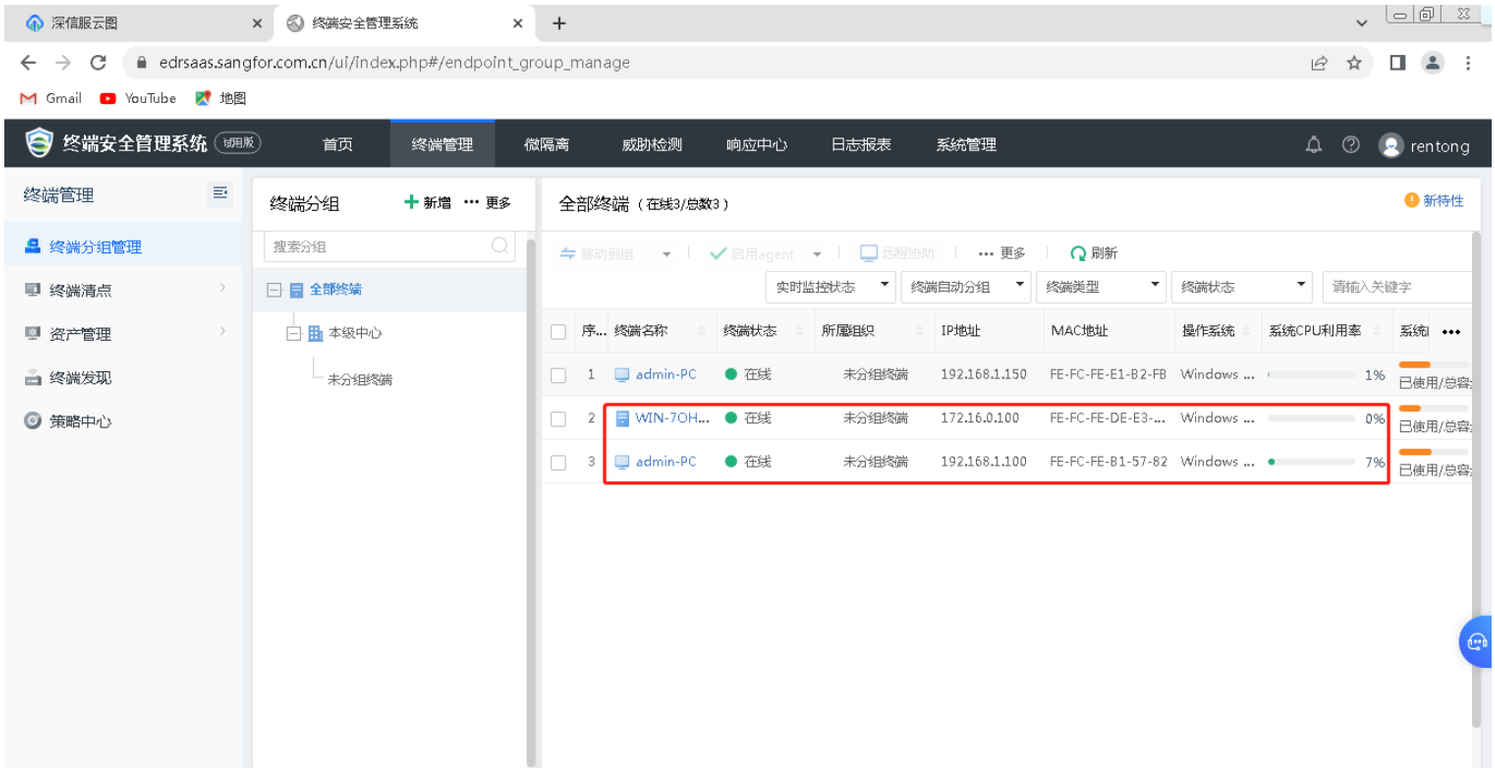
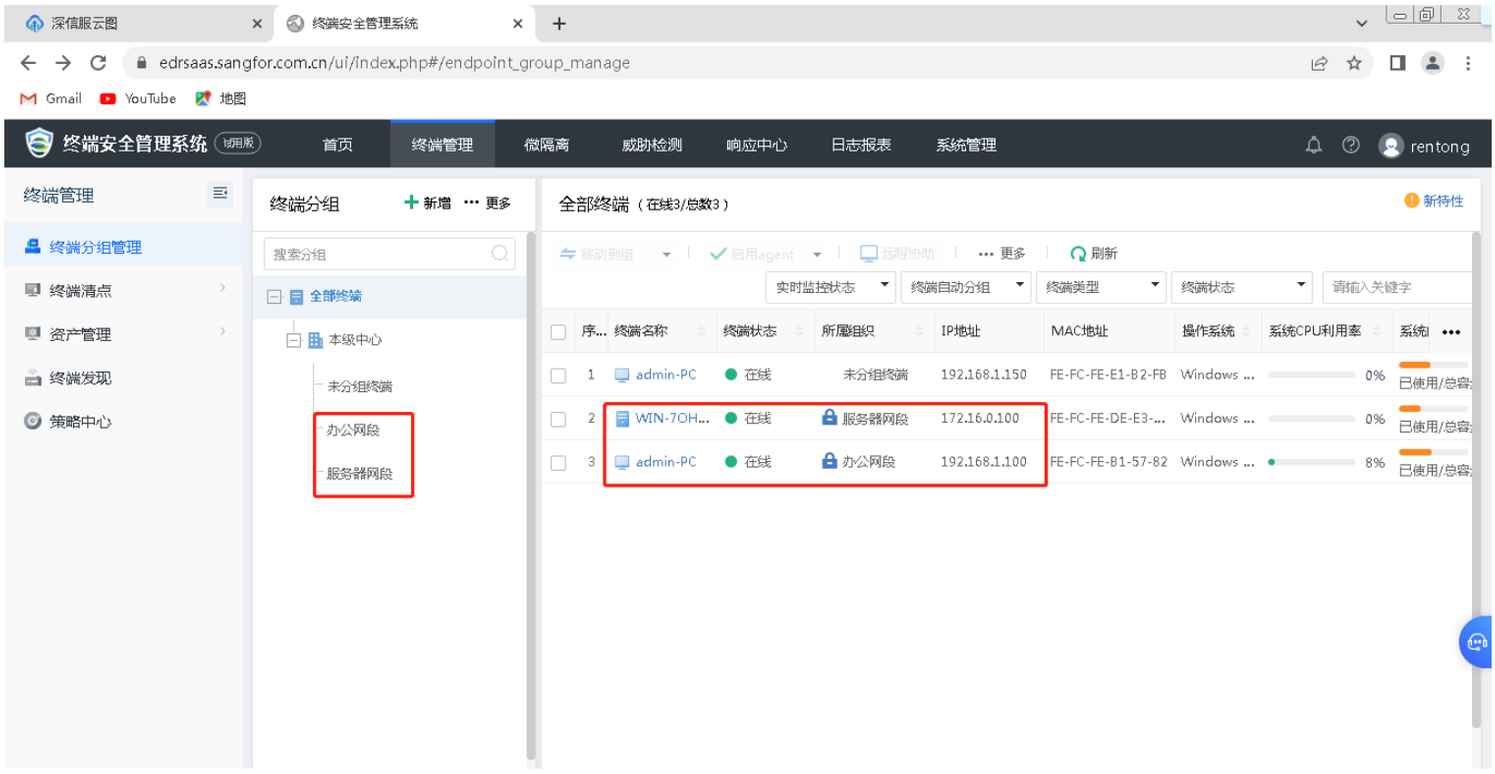
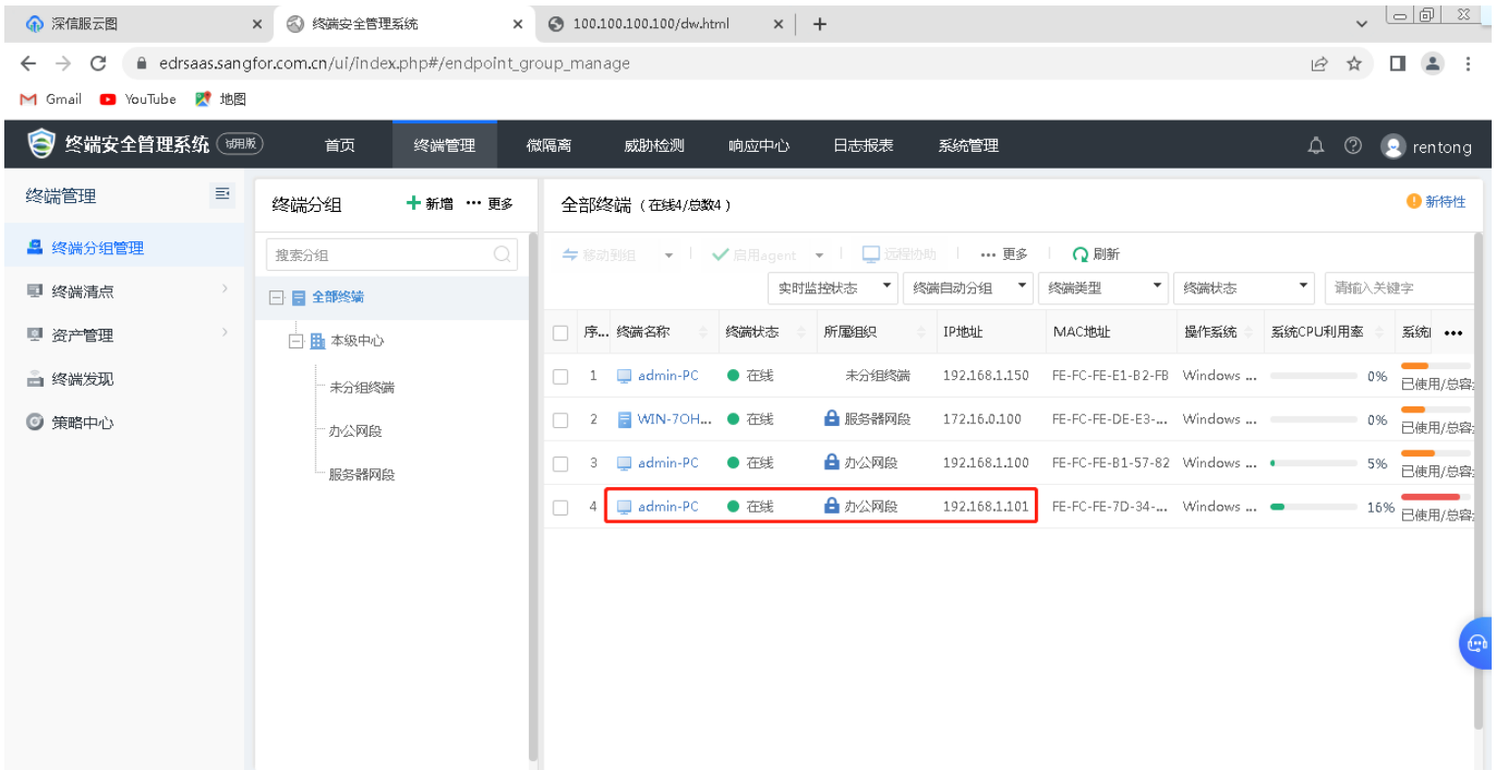
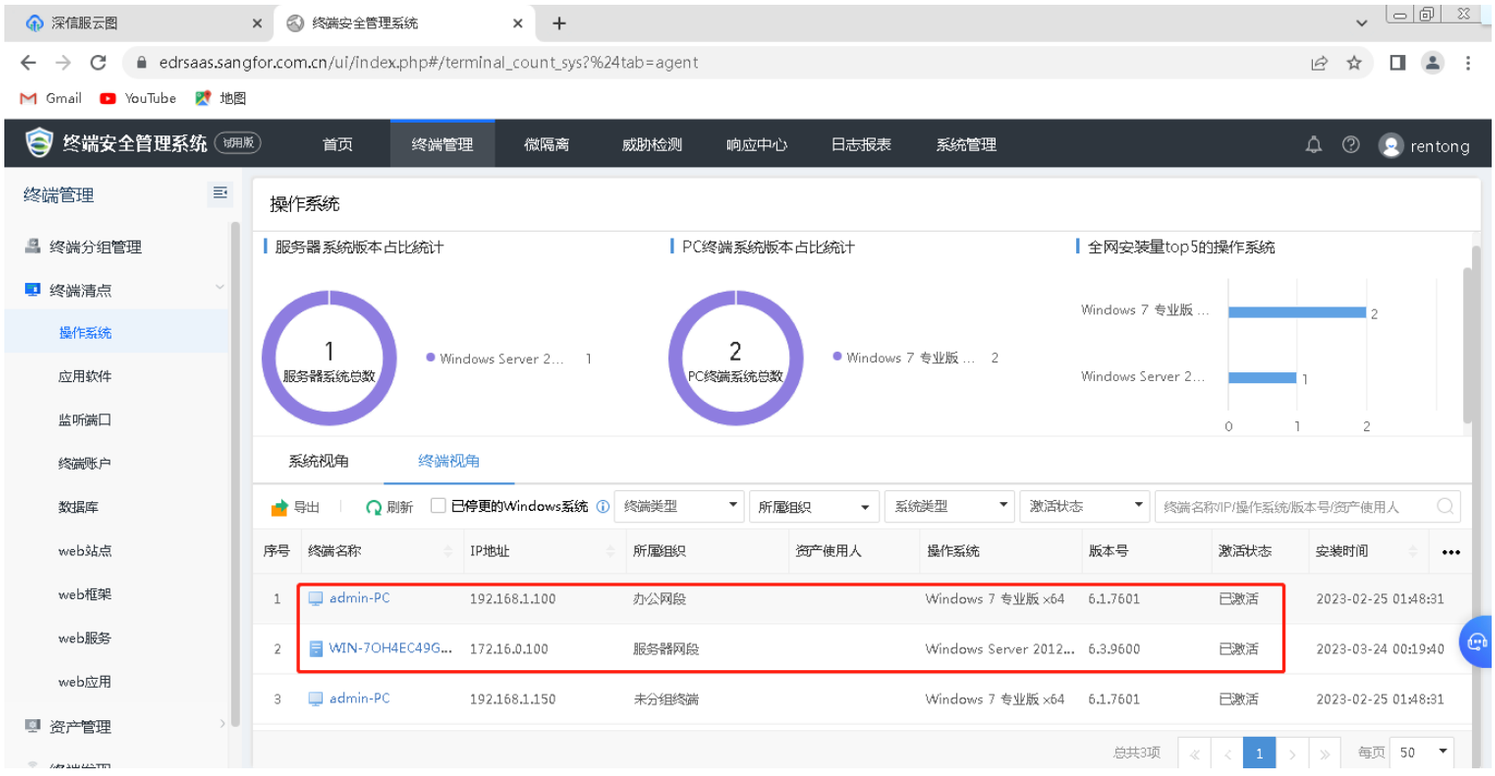
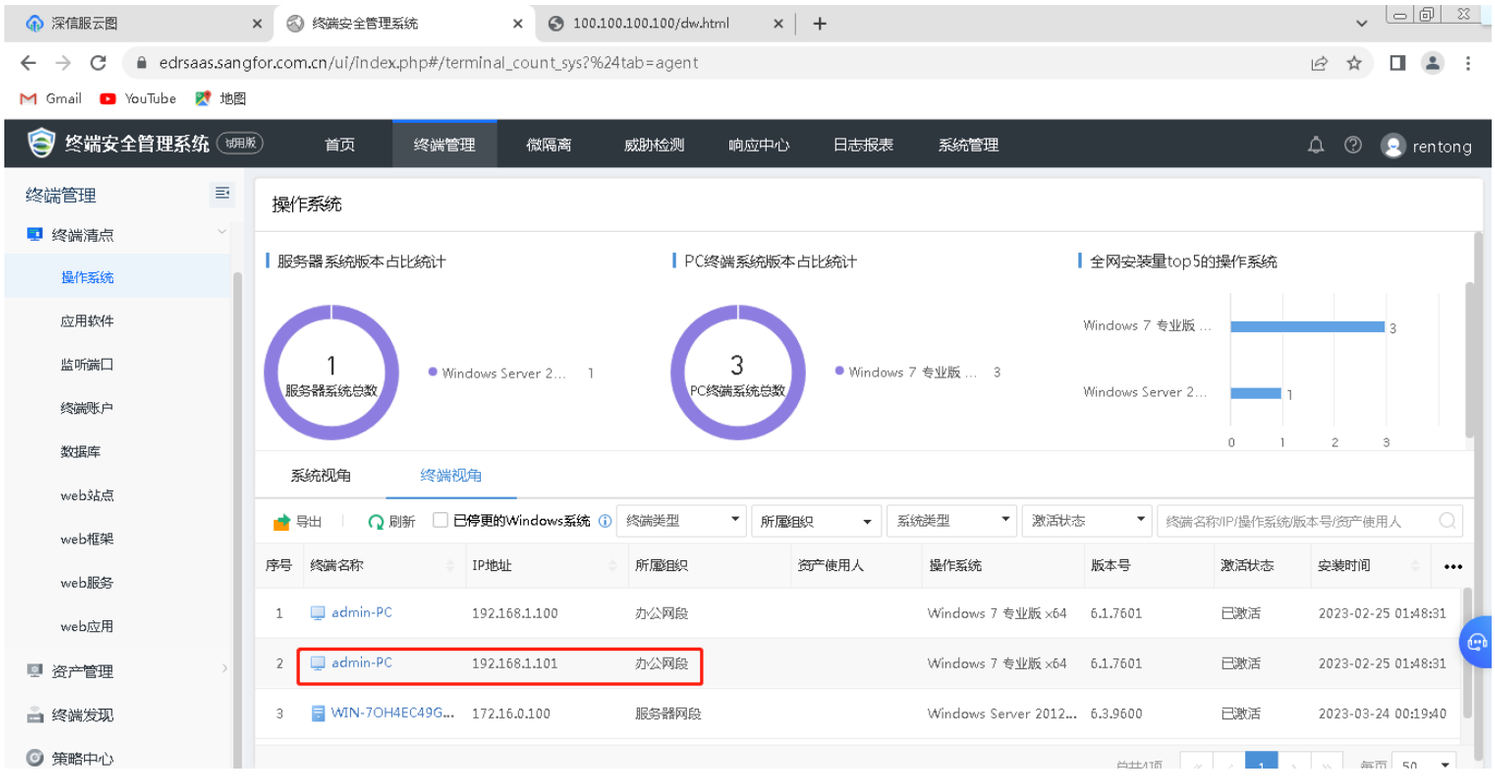

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/install_and_deploy?%24tab=windowsTab
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
系统管理
终端部署
升级管理
联动管理
授权管理
系统设置
终端部署
通用部署
收起
安装完成，开启您的防护之旅吧
开启防护
中心
windows客户端安装程序默认命名（类似：edr_installer_edrinterconnection.sangfor.com.cn_443_47266278.exe ）包含终端安全管理系统平台的通讯地址信息，下载后请勿更改安装程序名。
中心
1、下载后请勿更改安装程序名
2、安装包在部署过程中全程无感知，后台执行直至安装成功
3、若用户端已经安装了Agent，由于静默安装无法弹窗，可能会导致覆盖失败，建议您先在终端管理中卸载该终端的Agent再执行静

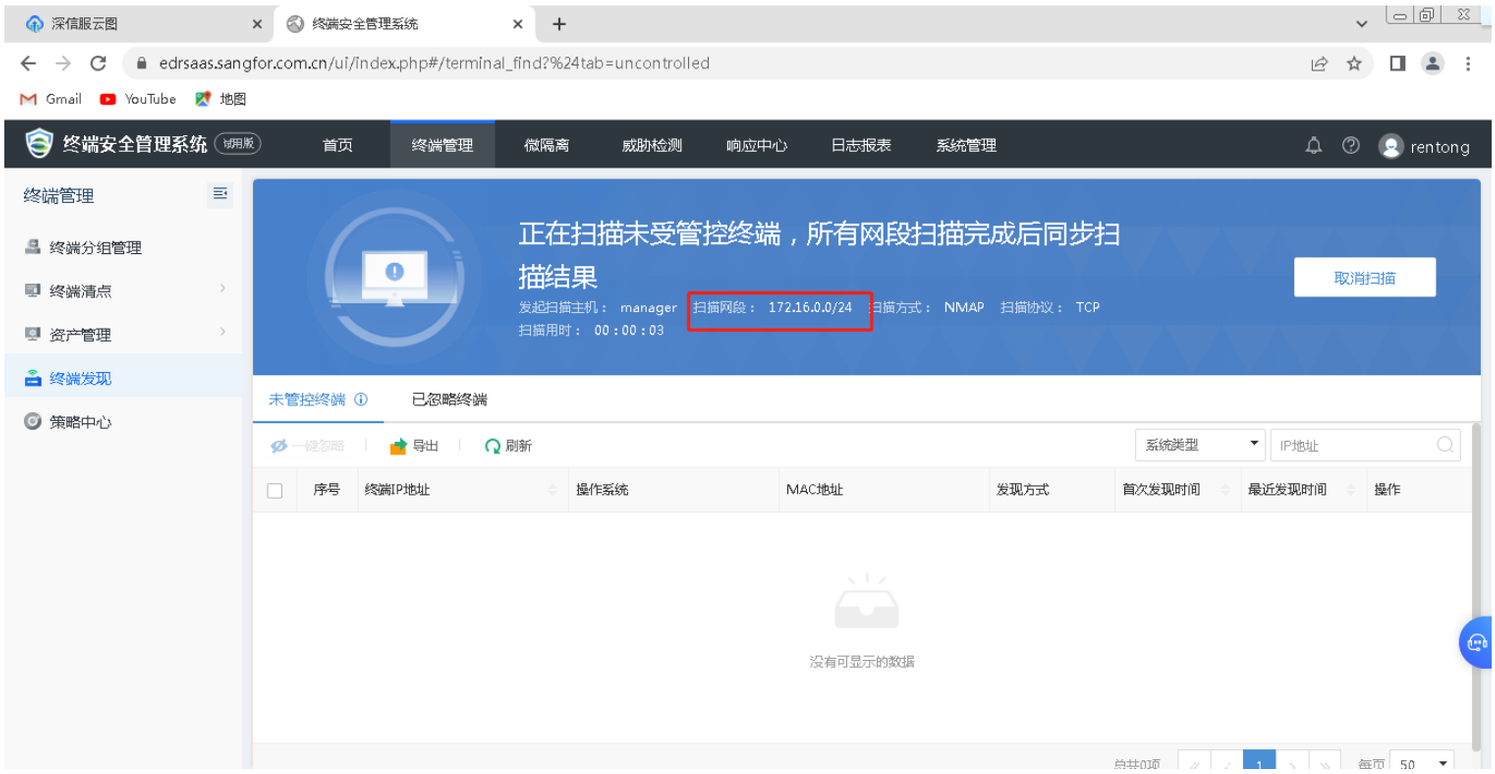

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_group_manage
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
新增
更多
搜索分组
全部终端
本级中心
未分组终端
全部终端（在线3/总数3）
新特性
移动到组
启用agent
远程协助
更多
刷新
实时监控状态
终端自动分组
终端类型
终端状态
请输入关键字
序...
终端名称
终端状态
所属组织
IP地址
MAC地址
操作系统
系统CPU利用率
1
admin-PC
在线
未分组终端
192.168.1.150
FE-FC-FE-E1-B2-FB
Windows ...
1%
2
WIN-7OH...
在线
未分组终端
172.16.0.100
FE-FC-FE-DE-E3-...
Windows ...
0%
3
admin-PC
在线
未分组终端
192.168.1.100
FE-FC-FE-B1-57-82
Windows ...
7%
已使用/总容


深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_group_manage
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
新增
更多
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
全部终端（在线3/总数3）
新特性
移动到组
启用agent
远程协助
更多
刷新
实时监控状态
终端自动分组
终端类型
终端状态
请输入关键字
序...
终端名称
终端状态
所属组织
IP地址
MAC地址
操作系统
系统CPU利用率
1
admin-PC
在线
未分组终端
192.168.1.150
FE-FC-FE-E1-B2-FB
Windows ...
0%
2
WIN-7OH...
在线
服务器网段
172.16.0.100
FE-FC-FE-DE-E3-...
Windows ...
0%
3
admin-PC
在线
办公网段
192.168.1.100
FE-FC-FE-B1-57-82
Windows ...
8%
已使用/总容

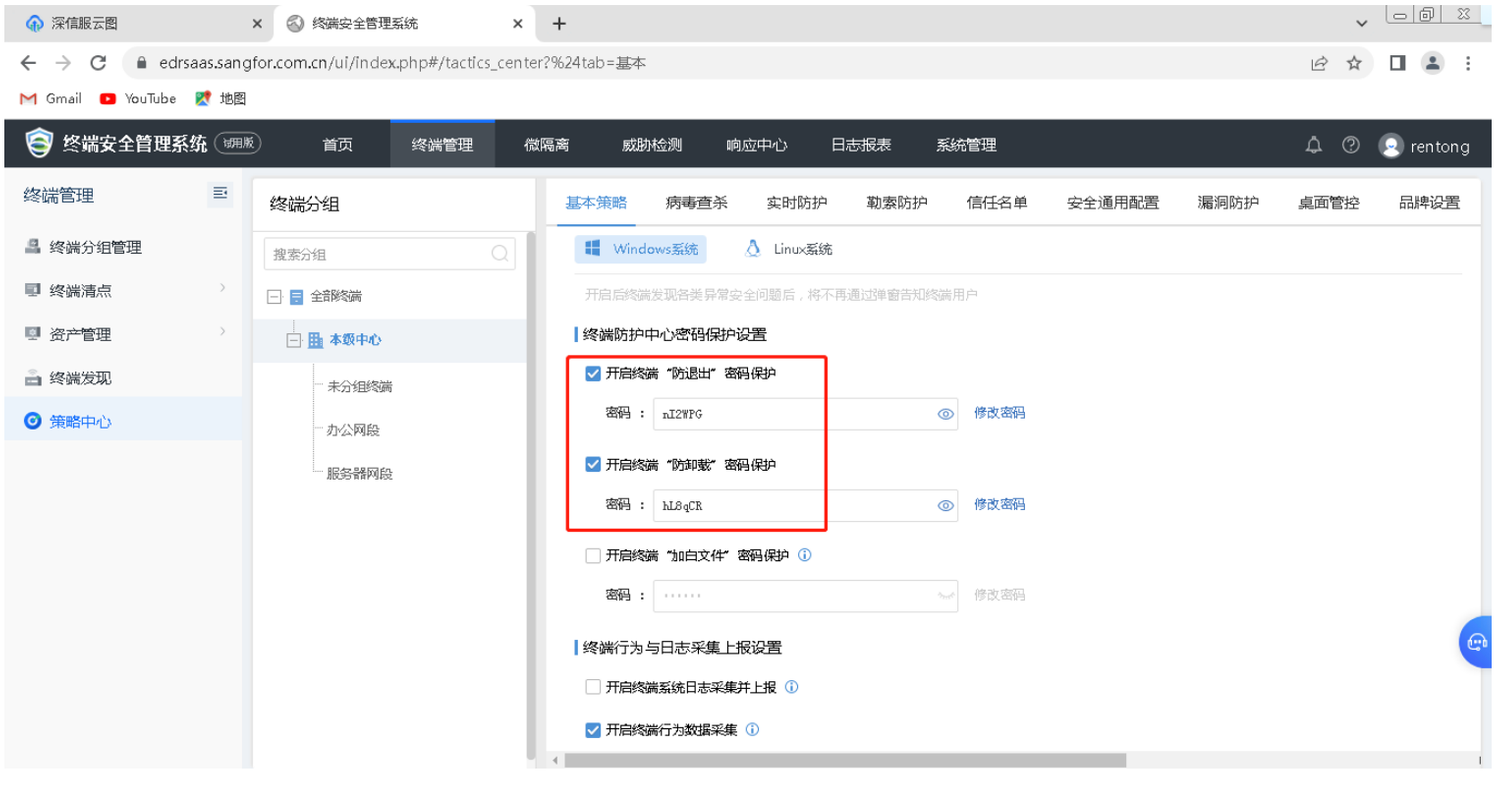

深信服云图
终端安全管理系统
100.100.100.100/dw.html
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_group_manage
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
新增
更多
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
全部终端（在线4/总数4）
新特性
移动到组
启用agent
远程协助
更多
刷新
实时监控状态
终端自动分组
终端类型
终端状态
请输入关键字
序...
终端名称
终端状态
所属组织
IP地址
MAC地址
操作系统
系统CPU利用率
系统
1 admin-PC 在线 未分组终端 192.168.1.150 FE-FC-FE-E1-B2-FB Windows ... 0% 已使用/总容
2 WIN-7OH... 在线 服务器网段 172.16.0.100 FE-FC-FE-DE-E3-... Windows ... 0% 已使用/总容
3 admin-PC 在线 办公网段 192.168.1.100 FE-FC-FE-B1-57-82 Windows ... 5% 已使用/总容
4 admin-PC 在线 办公网段 192.168.1.101 FE-FC-FE-7D-34-... Windows ... 16% 已使用/总容

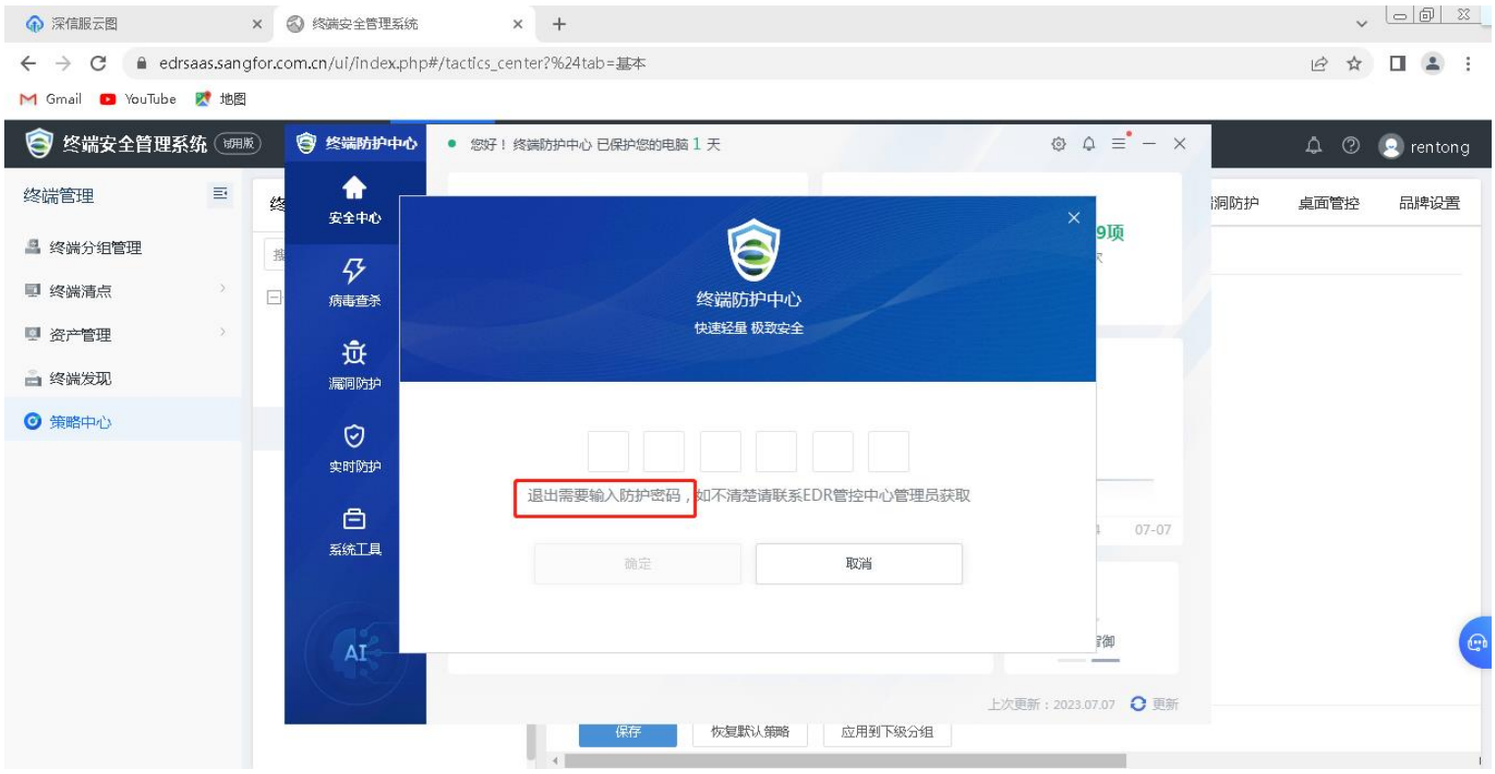

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/terminal_count_sys?%24tab=agent
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
操作系统
应用软件
监听端口
终端账户
数据库
web站点
web框架
web服务
web应用
资产管理
操作系统
服务器系统版本占比统计
1
服务器系统总数
Windows Server 2... 1
PC终端系统版本占比统计
2
PC终端系统总数
Windows 7 专业版 ... 2
全网安装量top5的操作系统
Windows 7 专业版 ... 2
Windows Server 2... 1
0 1 2
系统视角
终端视角
导出
刷新
已停更的Windows系统
终端类型
所属组织
系统类型
激活状态
终端名称/IP/操作系统/版本号/资产使用人
序号
终端名称
IP地址
所属组织
资产使用人
操作系统
版本号
激活状态
安装时间
1 admin-PC 192.168.1.100 办公网段 Windows 7 专业版 x64 6.1.7601 已激活 2023-02-25 01:48:31
2 WIN-7OH4EC49G... 172.16.0.100 服务器网段 Windows Server 2012... 6.3.9600 已激活 2023-03-24 00:19:40
3 admin-PC 192.168.1.150 未分组终端 Windows 7 专业版 x64 6.1.7601 已激活 2023-02-25 01:48:31
总共3项
1
每页 50

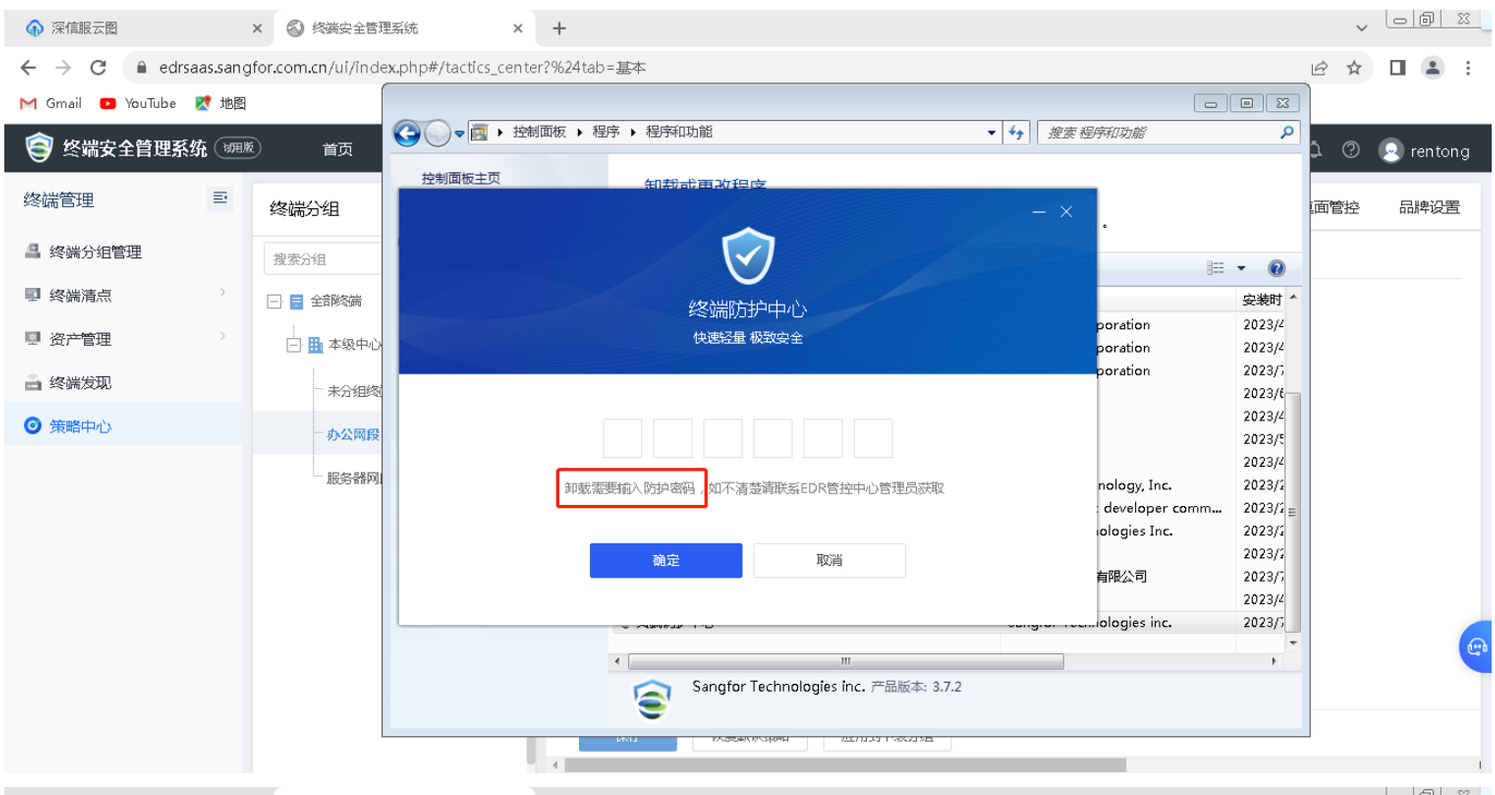

深信服云图
终端安全管理系统
100.100.100.100/dw.html
edrsaas.sangfor.com.cn/ui/index.php#/terminal_count_sys?%24tab=agent
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端清点
操作系统
应用软件
监听端口
终端账户
数据库
web站点
web框架
web服务
web应用
资产管理
终端发现
策略中心
操作系统
服务器系统版本占比统计
1
服务器系统总数
Windows Server 2... 1
PC终端系统版本占比统计
3
PC终端系统总数
Windows 7 专业版 ... 3
全网安装量top5的操作系统
Windows 7 专业版 ... 3
Windows Server 2... 1
0 1 2 3
系统视角
终端视角
导出
刷新
已停更的Windows系统
终端类型
所属组织
系统类型
激活状态
终端名称/IP/操作系统/版本号/资产使用人
序号
终端名称
IP地址
所属组织
资产使用人
操作系统
版本号
激活状态
安装时间
1 admin-PC 192.168.1.100 办公网段 Windows 7 专业版 x64 6.1.7601 已激活 2023-02-25 01:48:31
2 admin-PC 192.168.1.101 办公网段 Windows 7 专业版 x64 6.1.7601 已激活 2023-02-25 01:48:31
3 WIN-7OH4EC49G... 172.16.0.100 服务器网段 Windows Server 2012... 6.3.9600 已激活 2023-03-24 00:19:40

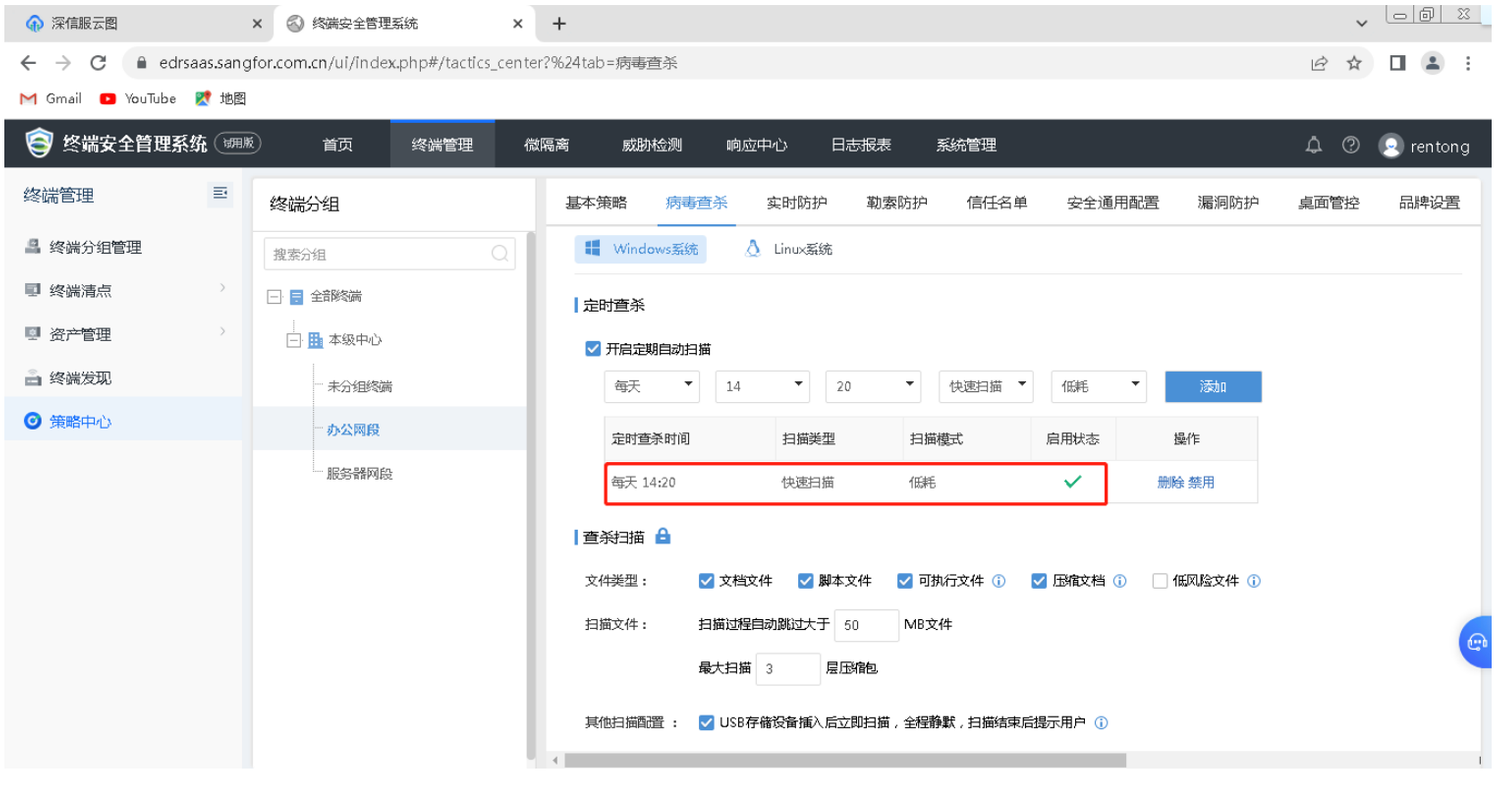

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/terminal_find?%24tab=uncontrolled
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
正在扫描未受管控终端，所有网段扫描完成后同步扫描结果
发起扫描主机： manager
扫描网段： 172.16.0.0/24
扫描方式： NMAP
扫描协议： TCP
扫描用时： 00：00：03
取消扫描
未管控终端
已忽略终端
一键忽略
导出
刷新
系统类型
IP地址
序号
终端IP地址
操作系统
MAC地址
发现方式
首次发现时间
最近发现时间
操作
没有可显示的数据
总共0项
每页 50

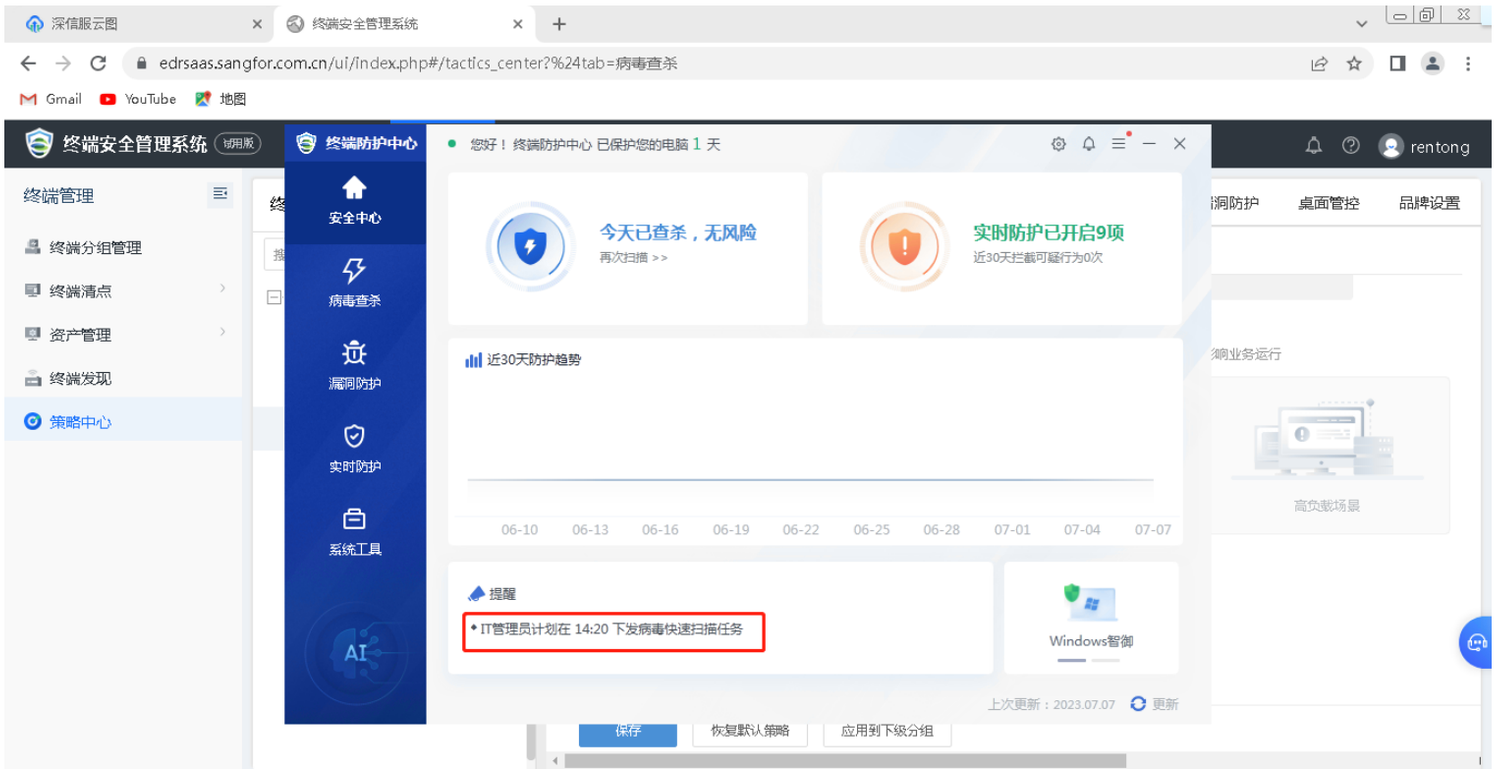

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/terminal_find?%24tab=uncontrolled
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
扫描内网中未部署终端安全管理系统客户端的活跃主机
已发现全网未受管控的终端0台
立即扫描
未管控终端
已忽略终端
一键忽略
导出
刷新
系统类型
IP地址
序号
终端IP地址
操作系统
MAC地址
发现方式
首次发现时间
最近发现时间
操作
没有可显示的数据
总共0项
每页 50


深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=基本
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
基本策略
病毒查杀
实时防护
勒索防护
信任名单
安全通用配置
漏洞防护
桌面管控
品牌设置
Windows系统
Linux系统
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
终端防护中心密码保护设置
开启终端“防退出”密码保护
密码：
nI2WPG
修改密码
开启终端“防卸载”密码保护
密码：
hL8qCR
修改密码
开启终端“加白文件”密码保护
密码：
修改密码
终端行为与日志采集上报设置
开启终端系统日志采集并上报
开启终端行为数据采集

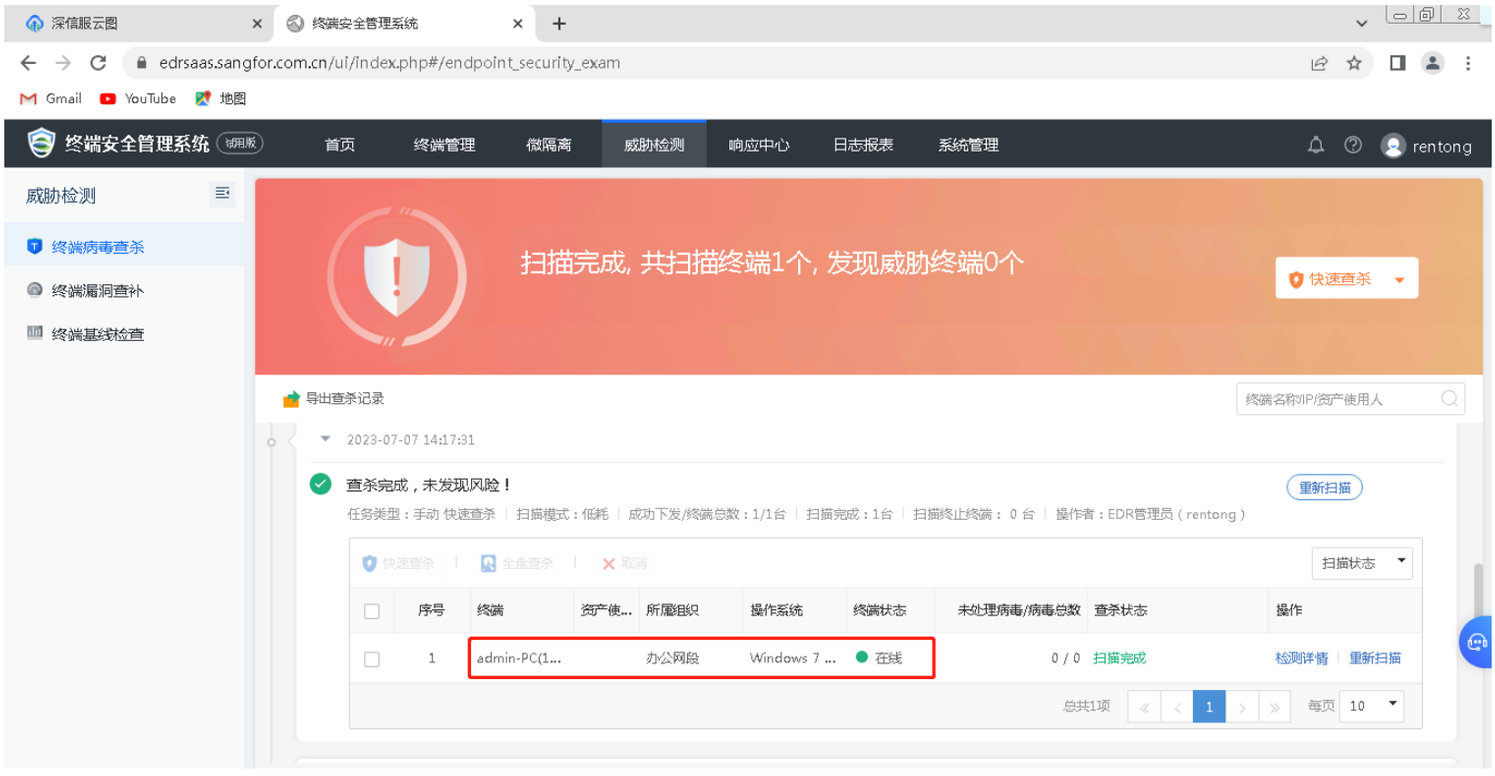

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=基本
Gmail
YouTube
地图
终端安全管理系统
试用版
终端防护中心
您好！终端防护中心 已保护您的电脑 1 天
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
安全中心
病毒查杀
漏洞防护
实时防护
系统工具
AI
终端防护中心
快速轻量 极致安全
退出需要输入防护密码，如不清楚请联系EDR管控中心管理员获取
确定
取消
漏洞防护
桌面管控
品牌设置
上次更新：2023.07.07
更新
保存
恢复默认策略
应用到下级分组

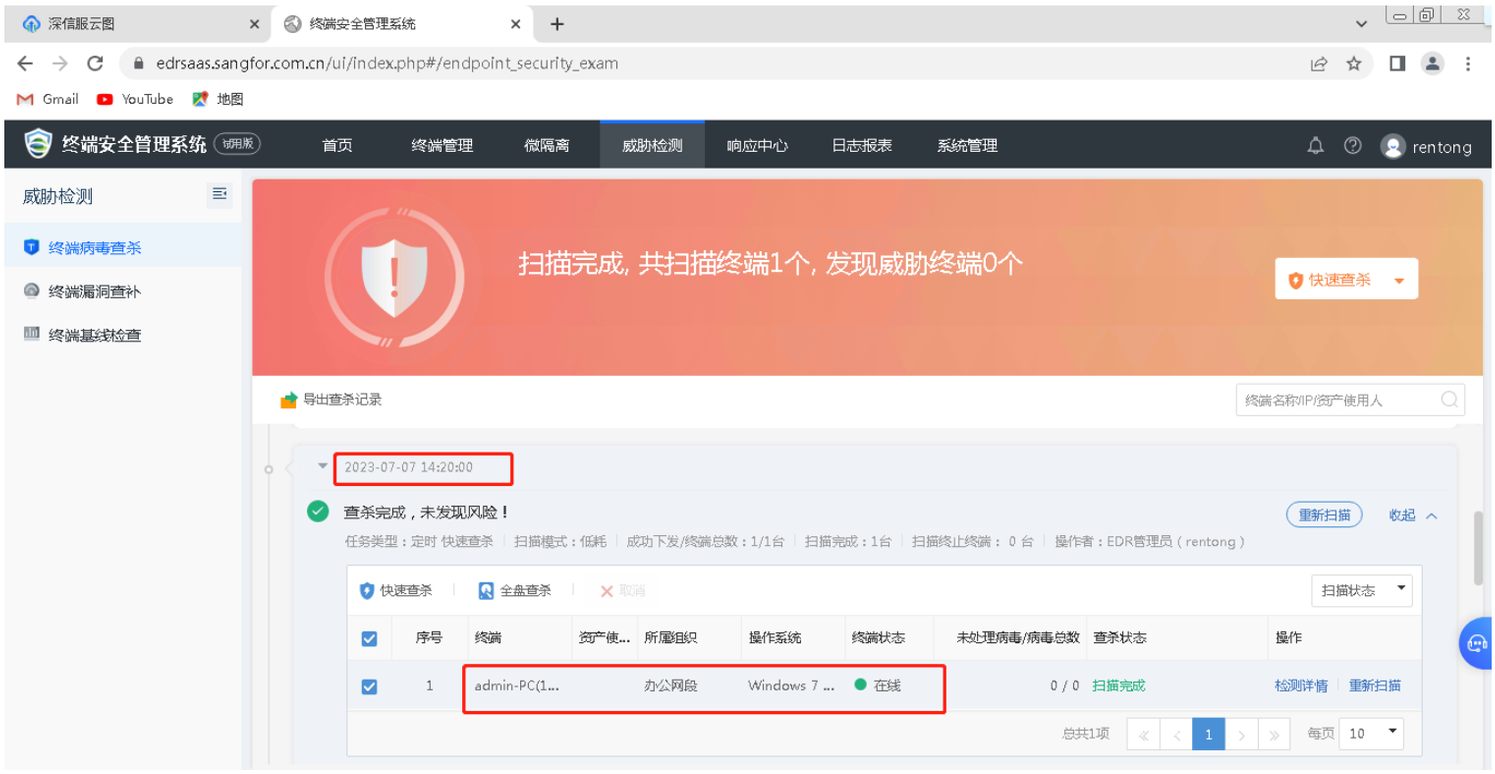

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=基本
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
控制面板
程序
程序和功能
控制面板主页
卸载或更改程序
终端防护中心
快速轻量 极致安全
卸载需要输入防护密码，如不清楚请联系EDR管控中心管理员获取
确定
取消
安装时
Sangfor Technologies Inc. 产品版本: 3.7.2
桌面管控
品牌设置

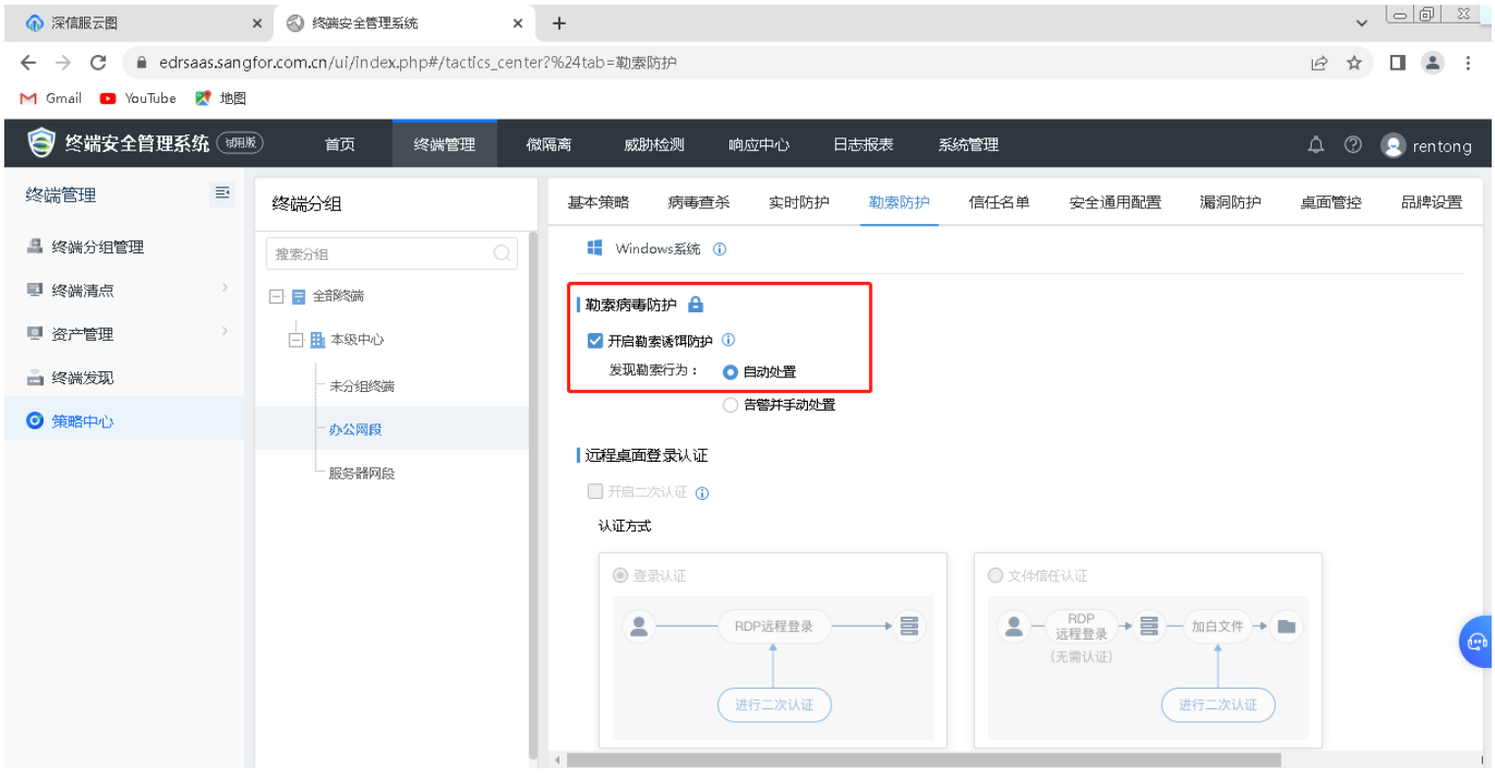

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=病毒查杀
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
基本策略
病毒查杀
实时防护
勒索防护
信任名单
安全通用配置
漏洞防护
桌面管控
品牌设置
Windows系统
Linux系统
定时查杀
开启定期自动扫描
每天
14
20
快速扫描
低耗
添加
定时查杀时间
扫描类型
扫描模式
启用状态
操作
每天 14:20
快速扫描
低耗
删除 禁用
查杀扫描
文件类型：
文档文件
脚本文件
可执行文件
压缩文档
低风险文件
扫描文件：
扫描过程自动跳过大于
50
MB文件
最大扫描
3
层压缩包
其他扫描配置：
USB存储设备插入后立即扫描，全程静默，扫描结束后提示用户

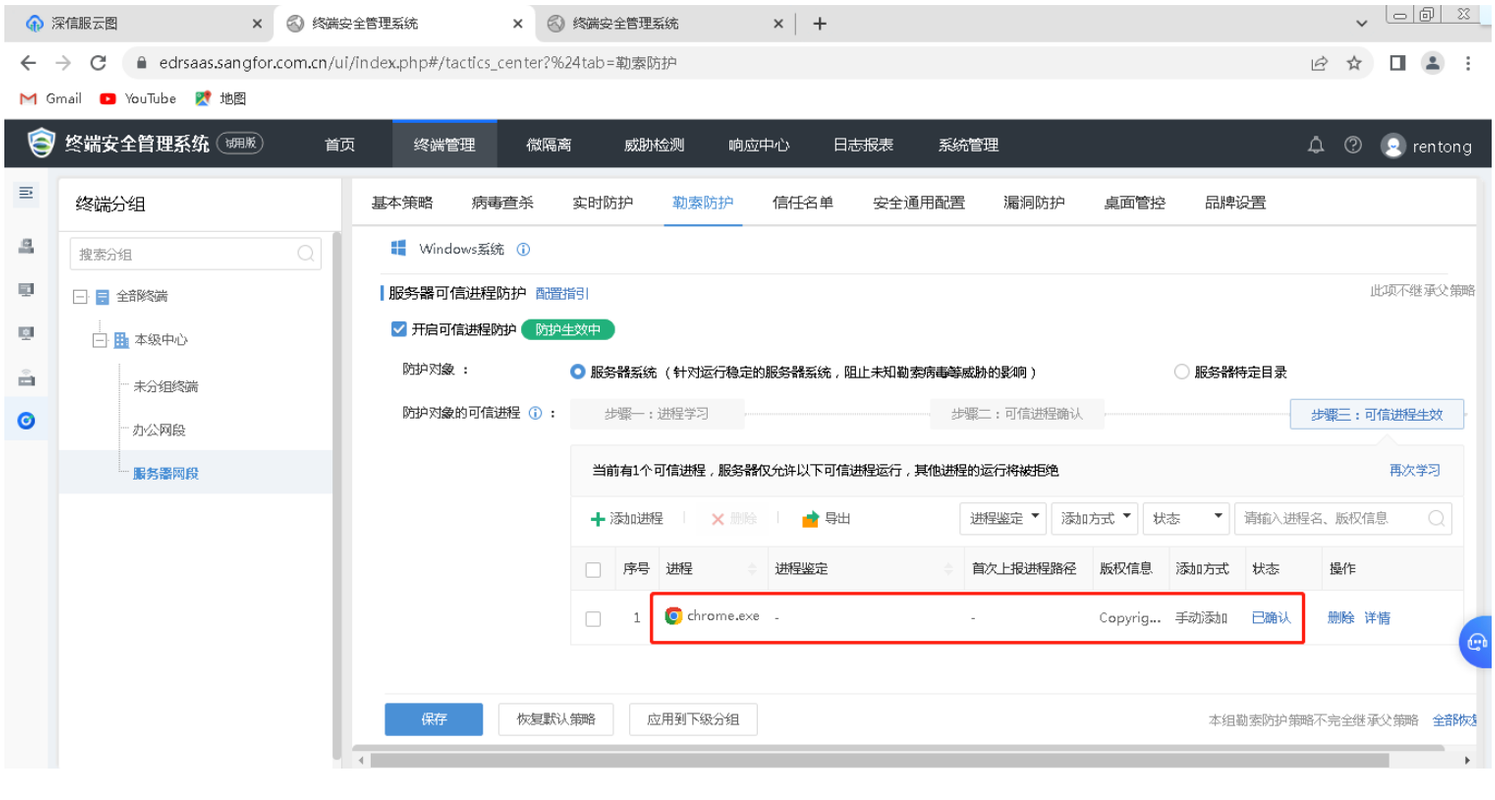

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=病毒查杀
Gmail
YouTube
地图
终端安全管理系统 试用版
终端防护中心
您好！终端防护中心 已保护您的电脑 1 天
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
安全中心
病毒查杀
漏洞防护
实时防护
系统工具
AI
今天已查杀，无风险
再次扫描 >>
实时防护已开启9项
近30天拦截可疑行为0次
近30天防护趋势
06-10
06-13
06-16
06-19
06-22
06-25
06-28
07-01
07-04
07-07
提醒
IT管理员计划在 14:20 下发病毒快速扫描任务
Windows智御
上次更新：2023.07.07
更新
保存
恢复默认策略
应用到下级分组
桌面管控
品牌设置
高负载场景

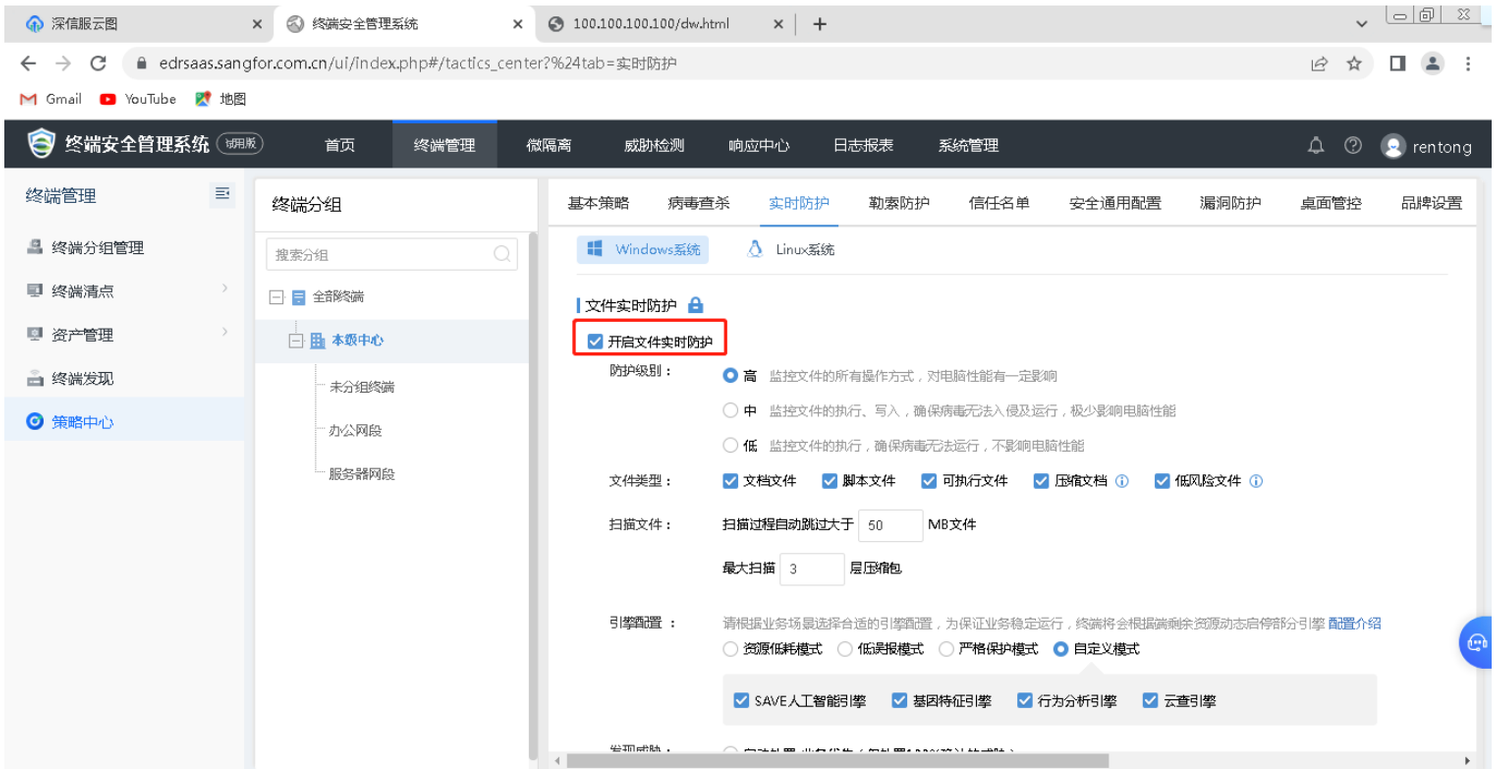

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_security_exam
Gmail
YouTube
地图
终端安全管理系统 试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
威胁检测
终端病毒查杀
终端漏洞查补
终端基线检查
当前正在进行1个病毒查杀任务...
累计发现威胁终端0个
快速查杀
导出查杀记
终端防护中心
安全中心
病毒查杀
漏洞防护
实时防护
快速扫描中...
00:00:30 C:\Users\admin\AppD...5\LCQ8SGL9\t[1].js
取消扫描
暂停
取消
内存
扫描73个文件
系统进程
扫描688个文件
重新扫描
系统启动项
扫描162个文件

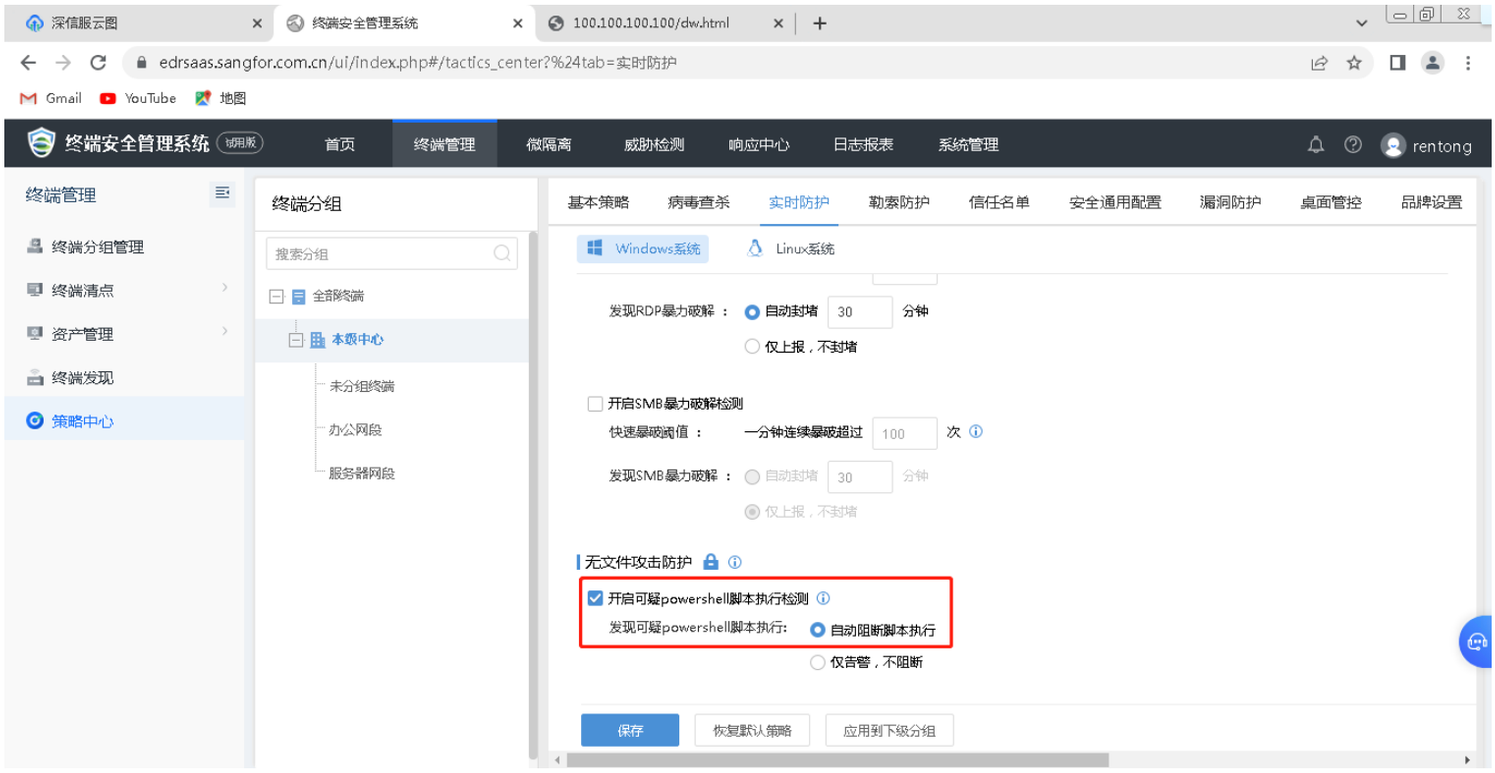

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_security_exam
Gmail
YouTube
地图
终端安全管理系统 试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
威胁检测
终端病毒查杀
终端漏洞查补
终端基线检查
扫描完成，共扫描终端1个，发现威胁终端0个
快速查杀
导出查杀记录
终端名称/IP/资产使用人
2023-07-07 14:17:31
查杀完成，未发现风险！
重新扫描
任务类型：手动 快速查杀 | 扫描模式：低耗 | 成功下发/终端总数：1/1台 | 扫描完成：1台 | 扫描终止终端：0 台 | 操作者：EDR管理员（rentong）
快速查杀
全盘查杀
取消
扫描状态
序号
终端
资产使...
所属组织
操作系统
终端状态
未处理病毒/病毒总数
查杀状态
操作
1
admin-PC(1...
办公网段
Windows 7 ...
在线
0 / 0
扫描完成
检测详情
重新扫描
总共1项
每页 10

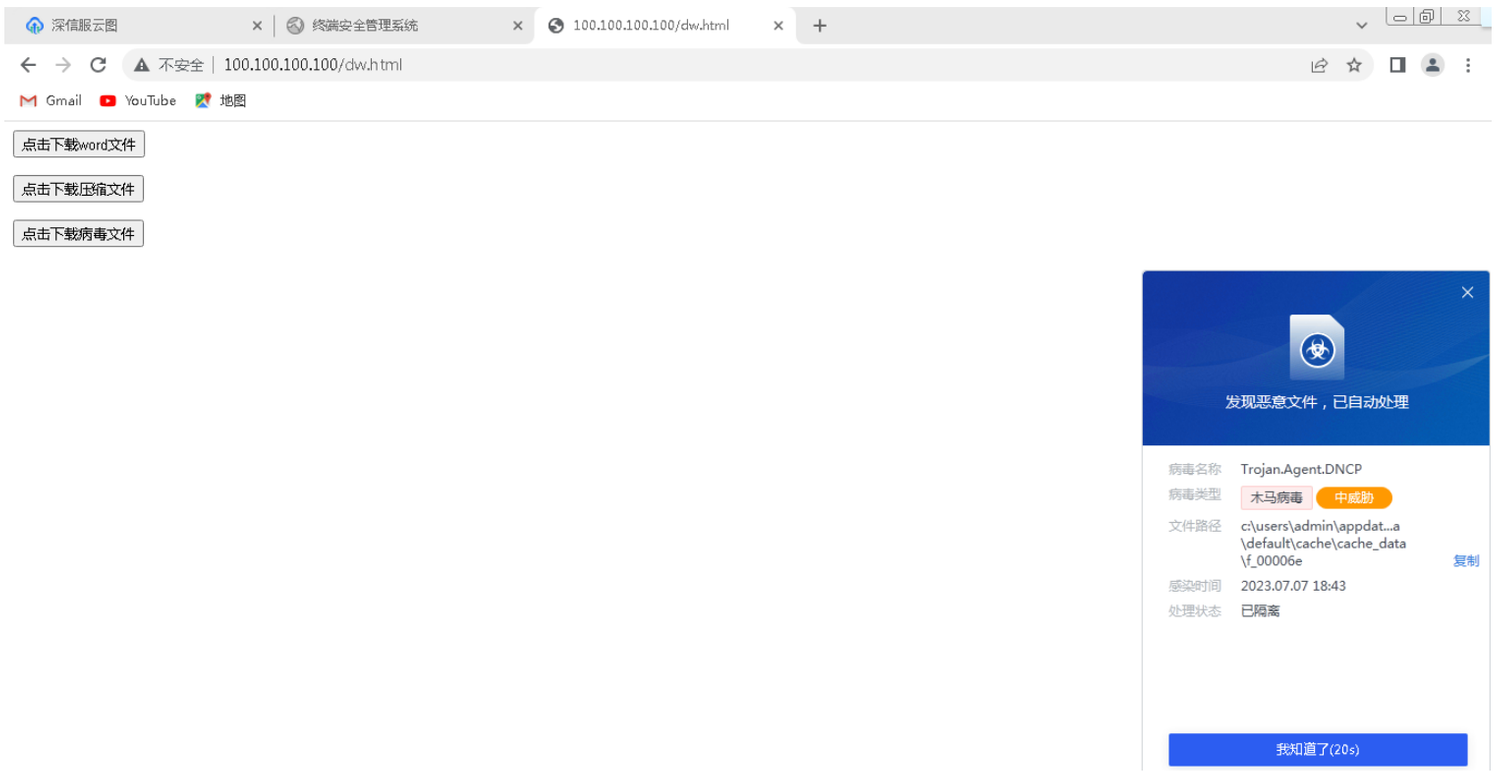

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_security_exam
Gmail
YouTube
地图
终端安全管理系统
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
威胁检测
终端病毒查杀
终端漏洞查补
终端基线检查
扫描完成，共扫描终端1个，发现威胁终端0个
快速查杀
导出查杀记录
终端名称/IP/资产使用人
2023-07-07 14:20:00
查杀完成，未发现风险！
重新扫描
收起
任务类型：定时 快速查杀 | 扫描模式：低耗 | 成功下发/终端总数：1/1台 | 扫描完成：1台 | 扫描终止终端：0台 | 操作者：EDR管理员（rentong）
快速查杀
全盘查杀
取消
扫描状态
序号
终端
资产使...
所属组织
操作系统
终端状态
未处理病毒/病毒总数
查杀状态
操作
1
admin-PC(1...
办公网段
Windows 7 ...
在线
0 / 0
扫描完成
检测详情
重新扫描
总共1项
每页 10

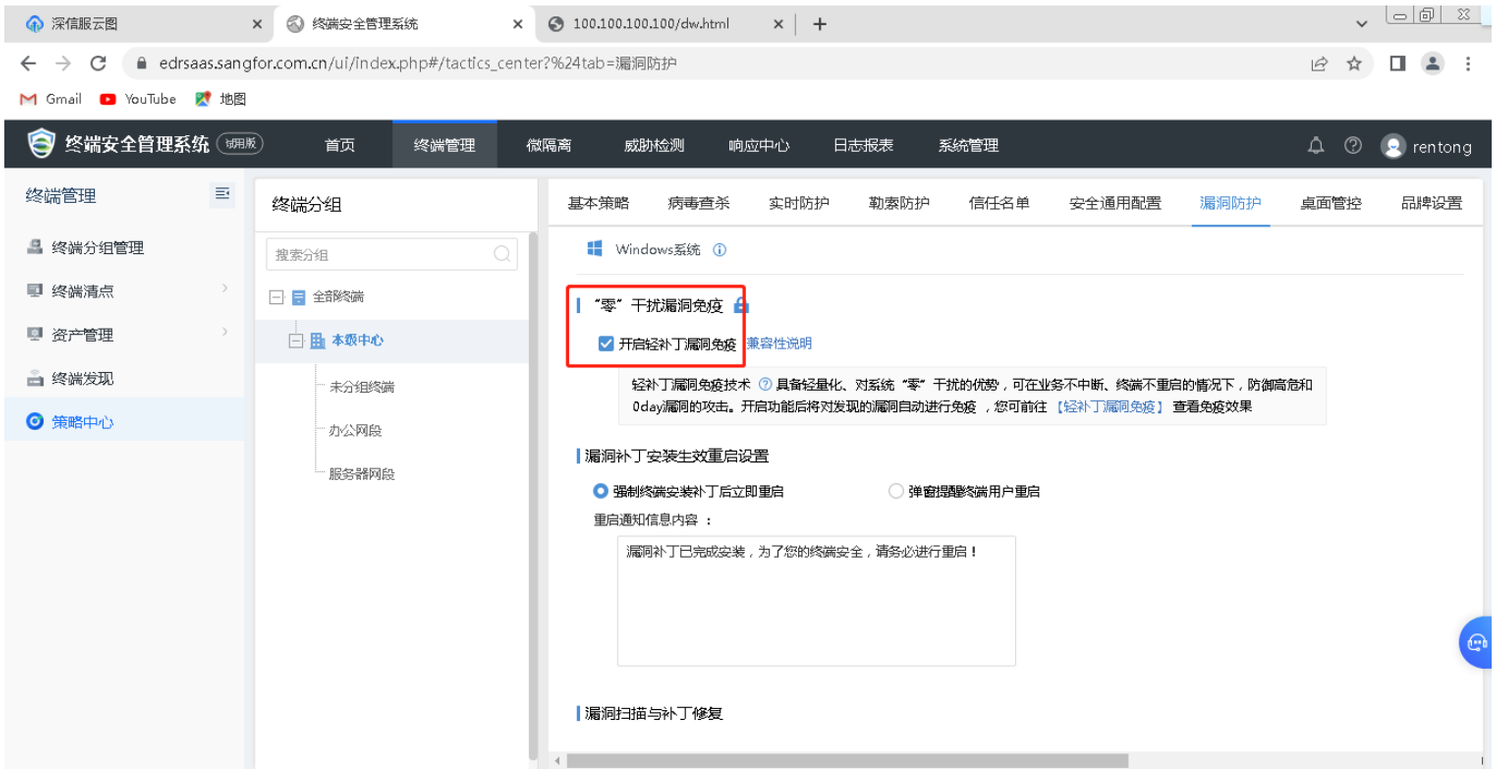

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=勒索防护
Gmail
YouTube
地图
终端安全管理系统
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
基本策略
病毒查杀
实时防护
勒索防护
信任名单
安全通用配置
漏洞防护
桌面管控
品牌设置
Windows系统
勒索病毒防护
开启勒索诱饵防护
发现勒索行为：
自动处置
告警并手动处置
远程桌面登录认证
开启二次认证
认证方式
登录认证
RDP远程登录
进行二次认证
文件信任认证
RDP远程登录
（无需认证）
加白文件
进行二次认证

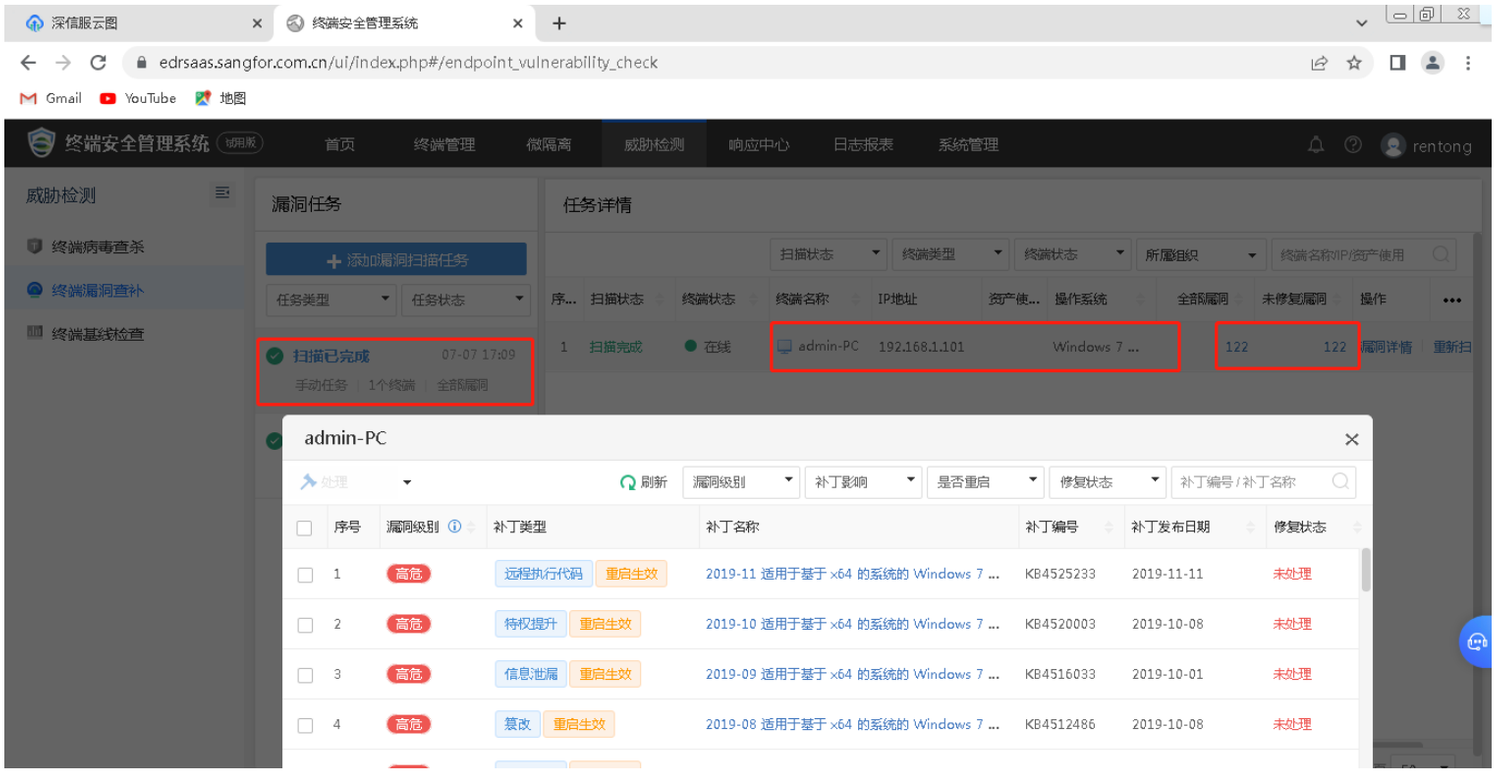

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=勒索防护
Gmail
YouTube
地图
终端安全管理系统
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端分组
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
基本策略
病毒查杀
实时防护
勒索防护
信任名单
安全通用配置
漏洞防护
桌面管控
品牌设置
Windows系统
服务器可信进程防护
配置指引
此项不继承父策略
开启可信进程防护
防护生效中
防护对象：
服务器系统（针对运行稳定的服务器系统，阻止未知勒索病毒等威胁的影响）
服务器特定目录
防护对象的可信进程：
步骤一：进程学习
步骤二：可信进程确认
步骤三：可信进程生效
当前有1个可信进程，服务器仅允许以下可信进程运行，其他进程的运行将被拒绝
再次学习
添加进程
删除
导出
进程鉴定
添加方式
状态
请输入进程名、版权信息
序号
进程
进程鉴定
首次上报进程路径
版权信息
添加方式
状态
操作
1
chrome.exe
-
-
Copyrig...
手动添加
已确认
删除
详情
保存
恢复默认策略
应用到下级分组
本组勒索防护策略不完全继承父策略
全部恢复

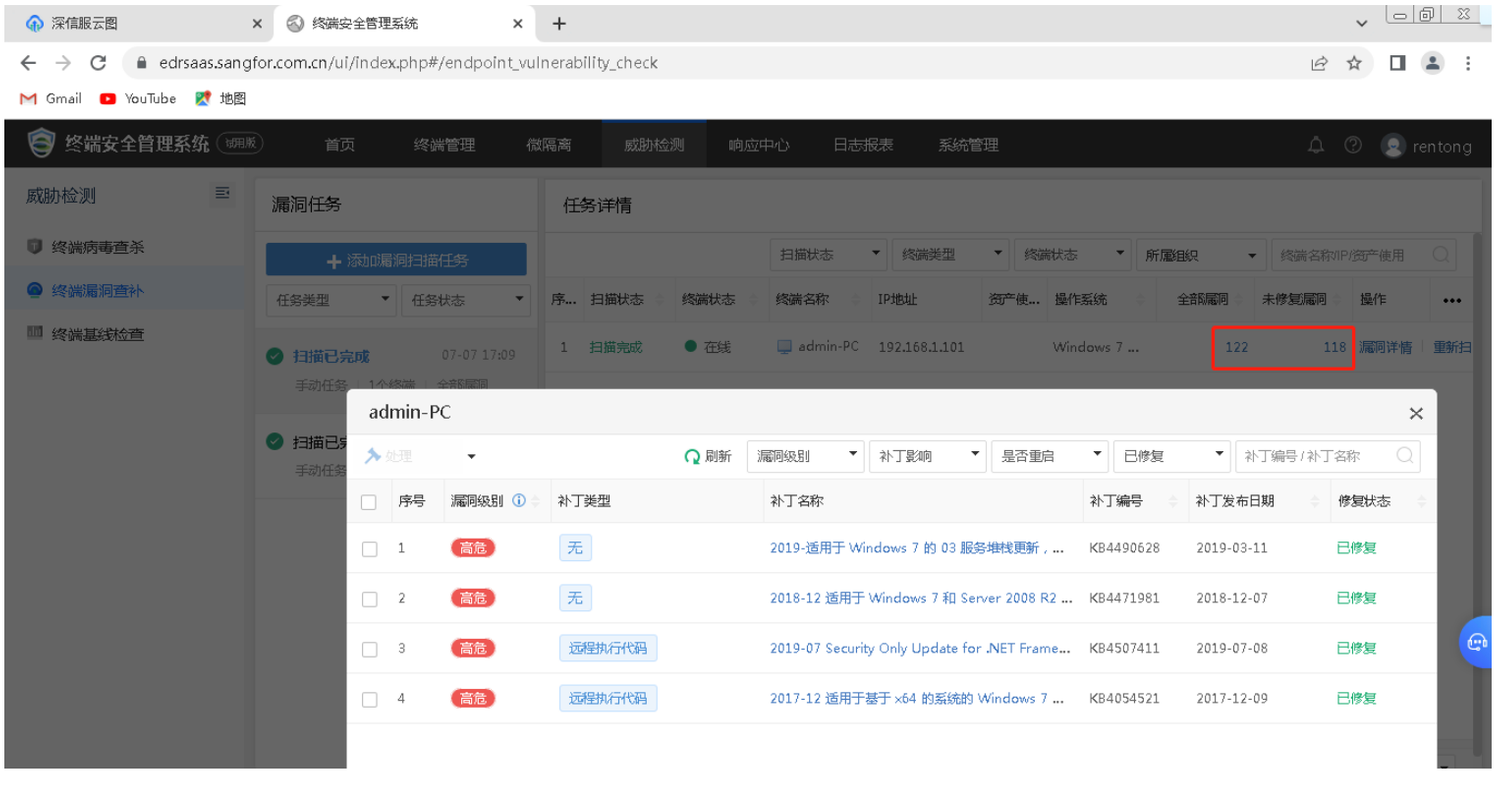

深信服云图
终端安全管理系统
100.100.100.100/dw.html
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=实时防护
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
基本策略
病毒查杀
实时防护
勒索防护
信任名单
安全通用配置
漏洞防护
桌面管控
品牌设置
Windows系统
Linux系统
文件实时防护
开启文件实时防护
防护级别：
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：
文档文件
脚本文件
可执行文件
压缩文档
低风险文件
扫描文件：
扫描过程自动跳过大于 50 MB文件
最大扫描 3 层压缩包
引擎配置：
请根据业务场景选择合适的引擎配置，为保证业务稳定运行，终端将会根据端侧余资源动态启停部分引擎 配置介绍
资源低耗模式
低误报模式
严格保护模式
自定义模式
SAVE人工智能引擎
基因特征引擎
行为分析引擎
云查引擎

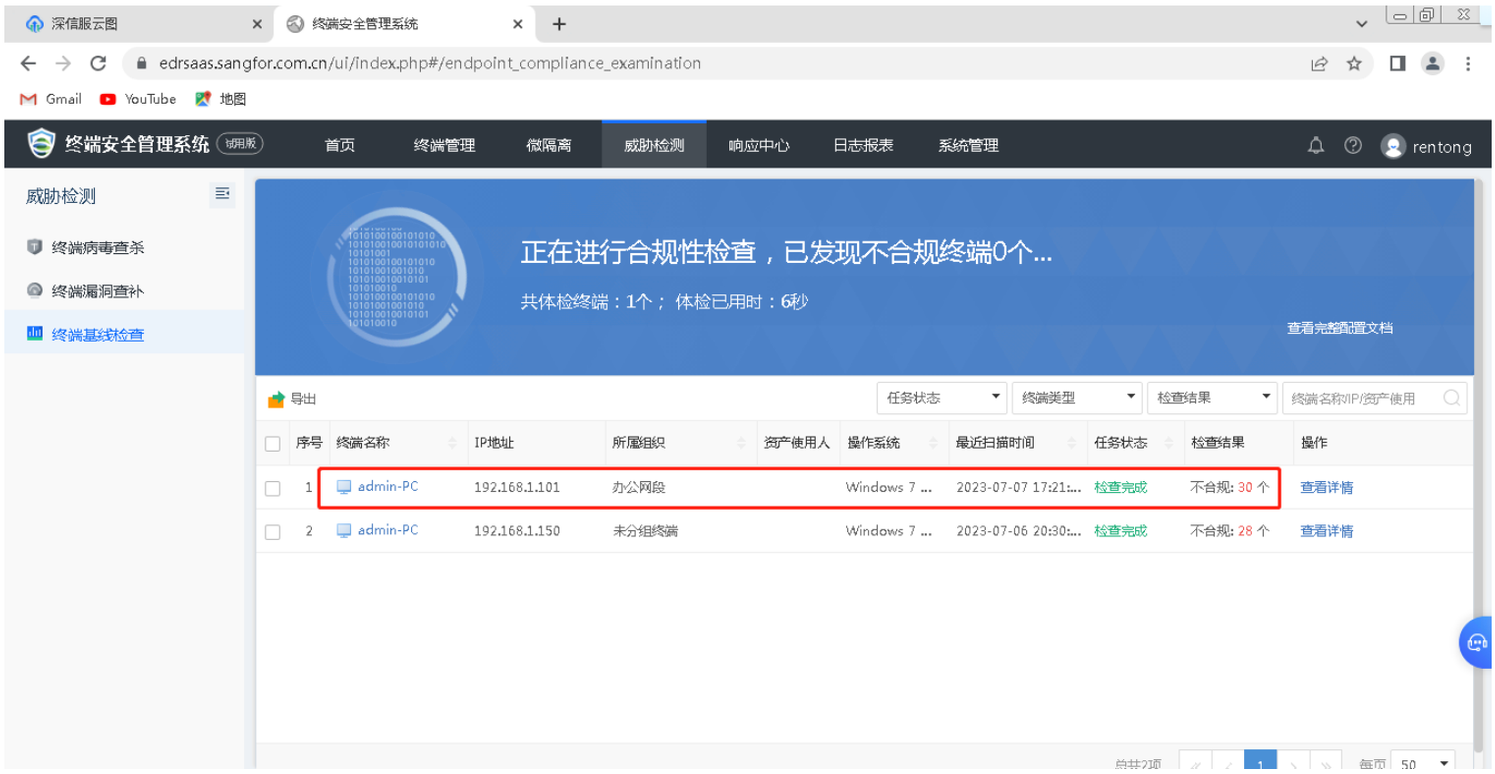

深信服云图
终端安全管理系统
100.100.100.100/dw.html
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=实时防护
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
基本策略
病毒查杀
实时防护
勒索防护
信任名单
安全通用配置
漏洞防护
桌面管控
品牌设置
Windows系统
Linux系统
发现RDP暴力破解：
自动封堵 30 分钟
仅上报，不封堵
开启SMB暴力破解检测
快速暴破阈值：
一分钟连续暴破超过 100 次
发现SMB暴力破解：
自动封堵 30 分钟
仅上报，不封堵
无文件攻击防护
开启可疑powershell脚本执行检测
发现可疑powershell脚本执行：
自动阻断脚本执行
仅告警，不阻断
保存
恢复默认策略
应用到下级分组

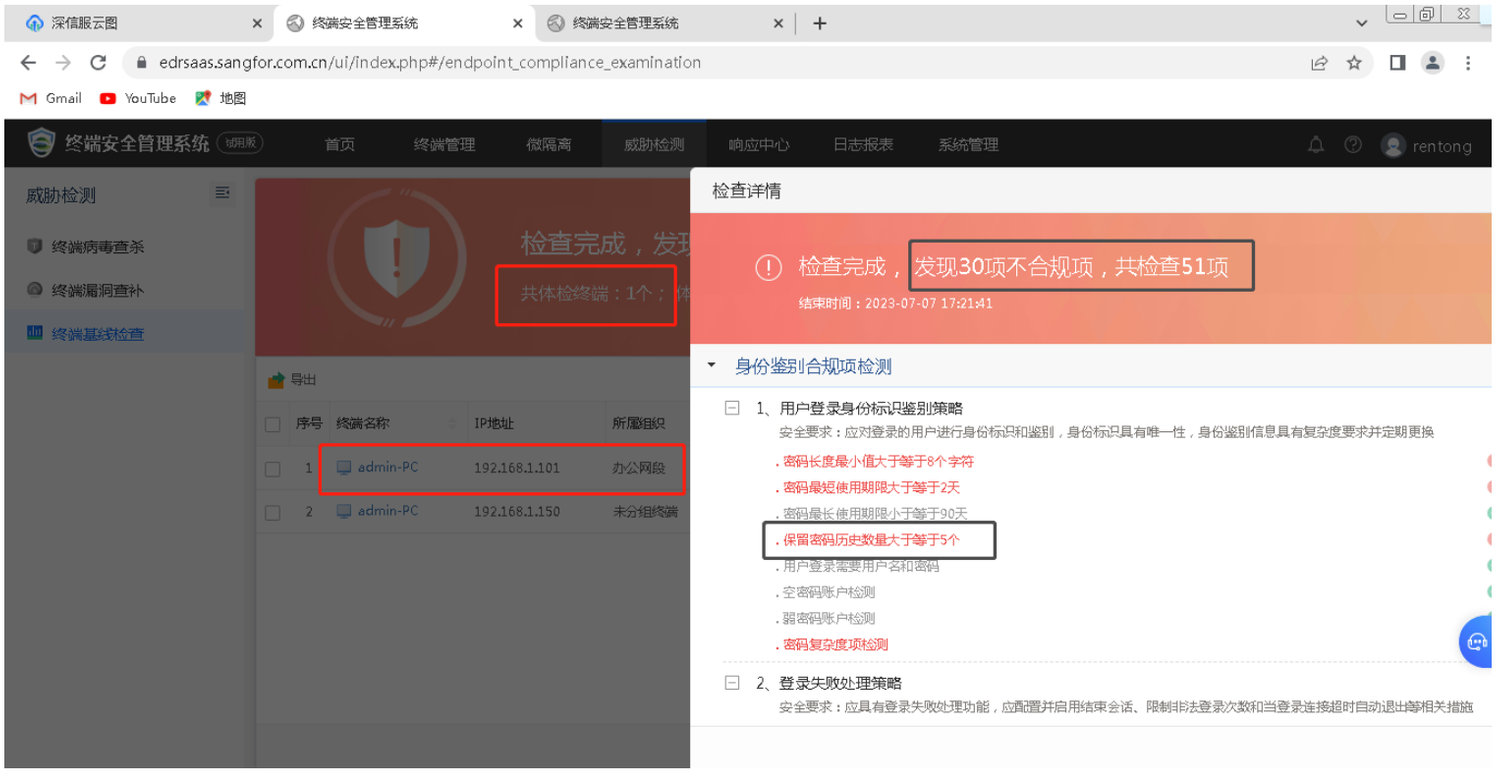

深信服云图
终端安全管理系统
100.100.100.100/dw.html
不安全 | 100.100.100.100/dw.html
Gmail
YouTube
地图
点击下载word文件
点击下载压缩文件
点击下载病毒文件
发现恶意文件，已自动处理
病毒名称 Trojan.Agent.DNCP
病毒类型 木马病毒 中威胁
文件路径 c:\users\admin\appdat...a\default\cache\cache_data\f_00006e
复制
感染时间 2023.07.07 18:43
处理状态 已隔离
我知道了(20s)

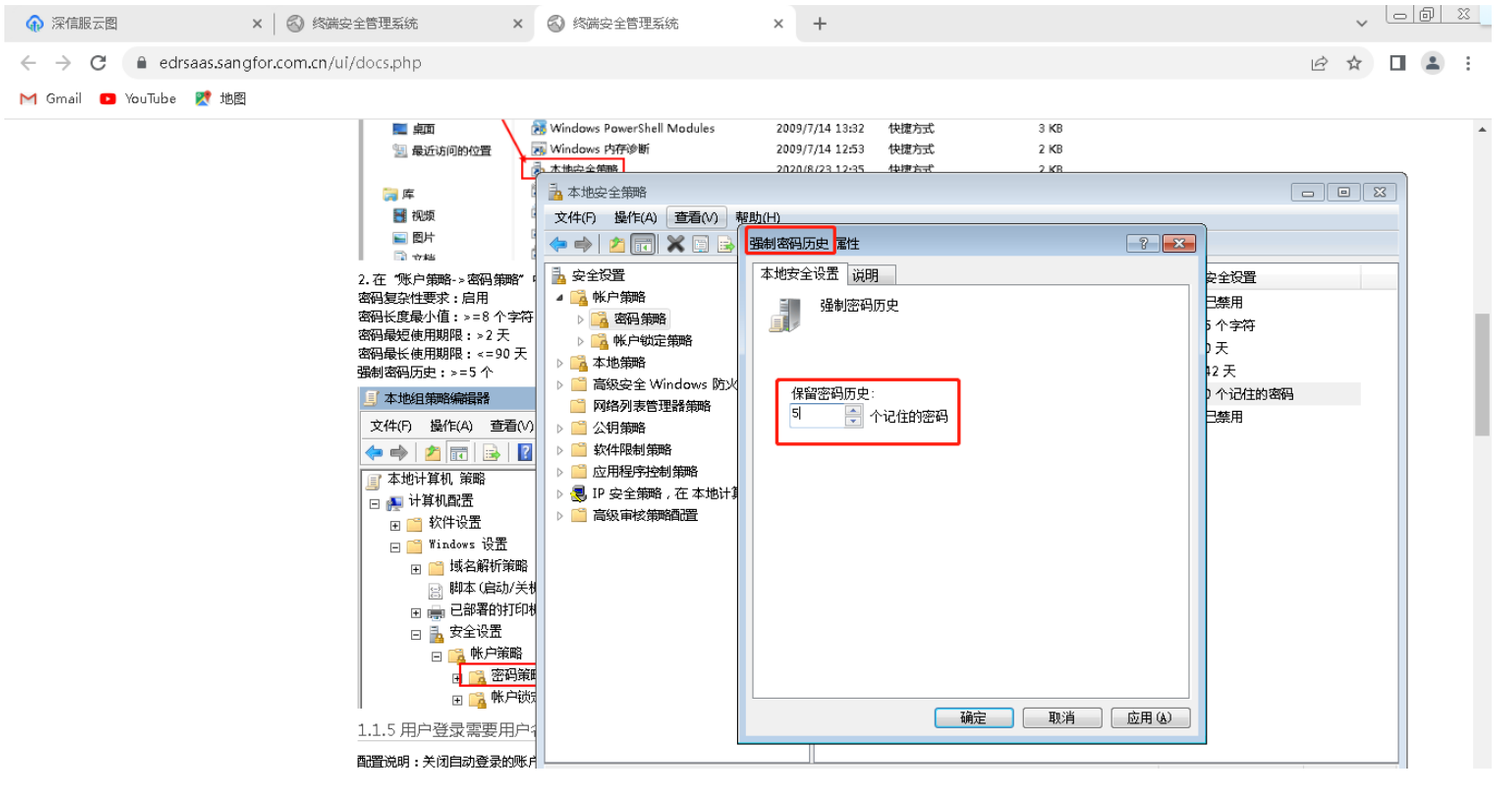

深信服云图
终端安全管理系统
100.100.100.100/dw.html
edrsaas.sangfor.com.cn/ui/index.php#/tactics_center?%24tab=漏洞防护
Gmail
YouTube
地图
终端安全管理系统
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
终端管理
终端分组管理
终端清点
资产管理
终端发现
策略中心
终端分组
搜索分组
全部终端
本级中心
未分组终端
办公网段
服务器网段
基本策略
病毒查杀
实时防护
勒索防护
信任名单
安全通用配置
漏洞防护
桌面管控
品牌设置
Windows系统
“零”干扰漏洞免疫
开启轻补丁漏洞免疫
兼容性说明
轻补丁漏洞免疫技术 具备轻量化、对系统“零”干扰的优势，可在业务不中断、终端不重启的情况下，防御高危和0day漏洞的攻击。开启功能后将对发现的漏洞自动进行免疫 ，您可前往【轻补丁漏洞免疫】查看免疫效果
漏洞补丁安装生效重启设置
强制终端安装补丁后立即重启
弹窗提醒终端用户重启
重启通知信息内容 ：
漏洞补丁已完成安装，为了您的终端安全，请务必进行重启！
漏洞扫描与补丁修复

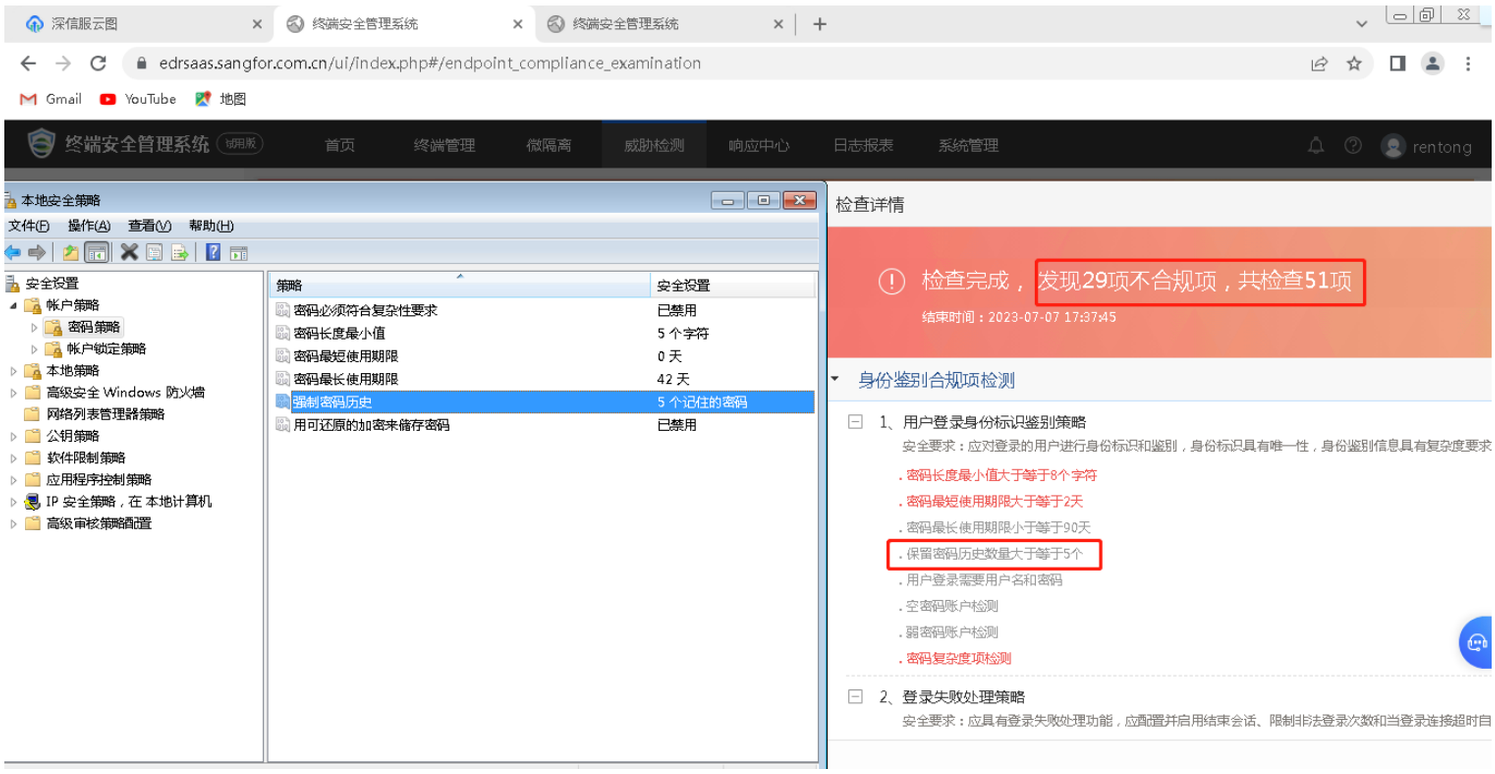

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_vulnerability_check
Gmail
YouTube
地图
威胁检测
终端病毒查杀
终端漏洞查补
终端基线检查
漏洞任务
添加漏洞扫描任务
任务类型
任务状态
扫描已完成
07-07 17:09
手动任务 | 1个终端 | 全部漏洞
任务详情
扫描状态
终端类型
终端状态
所属组织
终端名称/IP/资产使用
序...
扫描状态
终端状态
终端名称
IP地址
资产使...
操作系统
全部漏洞
未修复漏洞
操作
1
扫描完成
在线
admin-PC
192.168.1.101
Windows 7 ...
122
122
漏洞详情
重新扫
admin-PC
处理
刷新
漏洞级别
补丁影响
是否重启
修复状态
补丁编号 / 补丁名称
序号
漏洞级别
补丁类型
补丁名称
补丁编号
补丁发布日期
修复状态
1
高危
远程执行代码
重启生效
2019-11 适用于基于 x64 的系统的 Windows 7 ...
KB4525233
2019-11-11
未处理
2
高危
特权提升
重启生效
2019-10 适用于基于 x64 的系统的 Windows 7 ...
KB4520003
2019-10-08
未处理
3
高危
信息泄漏
重启生效
2019-09 适用于基于 x64 的系统的 Windows 7 ...
KB4516033
2019-10-01
未处理
4
高危
篡改
重启生效
2019-08 适用于基于 x64 的系统的 Windows 7 ...
KB4512486
2019-10-08
未处理

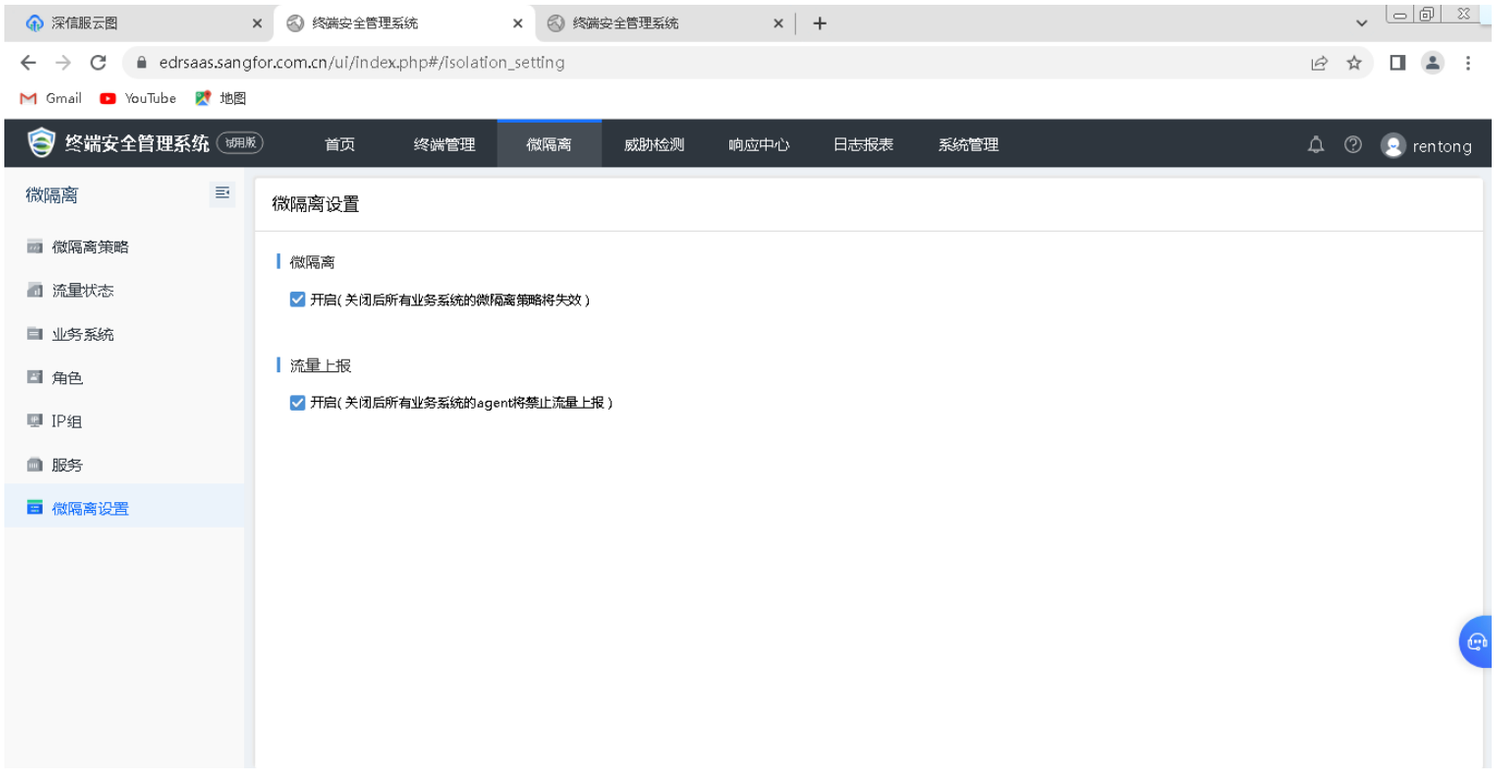

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_vulnerability_check
Gmail
YouTube
地图
威胁检测
终端病毒查杀
终端漏洞查补
终端基线检查
漏洞任务
添加漏洞扫描任务
任务类型
任务状态
扫描已完成
07-07 17:09
手动任务 | 1个终端 | 全部漏洞
任务详情
扫描状态
终端类型
终端状态
所属组织
终端名称/IP/资产使用
序...
扫描状态
终端状态
终端名称
IP地址
资产使...
操作系统
全部漏洞
未修复漏洞
操作
1
扫描完成
在线
admin-PC
192.168.1.101
Windows 7 ...
122
118
漏洞详情
重新扫
admin-PC
处理
刷新
漏洞级别
补丁影响
是否重启
已修复
补丁编号 / 补丁名称
序号
漏洞级别
补丁类型
补丁名称
补丁编号
补丁发布日期
修复状态
1
高危
无
2019-适用于 Windows 7 的 03 服务堆栈更新，...
KB4490628
2019-03-11
已修复
2
高危
无
2018-12 适用于 Windows 7 和 Server 2008 R2 ...
KB4471981
2018-12-07
已修复
3
高危
远程执行代码
2019-07 Security Only Update for .NET Frame...
KB4507411
2019-07-08
已修复
4
高危
远程执行代码
2017-12 适用于基于 x64 的系统的 Windows 7 ...
KB4054521
2017-12-09
已修复

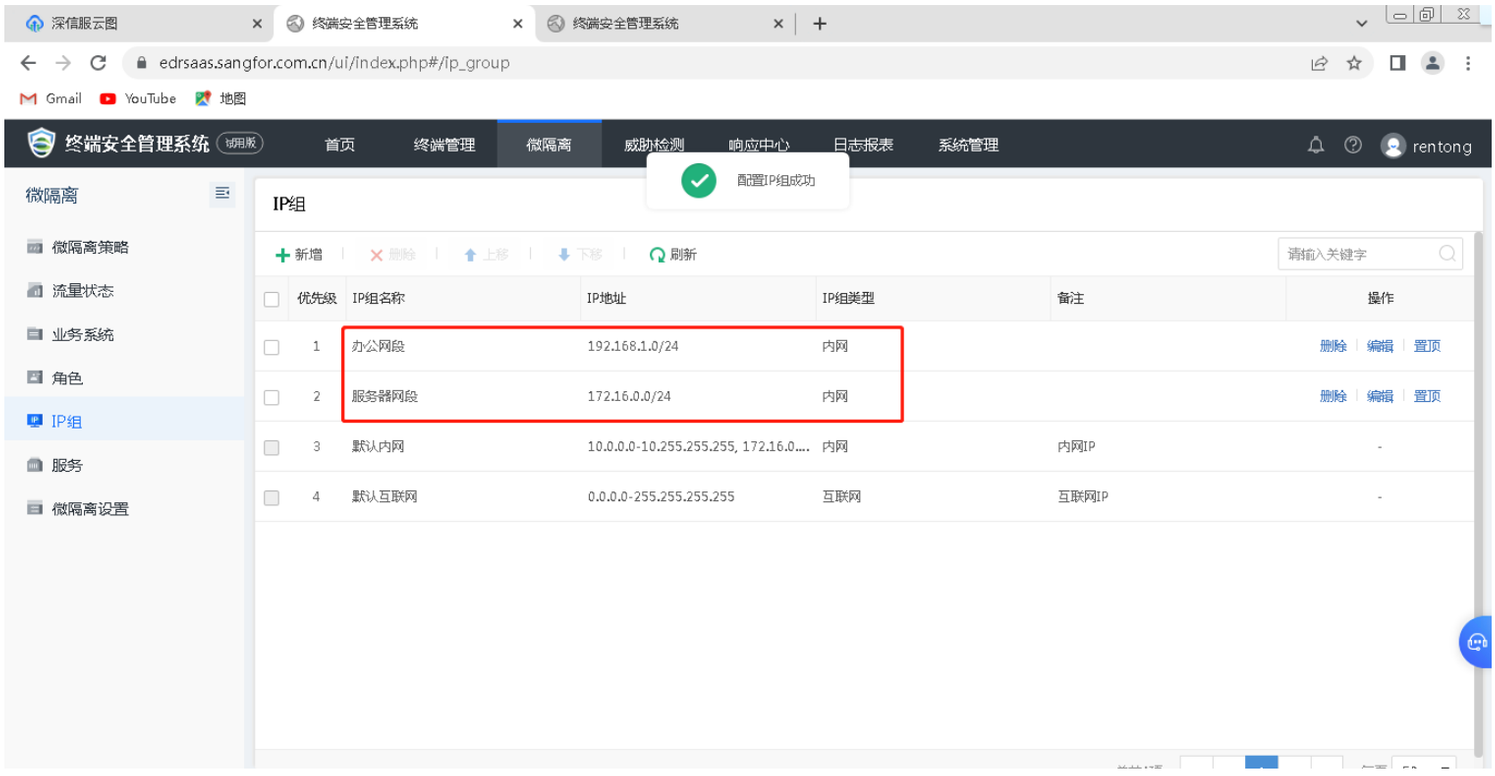

深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_compliance_examination
Gmail
YouTube
地图
终端安全管理系统
试用版
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
威胁检测
终端病毒查杀
终端漏洞查补
终端基线检查
正在进行合规性检查，已发现不合规终端0个...
共体检终端：1个； 体检已用时：6秒
查看完整配置文档
导出
任务状态
终端类型
检查结果
终端名称/IP/资产使用
序号
终端名称
IP地址
所属组织
资产使用人
操作系统
最近扫描时间
任务状态
检查结果
操作
1
admin-PC
192.168.1.101
办公网段
Windows 7 ...
2023-07-07 17:21:...
检查完成
不合规: 30 个
查看详情
2
admin-PC
192.168.1.150
未分组终端
Windows 7 ...
2023-07-06 20:30:...
检查完成
不合规: 28 个
查看详情


深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_compliance_examination
Gmail
YouTube
地图
终端安全管理系统
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
威胁检测
终端病毒查杀
终端漏洞查补
终端基线检查
检查详情
检查完成，发现30项不合规项，共检查51项
结束时间：2023-07-07 17:21:41
身份鉴别合规项检测
1、用户登录身份标识鉴别策略
安全要求：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换
. 密码长度最小值大于等于8个字符
. 密码最短使用期限大于等于2天
. 密码最长使用期限小于等于90天
. 保留密码历史数量大于等于5个
. 用户登录需要用户名和密码
. 空密码账户检测
. 弱密码账户检测
. 密码复杂度项检测
2、登录失败处理策略
安全要求：应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施


深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/docs.php
Gmail
YouTube
地图
2. 在 "账户策略-> 密码策略"
密码复杂性要求：启用
密码长度最小值：>=8 个字符
密码最短使用期限：>2 天
密码最长使用期限：<=90 天
强制密码历史：>=5 个
本地组策略编辑器
文件(F)
操作(A)
查看(V)
本地计算机 策略
计算机配置
软件设置
Windows 设置
域名解析策略
安全设置
帐户策略
密码策略
帐户锁定策略
本地安全策略
文件(F)
操作(A)
查看(V)
帮助(H)
强制密码历史 属性
本地安全设置
说明
强制密码历史
保留密码历史:
5
个记住的密码
确定
取消
应用 (A)
1.1.5 用户登录需要用户名
配置说明：关闭自动登录的账户


深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/endpoint_compliance_examination
Gmail
YouTube
地图
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
本地安全策略
文件(F) 操作(A) 查看(V) 帮助(H)
安全设置
帐户策略
密码策略
帐户锁定策略
本地策略
高级安全 Windows 防火墙
网络列表管理器策略
公钥策略
软件限制策略
应用程序控制策略
IP 安全策略，在 本地计算机
高级审核策略配置
策略
安全设置
密码必须符合复杂性要求 已禁用
密码长度最小值 5 个字符
密码最短使用期限 0 天
密码最长使用期限 42 天
强制密码历史 5 个记住的密码
用可还原的加密来储存密码 已禁用
检查详情
检查完成，发现29项不合规项，共检查51项
结束时间：2023-07-07 17:37:45
身份鉴别合规项检测
1、用户登录身份标识鉴别策略
安全要求：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求
. 密码长度最小值大于等于8个字符
. 密码最短使用期限大于等于2天
. 密码最长使用期限小于等于90天
. 保留密码历史数量大于等于5个
. 用户登录需要用户名和密码
. 空密码账户检测
. 弱密码账户检测
. 密码复杂度项检测
2、登录失败处理策略
安全要求：应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自


深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/isolation_setting
Gmail
YouTube
地图
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
微隔离
微隔离策略
流量状态
业务系统
角色
IP组
服务
微隔离设置
微隔离设置
微隔离
开启(关闭后所有业务系统的微隔离策略将失效)
流量上报
开启(关闭后所有业务系统的agent将禁止流量上报)


深信服云图
终端安全管理系统
edrsaas.sangfor.com.cn/ui/index.php#/ip_group
Gmail
YouTube
地图
首页
终端管理
微隔离
威胁检测
响应中心
日志报表
系统管理
rentong
配置IP组成功
微隔离
微隔离策略
流量状态
业务系统
角色
IP组
服务
微隔离设置
IP组
新增
删除
上移
下移
刷新
请输入关键字
优先级
IP组名称
IP地址
IP组类型
备注
操作
1 办公网段 192.168.1.0/24 内网 删除 编辑 置顶
2 服务器网段 172.16.0.0/24 内网 删除 编辑 置顶
3 默认内网 10.0.0.0-10.255.255.255, 172.16.0.... 内网 内网IP -
4 默认互联网 0.0.0.0-255.255.255.255 互联网 互联网IP -

深信服云图 | 终端安全管理系统

edrsaas.sangfor.com.cn/ui/index.php#/isolation_strategy

Gmail YouTube 地图

终端安全管理系统 试用版 | 首页 | 终端管理 | 微隔离 | 威胁检测 | 响应中心 | 日志报表 | 系统管理 | rentong

微隔离

- 微隔离策略
- 流量状态
- 业务系统
- 角色
- IP组
- 服务
- 微隔离设置

微隔离策略

策略生效开关：

新增 | 删除 | 上移 | 下移 | 启用 | 禁用 | 刷新 | 策略动作 | 匹配次数 | 请输入关键字

优先级	名称	源	目的	服务	动作	匹配...	最近匹配时间	启动...
1	办公_服务器	办公网段	服务器网段	rdp(TCP:3389)	拒绝	0	-	✓

深信服云图 | 终端安全管理系统

edrsaas.sangfor.com.cn/ui/index.php#/isolation_strategy

Gmail YouTube 地图

终端安全管理系统 试用版 | 首页 | 终端管理 | 微隔离 | 威胁检测 | 响应中心 | 日志报表 | 系统管理 | rentong

微隔离

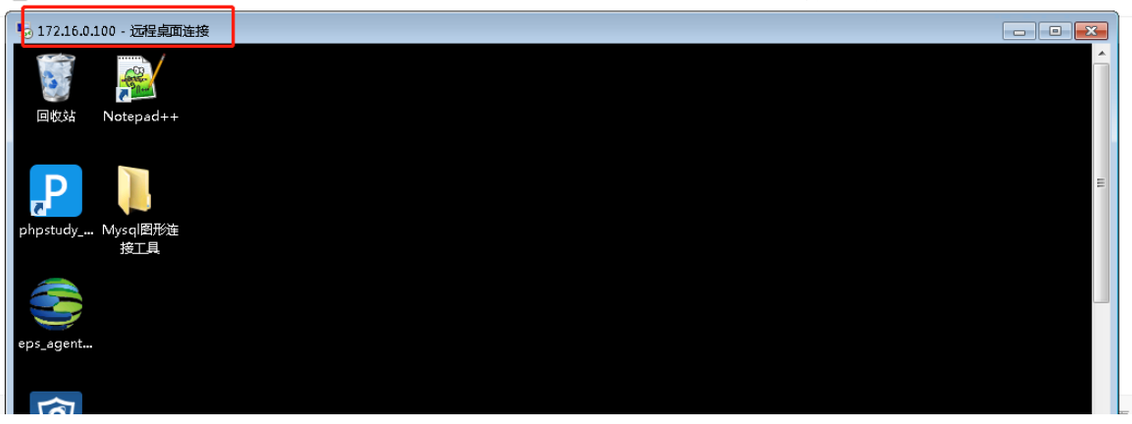
- 微隔离策略
- 流量状态
- 业务系统
- 角色
- IP组
- 服务
- 微隔离设置

微隔离策略

策略生效开关：

新增 | 删除 | 上移 | 下移 | 启用 | 禁用 | 刷新 | 策略动作 | 匹配次数 | 请输入关键字

优先级	名称	源	目的	服务	动作	匹配...	最近匹配时间	启动...
1	办公_服务器	办公网段	服务器网段	rdp(TCP:3389)	拒绝	0	-	⊘



深信服云图 | 终端安全管理系统

edrsaas.sangfor.com.cn/ui/index.php#/isolation_strategy

Gmail YouTube 地图

终端安全管理系统 试用版 | 首页 | 终端管理 | 微隔离 | 威胁检测 | 响应中心 | 日志报表 | 系统管理 | rentong

微隔离

- 微隔离策略
- 流量状态
- 业务系统
- 角色
- IP组
- 服务
- 微隔离设置

微隔离策略

策略生效开关：

新增 | 删除 | 上移 | 策略动作 | 匹配次数 | 请输入关键字

优先级	名称	服务	动作	匹配...	最近匹配时间	启动...
1	办公_服务器	rdp(TCP:3389)	拒绝	0	-	✓