深信服终端威胁防护系统 XDR
用户手册

产品版本 3.2.26

文档版本 01

发布日期 2020-09-14

深信服科技股份有限公司

注意

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。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。

前言

关于本文档

本文档针对深信服终端威胁防护系统 XDR 产品，介绍了XDR的架构、特性、安装和运维管理。

产品版本

本文档以下列产品版本为基准写作。（示例）

产品名称	版本
XDR	3.2.26

后续版本有配置内容变更时，本文档随之更新发布。

读者对象

本手册建议适用于以下对象：

- 网络设计工程师
- 运维人员

符号约定

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。

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本	发布时间	更新说明
01	2020-09-14	本文档第一次发布。

资料获取

您可以通过深信服官方网站获取产品的最新资讯：

www.sangfor.com.cn

获取安装/配置资料、软件版本及升级包、常用工具地址如下：

bbs.sangfor.com.cn

深信服科技

深信服技术服务

技术支持

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服科技服务商及服务有效期查询：

https://bbs.sangfor.com.cn/plugin.php?id=service:query

意见反馈

如果您在使用过程中发现任何产品资料的问题，可以通过以下方式联系我们。

- bbs.sangfor.com.cn
- 通过联系当地办事处电话反馈
- 售后服务电话 400-630-6430

目录

1. 产品简介

终端威胁防护系统（XDR）是深信服公司提供的一套终端安全解决方案，方案由轻量级的端点安全软件（Agent）和管理平台（MGR）共同组成。

XDR的管理平台支持统一的终端资产管理、终端病毒查杀、终端合规检查，支持微隔离的访问控制策略统一管理，支持对安全事件的一键隔离处置，以及热点事件IOC的全网威胁定位。

端点软件支持防病毒功能、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。

1.1. 产品特性

1. 终端资产的全面清点

全网终端资产的全面清点，包含业务服务器和用户PC的终端资产清点。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。

2. 终端安全的合规审查

每一个组织都有自己的终端安全合规要求，特别是等级保护的合规要求，对主机的安全要求。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。

3. 勒索病毒的实时防御

勒索病毒通过加密文件的方式，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XDR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，防止用户感染最新的勒索软件。

4. 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。XDR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。

5. 入侵攻击的主动检测

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。深信服的XDR主动检测暴力破解行为，并对发现攻击行为的IP进行封堵响应。针对Web安全攻击行为，则主动检测Web后门的文件。

6. 热点事件快速响应

深信服安全云脑通过全球的大数据安全分析，提供热点事件的IOC情报，推送情报数据给XDR产品。XDR产品能根据IOC情报数据快速的全网威胁定位分析，及时发现和响应最新的热点事件，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. XDR 安装部署

2.1. 部署介绍

终端威胁防护系统（XDR）部署在用户本地环境。XDR管理平台（管理平台）为软件交付，软件管理平台支持部署在X86架构国产化服务器（兆芯+中标麒麟）及非国产化服务器或虚拟机，负责集中管理所有Agent；端点安全软件（Agent）安装在每台终端上（支持安装在国化产终端和非国化产终端）。XDR管理平台（管理平台）通过公网与深信服安全云，内网每台终端Agent与终端威胁防护系统，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。

本地部署XDR终端威胁防护系统方案实现流程如下：

第一步，下载agent安装包，安装到需保护的终端；

第二步，终端威胁防护系统下发安全策略到终端；

第三步，终端进行安全扫描；

第四步，终端上报查杀结果到终端威胁防护系统；

第五步，终端威胁防护系统上报查杀结果到深信服安全云进行云查杀；

第六步，云查杀返回查杀结果到终端威胁防护系统。

2.2. 部署准备

2.2.1. 管理平台安装环境

XDR管理平台（管理平台）为软件交付，软件管理平台支持部署在X86架构国产化服务器（兆芯+中标麒麟）及非国产化服务器或虚拟机。其中服务器硬件和操作系统要求如下：

- 国产化服务器：兆芯 CPU、中标麒麟操作系统；
- 非国产化服务器：操作系统为 CentOS 7.x；
- 硬件要求：CPU 4 核，内存 8G，硬盘 500G。

需提前准备好安装管理平台的服务器（兆芯国产化服务器或非国产化服务器）、安装好操作系统、并且配置好服务器的网络配置（包括服务器地址、路由、网关、DNS地址）。确保服务器环境准备好，并且服务器是可以联通外网的。

2.2.2. 终端 Agent 安装环境

终端Agent支持在国产化终端和非国产化终端安装，具体如下。

类型	CPU类型	厂商	CPU型号	系统厂商	操作系统
客户端	X86	intel	intel X86		非国产终端（Windows/Linux）
	ARM	飞腾	FT1500A、FT2000+	银河	银河麒麟桌面操作系统V4
					银河麒麟服务器操作系统V4
		鲲鹏	鲲鹏920	银河	银河麒麟服务器操作系统V4
				中标	中标麒麟桌面操作系统软件V7.0
					中标麒麟高级服务器操作系统软件V7.0
				Centos	Centos7+
				统信UOS	统信UOS V20服务器
	MIPS	龙芯	3A3000（桌面） 3A4000（桌面） 3B3000（服务器）	中标	中标麒麟桌面操作系统软件V7.0
					中标麒麟高级服务器操作系统软件V7.0
	X86	兆芯	兆芯C	中标	中标麒麟桌面操作系统软件V7.0
					中标麒麟高级服务器操作系统软件V7.0
				中科	中科方德桌面操作系统
					中科方德高级服务器操作系统

2.2.3. 网络连通性

1. Agent与管理平台通信使用了443、8083、54120端口（443为下载agent端口，8083为业务端口，54120为管理端口），请配置对应的防火墙策略，保证连通性。
2. 管理平台需要能联网，确保到以下服务器联通。

   （云脑）漏洞补丁相关：https://upd.sangfor.com.cn

（云脑）接入云脑授权：https://auth.sangfor.com.cn

（云脑）云查服务器：https://analysis.sangfor.com.cn

（云脑）云安全计划：https://clt.sangfor.com.cn

（CDN）漏洞补丁、规则、病毒库地址：http://download.sangfor.com.cn

2.2.4. 部署计划

为了确保客户业务稳定性和连续性，我们需要提前做好部署计划，避免突发无法提前预知的情况影响到客户业务。部署计划遵从以下原则。

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。

2.3. 管理平台部署

2.3.1. 下载软件安装包

联系服务提供商获取软件安装包。

2.3.2. 管理平台安装

提前准备好安装管理平台的服务器（兆芯国产化服务器或非国产化服务器）、安装好操作系统、并且配置好服务器的网络配置（包括服务器地址、路由、网关、DNS地址）。确保服务器环境准备好，并且服务器是可以连通外网的。

步骤1. 上传安装包

将管理平台安装包（扩展名为pkg）和安装脚本（扩展名为sh）上传至服务器同一目录下。并给安装脚本添加可执行权限，“chmod u+x manager_deploy.sh”。

步骤2. 执行脚本安装

按如下参数执行安装脚本进行安装。

./manager_deploy.sh 包名称.pkg 127.0.0.1

2.4. 激活授权

2.4.1. 产品试用授权激活

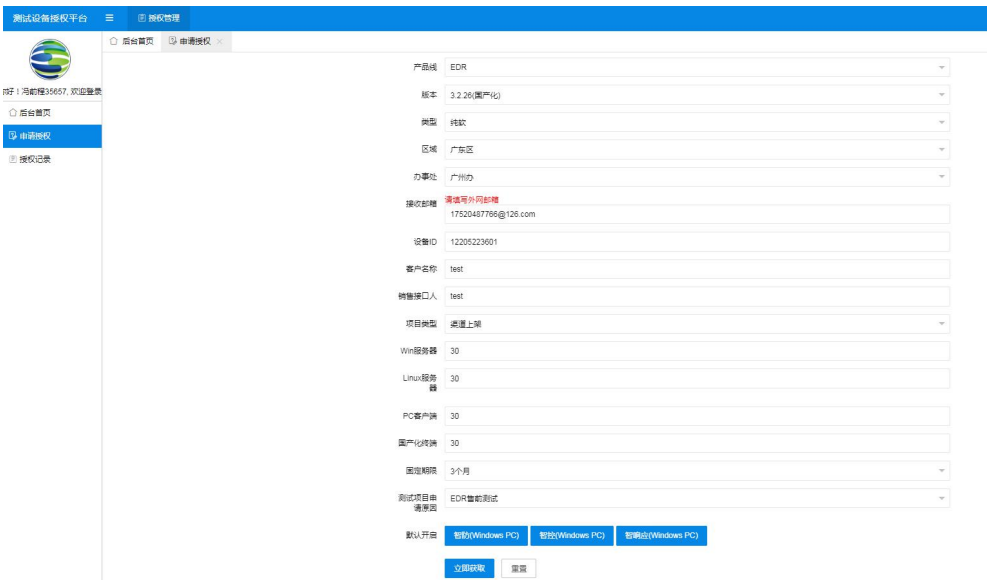
产品试用（测试项目）期间由厂商开通试用授权，开通方法如下。

步骤1. 获取XDR平台硬件信息

打开XDR管理平台，在[系统管理/授权管理]，导出硬件信息，如下图。

步骤2. 获取XDR测试授权文件

打开W3企业门户（w3.sangfor.com），打开“测试设备授权”系统，填写申请测试授权信息如下图所示。

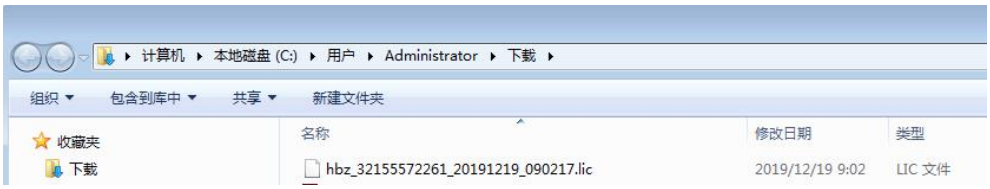


点击<立即获取>，弹出如下提示（需要记好授权ID）。

点击<立即前往> 或打开口袋助理提醒中的深信服企业门户授权平台，如下图。设备信息栏中导入步骤1中导出的XDR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3. 激活授权

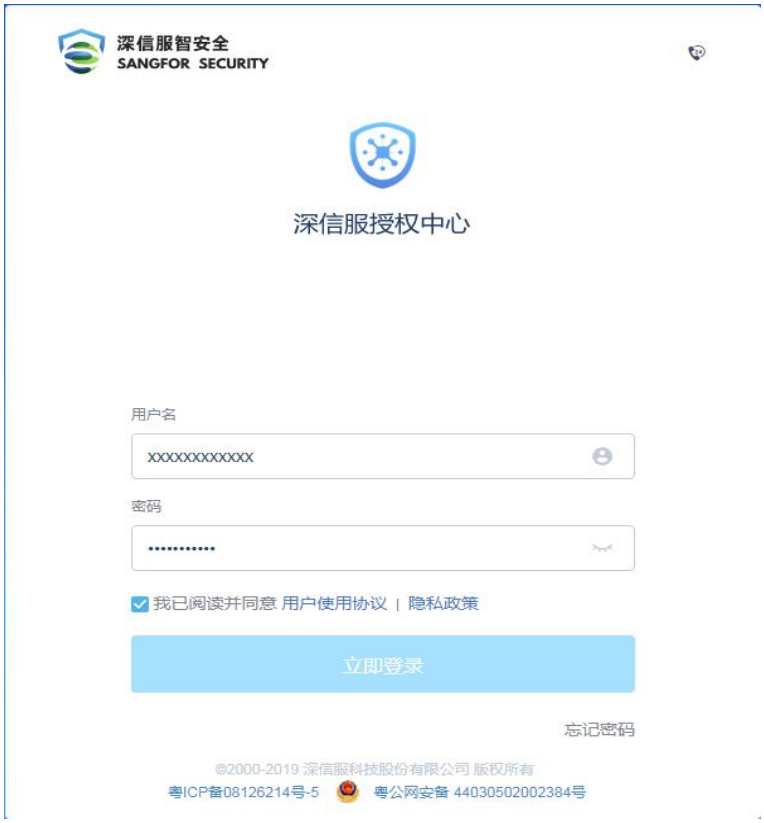
再次回到XDR管理平台授权管理页面，将步骤2获取的授权文件按下图导入，激活成功。

激活成功，如下图。

2.4.2. 已购买产品授权激活

步骤1. 授权平台导入XDR产品

打开浏览器，访问深信服授权中心地址：https://license.sangfor.com.cn，先进行用户注册，然后输入注册好的账号密码。

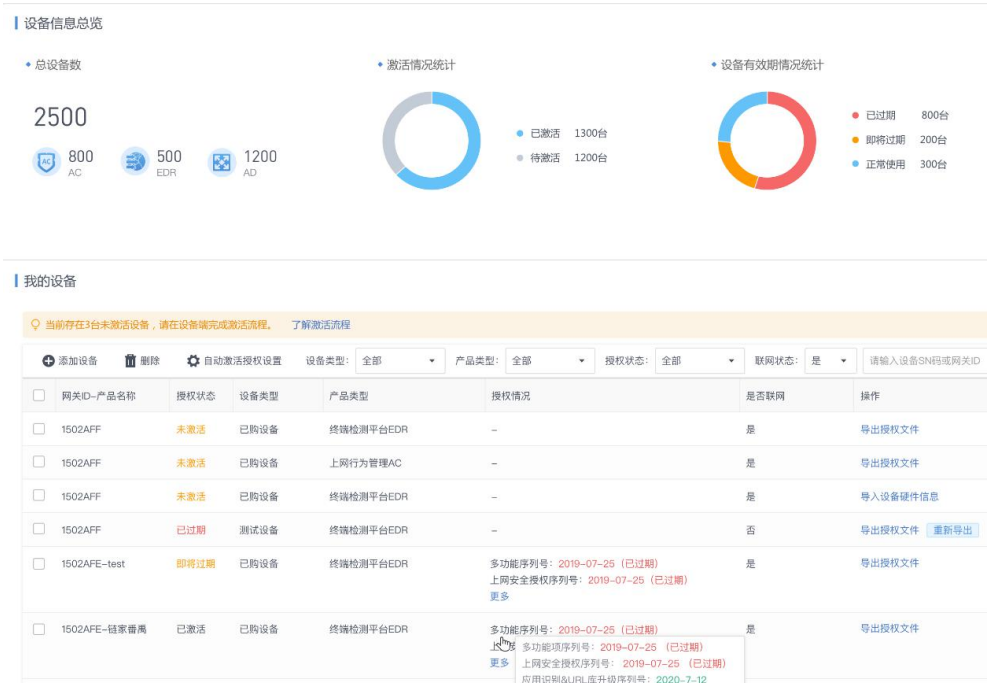


登录授权平台后，初始状态下未添加任何设备，点击<现在激活>去添加设备，如下图。

选择<通过订单号添加>，（注意，XDR开通授权只能通过下图订单号添加，不能通过网关ID添加）输入订单系统中的企业名称与订单号（企业名称与订单号可以通过渠道或销售人员获取），输入完成后点击<确认>。

导入设备成功，可以看到这个账号下绑定的所有深信服设备、激活状态、授权过期时

间等。

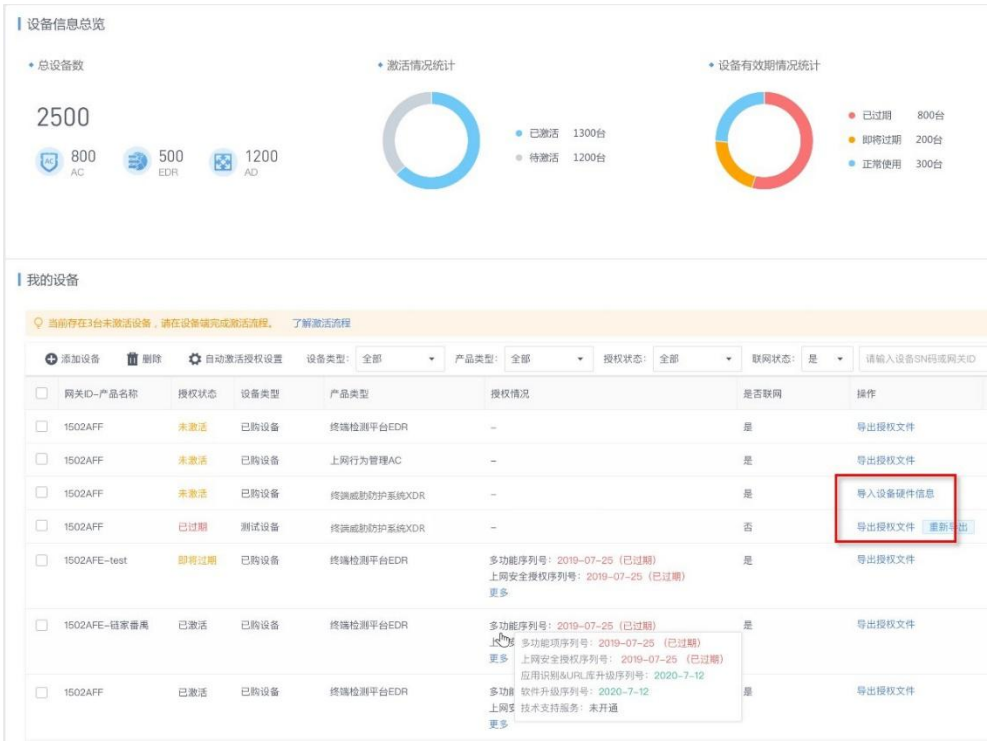


步骤2. 获取XDR平台硬件信息

拿到需要激活的XDR设备并登录，进入[系统管理/授权管理]，点击<导出设备硬件信息>，也可以点击<复制设备硬件信息>直接复制到粘贴板，二选一即可。接下来以复制设备硬件信息为例进行演示。

步骤3. 授权平台获取授权文件

再次访问深信服授权中心（https://license.sangfor.com.cn），在列表中找到对应的设备，点击<导出授权文件>。



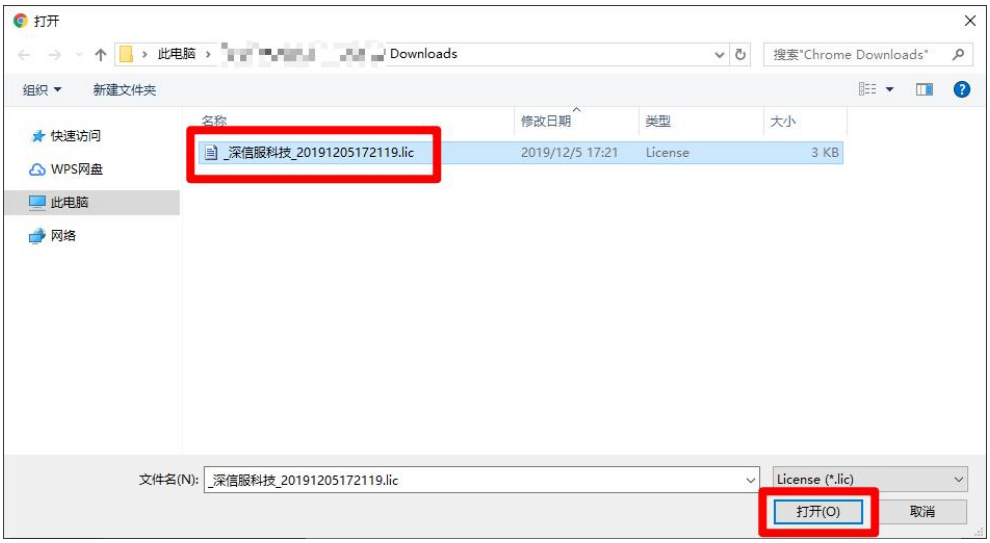
选择<以文本形式提供>，将步骤2中复制的硬件设备信息粘入，即可导出授权文件。

若步骤2选择<导出设备硬件信息文件>，那么此时选择<以文件形式提供（dev.info文件）>上传文件即可，导出的授权文件如下图。

步骤4. 激活授权

回到XDR的授权管理页面，点击<导入>。

选中第三步中获得的授权文件。



授权激活成功，如下图。

2.5. 终端 Agent 安装

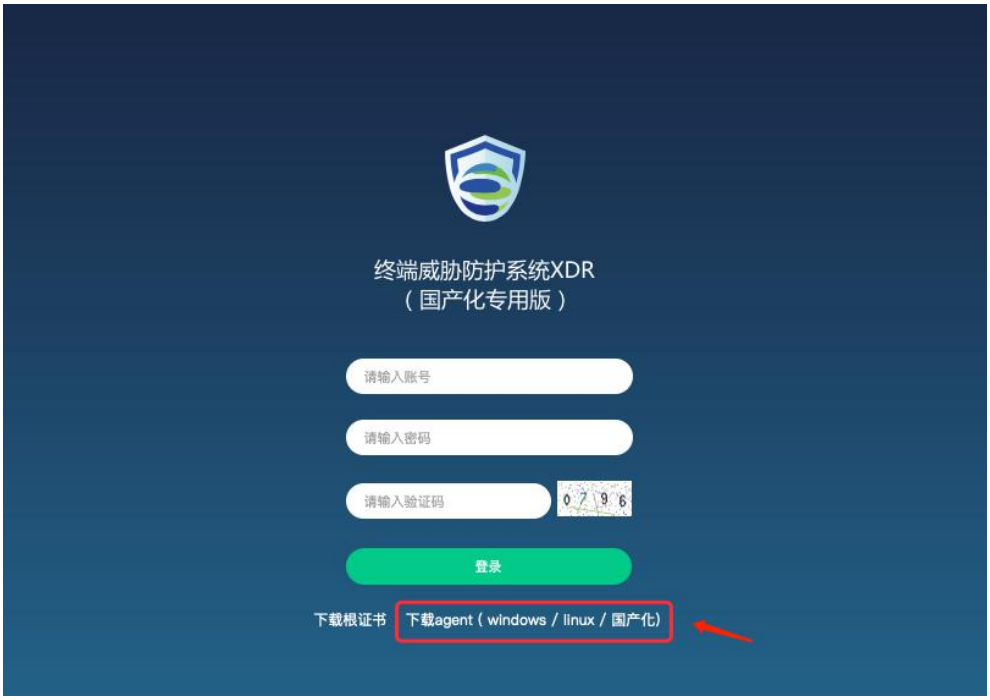
2.5.1. 下载 Agent 安装包

终端威胁防护系统搭建完成后，终端需要安装Agent从而使终端和终端威胁防护系统完成对接，实现实时保护终端端点安全。

从终端威胁防护系统的页面下载安装包，分为windows安装包、linux安装包和国产化安装包。

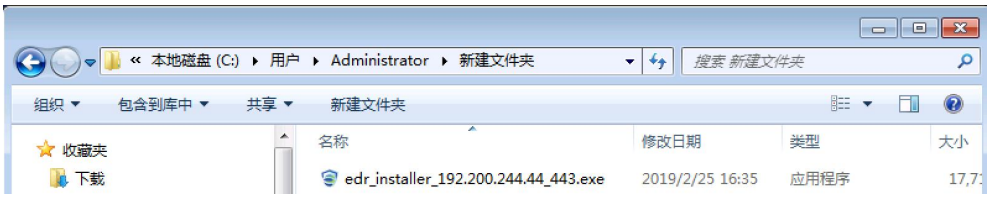
打开[系统管理/终端部署]，XDR平台Agent下载界面，下载安装包。

或者可以直接在登录控制台界面下载，如下图所示。



2.5.2. Windows 客户端安装方法

点击Windows<下载安装包>按钮，下载安装软件。



双击进行安装。

选择安装目录，默认为C:\Program Files\Sangfor\EDR\agent。

同意免责声明，点击<立即安装>，安装程序连接XDR管理平台下载必要的安装组件，如下图。

下载完成后，进入安装页面，如下图。

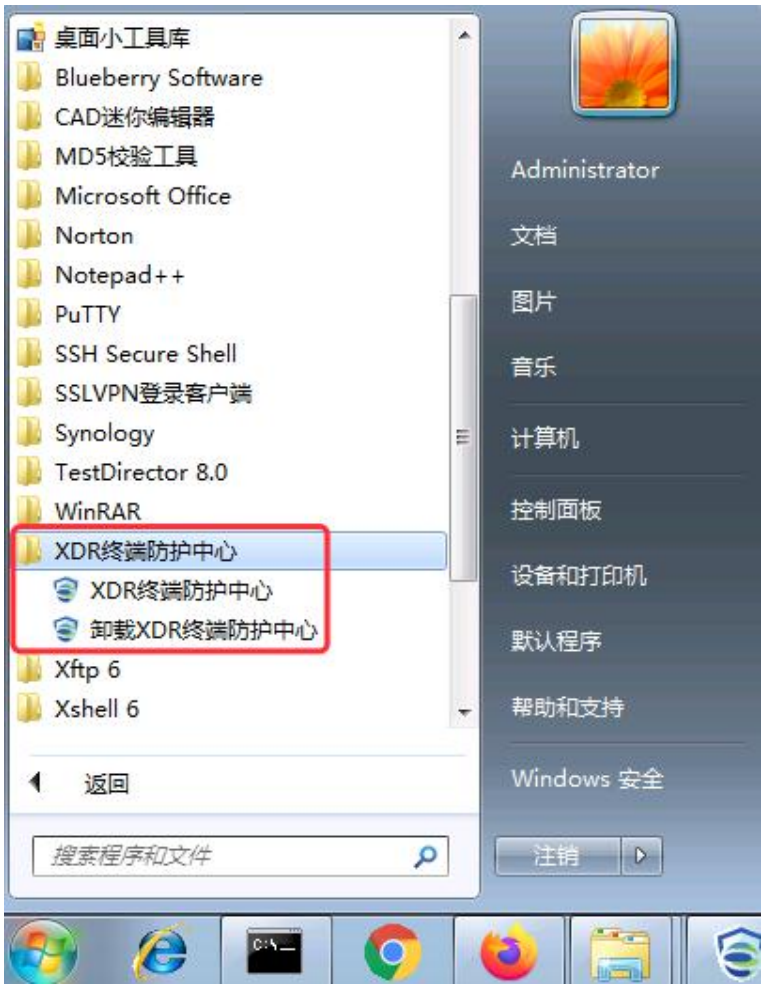
点击[开启防护]完成资产信息上报登记，如下图。

点击[保存]完成windows客户端安装，如下图。

安装完成，Agent将自动连接终端威胁防护系统，2分钟左右，在管理平台[终端管理/终端分组管理]即可看到终端上线信息，如下图。

其他说明:

1. 终端卸载Agent，通过开始菜单卸载Agent，如下图。



2. 管理员卸载Agent，通过XDR管理平台可以卸载位置[终端管理/终端分组管理/终端列表]找到对应的终端进行agent卸载,详细见“终端分组管理”章节。

2.5.3. Linux 客户端安装方法

Linux客户端有两种安装方法，详情如下。

方法一：

将安装文件上传到linux终端中，以一台64位操作系统终端为例，解压文件。

使用无参数安装，执行./agent_installer.sh。

或者

使用自定义安装(安装路径可选)./agent_installer.sh -h 管理平台地址 -p 管理平台端口（默认是443） -d 指定的安装路径 -f，即指定安装目录、管理平台IP地址和端口完成安装。

```
[root@redhat64-x64 ~]# ls
anaconda-ks.cfg  EPS_1.0_Build_20161201.tar.gz  install.log  install.log.syslog
[root@redhat64-x64 ~]# tar -zxvf EPS_1.0_Build_20161201.tar.gz
agent_installer.sh
manager_info.txt
[root@redhat64-x64 ~]# ./agent_installer.sh /home/eps/agent 200.200.128.60
start download eps module
download eps module success
/home/eps/agent install success
eps start success
[root@redhat64-x64 ~]#
```

```
[root@localhost zzp]# ./agent_installer.sh -h 10.62.7.15 -p 443 -d /home/ -t
edr agent is installing on x86_64 machines
systemd model
start download edr module
curr install path: /home/sangfor/edr/agent url:https://10.62.7.15:443
agent size is 103.9MB
[======                                                  ][11.77%]
```

方法二：

通过如下命令在Linux终端命令行方式下载agent安装包。

wget --no-check-certificate https://%管理平台IP%/html/linux_EDR_installer.tar.gz

后续安装步骤同方法一。

📖 说明：

Linux 客户端没有客户端界面。

2.5.4. 国产化客户端安装方法

下载单独的国产化客户端，国产化客户端安装的方法和linux客户端安装方法一样，请参考“linux客户端安装方法”章节介绍。

安装完成，Agent将自动连接终端威胁防护系统，2分钟左右，在管理平台[终端管理/终端分组管理]即可看到终端上线信息。

📖 说明：

国产化客户端没有客户端界面。

2.5.5. 其它安装方式

查看[系统管理/终端部署]还可以通过[网页推广部署]、 [虚拟机模板部署]。

[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，终端用户打开部署通知的web页面，自行下载agent安装包进行安装部署。

终端用户打开如下安装部署页面，自行下载安装包进行安装。

[虚拟机模板部署]管理员在虚拟化平台上通过虚拟机模板实现对虚拟机的镜像部署。

其他说明：

1. XDR需要联网更新特征库，为得到及时有效的防护，请确保管理平台和Agent客户端可以连接互联网，并且到以下服务器连通性正常。

   auth.sangfor.com.cn

   upd.sangfor.com.cn

   download.sangfor.com.cn

   analysis.sangfor.com.cn

   clt.sangfor.com.cn

2. XDR正常使用需要放行终端连接管理平台443、8083、54120三个端口，请确保环境中终端到管理端上述端口正常通信。

3. XDR 管理平台使用

3.1. 登录 XDR 管理平台

终端威胁防护系统支持安全的HTTPS登录，使用的是HTTPS标准端口登录。默认登录URL为https://XDR_IP。

首先打开浏览器，在地址栏输入https://XDR_IP，然后在浏览器中输入默认登陆IP及端口https://XDR_IP。出现一个如下图的安全提示。

点击<是>后进入终端威胁防护系统控制台登录界面如下图所示。

在登录框输入用户名和密码、验证码，点击<登录>按钮即可登录终端威胁防护系统进行配置，默认的用户名和密码为：admin/admin。

为了保护平台安全性，登录控制台后提示管理员修改初始密码，如下图。

登录控制面板不需要安装任何控件，支持使用IE10以上/Firefox/Chrome等浏览器登录使用。

3.2. 首页

登录终端威胁防护系统后即可看到[首页]，包含[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]。为管理员提供端点整体运行状态的查看页面。

同时展示了XDR守护全网终端安全的时间，版本和病毒库版本情况等信息，如下图所示。

[终端概况]：可以查看接入终端的总数，在线和离线的数量情况，终端类型数量情况，监听端口和帐号数量。以及最近7天的安全威胁防御情况。

[待处理高危事件]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。可点击进行跳转到响应中心并自动进行筛选，查看详细情况。

[勒索病毒防御]呈现勒索病毒防护体系介绍入口和XDR在最近7天内，协助客户处置了多少个勒索病毒，通过勒索诱饵组织了多少可疑勒索行为，通过服务器加固功能拦截了多少不可信进程（未知进程）的操作，同时通防暴力破解功能协助客户阻断了多少次暴力破解的攻击。

勒索防御体系介绍在预防、防护、检测和响应每个阶段XDR的防护手段和功能，同时告知客户当前的配置情况，引导客户进行功能的启用和配置。

[4层勒索入侵预防]包括漏洞检测及补丁修复、安全基线检查、深信服SAVE人工智能引擎防御未知勒索病毒、微隔离的横向传播控制。绿色表示功能已开启、黄色按钮表示功能未开启，点击黄色按钮跳转到策略配置页面进行配置。

[5级勒索反加密防护]包括文件实时防护防止勒索程序落地和运行、勒索诱饵防护阻止勒索的进一步加密、防暴力破解防护、服务器关键目录防护和服务器可信进程防护。绿色表示功能已开启、黄色按钮表示功能未开启，点击黄色按钮跳转到策略配置页面进行配置。

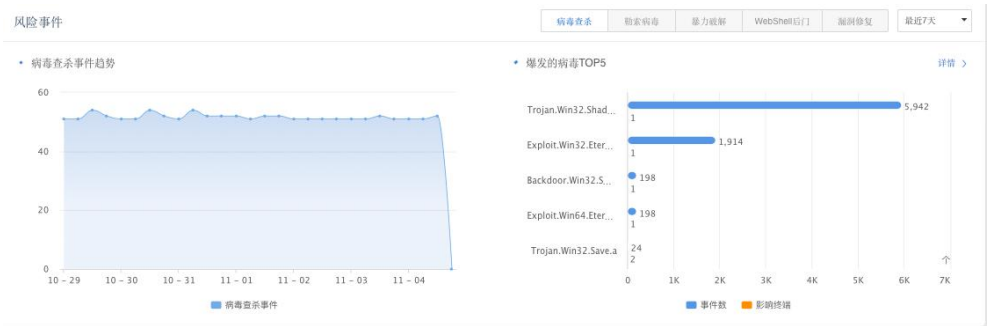
[5项勒索检测和响应机制]包括勒索病毒检测和查杀、被感染终端的一键网络隔离、情报的全网威胁快速定位、勒索病毒的已知解密工具提供、勒索病毒的威胁分析百科。

[威胁终端分布统计]中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/威胁响应]中。

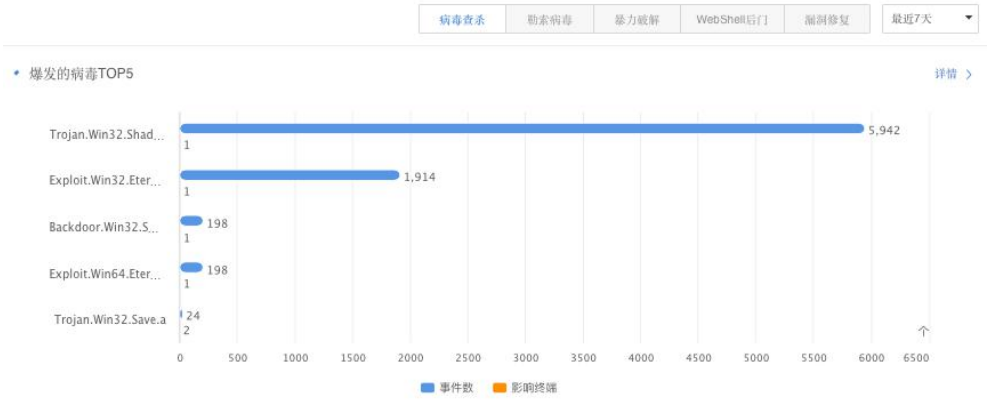
[病毒查杀事件趋势]统计7天、30天、90天内发现的病毒事件数量，包括勒索病毒事件、木马病毒事件和其他病毒事件。

[爆发的病毒TOP5]：列出终端上出现最多的5种病毒，可点击<详情>进行查看。



右上角可以选择查看[暴力破解]、[webshell后门]、[漏洞修复]等情况，并且可以选择

数据统计的天数。



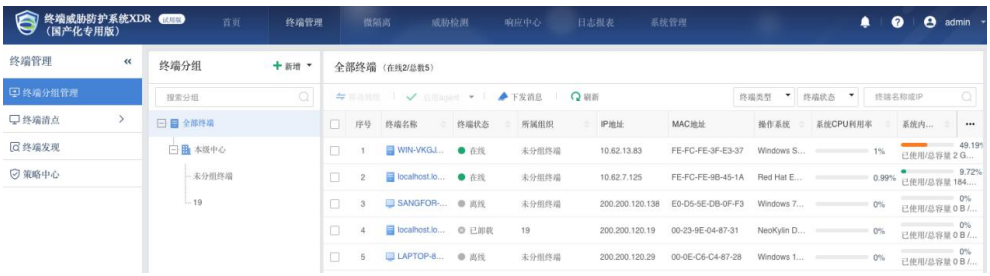
[全球热点威胁]显示全球最热点、威胁最大的安全事件及其在网内终端的爆发情况。

3.3. 终端管理

终端管理包括[终端分组管理]、[终端清点]、[终端发现]和[策略中心]。

3.3.1. 终端分组管理

打开[终端管理/终端分组管理]，如下图。



[终端分组管理]用于管理接入的终端，并通过分组的方式进行管理,显示终端的一些基本信息，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、最近接入时间，可以在上图右侧[...]处打开进行勾选需要展示的信息。

当终端的agent安装好后，会自动上线到[终端分组管理]的[未分组终端]中。

点击新增右侧的下三角，会弹出如下图所示。

点击<新增>及新增终端分组。

其中：

[分组名称]定义分组的名称。

[终端自动分组]点击<启用>，并配置IP范围，将上线的IP地址属于该范围时，会上线到对应的分组中。

配置完成后点击<确定>进行提交。

点击<导入分组>及可将通过excel填写好的终端信息一次性导入到XDR中。

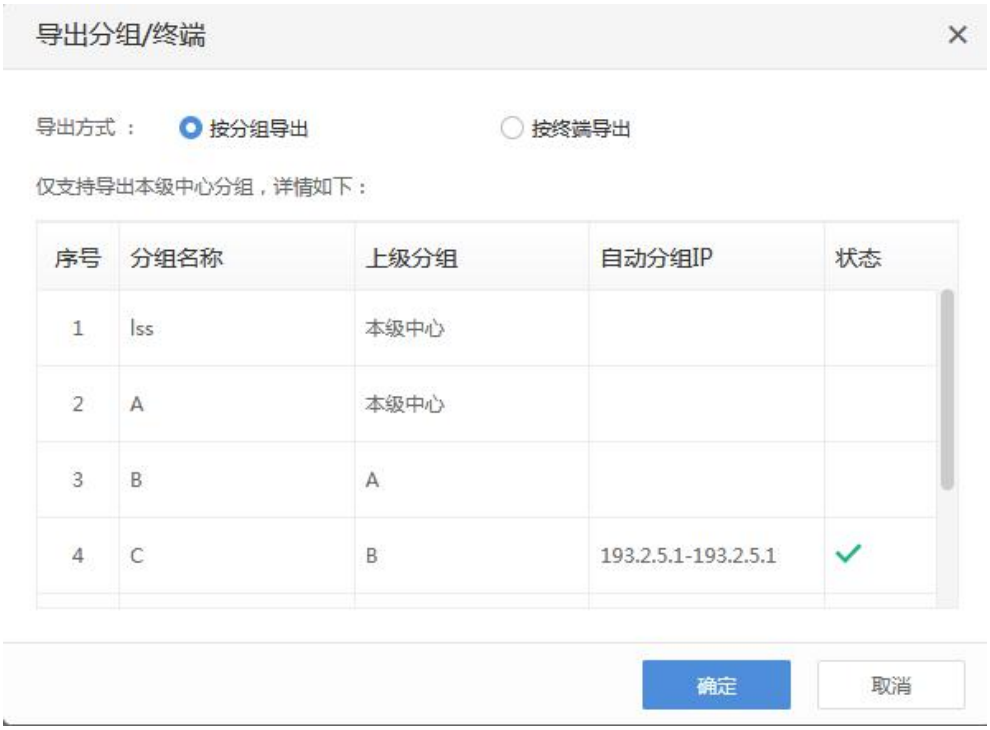
建议先下载示例文件如下。

	A	B	C	D
1	分组名	上级分组	自动分组IP段	状态
2	示例1	本级中心	192.168.0.1-192.168.0.255;192.168.1.1-192.168.1.255	禁用
3	示例2	示例1	192.168.2.1;192.168.3.1/16;192.168.4.1/255.255.255.0	启用
4	示例3	示例2		
5				
6				

按导出的示例文件将终端信息填写好，进行上传，选择导入方式，点击<确认>提交。

点击<导出分组/终端>将当前XDR上的所有终端信息导出到excel表格中。

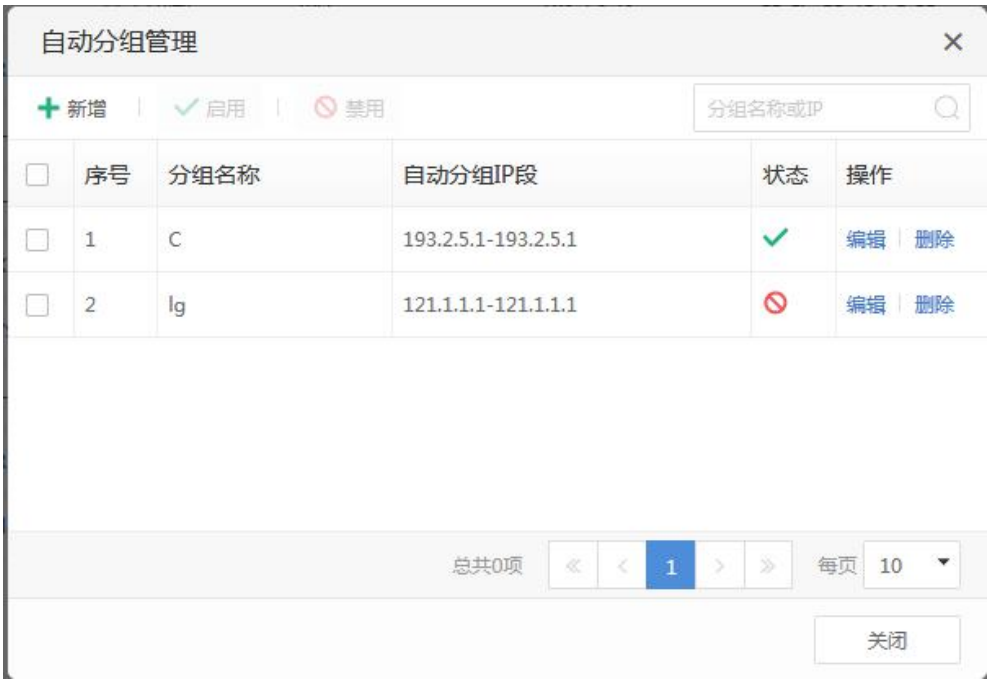
可选择导出方式为按分组导出或按终端导出，按分组导出如下图。



按终端导出如下图，可选择范围。

导出后的终端excel信息如下图所示。

最后点击<自动分组管理>，如下图。对终端自动分组进行统一管理，自动分组的IP段不能存在冲突。可以新增，也可以对已存在的分组进行启用、禁用或者编辑、删除。



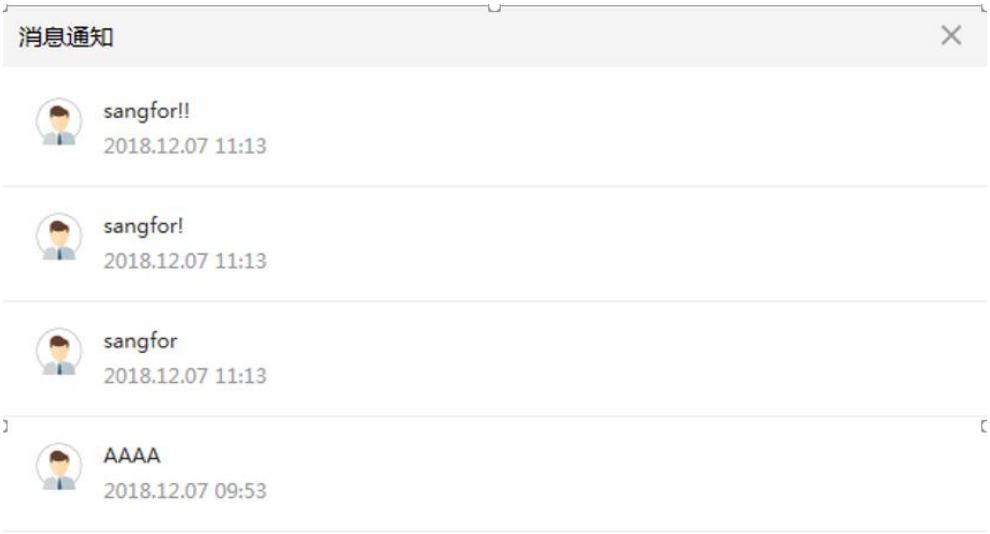
[启用agent]、[禁用agent]、[卸载agent]、[移除终端]当发现客户端安装Agent存在异常时，可以从管理端对当前终端进行启用、禁用、卸载操作。当需要释放授权数量，需要先将终端agent卸载，同时从管理端移除已卸载的终端。

[下发消息]可以在XDR管理平台上对安装了客户端的windows终端进行消息提示。

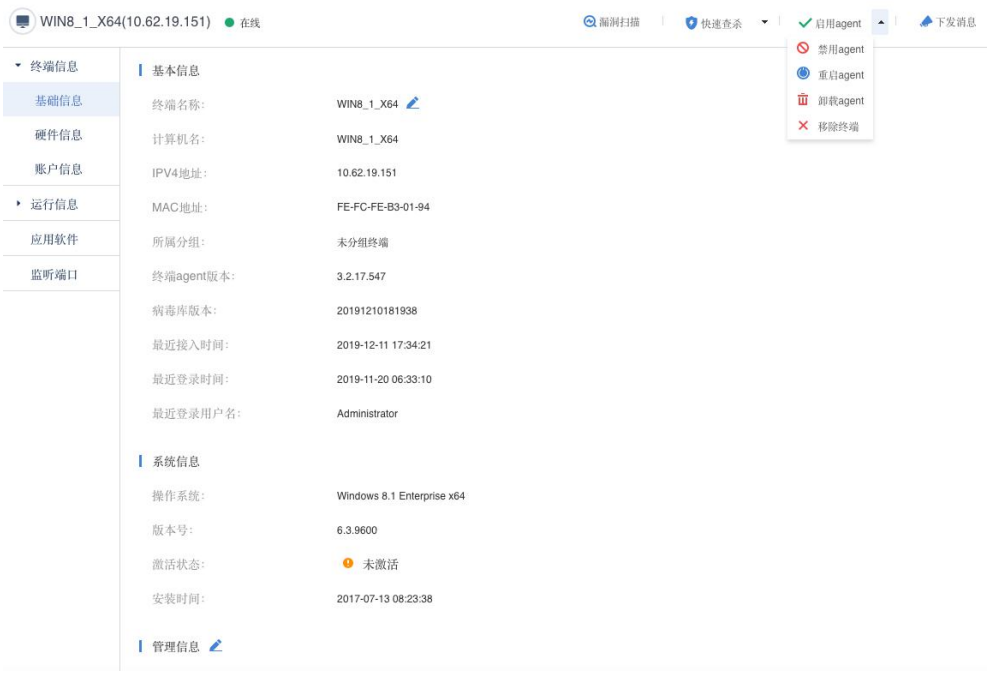
点击<确认>，终端接收到的通知消息如下图。

终端上可以点击“知道了”或点右上角的x关闭信息。当选择关闭信息时，客户端右上角会有一个小红点。

点击<通知>，查看历史的通知消息。



点击具体的终端名称可查看终端的详细信息。终端详情包括[终端信息]、[运行信息]、[应用软件]和[监听端口]。



终端详情页面的终端名称右边是对当前终端的常见操作，常见操作的内容如下：

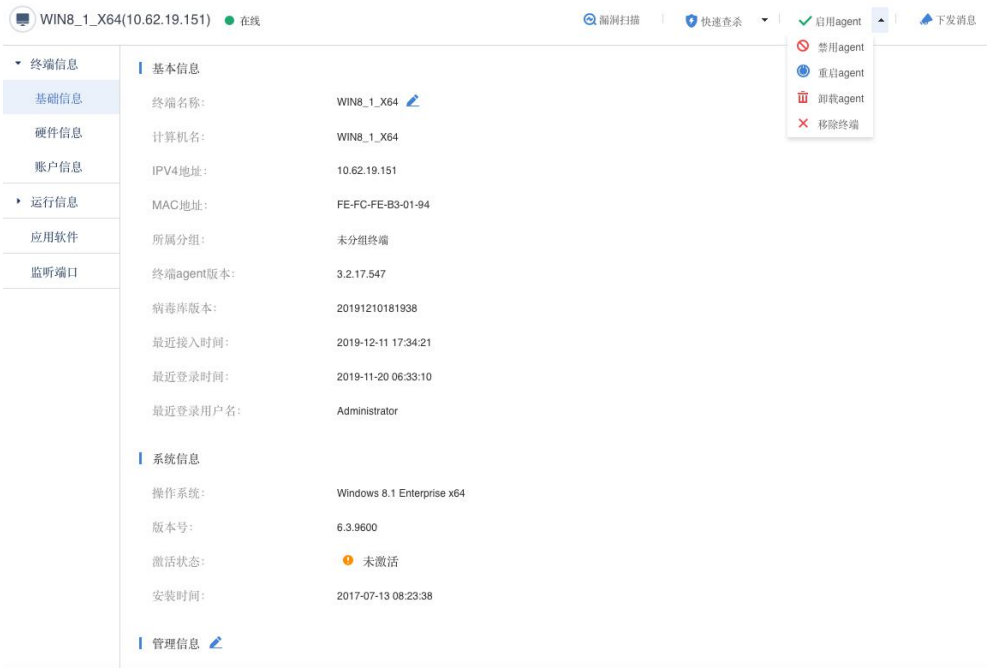
[漏洞扫描]漏洞扫描的快捷入口，可以对当前终端进行系统漏洞检测。

[快速查杀]、[全盘查杀]病毒查杀的快捷入口，可以选择对当前终端进行快速病毒查杀或全盘病毒查杀。

[启用agent]、[禁用agent]、[卸载agent]、[移除终端]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。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。

[下发消息]可以在XDR管理平台上对该客户端下发通知信息，并在客户端提示。

[终端信息]包括[基础信息]、[硬件信息]和[帐号信息]，如下图。



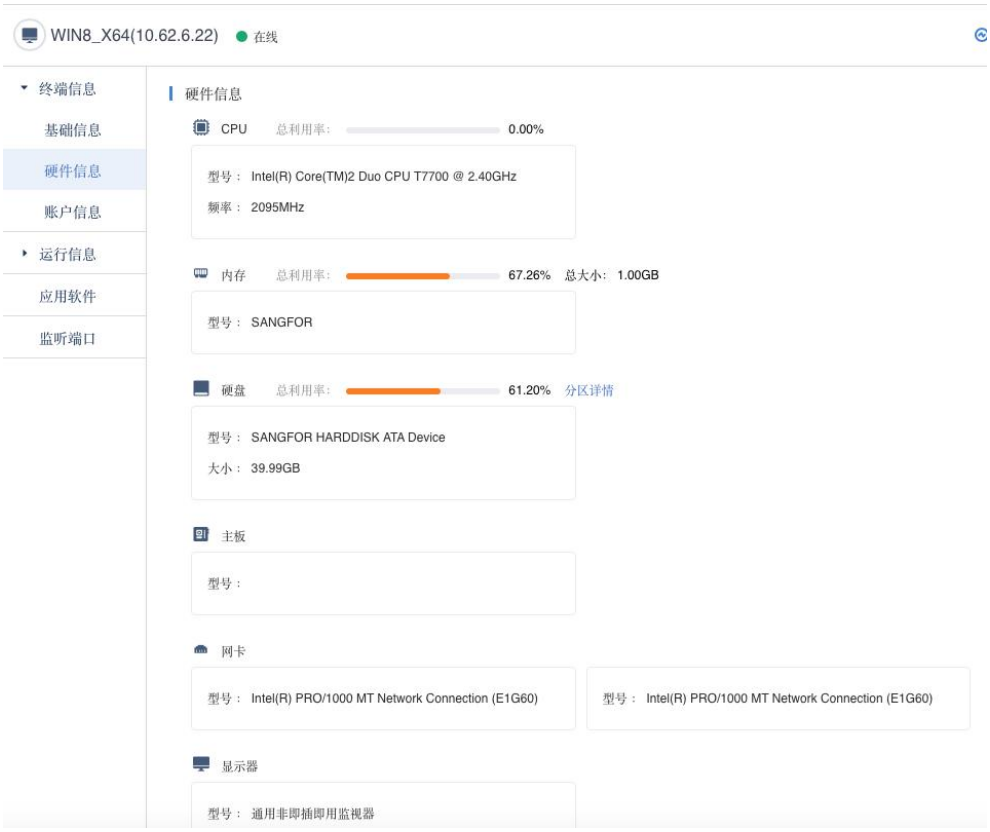
[基础信息]包括该终端的[基本信息]、[系统信息]和[管理信息]。

其中[基本信息]包括终端终端名称、计算机名称、IP地址等信息，详细如下图。

[系统信息]包括该终端的操作系统、操作系统版本号、操作系统激活状态及操作系统安装时间，如下图。

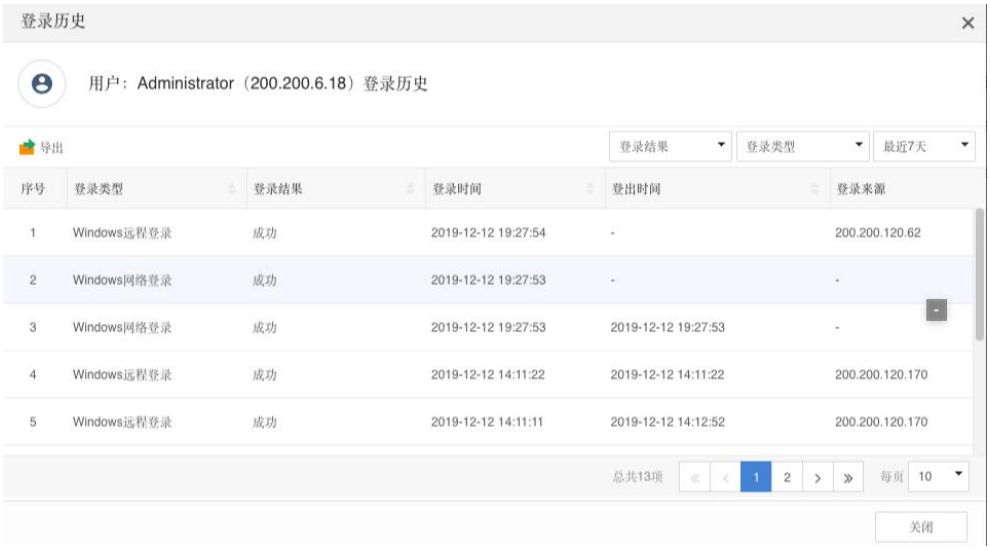
[管理信息]包括该主机责任人、资产编号、资产位置等信息，如下图。

[硬件信息]包括该终端的CPU、内存、硬盘、主板、网卡、显示器等详细硬件信息，如下图。

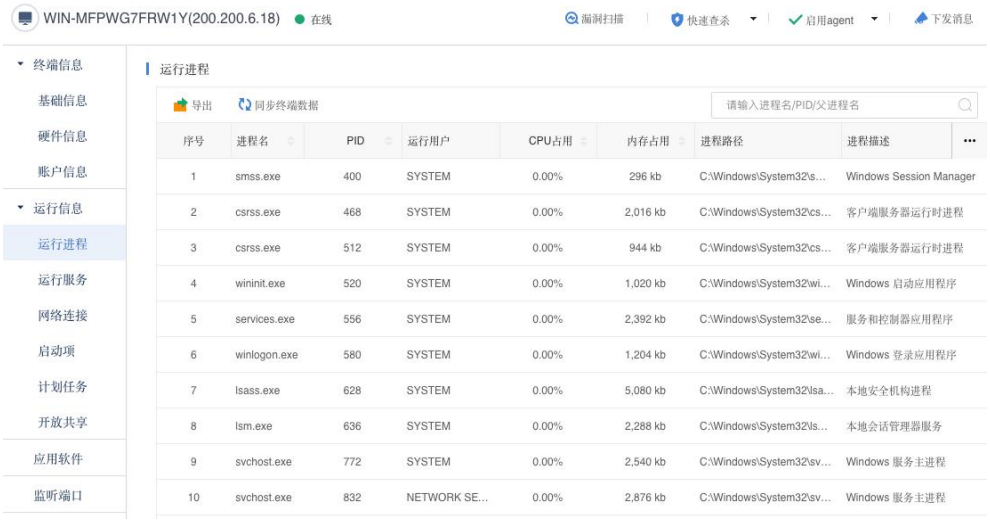


[账户信息]列举了该终端所有系统帐户的帐户名、账户状态、过期时间等详情信息，管理员可以通过采集的账户信息判断是否存在风险帐号，如下图。

具体的<登录历史>，查看该系统帐号的详细登录信息，如下图。



[运行信息]包括该终端[运行进程]、[运行服务]、[网络链接]、[启动项]、[计划任务]和[开放共享]信息，如下图。

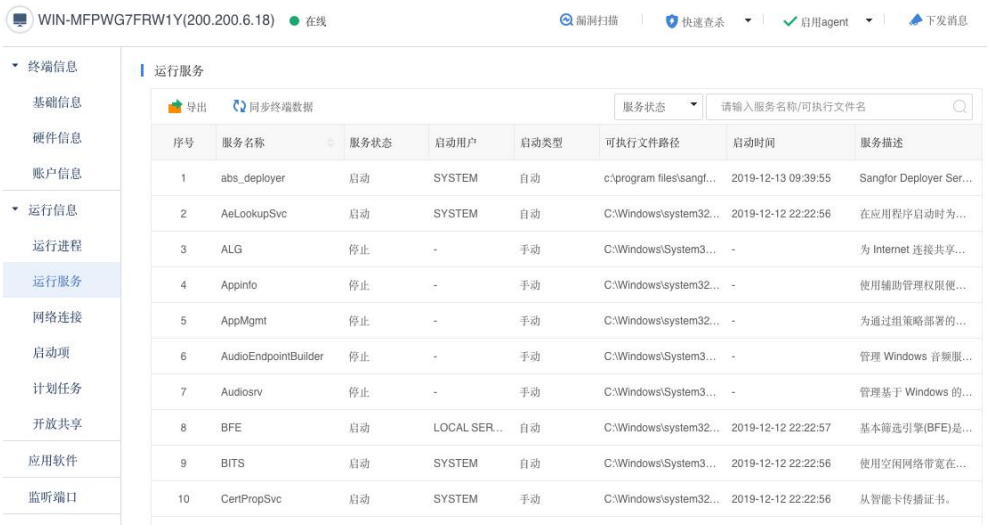


[运行进程]采集该终端所有运行的进程信息，包括进程名、运行用户、CPU占用、内存占用等信息。点击 同步终端数据 ，触发管理端下发采集进程指令，点击 导出 将终端当前运行的进程信息以表格形式导出，方便管理员进一步分析，如下图。

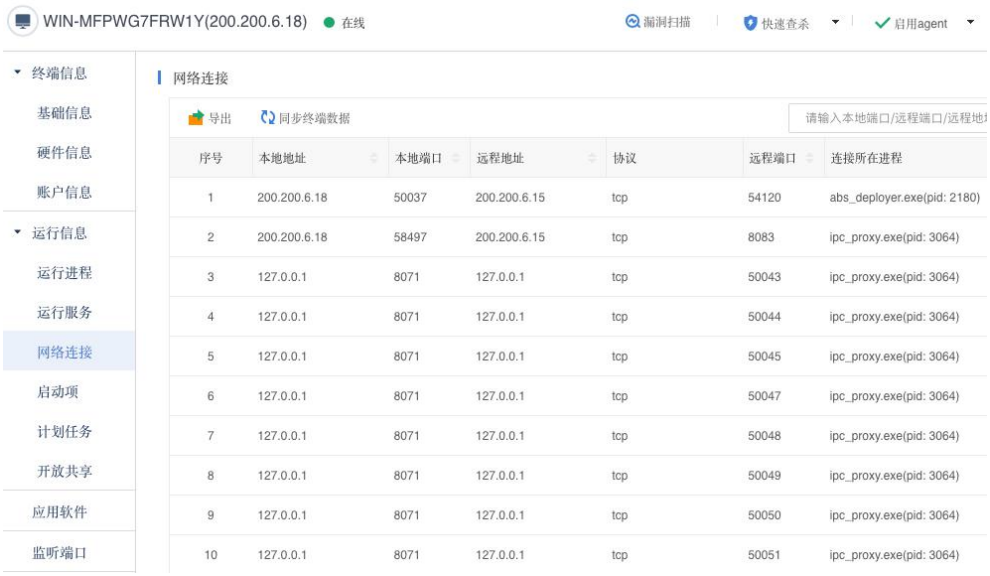
终端运行进程列表

汇总信息	符合查询条件的记录总数为47条，当前共导出47条										
查询条件											
进程名/PID/父	所有										
查询结果											
序号	进程名	PID	运行用户	CPU占用	内存占用	进程路径	进程描述	启动参数	启动时间	父进程名	父进程ID
1	smss.exe	400	SYSTEM	0%	296K	C:\Windows\System32\s	Windows Session Manag	\SystemRoot\System32\	2019-12-12 22:22:52		4
2	csrss.exe	468	SYSTEM	0%	2016K	C:\Windows\System32\s	客户端服务器运行时进	C:\Windows\system32\c	2019-12-12 22:22:54		456
3	csrss.exe	512	SYSTEM	0%	944K	C:\Windows\System32\s	客户端服务器运行时进	C:\Windows\system32\c	2019-12-12 22:22:54		504
4	wininit.exe	520	SYSTEM	0%	1020K	C:\Windows\System32\w	Windows 启动应用程序	wininit.exe	2019-12-12 22:22:54		456
5	services.exe	556	SYSTEM	0%	2392K	C:\Windows\System32\s	服务和控制器应用程序	C:\Windows\system32\s	2019-12-12 22:22:55	wininit.exe	520
6	winlogon.exe	580	SYSTEM	0%	1204K	C:\Windows\System32\w	Windows 登录应用程序	winlogon.exe	2019-12-12 22:22:55		504
7	lsass.exe	628	SYSTEM	0%	5080K	C:\Windows\System32\l	本地安全机构进程	C:\Windows\system32\l	2019-12-12 22:22:55	wininit.exe	520
8	lsm.exe	636	SYSTEM	0%	2288K	C:\Windows\System32\l	本地会话管理器服务	C:\Windows\system32\l	2019-12-12 22:22:55	wininit.exe	520
9	svchost.exe	772	SYSTEM	0%	2540K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:22:56	services.exe	556
10	svchost.exe	832	NETWORK SERVICE	0%	2876K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:22:56	services.exe	556
11	LogonUI.exe	900	SYSTEM	0%	6144K	C:\Windows\System32\L	Windows Logon User Int	"LogonUI.exe"	2019-12-12 22:22:56	winlogon.exe	580
12	svchost.exe	908	LOCAL SERVICE	0%	5260K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\System32\s	2019-12-12 22:22:56	services.exe	556
13	svchost.exe	956	SYSTEM	0%	2172K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:22:56	services.exe	556
14	svchost.exe	968	SYSTEM	0%	14252K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:22:56	services.exe	556
15	SLsvc.exe	988	NETWORK SERVICE	0%	6376K	C:\Windows\System32\S	Microsoft 软件授权服务	C:\Windows\system32\S	2019-12-12 22:22:56	services.exe	556
16	svchost.exe	1040	LOCAL SERVICE	0%	3168K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:22:57	services.exe	556
17	svchost.exe	1092	SYSTEM	0%	4020K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:22:57	services.exe	556
18	svchost.exe	1120	NETWORK SERVICE	0%	7668K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:22:57	services.exe	556
19	svchost.exe	1280	LOCAL SERVICE	0%	4008K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:22:57	services.exe	556
20	spoolsv.exe	1460	SYSTEM	0%	3736K	C:\Windows\System32\s	后台处理程序子系统应	C:\Windows\system32\s	2019-12-12 22:23:03	services.exe	556
21	svchost.exe	1672	NETWORK SERVICE	0%	1288K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:23:04	services.exe	556
22	svchost.exe	1696	LOCAL SERVICE	0%	684K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\system32\s	2019-12-12 22:23:04	services.exe	556
23	svchost.exe	1836	SYSTEM	0%	1128K	C:\Windows\System32\s	Windows 服务主进程	C:\Windows\System32\s	2019-12-12 22:23:04	services.exe	556
24	taskeng.exe	2136	SYSTEM	0%	1936K	C:\Windows\System32\t	任务计划程序引擎	taskeng.exe {DFC36893-I	2019-12-12 22:23:07	svchost.exe	968
25	msdtc.exe	2788	NETWORK SERVICE	0%	2320K	C:\Windows\System32\M	MS DTCconsole 程序	C:\Windows\System32\r	2019-12-12 22:25:06	services.exe	556
26	abs_deployer.exe	2180	SYSTEM	0%	1296K	C:\Program Files\Sangfor	Sangfor Deployer Service	"c:\program files\sangfor	2019-12-13 09:39:55	services.exe	556
27	sfavsvc.exe	2492	SYSTEM	0%	265492K	C:\Program Files\Sangfor	Sangfor Defender Antivir	"c:\program files\sangfor	2019-12-13 09:39:58	services.exe	556
28	edr_monitor.exe	2216	SYSTEM	0%	1644K	C:\Program Files\Sangfor	Sangfor Monitor Service	"c:\program files\sangfor	2019-12-13 09:40:01	services.exe	556
29	sfupdatemgr.exe	3188	SYSTEM	0%	2332K	C:\Program Files\Sangfor		"c:/program files/sangfor	2019-12-13 09:40:02	edr_monitor.exe	2216
30	ipc_proxy.exe	3064	SYSTEM	0%	1728K	C:\Program Files\Sangfor		"c:/program files/sangfor	2019-12-13 09:40:02	edr_monitor.exe	2216
31	edr_agent.exe	3592	SYSTEM	0%	30552K	C:\Program Files\Sangfor		"c:/program files/sangfor	2019-12-13 09:40:02	edr_monitor.exe	2216
32	edr_sec_plan.exe	1060	SYSTEM	0%	1576K	C:\Program Files\Sangfor		"c:/program files/sangfor	2019-12-13 09:40:02	edr_monitor.exe	2216
33	UI0Detect.exe	3164	SYSTEM	0%	1892K	C:\Windows\System32\U	交互服务检测	C:\Windows\system32\U	2019-12-13 09:40:02	services.exe	556
34	csrss.exe	6912	SYSTEM	0%	1804K	C:\Windows\System32\c	客户端服务器运行时进	C:\Windows\system32\c	2019-12-16 11:23:18		7188
35	winlogon.exe	7540	SYSTEM	0%	1420K	C:\Windows\System32\w	Windows 登录应用程序	winlogon.exe	2019-12-16 11:23:19		7188
36	taskeng.exe	5516	Administrator	0%	2524K	C:\Windows\System32\t	任务计划程序引擎	taskeng.exe {BD88BA2D-(	2019-12-16 11:23:20	svchost.exe	968
37	rdpclip.exe	6872	Administrator	0%	1136K	C:\Windows\System32\r	RDP Clip 监视程序	rdpclip	2019-12-16 11:23:20	svchost.exe	1120
38	dwm.exe	6624	Administrator	0%	1148K	C:\Windows\System32\d	桌面窗口管理器	"C:\Windows\system32\	2019-12-16 11:23:20	svchost.exe	1092
39	explorer.exe	7508	Administrator	0%	9476K	C:\Windows\explorer.exe	Windows 资源管理器	C:\Windows\Explorer.EX	2019-12-16 11:23:21		7240
40	WerFault.exe	6452	Administrator	0%	2176K	C:\Windows\System32\W	Windows 问题报告	C:\Windows\System32\W	2019-12-16 11:23:21		5052
41	sfavui.exe	6464	Administrator	0%	16708K	C:\Program Files\Sangfor	Sangfor Defender Antivir	"c:\program files\sangfor	2019-12-16 11:23:23	sfavsvc.exe	2492

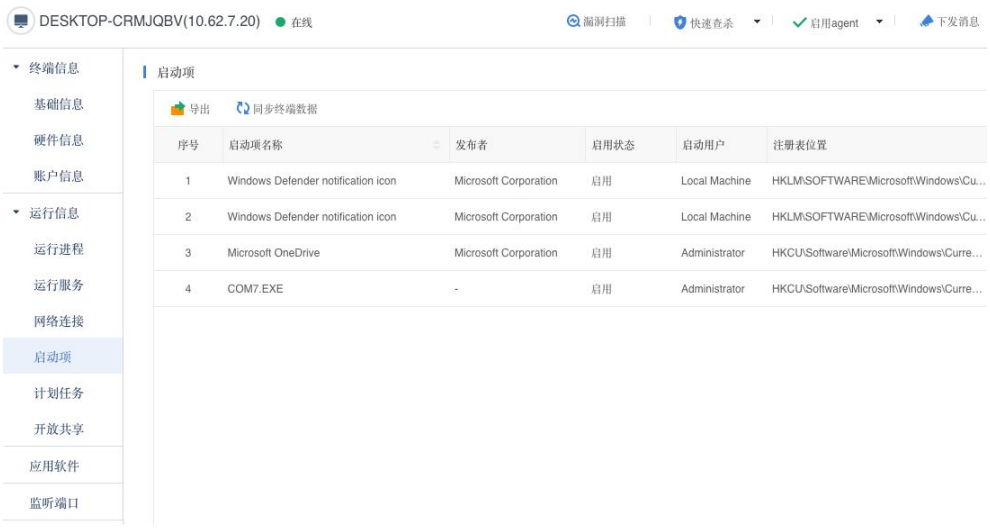
[运行服务]采集该终端所有运行的服务信息，包括服务名称、服务状态、启动用户等信息。点击 同步终端数据，触发管理端下发采集运行服务指令，点击 导出 将终端当前运行的服务信息以表格形式导出，方便管理员进一步分析。



[网络连接]采集该终端当前网络连接信息，包括本地地址、本地端口、远程地址、远程端口、协议等信息。点击 同步终端数据，触发管理端下发采集网络连接指令，点击 导出 将终端当前的网络连接以表格形式导出，方便管理员进一步分析。



[启动项]采集该终端启动项信息，包括启动项名称、发布者、启用状态等信息。点击 同步终端数据，触发管理端下发采集启动项指令，点击 导出 将终端当前的启动项以表格形式导出，方便管理员进一步分析。

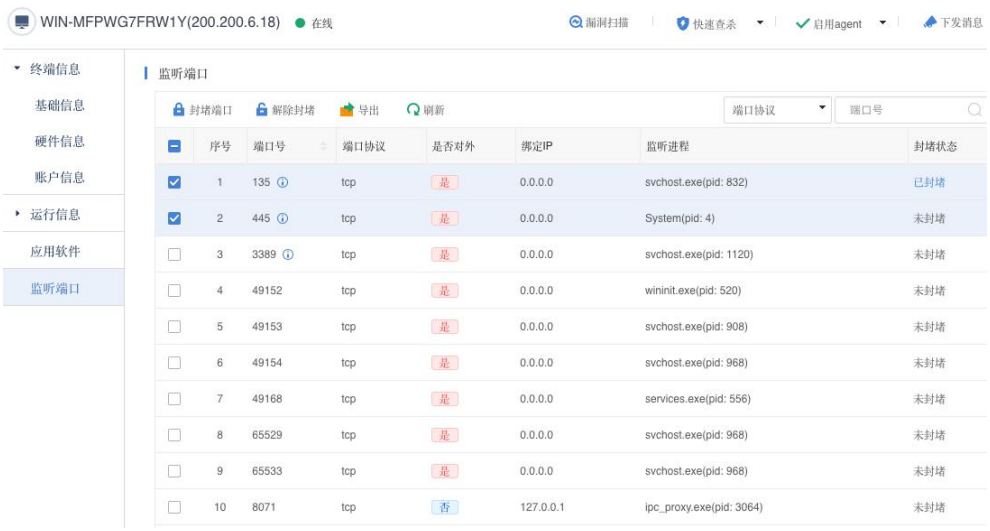


[计划任务]采集该终端计划任务信息，包括计划任务名称、执行信不信脚本、定时执行时间等信息。点击 同步终端数据，触发管理端下发采集计划任务指令，点击 导出 将终端当前的计划任务以表格形式导出，方便管理员进一步分析。

[开放共享]采集该终端共享目录或文件信息，包括共享名称、共享状态、共享路径等信息。点击同步终端数据，触发管理端下发采集共享信息指令，点击导出将终端当前的共享信息以表格形式导出，方便管理员进一步分析。

[应用软件]采集该终端安装的软件信息，包括软件名称、软件类型、软件版本等信息。点击导出将终端当前的共享信息以表格形式导出，方便管理员进一步分析。

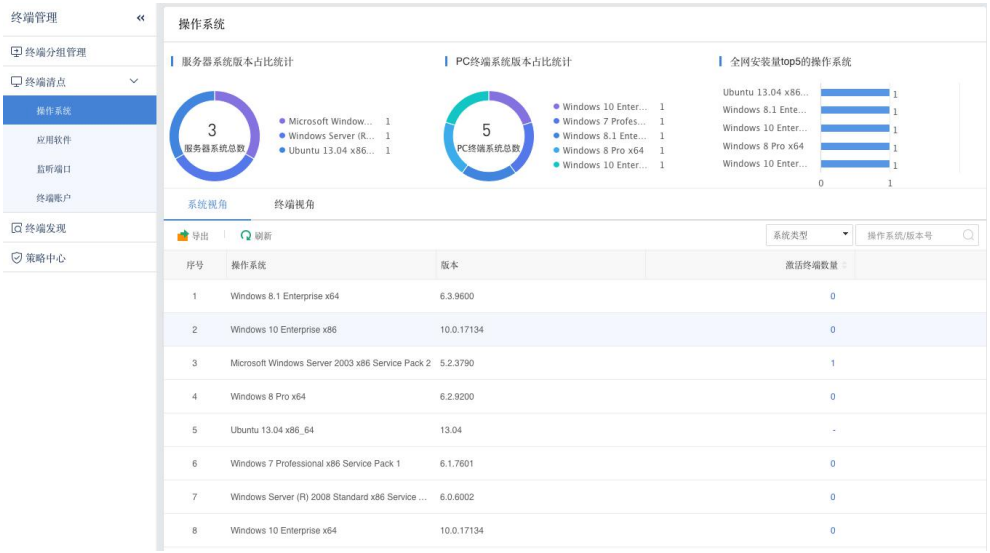
[监听端口]采集该终端的监听端口信息，包括端口号、端口协议、监听进程等信息。点击导出将终端当前的共享信息以表格形式导出，方便管理员进一步分析。



当发现风险端口时，选中此端口，点击 封堵端口，即可封堵终端的风险端口；点击 解除封堵将终端当前正处于被封堵状态的端口解除封堵。

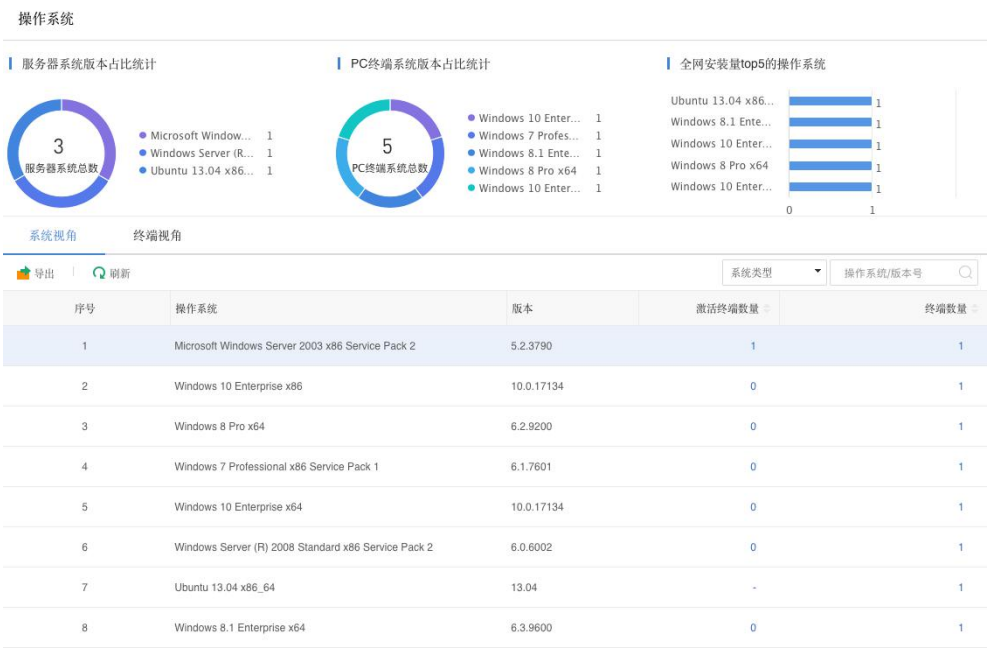
3.3.2. 终端清点

终端清点是指清点全网终端的操作系统、应用软件、监听端口和终端账户，如下图。



3.3.2.1. 操作系统

清点全网主机的操作系统版本及分布，以便对全网主机的系统有个全貌了解，如下图。



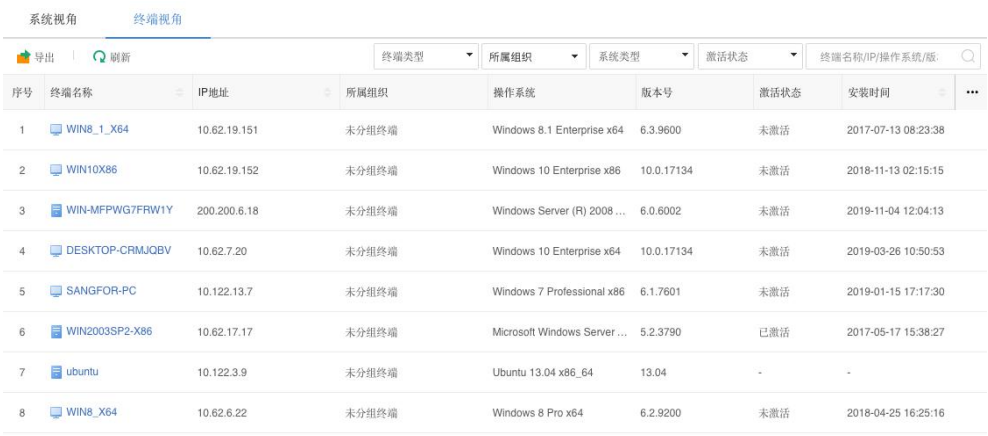
[服务器系统版本占比统计]采集全网服务器系统版本并统计版本分布情况。

[PC终端系统版本占比统计]采集全网PC终端系统版本并统计版本分布情况。

[全网安装量top5的操作系统]采集全网终端操作系统版本并按top5排行。

[系统视角]以系统为视角列出全网安装该系统的终端数量及激活系统的终端数量，点击终端数量或激活终端数量这两列的数字，显示安装该系统的终端详情，如下图。

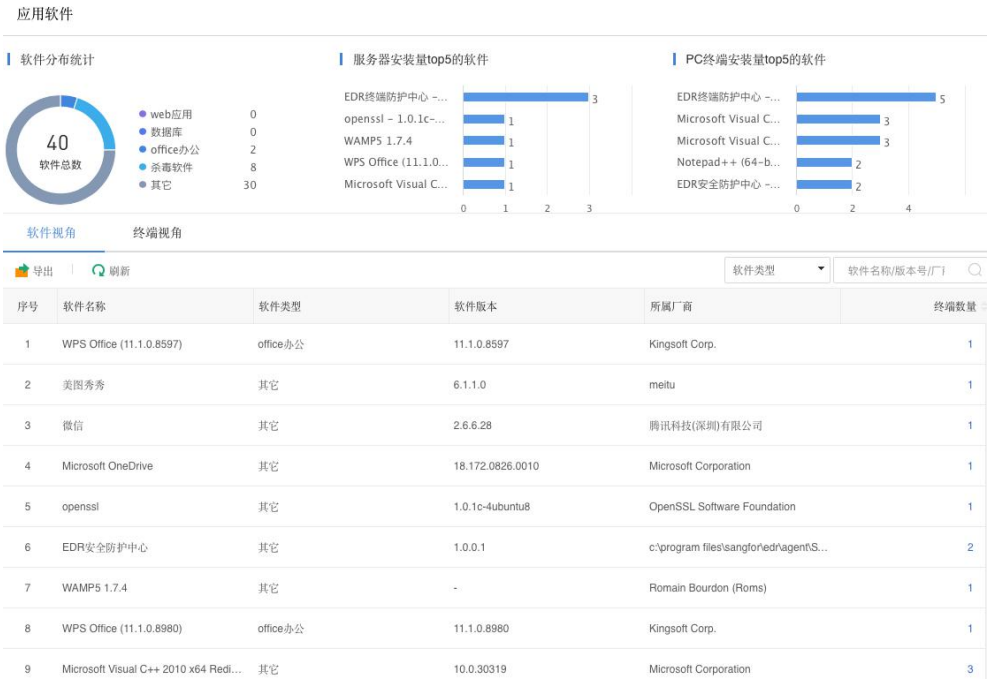
[终端视角]以终端为视角列出终端安装的操作系统类型、版本号及安装时间等信息，如下图。



点击  按钮，以表格形式导出，方便管理员进一步统计分析。同时可以根据终端类型、所属组织、系统类型、激活状态等条件进一步筛选。

3.3.2.2. 应用软件

统计全网主机安装软件汇总信息和详细信息，分别从软件视角和终端视角进行统计展示，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。



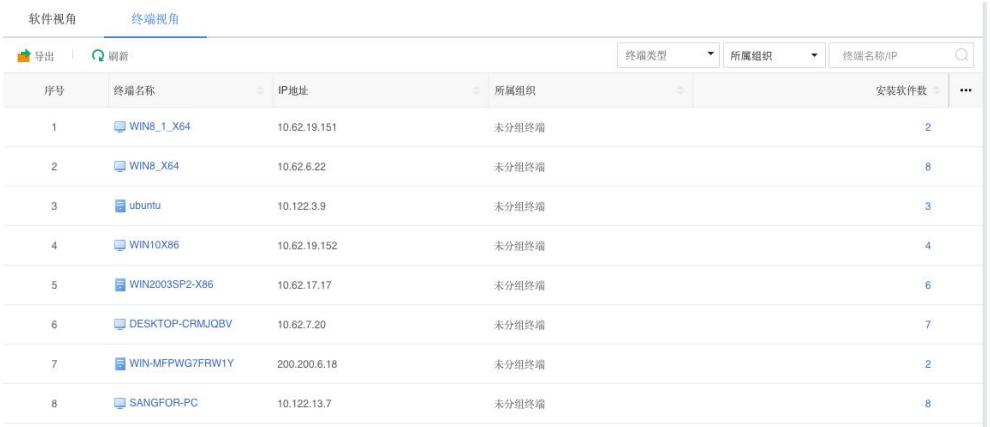
[软件分布统计]采集全网终端安装软件分布情况。

[服务器安装量top5的软件]采集全网服务器安装的软件并按top5排行。

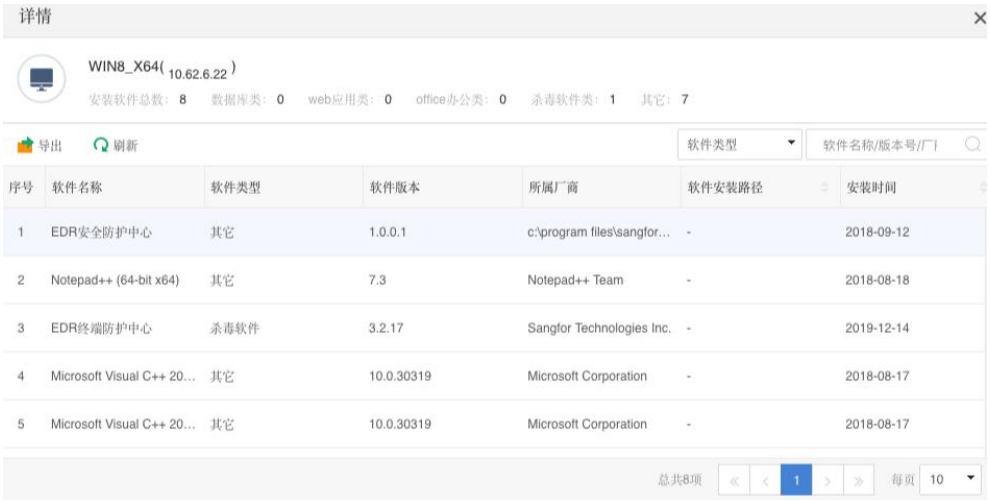
[PC终端安装量top5的软件]采集全网PC终端安装的软件并按top5排行。

[软件视角]从软件视角列出全网安装该软件的终端量及该软件的类型、软件版本、软件厂商等信息。点击终端数量这列具体的数字打开安装该软件的终端信息，如下图。

[终端视角]从终端视角列出终端安装软件数量，如下图。



点击安装软件数这列具体数字可以打开该终端安装的所有软件详情，如下图。

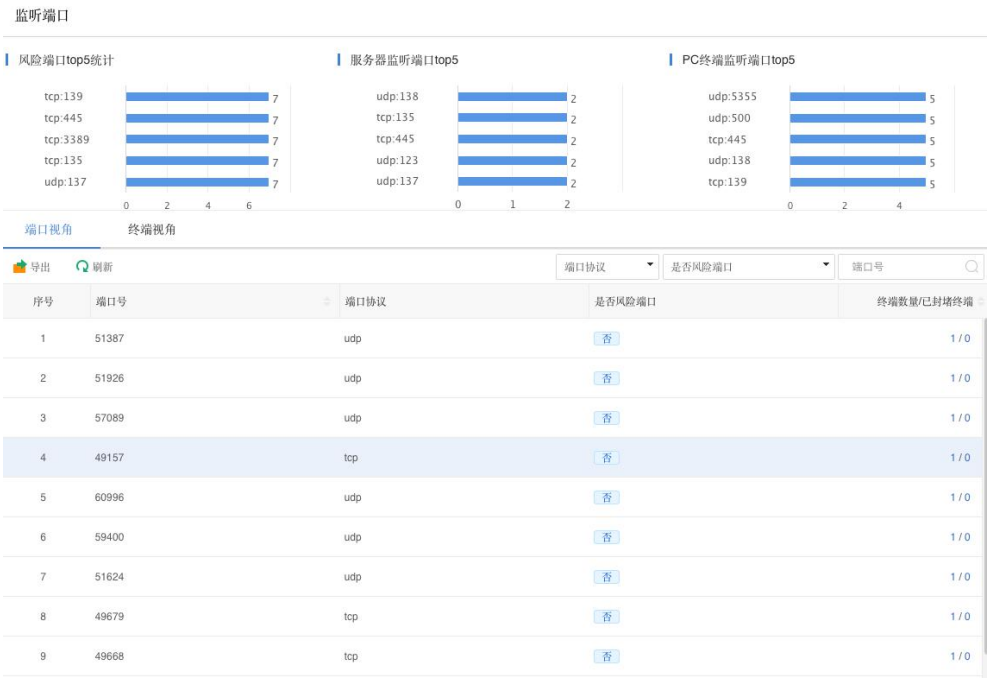


点击 

按钮，以表格形式导出，方便管理员进一步统计分析。同时可以根据软件类型、软件名称、版本号、厂商等条件进一步筛选或搜索。

3.3.2.3. 监听端口

提供快速方便地查看全网主机对外开放了哪些风险端口和没必要的端口，分别从服务器、PC终端维度统计展示对外开放端口情况，如下图。

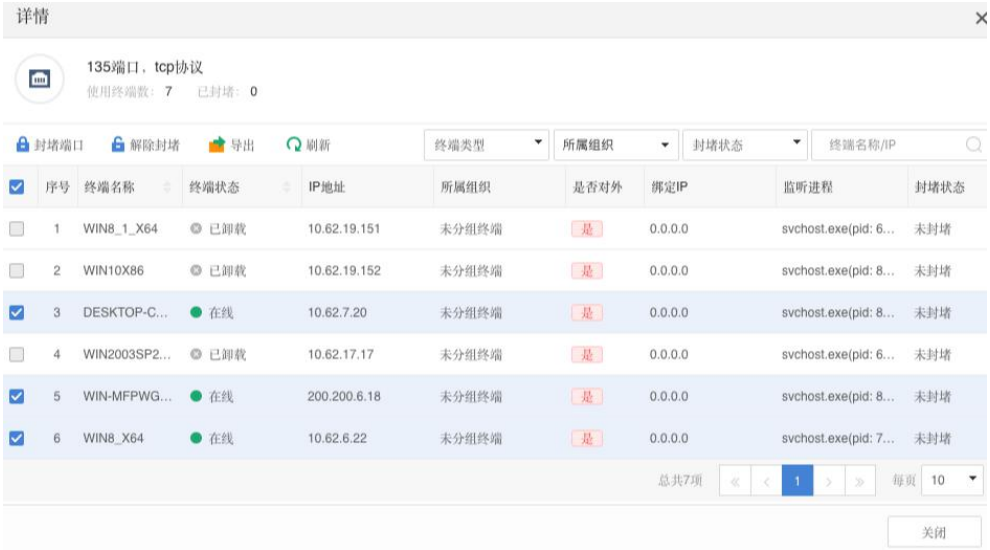


[风险端口top5统计]XDR内置了风险端口，采集全网终端开放的风险端口并按top5排行。

[服务器监听端口top5]采集全网服务器监听的端口并按top5排行。

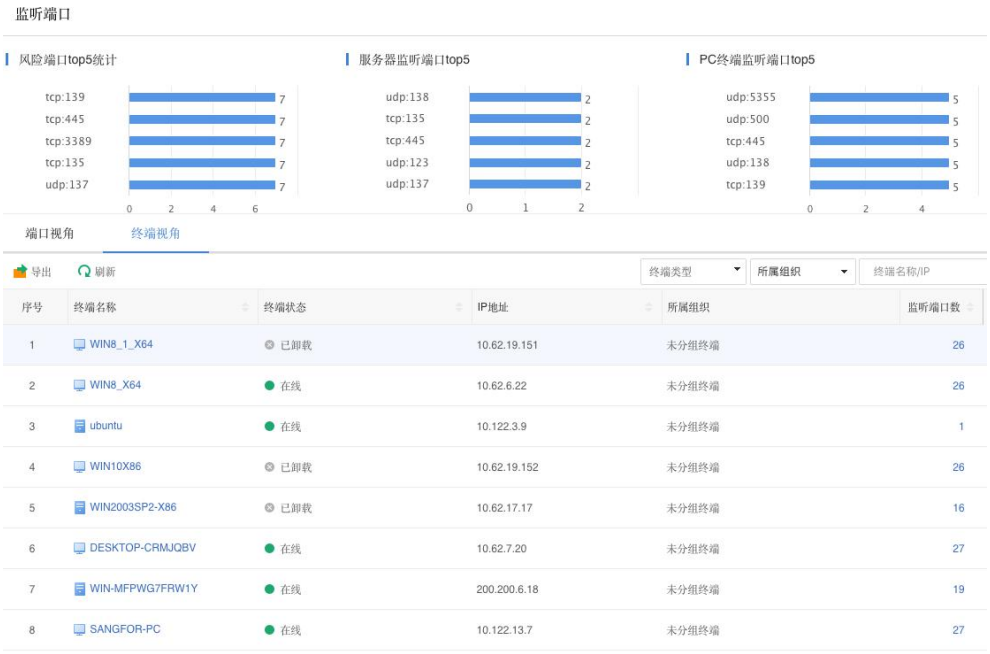
[PC终端监听端口top5]采集全网PC终端监听的端口并按top5排行。

[端口视角]从端口视角列出开放该端口的终端数量，点击“终端数量/已封堵终端”这列的数字，打开开放该端口的终端详情，如下图。

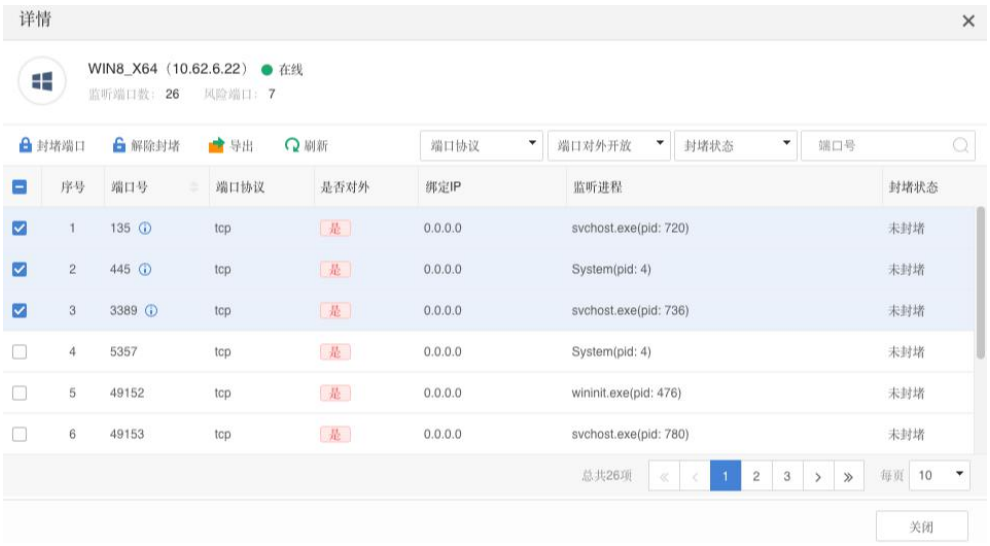


选中需要封堵该端口的终端，点击 封堵端口 可以对选中终端的风险端口进行封者，点击 解除封堵 可以对已封堵的端口解除封堵。点击 导出 按钮，以表格形式导出，方便管理员进一步统计分析。

[终端视角]从终端视角列出该终端开放的端口数量，如下图。



点击“监听端口数”这列数字，即打开该终端监听端口详情，如下图。



选中该终端需要封堵的端口，点击 封堵端口 可以对风险端口进行封者，点击 解除封堵 可以对已封堵的端口解除封口。点击 导出 按钮，以表格形式导出，方便管理员进一步统计分析。

3.3.2.4. 终端账户

统计汇总全网哪些主机存在风险账号，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，以便进一步要求相关人员进行自查和整改，从而削减主机的风险暴露面。

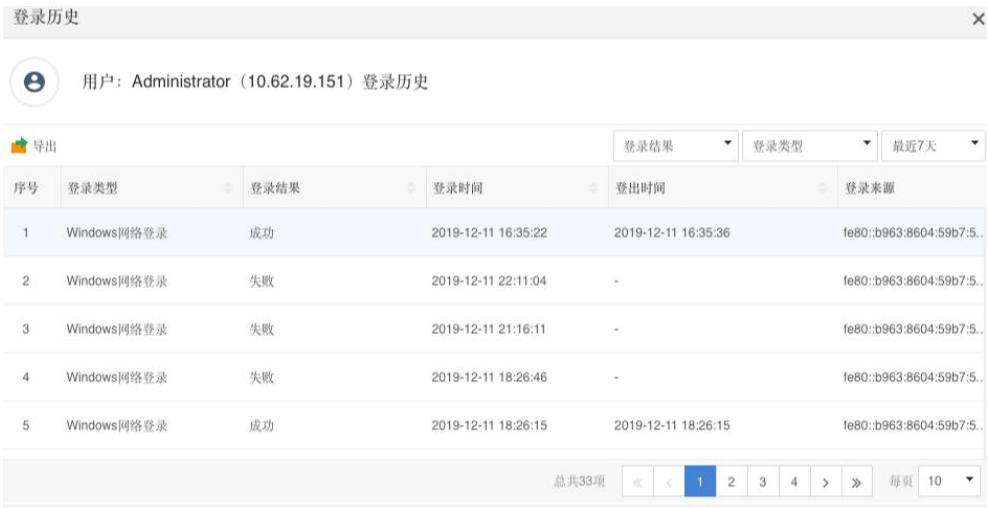
[账户权限分布统计]采集全网终端系统账户，并按管理员、非管理员、root、非root进行分布统计。

[风险账户分布统计]采集隐藏账号、弱密码账号、可疑root权限、长期未使用、夜间登录、多IP登录等帐号，并作为风险帐号进行统计。

[长期未修改密码账户分布统计]采集长时间未修改密码账户，并按最近90天、最近180天、最近一年进行统计。

点击导出按钮，以表格形式导出，方便管理员进一步统计分析。

打开终端帐户，以账户视角显示账户名称、终端名称、IP地址、账户状态、账户类型、权限、账户风险、密码最长使用期限、最近修改密码时间、最近登录时间和操作。点击登录历史打开该帐号在该终端上登录历史详情，如下图。



3.3.3. 终端发现

主动探测当前企业内网中有哪些主机未安装XDR客户端，以便对全网资产有个全貌了

解，从而快速识别出企业内网安全的薄弱节点，并及时做好防范。

点击立即扫描 设置扫描参数，如下图。

[发起扫描设备]可以设置由XDR管理平台发起扫描，也可以设置由已经安装了XDR客户端的Linux终端发起扫描。如果扫描范围大，为了增加扫描速度，建议设置由多个已经安装了XDR客户端的Linux终端发起扫描。

[扫描网段]设置扫描范围，支持填写主机地址或网段范围。

点击<高级设置>，可以定义扫描协议和端口，一般情况保持默认即可。

点击<确定>，完成扫描参数设置，弹出如下风险告警。

阅读风险告警，并得到扫描授权后，点击<确定>进行扫描，如下图。

扫描时长较长，扫描过程中可以点击<取消扫描>结束当前扫描任务。

[未管控终端]显示扫描发现的未安装XDR的终端，可以点击<导出>按钮，以表格形式导出，方便管理员进一步统计分析。如果某终端不需要安装XDR客户端，可以点击<忽略>操作。

[已忽略终端]显示管理员忽略的终端。

3.3.4. 策略中心

策略中心用于定义分组的安全策略，选中[终端管理/策略中心/全部终端]下的具体分组，可以定义该组的安全策略。共有[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

基本策略配置终端资产登记信息和终端防护密码设置，如下图。

[windows系统]说明基本策略支持的终端操作系统类型，基本策略只支持windows系统。

[终端资产信息登记]定义终端需要上传到MGR的资产信息。开启资产信息登记，终端安装Agent后弹出资产登记页，如下图。

[终端防护中心密码保护设置]定义终端Agent退出或卸载时需要输入的密码，如下图，需要先输入密码，才能退出Agent。

点击<保存>，保存当前策略配置。点击<恢复默认策略>，将当前策略恢复成默认配置。点击<一键继承>，将本组策略全部继承给他的下级子组。

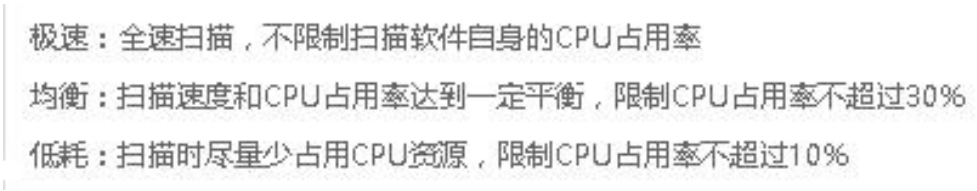
3.3.4.2. 病毒查杀

病毒查杀策略配置windows终端、linux终端和国产化终端病毒查杀和病毒库升级服务

器，如下图。

[windows系统]定义病毒查杀策略支持的终端操作系统类型，病毒查杀策略支持Windows系统、Linux系统和国产化操作系统，且支持的具体功能一致。点击[windows系统]右侧三角下拉箭头可以选择Windows系统、Linux系统或国产化操作系统，分别设置不同终端的病毒查杀策略。

[定时查杀]定义病毒查杀策略在指定时间内对内网终端进行查杀扫描。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，如下图。



[查杀扫描]定义扫描文件的条件、发现恶意文件后的处理方法以及设置扫描引擎。点亮[查杀扫描]后 图标，病毒查杀策略由MGR管理端统一设置下发，客户端无法单独设置病毒查杀策略。

[扫描文件]设置扫描文件大小和压缩包条件。

[发现恶意文件]设置发现恶意文件后的处理方法，有标准处置、严格处理和仅上报不处置三种处理方法，默认配置是标准处理。

- 标准处置：XDR 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：XDR 检测的所有威胁文件均隔处理。适用于严格保护场景。
- 仅上的不处置：XDR 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。

[扫描引擎设置]扫描引擎设置病毒查杀引擎，病毒查杀共用到四种引擎，包括深信服SAVE人工智能引擎、云查引擎、基因特征引擎和行为分析引擎。其中深信服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，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。

[终端病毒库升级]定义终端病毒库的升级服务器。可以选择为[从本控制中心升级]或从[启用服务升级]。选择[启用服务升级]时，如下图，可以配置多个升级服务器，从上到下匹配。

[高级设置]设置高启发式扫描，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启用。

3.3.4.3. 实时防护

实时防护策略配置windows终端[文件实时监控]、[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linux终端[webshell检测]和[暴力破解检测]策略，如下图。

[windows系统]定义实时防护策略支持的终端操作系统类型，实时防护策略支持Windows系统和Linux系统。但支持的具体功能有区别，点击[windows系统]右侧三角下拉箭头可以选择Windows系统或Linux系统，当前Linux终端只支持webshell检测和暴力破解检测防护策略。

[文件实时监控]定义文件实时监控的检测条件和发现恶意文件后的处理动作。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。

[防护级别]可以设置高、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及终端性能消耗不一样。

[文件类型]定义需要监控的文件类型。

[文件扫描]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，深信服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]设置发现恶意文件后的处理方法，有标准处置、严格处理和仅上报不处置三种处理方法，默认配置是标准处理。

- 标准处置：XDR 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：XDR 检测的所有威胁文件均隔处理。适用于严格保护场景。
- 仅上的不处置：XDR 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。

[勒索病毒防护]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，XDR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。点击右侧图标可以点亮小锁，终端勒索病毒防护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

勒索病毒防护策略。

[开启勒索诱饵防护]勒索病毒防护策略开关。使勒索病毒防护功能生效，需要同时开启文件实时监控策略。

[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。

[webshell检测]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，只检测web服务器根目录及其子目录下的webshell后门。

[检测方式]检测方式有[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。其中[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。

[暴力破解检测]XDR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。下图开启windows终端暴力破解功能及发现暴力破解事件后的处理方法。

[高级威胁防护]高级威胁防护设置无文件攻击防护。无文件攻击指的是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。点击右侧图标可以点亮小锁，高级威胁防护策略从管理端统一下发、无法单独配置，默认

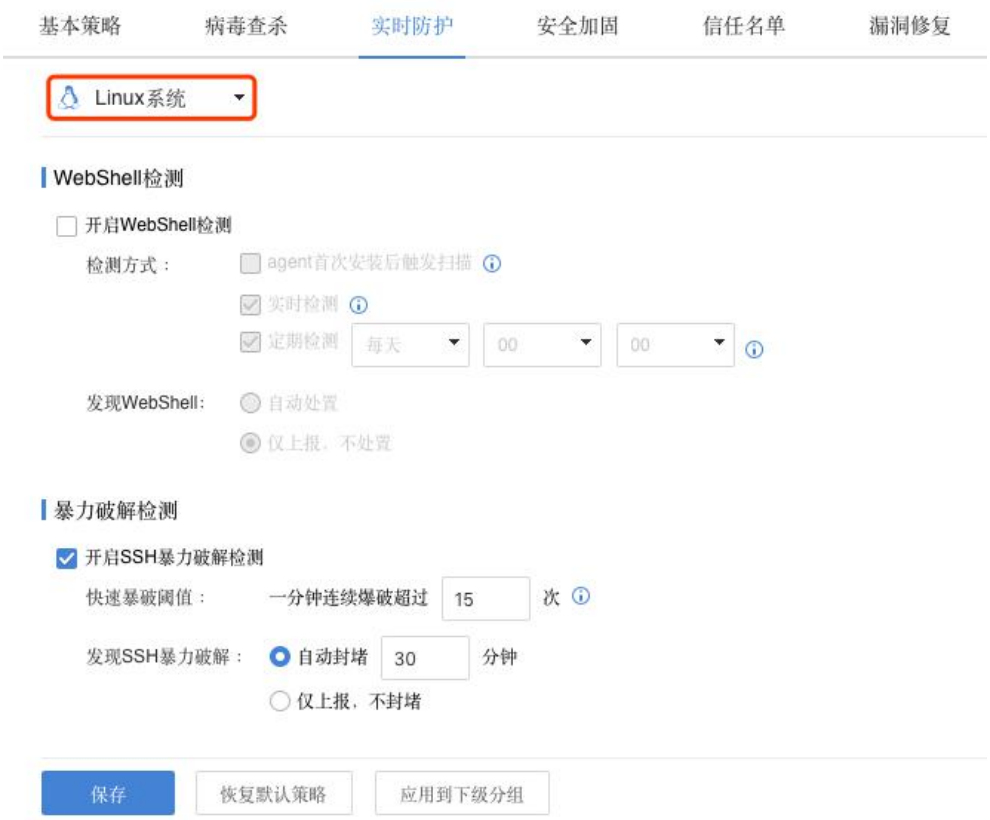
是允许终端配置高级威胁防护策略。

同时选中[开启无文件攻击防护]和[开启可疑powershell脚本执行检测]启用无文件攻击防护功能。

发现可疑powershell脚本执行后的处理动作，可以设置为“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，弹出如下告警。

选中“仅告警，不阻断”处理动作后，针对服务器和PC终端分别做不同处理，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。

对于Linux终端，实时防护策略只支持[webshell检测]和[暴力破解检测]，如下图。



3.3.4.4. 安全加固

安全加固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。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。

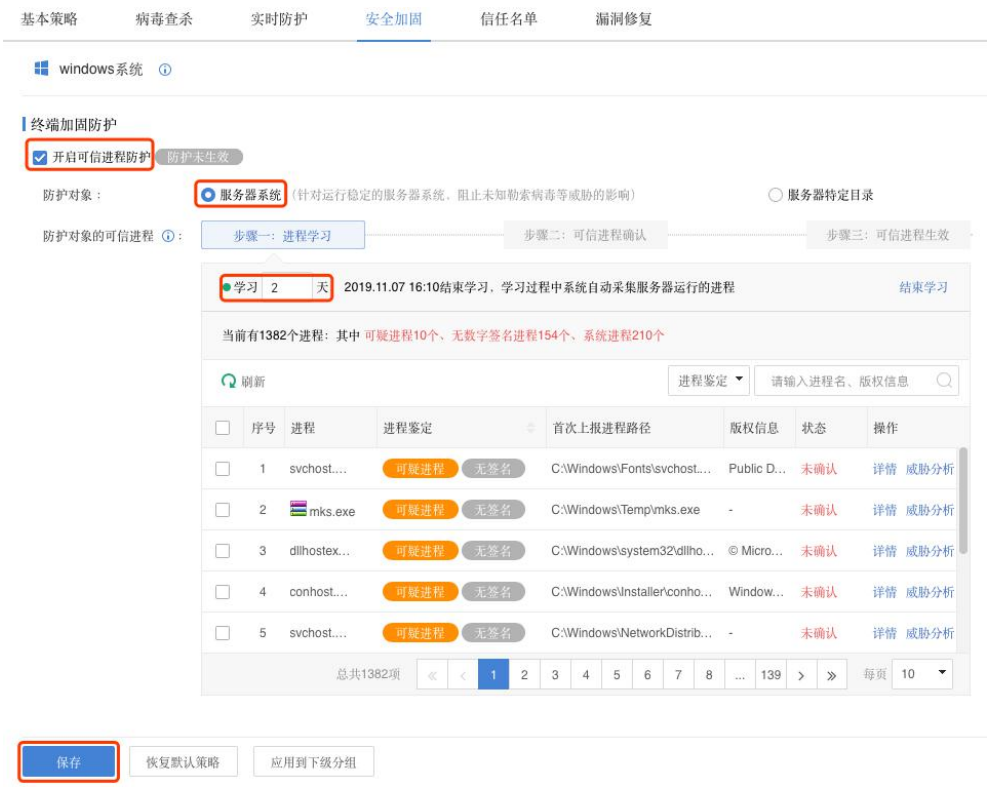
配置步骤

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。

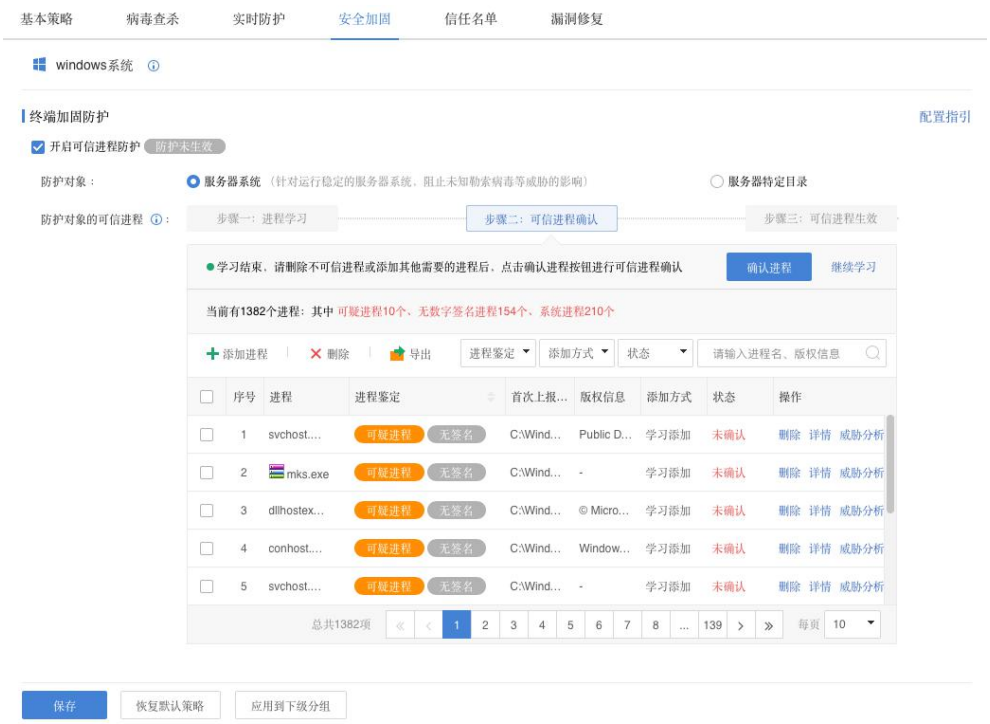
步骤2. 可信进程学习

设置服务器所在组的安全加固策略。启用[可信进程防护]，防护对象选择[服务器系统]；设置可信进行学习，学习时间范围从1天到30天可配，点击<保存>。



步骤3. 可行进程确认

进程学习结束，需要进行可信进程确认。管理员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，完成可信进程确认。



[进程]即进程的名称。

[进程鉴定]XDR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。

[版权信息]进程文件的版权信息。

[添加方式]显示进程的添加方式，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。

确认当前进程为不可信进程，点击<删除>操作。

需要查看进程详情，点击<详情>操作，如下图。

如果无法确认当前进程是否可信进程，可以点击<威胁分析>，借助深信服威胁情报对当前进程进一步分析后再确认。

如果发现需要添加为可信的进程不在学习结果中，可以点击<添加进程>进行添加。

[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。

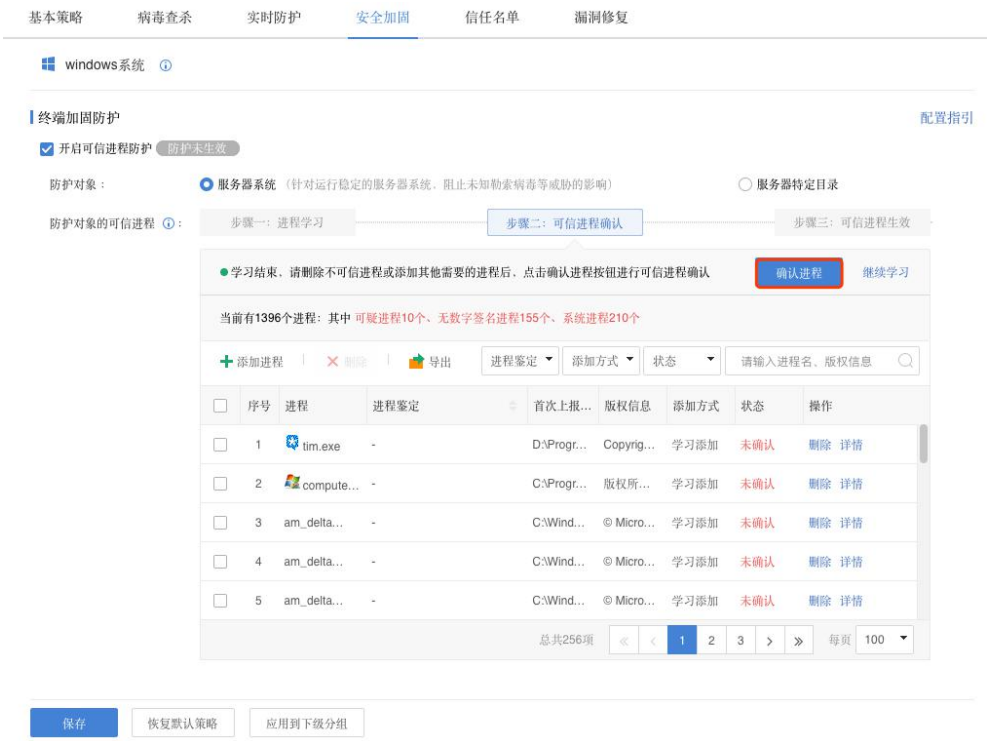
[按模板导入]适用于客户需要加固的服务器是模板中提供的web服务器或数据库服务器。

[上传进程文件]上传服务器中可信的进程文件。

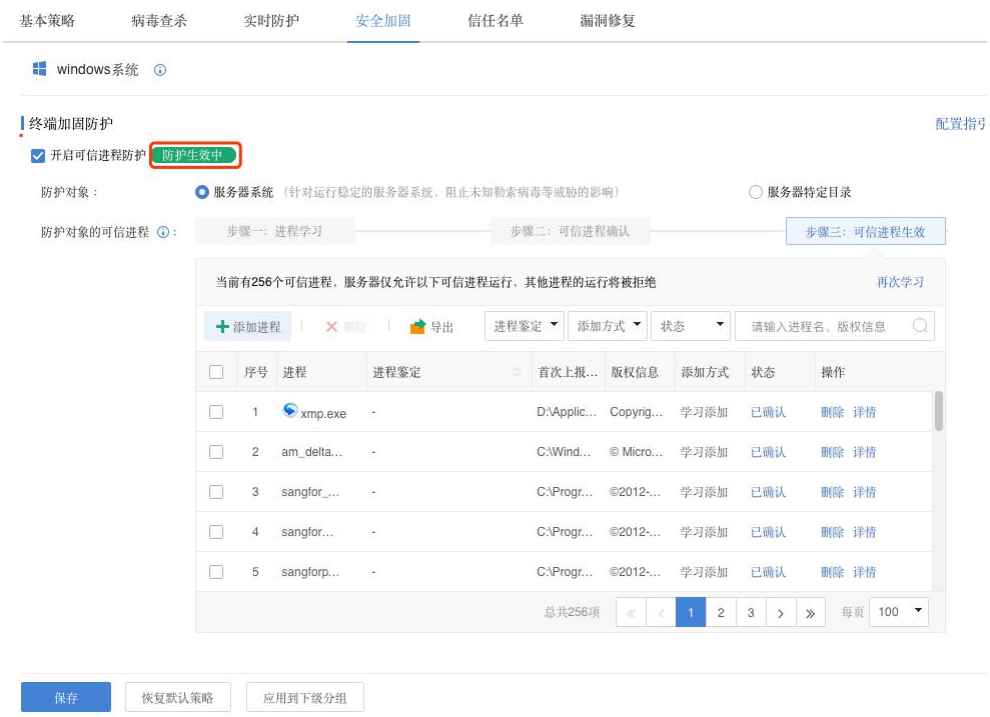
[手动输入进程文件信息]收集可信进程的进程名、原始文件名、版权信息手动录入。

步骤4. 可信进程生效

核对可信进程后，点击<确认进程>并完成可信进程确认。



点击<保存>保存安全加固策略，服务器防护生效。



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

设置服务器所在组的安全加固策略。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

进程学习和确认与服务器系统防护中的进程学习和确认配置方法一致，请参考此章节“场景一：服务器系统防护”。

步骤4. 可信进程生效

核对可信进程后，点击<确认>进程并完成可信进程确认。

设置发现不可信进程运行时的处理方式，如下图。

[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。

3.3.4.5. 信任名单

信任名单配置信任的文件、目录、防暴力破解白名单。

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。如下图。

[windows系统]下拉可以选择配置windows或Linux终端的信任名单策略，Linux终端信任名单策略只支持防暴力破解IP白名单，如下图。

[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

漏洞修复策略配置漏洞定时检测、修复，以及漏洞补丁下载服务器地址，如下图。

[windows系统]说明漏洞修复策略支持的终端操作系统类型，当前只支持windows系统。

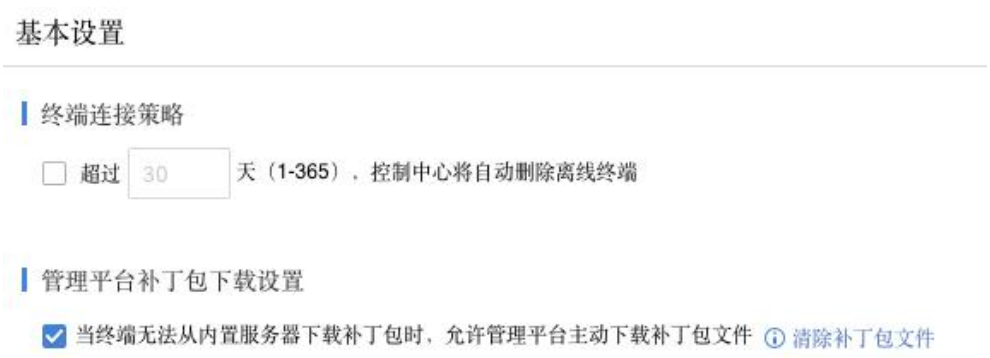
[定期漏洞扫描]定义漏洞定时检测的时间段。

[漏洞扫描结果]定义发现系统漏洞后的处理方法。

[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、MGR。

如果终端Agent无上网权限，无法从深信服CDN服务器或微软漏洞服务器下载漏洞补丁，可以使用以下两种解决方案，推荐给使用第一种方案：

1. 在内网搭建漏洞补丁服务器，Agent终端从内网服务器下载漏洞补丁。
2. MGR可以上网，由管理平台主动下载漏洞补丁，Agent终端从管理平台下载漏洞补丁。[系统管理/系统设置/基本设置]启用管理平台补丁包下载设置，如下图。



其他说明：

1. 漏洞补丁管理功能只适用Windows系统，不适用Linux系统。
2. 漏洞修复策略建议设置扫描后“仅上报，不自动修复”，根据实际情况进行人工修复。
3. 各安全策略对Windows PC、Windows Server、Linux、国产化终端不同终端的支持情况总结如下。

安全策略	Windows PC	Windows Server	Linux	国产化
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	√	√	×	×

3.4. 微隔离

通过微隔离功能可以对服务器进行防护，只放通必要的业务端口，禁止所有的非必要的端口，提升业务的安全性。通过可视化的方式查看到流量隔离状态。

3.4.1. 微隔离策略

点击右上用<策略生效开关>可将微隔离功能全局开启或禁用。

[微隔离策略]用于新增、删除或禁用策略，通过五元组匹配数据进行放通或拒绝访问。

点击<新增>，配置微隔离策略，如下图。

[策略名称]定义微隔离策略的名称。

[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。

源和目的可以点击 进行互换，点击<确定>，进行提交。

[删除]通过策略左侧方框选择需要删除的策略，点击删除将策略删除。

[上移]通过策略左侧方框选择需要上移的策略，点击上移将策略移动，一次最多只能选择一条策略。

[下移]通过策略左侧方框选择需要下移的策略，点击下移将策略移动，一次最多只能选择一条策略。

[启用]通过策略左侧方框选择需要启用的策略，点击启用将策略启用。

[禁用]通过策略左侧方框选择需要启用的策略，点击禁用将策略禁用。

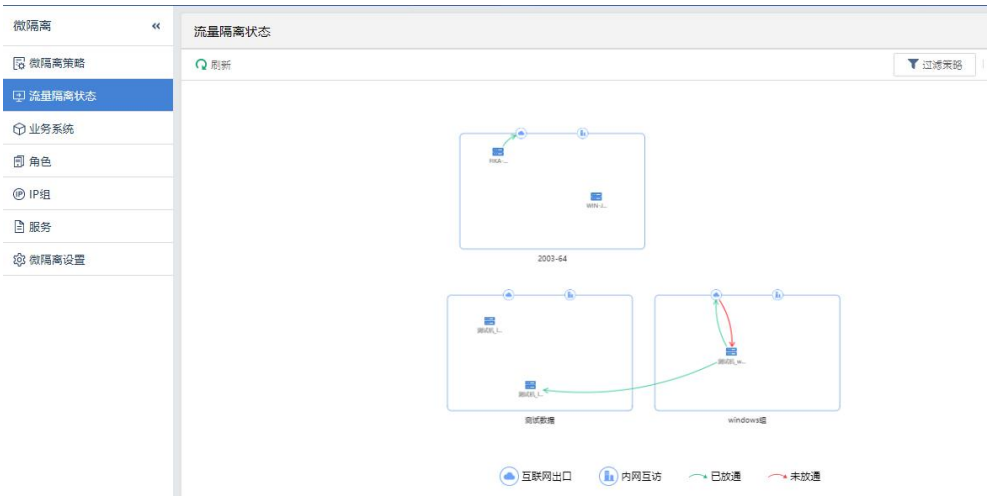
[匹配]查看匹配该策略的日志数量。

[最近匹配时间]最近一次匹配该策略产生日志的时间。

[启用]点击或完成启用或禁用操作。

3.4.2. 流量状态

可视化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，已放通和未放通的流量访问情况。通过过滤策略进行筛选查看。完成[策隔离策略]、[业务系统]、[IP组]、[服务]的配置并且有流量访问再进行查看。



点击<过滤策略>，筛选条件如下图。

[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。

[业务流量]、[运维流量]、[其他流量]需要通过[服务]进行定义，详见“服务”章节。

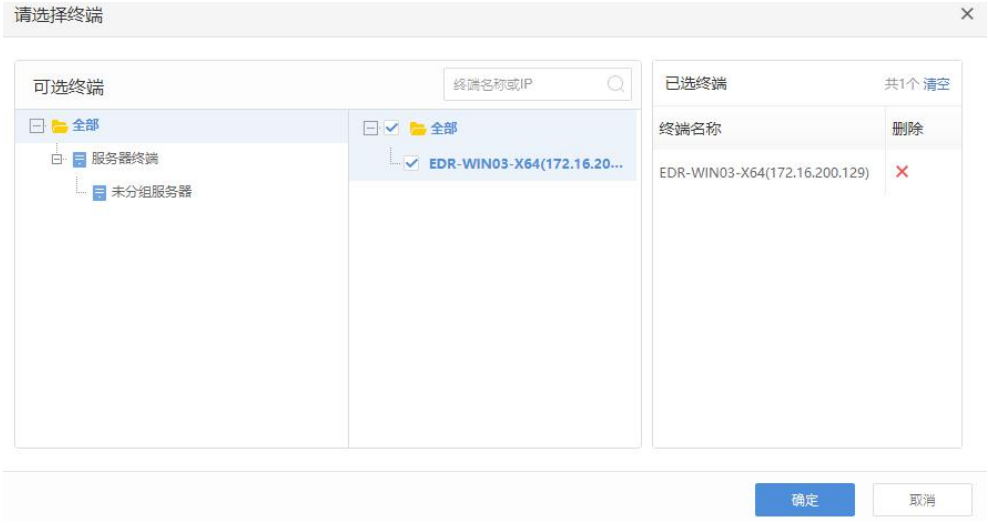
3.4.3. 业务系统

配置业务系统将多个服务器终端定义到一个业务系统，一台服务器终端只能加入一个业务系统。可用于微隔离策略调用，和流量隔离状态的展示。

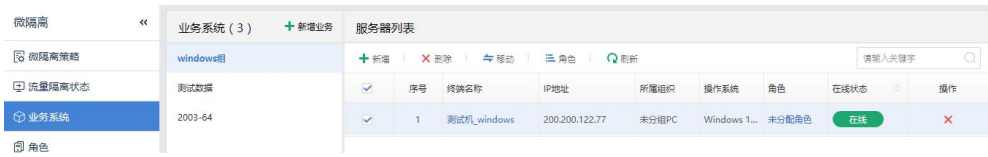
点击<新增业务>，新建业务系统，并将服务器终端加入该业务系统。

[业务系统名称]定义新建业务系统的名称。

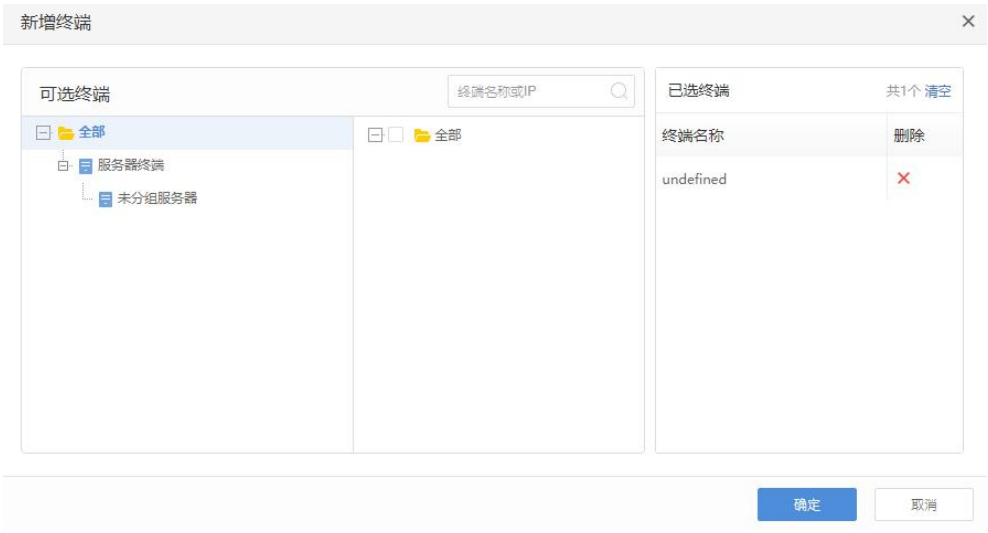
[选择终端]点击 选择在[终端管理]中在线的服务器终端，不包括PC终端。如下图。



勾选需要加入该组的服务器终端，点击<确定>，进行提交。



[新增]配置完成业务系统后再加入服务器终端，先选中已配置的业务系统名称，在[服务器列表]中的点击新增。如下图。



[删除]删除已经加入到对应业务系统中的服务器终端。

[移动]移动选中的服务器终端到其它业务系统分组中。

[角色]定义服务器终端的角色，如web、数据库等，角色可以自定义，一台服务器终端只能对应一个角色，点击<角色>如下图。

点击<新增角色>，如下图，详细说明查看“角色”章节。

3.4.4. 角色

用于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。不同角色的角色特征不能相同。平台内置了“WEB”、“数据库”、“FTP”、“SLB”、“邮件”、“消息队列”、“WebSphere”、“WebLogic”角色以及对应的角色特征。

点击<新增>，定义新的角色，如下图。

[角色名]定义角色名称，一般为服务器终端在业务系统中提供的服务名称。

[描述]描述角色的用途。

[角色特征]匹配到对应进程名或端口时，则认为服务器终端为该角色。

点击<确定>，进行提交。

[删除]可删除自定义的角色，内置角色不能删除。

[操作]可以对角色的角色特征进行修改，自定义的解决还可以删除或修改角色名。

3.4.5. IP 组

[IP组]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包括（10.0.0.0/8，172.16.0.0/12，192.168.0.0/16)，默认互联网地址包括（0.0.0.0-255.255.255.255）策略从上到下进行匹配。用于微隔离策略的调用。

点击<新增>，如下图。

[IP组名称]定义IP组的名称。

[地址范围]划分地址段到该IP组中，格式如上图所示。

[IP组类型]可选择为互联网或内网类型。

[备注]备注IP组的用途。

点击<确定>，进行提交。

[删除]可将自定义的IP组删除。

[上移]选中自定义的IP组上移，策略从上到下进行匹配。同时只能选择一个IP组。

[下移]选中自定义的IP组下移，策略从上到下进行匹配。同时只能选择一个IP组。

[操作]可通过操作对IP组进行删除，上移或编辑，不可下移操作。

3.4.6. 服务

[服务]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。自

定义服务端口不能与已有所使用端口不能重复。

点击<新增>，如下图。

[服务名称]定义服务的名称。

[协议]选择该服务需要使用到的协议。

[端口]服务所使用到的端口。

[流量类型]定义该服务的流量是用于业务、运维或其他，在[流量隔离状态]的展示。

[备注]备注服务的用途。

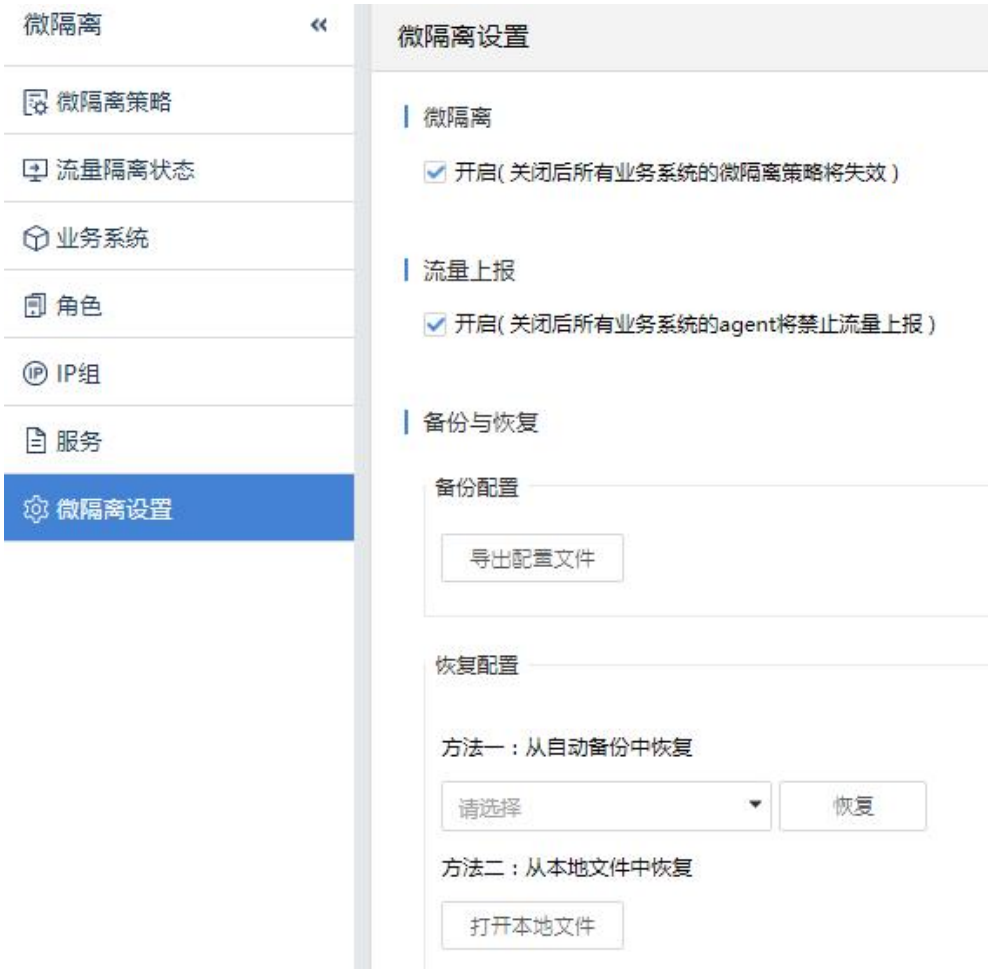
点击<确定>，进行提交。

[删除]可对自定义的服务进行删除，不可删除内置服务。

[操作]可对自定义服务进行删除和编辑，对内置服务只能进行编辑，不能删除。

3.4.7. 微隔离设置

[微隔离设置]微隔离功能的全局设置，包括微隔离功能的开启、禁用；流量上报的开启、禁用，以及微隔离策略的备份与恢复。



[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

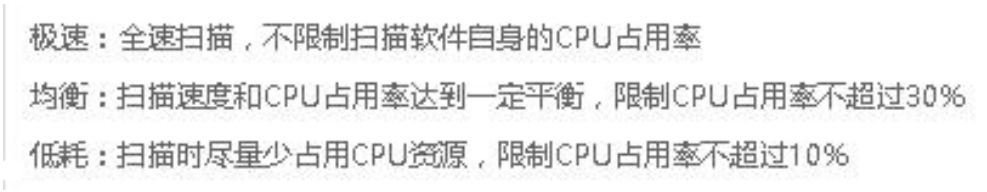
终端接入终端威胁防护系统后可通过[威胁检测/终端病毒查杀]页面对终端下发体检任务，通过结合本地信誉库、自研SAVE引擎、行为检测引擎、特征检测引擎、云查等多引擎对终端进行威胁文件扫描并展示查杀结果。终端体检情况展示主要展示：任务类型、扫描模式、成功下发终端台数、扫描完成情况、终端终止终端，终端名称IP地址、所属组织、操作系统、终端状态、末处理病毒和病毒总数的情况、查杀状态等信息。

查杀方式可以选择快速查杀和全盘查杀，点击[快速查杀]右侧的三角可以选择当前需要下发的策略为“快速查杀”还是“全盘查杀”。区别在于全盘查杀可以扫描终端所有硬盘的文件，快速查杀扫描系统盘中的一些重要文件目录。

点击<快速查杀>如下图。

[查杀终端]选择需要执行“快速查杀”的终端，如下图，可以查看到上次查杀时间，可让管理员直观知道哪些终端多久没有执行扫描操作。

[扫描模式]选择极速、均衡、低耗主要区别在CPU占用率情况点击 可以查看说明。

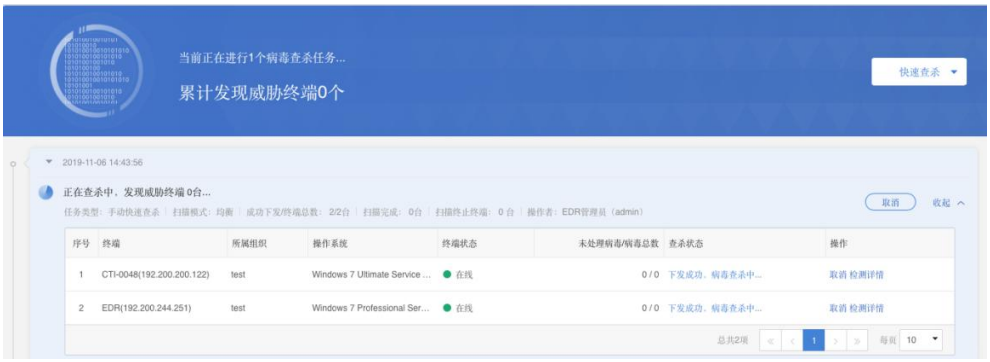


点击<全盘查杀>如下图。

[查杀终端]选择需要执行“全盘查杀”的终端，与“快速查杀”相同。

[扫描模式]选择极速、均衡、低耗主要区别在CPU占用率情况点击 可以查看说明。与快速查杀相同。

通过以上的配置完成病毒查杀下发并且可以查看到查杀的进展，如下图。



点击具体终端右侧<检测详情>可以查看该终端杀毒进度，如下图。

杀毒完成，可以查看此次查杀结果，如下图。

点击威胁终端<检测详情>查看该终端详细的扫描结果，如下图。

点击<处置>即可对病毒进行隔离。

📖 说明：

1.快速查杀目录 windows： /Windows 和/Windows/system32 本级目录， /Windows /system32/drivers 目录和其子目录；

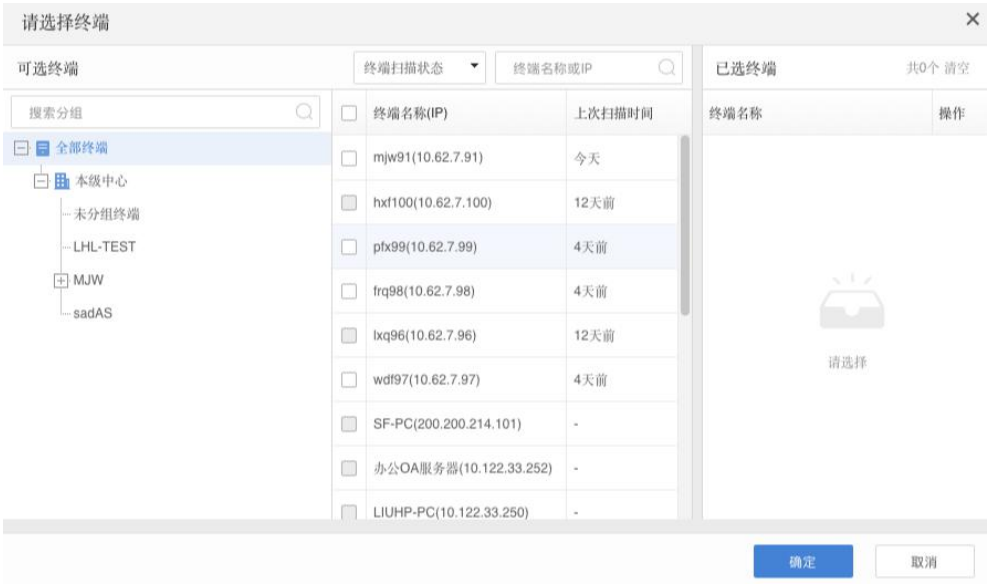
2.快速查杀目录 linux:/bin，/sbin，/usr/sbin，/usr/bin，/lib，/lib64，/usr/lib/usr/lib64，/usr/local/lib，/usr/local/lib64，/tmp，/var/tmp，/dev，/proc。

3.5.2. 终端漏洞查补

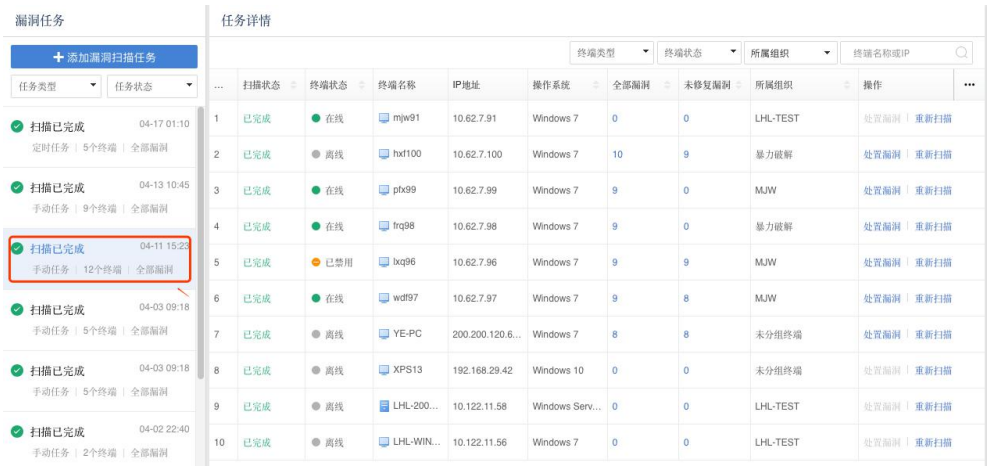
[威胁检测/终端漏洞查补]可检测windows终端系统漏洞并修复，当前支持远程执行代码、拒绝服务、特权提升、安全功能绕过、信息泄漏五种影响类型漏洞检测和修复。

[漏洞任务]可以添加手动漏洞扫描任务，并显示任务执行的结果。点击<添加漏洞扫描任务>，如下图，可以选择需要进行漏洞检查的终端和漏洞类型。

选择需要检查的漏洞终端，如下图。



点击具体任务执行结果，查看任务详情，如下图。任务详情显示漏洞检查的终端，以及终端全部漏洞和未修复的漏洞数，并可以对终端进行漏洞处理或重新扫描。



点击<处理漏洞>，可以对系统漏洞进行“修复”或“忽略”处理操作，如下图。

“高危”、“中危”、“低危”系统漏洞建议按如下说明处理。

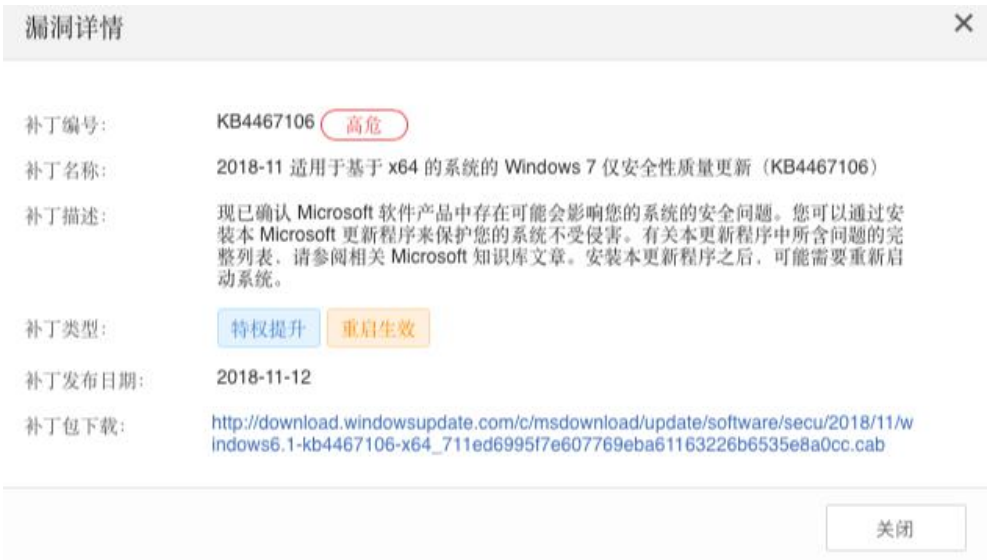
高危：建议立即修复。这些漏洞有非常大的风险被利用来破坏您的电脑。

中危：建议谨慎判断后修复。这些漏洞的补丁可能会给您带来风险。

低危：建议您根据自身情况选择修复。

选中需要修复的漏洞，点击<修复>，漏洞修复需要电脑重启才能生效，会给出下图提示，管理员可以选择“强制终端修复后立即重启生效”，也可以选修复后不重启，下次重启再生效。建议不要设置漏洞修复后强制重启，由管理员通知终端在非业务时间重启电脑使漏洞修复生效。

选中具体漏洞的[补丁名称]，显示该漏洞详情，通过漏洞详情可以了解漏洞危害及补丁下载地址，如下图。



📖 说明：

漏洞修复需要终端电脑能够连接互联网，并确保到以下服务器连通性正常。

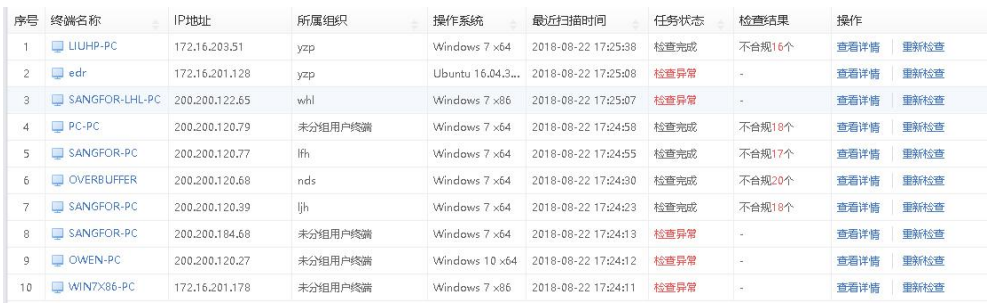
auth.sangfor.com.cn
upd.sangfor.com.cn
download.sangfor.com.cn
analysis.sangfor.com.cn
clt.sangfor.com.cn
download.windowsupdate.com

3.5.3. 终端基线检查

[威胁检测/终端合规检查]可对终端进行合规性检查。针对不同终端系统检查内容有所区别。Windows终端检查内容为：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终端检查内容为：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。



序号	终端名称	IP地址	所属组织	操作系统	最近扫描时间	任务状态	检查结果	操作
1	LIUHP-PC	172.16.203.51	yzp	Windows 7 x64	2018-08-22 17:25:38	检查完成	不合规16个	查看详情 | 重新检查
2	edr	172.16.201.128	yzp	Ubuntu 16.04.3...	2018-08-22 17:25:08	检查异常	-	查看详情 | 重新检查
3	SANGFOR-LHL-PC	200.200.122.65	whl	Windows 7 x86	2018-08-22 17:25:07	检查异常	-	查看详情 | 重新检查
4	PC-PC	200.200.120.79	未分组用户终端	Windows 7 x64	2018-08-22 17:24:58	检查完成	不合规18个	查看详情 | 重新检查
5	SANGFOR-PC	200.200.120.77	lfh	Windows 7 x64	2018-08-22 17:24:55	检查完成	不合规17个	查看详情 | 重新检查
6	OVERBUFFER	200.200.120.68	nds	Windows 7 x64	2018-08-22 17:24:30	检查完成	不合规20个	查看详情 | 重新检查
7	SANGFOR-PC	200.200.120.39	ljh	Windows 7 x64	2018-08-22 17:24:23	检查完成	不合规18个	查看详情 | 重新检查
8	SANGFOR-PC	200.200.184.68	未分组用户终端	Windows 7 x64	2018-08-22 17:24:13	检查异常	-	查看详情 | 重新检查
9	OWEN-PC	200.200.120.27	未分组用户终端	Windows 10 x64	2018-08-22 17:24:12	检查异常	-	查看详情 | 重新检查
10	WIN7X86-PC	172.16.201.178	未分组用户终端	Windows 7 x86	2018-08-22 17:24:11	检查异常	-	查看详情 | 重新检查

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<下载>可以下载合规检查报告。

说明：

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

3.6.1.1. 威胁终端视角

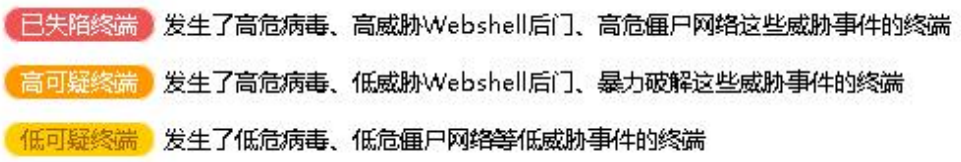
可以通过发现的[全部威胁终端]、[已失陷终端]、[高可疑终端]、[低可疑终端]、[已隔

离终端]进行筛选。同时也可以通过[终端类型]、[所属组织]、[全部时间]或直接搜索终端名称/ip进行搜索指定的终端。

[终端名称]上线的终端名称。

[所属组织]在终端管理中加入的分组。

[威胁等级]分为已失陷、高可疑、低可疑。其定义为



[关键风险事件]用标签的形式举证说明该主机存在的风险事件。

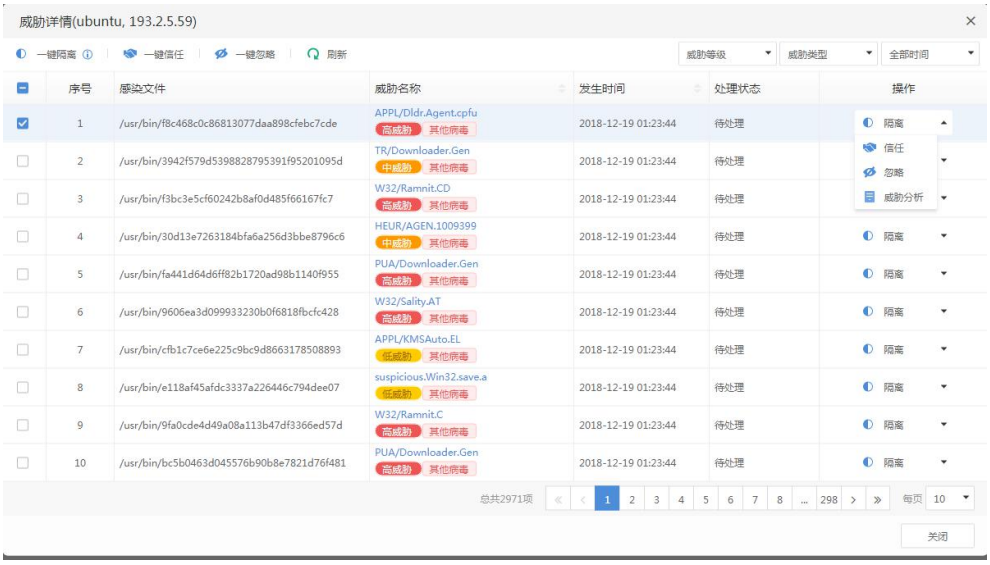
[未处理威胁/威胁总数]终端上否未处理的威胁数据与发现的威胁数据的情况。

[最近发生时间]最新一次发现威胁的时间。

[操作]可以对发现的威胁进行处理或直接将终端进行隔离之后再处理。

点击<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。

点击<处理威胁>如下图所示。



[一键隔离]勾选需要处理的终端进行一键隔离将病毒文件进行隔离以及宏病毒或感染型病毒的修复，至少需要勾选两个及以上的安全事件。对暴力破解的IP批量加入黑名单风险较大，只能单个加黑。如下图。

[一键信任]勾选需要信任的终端安全事件，将检测出来的文件或攻击源IP加入信任列表。

[一键忽略]勾选需要忽略检测的终端安全事件，将已经检测出来的文件或攻击源IP忽