



# 天翼云·终端杀毒

## 用户使用指南

天翼云科技有限公司

## 目录

1. 产品介绍 .....	2
1.1 产品定义 .....	2
1.2 产品优势 .....	3
1.3 功能特性 .....	4
1.4 应用场景 .....	5
2. 计费说明 .....	7
2.1 计费模式 .....	7
2.2 产品购买 .....	8
2.3 产品扩容 .....	8
2.4 续订 .....	8
2.5 退订 .....	8
3. 快速入门 .....	9
3.1 登录管理中心 .....	9
3.2 产品激活 .....	9
3.3 添加主机 .....	10
3.4 部署安全组件 .....	11
3.5 虚拟机/终端配置 .....	12
3.6 客户端安装 .....	17
4. 资产管理 .....	25
4.1 分组管理 .....	25
4.2 安全策略 .....	33

---

4.3	扫描指定目录.....	34
4.4	配置白名单.....	35
4.5	排序/过滤/搜索.....	36
5.	安全配置.....	37
5.1	默认安全配置.....	37
5.2	编辑安全配置.....	39
5.3	其他操作.....	43
6.	用户管理.....	41
7.	最佳实践.....	44
7.1	中国农业银行.....	44
7.2	山东省税务局.....	46
7.3	广安门医院.....	48
8.	常见问题.....	52
8.1	计费类.....	52
8.2	操作类.....	53
8.3	管理类.....	56

## 1. 产品介绍

### 1.1 产品定义

随着虚拟化及云计算的发展,企业环境逐步由物理环境转变为由物理环境、私有云及公有云混合的环境,传统内外网的网络边界消失了;特别是在提供多租户服务的公有云中,不

同组织的网络数据在数据中心内部、甚至是在同一台物理主机上进行交换，传统的安全设备已经无法对其进行检测及防护。云计算环境下需要基于每个终端节点、并且每个节点具有相同安全防护等级的全新的安全防护模型。

天翼云终端杀毒（统一服务器安全管理系统）面向政企用户的以大数据技术为支撑、以可靠服务为保障，能够精确检测已知病毒木马、未知恶意代码，有效防御 APT 攻击，为政企事业单位提供终端病毒、漏洞管控能力。

## 1.2 产品优势

**安全可靠：**多层防护恶意软件和病毒，以确保企业数据安全

**免疫防御：**云查杀系统提供全网实时监控，操作免疫防护，变种病毒爆发预警。

**快速部署：**分分钟部署关键防护，简单、快速、操作简单易上手的安全中控。

**自主可控：**国际一流杀毒软件，帮助政企对网络进行安全管控和安全加固，杜绝安全后门隐患。

**防护新的云端威胁：**防护在同一个数据中心、甚至是在同一主机上的两个虚拟机之间的攻击这种新的威胁，采用传统的网络安全设备无法检测。病毒安全防护，可支持云桌面以及云主机多种场景下的病毒查杀功能，解决传统杀毒软件造成的启动、更新、查杀风暴问题。自动检测虚拟机的系统和应用，并调整入侵检测的规则。使得虚拟机无需安装补丁即可防护利用系统漏洞的新的威胁。未知威胁的防护，通过对海量访问日志数据的分析，找到异常行为、定位未知的安全威胁。

**广泛的云平台的支持及统一管理：**支持主流的虚拟化平台，包括 VMware、Xen、KVM 等。与 OpenStack 的深度集成，支持绝大部分的国产云计算平台。支持虚拟化平台部署和非虚拟化平台部署的统一安全管理。

更低运营成本：管理中心采用中央控管的管理方式，集中的配置每一台虚拟机的安全策略，提供了便捷的管理、更高的灵活性。通过管理中心，可以为每个用户配置不同的安全策略。安全特征库的自动升级，避免用户频繁升级系统补丁而引起的服务中断，降低了管理成本。

## 1.3 功能特性

### 1.3.1 恶意软件防护

支持对系统进行实时防护，定期对虚拟机进行全盘扫描，手动对虚拟机进行磁盘扫描。

手动扫描支持快速、全盘、及指定目录扫描三种安全检测方式。

感染的文件在虚拟机内部隔离。

非虚拟机的用户，无权限读取隔离文件，避免数据泄露问题。

优化安全操作的资源调度，以避免全系统扫描时出现常见的防病毒风暴。

恶意代码特征库的自动更新，防范最新的攻击。

### 1.3.2 漏洞管理

提供对 Windows, Linux 部署系统安全风险的全面洞察，帮助快速和准确地识别、调查、划分优先级和纠正漏洞。

提供关于不断变化的 IT 环境中的所有资产和漏洞的最准确信息，帮助安全团队最大化效率和提高生产力。

支持 IPS 与漏洞扫描结果联动，在未安装实体补丁情况下，提供已知漏洞风险的安全防护。

### 1.3.3 实时扫描

通过强大的 QVM 引擎进行文件安全性的实时分析，并返回杀毒控制中心文件结果。

包含快速扫描项目外的在内的，所有磁盘（当前所有挂载的）目录的文件。

### 1.3.4 强力查杀

自定义查杀强度，自定义方式对终端进行扫描，支持选择启用的引擎类型，配置是否自动处理，是否扫描信任区。

终端恢复：

对终端隔离区指定时间段，指定文件路径或者文件名或者病毒文件进行恢复，恢复到原始路径。

### 1.3.5 定时查杀

对终端进行定时扫描，降低管理员的工作量。

云查杀是终端启用防病毒云查。每次云查杀包括终端提交一批文件 MD5 到云查杀引擎，云查杀引擎鉴定完毕后给予反馈。

## 1.4 应用场景

### 1.4.1 合规防护场景

满足等保 2.0 通用技术要求、云计算扩展技术要求；以满足合规技术要求为基础，提供计算环境的文件、网络、系统三个层面的防护能力。

在安全计算环境下实现多租户管理，解决恶意代码防范、入侵防范、访问控制与隔离、实现可信环境。

### 1.4.2 勒索挖矿防治场景

虚拟化安全的病毒防护能力更适合解决勒索挖矿问题，勒索、挖场景比较复杂，单一杀毒能力是无法全面解决的。

攻击方式：

- 1、暴力破解或者漏洞利用攻陷目标机器；
- 2、下载恶意脚本或者挖矿程序；
- 3、启动攻击模块横向渗透；
- 4、传播复制，扩大攻击范围。

解决思路：

- 1、防暴力破解、虚拟补丁防止被暴破和漏洞利用；
- 2、梳理本地进程和关键目录操作，使用进程管控、完整性监控建立运行时可信状态；
- 3、配置主机防火墙和入侵防御规则，防止横向渗透。

### 1.4.3 勒索病毒防护场景

攻击方式：

- 1.通过 SMB 漏洞上传 WannaCry 勒索病毒等恶意程序；
- 2.蠕虫代码运行后先会连接域名；
- 3.安装病毒服务，释放资源到 C:\WINDOWS 目录下的 tasksche.exe；
- 4.蠕虫病毒服务启动后，会利用 MS17-010 漏洞传播。

防护策略：

- 1.通过资产清点、漏洞管理、安全基线，检查关闭不必要端口、特权账号、避免使用弱口令，应用程序控制阻止拒绝未授权程序的运行，完整性监控避免系统重要目录非法添加和修改；

- 2.流行的勒索病毒落地即查杀；
- 3.通过威胁情报，阻断对勒索域名的非法外联，及时发现可能的失陷主机；
- 4.依靠强大的病毒识别能力，快速准确甄别恶意软件；
- 5.防火墙和入侵防御协同工作，切断横向蔓延路径。

#### 1.4.4 上云、多租场景

1.多租云平台（如 OpenStack、VMWare）支持用无代理或有代理方式部署，管理员可选择更适合的部署方式；

- 2.支持单点登录，云平台的租户账号可以直接对虚拟机进行安全配置；
- 3.支持自定义多租户，每个租户管理员各自管理本租户的虚拟机；
- 4.各租户的策略，日志，告警等信息相互隔离，互不影响，防止用户信息泄露。

#### 1.4.5 混合部署场景

- 1.无代理：安全防护在宿主机或独立虚拟机内完成；
- 2.轻代理：在虚拟机内部、物理服务器上部署轻量化的客户端，实现安全防护工作；
- 3.私有云、容器采用无代理防护，占用极少的系统资源，可以将虚拟机的部署密度提升3倍；
- 4.对于公有云、物理服务器，采用轻代理部署方式，与无代理统一控管；
- 5.灵活的授权方式：CPU 授权或客户端数量授权。

## 2. 计费说明

### 2.1 计费模式



产品规格	收费模式	标准价格 (元/月)
控制中心版	按月计费	40

## 2.2 产品购买

1.用户订购时，在客户端数量栏：请选择需要安装防病毒插件能力的终端数量（云主机或云桌面）总数，主机镜像数量：为制作授权填写需杀毒主机镜像数量，请用户根据自己终端中系统镜像类别填写各类镜像数量，此数量之和应等于购买的客户端数量。

注意：此产品为人工开通开通时间为小时计，请耐心等待。

2.在终端杀毒开通同时，用户需自行在控制中心（可任选节点）开通云主机，开通时请在公共镜像-安全产品中选择终端杀毒，并绑定弹性公网 IP。

3.终端杀毒完成开通后，在控制中心中找到对应的终端杀毒实例获取 license。

## 2.3 产品扩容

用户可在控制台实例处选择扩容按钮，对客户端数量进行扩容。

## 2.4 续订

用户可在控制台实例处选择续订按钮，对实例时长进行续订。

## 2.5 退订

无特殊情况本产品不支持退订。

## 3. 快速入门

### 3.1 登录管理中心

第一步：

用户完成开通后，需自行在控制中心（可任选节点）开通云主机，开通时请在公共镜像-安全产品中选择终端杀毒，并绑定弹性公网 IP（此 ip 作为终端杀毒控制中心的公网登录地址存在）。在控制中心中找到对应的终端杀毒实例获取 license。



第二步：

管理中心页面登录方式为 `https://X.X.X.X:8447`（X.X.X.X 就是第 1 步中为管理中心配置的 IP），其默认用户名密码请在天翼云官网提交工单咨询，首次登录需要修改初始密码，管理员登录到系统后可进入**管理->用户管理** 页面自己添加或删除用户。

### 3.2 产品激活

初次进入管理中心时必须对产品进行激活才可以正常使用。

- 1)登录管理中心，进入**管理 ->系统设置->使用许可** 页面
- 2)在页面中点击 **更新许可文件**，会打开如下图所示的 **使用许可 ->更新许可文件** 对话框，

选择正确的许可文件，点击 **确定**，即可激活。



### 3.3 添加主机

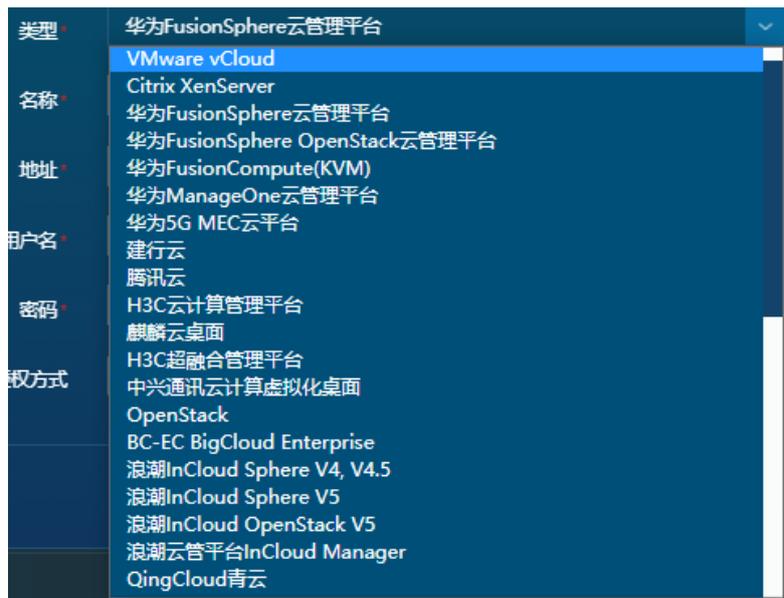
完成产品激活后，需要登录系统，添加主机。

(1) 登录系统后，在资产管理→主机界面下，点击“新增”按钮。



(2) 先选择主机平台，再选择具体类型，各类主流的虚拟化平台类型均支持，注意授权方式的选择。各个平台新增页面需要填入的参数有所不同，详细请参考各虚拟化平台对应的安装部署手册。



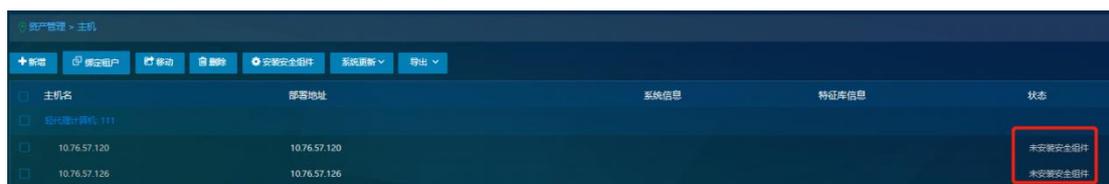


(3) 同样支持非虚拟化平台主机的添加。



### 3.4 部署安全组件

(1) 完成主机池添加后，查看资产管理→主机界面，已添加的主机，状态栏为“未安装安全组件”。



(2) 勾选具体的主机，点击“安装安全组件”，弹出下图界面，按需选择和填写对应参数即可。

安装安全组件

选定的主机	cvknode
操作系统	Linux
IP地址	10.76.57.119
主机用户名	
主机密码	管理中心不保存输入的密码
获取管理员权限	root或sudo免密
SSH端口	22
是否重启	<input checked="" type="checkbox"/> 是 <input type="checkbox"/> 否
安全模块	全功能模块

提示 主机各模块将自动升级到最新补丁，不支持撤销。

(3) 安装完成后，会显示“安装成功”，继续等待 1-2 分钟后，会刷新出主机的系统信息、特征库信息，主机状态为“在线”。



(4) 无代理主机（即虚拟化平台）还需为平台所管理的具体虚拟机安装消息中心，具体参照可参见对应平台的安装部署手册。

## 3.5 虚拟机/终端配置

### 执行防恶意软件扫描

查看资产管理→虚拟机/终端界面，查看各虚拟机的防恶意软件状态，在正确完成部署后，应为绿色的盾牌标记。

## 防恶意软件状态

 扫描成功  
2022-03-28 19:25

 扫描成功  
2022-03-28 20:01

### 执行手动扫描

在资产管理→虚拟机/终端界面下，勾选具体的虚拟机终端，点击安全操作，选择具体的手动扫描方式，如快速扫描等。



下发扫描操作后，防恶意软件状态会由“等待扫描”开始，然后显示具体扫描进度，最终显示扫描成功。



## 执行定期扫描

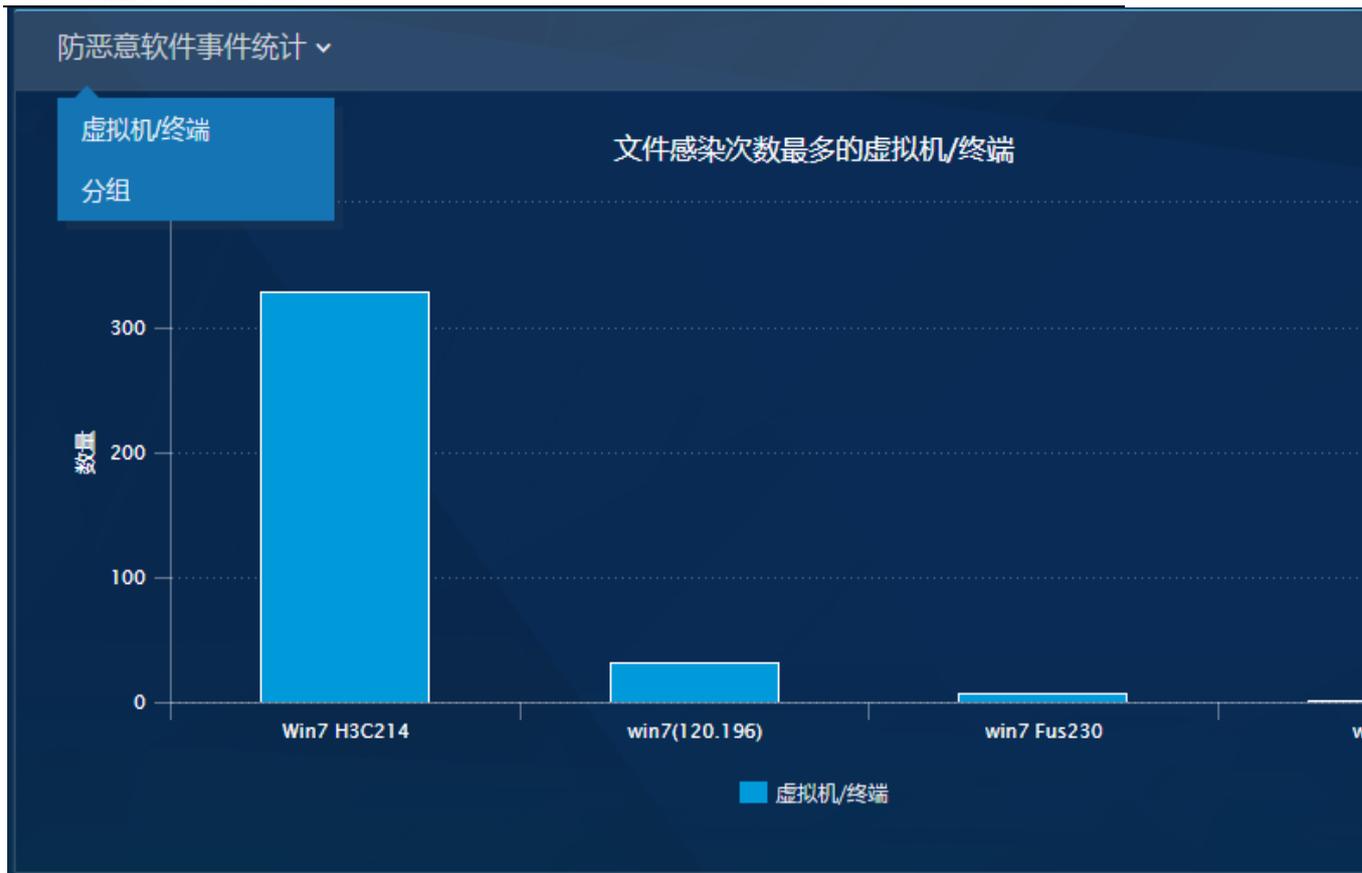
在安全策略→安全配置下，点击“防恶意软件”配置项的“手动/定期扫描”选项卡，配置具体的定期扫描参数，支持“每天”、“每月”、“每周”的定期频率，设置完成后，点击

保存，并将该安全策略应用于具体虚拟机。



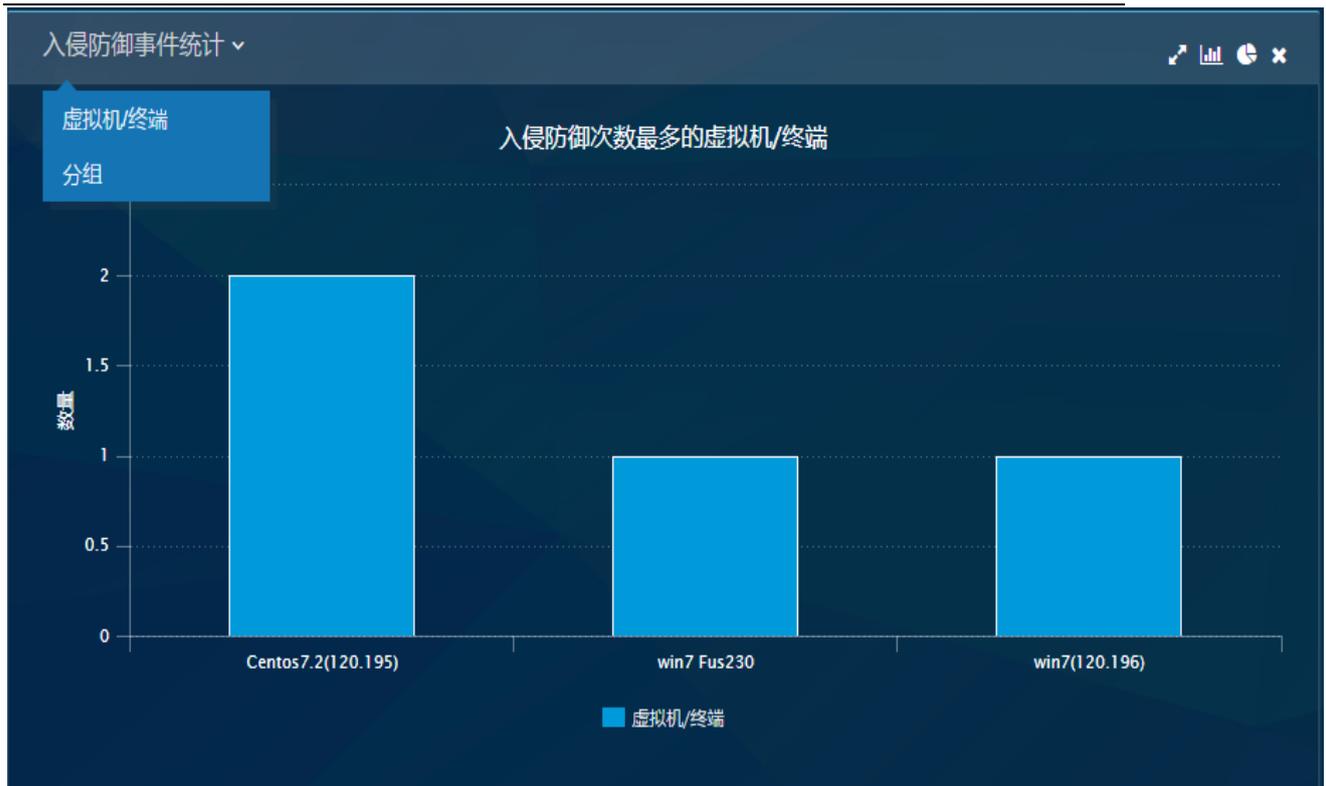
## 防恶意软件事件统计

默认以柱状图的形式展现文件感染次数排名前 5 的虚拟机/终端，排序从高到低。左上角可选择展现排名前 5 的分组，右上角可选择以饼图的形式展现。鼠标悬停至柱状图上，能显示具体的数值，鼠标点击柱状图，会自动跳转至 **分析-防恶意软件** 页面。



## 入侵防御事件统计

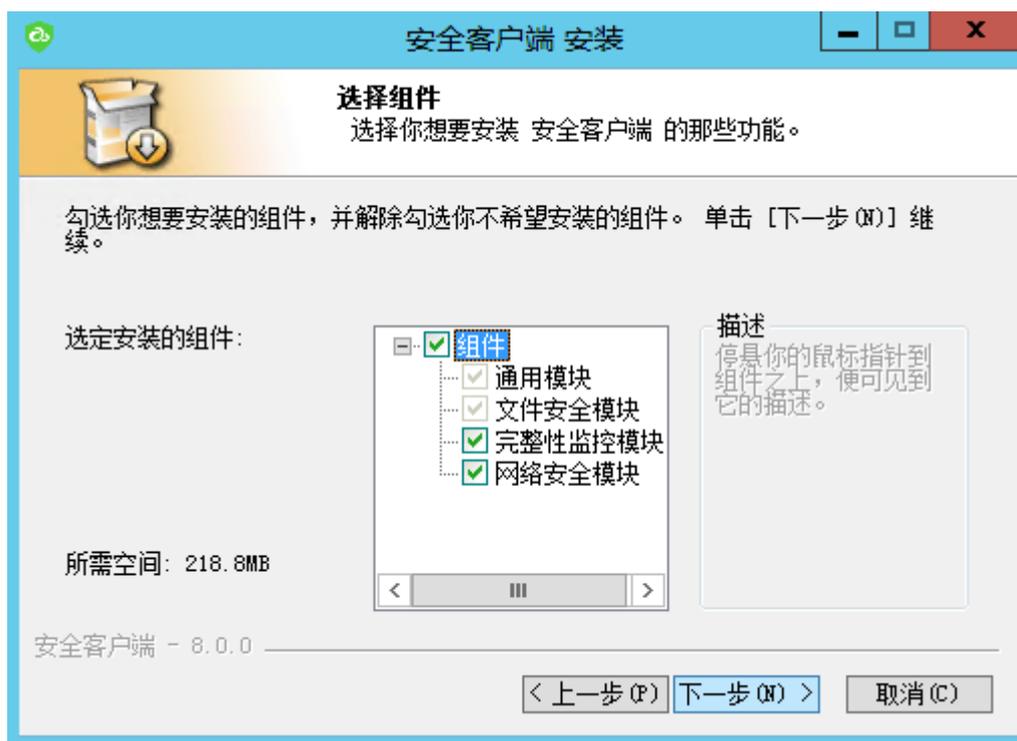
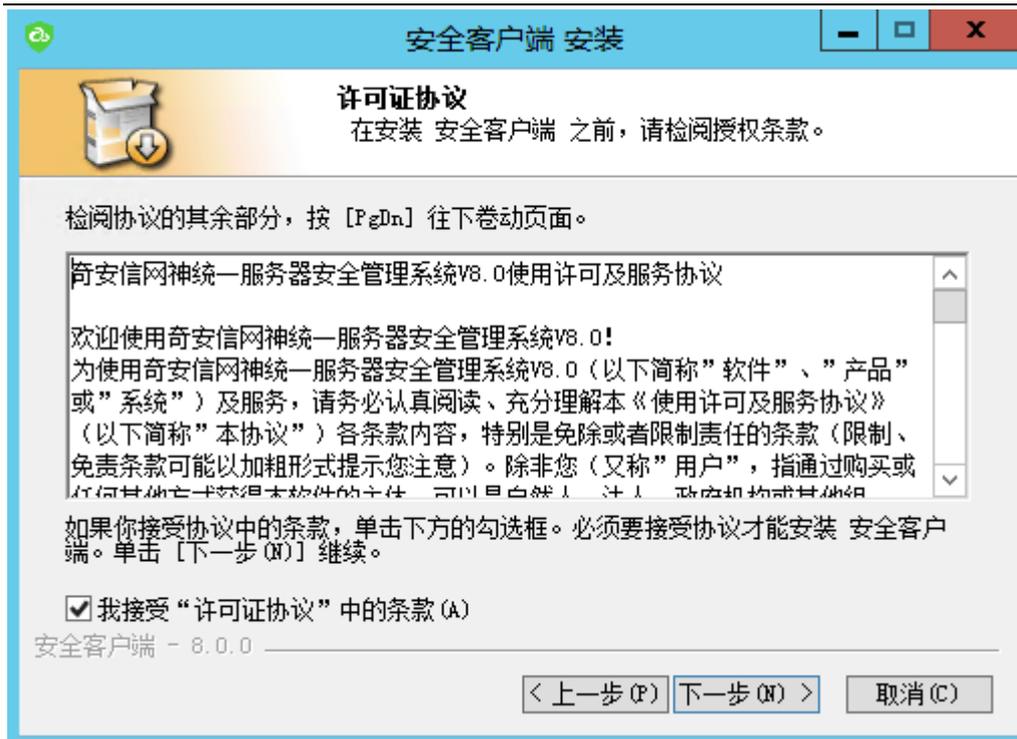
以柱状图的形式展现，指定时间范围和分组内入侵防御事件发生数量排名前 5 的虚拟机。左上角可选择展现排名前 5 的分组，右上角可选择以饼图的形式展现。鼠标悬停至柱状图上，能显示具体的数值，鼠标点击柱状图，会自动跳转至 **分析-入侵防御** 页面。



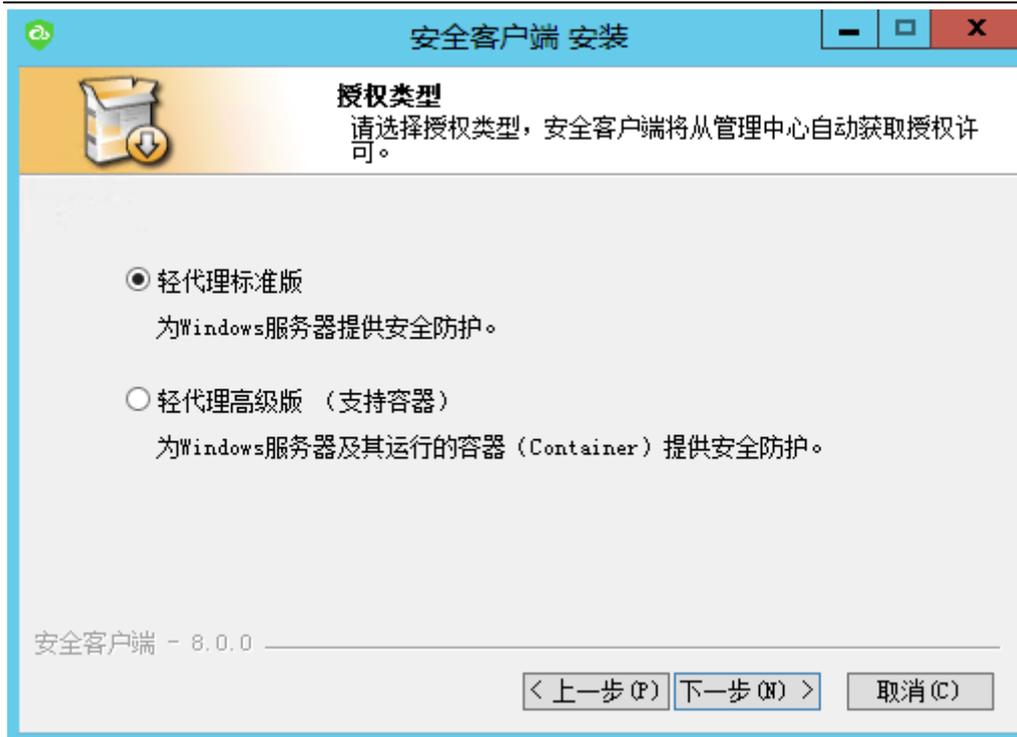
## 3.6 客户端安装

### 3.6.1 Windows 端

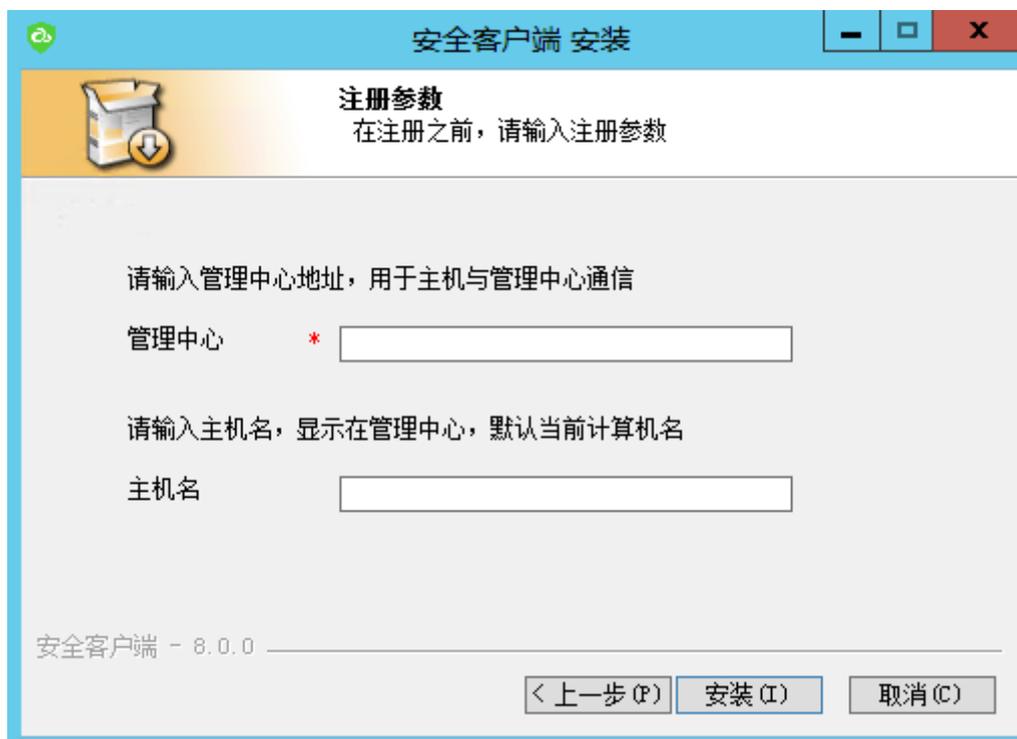
1. 在浏览器上通过访问 <http://IP:8080/agent/ics-agent.exe>，下载安装文件。（IP 是管理中心的 IP）
2. 执行安装文件，安装过程中可以选择是否安装网络模块和完整性监控模块。



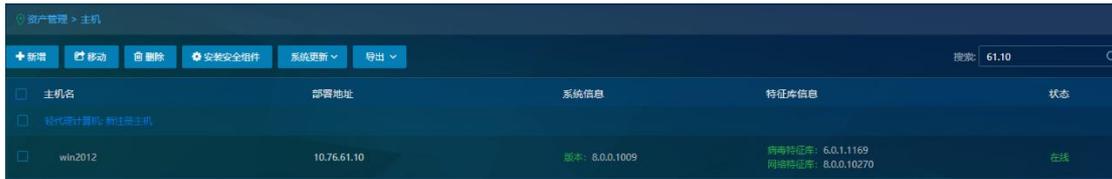
下一步之后根据需求选择轻代理标准版、轻代理高级版（支持容器）。



输入管理中心地址（必选）、主机名（可选），点击安装。



3. 注册成功后，管理中心能够看到该主机，主机状态显示为“已连接”，新注册的主机会被默认添加至名称为“新注册主机”的主机池中。



4. 管理中心 “资产管理” -> “虚拟机/终端” 页面能够看到该机器，其实时防护状态正确



### 3.6.2 Linux 端

#### 方法 1：通过管理中心一键部署

- 1) 进入 资产管理 ->主机 页面
- 2) 在页面中点击 新增 按钮，会弹出 新增主机池 对话框，平台选择 “非虚拟化平台”



3) 在对话框中输入主机池名称、选择添加方式、输入计算机名、IP 地址，点击确定即可。

参数说明：

名称：主机将要添加至的主机池名称，手动输入会新建一个以输入的名称命名的主机池，也可以选择管理中心现有的主机池。

添加方式：主机的添加方式分为单台计算机和网段范围内的多台计算机，默认为单台计算机，即一次添加一台主机；如果选择网段范围内的多台计算机，即一次性添加多台主机，如下图所示需要填写起始地址和结束地址。



新增主机池

平台	非虚拟化平台
名称	创建新的主机池，或加入已存在的主机池
添加方式	网段范围内的多台计算机
起始地址	网段的起始地址
结束地址	网段的结束地址

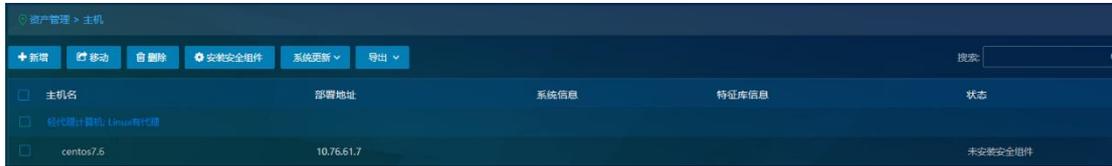
一次添加网段最多包含256个IP地址，系统将在后台添加指定网段范围内的计算机

确定 取消

计算机名：如果填写的是主机的域名，系统会根据域名去添加主机，不需要再输入计算机IP；如果填写的是主机的别名，则需要再输入正确的计算机IP。

计算机IP：主机的IP地址。

4) 添加成功后，主机状态为“未安装安全组件”



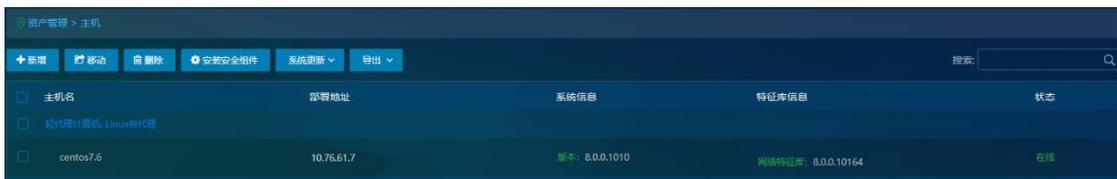
5) 选择刚才添加的主机，点击“安装安全组件”按钮

6) 在弹出的对话框中，输入主机用户名、密码（即 ssh 的用户名和密码），选择许可类型为服务器，点击确定，系统开始在主机上安装安全组件。



7) 安装安全组件过程中的状态变化由未安装安全组件->正在安装->安装成功->连接中断->已连接，整个过程大约需要 2 分钟。

8) 部署成功后，页面中会显示该主机池/资源池的服务器类型、部署地址，主机池名称、该主机池/资源池下的所有主机、系统版本信息、文件和网络特征库信息及当前的连接状态，如下图所示。



9) 主机注册成功后，管理中心“资产管理”->“虚拟机/终端”页面能够看到该机器，其实时防护状态正确。



10) 如果安装失败，主机状态会显示为“安装失败”，可点击“安装失败”字样查看失败原因。



## 方法 2：通过脚本部署

(1) 使用 ssh 工具连接主机

(2) 有主机端使用命令 `wget http://X.X.X.X:8080/agent/ics_agent.py` 下载安装脚本

(3) 执行安装脚本，在如下图所示的交互式视图中输入相应的参数

参数说明：

Ip address of management center: 管理中心 IP

host name : 主机名，如果不输入则会使用默认值

install network module? yes/no [Default yes]: 选择是否安装网络模块，默认为 yes

Authorization type : 授权类型，标准版 (standard) 、高级版 (container) ，默认为标准版

(4) 参数输入完成后，主机将从管理中心下载安装包，安装并注册

(5) 注册成功后，管理中心能够看到该机器，主机状态显示为“已连接”，使用脚本部署的主机会被默认添加至名称为“新注册主机”的主机池中。



虚拟机/终端	IP地址	部署方式	版本信息	安全配置	主机池/项目	主机	分组	特征库状态	防恶意软件状态
aaa	10.76.54.23	轻代理 (在线)	8.0.0.1010	Linux安全配置	ss	10.76.54.23	默认分组	最新	

(6) “资产管理” -> “虚拟机/终端” 页面也能够看到该机器，其实时防护状态正确



## 4. 资产管理

### 4.1 分组管理

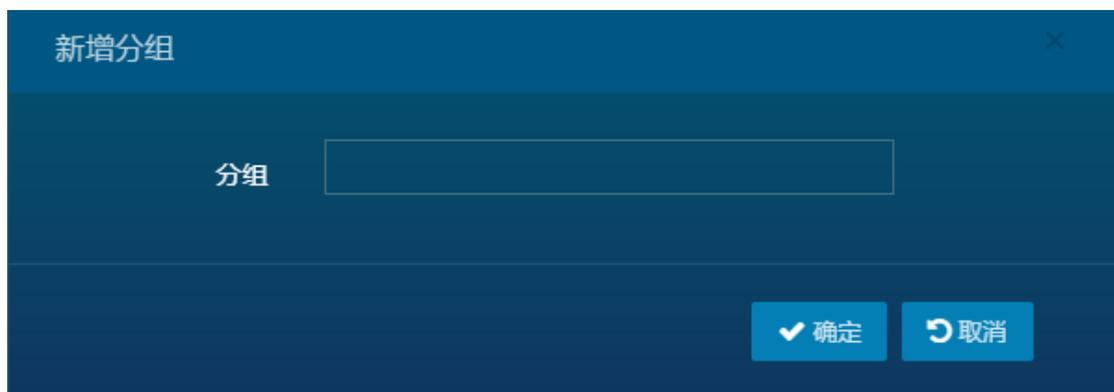
将被管理的计算机进行分组，方便后期管理。可以针对分组定义匹配规则，也可以指定分组来查看实时监控，日志分析，生成报表等。

在多租模式的“所有项目”视图下，不显示分组信息。如果在多租模式进行分组管理，请先切换到对应的项目视图。

默认分组：系统默认创建，虚拟机如果没有匹配上分组规则或没有被指定分组，则全部属于默认分组。

- 新增

- 1) 点击 资产管理->虚拟机/终端理->分组管理->新增
- 2) 在打开的“新增分组”对话框中输入分组名称，点击确定，左侧的分组列表中就能显示刚才创建的分组。



- 修改

- 1) 在左侧分组列表选择要修改名称的分组
- 2) 点击 分组管理->修改
- 3) 在打开的“修改分组”对话框中输入分组名称，点击确定即可

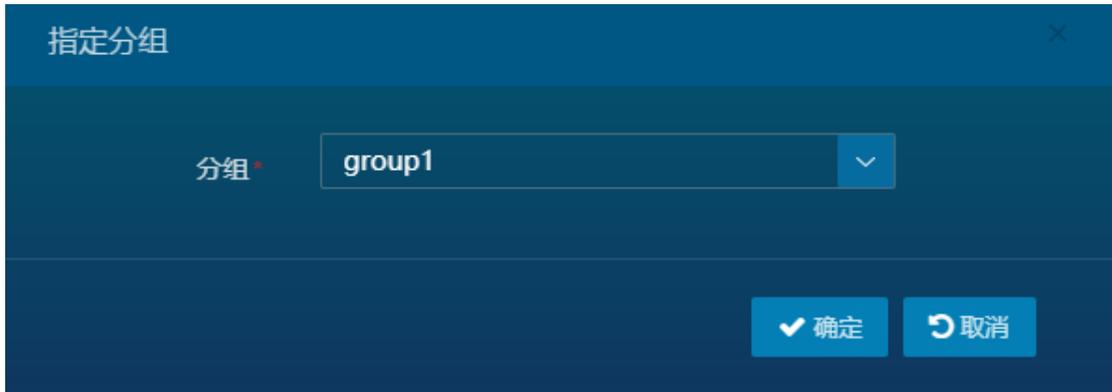


- 删除

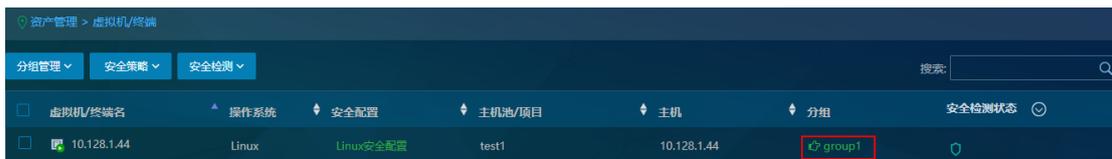
- 1) 在左侧分组列表选择要删除的分组
- 2) 点击 分组管理->删除
- 3) 在打开的“删除确认”对话框中点击确定即可

#### 指定分组

- 1) 选择要指定分组的虚拟机/终端
- 2) 点击 分组管理->指定分组
- 3) 在打开的“指定分组”对话框的分组列表中选择某个分组，点击确定即可



虚拟机的分组栏中有小手图标，表示是手动指定的分组



- 取消指定

- 1) 选择要取消指定分组的虚拟机/终端

- 2) 点击 分组管理-> 取消指定

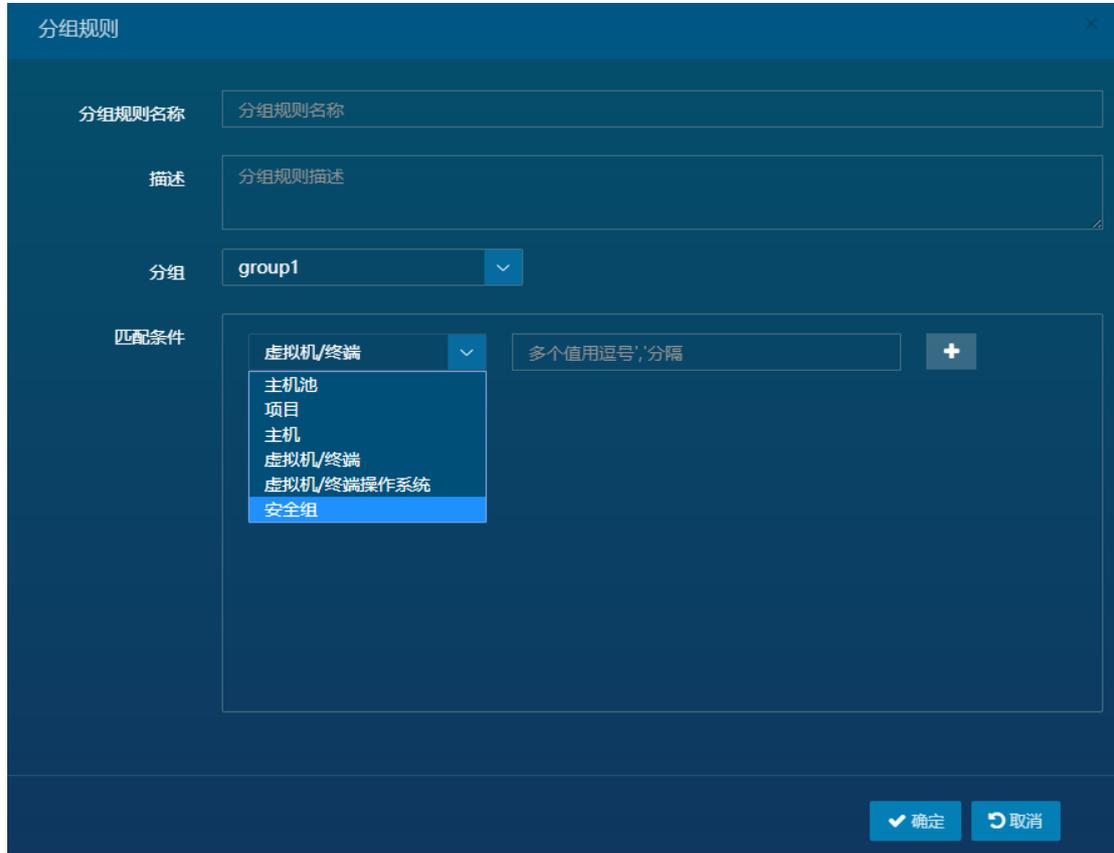
- 分组规则

- 新增

- 1) 在虚拟机/终端页面，点击 分组管理->分组规则

- 2) 在分组规则页面，点击 规则管理->新增

3) 在打开的“分组规则”对话框中输入分组规则的名称、描述、选择分组、配置匹配条件，点击确定即可



分组规则的匹配条件至少要包括下面的一项：

主机池：虚拟机所在主机池的名称，可以配置多个，多个主机池名称之间用英文的逗号 ‘,’， ‘分隔。此条件为单租户模式下使用。

项目：虚拟机所在租户的名称，可以配置多个，多个项目名称之间用英文的逗号 ‘,’， ‘分隔。为多租户模式系统管理员视图下使用。多租户模式普通租户视图无法使用项目作为筛选条件。

主机：虚拟机所在主机的名称，可以配置多个，多个主机名称之间用英文的逗号 ‘,’， ‘分隔。

虚拟机/终端：虚拟机/终端名称，即资产管理-虚拟机/终端页面 虚拟机列表中显示的虚拟机名，可以配置多个，多个虚拟机名称之间用英文的逗号 ‘,’ 分隔。

虚拟机/终端操作系统：操作系统目前支持 Windows 和 Linux，由用户创建虚拟机指定。

安全组：openstack 虚拟机或 VMware NSX 环境中虚拟机所属的安全组

通过点击  来添加匹配条件，点击  来删除匹配条件。最多可添加 6 个匹配条件，且不能是同类型的匹配条件。

多个匹配条件之间是 ‘与’ 的关系，即要满足所有匹配条件，才算匹配成功。

同一个匹配条件之间的多个值是 ‘或’ 的关系，只要匹配上其中某个值，即算匹配成功。

- 删除

- 1) 选择要删除的分组规则
- 2) 点击 规则管理->删除
- 3) 在打开的“删除确认”对话框中点击确定即可

- 调整优先级

分组规则按从上至下的顺序进行匹配，调整分组规则优先级可以改分组规则的匹配结果。

- 1) 选择要调整优先级的分组规则

2) 点击 调整优先级-置顶/上移/下移/置底

- 返回虚拟机/终端列表

在分组规则页面，点击 “返回虚拟机/终端列表” 按钮即可返回虚拟机/终端页面

主机添加成功后，虚拟机页面会显示主机中所有虚拟机信息。包括虚拟机名称、虚拟机状态、虚拟机操作系统、安全配置、所属主机池或项目、所属主机、实时防护状态和安全检测状态。



虚拟机/终端名	操作系统	安全配置	主机池/项目	主机	分组	安全检测状态
10.128.1.44	Linux	Linux安全配置	test	10.128.1.44	默认分组	🟢
CentOS	Linux	Linux安全配置	DataCenter	10.128.1.220	默认分组	🟢
CentOS 6.7	Linux	Linux安全配置			默认分组	🟢
NSVM-10.128.1.220	Linux	Linux安全配置	DataCenter	10.128.1.220	默认分组	🟢
win7	Windows	Windows Security Policy	E0301	E0301	默认分组	🟢
Windows 7	Windows	Windows Security Policy	DataCenter	10.128.1.220	默认分组	🟢
Windows 7	Windows	Windows Security Policy			默认分组	🟢
Windows Server 2008 R2	Windows	Windows Security Policy			默认分组	🟢

主机添加成功后，虚拟机页面会显示主机中所有虚拟机信息。包括虚拟机名称、虚拟机状态、虚拟机操作系统、安全配置、所属主机池或项目、所属主机、实时防护状态和安全检测状态。



虚拟机/终端名	操作系统	安全配置	主机池/项目	主机	分组	安全检测状态
10.128.1.44	Linux	Linux安全配置	test	10.128.1.44	默认分组	
CentOS	Linux	Linux安全配置	DataCenter	10.128.1.220	默认分组	
CentOS 6.7	Linux	Linux安全配置			默认分组	
NSVM-10.128.1.220	Linux	Linux安全配置	DataCenter	10.128.1.220	默认分组	
win7	Windows	Windows Security Policy	E0301	E0301	默认分组	
Windows 7	Windows	Windows Security Policy	DataCenter	10.128.1.220	默认分组	
Windows 7	Windows	Windows Security Policy			默认分组	
Windows Server 2008 R2	Windows	Windows Security Policy			默认分组	

以下是虚拟机列表中虚拟机状态和实时防护状态说明：

虚拟机状态		虚拟机正在运行
		虚拟机被挂起
		虚拟机被停止
实时防护状态		实时防护开启
		实时防护关闭
		虚拟机/终端未运行
		安全防护功能未开通
		VMware安全虚拟机
		管理中心
		此图标表示3种状态
		1.如果对应的虚拟机是VMware虚拟化平台中的Linux虚拟机，则此图标表示“虚拟机/终端未安装NSX File Introspection/vShield驱动程序或代理安全组件，请点击并根据提示进行安装” 2.如果对应的虚拟机是VMware虚拟化平台中的Windows虚拟机，则此图标表示“NSX/vShield Manager和ESXi主机时间不同步或虚拟机/终端可能没有安装NSX File Introspection/vShield驱动程序” 3.如果对应的虚拟机是非VMware虚拟化平台中的虚拟机，则表示“虚拟机没有安装消息中心，请点击下载“消息中心”并为虚拟机安装”

虚拟机处于挂起或停止状态时，管理中心是无法获取其实时防护状态的，所以会显示为空



虚拟机/终端名	操作系统	安全配置	主机池/项目	主机	分组	安全检测状态
10.128.1.44	Linux	Linux安全配置	test	10.128.1.44	默认分组	
CentOS	Linux	Linux安全配置	DataCenter	10.128.1.220	默认分组	
CentOS 6.7	Linux	Linux安全配置			默认分组	

## 4.2 安全策略

### 1) 默认安全配置

系统中有两种默认安全配置，即 Linux 安全配置、Windows 安全配置。系统会根据虚拟机的操作系统为其自动分配对应的安全配置。



虚拟机/终端名	操作系统	安全配置	主机池/项目	主机	分组	安全检测状态
centos 6.7	Linux	Linux安全配置	Datacenter	10.128.1.248	VMware	🔴
CentOS 6.7	Linux	Linux安全配置			默认分组	
NSVM-10.128.1.248	Linux	Linux安全配置	Datacenter	10.128.1.248	VMware	🟢
win7	Windows	Windows安全配置			默认分组	
win7	Windows	Windows安全配置	Datacenter	10.128.1.248	VMware	🔴
win7	Windows	Windows安全配置	E0301	E0301	H3C	🟢
Windows 10 (64-bit) (1)	Windows	Windows安全配置			默认分组	
Windows 7 (32-bit) (1)	Windows	Windows安全配置			默认分组	

### 2) 指定安全配置

在虚拟机页面，管理员也可以手动为虚拟机指定安全配置。手动指定的安全配置会优先于自动匹配安全配置。

- 在虚拟机列表选中一个或者多个虚拟机
- 点击“安全策略 > 指定安全配置”，在弹出页面选择安全配置，然后确认。
- 这些虚拟机将使用指定的安全配置，虚拟机列表的“安全配置”前有一个小图标 表示其由手动指定。如下图所示



虚拟机/终端名	操作系统	安全配置	主机池/项目	主机	分组	安全检测状态
centos 6.7	Linux	test	Datacenter	10.128.1.248	VMware	🛑
CentOS 6.7	Linux	test			默认分组	
NSVM-10.128.1.248	Linux	Linux安全配置	Datacenter	10.128.1.248	VMware	🛡️
win7	Windows	Windows安全配置			默认分组	
win7	Windows	Windows安全配置	Datacenter	10.128.1.248	VMware	🛑

### 3) 取消指定

手动指定安全配置后，也可以取消指定。

- 在虚拟机列表选中一个或者多个虚拟机
- 点击“安全策略 > 取消指定”即可恢复到默认的安全配置

### 4) 恢复默认安全功能

- 在虚拟机列表中选中一个或多个虚拟机
- 点击“安全策略 > 恢复默认安全功能”，虚拟机的安全功能会恢复到初始状态。

## 4.3 扫描指定目录

进入管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态关闭，恶意软件处理选择删除/隔离；在虚拟机页面，选择对应的虚拟机，点击 安全操作->快速扫描。



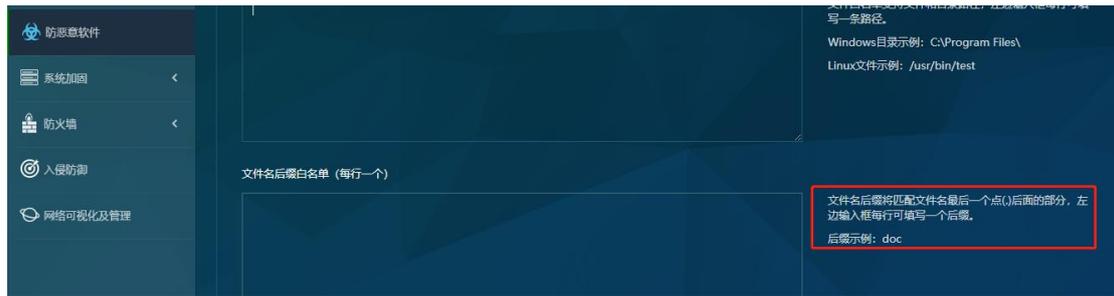
## 4.4 配置白名单

### 目录文件白名单

进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理配置为删除，目录/文件白名单配置。

### 文件后缀名白名单

进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理配置为删除，文件后缀名白名单配置。



## 4.5 排序/过滤/搜索

### 1) 虚拟机列表排序

点击虚拟机列表头中右侧的 ，可以按照虚拟机/终端 名、操作系统、安全配置、主机池/项目、主机对虚拟机列表进行排序，方便管理员查看。



### 2) 虚拟机过滤

虚拟机/终端页面可以根据实时防护状态来对虚拟机进行过滤，方便用户查看。



### 3) 搜索虚拟机

管理员可以按照虚拟机名、操作系统、安全配置和主机对虚拟机进行搜索。支持模糊匹配、不区分大小写。

## 5. 安全配置

### 5.1 默认安全配置

安全配置是防护系统针对每台虚拟机的所有安全设置的集合，包括防恶意软件设置，定义好安全配置后，可以将它应用到多台虚拟机。可以定义规则自动匹配，也可以手动为虚拟机指定安全配置。

系统默认安全配置：系统中有两种默认安全配置，即 Linux 安全配置和 Windows 安全配置。当主机添加成功后，管理中心会根据主机中虚拟机的操作系统，为其自动匹配默认的安全配置。



虚拟机/终端名	操作系统	安全配置	主机池/项目	主机	分组	安全检测状态
centos 6.7	Linux	Linux安全配置	Datacenter	10.128.1.248	VMware	🛡️
CentOS 6.7	Linux	Linux安全配置			默认分组	
NSVM-10.128.1.248	Linux	Linux安全配置	Datacenter	10.128.1.248	VMware	🛡️
win7	Windows	Windows安全配置			默认分组	
win7	Windows	Windows安全配置	Datacenter	10.128.1.248	VMware	🛡️
win7	Windows	Windows安全配置	E0301	E0301	H3C	🛡️
Windows 10 (64-bit) (1)	Windows	Windows安全配置			默认分组	
Windows 7 (32-bit) (1)	Windows	Windows安全配置			默认分组	

## 1) 指定安全配置

在虚拟机页面，管理员也可以手动为虚拟机指定安全配置。手动指定的安全配置会优先于自动匹配安全配置。

d) 在虚拟机列表选中一个或者多个虚拟机

e) 点击“安全策略 > 指定安全配置”，在弹出页面选择安全配置，然后确认。

f) 这些虚拟机将使用指定的安全配置，虚拟机列表的“安全配置”前有一个小图标 表示其由手动指定。如下图所示



虚拟机/终端名	操作系统	安全配置	主机池/项目	主机	分组	安全检测状态
centos 6.7	Linux	Linux安全配置	Datacenter	10.128.1.248	VMware	🛡️
CentOS 6.7	Linux	Linux安全配置			默认分组	
NSVM-10.128.1.248	Linux	Linux安全配置	Datacenter	10.128.1.248	VMware	🛡️
win7	Windows	Windows安全配置	Datacenter	10.128.1.248	VMware	🛡️
win7	Windows	Windows安全配置			默认分组	
Windows 10 (64-bit) (1)	Windows	Windows安全配置			默认分组	
Windows 7 (32-bit) (1)	Windows	Windows安全配置			默认分组	

## 2) 取消指定

手动指定安全配置后，也可以取消指定。

c) 在虚拟机列表选中一个或者多个虚拟机

d) 点击“安全策略 >取消指定”即可恢复到默认的安全配置

## 5.2 编辑安全配置

编辑安全配置页面包括 7 个选项卡，分别在每个选项卡内进行相应的设置。

- 通用设置

名字： 规则名称，支持中文名，是必选项。

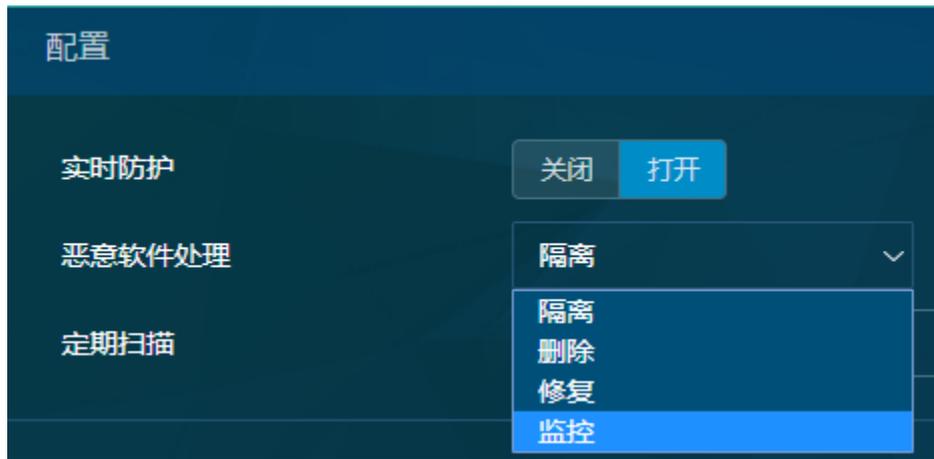
描述： 可选项。

- 防恶意软件

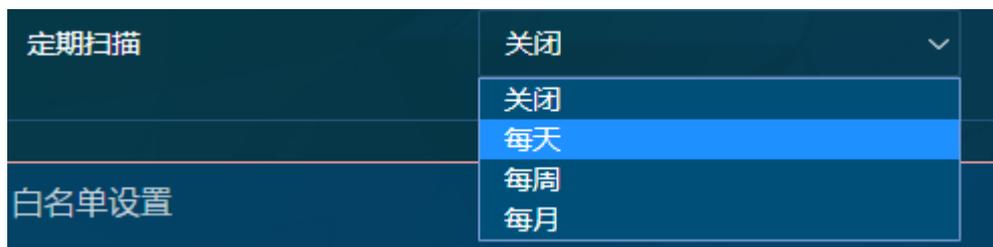
a) 实时防护： 如果打开实时防护  ，应用该安全配置的虚拟机将受到实时的防恶意软件防护，虚拟机列表中的实时防护状态会变为

如果关闭实时防护  ，应用该安全配置的虚拟机不会受到实时的防恶意软件防护，虚拟机列表中的实时防护状态会变为 ，默认是打开状态。

b) 恶意软件处理：如果在虚拟机中检测到病毒，系统提供了以下 4 种方式对病毒进行处理



c) 定期扫描：可以选择定期对虚拟机进行全盘扫描。时间可以是每天，每周或者每月的具体某个时间点，默认是关闭状态。



注：只有虚拟机为开启状态才会进行定期扫描。

例如，配置定期扫描时间为每天 15:00，则如果有虚拟机在 15:00 到 16:00 这段时间内从挂起或关闭状态变成开启状态，虚拟机起来后也会进行定期扫描。

d) 文件白名单：将文件夹或者文件路径加入白名单，安全模块将不对这些文件进行扫描和检测。匹配时采用模糊算法，如果要扫描的文件全路径中包含有白名单中的任何一项，则被算作匹配。编辑框中每行填入一个白名单路径。

例如：“C:\Program Files\”将匹配文件夹及其下面的所有文件和文件夹。

e) 文件名后缀白名单：如果文件名的后缀匹配这个白名单中任何一项，将跳过扫描和检测。可以配置多个文件后缀，每个文件后缀之间用换行符进行分隔。

f) 仅扫描指定目录设置：如果选中“仅扫描下列目录”复选框，可以把扫描目录限制到指定的目录范围。同时可以把指定目录范围应用到手动全盘扫描，实时扫描和定期扫描中的一项或者多项。

g) 仅扫描包含指定后缀名的文件：如果选中“仅扫描包含下列后缀名的文件”复选框，可以限定只扫描特定文件类型。同时可以把指定文件类型应用到手动全盘扫描，实时扫描和定期扫描中的一项或者多项。

## 5.3 用户管理

- **添加用户**

新增用户：在用户管理标签页点击“新增”按钮，在打开的“用户管理”对话框中填写各个选项，其中用户名和密码是必填项，根据需要选择合适的“角色”，点击确定按钮。

### 用户管理 ✕

用户名	<input type="text"/>
密码	<input type="text" value="密码必须至少包含八个字符且需要采用以下四"/>
确认密码	<input type="text" value="重复上面的密码"/>
角色	<input type="text" value="admin"/> <span>▼</span>
邮箱地址	<input type="text"/>
描述	<input type="text"/>

**密码复杂度**：新增用户时有密码复杂度要求，要求密码必须至少包含六个字符且需要采用以下四类字符中的三类：英文大写字符（A-Z）、英文小写字符（a-z）、10 个基本数字（0-9）和非字母字符（!、\$、#、% 等）。

**编辑用户**：如果想要修改用户的相关参数，在用户列表中点击需要修改参数的用户名，在打开的‘用户管理’对话框中修改即可。

**删除用户**：选中需要删除的用户，点击“删除”按钮。

**搜索用户**：可以根据用户名、邮箱地址和描述进行搜索，支持模糊搜索，不区分大小写。

**同一账号多次登录管理**：

- a) 多人同时用相同账号登陆，提醒用户其他地方有人用相同账号登陆（包括 先登录用户，和后登录用户）
- b) 用户可以查看当前使用相同账号登录会话的信息，包括登录 IP，登录在线时间
- c) 用户可以踢出已登录会话，让其强制退出登录



#### ● 角色管理

新增角色： 在角色管理标签页点击“新增”按钮，在打开的“角色管理”对话框中填写角色名，并根据需要选择合适的权限，点击确定按钮。

编辑角色： 如果想要修改角色的相关权限，在角色列表中点击需要修改的角色名，在打开的“角色管理”对话框中修改即可

删除角色： 选中需要删除的角色，点击“删除”按钮。 不能直接删除已经被用户关联的角色，必须先删除所有关联用户，然后再删除该角色。

## 5.4 其他操作

#### ● 搜索安全配置

可以根据安全配置的名称/描述/保护的机器来搜索安全配置，支持模糊搜索。



## ● 复制、删除安全配置

在安全配置列表中选择需要复制或删除的安全配置，点击复制/删除按钮即可。



## 6. 最佳实践

### 6.1 中国农业银行

#### 6.1.1 项目背景介绍

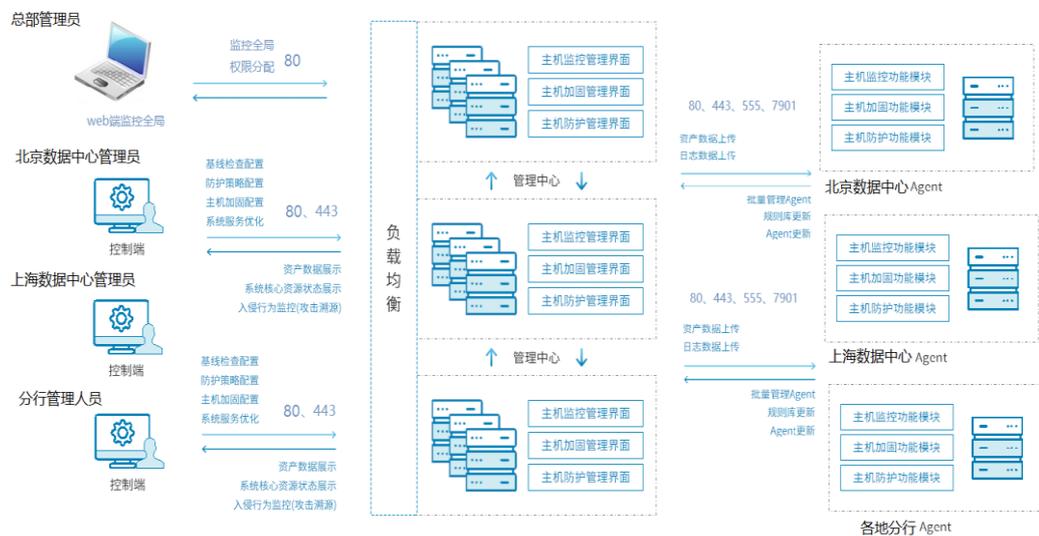
中国农业银行股份有限公司针对公网应用安全防护提出了多种解决方案和尝试，希望安全解决方案能够保证业务系统连续性和数据安全性。然而传统安全解决方案只能通过防火墙、IDS、网闸、UIM、透明加解密、SSL 加密、补丁管理、HIDS/HIPS、杀毒软件等滞后性的解决方案来缓解系统的安全威胁。这些产品只解决系统中某个点的安全，并没有解决整个系统的安全问题。

## 6.1.2 客户痛点及需求分析

- 1、需要解决日志缺失和关联性不足问题；
- 2、实现业务连续性和数据安全；
- 3、缺乏统一的服务器资产管理；
- 4、缺乏主机层面防护能力；
- 5、缺乏对持续性威胁（APT）防御能力；
- 6、业务流程防护体系缺失。

## 6.1.3 解决方案&实施过程

虚拟下图是在中国农业银行规划的实施方案部署结构图



部署时间是 2018 年起至今，客户的操作系统环境有实体机的 Windows、Linux 服务器以及，虚拟化环境：Vmware、KVM 。至今部署的机器数量 CentOS 6.5 64 位 8500 台、Windows 2008 Server 1200 台、Windows 2012 Server 300 台、共计部署台，预计后期部署 Agent 的服务器会超过 2 万台。

#### 6.1.4 实施效果/客户价值/项目亮点

在部署终端杀毒（统一服务器安全管理系统）后，农行打破传统的需要投入大量人力实时监控，频繁修复漏洞、升级补丁，以及以部分业务牺牲为代价的安全防护模式。转型主动防御，自适应网络安全架构，动态调整安全防护策略，保护了业务连续性和数据安全。

系统在风险识别、防御及威胁感知三个阶段均会产生安全事件，基于异常行为的检测技术，有效检测未知威胁，包括黑客渗透攻击、变形 webshell、后门等攻击事件回溯，自动回溯攻击过程并生成事件报告。可以做到快速及时发现攻击事件。统一服务器安全管理系统的部署解决了操作系统脆弱性的问题，而且通过建立安全边界、应用虚拟化沙箱技术解决了应用系统的安全。通过事件的回溯，更是可以精准定位黑客的攻击过程，也为调查取证提供了必要的支持。

## 6.2 山东省税务局

### 6.2.1 项目背景介绍

山东省国家税务局现有 16 个市局，1 所税务干部学校，126 个县（市、区）局和 34 个开发区局，共有内网终端 50000+。做为全国人口数量排名前三的省份，税务信息化建设对山东省税务局来说显的尤其重要，2013 年，“金税三期”率先在山东等省份试点，借助互联网+、云计算、大数据等技术的逐步部署应用，为全省搭建了统一的纳税服务平台，实现了全省税收数据大集中。

近两年随着《网络安全法》及等保 2.0 政策的出台，税务行业对信息安全建设重视程度日益提高，在税务总局制定的《税务系统云计算安全规范》（征求意见稿）中对虚拟机访问控制、入侵及恶意代码防范规范中进行了明确要求，各地陆续开展虚拟化安全建设。

## 6.2.2 客户痛点及需求分析

山东省税务局项目需求主要为针对虚拟化主机、云桌面终端以及物理服务器的病毒防护，结合客户业务场景及当前现状，需求分析如下：

**异构平台统一管理：**客户当前具有 Vmware5.1\6.0、深信服虚拟化平台、华为云桌面以及物理服务器，分开运维管理难度大、成本高，需要具备异构环境统一管理、集中运维的能力。

**大规模部署：**内外网虚拟化环境近 900 个 CPU（无代理）、以及约 2000 客户端（轻代理），要求能够批量导入，统一策略，减少部署及调试工作量。

**稳定性高：**所部署的系统运行的是山东税务核心征税业务，不容有失，对产品性能及稳定性要求高，需要有大规模部署应用案例。

**资源占用率低：**云桌面向大量的内部人员提供高效的日常办公处理，对资源占用敏感，杀毒产品不能影响正常办公，传统杀毒软件因资源占用较大不适用。

## 6.2.3 解决方案&实施过程

虚拟化安全产品兼容国内外主流的虚拟化平台，可实现多异构环境的统一部署与管理；

无代理模式因为不需要在每个虚拟机部署 Agent，部署效率高，资源占用率低，非常适合客户云桌面场景；

同时，针对客户的物理服务器资源以及深信服虚拟化平台，采用有代理的方式实现与虚拟化环境的统一管理与运维。



### 6.2.4 实施效果/客户价值/项目亮点

山东省税务局项目面对友商亚信、深信服的激烈竞争最终仍能够突破重围取得成功，对产品线及税务行业来说都是极大的鼓舞，“山东模式”无论在省内地市以及全国其他省份、地市的税务行业都具有标杆意义，为虚拟化安全产品在全国税务行业的推广提供了宝贵的项目经验。

基于国税《税务系统云计算安全规范》的标准要求，该项目在内网环境中以天擎覆盖终端安全，虚拟化安全覆盖服务器安全。在服务器侧虚拟化安全采取无代理部署模式，在保障资源低消耗的前提下对用户的服务器环境，包含物理服务器、虚拟机以及云桌面进行统一安全防护。

通过虚拟化安全的部署实施，在满足税务行业规范以及等保 2.0 要求的基础上，产品为客户提供服务器复杂环境下的安全防护，包括恶意代码防护、入侵防护、虚拟机环境访问控制等，有效的帮助客户筑起服务器安全护城河。

山东省局项目落地，首先有助于虚拟化安全产品在省内各地市、区县局虚拟化平台及用户桌面云场景迅速复制推广，已陆续有济南、临沂等地市甚至区县客户申请测试。

## 6.3 广安门医院

### 6.3.1 项目背景介绍

中国中医科学院广安门医院(暨中国中医科学院第二临床医药研究所)始建于 1955 年,是国家中医药管理局直属的集医疗、教学、科研和预防保健为一体的三级甲等中医医院。全院职工 1245 人,拥有 26 个临床科室及 8 个医技科室。目前开放病床 649 张,年门诊量 182 万余人次,日平均门诊量 7200 余人次;具有 HIS、PAAS、LIC 等多个业务系统,物理服务器 50 台以上,200 台左右终端设备等。

随着医院信息化建设的高速发展,在信息安全层面遇到如下挑战:

#### 1、对外系统增多带来的安全风险增加

随着最近几年互联网的发展成熟,国家也在不断推动互联网+医疗等政策,远程预约、微信支付、远程诊断等业务不断上线,使得原本只有内网业务的医院,不断开放业务模式,而旧的业务系统大多存在系统版本低、漏洞多等问题,增加了旧的系统被网络攻击风险;

#### 2、医院勒索事件频发,社会影响恶劣

医院设备众多,如工作站、自助机、服务器、前置机等多样性,而医院人员安全能力与意识不高,信息科人员多为业务科室转岗,对安全运维与管理意识不高,黑客往往利用这些弱点,通过社会工程学、暴力破解等方式,非法侵入内网,投放勒索病毒,造成大量业务系统瘫痪,病人无法看病,社会影响极差。

#### 3、国家对网络安全的重视

网络安全法的发布,护网行动的常态化,安全责任到人,促使大家对安全的重视度。

### 6.3.2 客户痛点及需求分析

结合广安门医院总体信息化建设规划,在推进各业务系统建设过程中,加强安全能力建

设，具体如下：

### 1、需要增加业务系统本身被漏洞攻击防御的能力

医院旧系统一旦安装运行，运维人员不会轻易升级、更换系统，一是运维人员能力有限；二是升级或重启等操作造成的系统中断，风险比较大；三是医院的特殊性，很多软件系统都是针对性开发或小公司开发，而这些开发人员一旦离职或公司倒闭，软件面临无人维护的状态。种种原因造成医院系统内存在大量漏洞包括操作系统、软件等。黑客一旦侵入内网，利用这些漏洞很容易进行网络攻击。网络入侵防御能力高低，决定业务稳定的一个重要环节。

### 2、需要增加业务系统杀毒能力

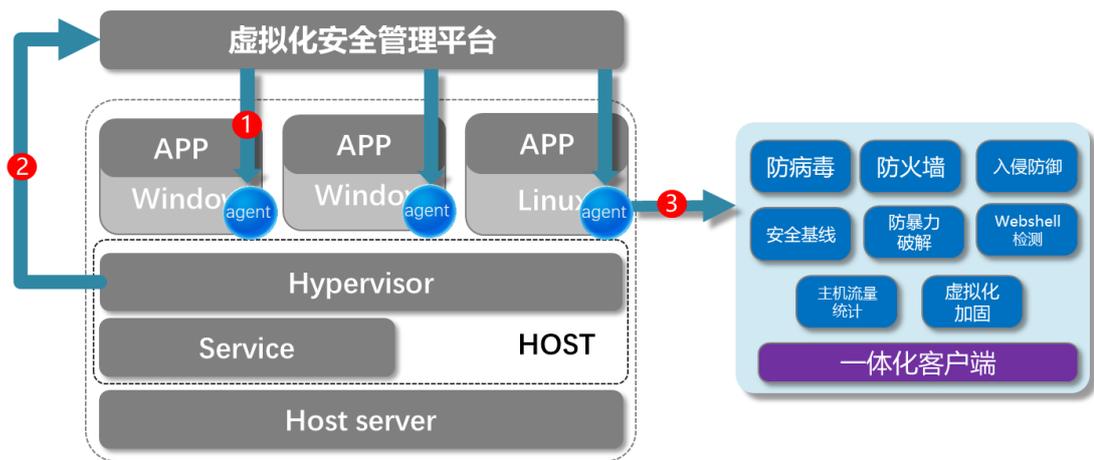
一个好的医院，特别是三甲医院，每天就诊、入院、出院的病人非常多，经营资金流水也相当多，同样所面临的社会责任也是很大，一旦发生系统瘫痪等恶性事件，会迅速传播，黑客往往利用医院系统的漏洞及社会责任，通过不同手段投放勒索病毒或挖矿病毒等病毒，故意索要钱财或肆意搞垮医院系统。杀毒能力决定了医院能否快速解决潜在恶性事件的重要能力。

### 3、需要业务系统安全满足等保需求

国家网络安全政策的出台，要求医院需要根据业务系统过等级保护，对于虚拟化环境下业务系统需要进行一定防护加固。

## 6.3.3 解决方案&实施过程

目前黑客攻击层出不穷，甚至愈演愈烈，针对网络、操作系统、应用等各个层面的攻击行为，最终目的是为了获取主机中的资源和权限。如果操作系统中某一应用出现漏洞，就可能导致整个操作系统沦陷，从而让整个服务器数据信息遭到破坏和窃取。对用户来说核心是保护操作系统中的数据信息，保障操作系统安全是信息安全的基础。



医院通过 IPS 入侵防御、内核级病毒查杀等技术等提高服务器操作系统对抗黑客攻击及恶意代码的能力，有效检测及拦截已知和未知安全威胁，全方位保障服务器操作系统、业务系统和数据内容的安全。通过主流的硬件平台、操作系统和应用，同时对物理机和虚拟化架构 (xen、vmware、hyper-v 等)，做好异构网络部署，实现跨平台的统一管理。

其中入侵防御功能，帮助医院防御新型、老系统漏洞、病毒攻击，阻拦可疑的行为，解决医院部分老系统或者业务不敢打补丁需求，减少了黑客利用漏洞攻击的概率。而防病毒功能能有效查杀主机上的文件、内存、进程中的恶意程序。管理员可以通过控制中心对主机进行统一的病毒查杀管理，制定定时查杀任务，辅以我们的主动防护引擎和文件监控模块，确保虚拟化的网络安全，解决勒索病毒、挖矿病毒等在医院内网存在及被攻击投放的风险。防暴力破解对暴力破解行为进行检测，并对触发主机防暴力破解规则的行为进行拦截，解决恶意破解医院业务系统进行攻击的行为。并通过 webshell、虚拟化加固等功能综合减少 被攻击风险，打造医院虚拟化系统强有力的防护系统。

#### 6.3.4 实施效果/客户价值/项目亮点

目前广安门医院已经部署虚拟化安全产品，并且不断的再增加安全产品的部署，符合国家等保、护网等政策和事件的基础上，增强了内网的安全，减少被攻击、勒索的几率。目前

医院虚拟化建设越来越多，虚拟化安全将受到越来越多的重视，可跟更多医院客户了解当前医院虚拟化安全的情况，突出我司虚拟化安全的优势，整体的优势如下：

### 1、支持多种部署方式及多数虚拟化平台

基于轻代理和无代理两种部署方式，可在物理机及虚拟机统一部署，兼容市面上大多虚拟化平台，无需对虚拟化层进行改造，轻代理直接安装，无代理对于已对接完毕的；

### 2、杀毒能力强

病毒防治采用云端大数据+多引擎结合的方式，云端拥有全球最大的病毒木马特征库和黑白名单库，本地内置多种专利杀毒引擎，还能对未知病毒威胁提供主动防御能力；webshell 检测同样利用云端 500 万的海量样本资源，结合自主研发的检测引擎，保证了对后门、挂马的检测；

### 3、IPS 规则库类型多

虚拟化安全目前入侵防御规则库达到 15000 多条，比主力竞争对手亚信多了 1.5 倍左右。能针对医院做很好的入侵防御。

### 4、立体防御

通过防病毒+虚拟 IPS+虚拟防火墙+webshell+防暴力破解等功能，建立立体防御能力。

## 7. 常见问题

### 7.1 计费类

#### 7.1.1 如何进行授权激活？

初次进入管理中心时必须对产品进行激活才可以正常使用。

(1) 登录管理中心，进入**管理 ->系统设置->使用许可** 页面

(2) 在页面中点击 **更新许可文件**，会打开如下图所示的 **使用许可 ->更新许可文件** 对话框，选择正确的许可文件，点击 **确定**，即可激活。



### 7.1.2 授权超时后怎么办？

授权计算方式为：按月按点数计算。授权超时以后，病毒特征库无法升级。点数超过限制以后，超限主机无法开启，激活功能，需要尽快增购授权点数。

## 7.2 操作类

### 7.2.1 Windows 客户端文件防护不生效？

问题现象：病毒查杀功能失效

排查步骤：

- 1) 排查客户端上 Anti-malware agent 服务是否正常开启。
- 2) 排查客户端上 nubfilter 驱动是否正常运行。使用命令 `sc query nubfilter` 查看：

```
c:\Program Files\Nubosh\icsagent>sc query nubfilter

SERVICE_NAME: nubfilter
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE                : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0
```

## 7.2.2 Windows 客户端网络功能不生效?

问题现象：防火墙规则不生效，或入侵检测规则不生效

排查步骤：

- 1) 排查客户端上 Agent Network Security Service 服务是否正常开启。
- 2) 排查客户端上 VmsecNetFilter 驱动是否正常运行。使用命令 `sc query vmsecnetfilter`

查看：

```
c:\Program Files\Nubosh\icsagent>sc query vmsecnetfilter

SERVICE_NAME: vmsecnetfilter
        TYPE               : 1  KERNEL_DRIVER
        STATE                : 4  RUNNING
                        (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0
```

## 7.2.3 Linux 客户端文件防护不生效?

问题现象：病毒查杀功能失效

排查步骤：

- 1) 排查/etc/init.d/ics-agent-file 服务是否正常运行。
- 2) 排查 vmsecmod 驱动是否正常运行。使用命令 `lsmod |grep vmsecmod` 查看：

```
lsmod |grep vmsecmod
vmsecmod                153213  3
```

## 7.2.4 Linux 客户端网络功能不生效?

问题现象：防火墙规则不生效，或入侵检测规则不生效

排查步骤:

- 1) 排查/etc/init.d/ics-agent-net 服务是否正常运行。
- 2) 排查 vmsec\_nfq 驱动是否正常运行。使用命令 `lsmod |grep vmsec_nfq` 查看:

```
lsmod |grep vmsec_nfq
vmsec_nfq                38615  2
```

### 7.2.5 Windows 客户端显示离线?

问题现象: 控制中心【虚拟机】页面, Windows 客户端显示离线

排查步骤:

- 1) 排查 Agent Common Module 服务是否正常运行。
- 2) 查看 `c:\program files\nubosh\icsagent\log` 文件夹下是否定期出现 `vmstatus` 文件, 且定期消失。若该文件不出现, 尝试重启 Anti-Malware-agent 服务; 若该文件存在且不消失, 尝试重启 Agent Common Module 服务。

### 7.2.6 Linux 客户端显示离线?

问题现象: 控制中心【虚拟机】页面, Linux 客户端显示离线

排查步骤:

- 1) 查看 `comm_srv` 进程是否正常运行。使用命令 `ps -ef |grep comm_srv`。若该进程未启动, 查看操作系统 `cron` 服务是否运行正常。
- 2) 查看 `/opt/nubosh/vmsec-host/log` 文件夹下是否定期出现 `vmstatus` 文件, 且定期消失。若该文件不出现, 尝试使用命令 `/etc/init.d/ics-agent-file restart` 命令重启服务; 若

该文件存在且不消失, 使用 kill 命令杀当前 comm\_srv 进程, 等待一分钟待新的 comm\_srv 进程启动。

### 7.2.7 客户端的 IP、主机名持续变化?

问题现象: 安装有代理客户端后, 在控制中心页面查看相关客户端 IP 地址、主机名会持续变化

排查步骤:

查看虚拟机操作系统 UUID 是否相同。虚拟化安全产品的有代理客户端通过系统的 UUID 进行客户端区分 (该 UUID 理论上不会重复)。当虚拟机为特殊情况克隆出来, 或通过特殊渠道进行的操作系统安装, 可能导致两台甚至多台虚拟机的操作系统 UUID 相同, 当这些虚拟机都安装了有代理客户端后, 控制中心会认为这些虚拟机为一台虚拟机, 只是相关信息在修改 (例如 IP 地址做了修改), 因此在控制中心上会显示一台主机记录, 其信息在不停变化。

### 7.2.8 如何导入安全组件包?

问题现象: 控制中心进行 VMware 云平台添加时报错 “添加主机池失败, 请导入安全组件包”

排查步骤:

控制中心未包含 VMware 平台的 NSVM 安装包, 需要手动下载 NSVM 包, 在控制中心页面【系统】-【下载中心】中使用 “导入” 功能先进行导入。

## 7.3 管理类

### 7.3.1 为什么管理中心实时监控中一直没有数据?

主机安全组件会把流量日志和安全事件发送回管理中心,由管理中心进行处理后最终在实时监控中显示。由于实时监控的数据具有实时性要求,如果收到的日志时间和当前时间误差大于 2 小时,管理中心将丢弃这些日志。这样就会导致实时监控中没有数据。通常是由于主机和管理中心的系统时间没有同步造成的,解决办法是同时在主机和管理中心上打开 NTP 时间同步机制。

注:如果管理中心与主机时间不同步,管理中心会产生对应的警报。

### 7.3.2 管理中心重新配置网卡或者克隆之后,ip 地址无法获取或配置失败怎么办?

新增的网卡的信息与旧网卡的配置不匹配,导致网络服务启动失败,接口无法获取 ip 地址。只要在管理中心运行“configure network reset”命令和“reboot”命令,在重启之后,重新配置 ip 地址即可生效。

### 7.3.3 浏览器不能正常显示怎么办?

防护系统支持近两年内发布的大部分浏览器。然而由于一些虚拟化特性,部分虚拟机不支持 WebGL。故这些浏览器查看具有 3D 效果的组件时,不能正常显示。建议使用物理机,高阶一些的浏览器。

浏览器/类型	物理机	虚拟机	备注

IE	IE9、IE10、IE11 兼容	IE9、IE10、IE11 兼容	IE 10 2013 年 2 月发布, IE 11 2014 年 1 月发布
firefox	Firefox 31.0 兼容	Firefox 31.0 兼容	31.0 2014 年 8 月发布
chrome	Chrome 35.0 兼容	Chrome 35.0 兼容	35.0 2014 年 6 月发布

管理网络和计算网络是相互隔离的, 虚拟机连的是计算网络, 无法连接管理网络, 但是又需要与管理中心进行通信, 如何解决?

在创建管理中心时, 需要添加两个网卡, 分别连接管理网络和计算网络。管理中心安装成功后, 可进入 CLI 配置其中一个网卡为管理口。输入命令: `configure network management interface` 并回车, 在下图所示的向导中输入对应的网卡编号即可

```
>
> configure network management interface
Interfaces:
-----
1. eth0 10.128.1.40
2. eth1 192.168.145.17
-----
There are 2 interfaces above in the system.
Please input the interface number(0 for no management interface):1
Interface eth0 has been set as management interface
Stopping vmsec controller: [ OK ]
Starting vmsec controller: [ OK ]
>
>
```

只有配置为管理口的接口才能访问管理中心的页面, 如果不配置的管理口的话, 则通过两个接口均能访问管理中心页面。

```
C:\Windows\system32>reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system" /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f  
操作成功完成。
```

使用 windows 系统普通权限用户安装安全组件时报错。

原因：被 windows UAC 拦截，需要添加注册表配置。

解决方法：以管理员身份运行 cmd，输入以下命令：

```
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system" /v  
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

保存成功即可。

角色名

权限

权限类别

无权限

读

读写

安全策略



报表



高可用



警告



实时监控&amp;日志分析



使用许可



系统更新



系统管理



虚拟机/终端管理



用户管理



主机管理



✓ 确定

↶ 取消