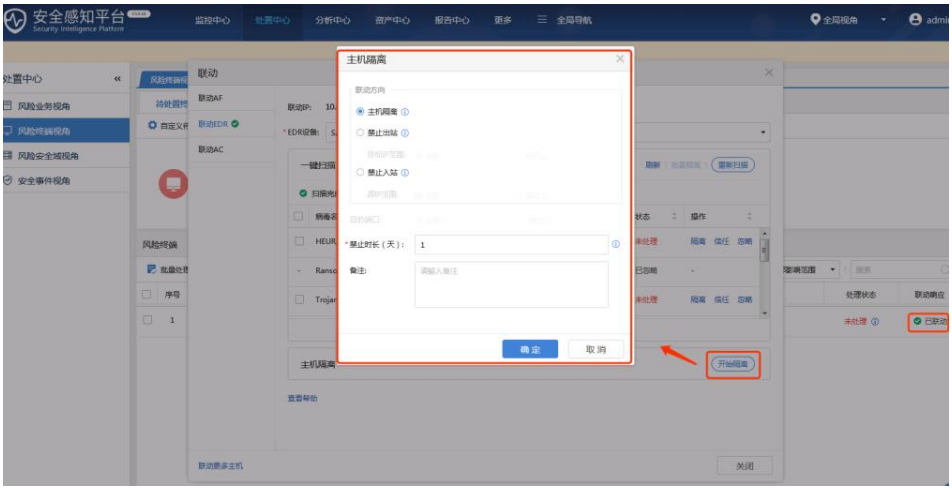
2. 联动杀毒

当SIP识别到风险终端时，可以联动EDR进行查杀。在SIP平台的[处置中心/风险终端视角]页签下，可针对识别到的风险终端联动EDR进行病毒查杀、针对识别到的威胁文件进行隔离、信任或忽略等操作，联动页面如下图所示。



3. 风险主机隔离

当SIP发现风险终端后，可以联动EDR进行风险主机进行网络隔离，在SIP平台的[处置中心/风险终端视角]页签下，对识别到的风险终端联动EDR进行主机隔离、出站隔离、入站隔离等操作，联动页面如下图所示。



3.8.1.3. 联动 AF 配置

EDR与AF联动可实现联动病毒查杀及僵尸网络举证等方案，如需进行联动需满足以下条件:

网络连通性：AF需与EDR的TCP443端口通信;

版本要求：SIP需使用8.0.12及以上版本。

EDR与AF实现联动仅需在AF平台进行配置即可，配置步骤如下:

联动操作步骤

步骤1. 登录AF平台，在[下一代安全防护体系/体系总览]页签下，点击最右侧三角符合，并在侧滑出的页面进行EDR平台IP的编辑，编辑完成后点击<立即接入>，

步骤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。

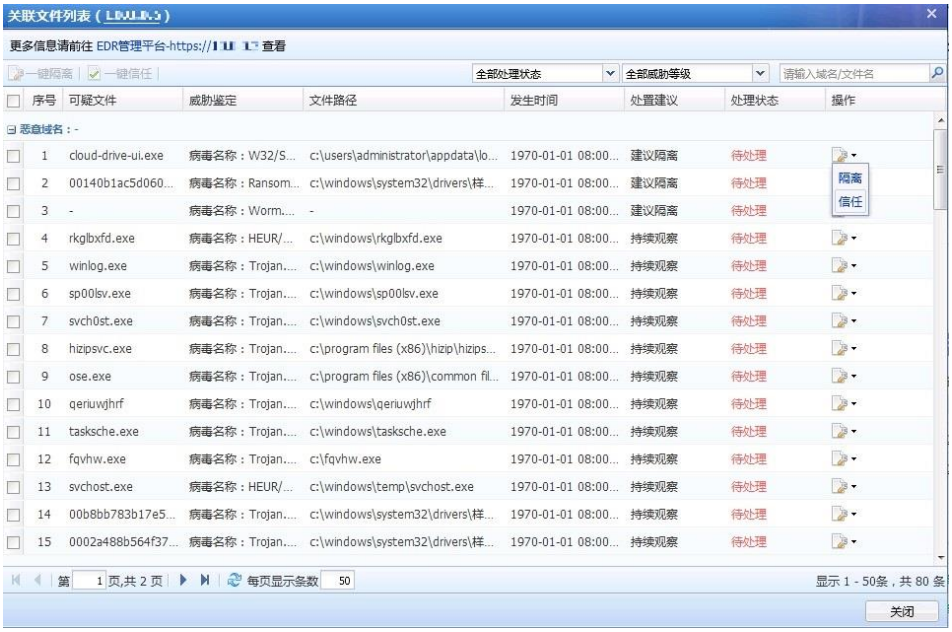
同时在[下一代安全防护体系/EDR]页签下，可查看联动的EDR终端与状态，如下图所示。

联动效果

联动成功后，可实现EDR与AF的联动病毒查杀及僵尸网络举证等操作。

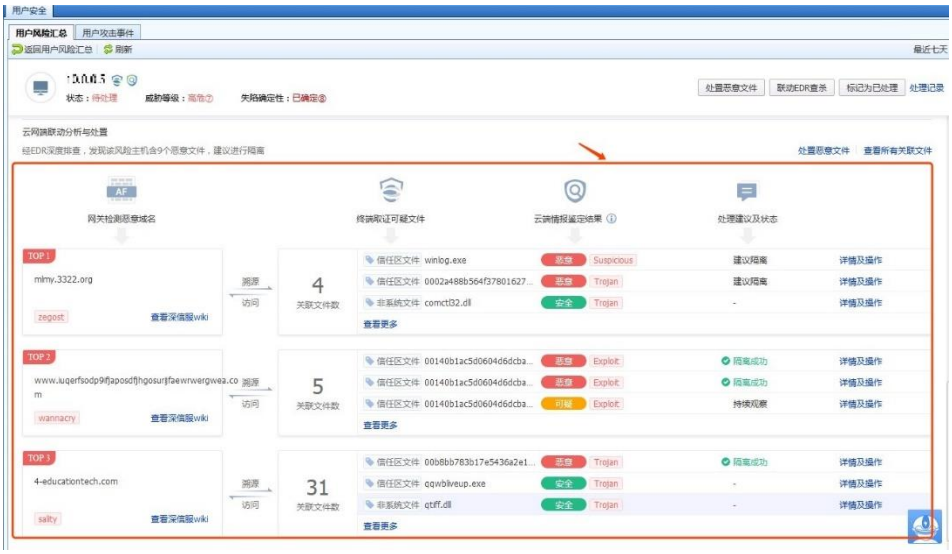
1. 联动杀毒

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. 联动僵尸网络举证

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。

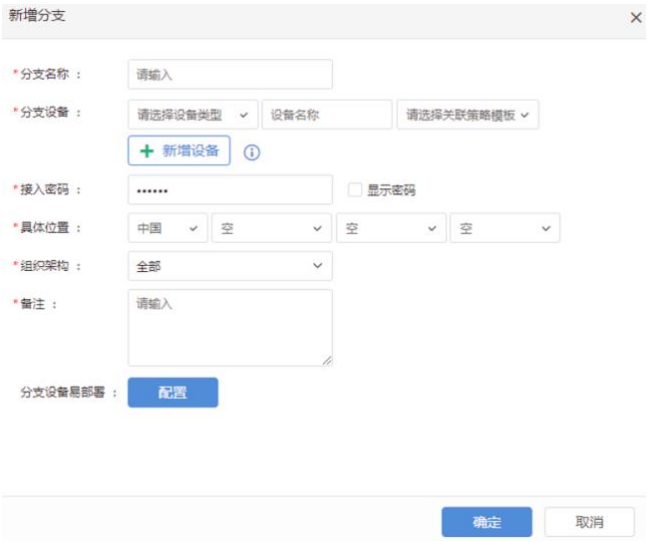
3.8.1.4. 联动 X-Central 配置

X-central，即云图。EDR和X-central联动能够实现联动处理威胁文件、僵尸网络举证。EDR和X-Central联动需要分别在X-Central平台和EDR平台填写对应的接入信息完成联动对接。

X-Central平台配置

登录X-Centra控制台，在[资产中心/设备]页面下，点击<新增>。

在新增弹窗填写必填项“设备信息”和“接入密码”即可完成SOC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。



在云图logo处获取云图企业ID。（用于在EDR平台对接X-Central时填写企业ID）

EDR平台配置

1. 在EDR的[系统管理/联动管理]页面，点击<接入联动设备>，如下图。

2. 信息上报设置，可以设置支持上报的日志类型。

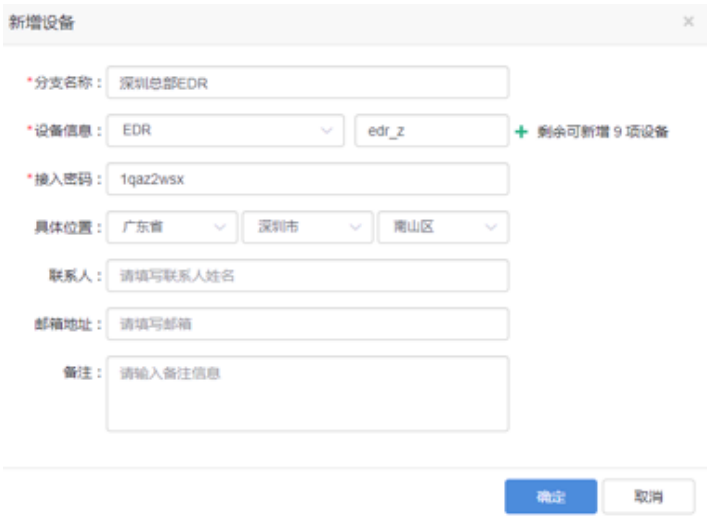
> 说明：
> 企业 ID 需要在云图平台获取；认账账号和密码需与云图创建的设备账号和密码保持一致；确保 EDR 管控平台网络要能联通云图平台。

3.8.1.5. 联动 SOC

SOC，即安全运营中心，是安全服务运营平台。EDR和SOC联动能够实现日志上报、联动查杀、安全日志取证。EDR和SOC的联动需要分别在SOC平台和EDR平台填写对应的接入信息完成联动对接。

SOC平台配置

在新增弹窗填写必填项“设备信息”和“接入密码”即可完成SOC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。



完成上述配置后，回到客户管理页面，获取配置好的上述EDR设备的客户ID信息。（用于在EDR平台对接SOC时填写企业ID）

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>，如下图。

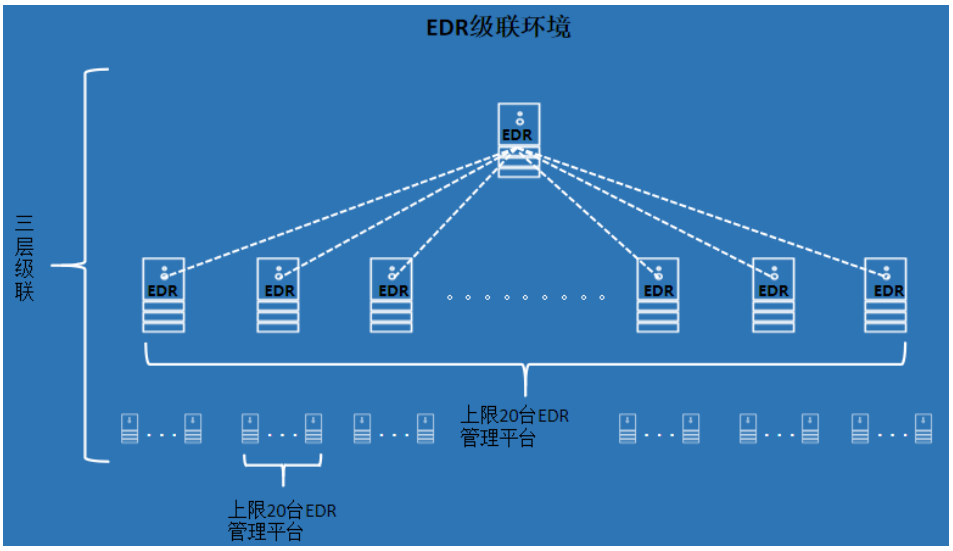
在新增弹窗选择联动设备类型SOC，输入SOC平台的平台名称、企业ID、认证账号和密码完成对接，需要开启日志上报后，联动后才能正常传输数据，信息上报设置可以选填。

说明：

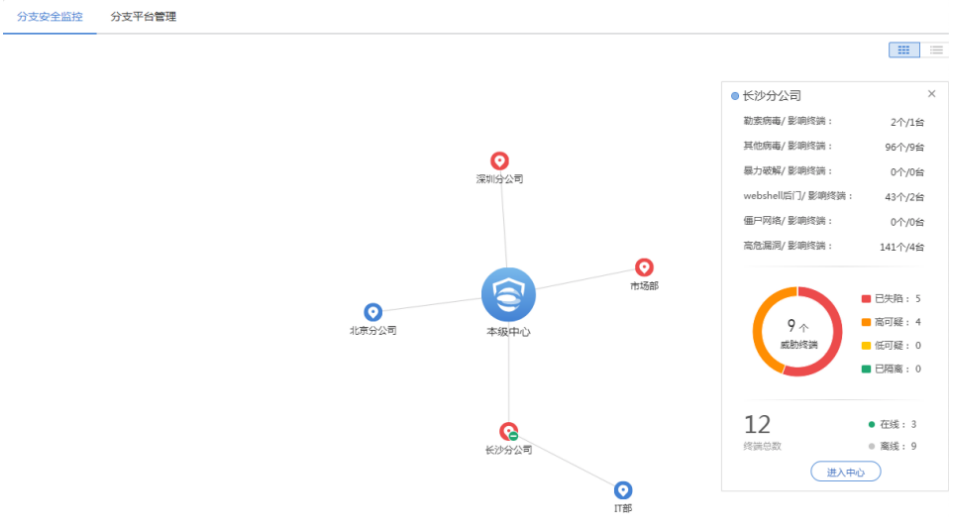
企业 ID 需要在云图平台获取；认账账号和密码需与云图创建的设备账号和密码保持一致；确保 EDR 管控平台网络要能联通云图平台。

3.8.2. 分支管控

分支管控功能通过分支安全监控及分支平台管理，实现多台EDR级联管理，可支持三级级联，每台EDR可级联至多20台EDR管理平台，EDR级联环境示意图如下图所示。



可在[分支安全监控]页签下，查看级联分支安全情况，可通过右上角标签进行拓扑形式/图表形式的切换，如下图所示。



级联分支配置需在[分支平台管理]页签下，点击<接入下级EDR>，并在弹出的页面下对下级EDR平台进行编辑，编辑完成后点击<测试连通性>，连通性无问题后点击<确定>进行接入，配置页面如下图所示。

其中：

分支EDR登录端口：为EDR平台HTTPS登录页面所用端口，默认端口为443端口，请以实际为准；

SSH端口/账号/密码：默认SSH端口为22345端口，账号为root，密码可按实际情况填写。

3.8.3. 账号管理

3.8.3.1. 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/帐号管理]页面，点击<新增>创建管理员帐号，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，从而实现管理平台账号的三权分立。

3.8.3.2. 密码安全策略

登录管理平台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/帐号管理]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：[1-30])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。

3.8.3.3. 管理平台账号登录认证

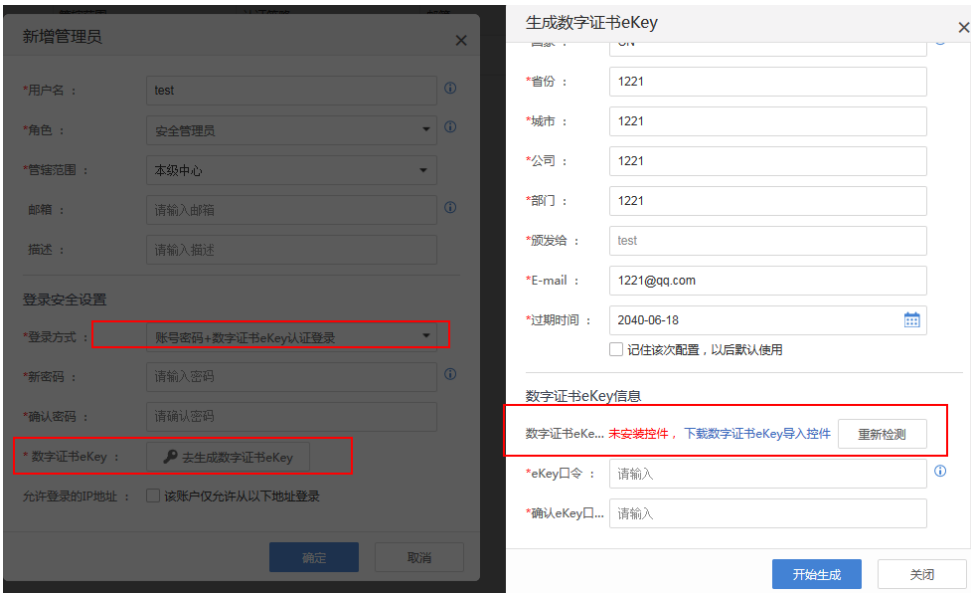
登录管理平台提供了两种认证方式，账号密码认证登录和账号密码+USB-KEY认证登录。在[系统管理/帐号管理]页面下，点击<新增>创建管理员帐号，如下图。

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：

步骤1. 生成管理平台的根证书。在[系统管理/帐号管理]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。

步骤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平

台，新增管理员帐号，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。

步骤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管理平台，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。

3.8.3.4. IP 地址限制登录

管理平台的帐号支持只允许在授权的电脑登录，打开新增管理员帐号页面，启用[允许登录的IP地址]，设置允许登录EDR管理平台的电脑IP地址，如下图。

3.8.4. 授权管理

EDR平台授权由智防、智控、智响应三个模块相关授权组成，完整授权如下图所示。

在[授权管理]页签下，可针对本平台授权状态及相关信息进行查看，页面如下图所示。

📖 **说明：**

EDR 管理平台需开通有效授权才可使用，授权方式请参考章节“安装部署”相关内容。

3.8.5. 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。

3.8.5.1. 基本设置

在[基本设置]页签下，可对管理平台日期/时间、终端连接策略、终端数据采集间隔、管理平台补丁包下载、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管理平台的时间。点击<获取本地时间>，则EDR管理平台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

管理平台服务器主板时间；EDR管理平台能够联网的场景下，也可以启用[自动与NTP服务器同步]，则管理平台的时间和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平台上长期不在线的终端信息，自动释放闲置授权。

3. 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。

4. 管理平台补丁包下载设置：终端无法上网的环境，无法下载漏洞补丁，此时可以通过管理平台代理下载漏洞补丁，终端从管理平台下载漏洞补丁修复漏洞。

5. 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，只有在管理平台上勾选该复选框，且在有效时间内才允许AC、AF、SIP等设备主动接入。

6. 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。

7. 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。

8. 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EDR 网站，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管理平台的日志通过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。

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，点击<打开>，等待恢复完成。

3.8.5.2. 网络设置

网络设置里面包含了接口设置、路由设置、高级设置。

1. 接口设置

接口设置配置管理平台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，同时用于接入管理平台。在[系统管理/系统设置/网络设置/接口设置]页面下，如下图所示。

点击接口名称配置该接口的地址，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管理平台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，打开[系统管理/系统设置/网络设置/高级设置]，如下图。

其中:

- SSH 端口设置：用于修改 EDR 管理平台后台的 SSH 端口，默认为 22345 端口。

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

3.8.5.3. 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。

3.8.5.4. 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：用于设置管理平台漏洞库自动更新时间，启用后，管理平台在指定时间范围自动更新漏洞。

3.8.5.5. 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。

3.8.5.6. 系统工具

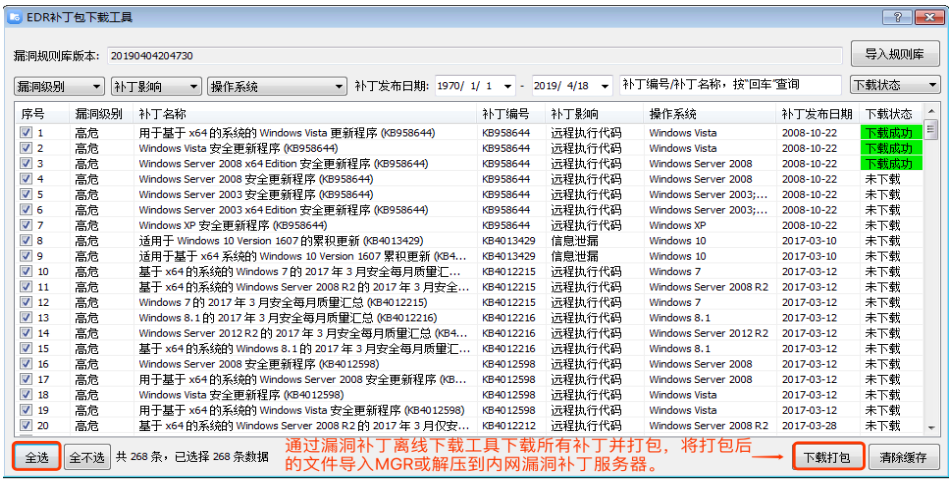
系统工具为漏洞补丁包离线下载工具，此工具和EDR系统漏洞检测与修复功能配合使用。当客户的EDR管理平台以及其所管理的所有终端都无法访问外网时，可以使用此工具下载系统漏洞补丁后导入平台进行终端系统漏洞修复。

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平台即可，如下图所示。

步骤4. 进行终端漏洞检测与修复操作。

4. 终端组件 Agent 使用

终端用户通过终端组件Agent，可进行病毒查杀操作、安全日志与隔离/信任区文件查看及自定义设置等操作，同时可通过托盘进行部分快捷操作等。

4.1. 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。

4.2. 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。

4.3. 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。

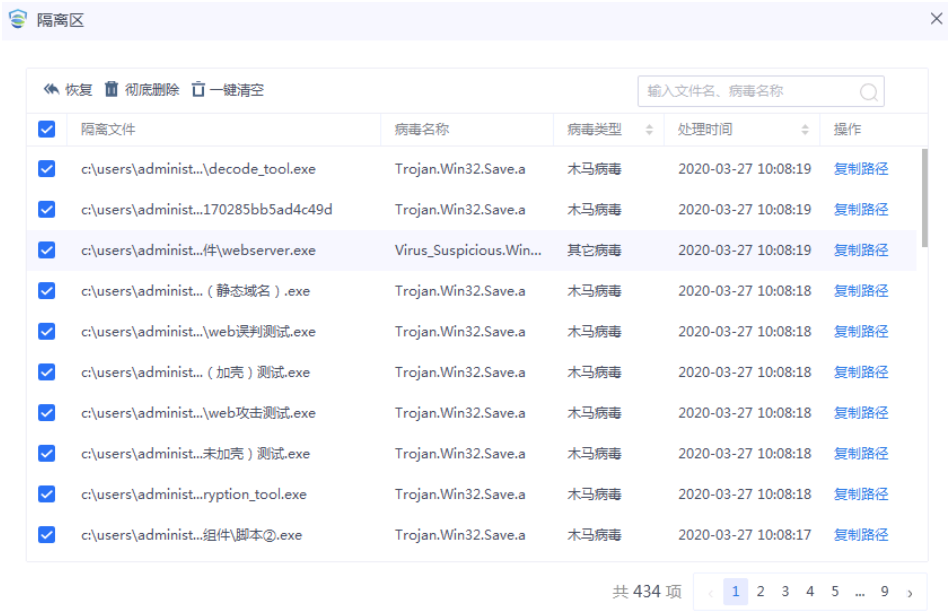
全盘扫描：对windows系统所有位置进行查杀。

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
	SAVE 人工智能引擎	提升未知病毒的检测能力。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	传统杀毒引擎，善于定位具备家族特征的病毒。
	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。

4.4. 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U盘防护，如下图。

U盘保护默认开启，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。

4.5. 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。

4.6. 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”，如下图。

病毒查杀：病毒查杀设置包括扫描模式设置、扫描引擎设置、扫描文件设置和处置方式设置。

扫描模式可选择“极速扫描”、“均衡扫描”、“低耗扫描”，其中：

- 极速扫描：全速扫描，不限制扫描软件自身的 CPU 占用率；
- 均衡扫描：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：扫描时尽量少占用 CPU 资源，限制 CPU 占用率不超过 10%。

扫描文件定义扫描文件的大小以及最大扫描的压缩层级，最大10级。

处置方式：设置发现威胁文件后的处置方式，有标准处置、严格处置和提醒我处置三种方式。

- 标准处置：EDR 检测结果属于黑名单库中的恶意文件隔离处理，不在黑名单库中的威胁文件不隔离，仅上报检测日志，默认配置为标准处置；
- 严格处理：EDR 检测的所有威胁文件均隔离处理，适用于严格保护场景；
- 提醒我处置：EDR 检测的所有威胁文件仅上报安全日志，不隔离，适用于有人值守且用户了解如何处置病毒的场景。

点击<保存>，保存当前页的配置，继续切换到其它功能页面进行配置。

点击<完成关闭>，保存当前页的配置并关闭设置中心。

系统防护：系统防护设置文件实时防护的防护级别、扫描引擎、文件类型、扫描文件和处置方式。各参数设置与管理平台文件实时监控设置方法一致，具体参考“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。各参数设置与管理平台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“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。各参数设置与管理平台暴力破解检测设置方法一致，具体参考“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和Powershell无文件攻击防护告警弹窗设置。用户可以根据实际需求，个性化设置是否允许弹窗提示。如果管理员从管理平台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。

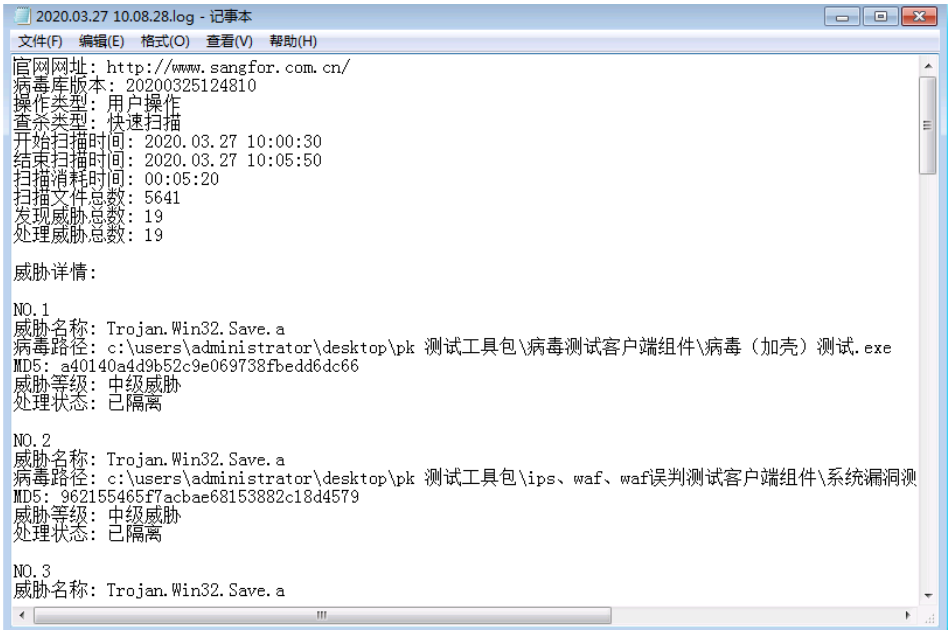
4.7. 安全日志

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。



4.8. 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. 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。

EDR已为您护航X天：查看EDR的防护时间。

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平台统下发。

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。

5. 日常维护

5.1. 终端管理

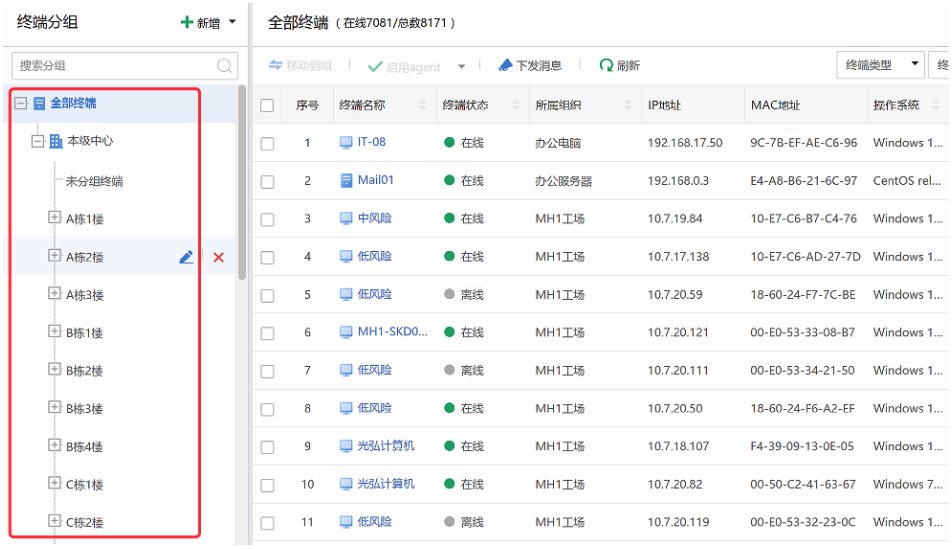
5.1.1. 终端分组管理

在多部门或多分支的场景，EDR新上线或者在后期有新的终端上线时，建议根据组织

架构建立树形分组、终端根据所属IP自动上线到正确的分组、并每个组织/分支建立单独的管理员进行管理，详情操作如下。

1. 按组织架构建立分组

打开[终端管理/终端分组管理]建立组织结构，如下图。



2. 终端根据IP上线分组

打开[终端管理/终端分组管理]，点击<新增>，打开自动分组管理，如下图，设置根据IP上线自动分组策略。

3. 多管理员管理

打开[系统管理/帐号管理]，为每个组织建立管理员帐号，进行单独管理，如下图。

5.1.2. 终端发现

终端电脑数量很多的情况下，管理员很难知道哪些终端未安装EDR客户端进行防护，

从而带来潜在的安全风险。所以管理员可以通过终端发现功能及时发现未安装EDR客户端的终端、并推动安装。终端发现功能详细使用参考“终端管理”章节。

5.2. 授权管理

管理员定期清理长期离线或已卸载终端，释放授权，确保新终端接入时有足够授权。清理授权有手动清理和自动清理两种方式。

1. 定期手动清理

打开[终端管理/终端分组管理]，选中并移除已卸载的终端或长期离线的终端，即可释放授权，如下图。

2. 产品自动清理

打开[系统管理/系统设置/基本设置]，设置终端连接策略，自动删除超过指定时间的离线终端，即可释放授权，如下图。

5.3. 安全加固

管理员应定期检查相应的安全策略、识别安全风险，并进行安全加固。安全加固主要包括版本和规则库检查、终端防退出和防卸载密码加强、管理平台控制台帐号和密码加强、远程登录保护密码加强、控制台限制IP登录、终端基线检查、终端漏洞修复和策略优化。

5.3.1. 版本和规则库检查

管理员应定期检查产品当前版本和病毒库当前版本。产品版本建议使用当前最新版本，病毒库需要使用当前最新版本。产品和病毒库当前已发布的最新版本可以通过社区路径：[自动服务/终端检测响应平台]。

5.3.2. 终端防退出和防卸载密码

管理员应定期修改终端防退出和防卸载密码，且防退出和防卸载密码为数字和大小写字母组合的强密码。

打开[终端管理/策略中心/基本策略]，修改终端防退出和防卸载密码如下。

5.3.3. 控制台帐号和密码

管理员应定期检查管理平台控制台帐号和密码，检查内容应做到如下两点。

1. 检查是否存在无效的管理员帐号，并进行清除。
2. 定期修改管理平台控制台帐号密码为强密码。

5.3.4. 远程登录保护密码

管理员应定期修改远程登录保护密码，且远程登录保护密码应符合密码复杂性要求。

打开[终端管理/策略中心/安全加固]，修改远程登录保护密码如下。

5.3.5. 控制台限制 IP 登录

建议设置管理员帐户限制IP登录，只允许授权的电脑登录EDR管理平台。

打开[系统管理/帐户管理]，设置管理员帐号只允许从指定地址登录，如下图。

5.3.6. 终端基线检查

管理员应定期对内网终端进行基线检查，并根据加固指导建议对不合规的检查项进行加固。

在[威胁检测/终端基线检查]页面下，如下图。

5.3.7. 终端漏洞修复

管理员应定期对内网终端进行系统漏洞检测，并对发现的漏洞进行修复。

打开[威胁检测/终端漏洞查补]，对内网windows终端进行漏洞修复，如下图。

5.3.8. 策略优化

管理员应定期检查内网安全策略并进行修复，各策略推荐配置如下表。

表7 策略优化表

策略名称	启用状态	策略配置推荐
病毒查杀	默认开启	在默认配置基础上，建议再开启定时查杀
文件实时监控	默认开启	建议保持默认配置
暴力破解检测	默认开启	建议保持默认配置
勒索诱饵防护	默认开启	建议保持默认配置
webshell 检测	默认开启	建议保持默认配置
无文件攻击防护	默认开启	内网如果存在调用 powershell 命令执行的脚本或程序，建议关闭无文件攻击防护；内网如果不存在调用 powershell 命令执行的脚本或程序，建议保持默认配置
服务器可信进程防护	按需开启	按需进行配置
远程登录保护	默认开启	建议保持默认配置
信任名单	按需开启	按需进行配置

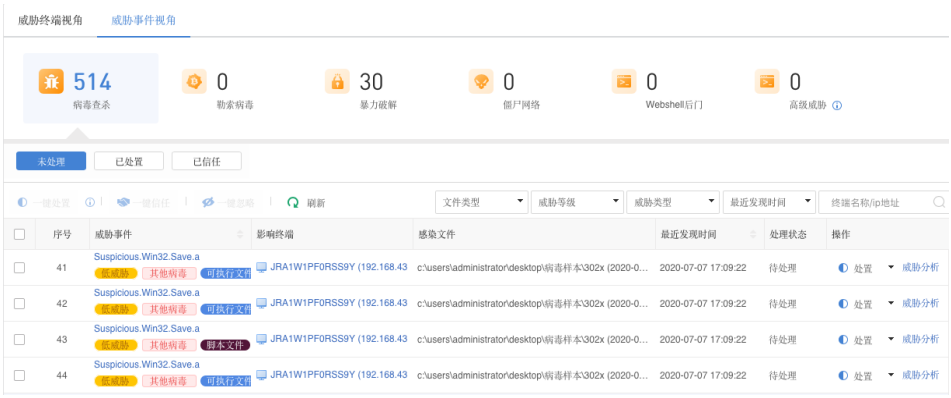
微隔离	按需开启	按需进行配置
告警策略	按需开启	建议开启邮件告警策略，当内网发现威胁事件时，能及时通知到管理员

5.4. 威胁事件处置

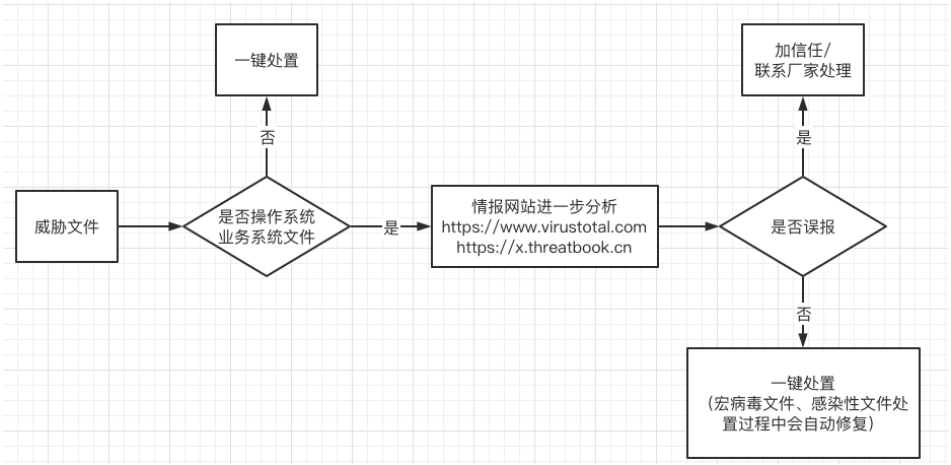
5.4.1. 威胁事件处置思路

管理员应定期检查管理平台是否存在未处理的威胁事件并进行处理。

在[响应中心/威胁响应]页签下，点击<威胁事件视角>，如下图。



威胁事件处置参考如下思路，应按照终端威胁程度，依次处理已失陷终端、高可疑终端、低可疑终端。



5.4.2. 威胁事件处置案例

下面以一个案例来说明威胁文件的处置方法。

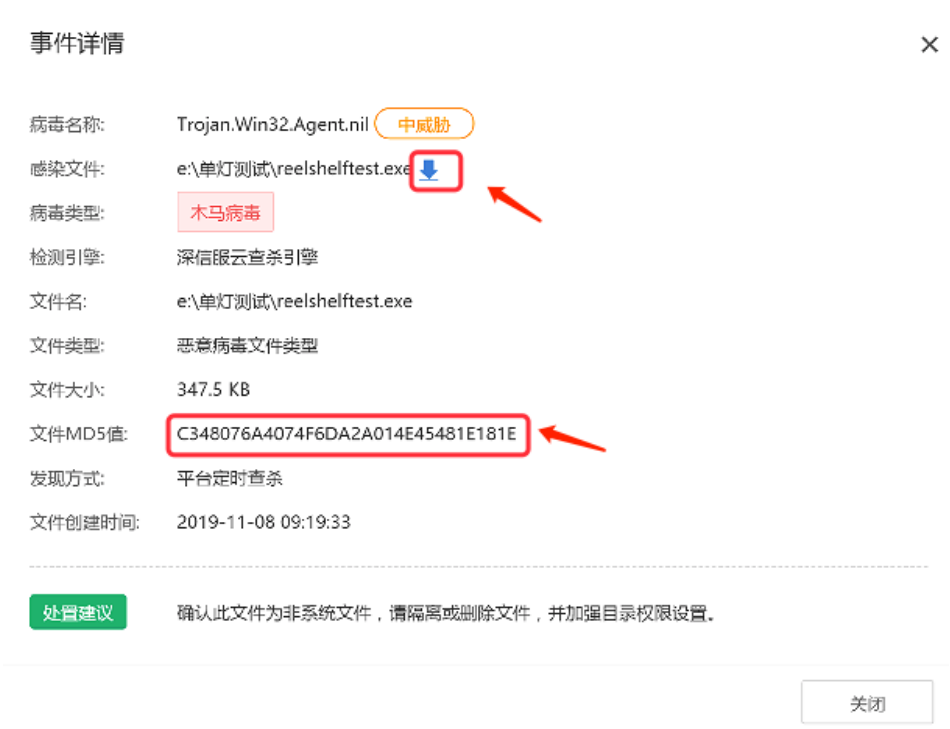
未自动隔离处理的文件会上报到EDR管理平台[响应中心/威胁响应]中，如下图。按终端威胁程度，依次处理已失陷终端、高可疑终端、低可疑终端。

步骤1. 判断威胁文件是否业务系统文件。

如下图，在某个终端上发现的威胁文件，其中2到7这几个威胁文件位于回收站中、且为非业务系统文件、可以一键处置，第1个文件为可疑文件需要进一步分析。

步骤2. 获取可疑文件进一步分析。

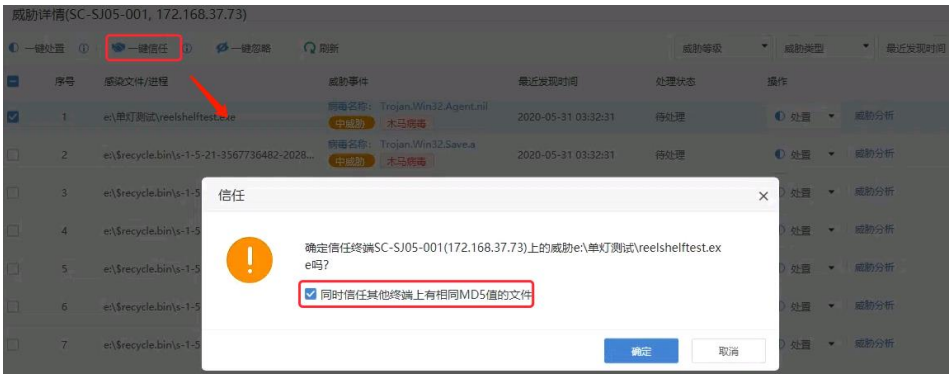
查看可疑文件详情，下载可疑文件样本，并上传至情报网站（https://www.virustotal.com/gui/home、https://x.threatbook.cn）进一步分析。



微步在线分析文件为安全，确认误报，加信任处理。

步骤3. 根据威胁情报分析结果，做进一步处理。

根据微步在线分析文件是安全的，确认为误报，所以需要加信任处理。


威胁详情(SC-SJ05-001, 172.168.37.73)
一键处置
一键信任
一键忽略
刷新
威胁等级
威胁类型
最近发现时间
序号
感染文件/进程
威胁事件
最近发现时间
处理状态
操作
信任
确定信任终端SC-SJ05-001(172.168.37.73)上的威胁e:\单灯测试\reelshelftest.exe吗?
同时信任其他终端上有相同MD5值的文件
确定
取消

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8 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“严格处置”	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“标准处置”
终端管理	策略中心	病毒查杀	日常使用时，启用了“高启发式扫描”	高启发式扫描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	正常使用时不启用“高启发式扫描”
终端	策略	实时防护	文件实时监控中，当发现威	可能存在误判，	高风险	将发现威胁文件后

管理	中心		胁文件后的处置动作设置为“严格处置”	将客户的业务文件隔离，导致业务系统异常		的处置动作设置为“标准处置”
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	高风险	在[响应中心/威胁响应/已隔离终端]进行移除

				常使用		
响应中心	漏洞响应	漏洞修复	某些漏洞需要系统才能完成修复，如果选择了修复后自动重启服务器，是业务会中断	服务器重启，导致业务中断	高风险	修复漏洞时建议不要选择重启服务器，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	安全加固	启用了服务器防护或服务器重要目录防护功能，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