有底安全卫士

用户操作手册

奇墨科技（广州）有限公司

二零二四年

目 录

1. 引言

1.1. 编写目的

本操作说明书的主要目的是为用户提供关于如何使用有底安全卫士的详细操作指导和使用方法。

通过本说明书，用户将了解有底安全卫士的基本原理、特点以及如何正确配置使用有底安全卫士。本操作说明书将以使用者的角度对有底安全卫士涉及内容进行详细描述，为使用者提供操作指引。

本操作说明书主要面向平台管理员及 IT 运维人员，读者应具备一定的网络管理和技术基础知识，了解网络资源管理基本概念。

1.2. 项目背景

在当今数字化转型的浪潮中，企业正面临着前所未有的安全挑战。随着信息技术的飞速发展和业务需求的不断增长，企业的 IT 环境变得日益复杂，涵盖了从本地设备到云端环境的多个层面。这种复杂性不仅为企业带来了运营上的便利，同时也为恶意攻击者提供了可乘之机。

首先，随着互联网的普及和数字化进程的加速，企业面临着来自各个方面的潜在威胁。恶意软件、病毒、勒索软件等安全风险层出不穷，它们能够利用各种漏洞侵入企业系统，窃取敏感数据、破坏业务流程，甚至导致整个系统的瘫痪。这些安全事件不仅会给企业带来巨大的经济损失，还可能损害企业的声誉和客户信任。

其次，企业在追求业务发展的同时，往往忽视了安全防护的重要性。在快速迭代和部署新应用的过程中，安全漏洞和弱点可能被忽视或未被及时修复，从而为攻击者提供了可乘之机。此外，随着云计算、大数据等新技术的应用，企业的安全边界变得更加模糊，传统的安全防护手段已经难以满足当前的安全需求。

最后，企业需要一种全面、高效的安全防护解决方案来应对这些挑战。有底安全卫士正是基于这样的背景应运而生。它为企业提供全面的主机安全防护，通过实时监控和主动防御机制，精准识别并阻止各类潜在威胁。无论是本地设备还是云端环境，有底安全卫士都能为企业构筑坚实的安全防线，确保终端设备和数

据的安全，保障业务的稳定运行。

1.3. 读者对象

有底安全卫士用户

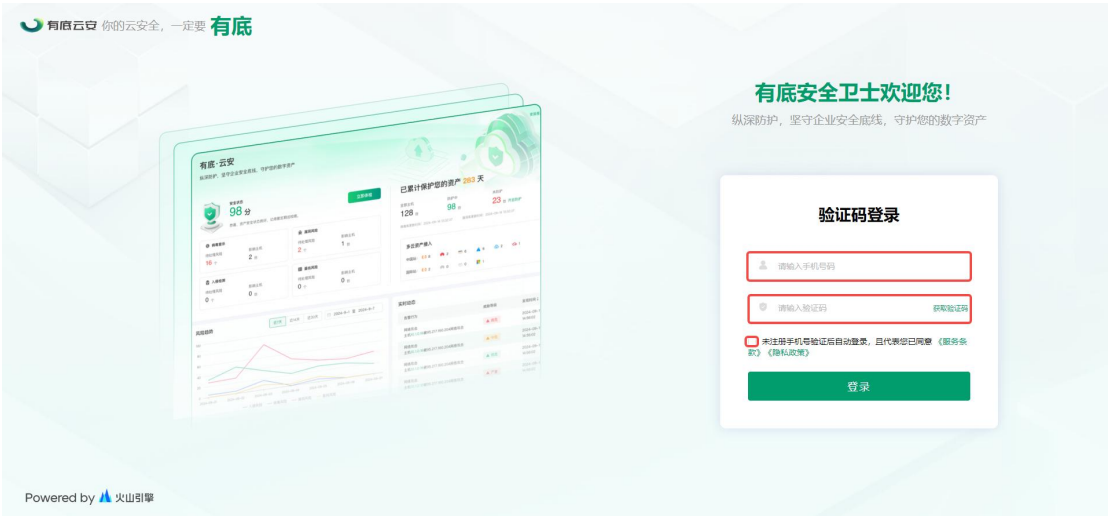
2. 有底安全卫士操作指南

2.1. 从这里开始

2.2. 登录

使用浏览器（推荐谷歌浏览器）访问 https://youdi.cloud/console/#/login，输入您的手机号、验证码，并勾选服务条款、隐私政策，单击登录按钮，即可成功进入到有底安全卫士简洁模式页面。

注：若手机号尚未注册有底安全卫士账号，登录后系统将自动为您注册新账号。



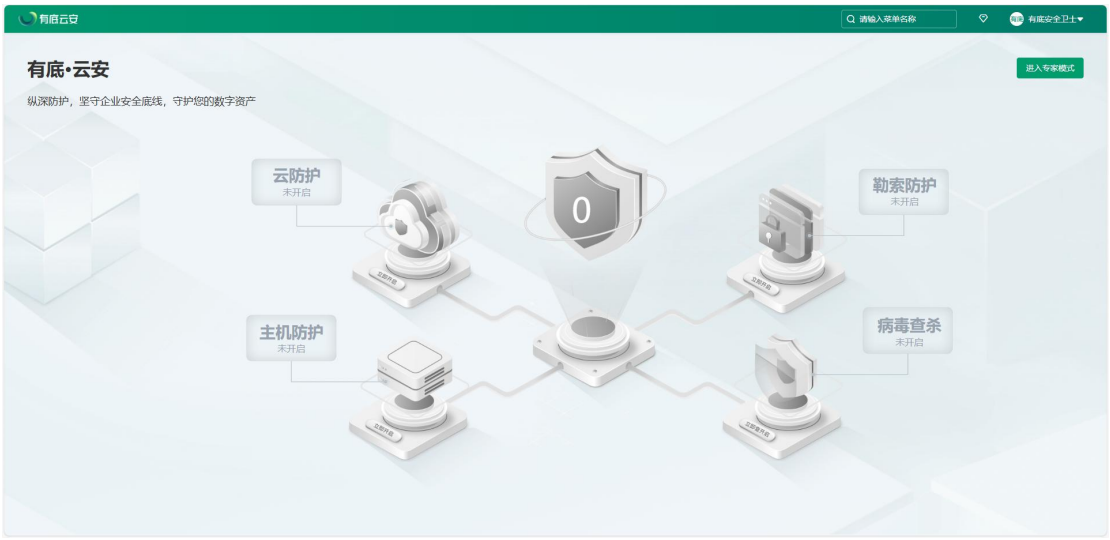
2.3. 有底安全卫士模式

有底安全卫士提供简洁模式和专家模式两种选择，用户登录后默认进入简洁模式，点击‘进入专家模式’按钮，即可切换到专家模式。

2.4. 简洁模式

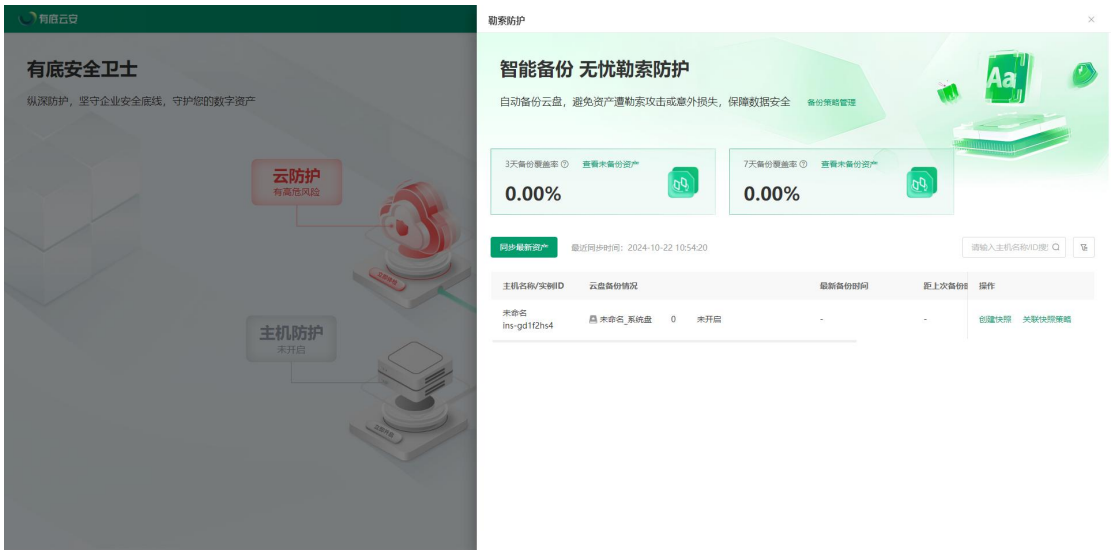
简洁模式展示了四个图标和一个评分，图标默认为未点亮，分数初始为 0

分。

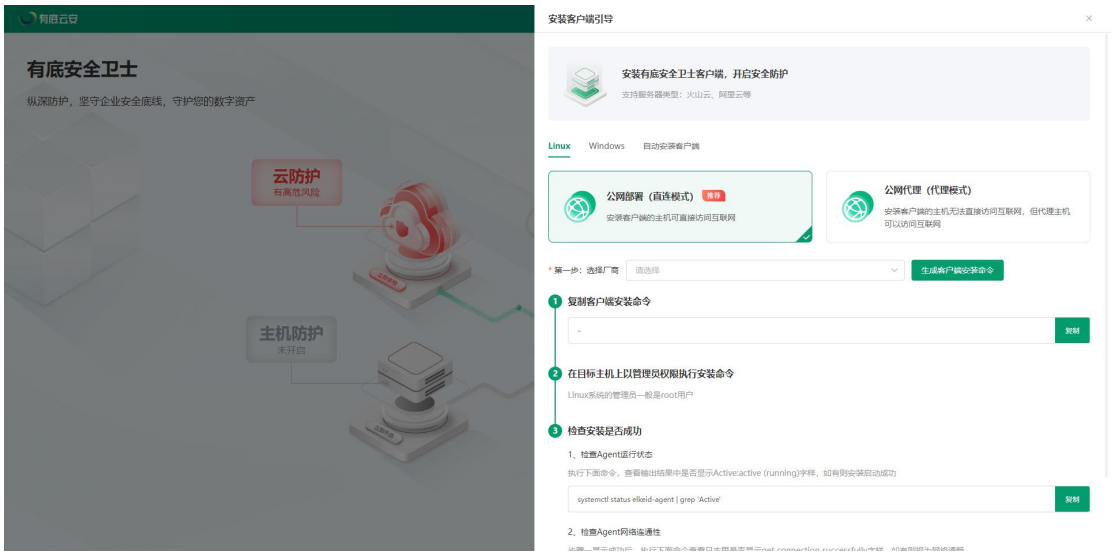


点击未点亮的云防护图标，弹出 AK 接入弹窗，选择云厂商填写对应 AK 即可同步资源并进行一次安全体检。

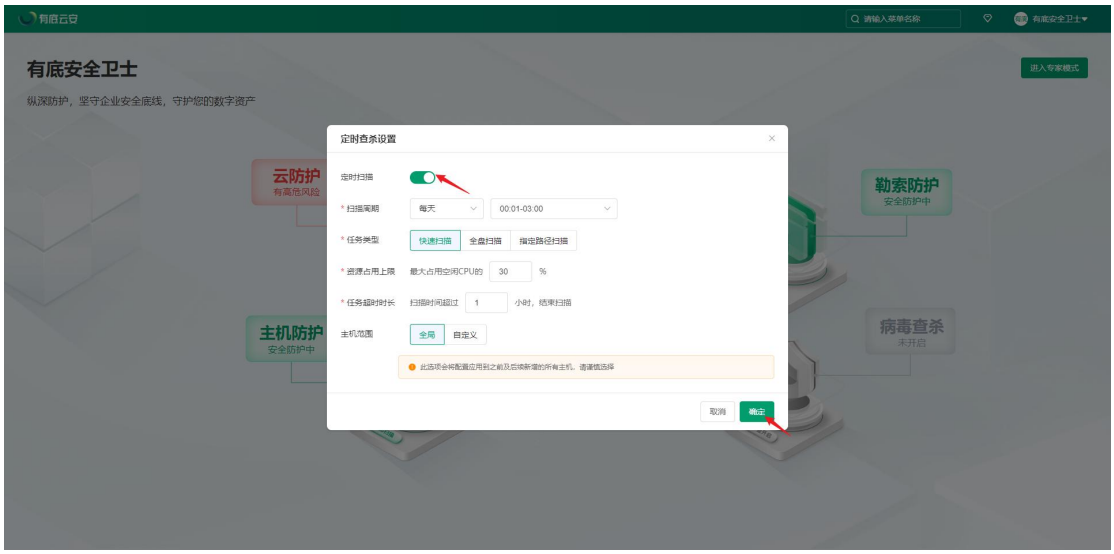
点击未点亮的勒索防护图标，弹出勒索防护弹窗，可对主机云盘进行创建快照以及关联快照策略等操作。



点击未点亮的主机防护图标，弹出安装客户端引导弹窗，可对需要安装客户端的主机执行对应的操作命令。



点击未点亮的病毒查杀图标，弹出定时查杀弹窗，可根据需要对主机进行定时查杀。



注：点亮勒索防护图标须先点亮云防护图标，点亮病毒查杀图标须先点亮主机防护图标。

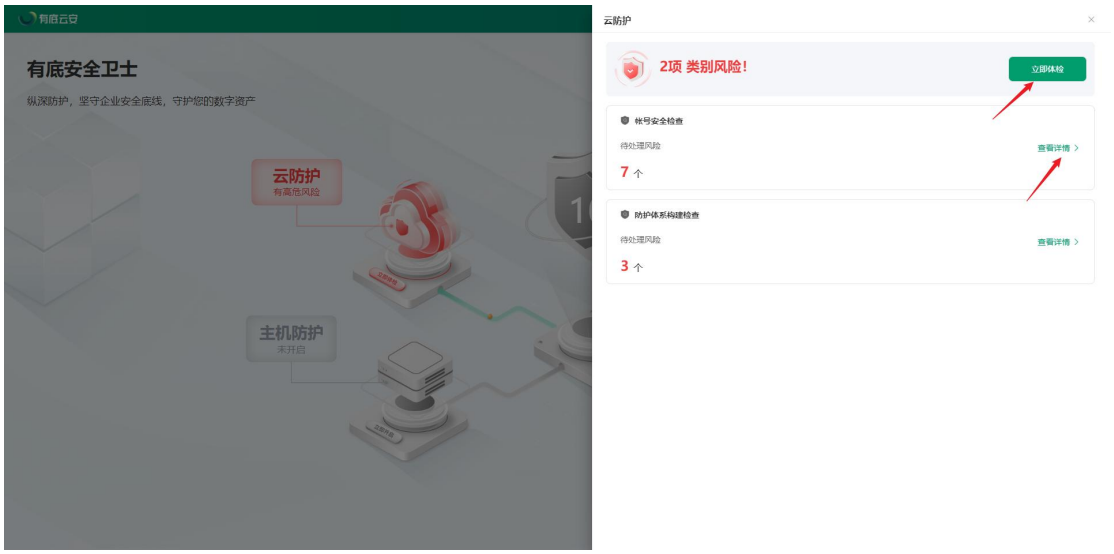
若成功接入 AK 并同步回大于等于 1 台服务器，则点亮云防护图标，获得初始分 25 分，体检发现 1 个高风险项则扣 5 分，1 个中风险项扣 2 分，扣到 10 分后停止扣分。

若存在大于等于 1 条关联了云盘的备份策略，则点亮勒索防护图标，获得初始分 25 分，3 天或 7 天任一一种备份覆盖率在 25%以下得 10 分，25%-69%得 15 分，70%以上得 25 分。

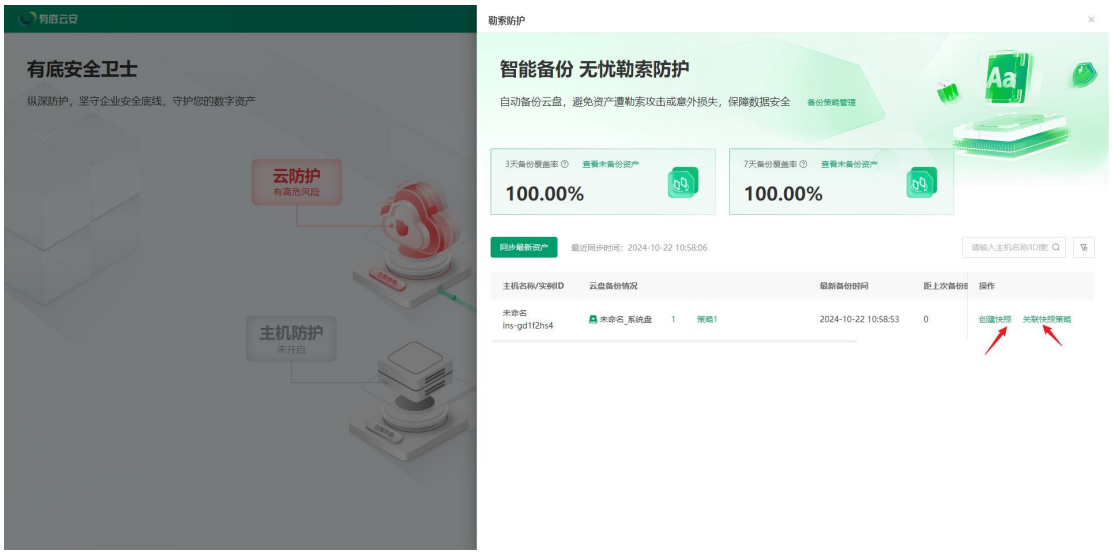
若存在大于等于 1 台服务器开启了防护，则点亮主机防护图标，获得初始分 30 分，存在 1 个未处理的高危告警/漏洞/基线风险则扣 5 分，1 个未处理的中危告警/漏洞/基线风险则扣 2 分，扣到 15 分后停止扣分。

若开启了病毒定时查杀，则点亮病毒查杀图标，获得初始分 20 分，存在 1 个未处理的高危病毒则扣 5 分，1 个未处理的中危病毒则扣 2 分，扣到 10 分后停止扣分。

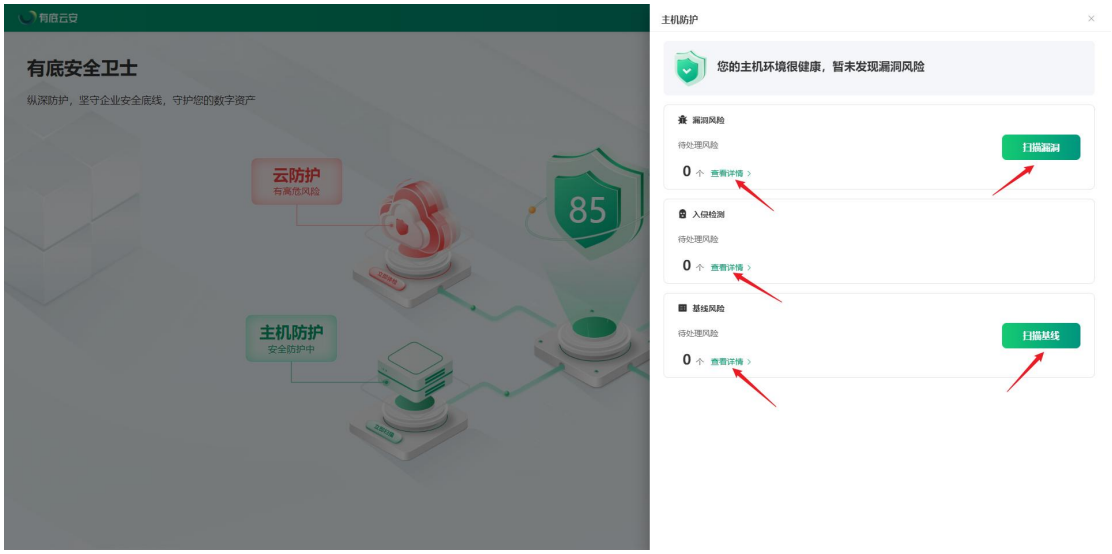
点击点亮后的云防护图标，若存在风险则展示待处理的风险项数量，点击‘查看详情’按钮即可跳转至安全体检报告详情页；点击‘立即体检’按钮即可进行一次安全体检。

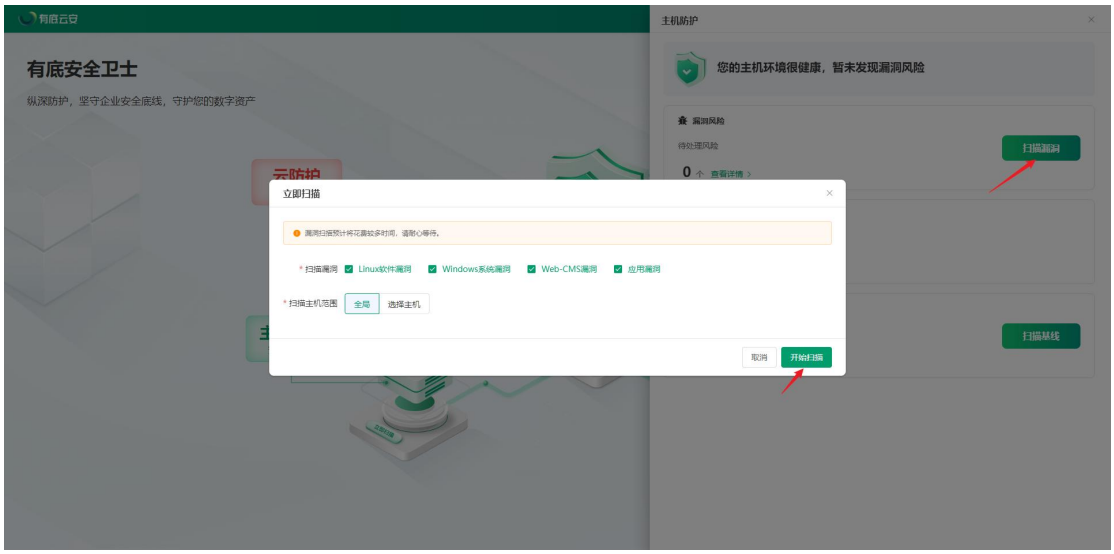


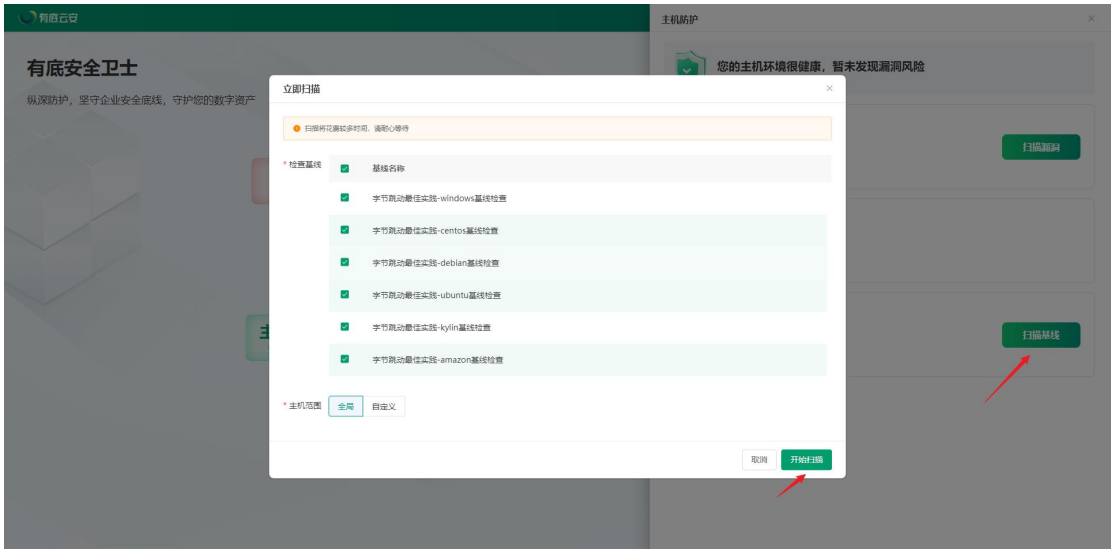
点击点亮的勒索防护图标，可查看主机云盘的备份情况，对主机云盘进行创建快照、关联快照策略等操作。



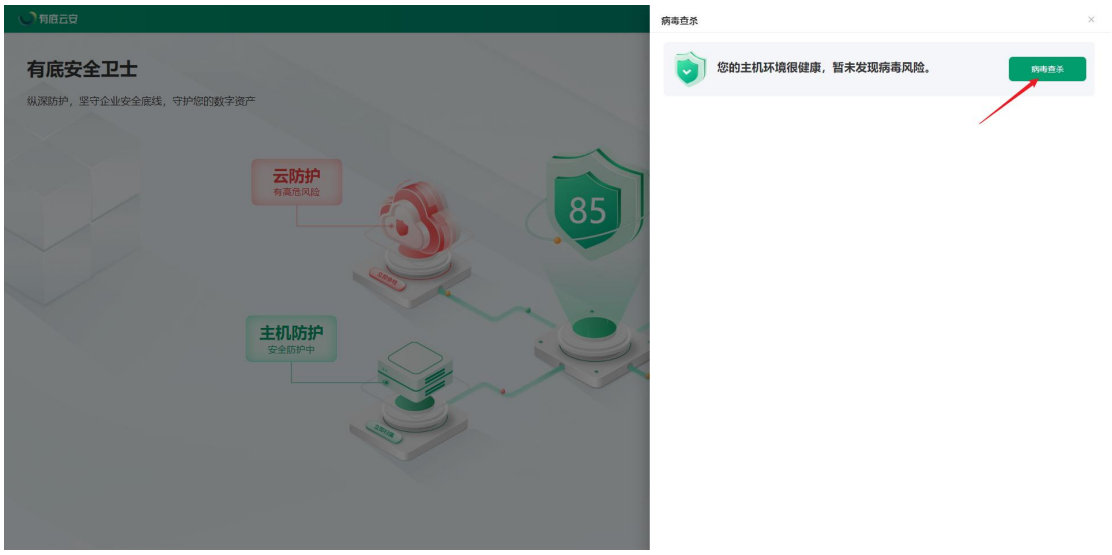
点击点亮的主机防护按钮，若存在漏洞风险/入侵检测风险/基线风险则展示各类风险待处理的风险数，点击‘查看详情’按钮即可跳转至对应页面；点击‘扫描漏洞’按钮，选择扫描漏洞类型和主机范围后即可进行扫描；点击‘扫描基线’按钮，选择检查基线和主机范围后即可进行扫描。







点击点亮的病毒查杀按钮，若存在病毒风险则展示待处理的风险数，点击‘查看详情’按钮即可跳转至病毒查杀页面；点击‘病毒查杀’按钮，选择任务类型和生效范围后即可进行查杀。



2.5. 专家模式

2.5.1. 总览

在简洁模式点击‘进入专家模式’按钮即可成功进入专家模式总览页面。总览提供安全状态、风险趋势和实时动态等内容。

安全状态

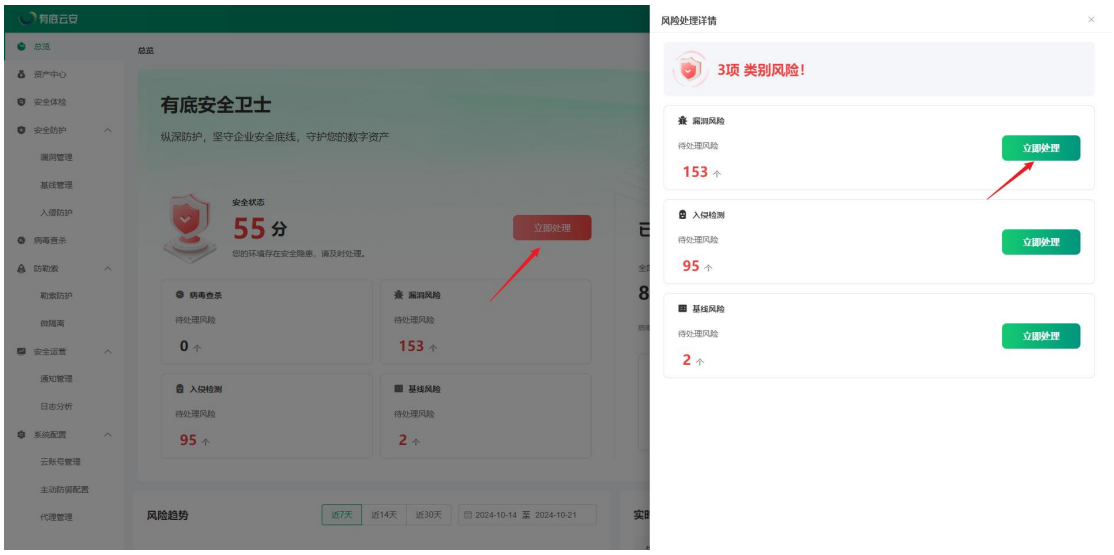
安全状态模块展示安全评分、待处理的病毒查杀风险数/漏洞风险数/入侵检测风险数/基线风险数、累计保护天数、主机总数/防护中主机数量/未防护主机数量以及云账号资产接入数量。

安全评分规则与简洁模式一致，若病毒查杀/漏洞风险/入侵风险/基线风险四

项中任何一种存在严重/高危的待处理风险，则分数显示红色；若存在中危的待处理风险，则分数显示橙色；其他情况则显示绿色。

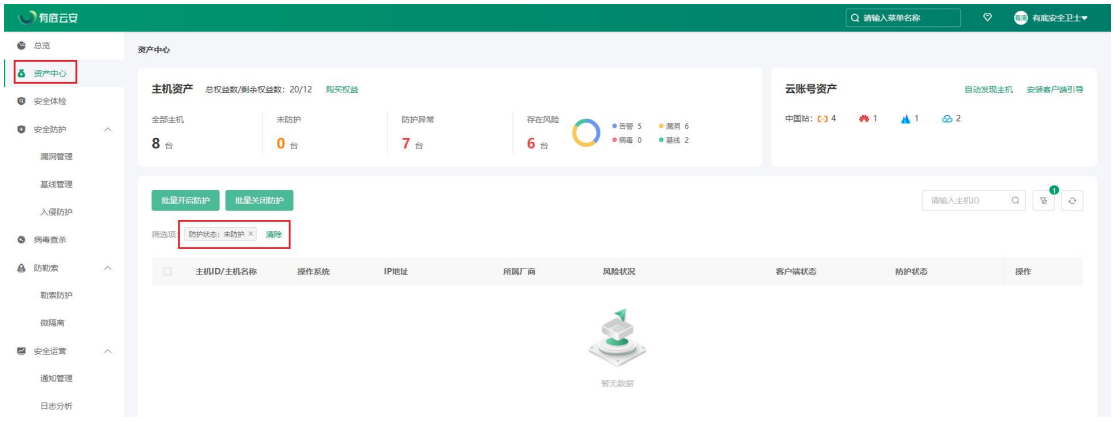
点击病毒查杀/漏洞风险/入侵风险/基线风险可跳转至相对应的模块页面。

点击‘立即处理’按钮，弹出风险详情弹窗，弹窗展示待处理的风险类别及数量，分别点击各类别的‘立即处理’按钮可跳转至相对应的页面对风险进行处理。

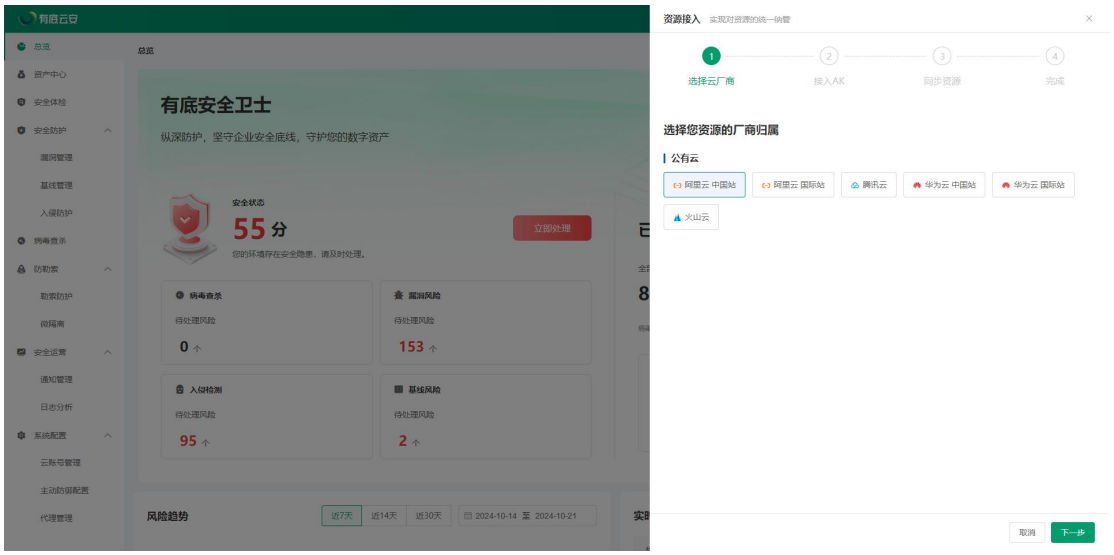


点击‘安装客户端引导’按钮弹出客户端引导弹窗，可对需要安装客户端的主机执行对应操作命令。

点击‘开启防护’按钮可跳转至资产中心页面并过滤出未开启防护的主机。



在云账号资产选择某个云厂商点击‘接入’按钮，可通过填写 AK 对该云厂商的资源进行接入；点击‘管理云账号’按钮可跳转至云账号管理页面。



风险趋势

风险趋势模块展示入侵风险数量和病毒风险数量趋势图，可调整时间范围进行查看。

实时动态

实时动态模块展示最近一天的入侵告警数据，点击告警名称可跳转至告警详情页面进行查看处理操作。

2.5.2. 资产中心

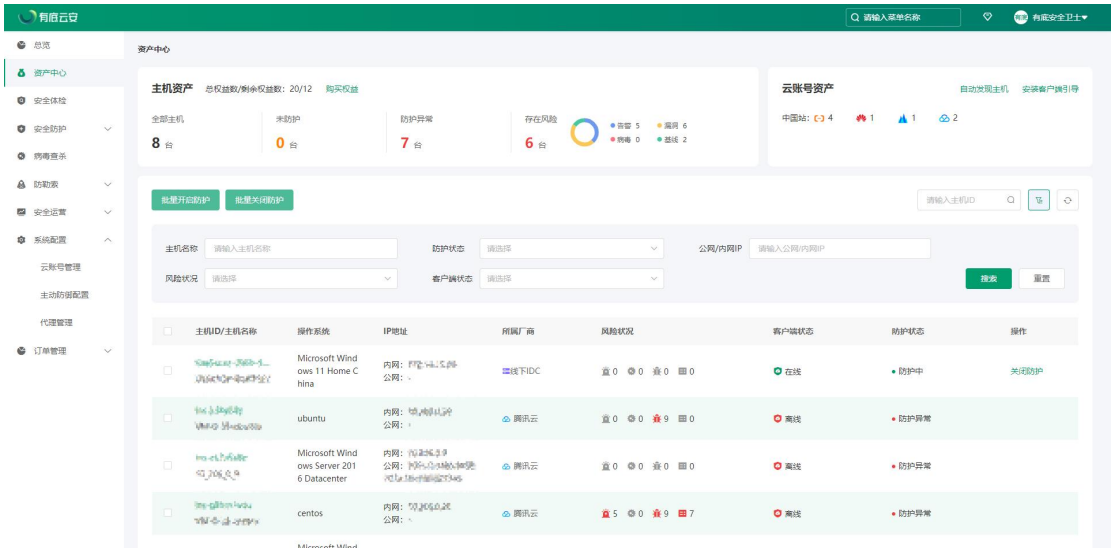
在资产中心页面，可查看主机资产和云账号资产。

主机资产展示该租户下的权益总数以及剩余数量，统计处于不同防护状态和包含各类风险的主机数量。

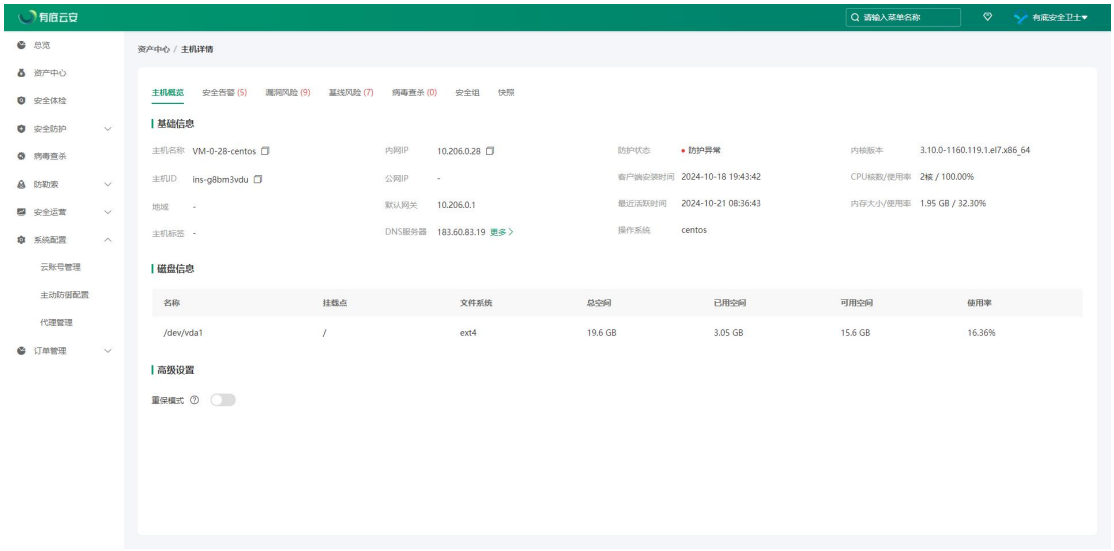
云账号资产展示可接入的云厂商以及已接入云厂商主机数量。

主机列表可查看主机信息，可通过主机 ID、主机名称、防护状态、公网/内网 IP、风险状况、客户端状态对主机进行搜索筛选，点击主机 ID 可进入其详情页查看各类信息（主机概览、安全告警、漏洞风险、基线风险、病毒查杀、安全组、快照）。

主机客户端状态为在线时，点击‘开启防护’按钮可对一个/多个主机开启防护；开启防护的主机也可通过点击‘关闭防护’按钮关闭防护。

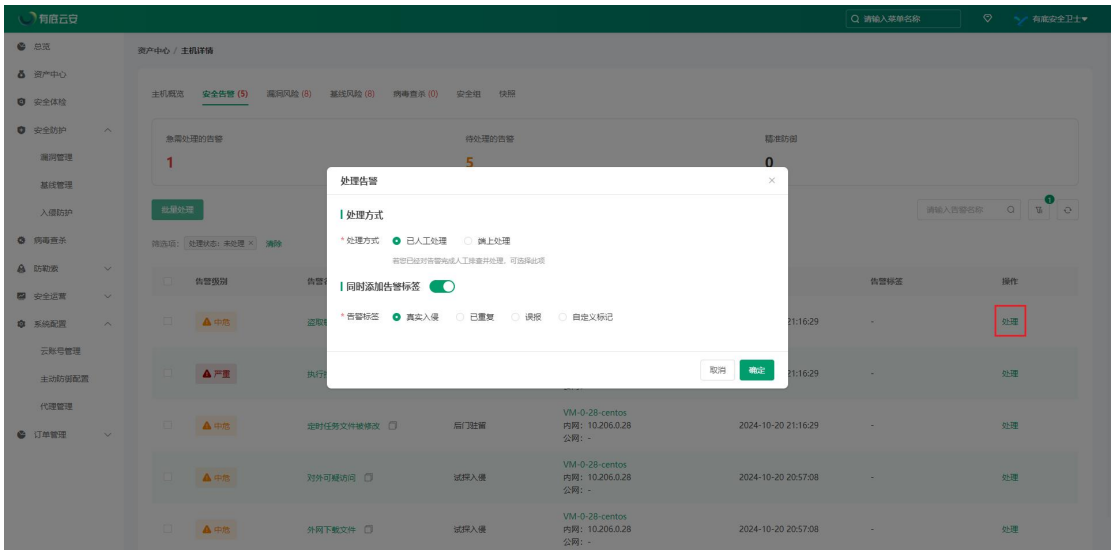


高级设置-重保模式将展示更多可疑入侵事件，请根据实际需求选择开启。

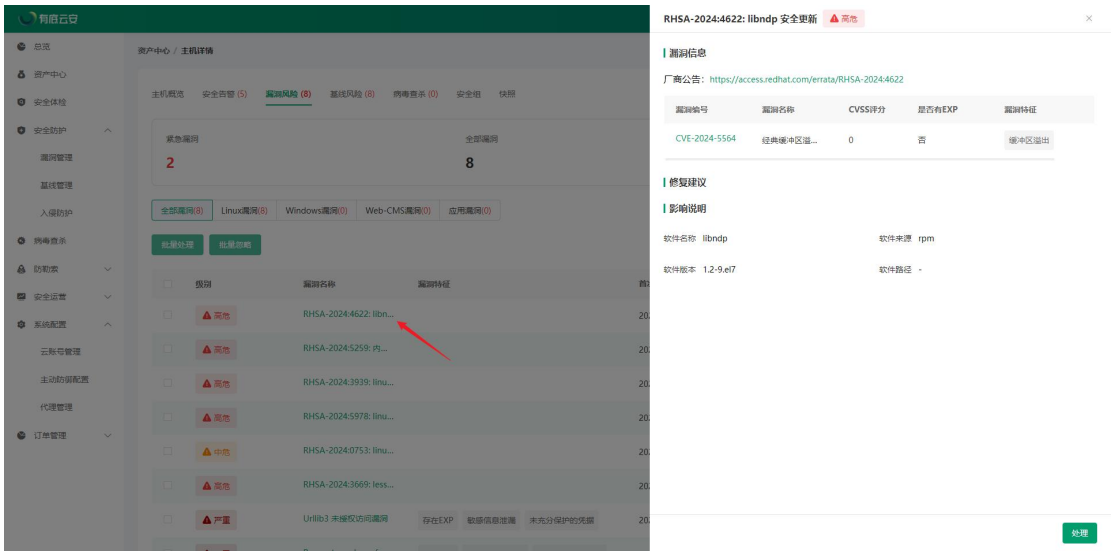


安全告警页签展示该主机下存在的告警数据，点击‘处理’按钮可对告警进行处理，处理方式分为已人工处理和端上处理，可根据需要自行选择处理方式。

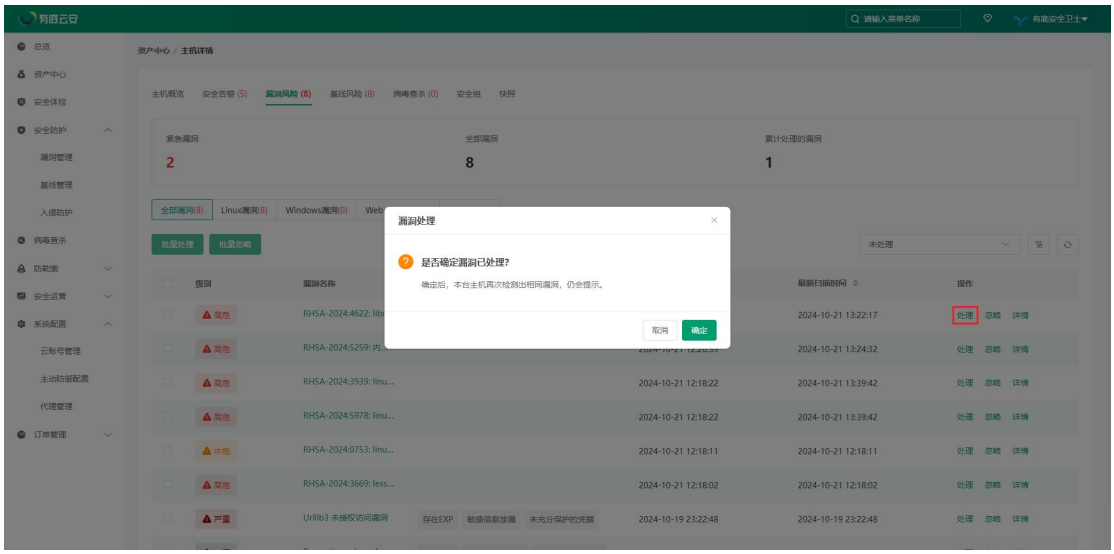
注：只有 Linux 支持端上处理（告警类型不等于杀伤链），Windows 不支持



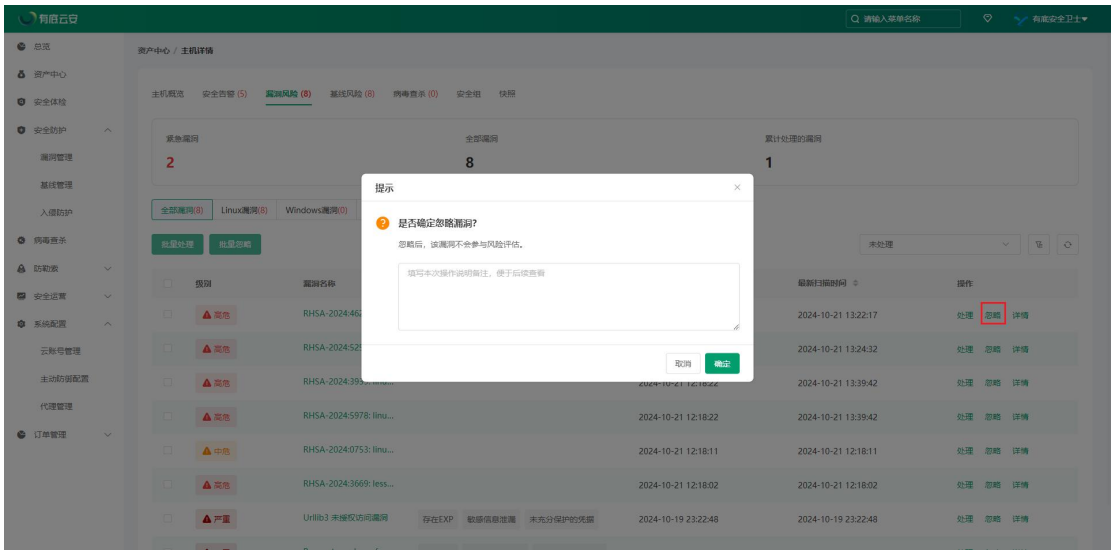
漏洞风险页签展示该主机下的仅高可利用性漏洞数据，点击漏洞名称可查看漏洞详情。

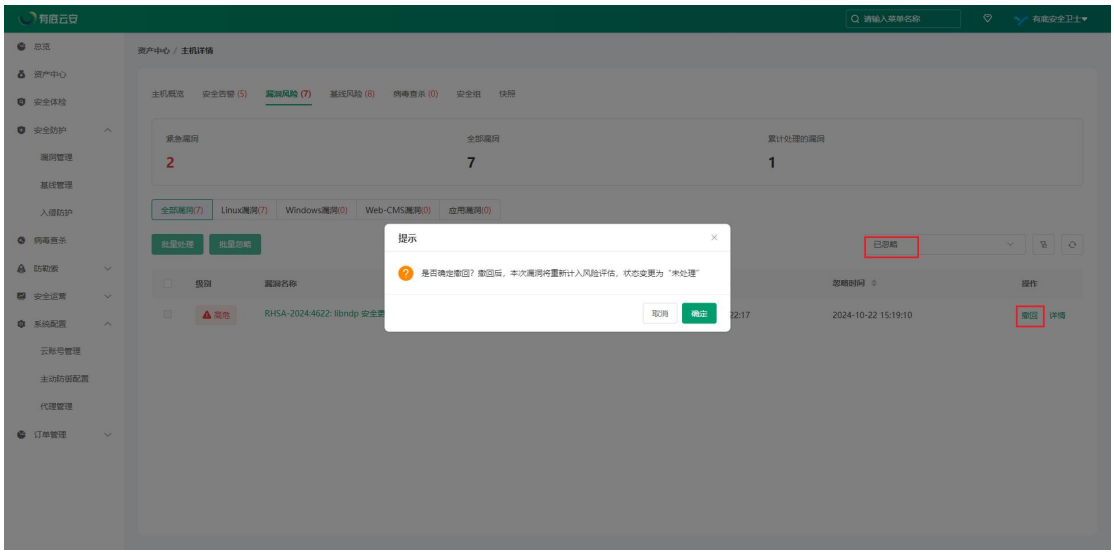


点击‘处理’按钮，该资产漏洞风险状态会变成已处理，并移至已处理列表。若该资产再次检测出相同漏洞，仍会提示。

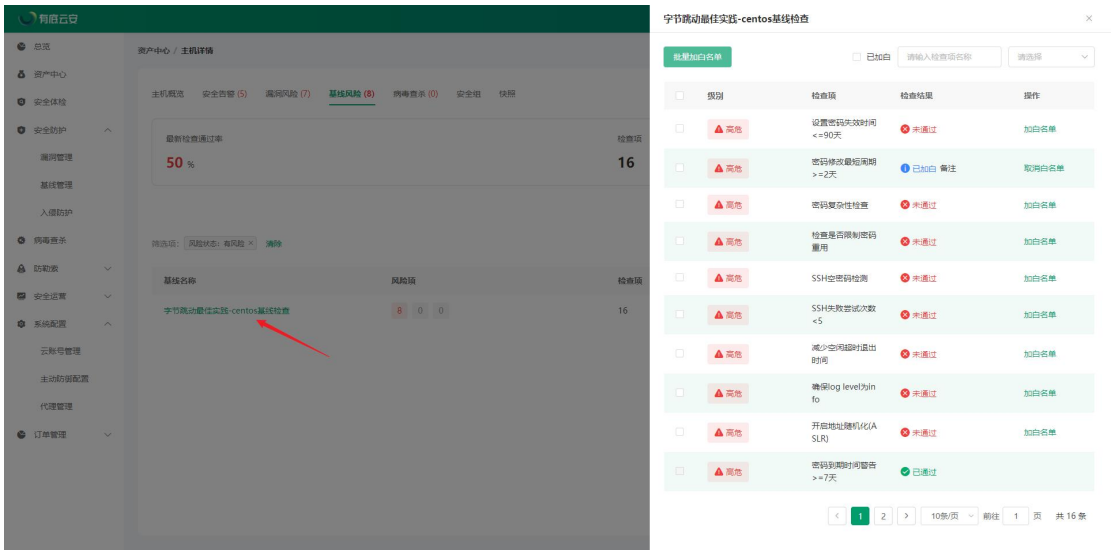


如您希望不再上报该资产的该漏洞风险，可单击忽略。该资产漏洞风险状态会变成已忽略，并移至已忽略列表。如需要取消忽略，可筛选已忽略漏洞进行撤回操作。

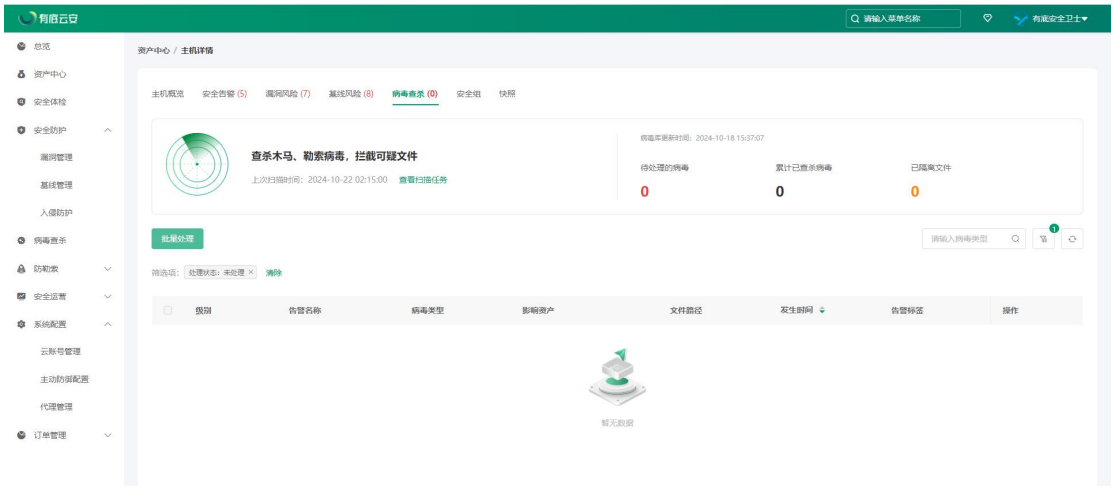




基线风险页签展示该主机下的基线风险数据，点击基线名称可查看基线详情。在基线详情弹窗内，可对未通过的基线基线加白操作，加白成功后，下次将不会对其进行扫描。



病毒查杀页签展示该主机下的病毒风险数据。点击‘下载文件’可成功下载压缩包；点击‘处理’按钮可对病毒进行处理。



安全组页签展示该主机的出战规则、入站规则以及安全组列表。

快照页签展示该主机的云盘数据，可对主机下的云盘进行创建快照以及管理快照策略操作。

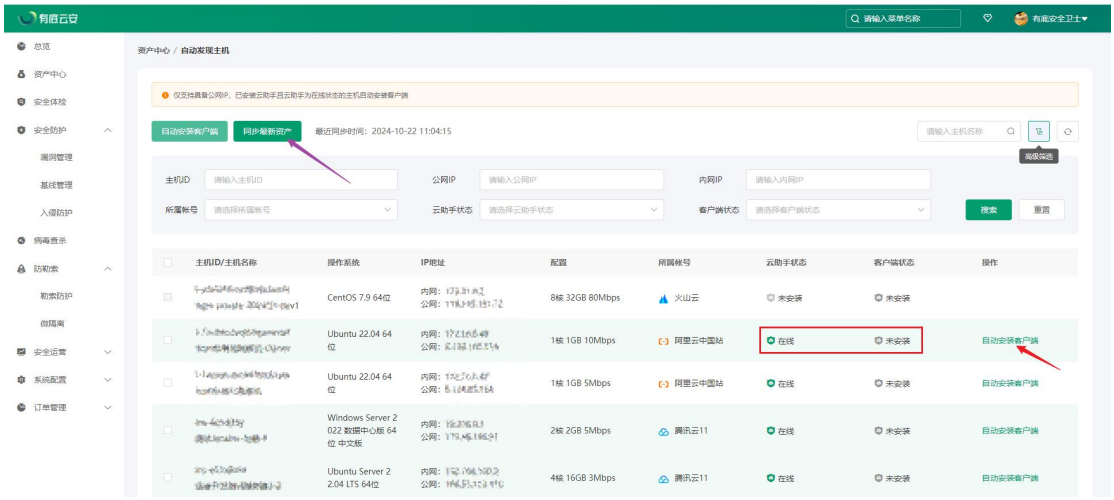
2.5.2.1. 自动发现主机

在资产中心点击‘自动发现主机’按钮即可进入自动发现主机页面，页面展示已接入云厂商资源中未安装火山客户端并且具备公网 IP 的主机。

点击‘同步最新资产’按钮可自动同步一次资产（30 分钟内仅可手动执行一次）。

若列表存在云助手状态为在线且客户端状态为未安装的主机，可点击‘自动安装客户端’按钮，系统将根据租户、云厂商、操作系统类型生成安装命令并下发安装客户端，安装成功后客户端状态将变为待启用。

注：列表目前支持展示云厂商阿里云、腾讯云、火山云数据。

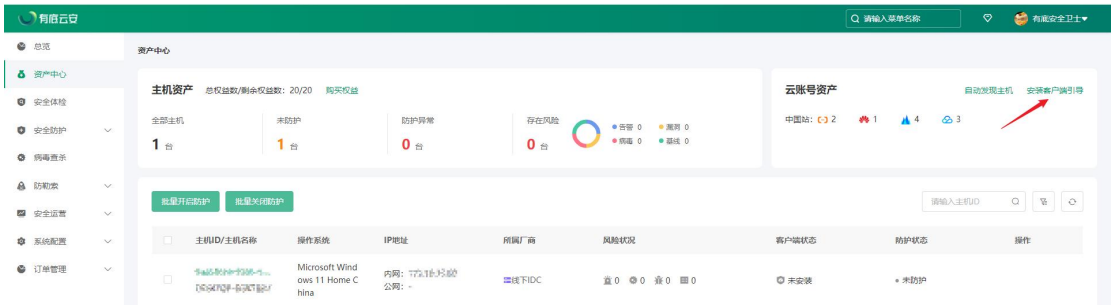


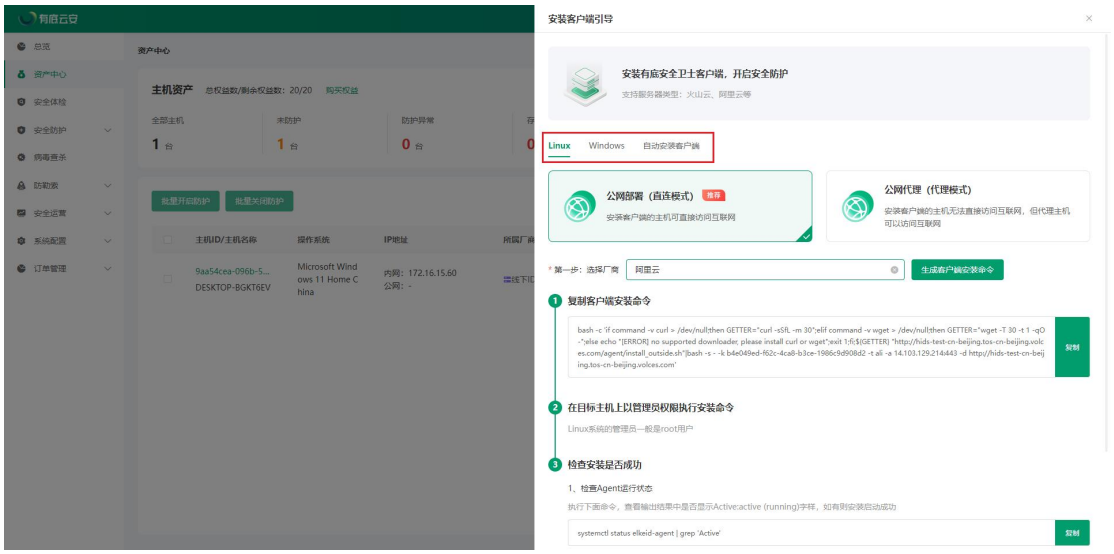
2.5.2.2. 安装客户端

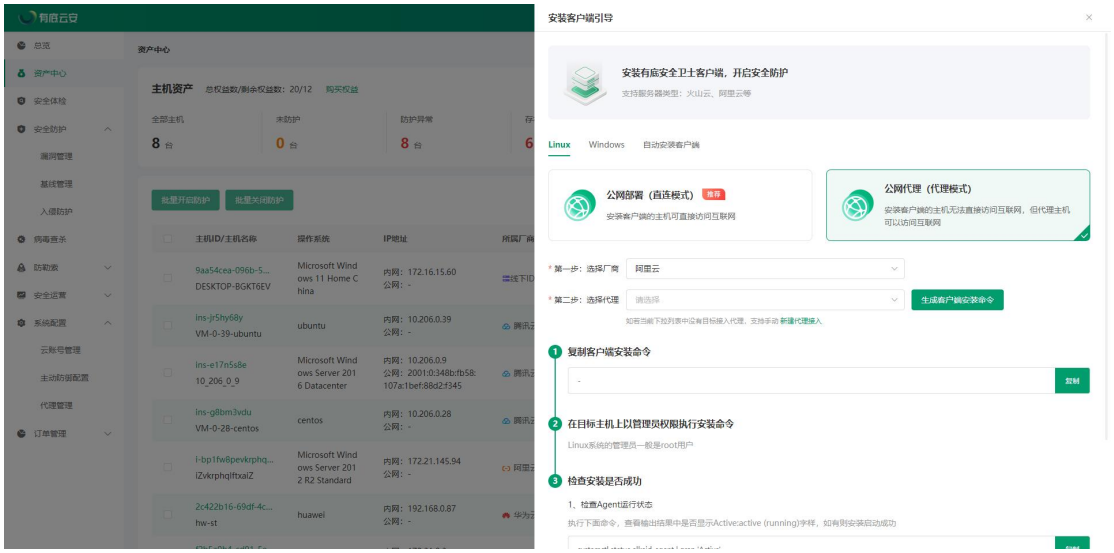
在资产中心点击‘安装客户端’按钮即可弹出安装客户端引导弹窗，可根据云厂商、服务器操作系统（Linux/Windows）以及公网部署/公网代理方式，点击‘生成客户端安装命令’按钮，使用管理员账号登录需要安装客户端的主机执行对应的安装命令；也可在自动安装客户端页面进行自动安装。

Linux：在服务器的命令行界面，执行已复制的命令。

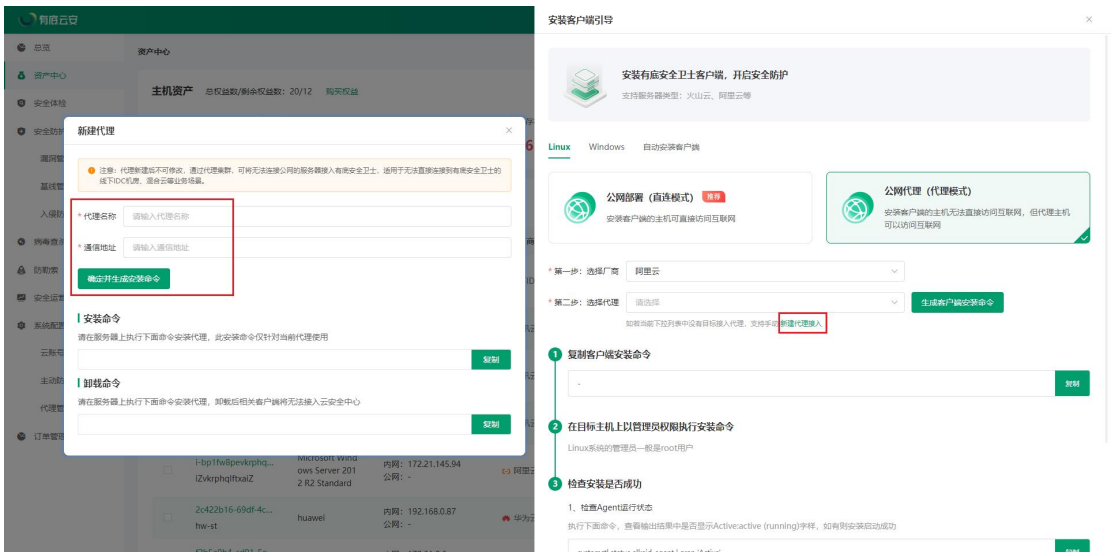
Windows：在命令提示符（CMD）界面中，执行已复制的命令。





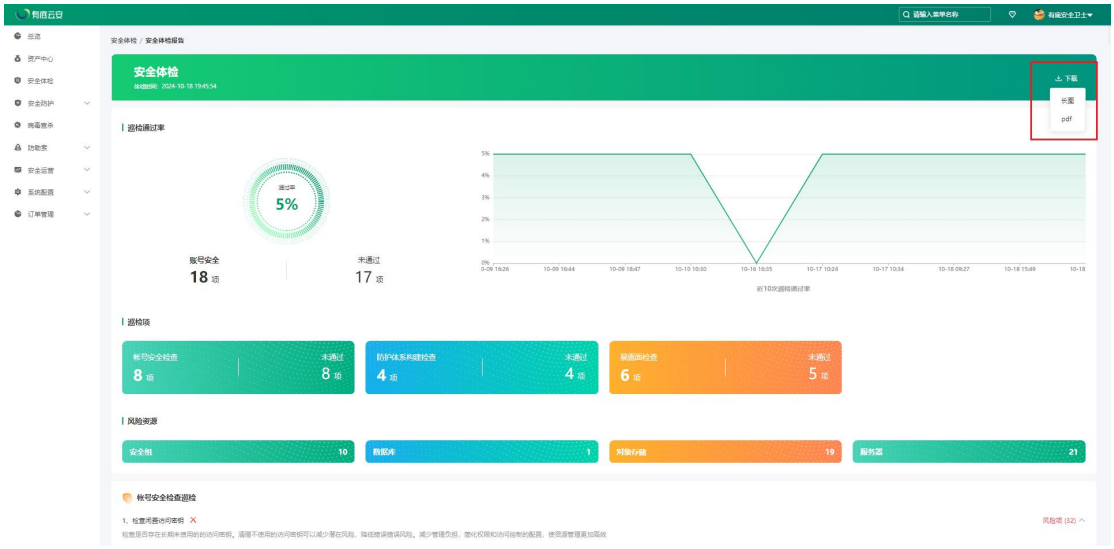


公网代理模式，若没有可用代理，可点击‘新建代理接入’按钮添加代理。添加成功的代理会在系统配置-代理管理页面展示。



2.5.3. 安全体检

用户接入 AK 后即可在安全体检页面点击‘马上体检’按钮进行一次安全体检。体检完成后，点击‘查看报告’按钮即可跳转至报告详情页面，查看体检过程中暴露出来的问题，还可以下载报告。



2.5.4. 安全防护

2.5.4.1. 漏洞管理

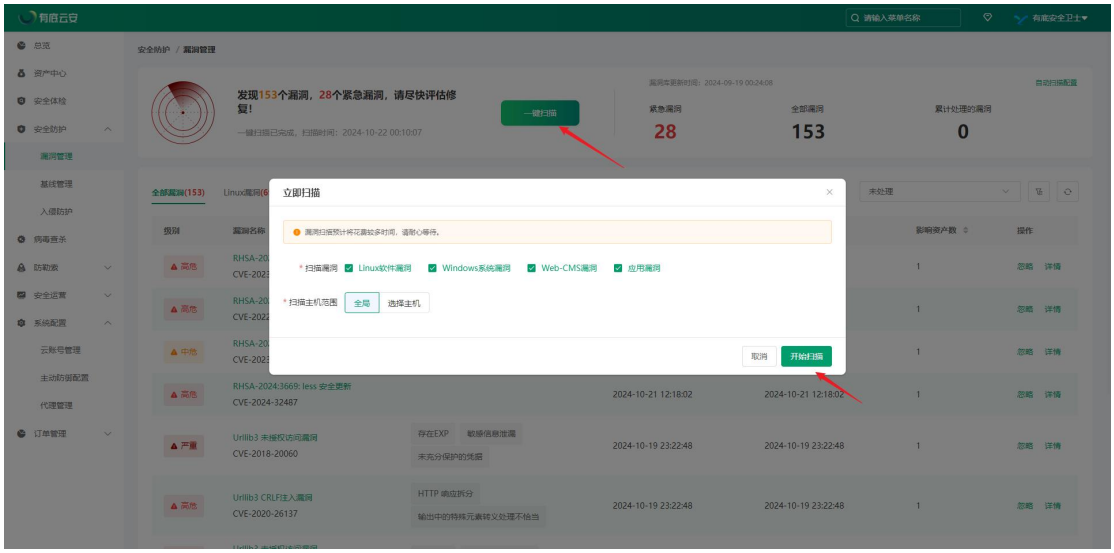
攻击者常利用 Linux 软件、Windows 系统、Web-CMS 以及各类应用程序的安全漏洞发起攻击，这些漏洞可能被用来执行远程代码、提升权限、数据泄露或发起拒绝服 务攻击。漏洞检测功能能够深入识别和评估这些潜在风险点，为您提

供具体的修复建议，通过及时修复这些问题，可以显著增强系统的抵御能力，降低被攻击者利用的风险。

2.5.4.1.1. 扫描漏洞

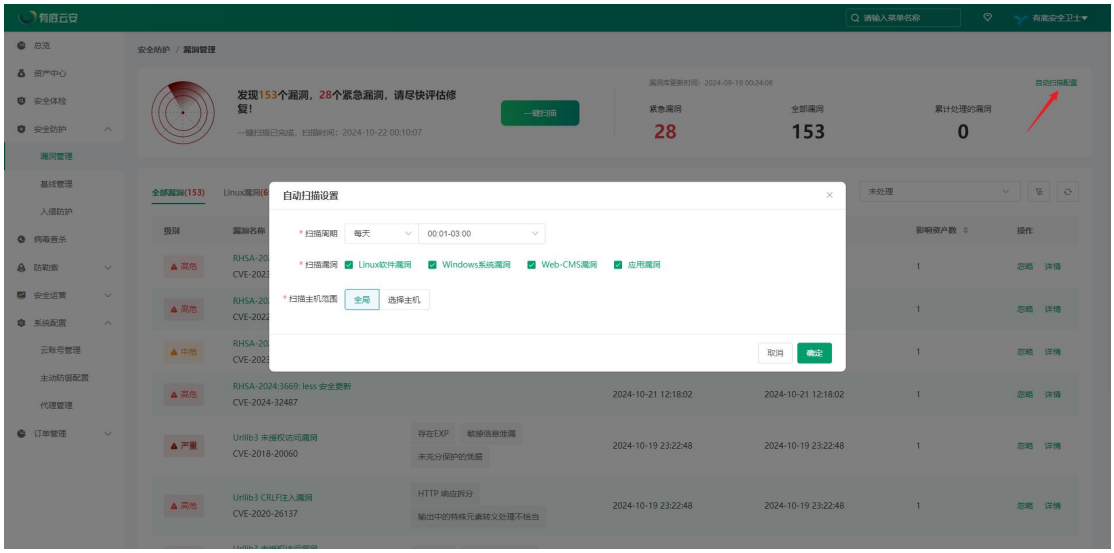
立即扫描

在漏洞扫描页面点击‘一键扫描’按钮，选择扫描的漏洞类型和扫描的主机范围，点击开始扫描即可。



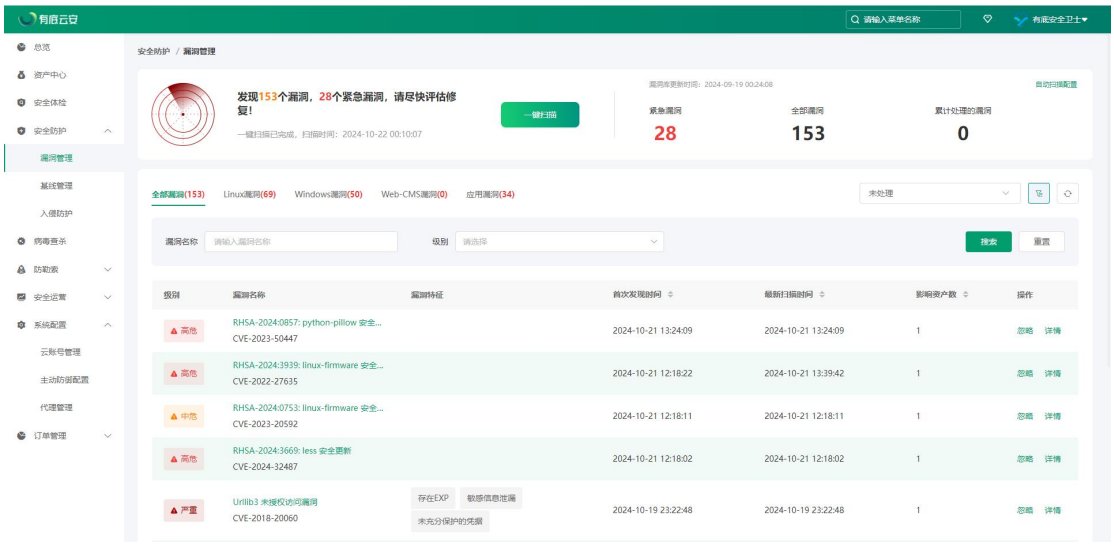
定时扫描

在漏洞扫描页面点击页面右上方的‘自动扫描设置’按钮，选择扫描周期、扫描的漏洞类型和扫描的主机范围，点击确定。

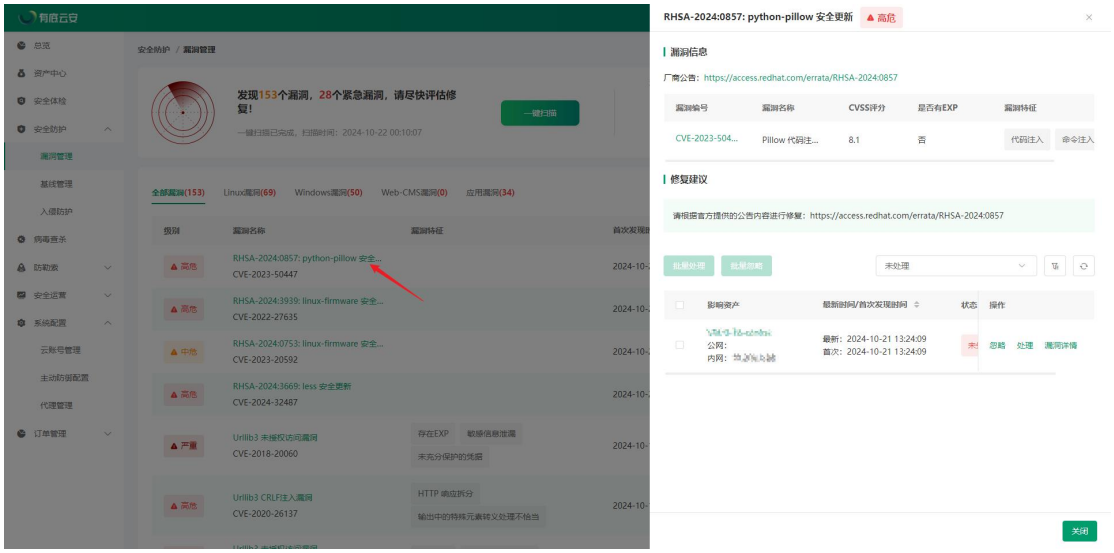


2.5.4.1.2. 查看漏洞

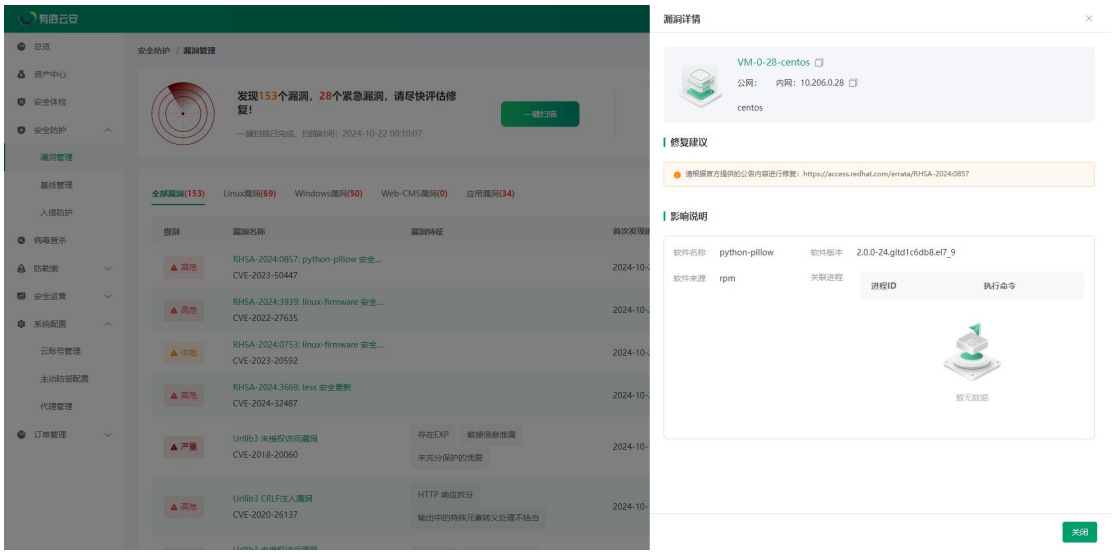
漏洞列表分为全部漏洞、Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞和应用漏洞五个页签。列表默认展示未处理的漏洞，其他状态的漏洞可手动筛选展示。漏洞列表以漏洞为视角进行聚合，一个漏洞可能影响多个资产。



点击漏洞名称，可查看漏洞信息及影响资产。

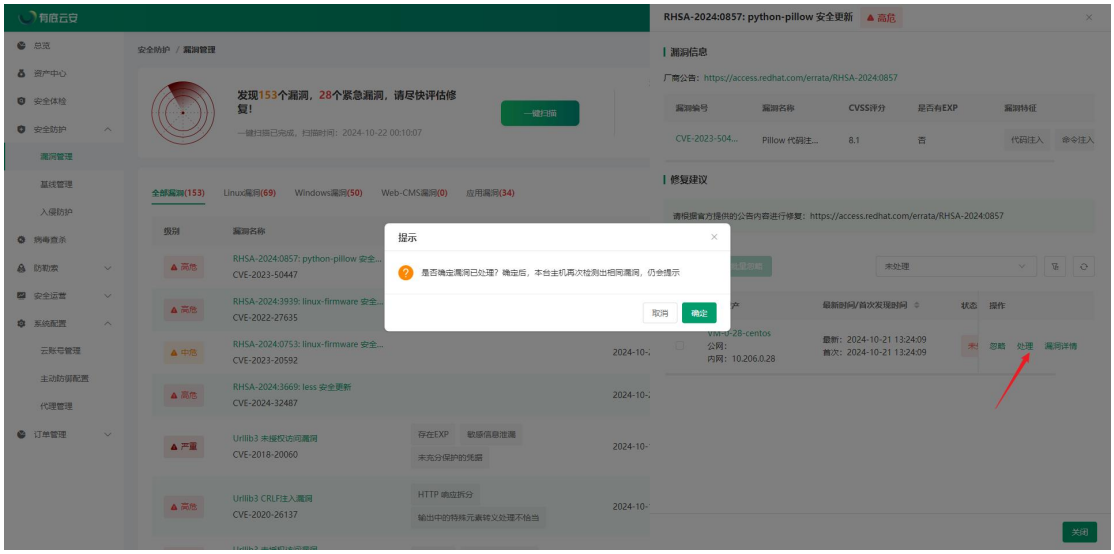


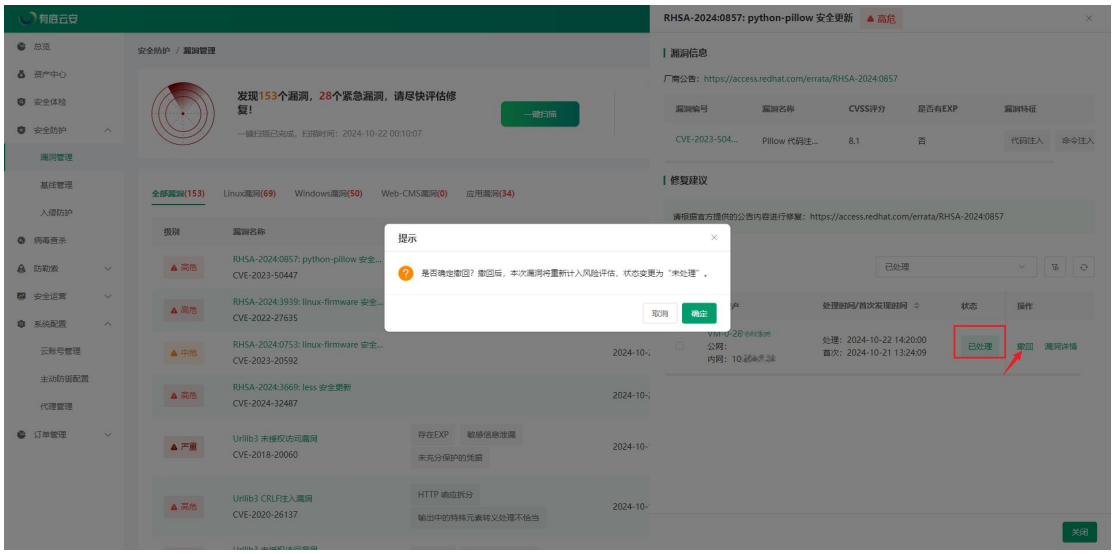
点击漏洞详情，可查看对应资产的影响说明。



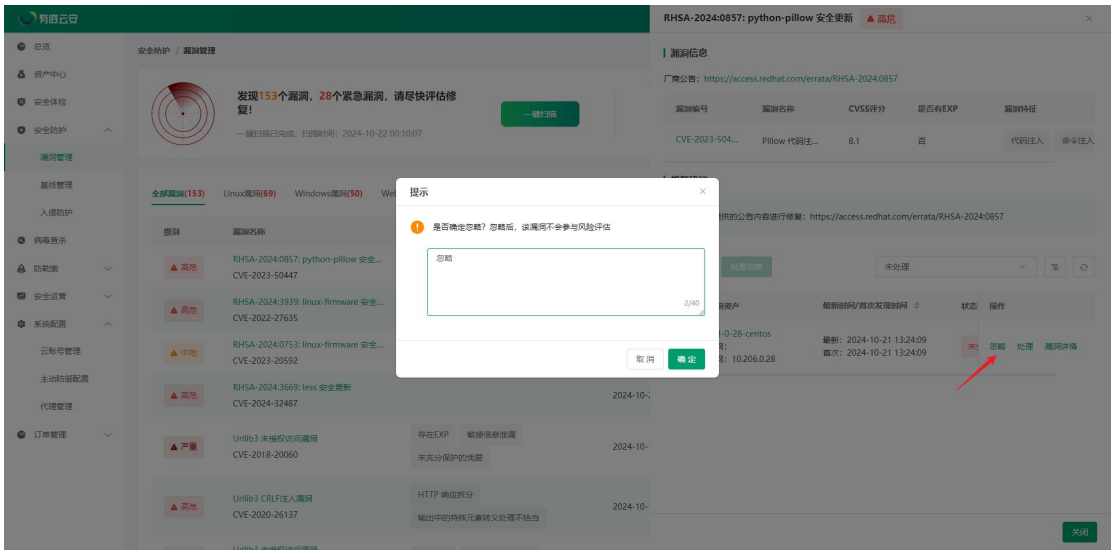
2.5.4.1.3. 处理漏洞

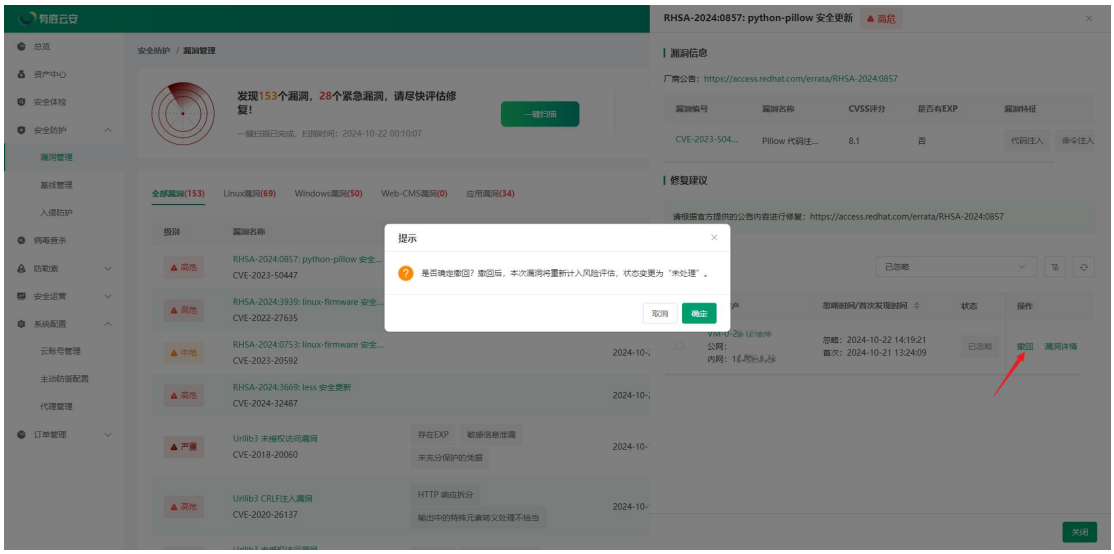
在漏洞详情弹窗，如您已经完成修复，可单击处理。该资产漏洞风险状态会变成已处理，并移至已处理列表。若该资产再次检测出相同漏洞，仍会提示。





如您希望不再上报该资产的该漏洞风险，可单击忽略。该资产漏洞风险状态会变成已忽略，并移至已忽略列表。如需要取消忽略，可筛选已忽略漏洞进行撤回操作。





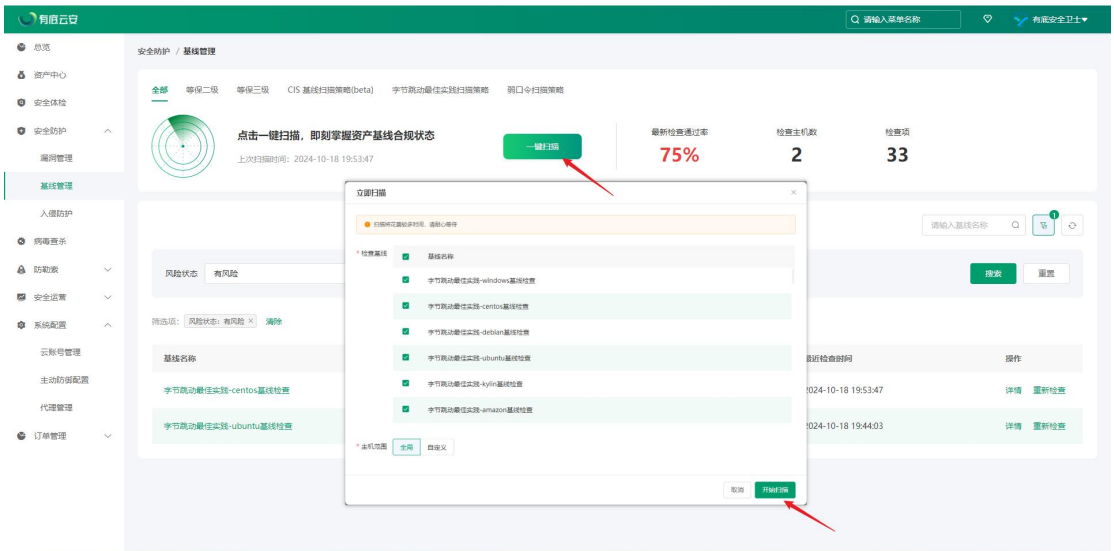
2.5.4.2. 基线管理

攻击者经常利用系统中的弱口令和配置缺陷来获取系统访问权限，进而危害企业的信息安全。

基线检查功能不仅支持对弱口令进行全面检查，还能帮助系统符合等保二级、三级的安全标准，以及 CIS 和字节跳动专家推荐的安全基线。该功能可以帮助企业及时发现并整改安全弱点，加固系统防护，满足法规合规性需求。

2. 5. 4. 2. 1. 扫描基线

在基线扫描页面点击‘一键扫描’按钮，选择扫描的基线名称和扫描的主机范围，点击‘开始扫描’即可开始扫描。

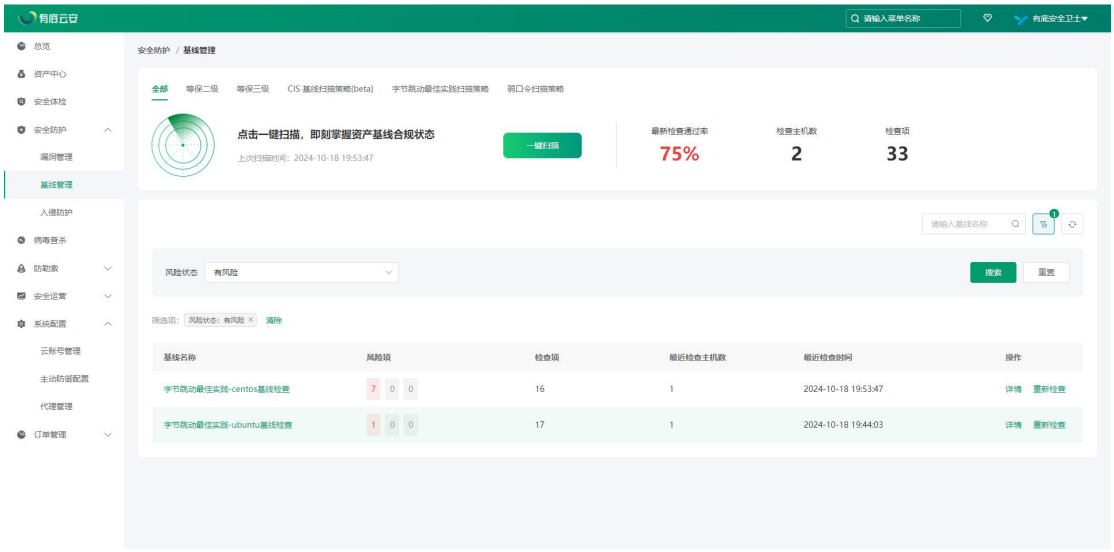


2.5.4.2.2. 查看基线

基线概览展示所有基线检查结果的统计信息。

基线列表会依据检查策略分为不同的页签。列表默认展示有风险的基线，其他状态的基线可手动筛选展示。基线列表以检查策略为视角进行聚合，一个基线检查策略可能影响多个资产。

注：通过率=通过项数量/总检查项数量*100%

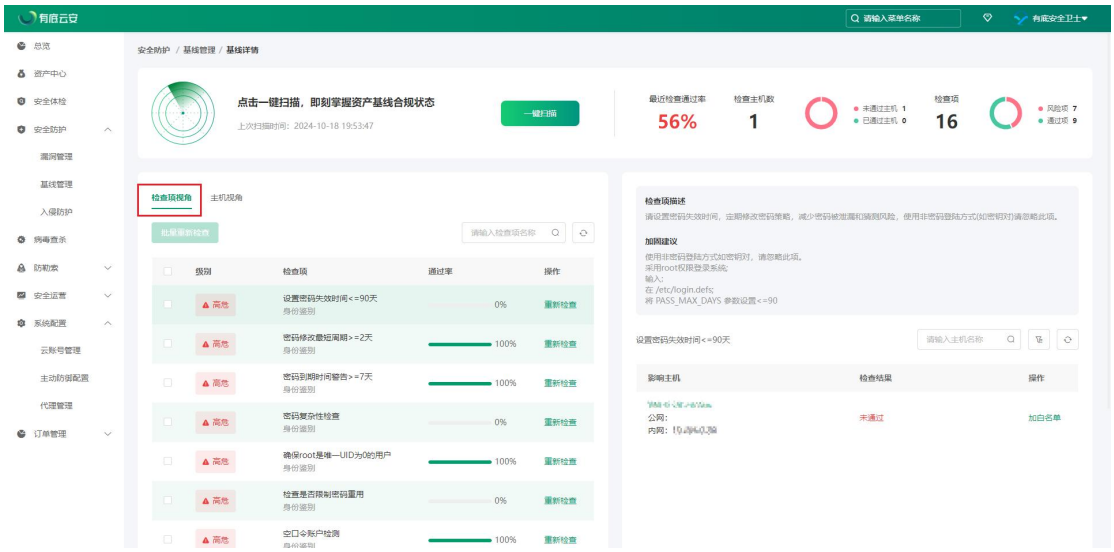


点击基线名称可进入基线详情页面，详情页面分为检查项视角和主机视角。

检查项视角

检查项视角是指按不同的检查项呈现基线检查的结果，切换不同的检查项可以查看该检查项影响的所有主机信息。

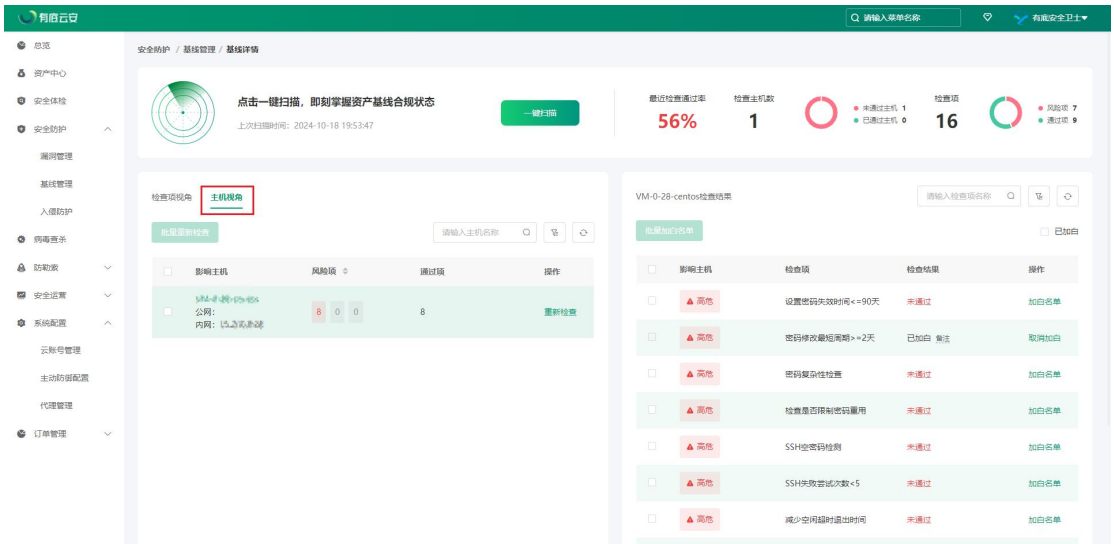
选择检查项视角，单击目标检查项可在右侧查看对应的加固建议及受影响的主机信息。



主机视角

主机视角是指按不同的主机呈现基线检查的结果，切换不同的主机可以查看该主机相关的所有基线检查项的检查结果。

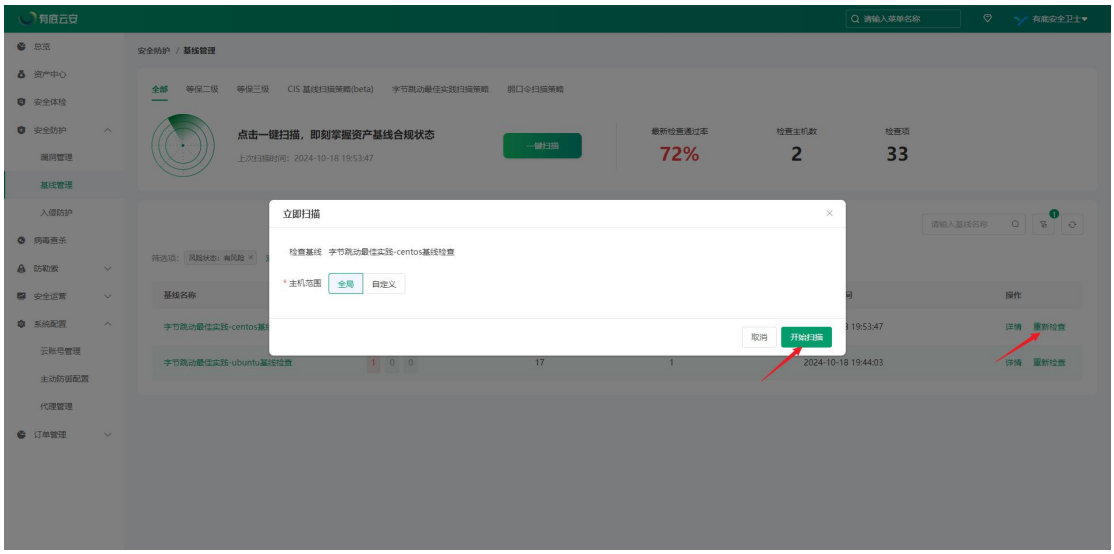
选择主机视角，单击目标主机可在右侧页面查看该主机的各个检查项结果。



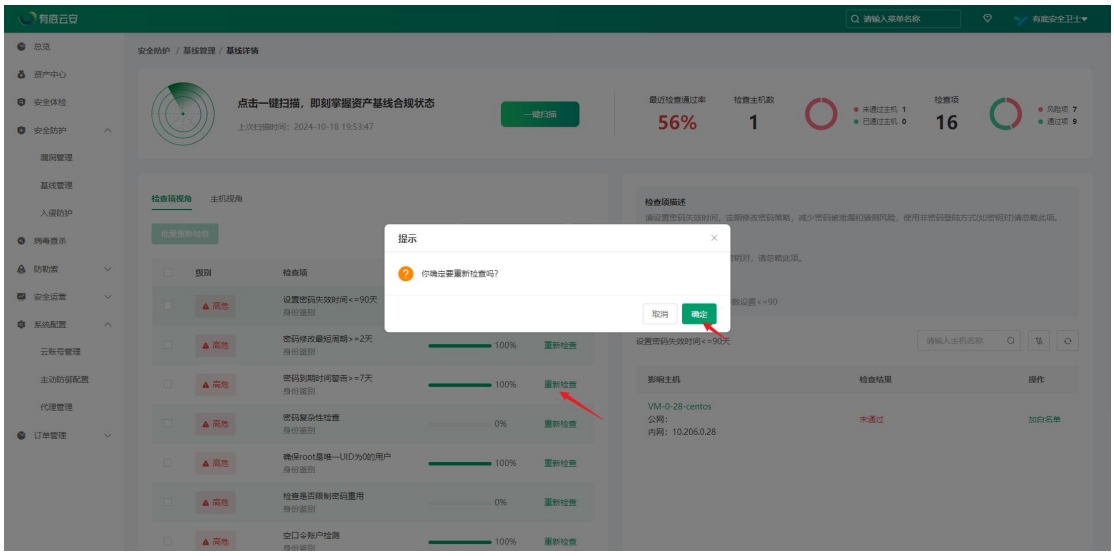
2.5.4.2.3. 处理基线

重新检查

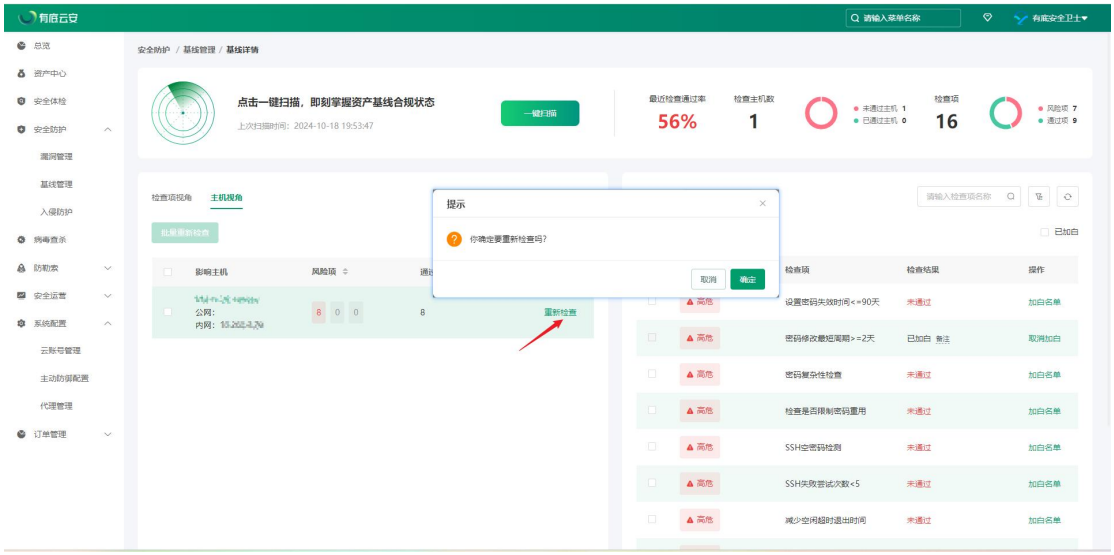
在基线管理页面，点击某条基线后面的‘重新检查’按钮，选择主机范围，可进行重新检查。



在基线详情页面，点击检查项视角的任一基线的‘重新检查’按钮，可重新检查该检查项的所有主机。

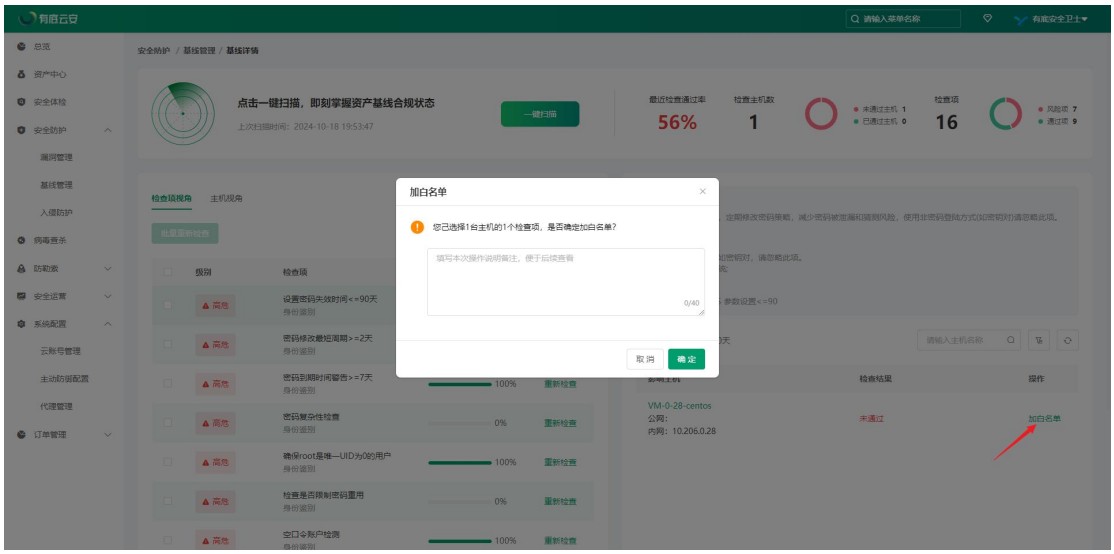


在基线详情页面，点击主机视角的任一主机的‘重新检查’按钮，可重新检查该主机的所有检查项。



添加白名单

如果您希望不再上报该资产的该检查项风险，可选择页面右侧选择目标主机与检查项，点击‘加白名单’按钮即可加入白名单。



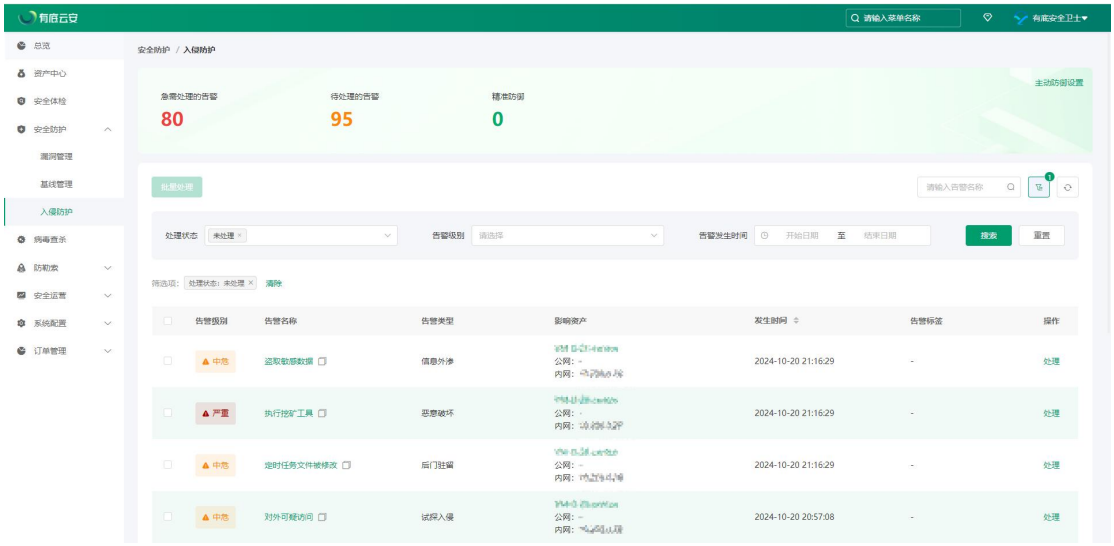
2.5.4.3. 入侵防护

安全告警是有底安全卫士检测到工作负载中存在的威胁而产生的告警，这些威胁可以是某个恶意 IP 对您资产进行的攻击，也可以是您资产中已被入侵的异常情况，例如您的主机在执行恶意脚本或访问恶意下载源等。安全告警页面可管理当前账号下主机和容器内发生的入侵检测告警。

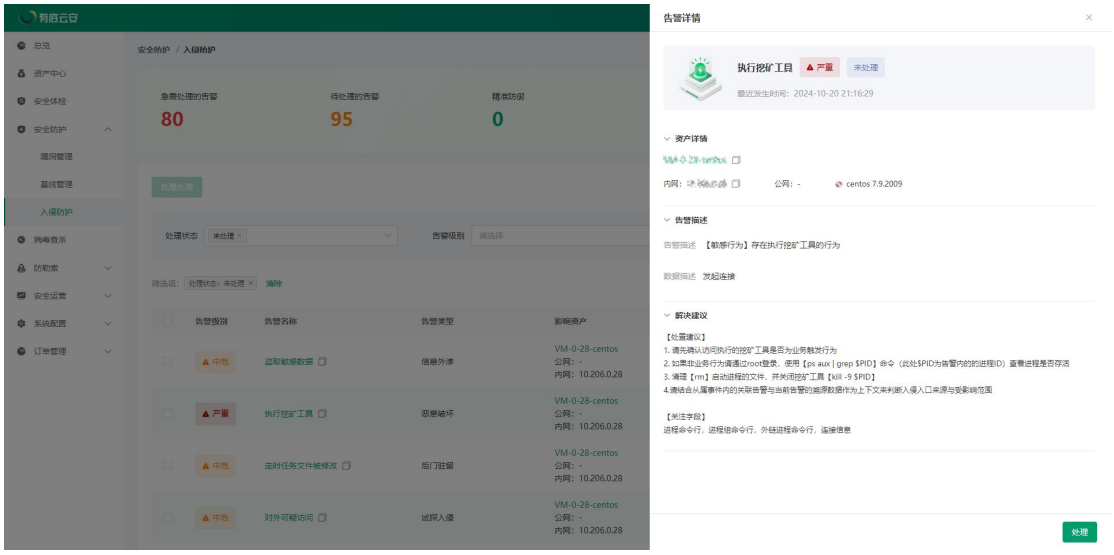
2.5.4.3.1. 查看告警

告警概览板块可展示所有安全告警的统计信息。

告警列表板块默认显示未处理的安全告警信息，包括告警级别、告警名称、告警类型、影响资产、发生时间、告警标签等。列表默认展示未处理的告警，其他状态的告警可手动筛选展示。



单击告警名称可查看告警具体信息，包括受影响主机的资产信息、告警详情以及处置建议等。

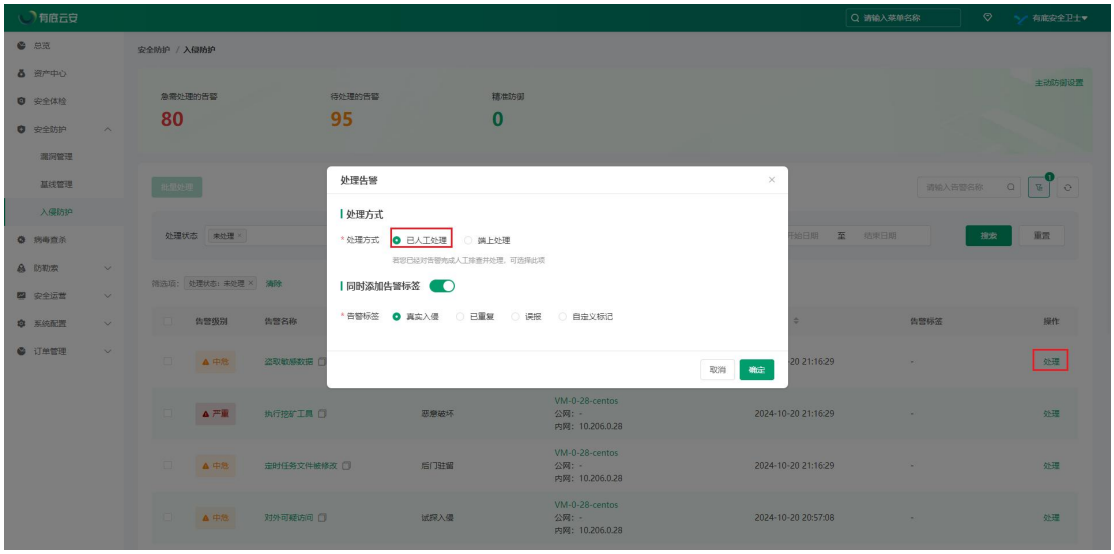


2.5.4.3.2. 处理告警

在入侵防护页面，可选择未处理的风险，点击‘处理’按钮对其进行处理。处理方式分为已人工处理和端上处理。

已人工处理

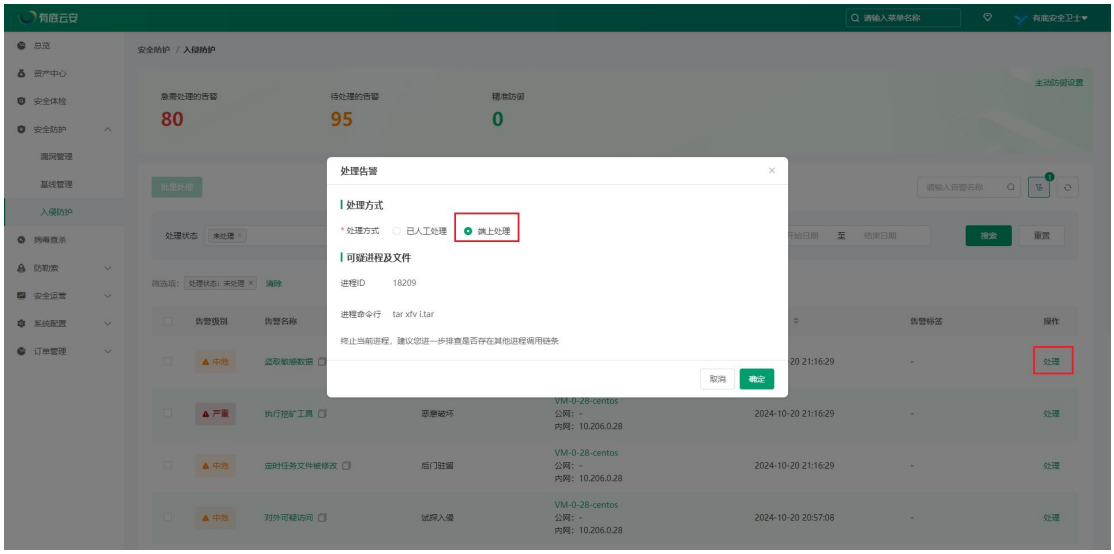
已人工处理操作会将此告警的处理状态变更为已处理，处理结果变更为已人工处理，同时可依据自身需要为告警添加标签，便于后续查找与管理。



端上处理

端上处理支持一键终止进程和隔离文件两种操作，不同的告警类型支持不同的处理方式。处理后可在已处理列表查看详细处理结果。

注：只有 Linux 支持端上处理（告警类型不等于杀伤链），Windows 不支持



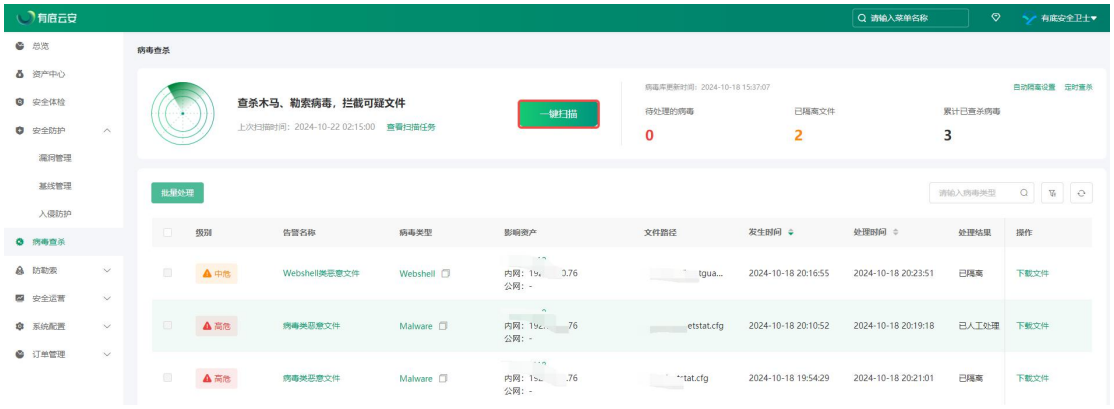
2.5.5. 病毒查杀

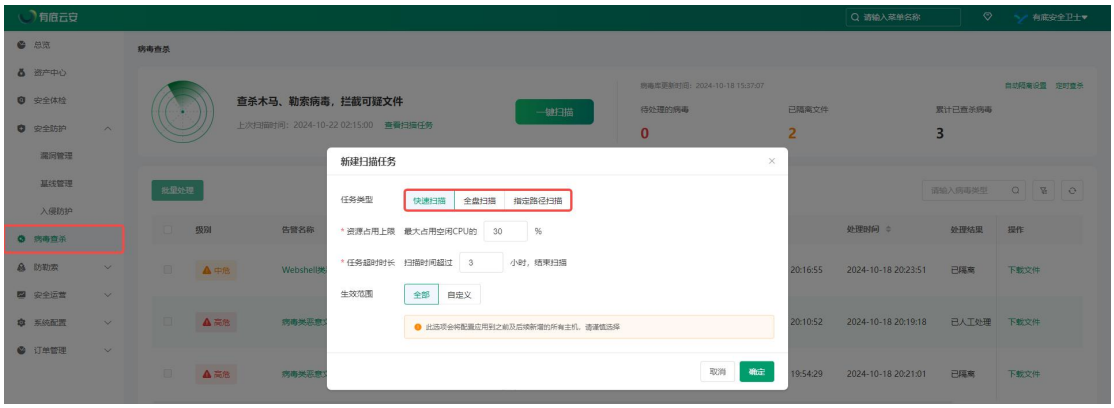
攻击者往往利用病毒木马、Webshell 等恶意软件，暗中窃取数据、控制主机甚至破坏系统。有底安全卫士病毒查杀解决方案则融合了复合病毒检测引擎、动

态行为沙箱、威胁情报及人工智能技术，能够迅速而准确地发现并清除主机内的恶意文件，不仅显著增强业务系统的安全防护能力，更助力企业轻松满足相关安全合规要求。

2.5.5.1. 一键扫描

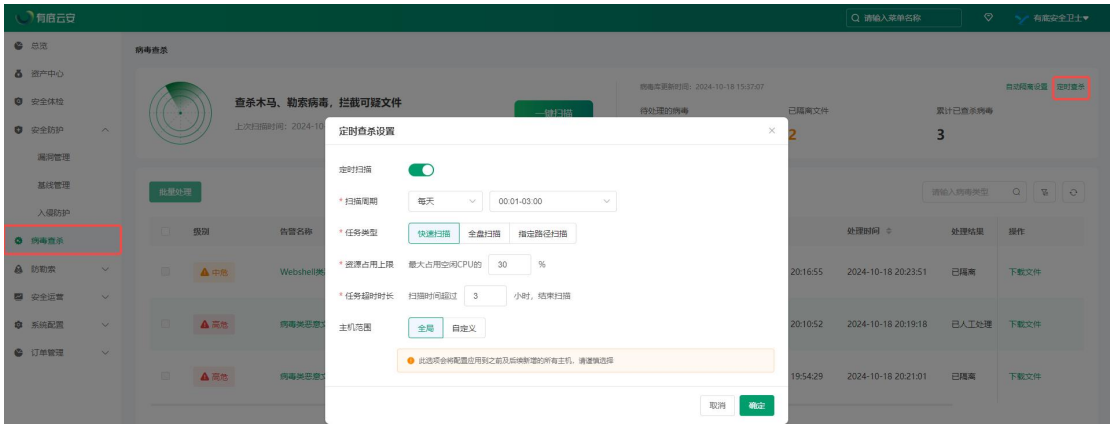
在病毒查杀页面可以点击‘一键扫描’按钮进行扫描，任务类型有快速扫描、全盘扫描、指定路径扫描。





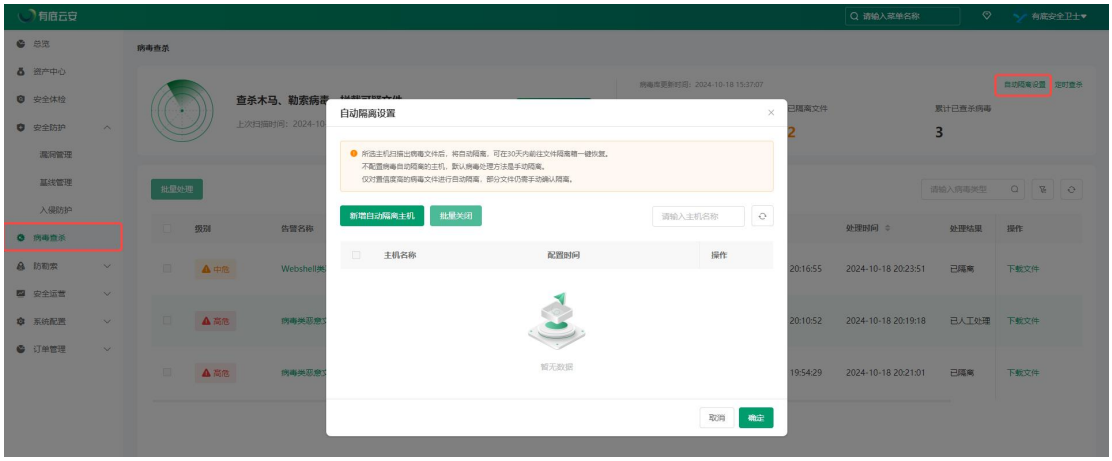
2.5.5.2. 定时查杀

在病毒查杀页面可以点击‘定时查杀’按钮，可对定时查杀自动运行进行设置，任务类型有快速扫描、全盘扫描、指定路径扫描。



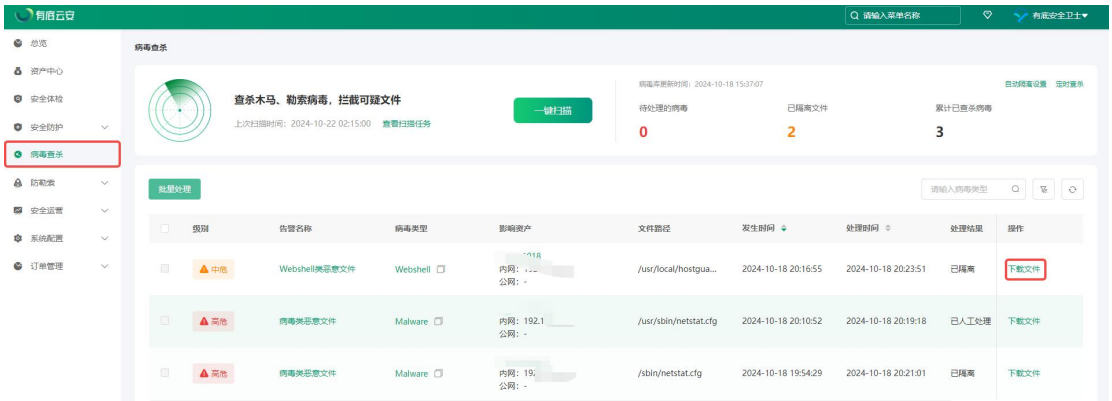
2.5.5.3. 自动隔离设置

在病毒查杀页面可以点击‘自动隔离设置’按钮，可对查杀主机运行进行文件自动隔离。



2.5.5.4. 下载文件

在病毒查杀页面可以点击‘下载文件’按钮，可对查杀文件进行下载。



2.5.6. 防勒索

2.5.6.1. 勒索防护

勒索防护功能强大，智能备份让您无忧。自动将数据存储至云盘，有效抵御勒索攻击与意外损失，全方位保障您的数据安全。

注：智能备份数据默认每天凌晨 2 点备份一次，可手动点击‘同步最新资产’实时同步数据。

关键字解释：

3 天备份覆盖率：统计 3 天内有进行备份的资源（3 天内有进行最少一次备份）占所有资源的比率

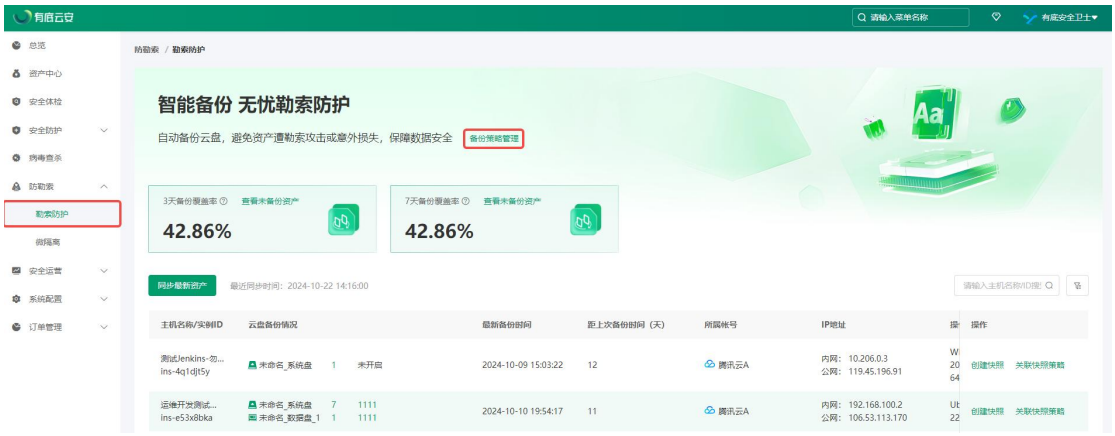
7 天备份覆盖率：统计 7 天内有进行备份的资源（7 天内有进行最少一次备份）占所有资源的比率

2.5.6.1.1. 同步最新资产

在勒索防护页面可以点击‘同步最新资产’按钮，即可同步最新智能备份数据。

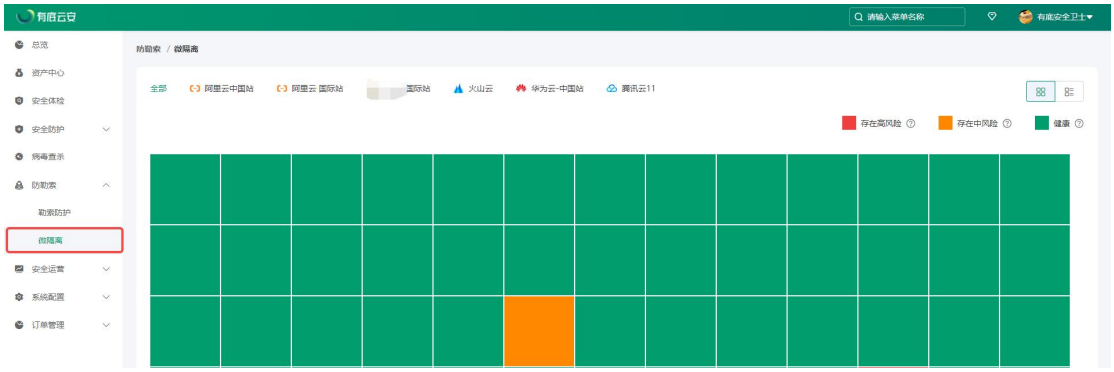
2.5.6.1.2. 备份策略管理

在勒索防护页面可以点击‘备份策略管理’按钮，即可创建及设置备份策略。



2.5.6.2. 微隔离

进入微隔离页面默认以矩阵视图展示，可点击矩阵视图进入到安全详情。



风险解释：

高风险：安全组入站规则存在对全部 IP 开放全部端口，建议最小化授权。

中风险：安全组入站规则存在对全部 IP 开放敏感端口(如 21，22，23，53，123，3891443，1521，3306，3389，5432，6379，27017)，建议最小化授权。

健康：符合最小化授权。

可切换表格视图，查看安全组详情信息，可进行安全组删除操作。

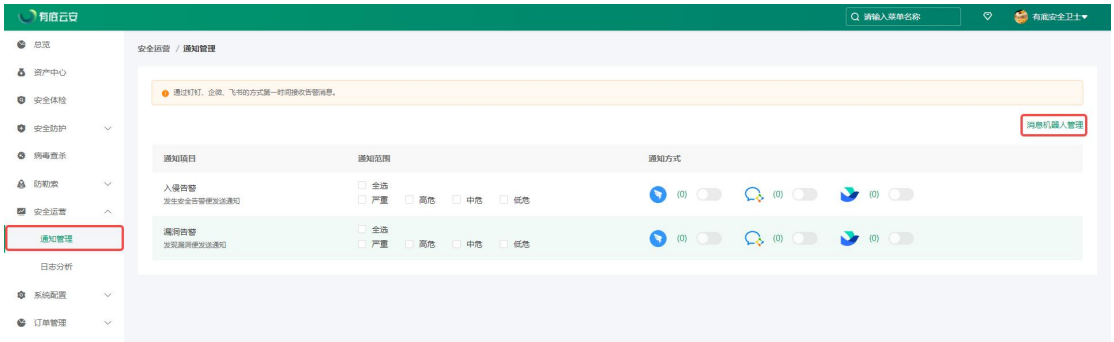
2.5.7. 安全运营

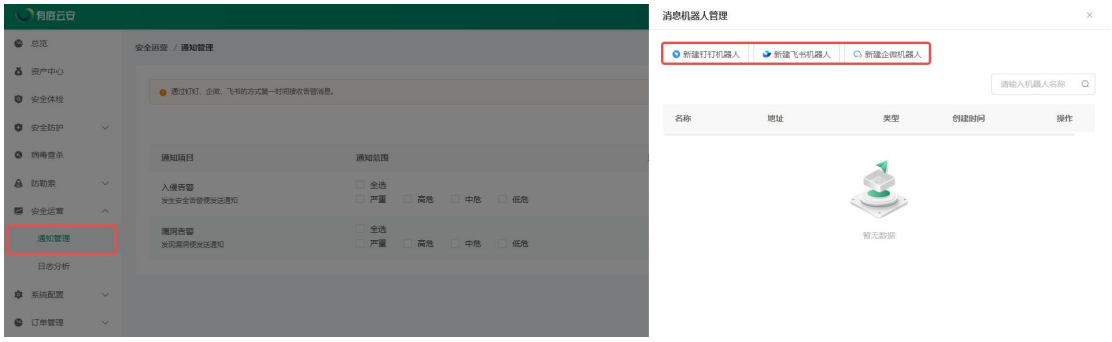
2.5.7.1. 通知管理

通知管理支持通过钉钉、企业微信及飞书接收告警消息。

2.5.7.1.1. 添加机器人管理

点击消息机器人管理，弹出消息机器人管理弹窗，用户可选择钉钉机器人、企微机器人、飞书机器人添加。





2.5.7.2. 日志分析

日志分析页面提供精准、实时的日志审计和高效的分析能力，可灵活设置报警，实现深入的数据分析与监控。

进入日志分析页面时，若默认未开通相关权益，请致电客服热线进行开通。

开通日志分析权益后，进入日志分析可实时查看日志信息。

2. 5. 8. 系统配置

2.5.8.1. 云账号管理

云账号管理模块展示客户接入的所有云账号，显示添加云账号按钮；添加云账号成功后，页面显示云账号列表，列表展示云厂商信息以及同步的云服务器、

快照、快照策略、对象存储的数量。在云账号管理列表页面，用户可以进行添加云账号、搜索云账号、导出云账号资源、刷新列表、同步云账号信息和删除等操作。

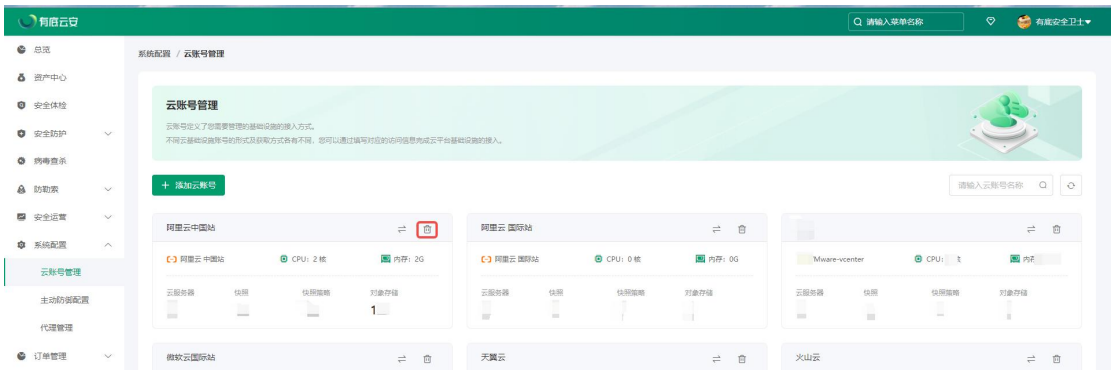
2.5.8.1.1. 添加云账号

点击添加云账号，弹出添加云账号弹窗，用户可以选择自动配置方案或手动配置方案添加接入云厂商。系统现支持接入阿里云中国站、阿里云国际站、腾讯云、华为云中国站、华为云国际站和火山云。

注：选择自动配置方案接入 AK，接入成功后系统将在主账号下自动创建一个新的 AK。

2. 5. 8. 1. 2. 删除云账号

在云账号管理列表页面，鼠标上移至选项卡右上角可进行删除操作。点击删除按钮，弹出二次确认框，点击确认，该云账号则被删除。



2.5.8.2. 主动防御配置

主动防御配置允许用户对威胁灵活配置，包括编辑、添加或移除主机数，以及操作开关威胁内容策略。

注：修改主动防御配置预计需要 5 分钟生效。

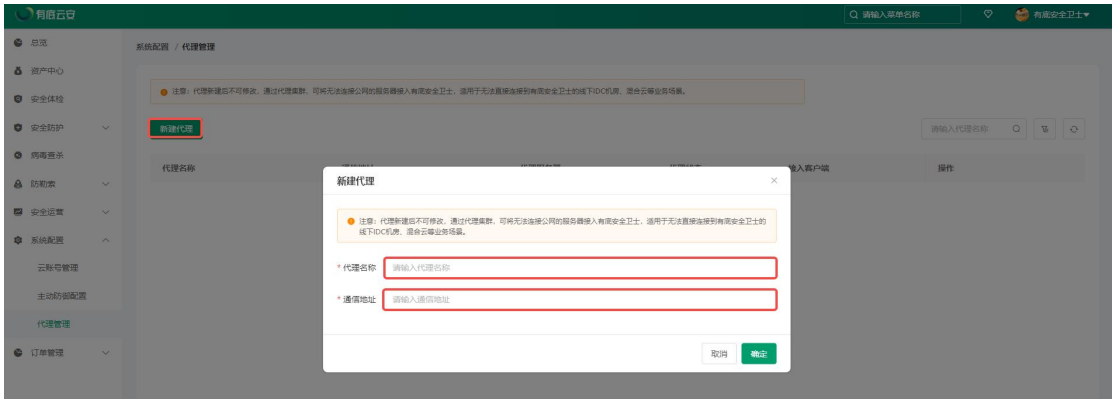
2.5.8.3. 代理管理

通过代理管理，可将无法连接公网的服务器接入有底安全卫士，适用于无法直接连接到有底安全卫士的线下 IDC 机房、混合云等业务场景。

2.5.8.3.1. 新建代理

点击新建代理按钮，输入代理名称、通讯地址，点击‘确定’按钮，可新建代理成功。

注：代理名称不可重复，通讯地址可输入 IP 地址或域名



2.5.8.3.2. 部署安装/卸载代理

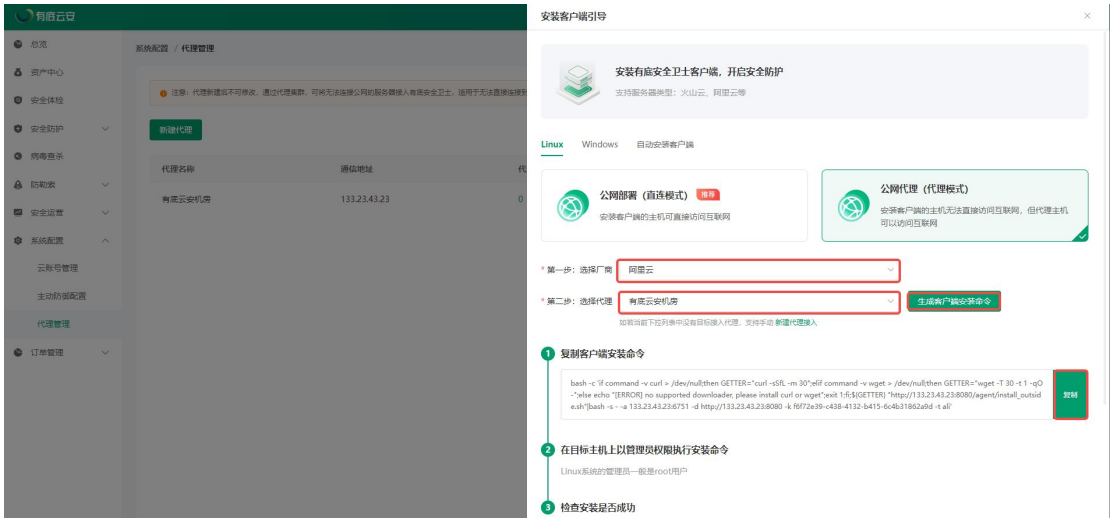
点击‘部署代理’弹出部署代理窗口安装/卸载命令，在代理服务器上执行命令安装代理。

注：执行命令后需要等待 1-5 分钟，刷新列表代理服务器才会显示。

2.5.8.3.3. 接入客户端

点击‘接入客户端’弹出安装客户端引导，‘接入代理’默认选中当前代理。

注：执行命令后需要等待 1-5 分钟，刷新列表接入客户端才会显示。



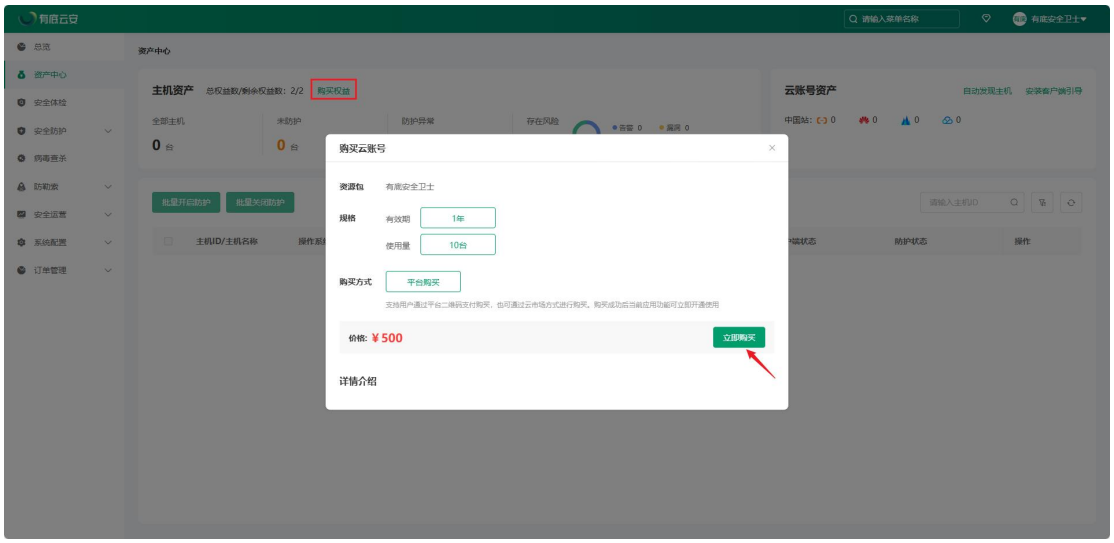
2.5.9. 订单管理

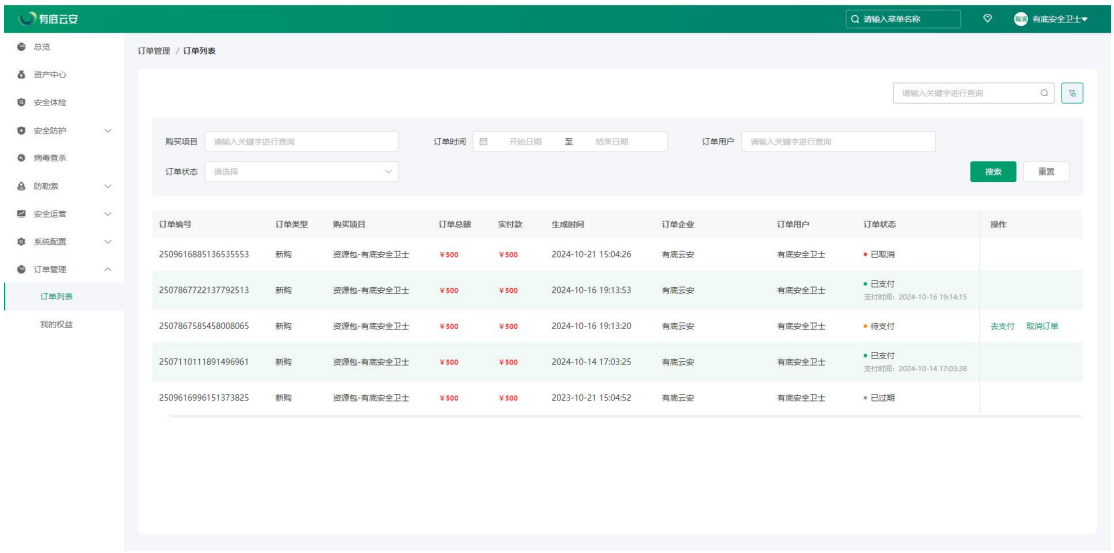
2.5.9.1. 订单列表

在使用有底安全卫士进行权益购买时，点击‘立即购买’后不管是否进行付款，系统均会自动在订单列表中生成相应的订单记录。这些记录以直观的形式展示详细的订单明细数据。列表还支持按订单 ID、购买项目、订单时间、订单用户和订单状态进行搜索筛选。

此外，您还可以对这些订单进行操作，目前暂只支持微信扫码支付。生成的未支付订单可以取消，取消后订单不会从订单列表删除，订单状态变为已取消，无法操作；若未支付订单在 60 天内没有完成支付，订单状态将会转为已过期，

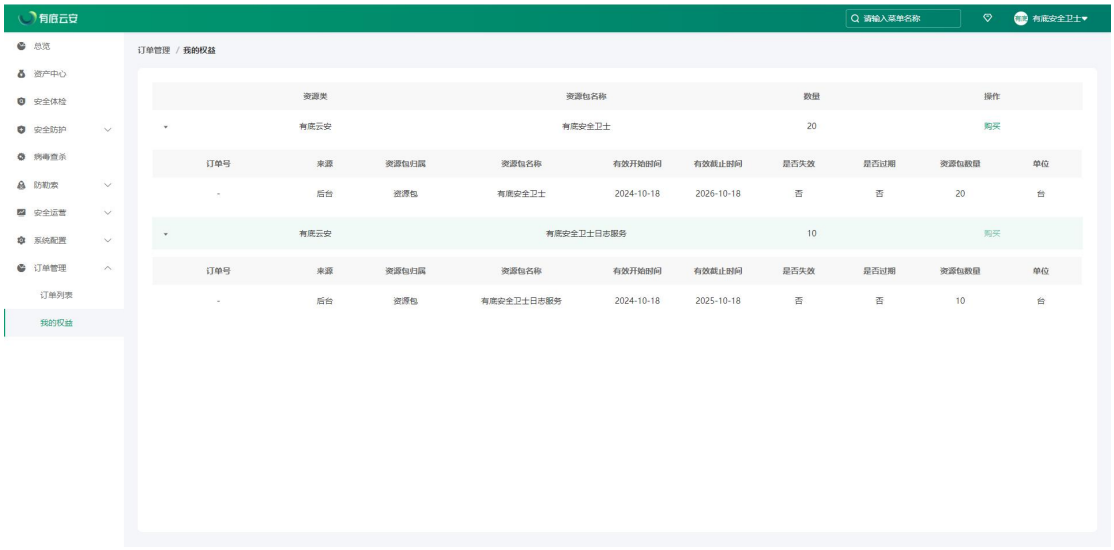
无法再进行操作，需重新下单。



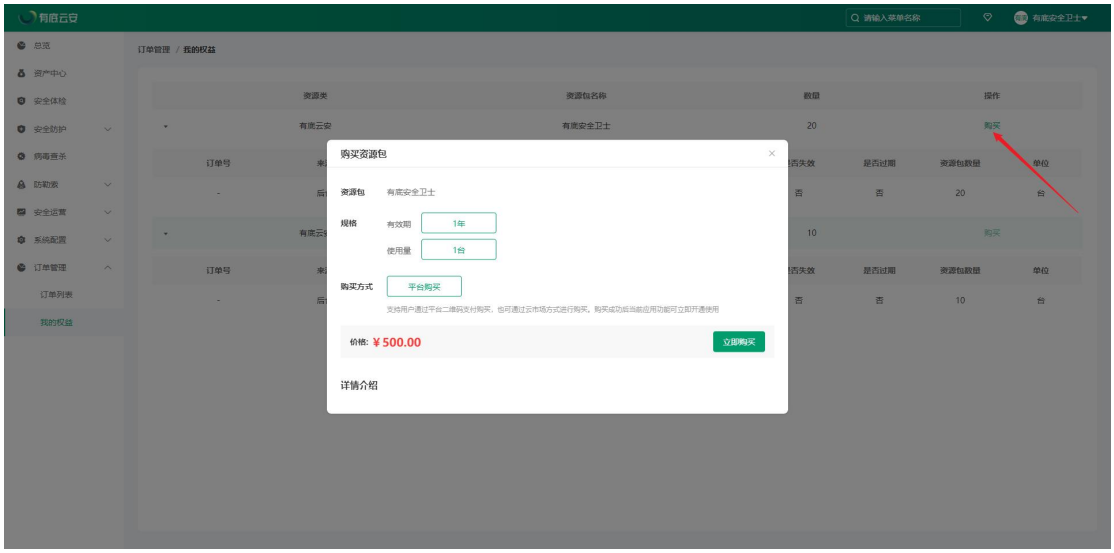


2.5.9.2. 我的权益

我的权益页面将展示此账号的所有权益，详细列表清晰展现每项权益的具体数据。



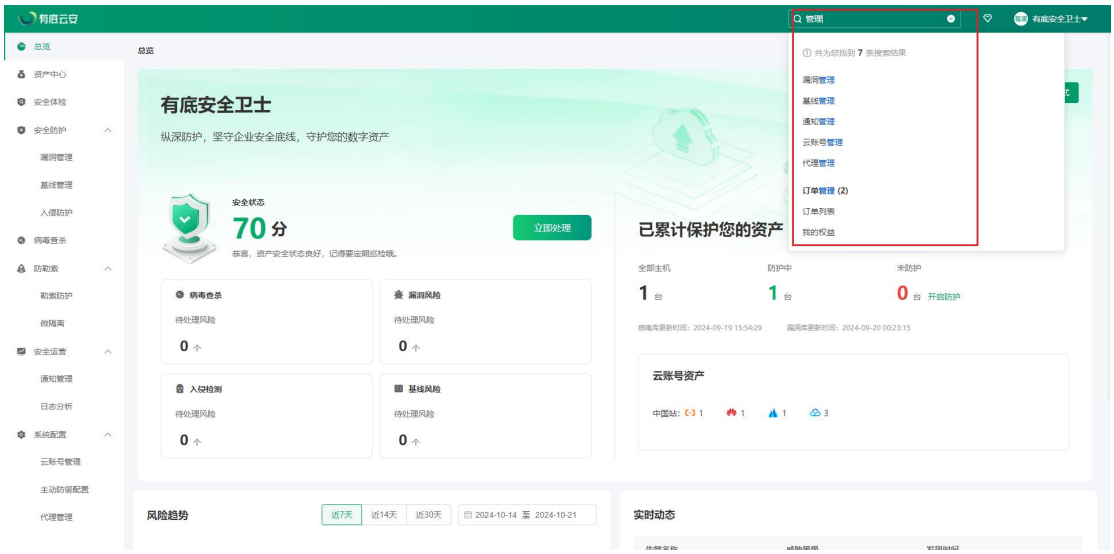
可点击操作界面下方的‘购买’按钮，即可快速购买对应权益项的专属权益。



2.6. 其他

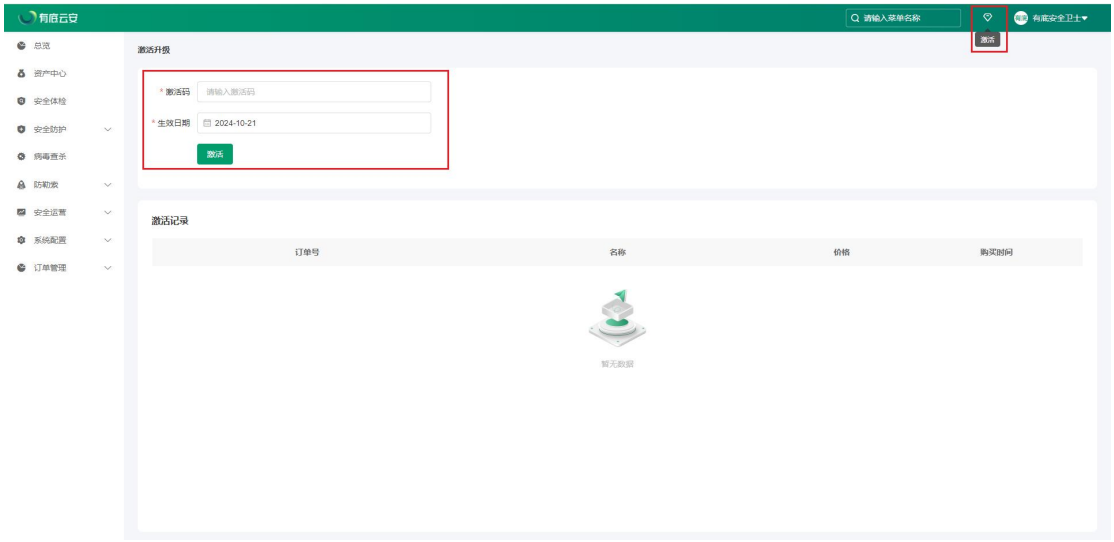
2.6.1. 全局搜索框

用户可在有底安全卫士首页搜索框输入菜单关键词，系统即自动识别并展示相关菜单结果。点击任一搜索结果，即可跳转至对应页面进行查看或操作。



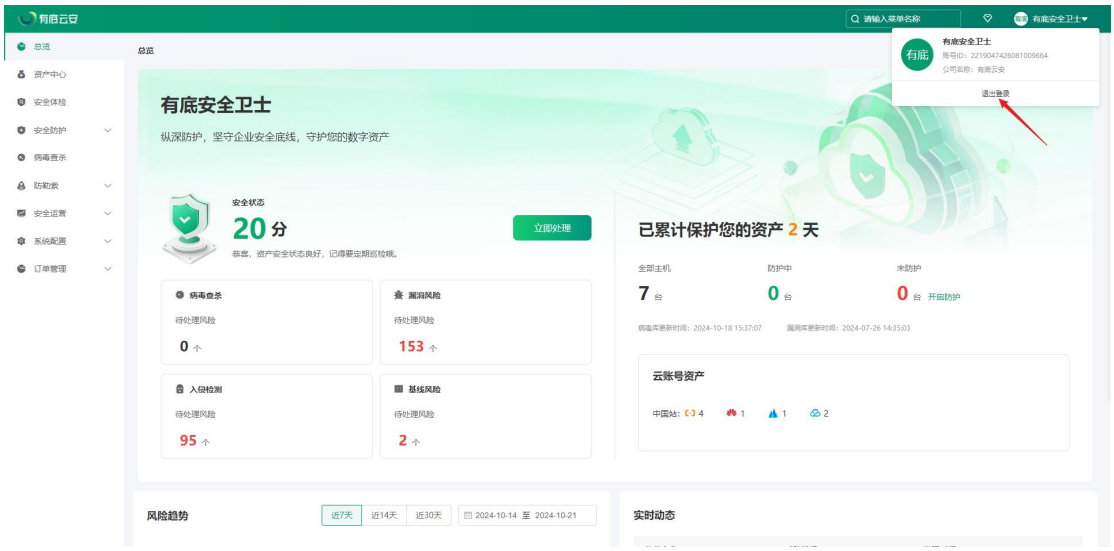
2.6.2. 激活

在云市场购买有底安全卫士权益后，您可通过有底安全卫士首页的导航栏，点击‘激活’按钮，快速跳转至激活页面，并复制所获取的激活码，粘贴确定即可激活您的有底安全卫士权益。



2.6.3. 退出

在有底安全卫士首页的导航栏中，鼠标移入‘账号信息’选项，再点击‘退出登录’按钮即可成功退出。


有底云安
请输入菜单名称
有底安全卫士
有底安全卫士
账号ID：2219047426081009664
公司名称：有底云安
退出登录
总览
资产中心
安全体检
安全防护
病毒查杀
防勒索
安全运营
系统配置
订单管理
总览
有底安全卫士
纵深防护，坚守企业安全底线，守护您的数字资产
安全状态
20 分
恭喜，资产安全状态良好，记得要定期巡检哦。
立即处理
已累计保护您的资产 2 天
全部主机
7 台
防护中
0 台
未防护
0 台 开启防护
病毒库更新时间：2024-10-18 15:37:07
漏洞库更新时间：2024-07-26 14:35:03
病毒查杀
待处理风险
0 个
漏洞风险
待处理风险
153 个
入侵检测
待处理风险
95 个
基线风险
待处理风险
2 个
云账号资产
中国站：4 1 1 2
风险趋势
近7天
近14天
近30天
2024-10-14 至 2024-10-21
实时动态